ReSPA
Shkolla Rajonale
e Administratës Publike

Keqpërdorimi i Teknologjisë së Informacionit (IT) për Qëllime Korrupsioni

Aktivitetet e ReSPA-s
financohen nga BE

ReSPA është një nismë e përbashkët e Bashkimit Europian dhe vendeve të Ballkanit Perëndimor që punojnë së bashku për nxitjen dhe forcimin e bashkëpunimit rajonal në fushën e administratës publike mes Shteteve të saj Anëtare. Ajo synon të ofrojë aktivitete trajnuese të shkëlqyera, inovative dhe krijuese, aktivitete të rrjetëzimit, shërbime për ngritjen e kapaciteteve dhe konsulencë për të garantuar që vlerat e përbashkëta të respektit, tolerancës, bashkëpunimit dhe integrimit të riafirmohen dhe zbatohen në të gjitha administratat publike në rajon.

KONTAKTI
Regional School of Public Administration
Branelovica
P.O.Box 31,81410
Danilovgrad, Montenegro
Telefoni: +382 (0)20 817 200
Internet: www.respaweb.eu
E-mail: respa-info@respaweb.eu

CIP – Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-9940-37-004-6
COBISS.CG-ID 29075472

Autorët

ReSPA

Goran Pastrovic, *Drejtues Trajnimi*

Autorë ndërkombëtarë

Hyrja, Panorama e përgjithshme për Kapitujt 1 dhe 2, nënkapitulli 2.9 & Kapitulli 3

Tilman Hoppe, *ekspert i antikorrupsionit*
Vera Devine, *ekspert i antikorrupsionit*
Louise Thomasen, *ekspert i eGovernment*

Autorë vendas

Shqipëri

Edlira Nasi, *eksperte e antikorrupsionit*
Ened Kercini, *ekspert i qeverisjes elektronike*

Bosnjë dhe Hercegovinë

Aleksandra Martinovic, *eksperte e antikorrupsionit*
Srdjan Nogo, *ekspert i qeverisjes elektronike*

Kroaci

Zorislav Petrovic, *ekspert i antikorrupsionit*
Ivana Andrijasevic, *ekspert i qeverisjes elektronike*

Kosovë

Hasan Preteni, *ekspert i antikorrupsionit*
Driart Elshani, *ekspert i qeverisjes elektronike*

Maqedoni

Marjan Stoilkovski, *ekspert i antikorrupsionit*
Rozalinda Stojova, *ekspert i qeverisjes elektronike*

Mali i Zi

Dusan Drakic, *ekspert i antikorrupsionit*
Ivan Lazarevic, *ekspert i qeverisjes elektronike*

Serbi

Nemanja Nenadic, *eksperte e antikorrupsionit*
Bojan Cvetkovic, *ekspert i qeverisjes elektronike*

* Ky emërtim është pa asnjë paragjykim për pozicionin mbi statusin dhe është në përputhje me Rezolutën 1244 të Këshillit të Sigurimit të OKB-së dhe opinionin e Gjykatës Ndërkombëtare të Drejtësisë (ICJ) mbi Deklaratën e Pavarësisë së Kosovës.

Parathënie

Nga Suad Music,
Drejtor i ReSPA-s

Konventa e Kombeve të Bashkuara kundër Korrupsionit (UNCAC) në Nenin 48, pika 3 të saj parashikon:

“Shtetet Palë përpiqen të bashkëpunojnë në mënyrë që t’u përgjigjen krimeve të mbuluara nga kjo Konventë të kryera nëpërmjet përdorimit të teknologjive moderne.”

Deri më sot, kësaj dispozite nuk i është kushtuar shumë vëmendje nga organizatat ndër-kombëtare. Në fakt, Udhëzuesi Teknik mbi zbatimin e UNCAC[1] përmban si udhëzim të vetëm shprehjen e mëposhtme:

“Paragrafi 3 (i Nenit 48) pranon rritjen e përdorimit të teknologjive për të kryer shumë prej krimeve të mbuluara nga Konventa dhe iu bën thirrje Shteteve Palë të përpiqen të bashkëpunojnë më nga afër me qëllim që t’u përgjigjen krimeve të lidhura me korrupsionin të kryera nëpërmjet përdorimit të teknologjive moderne.”

Ky studim krahasues synon të ofrojë për herë të parë udhëzime konkrete duke treguar raste të keqpërdorimit të “teknologjive moderne” (IT) për kryerjen e veprës penale të korrupsionit dhe hapat e mundshëm që mund të ndërmerren për t’u mbrojtur kundër ke-qpërdorimeve të tilla.

ReSPA ka qenë aktive për vite të tëra në të dyja fushat – integriteti dhe qeverisja elektronike (e-government). Me rrjetet e saj rajonale të ekspertëve për të dyja çështjet, ajo është në një pozitë të shkëlqyer që t’i trajtojë të dyja disiplinat së bashku për përfitim reciprok. Në dritën e rëndësisë së tij për zbatimin e UNCAC-ut, efekti i këtij studimi do të prekë rajonin e Ballkanit Perëndimor dhe njëkohësisht do të ketë efekt ndërkombëtar edhe përtej rajonit në secilin prej 172 vendeve që janë Shtete Palë në UNCAC.

1 Nga UNODC, 2009, www.unodc.org/unodc/en/treaties/CAC/technical-guide.html.

Tabela e përmbajtjes

Shkurtimet

Më poshtë është një listë me rend alfabetik me shkurtimet dhe kuptimet e tyre të përdorura në këtë raport.

	Udhëzim Administrativ
	Shkolla e Administratës Publike në Shqipëri
	Bosnja dhe Hercegovina
	Autoriteti Çertifikues (Maqedoni)
	Rrjeti Akademik dhe Studimor në Kroaci
	Televizioni me qark të mbyllur
	Ekipi i Reagimit të Emergjencave kompjuterike
	Sistemi i Mbrojtjes së Identifikimit të Qytetarëve (Bosnjë dhe Hercegovinë)
	Qendra e Komandës së Operacioneve (Serbi)
	Indeksi i Perceptimit të Korrupsionit
	Ekipi i Reagimit ndaj Incidentit të Sigurisë Kompjuterike
	Autoriteti i Aviacionit Civil (Shqipëri)
	Mohimi i Shpërndarjes së Shërbimit
	Departamenti i Krimit Ekonomik (Kroaci)
	Sistemi i Menaxhimit të Dokumentit
	Zyra e Prokurorit të Shtetit në Bashkinë e Dubrovnikut
	Pagesa elektronike për autostradën (Serbi)
	Enti Rregullator i Energjisë në Shqipëri
	Europa Juglindore Elektronike
	Bashkimi Europian
	Misioni Policor i Bashkimit Europian në Bosnjë dhe Hercegovinë
	Protokolli për Transferimin e Dosjes
	Kompania kroate e Autostradave Ltd.
	Bashkimi Demokrat Kroat
	Këshilli i Lartë i Gjyqësorit dhe Prokurorisë (Bosnjë dhe Hercegovinë)
IDS	Sistemi i Zbulimit të Ndërhyrjes
IMPACT	Partneriteti Ndërkombëtar Shumëpalësh kundër kërcënimeve kibernetike
IPA	Instrumenti për asistencën e para pranimit (Bosnja dhe Hercegovina)
ISO	Organizata për Standardet Ndërkombëtare
ISP	Ofruesi i Shërbimit të Internetit
IT	Teknologjia e Informacionit
JPTC	Qendra e Trajnimit të Gjyqësorit dhe Prokurorisë (Bosnjë dhe Hercegovinë)
MIST	Ministria e Shoqërisë së Informacionit dhe Telekomunikimeve
MLSP	Ministria e Punës dhe e Politikave Sociale (Maqedoni)
MoD	Ministria e Mbrojtjes
MoI	Ministria e Brendshme
MoJ	Ministria e Drejtësisë
MoJPA	Ministria e Drejtësisë dhe e Administratës Publike (Serbi)
MPALSGHR	Ministria e Administratës Publike, Vetëqeverisjes Vendore dhe e të Drejtave të Njeriut (Serbi)
MUP	Ministria e Brendshme (Kroaci)
NACS	Agjencia Kombëtare për Sigurinë Kompjuterike (Shqipëri)
NAIS	Agjencia Kombëtare e Shoqërisë së Informacionit (Shqipëri)
NDA	Marrëveshja e Moszbulimit
NFC	Komunikimi në terren
NGO	Organizatë Joqeveritare
OIB	Numri Personal i Identifikimit (Kroaci)
PARCO	Zyra për Reformën e Administratës Publike (Bosnjë dhe Hercegovinë)
PDA	Asistenti Personal Dixhital
PKI	Infrastruktura kryesore publike
PRO	Zyra e të ardhurave publike (Maqedoni)
SAI BiH	Institucioni i Lartë i Auditimit i Bosnjës dhe Hercegovinës
SAI RS	Institucioni i Lartë i Auditimit i Republikës Srpska
SCPC	Komisioni Shtetëror për Parandalimin e Korrupsionit (Maqedoni)
SDH	Synchronous Digital Hierarchy
SDP	Partia Socialdemokrate (Bosnjë dhe Hercegovinë)
SDS	Partia Demokratike serbe (Bosnjë dhe Hercegovinë)
SIPA	Agjencia Shtetërore e Hetimit dhe Mbrojtjes
SNSD	Partia e Socialdemokratëve të Pavarur (Bosnjë dhe Hercegovinë)
SOA	Agjencia e Sigurisë dhe Inteligjencës (Kroaci)
SOP-s	Procedurat operacionale standard
SSA	Kontrolli i Lartë i Shtetit (Shqipëri)
SSL	Secure Sockets Layer
TCMS	Sistemi i Përgjithshëm i Menaxhimit të Rastit (Bosnjë dhe Hercegovinë)
TIMS	Sistemi i Përgjithshëm i Menaxhimit të Informacionit (Shqipëri, Serbi)
UNODC	Zyra e Kombeve të Bashkuara për Drogat dhe Krimin
USKOK	Zyra kroate për Luftën kundër Korrupsionit dhe Krimit të Organizuar
VM	Ministria e Veteranëve (Kroaci)
VPN	Rrjeti Virtual Privat
VSOA	Agjencia për Sigurinë dhe Inteligjencën Ushtarake (Kroaci)
WAN	Rrjeti i Zonës së Gjerë

Hyrje

Nga Tilman Hoppe

Botime të shumta ka për çështjen se si mund të **parandalohet** korrupsioni përmes përdorimit të mirë të IT-së, të tilla si regjistrat publikë online, transparenca e deklaratave të pasurisë, ose prokurimi në formë elektronike (e-procurement). Botimet e mëposhtme janë shembuj të spikatur të shqyrtimit të metodave që përdorin IT për luftën kundër korrupsionit:

- Tim Davies/Silvana Fumega, "Mixed incentives: Adopting ICT innovations for transparency, accountability, and anti-corruption", U4 Numri 2014:4, 38 faqe[2]
- UNDP, "Fighting Corruption with e-Government Applications", APDIP e-Note 8/2006, 4 faqe[3]
- Spider, "Increasing Transparency & Fighting Corruption Through ICT - Empowering People & Communities", ICT4D Series nr. 3/2010, 102 faqe[4]
- Spider, "ICT for Anti-Corruption, Democracy and Education in East Africa", Spider ICT4D Series nr. 6/2013, 96 faqe[5]
- Jamshed J. Mistry/Abu Jalal, "An Empirical Analysis of the Relationship between e-government and Corruption", The International Journal of Digital Accounting Research, Vëllimi. 12, 2012, f. 145-176[6]
- Ionescu, Luminita, "The Impact That E-Government Can Have on Reducing Corruption and Enhancing Transparency", Economics, Management and Financial Markets, Vëllimi 8, nr. 2, 2013, faqe 210
- Bertot/Jaeger/Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies", Government Information Quarterly Vëllimi. 27 Numri 3, 2010, f. 264
- Richard Heeks, "Information Technology and Public Sector Corruption", Institute for Development Policy and Management, shtator 1998, 15 faqe[7]
- • Transnational Crime and Corruption Centre, "Transnational Crime, Corruption, and Information Technology", Raporti i konferencës 2000, 39 faqe[8]

Megjithatë, për përdorimin e kundërt të IT-së si një **mjet për** korrupsion, ekziston shumë pak, ose nuk ka fare literaturë. "Komisioni i Pavarur kundër Korrupsionit" nëHong-Kong ka botuar:

- "Ethics at Work - A Guide for Business Managers in the Use of IT", 2003, 77 faqe[9], që përqendrohet në sektorin privat.
- Ka vetëm pak raste kur organet antikorrupsion kanë përzgjedhur ICT si rrezik për korrupsion në sektorin publik. Më poshtë janë dy prej atyre pak shembujve:

2 http://www.u4.no/publications/mixed-incentives-adopting-ict-innovations-for-transparen- cy-accountability-and-anti-corruption/.
3 http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043296.pdf.
4 http://spidercentre.org/polopoly_fs/1.163640.1390315885!/menu/standard/file/Spider%20ICT4D%20series%203%20Increasing%20transparency%20and%20fighting%20cor- ruption%20through%20ICT.pdf.
5 http://spidercentre.org/polopoly_fs/1.163057.1390315079!/menu/standard/file/Spi- der%20ICT4D_no6_2013.pdf.
6 www.uhu.es/ijdar/10.4192/1577-8517-v12_6.pdf.
7 http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN015477.pdf.
8 http://traccc.gmu.edu/pdfs/publications/transnational_crime_publications/variou01.pdf.
9 http://www.icac.org.hk/new_icac/files/cms/eng/13857pdf.pdf.

- Komisioni Antikorrupsion në Kenia, "Corruption Prevention Guidelines on ICT Systems in the Public Sector", mars 2008[10]
- Komisioni i Pavaruar kundër Korrupsionit (ICAC) në New South Wales - NSW (Australia), "Knowing your risks: IT systems"[11]

Adresa e internetit e NSW ICAC tregon vetëm dy shembuj të shkurtër të rasteve të korrupsionit në sektorin publik të lidhur me IT. Për më tepër, edhe udhëzuesit e mëposhtëm teknikë mbi korrupsionin të hartuar nga organizata ndërkombëtare e përmendin IT-në si një risk vetëm rrallë ose nuk e përmendin fare:

- UNODC, UN Anti-corruption toolkit (3rd edition 2004)[12];
- UNODC, Technical guide to the UNCAC, 2009[13];
- OSCE, Best practices in combating corruption, 2004[14];
- Transparency International, Confronting corruption: the elements of a national integrity system, TI Source Book 2000[15];
- USAID Corruption Assessment Handbook (2006)[16].

Kjo mungesë e udhëzuesve është në kundërshtim të plotë me "Konventën e Kombeve të Bashkuara kundër Korrupsionit" (UNCAC) e cila në Nenin 48, pika 3 iu bën thirrje Shteteve Palë të"përpiqen të bashkëpunojnë brenda mjeteve të tyre në mënyrë që të u përgjigjen krimeve të mbuluara nga kjo Konventë të kryera nëpërmjet përdorimit të teknologjive moderne." Kështu, një studim rajonal mbi këtë temë është shumë i vonuar.

Lexuesi i këtij studimi mund të përfitojë nga rastet konkrete që tregojnë se si kryerësit e korrupsionit shfrytëzojnë dobësitënë strukturat e IT-së për përfitime të tyre personale. Rastet nga jeta reale si edhe **shembujt e mirë** për parandalimin dhe zbulimin e tyre do të frymëzojnë ekspertët që merren me parandalimin e korrupsionit si edhe ekspertët përgjegjës për sigurinë e IT-së.

Ky studim përqendrohet vetëm tek risqet e korrupsionit që lidhet në mënyrë specifike me IT. Për shembull, prokurimi i korruptuar përmes IT-së ose shitësi i përcaktuar janë risqe për korrupsion që mund të ndodhin edhe me mënyra të tjera, të tilla si prokurimi i trenave për transport publik ose shitësit e mundshëm të përcaktuar. Si rezultat, ato nuk përbëjnë risqe për korrupsion të lidhura vetëm me IT-në.

Pritet që anëtarët e ReSPA-s të kenë qasje dhe përdorime të ndryshme të IT-së. Kështu ata do të mësojnë nga **shkëmbimi** i përvojave të ndihmuar edhe nga ky studim krahasues. Meqënëse ende nuk ka një tipologji të rasteve në literaturën për IT-në ose antikorrupsionin, vlera e shtuar dhe efekti i këtij studimi mund të kalojnë përtej rajonit të ReSPA-s.

10 www.eacc.go.ke/docs/ICT_Guidelines.pdf.
11 http://www.icac.nsw.gov.au/preventing-corruption/knowing-your-risks/it-systems/4911.
12 www.unodc.org/documents/corruption/publications_toolkit_sep04.pdf.
13 www.unodc.org/unodc/en/treaties/CAC/technical-guide.html.
14 www.osce.org/eea/13738.
15 www.transparency.org/publications/sourcebook
16 www.usaid.gov/our_work/democracy_and_governance/technical_areas/anticorruption_ handbook/

1. Raste nga jeta reale mbi keqpërdorimin e IT-së për qëllime korrupsioni

Vështrim i përgjithshëm

Nga Tilman Hoppe dhe Louise Thomasen

Rastet e mëposhtme janë një zgjedhje e rastësishme, jopërfaqësuese, e rasteve nga vendet e rajonit të ReSPA-s. Është e rëndësishme të vihet në dukje se rastet e përshkruara nuk i janë nënshtruar domosdoshmërisht hetimit nga një gjykatë. Për qëllime të këtij studimi ishte e mjaftueshme që ato të ishin të raportuara ose të njoftuara nga aktorë të caktuar (të tillë si media, OJF, personel i brendshëm i administratës, etj.). Një sfidë e madhe për identifikimin e rasteve përkatëse ishte mungesa e informacionit statistikor mbi veprat korruptive që lidhen me shpërdorimin e IT-së. Po ashtu, abuzimi me IT-në me qëllim korrupsionin nuk duket të jetë në programin e shumë, nëse jo shumicës, organeve antikorrupsion në rajon. Nga ana tjetër, duket se ka një prirje të fortë kundër zbulimit pikave të dobëta të sistemeve tëIT-së: duket sikur institucionet publike rregullisht hezitonin të zbulonin informacionin që tregonte se sistemet e tyre tëIT-së ishin shumë më të dobëta sesa ndoshta besonte publiku. Megjithatë, iniciuesit e këtij studimi menduan që do të ishte mirë të vinin rastet e ndodhura në dispozicion të lexuesve ndërkombëtarë, edhe nëse problemet, të paktën jo në të gjitha rastet, nuk ishin të provuara, të plota ose përfaqësuese.

Rastet tregojnë se abuzimi me IT-në përfshin të gjithë gamën e veprave korruptive:
- Rryshfeti
- Abuzimi me detyrën
- Ushtrimi i influencës
- Konfliktet e interesit
- Shkeljet në prokurime
- Përvetësimi

Abuzimi me IT-në për qëllime korrupsioni ndodh në rastet kur janë në rrezik interesa financiare, si edhe në rastet kur abuzimi me IT-në i shërben vetëm interesave jomateriale të zyrtarit publik (të tillë si kënaqësia e bërjes publike të të dhënave të ndjeshme personale). Rastet duket që ndodhin në çdo sektor të mundshëm të qeverisjes publike, përfshirë kompanitë në pronësi të shtetit, dhe natyrisht në të gjitha nivelet e qeverisjes (qendrore dhe lokale). Keqpërdorimi i IT-së mund të ndodhë spontanisht për tu kujdesur për nevojat e individit (për shembull një pasaportë false) ose mund të jetë pjesë e skemave të vazhdueshme ose të krimit të organizuar (për shembull mashtrimi me sistemin e taksave në autostradë).

Gama e gjerë e rasteve tregon edhe se fakti që “qeverisja elektronike (e-government) ndihmon në luftën kundër korrupsionit” duhet të trajtohet më kujdes. IT nuk është në vetvete një ilaç kundër korrupsionit. Në disa raste dikush mund të thotë që IT e bën më të lehtë për shkelësit e ligjit të kryejnë krimet e tyre të korrupsionit: mungesa e dukshmërisë së sistemeve të IT-së mund të jetë në avantazh të tyre sepse gjurmët janë më pak tëdukshme në rrjete plotësisht komplekse dhe të dhëna elektronike ndoshta të përkohëshme. Rëndësia e masave mbrojtëse të forta (që do të diskutohen tek Kapitulli 2) bëhet edhe më e qartë nën dritën e këtyre rasteve studimore.

Tabela 1

Titullis	Vepra korruptive (jo domosdoshmërisht e provuar)	Përdorimi i IT-së	Dëmi tek financat publike	Si u zbulua vepra korruptive?	Niveli i qeverisjes (qendror ose lokal)	Sektori
Shqipëria, rasti 1: Korrupsioni në sistemin TIMS tëkontrollit kufitar	Rryshfeti	Shitja e të dhënave të falsifikuara	Po	Auditimi i brendshëm	Qendror	Zbatimi i ligjit
Shqipëria, rasti 2: Korrupsioni në Sistemin Elektroniktë Prokurimit Publik	Shkeljet në prokurime	Hyrje e paautorizuar/ falsifikim	Po	Auditimi i jashtëm	Qendror	Prokurimi
Shqipëria, rasti 3: Korrupsioni me IT-në tek Operatori i Shpërndarjes së Energjisë	Shpërdorimi i detyrës	Falsifikimi i të dhënave	Po	Ankesat e qytetarëve	Qendror	Energjia
Shqipëria, rasti 4: Përvetësimi dhe falsifikimi në mbajtjen e regjistrave kontabël	Shpërdorimi i detyrës Përvetësimi	Ndryshimi i të dhënave/ mashtrimi	Po	Auditimi i brendshëm	Qendror	Mbrojtja
Bosnja dhe Hercegovina, rasti 1: Hakeri më i famshëm boshnjak mes prokurorëve	Shpërdorimi i detyrës	Sabotazhi tek kompjuterat	Jo	Hetimi i brendshëm	Qendror	Gjyqësori
Bosnja dhe Hercegovina, rasti 2: Një punësim tjetër i diskutueshëm në Institucionin e Lartë të Auditimit të Republikës Srpska	Shpërdorimi i detyrës	Shkatërrimi i të dhënave	Jo	Informacion nga brenda	Lokal	Prokurimi

Titullis	Vepra korruptive (jo domosdoshmërisht e provuar)	Përdorimi i IT-së	Dëmi tek financat publike	Si u zbulua vepra korruptive?	Niveli i qeverisjes (qendror ose lokal)	Sektori
Bosnja dhe Hercegovina, rasti 3: Keqpërdorimi i sistemit elektronik të projektit CIPS	Shpërdorimi i detyrës	Falsifikimi i të dhënave	Jo	Raporti i medias	Lokal	Regjistri civil
Kroacia, rasti 1: Telefonata e doktorit për vota	Marrja e paligjshme e të dhënave	Përdorimi i paautorizuar i të dhënave të pacientit nga spitali	Jo	Ankesat e qytetarëve	Lokal	Shëndetësia Shëndetësia
Kroacia, rasti 2: Të dhënat konfidenciale të radio-televizionit kroat në tregun e zi	Marrja e paligjshme e të dhënave	Kopjimi dhe shitja e të dhënave të bazës së të dhënave HRT	Jo	Ankesë nga OJF	Qendror	Media
Kroacia, rasti 3: Në kërkim të veteranëve	Abuzimi me detyrën Marrja e paligjshme e të dhënave	Shitja ose nxjerrja e të dhënave të bazës së të dhënave	Jo	Raporti i medias	Qendror	Qeveria
Kroacia, rasti 4: Me një ndihmë të vogël të nëpunësve civilë,68 pasaporta kroate iu shitën kriminelëve	Marrja e paligjshme e të dhënave	Kontrolli i të dhënave konfidenciale në sistemin e informacionit të policisë	Jo	Policia	Qendror	Punët e Brendshme
Kroacia, rasti 5: Oficeri i policisë u kap ndërsa fuste të dhëna të rreme tek sistemi i informacionit të policisë	Manipulimi i të dhënave dhe procedurave ekzistuese	Krijimi i të dhënave të rreme në sistemin elektronik për të ndihmuar një shtetas të huaj për marrjen e shtetësisë kroate	Jo	Policia	Qendror	Punët e Brendshme
Kroacia, rasti 6: Oficerë policie që fshijnë kundravajtjet në trafik dhe zbulojnë të dhëna konfidenciale (bile ata pranuan si rryshfet edhe mish qingji të pjekur dhe 20 litra verë!)	Marrja e paligjshme e të dhënave Manipulimi i të dhënave dhe i procedurave	Marrja e paligjshme e të dhënave: zbulimi i të dhënave konfidenciale të sistemit të informacionit të policisë tek krimi i organizuar. Manipulimi i të dhënave dhe i procedurave ekzistuese: fshirja e veprave në trafik nga sistemi i informacionit të policisë	Jo	Policia	Lokal	Punët e Brendshme

Titullis	Vepra korruptive (jo domosdoshmërisht e provuar)	Përdorimi i IT-së	Dëmi tek financat publike	Si u zbulua vepra korruptive?	Niveli i qeverisjes (qendror ose lokal)	Sektori
Kroacia, rasti 7: I kapur rastësisht për zbulim të të dhënave konfidenciale përautomjetet dhe pronarët e tyre!	Marrja e paligjshme e të dhënave	Zbulimi i të dhënave konfidenciale të sistemit të informacionit të policisë tek krimi i organizuar	Jo	Policia	Lokal	Punët e Brendshme
Kroacia, rasti 8: Çdo vit zhduken 2 milion euro nga kabinat e taksës së autostradës	Përvetësimi	Fshirja e të dhënave dhe futja e të dhënave të rreme në sistemin e informacionit	Po (~2 milion euro/vit)	Auditimi i brendshëm	Qendror	Trafiku
Kroacia, rasti 9: Policë të pandershëm; oficerë policie që i dhanë të dhënakonfidenciale kontrabandistëve të armëve	Zbulimi i informacionit konfidencial Shpërdorimi i detyrës	Zbulimi i të dhënave konfidenciale të sistemit të informacionit të policisë tek krimi i organizuar	Jo	Policia	Lokal	Policia
Kroacia, rasti 10: Oficer policie i dënuar me një vit burgim sepse lejoi mikun e tij të peshkonte në mënyrë të paligjshme	Zbulimi i informacionit konfidencial Shpërdorimi i detyrës	Zbulimi i të dhënave konfidenciale të sistemit të informacionit të Ministrisë tek krimi i organizuar	Jo	Nuk dihet	Lokal	Policia
Kroacia, rasti 11: Inspektori i lartë përdori të dhëna konfidenaciale për të fituar zgjedhjet lokale	Shpërdorimi i detyrës Zbulimi i informacionit konfidencial	Akses i paligjshëm dhe zbulimi i të dhënave konfidenciale nga sistemi i informacionit të Administratës së Tatimeve	Jo	Ankesa e qytetarit	Lokal	Tatimet
Kroacia, rasti 12: Nuk keni kaluar asnjë ditë të jetës suaj në punë? Nuk ka problem, përsëri mund të marrësh pension të plotë!	Mashtrimi (falsifikimi i librit të punësimit) Përvetësimi duke iu dhënë një pension të pajustifikuar	Futja e të dhënave të rreme në sistemin e informacionit të Institutit kroat për sigurimet e pensioneve	Po (—20.000 euro)	Ankesë nga brenda	Qendror	Sigurimet shoqërore
Kosova, rasti 1: Shkatërrimi i provave	Shpërdorimi i detyrës Mashtrimi në detyrë Falsifikimi i dokumenteve zyrtare	Fshirja e të dhënave nga serveri	Po	Ankesa e qytetarit	Qendror	Ndërtimi
Kosova, rasti2: Marrja e statusit të invalidit të luftës	Falsifikimi i dokumenteve zyrtare Mashtrimi në zyrë	Falsifikimi i të dhënave	Po	Ankesa e qytetarit	Qendror	Çështjet sociale

Titullis	Vepra korruptive (jo domosdoshmërisht e provuar)	Përdorimi i IT-së	Dëmi tek financat publike	Si u zbulua vepra korruptive?	Niveli i qeverisjes (qendror ose lokal)	Sektori
Kosova, rasti3: Keqpërdorimi i fjalëkalimit	Abuzimi me lejehyrjen	Favoritizimi Thyerje e fjalëkalimit	Po	Ankesë nga brenda	Qendror	Shëndetësia
Kosova, rasti4: Falsifikimi i dokumenteve të taksave	Falsifikimi i dokumenteve zyrtare Mashtrimi në zyrë	Falsifikimi i dokumenteve	Po	Ankesë nga brenda(ish punonjës)	Lokal	Mirëmbajtja
Maqedonia, rasti1: Abuzimi i sistemeve të IT-së në tarifat autostradale	Abuzimi me detyrën Rryshfeti Përvetësimi	Regjistrimi i rremë i numrit dhe llojit të automjeteve në sistemin e IT-së për pagesën e taksës	Po (—2.000 euro)	Auditimi i brendshëm	Qendror	Transporti/ trafiku
Maqedonia, rasti 2: Sulm mbi sistemin e TI-së të prokurimit publik	Rryshfeti Përvetësimi Shkeljet në prokurime	Pengimi i procesit të prokurimit Ndërhyrje e paligjshme në sistemin kompjuterik	Jo/nuk dihet	Ankesë	Qendror	Prokurimi
Maqedonia, rasti 3: Abuzimi nëpërmjet sistemit të IT-së dhe zbulimi i kundërligjshëm i të dhënave personale	Përvetësimi Shpërdorimi i detyrës Rryshfeti i mundshëm	Nxjerrja e të dhënave personale dhe krijimi i një dokumenti zyrtar për një person tjetër	Nuk dihet	Zbulimi i dokumentit fals	Qendror	Administrata
Maqedonia, rasti 4: Keqpërdorimi i sistemit të regjistrimit të orëve të punës	Përvetësimi Shpërdorimi i detyrës	Ndryshimi i të dhënave në sistemin e orëve të punës	Po	Auditimi i brendshëm	Qendror	Administrata
Maqedonia, rasti 5: Shperdorimi i të drejtave të administratorit (garancia bankare/ kuotat e importit)	Përvetësimi Shpërdorimi i detyrës Rryshfeti	Ndryshimi dhe rindryshimi i të dhënave Hapja dhe përdorimi i llogarive false	Po (~ 160.000 euro)	Auditimi i brendshëm	Qendror	Administrata e kufirit
Mali i Zi, rasti 1: Shpërdorimi i detyrës dhe falsifikimi i dokumenteve zyrtare	Shpërdorimi i detyrës	Falsifikimi i të dhënave	Jo	Hetimi i brendshëm	Qendror	Ministria e Brendshme
Mali i Zi, rasti 2: Përdorimi i të dhënave të IT-së për të shkaktuar dëm politik	Manipulimi dhe abuzimi me sistemet e IT-së Shpërdorimi i detyrës	Abuzimi me sistemin e IT-së Falsifikimi i të dhënave	Jo	Raporti i medias	Qendror	Punët e Brendshme Telekomunikacioni

Titullis	Vepra korruptive (jo domosdoshmërisht e provuar)	Përdorimi i IT-së	Dëmi tek financat publike	Si u zbulua vepra korruptive?	Niveli i qeverisjes (qendror ose lokal)	Sektori
Mali i Zi, rasti 3: Keqërdorimi i funksioneve dhe futja e të dhënave të pasakta në regjistrat publikë	Shpërdorimi i detyrës Rryshfeti	Falsifikimi i të dhënave	Po	Hetimi i brendshëm	Lokal	Kadastra e tokës Punët e Brendshme
Mali i Zi, rasti 4: Lëshimi i paligjshëm i dokumenteve të udhëtimit	Shpërdorimi i detyrës	Falsifikimi i të dhënave	Jo	Hetimi i brendshëm	Qendror	Punët e Brendshme
Serbia, rasti 1: Seks në “Arenën e Beogradit”	Shpërdorimi i detyrës	Marrja e paligjshme e të dhënave Manipulimi i të dhënave dhe procedurave	Jo	Raporti i medias	Qendror	Policia
Serbia, rasti 2: Kur “zë rrënjë” kontraktori i IT-së	Shpërdorimi i detyrës NepotizmiShkeljet në prokurime	Risqet e lidhura me kontraktorin e IT-së Manipulimi i të dhënave dhe procedurave	Po	Auditimi i brendshëm	Qendror	Drejtësia
Serbia, rasti 3: Një funksionar publik i nivelit të lartë përgjon punonjësit	Përvetësimi Shpërdorimi i detyrës	Marrja e paligjshme e të dhënave Manipulimi i të dhënave dhe procedurave	Jo	Bilbilfryrësi	Qendror	Ekonomia
Serbia, rasti 4: “Mafia rrugore”	Shpërdorimi i detyrës Përvetësimi Krimi i organizuar	Sistemet e stacioneve të pagesës së taksës ishin kompromentuar. Printimi i biletave dy herë me numër serial identik për kamionët. Ngritja e traut të hyrjes në mënyrë të paligjshme .	Po	Sinjalizuesi	Qendror	Transporti /trafiku

Shqipëria

Nga Edlira Nasi dhe Ened Kercini

Shqipëria, rasti 1: Korrupsioni në sistemin TIMS të kontrollit kufitar

Rasti i mëposhtëm ka të bëjë me shpërdorimin e detyrës nga ana e oficerëve të policisë kufitare dhe ndryshimin e të dhënave në sistemin e IT-së të TIMS-it (Sistemi i Menaxhimit të Informacionit të Përgjithshëm), si një mjet për të shmangur taksën që i takon shtetit për përdorimin e një automjeti të importuar.

Historiku

Z. A.I., përmes një prokure të posaçme i kishte dhënë të drejtën z. E.H. të përdorte një makinë Ford, që kishte targë italiane. Nëpërmjet këtij dokumenti, z. H. I i ishte dhënë e drejta ligjore të shkonte dhe të kërkonte tek institucionet përkatëse procedurat e çdoganimit dhe të regjistrimit të makinës së importuar. Kështu, makina duhej të kalonte përmes procedurave specifike me qëllim që të përdorej lirisht dhe ligjërisht në Shqipëri.

Mirëpo, E.H. kishte një të njohur, z. A.T., një oficer në bazën ushtarake tëZall-Herrit. Mendohej qëE.H., pronari i makinës, i kishte thënë oficerit që makina kishte qenë në Shqipëri prej disa kohësh, por nuk shoqërohej me dokumentacionin përkatës të nevojshëm për të treguar hyrjen apo importin në vend, dhe ai - si pronar – nuk kishte aplikuar për të marrë dokumentet e përmendura meqënëse kishte disa detyrime financiare që duhej të paguheshin për të marrë dokumentet.

A.T. i tha E.H. se ai e njihte personin që punonte në Shkodër, në Pikën e Kalimit Kufitar të Muriqanit, i cili mund t'i "rregullonte" dokumentet në mënyrë të tillë që të dukej se makina kishte hyrë në Shqipëri vetëm kohët e fundit. Sigurisht që për këtë shërbim ai duhej të paguante një shumë lekësh.

Nga ana e tij, A.T. njihej me z. A.S., i cili punonte si përgjegjës në Qendrën e Shkëmbimit të Informacionit me Malin e Zi, në Drejtorinë Rajonale të Kufirit dhe Migracionit në qytetin e Shkodrës. A.T. i kishte premtuar E.H. që ai mund ta ndihmonte për të siguruar një dokument që vërtetonte se mjeti kishte hyrë në Shqipëri gjatë ditëve të fundit. Në fakt, A.T. e morri vetë përsipër ta kryente këtë punë dhe, si rezultat, kërkoi një fotokopje të dokumentit të vërtetë që provonte hyrjen e automjetit në Shqipëri me qëllim që të prodhonte një dokument të ri nga Pika Kufitare, sikur makina kishte hyrë në Shqipëri në një periudhë më të vonshme (pas vitit 2009). A.T. është regjistruar të ketë thënë se çmimi për këtë shërbim kishte qenë 15.000 lekë (afërsisht 105 euro) një vit më parë, por se çmimi ishte rritur që atëhere.

Me qëllim sigurimin e dokumentit dhe ndihmën e A.S., E.H., A.S. dhe A.T. u takuan në 9 shkurt 2013 në një kafe për të diskutuar për dokumentin e pikës së hyrjes që ishte i nevojshëm të prodhohej. Disa ditë më vonë, dy burrat u takuan përsëri dhe A.S. tha që e kishte përfunduar punën e tij dhe kështu kishte prodhuar një raport nga sistemi IT i TIMS[17].

Të dhëna false në sistemin e IT-së

Dokumenti fals i prodhuar informonte se pronari i ri i makinës E.H. kishte hyrë në Shqipëri nga Pika Kufitare e Muriqanit në 3 shkurt 2013, në orën 05:58 bashkë me një makinë me targën DK***L. Ky fakt dokumentohej edhe me të dhënat e sistemit elektronik të TIMS-it.

Sipas vlerësimeve dhe kontrolleve të mëvonshme të sistemit TIMS, u pa se personi që kishte bërë ndryshimet në sistemin e TI-së të TIMS-it ishte një person tjetër, Ad.S. Gjatë diskutimeve ndërmjet E.H. dhe A.T., që u treguan me hollësi më vonë nga E.H., A.T., pika e kontaktit, i kishte thënë E.H. që ai as nuk duhej të shkonte fare në pikën kufitare sepse të gjitha veprimet e nevojshme do të kryheshin nga A.S. që punonte në Pikën Kufitare.

Mënyra si u bë kjo ishte përmes hyrjes dhe falsifikimit të të dhënave elektronike në sistemin TIMS. Sistemi i Menaxhimit të të gjithë Informacionit (TIMS) është një bazë të dhënash e madhe që ka të dhëna për të gjithë shqiptarët të cilëve iu është dhënë një pasaportë biometrike, d.m.th. shumicës së shqiptarëve që kur u miratua pasaporta biometrike nga Shqipëria. Sistemi regjistron lëvizjet e shtetasve shqiptarë që kalojnë tek të gjitha pikat e kontrollit kufitar në Shqipëri. Përveç kësaj, sistemi ruan të dhëna për mjetet me të cilat kanë udhëtuar shtetasit, pikën e origjinës dhe/ose destinacionit të shtetasve, si edhe numrat e regjistrimit të mjetit. Të dhënat janë në dispozicion edhe të agjencive ligjzbatuese dhe komisariateve të policisë. Duke qenë se që nga 1 marsi 2012, pasaportat biometrike janë i vetmi dokument udhëtimi për shtetasit shqiptarë, të gjitha pikat e kontrollit kufitar përdorin lexuesin e pasaportës biometrike dhe pajisje për verifikimin e gjurmëve të gishtërinjve. Regjistrimi në kohë reale i dokumenteve në sistemin TIMS dhe leximi i tyre gjatë hyrjes/daljes në pikat e kalimit kufitar jep mundësi për krahasimin me të dhënat ekzistuese duke pakësuar kështu mundësi për abuzim[18].

Ndërhyrja dhe aktiviteti mbi sistemin TIMS u krye nga Ad.S. që kishte detyrën e operatorit të sistemit në Policinë Kufitare dhe të Migracionit të Muriqanit që nga 1 maji 2010. Në këtë detyrë ai mori pjesë në kontrollin e personave dhe mjeteve, dhe po ashtu ai i regjistronte ato gjatë kalimit në hyrje dhe dalje për në Shqipëri dhe nga Shqipëria. Ad.S. ishte edhe përgjegjës dhe e njihte të gjithë menaxhimin e sistemit të kontrollit të kufirit TIMS dhe sistemin e kamerave. Po ashtu, detyrat e tij ishin të përcaktuara në rregulloren përkatëse e cila parashikon udhëzimet dhe standardet për kryerjen e detyrës në këtë pozicion. Në këtë detyrë, ai kontrollonte dhe vinte në funksionim nënsistemet e TIMS-it të tilla si sistemin e kontrollit të kufirirt dhe sistemin me të dhënat kriminale. Ai kishte edhe detyrën të mbikëqyrte punën e personelit tjetër gjatë turnit të tij dhe të garantonte që zbatoheshin me saktësi të gjitha procedurat.

17 Vendimi i Gjykatës, nr. 1035, datë 23.07.2013
18 Shkëmbimi i informacionit mbi bazën e Kodit Etik të OSBE-së për aspektet politiko-ushtarake të sigurisë – Republika e Shqipërisë 2013, FSC.EMI/178/14, 22 maj 2014

Vlerësimi i sistemit që u krye si pjesë e procesit hetimor[19] tregoi se Ad.S. kishte bërë ndryshime në sistemin TIMS, në të cilin tregohej gabimisht se E.H. kishte hyrë në Shqipëri në 9 shkurt 2013, si një mënyrë për të shmangur pagesën e taksave ose detyrimeve përkatëse. Po ashtu, ky veprim provohet nga raporti i TIMS-it që tregon se emri i përdoruesit të personit që i ka bërë këto ndryshime ishte ai i Ad.S., si edhe nga fakti që sipas planit të punës së personelit, Ad.S. ishte operatori i sistemit në atë turn.

Për shkak të këtyre veprimeve dhe dhënies së parave për veprimet e përmendura, prokuroria ngriti akuza penale kundër Ad.S., me arsyetimin se ai kishte bërë ndryshime të rreme në sistem dhe veproi kundër interesit publik duke përgatitur një raport fals për automjetin e E.H.

A.S. u shpall fajtor për korrupsion pasiv të zyrtarëve publikë dhe u dënua me një vit e tetë muaj burgim (dënim i pezulluar nën rrethana specifike) dhe iu ndalua mbajtja e funksioneve publike për një vit. Ad.S. u shpall fajtor për shpërdorim të detyrës dhe u dënua me gjashtë muaj burgim (dënim i pezulluar nën rrethana specifike), dhe iu ndalua mbajtja e funksioneve publike për një vit. A.T. u shpall fajtor për ushtrimin e ndikimit të paligjshëm mbi zyrtarët publikë dhe u dënua me gjashtë muaj burgim (dënim i pezulluar nën rrethana specifike).

Shqipëria, rasti 2: Korrupsioni në sistemin elektronik të prokurimit publik

Rasti ka të bëjë me ndërhyrjet në sistemin e prokurimit publik për shkak të korrupsionit, si edhe me ndërhyrjen në administrimin elektronik të prokurimit publik.

Historiku

Në plotësimin e rolit të tij si institucion i lartë i pavarur i auditimit në vend, Kontrolli i Lartë i Shtetit (SSA) kreu një auditim tek Autoriteti i Aviacionit Civil (CAA) në vitin 2012. Raporti përfundimtar i auditimit "Mbi zbatimin e ligjshmërisë dhe rregullshmërisë së veprimtarisë ekonomiko-financiare" të CAA-së për periudhën 1 janar 2011 deri 31 mars 2012 dhe masat për përmirësimin e gjendjes përfshiu edhe vlerësimin dhe rishikimin e procedurave të prokurimit[20].

CAA është një ent publik me pavarësi financiare, një aspekt që e lejon CAA-në të kryejë veprimtarimë e saj në përputhje me standardet ndërkombëtare dhe në përgjigje të nevojës së CAA-së për të përmbushur detyrimet me standarde të larta profesionale.

19 Rasti u shqyrtua dhe u ndoq nga ICS përmes informatorëve të tyre, megjithatë të dhënat e IT-së duket që janë analizuar më vonë si prova nga prokuroria

20 Raporti i plotë gjendet tek adresa elektronike e KLSh http://www.klsh.org.al/web/pub/autoriteti_avia- cionit_civil_394_1.pdf

Administrimi i procedurave të prokurimit në Shqipëri kryhet në përputhje me ligjin nr. 9643 datë 20 nëntor 2006 "Për Prokurimin Publik", ligjin nr. 9880 datë 25 shkurt 2008 "Për firmën elektronike", dhe Vendimin e Këshillit të Ministrave nr. 659 datë 3 tetor 2007 "Për rregullat e kryerjes së procedurave të prokurimit publik me mjete elektronike", si edhe rregulloret dhe udhëzimet e Agjencisë së Prokurimit Publik.

Gjatë një prej procedurave të prokurimit në lidhje me "Blerja e pajisjeve dhe mobiljeve për zyra", Kontrolli i Lartë i Shtetit vuri re parregullsi në procesin e prokurimit, ndërsa përgjigjet e personave të përfshirë në proces treguan se kishte pasur manipulim të firmave elektronike në procesin e prokurimit.

Prokurimi

Gjatë procesit të prokurimit të sipërpërmendur, komunikimet me autoritetin kontraktor në proces, d.m.th. CAA-në, i treguan KLSh-së se kishte aspekte të prokurimit elektronik që nuk ishin të rregullta. Në 20 tetor 2011, një nga anëtarët e personelIt të CAA-së, z. T., ishte vënë në dijeni për firmosjen e procesverbalit të vendimit për skualifikimin e një kompanie në procesin e prokurimit të përmendur më sipër.

Pastaj, Z. T. informoi drejtorët e CAA-së që komisioni që kishte vlerësuar ofertat nuk e kishte bërë asnjëherë këtë vlerësim me mjete elektronike sepse ai kishte qenë jashtë vendit. Po ashtu, ai vuri në dukje se fjalëkalimi që ai përdorte si përdorues i sistemit elektronik ishte ndryshuar pa e njoftuar atë dhe pa miratimin e tij. Kështu që dikush tjetër e kishte plotësuar procedurën e shqyrtimit dhe vlerësimit të ofertave të kompanive.

Më tej, pas shqyrtimit të dokumentacionit të ofertave që ishin paraqitur në formë elektronike (duke përdorur fjalëkalimet e ndryshuara), z. T. vuri re se arsyet për skualifikimin e kompanisë që kishte dhënë ofertën më të ulët nuk mbështeteshin as tek arsye ligjore, as te dispozita ligjore. Meqënëse kompania në fjalë kishte paraqitur tamam të njëjtat specifikime teknike si ato të kërkuara nga CAA, skualifikimi nuk ishte i arsyeshëm dhe do të sillte dëme ekonomike në buxhetin e shtetit dhe të CAA-së.

Po ashtu, z. T. konfirmoi që ai nuk kishte marrë kurrë pjesë në këtë vlerësim të ofertave dhe as nuk kishte marrë pjesë në një mbledhje për të njëjtën çështje në vitin 2011. Nga verifikimi i bërë nga ky i dyti në portalin e Agjencisë së Prokurimit Publik, u zbulua se vlerësimi ishte bërë nga një person i tretë pas ndryshimit të fjalëkalimit. Në një dokument të mëvonshëm, si anëtar i komisionit të vlerësimit të ofertave, ai mohoi të kishte firmosur procesverbalin e mbledhjes për atë proces specifik prokurimi.

Me gjithë këto fakte, SSA vë në dukje se drejtorët e CAA-së nuk kishin vepruar për të rregulluar situatën duke mos marrë masa administrative për personat e përfshirë. Si rezultat, SSA e çoi çështjen në prokurori duke vënë në dukje se veprimet e CAA-së për prokurimin ishin të rreme përderisa anëtarët e grupit të vlerësimit të ofertave mohuan që të kishin marrë pjesë në vlerësimin e ofertave.

Shqipëria, rasti 3: Korrupsioni me IT-në tek Operatori i Shpërndarjes së Energjisë

Historiku

Në vitin 2009, Shqipëria kaloi në privatizimin e 76% të aksioneve të Operatorit të Shpërndarjes së Energjisë. 24% e aksioneve të Operatorit ishin pronë e shtetit shqiptar, dhe 76% e aksioneve iu shitën kompanisë "ÇEZ Shpërndarje". Aktiviteti shpërndarës i operatorit u rregullua nga Enti Rregullator i Energjisë në Shqipëri - ERE.

Në 20 janar 2011, Zyra për Mbrojtjen e Konsumatorit dërgoi në prokurorinë e Tiranës një ankesë kundër drejtuesve të kompanisë "ÇEZ Shpërndarje" për krimet e "mashtrimit" dhe "mashtrimit kompjuterik" të cilave u referohen nenet 143 dhe 143/b të Kodit Penal. Ankesa, së bashku me një ankesë tjetër të bërë më parë nga policia, theksonte se kompania "ÇEZ Shpërndarje" u lëshonte konsumatorëve fatura energjie që kishin një zë të veçantë të dyshimtë. Nën titullin "energji afrofe", klientëve familjarë iu ngarkoheshin 4000 kilovatë më tepër, ndërsa konsumatorëve jofamiljarë iu shtoheshin 20000 kilovatë. Zëri "energji afrofe" iu shtohej kryesisht klientëve që kishin lidhur në mënyrë të paligjshme energjinë e tyre tek rrjeti i shpërndarjes së energjisë elektrike pa u regjistruar ose pa paguar tarifat përkatëse ose klientëve që kishin ndërhyrë tek aparatet matëse të energjisë së konsumuar. Sidoqoftë, në shumicën e rasteve, klientët ankoheshin që faturat e tyre nuk informonin që sasitë e mëdha të faturuara ishin rezultat më shumë i një gjobe të tillë sesa rezultat i rritjes së konsumit.

Përmes njoftimit të vet në 12 janar 2011, Enti Rregullator i Energjisë (ERE) informoi publikun mbi vendimin e vet nr. 90, datë 15 nëntor 2010, se ai kishte arritur në përfundimin që përdorimi i zërit "energji afrofe" është i papërshtatshëm dhe arbitrar. Kjo gjë nuk mbështetet në ligj dhe është në kundërshtim me kuadrin rregullator në fuqi, dhe prandaj për këto veprime kompania ÇEZ Shpërndarje duhej të gjobitej. Në mbështetje të kësaj, ERE kishte marrë rreth 14000 ankesa nga qytetarë të ndryshëm[21]gjatë periudhës kohore prej tetorit 2010 deri në janar 2011, gjatë së cilës ishin paguar 490 gjoba nga qytetarët.

Sipas shtypit të asaj kohe (2011), Operatori i Shpërndarjes jo vetëm i kishte mbifaturuar klientët, por edhe e kishte bërë këtë në mënyrë abuzive duke i lejuar faturistët t'u vendosnin gjoba qytetarëve dhe bizneseve pa respektuar procedurat e përcaktuara nga kompania e shpërndarjes. Po ashtu, media pretendonte se punonjësit e Operatorit të Shpërndarjes merrnin shpërblim financiar për të gjobitur klientët[22] duke bërë kështu që shumë klientë të kishin fatura më të larta[23]. Megjithatë, kjo gjë nuk provohet tek procesverbalet apo vendimet e gjykatës. Nga ana tjetër, nuk jepet ndonjë arsyetim tjetër për veprimet e lartpërmendura të punonjësve të kompanisë së shpërndarjes.

21 Vendimi nr. 1663, datë 30 qershor 2014 i Gjykatës se Tiranës
22 Skandal/CEZ faturon më shume energji sesa blen, vë gjoba fiktive për të kërkuar rritje çmimi", datë 30.11.2011. Gjendet tek: http://www.gazetatema.net/web/2011/11/30/skan-dali-cez-faturon-me-shume-energji-sesa-blen-ve-gjoba-fiktive-per-te-kerkuar-rritje-cmimi/
23 "Hetimi, CEZ shpërblente punonjësit që mbifaturonin" http://time.ikub.al/2afad09e2d/44 5564cf92c2c-0259d0562e9238b8515/Lajm_Hetimi-CEZ-shperblente-punonjesit-qe-mbifaturo- nin-abonentet.aspx

Sasia e përgjithshme e dëmit financiar të shkaktuar klientëve gjatë periudhës së përmendur më sipër u vlerësua të kishte arritur në 4-5 milion euro[24].

Skema e mbifaturimit

Specifikimet e çdo faturimi të një klienti bëhen përmes operatorëve në terren që përdorin PDA-të (Asistentët Dixhitalë Personalë). PDA-të janë pajisje të përdorura nga personeli i kompanisë në kohën e vlerësimit të sahatëve për matjen e konsumit të energjisë. PDA-të transmetojnë menjëherë (online) tek serveri numrin e kabinës, numrin e kontratës së abonentit, pozicionin e aparatit matës në atë moment (do të thotë regjistrimin e sasisë së kilovatëve të konsumuara), dhe datën dhe orën në të cilën ishte kryer matja. Në atë kohë, edhe të dhënat për "anomalitë" (çështje teknike, ose lidhje të paligjshme në rrjetin e energjisë, etj.) gjithashtu regjistroheshin gjatë procesit normal të faturimit.

Leximet e PDA-së pastaj sinkronizohen me sistemin MYAvis në serverin tek Dhoma e Serverit me të dhënat (kalimi i të dhënave arrihet përmes një platforme GPRS) në fund të çdo dite pune. Të dhënat nga interface përkatës MYAvis kalojnë drejtpërdrejt në sistemin e faturimit, me përjashtim të informacionit të bllokuar për shkak të filtrave specifikë, të tilla si anomali apo faturime të dyshimta të cilat shqyrtohen më tej.

Gjatë kohës që një nga rastet po gjykohej në gjykatë, dëshmitë treguan se në fakt ishte e pamundur që punonjësit të ndryshonin elektronikisht të dhënat e klientit, sepse ata nuk kishin të drejtat e administratorit në sistem. Kjo bëri që prokurori të analizonte detajet e matjeve të ndryshme të kryera nga punonjës specifikë të kompanisë së shpërndarjes kundër të cilëve kishte pasur ankesa. Nga lista e matjeve të energjisë së konsumuar, që po ashtu tregonin vendin dhe kohën kur personeli i kompanisë kishte bërë matjet, u zbulua se kishte matje të bëra në orë të papërshtatshme të ditës, të tilla si në ora 22:00, 23:00, 24:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00 etj., megjithë faktin që punonjësit kishin thënë se koha e punës për matjet ishte ndërmjet orës 08:00-16:30.

Përveç tyre, kompania e shpërndarjes së energjisë kishte miratuar procedura të posaçme për matjen e konsumit të energjisë, të cilat, mes të tjerave, përcaktonin edhe rregulla dhe procedura të plota për rregullimin e sistemit të kontrollit të matjes së energjisë dhe për metodën për llogaritjen e energjisë së konsumuar dhe gjoba të tjera për shkak të shkeljeve në matje dhe lidhjeve të paligjshme në rrjetin e shpërndarjes. Kjo rregullore përcakton qartë se matja dhe gjobitja duhet të kryhen në prani të konsumatorit ose të të afërmve të tij (foto, video, dhe çdo fakt tjetër që provon ndërhyrjen në sahat). Në mungesë të konsumatorit ose të të afërmve të tij, ose në mungesë të dëshirës për të firmosur procesverbalin e matjes, procesverbali duhet të firmoset nga personeli i një njësie tjetër të kompanisë (njësia NTL). Nga procesverbalet e matjeve të bëra ishte e qartë se as konsumatorët, dhe as personeli i NTL-së nuk e kishin firmosur procesverbalin në kohën kur kryhej mbifaturimi ose gjobitja për shkak të lidhjeve të paligjshme në rrjetin e shpërndarjes së energjisë.

24 "Prokurorët, hetim 14 mijë ankesave për mbifaturim energjie", datë 27.11.2011 – gjendet tek http://www.shqiptarja.com/lajme/2706/prokuroret-hetim-14-mije-ankesave-per- mbifaturim-energjie-65833.html

Kështu, vetëm në 21 tetor 2010, ishin regjistruar gjoba për rreth 17 rilidhje të paligjshme në rrjetin elektrik. Të gjitha ato ishin vendosur me një interval kohor prej 2 minutash diferencë me njëra tjetrën, ose edhe në të njëjtën kohë[25].

Më shumë se 10 persona janë të dyshuar për pjesëmarrje në këtë skemë mbifaturimi. Skema të tjera të mbifaturimit të energjisë u zbuluan pas këtij rasti dhe u çuan për ndjekje penale. Gjykata tashmë ka shpallur fajtorë shumë punonjës të kompanisë dhe i ka dënuar ata, ndërsa ka ende raste të papërfunduara për punonjës të tjerë. Megjithëse në rastin e përmendur më sipër mbifaturimi u krye përmes PDA-së, në raste të tjera kishte pretendime që të dhënat elektronike ishin ndryshuar pasi ato ishin regjistruar nga PDA-të[26].

Shqipëria, rasti 4: Përvetësimi dhe falsifikimi në mbajtjen e regjistrave kontabël

Ky rast ka të bëjë me një punonjëse përgjegjëse për borderotë, e cila, përgjatë shumë viteve, përvetësonte para të administruara nga ajo dhe i depozitonte në llogarinë e saj bankare.

E pandehura Znj. M.K. ishte shefe e financës në Repartin Ushtarak Zall-Herr, në Tiranë. Në këtë detyrë, M.K. kreu veprime në kundërshtim me ligjin, duke përvetësuar fonde në llogarinë e saj bankare që nuk i përkisnin asaj, nëpërmjet falsifikimit të dokumenteve dhe të dhënave të tjera.

Në vitin 2009, Departamenti i Auditit të Brendshëm në Ministrinë e Mbrojtjes kreu “Auditimin tematik mbi zbatimin e legjislacionit në fuqi për trajtimin me pagë dhe shtesa mbi pagë të punonjësve në Regjimentin Komando Zall -Herr”. Auditimi zbuloi që M.K., në detyrën e saj si shefe e financës kishte falsifikuar dokumente zyrtare, kryesisht listëpagesat e punonjësve të Repartit Ushtarak nr. 1200[27].

Nga ekspertiza kontabël u zbulua se M.K kishte përvetësuar fonde në shumën prej 8668886 lekë (61.920 euro), nga të cilat 6.198.326 lekë ishin rezultat i rritjes së pagës neto të saj, dhe pjesa tjetër prej 24.70.560 lekë përmes shtesave në paga, dieta, shërbime, etj. Të gjitha fondet vinin nga buxheti i shtetit dhe fondi i caktuar në mënyrë specifike për Repartin Ushtarak nr. 1200 Zall Herr, Tiranë.

Mënyra se si puna ishte organizuar në zyrë ishte e tillë që specialisti i zyrës së financës kryente vetëm detyrat e përcaktuara nga shefja e financës, kryesisht hedhjen dhe përgatitjen konkrete të listëpagesave. Megjithatë, specialisti i financës nuk përpilonte tabelën përmbledhëse dhe pagat neto të punonjësve, sepse këto zëra të listëpagesës përpiloheshin nga ana e shefes së financës, pra M.K.

Pasi përgatiteshin listëpagesat, ato dërgoheshin përmes postës elektronike apo mjeteve të tjera elektronike të komunikimit dhe listëpagesa miratohej edhe nga shefi i personelit, edhe nga komandanti i regjimentit. Mënyrat se si ajo arrinte të falsifikonte listëpagesën dhe të merrte miratimin e shefit të personelit dhe komandantit ishte duke marrë në fillim miratimin me shkrim (kopje fizike) dhe pastaj ndryshonte të dhënat tek listëpagesa elektronike dhe në bankë.

Banka nuk kishte përgjegjësi për diferencat në paga, sepse banka nuk mund të kontrollonte të dhënat ose kishte një përmbledhje të pagave, edhe nëse shumat e transferuara në llogarinë bankare të M.K. dukej që ishin më të larta se çfarë mund të konsiderohej e arsyeshme për një pagë. Pas kalimit të shumave në llogarinë e saj, M.K. i tërhiqte ato nga llogaria dhe i fshihte paratë në mënyra të tjera.

M.K. u deklarua fajtore nga gjykata dhe u dënua me një vit burgim[28].

25 Vendimi i Gjykatës së Tiranës nr. 1633, datë 30.06.2014
26 “Prokuroria: Skema si CEZ vidhte 15 mije konsumatorë” datë 15.04.2013 gjendet tek: http://gazeta-shqip.com/lajme/2013/04/15/prokuroria-skema-si-cez-vidhte-15-mije-konsu- matore/
27 Bazuar tek Vendimi i Gjykatës së Rrethit gjyqësor Tiranë nr. 41 datë 20.01.2012
28 Po aty

Bosnja dhe Hercegovina

Nga Aleksandra Martinovic dhe Srdjan Nogo

1.2.1 Bosnja dhe Hercegovina, rasti 1: Hyrje e paautorizuar në postën elektronike të Prokurorit të Përgjithshëm

Të gjitha raportet përkatëse kombëtare dhe ndërkombëtare rreth sistemit gjyqësor në Bosnjë dhe Hercegovinë (BiH), përfshirë raportet e progresit të Komisionit Europian, vënë në dukje se gjyqësori dominohet, kontrollohet dhe ndikohet nga elitat politike, që bëjnë përpjekje të vazhdueshme politike për të rritur ndikimin për emërimet e gjyqtarëve dhe prokurorëve në të gjithë gjyqësorin në BiH. Natyra komplekse dhe e dyshimtë e sistemit gjyqësor në BiH dhe dobësitë e tij në lidhje me pavarësinë dhe paanshmërinë mund të pështkruhen nga rasti i një prokurori shteti (në vazhdim z. X), që u akuzua për hyrje të paautorizuar tek posta elektronike e Prokurorit të Përgjithshëm (në vazhdim z. Y) me qëllim që ta diskreditonte atë përpara pezullimit të z. Y nga detyra e tij si Prokuror i Përgjithshëm.

Një motiv i mundshëm i z. X për të abuzuar me postën elektronike të z. Y mund të gjendet në deklaratën e tij pas pezullimit të z. Y kur ai është regjistruar duke thënë që do të aplikonte për pozicionin e Prokurorit të Përgjithshëm të Bosnjës dhe Hercegovinës. Po ashtu, kishte thashetheme që z. X po mbronte disa të pandehur që i kishte hetuar z. Y.

Edhe z. X, edhe z. Y u lidhën qëllimisht me parti të caktuara politike në BiH. Kryesisht, z. Y ishte lidhur qëllimisht me partinë e Social-Demokratëve të Pavarur - SNSD –që është partia drejtuese në Republikën Serpska dhe një nga partitë më me ndikim në BiH, ndërsa z. Y në atë kohë u lidh me Partinë Social-Demokrate (SDP) në BiH, (partia më e fortë në Federatën e BiH), por edhe me Unionin për një të Ardhme më të Mirë në BiH.

Gjatë hetimit të mëtejshëm u konfirmua se z. X kishte hyrë tek posta elektronike e z. Y dhe kishte dërguar nga ajo adresë një dokument me “Udhëzime të Përgjithshme” false tek punonjësit e prokurorisë së BiH dhe disa media në Federatën e BiH. Dokumenti me “Udhëzimet e Përgjithshme”, që përmbante pohime kompromentuese u dërgua në 29 qershor 2011, me logon e prokurorisë së BiH dhe me një firmë të falsifikuar të Prokurorit të Përgjithshëm.

Në këto “Udhëzime të Përgjithshme” theksohej se u ndalohej të gjithë punonjësve të prokurorisë të BiH të jepnin komente mbi artikuj negativë në media për Prokurorin e Përgjithshëm, veçanërisht për artikuj mbi çështjet që ishin bërë publike atëhere “Prisluskivanje” (Regjistrimi), “Reket” (Racketeering) dhe të tjera në të cilat Prokurori i Përgjithshëm gjoja ishte i përfshirë.

Po ashtu, “Udhëzimet” ndalonin punonjësit të lexonin gazetat “Slobodna Bosna”, “Dani”, “Oslobodjenje”, “Avaz”, dhe “San”, të gjitha të botuara në Federatën e BiH, ose të shikonin programet e transmetuara në televizionin federal (një nga tre transmetuesit publikë në BiH), veçanërisht programin “60 minuta”, të transmetuar në atë kanal televiziv.

“Udhëzimet e Përgjithshme” theksonin gjithashtu që“prokurorët që mendojnë se do të fillojmë të organizojmë takime të rregullta mujore, sipas kuptimit të nenit 20, pika 2, e Librit të Rregullave, janë budallenj.”

Pasi zbuloi këtë mesazh në postën e tij elektronike, Prokurori i Përgjithshëm bëri një ankesë kundër një personi të panjohur në Gjykatën e BiH dhe prokurorinë e BiH. Pas kësaj, iu dha urdhër policisë federale (pjesë e Ministrisë së Brendshme të Federatës së BiH) të fillonte një hetim.

Gjatë hetimit, inspektori që drejtonte luftën kundër krimit kibernetik në Ministrinëe Brendshme Federale përcaktoi se kishte pasur ndërhyrje në postën elektronike të Prokurorit të Përgjithshëm me anë të përdorimit të një telefoni celular (iPhone 4), i regjistruar me emrin e mamasë së z. X, por përdorej vetëm nga ai. Me sa duket, me ndonjë mënyrë, z. X kishte shtënë në dorë fjalëkalimin e postës elektronike të Prokurorit të Përgjithshëm dhe e përdori për të hyrë tek adresa duke qenë në një zonë tjetër dhe dërgoi udhëzimet. Megjithë faktin që kishte shumë masa mbrojtëse për të parandaluar këtë veprim të ndaluar, duket që faktori njerëzor ishte vendimtar në këtë rast. Pas përfundimit të hetimit, u dërgua tek zyra kompetente e prokurorisë (d.m.th. zyra e prokurorisë së Bosnjës dhe Hercegovinës – Departamenti për Krimin e Organizuar dhe Korrupsionin) një raport që përmbante akuza penale kundër prokurorit, z. X , për shpërdorim të detyrës publike, falsifikim dhe mashtrim.

Sipas disa mediave, megjithë përpjekjet e mëdha të kolegëve të z. X në prokurori për të mbuluar këtë skandal të padëgjuar më parë, zyra e Këshillit të Disiplinës në Këshillin e Lartë të Gjyqësorit dhe Prokurorisë(HJCP) të BiH u informua për rastin.

Por këto nuk ishin akuzat e vetme kundër prokurorit të shtetit z. X. Po ashtu, ai u akuzua se kishte kryer edhe dy shkelje të tjera disiplinore. Kështu, ai kishte urdhëruar shkatërrimin e dokumenteve që lidheshin me pyetjen e dëshmitarëve, në prani të vetë atyre dëshmitarëve; dhe kishte dërguar një kërkesë për informacion tek Drejtori i Zyrës së Policisë Federale, me një përmbajtje që ishte e papërshtatshme për një korrespondencë zyrtare dhe funksionin që z. X kishte në atë kohë. Kështu, z. X kërkoi në një mënyrë shumë të papërshtatshme që drejtori të zbulonte burimin e informacionit dhe të rishikonte një shkresë zyrtare të policisë që i akuzonte z. X, zyrtarët e lartë të qeverisë së Federatës së Bosnjës dhe Hercegovinës dhe të Partisë Social-Demokrate të BiH për organizimin e një komploti kundër Drejtorit të Zyrës së Policisë Federale.

Më shumë se një vit më vonë, në 26 shtator 2012, Zyra e Këshillit të Disiplinës së HJPC në BiH arriti një marrëveshje të përbashkët me z. X për përcaktimin e përgjegjësisë disiplinore dhe shkeljet disiplinore. Ai njohu dhe pranoi përgjegjësinë për shkeljet disiplinore dhe Zyra e Këshillit të Disiplinës tërhoqi ankesa disiplinore kërkesën për përcaktimin e përgjegjësisë së tij disiplinore për zëra të caktuara.

Kur rekomandonte masat disiplinore, Zyra e Këshillit të Disiplinës kishte parasysh që*"i pandehuri kishte një karrierë të suksesshme si prokuror publik dhe që ai kishte marrë pjesë në çështje komplekse që kërkojnë nivel të lartë ekspertize dhe dedikimi".* Fakti që ai ishte familjar dhe baba i një fëmije të vogël, dhe fakti që ai kishte borxhe u morrën në konsideratë si rrethana lehtësuese. Ndërsa fakti që kishte edhe një hetim në vazhdim kundër tij për akuzën e marrjes së rryshfetit as nuk u morr fare në konsideratë.

Komisioni i Disiplinës i nivelit të parë i Prokurorëve tëHJCP-së e pranoi marrëveshjen ndërmjet z. X dhe Zyrës së Këshillit të Disiplinës dhe vendosi që z. X ishte përgjegjës për tre shkelje disiplinore dhe një shkelje të Kodit të Etikës së prokurorisë. Shkelja e Kodit të Etikës u konsiderua një shkelje e rëndë e detyrës zyrtare që vuri në dyshim besimin e publikut tek prokuroria dhe dëmtoi reputacionin e prokurorisë së BiH. Ai u gjobit, me uljen me 10% të rrogës së tij për një periudhë gjashtë mujore.

Vetëm një ditë pasi u ndërhy në postën e tij elektronike, z. Y, Prokuror i Përgjithshëm në atë kohë, u pezullua nga detyra e tij zyrtare për shkak të "kontakteve të tij të papërshtatshme" me kontrabandistë ndërkombëtarë të armëve. Kishte pasur të dhëna të shumta zyrtare (fotografi dhe regjistrime të zërit) të takimeve dhe telefonatave të tij me një tregtar armësh të vënë në listën e zezë nga OKB, që tregonin se z. Y merrte para dhe dhurata të shtrenjta për të ndihmuar një rrjet kriminal. Në fund, korrupsioni nuk u provua. Z. Y deklaroi se atij i vinte keq që takimet e tij të papërshtatshme kishin dëmtuar reputacionin e prokurorosë së BiH. Po ashtu, ai bëri një marrëveshje me HJCP, kështu që ai u emërua në një pozicion pune më të ulët – ai vazhdoi të punonte si prokuror për krimet e luftës në prokurorinë e BiH, dhe gjoba e tij disiplinore ishte 10% ulje e rrogës për një periudhë kohe për vetëm tre muaj.

Bosnja dhe Hercegovina, rasti 2: Një tjetër punësim i diskutueshëm në Institucionin e Lartë të Auditimit të Republikës Srpska

Institucioni i Lartë i Auditimit i Republikës Srpska (SAI RS) bëri njoftimin për vend të lirë pune për punësim të përhershëm për "dy auditues **të rinj** të performancës". Njoftimi për vende të lira pune u botua në Fletoren Zyrtare të Republikës Srpska në 3 maj 2014, në faqen e internetit të institucionit (në 29 prill 2014) dhe në media. Afati përfundimtar i aplikimit ishte 30 ditë pas këtij botimi.

Gjatë asaj periudhe, një numër prej 61 kandidatësh aplikuan për këto pozicione dhe të gjithë ata që plotësonin kriteret e përgjithshme dhe specifike të kërkuara dhe ofronin të gjitha provat dhe dokumentet përkatëse u ftuan të merrnin pjesë në një provim me shkrim.

Testimi u krye në 18 qershor 2014, në kabinetin e IT-së të Fakultetit të Ekonomisë në Banja Luka, dhe u krye në mënyrë elektronike duke përdorur kompjuterat e asaj salle.

Sipas përvojave të mëparshme për kryerjen e testimeve të ngjashme, puna e të gjithë kandidatëve supozohej të printohej menjëherë pas testit, të kopjohej në një USB që ishte e SAI RS, dhe të fshihej nga memorja e kompjuterëve të Fakultetit të Ekonomisë. Po ashtu, të gjithë kandidatët që e kishin zhvilluar testin kishin të drejtë të bënin një kopje të tij në USB-në e tyre.

Por kësaj here diçka nuk shkoi mirë. Megjithëse nuk ka ende ndonjë konfirmim zyrtar për këtë, disa të dhëna mungojnë për shkak të problemeve të sistemit të IT-së në Fakultetin e Ekonomisë. Ka spekulime të ndryshme brenda vetë SAI RS sipas të cilave ose nuk janë printuar të gjitha materialet e plota të testit, ose nuk janë regjistruar si duhet të gjitha ato dhe mungojnë disa të dhëna, ose edhe që nuk kishte ndonjë gabim me teknologjinë, por të dhënat janë mbajtur sekret nga drejtuesit e SAI RS (përfshirë anëtarët e komisionit përgjegjës për procedurën e përzgjedhjes), si një justifikim për përzgjedhjen e diskutueshme të një kandidati.

Megjithatë, në të gjitha rastet, nuk kishte masa të përshtatshme sigurie në fuqi dhe mungesa e tyre lejoi këtë veprim. Për shembull, në vend që të punonin në disa programe të sigurta, kandidatët i plotësuan testet e tyre në një format të thjeshtë wordi, pa zbatuar ndonjë masë mbrojtje, kështu që çdo person i komisionit përgjegjës të kishte mundësinë për të bërë ndryshime në teste. Për më tepër, këtë herë kandidatët nuk u lejuan të bënin kopje të testeve në memorien e USB-ve të tyre dhe testet nuk iu dhanë atyre për t'i parë pas vlerësimit.

Megjithëse rezultatet e testit nuk u bënë publike, kandidatët që e kaluan kufirin e pikëve u ftuan për intervistë me gojë në datat 25 dhe 26 qershor 2014, dhe, sipas informacionit të botuar në faqen e internetit të SAI RS, *"komisioni përgjegjës për procedurën e përzgjedhjes përcaktoi listën e kandidatëve fitues dhe e dorëzoi atë tek Audituesi i Përgjithshëm".* Mbështetur tek lista e propozuar, e cila ende nuk është bërë publike, Audituesi i Përgjithshëm zgjodhi dy kandidatët.

Ndërsa për kandidatin e parë të përzgjedhur nuk duket se ka kundërshtime apo diskutime, për kandidatin e dytë ka shkrime tashmë në shtyp me debate që lidhen me përzgjedhjen e kandidatit të dytë. Rasti u zbulua për shkak të dyshimeve të kandidatëve të tjerë (të ngritura si rezultat i mungesës së transparencës në procedurat e përshkruara më sipër). Prandaj, disa prej kandidatëve çuan ankesa tek SAI RS.

Sa u përket masave të sigurisë për parandalimin e këtyre llojeve të problemeve në të ardhmen, sipas burimeve brenda SAI RS, nuk është bërë asgjë deri më tani. Përveç faktit që për kandidatin e përzgjedhur kishte dokumente që tregonin vënien në rrezik të paqes dhe rendit publik, përzgjedhja e tij për pozicionin e audituesit të ri të performancës në moshën 48 vjeçare është shumë e dyshimtë. Kriteret për atë vend pune kërkonin vetëm një vit të domosdoshëm përvojë të mëparshme profesionale dhe nuk bëhej e qartë se kjo përvojë duhet të ishte në sektorin e auditimit. Në këtë moshë, kandidati i përzgjedhur ndoshta është i mbikualifikuar dhe mund të përzgjidhej për një pozicion pune tjetër më të lartë.

Sipas disa thënieve në media, ai u soll në atë pozicion pune nga një parti e caktuar politike e cila mund ta bënte atë të thyeshëm nga shantazhi, që nga fillimi i postit të tij të ri publik. Nëse dalin prova që provojnë këto deklarata, atëhere pritet që atij t'i kërkohet të kryejë disa ndere si shpërblim – për të mbrojtur interesin e elitave politike dhe për të fshehur informacionin dhe provat mbi praktikat korruptive në institucione publike që iu nënshtrohen auditimeve publike në mënyrë që ato të mos zbulohen dhe të mos hetohen.

Për të shtuar edhe një gjë tjetër tek historia e emërimeve dhe punësimeve të diskutueshme tek SAI RS gjatë dy viteve të fundit ia vlen të përmendet rasti i emërimit të Audituesit të Përgjithshëm. Kështu, zgjedhja e parë e Komisionit Parlamentar të RS që është përgjegjës për përzgjedhjen e kandidatëve ishte një person që dyshohej se kishte marrë një diplomë false. Por, për shkak të presionit të fortë të medias ai nuk u emërua.

Bosnja dhe Hercegovina, rasti 3: Keqpërdorimi i sistemit elektronik të projektit CIPS

Projekti i Sistemit të Mbrojtjes së Identifikimit të Qytetarit (CIPS) ka filluar në Bosnjë dhe Hercegovinë në prill 2002, kur, përkohësisht, u krijua drejtoria për zbatimin e tij. Detyra kryesore e projektit ishte krijimi i një pjese të sistemit përmes të cilit do të zbatohej Ligji për Regjistrat Qëndrorë dhe Shkëmbimin e të dhënave.

Në vitin 2008, në përputhje me strategjinë për zhvillimin e dokumenteve të identifikimit, drejtoria u kthye në Agjencia për Dokumentet e Identifikimit, Regjistrat dhe Shkëmbimin e të Dhënave (IDDEEA) e BiH. Ky institucion ndjek, koordinon dhe mbulon institucionalisht fushën e dokumenteve të identifikimit, duke zbatuar standardet dhe rregulloret përkatëse të Bashkimit Europian dhe duke u zhvilluar në përputhje me standardet. Agjencia është përgjegjëse për personalizimin dhe përpunimin teknik të dokumenteve të mëposhtme të identifikimit: kartat e identitetit; kartat e identitetit për të huajt; patentat e automjetit; dokumentet e udhëtimit; dokumentet për regjistrimin e automjeteve dhe dokumente të tjera identifikimi me miratimin e autoriteteve kompetente dhe vendimin e posaçëm të Këshillit të Ministrave.

Që në fazat e fillimit të projektit CIPS, u regjistruan një numër ankesash në lidhje me keqpërdorimin e sistemit të tij elektronik, veçanërisht kur lëshoheshin karta personale identiteti dhe pasaporta në të gjithë vendin.

Prokuroria e BiH urdhëroi një hetim të gjithanshëm që u krye në bashkëpunim me disa institucione të BiH: Agjencia Shtetërore e Hetimit dhe Mbrojtjes (SIPA), ministri të ndryshme përgjegjëse si Ministria e Brendshme dhe administratat e policisë, dhe Misioni Policor i Bashkimit Europian (EUPM) në BiH.

Operacioni i parë i madh u krye në 28 maj 2008, kur u arrestuan 20 persona nga qytete të ndryshme të BiH. Ky operacion u ndoq nga arrestime të tjera gjatë vitit 2009. Personat e arrestuar ishin kryesisht zyrtarë publikë, të tillë si oficerë policie, punonjës në administratat e bashkive, dhe regjistrues, por kishte edhe persona që nuk ishin zyrtarë publikë. Për shumë prej atyre që punonin në zyra publike kishte dyshime se ishin pjesë e krimit të organizuar përmes shpërdorimit të burimeve të tyre financiare dhe teknike, duke bërë të mundur kështu që i gjithë grupi i organizuar të përfitonte të mira materiale në mënyrë të paligjshme.

Të parët në këtë zinxhir ishin punonjës policie që kishin detyrë lëshimin e dokumenteve personale. Ata mund të shikonin regjistrin me të dhëna qendrore që është pjesë e sistemit të Agjencisë ku hidhen dhe ruhen të dhënat për të gjithë shtetasit e BiH-së. Oficerët e policisë përdornin kompjuterët e tyre në zyra dhe funksionet e tyre për të hyrë në sistem dhe ndryshuar të dhënat. Kryesisht, ata gjenin në bazën e të dhënave një person që kishte shtetësinë e BiH-së, por që ende nuk kishte marrë një kartë personale identiteti (për shembull, nëse personi kishte shkuar jashtë vendit gjatë luftës dhe nuk u kthye më). Ata e dërgonin personin që donte të merrte një dokument fals tek zyra e gjendjes civile (një pjesë tjetër e grupit të organizuar kriminal që vepron brenda juridiksionit të administratës së bashkisë) ku atij i jepej një çertifikatë lindje dhe çertifikatë shtetësie me një emër të rremë. Këto ishin të mjaftueshme për fillimin e procedurës për marrjen e kartës personale të identitetit. Po ashtu përdoreshin edhe të dhënat e personave të vdekur. Personi nuk regjistrohej zyrtarisht si i vdekur, por regjistrohej sikur kishte humbur kartën ekzistuese, të vlefshme të identitetit, dhe fillohej procedura për nxjerrjen e një karte të re identiteti.

Siç u vu në dukje nga prokuroria e BiH, *"të dyshuarit u akuzuan për keqpërdorim të sistemit të dokumenteve personale në BiH në mënyrë të tillë që iu bënin të mundur shtetasve të BiH-së dhe të vendeve të tjera të rajonit të nxirrnin dokumente identiteti origjinale të BiH-së, që përmbanin informacion të rremë për identitetin e personave ose kombësinë e tyre"*.

Hetimi nxorri prova që dokumente personale të marra në mënyrë të paligjshme ishin përdorur në një masë të madhe për aktivitete kriminale në pjesë të ndryshme të vendit dhe të rajonit. Për shembull, kishte të dyshuar që kishin qenë anëtarë të klanit Zemun, të dyshuar për vrasjen e ish-kryeministrit serb Zoran Indie, dhe vrasjen e mbetur në tentativë të politikanit serb Vuk Drashkoviç, si edhe shumë anëtarë të tjerë të organizatave të fshehta kriminale që kishin marrë dokumente të rreme identiteti të BiH-së.

Po ashtu, kishte dyshime që personat e arrestuar kishin shitur karta identiteti dhe pasaporta origjinale të BiH-së me identitete të rreme për 2.000 euro. Vetëm në Banja Luka ishin lëshuar më shumë se 200 karta identiteti dhe pasaporta të paligjshme.

Kjo çështje e madhe shkaktoi shumë dëm për reputacionin e shërbimit publik në të gjithë vendin. Si rezultat, u ndërmorrën një numër ndryshimesh tek procedurat me qëllim që të parandaloheshin raste të ngjashme në të ardhmen. Për shembull, u përforcuan shumë procedurat në zyrën e regjistrimit. Kështu, nuk është më e mundur që të merret njëçertifikatë lindje dhe çertifikatë shtetësie për një person të tretë pa autorizimin e vetë atij personi. Gjithashtu, ka edhe verifikime shtesë në zyrat e regjistrimit, ministritë e brendshme dhe organe të tjera kompetente administrative për përcaktimin e identitetit, qëndrimin dhe të dhëna të tjera të rëndësishme të personave kur u lëshohen dokumentet e tyre personale.

Kroacia

Nga Zorislav Petrovic dhe Ivana Andrijasevic

Kroacia, rasti 1: Telefonata e doktorit për vota

Gjatë një fushate për zgjedhjet lokale në maj 2013, qytetarët në Dubrovnik që vuanin nga diabeti morrën një letër nga një doktor diabeti që punonte në Spitalin e Përgjithshëm në Dubrovnik. Ai kandidonte për postin e kryetarit të bashkisë. Shumë prej pacientëve të tij morrën një letër personale prej tij në të cilën ai i kujtonte për kandidimin e tij dhe theksonte se ishte i gatshëm t'i ndihmonte ata: *"(...) zgjedhja ime e parë është të jem në shërbimin tuaj, pacientë të mi të dashur".* Po ashtu, ai i kujtonte pacientët e tij për përparimin e madh që ishte bërë me ngritjen e qendrës më moderne për diabetin dhe shkruante*"këtë vit festojmë 20 vjetorin e Shoqatës së Diabetit".* Kur një grup aktivistësh e zbuloi këtë gjë, kërkoi menjëherë një hetim nga ana e Zyrës së Prokurorit të Shtetit (DORH) në bashkinë e Dubrovnikut.

Hetimi filloi menjëherë dhe zbuloi se qendra telefonike e HNS (Partia Popullore në Kroaci), në të cilën ai ishte anëtar, kishte telefonuar në total 3133 numra fiks në rajonin Dubrovnik-Neretva, dhe që 3215 (98%) ishin numrat e pacientëve të tij. Të gjithë këta numra, së bashku me emrat dhe adresat ishin futur në dosjet personale të këtyre personave në klinikën e Diabetit dhe Endokrinologjisë ku ai punonte si doktor. Për DORH-in në Dubrovnik, një përqindje e tillë e lartë*"ishte një tregues se regjistri i pacientëve që përmbante të dhënat e tyre personale ishte përdorur për fushatën elektorale të mjekut diabetolog"*. Megjithatë, ai e mohoi që t'i kishte kërkuar ndonjëherë njeriu t'i sillte të dhëna të tilla për fushatën elektorale.

Gjatë hetimit, DORH-i zbuloi se shumë persona në spitalin e përgjithshëm në Dubrovnik mund të shihnin listën e pacientëve dhe të dhënat e tyre personale. Për më tepër, DORH-i zbuloi se lista e përdorur nga qendra telefonike e HNS ishte krijuar nga më shumë se një person dhe se ishin përdorur disa burime të ndryshme. Si rezultat *"nuk ishte e mundur të përcaktohej se ku dhe nga kush ishin marrë ato të dhëna"* dhe prandaj, nuk kishte bazë për hetim të mëtejshëm të kandidatit për kryetar bashkie.

Gjatë hetimit ai pretendoi se i përdorte të dhënat publike për dërgimin e letrave dhe se ai mund të merrte të dhëna vetëm për pacientët e tij, por jo për pacientët e mjekëve të tjerë. Megjithatë, një mjek tjetër, në të njëjtën klinikë ku punonte mjeku në fjalë, konfirmoi se çdo njeri me njohuri elementare për sistemin mund të merrte të dhëna për të gjithë pacientët. Ajo deklaroi se ai vetë i kishte dhënë asaj të dhëna për të gjithë pacientët për një studim që ajo po kryente. Administratori pohoi se pjesa më e madhe e infermierëve dhe mjekëve kanë leje të futen tek të dhënat. Po ashtu, ai konfirmoi se ai mori të dhëna për një mjek tjetër dhe një infermiere pas kërkesës së tyre për "një lloj përvjetori".

Si rezultat i vendimit të DORH-it për të mos ndjekur penalisht kandidatin për kryetar bashkie, në 5 mars 2014, një grup i anëtarëve të këshillit bashkiak "Srd je nas'' informoi Shoqatën kroate për Promovimin e të Drejtave të Pacientëve në lidhje me këtë rast të abuzimit me të dhënat e pacientit. Qëllimi i këtij komunikimi ishte t'i kërkonte shoqatës të përdorte ndikimin e saj dhe të mbështeste kërkesën e këshilltarëve tek DORH-i për ta çuar këtë rast tek Zyra e Prokurorisë së Shtetit jashtë qytetit të Dubrovnikut.

Vetëm disa ditë më vonë, në 7 mars 2014, shoqatat u mblodhën në "Platforma 112'' për të ngritur akuza kundër Zyrës së Prokurorisë së Shtetit në Bashkinë e Dubrovnikut për shkak të dyshimeve për korrupsion politik. Një akuzë specifike pretendonte se, megjithëse kishte prova, ky institucion në mënyrë të padrejtë i pushoi akuzat kundër mjekut diabetolog. Po ashtu, ato informuan Avokatin e Popullit në Kroaci rreth mungesës së hetimit nga ana e Agjencisë kroate për Mbrojtjen e të Dhënave Personale mbi këtë çështje dhe kritikuan Dhomën kroate të Shëndetësisë.

Në këtë rast ka të paktën tre skenarë të mundshëm të keqpërdorimit të IT-së:

a) të dhënat private të pacientëve merreshin në mënyrë të paligjshme nga dikush në Spitalin e Përgjithshëm të Dubrvonikut, me sa duket nga dikush afër kandidatit për kryetar bashkie, me qëllimin e vetëm të krijimit të një liste me adresa për zgjedhjet lokale;

b) dikush hyri në bazën e të dhënave nga jashtë – u ndërhy nga jashtë dhe askush nga spitali nuk mund të jetë drejtpërdrejtë përgjegjës për këtë gjë;

c) dikush nga spitali morri të dhënat për një qëllim tjetër dhe pastaj dikush tjetër, pranë kandidatit për kryetar bashkie, i shtiu në dorë ato të dhëna.

Kroacia, rasti 2: Të dhënat konfidenciale të radio-televizionit kroat në tregun e zi

Sipas ligjit kroat për radio-televizionin, çdo person fizik dhe juridik në Kroaci që ka në pronësi një televizion apo radio është i detyruar të paguajë një tarifë për licencën. HRT ka dhe administron një regjistër ku janë emrat e atyre që paguajnë për licencën çdo muaj në Republikën e Kroacisë. Ky regjistër nuk është i hapur për publikun. Meqënëse ai përmban të dhëna personale të përdoruesve, të tilla si emri dhe mbiemri, adresa, Numri Personal i Identifikimit (OIB), etj., menaxhimi dhe përdorimi i tij mbrohen me dispozita të legjislacionit për sigurinë e të dhënave personale. Sipas informacionit të Regjistrit Qendror, i hapur për publikun, me të dhëna personale që është në sistemet e Agjencisë për Mbrojtjen e të Dhënave Personale, regjistri i HRT-së është në një server në të cilin mund të kenë akses fizik vetëm personat e autorizuar. Përdoruesit e autorizuar i përdorin të dhënat e këtij regjistri duke futur emrin e tyre të përdoruesit dhe fjalëkalimet ose vërtetimin. Përdorimi

është i mundshëm nga rrjeti lokal dhe interneti duke përdorur kalime të mbrojtura të të dhënave. Së fundi, kopje të sigurta gjenden tek dhoma e serverit.

Por, në vitin 2004, një CD me një kopje të këtyre të dhënave doli në tregun e zi. U supozua se CD ishte përgatitur nga një punonjës i Radio-Televizionit kroat (HRT) që punonte me këtë listë të dhënash dhe përfitonte nga shitja e paligjshme e tyre.

Në këtë rast, IT është keqpërdorur nga një punonjës i HRT-së me synim kopjimin e qëllimshëm dhe shitjen e të dhënave. Ky punonjës ose kishte vetë autorizim të hynte tek regjistri, ose njihte dikë që kishte akses tek ai regjistër. Si rezultat, janë shkelur të gjitha masat teknike mbrojtëse të përmendura më sipër si edhe dispozitat e rregullave të përgjithshme të punës dhe etikës së HRT-së, sipas të cilave punonjësit e HRT-së duhet të punojnë në përputhje me standardet më të larta të punës dhe standardet themelore të etikës, mbi bazën e disa vlerave, përfshirë konfidencialiteti dhe mbrojtja e të dhënave, në përputhje me legjislacionin përkatës dhe rregullat e përgjithshme. Është e qartë që këto standarde nuk janë zbatuar.

Një anëtar i Bordit Drejtues të OJQ-së "Potrosac" ("Konsumatori") e raportoi këtë rast tek Departamenti i Krimit Ekonomik (DECO) në Ministrinë e Brendshme. Për shkak të ankesave të shpeshta të abonentëve dalmatianë, që ndjeheshin të lodhur nga kompanitë që ofronin shërbimet e tyre përmes ofertave të katalogut duke përdorur adresat e marra nga arkivi i HRT-së, në 2004, HRT ndërmorri një hetim të brendshëm tek departamenti për mbledhjen e tarifave të licencimit. Megjithatë, hetimi nuk solli rezultate dhe abonentët janë ende objektiva të ofertave të ndryshme të bujshme të kompanive.

1.3.3 Kroacia, rasti 3: Në kërkim të veteranëve

Për vite të tëra, një nga mosmarrëveshjet më të mëdha në shoqërinë kroate ka qenë përcaktimi i numrit të saktë të veteranëve të luftës. Gjithmonë ka pasur hamendësime se në mbrojtjen e vendit gjatë Luftës për Pavarësi kanë marrë pjesë më shumë njerëz se sa ishin regjistruar. Meqënëse të dhënat zyrtare për këtë çështje nuk janë bërë asnjëherë publike, kjo ka qenë një nga temat kryesore në luftën politike ndërmjet partisë nacional-konservative në pushtet HDZ (Hrvatska Demokratska Zajednica – Bashkimi Demokratik Kroat) dhe opozitës. HDZ gjithmonë nuk donte të publikonte regjistrin e veteranëve dhe opozita e akuzonte për fshehjen e shifrave sepse në këtë mënyrë kjo gjë bënte të mundur që shumë njerëz, që nuk kishin të drejtë të quheshin veteranë, të përdornin privilegjet e veteranëve. Veteranët gëzojnë një numër përfitimesh, duke filluar me pensione të larta, apartamente falas dhe privilegje kur blejnë një makinë. Sipas opozitës, në këtë mënyrë HDZ po blinte mbështetjen popullore. Në 6 prill 2010 adresa e internetit www.registarbranitelja.com papritur botoi një listë të paplotë të veteranëve[29]. Autorët e kësaj faqe ishin anonim, dhe siç shkruanin ata tek kjo faqe, qëllimi i tyre ishte të ndalonin korrupsionin dhe t'i detyronin autoritetet kroate të botonin një listë të plotë të veteranëve.

Ky botim shkaktoi reagime të forta në të gjithë vendin. Pastaj, kryeministri i vendit Jadranka Kosor e quajti atë "vepër e informacionit të fshehtë", dhe Ministria e Brendshme menjëherë deklaroi se ai ishte një akt kriminal i dënueshëm me deri në tre vjet burgim. Ministria e Mbrojtjes (MoD) dhe Ministria e Veteranëve (VM) kërkuan hetim të menjëhershëm nga Prokuroria e Shtetit. Po ashtu, DM njoftoi se sistemi i vet i IT-së nuk ishte vënë në rrezik dhe se nuk kishte pësuar ndonjë lloj sulmi kibernetik në tentativë.

Ish-Ministri i Veteranëve pretendoi se kishte shumë njerëz që mund të shihnin këto të dhëna. Ai tha se në vitin 2003, kur ai ishte në detyrë, i kishte marrë të dhënat në një CD. Sipas Pancic, qeveria mund të zbulonte se kur ishin vjedhur të dhënat thjesht duke krahasuar informacionin e publikuar me regjistrin aktual. *"Kur isha ministër, kishte 403000 veteranë, tani janë më shumë se 500000...ndoshta dikush e vodhi CD-në gjashtë vjet më parë dhe e botoi atë vetëm tani",* tha Pancic.

Disa ditë më vonë, policia zbuloi informacion për katër ish-punonjës të Zyrës së Mbrojtjes (një degë e MoD) në Karlovac, dhe dyshoi se ata kishin vjedhur të dhënat. Hetimi tregoi se këta të katër i kishin botuar të dhënat në internet, por gjithashtu se punonjësit e zyrës së Mbrojtjes, në total 23, kishin mundësi të shikonin të njëjtat të dhëna. Nuk u ngritën akuza kundër katër personave nga Karlovaci. Po ashtu, nuk pati lajme në media për ndonjë të akuzuar për shkelje. Qeveria kroate i kërkoi kompanisë që merrej me adresën www.registarbranitelja.com ta hiqte informacionin, por pronari refuzoi ta bënte këtë. Regjistri i veteranëve ishte në internet deri në prill 2012, kur mbaroi edhe afati i asaj adrese. Regjistri zyrtar u publikua në 19 dhjetor 2012, dhe përfshiu pjesën më të madhe të informacionit të botuar në adresën jozyrtare.

Ky është një shembull i shpërdorimit të detyrës. Meqënëse të dhënat u botuan, mund të supozohet se dikush nga një Zyrë e Mbrojtjes i kishte marrë ato, i botoi ose i dha, ose edhe i shiti tek dikush tjetër që pastaj i botoi. Mund të ketë shumë arsye të ndryshme për botimin e regjistrit, duke filluar nga mosmarrëveshjet politike deri tek motive fisnike, të tillë si përpjekja për rritjen e transparencës. Megjithatë, nuk ka dyshim se arsyeja kryesore pse ndodhi kjo gjë ishte mungesa e protokolleve për sigurinë minimale në procedurën e trajtimit të informacionit që i shpërndahej Zyrave të Mbrojtjes në qytete të ndryshme kroate.

29 Veteranët ishin përfshirë në mbrojtje përmes Ministrisë së Mbrojtjes dhe Ministrisë së Brendshme - kjo listë përmbante vetëm njerëzit e futur nga Ministria e Mbrojtjes.

Kroacia, rasti 4: Me një ndihmë të vogël të nëpunësve civilë, 68 pasaporta kroate iu shitën kriminelëve

Me anë të një aksioni të përbashkët nën emrin e koduar “Kufiri”, Ministria e Brendshme (MUP) dhe Zyra për Luftën kundër Korrupsionit dhe Krimit të Organizuar (USKOK) identifikuan shtatë persona të akuzuar për falsifikim dhe shitje të pasaportave kroate tek kriminelë nga Serbia, Bosnja dhe Hercegovina dhe Mali i Zi. Që nga viti 2006 deri në fund të vitit 2010 grupi shiti 68 pasaporta false për 10.000 euro secila, duke fituar kështu një shumë minimale të paktën 680.000 euro.

Një nëpunëse civile e Zyrës Konsullore kroate në Orasje të Bosnjës dhe Hercegovinës nuk u dërgua në gjykatë sepse ajo bëri një marrëveshje me USKOK dhe pranoi një dënim me një vit burgim. Një tjetër, që punonte si oficer i lartë tek Drejtoria e Pasaportave në Policinë e qarkut të Zagrebacka, u akuzua për shpërdorim detyre dhe u dënua me 13 muaj burgim. Pesë anëtarë të tjerë të kësaj organizate kriminale janë ende në pritje të gjyqit.

Roli i organizatorit të të gjithë kësaj veprimtarie ishte të merrte informacion rreth njerëzve që kishin shtetësi kroate por nuk kishin pasaporta. Ai rregullonte falsifikimin e pasaportave duke përfshirë palë të treta (kryesisht kriminelë), mblidhte fotografitë, dhe gjysmën e pagesës për të cilën ishte rënë dakord. Roli i dy policëve dhe një oficeri të lartë të Drejtorisë së Pasaportave në Policinë e qarkut të Zagrebacka ishte të kontrollonin saktësinë e të dhënave të mbledhura më parë nga kolegu i tyre rreth personave që kishin shtetësi kroate, por nuk kishin pasaporta. Ata i kontrollonin këto të dhëna në sistemin e informacionit të MUP-it, pikërisht tek regjistri për dokumentet e udhëtimit të shtetasve kroatë (hrv. Evidencija putnih isprava hrvatskih drzavljana), që përbën një nga regjistrat në sistemin e informacionit të MUP-it.

Ata mund ta kryenin këtë detyrë sepse në përputhje me pozicionin e tyre të punës, ata kishin emër përdoruesi dhe fjalëkalim që duheshin për të hyrë tek Regjistri me dokumentet e udhëtimit të shtetasve kroatë. Megjithëse këto të dhëna duhej të përdoreshin vetëm për qëllime pune, ata shpërdoruan detyrën dhe i përdorën ato të dhëna për qëllime kriminale.

Pas marrjes së të gjithë informacionit të nevojshëm për njerëzit pasaportat e falsifikuara të të cilëve do të përdoreshin, ata falsifikuan autorizimin për marrjen e pasaportës. Me këtë autorizim, pasaportat mund të merreshin tek Misionet Diplomatike dhe Konsullore të Republikës së Kroacisë në Bosnjë dhe Hercegovinë dhe Serbi. Kjo pjesë e punës i ishte caktuar një nëpunësi civil që punonte tek Zyra Konsullore kroate në Orasje, Bosnjë dhe Hercegovinë.

Kroacia, rasti 5: Polici u kap ndërsa fuste të dhëna të rreme tek sistemi i informacionit të policisë

Në vitin 2005, një polic nga Zagrebi futi të dhëna të rreme tek arkivi zyrtar i policisë që vërtetonin se një burrë i vjetër 64 vjeç nga Serbia dhe Mali i Zi raportoi humbjen e kartës së tij kroate të identitetit, megjithë faktin që nuk kishte as shtetësinë kroate, dhe as kartë identiteti kroate. Për më tepër, ai printoi një vërtetim mbi humbjen e kartës kroate të identitetit, i vuri një vulë zyrtare dhe e futi në sistemin e informacionit të MUP-it, pikërisht tek Regjistri i kartave të identitetit (hrv. Evidencija osobnih iskaznica), që përfaqëson një nga regjistrat e sistemit të informacionit të MUP-it. Ai mundi ta realizonte këtë detyrë sepse ai, në përputhje me pozicionin e tij të punës, kishte emër përdoruesi dhe fjalëkalim për të hyrë në Regjistrin e kartave të identitetit. Duke bërë këtë gjë, ai abuzoi me detyrën e tij duke futur të dhëna të rreme në Regjistër.

Gjatë procesit të zakonshëm të kontrollit, shefi i komisariatit të policisë vuri re këtë letër konfirmimi tek sistemi i informacionit dhe pati dyshime në lidhje me vërtetësinë e saj. Pas procesit të verifikimit u vërtetua se ky dokument ishte i falsifikuar dhe që polici i dyshuar kishte shpërdoruar detyrën e tij. Si rezultat, oficeri i policisë u hoq nga shërbimi dhe policia ngriti akuza penale kundër tij.

Sipas informacionit të policisë, polici i dyshuar nuk kishte marrë rryshfet nga qytetari i Serbisë dhe Malit të Zi. Ai falsifikoi vërtetimin mbi humbjen e kartës së identitetit si një favor për një shok të përbashkët për përmirësimin e situatës ligjore të një 64 vjeçari që u përpoq të merrte shtetësinë kroate.

1.3.6 Kroacia, rasti 6: Oficerë policie që fshijnë kundravajtjet në trafik dhe zbulojnë të dhëna konfidenciale: bile ata pranuan si rryshfet edhe mish qingji të pjekur dhe 20 litra verë!

Pas një periudhe të gjatë përgjimesh dhe ndjekjeje, një aksion i përbashkët i Ministrisë së Brendshme (MUP) dhe Zyrës për Luftën kundër Korrupsionit dhe Krimit të Organizuar (USKOK), i kryer nën emrin e koduar “Kamioni”, përfundoi me arrestimin e 37 personave, 11 nga të cilët ishin oficerë policie. Ata dyshoheshin se kishin zbuluar të dhëna konfidenciale nga sistemi i informacionit të MUP-it. Oficerët e policisë dyshohej se kishin shpërdoruar detyrën dhe kishin marrë rryshfete nga pronarët e kompanive të transportit, artizanët dhe transportuesit. Po ashtu, kishte dyshime se ata kishin dhënë informacion për vendin dhe kohën e kontrollit të mjeteve të transportit nga kompania kroate Motorways Ltd. (HAC) në të paktën 80 raste. HAC-u është një nga katër kompanitë që kryejnë aktivitetin e tyre në rrjetin kroat të autostradave duke mbikëqyrur transportin e mallrave të rrezikshme, duke marrë të dhëna mbi mjetet nga sistemi i informacionit i MUP-it. Së fundi, dyshohej se ata kishin fshirë kundravajtjet në trafik nga sistemi i informacionit të MUP-it. Rryshfetet e marra për shërbimin e sipërpërmendur ishin para, dhe në një rast mish qingji i pjekur dhe 20 litra verë. Në përputhje me kompetencat dhe nevojat e tyre si policë trafiku, ata kishin emër përdoruesi dhe fjalëkalim, gjë që i lejonte ata të hynin në informacione të ndryshme tek sistemi i informacionit të policisë, mes të tjerave edhe tek të dhënat për vendin dhe

kohën e kontrolleve të mjeteve të transportit nga kompania kroate Motorways Ltd. (HAC) që mbikëqyrte transportin e mallrave të rrezikshme, si edhe informacion mbi automjetet. Megjithëse roli i tyre kryesor ishte të siguronin sigurinë e të gjithë pjesëmarrësve në trafik, ata kishin vendosur të shpërdoronin kompetencat e tyre dhe të merrnin informacion që të përdorej për qëllime kriminale.

Kroacia, rasti 7: I kapur rastësisht për zbulim të të dhënave konfidenciale për automjetet dhe pronarët e tyre!

Ndërsa gjurmoheshin organizatorët e një rrethi ndërkombëtar prostitucioni gjatë një aksioni të policisë kroate dhe spanjolle, agjentët e policisë zbuluan rastësisht një shkelje të një oficeri policie dhe një oficeri në administratë në policinë e qarkut Medimurska. Për një periudhë dymujore, oficeri i policisë dhe punonjësi i administratës i kishin dhënë informacion konfidencial për makinat dhe pronarët e tyre njërit prej të arrestuarve gjatë aksionit "Catalunya". I arrestuari, që është ish-oficer policie, përveçse rekrutonte vajza për të punuar në Lloret de Mar, Spanjë, ku detyroheshin të punonin si prostituta, gjithashtu merrej edhe me rishitjen e makinave. Kur bliheshin makina të përdorura, polici rrugor dhe punonjësi i administratës ia kalonin informacionin për makinën dhe pronarin e saj të arrestuarit. Ata e merrnin këtë informacion nga sistemi i informacionit të MUP-it, pikërisht nga Regjistri i Regjistrimit të Automjeteve (hrv. Evidencija registracije cestovnih vozila). Ata mund ta kryenin këtë detyrë sepse në përputhje me pozicionin e tyre të punës, ata kishin emër përdoruesi dhe fjalëkalim për të hyrë tek të dhënat e Regjistrit. Duke bërë këtë, ata shpërdoruan detyrën e tyre dhe kishin shkelur ligjet për mbrojtjen e të dhënave personale.

Nuk dihet nëse kjo bëhej për përfitime monetare apo si një nder për ish-kolegun. Kundër të dyve u ngritën akuza penale dhe ata u pezulluan nga policia deri në përfundimin e procedurës disiplinore.

Kroacia, rasti 8: Çdo vit zhduken 2 milion euro nga kabinat e taksës së autostradës

Në 31 dhjetor 2003, gjatësia e përgjithshme e rrjetit të autostradave në Kroaci arriti në1288.5 km. Kur përdorin autostradën, shoferët janë të detyruar të paguajnë taksën e rrugës. Të ardhurat e përgjithshme në vitin 2003 arritën në 296.688.044 euro (përjashtuar TVSH)[30].

30 HUKA – Shoqata kroate e Koncesionarëve të taksës së Autostradës. Raporti Kombëtar për autostradat në Kroaci për vitin 2013. Gjendet tek: http://www.huka.hr/en/news/223-national- report-on-motorways-in-croatia-for-the-year-2013

Megjithatë, sipas disa drejtorëve të kompanisë kroate Motorways Ltd. (Hrvatske autoceste - HAC, një nga katër kompanitë që është pjesë e Rrjetit kroat të Autostradave), 1% e tarifave, që kap vlerën 1.7 deri 2 milion euro, zhduket çdo vit. Të dyshuarit kryesorë për këtë humbje janë punonjësit e HAC-ut që punojnë në kabinat e taksës së autostradës. HAC-u ka vënë re se disa prej punonjësve të tij prodhojnë deri në dhjetë herë numrin e faturave që pastaj anulohen dhe riprintohen me datë të ndryshuar. Për shembull, kur një kamion shfaqej tek kabina e taksës së autostradës, punonjësi që punonte aty i kërkonte shoferit të paguante taksën e rregullt të autostradës për kamionin (që është më e lartë sesa e makinave). Pastaj, ai hynte tek sistemi i informacionit, anulonte faturën e sapo prodhuar, fuste të dhëna të rreme – që regjistronte se automjeti që kalonte nuk ishte kamion, por një veturë – dhe printonte një faturë të re. Meqënëse taksa ishte (dhe ende është) më e lartë për kamionët krahasuar me veturat, ai e mbante tepricën e parave për vete.

Në gusht 2010, një kontroll i auditimit të brendshëm të Autocesta Rijeka Zagreb d.d., kompania e dytë që është pjesë e Rrjetit kroat të Autostradave zbuloi se 22 punonjës po vidhnin para nga taksat në Demerje dhe Lucko. Ata u raportuan në polici dhe menjëherë u pushuan nga puna. Të udhëhequr nga parimi *in dubio pro reo,* gjyqtari theksoi se gjykata ka dyshime se ata kishin abuzuar me kompetencat e tyre dhe kishin kryer një krim, por nuk kishte prova për të provuar krimin e tyre. Duke lexuar arsyetimin, gjyqtari i ftoi ata të lexonin poezinë e E.A. Poe "The Raven", dhe t'i kushtonin vëmendje të posaçme fjalisë së fundit të secilës strofë: *Asnjëherë përsëri!*

Në këtë rast, Autocesta Rijeka Zagreb d.d. kishte përdorur auditimin e sistemeve të brendshme të IT-së si një masë mbrojtëse kundër korrupsionit të IT. Si një vazhdim i arsyetimit poetik të gjyqtarëve për të parandaluar raste të ngjashme në të ardhmen dhe si një masë mbrojtëse për IT-në, drejtuesit e HAC-ut vendosën të instalonin kamera për të mbikëqyrur punën e punonjësve në kabina. Këto kamera nuk kapnin fytyrat e punonjësve, as zërat e tyre, por vetëm vendin e tyre të punës, duart dhe procesin e pagesës/mbledhjes së taksës. Shuma e përgjithshme e këtij investimi ishte 354.000 euro.

Kroacia, rasti 9: Policë të korruptuar–oficerë policie që u dhanë të dhëna konfidenciale kontrabandistëve të armëve

Tre oficerë policie nga Zagrebi u kapën rastësisht duke iu dhënë informacion konfidencial nga sistemi i informacionit të Ministrisë së Brendshme (MUP) kontrabandistëve të armëve. Duke përgjuar një bisedë ndërmjet kontrabandistëve të armëve dhe policisë, hetuesit e shërbimit të kontrollit të brendshëm dëgjuan dhënien e të dhënave konfidenciale të sistemit të informacionit të MUP-it. Përveç zbulimit të të dhënave konfidenciale, oficerët e policisë kishin fshirë akuzat penale; falsifikuar dokumentacionin, dhe edhe u kishin dhënë këshilla disa prej të arrestuarve se si të mbroheshin gjatë hetimit dhe i njoftonin në rast se ata ndiqeshin nga policia.

I dyshuari i parë u dha miqve të tij, disa prej të cilëve ishin kriminelë, shumë informacion dhe të dhëna të marra nga sistemi i informacionit të MUP-it. Informacioni i dhënë përmbante nxjerrjen e urdhër arresteve, informacion privat për një kamariere që ata kishin marrë në punë në kafenenë e tyre, ose informacion për një nip që ishte larguar nga shtëpia. Dy oficerët e tjerë të policisë e ndihmuan kolegun e tyre të merrte të gjithë këtë informacion dhe të dhëna nga sistemi i informacionit të MUP-it.

Ata arrinin ta kryenin këtë gjë sepse ata, për shkak të pozicionit të tyre të punës, kishin emër përdoruesi dhe fjalëkalime për të hyrë në regjistra të ndryshëm. Duke vepruar kështu, ata abuzonin me kompetencat e tyre dhe shkelnin ligjet për mbrojtjen e të dhënave personale.

Kryesisht, "fshehtësia, integriteti, disponueshmëria dhe kontrolli i vazhdueshëm i të dhënave dhe informacionit të sistemit të informacionit të MUP-it realizohen përmes një numri masash dhe procedurash të organizimit, sistemit dhe programit si edhe ndarjes së detyrave dhe autorizimeve. Të gjithë përdoruesit e sistemit të informacionit të MUP-it janë të detyruar të zbatojnë mbrojtjen e të dhënave, siç parashikohet tek Udhëzimi për mbrojtjen e sistemit të informacionit të MUP-it bazuar tek përpunimi elektronik i të dhënave, Udhëzimi për sigurinë dhe mbrojtjen e të dhënave zyrtare të MUP-it dhe direktiva dhe udhëzime të tjera të brendshme që drejtojnë aktivitetet e mbrojtjes së të dhënave të sistemit të informacionit të MUP-it".

Si rezultat i hetimit, policia ngriti akuza kundër 23 personave, mes tyre 3 oficerë policie. 13 nga të akuzuarit u shpallën fajtorë dhe bënë marrëveshje me USKOK-unpër dënime të buta. I dyshuari i parë në fund u dënua me 6 muaj burg, një dënim që tashmë është zëvendësuar me 50 ditë punë në komunitet. Po ashtu, gjykata e ndaloi të punonte si oficer policie për tre vjet. 2 oficerët e tjerë, së bashku me 8 peronat e akuzuar për marrjen e informacionit në mënyrë të paligjshme ende janë në pritje të gjyqit.

Kroaci, rasti 10: Oficeri i policisë i dënuar me një vit burgim sepse lejoi mikun e tij të peshkonte në mënyrë të paligjshme

Në maj 2012, Këshilli i Gjykatës së Qarkut Rijeka shpalli fajtorë dy ish-policë dhe një person tjetër për abuzim me të dhënat konfidenciale të policisë. Njëri ish-oficer i policisë i kishte dhënë një të njohuri të tij iformacion të fshehtë nga sistemi i informacionit të Ministrisë së Brendshme (MUP) mbi regjistrimet e mjeteve dhe profilet e pronarëve të tyre. Për të mbuluar hyrjen e tij në sistem dhe për të marrë vetë informacionin, ai përdori kredencialet e hyrjes në sistem të kolegëve të tij. Duke bërë kështu, ai kishte shpërdoruar detyrën e tij dhe kishte shkelur ligjin për mbrojtjen e të dhënave personale.

Kryesisht, "fshehtësia, integriteti, disponueshmëria dhe kontrolli i vazhdueshëm i të dhënave dhe informacionit të sistemit të informacionit të MUP-it realizohen përmes një numri masash dhe procedurash të organizimit, sistemit dhe programit si edhe ndarjes së detyrave dhe autorizimeve. Të gjithë përdoruesit e sistemit të informacionit të MUP-it janë të detyruar të zbatojnë mbrojtjen e të dhënave, siç parashikohet tek Udhëzimi për mbrojtjen e sistemit të informacionit të MUP-it bazuar tek përpunimi elektronik i të dhënave, Udhëzimi për sigurinë dhe mbrojtjen e të dhënave zyrtare të MUP-it dhe direktiva dhe udhëzime të tjera të brendshme që drejtojnë aktivitetet e mbrojtjes së të dhënave të sistemit të informacionit të MUP-it". Përgjegjësitë e pozicionit të punës së oficerëve përcaktojnë nivelin e mundësisë për marrjen e të dhënave ".

Ai u dënua me një vit burgim për kryerjen e tre veprave kriminale të shpërdorimit të detyrës. Po ashtu, ai u ndalua të punonte në të ardhmen në administratën shtetërore për pesë vjetët e ardhshëm. Një ish-polic tjetër u dënua me 5 muaj burgim për veprën e inkurajimit të tjetrit për të kryer vepra penale, ndërsa i njohuri i tyre u dënua me 4 muaj burgim për të njëjtën vepër.

Nga dhjetori 2007 deri në qershor 2008, polici i parë i dënuar i kishte dhënë informacion nga sistemi i informacionit të MUP-it edhe kolegut të tij të dalë në pension. Ky informacion kishte të bënte me kohën kur anijet e patrullimit të policisë patrullonin në detin Porec. Si rezultat, ai e dinte kur ishte e sigurt të nxirrej në mënyrë të paligjshme dater (lat. Lithophaga lithophaga, hrv. prstac), një lloj butaku që mbrohet fort me anë të Vendimit për Mbrojtjen e Specieve të Egra (Fletorja zyrtare, nr. 7/06 dhe 99/09).

1.3.11 Kroacia, rasti 11: Inspektori i lartë përdori të dhëna konfidenaciale për të fituar zgjedhjet lokale

Një inspektor i lartë i Administratës së Taksave dhe Tatimeve në Ministrinë e Financave hyri në sistemin e informacionit të administratës tatimore në vitin 2010, me qëllim të zbulonte sasinë e borxhit në tatime të rivalit të tij në zgjedhjet për kryetarin e degës të Partisë Demokratike të Kroacisë (HDZ) në një zonë të Zagrebit të quajtur Spansko. Po ashtu, ai përdori të dhënat e Regjistrit të Taksapaguesve që tregonin borxhin e rivalit të tij tek tatimet me qëllim që të përgatiste një fletëpalosje për zgjedhjet e ardhshme, në 1 qershor 2010. Në këtë fletëpalosje, përveç informacionit për borxhin tek tatimet, ai shkroi *"Me ata që shmangin pagimin e taksave në shtet do të ecim përpara ne ?"* Ai arriti ta kryente këtë gjë sepse ai kishte leje të merrte të dhëna të caktuara personale të taksapaguesve përfshirë, mes të tjerave, të rivalit të tij. Në fund, ai i fitoi zgjedhjet.

Si pasojë, rivali i tij ngriti akuza kundër tij për abuzim me detyrën tek Sekretari i Shtetit për Administratën Tatimore. Gjykata për Nëpunësit Civilë e shpalli atë fajtor për *"shkelje të rëndë të detyrës profesionale"* dhe e dënoi me 15 për qind ulje të pagës së tij për një periudhë katërmujore. Ai dorëzoi një kërkesë tek Gjykata e Lartë e Nëpunësve Civilë, kërkesë e cila

u refuzua. Mbi bazën e këtij vendimi, rivali i tij ngriti akuza kundër tij tek Gjykata e Nderit e HDZ-së. Megjithatë, partia u tregua e butë dhe vetëm e qortoi për veprimet e tij.

Sipas nenit 62 të Ligjit për Tatimet mbi të Ardhurat (Fletorja Zyrtare 177/04, 73/08, 80/10, 114/11, 22/12, 144/12, Vendimit të USRH-120/13, 125/13, 148/13) me qëllim ofrimin e të dhënave të nevojshme për llogaritjen e taksave, taksapaguesit ose përfaqësuesit e tyre ligjorë janë të detyruar të dorëzojnë një kërkesë për regjistrim në regjistrin e të ardhurave të taksapaguesit tek zyra lokale e administratës tatimore në vendbanimin ose vendqëndrimin e zakonshëm.

Neni 8 i Ligjit të Përgjithshëm për Taksat(147/08, 18/11, 78/12, 136/12, 73/13) fut konceptin e sekretit tatimor. Të gjitha të dhënat e deklaruara nga taksapaguesi dhe të gjitha të dhënat e marra gjatë procedurave të tatimeve konsiderohen të jenë sekret tatimor. Kjo përfaqëson një formë të mbrojtjes që parandalon përdorimin ose publikimin e paautorizuar të të dhënave të tilla tek publiku. Detyrimi i ruajtjes së sekretit tatimor zbatohet për të gjithë personelin zyrtar, ekspertët dhe persona të tjerë që marrin pjesë në procedurat tatimore. Sidoqoftë, neni 8, paragrafi 2, i Ligjit të Përgjithshëm për Taksat përmban dispozita, që nën disa rrethana të caktuara, disa të dhëna nuk konsiderohen sekret tatimor. Këto janë: të dhëna për datën e hyrjes dhe datën e daljes nga sistemi i taksës së vlerës së shtuar, dhe të dhëna për taksapaguesit që ofronin të dhëna të rreme në lidhje me taksën e vlerës së shtuar. Paragrafët 5, 6, 7 dhe 12 parashikojnë rastet në të cilat nuk shkelet detyrimi për ruajtjen e sekretit tatimor. Po ashtu, sipas parashikimeve të nenit 9 të Ligjit të Përgjithshëm për Taksat, palët që i nënshtrohen marrëdhënieve të ligjit për taksat, janë të detyruara të veprojnë në mirëbesim; që do të thotë në mënyrë të ndërgjegjshme dhe të drejtë. Në rastin e posaçëm të përshkruar më lart, inspektori i lartë i administratës tatimore në Ministrinë e Financave shpërdoroi detyrën e tij. Ndryshimi i të dhënave në Regjistrin e Taksapaguesve për të diskredituar kundërshtarin e tij politik shkeli sekretin tatimor. Sjellja e tij nuk ishte as etike, dhe as besnike.

Kroacia, rasti 12: Nuk keni kaluar asnjë ditë të jetës suaj në punë? Nuk ka problem, përsëri mund të marrësh pension të plotë!

Megjithëse ajo nuk kishte punuar asnjëherë, në vitin 2007 një zonjë e moshuar filloi të marrë pensionin. Gjatë tre viteve të fundit, ajo morri më shumë se 20.000 euro. Në vitin 2007, vajza e saj punonte tek Instituti kroat i Sigurimit të Pensioneve (HZMO) si përgjegjëse e Zyrës së Auditimit të Brendshëm. Kolegët e saj dyshonin se ajo hyri tek sistemi i informacionit të pensioneve dhe ndryshoi të dhënat e mamasë së saj për të bërë të mundur që ajo të merrte pension. Prandaj, ata e raportuan këtë mashtrim të dyshuar tek drejtuesit e HZMO-s. Ajo mundi ta kryente këtë mashtrim sepse ajo mund të hynte në të dy regjistrat e HZMO-s: regjistri kryesor për personat që përdornin sigurimin e pensionit dhe regjistri kryesor për përdoruesit e të drejtave të sigurimit të pensionit.

Gjatë hetimit, u zbulua se ajo kishte falsifikuar edhe librin e punësimit, kështu që kundër saj u ngritën akuza penale. Megjithatë, edhe pse hetimi provoi se mamaja e saj nuk kishte të drejtë të merrte pension, policia nuk mundi të provojë se e bija e kishte ndihmuar të fitonte këtë të drejtë. Në fund, ajo u transferua nga pozicioni i përgjegjëses së Zyrës së Auditimit të Brendshëm në pozicionin e koordinatores në sektorin e çështjeve të brendshme. Megjithëse mamaja e saj nuk kishte të drejtë të merrte fonde pensioni, ajo asnjëherë nuk e ktheu pensionin e marrë në mënyrë të paligjshme.

Kosova

Nga Hasan Preteni dhe Driart Elshani

Arritjet në fushën e Teknologjisë së Informacionit (IT) kanë ndihmuar shumë në modernizimin e institucioneve kombëtare, duke i dhënë kështu një forcë më të madhe efikasitetit të punës së institucioneve. Sidoqoftë, nuk është çdo gjë në favor të punës së ndershme dhe efektive. Mbështetur tek praktikat e punës të agjencive antikorrupsion që në vitin 2006, në Kosovë ka pasur shumë raste kur Teknologjia e Informacionit nuk është përdorur për qëllimet e synuara.

Çdo nëpunës civil në Kosovë ka postën elektronike zyrtare të tij/saj që ka në adresën @rks-gov.net. Kjo duhet të përdoret për komunikimet zyrtare ndërmjet punonjësve dhe të tjerëve – dhe vetëm për të kryer detyrën zyrtare. Çdo përdorues i kësaj fushe mund të gjejë lehtë dhe të shkruajë tek adresat e postës elektronike të punonjësve të tjerë të institucioneve shtetërore. Rreth 70000 punojës të institucioneve në Kosovë përdorin adresën e përmendur më lart. Ky numër përfshin nivelet e pushtetit qendror, rajonal dhe lokal; punonjësit e të gjithë "juridiksioneve" (legjislative, ekzekutive dhe gjyqësore); zyrën e presidentit, dhe mekanizma të tjerë të pavarur, të tillë si: policia e Kosovës, dhe agjenci të ndryshme të ngritura nga Parlamenti i Kosovës ose përmes mekanizmave të tjerë.

Adresat zyrtare të postës elektronike duhet të përdoren vetëm për komunikime zyrtare. Megjithatë, shpesh ka raste kur rrjeti përdoret për çështje private, personale ose për qëllime të partive politike ose për qëllime tregtare. Njerëz me influencë, gjatë fushatave elektorale, shpesh e shpërdorojnë adresën zyrtare duke u bërë thirrje nëpunësve civilë të votojnë për ta ose për partinë e tyre politike.

Disa prej nëpunësve civilë në bashkëpunim me biznese të ndryshme kanë krijuar të ashtuquajturat "Organizata profesionale për trajnimin e nëpunësve civilë", që kanë përvetësuar buxhete për trajnime. Po ashtu, është shpërdoruar edhe rrjeti kompjuterik i institucioneve të Kosvoës, duke dërguar reklama të ndryshme që ftojnë institucionet (nëpunësit civilë) të udhëtojnë jashtë vendit për seminare të paguara nga institucionet. Kjo ka bërë që shumë zyrtarë të marrin pjesë në seanca trajnimi joprofesionale me një organizim të dobët që nuk i sillnin ndonjë përfitim institucionit, por shumë fitimprurëse për kompanitë që organizonin trajnimin në bashkëpunim me punonjësit e IT-së.

Një shkelje flagrante u regjistrua në një rast kur drejtori i një departamenti në një prej ministrive hapi një restorant jashtë Prishtinës, dhe përmes postës me adresë @rks-ks.net njoftoi hapjen e restorantit dhe përdori postën elektronike zyrtare për të dërguar ftesat, edhe tek drejtuesit e institucioneve qendrore, të merrnin pjesë në ceremoninë e hapjes. Ky njoftim doli që ishte i dëmshëm për nëpunësin civil, meqënëse disa ditë pasi media zbuloi se nëpunësi civil e përdori e-mailin zyrtar për të njoftuar dhe dërguar ftesë private restoranti i tij u sulmua dhe u dogj deri në themele për të mos u hapur më kurrë përsëri. Megjithatë, kjo mund të ketë qenë më shumë për shkak të zemërimit të publikut sepse ai hapi një restorant si zyrtar publik, sesa për shkak të mjeteve të zgjedhura të komunikimit.

Të gjitha institucionet e Kosovës kanë faqet e tyre të internetit. Por, si rezultat i sigurisë së pamjaftueshme të rrjetit kompjuterik të institucioneve, pothuajse të gjitha institucionet janë sulmuar të paktën një herë nga "hackers".

Rastet kur nëpunësit civilë, gjatë orëve të punës, i përdorin kompjuterat për të komunikuar me persona të ndryshëm në rrjetet sociale, duke mos qenë kështu efikas në punën e tyre dhe duke keqpërdorur teknologjinë për nevoja personale nuk janë të rralla.

Po ashtu, janë identifikuar raste të ndryshme kur punonjësit e përdorin internetin, pas orëve të punës, për të parë materiale pornografike ose lundrojnë në rrjete të ndryshme që përhapin imoralitet.

Përveç këtyre formave të përdorimit të padëshiruar të teknologjisë së informacionit, më poshtë do të paraqiten disa raste specifike që dëmtuan institucionet dhe nga të cilat përfituan individët.

Kosova, rasti 1: Shkatërrimi i provave

Në Kosovën e pasluftës dolën shumë kërkesa për stabilizimin e situatës dhe sigurimin e menjëhershëm të mirëqenies së qytetarëve përmes krijimit të vendeve të reja të punës dhe krijimit të kushteve për zhvillimin e përgjithshëm të vendit. Në atë kohë, një nga prioritetet e qeverisë ishte përmirësimi i infrastrukturës rrugore. Një shumë e konsiderueshme fondesh u caktuan për asfaltimin e rrugëve lokale dhe rajonale. Për shkak të situatës pas konfliktit, shumë pak kompani ishin të specializuara për këtë lloj pune. Pritshmëritë e qytetarëve ishin të mëdha, prandaj çdo veprim mirëpritej nga qytetarët. Por, shumë shpejt publiku e kuptoi që puna për riparimin e rrugëve nuk ishte kryer me të njëjtin standard siç ndodhte para lufte.

Disa prej zyrtarëve të qeverisjes qendrore e shfrytëzuan këtë situatë. Zyrtarët, në bashkëpunim me pronarët e kompanive ndërtuese, filluan të shpërdoronin fondet dhe të mos zbatonin ligjin në fuqi. Zyrtarët e shtetit filluan të kërkonin rryshfet nga secila kompani që donte të fitonte kontratën e punës.

Sasia e kërkuar për kontraktimin e punës ishte 10-20% e vlerës së përgjithshme të tenderit. Që prej krijimit të saj, Agjencia Antikorrupsion ka marrë informacion për vepra të ndryshme korrupsioni në këtë fushë. Rasti më i veçantë ishte kur një pronar biznesi u ankua me qëllim që të fitonte një kontratë pune disa milionëshe, zyrtarët e shtetit i kishin kërkuar një pagesë të lartë, me shtatë shifra (ose 15%) të vlerës së përgjithshme të tenderit.

Ky ndërtues ishte shumë i shqetësuar dhe vendosi të kontaktojë me Agjencinë Antikorrupsion. Ai u prit nga zyrtarët e agjencisë, dhe duke pasur parasysh mandatin e agjencisë dhe

Memorandumin e Bashkëpunimit të firmosur me prokurorët e Misionit Europian për Shtetin Ligjor në Kosovë (EULEX), Agjencia vendosi t'ia përcjellë këtë informacion EULEX-it. Vlera e tenderit ishte shumë e lartë, dhe po kështu i lartë ishte edhe niveli i personave të dyshuar që kishin kërkuar rryshfet. Çështja ishte shumë e ndjeshme, dhe hetimet filluan menjëherë. Në mesin e vitit 2007, hetuesit u futën në ambjentet ku punonin këta zyrtarë dhe morën një numër të madh materialesh fizike, disa kompjutera dhe materiale të tjera në formë elektronike dhe disa prej zyrtarëve u arrestuan.

Disa ditë më vonë, zyrtarët e agjencisë sekuestruan disa pajisje elektronike të vendosura në Ministrinë e Administratës Publike. Sipas rregullave institucionale të zbatuara në të gjithë administratën publike në Kosovë, serverat për ruajtjen e të dhënave të të gjitha institucioneve qeveritare janë të vendosura brenda ministrisë. Në të njëjtën ditë, hetuesit e EULEX-it arrestuan dy punonjës të IT-së. U zbulua se të gjitha materialet që hetuesit prisnin të gjenin tek serverat e ministrisë dhe që do të provonin dyshimet e Agjencisë Antikorrupsion në lidhje me parregullsitë dhe shkeljet e ligjit, ishin fshirë nga serverat e qeverisë. Qëllimi i vetëm i këtyre hetuesve ishte të gjenin prova kundër zyrtarëve të përfshirë në korrupsion. Kishte supozime se ishte fshirë informacioni që përmbante prova për ofertat e kompanive të tjera me çmime më të ulëta. Duke fshirë të dhëna të tilla nga serveri, qëllimi ishte që tenderi t'i jepej kompanisëme çmimin më të lartë. Hetimet vazhduan për disa vite, dhe tashmë ky rast ka vajtur në gjykatë. Lista e personave të akuzuar, përveç punonjësve nga drejtoria e rrugëve, përfshin edhe dy punonjësit e IT-së në Ministrinë e Administratës Publike të cilët penguan hetimet duke fshirë të dhënat nga serverat qendrorë. Numri i përgjithshëm i punonjësve të akuzuar është 8-10 persona. Veprat penale për të cilat janë akuzuar janë shpërdorimi i detyrës zyrtare, mashtrimi në detyrë dhe falsifikimi i dokumenteve zyrtare. Si një masë për parandalimin e rasteve të tjera të ngjashme, serverat u vendosën nën një lloj forme të kontrollit të pavarur.

Kosova, rasti 2: Marrja e statusit "Invalid lufte"

Në Ministrinë e Punës dhe të Mirëqenies Sociale ka një drejtori të posaçme për invalidët e luftës. Në qershor të vitit 1999, pas luftës në Kosovë, shumë persona aplikuan për tu regjistruar në listën e veteranëve të luftës. Më vonë, në vitet 2003-2004, filloi puna për trajtimin e listës së veteranëve. Kishte shumë aplikantë, dhe ishte shumë tunduese të regjistroje njerëzit në atë listë, sepse, përveç përfitimeve materiale, ata do të fitonin edhe përfitime të tjera, të tilla si: trajtim shëndetësor preferencial, blerje automjeti pa paguar për zhdoganimin, dhe privilegje dhe përfitime të tjera për vete dhe anëtarët e familjes. Disa prej tyre e fituan menjëherë statusin, ndërsa disa e fituan më vonë – ata që e morën më vonë statusin shfaqën një problem.

Një person informoi dhe denoncoi tek Agjencia Antikorrupsion një person tjetër me inicialet F.M., që gëzonte pensionin e invalidit të luftës prej 250 euro në muaj, i vlerësuar me 30% aftësi të kufizuar. Informatori ishte nga i njëjti fshat si F.M. dhe e dinte faktin se F.M. nuk ishte me këtë nivel të aftësisë së kufizuar. Në Kosovë, ka tre shoqata të luftës: 1) Shoqata e veteranëve; 2) Shoqata e invalidëve; dhe 3) Shoqata e Martirëve Kombëtarë. Agjencia hapi çështjen, dhe në fillim kërkoi materiale nga tre shoqatat. F.M. ishte regjistruar si veteran – pjesëmarrës në luftë, por jo person me aftësi të kufizuar. Prandaj, agjencia përdori të drejtat e saj ligjore dhe kërkoi të dhëna dhe dokumentacion shoqërues për F.M. nga Ministria e Punës dhe e Mirëqenies Sociale. Pas marrjes së dokumentacionit, u vu re se kishte dallime thelbësore. Dokumenti bazë për dhënien e pensionit nuk ishte origjinal –ai ishte i falsifikuar. Një punonjës i IT-së ishte përgjegjës për falsifikimin e dosjes elektronike të F.M. duke futur dokumente të rreme të skanuara për marrjen e pensionit të aftësisë së kufizuar. Përfundimi i Agjencisë Antikorrupsion ishte se kishte një dyshim të fortë se punonjësit e kësaj zyre kishin falsifikuar të dhënat elektronike me qëllim që të bëhej e mundur një përfitim material – pensioni i aftësisë së kufizuar. Çështja u kalua nga agjencia tek prokuroria e shtetit, e cila për tre muaj angazhoi policinë në procesin e mbledhjes së provave. Gjatë hetimit penal, u gjetën shumë shkelje. Më shumë se1500 persona kishin fituar pensionin e aftësisë së kufizuar si viktima të aftësisë së kufizuar për shkak të luftës, pa qenë në fakt me aftësi të kufizuara, përmes falsisikimit të dokumentacionit. Edhe pasuria e personit që drejtonte zyrën ishte rritur shumë. Aktualisht çështja është në procesin e ngritjes së akuzave penale për aktet e parashikuara në Kodin Penal: mashtrimi në detyrë dhe falsifikimi i dokumenteve zyrtare. Tre zyrtarë të Drejtorisë së Pensionit të Aftësisë së Kufizuar të kësaj ministrie janë pezulluar nga detyra pa pagesë. Abuzimi kishte ndodhur gjatë skanimit të dokumentit, ku raporti mjekësor ishte falsifikuar. F.M. kishte paraqitur një dokument që vërtetonte se gjatë luftës në Kosovë ai kishte pasur probleme shëndetësore. Dokumenti nuk është që nga periudha e luftës, por ishte hartuar 5 vjet më vonë. Ai përmbante datat sikur ishte hartuar gjatë kohës së luftës. Ky rast tregon se nuk është e mjaftueshme të ushtrohen kontrolle tek sistemi i IT-së nëse këto kontrolle nuk shtrihen edhe tek dokumentet e shkruara që futen në sistem. Po ashtu, dobësitë e mundshme në sistemin e IT-së mund ta bëjnë të vështirë të tregohet se një dokument në fillim është skanuar dhe pastaj është futur në sistem.

1.4.3 Kosova, rasti 3: Keqpërdorimi i fjalëkalimit

Hartimi i listës për vendet bosh të punës me emrat e drejtorëve të klinikave në Qendren Universitare të Kosovës nuk ishte arritur disa herë. Ka një interes të veçantë tek personeli mjekësor për të qenë në krye të departamenteve. Në disa raste, Ministria e Shëndetësisë dhe në raste të tjera Komisioni i Pavarur mbikëqyrës, si organi që mbikëqyr nëpunësit civilë dhe punësimin apo shkarkimin e tyre, kanë anuluar vendet bosh. Për vite me radhë, pjesa më e madhe e klinikave janë drejtuar nga drejtorë të deleguar, të përkohshëm, ndërsa në qershor 2014, konkurrimi për vendet bosh u mbyll. U krijua komisioni i vlerësimit, u përgatitën pyetjet për intervista dhe u bënë të gjitha përgatitjet për procesin e marrjes në punë. Në disa klinika u emëruan drejtorët e rinj, por në tetë klinika nuk u emëruan drejtorët e rinj. Një prej kandidatëve për shef klinike mori informacion se disa prej kandidatëve të tjerë i kishin marrë që më përpara pyetjet, megjithëse supozohej se pyetjet ishin se-

kret deri në ditën e testimit. Një anëtar i komisionit mbikëqyrës informoi shtypin[31], dhe media publikoi adresën e postës elektronike nga e cila ishin dërguar pyetjet. Të kapur ngushtë nga të gjitha këto fakte dhe skandalit që do të pasonte, një anëtar i komisionit për përzgjedhjen e drejtorëve organizoi një konferencë për shtyp dhe pranoi se të dhënat u ishin dërguar disa prej kandidatëve nga kompjuteri i tij, por që nuk ishte ai përgjegjësi për këtë veprim. Zyrtari u përpoq ta hidhte përgjegjësinë tek një person që e akuzoi se kishte vjedhur dhe shpërdoruar fjalëkalimin e tij, dhe që e kishte përdorur kompjuterin e tij në mënyrë tëpaautorizuar, dhe se ai ia kishte dhënë fjalëkalimin e tij personal atij personi kur shkoi me pushime. Sidoqoftë, rezulatati i këtij skandali ishte se anëtari i komisionit dha dorëheqjen, vendi i lirë i punës do të shpallej përsëri, ndërsa përsa i përket masave të tjera që do të ndërmerreshin Agjencia Antikorrupsion nuk ka ende informacion për to.

Vitin e kaluar, Agjencia Antikorrupsion u informua në mënyrë jozyrtare se zëvendës drejtori i një departamenti në një prej mekanizmave të pavarura përdori adresën e postës elektronike të drejtorit në mënyrë të paautorizuar. Ka disa raste kur zyrtarë të lartë i japin të drejtë ndihmësve të tyre të përdorin adresat e tyre të postës elektronike për të komunikuar në emër të tyre. Megjithatë, rasti në fjalë përbën një sjellje joetike të një asistenteje që përdori adresën e postës elektronike të drejtorit të institucionit nga shtëpia e saj meqënëse ajo ishte me leje lindje.

Kosova, rasti 4: Falsifikimi i dokumenteve të taksave

Një kompani pastrimi morri pjesë në tender dhe fitoi kontratën për pastrimin e ndërtesës së një ministrie. E gjithë procedura filloi të zbatohet në përputhje me legjislacionin në fuqi. U shpall fituesi me çmimin më të ulët; kontrata u lidh dhe filloi zbatimi i kontratës. Pas disa muajve të zbatimit të kontratës, u përkeqësuan marrëdhëniet ndërpersonale ndërmjet personelit të kompanisë së kontraktuar. Pronari i kompanisë pushon nga puna një person që kishte punuar për shumë vite në ministri dhe që ishte përgjegjës për financat dhe prokurimet. I papunë dhe i zhgënjyer me situatën, ky person vendos “të hakmerret” kundër punëdhënësit të mëparshëm. Ai vendos të denoncojë kompaninë. Një ditë, Agjencia Antikorrupsion morri informacion nga një person anonim përmes postës elektronike: kompania e pastrimit që ishte në pronësi të një personi me një të kaluar të dyshimtë, fiton shumë tendera për mirëmbajtjen e ndërtesave të institucioneve qendrore të Kosovës. Informatori i tregon Agjencisë se si i fiton kompania të gjitha tenderat. Thelbi është që kjo kompani nuk i paguan taksat dhe prandaj jep oferta me çmimin më të ulët. Prova që taksat paguhen rregullisht është një nga dokumentet themelore që ofertuesi duhet të fusë në dosjen e tenderit kur shpreh interesin për një kontratë. Pronari i kompanisë kishte përdorur aftësitë e tij për ta marrë këtë dokument mbi bazën e marrëdhënieve të mira me zyrtarët e taksave dhe tatimeve. Pas një pagese fillestare të një takse me vlerë të madhe, ai kishte përdorur të njëjtën faturë, por me data të falsifikuara. Të gjithë punonjësit e institucioneve mund të kërkojnë dokumentin origjinal, por ata ngurruan ta bënin këtë sepse ata e ndienin që kishin të bënin me një person me pushtet dhe dhanë shfajësimin se dokumenti ishte i skanuar dhe i plotësonte kushtet e tyre.

Agjencia kërkoi informacion për këtë kompani tek Administrata Tatimore. Dyshimet dolën që ishin të vërteta. Taksat nuk ishin paguar rregullisht, dhe dokumentet e përdorura nga kjo kompani për të fituar tenderin ishin të rreme dhe si të tilla nuk duhej të ishin pranuar. Agjencia shqyrtoi edhe shumë tendera të tjera të fituara nga kjo kompani dhe identifikoi tre institucione vendase dhe një institucion ndërkombëtar ku kishte punuar kjo kompani. Interesant ishte fakti që kompania paraqiti edhe një ofertë për mirëmbajtjen e ndërtesës së Agjencisë; megjithatë, në momentin e fundit oferta u tërhoq pa dhënë asnjë shpjegim. Një relacion kundër kësaj kompanie u dërgua disa muaj më parë në prokurori. Të gjitha institucionet janë njoftuar për gjetjet dhe kanë marrë kërkesë nga Agjencia që t’i japin fund kontratave të tyre me kompaninë. Por, pavarësisht kësaj, kjo gjë nuk ka ndodhur kudo. Institucioni ndërkombëtar e ndërpreu kontratën dhe filloi një çështje me prokurorinë e EULEX-it për kompensimin e dëmeve. Po ashtu, Agjencia i kërkoi Organit të Vlerësimit të Prokurimeve – Gjykatës së Tenderave ta vinte këtë kompani në listën e zezë, me qëllim që kompanisë të mos i jepej ndonjë punë tjetër me institucionet qeveritare. Fatkeqësisht, Agjencia ende nuk ka marrë konfirmimin që një veprim i tillë të jetë ndërmarrë nga institucionet e pushtetit vendor.

31 Daily Newspaper Tribuna, e mërkurë, 13 gusht, 2014, nr. 1538, viti 2014, faqe 10-11 http://www.gazetatribuna.com/?FaqeID=1

Maqedonia

Nga Marjan Stoilkovski dhe Rozalinda Stojova

Përkufizimi i korrupsionit në Maqedoni

Në terma ligjore në Republikën e Maqedonisë "korrupsion do të thotë përdorimi i funksionit, autorizimit publik, detyrës dhe pozitës zyrtare për qëllimin e fitimit dhe përfitimit për veten ose për një person tjetër"[32].

Korrupsioni mund të ndodhë në të gjitha nivelet e qeverisë, dhe viktima të tij mund të jenë individët, ose edhe komunitete të tëra. Korrupsioni është një krim kompleks që shpesh përfshin më shumë se dy palë, gjë që e bën më të vështirë për ta dalluar nga format e tjera të krimit; për këtë shkak, shpesh, hetimi nuk e trajton kurrë korrupsionin (përfshirë korrupsionin që ka të bëjë me manipulimin ose abuzimin e sistemeve IT) si një veprim të veçuar, përkundrazi ai është i lidhur me shkelje të tjera penale.

Renditja

Rezultatet e dy llogaritjeve më të fundit të Indekseve të Perceptimit të Korrupsionit (CPI) nga organizata "Transparency International" tregojnë se Maqedonia u rendit, përkatësisht, në vendin 69 dhe 67 në vitet 2012 dhe 2013, që në kontekstin rajonal e vendos Maqedoninë në vendin e dytë ndërmjet vendeve të ReSPA-s[33].

Sidoqoftë, nga një këndvështrim kulturor dhe social, është e rëndësishme që "qytetarët maqedonas renditin korrupsionin si problemin më të madh me të cilin përballet vendi i tyre pas papunësisë dhe varfërisë/standardeve të ulëta të jetesës" (hulumtimi i UNODC-së, 2011 – *Zyra e OKB-së Kundër Drogës dhe Krimit)*[34]

Viti	Renditja e vendit	Vendi/territori	Rezultati CPI
2012	69	Maqedonia	43
2013	67	Maqedonia	44

32 Ligji për Parandalimin e Korrupsionit, amendamentet e datës 2 korrik 2004 Përkufizimi i korrupsionit, neni 1-a http://www.dksk.org.mk/en/images/stories/PDF/law/2004.pdf
33 Në 2013, kjo është ndarë në vendin e dytë me Malin e Zi.
34 https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Corruption report_fYR_Macedonia_FINAL_web.pdf

Maqedonia, rasti 1: Abuzimi me sistemet e IT-së në tarifat autostradale

Ky është një rast ku është gjykuar abuzimi i pozitës zyrtare dhe që, sipas legjislacionit maqedon, konsiderohet veprim bazë korrupsioni. Ai ka të bëjë me manipulimin e sistemit të IT-së të tarifave autostradale, i cili përdoret për menaxhimin e procesit të pagesës së tarifave autostradale; menaxhimin e turneve të punonjësve; dhe proceseve të tyre të punës në pagesat autostradale.

Njësia për luftën kundër korrupsionit dhe njësia e krimit financiar u ngarkuan për hetimin e këtij rasti. Në fillim të hetimit, njësitë kërkuan zyrtarisht marrjen e të gjitha informacioneve të nevojshme për sistemin e IT-së nga kompania që instaloi dhe mirëmbante manaxhimin e tarifave autostradale. Hetimi zbuloi se kishte një gërshetim të disa lloje të abuzimeve të sistemit të IT-së, të kryera nga punonjësit:

- abuzimi i sistemit të IT-së duke përdorur të dhëna të ndryshme autentifikimi dhe duke përdorur kredencialet e punojësve të tjerë,
- të kombinuar me dhënien e urdhërit për zhdoganimin e automjetit, ose
- manipulimi i sistemit të IT-së duke ndryshuar shumën e paguar, ose
- duke mos regjistruar çdo automjet që kalonte në daljen e vendpagesës së tarifës, ose
- duke mos dhënë fatura dhe duke e ndarë tarifën me shoferët sipas parimit të ndarjes 50:50, ose
- duke shënuar një kategori të ndryshme të automjeteve.

U përdoren metoda speciale hetimore me qëllim mbledhjen e provave përkatëse. Të dhënat dhe informacionet e grumbulluara nga sistemi i IT-së gjatë hetimit ndihmuan për të identifikuar dhe provuar veprimtaritë e kundërligjshme të një grupi të organizuar kriminal. Në fund, dhe kryesisht përmes analizave të ndryshme të ndërmarra në të dhënat e sistemit të IT-së, u bë e mundur vlerësimi dhe llogaritja e dëmtimeve nga kompania.

Hetimi tregoi se pati abuzime nga persona në funksione zyrtare duke përdorur sistemin e IT-së, duke u mundësuar në këtë mënyrë punonjësve për të siguruar fitim të kundërligjshëm, i cili më vonë pastrohej përmes investimeve të ligjshme për mallra.

Akuza penale për këtë rast u depozitua më 1 dhjetor 2011, dhe 92 persona u dënuan për shpërdorim detyre dhe shërbimesh zyrtare, falsifikim, korrupsion (pranim i rryshfeteve) dhe për anëtarësim në një grup të organizuar kriminal. Duke përdorur veprimtari të tilla kriminale, grupi i organizuar kriminal fitoi në mënyrë të kundërligjshme 120 milionë denarë maqedon dhe u bë shkak që kompania të paguante gjoba me të njëjtën shumë.

Procedura gjyqësore u mbyll më 23 maj 2013 me dënime që varionin nga 3 deri në 6 vjet burg për 86 persona, ku dënimet përfshinin ripagimin e dëmeve të shkaktuara nga kompania për rreth 107 milionë denarë. Njëmbëdhjetë persona u dënuan me konfiskim të pasurive të tyre për një vlerë prej 5 milion denarë.

Pasi mbylljes së çështjes, kompania që zotëron pagesat autostradale në Republikën e Maqedonisë përmirësoi sistemin e IT-së për menaxhimin e procesit të tarifave autostradale dhe monitorimin e punës së punonjësve. U projektuan dhe u zhvilluan përmirësime në sistem për të kapërcyer problemet e identifikuara dhe të parashikuara si pasojë e automatizimit të proceseve të punës, shmangur futjen e të dhënave në sistemin e IT-së, dhe të ndërveprimit me vetë procesin.

Maqedonia, rasti 2: Sulmi në sistemin e IT-së të prokurimit publik

Në Republikën e Maqedonisë, duke filluar nga 1 janari 2012, sipas nenit 8 të Ligjit për Prokurimin Publik, autoritetet kontraktuese janë të detyruara të përdorin ankandin elektronik në 100% të njoftimeve për tender, të botuara, për procedurën e hapur, procedurën e kufizuar, procedurën e negociuar me botim të mëparshëm, dhe procedurën konkurruese të thjeshtuar.

Sistemi elektronik për prokurimin publik është një aplikacion i bazuar në internet ku reklamat, njoftimet, dhe tenderat botohen plotësisht në mënyrë elektronike dhe ku ofertuesit dërgojnë elektronikisht ofertat e tyre të depozituara fillimisht.

Sistemi është pronë e Zyrës së Prokurimit Publik, dhe menaxhohet nga një ofrues shërbimi lokal. Sistemi ka të instaluar një “firewall” dhe është i konfiguruar me Sistemin e Zbulimit të Ndërhyrjes (IDS), dhe me një VPN (Rrjet Privat Virtual) në mënyrë që të ofrojë akses të sigurtë në sistem. Vetë sistemi përdor protokollin e sigurtë https, dhe çertifikata SSL (Shtresë e Prizave të Sigurta).

Në nivel aplikacioni, sistemi regjistron lloje të ndryshme përdoruesish, autoritetesh kontraktuese, dhe operatorësh ekonomikë (kompanish). Sistemi ka nivelin e vet të moduleve të aplikacionit dhe u jep përdoruesve privilegje të përshtatshme aksesi.

Autoritetet kontraktuese kanë përdoruesit e tyre të brendshëm në nivel aplikacioni, d.m.th. administratori lokal, njësia e prokurimit, komisioni i prokurimit publik, dhe personi përgjegjës. Operatorët ekonomikë (kompanitë) kanë gjithashtu perdoruesit e tyre të brendshëm, dhe të gjithë ata gëzojnë privilegje të njëjta: aftësinë për të ndarë të njëjtat procedura elektronike, pjesëmarrjen në ankandet elektronike, drejtimin e pyetjeve, etj. Një seancë e autentifikuar nga një përdorues në nivel aplikacioni zgjat 40 minuta; nëse gjatë kësaj periudhe nuk ka aktivitet nga përdoruesi, atëherë ai çregjistrohet automatikisht.

Në gusht të vitit 2012 u botua një ofertë për prokurimin e automjeteve duke përdorur sistemin e IT-së për Prokurimin Publik. Procesi i ofertave për tender u menaxhua nga Sistemi i IT-së për Prokurimin Publik, dhe më shumë se një ofertues depozitoi ofertë. Gjatë procesit të ofertimit, sistemi i IT-së po funksiononte mirë deri në pak minutat e fundit, kur sistemi pësoi defekt – në këtë periudhë kohore nuk qe në gjendje të pranonte oferta, pavarësisht faktit që u bënë përpjekje për depozitim të ofertave të reja nga përdoruesit.

Në fillim, ky rast u raportua si ndërhyrje në sistemin kompjuterik dhe si një rast krimi kompjuterik. Kjo është një praktikë procedurale, e cila nënkupton që, fillimisht, të tilla raste hetohen si krim kompjuterik, ndërsa në fazën vijuese të hetimit dhe nëse ka prova për krime të tjera të kryera, rasti do të hetohet paralelisht edhe për vepra të tjera penale. Meqenëse ky incident ishte një rast që përfshinte prokurimin publik të një pajisjeje me vlerë të lartë, ai u konsiderua dhe u trajtua si një rast krimi kompjuterik dhe njëkohësisht si një lloj korrupsioni. Edhe pse, në fillim, nuk pati prova dhe informacione që ishte konsumuar korrupsion ose abuzim, hetimi mbuloi të dy aspektet e rastit.

Njësia e krimit kompjuterik e hetoi këtë çështje dhe u sigurua të ndërmerrte të gjitha hapat e nevojshëm që do të ndihmonin hetimin. Në fillim, nga kompania menaxhuese dhe nga Zyra e Prokurimit Publik, u kërkuan informacione bazë nga sistemi i IT-së, informacione teknike të detajuara, të gjitha loget përkatëse të sistemit, sigurisë, dhe administratës.

Njësia e krimit kibernetik mori loget *intepub nga serveri, të cilat përmbanin të dhënat e regjistruara të adresave IP që kishin hyrë në aplikacion, loget e aplikacionit dhe loget gjatë procesit të ankandit. Pas analizës së detajuar të informacionit të siguruar, duke përdorur sistemin operativ Linux dhe “bashscript-e”, u zbulua se në periudhën kritike sistemi pësoi defekt për shkak të sulmeve DDoS (Mosofrim i Shërbimit) të kryera nga një numër adresash IP që e kishin origjinën nga vende të huaja. Gjithashtu, hetimi identifikoi që oferta e fundit u depozitua nga kompania A vetëm pak sekonda para se sistemi të pësonte defekt, por kur kompania B u përpoq të depozitonte ofertën e saj, sistemi nuk ishte i disponueshëm dhe si rrjedhojë nuk ishte në gjendje të pranonte oferta.*

Kompania B e raportoi rastin si abuzim të mundshëm dhe dërgoi të dhënat, të cilat provonin që ata kishin depozituar një ofertë të re gjatë periudhës kur Sistemi për Prokurime Publike ishte i padisponueshëm dhe kjo ofertë nuk ishte regjistruar dhe për rrjedhojë nuk ishte pranuar.

Më vonë hetimi zbuloi që Sistemi i IT-së për Prokurim Publik nuk ishte faqja e internetit e vënë në shenjestër për sulmin DDoS, por shënjestra ishte një faqe tjetër interneti (faqe interneti informative). Për shkak se të dy sistemet ndodheshin në të njëjtin server, të dy shërbimet e internetit ishin të padisponueshëm.

Bazuar në loget e siguruara, u përcaktua se gjatë periudhës kritike pati shumë kërkesa që dërgoheshin në sistemin ndaj të cilit u kryen sulmet dhe jo në shërbimin e internetit që menaxhonte sistemin e prokurimit publik.

Sulmi DDoS është një nga metodat e përdorura për të bërë të padisponueshme disa shërbime në Internet. Duke dërguar në sistem një numër të madh kërkesash, ai bëhet i padisponueshëm meqenëse sistemi nuk mund të trajtojë dhe përpunojë të gjitha kërkesat. Kur sistemi arrin në atë pikë ku nuk mund të trajtojë të gjitha kërkesat që i dërgohen,

zakonisht ai fiket vetvetiu. Në shumicën e raste ky lloj sulmi kryhet duke përdorur botnets (një rrjet i përbërë nga shumë kompjutera të kontrolluara nga një kompjuter me qëllimin e kryerjes së disa aktiviteteve).

Ky lloj sulmi nuk i shkakton shumë dëme sistemit që sulmohet, siç janë fshirja apo ndryshimi i të dhënave. Ai vetëm sa bën që sistemi të jetë i padisponueshëm, zakonisht, duke fikur disa shërbime të sistemit ose duke e fikur plotësisht sistemin.

Në fund, ky rast nuk u provua se ishte një rast shpërdorimi detyre dhe korrupsioni, por ai jep një vështrim të përgjithshëm të procedurës dhe metodave të mundshme të abuzimit të sistemeve të IT-së për qëllim korrupsioni, nëpërmjet shpërdorimit të detyrës ose të "*social engineering*-ut" (manipulimit të njerëzve për të marrë informacione konfidenciale). Duke patur parasysh teknologjitë që përdoren për mbështetjen dhe përmirësimin e punës dhe shërbimeve të përditshme, mund të identifikojmë shumë *modioperandi* (mënyra veprimi) për abuzim të sistemeve të IT-së.

Administratori i sistemit ka privilegje të plota në sisteme për një periudhë kohe të zgjatur, dhe nëse veprimet e tij/saj nuk kontrollohen dhe monitorohen siç duhet, ai/ajo mund të abuzojë sistemin duke shkatërruar ose ndryshuar provat dixhitale, dhe për pasojë, duke e bërë të pamundur hetimin e rastit dhe të vërtetimit të abuzimit.

Maqedonia, rasti 3: Abuzimi nëpërmjet sistemit të IT-së dhe zbulimi i kundërligjshëm i të dhënave personale

Zhvillimi i teknologjive dhe instalimi i zgjidhjeve të reja teknike si instrumente për lëvrimin e shërbimeve në sektorin publik rrisin rreziqet e abuzimit të mundshëm të pozitës zyrtare nga nëpunësit e institucioneve të sektorit publik.

Rasti i përshkruar këtu është një rast rast shpërdorimi detyre dhe lejes për akses në sistemin e IT-së që përmban të dhëna të kufizuara ose të dhëna që mund të bëhen të njohura vetëm sipas kushteve specifike. Mbështetur në legjislacionin kombëtar për mbrojtjen e të dhënave personale, institucioni që mban ose përpunon të dhëna personale është i detyruar të ndjekë procedura të veçanta për zbulimin e të dhënave personale.

Në rastin në fjalë, një nëpunës i një institucioni të sektorit publik me të drejtën e aksesit në të dhënat e sistemit të të ardhurave financiare shpërdoroi pozitën e tij dhe zbuloi informacione të tilla. Megjithëse procedurat përcaktojnë që informacione të tilla mund të bëhen të njohura me kërkesë personale të qytetarit ose të përfaqësuesve nga agjencia ligjzbatuese me urdhër gjykate, në këtë rast nëpunësi nuk respektoi procedurat për zbulimin e të dhënave personale, dhe lëshoi një dokument zyrtar të krijuar nga sistemi i IT-së, i cili përmbante të dhëna personale. Më vonë ky dokument zyrtar u përdor si provë në një proces civil.

Ky rast u hetua nga tre aspekte: abuzim i të dhënave personale nga ana e nëpunësit dhe institucionit (hetuar nga Drejtoria për Mbrojtjen e të Dhënave Personale); shpërdorim detyre dhe shërbimit zyrtar i nëpunësve (korrupsion i mundshëm, d.m.th. mitmarrje ose me qëllim sigurimin e përfitimeve dhe avantazheve të tjera); dhe abuzim i të dhënave personale sipas Kodit Penal Kombëtar, neni 149 për abuzimin me të dhënat personale (hetuar nga Ministria e Brendshme).

Nga hetimi i kryer për abuzim të të dhënave personale dhe abuzim të postit zyrtar u grumbulluan prova që tregonin se nëpunësi kishte lëshuar në mënyrë të paligjshme një dokument nga sistemi i IT-së dhe se ai/ajo kreu një vepër penale. Provat u nxorën nga sistemi i IT-së dhe nga sistemi i vëzhgimit me kamera (CCTV). Megjithëse në këtë rast nuk u provua ligjërisht mitmarrja ose marrja e përfitimeve dhe avantazheve të tjera, fakti që nëpunësi kishte lejen për të përdorur sistemin por nuk kishte autorizim nga zotëruesi i të dhënave për t'i bërë ato publike, u konsiderua nga organi hetimor (policia dhe prokuroria) si një formë korrupsioni, siç përcaktohet nga legjislacioni kombëtar.

Ky është vetëm një nga shembujt e shpërdorimit të detyrës dhe ka mjaft raste të ngjashme me të, d.m.th. shpërdorim të detyre për publikimin e informacionit. Fakti është se shpesh raste të tilla nuk raportohen si vepra penale, por hetohen vetëm brenda institucionit.

Maqedonia, rasti 4: Keqpërdorimi i sistemit të regjistrimit të orëve të punës

Në dekadën e fundit sistemet që regjistrojnë orët e punës janë integruar në punën e përditshme të shumë institucioneve, ndërmarrjeve publike, spitaleve, dhe shkollave. Sistemet regjistrojnë kohën e ardhjes dhe të largimit nga vendi i punës, si dhe mungesat private dhe zyrtare, dhe të dhëna e ruajtuara përdoren për të numëruar orët e punës së punonjësve gjatë një periudhe të caktuar kohe. Numri i orëve të punës përdoret për të llogaritur pagat e punëtorëve, për të përcaktuar periudhat e mungesës së vazhdueshme të punonjësit, dhe për analiza të tjera. Sipas ligjeve përkatëse qëndrimi në punë pas orëve të përcaktuara të punës nuk do të thotë automatikisht orë pune ekstra. Nga ana tjetër, ardhja me vonesë në punë në mënyrë të përsëritur gjatë një periudhe të shkurtër pune përbën një arsye për nisjen e procedurave disiplinore. Kjo është e zbatueshme në veçanti në institucione që punojnë me një turn, duke ditur se në Maqedoni nuk ka orar pune "me turne" në administratë.

Në një nga institucionet ku ishte instaluar një sistem i tillë për të regjistruar orët e punës, ishte caktuar një person i vetëm në rolin e administratorit përgjegjës për menaxhimin e të gjithë sistemit. Privilegjet e administratorëve përfshijnë mundësinë për të inspektuar dhe parë paraprakisht regjistrat e pranisë në punë dhe për të hartuar raporte të përgjithshme dhe raporte specifike të tilla si për një punonjës të veçantë, për një grup punonjësish, ose raporte për një periudhë të caktuar.

Pasi luajti rolin e administratorit për më shumë se dy vjet, punonjësi dalloi mundësinë e shfrytëzimit të sistemit për avantazh të tij/saj në një mënyrë që ai/ajo mund të ndryshonte kohën e ardhjeve dhe largimeve që ato të përputheshin me ato të përcaktuara ligjërisht, dhe jo me ato realet. Këtë gjë punonjësi e bëri për më shumë se një vit e gjysëm pa u vënë re nga kolegët apo supervizorët. Një ditë punonjësit i lindi nevoja të ndryshonte të dhënat për atë mëngjes ose për ditën e fundit të punës, pa kontrolluar mënyrën se si po menaxhoheshin dhe mbaheshin të dhënat në sistem, dhe sidomos pa kontrolluar mënyrën se si regjistroheshin aktivitetet e administratorit. Megjithëse rrallë, kur jepej rasti, mundësia për të keqpërdorur sistemin u përdor jo vetëm për ardhjet me vonesë, por për gjithë ditën.

Afërsisht dy vjet pasi ishte caktuar roli i administratorit, institucioni bëri ricaktimin e detyrave për punonjësit, gjë që bëri që administratori të ishte një person tjetër. Administratori i ri hapi rastësisht regjistrat e ngjarjeve dhe vuri re se disa nga ngjarjet ishin shënuar, duke i bërë ato të ndryshme nga të tjerat. I interesuar për të zbuluar se si ndryshonin nga të tjerat, administratori i ri nisi t'i vëzhgonte regjistrat me detaje. Shumë shpejt u bë e qartë se çfarë kuptimi kishin ngjarjet e shënuara dhe ai/ajo i raportoi ato tek bordi drejtues.

Procesi hetimor nisi me caktimin e një personi zyrtar IT-je nga institucioni, detyra kryesore e të cilit ishte të rishikonte të gjitha raportet dhe regjistrat e ngjarjeve. Përfundimi i kësaj procedure përkoi plotësisht me hamendësimet e bëra nga administratori i ri.

Për shkak se punonjësi bëri rrëfimin e ngjarjes, rasti nuk u ndoq penalisht por u zgjidh brenda institucionit. U bë vlerësimi i dëmit të shkaktuar nga ai/ajo nga mosardhja në punë dhe mospërmbushja e detyrave, dhe për këtë vlerë punonjësi u dënua me masa të përshtatshme disiplinore. Megjithatë, kontrata e punonjësit nuk u zgjidh.

Maqedonia, rasti 5: Abuzimi i të drejtave të administratorit

Në procesin e dhënies së lejeve për import, midis një liste dokumentash që kërkohen, duhet depozituar një garanci bankare me një vlerë të atillë që është proporcionale me vlerën e mallrave ose shërbimeve që importohen. Rregullat janë shumë strikte, sa më e lartë të jetë garancia bankare, aq më e lartë është vlera e lejuar e mallrave të importuara.

Sistemi për kontrollin e të dhënave në pikat kufitare dhe dhënies së lejeve përdor të dhënat që futen, ruhen, dhe mbahen në qendrën administrative të Institucionit A. Ndërkohë që disa nga të dhënat grumbullohen mbi bazën e shkëmbimit ndërmjet këtij sistemi dhe sistemeve të institicioneve të tjera, vlera e limituar nga garancia aktuale bankare futet në sistem nga nëpunësit e administratës dhe jo nga sistemet e informacionit të bankave.

Gjatë kryerjes së transfertave nga një qendër administrative tek tjetra, një administrator zbuloi një mënyrë për të përfituar nga pozicioni i tij. Pasi ai lëvizi nga qendra administrative

B tek qendra administrative C ai vuri re që privilegjet e tij të aksesit ishin të njëjta, kështu që ai krijoi vetë një llogari përdoruesi. Kryeadministratori nuk kreu kontrolle dhe rishikime të rregullta të privilegjeve të administratorëve të rivendosur në qendra të tjera, kështu që administratori në fjalë pati mundësinë të kryente shkelje duke përdorur llogarinë e re të përdoruesit të cilën e kishte krijuar.

Gjatë periudhës dyvjeçare dhe duke përdorur llogarinë e rreme në mbi 100 raste dhe llogarinë e tij në një dyzinë rastesh të tjera, nëpunësi futi në sistem vlera më të larta të garancisë bankare para kryerjes së kontrolleve në pikat kufitare dhe pas kryerjes së kontrolleve vendoste vlerat e vërteta. Në momentin kur punonjësit e kufirit kontrolluan sistemin e tyre, të dhënat e ndryshuara nga administratori shfaqeshin ashtu siç i përshkruan ligji. Ai qëndronte në kontakt të vazhdueshëm me drejtuesit e kompanisë me qëllim që të dinte me ekzaktësi kohën kur mallrat do të arrinin në kufi. Për një periudhë mundësisht sa më të shkurtër, regjistrat në institutin A përmbanin deklarime të garancive bankare me vlerë më të lartë.

Ky rast u zbulua nga kontrolli dhe auditi i brendshëm në bashkëpunim me departamentin dixhital gjatë kryerjes së auditimeve të zakonshme. U krijua një ekip hetimor për të shqyrtuar rastin dhe për të identifikuar që ai ishte faktikisht një rast korrupsioni, për të mos thëne se ndoshta ishin konsumuar edhe vepra të tjera penale, dhe për të parë se në çfarë shkalle ishin kryer vepra penale.

Gjatë analizimit të ngjarjeve në regjistrat e sistemit, ekipi hetimor i IT-së përcaktoi adresën IP nga e cila ishin kryer ndryshimet, e cila i çoi ata tek kompjuteri i administratorit. Dosjet e regjistrave nuk mund të ndryshoheshin kështu që është shumë e lehtë për të bërë një listë veprimesh të kryera nga administratori.

Fakti që veprimi ishte i paramenduar u zbulua më tej nga zgjedhja që kishte bërë për emrin dhe fjalëkalimin e llogarisë. Ai kishte siguruar që gjatë kontrolleve të zakonshme llogaria dhe fjalëkalimi do të ishin gjërat më të fundit që do të kontrolloheshin dhe që të ishin ato që nuk do të dilnin në pah, duke shmanguar në këtë mënyrë çdo dyshim që mund të lindte.

Është provuar vetëm që ai përdori këtë mënyrë abuzimi të sistemit të Institucionit A në bashkëpunim me një kompani lokale. U vlerësua që dëmi financiar që iu shkaktua vendit kapte vlerën 10.614.779.00 dinarë.

Mali i Zi

Nga Dusan Drakic dhe Ivan Lazarevic

Mali i Zi, rasti 1: Shpërdorimi i detyrës dhe falsifikimi i dokumenteve zyrtare

Rasti në shqyrtim është një shembull i neglizhencës në vendin e punës dhe ushtrim i paligjshëm i autoritetit shtetëror, d.m.th. abuzim autoriteti dhe shpërdorim detyre nga persona të punësuar në atë autoritet.

Pasaporta e personit "A" kishte skaduar dhe ai mori një pasaportë të re. Funksionarët në autoritetin kompetent të Ministrisë së Brendshme të Malit të Zi vendosen të përdorin pasaportën e vjetër, që kishte skaduar, për qëllime kriminale. Duke përdorur vulën e atij autoriteti ata zgjatën vlefshmërinë e pasaportës së vjetër, të skaduar, për pesë vjet duke mbajtur emrin e "A-së", por me fotografinë e një personi të tretë "B".

Me sa duket, personi "B" kërkohej nga policia. Si pasojë, "A" u ndalua në terminalin e pasagjerëve në aeroportin e Lizbonës, ku ai ishte nisur për të punuar në një anije gjatë periudhës së ardhshme. Pasi i kontrolluan dokumentet e identifikimit, një skuadër e ndërhyrjes e policisë e çoi atë (me pranga) në Qendrën e Emigracionit që ndodhej në aeroport, ku u mbajt për 48 orë, dhe më pas policia e vuri (me duar të lidhura) në një aeroplan për ta deportuar nga Portugalia në Beograd përmes Zvicrës. Ai nuk i kishte parë dokumentet e tij deri sa mbërriti në Zvicër. Trajtimi që i bënë autoritetet portugeze dhe imazhi që u krijua për të si kriminel nënkuptuan që personi "A" pësoi ankth mendor, dhe emri i tij i mirë u dëmtua në qytetin e tij të lindjes, para familjes së tij, miqve etj.

Mungesa e asgjeësimit të pasaportës së skaduar nga personi i autorizuar dhe veprimet e marra për të zgjatur perudhën e vlefshmërisë së pasaportës me të njëjtin emër, por me fotografi të një personi të tretë ("B") dhe vertetimi i gjithçkaje me vulë zyrtare, përfaqësojnë veprime që përbëjnë shkeljen penale të shpërdorimit të detyrës dhe njëkohësisht konfirmojnë sjellje të paligjshme të autoriteteve shtetërore.

Në këtë rast, funksionarët në autoritetin kompetent të Ministrisë së Brendshme të Malit të Zi nuk e asgjësuan pasaportën, e cila me lëshimin e një pasaporte të re ishte marrë nga personi "A", shtetas i Malit të Zi.

Gjykata e shkallës së parë në këtoë proces penal doli me përfundimin se mungesa e asgjësimit të pasaportës së skaduar nga personat e autorizuar, dhe veprimet e mëposhtme të shpjeguara në paragrafët e mëparshëm, përfaqësojnë veprime që përbëjnë shkeljen penale të shpërdorimit të detyrës, sipas nenit 216, paragrafi 1 të Kodit Penal të Malit të Zi, dhe shkeljen penale të falsifikimit të dokumenteve zyrtarë, sipas nenit 207, paragrafi 3 në lidhje me paragrafin 1 të Kodit Penal. Në atë kohë, shkelja parashikohej me një dëmin me burg nga 3 muaj deri në pesë vjet. Në përputhje me nenin 216 të Kodit Penal të Malit të Zi, shpërdorimi i detyrës shtetërore konsumohet nëse një zyrtar, duke përdorur funksionet ose kompetencat e tij/saj, duke tejkaluar kufijtë e kompetencave të tij/saj zyrtare ose nuk përmbush detyrat zyrtare të tij/saj, siguron për vete ose një person tjetër përfitime, shkakton dëme ose shkel rëndë të drejtat e një personi tjetër.

Pas apelimit të vendimit në shkallën e parë, Gjykata e Lartë e Malit të Zi konfirmoi vendimin e gjykatës më të ulët dhe në motivacionin e gjykimit, nr. 902/13 datë 12 prill 2013, përcaktoi qartë se:

"të gjitha faktet e paraqitura konfirmojnë gjithashtu sjellje të paligjshme të autoritetit të të pandehurit – shërbimet kompetente të Ministrisë së Brendshme të vendosura në Cetinje, e cila i shkaktoi dëm palës së prekur, për të cilën në përputhje me dispozitat e nenit 172, paragrafi 1 të ligjit të mëparshëm të vlefshëm për Kontratat dhe Përgjegjësitë Civile i pandehuri është përgjegjës dhe në përputhje me dispozitat e nenit 154 të të njëjtit ligj kompenson dëmin e shkaktuar. Në paraqitjen e përfundimit, Gjykata gjithashtu mori parasysh përmbajtjen e veprimeve konkrete të paraqitura më parë në këtë çështje të cilat përbëjnë sjellje të paligjshme të autoritetit të viktimës dhe të gjitha rrethanat e tjera të faktit, si dhe faktin që identiteti i personit të tretë, i cili abuzoi dokumentin e mëparshëm zyrtar të paditësit dhe të dhënat e tij të identifikimit, është konfirmuar, dhe që ai person ishte përshtatur për një sërë krimesh të kryera në një vend tjetër (Itali)."

Gjatë seancave gjyqësore, viktima provoi se, për shkak të sjelljes së paligjshme të autoritetit të të pandehurit, ai pësoi gjithashtu edhe dëm moral si pasojë e dëmit që iu shkaktua emrit të tij të mirë, nderit, shkeljes së lirisë dhe të drejtave të personalitetit.

Gjithashtu, duke u mbështetur në të dhënat e siguruara nga kompania e transportit detar në fjalë për sasinë e fitimeve (për të gjitha arsyet) të paditësit, të fituara gjatë kohës së lundrimit (dhe të hequra për periudhën për të cilën pati kundërshti), dhe në rregullat që përcaktojnë dëmtimet sipas kritereve në datën e vendimit (neni 189 paragrafi 2 i Ligjit për Kontratat dhe Përgjegjësitë Civile), shuma e dëmit material përkatës ndaj paditësit u përcaktua saktësisht nga një ekspert financiar që caktoi gjykata.

Përfundim 1

Shembulli i mësipërm tregon se ka një gabim apo defekt në sistemin e informacionit për lëshimin e pasaportave. Sistemi duhet, por nuk arrin, të eliminojë risqet që pasaportat të përdoren ose lëshohen pasi të ketë skaduar periudha e vlefshmërisë. Gjithashtu, është e qartë se një dokument i tillë nuk mund të zgjatej pa futur të dhëna të pasakta në sistemin e informacionit për lëshimin e dokumenteve të udhëtimit. Është interesante mungesa e gjurmëve elektronike të funksionarëve që lëshuan këtë dokument. Të dhëna duhet të jenë të disponueshme në sistemin e informacionit që shënojnë datën, kohën dhe emrin e funksionarit që hyri në sistem dhe përpunoi dhe lëshoi dokumentin. Sa më sipër tregon, gjithashtu, që sistemi për lëshimin dhe kontrollin e dokumenteve të udhëtimit, veçanërisht në pikat e kalimit kufitar dhe në aeroporte, duhet të jetë në gjendje të analizojë dhe zhdukë dokumente të tilla, të falsifikuara nëse shfaqen në sistemin e tyre. Numrat e identifikimit

të të tilla dokumenteve duhet të identifikohen automatikisht dhe të hiqen plotësisht nga regjistrat elektronikë, dhe vetë sistemi i IT-së duhet të jetë në gjendje t'i njohë ato si të pavlefshme (edhe pse këto të dhëna do të mund të përdoreshin vetëm në Malin e Zi, dhe jo në vende të huaja).

Për të zgjidhur këtë çështje dhe të tjera të ngjashme me të, është e nevojshme që bankat e të dhënave të IT-së të përditësohen rregullisht dhe të lidhen në shkallën më të madhe të mundshme, në mënyrë që numri i identifikimit i të tilla dokumenteve të mund të eliminohej elektronikisht nga përdorimi i mëtejshëm ose abuzimi nga faktorët njerëzorë. Sidoqoftë, mbetet ende rreziku nëse një dokument i tillë transferohet fizikisht në një vend të tretë, dhe përdoret atje si i vlefshëm, gjë që ngre çështjen e nevojës për bashkëpunim rajonal, me synimin e e zhdukjes së rreziqeve të mundshme.

Mali i Zi, rasti 2: Përdorimi i të dhënave të IT-së për të shkaktuar dëm politik

Për të provokuar destabilizim politik dhe për të diskredituar funksionarë të nivelit më të lartë, të qeverisë/politikanë ose për të siguruar fitim personal, u botua në media një listë e supozuar me numrat e telefonit të anëtarëve të një organizate të organizuar kriminale, e cila përmbante numrat e telefonit të funksionarëve të nivelit më të lartë të qeverisë/politikanë. Qëllimi ishte për të ndikuar opinionin publik duke i lidhur tërthorazi funksionarët me grupin e organizuar kriminal në fjalë, në mënyrë që të krijohej një imazh i një lidhjeje të supozuar ndërmjet autoriteteve dhe krimit të organizuar.

Në fund të vitit 2011, lista iu dërgua nga dy posta lokale një gazete të përditshme, si dhe në rrugë elektronike në një adresë IP-je nëpërmjet një rrjeti pa kabëll i cili ndodhej në një ndërtesë ku banonte një funksionar publik. Gazeta e përditshme botoi listën e supozuar, sipas së cilës kryetari i grupit kriminal, për të cilin ishte lëshuar një urdhër arresti nga Interpoli për trafik narkotikësh, kishte komunikime telefonike me një numër zyrtarësh qeveritarë në Malin e Zi. Çfarë është veçanërisht interesante është se lista i referohej komunikimeve telefonike të kryetarit të grupit kriminal nga viti 2008, dhe ishte mbajtur për tre vjet para se të publikohej. Ajo thelloi më tej dyshimet dhe spekulimet se dikush nga struktura operacionale e policisë/sektorit të çështjeve të brendshme/sektorit të sigurisë ishte përfshirë në këtë rast, i shtyrë nga lakimia apo hakmarrja, me qëllim që të shkaktonte destabilizim politik në vend në emër të tij ose në emër të personave ende të panjohur.

Rasti nuk u dërgua në gjyq, meqenëse hetimi zbuloi se nuk kishte patur komunikim telefonik ndërmjet funksionarëve të nivelit të lartë qeveritar/politikanëve dhe organizatorit kryesor të grupit kriminal, dhe që regjistrimi ishte i falsifikuar dhe nuk ishte një dokument i policisë, siç ishte botuar në media. Përveç kësaj, kompania telefonike e bëri të qartë se lista e publikuar, të cilën gazeta e përditshme pretendoi se operatori i telefonisë celulare ia kishte dorëzuar policisë për hetim, nuk ishte një listë nga kompania, d.m.th. nuk përputhej as në formë as në përmbajtje me ato që raportohen si të dhëna për trafikun e komunikacionit me kërkesë të organit kompetent, në përputhje me legjislacionin në fuqi të Malit të Zi. U konstatua që regjistrimi i personit, i përcaktuar si organizatori kryesor i grupit kriminal, dhe i bërë nga Drejtoria e Policisë për nevojat e tyre hetimore/operacionale, ishte falsifikuar, d.m.th. duke futur në të emrat dhe numrat e funsionarëve qeveritarë/politikanëve të nivelit më të lartë dhe adresat e tyre.

Megjithatë, ende nuk dihet se kush e siguroi listën origjinale ose atë që policia krijon për nevoja operacionale, as se kush ishte falsifikuesi i cili bëri që regjistrimi të dukej si origjinal. Po ashtu, nuk është e qartë si dhe mbi çfarë bazash Drejtoria e Policisë siguroi regjistrimin nga viti 2008, dhe çfarë lloj hetimi ishte kryer atëherë kundër organizatorit kryesor, të përmendur, të grupit kriminal, as se cilat ishin rezultatet e këtij hetimi dhe çfarë lloj provash ishin mbledhur në atë kohë.

Ajo që gjithashtu mbetet pa u zbuluar është dhe personi që dërgoi materialet, d.m.th. mesazhet e-mail nga adresa IP e përmendur më lart.

Ky rast paraqet një shembull klasik të shkeljes së të drejtave të njeriut të garantuara nga Kushtetuta dhe konventat ndërkombëtare, shkeljes së të drejtave të jetës private, abuzim i mundshëm i kompetencave, sepse regjistrimi i bisedës nuk mund të sigurohet pa vendim gjyqësor, as nuk mund të botohet në media. Gjithashtu, ky rast përfaqëson, me një mundësi të lartë, rastin e mitmarrjes dhe shpërdorimit të detyrës, si dhe falsifikimin e të dhënave dhe abuzim të sitemit të IT-së.

Përfundim 2

Shembulli i mësipërm tregon qartë dobësinë e sistemit të IT-së dhe mundësitë për abuzimin e tij. Ai ka të bëjë në plan të parë me parimin kushtetues që zbatohet për paprekshmërinë e konfidencialitetit të letrave, bisedave telefonike, dhe mjeteve të tjera të komunikacionit. Nga ana tjetër, qëndron çështja e përgjegjësisë së mundshme të personave përgjegjës në kompaninë operatore, kryesisht në lidhje me konfidencialitetin dhe përgjimin dhe abuzimin e postës elektronike. Operatori ka detyrimin të sigurojë parakushte të nevojshme teknike dhe organizative që lejojnë përgjimin e komunikimeve, d.m.th. për t'u mundësuar autoriteteve shtetërore përkatëse të sigurojnë të dhënat e ruajtura për trafikun dhe vendndodhjen, por vetëm pasi është dhënë një vendim gjykate, nëse është e nevojshme për zhvillimin e procedimeve penale, ose për arsye të sigurisë së Malit të Zi. Publiku nuk mori përgjigje nëse ekzistonte një miratim i tillë dhe cilat hetime ishin ndërmarrë nga policia në atë kohë dhe pse. Rasti doli që kishte qenë tepër i ndërlikuar, sepse përveç elementeve të mundshëm të abuzimit të pushtetit ai ndërthur edhe elementë të krimit kibernetik, i cili kërkon një nivel të lartë njohurie, aftësi trajnuese dhe teknike, si dhe mbështetje cilësore ndërkombëtare.

Rasti nuk pati një epilog gjyqësor as nuk dha përgjigje për një sërë pyetjesh të mësipërme. Nuk u përcaktuan përgjegjësi objektive apo subjektive. Sigurisht, përveç dëmit politik që ishte shkaktuar nga këto ngjarje, ajo që është edhe më e rëndësishme është fakti që nëse

ky rast, pavarësisht motivit dhe arsyeve, mund të ndodhte tek funksionarët shtetërore të nivelit më të lartë, çfarë mund të priste qytetari i zakonshëm i Malit të Zi, nëse ai/ajo do ta gjente veten në një situatë të njëjtë ose të ngjashme.

Gjithashtu, do të përmendim këtu edhe reagimin e papërshtatshëm dhe të pamjaftueshëm nga ana e autoriteteve shtetërore për të përcaktuar përgjegjësi objektive për punën e institucioneve dhe aftësi për zbulimin e shkelësve, e cila shkakton pa dyshim dëm të pallogaritshëm në humbjen e besimit të qytetarëve në punën e institucioneve. Kërkohet të bëhen përpjekje të mëtejshme dhe të analizohet plotësisht sistemi ekzistues me qëllim që të përcaktohen proceduara të qarta për marrjen dhe përdorimin e të dhënave operacionale dhe për të përcaktuar masa parandaluese, të qarta dhe specifike, me përdorimin e softuereve dhe aftësive të IT-së. Në veçanti, është e nevojshme të vazhdohet në përmirësimin e komunikimit me publikun dhe mediat në të tilla raste me qëllim që të rritet besimi i publikut në punën e tyre.

Mali i Zi, rasti 3: Shpërdorimi i funksioneve dhe futja e të dhënave të pasakta në regjistrat publikë

Ky rast ka të bëjë me prodhimin elektronik të licensave fallso ose certifikatave të tjera, me qëllim përdorimin e certifikatave të tilla në procedime ligjore.

Nga gjykimi i Gjykatës Bazë në Kotorr në vitin 2010, dy persona, një funksionar dhe kryetari i kadastrës bashkiake të një bashkie në Malin e Zi, u shpallen fajtorë për veprën penale të shpërdorimit të detyrës publike, sipas nenit 416, paragrafi 3 në lidhje me paragrafin 1 të Kodit Penal të Malit të Zi. Gjykimet përcaktuan se ata kishin përdorur postet e tyre për të siguruar fitim të paligjshëm, dhe kishin tejkaluar kufijtë e kompetencave zyrtare duke marrë dhe publikuar vendime për të cilat nuk kishin kompetencë. Nëpërmjet vendimit të parë ata mundësuan rikthimin dhe transferimin e tokës shtetërore tek pronarët e supozuar të mëparshëm, të cilët regjistruan tokën në regjistrin elektronik të tokës, dhe e shitën atë menjëherë pas regjistrimit. Në të njëjtën kohë dhe në të njëjtën mënyrë ata lëshuan një vendim tjetër me përmbajtje të rremë, dhe më pas sipërfaqe të tjera të specifikuara iu kthyen pronarëve të mëparshëm, të supozuar. Në këtë rast, pronari i supozuar e shiti tokën menjëherë pas regjistrimit të pabazuar, edhe pse pronari nuk kishte një tapi të vlefshme, me ndihmën e firmave të personave të akuzuar. Duke kryer dhe mundësuar veprime të tilla dhe me rikthimin e tokës, personat e akuzuar siguruan fitime në shumën 571.307.32 euro.

Këta dy persona u dënuan me dy vjet burg.

Është provuar që të dy të pandehurit në rastin e caktuar kishin tejkaluar kufijtë e kompetencave të tyre zyrtare. Gjithashtu, është provuar që procedura e rikthimit dhe transferimit të tokës nuk ishte paraprirë nga një vendim i Parlamentit lokal, si dhe që ai vendim ishte marrë pa kërkesën e personave të autorizuar, ish-pronarëve, duke shmangur në këtë mënyrë procedurën e parashikuar për procedurën administrative. Veprimet vijuese rezultuan në miratimin e vendimeve në kadastër, ku qartësisht procedura nuk ishte në përputhje dhe as nuk përfaqësonte interesat e bashkisë së mbrojtur.

Kodi Penal i Malit të Zi përcakton shkeljen penale të shpërdorimit të detyrës shtetërore si: tejkalimi i kufijve të autoritetit të tij/saj zyrtar për të siguruar fitim material të paligjshëm që tejkalonin 30.000 euro.

Si rrjedhojë, gjykata vendosi që të pandehurit (një funksionar dhe kryetari i Kadastrës bashkiake) vepruan pa autorizim në ato raste. Ata e dinin që nuk ishin të autorizuar për rikthimin e tokës dhe nuk mund të transferonin tokë tek pronarët e mëparshëm, të supozuar. Ata e dinin, gjithashtu, që toka ishte nën juridiksionin e një autoriteti tjetër bashkiak. Përveç kësaj, provat treguan që vendimet e marra nga të pandehurit nuk ishin mbështetur me dokumentacionin që provonte pronësinë e pronarëve të mëparshëm, të supozuar, të cilëve u ishte kthyer toka. Më tej, procedura vijuese e rikthimit ishte kryer nëpërmjet kërkesës me gojë të një personi i cili kishte blerë tokën nga pronarët e mëparshëm, të supozuar, pavarësisht faktit që toka ishte pasuri kombëtare dhe nuk mund të vihej në dispozicion për shitje. Për gjykatën, ishte e padiskutueshme që të dy të pandehurit tejkaluan kompetencat e tyre, që procedura e përcaktuar për veprimet administrative nuk ishte ndjekur, as që interesat e bashkisë nuk ishin mbrojtur, dhe kështu të dy të pandehurit kryen shkeljen penale për të cilën ishin akuzuar.

Përfundim 3

Shembulli i mësipërm tregon qartë që të dhënat nga regjistrat publikë, të mbajtura në rrugë elektronike, mund të jenë pre e manipulimit nga personat e autorizuar për t'i përdorur ato dhe për të futur të dhëna në to.

Futja e të dhënave në regjistrat elektronikë të tokës ishte paraprirë nga miratimi i një vendimi të paligjshëm, kështu që ky rast mund të përbënte jo vetëm shkeljen penale të shpërdorimit të detyrës sipas nenit 416, paragrafi 3, në lidhje me paragrafin 1 të Kodit Penal të Malit të Zi, por ndoshta edhe disa nga shkeljet që lidhen me sigurinë e të dhënave kompjuterike. Për shkak të kësaj, është e qartë së blerësit e mundshëm të tokës, mund të keqinformohen kur ata kontrollojnë të dhënat në zyrat e regjistrimit të tokës, dhe mund të jenë të hapur ndaj padive civile për përcaktimin e të drejtave të pronësisë, ku mungesa më e vogël e vigjilencës së marrësit apo blerësit të pronës mund të shkaktojë dëm material të qenësishëm.

Në këtë rast u demonstrua qartë që, në vijim të vendimit të Kadastrës bashkiake, e cila nuk ka autoritet për të marrë vendime të tilla, janë bërë ndryshime në regjistrat e bankës së të dhënave kadastrale. Rasti verteton që sistemi ekzistues i IT-së dhe procedura e mbajtjes së regjistrave, në veçanti mënyrat e aksesit në bazën e të dhënave dhe në sistemin IT, dhe mundësia për të bërë ndryshime në regjistra pa baza ligjore të vlefshme, janë të paplota dhe të papërshtashme. Është thelbësore të përmirësohet sistemi IT në mënyrë të atillë që ai do të përcaktonte qartë dhe pa hezitim procedurën e aksesit, si dhe autoritetet të cilat marrin vendime për të bërë të mundur aksesin dhe ndryshimin e të dhënave në regjistra.

1.6.4 Mali i Zi, rasti 4: Lëshimi i paligjshëm i dokumenteve të udhëtimit

Një punonjëse në Drejtorinë e Policisë së Malit të Zi, në Podgoricë, në cilësinë e sekretares në Departamentin për Dokumentet e Udhëtimit dhe Armët, u akuzua për përdorimin e postit të saj zyrtar me qëllim që të siguronte avantazhe për persona të tjerë gjatë periudhës 2004 deri 2005. Sekretarja veproi në kundërshtim me Ligjin për Dokumentet e Udhëtimit dhe Vendimi për lëshimin e pasaportave, pasaportave të zakonshme, certifikatat e udhëtimit dhe vizave, pasi kishte marrë një kërkesë për lëshimin e dy dokumenteve të udhëtimit (pasaportave), dhe plotësoi dokumentet pa kontrolluar më parë identitetin e aplikuesit ose personit për të cilin ishte kërkuar lëshimi i dokumeteve të udhëtimit. Ajo nuk bëri as verifikime në përputhje me rregulloret e mësipërme. Për rrjedhojë, ajo kreu shkeljen penale të Shpërdorimit të Detyrës, të parashikuar në nenin 416, paragrafi 1 i Kodit Penal.

Është interesante se në vendimin e shkallës së parë, gjykata, duke marrë parasysh akuzat, mbrojtjen dhe të gjitha provat, doli në përfundimin që e pandehura nuk duhet të procedohet në përputhje me nenin 363, paragrafi 1, pika 1, të Kodit të Procedurës Penale – pasi shkelja për të cilën ishte akuzuar ajo nuk përbënte një shkelje penale sipas ligjit. Në pretencë, theksi është vënë mbi faktin se e pandehura bëri veprime me qëllim që të siguronte fitime për ato persona, por përshkrimi faktik i shkeljes la pa përfshirë pjesën që i referohet faktit se pasaportat në fjalë u ishin lëshuar personave të cilësuar në akuzë, dhe në këtë mënyrë nuk përfshiu pjesën që lidhet me fitimin që u ishte siguruar këtyre personave.

Një detaj veçanërisht interesant nga gjykimi është që e pandehura deklaroi se pavarësisht se ajo kishte akses në dokumentet e udhëtimit në fjalë, nuk u gjenden shënime në regjistra për dokumentet e udhëtimit, as aplikimet. Të gjitha ishin zhdukur. Kur supervizori urdhëroi qëtë kërkoheshin dokumentet në sistem, kuptuan që i gjithë dokumentacioni ishte zhdukur. Hetimi i brendshëm nuk mundi të identifikonte asnjë person që kishte marrë pjesë në zhdukjen e dokumentacionit, dhe as çfarë kishte ndodhur me të. Fakti është se dokumentet ishin mbajtur në sallën e arkivit, e cila ndodhej në bodrumin e Qendrës së Sigurisë, dhe ruhej nga një oficer special. Sidoqoftë, të gjithë punonjësit e Departamentit kanë akses në sallën e arkivave. Kështu që e pandehura spekuloi se mbi çfarë bazash eprori i saj doli në përfundimin, që nga shtatë kolegët e saj, ishte pikërisht ajo që kishte kryer shkeljen.

Gjatë procedurës u amendua Kodi Penal. Shkelja për të cilën u akuzua sekretarja nuk përbënte më shkelje penale në përputhje me amendamentet. Në përputhje me nenin 133, paragrafi 3 i Kodit Penal, gjykata qe e detyruar kështu të zbatonte ligjin që ishte më i favorshmi për të pandehurën. Në përputhje me këtë, e pandehura u shpall e pafajshme për shkeljen në fjalë dhe procesi u kthye për rigjykim.

U nis një proces i ri. Procesi përfshiu jo vetëm funksionaren e lartpërmendur, por edhe dy funksionarë të tjerë nga Drejtoria e Policisë/Ministria e Brendshme. Dy të pandehurit e rinj u akuzuan për përdorimin e autoritetit zyrtar për falsifikim dhe lëshim të një numri të madh kartash identiteti, patentash, dhe pasaportash gjatë periudhës 2011 dhe janar 2013. Gjithashtu, ata u akuzuan për nënshkrimin e personave për të cilët ata kishin dhënë legjitimitet në Regjistrin e Gjendjes Civile të Shtetasve Malazes. Së fundi, ata u akuzuan për marrje ryshfetesh për çdo lëshim të dokumentacionit fals me vlerë nga 50 – 1.300 euro. Në total, organi i akuzës akuzoi 17 persona për korrupsion, d.m.th. mitmarrje dhe falsifikim dokumentesh.

Dy persona u akuzuan për ndërmjetësim mitmarrjeje. Ata kërkonin shtetas të cilët kishin nevojë për dokumente të tilla, dhe një tarifë për t'i lidhur ata me funksionarin e akuzuar.

Një person tjetër, një inxhinier kompjuteri, u akuzua për falsifikim dokumentesh. Në marrëveshje me mbështetësit e mësipërm, ai krijonte vertetime false të provimeve të marra të patentës.

Shtatëmbëdhjetë persona u akuzuan për pagesë ryshfeti dhe falsifikim dokumentesh.

Rasti i plotë u mbyll në Gjykatë në korrik 2014. Sekretarja, si e akuzuara kryesore, u dënua për mitmarrje, ushtrim ndikimi të paligjshëm, dhe për ndihmë për falsifikim të dokumenteve. Ajo u dënua me një dënim të vetëm me katër vjet e gjysmë burg.

Në tërësi, gjykimi i prerë i Këshillit Special të Gjykatës së Lartë në Podgoricë, dënoi grupin me 17 anëtarë me shtatëmbëdhjetë vite dhe katër muaj burg në total për falsifikim dokumentesh, dhe mitmarrje e mitdhënie.

Përfundim 4

Shembujt e mësipërm tregojnë se ekziston, ose ekzistonte, një gabim ose mospërfshirje në sistemin e e menaxhimit të dokumenteve të Ministrisë së Brendshme. Nuk ka të dhëna elektronike të kërkesave të skanuara për lëshimin e pasaportave në sistemin e informacionit, të cilat do të eleminonin risqet e përdorimit dhe lëshimit të dokumenteve të falsifikuara. Gjithashtu, është e qartë se nuk ekzistojnë gjurmë elektronike të cilat do të tregonin kush i lëshoi këto dokumente.

Për një zgjidhje të mundshme ndaj këtij rasti dhe të tjera rasteve të ngjashme, është e nevojshme të instalohet skanimi i dokumenteve ose të instalohen databaza elektronike të të gjithë dokumenteve të depozituara dhe lëshuara në formë jo elektronike me opsionin e detyrueshëm të ruajtjes së dyfishtë, për të garantuar sigurinë e të dhënave në rast asgjësimi me dashje apo pa dashje. Gjithashtu, është e nevojshme përmirësimi i sigurisë së sistemit elektronik duke regjistruar aksesin fizik në zyrat ku mbahen dosjet dhe dokumentet zyrtare.

Përmbledhje

Përmbledhtas, vini re se kur bëhet fjalë për sistemin e drejtësisë penale në Malin e Zi, krimet e korrupsionit përcaktohen si shkelje penale përkundrejt detyrës zyrtare në Kapitujt

XXXIV dhe XXII të Kodit Penal. Në këtë mënyrë, këto shkelje penale nuk janë asgjë më tepër se forma të ndryshme të abuzimit dhe një devijim nga mënyrat e përcaktuara me ligj të kryerjes së detyrës. Prandaj shkeljet penale të korrupsionit përbëjnë një cënim më të madh ndaj shoqërisë meqë shkelësit janë funksionarë publikë. Përmes veprimeve të tyre, ata shkelin sistemin ligjor dhe administrativ dhe ulin efikasitetin e shtetit. Përveç pasojave të dukshme materiale të shkaktuara nga shkelje të tilla, pasojat më të dëmshme përfshijnë cënimet ndaj integritetit të institucioneve dhe një ulje të besimit publik në punën e autoriteteve shtetërore dhe lokale; pra, në fund të fundit, funksionimin e shtetit.

Kodi Penal i Malit të Zi përshkruan krimet e mëposhtme të korrupsionit:

- pastrimi i parave (neni 268 i KP); shkelja e barazisë në ushtrimin e një veprimtarie ekonomike (neni 269 KP);
- shpqrdorimi i pozicionit të monopolit (neni 270 KP);
- shpërdorimi i detyrës në veprimtarinë e biznesit (neni 272 KP);
- shkaktim falimentimi (neni 273 KP) dhe shkaktim falimentimi të rremë (neni 274 KP);
- shpërdorim i autoritetit në ekonomi (neni 276 KP);
- mitmarrje pasive në veprimtaritë e biznesit (neni 276a KP);
- mitmarrje aktive në veprimtaritë e biznesit (neni 276b KP), falsifikimi në bilanc (neni 278 KP);
- shpërdorimi i vlerësimit (neni 279 KP);
- nxjerrja e sekreteve tregtare (neni 280 KP);
- nxjerrja dhe përdorimi i sekretit të bursës (neni 281 KP);
- shpërdorim i detyrës shtetërore (neni 416 KP);
- moskryerje e detyrës (neni 417 KP);
- mashtrim në shërbime (neni 419 KP);
- ndikim i paligjshëm (neni 422 KP);
- nxitje për ndikim të paligjshëm (neni 422A KP);
- mitmarrje pasive (neni 423 KP);
- mitmarrje aktive (neni 424 KP).

Në përgjithësi, krime të tilla dënohen me burg, dhe ku është e mundur me konfiskim të produkteve të krimit. Sidoqoftë, në praktikë, këto shkelje penale shpesh lidhen me shkelje të tjera penale, që në thelb nuk janë krime korrupsioni, por lidhen ngushtë me to. Këtu përfshihen falsifikimi i dokumenteve zyrtarë dhe shkeljet lidhur me sigurinë e të dhënave kompjuterike. Duket se në jurisprudencë ka ende shembujt të mjaftueshëm të veprave penale të korrupsionit të abuzimit të të dhënave kompjuterike, por praktika do të tregojë sa të duhura janë masat ligjore, dhe nëse ekziston nevoja të futen vepra të reja penale të lidhura me krimin kompjuterik.

Sigurisht, mbetet fakt se një ndër mekanizmat për të luftuar me efikasitet korrupsionin është procedimi i suksesshëm penal. Kjo nënkupton zbatimin e metodave efektive për zbulimin dhe grumbullimin e provave, dhe vendosjen e sanksioneve efikase dhe të përshtashme.

Institucionet kompetente për zbulimin, procedimin, dhe sanksionimin në Malin e Zi janë policia, prokuroria dhe gjykatat. Këto institucione janë të lidhura në mënyrë funksionale dhe secili prej tyre, brenda rrezes së tyre të kompetencave, zbaton parime të përshkruara nga ligji për luftën kundër korrupsionit. Sidoqoftë, ato ndonjëherë hasin vështirësi në zbatimin e parimeve të tilla, të cilat sjellin nevojën për diskutime të ndryshme profesionale dhe amendim të ligjeve në fushën e korrupsionit. Policia, si autoriteti përgjegjës për zbulimin e krimeve, ka nevojë për bashkëpunim dhe përfshirje të institucioneve të tjera: në radhë të parë, të bankave dhe institucioneve të tjera financiare, të Drejtorisë për Iniciativën Antikorrupsion, të Drejtorisë për Parandalimin e Pastrimit të Parave, të sektorit joqeveritar, dhe të vetë qytetarëve. Nga njëra anë, policia është e autorizuar të zbatojë metodat më të gjëra për grumbullimin e provave, d.m.th. masat e vëzhgimit të fshehtë për shkeljet penale të korrupsionit, pavarësisht nga mënyra e ekzekutimit të shkeljeve penale dhe dënimit që parashikon ligji. Nga ana tjetër, metoda të tilla ngrenë, gjithashtu, çështjen e shkeljeve të mundshme të të drejtave themelore të njeriut dhe të jetës private.

Pavarësisht këtyre masave frenuese, parandalimi i korrupsionit ka një rëndësi të madhe. Ai përfshin kryesisht rritjen e nivelit të ndërgjegjësimit, njohurive, dhe aftësive, si dhe përgjegjësinë e punonjësve, nga njëra anë, dhe sigurimin e kushteve te duhura fizike, teknike, dhe financiare të punonjësve nga ana tjertër. Si rrjedhojë, një nga metodat parandaluese moderne për sigurimin dhe përcaktimin e cilësisë ligjore dhe etike të punës në organet shtetërore është përgatitja e planeve të integritetit për institucionet. Këto plane përfaqësojnë dokumente të brendshme antikorrupsioni, përcaktimin e zonave të ndjeshme në institucione, d.m.th. analizë e riskut të proceseve të punës në secilin organ shtetëror, organizatë, ose shërbim. Së fundi, planet e integritetit duhet të kuptohen si një formë e menaxhimit strategjik, të cilësisë dhe riskut, e të cilët duhet të çojnë në cilësi më të lartë të shërbimeve në sektorin publik, duhet të ulin kostot dhe rrisin kapacitetin mbrojtës të institucioneve ndaj efekteve të paligjshme dhe të padëshiruara. Kjo përfshin, si një ndër elementet kyçe, dixhitalizimin dhe përdorimin e IT-së.

Serbia

Nga Nemanja Nenadic dhe Bojan Cvetkovic

Gjatë kryerjes së studimit për korrupsionin lidhur me IT-në, kontaktuam institucionet e mëposhtme për të dhënë intervista:

- Ministria e Drejtësisë
- Zyra e Komisionerit për Informacionin me Rëndësi Publike dhe Mbrojtjen e të Dhënave Personale
- Drejtoria për Qeverisjen Elektronike
- Ministria e Brendshme
- Ministria e Financës
- Avokati i Popullit

Vetëm dy institucionet e para iu përgjigjen kërkesës dhe u organizuan takime për intervistat. Drejtoria për Qeverinë elektronike iu përgjigj kerkesës, por intervista nuk u organizua asnjëherë.

Serbia, rasti 1: Seks në "Arenën e Beogradit"

Në fillim të marsit të vitit 2011, u publikua një video në Internet në të cilën shfaqej marrëdhënie seksuale para "Arenës së Beogradit". Vetë videokaseta ishte regjistruar në mëngjesin e 24 prillit 2010. Meqenëse video ishte regjistruar nga sistemi i vëzhgimit video i përdorur nga Ministria e Brendshme (MoI) për të kontrolluar trafikun në Beograd, ky përfaqëson një rast të pastër të veprës penale të korrupsionit "shpërdorimit të detyrës".

Reagimi i parë i njerëzve të përfshirë në videon origjinale të publikuar në Internet ishte relativisht i butë, por gjatë muajve që pasuan incidentin u bë mjaft e qartë se videoja kishte ndikuar mjaft në jetën e tyre, dhe jetën e familjeve të tyre. Identiteti i Elizabeta M. (22) dhe Milovan S. (24) u zbulua publikisht, dhe atyre iu desh që të shmangnin pothuajse çdo shfaqje në publik, dhe familjeve të tyre, siç pretenduan ata, "iu bë jeta ferr".

Komisioneri për Informacione me Rëndësi Publike dhe Mbrojten e të Dhënave Personale Rodoljub Sabic (Komisioner) dërgoi një ankimim pranë Prokurorisë së Përgjithshme në Beograd kundër "një punonjësi të zakonshëm të policisë" për publikim video në Internet të marrëdhënies seksuale midis dy të rriturve, duke përdorur regjistrime nga një sistem i vëzhgimit video të përdorur nga Ministria e Brendshme (MoI) për të kontrolluar trafikun në Beograd. Ai deklaroi se ishte e qartë që MoI-ja nuk ndërmori të gjitha masat parandaluese teknike, njerëzore dhe organizative për të parandaluar të dhëna që parandalojnë keqpërdorim të mundshëm të regjistrimeve nga sistemi i vëzhgimit video. Në këtë rast të veçantë, IT-ja ishte keqpërdorur duke siguruar në mënyrë të paligjshme të dhëna përmes manipulimit të të dhënave dhe procedurave ekzistuese. Në kohën kur ndodhi kjo, e vetmja rregullore që mbulonte gjerësisht këtë rast ishte një rregullore e brendshme e Policisë

Rrugore pranë MoI-së e cila përcaktonte se regjistrimi nga sistemi i vëzhgimit video mund të përdoret vetëm brenda MB-së për hetimin e rrethanave të aksidenteve rrugore. Është e rëndësishme të theksohet që nuk kishte legjislacion kombëtar që mbulonte këtë rast. Gjithashtu, politika e brendshme kyçe e nivelit të lartë të MoI-së*"në rast se diçka nuk rregullohet qartë as nga rregullore kombëtare as nga rregullore të brendshme të MoI-së, punonjësit e MoI-së duhet t'i drejtohen MoI-së për të siguruar leje zyrtare në vend që të marrin përsipër se ata mund ta bëjnë atë diçka"* u manipulua.

"Kjo ka të bëjë me një ngjarje që përbën një shkelje shumë të rëndë të jetës private dhe një shkelje të rëndë të Ligjit për Mbrojtjen e të dhënave personale", - tha Komisioneri, duke shtuar se mungesa e procedurave të nevojshme dhe ekzistenca e mangësive të elementeve të sigurisë çuan në këtë incident.

Në përputhje me detyrat e tij, Komisioneri nisi një inspektim për mënyrën se si ekzekutohet dhe zbatohet Ligji për Mbrojtjen e të Dhënave Personale nga MoI-ja, i cili përfundoi me dhënie paralajmërimi për MoI-në, i cili përmbante një listë me 14 masa dhe veprime që duhet të ndërmerren në nivelet teknike, të personelit dhe organizative për mbrojtjen e të dhënave me qëllim që të shmangej çdo lloj abuzimi në të ardhmen. Gjithashtu, Komisioneri kërkoi që MoI-ja ta njoftonte zyrtarisht atë brenda 15 ditëve nga afati ligjor për masat dhe veprimet e planifikuara që do të miratojë dhe zbatojë MoI-ja për të elimininuar parregullsitë. Në këtë rast Komisioneri rikujtoi se Serbia nuk ka një ligj për vëzhgimin video, pavarësisht se ka një numër të madh njerëzish të përfshirë nëtë.

Reagimi i parë i MoI-së ishte se do të ishte shumë e vështirë të përcaktohej se kush e kishte kopjuar regjistrimin dhe publikuar atë në internet, sepse kryetarët, operatorët dhe administratorët në Qendrën e Komandës së Operacioneve (COC) kishin të gjithë akses në regjistrimet e sistemit të vëzhgimit video të cilat, së bashku me mungesën e procedurave të aksesit të të dhënave dhe të sigurisë, paraqitnin një dobësi të qartë në administrimin e sistemit të vëzhgimit video COC të MoI-së.

Pas paralajmërimit të lëshuar nga Komisioneri, MoI-ja mori hapa konkrete në dënimin e personave të përfshirë në incident. Një hetim i brendshëm përcaktoi se kishin qenë 10 pika kompjuteri nga të cilat mund të ishte kopjuar (ngarkuar) regjistrimi.

Ndaj oficerëve të policisë që u përfshinë, të cilët kishin patur detyrë mbikëqyrjeje në COC e MoI-së në Beograd, në ditën kur ishte kopjuar regjistrimi. u morën masa disiplinore për shpërdorim detyre. MoI-ja publikoi udhëzime të detajuara në udhëzimin zyrtar "Kushte të detyrueshme për përdorimin dhe mirëmbajtjen e vëzhgimit video të rrugëve dhe kryqëzimeve në qytetin e Beogradit," me qëllim që të mbyllte boshllëqet ekzistuese në sistemin e sigurisë (siç është fakti që shumë persona kishin akses, mungesa e regjistrimeve se kush kishte hyrë në një pjesë të caktuar të sistemit, etj.), jo vetëm për sistemin e vëzhgimit video COC të MoI-së në Beograd, por edhe për edhe për sisteme të ngjashme të MoI-së anëmbanë vendit. Sidoqoftë, MoI-ja nuk publikoi detaje të hetimeve dhe procedurave disiplinore kështu që ne nuk kemi të dhëna për motivet e mundshme të atyre që kishin kryer shkelje.

Komisioneri reagoi menjëherë ndaj veprimeve të MoI-së, duke i drejtuar ata për një reagim konstruktiv dhe të dobishëm ndaj paralajmërimit të tij duke thënë se, megjithëse sipas kritereve të sotme të mbrojtjes dhe sigurisë së të dhënave, hapat e marra nuk kanë asgjë të veçantë dhe konsiderohen standard, ato, në kushtet specifike serbe, janë të mirëpritura për arsye se përfaqësojnë pa dyshim diçka të dobishme.

Megjithëse pas kësaj nuk ka patur incidente të ngjashme në Serbi, viti 2014 e ngriti problemin e regjistrimeve të sistemit të vëzhgimit video në maja të reja.

Midis periudhës së 8 qershorit dhe 10 qershorit 2014, u shfaqen në YouTube dy video. Në videon e parë paraqitej një aksident rrugor që ndodhi gjatë natës së të shtunës, më 7 qershor duke u gdhirë e dielë, 8 qershor 2014 në qytetin e Novi Sadit. Në video tregohej momenti kur një Audi që e ngiste DV (21 veç) përplaset anash me një Polo, duke vrarë dy vajza, ML dhe VM, dhe një djalë të ri, AM (të gjithë të moshës 20 vjeç).

Klipi i dytë që tërhoqi vëmendjen publike erdhi nga qyteti i Nishit dhe në të tregohej një këmbësor, MZ (17 vjeç), teksa u përplas nga një Audi në një kryqëzim këmbësorësh, dhe, si rezultat i përplasjes, atij iu shkaktuan dëmtime të rënda.

Të dyja videot u transmetuan nga një sërë mediash vendase, së bashku me publikimin e informacionit personal të të gjithë personave të përfshirë.

Komisioneri që ishte në detyrë hapi menjëherë një inspektim dhe mbikëqyrje të Departamentit të Policisë Rrugore të MoI-së në Novi Sad, në Ndërmarrjen Komunale Publike "Informatika", sistemi i saj i vëzhgimit kishte regjistruar videon e aksidentit me makinë të Novi Sadit, dhe të Departamentit të Policisë Rrugore në Nish. Komisioneri vuri në dukje se "ne përballemi me një rrezik të vërtetë që shumë sisteme CCTV kthehen në prodhimin e skenave horror dhe skandali", duke nxitur median "të vënë në pikëpyetje standardet etike të profesionit të tyre". Sipas Komisionerit, informacioni objektiv mund t'i ofrohet publikut pa qenë nevoja e ndërhyrjes së papërshtatshme në jetën private të personave të përfshirë, dhe pa shtuar dhimbjen e familjarëve të tyre. Ai i rikujtoi policisë dhe autoriteteve të tjera shtetërore dispozitat e nenit 42, paragrafi 3 të Kushtetutës, i cili ndalon dhe dënon qartë përdorimin e të dhënave personale përtej qëllimeve për të cilat ato janë grumbulluar – në këtë rast, për të kontribuar në sigurinë rrugore dhe për të mbështetur zbulimin dhe provimin e krimit.

Familjet e viktimave nga Novi Sadi dhe familja e të riut, të dëmtuar rëndë, nga qyteti i Nishit, deklaruan se publikimi i videove të aksidentit në të cilin ishin regjistruar fëmijët e tyre ishte shumë i rëndësishëm për publikun, duke nxjerrë në pah mënyrën si ndodhin këto aksidente, por edhe për të ulur mundësinë e çfarëdo lloj fshehjeje të krimeve.

Megjithëse në momentin kur u shkrua ky studim, rezultatet e këtij inspektimi dhe mbikëqyrjeje nuk janë ende të njohura, mësimet e nxjerra nga ky rast përfshijnë se Serbia duhet të krijojë dhe miratojë një ligj për vëzhgimin video, i cili duhet të jetë në përputhje me versionin e ri të Ligjit për Mbrojtjen e të Dhënave Personale[35] dhe direktivat BE-së në këtë fushë.

Serbia, rasti 2: Kur "zë rrënjë" kontraktori i IT-së

Ministria e Drejtësisë aktuale (MoJ e re) e Republikës së Serbisë trashëgoi detyrat e ish Ministrisë së Drejtësisë dhe Administratës Publike (MoJPA) si rezultat i shkrirjes së Ministrisë së Drejtësisë së mëparshme (MoJ-së së mëparshme) dhe administratës publike që ishte pjesë e Ministrisë së Administratës Publike të mëparshme, të Vetë Qeverisjes Lokale dhe të Drejtave të Njeriut (MPALSGHR).

Mandati i MoJ-së së mëparshme (sipas *"afateve të mandatit"*) zgjati deri në korrik 2012. MoJPA -ja u krijua në korrik 2012, dhe ushtroi aktivitetin deri në prill 2014, kur u formua MoJ-ja e re.

Për gati 10 vjet të qeverisjes publike në Serbi, funksioni i drejtësisë së qeverisë ishte vendosur në MoJ-në e mëparshme, e ndjekur nga më pak se dy vjet qeverisje të përbashkët midis funksioneve të drejtësisë dhe administratës publike. Sidoqoftë, si rezultat i riorganizimit të fundit qeveritar, funkioni i drejtësisë tani është kthyer brenda funksionit të vetëm të organit ministerial të MoJ-së së re.

Sektori i drejtësisë me të gjithë njësitë e saj të ndërlidhura, por të pavaruara, është një mjedis tepër kompleks, ku secila njësi brenda sektorit ka funksionet, proceset dhe përgjegjësitë e saja, të përcaktuara qartë, dhe ku ndërveprimet me njësitë e tjera të sektorit rregullohen më së miri. MoJPA -ja, si dhe MoJ-ja e re, kishin besimin e patundur që me qëllim që të menaxhojnë dhe qeverisin me sukses sektorin e drejtësisë, duhet përdorur ICT-në (Teknologji Informacionit Kompjuterik) thjesht si një mjet për të zvogëluar kompleksitetin e sektorit. Strategjia e MoJ-së së mëparshme ishte krejtësisht e kundërt dhe ishte e drejtuar drejt krijimit të sistemeve komplekse ICT të cilët përvijojnë kompleksitetin e sektorit, që kërkon investime të konsiderueshme buxhetore si për kostot operative dhe të mirëmbajtjes. Veprime të tilla çuan në diversitet të gjërë të harduereve, softuereve dhe sistemeve që lidhen me ICT-në të përdorur brenda ekosistemit ICT të sektorit të drejtësisë, i cili ende shkakton probleme të mëdha për sa u përket risqeve ICT të lidhura me ICT-në dhe mundësive përkatëse për korrupsion.

Aktualisht, dhe sipas Zëvendës Ministrit të ngarkuar për IT të MoJ-së së re, ka tre sisteme kryesore të informacionit në sektorin e drejtësisë, të cilët përdorin dy platforma të ndryshme të aplikacioneve softuer; dy platforma të ndryshme të bazes së të dhënave; dhe një platformë të sistemit operativ, megjithëse të gjithë i përkasin së njëjtës familje të aplikacionit IT – menaxhim dokumenti. Nëse numerohen sistemet më të vogla, si

35 https://docs.google.com/viewer?url =http%3A%2F%2F www.poverenik.rs%2Fimages%2Fstories%2Fmodel-zakona%2Fmodelzzpl.docx

për shembull ato që përdoren në Gjykatën Kushtetuese, numri është edhe më i madh. Këto sisteme kanë shkaktuar shpenzimin e më shumë se 10 milion eurove nga paratë e donatorëve, dhe kanë patur ndikim edhe në buxhetin serb për kostot operative dhe të mirëmbajtjes me 1.5 milion euro në vit! Një gjë e tillë mund të kishte qenë e pranueshme nëse i gjithë sektori i drejtësisë do të ishte mbuluar nga njëri ose të gjithë nga tre sistemet e kryesore të informacionit; sidoqoftë, mbulimi aktual i sektorit është më pak se 25 përqind. Përfundimi është se me qëllim që të mbulohet pjesa e mbetur e njësive të sektorit të drejtësisë (d.m.th 75 përqind), janë të nevojshme investime të reja me shumë nga 20 deri në 30 milion euro. Një fond i tillë nuk e disponohet nga MoJ-ja e re, sepse kjo do të bënte që buxheti vjetor për funksionimin dhe mirëmbajtjen të pësonte një rritje të jashtëzakonshme me më tepër se 3 milion euro. Është e qartë nga faktet e mësipërme, si dhe nga fakti që kriza financiare globale ka ndikuar burimet e disponueshme përmes shkurtimeve të buxhetit, se gjetja e burimeve të tilla është e vështirë. MoJ-ja e re ka probleme të konsiderueshme për sa i përket risqeve që lidhen me kontraktorin ICT, diçka që çon lehtësisht në lindjen e shkeljeve të korrupsionit.

Gjatë prokurimit publik të shërbimeve të rrjetit dhe komunikacionit (Internet dhe VPN WAN), pati probleme që konsiderohen si korrupsion IT-je, dhe mund të përshkruhen specifikisht si “shpërdorim detyre”, “nepotizëm dhe favorizim”, dhe “shkelje të prokurimit” nga punonjësi i MoJ-së së mëparshme, dhe në favor të të njëjtit kontraktor të IT-së të MoJ-së së mëparshme i përdorur si ofrues i një rrjeti të vetëm kombëtar dhe për shërbime të komunikacionit. Një punonjës i MD-së së mëparshme përgjegjës për shërbimet e rrjetit kompjuterik manipuloi procedurat e përcaktuara në kontratën e lidhur midis MoJ -së së mëparshme dhe kontraktorit IT në kuptimin që procedurat e kontrollit dhe sigurisë ose nuk ishin ndjekur ose ishin thjeshtëzuar së tepërmi në favor të kontraktorit IT dhe me qëllim të shkurtimit të shpenzimeve. Gjithashtu, ai shpërdoroi detyrën duke fshehur (duke i bërë të padisponueshme) të dhënat lidhur me aksesin e kontraktorit IT në sistemin VPN WAN dhe duke asgjësuar dokumentacionin elektronik të sistemit në mënyrë që MoJPA-ja dhe MoJ-ja e re nuk mund të kontrollonin, monitoronin dhe mbikqyrnin sistemin.

I njëjti punonjës i MoJ-së së mëparshme shfaqi nepotizëm dhe favorizim duke kryer shkelje në prokurim kur ai përdori të dhënat dhe informacionin për sistemin, të cilat nuk ishin të disponueshme për funksionarët më të lartë të MoJ-së së re për të krijuar dokumentacion tenderi për tenderin e ri për rrjetin e prokurimit dhe shërbimet e komunikacionit. Sidoqoftë, Ministri i MoJPA-së nuk lejoi botimin e këtij dokumentacioni të tenderit sepse ai kishte frikë nga efektet negative të tenderit, i cili mund të manipulohej potencialisht në favor të Ofruesit të Shërbimit të Internetit (ISP), kontraktorit IT, i cili, në kohën e tenderit, kishte vazhduar tashmë të siguronte rrjet mbarëkombëtar dhe shërbime komunikacioni (Internet dhe VPN WAN) për tetë vjet. Në vend të kësaj, ministri i MoJPA-së dha urdhrin të përgatitej një dokumentacion e ri dhe i drejtë tenderi i cili respekton ligjet dhe përdor praktikat më të mira.

MoJ-së së re dhe tatimpaguesve serbë iu shkaktua dëm financiar, për arsye se kontraktori i IT-së në fillim nuk deshi të rinegocionte çmimin dhe cilësinë e shërbimit, as të lejonte MoJ-në e re të niste procedurë të re tenderi. Kontraktori i IT-së kishte mundur të ndalonte tenderin e ri duke përdorur një skeme ankimimi komplekse dhe shterruese të mundësuar nga hapësirat në Ligjin për Prokurimin Publik që ishte në fuqi në atë kohë. Punonjësi i MoJ-së së mëparshme, kur u përball me realitetin, u largua nga ministria gjatë mandatit në detyrë të MoJPA-së. MoJPA-ja kishte nisur një hetim formal dhe e dërgoi çështjen në gjyq (përfaqësuesit e MoJ-së së re po e trajtojnë çështjen në këtë moment).

Përfundimet që duhet të nxirren nga ky rast janë që organizatat publike nuk duhet të nënvlerësojnë risqet që lidhen me kontraktorin e IT-së. Ato duhet të kenë procedura të parashtruara në ligj gjatë kontraktimeve të jashtme. Meqenëse sektori privat do të lëvrojë më shumë shërbime të IT-së në të ardhmen, duke qenë se po shkurtohen buxhetet e fuqisë së brendshme punëtore të organizatës, kontraktorët e IT-së do të bëhen më të rëndësishëm.

Serbia, rasti 3: Një funksionar publik i nivelit të lartë përgjon punonjësit

Për të gjetur se kush po fliste për punën e saj të dobët, Menaxherja e Përgjithshme e Agjencisë së Privatizimit (Agjencia) e asaj kohe, zëvendësoi menaxherin e IT-së së Agjencisë sepse kishte refuzuar të kopjonte postën elektronike të punonjësve, dhe në vijim, urdhëroi dikë tjetër të personelit për ta bërë këtë, duke arritur në këtë mënyrë të kishte akses në një numër të madh të e-maileve të personelit. Ky rast “shpërdorim detyre” çoi në nxjerrjen e saj në pension të parakohshëm, fundin e mandatit të saj si Menaxhere e Përgjithshme e Agjencisë.

Menaxherja e Përgjithshme e Agjencisë, në pension, kërkoi kopje të emaileve nga punonjësit e Agjencisë pa dijeninë e tyre, duke shkelur kështu privacinë e tyre. Aktualisht, Serbia nuk ka ligje që rregullojnë pronësinë dhe aksesin e komunikimeve elektronike të bërë nga punonjësit gjatë orëve të punës, prandaj çdo lloj komunikimi i tillë (e-mail, çat, telefon, media sociale, etj.) konsiderohet të jetë pronë personale e punonjësit. Kjo është arsyeja pse shumë kompani që punojnë në Serbi zbatojnë politikat dhe procedurat e tyre të brendshme në lidhje me të drejtat, detyrat, dhe detyrimet e punonjësit lidhur me komunikimin elektronik. Kështu që, pavarësisht se këto ishin e-maile biznesi dhe ajo ishte Menaxherja e Përgjithshme e Agjencisë, asaj nuk i lejohej t’i lexonte sepse Agjencia nuk kishte politika dhe procedura përkatëse. Nuk dihet se kush ka tani akses në qindra dhe mijëra emailet e 300 punonjësve të shkarkuara pas orarit të punës dhe gjatë fundjavave. Gjithashtu, nuk dihet nëse ajo ua tregoi ato dikujt tjetër dhe nëse po, kujt ia tregoi.

Arsyeja për një kërkesë të tillë ishte një artikull kritik për të, i botuar nëntorin e kaluar në revistën “Weekly” me titullin “Vjedhje e Serbisë – si janë të lidhur ndërmjet tyre personat e përfshirë” me nëntitull kushtuar asaj “Kush e ktheu mbretëreshën e privatizimit në skenën e krimit?”. Artikulli citon një email të një prej punonjësve ku njoftohen disa institucione se bordi drejtues i Agjencisë ka ndaluar të gjitha mbledhjet e punës dhe të gjitha komunikimet nëpërmjet emailit të punonjësve.

Menaxheri i IT-së i Agjencisë në atë kohë deklaroi se artikulli i botuar ishte arsyeja kryesore që qëndronte pas qëllimit të Menaxheres së Përgjithshme "për të provuar rrjedhje të informacionit nga Agjencia", ndërsa në fakt ajo donte të zbulonte se kush i kishte treguar gazetarëve për menaxhimin e keq të biznesit në Agjenci. Sipas gojëdhënave, menaxheri i IT-së u konsultua me avokatin e tij lidhur me ligjshmërinë e kopjimit të emaileve pa lejen e punonjësve. Avokati i tha se një urdhër i tillë nuk është në përputhje me Ligjin për Mbrojtjen e të Dhënat Personale dhe Të Drejtën Penale. Në fakt, avokati e informoi se gjobat për përpunim të pautorizuar të të dhënave dhe shkelja e konfidencialitetit, variojnë nga 50.000 deri 1.000.000 RSD por mund të dënohen edhe me burg deri në dy vjet.

Menaxheri i IT-së deklaroi se kur e pyeti Menaxheren e Përgjithshme pse i duheshin kopjet, ajo i tha se një gjë e tillë nuk ishte puna e tij. Gjithashtu, ai tha se personat që nuk ishin punësuar apo angazhuar, dhe ata që nuk kishin as lidhje formale me Agjencinë, ishin të pranishëm në mbledhjet që kishin të bënin me këtë çështje.

Në një përgjigje për mediat, Menaxherja e Përgjithshme e Agjencisë tha se ajo nuk kishte kërkuar kurrë që të kopjoheshin emailet, dhe mohoi se ishte kopjuar ndonjë email të ndonjë punonjësi. E pyetur nëse ishte pushuar nga puna menaxheri i IT-së sepse kundërshtoi këtë veprim, ajo u përgjigj se ai ishte pushuar ngaqë nuk kishte bërë punën e tij në përputhje me kontratën por nuk dha detaje të mëtejshme. Ish-Menaxherja e Përgjithshme thekson se nuk ishte në dijeni për artikullin e revistës që shkruante për të dhe që ajo ishte larguar nga pozicioni i Menaxheres së Përgjithshme të Agjencisë pak ditë para se të dilte artikulli.

Nuk dihet se çfarë masash janë ndërmarrë për të mbyllur hendekun në sistemin e sigurisë së Agjencisë, sepse sistemi i IT-së i Agjencisë ishte keqpërdorur përmes një zinxhiri formal të komandës. Përfundimi më i mirë që nxirret nga ky rast është se mungesa e etikës dhe trajnimit dhe ndërgjegjësimit lidhur me korrupsionin e IT-së së nëpunësve mund të jenë një problem i madh sepse janë të rëndësishme si masa vendimtare afatgjata kundër korrupsionit që ka të bëjë me IT-në.

1.7.4 Serbia, rasti 4: "Mafia e rrugëve"

Gjyqi për "Mafien rrugore" në Serbi që filloi në maj 2007 përfshiu 53 persona, shumica punonjës të kompanisë shtetërore Rrugët e Serbisë ("Putevi Srbije"), e cila devijonte elektronikisht tarifat rrugore. Ky rast është përshkruar si vjedhja më e madhe elektronike në historinë e drejtësisë së Serbisë[36].

Në nëntor 2009, Departamenti Special i Gjykatës së Qarkut të Beogradit dënoi 41 persona në total me 131 vjet dhe 10 muaj në burg. Të pandehurit u shpallen fajtorë për mbajtjen e një pjese të parave të mbledhura nga tarifat rrugore, duke vjedhur nga kompania publike e rrugëve të Serbisë "Rrugët e Serbisë" afërsisht 6.5 milion euro në këtë proces. Nëntë nga të akuzuarit u shpallen të pafajshëm, ndërsa tre persona bënë vetëvrasje gjatë seancave gjyqësore[37]. Milan Jovetic, i cili ishte punësuar për kontrollin e brendshëm të kompanisë "Rrugët e Serbisë", dhe që ishte cilësuar si organizatori i grupit, mori dënimin më të lartë me gjashtë vjet burg. I akuzuari i dytë, Zivorad Djordjevic, i cili besohet gjithashtu të jetë një nga drejtuesit e grupit, u dënua me tre vjet dhe dy muaj burg[38].

Në ligjeratën publike serbe është mjaft e zakonshme të dyshohet se njerëzit e akuzuar dhe dënuar për korrupsion shpesh janë vetëm pak më shumë se "koka turku", meqenëse korrupsioni në nivel të lartë nuk mund të funksionojë pa patur ose përfshirje aktive ose "miratim të heshtur" nga niveli politik. Sidoqoftë, është mjaft unike për një skenar të tillë që ai të konfirmohet pothuajse plotësisht nga organet gjyqësore:

"Gjykata është e mendimit se Jovetic dhe Djordjevic nuk janë organizatorët e vërtetë të grupit dhe që organizatorët e vërtetë, fatkeqësisht, mbeten të pazbuluar. Ne kemi prova ... që disa njerëz të tjerë janë fajtorë... Mbetet e pazbuluar se kush ishte organizatori në Beograd dhe kush merrte 40 përqind të parave"[39].

Një punëtor i dënuar nga "Micros Electronics", siç lexohet në vendim, "projektoi dhe zhvilloi mekanizmat dhe mjetet teknike që mundësuan punën e paligjshme dhe mbledhjen e parave", duke "përdorur kabllo lidhëse, pajisje elektronike ekzistuese dhe një program softuer special dhe të parregullt". Një set kabllosh lidhnin printerin e sipërm dhe të poshtëm në automatin e biletave. Një set tjetër kabllosh, me një çelës, lidhte (ose zgjidhte) traun e hyrjes së automjeteve dhe kompjuterin në stacionin e pagesës së tarifave. Mekanizmi ishte instaluar në stacionet e "Bubanj Potok" dhe "Nais" (dy pikat fundore të autostradës Beograd – Nish). Gjithashtu, ai futi një kopje të papastër të dosjes softuer "EMU-87", në sistemin operativ ekzistues për arkëtimin e tarifës. Një gjë e tillë mundësoi, pa ndryshuar sistemin elektronik, regjistrimin e faturave të pagesës së tarifës. Mbikëqyrësi i turnit aktivizonte programin e paligjshëm para se arkëtarët e përzgjedhur të fillonin turnin.

Sofuere të rregullta, përfshirë dhe dosjen origjinale "EMU 87" shërbenin si bashkëprocesor matematik për veprime aritmetike. Meqenëse kompjuterat e vjetër nuk kishin bashkëprocesorë të tillë, dosja EMU 87 shërbeu fillimisht vetëm për ta "rivalizuar" atë. Duke qenë se ajo dosje ishte pjesë e sistemit origjinal, punonjësi i mirëmbajtjes vetëm sa mbishkruajti dokumentin origjinal me atë të paligjshëm. Ndryshimet midis dokumentit origjinal dhe EMU 87 falso mund të vëreheshin kur hapej dokumentinë editorin e tekstit. Ndërsa dokumenti origjinal ka "disa grepa dhe doreza" për ta bërë atë të palexueshëm, dokumenti i paligjshëm përmbante një formë fature lehtësisht të lexueshme ku shënohej se tarifa rrugore ishte arkëtuar. Sistemi bënte të mundur shikimin e veçorive të dokumentit, datave të aksesit, etj. Siç shpjegoi njëri nga kontrolluesit, kontrolli dhe auditimi nuk identifikuan mashtrimin, meqenëse ai nuk linte gjurmë në sistem.

36 http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/lajme të shkurtra/2007/05/29/nb-06

37 http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-yearsRezultatet e vendimit të shkallës së dytë të Gjykatës së Apeliti ishin dënime pak më të ulëta.

38 Po aty.

39 Gjyqtari Vladimir Vucinic, sipas së përditshmes "Politika", http://www.balkaninsight.com/en/ article/serbia-s-road-mafia-get-131-years.

Kombiminimi i kabllove, pajisjeve elektronike speciale dhe softueri i paligjshëm mundësonin arkëtuesit e tarifës (anëtarë të bandës) të printonin njëkohësisht dy kopje të një bilete të tarifës autostradale me numra serie identike, ndërsa sistemi elektronik regjistronte vetëm një. Kur paguhej tarifa, mbi bazën e biletës së parë të dubluar, softueri mundësonte printimin e faturës pa e regjistruar atë në sistemin elektronik për arkëtimin e pagesës. Në të njëjtën kohë, duke shtypur çelësin, ishte e mundur që kamioni të lejohej të vazhdonte udhëtimin pas pagesës, meqenëse ky çelës ndërpriste lidhjen ndërmjet sistemit për kontrollin elektronik të pagesave, kompjuterit, dhe traut rrugor. I njëjti punëtor i Micros Electronics, i cili instaloi dokumentin e paligjshëm, mirëmbante edhe sistemin e paligjshëm kur ishte e nevojshme (duke ndryshuar kabllo, fshehur softuere të paligjshme kur ishte e nevojshme, mësuar të tjerët si ta përdornin sistemin, etj.).

Arsyeja pse sistemi mundi të operonte për një kohë kaq të gjatë ishte mungesa e kontrollit efikas dhe me shtrirjen e madhe në të vërtetë të rrjetit kriminal. Anëtarët e bandës madje as nuk i hiqnin kabllot e paligjshme pasi mbaronin turnin, përgjegjësit e turnit nuk i parajlamëronin që ta bënin këtë, dhe paratë e fituara në mënyrë të paligjshme zakonisht mbaheshin në kabinat ku mblidheshin. Kontrolli kryhej zakonisht pas orës 6 të pasdites (kur nuk punonte banda), dhe kishte kode për paralajmërime para se të kishte kontroll, etj.

Është fakt interesant, i përmendur edhe në vendimin e gjykatës por që nuk u shqyrtua më tej, se në periudhën e mbuluar nga vendimi (midis vitit 2004 dhe 2006) shuma e përgjithshme e parave të mbledhura nga tarifat autostradale efektivisht u rrit, ndërsa do të ishte pritur e kundërta si pasojë e vjedhjes. Sidoqoftë, ky është një tregues i fortë se sistemi i mashtrimit funksionoi gjatë një periudhe shumë më të gjatë, dhe që hetimi mbuloi vetëm disa nga aspektet dhe aktorët e tij.

Rasti “mafia rrugore” ishte i pari që vuri në dijeni publikun për njërin nga bilbilfryrësit[40] më të njohur të Serbisë, një burrë i cili ishte përkohësisht punonjës i kompanisë “Rrugët e Serbisë”. Kur ai filloi të flasë me kolegët e tjerë për problemet, reagimi ishte që kontrata e tij të skadonte në fillim të vitit 2006, duke dhënë si shpjegim “mungesën e nevojës për shërbime të tilla”.

“Pastaj vendosa të provoja dyshimet për vjedhje në stacionet e mbledhjes së tarifave, njëçështje që askush nuk dëshironte ta ngrinte nga frika se mos pushoheshin nga puna. Fshehurazi, regjistrova automjetet që kalonin stacionin e tarifës së Nishit dhe Beogradit, përfshirë biletat. Megjithatë, me qëllim që të provoja rastin, kisha nevojë për regjistrimin zyrtar të biletave, kështu që mund të demonstroja se kishte duplikata”, thotë ai.

Bilbilfryrësi regjistroi biletën që merrte një shofer kamioni, përfshirë komunikimin me shoferin. Pastaj, ai kishte nevojë për regjistrimin zyrtar. Sidoqoftë, “Rrugët e Serbisë” refuzuan të jepnin akses të lirë për kërkesat e informacionit. Komisioneri për Informacion ka folur disa herë në publik për këtë rast. Kur bilbilfryrësi kërkoi ndihmën e tij në mënyrë që të merrte regjistrimin e automatit të biletave të tarifave autostradale, Komisioneri i kërkoi “Rrugëve të Serbisë” të shpjegonin arsyet pse ata refuzuan informacionin e kërkuar. Komisioneri nuk e pranoi argumentin se ishte një sekret tregtar, dhe kështu miratoi urdhrin që regjistrimet të bëheshin publike.

“Vendimi im ishte i detyrueshëm me ligj për ‘Rrugët e Serbisë’, por ato nuk vepruan sipas vendimit. Qeveria e Serbisë, e cila duhet të sigurojë zbatim të vendimeve të Komisionerit nëse është e nevojshme, nuk e bëri këtë.”

Personi që e sollli këtë çështje në vëmendjen e publiku dëshmoi edhe si dëshmitar në gjyqin që vijoi. Është interesante se kaseta e tij, një nga provat potenciale të sipërmarrjes kriminale, u zhduk nga dosjet e gjykatës para se të zhvillohej seanca kryesore.

40 Serbia nuk ka ende një ligj që do të mundësonte mbrojtjen efektive të bilbilfryrësve.

2. Masat mbrojtëse kundër keqërdorimit të IT-së

Hyrje

Nga Louise Thomasen

Shembujt e rasteve të paraqitura në kapitullin 1 kanë të bëjnë me një sërë abuzimesh në fushën e Teknologjisë së Informacionit dhe Komunikacionit (ICT) dhe shkeljeve lidhur me korrupsionin. Me qëllim që të mësohet nga rastet lidhur me masat mbrojtëse që mungojnë si dhe të mënyrës se si vendet kanë nxjerrë mësime nga shembujt e rasteve, në këtë kapitull autorë kombëtarë do të përshkruajnë si masa mbrojtëse specifike ashtu dhe ato të përgjithshme kundër korrupsionit të ICT-së për vendet e tyre përkatëse.

Masat mbrojtëse specifike kundër korrupsionit në Teknologjinë e Informacionit (IT) janë:

- Masa mbrojtëse teknike kundër aksesit të paautorizuar dhe abuzimit të sistemeve ICT
- Masa mbrojtëse organizative dhe procedurale, të tilla si 'parimi i shumë syve'
- Monitorimi i trafikut të të dhënave dhe aksesit të punonjësve në sistemet e të dhënave
- Trajnim dhe masa mbrojtëse ndërgjegjësimi për nëpunësit e administratës publike lidhur me rreziqet e korrupsionit ICT dhe masa mbrojtëse
- Auditimi i sistemeve ICT (auditime të brendshme ose të jashtme; të nisura nga autoriteti shtetëror, ose nga raportimet apo ankesat e qytetarëve ose të shtypit)
- Masa mbrojtëse legjislative, të tilla si legjislacion gjithëpërfshirës administrativ, civil, dhe penal për parandalimin dhe sanksionimin e abuzimit të ICT-së për qëllim korrupsioni

Meqenëse rastet përshkruajnë abuzim të ICT-së për korrupsion që tashmë ka ndodhur, nuk kemi kërkuar të sjellim shembuj që patën rezultate specifike që çuan në masa mbrojtëse shtesë apo të planifikuara. Rastet në kapitullin 1 janë të gjitha raste korrupsioni nga jeta reale, dhe si të tilla ato do të plotësojnë dhe pasurojnë atë që mund të mësojmë për masat mbrojtëse që duhet të vendosen për të luftuar korrupsionin që përfshin ICT-në.

Disa shembuj rastesh mund të mos kenë asnjë pasojë, p.sh. duke qenë se janë paraqitur në gjyq, dhe në disa shembuj është e paqartë kush e bëri diçka, ku, dhe si. Ajo që është e rëndësisme është fakti se ne mund të mësojnë nga rastet – mund të mësojmë se çfarë masash duhet të ishin vendosur, aty ku sistemet IT janë të dobët ndaj abuzimit dhe korrupsionit ICT, dhe të mësojmë se në çfarë pike kanë arritur vendet e Ballkanit Perendimor në rrjetin ReSPA (*Shkolla Rajonale e Administratës Publike) në realizimin dhe zbatimin e masave mbrojtëse kundër abuzimit ICT dhe korrupsionit në sektorin publik.*

Shqipëria

Nga Edlira Nasi dhe Ened Kercini

Në epokën e informacionit, ndërsa jemi bërë gjithnjë e më të varur ndaj sistemeve komplekse të informacionit, është për t'u habitur se sa pak vëmendje u është kushtuar personave të ngarkuar për operimin dhe administrimin e këtyre sistemeve. Këta persona mbajnë pozicione me rëndësi dhe besim të pashoq. Veprime dashakeqe nga ana e një personi që punon në këto sisteme mund të çojë në pasoja të rënda.

Këto raste demonstrojnë një sërë pikash për kërcenimin e personit të brendshëm ndaj sistemeve të informacionit. Megjithatë, do të bëhet e qartë se problemet nga personat e brendshëm ekzistojnë tashmë brenda sektorëve, përfshirë policinë, ushtrinë, shoqëritë private dhe sektorëve të energjisë. Do të tregohet, gjithashtu, se ka një prirje të fortë nga ana e drejtuesve për t'i zgjidhur këto probleme shpejt dhe qetë, duke shmangur kështu impakte personale dhe organizative si dhe rrjedhjet në publik.

Nuk jemi në gjendje të provojmë se sa të përhapura janë problemet. Çka raportohet këtu duket sikur është vetëm maja e ajsbergut.

Përveç kësaj, dhe në mënyrë paradoksale, pavarësisht çështjeve të brendshme të evidentuara dhe potencialit të cënueshmërisë së infrastrukturës publike, janë bërë pak përpjekje për të rritur mbrojtjen nga brenda, ndërkohë që investime të rëndësishme i kushtohen vazhdimisht zbulimit dhe parandalimit tëndërhyrjeve të jashtme. Ndërkohë që mbrojtja ndaj kërcenimeve të jashtme faktikisht është e rëndësishme, problemet njerëzore nuk mund të zgjidhen nëpërmjet teknologjisë.

Sistemet e infrastrukturës publike të informacionit do të mbeten për një kohë të gjatë pre e keqpërdorimit dhe abuzimit nga ana e atyre që thjesht e njohin sistemin: punonjësit brenda këtyre sistemeve.

Çështjet kryesore që kemi vënë re në rastet e paraqitura janë paaftësia për të kuptuar pikat e dobëta të punonjësit në rrezik dhe paaftësia për të vendosur rregulla të standardizuara, të cilat drejtojnë sistemet e informacionit që parashikojnë edhe pasoja të qarta në rast keqpërdorimi.

Shqipëria, rasti 1: Korrupsioni në sistemin TIMS të kontrollit kufitar

Ky rast pëfaqëson një abuzim tipik të detyrës dhe mitmarrje nga ana e oficerëve të policisë kufitare duke shënuar me dashje të dhëna të rreme në sistemin IT të TIMS-it (Sistemi i Menaxhinit të Informacionit të Përgjithshëm), që ka për qëllim shmangien e pagesave që i detyrohen shtetit për përdorimin e një automjeti të importuar.

Këtu, çështja kryesore është fakti se ka një ndryshim të madh midis mënyrës se si funksionon në të vërtetë sistemi lidhur me gjurmimin e njerëzve kur kalojnë kufirin, dhe mënyrës që sistemi është projektuar për gjurmimin e targave të automjeteve.

Zhvillimet që kanë ndodhur vitet e fundit lidhur me dokumentet e identiteti dhe pajisjeve elektronike të leximit të instaluara në pikat e kalimit të kufirit, kanë përmirësuar mjaft procesin e regjistrimit të njerëzve, duke përmirësuar kështu cilësinë e sigurimit të të dhënave, duke e bërë më të lehtë dhe transparente nëpërmjet leximit të informacionit nga dokumentet biometetrikë të identitetit, i cili është ruajtur elektronikisht brenda një çipi të sigurisë me funksion RFID.

E njëjta gjë nuk mund të thuhet për gjurmimin e numrit të targave të automjeteve. Ky vazhdon ende të mbetet një proces manual që përfshin punën e njeriut për të lexuar dokumentacionin e duhur, duke verifikuar vërtetësinë e informacionit, dhe, gjithashtu, duke e verifikuar në mënyrë të kryqësuar me numrat unikë të shënuar në brendësi të vendeve specifike dhe të mirënjohura brenda automjetit.

Është pikërisht dobësia e sistemit që u shfrytëzua nga një punonjës i brendshëm, i cili arriti të hartonte një dokument 'origjinal' të bazuar në informacion të rremë të kyçur në Sistemin TIMS. Na duhet të theksojmë se, në fakt, informacioni ishte i vërtetë; vetëm vula e datës u falsifikuar. Një çështje shumë më e madhe (përtej objekti të këtij studimi) është fakti se automjeti kaloi përmes doganës nga fundi i vitit 2009 pa asnjë procedurë të duhur regjistrimi.

Në këtë rast, nuk u përdoren asnjë mjet special apo i sofistikuar IT-je, meqenëse ai ishte thjesht një keqpërdorim i qëllimshëm të sistemit të informacionit; IT-ja u startua fillimisht duke regjistuar autoveturën në sistemin TIMS në momentin që ajo hyri fillimisht në vend, dhe pastaj u bë një keqpërdorim i përsëritur kur – pas 4 viteve – pronari i autoveturës kërkoi së fundi ta regjistronte atë.

Sistemi i informacionit TIMS ka privilegje nivelesh përdorimi dhe administrim shumë të mirë. Rregullorja dhe procedurat ishin ndjekur siç duhet nga forcat e policisë kufitare duke shënuar informacionin dhe firmat përkatëse në regjistrat tradicionale prej letre. Gjithashtu, TIMS-i ka një kapacitet të brendshëm për të regjistruar dhe gjurmuar personat dhe çfarë bëjnë ata, kështu që ishte e lehtë për të dalluar 'punonjësin' në momentin që merreshin dhe konfirmoheshin tregues nga prova të tjera. Në këtë mënyrë, sistemi TIMS ka provuar mundësinë që ka për të mbështetur procesin e auditimit.

Nuk ishim në gjendje të konfirmonim që ky rast shkaktoi një përmirësim sistemi; sidoqoftë, kjo gjë nuk përjashton shumë përmirësime të softuerit të sistemit, riparime softuer dhe ndryshime të tjera procedurale që zbatohen periodikisht. Monitorimi dhe regjistrimi nëpërmjet TV me qark të mbyllur u konsiderua dhe u zbatua me sukses si një parandalues i mirë për minimizimin e shkeljeve të rregullave dhe për të ndihmuar autoritetet në identifikimin e shkeljeve në rast hetimi.

Shqipëria, rasti 2: Korrupsioni në Sistemin Elektronik të Prokurimit Publik

Rasti ka të bëjë me vjedhjen e identitetit të përdoruesit për të siguruar privilegje të sistemit të prokurimit publik që ka si qëllim të qartë të deformojë vendimin final të procesit të prokurimit.

Shqipëria ka vite që ka një sistem elektronik prokurimi, dhe konsiderohet një projekt i suksesshëm. Sistemi ka ndikuar pozitivisht në kostot e përgjithshme të qeverisë në prokurimin e mallrave apo shërbimeve.

Thënë shkurt, sistemi lejon botimin e dokumenteve të tenderit. Pas kësaj, ofertuesit mund të ngarkojnë dokumentat e tyre në sistem dhe të depozitojnë ofertën e tyre financiare. Procesi është i koduar. Ai mbetet i koduar deri në arritjen e afatit të ofertimit, dhe mund të çkodohet vetëm nëse tre ose më shumë nëpunës të autorizuar më parë shënojnë 'emrin e përdoruesit' dhe 'fjalëkalimet' e tyre brenda një afati kohor të përcaktuar mirë. Në disa mënyra, kjo siguron një nivel të mirë transparence ofertimi për tender. Po ashtu, sistemi i prokurimit është gjendje të seleksionojë dhe të regjistrojë dhe njoftojë në mënyrë automatike ofertuesit në përputhje të plotë me ligjin e prokurimit, aktet nënligjore, dhe direktivat. Është e rëndësishme të theksohet se po bëhet një praktikë e mirë fakti qëpara se Kontrolli i Lartë i Shtetit të bëjë një kontroll të një enti publik, zakonisht ata marrin një raport të plotë, të hollësishëm, nga sistemi i prokurimit publik lidhur me entin publik dhe periudhën kohore që kanë në plan të bëjnë kontrollin.

Ajo që u bë shkas për këtë rast ishte fakti që Kontrolli i Lartë i Shtetit qe në gjendje të identifikonte një mospërputhje midis informacionit të siguruar nga sistemi elektronik i prokurimit publik dhe dokumentacionit në letër të tenderit të nënshkruar nga komisioni i caktuar i tenderit.

Si mund të ndodhte një gjë e tillë? Në fillim, kur komisioni i tenderit nis procedurën e tenderit, anëtarët kyçen në hapësirën e dedikuar të sistemit elektronik të prokurimit. Në

mënyrë të ngjashme më një aplikacion vetëshërbimi, pas instalimit fillestar, secili nga anëtarët mund të shënojë një 'emër përdorimi' dhe të zgjedhë një 'fjalëkalim'.

Ky sistem ofron funksionin e rivendosjes së fjalëkalimit, në rast se ai humbet. Kjo veçori mund të aktivizohet nga kryetari i emëruar i komisionit të tenderit. Për këtë, përdoruesve u dërgohet një email, e cila përmban linkun e rivendosjes së fjalëkalimit, meqenëse çdo përdorues duhet të ketë një adresë email-i për t'u regjistruar në sistem. Kjo duket qëështë në rregull, por në fakt ajo e ul sigurinë në nivelin e fjalëkalimit të email-it të përdoruesit, meqenëse të gjithë përdoruesit janë të regjistruar me një adresë zyrtare email-i, e cila nganjëherëështë e përbashkët ose që njerëzit ia dinë fjalëkalimin. Kjo do të thotë se në realitet ata ia dinë 'fjalëkalimet' njëri-tjetrit. Megjithëse kjo praktikë u zbatuar me qëllimet e mira të zgjidhjes së problemeve të punës, ajo e ul sigurinë e përgjithshme të sistemit.

Gjithashtu, kemi identifikuar një çështje tjetër. Edhe kur procedurat dhe rregulloret vendoseshin dhe zbatoheshin nga kapacitetet e sistemit të informacionit të tilla si pranimi vetëm i fjalëkalimeve të forta dhe kërkesa për ndryshimin e herëpashershëm të fjalëkalimit, fillon të shfaqet një faktor tjetër njerëzor – 'lehtësi më e madhe përdorimi'. Ne kemi parë të dhënat që e konfirmojnë këtë. Shumica e përdoruesve bezdisen, sidomos me ndërrimin e herëpashershëm të fjalëkalimeve të ndërlikuara, dhe zgjedhin rrugën e shkurtër duke i lënë fjalëkalimet e pandryshuara me vlerën e paracaktuar që u jepet e atyre në fillim nga administrata e sistemit kur kyçen për herë të parë në sistem. Pas tre muajsh, llogaritë e tyre bllokohen, por është shumë më e lehtë për të kërkuar rivendosjen e fjalëkalimit në vlerën e njëjtë fillestare që u sigurohet atyre gjithmonë nga admisnitrata e sistemit. Në fund, pothuajse të gjitha fjalëkalimet do të jenë të ngjashme.

Është mjaft e pamundur për të provuar se çfarë ndodh dhe nuk disponohen fajle logimi për ta gjurmuar më thellë këtë problem. Në sytë e Kontrollit të Lartë të Shtetit, e vetmja gjë e sigurtë ishte që anëtari i komisionit të tenderit mund të provonte se ai madje nuk ndodhej as në Shqipëri.

Në fund, dizajni i mirë i sistemit dhe procedura do të dështojnë, zinxhiri është aq i fortë sa hallka e tij më e dobët dhe në këtë rast në besojmë fort se ishte shumë e lehtë të përvetësohej identiteti i një përdoruesi duke njohur dobësinë e fjalëkalimit të email-it të tij dhe duke shfrytëzuar aftësinë e rivendosjes së fjalëkalimit që ofrohet nga sistemi i prokurimit.

Ne mendojmë me bindje se nuk ka asnjë mënyrë për të garantuar sigurinë dhe mbrojtjen e duhur duke përdorur vetëm fjalëkalimet. Sistemi i ri duhet të përditësohet me mundësinë për të përdorur autentikimin e dyfaktorësh, i cili të paktën nuk do të linte hapësirë për argumente abstrakte dhe trashanike për të të shmangur identitetin e përdoruesve.

Shqipëria, rasti 3: Korrupsioni nëpërmjet IT-së tek Operatori i Shpërndarjes së Energjisë

Ky rast përfaqëson një manipulim nga 'punonjësi i brendshëm' i një sistemit të informacionit të profilit të lartë; sistemi ishte programuar për të siguruar ndrsyhime sistematike të vlerave për nivelet e konsumit brenda sistemit të faturimit. Kjo gjë e lejoi manipuluesin për të rritur vlerat e faturave të energjisë me qëllimin e arritjes së përfitimeve financiare për kompaninë.

Ky rast shfaqi, gjithashtu, vështirësitë më të mëdha për grumbullimin e informacionit për shkak të ekspertizës së përdorur në menaxhimin e tij të brendshëm nga kompania private, të vlerave të larta monetare të përfshira, dhe vëmendjes më të madhe të publikut të pakënaqur.

Në këtë rast, nuk disponojmë të dhënat e zakonshme që do të siguronin informacion të mjaftueshëm për të kuptuar atë çka ndodhi në të vërtetë me sistemin e informacionit. Sidoqoftë, jemi në gjendje të bëjmë supozime të mjaftueshme bazuar në faktet të besueshme që u siguruan në atë kohë.

Në të dhënat e matjeve të Operatorit për Shpërndarjen e Energjisë ka një vegëz, ku këto të dhëna, bazuar në tregues të caktuar, mund të filtrohen dhe nuk dërgohen drejtpërdrejt për faturim, meqenëse ato mund të paraqesin klientë problematikë, gjoba dhe të tjera çështje të pazakonshme faturimi të cilat duhet të rishqyrtohen më tej nga personeli. Është kuptimplotë fakti se këto të dhëna u filtruan duke patur parasysh çështje të mëparshme pagese, ose ato raste kur personat e ngarkuar për matjen kishin dyshime se konsumatorët po bënin mashtrime me konsumin e energjisë. Fakti se procesi i matjes u krye, sipas regjistrave, gjatë orëve të vona dhe përtej orarit të punës ditor të personelit matës, mund të jetë një tregues kyç që mbifaturimi ishte i qëllimshëm dhe abuziv.

Vula e kohës kur u krye veprimi ishte shumë e dyshimtë dhe ishte një nga pikat kryeosore alarmuese gjatë hetimit. Operatorët e matjes në terren të OSHE-së kishin shkelur jo vetëm protokollin lidhur me shënimin e kohës së grumbullimit të të dhënave, por vulat e kohës tregojnë shpeshtësi përdorimi që nuk janë të mundshme nga njeriu. Prandaj, kjo kishte të bënte ose me manipulimin e të dhënave ose mbledhjen fiktive të tyre. Analiza e të dhënave tregoi këtë të fundit.

Gjithashtu, kjo mund të konsiderohet edhe si përpjekje për të kryer potencialisht një mashtrim ndaj 15.000 konsumatorëve. Përsëri mund të identifikohet i njëjti model, keqpërdorim i qëllimshëm i sistemit të informacionit – këtë herë për rritjen e fitimeve të kompanisë. Ndryshimi qëndrom në faktin se ky operacion nuk mund të jetë veprimi i një personi të vetëm, dhe për kryerjen e një operacioni të tillë janë të nevojshme miratime të caktuara, dhe mëqenëse fitimi shkon drejtpërdrejt në financat e kompanisë, nuk mbetët asgjë që mbështet justifikimin të tilla si gabim i sistemit të faturimit ose gabim i personelit.

Shqipëria, rasti 4: Përvetësimi dhe mashtrimi në mbajtjen e regjistrave kontabël

Ky rast, i cili duket mjaft i padëmshëm, përfaqëson një keqpërdorim të veçantë të sistemit nga ana e një punonjëse përgjegjëse për mbajtjen e librave kontabël, e cila gjatë viteve përvetësoi fonde të cilat ishte caktuar që t'i adminstronte.

Çelësi për të kuptuar se pse kjo është interesante është se ajo nuk përfshin në të vërtetë teknologjinë e informacionit të përdorur por shfrytëzimin, nga ana e financierës, të mungesës së mbikëqyrjes ose vëmendjes së treguar nga supërvizorët.

Po si ka funksionuar një gjë e tillë? Së pari, sistemi financiar përgjegjës për pranimin e pagave dhe dërgimit të tyre përmes sistemit bankar duket që nuk ka qenë në gjendje për të procesuar njëkohësisht detajat individuale të pagës për të gjithë administratën publike dhe njësive të tjera administrative, e tillë si ushtria në fjalë. Së dyti, pati një çështje serioze besimi që përfshinte administratën e brendshme të nivelit të lartë dhe një kontroll i tërthortë i munguar ndërmjet dokumeteve të ndryshme të nënshkruar për paga ndërmjet autoriteteve financiare.

Mund të ndodhë se treguesi i parë për këto çështje potenciale mund të dalë në dritë qëllimisht, por si rezultat i një gabimi të zakonshëm, diçka që mund të vëjë në dijeni punonjësin e financës për dobësinë e sistemit. Pas kësaj, punonjësja futi qëllimisht një gabim tjetër në pagë për të provuar se sistemi financiar ishte i paaftë për ta dalluar siç duhet gabimin, dhe nga kjo merr konfirmimin se kontrolli kryesor financiar kryhet për totalin e shpenzimeve të pagave, i cili nuk duhet të tejkalojë një kufi të caktuar buxhetor, të paraprogramuar, i cili është specifikuar në fillim të vitit fiskal.

E vetmja gjë që mbetet për t'u zbuluar është që një skemë e tillë të funksionojë nevojitetj një rregullim perfekt në një sërë dokumentesh të pagave. Këto paga nevojiten të mbeten vetëm me shumën e njëjtë të totalit në fund të muajit. Në këtë mënyrë, tabelat mund të manipulohen lehtësisht për aq sa detajet individuale mbahen brenda asaj çka sistemi i financës parashikon si shuma totale në mënyrë që të mos ngrejë ndonjë dyshim. Në të njëjten kohë, do të ketë ndrsyhime të vogla negative për shumicën e pagave të individëve, të cilat mund të përmblidhen në një llogari të vetme që përfshin shumën finale. Një gjë e tillë ishte e mundur sepse bankat zakonisht nuk janë të interesuara se cila është vlera e pagës individuale të një personi. E rëndësishme është që numri i cili u disbursua nga financa përputhet me totalin e të gjitha pagave. Komponentet dhe shkallët që ka paga ushtarake, të tilla si përfitimet dhe shtesat e tjera, e bëjnë edhe më të vështirë për personelin e financës dhe bankën të dyshojë për diçka që mund të jetë përtej normave normale të pagës.

Kjo është arsyeja pse qe i mundur përvetësimi për një periudhë të zgjatur kohe. Për aq sa shuma totale nuk tejkalonte shumën e miratuar nga Shefi i Shtabit dhe Komandanti, skema mund të vazhdonte të funksiononte.

Ky lloj keqpërdorimi i sistemit mund të përshkruhet si një sulm ndaj një personi të rrethuar ~~në mes shumë të tjerëve. Në këtë rast, sulmi u krye nga dikush brenda sistemit që ishte i/e~~ besuar nga shefat e tij/saj, të cilët konfirmonin librin e pagës pa e rishqyrtuar më tej, dhe shfrytëzoi faktin interesant se financa dhe banka shkëmbenin midis tyre vetëm shumën totale.

Në fakt, kjo lloj vegëze është mbyllur tashmë, meqë softueri i financës është modernizuar dhe shkëmbimi i të dhënave me bankat tani përmban më shumë detaje nga sistemi i financës.

Masat mbrojtëse kundër korrupsionit nëpërmjet IT-së në Shqipëri

Masat mbrojtëse ligjore

Për sa i përket garancive ligjore, Shqipëria ka rishikuar, kohët e fundit, kuadrin e saj ligjor dhe Kodin Penal me qëllim që të pasqyrojë shfaqjen e krimeve kibernetike ose krimeve që lidhen me IT-në. Ligjet më kryesore kanë të bëjnë edhe me fushën e abuzimit të arkivave ose burimeve të IT-së, Ligji nr. 10023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.11.1995 "Kodi i Republikës së Shqipërisë", i ndryshuar, shtoi shkelje të reja në Kodin Penal, përfshirëmashtrimin kompjuterik[41], falsifikimi kompjuterik[42], hyrja e paautorizuar kompjuterike[43], përgjimi i paligjshëm i të dhënave kompjuterike[44], ndërhyrja

41 Neni 143/b – "Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet. Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet."

42 Neni 186/a - Falsifikimi kompjuterik- "Futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.. Kur kjo vepër kryhet nga personi, që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike, në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda për interesin publik, dënohet me burgim tre deri në dhjetë vjet."

43 Neni 192/b - Hyrja e paautorizuar kompjuterike- "Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet.Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet."

44 Neni 293/a - Përgjimi i paligjshëm i të dhënave kompjuterike- "Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet.. Kur kjo vepër kryhet nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet."

në të dhënat kompjuterike[45], ndërhyrja në sistemet kompjuterike[46], si dhe keqpërdorimi i pajisjeve[47].

Përveç kësaj, kohët e fundit është miratuar legjislacioni që mbulon databazat elektronike, duke iu përgjigjur nevojës për bazën ligjore që lidhet me krijimin e databazave elektronike me qëllim përmirësimin e shërbimeve publike; këto akte ligjore ndikojnë edhe në përdorimin dhe menaxhimin e informacionit të databazave dhe procedurat që duhen ndjekur nga nëpunësit me qëllim arritjen e standardeve të kërkuara nga ligji për sigurinë e të dhënave. Ligji nr. 10 325, datë 23.09.2010 "Për bazat e të dhënave shtetërore" përshkruan mjetet e regjistrimit dhe menaxhimit të databazave shtetërore, ndërkohë që cakton gjithashtu një Autoritet Koordinues Përgjegjës, që lidhet me rregulloren e databazave dhe përdorimin e tyre.

Ministri i Inovacionit dhe Teknologjisë së Informacionit e të Komunikimit (tani Ministri i Shtetit për Inovacionin dhe Administratën Publike) i ka propozuar Këshillit të Ministrave masa specifike për të garantuar sigurinë e databazave. Ne veçanti, Vendimi i Këshillit të Ministrave nr. 961, datë 24.11.2012 cakton si Autoritetin Përgjegjës të Koordinimit Agjencinë Kombëtare të Shoqërisë së Informacionit, ndërsa Vendimi i Këshillit të Ministrave nr. 945, datë 02.11.2012, miraton rregulloren për administrimin e databazave. Aspekt i rëndësishëm i kësaj rregullore për administrimin e databazave është përcaktimi i niveleve të sigurisë, në nivel të lartë, të mesëm dhe të ulët[48], ku niveli i sigurisë përcaktohet bazuar në parametrat e integritetit, konfidencialitetit, dhe disponueshmërisë së të dhënave[49]. Në këtë mënyrë, masat e sigurisë teknike merren bazuar në kategorizimin e databazave. Masat e sigurisë që duhet të merren mbikëqyren nga Agjencia Kombëtare e Sigurisë Kompjuterike. Megjithatë, meqenëse Agjencia Kombëtare e Sigurisë Kompjuterike është një institucion relativisht i ri me burime njerëzore mjaft të kufizuara, ajo është në procesin e rritjes së kapaciteteve të saj me qëllim plotësimin e kërkesave që ia ngarkon ligji.

Ndër ligjet e tjera kryesore lidhur me çështjet e IT-së përfshijnë ligjet dhe dokumentet e mëposhtme, të cilat garantojnë zbatimin dhe përdorimin e duhur të sistemeve IT:

- Ligji nr. 9880, datë 25.02.2008 "Për nënshkrimin elektronik"
- Ligji nr. 9887, datë 10.03.2008, i ndryshuar meLigjin nr. 48/2012 "Për mbrojtjen e të dhënave personale"

45 Neni 293/b - Ndërhyrja në të dhënat kompjuterike- "Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet.Kur kjo vepër kryhet në të dhënat kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet."

46 Neni 293/c - Ndërhyrja në sistemet kompjuterike- "Krijimi i pengesave serioze dhe të paautorizuara për të cënuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet.Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet."

47 Neni 293/ç - Keqpërdorimi i pajisjeve- "Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenet 192/b, 293/a, 293/b e 293/c të këtij Kodi, dënohen me burgim nga gjashtë muaj deri në pesë vjet."

48 Neni 17, VKM nr. 945 datë 2.11.2012 (Aneksi 1)

49 Po aty, Neni 18

- Strategjia ndersektoriale per shoqerine e informacionit2008-2013
- Ligji nr. 72/2012, "Për organizimin dhe funksionimin e Autoritetit Shtetëror për Informacionin Gjeohapësinor në Republikën e Shqipërisë"
- Ligji nr. 9918, datë 19.05.2008 (i ndryshuar) "Për komunikimet elektronike në Republikën e Shqipërisë
- Ligji nr. 119/2014 "Për të drejtën e informimit". (votuar në fund të muajit shtator 2014 dhe duke zëvendësuar Ligjin nr. 8503, datë 30.06.1999 "Për të drejtën e informimit për dokumentet zyrtarë")

Masat mbrojtëse teknike kundër korrupsionit

Me më pak interes për njerëzit, një pjesë kryesore e strategjive të sigurisë së sistemeve të informacionit janë të një natyre njerëzore. Dy agjenci kryesore qeveritare në Shqipëri, AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit) dhe ALCIRT (Agjencia Kombëtare për Sigurinë Kompjuterike) me ndihmën e ASPA (Shkolla Shqiptare e Administratës Publike) janë të angazhuara në trajnimin e personelit të teknologjisë së informacionit për të mbrojtur më mirë sistemet qeveritare kundër abuzimeve të mundshme korruptive. Roli i Agjencisë Kombëtare për Sigurinë Kompjuterike është veçanërisht i rëndësishëm, nëse kemi parasysh se do të ishte institucioni që ka për detyrë të sigurojë ekspertizën e nevojshme për kontrollin e sigurisë dhe masave të tjera të databazave. Veçoritë specifike të kontrollit të databazave sigurojnë një bazë interesante për të kuptuar më mirë nëse masat e sigurisë së IT-së janë të instaluara. Mbështetur në rregulloren për administrimin e databazave, sistemet kontrollohen rregullisht, çdo dy vjet për databaza të sigurisë së lartë, dhe çdo tre vjet për ato me nivel të mesëm sigurie dhe çdo katër vjet për ato me nivel të ulët sigurie. Procesi i ndjekur garanton se janë vendosur masat mbrojtëse teknike, ndërsa Rregullorja parashikon se kontrolli duhet të përfshijë verifikimin e përputhjes me inventarin e aseteve të sistemit, kontrollin nëse masat e sigurisë janë të përshtatshme, si dhe kontrollin nëse masat teknike dhe të sigurisë zbatuar siç duhet[50]. Bazuar në raportet dhe procesverbalet e kontrolleve, institucionet duhet të marrin hapa të nevojshme për të ndrequr mospërputhjet e evidentuara.

Masat mbrojtëse organizative dhe procedurale

Tashmë zbatohet një procedurë e rregulluar me ligj (Udhëzimi nr. 2, datë 9 shkurt 2013 i Ministrit për ICT "Për standartizimin e zhvillimit të Termave të Referencës për projektet e ICT-së në administratën publike"), sipas së cilit çdo subjekt qeveritar që rishikon ose ndërton një sistem informacioni duhet të marrë edhe një rishikim të dizajnit, dhe asnjë kundërshtim të termave të referencës nga ekspertë të Agjencisë Kombëtare për Shoqërinë e Informacionit. Kjo është një strategji shqiptare për shfrytëzimin e ekspertizës më të mirë vendase dhe njohurive teknike, nga ngjizja fillestare publike e projektit të IT-së deri në dokumentet e përfunduara të tenderit.

50 Neni 24 (3), Vendimi i Këshillit të Ministrave nr. 945 datë 02.11.2012

Qeveria e re shqiptare, me axhendën për të luftuar korrupsionin, ka prezantuar kohët e fundit një procedurë të re me mbështetjen e Agjencisë Kombëtare për Shoqërinë e Informacionit në lidhje me pranimet e sistemeve të informacionit. Pasi sistemet e informacionit të jenë pranuar, ajo pritet të ketë një qasje të ndryshme, duke hapur pjesëmarrjen në këtë grup pune të caktuar për pranimin e ekspertëve të jashtëm. Shpresohet se kjo mund të zvogëlojë në masë të madhe disa probleme të cilat janë gjetur më parë me projektete e sistemeve të informacionit gjatë periudhës së pranimit (për shumë toleranca dhe shumë punime të papërfunduara) kryesisht të lidhura me stafin teknik dhe stafin drejtues

Të thuash se siguria është diçka që mund të blihet lehtë është një supozim i gabuar; faktori njeri mund të demonstrojë se pritjet më të besueshme janë të pasakta.

Trajnimi dhe ndërgjegjësimi

Shqipëria ka një tjetër iniciativë të vazhdueshme që vjen nga "Agjencia Kombëtare për Sigurinë Kibernetike" në bashkëpunim me "Shkollën Shqiptare të Administratës Publike" për organizimin e kurseve të trajnimit për pothuajse të gjithë stafin e teknologjisë së informacionit në institucionet publike dhe subjektet e tjera qeveritare. Kurset e trajnimit ndryshojnë për nga shumëllojshmëria e temave të ndryshme të tilla si siguria e sistemeve, mbrojtja dhe vlerësimi i rrezikut të jashtëm dhe të brendshëm. Kjo mund të jetë shenja e parë e një zhvillimi pozitiv duke ndryshuar fokusin nga pajisjet dhe softueret tek njerëzit që i administrojnë dhe i përdorin ato.

Përfundim

Në përfundim, ne besojmë se është i nevojshëm hetimi i mënyrave të tjera të menaxhimit të sigurisë së sistemeve të informacionit dhe parandalimit të korrupsionit nga brenda sistemit, duke qenë se ata zakonisht kanë tendencën për të mos i marrë parasysh faktorët socialë të rreziqeve nga "kërcënimi i brendshëm" dhe vështirësitë për të përshtatur proceset e informacionit me struktura joformale të institucioneve publike.

Bosnja dhe Hercegovina

Nga Aleksandra Martinovic dhe Srdjan Nogo

Hyrje në shembujt e masave mbrojtëse kundër keqpërdorimit të IT-së

Kur mjetet e IT-së dëmtojnë reputacionin e individëve apo institucioneve, atëherë përdorimi i këtyre mjeteve dhe teknologjive përbën një formë të veprës penale. Në shumë raste, aktivitetet kriminale kibernetike në BiH janë shumë të vështira për t'u provuar dhe pasojat dhe dënimet ligjore për këto aktivitete janë të dobëta. Me qëllim të parandalimit të aktiviteteve të tilla kriminale, Bosnja dhe Hercegovina ka ndërmarrë tashmë hapat në luftën kundër krimit kibernetik, nëpërmjet zbatimit të projekteve në vijim:

- sistemi mbrojtës identifikimi i centralizuar i qytetarëve (IDDEEA),
- infrastruktura PKI (Akti i Nënshkrimit Elektronik në BiH),
- sistemi i centralizuar ombrellë i projekteve elektronike të Qeverisë për
- shkëmbimin e informacionit ndërmjet të gjitha niveleve të qeverisjes në BiH,
- projekte të Zyrës së Reformës së Administratës Publike (Parco) për
- përmirësimin e administratës publike.

Ka edhe shumë aktivitete dhe projekte të tjera, të zbatuara përmes Ndihmës Europiane dhe fondeve të tjera dypalëshe, të cilat në mënyrë të konsiderueshme ndihmojnë në luftën kundër korrupsionit.

Bosnja dhe Hercegovina nënshkruan "Axhendën e-SEE për Shoqërinë e Informacionit", në vitin 2002 në Beograd, dhe u bë një anëtar i Europës Elektronike Juglindore. Në axhendë, u ra dakord që palët shtetërore duhet të zhvillonin dhe të miratonin një politikë dhe strategji për zhvillimin e shoqërisë së informacionit SEE, dhe një "Zonë prioriteti - Hapësirë e Vetme Informacioni për SEE", e cila përcakton mënyrën për krijimin e një infrastrukture publike për operacione të sigurta bazuar në nënshkrime të kualifikuara elektronike.

"Ligji për Nënshkrimet Elektronike" dhe "Ligji për Transportin Elektronik Ligjor dhe Tregtar "u miratuan në vitin 2006. Vendimet që rregullojnë përdorimin e fushës së nënshkrimeve elektronike dhe çertifikimet janë miratuar gjithashtu për të siguruar kuadrin e nevojshëm ligjor për implementimin e nënshkrimit dixhital.

Masat mbrojtëse në shembujt e rasteve në Bosnjë dhe Hercegovinë

Ky është një rast që lidhet me Prokurorin e Shtetit i cili pretendohet të ketë hyrë padrejtësisht dhe qëllimisht në llogarinë e-mail të ish-Prokurorit të Përgjithshëm, me qëllimin për t'a diskreditуar atë, pikërisht para pezullimit të tij nga detyra zyrtare si prokuror i Përgjithshëm.

Masat mbrojtëse teknike kundër qasjes së paautorizuar dhe keqpërdorimit të sistemeve të IT-së

Personat përgjegjës nga gjyqësori i BiH kanë mësuar se masat ekzistuese të sigurisë nuk kanë qenë të mjaftueshme për parandalimin e qasjes së qëllimshme dhe të paligjshme në një sistem kompjuterik - domethënë, një llogari zyrtare postare të një punonjësi. Prandaj, gjyqësori i BiH ka përmirësuar procedurat e sigurisë në të gjitha nivelet dhe zbaton standardin ISO/IEC 27001:2005.

Masat mbrojtëse organizative dhe procedurale të tilla si "Parimi i shumë syve"

Edhe pse çdo gjë është zbatuar sipas ligjit, masat mbrojtëse procedurale që ishin tashmë në vend ishin të pamjaftueshme dhe të papërshtatshme për të parandaluar gabimin e faktorit njerëzor dhe ndërgjegjësimin e sigurisë së dobët të njerëzve duke përdorur sistemin infrastrukturor të IT-së.

Monitorimi i trafikut të të dhënave dhe aksesit të punonjësit në sistemet e të dhënave

Ligjet dhe procedurat e gjyqësorit të BiH përshkruajnë monitorimin e trafikut të të dhënave dhe monitorimin e aksesit të punonjësve në sistemet e të dhënave. Sipas raporteve të brendshme, të kryera nga institucione të ndryshme gjyqësore, ai u njoh si një masë paraprake e nevojshme, dhe si i tillë është përdorur për mbrojtjen kundër korrupsionit dhe krimit kibernetik.

Masat e trajnimit dhe ato sensibilizuese për nëpunësit civilë mbi rreziqet e korrupsionit nëpërmjet IT-së dhe masat mbrojtëse

Po, Agjencia për Nëpunësit Shtetërorë të Bosnjës dhe Hercegovinës dhe agjencive të ngjashme në nivel entiteti, kanë trajnuar nëpunësit e tyre civilë për të zvogëluar rrezikun e konfliktit të interesave që krijohet, dhe për rritjen e një kodi sjelljeje në administratën publike në të gjitha nivelet administrative qeveritare.

Agjencia për Parandalimin e Korrupsionit dhe Bashkërendimit të Luftës Kundër Korrupsionit është një institucion në nivel shtetëror, e cila është gjithashtu përgjegjëse për zhvillimin dhe monitorimin e trajnimit arsimor për parandalimin dhe luftën kundër formave të ndryshme të korrupsionit. Për shkak të mungesës së vullnetit politik të plotësimit dhe pajisjes me staf të Agjencisë, nuk kapacitetet për të zbatuar plotësisht të gjitha detyrat e përcaktuara sipas ligjeve përkatëse.

Auditimi i sistemeve të IT-së

Organizata tani zbaton auditim shtesë të sistemeve të IT-së për parandalimin e shpërdorimit të sistemit të IT-së në të ardhmen.

Masat mbrojtëse legjislative

- Ligji për Nënshkrimin Elektronik
- Ligji për Biznesin Elektronik
- Ligji për Transportin Elektronik Ligjore të Biznesit
- Ligji për Mbrojtjen e Informacionit të Klasifikuar

Bosnja dhe Hercegovina, rasti 2: Një tjetër punësim i mundshëm i diskutueshëm në Institucionin e Lartë të Auditimit të Republikës Srpska

Rasti i një testi me shkrim për zgjedhjen e dy auditorëve të rinj të performancës për Institucionin Suprem të Auditimit të Republikës Srpska, ku të dhënat nga testi mungonin, dhe ku ekziston mundësia e përzgjedhjes së një kandidati para publikimit të rezultateve të testimit.

Masat mbrojtëse teknike kundër qasjes së paautorizuar dhe keqpërdorimit të sistemeve të IT-së

Sa për masat e sigurisë (masat mbrojtëse teknike) për parandalimin e këtyre llojeve të problemeve në të ardhmen, sipas burimeve brenda ISA së RS asgjë nuk është bërë deri më tani.

Masat mbrojtëse organizative dhe procedurale të tilla si "parimi i shumë syve"

Atje, përveç fushave të cilat nuk ishin zbatuar si duhet sipas ligjit, kishte madje edhe disa masa mbrojtëse procedurale të pamjaftueshme dhe të papërshtatshme. Kandidatët duhet të kryenin testet duke përdorur softuerë të sigurt, por në vend të kësaj, kandidatët i plotësonin testet e tyre në një format të thjeshtë ëord-i pa zbatuar ndonjëmbrojtje, në mënyrë që çdo person nga komisioni përgjegjës të kishte mundësinë për të bërë ndryshime në teste. Për më tepër, këtë herë kandidatët nuk u lejuan të bënin kopje të testeve në memorien e USB-ve të tyre dhe testet nuk iu dhanë atyre për shqyrtim.

Monitorimi i trafikut të të dhënave dhe aksesi i punonjësve në sistemet e të dhënave

Organizata nuk ka mësuar asgjë nga ky rast dhe nuk ka asnjë vetëdije se monitorimi i trafikut të të dhënave është i nevojshëm si një masë mbrojtëse.

Masat e trajnimit dhe ato sensibilizuese për nëpunësit civilë mbi rreziqet e korrupsionit nëpërmjet IT-së dhe masat mbrojtëse.

Po, Agjencia për Nëpunësit Shtetërorë të Bosnjës dhe Hercegovinës dhe agjencive të ngjashme në nivel entiteti, kanë trajnuar nëpunësit e tyre civilë për të zvogëluar rrezikun e konfliktit të interesave që lind, dhe për rritjen e një kodi sjelljeje në administratën publike në të gjitha nivelet administrative qeveritare.

Auditimi i sistemeve të IT-së

Organizata duhet të zbatojë auditimin e brendshëm të sistemeve të IT-së dhe ky është një detyrim i tyre sipas ligjit.

Masat mbrojtëse legjislative

E pazbatueshme.

Bosnja dhe Hercegovina, rasti 3: Keqpërdorimi i sistemit elektronik të projektit CIPS.

Projekti i Sistemit të Mbrojtjes së Identifikimit të Qytetarit (CIPS) ka filluar në Bosnjë dhe Hercegovinë në prill 2002, kur, në baza të përkohshme, u krijua drejtoria për zbatimin e tij. Detyra kryesore e projektit ishte krijimi i një pjese të sistemit përmes të cilit do të zbatohet Ligji për Regjistrat Qëndrorë dhe Shkëmbimit të të dhënave. Nga faza shumë të hershme të projektit CIPS, një numër ankesash janë regjistruar rreth keqpërdorimit të sistemit të tij elektronik, veçanërisht në nxjerrjen e kartave të identitetit dhe pasaportave personale në të gjithë vendin.

Masat mbrojtëse teknike kundër qasjes së paautorizuar dhe keqpërdorimit të sistemeve të IT-së.

Ndërmjet 2012 dhe 2015, IDDEEA ka zbatuar standardet në vijim: ISO/27001:2005 dhe ISO/90001:2008 (me auditimet e tyre të skeduluara[51]).

Sistemi i Menaxhimit të të Dhënave (DMS) të IDDEEA, i përdorur për mbajtjen e të dhënave në institucionet shtetërore dhe në nivel entiteti, si dhe agjencitë kërkesat e të cilave duhet të jenë në përputhje me një standard shumë të lartë të sigurisë dhe sigurimit të IT.

Masat mbrojtëse organizative dhe procedurale të tilla si "parimi i shumë syve"'

- Për të vazhduar me zbatimin e standardeve më të rëndësishme dhe për të përdorur rregullisht shërbimin e auditimit në përputhje me rregullat dhe legjislacionin e BE-së me një kujdes të veçantë ndaj Standardeve të Menaxhimit të Cilësisë ISO 9001.

- Kontrolli i sigurisë së punonjësve zbatohet në autoritetet kompetente (Agjencia e Inteligjencës dhe e Sigurimit të BiH) i cili siguron shmangien e shkeljeve të sigurisë së IT-së dhe gjithashtu mbledh të dhëna personale të të gjithë personelit të kontraktuar për krijimin e një profili social për përdorim në të ardhmen.

Monitorimi i trafikut të të dhënave dhe qasje e punonjësve në sistemet e të dhënave sa i përket infrastrukturës, institucionet e sigurisë së transmetimit të të dhënave në BiH kanë krijuar një rrjet shumë të sofistikuar të komunikimit përmes teknologjisë së Hierarkisë Dixhitale të Sinkronizuar (SDH) që mundëson ndarjen e shpejtë, të besueshme dhe efikase të të dhënave, imazheve dhe tingujve. Rrjeti SDH është një sistem i mbyllur, i pa lidhur në internet dhe punon në një gamë të veçantë të frekuencave të mbuluara për këtë qëllim. Institucioni që mirëmban rrjetin teknik SDH, Agjencinë për dokumentet e identifikimit, regjistrat dhe shkëmbimin e të dhënave (IDDEEA), është përgjegjës për dokumentet e identifikimit, ruajtjen, personalizimin dhe transportin e dokumenteve, si dhe mbajtjen e procesverbalit qendror dhe shkëmbimin e informacionit ndërmjet autoriteteve kompetente në Bosnjë dhe Hercegovinë.

IDDEEA[52] monitoron, koordinon dhe rregullon fushën institucionale të dokumenteve të identifikimit, dhe si e tillë ka zhvilluar një nënshkrim elektronik në një sistem të mbyllur - dhe përvoja e saj në zbatimin e nënshkrimeve elektronike në sistemet e mbyllura është shumë e rëndësishme për zbatimin e Ligjit për Nënshkrimin Elektronik BiH dhe sistemet e hapura.

51 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemi d=214&lang=en
52 http://www.iddeea.gov.ba/images/stories/PDF/law_on_agency_final.pdf

Problemet kyçe përfshijnë:

- Mungesën e marrëveshjeve institucionale të nevojshme për koordinimin e aktiviteteve në fushën e shërbimeve të qeverisjes elektronike (të kryer nga nivele dhe ministri të ndryshme),
- Përdorimin joracional (të shpërndarë në nivel të pamjaftueshëm) të personelit të IT-së (teknologjisë së informacionit),
- Kuadro të pamjaftueshme ligjore dhe të politikave të ICT-së në përdorim nga autoritetet qeveritare në nivele shtetërore dhe subjektesh, dhe
- Moszbatimin e udhëzimeve të IDDEEA-s.

Trajnimi dhe masat ndërgjegjësuese për nëpunësit civilë për rreziqet e korrupsionit dhe msat mbrojtëse të IT-së

Agjencia për nëpunësit civilë të BiH (Bosnjë Hercegovinës) dhe agjenci të ngjashme të nivelit të subjekteve janë duke trajnuar nëpunësit e tyre civilë për të zvogëluar rreziqet e konflikteve të interesit, dhe për të përmirësuar kodin e sjelljes në administratën publike në të gjitha nivelet administrative qeveritare.

IDDEEA ka zbatuar një platformë të mësimit me anë të internetit për edukimin e vazhdueshëm dhe përmirësimin e aftësive të personelit të saj, e cila është e nevojshme për të arritur standardet më të larta të efikasitetit dhe profesionalizmit.

Agjencia për Parandalimin e Korrupsionit dhe Bashkërendimin e Luftës Kundër Korrupsionit është një institucion në nivel shtetëror, e cila është gjithashtu përgjegjëse për zhvillimin dhe monitorimin e trajnimit arsimor për parandalimin dhe luftimin e formave të ndryshme të korrupsionit. Për shkak të mungesës së vullnetit politik për plotësimin e stafit dhe pajisjen e Agjencisë, asaj i mungojnë kapacitetet për zbatim të plotë të të gjitha detyrave të parashikuara nga ligjet përkatëse.

Auditimi i sistemeve të IT-së

Po, departamenti i auditimit të brendshëm për sistemin informativ të IT-së u krijua për parandalimin e abuzimit me sistemet e teknologjisë së informacionit.

Garancitë/masat mbrojtëse legjislative

- Ligji për mbrojtjen e personave që denoncojnë korrupsionin në institucionet e Bosnjës dhe Hercegovinës (“Fletorja Zyrtare e Bosnjës dhe Hercegovinës” nr. 100/13)
- Ligji për Administratën (“Fletorja Zyrtare e Bosnjës dhe Hercegovinës” nr. 32/02 dhe 102/09),
- “Udhëzimet” për paraqitjen e raporteve të brendshme për dyshime ose probleme rreth korrupsionit nga punonjës të Agjencisë për Dokumentet e Identifikimit, Regjistrat dhe Shkëmbimin e të Dhënave të Bosnjës dhe Hercegovinës, 31 mars 2014.

MASAT MBROJTËSE KUNDËR KORRUPSIONIT NËPËRMJET IT-SË NË BOSNJË DHE HERCEGOVINË

Lufta kundër korrupsionit

Të gjitha raportet përkatëse vendore dhe ndërkombëtare mbi gjendjen e korrupsionit në BiH theksojnë se korrupsioni është ndër problemet më të mëdha në shoqëri dhe pengesë e madhe për reformat e ndryshme dhe progresin e përgjithshëm ekonomik dhe social. Raport progresi më i fundit i BE-së për BiH tregon sërish se vendi është në një fazë të hershme në luftën kundër korrupsionit[53]. Për më tepër, pjesët kryesore të legjislacionit kundër korrupsionit janë ndryshuar në mënyra që cënojnë arritjet e mëparshme. Korrupsioni mbetet i përhapur, me të dhëna të pamjaftueshme të hetimit dhe ndjekjes penale në çështje të njohura.

Sistemi gjyqësor

Në vitin 2013 Këshilli i Lartë i Gjyqësorit dhe i Prokurorisë (HJPC) ndërmori një sërë masash dhe veprimesh konkrete që duhet të kontribuojnë për një punë më profesionale dhe të një cilësie më të mirë nga prokurorët. Siç besojmë, çështja 1 e përshkruar në kapitullin 1 kontribuoi për automatizimin dhe profesionalizimin e shpejtë të këtij sistemi. Njohuria, aftësitë dhe perceptimi i çështjeve aktuale për rëndësinë e punës së prokurorisë u rritën nëpërmjet një angazhimi të veçantë të projektit “Forcimi i kapacitetit të prokurorëve në sistemin e drejtësisë penale” në fushën e arsimit.Këto objektiva arrihen me anë të përgatitjes së moduleve të trajnimit, organizimit të disa strategjive arsimore, bashkëpunimit me JPTC-të (Qendrat e Trajnimit të Gjyqësorit dhe Prokurorisë), me qëllim përmirësimin e modelit aktual të përdorur për prokurorët në rol edukuesdhe menaxhimin e rrjeteve tëtë gjithë grupeve të interesit të hetimit penal në procesin arsimor. Në këtë proces më shumë se 150 prokurorë zgjerojnë njohuritë e tyre në fushat e mëposhtme:

- procedimet penale kundër personave juridikë,
- imuniteti i dëshmitarëve,
- aftësitë e studimit dhe kërkimit,
- hetimet e posaçme,
- krimi kibernetik,
- pastrimi i parave dhe hetimet financiare,
- trafikimi dhe
- aftësitë dhe metodologjitë e komunikimit.

Sa më sipër, ne vërejtëm shumë fakte të rëndësishme në lidhje me legjislacionin dhe treguam se respektimi i kuadrit ligjor mund të parandalojë ndjeshëm këtë lloj krimi dhe korrupsioni.

53 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

Përveç auditimeve të rregullta, gjatë vitit 2013 Zyra e Kontrollit të Lartë të BiH (SAI BiH) kreu një auditim performance: "Shërbimet e telekomunikacionit në institucionet e Bosnjës dhe Hercegovinës". Raporti përkatës i auditimit theksoi shembuj pozitivë të HJPC-së, të cilat shpenzonin një shumë mjaft më të vogël për shërbimet e Internetit në krahasim me institucione të tjera nga grupi model i audituar, megjithëse HJPC ka një numër shumë më madh përdoruesish.

Siguria e përforcuar e sistemit të informacionit gjyqësor të BiH-së vazhdon të jetë një prej prioriteteve të saj strategjike, siç përcaktohet në Strategjinë për reformën e sistemit gjyqësor në BiH 2014-2018[54] . Gjithashtu, ka rekomandime të HCJP-së se investimet kapitale gjyqësore duhet të përfshijnë zëvendësimin e pajisjeve tëvjetëruara dhe prokurimin e pajisjeve kompjuterike që mungojnë; zhvillimin e mëtejshëm të sistemeve informative në sistemin gjyqësor; mirëmbajtjen e pajisjeve ekzistuese dhe licencave të softuerëve; dhe trajnimin e IT-së dhe stafit tjetër të gjyqësorit.

Në kuadër të procesit, kompjuterizimi i gjyqësorit, një sistem për shkëmbimin elektronik të të dhënave midis agjencive të policisë dhe zyrave të prokurorëve, është krijuar dhe ka filluar zyrtarisht në qershor të vitit 2013. Prokurorët pranë prokurorive në të gjithë vendin tashmë kanë mundësinë për të monitoruar të dhënat elektronike nën juridiksionin e agjencive policore, në përputhje me kuadrin e zbatueshëm ligjor. Për më tepër, agjencitë policore kanë aftësinë për të ndjekur statusin e raporteve policore për krime, të paraqitura në zyrat e prokurorëve të ruajtura në sistemin e tyre për menaxhimin automatik të çështjeve (TCMS). Sistemi u krijua në bazë të Marrëveshjes së lidhur ndërmjet HJPC-së, Ministrisë së Sigurisë të BiH, Agjencisë Shtetërore të Hetimit dhe, Policisë Kufitare, si dhe Ministrisë së Brendshme, në të gjitha nivelet e qeverisjes. Mbështetja për Gjyqësorin e Bosnjës dhe Hercegovinës (IPA 2009) dhe projekti IPA "Mbështetje për reformën e policisë" janë dy projektet kryesore që çuan në këtë sistem.

Me qëllim që t'i përgjigjen nevojave në rritje të sistemit, veçanërisht në lidhje me një sistem të ri të menaxhimit të çështjeve automatike për gjykatat dhe prokuroritë (CMS/TCMS) dhe për të garantuar zgjidhje softueri në përputhje me standardet aktuale të softuerit, procesi i përditësimit të të gjithë komponentëve të harduerit dhe softuerit të sistemit ICT (optimizimi dhe konsolidimi i sistemit ICT në gjyqësorin e BiH-së) vazhdoi në vitin 2013. Ky proces u krye me qëllim që:

- të reduktojë, në nivelin më të ulët të mundshëm, kohën e mosfunksionimit të sistemit të shkaktuar nga vjetërimii pajisjeve të teknologjisë së informacionit dhe softuerëve;
- të garantojë shfrytëzimin optimal të serverit ekzistues dhe kapaciteteve të rrjetit në qendrat e të dhënave të HJPC-së;
- të mundësojë operacionet normale të përdoruesve në sistemin gjyqësor dhe akses të lehtë tek shërbimet elektronike të gjyqësorit, të vëna në dispozicion publikisht nëpërmjet Internetit;
- të përmirësojë sigurinë e të dhënave të ruajtura në bazat e të dhënave të sistemit të informacionit gjyqësor; dhe
- të garantojë përmbushjen e kërkesave teknike për shkëmbimin normal tëtë dhënave në sistemet e jashtme (regjistrat policorë, tatimorë dhe regjistra të tjerë elektronikë qeveritarë) qëështëi një rëndësie themelore për luftën kundër korrupsionit dhe krimit të organizuar.

Në kuadër të këtij projekti, stafi i Departamentit të HJPC-së për ICT-në ka kryer një përditësim të sistemit për menaxhimin e identiteteve dixhitale, si dhe sistemet e e-mailit në qendrat e të dhënave për përpunimin dhe ruajtjen e të dhënave brenda HJPC-së.

Të gjitha këto masa pranohen nga raporti i fundit i progresit të BE-së për BiH. Ai thekson se sistemi i informacionit dhe komunikimi gjyqësor janë plotësisht funksionalë. CMS/TCMS përfshin mbi 3.4 milionë raste të regjistruara, dhe përgatit raporte automatike mbi performancën e gjyqësorit, të cilat kontribuojnë në politikat dhe vendimet e planifikimit strategjik. Qasja në portalin gjyqësor është rritur ndjeshëm, si dhe qasja në shkresat informative nga palët e procedimit apo avokatët e tyre. Qendra e Dokumentacionit Gjyqësor ka regjistruar gjithashtu një rritje të ndjeshme të vizitave online.

Qendrat e Trajnimit të Gjyqësorit dhe të Prokurorisë të dy subjekteve ofruan trajnim për gjyqësorin. Në përpjekje për të përmirësuar dhe rritur ndërtimin e kapaciteteve, të dyja qendrat janë duke prezantuar mësimin në distancë[55].

Policia

Siç konfirmohet në raport progresin e BE-së të vitit 2013 për BiH, agjencitë dhe bordet e krijuara sipas ligjeve të reformës policore janë ende duke konsoliduar funksionet e tyre[56].

Është krijuar një ekip i monitorimit midis agjenciveqëmbikëqyr zbatimin e sistemit elektronik të shkëmbimit të të dhënave për policinë dhe regjistrat e prokurorëve. Gjithsesi, duhet të trajtohen disa aspekte teknike të sistemit, duke përfshirë faktin se drejtoria për koordinimin e organeve të policisë ende nuk ka qasje në bazat e të dhënave të sistemit. Ka përfunduar një auditim nga Europol për mbrojtjen e të dhënave.

Agjencia për Mbështetjen Policore është bashkë-pozicionuar me drejtorinë për koordinimin e organeve të policisë dhe ka përfunduar Rregulloren për Standardizimin e Pajisjeve Policore.

Ndryshimet në Ligjet për Zyrtarët e policisë janë në proces miratimi në nivel shtetëror. Federata e BiH, kantonet dhe Rrethi Brckokanë ndërmarrë nisma për të harmonizuar ligjet e tyre përkatëse.

54 http://www.mpr.gov.ba/aktuelnosti/propisi/konsultacije /SRSP/BIH.pdf

55 .http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

56 Procesi i Zgjeruar i Reformës Policore në BiH, i cili filloi pas luftës civile, përfshiu krijimin e disa institucioneve të rëndësishme në nivel shtetëror, të tilla si policia kufitare e shtetit, Shërbimi për Çështjet e të Huajve i BiH pranë Ministrisë së Sigurisë, Agjencia e Mbrojtjes dhe e Hetimit Shtetëror (SIPA), Drejtoria për Koordinimin e Organeve Policore e BiH-së etj.

Amendimet lidhen me çështje teknike dhe operative, si për shembull përdorimi i armëve dhe kompetencave policore dhe përmirësimi i mbrojtjes së të dhënave personale[57].

Ligji i BiH-së[58] njeh krimin kibernetik si formë të sjelljes kriminale në të cilën shfrytëzimi i teknologjisë kompjuterike dhe sistemeve të informacionit përdoret si instrument ose objektiv që përmbush kushtet penale-ligjore me pasojat përkatëse.

Karakteristikat ose tiparet kryesore të krimit kibernetik:

- Sjellje e rrezikshme nga pikëpamja sociale, sjellje e paligjshme për të cilën ligji parashikon sanksione penale;
- Mënyra specifike dhe mjeti i kryerjes së veprave penale me ose nëpërmjet kompjuterëve;
- Objekti i posaçëm mbrojtjeje, siguria e të dhënave kompjuterike ose sistemit informative në tërësi ose e segmenteve të saj individuale; dhe
- Synimi i vetë autorit të veprës penale ose një tjetri që nxjerr përfitim nga ky dëm[59].

Vepra të lidhura me kompjuterët dhe Internetin [60]:

- Falsifikimi kompjuterik
- Mashtrimi kompjuterik
- Pornografia me fëmijët
- Shkelje e pronësisë intelektuale

Qasja e paautorizuar:

- Qasje e paqëllimshme jo-ligjore ndaj një sistemi kompjuterik
- Dëmtimi i sistemeve dhe të dhënave kompjuterike
- Cënimi i të dhënave konfidenciale

Keqpërdorimi i aparaturave:

- Veprimi i qëllimshëm i paautorizuar i prodhimit, shitjes, prokurimit ose shpërndarjes
- Aparaturat e qasjes/aksesit (duke përfshirë programet kompjuterike)
- Fjalëkalime kompjuterike
- KODI
- Tipe të tjera të informacionit të qasjes ndaj kryerjes së akteve të krimit kompjuterik

Përgjimi i paautorizuar i të dhënave:

- Përgjimi i paqëllimshëm i paligjshëm i të dhënave nga një sistem kompjuterik.
- Mbrojtja e privatësisë së transmetimit jopublik të të dhënave kompjuterike nga monitorimi dhe regjistrimi.

57 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf
58 Krivicni zakon Federacije Bosne i Hercegovine - Clan 393 do 398
59 http://www.fup.gov.ba/?p = 1697 – Administrata Policore Federale
60 http://www.rs.cest.gov.ba/

Ndërhyrja tek të dhënat:

- Dëmtimi i qëllimshëm i paautorizuar, fshirja, shkatërrimi, ndryshimi ose të dhënat e papërdorshme kompjuterike
- Vendosja e kodit dashakeq që përfaqëson një rrezik ndaj integritetit ose aftësisë për përdorimin e të dhënave dhe programeve
- Viruse që ndërhyjnë tek të dhënat

Përfundimisht, ekzistojnë masa ligjore për ndjekjen penale në këtë kontekst dhe të çështjeve të ngjashme të lidhura me korrupsionin e IT-së, pavarësisht nëse është vjedhje e të dhënave ose “dëgjim” i të dhënave, me qëllimin e ndarjes së informacionit “të dëgjuar” me palët e interesuara.

Sistemet e IT-së dhe procedurat e brendshme që lidhen me Sistemin e Menaxhimit të Dokumenteve, Arkivat, çështjet e prokurorëve dhe dokumentet tjera përkatëse dhe materialet, duke përfshirë personelin që punon në këto sisteme,i nënshtrohen inspektimit të rregullt nga autoriteti kompetent. Në disa institucione kjo përcaktohet me anë të procedurave të brendshme, në varësi tëprofilittë institucionit. Në këtë rast, hapi kryesor është zbatimi i ISO/IEC 27001: 2005, për të garantuar se siguria e të dhënave është e kënaqshme.

Çfarë duhet bërë

Të vazhdohet me zbatimin e standardeve më të rëndësishme dhe për të përdorur shërbimin e auditimit rregullisht sipas rregullave dhe legjislacionit të BE-së, me konsideratë të veçantë ndaj Standardeve ISO 9001 Menaxhimi i Cilësisë ISO/27001: 2005 dhe ISO/90001: 2008.

Të vazhdohet me kontrolle sigurie të punonjësve të zbatuara nga autoritetet kompetente, të cilat garantojnë shmangien e shkeljeve të sigurisë së IT-së dhe gjithashtu të mblidhen të dhëna personale të të gjithë personelit të kontraktuar dhe të ardhshëm, në mënyrë që të ndërtohet një profil shoqëror për përdorim në të ardhmen.

Lufta kundër krimit të organizuar dhe terrorizmit

Të metat në mbledhjen sistematike, analizën dhe përdorimin e zbulimit nga agjencitë e zbatimit të ligjit pengojnë shënjestrimin strategjik të grupeve dhe aktiviteteve të krimit të organizuar. Nuk ka shkëmbim sistematik të zbulimit midis agjencive në lidhje me zbatimin e ligjit për planifikim të përbashkët operacional.

Janë përgatitur ndryshimet në Kodin Shtetëror të Procedurës Penale për shpërndarje më efektive të Masave të Posaçme Hetimore por pritet ende që të miratohen.

Në fushën e bashkëpunimit gjyqësor në çështjet penale, përgatitjet për nënshkrimin e një marrëveshjeje bashkëpunimi me Eurojust-in janë në një fazë të hershme por kanë

përparuar. Vlerësimi i legjislacionit për mbrojtjen e të dhënave ka përfunduar. Ndryshimet në Ligjin për Mbrojtjen e Informacionit të Klasifikuar që sjellin ligjin në përputhje me standardet përkatëse të BE-së dhe që parashikojnë zbatimin e marrëveshjeve dypalëshe të sigurisë, mbeten për t'u miratuar.

Krimi kibernetik

Progres Raporti i vitit 2013 i Komisionit Europian për Bosnjën dhe Hercegovinën deklaron mungesën e strategjisë dhe institucioneve për luftën kundër krimit dhe kërcënimeve kibernetike:

"Bosnja dhe Hercegovina nuk kanë as strategji, as institucione funksionale për të trajtuar çështjen e krimit kibernetik dhe kërcënimeve të sigurisë kibernetike. Një plan veprimi për të ngritur një Ekip të Gatshëm/për Reagim në Raste Emergjente Kompjuterike për Bosnjën dhe Hercegovinën (CERT) është në pritje të miratimit nga Këshilli i Ministrave. Janë ndërmarrë aktivitete për të krijuar CERT-in. Denoncimet e krimeve të përgatitura nga agjencitë e zbatimit të ligjit në Bosnjë dhe Hercegovinë nuk i referohen krimeve kibernetike. Ato nuk japin të dhëna të sakta mbi numrin e rasteve, hetimet apo të dyshuarve. Mjekësia Ligjore dixhitale dhe mjete të tjera teknike të luftës kundër krimit kibernetik në nivel kombëtar dhe ndërkombëtar janë të kufizuara dhe të pamjaftueshme. Drejtoria për Koordinimin e Organeve Policore është caktuar si pikë kontakti për 24 orë në 7 ditë të javës, duke marrë parasysh Konventën e Krimit Kibernetik (Konventa e Budapestit) por mungojnë kapacitetet e kërkuara"[61].

MASA TË TJERA

Shkëmbimi i të dhënave midis organeve publike

Me projektin "Mbështetja e gjyqësorit të Bosnjës dhe Hercegovinës" (IPA 2009) dhe projektin IPA "Mbështetja ndaj reformës policore", i cili filloi në vitin 2013, me njëproces të mirë-strukturuar zbatimi, dhe sipas marrëveshjes që themeloi një sistem për shkëmbimin në formë elektronike të të dhënave midis autoriteteve policore dhe prokurorëve, - të lidhur midis HJPC-së, Ministrisë së Sigurisë të BiH, Policisë Kufitare, Agjencisë Shtetërore për Mbrojtjen dhe Hetimin (SIPA) dhe me ministritë e brendshme - HJCP kishte filluar aktivitete që sipas pritshmërive do të çonin në një gjenerim të ri të shkëmbimit të të dhënave në BiH. Gjatë këtij procesi, të gjitha standardet e lartpërmendura duhet të zbatohen dhe sistemet e të dhënave duhet të "përditësohen", me qëllim që të shmangin shembuj të korrupsionit të përmendur në këtë studim. Për këtë qëllim në këtë sistem do të zbatohen instrumentet dhe garancitë, të cilat përfshijnë: sisteme mbrojtëse, Sistemet e Ndërhyrjes, Zbulimit dhe Parandalimit (IDS), Testimi për Depërtimin dhe Identifikimi i Pikave të Dobëta, procedurat e transmetimit tëtë dhënave sensitive, rregullat dhe procedurat për Lidhjet e Jashtme të Sistemit, mjetet kundër viruseve dhe pro mbrojtjes, kontrollet e aksesit në distancë, kontrollet dhe procedurat për hyrjen dhe daljen në ambiente, kopjet rezervë tëtë dhënave për vendndodhjen në distancë që kombinojnë mbrojtjen e fortë të fjalëkalimit dhe sigurinë fizike, dhe arsimin e përhershëm të punonjësve për teknologjinë e informacionit.

Agjencia për Dokumentet e Identifikimit, Regjistrat dhe Shkëmbimin e të Dhënave të BiH, ish Sistemi i Mbrojtjes së Identifikimit të Qytetarëve (CIPS)[62] është shembull shumë i mirë i zbatimit të sigurisë dhe garancisë. Megjithatë, ndërsa janë një Agjenci e organizuar shumë mirë në nivel shtetëror, për fat të keq në nivel autoriteti vendor ekziston shpërdorim apo abuzim.

Mësimet e nxjerra nga keqpërdorimi i sistemit elektronik të projektit CIPS

Ata janë duke zbatuar standardet ISO/27001:2005 dhe ISO/90001:2008 në periudhën 2012- 2015, me auditime të planifikuara[63]. Sistemi i tyre i menaxhimit të dokumenteve, Regjistri i të Dhënave të Gjendjes Civile dhe mjedisi i brendshëm Oracle, i cili përdoret për ruajtjen e të dhënave tëtë gjitha institucioneve dhe agjencive shtetërore, është mjaft i sigurt. Në këtë rast, problemi i përshkruar në kapitullin 1është se autoritetet kompetente (Federata e BiH-së nga Ministritë e Brendshme të kantoneve, Ministria e Brendshme e Republikës Srpska dhe nga autoriteti kompetent që vepron funksionalisht si institucion shtetëror në Rrethin Brcko) me procedura të rrepta pune me të dhënat dhe të njëjtën kohë që ndryshojnë, shtojnë, fshijnë dhe përditësojnë të dhënat personale të qytetarëve.

Siç përcaktohet me ligj, autoritetet kompetente janë pronarë të të dhënave të tyre dhe roli i IDDEEA-s në këtë proces është vetëm që të ruajë dhe sigurojë të dhënat, dhe të zbatojë të gjitha garancitë e njohura dhe praktikat e mira të sigurisë[64] . Ndërsa ky është një fakt, ne duhet të ndajmë përgjegjësinë për këto raste midis administratave policore në BiH dhe autoriteteve kompetente me çështje të tjera, nëse ka. Kjo do të thotë se standardet, procedurat e tyre dhe mënyra e përgjithshme e trajtimit të këtyre problemeve nuk janë të pranueshme.

IDDEEA ka ofruar garanci të plotë në të gjitha nivelet e mbrojtjes të të dhënave për agjencitë policore kompetente dhe autoritetet kompetente në Bosnjë dhe Hercegovinë. Si rrjedhojë, korrupsioni dhe abuzimi me teknologjinë e informacionit duhet të kërkohet në nivel të autoritetit kompetent, ku shteti duhet të garantojë dhe përmirësojë sigurinë e informacionit.

61 http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/ba_rapport_2013.pdf

62 www.iddeea.gov.ba
63 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemi d=214&lang=en
64 http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=415&Itemi d=214&lang=en

IDDEEA realizoi nënshkrime dixhitale për të gjitha kanalet e komunikimit brenda Agjencisë dhe gjithashtu për përdorim të jashtëm me komunikim tek autoritetet kompetente.

Megjithatë, çka mungon është një Ekip Gatishmërie/për Reagimin ndaj Emergjencave Kompjuterike[65] (CERT). Megjithëse parashikohet që do të përgatitet një plan veprimi për një CERT[66], ky plan nuk është krijuar ende.

Nënshkrimi Elektronik

Përshkrimi teknik i Infrastrukturës Kyçe Publike (PKI)[67] duhet të përmirësojë nivelin e sigurisë për shkëmbimin e të dhënave në nivel të komponentit teknik parësor në nivel shtetëror. Kjo mund të jetë ose infrastrukturë qendrore me autoritet të vetëm për lëshimin e çertifikatave dhe organeve të varësisë që lëshojnë çertifikata për nënshkrime elektronike, ose infrastrukturë e pavarur në nivel ndërveprimi.

Në Bosnjë dhe Hercegovinë nuk ka PKI për shoqëritë dhe individët në nivel shtetëror. Megjithatë, ka një numër të pavarur përdoruesish të PKI-së, veçanërisht brenda sistemit elektronik bankar dhe pjesërisht në fushën e qeverisjes elektronike, të cilët veprojnë në sistemet e mbyllura. Kështu, problemi teknik nuk bazohet aq gjerësisht në mungesën e PKI-së në nivel shtetëror por që të integrohen dhe t'u bashkohen sistemeve ekzistuese të PKI-së dhe informacionit. Lidhja me PKI të ndryshme do të lehtësonte procesin e biznesit dhe punës në administratën publike.

Siguria do të forcohet ndërsa të gjithë pjesëmarrësit në shkëmbimin elektronik tëtë dhënave ose qytetarët e zakonshëm kanë një identitet për këtë sistem. Ky hap minimizon mundësinë e abuzimit dhe mundëson monitorimin e kujdesshëm të veprimeve të individëve. Të gjitha sistemet që integrohen me PKI-në dhe në fakt krijojnë një sistem të gjerë, ulin ndjeshëm mundësinë e abuzimit.

KUADRI LIGJOR

Direktiva 1999/93/KE për kuadrin e Komunitetit për nënshkrimet elektronike

Kjo Direktivë krijon një kuadër ligjor për nënshkrimet elektronike dhe çertifikimin e shërbimeve në nivel evropian. Qëllimi është lehtësimi i përdorimit të nënshkrimeve elektronike dhe t'i ndihmojë ato që të bëhen të njohura ligjërisht brenda Shteteve Anëtare.

65 http://www.msb.gov.ba/docs/Strategija_za_CERT.doc
66 http://www.us-cert.gov/
67 http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

Vendimi i Komisionit 2003/511/KE i 14 korrikut 2003 për botimin e numrave referues të standardeve të njohura përgjithësisht për produktet e nënshkrimeve elektronike në përputhje me Direktivën 1999/93/KE

Bosnja dhe Hercegovina, me këtë vendim të Komisionit të Bashkimit Europian, bazohet në tre standardet e produkteve të pranuara gjerësisht për nënshkrimet elektronike, të cilat presupozojnë respektimin e nënshkrimit elektronik të kualifikuar.

Vendimi i Komisionit 2000/709/KE - nëntor 2000

Në pajtim me nenin 3 (4) të Direktivës 1999/93/KE të Parlamentit Europian dhe të Këshillit për një kuadër Komunitar për nënshkrimin elektronik, ky vendim paraqet kriteret që Shtetet Anëtare duhet të kenë parasysh gjatë përcaktimit të shtetit të organit që do të mbështesë instrumentin e vlerësimit të pajtueshmërisë për krijimin e një nënshkrimi të sigurt.

Kuadri ligjor i BiH-së

Në nivel shtetëror (BiH), aktualisht janë në fuqi aktet e mëposhtme ligjore:

- Ligji për Nënshkrimet Elektronike ("Fletorja Zyrtare e BiH", nr. 91/06)
- Ligji për Operacionet e Biznesit dhe Operacionet Ligjore Elektronike ("Fletorja Zyrtare e BiH", nr. 88/07)
- Ligji për Procedurën Administrative ("Fletorja Zyrtare" nr.: 29/02, 12/04, 88/07, 93/09)
- Vendimi mbi bazën e përdorimit të nënshkrimeve elektronike dhe dhënien e verifikimit ("Fletorja Zyrtare e BiH", nr. 21/09)
- Vendimi mbi tregtinë elektronike dhe qeverisjen elektronike ("Fletorja Zyrtare" nr. 07/10)
- Vendimi për operacionet zyrtare të ministrive, departamenteve, institucioneve dhe organeve të tjera të Këshillit të Ministrave ("Fletorja Zyrtare e BiH" nr. 21/01, 29/03)
- Udhëzime mbi përgatitjen dhe mirëmbajtjen e faqes zyrtare të Internetit të institucionit të BiH (Fletorja Zyrtare nr. 21/09)
- Ligji për mbrojtjen e personave që raportojnë korrupsionin në institucionet e Bosnjës dhe Hercegovinës ("Fletorja Zyrtare e Bosnjës dhe Hercegovinës" nr. 100/13)
- Ligji për agjencinë për parandalimin e korrupsionit dhe koordinimin e luftës kundër korrupsionit ("Fletorja Zyrtare e Bosnjës dhe Hercegovinës", dhjetor 2009).

Përveç kësaj, aktualisht janë duke u përgatitur aktet e mëposhtme ligjore:

- Rregullorja e organizimit të brendshëm të Ministrisë së Komunikacionit dhe Transportit (krijimi i Zyrës së Mbikëqyrjes dhe Akreditimit)
- Këshilli i Lartë i Gjyqësorit dhe i Prokurorisë (HJPC) i rekomandoi autoriteteve ekzekutive pranë BiH që Ministria e Transportit dhe Komunikacionit duhet të miratojë aktet përkatëse nënligjore dhe të ndërtojë kapacitete institucionale për të mundësuar zbatimin e plotë të Ligjit për Nënshkrimin Elektronik dhe Ligjit për Biznesin Elektronik

në sistemin e informacionit gjyqësor, i cili reflektohet kryesisht në mundësinë e depozitimit të dokumenteve pranë gjykatës në formë elektronike, si dhe dhënien e vendimeve gjyqësore në mënyrë elektronike (verifikuar nga çertifikata e kualifikuar dixhitale)[68].

Prokurimi Publik

Ligji për Prokurimin Publik për Bosnjën dhe Hercegovinën [69] në mënyrë unike përfshinte të gjitha autoritetet kontraktuese në bazë të Direktivës së BE-së 17/2004 dhe Direktivës 18/2004. Rregullat specifike të BE-së për prokurimin publik janë përpunuar nëpërmjet një sërë direktivash të detajuara që specifikojnë kërkesat gjithëpërfshirëse për rregullimin e procedurave të prokurimit publik. Në Bosnjë dhe Hercegovinë ka rregulla të pamjaftueshme të veçanta që përcaktojnë këtë fushë në përputhje me rregulloret e BE-së.

Zgjidhja për të trajtuar të metat në sistemin e prokurimit publik mund të jetë lejimi i një organi të vetëm për të zbatuar procesin e prokurimit për të gjitha autoritetet kompetente. Ky organ do të zotërojë, nëse ata kryejnë një rishikim të IT-së dhe korrupsionit, një softuer unik dhe të centralizuar të projektuar në pajtim me Ligjin mbi Prokurimin Publik të Bosnjës dhe Hercegovinës, i cili do të trajtojë nevojat e të gjitha niveleve të qeverisë që e lejojnë atë të realizojë të gjithë prokurimin publik.
Natyrisht, një kusht paraprak do të ishte prezantimi i standardeve dhe garantimi i njohurive rreth tregut të punonjësve në lidhje me informacionin e përditësuar dhe kontaktin me shitësit. Kjo nevojitet për të garantuar se vetëm mallrat dhe shërbimet e nevojshme blihen dhe se këto produkte janë më të mirat në dispozicion.

68 http://www.hjpc.ba/intro/gizvjestaj/?cid=5889,2,133http://www.ohr.int/ohr-dept/le- gal/laws-of-bih/police.asp
69 https://www.parlament.ba/sadrzaj/zakonodavstvo/usvojeni/default. aspx?id=46717&langTag=bs-BA&pril=b

Kroacia

Nga Zorislav Petrovic dhe Ivana Andrijasevic

Kuadri kryesor legjislativ për sigurinë e informacionit

Kuadri legjislativ për garantimin e sigurisë së informacionit në sistemet e informacionit të administratës publike në Republikën e Kroacisë bazohet në ligjet e mëposhtme më të rëndësishme dhe aktet nënligjore: Ligji për Sigurinë e Informacionit; Ligji për Fshehtësinë e të Dhënave; Ligji për Mbrojtjen e të Dhënave Personale; Ligji për Sigurinë dhe Sistemin e Zbulimit; Ligji për Dokumentet Elektronike; Ligji për Nënshkrimin Elektronik; Ligji për Sigurimin e Verifikimit; Rregullorja mbi Masat e Sigurisë së Informacionit; Rregullorja për Përmbajtjen, Formën, Plotësimin dhe Trajtimin e Pyetësorit të Verifikimit të Sigurisë; dhe Urdhëresa mbi Kriteret për Krijimin e Pozicioneve për Këshilltarë të Sigurisë së Informacionit.

Ligji për Sigurinë e Informacionit (Fletorja Zyrtare, nr. 79/07) përcakton nocionin e sigurisë së informacionit; informacionin mbi masat dhe standardet e sigurisë; fushat e sigurisë së informacionit; dhe autoritetet kompetente për miratimin, zbatimin dhe mbikëqyrjen e masave dhe standardeve të sigurisë të informacionit. Ky ligj zbatohet për autoritetet shtetërore; organet lokale dhe rajonale të vetëqeverisjes dhe personat juridikë me autoritet publik të cilët, brenda fushës së tyre të punës, përdorin të dhëna të klasifikuara dhe të paklasifikuara; si dhe personat juridikë dhe fizikë që fitojnë qasje ose trajtojnë të dhënat e klasifikuara dhe të paklasifikuara.

Ligji për Fshehtësinë e të Dhënave (Fletorja Zyrtare nr. 79/07, 86/12) përcakton nocionin e informacioneve të klasifikuara dhe të paklasifikuara; nivelet e fshehtësisë; procedurën e klasifikimit dhe deklasifikimit; qasjen në informacionin e klasifikuar dhe të paklasifikuar; mbrojtjen e informacionit të klasifikuar dhe të paklasifikuar; dhe mbikëqyrjen mbi zbatimin e këtij Akti. Ai zbatohet edhe për organet shtetërore; organet e vetëqeverisjes vendore dhe rajonale; personat juridikë me autoritet publik; dhe personat juridikë dhe fizikë që në përputhje me këtë Akt, fitojnë qasje ose trajtojnë informacionin e klasifikuar dhe të paklasifikuar.

Ligji për Mbrojtjen e të Dhënave Personale (Fletorja Zyrtare nr. 103/03, 118/06, 41/08, 130/11, 106/12) rregullon mbrojtjen e të dhënave personale në lidhje me personat fizikë dhe mbikëqyrjen e mbledhjes, përpunimit dhe përdorimit tëtë dhënave personale në Republikën e Kroacisë. Qëllimi i tij është mbrojtja e privatësisë së individëve, si dhe të drejtave të tjera të njeriut dhe të drejtave themelore në mbledhjen, përpunimin dhe përdorimin e të dhënave personale.

Ligji për Sistemin e Sigurisë dhe Zbulimit i Republikës së Kroacisë (Fletorja Zyrtare nr. 85/08, 86/12) përcakton, për qëllimin e mbledhjes, analizimit, përpunimit dhe vlerësimit sistematik tëinformacionit që lidhet me sigurinë kombëtare, me synimin e zbulimit dhe

parandalimit të aktiviteteve, nga individë ose grupe, të drejtuar kundër suksesit, pavarësisë, integritetit dhe sovranitetit të Republikës së Kroacisë, duke synuar përmbysjen e dhunshme të strukturave të autoritetit shtetëror që kërcënojnë të shkelin të drejtat e njeriut dhe liritë themelore të përcaktuara nga Kushtetuta dhe legjislacioni i Republikës së Kroacisë për të rrezikuar themelet e sistemit ekonomik të Republikës së Kroacisë të kërkuar për marrjen e vendimeve të lidhura me arritjen e suksesshme të interesave kombëtare në fushën e sigurisë kombëtare, specifikisht mbrojtjen e dy agjencive të sigurisë-zbulimit: Agjencia e Sigurimit dhe Zbulimit (SOA) dhe Agjencia e Sigurisë Ushtarake dhe Zbulimit (VSOA).

Akti për Dokumentet Elektronike (Fletorja Zyrtare nr. 150/05) rregullon të drejtën e personave fizikë dhe juridikë për të përdorur një dokument elektronik në të gjitha operacionet dhe aktivitetet e biznesit dhe në procedurat e kryera para autoriteteve publike në të cilat pajisjet dhe programet elektronike mund të zbatohenpër krijimin, transferimin, magazinimin dhe ruajtjen e informacionit në formë elektronike, vlefshmërinë ligjore të një dokumenti elektronik, si dhe përdorimin dhe trafikun e dokumenteve elektronike.

Ligji për Nënshkrimet Elektronike (Fletorja Zyrtare nr. 10/02, 80/08, 30/14) rregullon të drejtën e personave fizikë dhe juridike për të përdorur nënshkrime elektronike në veprimet administrative, tregtare dhe veprime të tjera dhe të drejtat, detyrimet dhe përgjegjësitë e personave fizikë dhe juridikë të shoqëruara me ofrimin e shërbimeve për vërtetimin e nënshkrimeve elektronike.

Ligji për Sigurimin e Verifikimeve (Fletorja Zyrtare nr. 85/08, 86/12) përcakton nocionin, llojet dhe shkallën e verifikimit të sigurisë, pengesat ndaj sigurisë dhe procedurat për kryerjen e verifikimit të sigurisë. Sipas këtij Akti, verifikimi është procedura me anë tëtë cilës autoritetet kompetente konstatojnë ekzistencën e pengesave ndaj sigurisë për personat fizikë dhe juridikë.

Rregullorja për Masat e Sigurisë për Informacionin (Fletorja Zyrtare nr. 46/08) parashikon masat e sigurisë së informacionit të përcaktuara për trajtimin e informacionit të klasifikuar dhe të paklasifikuar. Ajo zbatohet për autoritetet shtetërore; organet e vetëqeverisjes vendore dhe rajonale; dhe personat juridikë që me autoritete publike në fushën e tyre përkatëse të veprimit, përdorin informacion të klasifikuar dhe të paklasifikuar; si dhe personat fizikë dhe juridikë që fitojnë akses ose trajtojnë informacionin e klasifikuar dhe të paklasifikuar.

Rregullorja për Përmbajtjen, Formën, Plotësimin dhe Trajtimin e Pyetësorit të Verifikimit të Sigurisë (Fletorja Zyrtare nr.114/08) përcakton përmbajtjen, formën, plotësimin dhe trajtimin e Pyetësorit të Verifikimit të Sigurisë për individët dhe personat juridikë.

Urdhëresa mbi Kriteret për Përcaktimin e Pozicioneve të Këshilltarit të Sigurisë së Informacionit (Fletorja Zyrtare nr. 100/08, 30/11) vendos kriteret për përcaktimin e pozicioneve të këshilltarit të sigurisë së informacionit. Përveç rregulloreve të lartpërmendura, ka një numër të madh ligjesh dhe aktesh nënligjore që trajtojnë pjesërisht vetëm çështjen e sigurisë së informacionit, si për shembull Akti mbi Tregtinë Elektronike; Kodi Penal, Akti mbi Materialet e Arkivave, Akti mbi Sigurinë dhe Mbrojtjen etj. Së fundi, është e rëndësishme të vërejmë se si anëtare e NATO-s dhe BE-së, Kroacia harmonizon rregulloret e saj në fushën e sigurisë së informacionit me shtete të tjera anëtare të NATO-s dhe BE-së.

Autoritetet qendrore shtetërore kompetente për sigurinë e informacionit

Autoritetet qendrore shtetërore kompetente për sigurinë e informacionit në Kroaci janë:

- **Zyra e Këshillit Kombëtar të Sigurisë:** autoriteti qendror shtetëror përgjegjës për sigurinë e informacionit koordinon dhe harmonizon miratimin dhe zbatimin e masave dhe standardeve të sigurisë së informacionit në Republikën e Kroacisë dhe për shkëmbimin e informacionit të klasifikuar dhe të paklasifikuar midis Republikës së Kroacisë dhe vendeve dhe organizatave të huaja (Neni 14 i Aktit të Sigurisë së Informacionit);
- **Byroja e Sigurisë së Sistemeve të Informacionit:** autoriteti qendror shtetëror për fushat teknike të sigurisë së sistemeve të informacionit në organet dhe personat juridikë. Specifikisht, kjo do të thotë: standardet e sistemeve të sigurisë së informacionit; akreditimet e sigurisë së sistemeve të informacionit; menaxhimi i materialeve të koduara të përdorura në shkëmbimin e informacionit të klasifikuar; dhe koordinimi i parandalimit dhe reagimit ndaj kërcënimeve të sigurisë ndaj sigurisë së sistemeve të informacionit (Neni 17 i Aktit të Sigurisë së Informacionit); dhe
- **CERT kombëtare:** autoriteti kombëtar përgjegjës për parandalimin dhe mbrojtjen kundër kërcënimeve kompjuterike ndaj sistemeve të informacionit publik në Republikën e Kroacisë që veprojnë brenda Rrjetit Kërkimor dhe Akademik kroat (CARNet) – elementi kryesor i internetit për sektorët htetërore në Kroaci. Detyra e tij kryesore është trajtimi i incidenteve në internet; dmth ruajtja e sigurisë së informacionit në Kroaci. CERT kombëtare realizon masa proaktive dhe reaguese brenda kuadrit të aktiviteteve të saj për të parandaluar ose zbutur dëmin e mundshëm. Përdoruesit e CERT kombëtare janë të gjithë përdorues të Internetit në Republikën e Kroacisë dhe ofrues të shërbimeve të drejtimit të serverëve, si dhe ofrues të shërbimit të Internetit (ISP)[70].

Siguria e sistemit të informacionit në përgjithësi

Akti i Sigurisë së Informacionit përcakton pesë fusha të informacionit për sigurinë për të cilat përcaktohen standardet dhe masat e sigurisë së informacionit: kontrolli i sigurisë; siguria fizike; siguria e informacionit; siguria e sistemit të informacionit; dhe siguria e bashkëpunimit të biznesit.

Fusha e sigurisë së informacionit që lidhet me këtë studim është siguria e sistemit të informacionit. Sipas paragrafit 1 të Nenit 12 të Ligjit për Sigurinë e Informacionit, siguria

70 http://www.carnet.hr/ncd

e sistemit të informacionit “është fusha e sigurisë së informacionit brenda të cilës masat për sigurinë e informacionit dhe standardet përcaktohen për informacionin e klasifikuar dhe të paklasifikuar që përpunohet, ruhet ose transmetohet brenda sistemit informativ dhe mbrojtja e integritetit dhe disponueshmërisë së sistemit të informacionit në procesin e planifikimit, projektimit, kryerjes, përdorimit dhe ndërprerjes së punëstë sistemit informativ’’. Për më tepër, sipas të njëjtit Nen, “akreditimi i sigurisë së sistemit informativ kryhet për sistemin informativ ku përdoren të dhënat e klasifikuara si KONFIDENCIALE, SEKRETE dhe TEPËR SEKRETE. Personat që marrin pjesë nëproces të përmendur në paragrafin 1 të këtij Neni kanë Certifikatë me nivel TEPËR SEKRET ose një nivel më të lartë sesa niveli më i lartë i informacionit të klasifikuar që përpunohet, ruhet ose transmetohet në sistemet informative sipas kompetencës së tyre. Masat e mbrojtjes fizike të ambienteve ku ndodhen sistemet e informacionit duhet të merren në përputhje me nivelin më të lartë të informacioneve të klasifikuara që përpunohen, ruhen ose transmetohen në ambientet e lartpërmendura”. Së fundi, “autoritetet qendrore shtetërore kompetente për sigurinë e informacionit formojnë regjistrin e pajisjeve dhe makinerive të vërtetuara të përdorura në sistemin informativ të nivelit KONFIDENCIAL, SEKRET dhe TEPËR SEKRET. Regjistri i pajisjeve dhe makinerive tëçertifikuara formohet mbi bazën e marrjes në dorëzim të regjistrave përkatës të organizatave ndërkombëtare ose nga vetë procesi çertifikues në përputhje me standardet ndërkombëtare’’.

Masat e sigurisë së informacionit për fushën e sigurisë së sistemit të informacionit, siç përcaktohen sipas Rregullores për Masat e Sigurisë së Informacionit, janë:

- masat për mbrojtjen e sistemit të informacionit (mbrojtja e harduerit, softuerit dhe mediave për ruajtjen e të dhënave, menaxhimi i konfigurimit të sistemit dhe aksesi i përdoruesve, kontrolli i ndërlidhjes së sistemeve etj);
- ndërgjegjësimi për sigurinë (përcaktimi i rregullave të sigurisë për punonjësit dhe edukimi mbi sigurinë); dhe
- planifikimi i procedurave për situata emergjente (zhvillimi i procedurave për t’u ndjekur në rast të një incidenti; dhe menaxhimi i vazhdimësisë së një biznesi).

Siguria e sistemit të informacionit realizohet në të gjithë ciklin jetësor të sistemit informativ për sistemet e klasifikuara (nëpërmjet akreditimit të sigurisë) dhe të paklasifikuara (përshtatje ndaj standardeve HRN ISO/IEC 27001 dhe HRN ISO/IEC 17799)[71].

71 Faqja zyrtare e internetit e Byrosë së Sigurisë së Sistemit Informativ, e disponueshme në adresën: https://www.zsis.hr/de- fault.aspx?id=34

Shembuj të rasteve të masave mbrojtëse të teknologjisë së informacionit në Kroaci

Kroacia, rasti 1: Telefonata e mjekut për vota

Ky është rasti i një mjeku që nxjerr të dhëna nga një sistem spitalor. Sipas informacionit nga Regjistri Qendror i vënë publikisht në dispozicion me informacione në sistemin e depozitimit të dhënave personale të mbajtur nga Agjencia për Mbrojtjen e të Dhënave Personale, mbrojtja e të dhënave personale brenda një regjistri tëtë dhënave personale të një pacienti (hrv. Zbirka o osobnimpodacimapacijenata), e cila është pjesërisht në formë elektronike dhe pjesërisht në formë të printuar, garantohet nga masat e mëposhtme mbrojtësepër mbylljen/ruajtjen e dokumentacionit në raftet e librave, një sistem monitorimi video, emër përdoruesi dhe regjistrimi, dhe një sistem për mbrojtjen kundër zjarrit. Në këtë rast të veçantë, problemi kryesor ishtembrojtja e dobët e të dhënave, duke përfshirë faktin se shumë persona kishin akses tek baza e të dhënave. Sipas gjasave, nuk ka asnjë funksion në sistemin e bazave tëtë dhënave që regjistronte se cili ishte personi i fundit që shkarkonte të dhënat. Si rrjedhojë, është e pamundur të zbulohet se kush e kishte shkarkuar informacionin për letrat e kandidatit për kryetar bashkie.

Kroacia, rasti 2: Të dhënat konfidenciale të radiotelevizionit kroat në tregun e zi

Sipas Ligjit për Radio-Televizionin kroat, çdo person fizik dhe juridik në Kroaci i cili zotëron një televizor ose radio, është i detyruar të paguajë një tarifë licence. HRT mban dhe administron regjistrin e paguesve të licencës mujore të HRT-së në Republikën e Kroacisë. Ky regjistër nuk është në dispozicion të publikut. Meqë përmban të dhënat personale të përdoruesve, të tilla si emri dhe mbiemri, adresa, numri personal i identifikimit (OIB) etj, menaxhimi dhe përdorimi i tij mbrohen nga dispozitat e legjislacionit për sigurinë e të dhënave personale. Sipas informacioneve nga Regjistri Qendror në dispozicion të publikut me të dhënat mbi sistemet e plotësimit tëtë dhënave personale në Agjencinë e Mbrojtjes të të Dhënave Personale, regjistri i HRT-së është në server tek i cili qasja fizike sigurohet ekskluzivisht për personat e autorizuar. Përdoruesit e autorizuar përdorin të dhënat nga regjistri nëpërmjet aplikimit me emrin e përdoruesit dhe fjalëkalimet ose çertifikatën e tyre. Aplikimi është në dispozicion nga rrjeti lokal dhe interneti, duke përdorur kanale të dhënash të mbrojtura. Së fundi, kopjet e sigurisë janë të sigurta nësallën e serverit.

Në këtë rast, IT është keqpërdorur për kopjimin e qëllimshëm dhe shitjen e paligjshme tëtë dhënave nga një punonjës i HRT-së, i cili ose ka pasur akses në regjistër, ose ka njohur dikë me akses në regjistër. Si rezultat, të gjitha garancitë e lartpërmendura teknike janë shkelur, si dhe dispozitat e rregullave të përgjithshme për punën dhe modalitetet e HRT-së sipas të cilave punonjësit e HRT-së duhet të punojnë në përputhje me standardet

më të larta të biznesit dhe standardet bazë etike, në bazë të disa vlerave, duke përfshirë fshehtësinë dhe mbrojtjen e të dhënave në pajtim me legjislacionin përkatës dhe rregullat e përgjithshme. Është e qartë se këto standarde nuk janë zbatuar.

Kroacia, rasti 3: Në kërkim të veteranëve

Ky është një shembull i shpërdorimit të detyrës. Me sa duket, dikush nga një Zyrë për Mbrojtjen mori të dhëna, i publikoi ose ia dha apo edhe ia shiti dikujt tjetër që më pas i publikoi. Mund të ketë shumë motive të ndryshme për publikimin e regjistrit, të cilat variojnë nga mosmarrëveshjet politike në motive fisnike të tilla si përpjekja për të rritur transparencën. Megjithatë, nuk ka dyshim se arsyeja kryesore pse ndodhi kjo ishte mungesa e protokolleve të sigurisë minimale të përfshira në procedurën e trajtimit tëtë dhënave të shpërndara tek Zyrat për Mbrojtje në qytete të ndryshme kroate.

Kroacia, rasti 4: Me një ndihmë të vogël të nëpunësve civilë, 68 pasaporta kroate iu shitën kriminelëve; rasti 5: Oficeri i policisë u kap ndërsa fuste të dhëna të rreme tek sistemi i informacionit të policisë; rasti 6: Oficerë policie që fshijnë kundravajtjet në trafik dhe zbulojnë të dhëna konfidenciale (bile ata pranuan si rryshfet edhe mish qingji të pjekur dhe 20 litra verë!) dhe rasti 7: I kapur rastësisht për zbulim të të dhënave konfidenciale përautomjetet dhe pronarët e tyre!

“”Fshehtësia, integriteti, disponueshmëria e vazhdueshme dhe kontrolli i të dhënave dhe informacionit ngapërdorimi i sistemit informativ të MUP-it është zbatuar nëpërmjet disa masave dhe procedurave të programeve, sistemeve dhe organizative, si dhe ndarjen e përgjegjësisë dhe autorizimit. Të gjithë përdoruesit e sistemit informativ të MUP-it janë të detyruar të realizojnë mbrojtjen e të dhënave, siç parashikohet nga Urdhëresa për mbrojtjen e sistemit informativ të MUP-it bazuar në përpunimin e të dhënave elektronike, Urdhëresën për sigurinë dhe mbrojtjen e të dhënave zyrtare të MUP-it, si dhe udhëzimet dhe direktivat e tjera të brendshme që drejtojnë aktivitete për mbrojtjen e të dhënave të sistemit informativ të MUP-it. Përgjegjësitë e pozicionit të punës të punonjësit përcaktojnë nivelin e aksesueshmërisë së të dhënave.”

Çështje të tilla si këto mund të parandaloheshin nga monitorimi i trafikut tëtë dhënave dhe aksesi i punonjësve tek sistemi i të dhënave, si dhe masat e ndërgjegjësimit dhe trajnimit

për rreziqet e korrupsionit të IT-së dhe garancitë. Nëpunësit civilë duhet të jenë në dijeni të rëndësisë për mbajtjen të fshehtë të fjalëkalimeve të tyre, si dhe për faktin se çdo akses tek baza e të dhënave do të monitorohet. Lidhja më e dobët e procesit të garancive është individi me të gjitha të metat dhe virtytet e tij/të saj.

Kroacia, rasti 8: Çdo vit 2 milionë Euro zhduken nga kabinat e taksave rrugore

Në këtë rast, Autocesta Rijeka-Zagreb d.d. kishte përdorur auditime të sistemit të brendshëm të IT-së si garanci kundër korrupsionit të IT-së. Si monitorim apo ndjekje e shfajësimit simbolik të gjyqtarëve, me qëllim parandalimin e rasteve të ngjashme në të ardhmen dhe si një masë garancie e IT-së, menaxhimi i HAC-it vendosi të instalonte kamera që monitoronin punën e punonjësve nëkabinat e taksave rrugore. Këto kamera nuk do të fokusojnë fytyrat e punonjësve, as zërat e tyre por vetëm hapësirën e tyre të punës dhe procesin e pagimit/mbledhjes së tarifës rrugore. Shuma totale e këtij investimi ishte 354.000 Euro.

Kroacia, rasti 9: Policë të korruptuar; oficerë policie që i dhanë të dhëna konfidenciale kontrabandistëve të armëve; dhe rasti 10: Oficeri i policisë i dënuar me një vit burgim sepse lejoi mikun e tij të peshkonte në mënyrë të paligjshme

Këto dy raste tregojnë se edhe garancitë e përcaktuara saktësisht kundër korrupsionit në IT mund të dështojnë. Sipas legjislacionit përkatës mbi sigurinë e informacionit, kjo do të thotë se Ministria e Brendshme (MUP) ka parashikuar masa të ndryshme për mbrojtjen kundër shpërdorimit të sistemit të saj informativ që përmban një numër të madh regjistrash të ndryshëm[72]. Sipas politikës së sigurisë dhe faktit se disa dokumente që parashikojnë masa mbrojtëse të përdorura për mbrojtjen e këtij sistemi nga abuzimi, janë vetëm për përdorim zyrtar, është e pamundur që të renditen të gjitha masat mbrojtëse për IT-në. Sidoqoftë, disa prej tyre mund të njihen nga dokumentacioni i vënë në dispozicion dhe nga mbulime mediatike të tilla si

- **Masa mbrojtëse teknike kundër aksesit të paautorizuar dhe shpërdorimit të sistemeve të IT-së**. Kjo garanci përfaqëson kërcënimin më të zakonshëm në një sistem të lidhur në rrjet. Linja e parë e mbrojtjes kundër aksesit të paautorizuar dhe shpërdorimit të sistemeve të IT-së janë fjalëkalimet. “Çdo polic ka fjalëkalimin e tij/të saj që i mundëson atij/asaj akses në baza të ndryshme të dhënash brenda sistemit informativ policor”[73], tha eksperti i kriminalistikës Zeljko Cvrtila. Në përputhje me autoritetet dhe nevojat e tyre, punonjësve të policisë u jepet akses në disa nivele informacioni të klasifikuar. Kjo u jep atyre “akses në regjistrin më të madh tëtë dhë-

72 Lista e të gjithë regjistrave të MUP-it vihet në dispozicion në linkun e mëposhtëm: https://registar.azop.hr/index.php?action=search_results&query=ministarstvo+ unutarnjih+poslova&cl_p = 1&cl_ n=10&cl_n=200&cl_p=1

73 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze- podataka.html

nave personale në Republikën e Kroacisë"[74]. Sipas dispozitave të rregullores së renditur më lart mbi sigurinë e informacionit, të dhënat nga kjo bazë të dhënash mund të përdoren vetëm për përdorim profesional.

- **Monitorimi i trafikut të të dhënave dhe aksesi i punonjësve tek sistemet e të dhënave.** Megjithatë, "është thjesht e vështirë që ky proces të kontrollohet. Me sa jam në dijeni, ky proces nuk është monitoruar mjaftueshëm", tha ekspertja e kriminalistikës Zeljko Cvrtila. "Disa mijëra çështje kontrollohen çdo ditë. Megjithëse të mbrojtura nga sulmet e hakerave –ai thotë se kjo bazë nuk është e vështirë për t'u gjurmuar", sipas përfundimit të nxjerrë prej tij[75]. Siç u përmend më parë, çdo punonjësi policie i është dhënë një nivel i caktuar aksesi tek të dhënat nëpërmjet fjalëkalimit të tij/të saj por askush nuk kontrollon punonjësin më pas se përse ai ose ajo ka kontrolluar ndonjë informacion specifik, tha Cvrtila.

- **Trajnimi dhe masat ndërgjegjësuese për nëpunësit civilë mbi rreziqet e korrupsionit nëpërmjet IT-së dhe msat mbrojtëse**. Punonjësit e Ministrisë së Brendshme janë duke marrë pjesë në trajnime të ndryshme dhe projekte për rritjen e ndërgjegjësimit mbi rreziqet e korrupsionit të IT-së dhe garancitë. Shembujt e kësaj mase mbrojtëse kundër korrupsionit në IT janë dy projekte që synojnë forcimin e kapacitetit administrativ të Ministrisë në fushën e abuzimit me IT-në: forcimi i kapaciteteve administrative të Ministrisë së Brendshme në Luftën kundër Krimit Kibernetik (një projekt me kosto prej 700.000 Euro) dhe Bashkëpunimi Rajonal në Drejtësinë Penale: Forcimi i Kapaciteteve në Luftën kundër Krimit Kibernetik (kostot e projektit arrinin shumën prej 2.777,778 Euro), si dhe seminaret për rrjetin mjekoligjor të realizuara nga Ministria e Brendshme dhe Rrjeti Kërkimor dhe Akademik Kroat.

- **Kodi i Etikës**. Sipas Kodit të Etikës "çdo punonjës është përgjegjës për përdorimin etik të autoritetit të besuar të aksesit tek të dhënat personale nga bazat policore tëtë dhënave"[76]. Punonjësit e Ministrisë së Brendshme janë të detyruar të veprojnë në përputhje me Kodin e Etikës. Shtetasit mund të denoncojnë sjelljen joetike të nëpunësve civilë tek punonjësit e etikës.

- **Auditimi i sistemit të IT-së**. Sipas Rregullores për Organizimin e Brendshëm të Ministrisë së Brendshme (Fletorja Zyrtare nr. 70/12, 140/13), ka dy organizata të brendshme të ngarkuara për auditimet e sistemit informativ policor. Njëri është Departamenti i Sigurisë së Informacionit, i cili kryen monitorimin e organizatës, zbatimin dhe efiçencën e masave dhe standardeve të parashikuara të sigurisë së informacionit, dhe tjetri është Departamenti i Auditimit të Brendshëm, i cili kryen auditime të sistemit të informacionit.

74 Potrka, Nikola (2013) Normativna uredenost zastite osobnih podataka u Republici Hrvat- skoj. Policijska sigurnost 22(4): 509-521
75 http://dnevnik.hr/vijesti/hrvatska/svaki-policijski-sluzbenik-ima-lozinku-za-razlicite-baze- podataka.html
76 Potrka, Nikola (2013) Normativna uredenost zastite osobnih podataka u Republici Hrvat- skoj. Policijska sigurnost 22(4): 509-521

- **Garancitë ligjjore**. Nenet 266 deri 273 të Kodit Penal (Fletorja Zyrtare nr. 125/11, 144/12): përcaktojnë veprat penale kundër sistemeve, programeve dhe të dhënave kompjuterike: qasje të paautorizuar dhe të paligjshmenë sistemet kompjuterike ose të dhëna kompjuterike (sulmet e hakerave te kompjuterëve); pengimi i performancës së sistemit kompjuterik; dëmtimi i të dhënave kompjuterike; përgjimi i paautorizuar i të dhënave kompjuterike; falsifikimi kompjuterik; mashtrimi kompjuterik dhe shpërdorimi i pajisjeve. Sipas kodit penal, veprat e rënda penale kundër sistemeve, programeve dhe të dhënave kompjuterike janë konsideruar ato në lidhje me sistemet dhe të dhënat kompjuterike në pronësi të autoriteteve shtetërore dhe lokale, si dhe kompanitë publike. Së fundi, Kodi përfshin vepra penale që lidhen me pornografinë me fëmijët nëpërmjet sistemeve kompjuterike dhe dhunës në internet.

Sërish, është e rëndësishme të vërejmë se masat mbrojtëse të renditura këtu janë vetëm pjesë e rrjetit të masave mbrojtëse të zbatuara nga Ministria e Brendshme. Për arsye sigurie, në dispozicion të publikut nuk është vënë informacion mbi masa të tjera.

Çështjet e përshkruara më lart tregojnë se pavarësisht nga kuadri legjislativ; procedurat e parashikuara; Kodi i Etikës dhe masa të ndryshme mbrojtëse, abuzimi me sistemet e IT-së është ende i mundur. Lidhja më e dobët e procesit mbrojtës është individi me të gjitha virtytet dhe të metat e tij/të saj. Është madje e vështirë të imagjinohet një masë mbrojtëse që mund të garantonte sjellje jokorruptive.

Kroacia, rasti 11: Inspektori i nivelit të lartë shpërdoroi të dhëna konfidenciale për të fituar zgjedhjet vendore

Sipas legjislacionit përkatës për sigurinë e informacionit, Ministria e Financave ka parashikuar masa të ndryshme për mbrojtjen kundër shpërdorimit tëtë dhënave të taksapaguesve nga sistemet e tyre informative. Për shkak të politikës së sigurisë dhe faktit se dokumentet që parashikojnë masa mbrojtëse të përdorura për mbrojtjen e këtij sistemi nga abuzimi janë vetëm për përdorim zyrtar, dhe siç vërehet në rastet e mëparshme, është e pamundur të renditen të gjitha prej tyre. Megjithatë, ato që janë zbuluar renditen më sipër në rastin 10.

Në një sistem gjigand organizativ të tillë si Ministria e Financave që punëson mbi nëntë mijë persona dhe me njësi organizative në të gjithë vendin, çështje të politikave të sigurisë janë problematike për disa njësi organizative:

- Sektori i Sistemit të Informacionit pranë Sekretariatit të Përgjithshëm. Ky Sektor, midis të tjerash, përfshin detyrat e organizimit, krijimit dhe ruajtjes së një sistemi unik informacioni për Zyrën Qendrore të Ministrisë; ai kujdeset për përdorimin efiçent dhe të saktë të informacionit-burimet e komunikimit; organizon dhe menaxhon procesin e zhvillimit, analizës dhe kthimit të kopjeve të sigurisë tëtë dhënave; monitoron

sigurinë e komunikimeve dhe zbaton masat mbrojtëse të sistemit informativ.

- Sektori i Sistemit të Informacionit pranë Administratës Tatimore, midis të tjerash, kryen planifikimin, zhvillimin dhe përdorimin e sistemit informative dhe edukon përdoruesit e sistemit të IT-së.
- Sektori i Sistemit të Informacionit pranë Administratës Doganore, midis të tjerash, kryen planifikimin, menaxhimin, mbikqyrjen dhe koordinimin e zhvillimit, furnizimit dhe punës së aplikimeve të biznesit, shërbimet e IT-së dhe teknologjinë; zhvillon dhe zbaton politika të mbrojtjes dhe jep të drejta aksesi tek sistemi informativ; përcakton masa dhe cilësinë e shërbimit; garanton realizimin e kopjeve të sigurisë të sistemit informativ; planifikimin e mjeteve financiare për licencat, zhvillimin dhe mirëmbajtjen e sistemit informativ; strategjinë me shkrim për projektimin e sistemit të IT-së dhe edukon përdoruesit mbi sistemin e IT-së të Departamentit Doganor.
- Shërbimi për Zhvillimin dhe Mbështetjen ndaj Sistemit Operativ-Informativ të Thesarit të Shtetit, midis detyrave të tjera, garanton vazhdimësinë dhe qëndrueshmërinë dhe nivelin e nevojshëm të mbrojtjes së procedurave të biznesit të Thesarit të Shtetit; kryen detyra të projektimit, optimizimit, analizës, përditësimit dhe standardizimit të procedurave të biznesit; si dhe detyrat e autorizimit, sigurisë dhe mbrojtjes së të dhënave.
- Departamenti për Analizën Strategjike dhe Sistemin Informativ të Zyrës kundër Pastrimit të Parave, i cili, midis detyrave të tjera, projekton dhe përgatit informacion dhe nënsisteme të kësaj zyre; propozon akte nënligjore dhe rregullore të brendshme në fushën e të dhënave të sistemit dhe regjistron mbrojtje në zyrë; ruan dhe mbikqyr sistemin e të dhënave dhe regjistron mbrojtjen e zyrës.

Sërish, është e rëndësishme të vërehet se garancitë e renditura janë vetëm një pjesë e rrjetit të masave mbrojtëse të zbatuara nga Ministria e Brendshme por që për shkak të arsyeve të sigurisë, nuk janë plotësisht të disponueshme për publikun.

Megjithatë, si në rastet e mëparshme dhe pavarësisht nga kuadri legjislativ, procedurat e parashikuara, Kodi i Etikës dhe masa të ndryshme mbrojtëse, shpërdorimi i sistemeve të IT-së është ende i mundur. Lidhja më e dobët e procesit të mbrojtjes është individi me të gjitha virtytet dhe të metat e tij/të saj. Është e vështirë madje të imagjinohet një masë praktike mbrojtëse që mund të garantonte një sjellje pa korrupsion.

Kroacia, rasti 12: Ju nuk kaluat asnjë ditë të jetës suaj në punë? Nuk ka problem, ju gjithsesi mund të merrni pension të plotë!

Masat mbrojtëse të projektuara për të parandaluar abuzimin me regjistrin kryesor të personave që marrin sigurime për pension dhe regjistrin kryesor për përdoruesit e të drejtave të sigurimeve për pension pranë HZMO-s, janë: 1) gjurmimi/ndjekja e kronologjisë të ndryshimit të të dhënave (duke përdorur kartën e identitetit të përdoruesit dhe datën); 2) politika e miratimit të aksesit tek të dhënat sipas pozicionit të punës dhe përdorimit të masave mbrojtëse të softuerit dhe harduerit modern. Përveç këtyre masave kryesore mbrojtëse, ka gjithashtu: 3) dispozita të legjislacionit përkatës për mbrojtjen e të dhënave personale; dhe 4) dispozita të kodit të etikës dhe auditimit të brendshëm. Megjithatë, raste si ky provojnë se të gjitha këto masa mbrojtëse mund të vazhdojnë të shkelen.

Në dy vitet e shkuara, HZMO është bërë një prej institucioneve të para për të marrë pjesë në projektin e integrimit të sistemit të Numrit të Identifikimit Personal (OIB), së bashku me Administratën Tatimore të Ministrisë së Financave, Ministrinë e Administrimit Publik dhe Ministrinë e Punëve të Brendshme. *"Synimi i prezantimit të OIB-it ka qenë krijimi i një identifikuesi personal unik, i cili do të pranohej ligjërisht nga organet ligjore publike të Republikës së Kroacisë. Si rezultat i krijimit të identifikuesit personal unik në të gjitha të dhënat zyrtare, kushtet paraprake janë ndërmarrë për shkëmbimin e të dhënave kompjuterike tek organet ligjore publike. Vetëm me anë të shkëmbimit të të dhënave kompjuterike, organet ligjore publike mund të shkëmbejnë, ekonomikisht dhe në mënyrë efikase, të dhënat e nevojshme nga të dhënat zyrtare për zbatimin e qëndrueshëm dhe në kohë të të gjitha procedimeve administrative, tatimore dhe penale"*[77]. Duke pasur këtë parasysh, OIB është njohur si një instrument i fuqishëm që, ndër të tjera, do të mundësojë luftën sistematike kundër korrupsionit.

Para integrimit në rrjetin e shkëmbimit të OIB-it, HZMO operonte e izoluar brenda administratës shtetërore. Ajo kishte bazën e vet të të dhënave të përdoruesve dhe u paguante atyre rregullisht pensionet e tyre. Meqë shkëmbimi i të dhënave mes organeve ligjore publike nuk ishte i mundur, pas vdekjes së një anëtari familjeje, anëtarë të tjerë familjeje[77] ishin të detyruar të sillnin një çertifikatë vdekjeje tek shërbimi rajonal HZMO, i cili ishte organi që do të kishte paguar pensionin tek personi tashmë i ndjerë. Kjo procedurëhapi një mundësi për mashtrime të mundshme. Nëse askush nuk e mori çertifikatën e vdekjes tek shërbimi rajonal HZMO, familja mund të vazhdonte të merrte pensionin.

Megjithatë, pas shtatorit 2013, integrimi i HZMO-s në rrjetin e OIB-it ka mbyllur këtë boshllëk. Meqë parakushti i shkëmbimit të të dhënave kompjuterike mes organeve ligjore publike është zotërimi i një OIB-i, hapi i parë i HZMO-s ishte që të garantohej se të gjithë përdoruesit e tyre të zotërojnë një OIB. Në fakt u zbulua se 125,867 pensionistë nga 1.2 milion nuk kishin një OIB. Hapi i dytë ishte mohimi i mundësisë së marrjes së pensioneve nga zyra postare, dhe marrja e një pensioni vetëm nëpërmjet llogarisë së tyre bankare.

77 http://www.mfin.hr/en/novosti/full-application-of-oib-personal-identification-number

Nëse përdoruesit e HZMO-s dëshironin të vazhdonin të merrnin pensionet e tyre, ata ishin të detyruar t'i dorëzonin HZMO-s OIB-in e tyre.

Numri i pensionistëve pa OIB-in ra në 49.586 në muajin prill 2014 dhe përbëhet nga kryesisht përdorues të huaj. Nëpërmjet shkëmbimit shtesë të të dhënave me Administratën Tatimore të Ministrisë së Financave, Ministrisë së Administratës Publike dhe Ministrisë së Punëve të Brendshme, në datën 8 prill 2014 pagesa e 9.593 pensioneve u ndërpre – 9.108 nga jashtë vendit dhe 485 nga Kroacia. HZMO ende po përpiqet të zbulojë arsyet përse këta pensionistë nuk i dorëzonin atyre OIB-in e tyre. *"A janë këta përdorues në Kroaci ende gjallë, a merr dikush tjetër pensionin e tyre dhe a fiton para në mënyrë të paligjshme?"* tha ministri i punës dhe sistemit të pensioneve, Z. Mirando Mrsic dhe shtoi: *"A ka mashtrime, a janë këta persona në Kroaci, ku shkojnë këto pensione, ne dëshirojmë të eliminojmë këto gjëra. Ne nuk po i referohemi shumave të vogla por rreth më shumë se 16.6 milionë Euro dhe dëshirojmë t'i paguajmë këto para atyre që kanë të drejtë për t'i marrë ato"*[78].

Deri tani, integrimi i HZMO-s në rrjetin e OIB-it tregoi se 26 familje vazhdonin të merrnin pensione të anëtarëve të ndjerë të familjes. Midis tyre, pati një rast ku një postier i dorëzonte rregullisht pagesat e pensionit familjes së një burri që kishte vdekur 20 vjet më parë! Vetëm në këtë rast ka ndodhur që shteti u përball me një humbje reale prej 65.000 Euro. Me integrimin në sistemin OIB, raste si këto të përshkruara më parë nuk janë më të mundura pasi shkëmbimi i të dhënave mes organeve ligjore publike mbledh dhe krahason të dhëna dhe njofton automatikisht autoritetet për mospërputhshmërinë e të dhënave.

78 http://dnevnik.hr/vijesti/hrvatska/nema-oib-a-nema-mirovine-pod-povecalom-2-400-umirovljenika---309572.html

Kosova

Nga Hasan Preteni dhe Driart Elshani

Hyrje në shembujt e masave mbrojtëse kundër abuzimit me IT-në

Agjencitë e sektorit public mbështeten në sistemet e teknologjisë së informacionit (IT) për funksionet operative dhe shumë për ofrimin e shërbimit të tyre. Është e rëndësishme të garantohet se informacioni i mbajtur në këto sisteme të jetë i saktë dhe i plotë. Është gjithashtu e rëndësishme që ky informacion të jetë lehtësisht i aksesueshëm për qëllime të ligjshme dhe njëkohësisht i mbrojtur nga shpërdorimi. Në Kosovë ekzistojnë vetëm disa regjistra elektronikëdhe si rrjedhojë, rastet e korrupsionit në IT janë të pakta pasi nuk ka asnjë hapësirë për të kryer ndryshimin e të dhënave elektronike. Në fakt, rastet që ne zgjodhëm tregojnë mungesën e garancive që mbrojnë shpërdorimin e të dhënave dhe sistemet IT në përgjithësi.

Të gjitha rastet e paraqitura në kapitullin 1 të këtij studimi theksojnë rëndësinë e pasjes së garancive administrative (ose legjislative) dhe teknike të vëna në funksionim dhe të zbatuara nga secili institucion korrespondues. Për më tepër, çka mësojmë nga secili prej këtyre rasteve është se garancitë e lartpërmendura ose nuk janë vënë në funksionim, ose nuk janë respektuar. Edhe kur garancitë ishin hartuar, ato ishin të paplota ose u mungonte një përkufizim i qartë i procedurave dhe roleve për lehtësimin e rreziqeve të të dhënave, dhe abuzimin me sistemet e teknologjisë së informacionit të përgjithshëm. Kosova duhet të punojë më shumë për të krijuar dhe zbatuar këto garanci, veçanërisht që kur Kosova do të zbatojë shumë sisteme IT në të ardhmen dhe duhet të lehtësojë rreziqet e të dhënave dhe abuzimin me sistemet e teknologjisë së informacionit. Kosova ende nuk ka marrë ndonjë masë specifike për trajtimin e duhur të këtyre garancive.

Garancitë e paraqitura këtu do të lehtësonin ato rreziqe dhe parandalonin shpërdorimin e sistemeve të teknologjisë së informacionit. Në të ardhmen gjithçka do të jetë dixhitale – dmth përdorimi i letrës do të ishte vetëm i kufizuar dhe si rrjedhojë mund të lindnin forma të reja abuzimi që duhet të trajtohen me metoda të ndryshme. Këto metoda duhet të bazohen në garancitë e paraqitura këtu.

Në fakt, në këtë studim ne kemi propozuar garanci specifike për mbrojtjen e integritetit të të dhënave dhe integritetit të sistemeve IT, me qëllim mbrojtje ne tyre nga abuzimi i mundshëm nga njerëzit. Ne kemi përgatitur propozime për udhëzime dhe mekanizma të përgjithshme për sistemet elektronike. Këto garanci dhe udhëzime duhet të zbatohen për çdo institucion.

Këto standarde dhe politika janë projektuar për mbrojtjen e sistemeve dhe të dhënave të IT-së kundër shkatërrimit, ndryshimit ose falsifikimit. Garancitë që propozojmë në kapitullin 2 të këtij studimi mund të miratohen në formën e një politike për të gjithë spektrin e institucioneve, me qëllim mbrojtjen e sistemeve të tyre të IT-së nga abuzimi i mundshëm.

- Për sa i përket garancive teknike, përveç centralizimit të disa sistemeve IT, natyrisht që mungojnë të gjitha garancitë e tjera teknike. Ne nuk kemi asnjë informacion nëse janë përgatitur garanci shtesë teknike. Megjithatë, tashmë e dimë se në disa agjenci proceset e përgjithshme të miratimit dhe zbatimit janë duke u rishikuar.
- Në lidhje me garancitë organizative dhe procedural nuk janë përgatitur garanci të tilla. Për shembull, mungesa e një përkufizimi të qartë të roleve dhe përgjegjësive mund të kishte ekzistuar ose parimi i "shumë syve" mund të ishte vënë në funksionim. Nuk është përgatitur asnjë garanci shtesë e kësaj natyre.
- Në lidhje me monitorimin e aksesit tëpunonjësve tek sistemet e të dhënave, organizatat kanë mësuar nga ky rast se këto masa duhet të vihen në funksionim. Disa prej këtyre masave të tilla si monitorimi që akseson sistemet e të dhënave, janë aktualisht të disponueshme.
- Për sa i përket masave ndërgjegjësuese dhe trajnimit, nuk ka ekzistuar asnjë masë e tillë dhe aktualisht nuk ekziston një masë e tillë. Nuk ka madje as plane për masa të tilla.
- Në lidhje me auditimin, shumica e organizatave nuk ka pasur ndonjë auditim kur u zbulua kjo çështje dhe ne nuk kemi asnjë informacion nëse ekzistojnë aktualisht masa të tilla. Që prej asaj kohe disa organizata kanë kryer një auditim të përgjithshëm sigurie dhe janë në procesin e zbatimit të rekomandimeve. Megjithatë, këto rekomandime janë vetëm në lidhje me sigurinë, si për shembull mbrojtja nga sulmet kibernetike dhe nuk trajtojnë probleme që kanë lindur në kuadrin e kësaj çështjeje.
- Për sa i përket garancive legjislative, nuk ka pasur asnjë të tillë në kohën e kësaj çështjeje.

Për më tepër, çfarë mësojmë kryesisht nga ky rast është se shkëmbimi i të dhënave midis organeve publike mund të ishte thelbësor në luftën për parandalimin e ndodhjes së këtij tipi. Nëse sistemet ishin të ndëveprueshme midis atyre, atëherë kjo do të përshpejtonte procesin; për shembull, pasja e një procesitë ndërveprueshëm për verifikimin e dokumenteve tatimore do të vështirësonte falsifikimin e këtyre dokumenteve.

Masat mbrojtëse kundër korrupsionit nëpërmjet IT-së në Kosovë

Garancitë duhet të përgatiten për të zbuluar si duhet, monitoruar dhe marrë masa kundër rasteve të korrupsionit. Këto garanci duhet të jenë të zgjeruara dhe të larmishme, duke përfshirë garanci teknike, garanci organizative dhe procedurale, monitorim të trafikut tëtë dhënave dhe aksesin e punonjësve tek sistemet e të dhënave, masa trajnimi dhe ndërgjegjësimi, auditim të brendshëm dhe të jashtëm, si dhe garanci legjislative.

Për më tepër, do të ishte e këshillueshme që një organ i posaçëm i specializuar të krijohet në vend, me qëllim mbrojtjen dhe parandalimin e kryerjes së ndonjë shkeljeje ndaj integritetit të sistemeve të teknologjisë së informacionit. Ia vlen të deklarojmë se një organ i tillë i specializuar nuk ekziston në Kosovë. Në Kosovë ka një agjenci të dedikuar për Mbrojtjen e Privatësisë dhe të Dhënave por kjo Agjenci vepron vetëm në formën e një monitoruesi për privatësinë. Mandati i saj nuk është i mjaftueshëm dhe nuk shtrihet tek detyrimet e garantimit të mbrojtjeve/garancive në lidhje me abuzimin e teknologjisë së informacionit.

Në fakt nuk ka asnjë lloj institucioni që trajton hartimin dhe zbatimin e garancive dhe standardeve në këtë çështje. Shumë raste të abuzimit me teknologjinë e informacionit mbetentë përgjithshme, shpesh tërësisht të pazbuluara. Kur flasim rreth garancive/mbrojtjeve, ia vlen të përmendim se garancitë mund të jenë dyfishe: teknike dhe administrative.

Garancitë administrative mund të ishin në formën e ligjeve, akteve normative dhe rregulloreve administrative që sanksionojnë ndonjë veprim të gabuar të lidhur me integritetin e të dhënave dhe integritetin e sistemeve të teknologjisë së informacionit në përgjithësi. Secili institucion do të ndjekë një infrastrukturë të rregullores të parashikuar me ligj.

Garancitë teknike mund të ishin në formën e Procedurave Operative Standarde (SOP) që çdo institucion duhet të ndjekë me qëllim mbrojtjen e tyre nga shpërdorimi i të dhënave dhe i sistemeve të teknologjisë së informacionit të përgjithshëm. Çdo institucion duhet të ndjekë një listë kontrolli të SOP-eve që garanton mbrojtjen dhe fleksibilitetin e tyre maksimal kundër këtyre veprave penale. Udhëzimet aktuale administrative nuk kanë asnjë lloj SOP-je teknike në vetvete.

Për sa i përket garancive administrative, Kosova ka miratuar një grup ligjesh, strategjish dhe udhëzimesh administrative (akte normative) që lidhen me përdorimin e teknologjive të komunikimit dhe informacionit por deri tani infrastruktura legjislative nuk trajton siç duhet çështjen e integritetit të të dhënave dhe shpërdorimin e sistemeve të teknologjisë së informacionit në mënyrë specifike ose të përgjithshme.

Krimi kibernetik

Kosova ende nuk ka një Ekip për Reagimin ndaj Emergjencave Kompjuterike (CERT) që mund të ishte gjithashtu i ngarkuar për mbrojtjen e sistemeve të IT-së. Parashikohet që CERT-i do të krijohet në të ardhmen e afërt. Megjithatë, CERT-i do të vazhdonte të ishte i pamjaftueshëm pasi gabimisht CERT-i do të trajtonte vetëm në formë reaguese mbrojtjen kundër abuzimit dhe jo sigurimin e masave proaktive parandaluese.

Masa mbrojtëse të tjera

Masa të tjera mund të përdoren gjithashtu në luftën kundër korrupsionit të IT-së. Për shembull, shkëmbimi i të dhënave midis organeve publike dhe zbatimi i një kuadri të përgjithshëm ndëroperueshmërie mund të ndihmonte në parandalimin e disa prej rasteve, për shembull rasti 2. Masa të veçanta në sistemet e IT-së të prokurimit publik, të tilla si prokurimi elektronik, mund të konsiderohen gjithashtu të rëndësishme. Kosova është në

procesin e zbatimit të një sistemi të prokurimit elektronik. Gjithashtu, masa të tillë si të dhëna të qeverisë së hapur mund të jenë gjithashtu të dëshirueshme. Kjo do të favorizonte shkëmbimin e të dhënave midis organeve publike. Kosova është në fazën fillestare të këtij procesi.

LIGJET, STRATEGJITË DHE UDHËZIMET ADMINISTRATIVE NË LIDHJE ME ICT-NË NË KOSOVË

Ligjet

Ligjet në lidhje me Teknologjitë e Informacionit dhe Komunikimit (ICT) që janë zbatuar nga viti 2009 deri tani në Kosovë, përcaktohen në tabelën e mëposhtme:

Tabela 2 Ligjet e zbatuara dhe të ndryshuara nga viti 2009 deri në 201479

Nr	Emërtimi i ligjit	Në Plan Veprimi?	Ligji nr.	Data e miratimit	Akti dhe data e shpalljes
1	**Ligji për Mbrojtjen e të Dhënave Personale**	PO	03/L-172	29.04.2010	Dekreti nr. DL-020-2010, datë 13.05.2010
2	**Ligji për Parandalimin dhe Luftën kundër Krimit Kompjuterik**	PO	03/L-166	10.06.2010	Dekreti nr. DL-028-2010, datë 02.07.2010
3	**Ligji për Aksesin tek Dokumentet Publike**	PO	03/L-215	07.10.2010	Dekreti nr. DL-063-2010, datë 01.11.2010
4	**Ligji për Shërbimet e Shoqërisë së Informacionit**	PO	04/L-094	15.03.2012	Dekreti nr. DL-010-2012, datë 02.04.2012
5	**Ligji për Parandalimin e Konfliktit të Interesit në Përmbushje të Funksioneve Publike**	PO	04/L-051	31.08.2011	Dekreti nr. DL-029-2011, datë 31.08.2011
6	**Ligji për Arkivat Shtetërore**	PO	04/L-088	15.02.2012	Dekreti nr. DL-007-2012, datë 01.03.2012
7	**Ligji për Konfliktet Administrative**	PO	03/L-202	16.09.2010	Shpallur në përputhje me Nenin 80.5 të Kushtetutës së Republikës së Kosovës, datë 06. 10.2010
8	**Ligji për Arsimin e Lartë në Republikën e Kosovës**	PO	04/L-037	29.08.2011	Dekreti nr. DL-036-2011, datë 31.08.2011

79 Të dhënat janë marrë nga Kuvendi i Kosovës* - Departamenti për Mbështetjen dhe Procedurën Ligjore (AK - DSLP) (2014)

Strategjitë

Strategjitë e mëposhtme që janë miratuar deri tani:

- Strategjia Kombëtare për Shoqërinë e Informacionit 2006-2012
- Strategjia e Qeverisjes Elektronike 2009-2015
- Strategjia për të Mësuarin Elektronik për Kosovën 2010-2015 me objektiv kryesor transformimin e të mësuarit elektronik në një pjesë integrale të sistemit të përgjithshëm kombëtar arsimor
- Plani Strategjik për Arsimin në Kosovë 2011-2016 që përmban tetë programe prioritare, duke përfshirë Ndërtimin e Kapaciteteve dhe Teknologjinë e Komunikimit dhe Informimit
- Strategjia për Zhvillimin e Arsimit Parauniversitar për periudhën 2007-2017

Megjithatë, asnjë prej këtyre ligjeve dhe strategjive nuk trajton specifikisht integritetin e të dhënave ose keqpërdorimin e sistemeve të teknologjisë së informacionit.

Udhëzimet Administrative

Së fundi, udhëzimet e mëposhtme administrative (AI) janë miratuar deri tani në çështjen e IT-së:

1. AI nr. 02/2010 për Menaxhimin e Sigurisë së Informacionit
2. AI nr. 01/2010 për Sigurinë dhe Aksesin në Bazën e të Dhënave
3. AI nr. 04/2010 për Përdorimin e Pozicionit Zyrtar Elektronik në Institucionet e Kosovës
4. AI nr. 01/2011 për Menaxhimin dhe Përdorimin e Internetit në Institucionet e Kosovës
5. AI nr. 07/2008 për Forcimin e Transparencës dhe Standardizimin e Faqeve të Internetit në Institucionet e Kosovës
6. AI nr. 03/2010 për Përdorimin e Harduerëve dhe Softuerëve
7. AI nr. 02/2011 për Portalin Qeveritar të Republikës së Kosovës

Analizimi i përmbajtjes së këtyre dokumenteve gjithashtu zbulon çështjet e mëposhtme:

- AI për Sigurinë e Informacionit është botuar zyrtarisht që prej vitit 2010 por nuk ka pasur asnjë program socializimi për të garantuar që të gjitha palët të kuptojnë përgjegjësitë dhe detyrimet e tyre;
- AI mbi Sigurinë e Informacionit përshkruan politikat teknike dhe nuk përkufizon kuadrin e një sistemi menaxhimi, përshirë rolet, përgjegjësitë dhe autoritetin;
- Nuk ka asnjë marrëdhënie të qartë midis Udhëzimeve të ndryshme Administrative ose mënyrës sesi ato janë përcaktuar të përmbushin kërkesa të caktuara.

Për më tepër, këto udhëzime administrative trajtojnë pjesërisht vetëm probleme të tilla si të drejtat e aksesit tek bazat e të dhënave dhe Interneti në vend që të mbeten të paqarta. Më tej, zbatimi i tij është tepër i ngarkuar pasi asnjë institucion specifik nuk trajton pajtueshmërinë. Mbi të gjitha, megjithëse opinioni i përgjithshëm është se ekziston një infrastrukturë e përshtatshme ligjore në Kosovë, mund të vërehet se ende mungojnë

shumë pjesë dhe/ose janë kryesisht të paplota. Kosova ende duhet tëpunojë më shumë për tësiguruar se garancitë e mbrojtura nga pikëpamja legjislative janë të mirë-formuluara, të miratuara dhe të pajtueshme.

Masat mbrojtëse teknike

Deri tani, garancitë kufizohen tek mbrojtja e thjeshtë e fjalëkalimit të përdoruesve individualë, kodimi i të dhënave në disa raste të veçanta, dhe synimi për t'i mbajtur serverët të mbrojtur nga ndërhyrja fizike. Strategji dhe standarde më të sofistikuara për garancitë teknike në IT publike aktualisht mungojnë në Kosovë.

Maqedonia

Nga Marjan Stoilkovski dhe Rozalinda Stojova

Masat mbrojtëse institucionale

Në vitin 2002, sipas neneve të Ligjit për Parandalimin e Korrupsionit, Komisioni Shtetëror për Parandalimin e Korrupsionit (SCPC) u krijua si një organ i pavarur. Në nenin 1 të Ligjit, SCPC-së iu dha përgjegjësia për të zbatuar masat dhe aktivitetet që parandalojnë korrupsionin në përmbushjene masave dhe aktiviteteve qeveritare, të pushtetit publik, detyrës dhe policisë për parandalimin e konfliktit të interesit, si dhe masat dhe aktivitetet për parandalimin e korrupsionit në kryerjen e aktiviteteve me interes publik nga persona juridikë të lidhur me ushtrimin e autoritetit publik, si dhe masa dhe aktivitete për parandalimin e korrupsionit në kompani.

Gjithashtu, në vitin 2008 u krijua Njësia për Luftën kundër Korrupsionit. Ajo është njësi e dedikuar organizative nën Departamentin e Krimit të Organizuar të Ministrisë së Brendshme. Përgjegjësitë e Njësisë për Luftën kundër Korrupsionit janë identifikimi dhe hetimi i çdo tipi korrupsioni në Republikën e Maqedonisë.

Masat mbrojtëse teknike ndaj aksesit të paautorizuar dhe abuzimit me sistemet e teknologjisë së informacionit (IT) dhe monitorimit të trafikut të të dhënave dhe aksesit të punonjësve ndaj sistemeve të të dhënave

Në kuadër të specifikimit teknik të sistemeve të informacionit, pavarësisht nga fakti nëse ato janë "të nënkontraktuara" apo janë zhvilluar "në nivel të brendshëm", ekzistojnë praktika të aplikuara dhe të ndjekura. Disa praktika janë themeluar sipas ligjit përkatës por disa prej më të rëndësishmeve janë ato që përcaktohen nga praktika më shumë sesa të përmbledhura në ligj. Ato synojnë të parandalojnë përdorimin e IT-së për korrupsion dhe konsiderohen nga kërkesat më të rëndësishme që duhet të përmbushen në fillim të procesit të testit të pranimit. Ato janë:

- Duke mbajtur logje për çdo akses, shtim, fshirje dhe redaktim të të dhënave dhe duke i bërë të disponueshme skedarët regjistrues (logfile) sipas kërkesës, për qëllimet e rishikimit dhe auditimit. Përveç mbajtjes dhe arkivimit të logjeve, nuk lejohet asnjë operacion tjetër.
- Duke siguruar nivele të ndryshme identifikimi dhe autorizimi. Konfidencialiteti i nivelit të të dhënave të përpunuara nga sistemi ndikon në nivelin dhe kompleksitetin e procesit të identifikimit dhe autorizimit. Në të gjitha sistemet, rolet e përdoruesve të ndryshëm përcaktohen në varësi të privilegjeve të tyre të caktuara, duke filluar me emrin e thjeshtë të përdoruesit dhe fjalëkalimin për disa dhe për të tjerë, ekzistojnë kërkesa për përdorimin e çertifikatave dixhitale ose madje vetëm lejimi i aksesit të të dhënave nga një stacion i posaçëm pune në një vendndodhje fizike specifike rreptësisht të përcaktuar.

- Sipas Ligjit për Menaxhimin Elektronik, në rastet e zhvillimit “të nënkontraktuar” të sistemeve të ruajtjes dhe/ose përpunimit të të dhënave personale, por pa përjashtuar rastet e zhvillimit të sistemit “të brendshëm”, një prej kërkesave është përcaktimi i mjediseve të zhvillimit dhe testimit duke përdorur të dhënat e testimit, ndërsa të dhënat reale të drejtpërdrejta ruhen vetëm në mjedisin e prodhimit. Kjo mundëson akses të kanalizuar dhe të kontrolluar ndaj të dhënave dhe vetëm nga nëpunës të caktuar zyrtarisht.
- Gjenerimi i raporteve të rregullta të aktivitetit të përdoruesit nga tipe të ndryshme përdoruesish dhe role është gjithashtu kërkesë që garanton një mënyrë të rregullt të monitorimit të aktiviteteve të përdoruesve. Këto raporte u dërgohen administratorëve kryesorë dhe nivelit të lartë të menaxhimit.
- Një prej praktikave më pozitive për pjesën më të madhe të sistemeve lokale është dërgimi i postës elektronike dhe/ose njoftimet me mesazhe tek administratorët kryesorë dhe niveli i lartë i menaxhimit në rastet kur janë zbuluar aktivitete të dyshimta ose janë në procesin e kryerjes.
- Për të garantuar lidhjen me internet të sistemit kur shkëmbehen të dhëna mes sistemeve dhe përgjimin e komunikimit të të dhënave, të gjitha institucionet krijojnë lidhje VPN duke përdorur të dhëna të koduara.
- Në përputhje me punën e tyre, nëpunësit e zyrës qendrore përdorin stacione pune që kanë akses vetëm tek të dhënat për të cilat është përgjegjës institucioni i tyre dhe nuk kanë akses në internet ose në sistemet e tjera.
- Sistemet e IT-së të sektorit privat dhe publik janë testuar për pika të dobëta dhe depërtim të mundshëm në sistem. Megjithëse testimi i depërtimit në sistem është më i përdorshëm në sektorin financiar privat, ndodh që sektori publik të rekrutojë kompani të çertifikuara për testimet e depërtimit në sistem dhe ta përdorë këtë metodë për të parandaluar sistemet e IT-së nga aksesi i paautorizuar.

Masat mbrojtëse organizative dhe procedurale, si për shembull “Parimi i shumë syve”

- Ekziston një prirje për nënshkrimin e NDA-ve (Marrëveshje për Moszbulimin e Informacionit) me operatorët ekonomikë dhe zbatuesit. Këto marrëveshje janë amenduar me deklaratat për moszbulimin e informacionit nga të dyja palët – kontraktuesi dhe zbatuesi – për personat me akses në sistem.
- Aksesi fizik tek sistemet në çdo interval kohe, qoftë nëse bëhet gjatë zbatimit ose gjatë mirëmbajtjes, është i mundshëm vetëm pasi të sigurohet çertifikata e sigurisë nga Ministria e Punëve të Brendshme për secilin person të përfshirë.
- Ekziston një praktikë e miratuar në institucione për caktimin e dy roleve kryesore themelore për dy tipet e ndryshme të punonjësve: administratorët teknikë dhe administratorët e përmbajtjes. Administratorët e përmbajtjes janë përgjegjës për sistemin në nivel zbatueshmërie dhe përveç menaxhimit të sistemit dhe bazës së të dhënave, punonjësit në këtë rol menaxhojnë gjithashtu përdoruesit dhe lejimet e tyre, por jo të dhënat e ruajtura/të mbajtura në bazat e të dhënave. Administratori i përmbajtjes është përgjegjës për menaxhimin e të dhënave të ruajtura në bazat e të dhënave.

Trajnimi dhe masat ndërgjegjësuese për nëpunësit civilë në lidhje me rrezikun e korrupsionit dhe masat mbrojtëse

Viktimat e korrupsionit mund të jenë qytetarë individualë, biznes ose grup subjektesh, por në disa raste viktima është shoqëria në tërësi. Lufta kundër korrupsionit është një prej objektivave strategjikë më të rëndësishëm të miratuar nga ministritë dhe institucionet e tjera që tregon angazhimin e qeverisë së Republikës së Maqedonisë (p.sh. shihni Strategjinë e Reformës së Administratës Publike dhe Planin e saj të Veprimit[80]). Për më tepër, sektori publik dhe qytetarët luajnë rol aktiv në reformën e shoqërisë, duke garantuar rëndësinë e vullnetit dhe gatishmërisë për të mësuar në lidhje me mënyrat e parandalimit të korrupsionit dhe mundësitë e disponueshme për veprim ligjor. Si rrjedhojë, veprimet e mëposhtme janë ndërmarrë nga institucionet dhe sektori publik (NGO): trajnimi i punonjësve dhe qytetarëve më i shpeshtë në institucionet që janë më të cenueshme nga korrupsioni; fushatat e ndërgjegjësimit publik nëpërmjet kanaleve të ndryshme; fletushka të printuara, tabela lajmërimesh, reklama të shkurtra televizive.

Auditimi i sistemeve të IT-së (auditet e brendshme ose të jashtme; të filluara nga një organ shtetëror ose nga raportet apo ankesat e qytetarëve apo shtypit)

Megjithëse auditimi i sistemeve të IT-së nga auditët e brendshëm dhe të jashtëm po kryhet për një numër shumë të vogël sistemesh, ai është një prej masave të mundshme. Ai është zbatuar në raste shumë të rralla, si për shembull kur sistemi trajton të dhëna konfidenciale ose të dhëna me rëndësi për shtetin dhe në rastet kur alokohet buxhet dhe kohë e mjaftuesh.

Masat mbrojtëse legjislative

Në vitin 2002 **Ligji për Parandalimin e Korrupsionit** u miratua duke mundësuar zbatimin e një marrëveshjeje ligjore në luftën kundër korrupsionit. Herën e fundit i shqyrtuar në vitin 2010, ky ligj:

“Rregullon masat dhe aktivitetet për parandalimin e korrupsionit në ushtrimin e kompetencave, autorizimet publike, detyrën zyrtare dhe politikat, masat dhe aktivitetet për parandalimin e konfliktit të interesit, masat dhe aktivitetet për parandalimin e korrupsionit në kryerjen e aktiviteteve me interes publik nga personat juridikë lidhur me ushtrimin e autorizimeve publike, si dhe masat dhe aktivitetet për parandalimin e korrupsionit në shoqëritë tregtare”. (Neni 1).

Ai paraqiti një sistem integriteti (pakt integriteti) dhe mbrojtje nga “informatorët”.

80 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

- **Ligji për Menaxhimin Elektronik** përshkruan standarde që duhet të përmbushen kur sistemet e zhvillimit të informacionit komunikojnë dhe ndajnë të dhëna dhe dokumente me sistemet e informacionit nga institucione të tjera për qëllimet e procedurës administrative[81]. Projektligji për njohjen e mjedisit unik dhe komunikimit elektronik midis institucioneve për shkëmbim të dhënash dhe dokumentesh dhe udhëzimet rrjedhuese të tij për kërkesat teknike, mënyra e funksionimit, klienti që komunikon dhe rekomandimi për përdorimin e sistemit të ndëroperueshmërisë përshkruan:
  - Kërkesën teknike të infrastrukturës së harduerit dhe softuerit të klientëve që komunikojnë;
  - Testimin e mjedisit;
  - Mirëmbajtjen dhe zhvillimin e shërbimeve të rrjetit;
  - Protokollet e postës elektronike
  - Aksesin ndaj të dhënave që i nënshtrohen shkëmbimit;
  - Sigurinë dhe integritetin e të dhënave dhe në udhëzimet rrjedhuese paraqiten shumë prej kontrolleve të serive të standardit ISO 27000;
  - Strukturën e të dhënave dhe dokumenteve që i nënshtrohet shkëmbimit dhe;
  - Planifikimin e elementeve bazë të arkitekturës për komunikimin me sistemin e ndërveprimit.

- **Ligji për Komunikimin Elektronik** siguron mbrojtjen e të drejtave të përdoruesve, duke përfshirë përdoruesit e fundit me aftësi të kufizuara dhe përdoruesit e fundit me nevoja të posaçme sociale dhe garanton konfidencialitetin e komunikimeve.

- **Ligji për Mbrojtjen e të Dhënave Personale**, i shqyrtuar herën e fundit në vitin 2012 harmonizohet me direktivat përkatëse të BE-së dhe zbatohet plotësisht ose pjesërisht në përpunimin automatik të të dhënave personale. Mes temave të tjera, ai përshkruan mënyrat e përpunimit të të dhënave personale dhe përcakton masat e kërkuara teknike për mbrojtjen e përpunimit të të dhënave personale.

- **Ligji për Përdorimin e të Dhënave nga Sektori Publik**, i miratuar në vitin 2014 është një pasqyrim i aktiviteteve të ndërmarra në kuadër të Nismës së Partneritetit të Hapur Qeverisës. Ai renditet me Direktivën 2003/98/KE të Parlamentit Evropian dhe Këshillit të Evropës për ripërdorimin e informacionit në sektorin publik. “Ky ligj përcakton detyrimin e autoriteteve dhe institucioneve të sektorit publik për ekspozimin publik të të dhënave që gjenerohen nga ushtrimi i kompetencave të tyre në përputhje me ligjin, me qëllim që të mundësohet përdorimi i të dhënave të tilla nga biznese ose individë për të krijuar informacion të ri, përmbajtje, aplikime ose shërbime”. Një prej objektivave është të inkurajohet “përgjegjshmëria në rritje dhe transparenca e sektorit publik”, që është një prej instrumenteve për parandalimin e korrupsionit.

81 http://mioa.gov.mk/files/pdf/dokumenti/zakoni/zeu/Zakon_za_elektronsko_upravuvan- je_konsolidiran_tekst.pdf

- **Ligji për Disiplinën Financiare**, i miratuar në vitin 2013, rregullon përmbushjen në kohën e duhur të detyrimeve financiare që rrjedhin nga zbatimi i transaksioneve të biznesit midis operatorëve ekonomikë në sektorin privat ose midis enteve të sektorit publik dhe operatorëve ekonomikë nga sektori privat, me qëllim parandalimin e mosarritjes së detyrimeve të parashikuara me para në dorë në përputhje me përcaktimet sipas ligjit. Janë përcaktuar gjoba për secilin kontraktues që nuk pajtohet me këtë detyrim. Zbatimi i pagesës së kontrolluar të detyrimeve me para në dorë mbështet fuqishëm aktivitetet anti-korrupsion.

- Rishikimet e fundit të **Ligjit për Prokurimin Publik** u kryen në vitin 2014 me disa ndryshime të mëdha. Përpara prokurimeve të mallrave dhe shërbimeve që kanë një vlerë më të lartë vlerësimi sesa është përcaktuar në muaj për prokurimet e vogla, kontraktuesit janë të detyruar të kryejnë studime tregu. Kjo nënkupton sigurimin e një numri të caktuar (në varësi të vlerës së vlerësuar) të pranimit të kërkesave nga furnizues të ndryshëm. Nëse ka më pak sesa numri i parashikuar i furnizuesve të aftë për dorëzimin e mallrave të kërkuara ose shërbimit që autorizohet të zbatohet, kontraktuesi duhet të marrë pëlqimin me shkrim nga Këshilli i Prokurimit Publik, organ i themeluar me këtë rishikim të ligjit.

- Sipas legjislacionit kombëtar për informacionin e klasifikuar, çdo sistem IT-je që mban ose përpunon informacion të klasifikuar, duhet të akreditohet nga akreditues të çertifikuar nga Drejtoria Kombëtare e Informacionit të Klasifikuar. Kur zhvillohen sisteme IT-je për përpunimin e informacionit të klasifikuar, direktiva të posaçme miratohen për karakteristikat teknike të harduerit dhe softuerit që do të përdoret në sistemin IT-së për informacionin e klasifikuar.

- Mes akteve të tjera ligjore, **Ligji për Informacionin e Klasifikuar** në nivel kombëtar përdoret si mbrojtje ndaj aksesit të paautorizuar dhe abuzimit të sistemeve të IT-së.

MASA MBROJTËSE TË TJERA

Masa mbrojtëse në procesin e prokurimit dhe disiplinimit financiar

Në vijim, janë paraqitur kushtet e mëposhtme që mbështesin parandalimin e korrupsionit në procedurat e prokurimit publik:

- Specifikimet teknike nuk duhet të përmbajnë ndonjë markë, edhe në rast se janë shoqëruar me përshkrime udhëzuese dhe kërkesat e detajuara në specifikim duhet të përmbushen nga më shumë se një shitës; përveç rasteve të parashikuara në ligj kur respektohet procesi para parashikimit;
- I gjithë prokurimi publik i të gjitha institucioneve të shtetit dhe atyre publike duhet të kryhet përmes sistemit të prokurimit publik.

Aplikimi i softuerit karakteristik si masë mbrojtëse

Ministri i Ministrisë së Punës dhe Politikës Sociale (MLSP) theksoi se ministria ka kryer një sërë aktivitetesh dhe analizash në fushën e të drejtave të mirëqenies sociale. Ai shtoi se me zbatimin e softuer-it të ri për mirëqenien sociale, janë zbuluar raste të abuzimit dhe ekspozimit të rremë të informacionit nga përdoruesit. Analizat e thelluara zbuluan se abuzime të tilla nuk mund të jenë kryer vetëm në rast se ka pasur bashkëpunim me disa nëpunës. Si rrjedhojë, auditimet e brendshme dhe monitorimi i punës së qendrave të kujdesit social kanë nisur kur janë konstatuar disa raste abuzimi të së drejtës për mirëqenie sociale dhe për të gjitha ato janë ngritur padi penale. Është provuar se nëntë qytetarë nga një qytet A të punësuar si nëpunës në institucionin publik "Qendra për Punë Sociale" në qytetin A, kishin abuzuar dhe keqpërdorur pozicionin e tyre zyrtar dhe kishin ndihmuar një numër specifik qytetarësh të siguronin të drejta të mirëqenies sociale në mënyrë të paligjshme.

Në rastet që më parë ishin të prekshme nga korrupsioni, sistemet IT shpërndajnë tashmë licenca CEMT, apartamente për strehim social, dhoma konvikti për studentët dhe shërbime të tjera. Një prej shërbimeve më të rëndësishme është shpërndarja elektronike e çështjeve gjyqësore tek gjykatësit, e identifikuar dhe paraqitur si masa 11 në Strategjinë e Reformës së Administratës Publike dhe Plani i saj i Veprimit[82].

Ekziston një formular elektronik për njoftimin anonim të korrupsionit të kryer apo që është duke u kryer, i disponueshëm në portalin e Zyrës së të Ardhurave Publike (PRO). Ai është më i përdoruri në llojin e tij. Anonimati i dërguesit është i garantuar, duke e bërë adresën e tij/e saj të padukshme për përdoruesit PRO.

Qeveria e hapur si masë mbrojtëse

Hapja e të dhënave publike dhe publikimi i tyre në portalet institucionale është një prej formateve të nivelit me 5 yje[83] që me pak fjalë është Nisma për Partneritet e Qeverisë së Hapur. Ajo është një qasje e re për aktivitetet anti-korrupsion dhe i mundëson çdo subjekti të ketë rol aktiv në parandalimin dhe përcaktimin e korrupsionit. Për shembull, një prej tipeve të të dhënave që është publikuar në rast se dorëzohet, janë të dhënat për statusin e aseteve financiare dhe pasurisë së zyrtarëve të lartë.

Si provë tjetër e angazhimit të qeverisë, në vitin 2014 u miratua Ligji për Përdorimin e të Dhënave nga Sektori Publik. Ai përcakton detyrimin e autoriteteve dhe institucioneve nga sektori publik për të ekspozuar publikisht të dhënat e gjeneruara në linjën e përgjegjësive të tyre, me qëllim që të mundësojnë përdorimin e të dhënave të tilla nga bizneset ose individët për të krijuar informacion të ri, përmbajtje, aplikacione ose shërbime. Ky ligj përcakton gjithashtu kufizimet për kontratat ekskluzive nga institucionet.

Në përputhje me të dhënat e hapura, ligjet që trajtojnë lëshimin e licencave profesionale që përfundojnë me procesin e testimit, p.sh., zbatuesit, ekspertët e mjekësisë ligjore, vlerësuesit, noterët dhe të tjerë, po renditen sipas parimeve të mëposhtme: për secilin profesion, duhet të ketë një listë me të paktën 500 pyetje të paracaktuara të bëra publike dhe të disponueshme në portalet përkatëse. Testimi kryhet elektronikisht vetëm duke përdorur sistemet e testimit elektronik. Një model pyetjesh lidhur me testimin real përzgjidhet rastësisht sipas kritereve të caktuara dhe ofron mundësi të barabarta për të gjithë kandidatët. Për më tepër, testimi duhet të regjistrohet me video ose të transmetohet përmes internetit dhe mund të refuzohet në rast se vihen re dhe provohen parregullsi.

Ky parim duhet të zbatohet edhe në procesin e punësimit të nëpunësve administrativë dhe në kryerjen e testimit të jashtëm të studentëve por në ato raste pa vëzhgim video dhe duke përdorur pyetje të ndryshme për çdo student.

82 http://mioa.gov.mk/files/pdf/dokumenti/RevidiranAP_SRJA_mioagov.pdf

83 Plani me pesë yje i Të dhënave të Hapura siç sugjerohet nga Tim Bemers-Lee, shpikësi i rrjetit të gjerë botëror dhe nismëtari i të dhënave të hapura, shpërblen me yje lidhur me faktin se sa i lidhshëm është një format të dhënash. Një yll përshkruan bërjen e të dhënave të disponueshme në rrjet (cilido qoftë formati) sipasnjë license të hapur, por të dhënat nuk duhet të jenë të strukturuara, mund të përdoren formate pronësore, nuk duhet të përdoren URI për të shënuar elementë dhe nuk duhet të jetë i lidhshëm me të dhëna të tjera që japin kontekstin. Një yll është niveli më i ulët i bërjes së të dhënave të hapura.

Mali i Zi

Nga Dusan Drakic dhe Ivan Lazarevic

Hyrje në shembujt e masave mbrojtëse kundër abuzimit me Teknologjinë e Informacionit (IT)

Për të zvogëluar keqpërdorimin e të dhënave duhet të monitorojmë dhe zhvillojmë disa aspekte të caktuara të ICT-së. Megjithatë, në një kuptim të ngushtë, keqpërdorimi i të dhënave në nivel kombëtar dhe ndonjëherë lokal ka më shumë gjasa të jetë pasojë e gjendjes morale të shoqërisë, dhe mungesës së dëshirës së individit për të respektuar rregullat dhe standardet e pranuara. Regjistrat me bazë të dhënash cilësore që mundësohen nga ICT-ja, të përcaktuara në përputhje me standardet ndërkombëtare, mundësojnë njohjen dhe mbrojtjen e personave fizikë dhe juridikë vendas dhe të huaj, si dhe pronat e luajtshme dhe të paluajtshme brenda territorit kombëtar.

Rastet e përzgjedhura tërheqin vëmendjen për nevojën e një numri më të madh të regjistrave elektronikë, të cilët do të na mundësojnë përcaktimin e vendit të origjinës së të dhënave, ruajtjen e tyre në internet në një bazë të centralizuar të dhënash, si dhe lehtësimin e përdorimit të tyre.

Është i nevojshëm përmirësimi dhe standardizimi i shkëmbimit të të dhënave ndër-qeveritare nëpërmjet vendosjes së një infrastrukture të qëndrueshme dhe të besueshme të ICT-së. Është e rëndësishme të bëhet modernizimi i administratës publike dhe zgjerimi i shërbimeve publike që kanë në qendër përdoruesit, duke rritur disponueshmërinë dhe ofrimin e sigurt të tyre përmes kanaleve të shumta.

Rastet tregojnë se ekziston gjithashtu nevoja për krijimin e një kuadri të ndërveprimit që do të krijojë kushtet për përmirësimin e cilësisë së menaxhimit të informacionit dhe shkëmbimit të tij ndërmjet agjencive qeveritare, si dhe lejimin e shkëmbimit automatik dhe përdorimin e të dhënave të ruajtura në regjistrat publikë dhe sistemet e tjera të informacionit.

Mali i Zi, rasti 1: Shpërdorimi i detyrës dhe falsifikimi i dokumenteve zyrtare

Rasti i një pasaporte të skaduar që falsifikohet dhe përdoret nga një person i tretë tregon defektin apo dështimin e sistemit të informacionit në Ministrinë e Brendshme për lëshimin e pasaportave, e cila duhet të eliminojë rrezikun e përdorimit dhe ri-lëshimin e dokumenteve të udhëtimit, kur periudha e vlefshmërisë së tyre ka skaduar. Sistemi nuk lidhi dokumentin fizik (pasaportën) me një të dhënë të pasqyruar të bazës së të dhënave që përmban të njëjtin informacion të saktë, duke përfshirë fotografinë e mbajtësit të pasaportës. Po ashtu, nuk kishte gjurmë elektronike brenda sistemit që të identifikonte nëpunësit që kishin lëshuar pasaportën e falsifikuar.

Ky rast tregon një mungesë të masave mbrojtëse, si të atyre teknike, ashtu dhe atyre të monitorimit/ auditimit kundër abuzimeve.

Dokumentet e udhëtimit përdoren ndërkombëtarisht, prandaj ky rast tregon gjithashtu nevojën për shkëmbimin elektronik të të dhënave dhe verifikimin midis vendeve, siç është rasti midis shteteve të hapësirës Shengen.

Mali i Zi, rasti 2: Përdorimi i të dhënave të IT-së për të shkaktuar dëm politik

Ky është një rast kur medias i është dërguar një listë e rremë numrash telefonikë, duke supozuar se zyrtarë të lartë kishin komunikuar me anëtarët e një njësie të krimit të organizuar.

Shembulli i mësipërm tregon qartë se ekziston çështja e përgjegjshmërisë të personave përgjegjës në kompanitë operatore, kryesisht për çështje që lidhen me konfidencialitetin, përgjimin dhe abuzimin e postës elektronike.

Pronësia më e rëndësishme e një kompanie janë të dhënat e saj. Humbja e të dhënave të një kompanie e ekspozon atë ndaj çështjeve gjyqësore dhe humbjes së reputacionit. Informacioni i ruajtur në bazat e të dhënave është i rëndësishëm. Kompanitë në mënyrë të rregullt ruajnë informacione sensitive, private dhe të pronësisë, disa prej të cilave mund të jenë numrat e sigurimeve shoqërore, kartat e kreditit, të dhënat e listëpagesave dhe të dhënat personale. Kompanitë duhet ta mbajnë dhe sigurojnë këtë informacion në mënyrë konfidenciale, ndryshe ato mund të ekspozohen dhe përballen me humbjen e reputacionit dhe/ose të ardhurave.

Operatori është i detyruar që të sigurojë parakushtet e nevojshme teknike dhe organizative që lejojnë përgjimin e komunikimeve, dmth për t'u mundësuar autoriteteve shtetërore përkatëse marrjen e të dhënave që gjenden në trafik dhe vendndodhjen e tyre por kjo bëhet vetëm në bazë të një vendimi të gjykatës, dhe nëse kjo është e nevojshme për kryerjen e procedurave penale (në bazë të kodit të procedurës penale), ose për arsye të sigurisë së Malit të Zi (në veçanti në përputhje me legjislacionin që rregullon shërbimet e zbulimit).

Ky rast nuk kishte ndonjë përfundim gjyqësor dhe nuk u arrit ndonjë përgjegjësi objektive apo subjektive për të. Si rrjedhojë, nuk u bë e mundur që të përcaktoheshin saktësisht se çfarë masa mbrojtëse mungonin.

Mali i Zi, rasti 3: Keqërdorimi i funksioneve dhe futja e të dhënave të pasakta në regjistrat publikë

Ky rast lidhej me transferimin e paligjshëm të tokës shtetërore të kadastrës bashkiake tek një person i tretë, nëpërmjet regjistrimeve të paligjshme të kadastrës. Kjo rezultoi në prodhimin e një çertifikate elektronike të rreme që mund të përdorej më vonë në një procedurë ligjore.

Në Mal të Zi ka një kombinim të regjistrave të ndryshëm elektronikë dhe fizikë të tokës. Megjithatë, çdo vit numri i regjistrave rritet. Disa prej regjistrave janë dixhitalizuar, dhe në disa raste të dhënat mund të shkëmbehen në mënyrë elektronike. Të njëjtat dokumente mund të ketë origjina të ndryshme dhe nganjëherë është e pamundur të gjendet saktësisht se kush i ka krijuar ato, dhe kush ka akses të plotë në këto dokumente. Në këtë rast, është një kërkesë që dokumentacioni të mbahet në mënyrë elektronike, dhe aksesi në regjistra të lejohet vetëm për personat e autorizuar.

Si parim sigurie, personeli duhet të ketë pikërisht nivelin e nevojshëm të privilegjit të aksesit për të përmbushur funksionin e vet të punës apo detyrën. Dhënia e një privilegji të përdoruesit përtej nevojës së tyre është një praktikë e zakonshme, e cila mund të çojë në abuzimin e privilegjit të tepërt.

Monitorimi i përdoruesve ndihmon për të siguruar:

- privatësinë e të dhënave, në mënyrë që vetëm aplikacionet dhe përdoruesit e autorizuar mund të shohin të dhëna sensitive.
- qeverisjen e të dhënave, në mënyrë që strukturat dhe vlerat kritike të bazës së të dhënave të mos ndryshohen jashtë procedurave të kontrollit të ndryshimit të korporatave.

Ky rast ilustron se çfarë ndodh kur monitorimi i aksesit të punonjësve është i pamjaftueshëm. Po ashtu, regjistrimeve të kadastrës bashkiake u mungonin masat mbrojtëse organizative dhe procedurale, të tilla si "parimi i shumë syve". Asnjë kontroll i përgjithshëm nuk është kryer mbi statusin e tokës dhe pronësinë, as teknikisht dhe as nga ndonjë punonjës tjetër në regjistrin bashkiak ose nga një auditim i jashtëm.

Mali i Zi, rasti 4: Lëshimi i paligjshëm i dokumenteve të udhëtimit

Në Drejtorinë e Policisë në Podgoricë dy kërkesa për lëshimin e pasaportave të reja nuk ishin verifikuar nga nëpunësi që merrej me trajtimin e këtyre rasteve. Megjithatë, hetuesit nuk gjetën të dhëna elektronike në sistemin e informacionit në lidhje me sigurimin e pasaportave, dhe i gjithë dokumentacioni sipas kërkesave të skanuara për pasaportat mungonte në dhomën e ruajtjes të dokumenteve.

Ky shembull tregon se nuk ka pasur regjistrim elektronik të kërkesave të skanuara për lëshimin e pasaportave në sistemin e informacionit, e cila do të eliminonte rreziqet e përdorimit dhe lëshimit të dokumenteve të falsifikuara. Është gjithashtu e nevojshme të përmirësohet siguria e sistemit elektronik duke regjistruar aksesin fizik në mjediset ku mbahen dosjet dhe dokumentet zyrtare.

Kompjuterët për menaxhimin e bazës së të dhënave dhe të sistemit të informacionit (serverët) duhet të jenë të pajisur me:

- një sistem të aksesit të sigurt (log-on) dhe regjistrimit të të gjitha hyrjeve, në mënyrë që hyrja në server të mund të jetë e kontrolluar dhe e kufizuar; dhe
- një mekanizëm për parandalimin e tërheqjeve dhe depozitave të paautorizuara të mediave me IT të lëvizshme/ portative, të portave ose lidhjeve të komunikimit për printimin e të dhënave.

Vërtetësia (autenticiteti) është verifikimi i identitetit nga një sistem apo bazë të dhënash bazuar në paraqitjen e kredencialeve të veçanta në atë sistem. Vërtetësia kontribuon në konfidencialitetin e të dhënave dhe përgjegjshmërinë e veprimeve të kryera në sistemet e informacionit duke verifikuar identitetin unik të një përdoruesi. Aksesi në sistemet e telekomunikacionit, kompjuterik dhe ato të aplikimit për përpunimin e të dhënave duhet të lejohet vetëm duke futur emrin e përdoruesit dhe fjalëkalimin e duhur përkatës.

Një numër në rritje i aplikimeve dhe shërbimeve në Rrjetin e Qeverisjes Elektronike kërkojnë/lejojnë autenticitetin dhe nënshkrimin dixhital duke përdorur një identitet dixhital. Në këtë rast, është e domosdoshme që të gjitha dokumentet e nevojshme të jenë vendosur në një vend - regjistër elektronik - dhe aksesi në këtë regjistër duhet të jepet vetëm për personelin e autorizuar të cilët kanë çertifikatën përkatëse dixhitale.

Autoriteti i Çertifikimit të Brendshëm (CA) në Ministrinë për Shoqërinë e Informacionit dhe Telekomunikacionet (GOV.ME) është ngritur me qëllimin e përdorimit të çertifikatavedixhitale për të mundësuar korrespondencë të sigurt dhe të besueshme midis auto-

riteteve shtetërore. Që nga fillimi, përdorimi i çertifikatësdixhitale në administratën publike është promovuar dhe zbatuar në mënyrë aktive nga Ministria për Shoqërinë e Informacionit dhe Telekomunikacionet (MIST). Shërbimet e qeverisjes elektronike si në MIST ashtu dhe në institucione të tjera, synojnë rritjen e përdorimit të çertifikatavedixhitale, kryesisht në interes të shkëmbimit të sigurt të të dhënave dhe identifikimin e përdoruesve.

Masat mbojtëse kundër korrupsionit të IT-së në Malin e Zi

Në dekadën e fundit, në Malin e Zi është rritur ndërgjegjësimi mbi korrupsionin duke u bërë një prioritet i rëndësishëm në axhendën politike të vendit. Qeveritë e njëpasnjëshme malazeze janë angazhuar për të luftuar korrupsionin dhe kanë ndërmarrë hapa të rëndësishme për të trajtuar këtë çështje, pjesërisht edhe për shkak të angazhimeve që rrjedhin nga procesi i anëtarësimit në Bashkimin Europian dhe nevojës në vijim për përshtatjen e legjislacionin kombëtar me *acquis communautaire*.

Teknologjitë e informacionit dhe komunikimit janë pjesë e domosdoshme e jetës moderne. Integrimi i ICT-së në kryerjen e aktiviteteve dhe detyrave të përditshme është bërë gjithnjë e më shumë i pranishëm. Në këtë drejtim, kërcënimet ndaj informacionit dhe infrastrukturës së komunikimit që mund të rrezikojnë disponueshmërinë, privatësinë dhe integritetin e këtij sistemi, mund të ndikojë gjithashtu edhe në funksionimin e shoqërisë si një e tërë. Ekzistojnë mjete të shumta të ICT-së që mund të përdoren gjatë fazave të ndryshme për të luftuar korrupsionin, duke përfshirë parandalimin, zbulimin, analizën dhe masat korrigjuese.

ICT-ja nuk është një 'zgjidhje e artë' kur është fjala për garantimin e transparencës më të madhe dhe korrupsionit më të ulët apo për forcimin e demokracisë.

- ICT-ja mund të lehtësojë shkëmbimin e informacionit dhe mobilizimin shoqëror, dhe në fund të fundit të ofrojë platforma dixhitale ku qytetarët mund të raportojnë incidentet në mënyrë anonime.
- ICT-ja mund të lehtësojë punën e organizatave të shoqërisë civile që punojnë për një transparencë më të madhe dhe kundër korrupsionit, duke mbështetur një numër metodash të fushatës për transparencën dhe edukimin e qytetarëve për njohjen e korrupsionit dhe të drejtat e tyre civile.
- ICT-ja mund të përmirësojë transparencën në sektorin publik duke rritur koordinimin, shpërndarjen dhe kapacitetet administrative të sektorit publik, si dhe përmirësimin e ofrimit të shërbimeve nëpërmjet përdorimit të sistemeve administrative të përshtatshme për përdoruesit.

ICT-ja mundet gjithashtu të ndërhyjë edhe në mënyrë më të drejtpërdrejtë. Nëpërmjet përdorimit të proceseve të automatizuara është e mundur të ulen ndjeshëm mundësitë për korrupsion duke hequr agjentët njerëzorë nga mbledhja e të dhënave dhe nga pikat e ofrimit të shërbimeve – p.sh, kur njerëzit i realizojnë shërbimet nëpërmjet bankave elektronike (bankingu elektronik), nuk ka asnjë zyrtar të cilit t'i ofrojnë ryshfet për shërbimin e ofruar.

Më poshtë po paraqesim disa nga llojet e korrupsionit për të cilat ICT-ja mund të japë ndihmë në parim për t'i luftuar:

- Automatizimi: heqja e agjentëve njerëzorë nga shërbimet, dhe si pasojë edhe mundësitë për korrupsion nga operacionet që kryhen.
- Transparenca: eliminimi i mundësive për zgjedhje/ liri veprimi.
- Zbulimi në operacionet e kryera: veprimet e detajuara dhe të përgjithshme të operacioneve që kryhen mund të monitorohen për të zbuluar anomalitë dhe rezultatet e papritura.
- Zbulimi parandalues: rrjetet sociale online dhe individët mund të monitorohen për të zbuluar përgatitjet për veprime korruptive
- Rritja e vetëdijes: nëse publiku është i mirëinformuar me rregullat dhe procedurat e qeverisë, ai është më i aftë për t'i rezistuar trajtimit arbitrar.
- Raportimi: mobilizimi i përdoruesve/komunitetit për raportimin e rasteve do të lehtësojë marrjen e veprimeve korrigjuese ndaj individëve dhe riorganizimin e sistemit për të shmangur "defektet".
- Frenimi: publikimi i informacionit në lidhje me rastet e raportuara të korrupsionit, si dhe treguesit (si psh, mungesa e ekuilibrit midis të ardhurave dhe pasurisë) do të distancojë nëpunësit civilë nga përfshirja në veprime korruptive.
- Promovimi i qëndrimeve etike: angazhimi i publikut në ndjekjen e diskutimeve në forume të ndryshme në internet

Është shumë e rëndësishme që të vendoset një procedurë e sigurisë të të dhënave për të shmangur ndonjë problem në fushën e abuzimit me IT-në. Është gjithashtu e nevojshme për përcaktimin e disa masave mbrojtëse kundër keqpërdorimit të teknologjisë IT për qëllime të kryerjes së një akti korrupsioni.

Kuadri legjislativ

Dokumentet ligjore që janë në themel të bazës së funksionimit për përmirësimin e mëtejshëm të konceptit modern të sigurisë së informacionit në Mal të Zi janë:

- **Ligji për Masat e Sigurisë së Informacionit** (Fletorja Zyrtare e Republikës së Malit të Zi, nr. 14/10) paraqet zbatimin e masave dhe standardeve për sigurinë e informacionit, duke përfshirë edhe gjendjen e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave. Ky ligj zbatohet ndaj autoriteteve shtetërore, organet e qeverisjes qendrore, organet e qeverisjes vendore, personat juridikë dhe individët të cilët kanë akses në përdorimin ose përpunimin e të dhënave. Ky ligj nuk zbatohet për informacionin që ofron siguri të informacionit sipas rregullave që rregullojnë konfidencialitetin e të dhënave;
- **Ligji për Nënshkrimet Elektronike** ("Fletorja Zyrtare e Republikës së Malit të Zi", nr. 55/03 dhe "Fletorja Zyrtare e Malit të Zi", nr. 41/10) rregullojnë përdorimin e nënshkrimeve elektronike në procedurat ligjore, administrative, gjyqësore dhe të tjera, si dhe të drejtat, detyrat dhe përgjegjësitë e personave fizikë dhe juridikë në lidhje me çertifikatat elektronike, përveç në rastet kur janë parashikuar ndryshe me rregullore përkatëse;

- **Ligji për Dokumentet Elektronike** rregullon mënyrën e përdorimit të dokumenteve elektronike në procedurat ligjore, administrative, gjyqësore dhe të tjera, si dhe të drejtat, detyrat dhe përgjegjësitë e kompanive, sipërmarrësve, personave juridikë dhe fizikë, organeve qeveritare, organeve shtetërore, organeve, agjencive dhe organizatave të pushtetit vendor që ushtrojnë autoritet publik në lidhje me dokumentet elektronike;
- **Akti i Informacionit të Klasifikuar** - kuadri ligjor mbi procedurat e sigurisë për shkëmbimin e informacionit të klasifikuar është në fuqi dhe përfshin Ligjin për Klasifikimin e Informacioneve dhe Kodin Penal, Rregulloren për mënyrën dhe caktimin e procedurës së klasifikimit të informacionit, si dhe Rregulloren për dëshmitë e informacionit të klasifikuar;
- **Ligji për Ratifikimin e Konventës mbi Krimin Kibernetik** - Mali i Zi miratoi Ligjin për Ratifikimin e Konventës për Krimin Kibernetik më 3 mars 2010, e cila hyri në fuqi në datën 1 korrik 2010. Veprat penale të përfshira në këtë Konventë si krime kibernetike përfshijnë një gamë të gjerë të përhapjes së viruseve, aksesin e paautorizuar në një rrjet kompjuterik nëpërmjet piraterisë, me pornografinë dhe ndërhyrjet në sistemet bankare, abuzimin me kartat e kreditit dhe të gjitha veprat e tjera penale ku përdoren kompjuterët.

Dokumente të tjera të rëndësishme që duhet të përmenden:

- Studimi me përgjegjësitë e përcaktuara për autoritetet shtetërore në luftën kundër krimit kibernetik, duke përfshirë vlerësimin e gjendjes shtetërore dhe gatishmërisë në fushën e sigurisë kibernetike;
- Rregullorja me kushtet e detajuara dhe mënyrën e zbatimit të masave të IT për mbrojtjen e informacionit të klasifikuar;
- Rregullorja me kushtet e detajuara dhe mënyrën e zbatimit të masave për mbrojtjen e informacionit të klasifikuar;
- Rregullorja me kushtet e detajuara dhe mënyrën e kryerjes së masave industriale për mbrojtjen e informacionit të klasifikuar;
- Rregullorja me përmbushjen dhe përmbajtjen e kontrollit të brendshëm mbi zbatimin e masave për mbrojtjen e informacionit të klasifikuar.

Kontrollet e Sigurisë

Duhet të vendosen kontrolle të sigurisë në lidhje me korrupsionin nëpërmjet IT-së. “Kontrollet e sigurisë së informacionit janë masat mbrojtëse teknike, të procesit dhe politikave të projektuara, me synim për të mbrojtur të dhënat sensitive duke zbutur rreziqet e identifikuara dhe të vlerësuara ndaj fshehtësisë, integritetit, dhe disponueshmërisë së tyre”[84]. Në Ministrinë për Shoqërinë e Informacionit dhe Telekomunikacionet ka një drejtori për infrastrukturën e informacionit, e cila ka tre sektorë: Njësia e Analizës së Projektit, Njësia e Planifikimit dhe Monitorimit, Njësia e Shërbimeve të Infrastrukturësdhe Njësia

84 http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Controls-and-Safe- guards.pdf

e Mbrojtjes nga Incidentet Kompjuterike dhe të Sigurisë në Internet (CIRT). Objektivat kryesore të njësisë CIRT janë:

Parandalimi, trajtimi dhe eliminimi i pasojave të incidenteve të sigurisë kompjuterike mbi rreziqet në Internet dhe në sistemet e tjera të informacionit të sigurisë:

- Parandalimi është pasqyruar në mënyrë proaktive të veprimit, i cili përfshin dhënien e informacionit dhe vlerësimin e sigurisë së informacionit, testimin e cenueshmërisë, mbledhjen, regjistrimin dhe përpunimin e të dhënave për incidentet, testimin dhe zbatimin e sistemeve të reja softuer dhe harduer për mbrojtjen e burimeve të IT-së;
- Përpunimi i të dhënave dhe eliminimi i pasojave përfshin: përcaktimin e ndodhjes dhe shkallës së incidentit, shkakun e incidentit, ndërmjetësimin në komunikimin midis të gjitha palëve të përfshira në incident, raportimine ekipeve të tjera CERT/ CIRT/ CSIRT, përgatitjen e raporteve dhe paralajmërimet për përdoruesit e tjerë, duke eliminuar dobësitë e sistemit dhe mbrojtur sistemet ndaj incidenteve të mundshme dhe analizave tekniko-ligjore.

Arsimimi i përdoruesve në fushën e sigurisë së informacionit përfshin:

- Përgatitja e botimeve, manualeve, informacioneve mbi mekanizmat e softuerit dhe informacioneve të tjera të dobishme në lidhje me përdorimin e sigurt të teknologjisë së informacionit në portalin në internet (www.cirt.me);
- Organizimi i kurseve dhe trajnimeve mbi çështje të sigurisë së IT-së dhe mjetet e mundshme të mbrojtjes dhe parandalimit të incidenteve të sigurisë kompjuterike.

Ministria për Shoqërinë e Informacionit dhe Telekomunikacionet ka përgatitur disa rregullore:

- Rregullore për masat dhe procedurat për mbrojtjen e çertifikatave dhe të dhënave që lidhen me nënshkruesit. Kjo Rregullore rregullon masat organizative dhe teknike për mbrojtjen e një sistemi të çertifikimit në lidhje me mbrojtjen e çertifikatave të zakonshme dhe të kualifikuara, të dhëna që lidhen me nënshkruesit, si dhe me instalimin dhe aplikimin e sistemit për mbrojtjen e aksesit të të dhënave të çertifikatave;
- Rregullore për standardet e sigurisë së informacionit, e cila përcakton standardet e sigurisë së informacionit që aplikohet për zbatimin e masave të sigurisë të informacionit të përcaktuara nga rregullorja e Qeverisë së Malit të Zi;
- Rregullore për Menaxhimin e Incidenteve të Sigurisë së Informacionit - CIRT zhvillon dhe mirëmban një plan për reagimin ndaj incidenteve të sigurisë së informacionit, i cili pasqyrohet në përcaktimin e procedurave përkatëse për menaxhimin e incidenteve;
- Rregullore për përmbajtjen dhe mënyrën e mbajtjes së shënimeve dhe të regjistrit të ofruesve të shërbimeve të çertifikimit. Ky dokument rregullon përmbajtjen dhe mënyrën e mbajtjes së shënimeve të ofruesve të shërbimeve të çertifikimit, mënyrën e mbajtjes së regjistrit të ofruesve të shërbimeve të çertifikimit të akreditуar; si dhe madhësinë minimale të sigurisë ndaj rrezikut të përgjegjësisë për dëmet që mund të ndodhin gjatë punës së shërbimeve të çertifikimit;
- Rregullore për nënshkrimin elektronik dhe masat mbrojtëse të nënshkrimit elektronik të avancuar. Kjo Rregullore rregullon nënshkrimin elektronik dhe masat mbrojtëse për nënshkrimin elektronik të avancuar, masat për verifikimin e identitetit të nënshkruesit

nga ana e vetë nënshkruesit apo nga ofruesi i shërbimeve të çertifikimit në Mal të Zi, procedurat teknike dhe teknologjike për krijimin e nënshkrimit elektronik të avancuar dhe kërkesat që duhet të përmbushin pajisjet e krijimit të nënshkrimit elektronik të avancuar;
- Rregullore për mënyrën dhe kushtet për aksesin administrativ në portalin elektronik të Qeverisë së Malit të Zi;
- Rregullore për përdorimin e burimeve të informimit dhe komunikimit në rrjetin e organeve shtetërore;

Deklarata e Praktikës së Çertifikimit - CPS.

Siguria e informacionit duhet gjithashtu të përmbushë kushtet e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave. Siguria e informacionit fokusohet në të dhënat, pavarësisht nga forma e saj: elektronike, të printuara apo forma të tjera të të dhënave.

Për shkak të rritjes së vazhdueshme të numrit të shërbimeve që ofrohen nga autoritetet shtetërore dhe subjektet e sektorit privat për qytetarët dhe subjektet e tjera juridike, është e nevojshme të përcaktohet një infrastrukturë kritike e informacionit në Mal të Zi dhe të zhvillohen procedurat e mbrojtjes.

Aktivitetet kryesore:
- Përcaktimi dhe mbrojtja e infrastrukturës kritike të informacionit;
- Forcimi i qëndrueshmërisë së sistemeve të informacionit ndaj incidenteve;
- Kryerja e analizave të kërcënimeve ndaj infrastrukturës së IT-së.

Mbrojtja e të dhënave

Në Ministrinë për Shoqërinë e Informacionit dhe Telekomunikacionet është ngritur një Ekip i Reagimit ndaj Incidenteve Kompjuterike/Ekip i Reagimit ndaj Incidenteve të Sigurisë Kompjuterike-CERT/CSIRT (drejtori për mbrojtjen kundër incidenteve kompjuterike dhe sigurisë në internet). Është nënshkruar marrëveshje administrative midis Ministrisë së Shoqërisë së Informacionit dhe Telekomunikacioneve dhe Unionit Ndërkombëtar të Telekomunikacioneve për marrjen e asistencës së specializuar teknike për nevojat e institucionit të Ekipit të Reagimit ndaj Incidenteve Kompjuterike-CIRT (Ekip kombëtar për përpunimin dhe mbrojtjen nga incidentet kompjuterike), i cili do të veprojë në bashkëpunim me rrjetin CIRT që është krijuar nga Partneriteti Ndërkombëtar Shumëpalësh kundër Kërcënimeve Kibernetike (IMPACT).

Nëpërmjet sistemit të mbikëqyrjes inspektuese, është mbështetur zbatimi i Ligjit për Sigurinë e Informacionit dhe Rregulloren mbi Masat për Sigurinë e Informacionit, i cili kontribuon në rritjen e nivelit të mbrojtjes së të dhënave.

Kontribues parësor për CIRT.ME janë përcaktuar:
- Të gjitha institucionet qeveritare në Malin e Zi;
- Infrastruktura kryesore kombëtare në Malin e Zi.

CIRT-i malazez është ngritur në pajtim me Ligjin për Sigurinë e Informacionit të Malit të Zi, në kuadër të Ministrisë së Shoqërisë së Informacionit dhe Telekomunikacioneve (MIST). E formuar si një njësi e veçantë organizative e Ministrisë, e cila vepron në përbërje të Departamentit të Infrastrukturës së IT-së dhe do të mbulojë zonën e CIRT-it kombëtar. CIRT është i angazhuar në trajtimin e incidenteve të sigurisë të informacionit, nëse njëra palë e përfshirë në një incident është në Mal të Zi (nëse i takon domenit ".me" ose nëse është brenda hapësirës së adresës IP malazeze).

Misioni i CIRT-it

- CIRT-i koordinon dhe ndihmon agjencitë qeveritare në zbatimin e shërbimeve pro-aktive për të ulur rrezikun e incidenteve të sigurisë kompjuterike, si dhe për të re-aguar ndaj incidenteve të tilla kur ato ndodhin;
- CIRT.ME kryen fushata ndërgjegjësimi, me synimin për të edukuar popullatën lokale për efektet negative të kërcënimeve dhe krimit kibernetik.

Brenda administratës duhet të ketë një hierarki organizative të përcaktuar për të qenë ofruesja më efektive dhe me qëndrueshmëri afatgjatë e menaxhimit të duhur të informacionit të sigurisë.

Edhe pse ekziston një mungesë e të dhënave të besueshme, ka të paktën disa prova që ICT-ja mund të jetë një mjet efektiv për të luftuar korrupsionin. Megjithatë, potenciali i ICT-së mund të realizohet vetëm kur kombinohet me reforma reale administrative.

Masat mbrojtëse teknike

Këto janë kontrollet e harduerëve dhe softuerëve për të mbrojtur LAN dhe WAN nga aksesi i paautorizuar ose keqpërdorimi, për të ndihmuar në zbulimin e abuzimeve dhe shkeljet e sigurisë, dhe për të ofruar siguri për aplikimet LAN. Masat mbrojtëse teknike përfshijnë identifikimin e përdoruesit dhe autenticitetin e tij, kontrollin e autorizimit dhe aksesit, kontrollet e integritetit, mekanizmat e gjurmës së auditimit, kontrollet e konfidencialitetit, dhe kontrollet parandaluese të mirëmbajtjes së harduerit.

Fjalëkalimet janë një metodë kryesore të përdorura për të kontrolluar aksesin tek burimet dhe janë mekanizmat më të zakonshëm të autenticitetit[85]. Ministria e Shoqërisë së Informacionit dhe Telekomunikacioneve (MIST) është përgjegjëse për administrimin e rrjetit qeveritar. MIST-i ofron monitorimin dhe administrimin e rrjetit: funksioneve të operacioneve të IT-së i është dhënë përgjegjësia për të garantuar që lidhjet e komunikimit janë të

85 books.google.de/books?isbn=0080558712

mirëmbajtura dhe t'u ofrojnë përdoruesve nivelin e miratuar të aksesit në rrjet. Ekziston një politikë në lidhje me fjalëkalimet për të gjithë rrjetin qeveritar, e cila përcakton metodën e realizimit të fjalëkalimit të ri çdo muaj.

Identifikimi i kontrollit

Sfida për çdo organizatë është përcaktimi i grupimit të nevojshëm të kontrolleve të sigurisë, të cilat nëse zbatohen dhe vlerësohen se janë efektive në zbatimin e tyre, do të jenë në përputhje me kërkesat e caktuara të sigurisë duke çuar në zbutjen e ndikimit apo mundësisë së çdo kërcënimi të identifikuar. Për çdo kategori të sigurisë, bëhet i nevojshëm realizimi i një numri kontrollesh për të arritur një kuadër të plotë dhe të fuqishëm të sigurisë.

Përdorimi i kodifikimit për të mbrojtur të dhënat e përdoruesit nga burimi në destinacion, e cila quhet kodim i plotë, është një mjet i fuqishëm për të ofruar sigurinë e rrjetit.

Ministria e Shoqërisë së Informacionit dhe Telekomunikacionit e Qeverisë së Malit të Zi (MIST) menaxhoi çelësat publikë të infrastrukturës (GOV.ME-PKI) për qëllime të brendshme të administratës publike në Malin e Zi. Pranë MIST-së është krijuar një organ çertifikimi me një Autoriteti Unik Çertifikimi, i cili çertifikon nëpunësit civilë të Ministrisë së Shoqërisë së Informacionit dhe personelin e Qeverisë së Malit të Zi. Ky sistem është zbatuar plotësisht në përputhje me legjislacionin përkatës, kryesisht Ligjin për Nënshkrimin Elektronik.

Aktualisht janë përgatitur plane për fillimin e përdorimit të çertifikatave dixhitale për kryerjen e logimit/regjistrimit në çdo Kompjuter Personal (PC) në qeveri, por çështja e mungesës së fondeve është ende një pengesë për zbatimin e një mase të tillë.

Transferimi i të dhënave

Transferimi i të dhënave sensitive, qoftë përmes FTP-së, sistem-me-sistem ose dërgimit në formë elektronike (rrjeti i internetit) duhet të kryhet vetëm nëpërmjet një mënyre apo mediumi të besueshëm me kontrolle për të garantuar konfidencialitetin, integritetin dhe vërtetësinë e përmbajtjes së tyre. Të gjitha lidhjet e një sistemi të brendshëm apo baze të dhënash me sistemet e tjera jashtë kufirit të akreditimit duhet të autorizohen vetëm nëpërmjet përdorimit të marrëveshjeve për lidhjet e sistemeve, dhe lidhjet duhet të monitorohen dhe kontrollohen mbi baza të vazhdueshme.

Është e nevojshme që të përdoren kodifikim dhe protokolle të fuqishme të sigurisë për të ruajtur të dhënat gjatë transmetimit mbi rrjetet e hapura publike. Transferimi i të dhënave personale nga palët e jashtme për organizatën, zakonisht nëpërmjet një faqeje interneti, duhet të realizohet nëpërmjet serverëve të sigurt duke përdorur një nivel të lartë kodifikimi.

Aktualisht, transferimi apo shkëmbimi i të dhënave kryhet përmes shërbimeve të sigurta të internetit për qëllime të sistemeve të specializuara të IT-së. Lidhja ofrohet nëpërmjet një rrjeti të sigurt, dhe kodohet me certifikata dixhitale.

Sistemi i specializuar për shkëmbimin e të dhënave ende mbetet një sfidë për Malin e Zi. Aktualisht ne po përgatisim një projekt të quajtur "Enterprise Service Bus", i cili do t'u mundësojë institucioneve qeveritare të shkëmbejnë të dhëna të sigurta ndërmjet tyre. Megjithatë, mungesa e fondeve mbetet edhe këtu një problem për zbatimin e këtij projekti.

Aksesi në distancë

Përkufizimi për aksesin në distancë nënkupton çdo akses tek një burim informacioni organizativ nga një përdorues apo sistem komunikimi nëpërmjet një rrjeti ose lidhjeje të jashtme, të cilat nuk janë nën kontrollin e organizatës. Organizata mund ta çmojë të nevojshëm sigurimin e një aksesi në distancë për të dhënat dhe sistemet për punonjësit që punojnë në largësi të mëdha ose për mbështetjen e operacioneve që kryhen në vende të largëta. Në disa raste, aksesi në distancë është i nevojshëm në mënyrë periodike edhe nga shitësit për kryerjen e mbështetjes së rregullt ose të sistemit në rast emergjencash.

Në Qeverinë e Malit të Zi vetëm zëvendësministrat dhe ministrat mund të kenë akses në distancë në kompjuterin e tyre në rrjetin GOV.

Në Mal të Zi, 88.3% e kompanive të anketuara kanë deklaruar se ata kanë përdorur kompjuterët në operacionet e kryera prej tyre gjatë muajit janar 2012. Sipas rezultateve të anketës, në janar 2012 një sasi prej 53.3% e kompanive (që përdorën kompjuterët në operacionet e tyre) u mundësuan punonjësve të tyre akses në distancë në sistemet e postës elektronike (e-mail), dokumentet ose aplikimet e kompanisë.

Si rezultat i rritjes së rreziqeve që lidhen me akseset nga jashtë perimetrit të besuar, organizata duhet të zbatojë politika dhe procese që rregullojnë kushtet në të cilat jepet apo merret aksesi në distancë. Aksesi në distancë duhet të jepet në bazë të nevojave të autorizuara të biznesit, të jetë i kufizuar tek privilegjet minimale të nevojshme, të kërkojë miratimin e drejtuesve të autorizuar, si dhe të gjitha miratimet duhet të rishikohen dhe justifikohen herë pas here në mënyrë periodike.

Në Mal të Zi, vetëm 27.9% e kompanive kanë Rregulloren që rregullon çështjet normative të sigurisë së informacionit. Ekziston edhe një përqindje shumë e vogël e kompanive, vetëm 26.9%, të cilat kryejnë vlerësimin e njohurive të punonjësve rreth masave të sigurisë së informacionit.

Zhvillimi i koordinuar i kapaciteteve organizative, institucionale dhe menaxhuese, duke përmirësuar ligjet dhe rregulloret, janë objekte të rëndësishme për forcimin e gjendjes së sigurisë së informacionit në Mal të Zi.

2.8 Serbia

Nga Nemanja Nenadiç dhe Bojan Cvetkoviç

Masat mbrojtëse në shembujt serbë

Serbia, rasti 1: Seks në Arenën e Beogradit

Sipas udhëzimeve të Komisionerit për Informimin e Rëndësisë Publike dhe Mbrojtjen e të Dhënave Personale, Ministria e Punëve të Brendshme (MoI) vuri në zbatim masa afatshkurtra, afatmesme dhe afatgjata për mbrojtjen kundër korrupsionit që kishin lidhje me IT-në.

Masat mbrojtëse afatshkurtra kundër korrupsionit të IT-së përfshinin:

- Masa mbrojtëse teknike;
  - Çdo lloj i aksesit teknik i çdo lloji të sistemit të IT-së duhet të mbahet shënim për auditim dhe rishikim të mëvonshëm;
  - U prezantuan kartat universale/kryesore për të kufizuar aksesin në objektet e ruajtjes së të dhënave;
- Masa mbrojtëse organizative dhe procedurale;
  - Aksesi në të dhënat duhet të shoqërohet me procedura me shkrim që përcaktojnë se çfarë të dhëna mund të aksesohen, si dhe autorizimi i aksesit;
  - Numri i punonjësve me akses të drejtpërdrejtë në të dhënat operative është ulur në minimumin e nevojshëm për operacionet normale;
  - Përdorimi i medias elektronike të lëvizshme brenda objekteve ku ruhen të dhënat është tashmë i kufizuar rreptësisht dhe shoqërohet me procedurat specifike të aksesit në të dhënat apo është ndaluar tërësisht (në varësi të llojit të objektit);
- Masa mbrojtëse të monitorimit;
  - Vendosja e sistemeve të veçanta të mbikëqyrjes me video që monitorojnë drejtpërdrejt aksesin në nënsistemet e IT-së për ruajtjen e të dhënave të instaluara.

Masat mbrojtëse afatmesme kundër korrupsionit në IT përfshinin:

- Masa mbrojtëse për trajnimin dhe ndërgjegjësimin;
  - Trajnimi i punonjësve të MoI-së lidhur me rreziqet e korrupsionit në IT;
- Auditimin e sistemeve të IT-së;
  - MoI-ja ka bërë planet për të prezantuar një auditim të brendshëm të IT-së, si dhe standardizimin sipas ISO 27001 në të ardhmen e afërt.

Masat mbrojtëse afatgjata kundër korrupsionit të IT-së përfshinin:

- Masa mbrojtëse legjislative;
  - U përditësuan rregulloret e brendshme administrative, duke vlerësuar se aksesi i paautorizuar tek të dhënat deri tani të përcaktuara vetëm si shkelje disiplinore, të konsiderohet edhe si vepër penale;
  - U përmirësuan rregulloret e brendshme administrative, duke përfshirë qëndrimin specifik brenda MoI-së që përdorimi i të dhënave për ndonjë qëllim tjetër ndryshe nga ai fillestar për të cilin të dhënat janë mbledhur, të konsiderohet tashmë si vepër penale (jo vetëm disiplinore);
  - Rregulloret e brendshme administrative për sa i përket procedurave për përdorimin dhe zbatimin e llojeve të veçanta të mediave elektronike të lëvizshme (si disqe optikë, karta memorie, telefon smartphone, kamera dixhitale etj.) u përditësuan për të kufizuar apo ndaluar përdorimin e tyre në vende të MoI-së në varësi të llojit të të dhënave që mund të shpërdorohen;
  - Neni 42, paragrafi 3 i Kushtetutës shprehimisht ndalon dhe dënon përdorimin e të dhënave personale përtej qëllimeve për të cilat janë mbledhur.

Serbia, rasti 2: Kur një kontraktues IT-je "zë rrënjë"

Sipas një rasti real, Ministria e Drejtësisë ekspozoi vartësinë e saj ndaj kontraktuesve të IT-së, duke zbuluar disa lloje të ndryshme të rreziqeve që lidheshin me kontraktuesin e IT-së. Masat mbrojtëse që kishin filluar përfshinin masa afatshkurtra, afatmesme dhe afatgjata për të ulur në mënyrë të konsiderueshme rreziqet e IT-së që lidheshin me kontraktuesin.

Masat mbrojtëse afatshkurtra kundër korrupsionit të IT-së përfshinin:

- Masa mbrojtëse teknike;
  - Çdo lloj i aksesit teknik në çdo lloj të sistemit të IT-së duhet të mbahet shënim;
  - U prezantuan sistemet e sigurimit fizik si një masë për të kufizuar dhe kontrolluar aksesin në të dhënat e qendrës së Ministrisë së Drejtësisë, e cila i ruan të gjitha të dhënat në mënyrë të centralizuar;
- Masa mbrojtëse organizative dhe procedurale;
  - Aksesi tek të dhënat duhet të shoqërohet me kërkesën zyrtare dhe miratimin (lejen) nga gjykata përkatëse (ose prokurori) për të hyrë në të dhënat e një rasti/rasteve të veçantë/a;
  - Askush, madje as niveli më i lartë i nëpunësve të Ministrisë së Drejtësisë, nuk ka akses tek të dhënat pa miratimin paraprak (lejen) nga gjykata ose (prokuroria);
  - Çdo gjykatë (ose zyrë prokurorie) mund të ketë akses vetëm tek të dhënat e tyre – aksesi tek të dhënat që u përkasin subjekteve të tjera është i ndaluar;
  - Punonjësit e kontraktuesit të IT-së nuk mund të hyjnë në qendrën kryesore të të dhënave dhe as në vetë të dhënat, pa qenë të shoqëruar me një numër minimal prej dy punonjësish të ministrisë;
  - Numri i të punësuarve me akses të drejtpërdrejtë tek të dhënat operative është ulur në minimumin e nevojshëm për operacionet normale;
  - Çdo lloj përmirësimi apo përditësimi i sistemeve të IT-së duhet të bëhet brenda qendrës kryesore të të dhënave – asnjë akses në distancë nuk lejohet për askënd;

- Përdorimi i medias elektronike të lëvizshme brenda objekteve ku ruhen të dhënat është i ndaluar plotësisht;
- Masa mbrojtëse të monitorimit;
  - Është instaluar një sistem i veçantë i mbikëqyrjes video që monitoron drejtpërdrejt aksesin në qendrën kryesore ku ruhen të gjitha të dhënat.

Masat mbrojtëse afatmesme kundër korrupsionit të IT-së përfshinin:

- Masa mbrojtëse të trajnimit dhe ndërgjegjësimit;
  - Trajnimi i punonjësve të Ministrisë së Drejtësisë në lidhje me rreziqet e korrupsionit të IT-së;
- Auditimi i sistemeve të IT-së;
  - Ministria e Drejtësisë ka prezantuar tashmë një auditim të jashtëm të IT-së;
  - Ministria e Drejtësisë ka plane për të zbatuar standardizimin sipas ISO 27001 dhe ISO 20000 në të ardhmen e afërt.

Masat mbrojtëse afatgjata kundër korrupsionit të IT-së përfshinin:

- Masa mbrojtëse legjislative;
  - U përditësuan rregulloret e brendshme administrative, duke përfshirë një ndalim të aksesit të paautorizuar tek të dhënat në Ministrinë e Drejtësisë;
  - U përditësuan rregulloret e brendshme administrative, duke përfshirë që aksesi tek të dhënat të kryhet në përputhje me "ndarjen e pushteteve" midis ministrisë, gjykatave, prokurorisë dhe burgjeve;
  - Rregulloret e brendshme administrative për procedurat për përdorimin dhe zbatimin e llojeve të veçanta të mediave elektronike të lëvizshme (si disqe optike, karta memorie, telefonë smartphone, kamera dixhitale etj.) u përditësuan në mënyrë që të ndalohet përdorimi i tyre në mjediset e qendrës kryesore të dhënave të Ministrisë së Drejtësisë;
  - Ligji për Prokurimin Publik ("Fletorja Zyrtare e Republikës së Serbisë", nr. 124/12).

Serbia, rasti 3: Një funksionar publik i nivelit të lartë përgjon punonjësit

Nuk dihet se çfarë masa janë ndërmarrë për të mbyllur boshllëkun në Agjencinë e Privatizimit në lidhje me parandalimin e abuzimit të IT-së, pasi rasti i paraqitur ka treguar qartë dobësinë e faktorit njerëzor në Agjencinë e Privatizimit që ishte pika kyçe dhe kryesore e keqpërdorimit të IT-së.

Serbia, rasti 4: "Mafia e Rrugës"

Siç shpjegohet në gjykimin e "Mafias së Rrugës", masat mbrojtëse nga korrupsioni i IT-së nuk funksionuan për një kohë të gjatë. Anëtarët e bandës janë informuar me kohë për kontrollet, kështu që ata kishin kohë të mjaftueshme për të fshehur provat e krimit. Kontrollet u kryen zakonisht pas orës 18:00 kur banda nuk vepronte. Për më tepër, pavarësisht nga fakti se dosja e EMU-87 ishte e rremë dhe e ndryshme nga ajo origjinale, e vërteta mbeti e panjohur për vite me radhë. Meqë sistemi elektronik për pagesat dhe regjistrimin e automjeteve po funksiononte "normalisht", asnjë kontroll nuk e identifikoi këtë ndërprerje. Punonjësi nga kompania e cila menaxhonte sistemin elektronik "Rrugët e Serbisë" kishte kompetenca administrative, dhe duket se askush nga "Rrugët e Serbisë" nuk e mbikëqyrte punën e tyre.

Sistemi për regjistrimin e mbledhësve individualë të taksave me ID-në e tyre unike nuk funksionoi në praktikë. Numrat e ID-së ishin të dukshëm për kolegët dhe menaxherët e turneve kryen zëvendësime të shpeshta të punonjësve.

Masat mbrojtëse afatshkurtra ndaj korrupsionit të IT-së përfshinin:

- Masa mbrojtëse teknike
  - U instalua një sistem plotësues por i veçantë, me bazë sensorësh IT-je, me synimin e gjurmimit të llojeve dhe sasisë së mjeteve që kalonin traun e kalimit të makinave (tashmë statistikat nga sistemi origjinal duhet të përputhen me sistemin e ri të bazuar në sensorë)
  - U prezantuan sistemet e sigurimit fizik si një masë për të kufizuar dhe kontrolluar aksesin në objektet që ruajnë të dhënat e përdoruesit.

Nuk kemi asnjë informacion nëse janë marrë masa dhe nëse po, çfarë lloj masash organizative, mbrojtëse, procedurale si dhe të monitorimit janë marrë.

Nuk kemi asnjë informacion nëse janë marrë masa dhe nëse po, çfarë lloj masash mbrojtëse afatmesme kundër korrupsionit në IT janë marrë.

Masat mbrojtëse afatgjata kundër korrupsionit në IT përfshinin prezantimin e një lloji të ri të shërbimit të pagesës të taksës të quajtur "ENP" (në anglisht, "Pagesë Elektronike e Kalimit të Makinave") që bazohet tërësisht në pagesën elektronike nëpërmjet kartave NFC për të shmangur transferimet e drejtpërdrejta të parave në dorë ndërmjet palëve të përfshira në taksa.

Publikimi proaktiv i informacionit - mjet për të parandaluar korrupsionin nëpërmjet IT-së

Ligji serb për Aksesin e Lirë në Informacion ("Fletorja Zyrtare e Republikës së Serbisë", Nr. 120/04, 54/07, 104/09 dhe 36/10) parashikon botimin e detyrueshëm të një "Broshure të Informacionit" për të gjitha institucionet publike (të financuar nga buxheti), një dokument

përmbajtja e të cilit përcaktohet nëpërmjet 'Udhëzimit të Komisionerit" (udhëzimet e fundit janë lëshuar në vitin 2010)[86]. Broshura Informative duhet të publikohet në internet dhe të përditësohet të paktën çdo muaj. Ky publikim synon të japë një informacion të plotë e të dobishëm për të garantuar përgjegjshmërinë e organeve qeveritare si prokurimi publik, buxheti, donacionet dhe të dhënat e ndihmës shtetërore. Informacione të tjera lidhen me strukturën e organeve qeveritare apo shërbimet që ofrojnë për qytetarët. Megjithatë, për këtë analizë pjesët më interesante janë dispozitat e neneve 37, 38 dhe 39.

Neni 37 merret me "ruajtjen e mbartësve të informacionit". Mbartësit e informacionit janë pajisjet e medias ku ruhen të dhënat si dokumentet, hard-disqet, bazat e të dhënave, videokasetat etj. Një autoritet publik duhet të identifikojë llojet e ndryshme të këtyre mediave të përdorura për ruajtjen e informacionit, sipas llojit, sasisë (me saktësi apo përafërsi), si dhe llojin e të dhënave që ato ruajnë. Për më tepër, autoritetet duhet të identifikojnë ku ruhen "mbartësit e informacionit" (njësi organizative apo fusha të veçanta brenda autoritetit, të tilla si arkivat, bibliotekat dhe bazat e të dhënave elektronike) dhe vendet e ruajtjes brenda këtyre objekteve (p.sh. rafte metalike, rafte me dosje, serverë të përbashkët ose pajisje kompjuterike individuale). Autoritetet publike duhet të përshkruajnë shkurtimisht sesi mbahen dhe mirëmbahen në praktikë mbartësit e informacionit (nëse është kryer regjistrimi i sigurtë i të dhënave në një tjetër mbartës, nëse kompjuterët janë mbrojtur nga viruset, nëse dikush tjetër përveç punonjësve ka akses tek mbartësi i informacionit, nëse ka një rishikim periodik të pajtueshmërisë me kërkesat për ruajtjen e mbartësve të informacionit etj.) dhe nëse kushtet e ruajtjes janë në përputhje me rregulloret ose me nevojën për t'i ruajtur ato, nëse nuk ka rregullore të tilla.

Nenet 38 dhe 39 detyrojnë autoritetet publike për botim të detyrueshëm të informacionit në lidhje me llojet e informacionit që zotërojnë dhe llojet e të dhënave për të cilat mund të jepet akses. Si shembull, llojet e informacionit mund të jenë si vijon (të renditura sipas Udhëzimeve),:

- Koleksioni i rregulloreve
- Opinionet e nxjerra
- Procesverbalet e mbledhjeve
- Vendimet
- Ankesat
- Kontratat e lidhura
- Video-klipet me zë dhe figurë nga veprimtaritë e organizuara nga autoriteti shtetëror
- Letrat e qytetarëve
- Lloje të ndryshme të komunikimit me publikun
- Dokumentet mbi pagesat, punonjësit, prokurimin publik
- Draftet e dokumenteve në proces përgatitor
- Të dhënat zyrtare
- Kërkesat dhe aplikimet e klientëve etj

86 http://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/uputstvo- informator/uputstvoen.doc

Informacioni në lidhje me disponueshmërinë e të dhënave duhet të jepet pasi të jetë bërë i mundur një krahasim me listën e llojeve të disponueshme të informacionit. Nëse informacioni është i saktë dhe i plotë, publiku mund të konsiderojë autoritetet të përgjegjshëm dhe kjo mund të parandalojë, ndër të tjera, situata ku nëpunësit civilë pretendojnë që një informacion i tillë nuk zotërohet nga autoriteti ose që ai informacion ka humbur etj. Në të vërtetë, shumica e autoriteteve nuk përputhen dhe nuk japin hollësisht as informacion mbi mbartësit e të dhënave dhe as informacione mbi llojet e të dhënave. Kjo situatë pritet të ndryshojë shumë shpejt me ndryshimet e pritshme në Ligjin për Aksesin e Lirë në Informacion, i cili do t'i bëjë procedurat e mbikëqyrjes dhe sanksionet më efikase.

Veprat penale ekzistojnë, zbatimi i panjohur

Kodi Penal i Republikës së Serbisë (Fletorja Zyrtare e Republikës së Serbisë, nr. 85/2005, 88/2005, 107/2005), me amendamentet e shtuara nga 31 gushti dhe 29 dhjetori 2009, dhe 24 dhjetori 2012, parashikon sanksione në kapitullin XXVII për veprat penale ndaj sigurisë së të dhënave kompjuterike.

Vepra e parë penale brenda këtij grupi është "*dëmtimi i të dhënave dhe programeve kompjuterike*" (Neni 298). Një person mund të dënohet me gjobë ose me burgim deri në një vit, nëse ai/ajo "*pa autorizim fshin, ndryshon, dëmton, fsheh ose ndryshe bën të papërdorshme të dhënat ose programet kompjuterike*". Në rastet kur dëmet janë më të larta, kjo mund të çojë në burgim deri në pesë vjet. Po ashtu, pajisjet dhe mjetet e përdorura për kryerjen e veprës penale do të konfiskohen.

"*Sabotazhi Kompjuterik*" (neni 299) parashikon dënim deri në pesë vjet burgim, për cilindo person që:

"*Hyn, shkatërron, fshin, ndryshon, dëmton, fsheh ose ndryshe bën të papërdorshëm një kompjuter ose program, ose kur dëmton ose shkatërron një kompjuter ose pajisje të tjera për përpunimin elektronik dhe transferimin e të dhënave, me qëllim të parandalimit ose të prishjes së konsiderueshme të përpunimit elektronik dhe transferimit të të dhënave me rëndësi për autoritetet qeveritare, ndërmarrjeve apo subjekteve të tjera*".

"*Krijimi dhe futja e viruseve kompjuterike" (neni 300) parashikon një dënim deri në gjashtë muaj burgim për "cilindo që prodhon një virus kompjuterime qëllim për ta futur atë në kompjuterin e një tjetri ose në rrjetin e kompjuterëve të një tjetri". Nëse shkelësi "fut një virus kompjuterik në kompjuterin e një tjetri apo në rrjetin e kompjuterëve të një tjetri duke shkaktuar dëme me këtë veprim*", dënimi do të jetë deri në dy vjet burgim. Pajisjet dhe mjetet e përdorura për kryerjen e veprës konfiskohen.

"*Mashtrimi kompjuterik*" (neni 301) është parashikuar në mënyrën e mëposhtme:

"*Kushdo që fut të dhëna të pasakta, nuk arrin të fusë të dhëna të sakta, ose ndryshe fsheh ose në mënyrë të gabuar paraqet të dhëna të cilat ndikojnë në rezultatet e përpunimit elektronik dhe transferimin e të dhënave, dhe që ka synimin për të marrë përfitim të paligjshëm material për veten e tij ose për dikë tjetër, duke i shkaktuar në këtë mënyrë dëme materiale një personi tjetër, dënohet me gjobë ose me burgim deri në tre vjet*."

Për procedura më të vlefshme të krimit ose të dëmit të shkaktuar, dënimi mund të jetë deri në dhjetë vjet burgim.

"*Aksesi i paautorizuar në kompjutera" dhe "në rrjetin kompjuterik ose në përpunimin e të dhënave elektronike*" (neni 302), mund të dënohet deri në tre vjet burgim, në varësi të dëmit të shkaktuar.

Parandalimi ose kufizimi i aksesit në një rrjet kompjuterik publik (neni 303) dënohet deri në tre vjet.

"*Përdorimi i paautorizuar i kompjuterit ose rrjetit kompjuterik*" (neni 304) përcakton se:

"*Kushdo që përdor shërbimet kompjuterike ose rrjetin kompjuterik me synimin për të nxjerrë fitime të kundërligjshme për vete ose për dikë tjetër, dënohet me gjobë ose me burgim deri në tre muaj. Ndjekja ligjore për këtë vepër të caktuar fillohet përmes një padie private.*"

Amendamenti i fundit nga ky grup ka lidhje me: "*Prodhimin, prokurimin, dhe ofrimin për të tjerët si mjet për kryerjen e veprave penale kundër sigurisë së të dhënave kompjuterike*" (neni 304a), i cili shprehet si vijon:

"*Kushdo që zotëron, prodhon, prokuron, shet ose u jep të tjerëve për përdorim kompjuterët, sistemet kompjuterike, të dhënat e tyre kompjuterike ose programet e destinuara për kryerjen e njërës prej veprave penale të përmendura në nenet 298 deri 303 të këtij ligji, dënohet me burgim nga gjashtë muaj deri tre vjet. Produktet e veprave penale të përmendura në paragrafin 1 të këtij ligji konfiskohen*. "

Serbia ka një numër të madh të veprave penale që mund të përdoren për të ndëshkuar korrupsionin (shpërdorim të pushtetit, marrje e ryshfetit, dhënie e ryshfetit, influencim në tregti etj), veprat penale që janë pothuajse tërësisht në përputhje me standardet përkatëse ndërkombëtare. Ndonjë mund të nxjerrë përfundimin e gabuar se sistemi i të drejtës penale për të luftuar korrupsionin në IT është i efektshëm. Megjithatë, vështirë se kjo është e vërtetë. Numri i përgjithshëm i rasteve kur korrupsioni (IT ose të tjera) të jetë hetuar dhe finalizuar plotësisht është ende mjaft i ulët, dhe veçanërisht në rastet kur në të përfshihen zyrtarë të lartë publikë apo sasi të mëdha të parave, është edhe më i rrallë. Situata nuk është më pozitive kur është fjala për hetimin e krimit që ka lidhje me IT-në në përgjithësi. Serbia ka pasur një njësi të veçantë të prokurorisë për të luftuar krimin kibernetik në internet për vite me radhë. Kjo njësi, e cila është në fuqi që nga viti 2006, ende ka një faqe interneti "në ndërtim e sipër" dhe statistikat më të fundit i ka ato të tre vjetëve më parë[87].

Mësimet e nxjerra – Masat mbrojtëse kundër ushtrimit të korrupsionit nëpërmjet përdorimit të ICT-së në sektorin publik në Ballkanin Perëndimor

Nga LouiseThomas

Garancitë/masat mbrojtëse individuale të renditura në hyrje dhe të përshkruara në këtë kapitull, theksojnë faktin se një garanci nuk mund të qëndrojë kurrë vetëm. Mbrojtja kundër korrupsionit nëpërmjet ICT-së kërkon që të ekzistojnë të gjitha masat mbrojtëse pasi ato mbështesin dhe plotësojnë njëra-tjetrën. Qeverisja elektronike nuk është kurrë një çështje thjesht teknike. Qeverisja elektronike nuk ka të bëjë vetëm me teknologjinë. Ajo ka të bëjë gjithashtu me administratën publike dhe mënyrën sesi i bëjmë gjërat, si bashkëpunojmë brenda qeverisë, administratës publike, komunitetit, ekonomisë dhe shoqërisë si një e tërë. Qeverisja elektronike nuk duhet të konsiderohet si e izoluar dhe e pavarur nga pjesa tjetër e shoqërisë.

Lufta kundër korrupsionit po bëhet prioritet për vendet e Ballkanit Perëndimor në rrjetin e ReSPA-s. Disa autorë kombëtarë vënë në dukje mënyrën se si rastet e marra si shembull theksojnë nevojën për ndërgjegjësim në rritje për çështje të veçanta që lidhen me korrupsionin dhe qeverisjen elektronike, megjithatë fokusi dhe masat ndryshojnë. Në Shqipëri, qeveria e re shqiptare ka përditësuar axhendën e saj të luftës kundër korrupsionit dhe ka prezantuar kohët e fundit një procedurë të re për pranimet në sistemin e informacionit. Në Bosnjë dhe Hercegovinë raportet kombëtare dhe të brendshme pohojnë se korrupsioni është ndër problemet më të mëdha në shoqëri dhe progres raporti i Komisionit Evropian 2013 për vendin thekson mungesën e strategjisë dhe institucioneve për të luftuar krimin kibernetik dhe kërcënimet. Në Kosovë autorët kombëtarë vërejnë se nuk ka institucione, cilatdo qofshin, që merren me hartimin dhe zbatimin e mbrojtjes dhe standardeve të ICT-së dhe se shumë raste të abuzimit me ICT-në janë plotësisht të pazbulueshme, ndërsa autorët kombëtarë serbë vërejnë se numri i përgjithshëm i rasteve ku korrupsioni (me ose pa ICT) hetohet plotësisht është mjaft i ulët, veçanërisht rastet që përfshijnë zyrtarë të lartë apo sasi të mëdha të parave. Edhe pse Serbia ka pasur një njësi të veçantë në prokurori që nga viti 2006 për të luftuar krimin kibernetik, kjo njësi nuk ka siguruar shumë informacion.

Autorët malazezë vërejnë se ndërgjegjësimi nga korrupsioni është rritur dhe është bërë një prioritet i rëndësishëm në axhendën politike në vend dhe jo vetëm për qeverisjen e tanishme. Në Ministrinë për Shoqërinë e Informacionit dhe Telekomunikacionit të Malit

87 http://www.beograd.vtk.jt.rs/

të Zi ndodhet një drejtori për infrastrukturën e informacionit me tre sektorë: Analiza e projektit, Njësia e Planifikimit dhe Monitorimit; Njësia për Shërbimet e Infrastrukturës dhe Mbrojtjes; dhe CIRT (Ekipi i Reagimit në raste Incidentesh Kompjuterike). Autorët malazezë kanë theksuar gjithashtu disa studime dhe rregullore për luftën kundër krimit kibernetik dhe mbrojtjen e informacionit. Në Malin e Zi, lufta kundër korrupsionit është një nga qëllimet më të rëndësishme strategjike për qeverisjen. Përveç kësaj, malazezët organizojnë gjithashtu fushata të ndërgjegjësimit publik, trajnimin e punonjësve dhe qytetarëve mbi mënyrat lidhur me parandalimin e korrupsionit, informojnë mbi mundësitë në dispozicion për veprim ligjor, si edhe ofrojnë angazhim të qeverisë në Strategjinë e Reformës së Administratës Publike dhe Planin e Veprimit. Në Kroaci ekziston një organ i legjislacionit për sigurinë e informacionit, si dhe autoritete të veçanta shtetërore qendrore të ngarkuara për mbrojtjen e "integritetit dhe disponueshmërisë së sistemit të informacionit në procesin e planifikimit, projektimit, përgatitjes, përdorimit dhe ndërprerjes së punës të sistemit të informacionit".

Nuk mund të bëjmë një krahasim të drejtpërdrejtë midis vendeve, për të përcaktuar se sa larg janë vendet në luftën kundër korrupsionit nëpmjet ICT-së, pasi nuk kemi të dhëna statistikore që të na mbështesin. Megjithatë, nga kontributet e autorëve kombëtare paraprakisht mund të bëjmë dallimin ndërmjet përpjekjeve kombëtare dhe duket se Kroacia, Maqedonia dhe Mali i Zi janë më të zellshme në mbrojtjen nga abuzimi dhe korrupsioni të përdorimit të ICT-së në sektorin publik sesa vendet e tjera pjesëmarrëse në këtë studim.

Mbrojtja teknike – aksesi tek të dhënat

ICT-ja në sektorin publik mund të mundësojë rritjen e transparencës në lidhje me faktin se kush ka akses dhe kush përdor të dhënat e sektorit publik. Sidoqoftë, gjithashtu mund të mundësojë abuzim shumë më të gjerë se sa është e mundur pa ICT, të tilla si falsifikimi, marrja e paligjshme dhe shkatërrimi i të dhënave.

Sërish, na lejoni të theksojmë se shembujt e rasteve tona nuk përbëjnë një shembull përfaqësimi por në Tabelën 3 tregohen më shumë raste të falsifikimit të të dhënave sesa marrja e paligjshme e të dhënave dhe rastet më të pakta lidhen me shkatërrimin aktual të të dhënave.

Tabela 3 Shembuj të rasteve të abuzimit të mundësuara nga aksesi tek të dhënat

Falsifikovanje podataka	Nezakonito pribavljanje podataka	Uništavanje podataka
Bosnja dhe Hercegovina, rasti 3: Keqpërdorimi i sistemit elektronik të projektit CIPS	Kroacia, rasti 1: Telefonata e doktorit për vota	Bosnja dhe Hercegovina, rasti 2: Një punësim tjetër i diskutueshëm në Institucionin e Lartë të Auditimit të Republikës Srpska
Kroacia, rasti 8: Çdo vit zhduken 2 milion euro nga kabinat e taksës së autostradës	Kroacia, rasti 11: Inspektori i lartë përdori të dhëna konfidenciale për të fituar zgjedhjet lokale	Kroacia, rasti 6: Oficerë policie që fshijnë kundravajtjet në trafik dhe zbulojnë të dhëna konfidenciale (bile ata pranuan si rryshfet edhe mish qingji të pjekur dhe 20 litra verë!)
Kroacia, rasti 12: Nuk keni kaluar asnjë ditë të jetës suaj në punë? Nuk ka problem, përsëri mund të marrësh pension të plotë!	Kroacia, rasti 2: Të dhënat konfidenciale të radio-televizionit kroat në tregun e zi	Kroacia, rasti 8: Çdo vit zhduken 2 milion euro nga kabinat e taksës së autostradës
Kosova, rasti 1: Zhdukja e provave	Kroacia, rasti 3: Në kërkim të veteranëve	Kosova, rasti 1: Zhdukja e provave
Kosova, rasti 2: Marrja e statusit të invalidit të luftës	Kroacia, rasti 4: Me një ndihmë të vogël të nëpunësve civilë,68 pasaporta kroate iu shitën kriminelëve	
Kosova, rasti 4: Falsifikimi i dokumenteve tatimore	Kroacia, rasti 6: Oficerë policie që fshijnë kundravajtjet në trafik dhe zbulojnë të dhëna konfidenciale (bile ata pranuan si rryshfet edhe mish qingji të pjekur dhe 20 litra verë!)	
Maqedonia, rasti 1: Abuzimi i sistemeve të IT-së në tarifat autostradale	Kroacia, rasti 7: I kapur rastësisht për zbulim të të dhënave konfidenciale për automjetet dhe pronarët e tyre!	
Maqedonia, rasti 3: Abuzimi nëpërmjet sistemit të IT-së dhe zbulimi i kundërligjshëm i të dhënave personale	Mali i Zi, rasti 2: Përdorimi i të dhënave të IT-së për të shkaktuar dëm politik	
Maqedonia, rasti 4: Keqpërdorimi i sistemit të regjistrimit të orëve të punës	Maqedonia, rasti 3: Abuzimi nëpërmjet sistemit të IT-së dhe zbulimi i kundërligjshëm i të dhënave personale	
Mali i Zi, rasti 1: Shpërdorimi i detyrës dhe falsifikimi i dokumenteve zyrtare	Serbia, rasti 1: Seks në Arenën e Beogradit	
Mali i Zi, rasti 2: Përdorimi i të dhënave të IT-së për të shkaktuar dëm politik		
Mali i Zi, rasti 3: Keqërdorimi i funksioneve dhe futja e të dhënave të pasakta në regjistrat publikë		
Mali i Zi, rasti 4: Lëshimi i paligjshëm i dokumenteve të udhëtimit		
Serbia, rasti 4: "Mafia e rrugës"		

Mbrojtja e aksesit tek të dhënat bëhet çështje kryesore dhe përfshin jo vetëm kontrollin e aksesit por edhe përdorimin e niveleve të duhura të aksesit.

Kontrolli i aksesit - fjalëkalime dhe menaxhimi i ID-së së përdoruesit

Kontrolli dhe kufizimet për të hyrë në sistem kryhen përmes caktimit të identifikimit dhe fjalëkalimeve të përdoruesit. Shumica e sistemeve që shkëmbejnë të dhëna apo kanë më shumë se një përdorues, kanë një lloj kontrolli në akses, ID të përdoruesit dhe skemë të fjalëkalimit. Në sistemet e pavarura, të dhënat dhe programet kompjuterike duhet të sigurohen nga kontrolli në akses tek kompjuteri. Mund të duket e vetëkuptueshme se aksesi duhet të jetë i kufizuar për përdoruesit e autorizuar, por nuk ndodh gjithmonë kështu.

Në shembullin e rastit 4 në Serbi (mafia e rrugës), sistemi për regjistrimin e mbledhësve të taksave individuale me ID unike të tyre nuk ka funksionuar në praktikë. Numrat e ID-së ishin të dukshme për kolegët dhe menaxherët e turnit zëvendësonin shpesh punonjësit.

Në rastin 5 në Maqedoni (shpërdorimi i të drejtave të administratorit - garancive bankare/kuotave të importit), një punonjës me të drejta administratori zbuloi se kishte mbajtur privilegje aksesi pas transferimit të tij nga një qendër administrative në një tjetër. Ai më pas krijoi një llogari të rremë të përdoruesit dhe e përdori për të ndryshuar përkohësisht të dhënat e garancisë bankare dhe në bashkëpunim me një kompani lokale kishin kryer mashtrime në kufi. Super Administratori nuk kishte kontrolluar dhe rishikuar rregullisht privilegjet e administratorëve të caktuar dhe në këtë mënyrë administratori mund të kryente vepra penale duke përdorur një llogari përdoruesi të sapokrijuar. Në raste të tjera, keqpërdorimi apo vjedhja e fjalëkalimeve të tilla si në rastin 3 në Kosovë (keqpërdorimi i fjalëkalimit), rasti 1 në Bosnjë dhe Hercegovinë (hakeri më i famshëm boshnjak ndërmjet prokurorëve) dhe rasti 2 në Shqipëri (korrupsioni në Sistemin Elektronik të Prokurimeve Publike) krijon mundësi për korrupsion. Pavarësisht se sistemi i prokurimit elektronik që përdoret në Shqipëri dukej se zbatonte të gjitha masat e nevojshme, sistemi i postës elektronike që përdoret për të mbështetur sistemin e prokurimit ka shkatërruar të gjitha qëllimet e mira, sikurse u zbulua kur vlerësimi i prokurimit u krye nga një person i tretë, pas një ndryshimi të fjalëkalimit. Në fakt, të gjithë përdoruesit i dinin fjalëkalimet e njëri-tjetrit. Edhe pse kjo praktikë është zbatuar me qëllimet e mira për të zgjidhur çështjet e punës, ajo ka ulur sigurinë e sistemit në përgjithësi.

ID-të dhe fjalëkalimet e përdoruesit duhet të jenë gjithmonë personale dhe konfidenciale. Situatat që mund të fillojnë si një mënyrë e përshtatshme për të bërë çdo ditë jetën e punës të menaxhueshme, të tilla si: dhënia e fjalëkalimeve për kolegët apo vartësit për zgjidhjen e menjëhershme të detyrës, ose rivendosja e fjalëkalimeve në një vlerë të paracaktuar të njohur nga të tjerët dhe në këtë mënyrë nuk janë më sekrete, mund të keqpërdoren, siç tregohet në shembujt e mësipërm. Nëse është e nevojshme të delegohet akses tek sistemet dhe të dhënat për një koleg, sistemet duhet ta lejojnë këtë por në mënyrë të tillë që: 1) Punëmarrësi të përdorë kartën e tij/të saj personale të Internetit kur futet në sistem; 2)Dosjet mbahen për akses në sistemin e të dhënave; dhe 3) Garantohet vetëm akses i kufizuar dhe i synuar dhe kjo mund të skadojë.

Nivel i përshtatshëm aksesi tek të dhënat dhe sistemet

Disa raste theksojnë në mënyrë të qartë se çfarë mund të ndodhë kur nivelet e aksesit tek të dhënat janë të papërshtatshme, që do të thotë dhënie e aksesit më të gjerë tek sistemet dhe të dhënat se sa është e nevojshme për kryerjen e menjëhershme të detyrave të punëtorëve. Në rastin 5 në Maqedoni (abuzimi i të drejtave të administratorit (garanci bankare/kuotat e importit) dhe rasti 3 në Mali të Zi (keqpërdorimi i funksioneve dhe hedhja e të dhënave të pasakta në regjistrat publikë), punëtorët kishin akses shumë më të gjerë për të ndryshuar ose futur të dhëna se sa ishte e domosdoshme për ta që të bënin punën e tyre. Në të dy rastet ata abuzuan me funksionet e tyre dhe mundësuan të paraqisnin të dhëna/dokumente që dukeshin të paligjshme për palë të jashtme.

Aksesi fizik tek të dhënat dhe dokumentet

Aksesi fizik tek objektet që ruajnë të dhënat apo kopjet fizike të të dhënave për verifikim, legjitimim etj duhet të kufizohet për personelin e autorizuar, aksesi i të cilit regjistrohet dhe monitorohet. Në rastin 2 në Kroaci (baza e të dhënave konfidenciale të radiotelevizionit kroat në tregun e zi) një kopje e të dhënave të tarifës së liçencës të radio-televizionit kroat (Regjistri HRT) është shitur në tregun e zi. Aksesi fizik në sallën e serverit që ruan regjistrin HRT i jepet ekskluzivisht personave të autorizuar, por aksesi në bazën e të dhënave mundësohet gjithashtu përmes një rrjeti lokal dhe internetit, duke përdorur tunelet e mbrojtura për të dhënat. Pavarësisht nëse baza e të dhënave ishte kopjuar direkt nga serveri në sallën e serverit apo nga një distancë, autorët kroatë vërejnë se nuk janë zbatuar standardet për të kufizuar aksesin fizik.

Në rastin 4 në Malin e Zi (lëshimi i paligjshëm i dokumenteve të udhëtimit) autorët shkruajnë se është e nevojshme të skanohet dokumenti ose të krijohet baza e të dhënave elektronike e të gjitha dokumenteve të dorëzuara dhe të lëshuara në kopje me opsionin për kontroll të dyfishtë të detyrueshëm, me qëllim për të garantuar sigurinë e të dhënave në rast të shkatërrimit të tyre të qëllimshëm apo aksidental. Gjithashtu, është e nevojshme të përmirësohet siguria e sistemit elektronik duke regjistruar aksesin fizik në ambientet ku mbahen dosjet dhe dokumentet zyrtare. Më i ndërlikuar është rasti 3 në Malin e Zi (shpërdorimi i funksioneve dhe hedhja e të dhënave të pasakta në regjistrat publikë), ku ekziston një kombinim i regjistrave të ndryshëm dhe regjistrave elektronik të tokës/truallit. Të njëjtat dokumente mund të kenë origjina të ndryshme dhe ndonjëherë është e pamundur të përcaktohet saktësisht se kush i ka krijuar dokumentet dhe kush ka akses të plotë tek këto dokumente. Në këtë mënyrë duhet që dokumentet të ruhen në formë elektronike, dhe aksesi si tek regjistrat fizikë edhe elektronikë të lejohet për personat e autorizuar.

Në rastin 1 në Serbi (seks në arenën e Beogradit), kartat kryesore nuk janë paraqitur për të kufizuar aksesin në objektet që ruajnë të dhënat. Përdorimi i mediave elektronike portative brenda objekteve që ruajnë të dhënat është rreptësishti kufizuar dhe shoqërohet me procedura specifike për akses tek të dhënat apo ndalohet plotësisht (në varësi të llojit të objektit). Në Malin e Zi, aksesi fizik tek sistemet, qoftë gjatë zbatimit apo mirëmbajtjes, kërkon autorizimin e Ministrisë së Punëve të Brendshme për çdo person të përfshirë.

Procedurat dhe standardet e sigurisë

Autorët boshnjakë, maqedonas, malazez dhe serbë i referohen zbatimit të standardit ISO 27001 mbi Menaxhimin e Sigurisë së Informacionit dhe Standardit të Menaxhimit të Cilësisë ISO 9001, si masa mbrojtëse konkrete të zbatuara si procedura sigurie për të garantuar sigurinë dhe integritetin e të dhënave. Në Bosnjë dhe Hercegovinë pushteti gjyqësor ka përmirësuar procedurat e sigurisë, të tilla si ato të përmendura në procedurat e sigurisë ISO 27001, në të gjitha nivelet dhe ka zbatuar standardin ISO/IEC 27001: 2005. Në Serbi, Ministria e Punëve të Brendshme dhe Ministria e Drejtësisë planifikojnë të prezantojnë ISO 27001 në të ardhmen e afërt. Në Mal të Zi zbatohet një rregullore për standardete sigurisë, e cila paraqetstandardet e sigurisë së informacionit që aplikohen për zbatimin e masave të sigurisë të informacionit, të përcaktuara nga rregullorja e qeverisë së Malit të Zi. Në Maqedoni ligji për Menaxhimin Elektronik përshkruan standardet që duhet të përmbushen kur zhvillohen sistemet e ICT-së që komunikojnë, shkëmbejnë të dhëna dhe dokumente në administratën publike. Në aktin nënligjor janë paraqitur udhëzimet e mëvonshme mbi kryerjen e kontrolleve nga seria ISO 27001.

Kopjet rezervë dhe skedarët regjistrues (logfile)

Skedarët regjistrues (logfile) sigurojnë se një sistem mund të kontrollohet më vonë për të përcaktuar saktësisht se kush dhe kur e bëri. E njëjta gjë vlen edhe për dosjet në kopje rezervë, pasi kopjet rezervë regjistrojnë mënyrën se si duken të dhënat në një moment të caktuar.

Në rastin 1 në Kosovë (shkatërrimi i provave) lista e të gjithë hetuesve materialë në serverët e Ministrisë së Administratës Publike dhe që do të provonin dyshimet e Agjencisë kundër Korrupsionit lidhur me parregullsi dhe shkelje të ligjit, është fshirë nga serverët e qeverisë.Më e vështirë në këtë rast është se për të gjithë administratat publike në Kosovë, serverët që ruajnë të dhënat e të gjithë institucioneve qeveritare janë të vendosur brenda kësaj Ministrie. Këto të dhëna janë fshirë nga sistemi që konsiderohet se është mjedisi më i mirë i mbrojtur për të dhënat në Kosovë.

Në rastin 4 në Maqedoni (keqpërdorimi i sistemit të regjistrimit të orëve të punës) hetimi mbi skedarët regjistrues (logfile) u konsiderua si proces tepër i rëndësishëm për zbulimin e abuzimit. Autorët maqedonas vërejnë se janë krijuar disa praktika sipas ligjit përkatës por disa praktika janë vendosur pa pasur një bazë formale në ligje dhe akte nënligjore.

Ndër këto praktika është mbajtja e logos për çdo akses, plotësimi, fshirja ose redaktimi i të dhënave dhe vendosja e skedarëve regjistrues (logfile) në dispozicion sipas kërkesës, për qëllim të rishikimit dhe auditimit. Përveç mbajtjes dhe arkivimit të logeve, nuk lejohet asnjë operacion tjetër. Së fundi është rasti i IDDEEA (Agjencia për Identifikimin e Dokumenteve, Regjistrat dhe Shkëmbimin e të Dhënave) në Bosnjë dhe Hercegovinë, përgjegjëse për krijimin e shkëmbimit të të dhënave elektronike ndërmjet autoriteteve të policisë dhe prokurorëve, e cila filloi një aktivitet që krijoi gjenerimin e ri të shkëmbimit të të dhënave në Bosnjë dhe Hercegovinë. Ndër këto kërkesa është kopja rezervë e të dhënave në distancë të largët me mbrojtje të mirë të fjalëkalimit të kombinuar me sigurinë fizike.

Ndërveprimi midis sistemeve të organeve publike të ICT-së dhe krijimi i regjistrave bazë

Ndërveprimi është termi që përdoret për të përshkruar aftësinë e sistemeve të organizatave të ndryshme të cilat punojnë së bashku (ndërveprojnë). Që sistemet të jenë të ndërveprueshme duhet të shkëmbejnë të dhëna. Pengesat për shkëmbimin e të dhënave përfshijnë zakonisht pengesa teknike, semantike, organizative dhe ligjore por një komponent shtesë mund të jetë besimi i shtuar. Për të shfaqur të dhënat e një organizate tek një tjetër organizatë, duhet të ekzistojë një nivel besimi midis palëve në shkëmbim, ndryshe përvoja na tregon se bashkëpunimi do të pushojë shpejt së ekzistuari. Garantimi i integritetit dhe ruajtja e të dhënave ndaj abuzimit është shumë e rëndësishme për ndërveprime dhe vendimtare për realizimin e qeverisjes elektronike, si mundësi për pakësimin e pengesave administrative përmes integrimit të mjeteve të qeverisjes elektronike. Përdorimi i mençur i informacionit që qytetarët dhe bizneset duhet tu japin autoriteteve publike për përfundim të procedurave administrative; kryerja e procedurave elektronike si kanal dominues për ofrimin e shërbimeve të qeverisjes elektronike; dhe parimi i regjistrimit “vetëm një herë” i të dhënave përkatëse. Ky i fundit garanton se qytetarët dhe bizneset japin informacion të caktuar standard vetëm njëherë sepse zyrat e administratës publike marrin masa për të shkëmbyer këto të dhëna, në mënyrë që asnjë pengesë të mos bjerë mbi qytetarët dhe bizneset.

Ruajtja e integritetit të regjistrave bazë të një vendi është shumë e rëndësishme. Regjistrat bazë janë blloqe themelore të ndërtimit të qeverisjes elektronike moderne brenda një vendi dhe gjithnjë e më shumë ndërmjet vendeve. Ato përbëhen nga baza e të dhënave kryesore që përmbajnë kategoritë më të fundit të çdo elementi që qeverisja dhe sektori publik kanë nevojë për tu bërë një administratë efikase, duke ofruar shërbime të mira (elektronike dhe jo elektronike) për qytetarët dhe bizneset, si dhe zhvillimin dhe zbatimin efektiv të politikave. Regjistrat bazë janë mishërim i parimit “vetëm një herë”. Regjistrat më tipikë mbajnë detajet e të gjithë qytetarëve, si lindje, martesë, vdekje, adresë, numër identifikimi të qytetarëve, pasaportë, kartë identiteti etj”, të të gjithë kompanive (madhësia, viti i themelimit, numri i të punësuarve, fusha e aktivitetit, taksat që duhen të paguhen dhe taksat që janë paguar, shpesh të lidhura edhe me regjistrat që tregojnë xhiron vjetore, fitiminetj). Regjistrat mbi tokën dhe ndërtimet janë gjithashtu të zakonshme, siç janë regjistrat lidhur me automjetet, mjetet e transportit, rrugët ujore etj. Regjistrat bazë

mund të eliminojnë përpjekjet e dyfishta nga autoritetet publike dhe uljen e mundësisë për gabime. Krijimi i regjistrave bazë dhe sistemi i ndërveprimit që nevojitet që ata të ndahen nga Ministritë dhe Agjencitë përkatëse, është një element kryesor i qeverisjes elektronike. Megjithatë, nëse sistemet ICT publike ngatërrohen apo nuk mbrohen ndaj abuzimit, pasojat mund të kenë ndikime të rënda ekonomike, shoqërore dhe ligjore për të gjithë, qofshin ato administratë publike, qytetarë, biznese, etj.

Në rastin 12 në Kroaci (nuk keni punuar asnjë ditë në jetën tuaj?) Nuk ka problem, ju sërish mund të merrni një pension të plotë!", integrimi i të dhënave dhe konsolidimi i regjistrit themeltar midis autoriteteve, duke përdorur një numër identifikues personal, kombëtar (numri i identifikimit të personit "OIB", rrjeti i këmbimit), arrin masën mbrojtëse të "parimit të pasjes shumë sy", dhe kështu ka zgjidhur problemet e përshkruara në rastin kur Instituti Kroat i Sigurimeve të Pensioneve (HZMO) është integruar në rrjetin e këmbimit OIB dhe u zhvillua kontrolli i të dhënave të pensionistëve. Rastet në kapitullin 1 përfshijnë edhe shembuj të përmbajtjes së regjistrave bazë, siç është rasti 3 në Bosnjë dhe Hercegovinë (keqpërdorimi i sistemit elektronik të projektit CIPS) dhe rasti 3 në Malin e Zi (shpërdorim i funksioneve dhe hedhja e të dhënave të pasakta në regjistrat publikë).

Në rastin e Bosnjës është vërejtur se që prej fillimit të Projektit për Sistemin e Mbrojtjes së Identifikimit të Shtetasve (CIPS) në vitin 2002 ka pasur një numër të ankesave, veçanërisht kur bëhej fjalë për lëshimin e kartave të identitetit dhe pasaportave personale në të gjithë vendin. Mënyra sesi një regjistër i tillë qendror është ngatërruar, është shumë e rëndësishme dhe autorët e Bosnjës vërejnë që edhe përmes Agjencisë për Dokumente Identifikimi, Regjistra dhe Shkëmbim të të Dhënave (IDDEEA) tani përgjegjëse për CIPS, kanë zbatuar një gamë të gjerë të masave mbrojtëse dhe në përputhje me standardet e një niveli shumë të lartë të sigurisë të ICT-së dhe ekziston ende problemi në lidhje me shkëmbimin e të dhënave me autoritetet e tjera, mungesa e marrëveshjeve institucionale për të koordinuar aktivitetet e qeverisjes elektronike dhe dështimi për të zbatuar udhëzimet IDDEEA në të gjithë administratën publike. Kjo situatë jo vetëm që zgjidh sistemin CIPS por edhe gatishmërinë e autoriteteve publike për të bërë sistemet e tyre të ndërveprueshme.

Rasti 3 në Malin e Zi lidhet me kadastrën komunale ku redaktimet e paligjshme të kadastrës mundësuan transferimin e paligjshëm të tokës shtetërore në kadastrën komunale tek një person i tretë. Rasti përfshiu prodhimin e një çertifikate të rremë elektronike që më vonë do të përdorej në një procedurë ligjore. Në këtë rast nuk përmenden mësimet e nxjerra dhe masat mbrojtëse shtesë të realizuara. Sidoqoftë, rasti ilustron se çfarë ndodh kur aksesi i monitorimit të punonjësit është i pamjaftueshëm dhe si mund të cenojë të gjithë regjistrimin.

Rasti 5 në Maqedoni (abuzimi i të drejtave të administratorit/garanci bankare, kuotat e importit) ilustron se çfarë ndodh kur një autoritet publik, zyrtarët e kufirit, varet/varen nga informacionet dhe të dhënat e një autoriteti tjetër si garanci e informacionit të palës së tretë (garanci bankare) dhe kur vlera e kufizuar nga garanci bankare aktuale prezantohet nga zyrtarët e administratës në vend të marrjes së drejtpërdrejtë nga sistemet e informacionit të bankave. Autorët nuk përmendin pasoja mbi bashkëpunimin ndërmjet autoriteteve publike të përfshira, por mund të pritet që të tregohet kujdes dhe të jepen kërkesa për integritetin e të dhënave.

Monitorimi dhe auditimi

Kopjet rezervë dhe skedarët regjistrues (logfile) janë ofruesit teknikë "të masave mbrojtëse të monitorimit dhe auditimit, por ka disa çështje të tjera të rëndësishme kur bëhet fjalë për nevoja për të monitoruar dhe kontrolluar sistemet e ICT-së.

Ndërmjet sistemeve dhe proceseve – hallka më e dobët

Disa raste nga kapitulli 1 ilustrojnë mënyrën sesi organizata duhet të mbrojë të gjithë proceset e saj, si dhe hapat individualë nga abuzimi elektronik dhe fizik. Edhe sistemet "e përsosura" e ICT-së janë vetëm të sigurta dhe të dhënat janë po aq të besueshme sa edhe kontributi i tyre. Në rast se në sistemet e ICT-së futen të dhëna të rreme, integriteti i të gjithë sistemit cënohet. Monitorimi dhe auditimi duhet të shtrihen tek të gjitha proceset dhe sistemet e biznesit, pavarësisht nëse ato janë fizike apo elektronike.

Në rastin e Shqipërisë 4 (përvetësimi i fondeve dhe mashtrimi në kontabilitet) një nëpunës përgjegjës për kontabilitetin përvetëson para duke falsifikuar pagat përmes marrjes së miratimit me shkrim (kopje fizike) dhe më pas ndryshon të dhënat elektronike për pagat dhe të dhënat që i janë dërguar bankës. Meqenëse nuk ka pasur auditim lidhur me përputhshmërinë mes kopjes fizike dhe të dhënave elektronike, lidhja e dobët është bërë mes këtyre dy "procedurave". Autorët shqiptarë përmendin gjithashtu mungesën e çeqeve nga sistemi financiar që nuk ka qenë i aftë të përpunojë njëkohësisht detajet individuale të pagave kundrejt shumës totale. Më tej, ka pasur një verifikim midis dokumenteve të ndryshme të nënshkruara për pagën mes autoriteteve financiare.

Në rastin 2 të Kosovës (Marrja e Statusit të Invalidit të Luftës), abuzimi është kryer gjatë skanimit, ku është falsifikuar raporti mjekësor. Autori F.M. kishte siguruar një dokument me të cilin ai paraqiste se gjatë luftës në Kosovë, kishte vuajtur nga probleme shëndetësore. Dokumenti nuk është i periudhës së luftës por është hartuar 5 vjet më vonë. Ai përmban data sikur të ishte hartuar gjatë luftës. Shembulli i një pasaporte të skaduar që është falsifikuar dhe përdorur nga një person i tretë në rastin 1 në Malin e Zi (abuzimi me detyrën dhe falsifikimi i dokumenteve zyrtare) tregon precedentin e dështimit të sistemit të informacionit në Ministrinë e Brendshme (MoI) për lëshimin e pasaportave, që duhet të eliminonterreziqet e përdorimit dhe të ri-lëshimit të dokumenteve të udhëtimit kur periudha e tyre e vlefshmërisë ka skaduar. Sistemi nuk lidhte dokumentin fizik (pasaportën) me një tregues të bazës së të dhënave të pasqyruara që përmbajnë informacionin e njëjtë të saktë, duke përfshirë foto të mbajtësit të pasaportës. Më tej, nuk ka pasur gjurmë elektronike brenda sistemit që identifikonte nëpunësit që lëshuan pasaportën e falsifikuar.

Cenueshmëria e sistemit në këtë shembull ishte inkoherenca midis pasaportave aktuale dhe atyre fizike dhe sistemit të MoI-së.

Në fund, rasti 4 i Kosovës (Falsifikimi i dokumenteve tatimore) ilustron çfarë ndodh kur askush nuk kontrollon për një dobësi ose hallkë të dobët. Në këtë rast, pronari i një kompanie që kontraktonte me institucione publike për shërbime pastrimi kishte përdorur "pushtetin" e tij bazuar në pasjen e marrëdhënieve të mira me zyrtarët tatimorë. Pas një pagese fillestare të një tatimi me vlerë të lartë, në të gjitha ofertat e ardhshme ai kishte pasur të njëjtën faturë por me data të falsifikuara. Të gjithë zyrtarët e institucioneve mund të kërkojnë dokumentin origjinal por ata ishin të pavendosur ta bënin këtë, meqenëse mendonin se kishin të bënin me një person të një niveli të caktuar dhe dhanë justifikimin se dokumenti i skanuar përmbushte kërkesat e tyre. Sidoqoftë, askush nuk kontrolloi dhe kështu kjo përbën dobësi. Këtu kemi të bëjmë me një rast ku zyrtarët mund të kenë mbrojtur procesin e prokurimit duke kërkuar dokumentin tatimor, por askush nuk e bëri një gjë të tillë.

Monitorimi dhe auditimi si dhe mbrojtja ligjore dhe procedurale duhet të zgjerohen dhe të vlejnë për të gjitha sistemet dhe proceset (elektronike dhe fizike) që përdoren nga institucioni publik.

Pengesat në nënkontraktim dhe rreziqet që lidhen me kontraktuesin e IT-së

Rasti 2 i Maqedonisë (Sulmi kundër sistemit të IT-së për prokurimin publik) përfaqëson një rast të rëndësishëm ku një sistem i prokurimit elektronik respekton të gjitha garancitë/mbrojtjet e mundshme teknike, por bëhet i cenueshëm nga një refuzim i shpërndarë i sulmit të shërbimit (DdoS) duke u ofruar në një mjedis të përbashkët me ISP. Megjithëse autoritetet maqedonase nuk kanë provuar abuzim me pozicionin zyrtar dhe korrupsion, çështja jep një vështrim të përgjithshëm të procedurës dhe metodave të mundshme të abuzimit të sistemeve IT për korrupsion, nëpërmjet abuzimit me pozicionin zyrtar ose mashtrimit virtual social. Administratori i sistemit ka privilegje të plota në sisteme gjatë një periudhe të zvarritur në kohë dhe në rast se aktivitetet e tij/e saj nuk kontrollohen dhe monitorohen siç duhet, ai/ajo mund të abuzojë me sistemin duke shkatërruar ose ndryshuar të dhënat dixhitale, duke e bërë të pamundur që rasti të hetohet rasti dhe abuzimi të provohet.

Rasti 2 i Serbisë (kur kontraktuesi i IT-së "zë rrënjë") përfaqëson rastin kur një kontraktues IT-je ka një kontakt të brendshëm që manipulon të dhënat dhe procedurat në favor të kontraktuesit duke zgjatur kontratën e favorshme të nënkontraktimit. Ligjet dhe rregulloret e prokurimit janë ndryshuar që prej asaj kohe në Serbi, por nëpunësi i pandershëm shfrytëzoi njohuritë e tij për sistemet dhe kërkesat për të favorizuar një kontraktues IT-je të veçantë ekzistues, me qëllim që të shkurtonte shpenzimet e kontraktuesit. Ai fshehu ose bëri të padisponueshme të dhëna në lidhje me aksesin e kontraktuesit të IT-së në sistemin VPN WAN dhe shkatërroi dokumentacionin elektronik brenda sistemit, në

mënyrë që institucioni publik (MoJPA dhe më vonë MoJ) të mos kontrollonin, monitoronin dhe mbikëqyrnin sistemin.

Në rastin shqiptar 3 (Korrupsioni nëpërmjet IT-së në Operatorin e Shpërndarjes së Energjisë Elektrike), kompania e operatorit të shpërndarjes së energjisë u privatizua në pjesën më të madhe të saj. Përmes një skeme mbifaturimi, leximeve false nga pajisjet matëse PDA të personelit dhe në raste të tjera dyshime lidhur me të dhëna elektronike që janë tjetërsuar në sistemin e IT-së të kompanisë pasi janë regjistruar nga PDA-të, fatura të energjisë elektrike të fryra në kurriz të konsumatorëve. PDA-të dhe procedurat për leximet e matësve të energjisë fillimisht nënkuptohej të siguronin një faturim të saktë, por aksesi i paautorizuar dhe falsifikimi i të dhënave, ndoshta (por ende jo e provuar) edhe me ndihmën e menaxhimit, shkatërron çdolloj besimi që publiku ka në procesin e leximit të drejtë të matësve.

Në fund, grumbullimi që i kemi bërë rasteve të korrupsionit përmes ICT-së përmban tre shembuj mashtrimi dhe përvetësimi në taksën e rrugës së kompanive, (rasti kroat 8, rasti maqedonas 1, dhe rasti serb 4[88]). Në rastin e mbledhjes së taksës rrugore në rastin e Kroacisë dhe Maqedonisë, ajoishte nënkontraktuar tek kompanitë private, ndërsa në Serbi kompania ishte tërësisht në pronësi të shtetit. Përmes skemave që variojnë nga mashtrimi i thjeshtë i një punonjësi në rastet e Maqedonisë dhe Kroacisë, deri tek një skemë e përpunuar dhe më e sofistikuar në shembullin serb, rreziku i mashtrimit dhe përvetësimit të parave është i pranishëm kur ekziston mbledhja e drejtpërdrejtë e tarifës dhe kur ekziston një monitorim i papërshtatshëm i nëpunësve. Në rastet e Kroacisë dhe Maqedonisë, abuzimi u zbulua përmes auditit të brendshëm. Në rastin e Serbisë, ishte një "informator" i brendshëm i cili zbuloi abuzimin. Në të tre rastet, mbrojtja e përforcuar teknike dhe monitorimi i nëpunësve është zbatuar më vonë.

Kur sistemet ICT janë nënkontraktuar, organet publike duhet në kontaktin e tyre me kontraktuesin IT të sigurojnë se janë në gjendje të monitorojnë dhe auditojnë sistemet jo thjesht në të njëjtën mënyrë që do ta bënin në rast se do të ishte sistem i brendshëm, por në një masë edhe më të madhe pasi nënkontraktimi nënkupton humbje të kontrollit ndaj sistemeve.

Masat mbrojtëse organizative dhe proceduriale

Në Shqipëri çdo subjekt qeveritar që rishikon ose ndërton një sistem informacioni duhet tashmë të sigurojë shqyrtimin e projektimit/dizajnit dhe të mos marrë asnjë kundërshtim ndaj termave të referencës nga ekspertët e Agjencisë Kombëtare për Shoqërinë e Informacionit. Më tej, kalimi i sistemit nga zhvilluesi kontraktues tek klienti i sektorit publik nëpërmjet një procedure "pranimi të sistemit të informacionit" që synon të sigurojë integritet dhe cilësi më të mirë të sistemeve të informacionit në sektorin publik. Në Bosnjë dhe

88 Kroacia, rasti 8 (çdo vit 2 milionë Euro zhduken nga kabinat për pagesat e tarifave rrugore), Maqedonia, rasti 1 (Abuzimi me Sistemin e IT-së për tarifat e pagesave) dhe Serbia, rasti 4 ("Mafia e Rrugës")

Hercegovinë, sistemet IT të policisë dhe personelit që punon në to u nënshtrohen tashmë kontrolleve të rregullta nga autoriteti kompetent. Në Kroaci, sipas Rregullores për Masat e Sigurisë së Informacionit, procedurat e planifikimit të emergjencës (zhvillimi i procedurave që duhen ndjekur në rast incidenti të sigurisë dhe vazhdimësia e menaxhimit të biznesit) janë përcaktuar tashmë. Autorët maqedonas kanë ndjekur një prirje të nënshkrimit të marrëveshjeve të konfidencialitetit ndërmjet operatorëve ekonomikë dhe zbatuesve, ku të dyja palët bien dakord të mos ekspozojnë informacionin tek personat me akses në sistem. Më tej, tashmë ekziston një praktikë e miratuar në institucionet maqedonase e ndarjes së roleve të administratorëve teknikë dhe administratorëve (të të dhënave) përmbajtjes. Administratorët teknikë janë përgjegjës për sistemin në nivel zbatimi dhe menaxhojnë përdoruesit dhe aksesojnë lejimet. Administratorët ekzistues për menaxhimin e të dhënave të ruajtura në bazat e të dhënave, por jo në menaxhimin e sistemeve nga vetë ata. Në Malin e Zi, Ministria për Shoqërinë e Informacionit dhe Telekomunikacionet ka hartuar disa broshura me rregulla për të siguruar standardet, mbrojtjen e të dhënave, menaxhimin e incidenteve, përmbajtjen dhe mënyrën e ruajtjes së të dhënave të çertifikimit të siguruesve të shërbimit, nënshkrimi elektronik, aksesi në portalin elektronik të qeverisë dhe përdorimi i rrjetit të brendshëm të organeve shtetërore. Përfundimisht në Serbi, qoftë Ministria e Brendshme, qoftë Ministria e Drejtësisë kanë zbatuar tashmë procedurat që rregullojnë aksesin tek të dhënat për mbrojtje kundër abuzimit. Më tej, në Ministrinë e Drejtësisë askush, madje edhe nëpunësit e niveleve të larta nuk kanë akses tek të dhënat pa miratimin paraprak nga gjykata ose prokuroria.

Mbrojtja nëpërmjet parimit "të shumë syve"

Disa shembuj nga kapitulli 1 tregojnë zbatimin "e thjeshtë" të parimit "të shumë syve". Për shembull, Kroacia rasti 5 (polici u kap ndërsa hidhte të dhëna të falsifikuara në sistemin e informacionit të policisë) ku shefi i rajonit të policisë e vuri re letrën e konfirmimit në sistemin e informacionit të Ministrisë së Brendshme, ose rasti maqedonas 4 (keqpërdorimi i sistemit të regjistrimit të orëve të punës) ku një ricaktim i detyrave nënkuptonte se një administrator i ri i hodhi një sy skedarëve regjistrues (logfile) nga sistemi i orëve të punës duke kryer në këtë mënyrë "parimin e shumë syve" duke audituar dhe zbuluar mospërputhjen.

Në rastin 12 të Kroacisë (Nuk keni kaluar asnjë ditë të jetës tuaj në punë? Nuk ka problem, ju ende mund të përfitoni një pension të plotë!), konsolidimi i të dhënave në regjistrin OIB (OIB-Numri i Identifikimit Personal) arrin zbatimin e "parimit të shumë syve". Ndërsa "shumë sy" mund të ishte arritur në rastin Kosova 4 (falsifikimi i dokumenteve tatimore) në rast se zyrtarët publikë në institucione të ndryshme kontraktuese qeveritare do të kishin këmbëngulur në verifikimin e saktësisë së dokumentit tatimor, abuzimi do të ishte zbuluar shumë më herët dhe procesi i prokurimit mund të ishte mbrojtur nëpërmjet "parimit të shumë syve". E njëjta mungesë kontrolli vlen për rastin Mali i Zi 3 (abuzimi i funksioneve dhe vendosja e të dhënave të pasakta në regjistrat publikë), ku modifikimeve në kadastrën bashkiake u mungonin garancitë/mbrojtjet organizative dhe procedurale, si për shembull "parimi i shumë syve". Asnjë kontroll nuk u krye lidhur me statusin e tokës dhe pronësisë, as teknikisht, as nga ndonjë punonjës tjetër në regjistrin bashkiak dhe as nga ndonjë audit i jashtëm.

Kodi i Etikës

Ndoshta si rezultat i rasteve kroate 9 dhe 10 lidhur me keqpërdorimin e sistemit IT nga oficeri i policisë dhe rasti kroat 11 (inspektori i lartë keqpërdori të dhënat konfidenciale për të fituar në zgjedhjet lokale!), "Kodi i Etikës" është "injektuar" tek zyrtarët publikë dhe nëpunësit në Ministrinë e Brendshme dhe Ministrinë e Financave janë të detyruar të veprojnë në përputhje me të. Po aq i rëndësishëm është fakti se qytetarët mund të raportojnë sjelljet joetike të nëpunësve civilë tek oficerët e etikës.

Të dhënat dhe qeverisja e hapur, lejojnë publikun të ndihmojë në mbrojtjen e integritetit dhe saktësisë së të dhënave

Autorët maqedonas përmendin qeverisjen e hapur dhe të dhënat e hapura si shembull i aktiviteteve antikorrupsion që u mundësojnë qytetarëve të luajnë rol aktiv në parandalimin dhe përcaktimin e korrupsionit. Si të tilla, parimi i 'shumë syve' përmes pjesëmarrjes së qytetarëve në shqyrtimin e hollësishëm të të dhënave, për shembull statusi përfundimtar dhe i pronësisë/pasurisë së zyrtarëve të lartë, mund të mundësohet me hapjen e të dhënave qeveritare. Ne e dimë nga studimi i mëparshëm i ReSPA-s i kryer në vitin 2012[89] se në atë kohë Kroacia, Serbia dhe Maqedonia po fillonin të zbatonin disa nisma lidhur me të dhënat e hapura.

Trajnimi, etika dhe ndërgjegjësimi për Integritetin

Shqipëria tashmë ka një nismë të vazhdueshme të ndërmarrë nga Agjencia Kombëtare për Sigurinë Kibernetike në bashkëpunim me Shkollën Shqiptare të Administratës Publike, duke organizuar kurse trajnimi për pothuajse të gjithë personelin e IT-së në institucionet publike. Trajnimi përfshin sigurinë e sistemit, mbrojtjen dhe vlerësimin e rrezikut. Në Bosnjë dhe Hercegovinë ka tashmë module trajnimi për prokurorët për shembull, për krimin kibernetik dhe aftësitë e komunikimit.

Në Kroaci, Rregullorja për Masat e Sigurisë së Informacionit përcakton ndërgjegjësimin për sigurinë, siç parashikohet në rregullat e sigurisë dhe ndërgjegjësimin e nëpunësve. Nëpunësit në Ministrinë e Brendshme marrin pjesë në trajnime të ndryshme dhe projekte për rritjen e ndërgjegjësimit lidhur me rreziqet e korrupsionit nëpërmjet ICT-së dhe mbrojtjen ndaj tij. Shembujt përfshijnë dy projekte që synojnë forcimin e kapaciteteve administrative të Ministrisë së Brendshme në luftën kundër krimit kibernetik dhe një projekt për

89 Studimi Krahasues Rajonal i Qeverisjes Elektronike ReSPA (2012), i vënë në dispozicion: http://respaweb.eu/download/doc/Regional+comparative+eGov+study+-+web.pdf/dfab3d5a78e0d10e9- a6a80827e36a277.pdf

Bashkëpunimin Rajonal në Drejtësinë Penale; forcimin e kapaciteteve në luftën kundër krimit kibernetik. Projekti përfshin gjithashtu seminare për rrjetet ligjore të zhvilluara nga Ministria e Brendshme dhe Akademia Kroate, si dhe Rrjeti i Studiuesve.

Në Serbi, Ministria e Drejtësisë dhe ajo e Brendshme trajnojnë tashmë nëpunësit e tyre lidhur me rreziqet e korrupsionit nëpërmjet ICT-së.

Në Maqedoni, Strategjia e Reformës së Administratës Publike dhe Plani i Veprimit përcaktojnë trajnimin dhe ndërgjegjësimin e nëpunësve civilë dhe qytetarëve ndaj korrupsionit. Mali i Zi ofron ndërgjegjësim të përdoruesit në fushën e sigurisë së informacionit dhe parandalimin e incidenteve të sigurisë kompjuterike.

Vetëm Kosova raporton se nuk ka ndërmarrë masa dhe plane për të ofruar trajnim dhe rritje ndërgjegjësimi për nëpunësit civilë lidhur me rreziqet dhe mbrojtjen ndaj korrupsionit nëpërmjet ICT-së.

"Informatorët"

Disa vepra penale korrupsioni do të diktohen vetëm nga burime të brendshme të cilët "informojnë" lidhur me gjendjen reale të çështjeve. Kjo është veçanërisht e vërtetë në rast se menaxhimi përfshihet në korrupsion. Rasti 4 i Kosovës (falsifikimi i dokumentit tatimor) dhe rasti 4 i Serbisë (Mafia e Rrugës) pasqyron sesi menaxhimi dhe/ose i gjithë organizimi mund të anashkalojë abuzimin me detyrën, mashtrimin në detyrë, përvetësimin e fondeve dhe krimin e organizuar, duke krijuar një kulturë ku gjithkush është "brenda" abuzimit, nuk guxon të bëjë asgjë për të dhe e pranon situatën, qoftë pasi ka frikë nga pasojat e zbulimit të abuzimit, qoftë pasi përfiton prej këtij abuzimi.

Faktori njerëzor

Edhe në rast se të gjitha garancitë/mbrojtjet antikorrupsion në lidhje me ICT-në janë realizuar, nuk ekziston asnjë garanci se sistemet nuk do të abuzohen. Një urdhër i paligjshëm nga një menaxher për të tërhequr postën elektronike si në rastin serb 3 (një zyrtar i lartë publik përgjon punonjësit), ose në rastin 2 të Shqipërisë (korrupsioni në sistemin e prokurimit publik elektronik) ku shumica e përdoruesve shfaqin pakënaqësi, veçanërisht me ndryshimin periodik të fjalëkalimeve komplekse dhe marrin shortcut-in (opsionin më të shkurtër) për ta lënë të pandryshuar fjalëkalimin me vlerën fillestare me të cilën i ka furnizuar fillimisht administratori i sistemit gjatë regjistrimit për herë të parë, do të ekzistojë gjithmonë. Ndërgjegjësimi i nëpunësve lidhur me shkallën e cënimit të sistemeve të jetë çelësi për sisteme të sigurisë dhe të mbrojtjes. Ky përfshin ndërgjegjësimin jo vetëm ndaj pasojave të sigurisë, por edhe të dimensionit etik dhe të integritetit të punës së nëpunësve civilë. Nëpunësit civilë duhet të jenë të ndërgjegjshëm për të drejtat dhe detyrimet e tyre dhe shtetet individuale duhet të përcaktojnë modalitete që mbështesin sjelljen etike.

Masat mbrojtëse legjislative

Autorët vendas renditin një sërë aktesh legjislative dhe strategji kombëtare që mbulojnë fusha si për shembull: procedurat administrative; dokumentet elektronike; informacioni i klasifikuar; nënshkrimi elektronik; mbrojtja e të dhënave personale; prokurimi publik; korrupsioni dhe kodi penal. Është jashtë qëllimit të këtij studimi që të kryhet një analizë krahasuese midis mbrojtjes legjislative të secilit vend, meqenëse ato janë përfshirë si kontribute për të ilustruar mbrojtjen ligjore në lidhje me shembujt e rasteve individuale.

Një mësim interesant i nxjerrë nga ky studim është fakti se ka raste kur mbrojta ligjore ka qenë e papërshtatshme për mbrojtje nga korrupsioni i ICT-së.

Autorët nga Kosova raportojnë se: "Për sa i përket mbrojtjes administrative, Kosova ka miratuar një sërë ligjesh, strategjish dhe udhëzimesh administrative (aktesh normative) që lidhen me përdorimin e teknologjive të informacionit dhe komunikimit, por infrastruktura legjislative deri tani nuk trajton siç duhet çështjen e integritetit të të dhënave dhe abuzimin e sistemeve të teknologjisë së informacionit në mënyrë specifike ose në përgjithësi".

Ekzistojnë vetëm pak shembuj rastesh në këtë studim që përshkruajnë mbrojtjen e papërshtatshme legjislative ndaj abuzimit dhe si të tilla, duhen nxjerrë mësime nga to. Në rastin 2 të Maqedonisë (sulmi ndaj sistemit të IT-së për prokurimin publik), rregullat e prokurimit duket se nuk kanë parashikuar një situatë ku procesi i ofertës elektronike është ndërprerë për shkak të arsyeve "teknike". Në një tjetër shembull prokurimi – rasti serb 2 (kur kontraktuesi i IT-së "zë rrënjë") – u raportua se kontraktuesi i IT-së kishte ndërprerë procesin e ri të tenderimit duke përdorur një skemë komplekse dhe të lodhshme ankimimi të krijuar nga boshllëqet në Ligjin për Prokurimin Publik. Që nga ajo kohë ligji është ndryshuar ("Fletorja Zyrtare e Republikës së Serbisë", nr. 124/12).

Në rastin serb 1 (Seks në Arenën e Beogradit) rregulloret e brendshme administrative u përditësuan për të përfshirë: 1) aksesi i paautorizuar i të dhënave të Ministrisë së Brendshme tashmë përcaktohet jo thjesht si shkelje disiplinore, por si një vepër penale; dhe 2) përdorimi i të dhënave për ndonjë qëllim tjetër nga ai fillestar se përse janë grumbulluar të dhënat tashmë parashikohet si vepër penale (jo thjesht disiplinore).

Shembujt e rasteve në këtë studim janë thjesht shembuj. Nuk ekziston informacion përfaqësues për të nxjerrë një përfundim për boshllëqet e përgjithshme në mbrojtjen legjislative.

3. Rekomandimet e politikave për zbutjen e rreziqeve të korrupsionit nëpërmjet ICT-së

Nga Tilman Hoppe dhe Luoise Thomasen

Pjesa 1 – Rekomandime në adresë të ekspertëve të antikorrupsionit

Çdo grup interesi që punon për parandalimin e korrupsionit duhet të pranojë ICT-në jo vetëm si një instrument për të luftuar korrupsionin, por edhe si rrezik për kryerjen e tij. Në këtë përfundim, masat e mëposhtme janë të nevojshme për ekspertët antikorrupsion:

1. Ekspertët antikorrupsion duhet **të bashkëpunojnë** ngushtë për identifikimin dhe parandalimin e rreziqeve të korrupsionit nga abuzimi i ICT-së.

2. Organet e parandalimit të korrupsionit duhet të përfshijnë mundësinë e abuzimit të ICT-së për korrupsion në listën standarde të rreziqeve të korrupsionit. **Vlerësimet e rreziqeve** në administratën publike duhet të përfshijnë sigurinë e IT-së kundër rreziqeve të korrupsionit. Vlerësimet e rrezikut duhet të shqyrtojnë secilën prej veçorive të IT-së të renditua më poshtë (Pjesa 2 e rekomandimeve).

3. Krerët e enteve publike si dhe zyrtarët publikë duhet **të ndërgjegjësohen** për rreziqet që mund të përbëjnë ICT-në për sa i përket korrupsionit. Organet e parandalimit të korrupsionit duhet të ofrojnë aktivisht këshillim për mbylljen e boshllëqeve të sigurisë në IT-në e administratës publike.

4. Organet e parandalimit të korrupsionit dhe qendrat e trajnimit profesional duhet të ofrojnë **trajnim** për rreziqet e korrupsionit që lidhen me ICT-në; si për shembull trajnimi përfshin ekspertët e IT-së.

5. **Strategjitë** kombëtare antikorrupsion dhe planet e veprimit duhet të përfshijnë një seksion për parandalimin e korrupsionit që lidhet me abuzimin e IT-së. Në rast se strategjitë e tjera (si për shembull qeverisja elektronike ose reforma e administratës publike) që trajtojnë tashmë në mënyrë gjithëpërfshirëse fuqizimin e IT-së ndaj abuzimit, politika antikorrupsion duhet të paktën të përmbajë një referencë ndaj strategjive të tjera dhe të sigurojë koordinim mes antikorrupsionit dhe ekspertëve të IT-së për masat e reformave.

6. Organet e zbatimit të ligjit dhe organet e parandalimit të korrupsionit duhet të grumbullojnë **të dhëna statistikore** për korrupsionin në IT, të analizojnë veçoritë dhe të miratojnë siç duhet masat për reforma.

Pjesa 2 – Rekomandime në adresë të ekspertëve të qeverisjes elektronike

1. Akses ndaj të gjitha të dhënave të pronësisë dhe sistemeve që duhen mbrojtur me **kontrollin ndaj aksesit** duke përdorur ID-të dhe fjalëkalimet individuale private të përdoruesve.

2. Në secilin organ publik është përgjegjësi e menaxhimit të sigurojë se aksesi në të dhëna është **në nivel të përshtatshëm**. Aksesi ndaj të dhënave të pronësisë duhet të garantohet vetëm kur kërkohet për detyra të menjëhershme.

3. **Aksesi fizik** ndaj pajisjeve që ruajnë të dhëna ose kopje fizike të të dhënave duhet të kufizohet në personel të autorizuar, aksesi i të cilit është i loguar dhe monitoruar.

4. Organizatat publike duhet të zbatojnë **standardet e sigurisë së informacionit** si për shembull ISO 27001 për të garantuar sigurinë dhe integritetin e të dhënave.

5. **Rikuperimi i prishjes së rrjetit dhe planet e vazhdimësisë** në rast incidentesh të sigurisë duhet të hartohen për çdo organizatë publike. Planet duhet të përshkruajnë procedurat që duhen ndjekur në rast incidentesh, mënyrën e menaxhimit të vazhdimësisë së biznesit dhe identifikimi dhe rënia dakord për përgjegjësitë lidhur me masat e emergjencës.

6. Të gjitha organizatat publike duhet të zbatojnë **procedura për kopjet rezervë** me mbështetje të plotë periodike të të gjitha sistemeve dhe të dhënave. Kjo përfshin kompjuterët desktop dhe laptop. Kopjet rezervë duhet të ruhen fizikisht jashtë sistemit.

7. **Skedarët regjistrues** janë pjesë e monitorimit të organizatës dhe strukturës së mbikëqyrjes. Ato përbëjnë gjithashtu një instrument të rëndësishëm auditimi. Kopjet e skedarëve regjistrues duhet të ruhen gjithashtu jashtë sistemit dhe/ose ndarazi nga vetë aplikacioni. Personeli përgjegjës për ndryshimin e përmbajtjes (të dhënave) nuk duhet të jenë administratorët (teknikë) të skedarëve regjistrues.

8. Organet publike duhet të garantojnë që të gjitha proceset e tyre, pavarësisht nëse janë apo jo fizike apo elektronike, të mos jenë të cenueshme nga abuzimi i korrupsionit. **Një proces ose hap i kompromentuar në një proces do të ndikojë tek të gjitha proceset e tjera me të cilat ndërvepron.** Sistemet ICT që mbështeten në kontributin e sistemeve dhe proceseve të tjera janë aq të sigurt nga korrupsioni sa edhe sistemet dhe proceset me të cilat ndërveprojnë.

9. **Regjistrat bazë** kërkojnë masa të posaçme dhe të larta sigurie meqenëse ato janë elementët bazë të nevojshëm për ndërfunksionalitetin koherent të qeverisjes elektronike.

10. **Nënkontraktimi** i zhvillimit të IT-së, mirëmbajtja ose vënia në funksionim kërkojnë vullnet të qëndrueshëm nga organizata publike që kryen nënkontraktimin. Përgjegjësia nuk mund të jetë kurrë e nënkontraktuesit. Kur kryhet nënkontraktim, sigurohuni se aksesi tek të dhënat të jetë i mundshëm vetëm për personelin e caktuar dhe të autorizuar dhe se ato do të monitorohen dhe auditohen.

11. Duhet të ketë një **ndarje rolesh** mes personelit përgjegjës për të dhënat (përmbajtjen) dhe personelit përgjegjës për sistemet (teknologjinë).

12. **Auditimet** e sistemeve dhe gjurmët e auditimeve nuk duhen monitoruar asnjëherë dhe administruar nga i njëjti administrator IT-je.

13. Mbikëqyrja dhe zbatimi i parimit **të shumë syve** duhet të jetë pjesë integrale, jo thjesht në projektimin dhe zhvillimin e sistemit, por gjithashtu në punën ditore.

14. Të dhënat e qeverisë së hapur dhe pjesëmarrja e qytetarëve në shqyrtimin me hollësi të të dhënave të sektorit publik mund të sigurojnë “kontrolle reale” dhe të përmirësojnë cilësinë e të dhënave si dhe të nxjerrin në pah parregullsitë dhe abuzimin. Gjithashtu i rëndësishëm në këtë kontekst është furnizimi i publikut me kanale për të dhënë komente ndaj qeverisë dhe sektorit publik. Në rastin e korrupsionit/parregullsive punonjësit e etikës, të cilëve qytetarët mund t’u raportojnë sjelljen joetike të nëpunësve civilë, mund të jenë një kanal i tillë.

15. Duhet garantuar se trajnimi i vazhdueshëm dhe rritja e ndërgjegjësimit të etikës dhe integritetit përfshin gjithashtu personelin përgjegjës për ICT-në.