ReSPA
Regional School
of Public Administration

Zloupotreba informacionih tehnologija (IT) u svrhe korupcije

ReSPA aktivnosti
finansira EU

ReSPA je zajednička inicijativa EU i zemalja Zapadnog Balkana sa ciljem podsticanja i jačanja regionalne saradnje njenih članica u oblasti državne uprave. ReSPA nastoji da ponudi odlične inovativne i kreativne skupove za edukaciju, aktivnosti za umrežavanje, kao i usluge izgradnje kapaciteta i savetovanja, kako bi se osiguralo da se zajedničke vrednosti poštovanja, tolerancije, saradnje i integracije potvrđuju i sprovode u svim državnim upravama u region.

Naslov originala: Abuse of Information Technology (IT) for Corruption

KONTAKT
Regionalna škola za državnu upravu
Branelovica
Poštanski fah 31, 81400
Danilovgrad, Crna Gora

Telefon +382 (0)20 817 200
Internet: www.respaweb.eu
I-mejl: respa-info@respaweb.eu

CIP - Katalogizacija u publikaciji
Centralna narodna biblioteka Crne Gore, Cetinje

Komparativna studija slucaja: Zloupotreba informacionih tehnologija (IT) u svrhe korupcije
Danilovgrad, ReSPA, 2016. Elektronsko izdanje, 160 strana; Bilješke uz tekst. Urednik: Paštrovic Goran
Autori: Hoppe Tilman, Devine Vera, Thomasen Louise, Nasi Edlira,Kercini Ened, Martinović Aleksandra, Nogo Srđan, Petrović Zorislav, Andrijašević Ivana, Preteni Hasan, Elshani Driart, Stoilkovski Marjan, Stojova Rozalinda, Drakić Dušan, Lazarević Ivan, Nenadić Nemanja, Cvetković Bojan.
Prevod: Porta Aperta, Podgorica

ISBN 978-9940-37-002-2

Komparativna studija slucaja
COBISS.CG-ID 29068560

Autori

ReSPA

Goran Paštrović, *menadžer za obuke*

Međunarodni autori

Uvod, pregledi za poglavlja 1 i 2, podpoglavlje 2.9 i poglavlje 3

Tilman Hoppe, *ekspert za antikorupciju*
Vera Devine, *ekspert za antikorupciju*
Louise Thomasen, *ekspert za elektronsku vladu*

Nacionalni autori

Albanija

Edlira Nasi, *ekspert za antikorupciju*
Ened Kercini, *ekspert za elektronsku vladu*

Bosna i Hercegovina

Aleksandra Martinović, *ekspert za antikorupciju*
Srđan Nogo, *ekspert za elektronsku vladu*

Hrvatska

Zorislav Petrović, *ekspert za antikorupciju*
Ivana Andrijašević, *ekspert za elektronsku vladu*

Kosovo*

Hasan Preteni, *ekspert za antikorupciju*
Driart Elshani, *ekspert za elektronsku vladu*

Makedonija

Marjan Stoilkovski, *ekspert za antikorupciju*
Rozalinda Stojova, *ekspert za elektronsku vladu*

Crna Gora

Dušan Drakić, *ekspert za antikorupciju*
Ivan Lazarević, *ekspert za elektronsku vladu*

Srbija

Nemanja Nenadić, *ekspert za antikorupciju*
Bojan Cvetković, *ekspert za elektronsku vladu*

*Ovaj naziv ne prejudiciranja stavove o statusu i u skladu je sa Rezolucijom 1244 Saveta bezbednosti ujedinjenih nacija i odlukom Međunarodnog suda pravde o kosovskoj deklaraciji o nezavisnosti.

Predgovor

Suad Musić,
Direktor ReSPA-e

U Konvenciji Ujedinjenih nacija protiv korupcije (UNCAC) navedeno je, u Članu 48, stav 3:

„Države ugovornice će nastojati da u okviru svojih mogućnosti sarađuju u otkrivanju krivičnih dela obuhvaćenih ovom Konvencijom koja su počinjena korišćenjem savremene tehnologije."

Do danas, međunarodne organizacije ovoj odredbi nisu pridavale mnogo pažnje u svom radu. U stvari, Tehnički vodič o implementaciji UNCAC-a[1] sadrži sledeće kao jedinu smernicu:

„Stav 3 (Člana 48) prepoznaje sve intenzivniju upotrebu računarskih tehnologija u počinjavanju mnogih krivičnih dela opisanih u Konvenciji i poziva Države ugovornice da bliže sarađuju kako bi reagovale na krivična dela vezana za korupciju, počinjena kroz upotrebu modernih tehnologija."

Ova komparativna studija ima za cilj da obezbedi, po prvi put, konkretne smernice, prikazujući slučajeve zloupotrebe „moderne tehnologije" (IT) kod krivičnih dela vezanih za korupciju, kao i smernice o mogućim koracima koje treba preduzeti u zaštiti od takvih zloupotreba.

ReSPA je godinama aktivna na oba polja – kako integriteta tako i elektronske uprave. Sa svojim regionalnim mrežama stručnjaka za oba polja, u odličnoj je poziciji da objedini obe discipline na obostranu korist. U svetlu njene važnosti za implementaciju UNCAC, ova Studija će imati uticaja na region Zapadnog Balkana, a, u isto vreme, taj uticaj će se proširiti i znatno van regiona, na svaku od 172 ugovornice UNCAC-a.

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

Sadržaj

Skraćenice

Sledeća lista je popis po abecednom redu skraćenica i njihovih značenja, onako kako su upotrebljene u izveštaju.

ARTE	Albansko regulatorno telo za energetiku
AŠDU	Albanska škola za državnu upravu
AU	Administrativno uputstvo
BiH	Bosna i Hercegovina
CARNet	Hrvatska akademska i istraživačka mreža
CCTV	Sistem video nadzora (televizija zatvorenog kola)
CERT	Tim za odgovor na računarske bezbednosne incidente
CIPS	Sistem za zaštitu identifikacije građana (Bosna i Hercegovina)
DDoS	Distribuirani napad radi blokiranja usluga
DKSK	Državna komisija za sprečavanje korupcije (Makedonija)
DMS	Sistem upravljanja dokumentima (Document management system)
DORH	Državno tužilaštvo Republike Hrvatske
e- SEE	Elektronska jugoistočna Evropa (Electronic South Eastern Europe)
ENP	Elektronska naplata putarine (Srbija)
EU	Evropska unija
EUPM	Policijska misija Evropske unije u Bosni i Hercegovini
FTP	Protokol transfera fajlova (File transfer protocol)
HAC	Hrvatske autoceste
HDZ	Hrvatska demokratska zajednica
HNS	Hrvatska narodna stranka
HRT	Hrvatska radio-televizija
HZPO	Hrvatski zavod za penzijsko osiguranje
IDDEEA	Agencija za lične isprave, registre i razmenu podataka (Bosna i Hercegovina)
ICT	Informaciono-komunikaciona tehnologija
IMPACT	Međunarodno multilateralno partnerstvo protiv sajber pretnji
IPA	Instrument za predpristupnu pomoć (Bosna i Hercegovina)
IPK	Indeksi percepcije korupcije
ISO	Međunarodna organizacija za standarde
ISP	Provajder internet usluga (Internet Service Provider)
IT	Informacione tehnologije
KJP	Kancelarija za javne prihode (Makedonija)
KOC	Komandno-operativni centar (Srbija)
LDA	Lični digitalni asistent
MDULS	Ministarstvo državne uprave i lokalne samouprave (Srbija)
MIDT	Ministarstvo za informaciono društvo i telekomunikacije
MO	Ministarstvo odbrane

MP	Ministarstvo pravde
MPB	Ministarstvo za pitanja boraca (Hrvatska)
MPDU	Ministarstvo pravde i državne uprave (Srbija)
MRSP	Ministarstvo rada i socijalne politike (Makedonija)
MUP	Ministarstvo unutrašnjih poslova
NAID	Nacionalna agencija za informaciono društvo (Albanija)
NARB	Nacionalna agencija za računarsku bezbednost (Albanija)
NFC	Bežična tehnologija kratkog dometa (Near-field communication)
NVO	Nevladina organizacija
OPK	Odeljenje za privredni kriminal (Hrvatska)
OIB	Lični (osobni) identifikacioni broj (Hrvatska)
PARCO	Kancelarija koordinatora za reformu javne uprave (Bosna i Hercegovina)
PKI	Ključna javna infrastruktura (Public Key Infrastructure)
SDH	Sinhrona digitalna hijerarhija (Synchronous Digital Hierarchy)
SDS	Srpska demokratska stranka (Bosna i Hercegovina)
SDU	Sistem za detekciju upada
SIPA	Državna agencija za istrage i zaštitu
SNSD	Stranka nezavisnih socijaldemokrata (Bosna i Hercegovina)
SOA	Sigurnosno - obaveštajna agencija (Hrvatska)
SOP	Standardne operativne procedure
SSL	Sloj bezbednih utičnica (Secure Sockets Layer)
SUPDO	Sistem za upravljanje predmetima u digitalnom obliku (Bosna i Hercegovina)
TCPT	Trening centri za pravosuđe i tužilaštvo (Bosna i Hercegovina)
TIMS	Sistem za upravljanje celokupnim podacima (Albanija, Srbija)
TORI	Tim za odgovor na računarske incidente
UCV	Uprava za civilno vazduhoplovstvo (Albanija)
UNODC	Kancelarija ujedinjenih nacija za pitanje droge i kriminala
UoP	Ugovor o poverljivosti
US	Uprava za sertifikaciju (Makedonija)
USKOK	Kancelarija za suzbijanje korupcije i organizovanog kriminala (Hrvatska)
VDRI	Vrhovna državna revizorska institucija (Albanija)
VPN	Virtualna privatna mreža (Virtual Private Network)
VRIRS	Vrhovna revizorska institucija Republike Srpske
VRK BiH	Vrhovna revizorska kancelarija Bosne i Hercegovine
VSOA	Vojna sigurnosno - obaveštajna agencija (Hrvatska)
VSTS	Visoki sudski i tužilački savet (Bosna i Hercegovina)
WAN	Regionalna računarska mreža (Wide Area Network)

Uvod

Priredio Tilman Hoppe

Postoje brojne publikacije o tome na koji način se može **sprečiti** korupcija kroz dobru upotrebu IT sistema, kao što su javni registri, transparentnost u prijavi imovine ili u elektronskim nabavkama. Sledeće publikacije su istaknuti primeri analize metoda upotrebe IT sistema u borbi protiv korupcije:

- Tim Davies/Silvana Fumega, „Mešoviti podsticaji: Usvajanje inovacija u ICT za poboljšanje transparentnosti, odgovornosti i antikorupcije", U4 izdanje 2014:4, 38 strana [2]
- UNDP, „Borba protiv korupcije putem primene elektronske uprave", APDIP e-Note 8/2006, 4 strane[3]
- Spider, „Povećanje transparentnosti i intenziviranje borbe protiv korupcije kroz ICT – Osnaživanje pojedinaca i zajednica", ICT4D Serija br. 3/2010, 102 strane[4]
- Spider, „ICT za antikorupciju, demokratiju i obrazovanje u Istočnoj Africi", Spider ICT4D Serija br. 6/2013, 96 strana[5]
- Jamshed J. Mistry/Abu Jalal, „Empirijska analiza odnosa između elektronske uprave i korupcije", Međunarodni žurnal istraživanja elektronskog računovodstva, 12. deo, 2012, str. 145-176[6]
- Ionescu, Luminita, „Uticaj koji elektronska uprava može imati na smanjenje korupcije i povećanje transparentnosti", Ekonomija, menadžment i finansijska tržišta, 8. deo, br. 2, 2013, strana 210
- Bertot/Jaeger/Grimes, „Upotreba ICT za stvaranje kulture transparentnosti: elektronska uprava i društveni mediji kao alati za postizanje otvorenosti i borbu protiv korupcije u društvu", Vladin informatički tromesečnik 27. deo izdanje 3, 2010, str. 264
- Richard Heeks, „Informacione tehnologije i korupcija u javnom sektoru", Institut za razvojnu politiku i menadžment, septembar 1998., 15 strana[7]
- Transnacionalni centar za kriminal i korupciju, „Transnacionalni kriminal, korupcija i informacione tehnologije", Izveštaj sa konferencije 2000, 39 strana 8

Međutim, postoji jako malo literature, ako uopšte i postoji, o obratnoj upotrebi informacionih tehnologija kao **alata** za korupciju. Hongkonška „Nezavisna komisija za borbu protiv korupcije" je izdala sledeće publikacije:

- „Etika na radnom mestu – vodič za poslovne menadžere za upotrebu informacionih tehnologija", 2003., 77 strana[9], koja se fokusira na privatni poslovni sektor.
- Postoji nekoliko incidenata gde su antikorupcijska tela označila ICT kao rizičnu za

2 http://www.u4.no/publications/mixed-incentives-adopting-ict-innovations-for-transparency-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/Spider%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.

korupciju u javnom sektoru. Sledeći primeri su dva od nekoliko:

- Antikorupcijska komisija Kenije, „Smernice za prevenciju korupcije putem ICT sistema u javnom sektoru“, mart 2008.[10]
- Nezavisna komisija protiv korupcije (ICAC) Novog južnog Velsa, (Australija), „Poznavanje rizika: IT sistemi”[11]

Veb stranica ICAC prikazuje samo dva kratka primera korupcije u javnom sektoru koji su vezani za IT. Štaviše, tehničke smernice međunarodnih organizacija o korupciji, koje slede, retko ili nikako ne spominju IT kao rizik:

- UNODC, UN Antikorupcijski alat (3. Izdanje, 2004.)[12];
- UNODC, Tehnički vodič za UNCAC, 2009.[13];
- OEBS, Najbolja praksa u borbi protiv korupcije, 2004.[14];
- Transparency International, Suprotstavljanje korupciji: elementi nacionalnog sistema integriteta, TI Izvorna knjiga 2000.[15];
- USAID Priručnik za procenu korupcije (2006)[16].

Nedostatak smernica je u velikom kontrastu sa „Konvencijom UN protiv korupcije“ (UNCAC) koja poziva, u Članu 48, stav 3, Države ugovornice da „nastoje da u okviru svojih mogućnosti sarađuju u otkrivanju krivičnih dela obuhvaćenih ovom Konvencijom koja su počinjena korišćenjem savremene tehnologije“. U tom smislu, krajnje je vreme da se izradi jedna sveobuhvatna regionalna studija na ovu temu.

Čitalac ove studije imaće koristi od proučavanja konkretnih primera, koji ilustruju to na koji način prestupnici umešani u korupciju koriste slabosti u IT strukturama za svoju ličnu korist. Primeri zloupotrebe IT u svrhe korupcije iz svakodnevnog života, kao i **dobri primeri** njihove prevencije i detekcije, pružiće inspiraciju stručnjacima koji se bave prevencijom korupcije kao i stručnjacima nedležnim za IT bezbednost.

Ova studija se odnosi **isključivo** na rizike od korupcije vezane za IT. Na primer, korupcija prilikom nabavke IT opreme ili fiksacija na samo jednog dobavljača takve opreme jesu koruptivni rizici do kojih može doći prilikom upotrebe bilo kog alata za javnu nabavku, kao što je nabavka vozova za javni prevoz ili moguća fiksacija na samo jednog dobavljača; stoga, to nisu koruptivni rizici koji su vezani samo za IT.

Očekuje se da će članovi ReSPA-e imati različit pristup i način upotrebe IT i tako će učiti putem **razmene**, koja će biti olakšana putem ove Komparativne studije. Pošto još uvek ne postoji tipologija slučajeva u literaturi koja se odnosi na IT ili borbu protiv korupcije, dodatna vrednost i uticaj ove studije mogu se proširiti mnogo dalje van ReSPA regiona.

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. Slučajevi zloupotrebe IT u svrhe korupcije iz svakodnevnog života

Pregled

Priredili Tilman Hoppe i Louise Thomasen

Slučajevi koji slede nisu reprezentativni i odabrani su metodom slučajnog uzorka iz ReSPA regiona. Važno je napomenuti da navedeni slučajevi nisu neophodno bili podvrgnuti sudskom ispitivanju; za potrebe studije, bilo je dovoljno samo to što su ih određene zainteresovane strane prijavile ili primetile (kao što su mediji, NVO, osoblje interne administracije, itd.) Veliki izazov u identifikaciji relevantnih slučajeva predstavljao je manjak statističkih informacija o koruptivnim krivičnim delima vezanim za zloupotrebu IT kao i činjenica da se zloupotreba IT u svrhe korupcije ne nalazi na dnevnom redu mnogih, ako ne i većine, antikorupcijskih tela u regionu. U isto vreme, izgleda da postoji snažan tabu kada je u pitanju otkrivanje slabosti u IT sistemima; činilo se da su javne institucije gotovo po pravilu nerado otkrivale informacije o tome da njihovi IT sistemi imaju mnogo više slabosti nego što bi to javnost mogla da misli. Međutim, inicijatori izrade ove studije smatrali su da je bolje da se svetskom čitalaštvu obezbede konkretni primeri iz prakse, čak i ako materijal nije sasvim proveren, potpun ili reprezentativan, ili bar ne u svim slučajevima.

Primeri pokazuju da se zloupotreba IT tiče čitavog dijapazona korupcijskih prekršaja:
- Mito
- Zloupotreba položaja
- Protivzakonito posredovanje
- Sukob interesa
- Kršenje pravila nabavki
- Pronevere

Zloupotreba IT u svrhe korupcije dešava se u slučajevima kada su u pitanju finansijski interesi, kao i u slučajevima kad zloupotreba IT služi samo za ispunjenje nematerijalnih interesa javnog zvaničnika (kao što je satisfakcija objavljivanjem senzacionalnih ličnih podataka). Izgleda da se ovakvi slučajevi dešavaju u svakom mogućem sektoru državne uprave, uključujući i kompanije u državnom vlasništvu, i, prirodno, sve nivoe državne uprave (i centralne i lokalne). Do zloupotrebe IT može doći spontano, radi zadovoljenja individualnih potreba (kao kad je u pitanu krivotvorenje pasoša) ili u sklopu kontinuiranih operacija organizovanog kriminala (kao u slučaju prevare sa sistemom naplatnih rampi).

Veliki broj različitih slučajeva isto tako pokazuje da se mantra „elektronska uprava pomaže u borbi protiv korupcije“ mora prihvatati sa oprezom. IT nisu, same po sebi, univerzalni lek protiv korupcije. U nekim slučajevima, moglo bi se čak reći i da IT olakšavaju prestupnicima da počine korupcijska krivična dela: nedostaci IT sistema mogu im ići u prilog jer su tragovi manje vidljivi u jako kompleksnim mrežama i u moguće kratkotrajnoj elektronskoj evidenciji. Važnost pouzdanih mera zaštite (o kojima će biti reči u poglavlju 2) postaje očiglednija u svetlu ovih primera.

Tabela 1

Naslov	Korupcijsko krivično delo (ne mora neophodno da bude dokazano)	Upotreba IT	Šteta za javne finansije	Kako je detektovano korupcijsko krivično delo?	Nivo državne uprave (centralni ili lokalni)	Sektor
Slučaj iz Albanije 1: Korupcija u TIMS sistemu granične kontrole	Mito	Prodaja falsifikovanih podataka	Da	Interna kontrola	Centralni	Primena zakona
Slučaj iz Albanije 2: Korupcija u elektronskom sistemu javnih nabavki	Krivično delo vezano za nabavku	Neovlašten unos/ falsifikat	Da	Eksterna kontrola	Centralni	Nabavke
Slučaj iz Albanije 3: Zloupotreba IT u svrhe korupcije kod distributera električne energije	Zloupotreba položaja Falsifikovanje	Falsifikovanje podataka	Da	Pritužba građana	Centralni	Energetika
Slučaj iz Albanije 4: Pronevera i falsifikovanje u knjigovodstvu	Zloupotreba položaja Pronevera	Izmena podataka/ prevara	Da	Interna kontrola	Centralni	Odbrana
Slučaj iz Bosne i Hercegovine 1: Najpoznatiji bosanski haker istovremeno i tužilac	Zloupotreba položaja	Računarska sabotaža	Ne	Interna istraga	Centralni	Pravosuđe
Slučaj iz Bosne i Hercegovine 2: Još jedno kontroverzno zaposlenje u Vrhovnoj revizorskoj instituciji u Republici Srpskoj	Zloupotreba položaja	Uništavanje podataka	Ne	Informacija od insajdera	Lokalni	Nabavke

Naslov	Korupcijsko krivično delo (ne mora neophodno da bude dokazano)	Upotreba IT	Šteta za javne finansije	Kako je detektovano korupcijsko krivično delo?	Nivo državne uprave (centralni ili lokalni)	Sektor
Slučaj iz Bosne i Hercegovine 3: Zloupotreba elektronskog sistema projekta CIPS	Zloupotreba položaja	Falsifikovanje podataka	Ne	Medijski izveštaj	Lokalni	Civilni registar
Slučaj iz Hrvatske 1: Poziv od doktora radi glasanja	Nezakonito pribavljanje podataka	Neovlaštena upotreba podataka pacijenata iz bolnice	Ne	Pritužba građana	Lokalni	Zdravstvo
Slučaj iz Hrvatske 2: Poverljiva baza podataka hrvatske radio-televizije na crnom tržištu	Nezakonito pribavljanje podataka	Kopiranje i prodaja podataka iz baze podataka HRT	Ne	Pritužba NVO	Centralni	Mediji
Slučaj iz Hrvatske 3: U potrazi za veteranima	Zloupotreba položaja Nezakonito pribavljanje podataka	Prodaja ili ustupanje podataka iz baze	Ne	Medijski izveštaj	Centralni	Vlada
Slučaj iz Hrvatske 4: Uz malu pomoć državnih službenika, 68 hrvatskih pasoša prodato kriminalcima	Nezakonito pribavljanje podataka	Provera poverljivih podataka iz policijskog informacionog sistema	Ne	Policija	Centralni	Unutrašnji poslovi
Slučaj iz Hrvatske 5: Policajac uhvaćen dok je unosio falsifikovane podatke u policijski informacioni sistem	Manipulacija postojećim podacima i procedurama	Stvaranje lažne dokumentacije elektronskim putem kako bi se stranom državljaninu pomoglo da dobije hrvatski pasoš	Ne	Policija	Centralni	Unutrašnji poslovi
Slučaj iz Hrvatske 6: Policajci brisali saobraćajne prekršaje iz evidencije i otkrivali poverljive podatke: prihvatali čak i pečeno jagnje i 20 litara vina kao mito!	Nezakonito pribavljanje podataka Manipulacija podacima i procedurama	Nezakonito pribavljanje podataka: otkrivanje poverljivih podataka iz policijskog info. sistema pripadnicima organizovanog kriminala. Manipulacija postojećim podacima i procedurama: brisanje saobraćajnih prekršaja iz policijskog info. sistema	Ne	Policija	Lokalni	Unutrašnji poslovi

Naslov	Korupcijsko krivično delo (ne mora neophodno da bude dokazano)	Upotreba IT	Šteta za javne finansije	Kako je detektovano korupcijsko krivično delo?	Nivo državne uprave (centralni ili lokalni)	Sektor
Slučaj iz Hrvatske 7: Slučajno uhvaćeni u otkrivanju poverljivih podataka o automobilima i njihovim vlasnicima!	Nezakonito pribavljanje podataka	Otkrivanje poverljivih podataka iz policijskog informacionog sistema pripadnicima organizovanog kriminala	Ne	Policija	Lokalni	Unutrašnji poslovi
Slučaj iz Hrvatske 8: Svake godine nestane 2 miliona evra sa naplatnih rampi	Pronevera	Brisanje podataka i ubacivanje lažnih podataka u informacioni sistem	Da (≈2 evra / godišnje)	Interna kontrola	Centralni	Saobraćaj
Slučaj iz Hrvatske 9: Korumpirani policajci otkrivali poverljive podatke krijumčarima oružja	Otkrivanje poverljivih podataka Zloupotreba položaja	Otkrivanje poverljivih podataka iz policijskog informacionog sistema pripadnicima organizovanog kriminala	Ne	Policija	Lokalni	Policija
Slučaj iz Hrvatske 10: Policajac osuđen na kaznu zatvora od godinu dana jer je dozvolio prijatelju nelegalan ribolov	Otkrivanje poverljivih podataka Zloupotreba položaja	Otkrivanje poverljivih podataka iz informacionog sistema Ministarstva unutrašnjih poslova pripadnicima organizovanog kriminala	Ne	Nepoznato	Lokalni	Policija
Slučaj iz Hrvatske 11: Viši inspektor zloupotrebio poverljive podatke kako bi pobedio na lokalnim izborima	Zloupotreba položaja Otkrivanje poverljivih podataka	Nezakonit pristup i otkrivanje poverljivih podataka iz informacionog sistema Poreske uprave	Ne	Pritužba građana	Lokalni	Porezi
Slučaj iz Hrvatske 12: Ni dana svog života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!	Prevara (falsifikovanje radne knjižice) Pronevera neopravdanom dodelom penzije	Ubacivanje lažnih podataka u informacioni sistem Hrvatskog zavoda za penzijsko osiguranje	Da (≈20,000 evra)	Unutrašnja pritužba	Centralni	Socijalno osiguranje
Slučaj sa Kosova 1: Uništavanje dokaza	Zloupotreba položaja Prevara na radnom mestu Falsifikovanje zvaničnih dokumenata	Brisanje podataka sa servera	Da	Pritužba građana	Centralni	Građevina
Slučaj sa Kosova 2: Dobijanje statusa „ratnog invalida“	Falsifikovanje zvaničnih dokumenata Prevara na radnom mestu	Falsifikovanje podataka	Da	Pritužba građana	Centralni	Društveni poslovi

Naslov	Korupcijsko krivično delo (ne mora neophodno da bude dokazano)	Upotreba IT	Šteta za javne finansije	Kako je detektovano korupcijsko krivično delo?	Nivo državne uprave (centralni ili lokalni)	Sektor
Slučaj sa Kosova 3: Zloupotreba lozinke	Zloupotreba ovlašćenja	Favorizovanje Krađa lozinke	Da	Unutrašnja pritužba	Centralni	Zdravstvo
Slučaj sa Kosova 4: Falsifikovanje poreske dokumentacije	Falsifikovanje zvaničnih dokumenata Prevara na radnom mestu	Falsifikovanje dokumenata	Da	Unutrašnja pritužba (bivši zaposleni)	Lokalni	Održavanje
Slučaj iz Makedonije 1: Zloupotreba IT sistema na naplatnim rampama	Zloupotreba položaja Mito Pronevera	Lažno beleženje broja i tipa vozila u IT sistemu naplatne rampe	Da (≈2,000 evra)	Interna kontrola	Centralni	Transport/ saobraćaj
Slučaj iz Makedonije 2: Napad na IT sistem javnih nabavki	Mito Pronevera Krivična dela vezana za nabavke	Ometanje procesa nabavke Nezakonit upad u računarskiki sistem	Ne/nije poznato	Pritužba građana	Centralni	Nabavke
Slučaj iz Makedonije 3: Zloupotreba IT sistema i nelegalno otkrivanje ličnih podataka	Pronevera Zloupotreba položaja Moguće mito	Izvlačenje ličnih podataka i stvaranje zvaničnog dokumenta za drugu osobu	Nepoznato	Detekcija lažnog dokumenta	Centralni	Administracija
Slučaj iz Makedonije 4: Zloupotreba sistema evidentiranja broja radnih sati	Pronevera Zloupotreba položaja	Izmena podataka u sistemu beleženja broja radnih sati	Da	Interna kontrola	Centralni	Administracija
Slučaj iz Makedonije 5: Zloupotreba prava administratora (bankarske garancije/ uvozne kvote)	Pronevera Zloupotreba položaja Mito	Izmena i ponovna izmena podataka Otvaranje i korištenje lažnog naloga	Da (≈160,000 evra)	Interna kontrola	Centralni	Granična administracija
Slučaj iz Crne Gore 1: Zloupotreba službenog položaja i falsifikovanje zvaničnih dokumenata	Zloupotreba položaja	Falsifikovanje podataka	Ne	Interna istraga	Centralni	Ministarstvo unutrašnjih poslova
Slučaj iz Crne Gore 2: Upotreba IT podataka sa ciljem nanošenja političke štete	Manipulacija i zloupotreba IT sistema Zloupotreba položaja	Zloupotreba IT sistema Falsifikovanje podataka	Ne	Medijski izveštaj (koji su objavili počinioci)	Centralni	Unutrašnji poslovi Tele-komunikacije

Naslov	Korupcijsko krivično delo (ne mora neophodno da bude dokazano)	Upotreba IT	Šteta za javne finansije	Kako je detektovano korupcijsko krivično delo?	Nivo državne uprave (centralni ili lokalni)	Sektor
Slučaj iz Crne Gore 3: Zloupotreba položaja i unošenje netačnih podataka u javne registre	Zloupotreba položaja Mito	Falsifikovanje podataka	Da	Interna istraga	Lokalni	Zemljišni katastar Unutrašnji poslovi
Slučaj iz Crne Gore 4: Nezakonito izdavanje putnih isprava	Zloupotreba položaja	Falsifikovanje podataka	Ne	Interna istraga	Centralni	Unutrašnji poslovi
Slučaj iz Srbije 1: Seks ispred Beogradske arene	Zloupotreba položaja	Nezakonito pribavljanje podataka Manipulacija podacima i procedurama	Ne	Medijski izveštaj	Centralni	Policija
Slučaj iz Srbije 2: Kad IT izvođač „pusti korenje“	Zloupotreba položaja Nepotizam Krivična dela vezana za nabavke	Rizici vezani za IT ponuđača Manipulacija podacima i procedurama	Da	Interna kontrola	Centralni	Pravosuđe
Slučaj iz Srbije 3: Viši državni zvaničnik špijunira zaposlene	Pronevera Zloupotreba položaja	Nezakonito pribavljanje podataka Manipulacija podacima i procedurama	Ne	Zviždač	Centralni	Ekonomija
Slučaj iz Srbije 4: „Drumska mafija”	Zloupotreba funkcija Pronevera Organizovani kriminal	Sistemi naplatne rampe su bili kompromitovani lažnim emulatorom koprocesora. Štampanje duplih tiketa sa identičnim serijskim brojevima za kamione. Nezakonito podizanje ulazne rampe	Da	Zviždač	Centralni	Transport /saobraćaj

Albanija

Priredili Edlira Nasi i Ened Kercini

Slučaj iz Albanije 1: Korupcija u TIMS sistemu granične kontrole

Slučaj u tekstu ispod tiče se zloupotrebe položaja od strane graničnih policajaca i njihove manipulacije TIMS IT sistemom (Total Information Management System – Sistem upravljanja celokupnim informacijama) kako bi se izbegla plaćanja državi za upotrebu uvezenog vozila.

Osnovne informacije

Putem specijalnog odobrenja, g. A.I. je dao pravo korištenja vozila marke „Ford“, italijanskih registarskih oznaka, g. E.H. Ovaj dokument je g. E.H. davao zakonsko pravo da se pojavi pred relevantnim institucijama i aplicira za procedure odobrenja i registracije vozila, koje je bilo uvezeno, i moralo je, u tom smislu, da prođe kroz određenu proceduru kako bi moglo biti slobodno i legalno upotrebljavano u Albaniji.

Međutim, g. E.H. je imao poznanika, g. A.T., oficira u vojnoj bazi Zall-Herr. Izgleda da je E.H., vlasnik vozila, poverio oficiru da je vozilo bilo u Albaniji već dosta dugo, ali da nije imalo odgovarajuću dokumentaciju neophodnu za evidentiranje ulaska vozila u zemlju ili njegovog uvoza, a on – kao vlasnik – nije aplicirao za dobijanje navedene dokumentacije jer su za taj proces bile vezane znatne finansijske obaveze.

A.T. je rekao E.H. da poznaje osobu koja radi u Skadru, na graničnom prelazu Murićan, koji bi mogao da „sredi“ dokumentaciju za vozilo tako da izgleda kao da je tek nedavno uvezeno u Albaniju. Naravno, za tu uslugu bi moralo nešto da se plati.

A.T. je poznavao g. A.S., koji je radio kao šef Centra za razmenu informacija sa Crnom Gorom, pri Regionalnoj upravi za granice i migracije, u Skadru. A.T. je obećao E.H. da može da mu pomogne u pribavljanju dokumenta, prema kom je vozilo ušlo u Albaniju u poslednjih nekoliko dana. U stvari, A.T. je na sebe preuzeo to da završi ovaj posao i, kao rezultat te odluke, zahtevao da mu E.H. dostavi fotokopiju pravog dokumenta kojim je evidentiran ulazak vozila u Albaniju, kako bi napravio novi dokument sa graničnog prelaza u kom bi bilo navedeno da je vozilo ušlo u Albaniju kasnije (posle 2009.). Zabeleženo je da je A.T. izjavio da je cena za tu uslugu bila oko 15.000 leka (ALL), ili otprilike 105 evra, prošle godine ali da se od tad povećala.

Kako bi se obezbedili dokument i pomoć A.S., E.H., A.T. i A.S. su se sreli 9. februara 2013. U jednom kafeu kako bi porazgovarali o detaljima. Narednog dana, E.H. i A.S. su se ponovo sreli kako bi razgovarali o dokumentu sa ulazne tačke u zemlju koji je trebalo

napraviti. Nekoliko dana kasnije, njih dvojica su se ponovo sreli i A.S. je rekao da je obavio svoj deo posla i obezbedio izveštaj sa TIMS[17] IT sistema.

Lažna evidencija u IT sistemu

Proizvedeni dokument je lažno prikazivao da je novi vlasnik automobila, E.H., ušao u Albaniju na graničnom prelazu Muričan 3. februara 2013, u 05.58, u automobilu registarskih oznaka DK***L. Ovo je takođe zabeleženo i u evidenciji koju pravi elektronski TIMS sistem.

Prema kasnijim pregledima i revizijama TIMS sistema, pokazalo se da je izmene u TIMS IT sistemu napravila druga osoba, Ad. S. Tokom razgovora između E.H. i A.T., koje je kasnije prepričao E.H., A.T., kontakt osoba, je rekao E.H. da ne mora čak ni da se pojavi na graničnom prelazu, jer će sve potrebne radnje preduzeti A.S., koji je radio na graničnom prelazu.

Sve ovo je urađeno putem pristupa elektronskim podacima u TIMS sistemu i njihovim falsifikovanjem. Sistem upravljanja celokupnim informacijama (TIMS) je velika baza podataka koja sadrži informacije o svim Albancima kojima su izdati biometrijski pasoši, tj. o većini Albanaca od trenutka kad su usvojeni biometrijski pasoši. Sistem beleži kretanje Albanaca koji prelaze granicu, na svim graničnim prelazima. Uz to, sistem čuva podatke o tome čime su osobe koje su prešle granicu putovale, tačku odakle su krenuli na put i krajnju destinaciju, kao i brojeve registarskih oznaka vozila. Ovim podacima, isto tako, mogu da pristupe i organi reda i komesarijati policije. S obzirom na to da su od 1. marta 2012. Biometrijski pasoši jedina putna isprava za Albanske građane, svi granični kontrolni punktovi koriste čitače biometrijskih pasoša i opremu za proveru otisaka prstiju. Registracija u realnom vremenu u TIMS sistemu dokumenata i njihovo očitavanje tokom ulaska/izlaska na graničnim kontrolnim punktovima, pruža mogućnost poređenja sa postojećim podacima i na taj način smanjuje mogućnost zloupotreba[18].

Glavni akter intervencije i aktivnosti na TIMS sistemu bio je Ad.S. koji je bio operater na sistemu, u jedinici Granične i migracione policije na graničnom prelazu Muričan, od 1. maja 2010. Radeći na ovoj poziciji, učestvovao je u kontroli osoba i vozila dok ih je istovremeno uvodio i u evidenciju prilikom ulaska i izlaska iz Albanije. Ad.S. je isto tako bio odgovoran za i upućen u sveukupni proces upravljanja TIMS sistemom granične kontrole kao i sistemom kamera. Njegova zaduženja su takođe bila definisana i relevantnom regulativom, koja daje smernice i postavlja standarde vršenja dužnosti za ovu poziciju. Na ovoj poziciji, on je kontrolisao i radio sa TIMS podsistemima, kao što su sistemi granične kontrole i sistem kriminalnih podataka, a imao je i dužnost da nadgleda rad ostalog pomoćnog osoblja tokom svoje smene, te da se pobrine za to da se poštuju procedure.

17 Odluka suda br. 1035, datirana 23.07.2013.
18 Razmena informacija za OEBS Kodeks ponašanja o političko-vojnim aspektima bezbednosti - Republika Albanija 2013., FSC.EMI/178/14, 22. maj 2014.

Revizija sistema, koja je obavljena kao deo istražnog procesa[19], pokazala je da je Ad.S. napravio izmene u TIMS sistemu posle čega je sistem (lažno) prikazivao da je E.H. ušao u Albaniju 9. februara 2013., što je bio način da se izbegne plaćanje relevantnih poreza i taksi. Ova aktivnost je dokazana i TIMS izveštajem koji pokazuje da je korisničko ime osobe koja je napravila ove izmene bilo ono koje je upotrebljavao Ad.S., kao i činjenicom da je, sudeći prema rasporedu posla osoblja, Ad.S. bio operater na sistemu tokom te smene.

Zbog ovih postupaka i zbog novca primljenog za navedene aktivnosti, kancelarija tužioca je podigla optužnicu protiv Ad.S., na osnovu toga što je on napravio izmene u sistemu, radeći tako suprotno javnom interesu jer je napravio lažni izveštaj koji se tiče vozila koje je pripadalo E.H.

A.S. je proglašen krivim za pasivnu korupciju javnih zvaničnika i osuđen na osam meseci do godinu dana zatvora (uslovna kazna, pod određenim uslovima). Zabranjeno mu je i da obavlja bilo kakve javne funkcije tokom perioda od godinu dana. Ad.S. je osuđen za zloupotrebu položaja i osuđen na šest meseci zatvora (uslovna kazna pod određenim uslovima). I njemu je zabranjeno da obavlja bilo kakve javne funkcije tokom perioda od godinu dana. A.T. je optužen za vršenje nezakonitog uticaja na javne zvaničnike i osuđen na šest meseci zatvora (uslovna kazna pod određenim uslovima).

Slučaj iz Albanije 2: Korupcija u elektronskom sistemu javnih nabavki

Slučaj se odnosi na intervenciju u sistemu javnih nabavki, usled korupcije, kao i intervencije u elektronskom upravljanju javnim nabavkama.

Osnovne informacije

Ispunjavajući svoju ulogu vrhovne nezavisne revizorske institucije u državi, Vrhovna državna revizorska institucija (VDRI) sprovela je reviziju Uprave za civilno vazduhoplovstvo (UCV), 2012. godine. Finalni izveštaj revizije „O implementaciji legalnosti i regularnosti ekonomsko-finansijskih aktivnosti“ UCV, za period između 1. januara 2011. i 31. marta 2012. i mere za unapređenje procesa takođe su uključivale i reviziju procedura nabavki[20].

UCV je javno telo sa finansijskom nezavisnošću, što je aspekat koji dozvoljava UCV da svoje aktivnosti sprovodi u skladu sa međunarodnim standardima i da bi zbog toga ispunila potrebu da posluje u skladu sa visokim profesionalnim standardima.

19 Ovaj slučaj je revidiran i izgrađen od strane ICS preko njihovih doušnika, međutim čini se da su IT podaci revidirani kasnije kao dokaz od strane tužilaštva

20 Celokupan izveštaj je dostupan na SSA veb sajtu http://www.klsh.org.al/web/pub/autoriteti_avia- cionit_civil_394_1.pdf

Upravljanje procedurama nabavke u Albaniji odvija se u skladu sa zakonima br. 9643, od 20. novembra 2006. „O javnim nabavkama“, br. 9880, od 25. februara 2008. „O elektronskom potpisu“ i u skladu sa Odlukom Saveta ministara br. 659, od 3. oktobra 2007. „O pravilima ponašanja u procedurama javnih nabavki elektronskim putem“, kao i u skladu sa propisima i instrukcijama Agencije za javne nabavke.

Tokom jedne od navedenih procedura nabavke, koja se odnosila na „Kupovinu kancelarijske opreme i nameštaja“, Vrhovna državna revizorska institucija ukazala je na nepravilnosti u procesu nabavke dok su odgovori zvaničnika koji su učestvovali u procesu ukazivali na to da je bilo manipulacije elektronskim potpisima tokom procesa nabavke.

Nabavka

Tokom ranije pomenutog procesa nabavke, komunikacija između članova institucije naručioca (tj. UCV), poslužile su SSA kao pokazatelj da je zaista bilo nekih aspekata elektronske nabavke koji su bili neregularni. 20. oktobra 2011., jedan od članova osoblja UCV, g. T., je saznao za potpisivanje zapisnika sa sastanka na kom je donešena odluka koja se ticala diskvalifikacije kompanije tokom pomenutog procesa nabavke.

G. T. je zatim obavestio direktore UCV da komisija koja je procenjivala ponude nikad nije obavila navedene procene elektronskim putem, pošto je on bio njen član. Štaviše, primetio je da je lozinka, koju je on kao korisnik elektronskog sistema upotrebljavao, bila promenjena, a da on o tome prethodno nije bio obavešten i da je to urađeno bez njegovog pristanka. Tako da je neko drugi završio proceduru pregleda i procene ponuda kompanija.

Uz to, posle pregleda dokumentacije koja je sadržavala ponude prezentovane u elektronskoj formi (upotrebom promenjene lozinke), g. T. je primetio da razlozi za diskvalifikaciju najniže rangirane kompanije nisu bili utemeljeni na pravno opravdanim razlozima i odredbama. Pošto je diskvalifikovana kompanija ponudila uslove koji su tačno odgovarali tehničkoj specifikaciji UCV, diskvalifikacija nije imala smisla i bila je ekonomski štetna po državni budžet i UCV.

G. T. je isto tako potvrdio da nikad nije uzeo učešća u ovoj proceni ponuda za nabavku, a nije učestvovao ni na sastanku istim povodom 2011. Verifikacija koju je ovaj gospodin postavio na portalu Agencije za javne nabavke, otkrila je da je procenu obavila treća osoba, posle promene lozinke. U kasnijem dokumentu, kao član komisije za procenu ponuda, on je negirao da je potpisao zapisnik sa sastanka koji se odnosio na taj konkretan proces nabavke.

Uprkos ovim činjenicama, VDRI napominje da direktori UCV nisu reagovali kako bi popravili nastalu situaciju preduzimanjem administrativnih mera. Kao rezultat toga, VDRI je poslala slučaj Tužilaštvu uz napomenu da su aktivnosti UCV u vezi sa nabavkom bile fiktivne, pošto su članovi grupe za procenu ponuda poricali da su učestvovali u proceni ponuda.

Slučaj iz Albanije 3: Zloupotreba IT u svrhe korupcije kod distributera električne energije

Osnovne informacije

Godine 2009. Albanija je prošla kroz proces privatizacije za 76% deonica Elektrodistribucije, pri čemu je 24% deonica Elektrodistribucije bilo u vlasništvu države Albanije, a 76% deonica je prodato privatnoj kompaniji „CEZ Distribution". Aktivnosti Elektrodistribucije regulisalo je Albansko regulatorno telo za energetiku – ARTE.

20. januara 2011., Kancelarija za zaštitu potrošača podnela je kancelariji Tužilaštva u Tirani pritužbu protiv menadžmenta kompanije „CEZ Distribution" zbog krivičnog dela „prevare" i „računarskeke prevare", u skladu sa Članovima 143 i 143/b Krivičnog zakonika. Pritužba je, uz još jednu pritužbu podnetu ranije od strane policije, navodila da je kompanija „CEZ Distribution" izdavala potrošačima račune za električnu energiju koji su sadržavali još jednu dodatnu upitnu stavku. Pod stavkom naslovljenom kao „Neevidentirana električna energija" nalazio se dodatni novčani iznos za koji je račun uvećan, za količinu energije od 4.000 kW, za domaćinstva, dok je za druge, veće potrošače ta dodatna količina električne energije iznosila 20.000 kW, uz pripadajuće uvećanje novčanog iznosa na računu. Stavka „Neevidentirana električna energija" odnosila se uglavnom na potrošače koji su imali nelegalne priključke na elektrodistributivnu mrežu, bez prethodne registracije priključka i plaćanja svih pripadajućih taksi i nadoknada, ili na potrošače koji su neovlašteno podešavali svoje strujomere da prikazuju netačna merenja. Međutim, u najvećem broju slučajeva, potrošači su se žalili na to da su na njihovim računima nedostajale informacije koje bi im ukazale na to da je uvećani iznos računa u stvari neka vrsta kazne za iznad navedene nelegalne radnje, a ne rezultat povećane potrošnje električne energije.

Putem objave, od 12. januara 2011., Regulatorna agencija za energetiku je informisala javnost, u skladu sa svojom odlukom br.90, od 15. novembra 2010., da je zaključila da je praksa uključivanja stavke „Neevidentirana električna energija" na račune za struju neprikladna i upitna. Nema podršku u zakonu i u suprotnosti je sa regulatornim okvirom koji je trenutno na snazi, i da će zbog ovakvih aktivnosti kompanija „CEZ Distribution" biti kažnjena. Kao podršku ovome, ARTE je isto tako primila i nekih 14.000 pritužbi od više građana[21] u periodu od oktobra 2010. do januara 2011., od kojih su građani već platili 490 kazni.

Prema medijskim izveštajima, u to vreme (2011. god.), Elektrodistribucija ne samo da je naplaćivala više potrošačima već je tome pridodala i zloupotrebe druge vrste, tako što je, na primer, dozvoljavala inspektorima da građane kažnjavaju bez pridržavanja procedure koju je sama Elektrodistribucija propisala. Štaviše, mediji su tvrdili da je osoblje Elektrodistribucije bilo podsticano i finansijski nagrađivano za kažnjavanje klijenata,[22]zbog

21 Odluka suda u Tirani br. 1633, datirana 30. juna 2014.
22 Skandal/CEZ faturon me shume energji sesa blen, ve gjoba fiktive per te kerkuar rritje cmimi" dated 30.11.2011. Available at: http://www.gazetatema.net/web/2011/11/30/skan-dali-cez-faturon-me-shume-energji-sesa-blen-ve-gjoba

čega su od nekih klijenata i naplaćeni mnogo veći računi[23]. Ovo, međutim, nije potvrđeno i u sudskim beleškama ili odlukama, uprkos činjenici da nijedno drugo obrazloženje nije dato za navedene postupke osoblja Elektrodistribucije.

Procenjeno je da je ukupan iznos finansijske štete za potrošače tokom ranije pomenutog perioda iznosio 4-5 miliona evra[24].

Šema naplate većih računa

Pojedinosti svake naplate računa od potrošača obrađuju operateri na terenu, koji koriste LDA (Lični digitalni asistent) uređaje. To su uređaji koje upotrebljava osoblje kompanije u vreme kada očitavaju potrošnju električne energije sa strujomera. LDA momentalno emituju (putem interneta) serveru broj ormarića, broj ugovora potrošača, očitanu vrednost na strujomeru u tom trenutku (npr. očitavanje broja utrošenih kilovat sati električne energije) i vreme i datum kada je očitavanje izvršeno. U tom trenutku, podaci o anomalijama (npr. tehnički problemi, ili nelegalno priključenje na elektrodistributivnu mrežu, itd.) takođe su registrovani tokom normalnog procesa naplate računa.

LDA očitavanja se zatim sinhronizuju sa MYAvis sistemom koji je operativan na serveru u serverskoj sobi Centra sa podacima (prenos tehnoloških podataka postiže se putem GPRS platforme) na kraju svakog dana. Podaci sa interfejsa MYAvis prolaze direktno kroz sistem ispostave računa osim u slučaju informacija blokiranih specifičnim filterima, kao što su anomalije ili sumnjive kalkulacije računa, koje se dodatno proveravaju.

U periodu kad je sud presuđivao o jednom od slučajeva, svedočenja su ukazivala na to da je za zaposlene u stvari bilo nemoguće da elektronski menjaju podatke o klijentima, pošto nisu imali administratorska ovlaštenja na sistemu. To je navelo Tužilaštvo da revidira detalje nekoliko merenja sprovedenih od strane određenih zaposlenih distribucione kompanije, protiv kojih je bilo pritužbi. Uz pomoć liste merenja utrošene energije, koja je isto tako sadržavala i podatke o mestu i vremenu kada je osoblje kompanije izvršilo očitavanje, otkriveno je da su očitavanja vršena u neuobičajeno doba dana, kao što je 22:00h, 23:00h, 24:00h, 01:00h, 02:00h, 03:00h, 04:00h, 05:00h, 06:00h, itd., uprkos činjenici da su članovi osoblja već izjavili da su očitavanja vršena u vremenu od 08:00 – 16.30h.

Uz to, distributivna kompanija je već odobrila sprovođenje određenih procedura za merenje potrošnje energije koje, između ostalog, sadrže i sveukupna pravila i procedure za regulaciju kontrolnog sistema za merenje snage kao i metodu za proračunavanje utrošene energije i druge kazne za prekršaje u merenju za ilegalno povezivanje na elektrodistributivnu mrežu.

-fiktive-per-te-kerkuar-rritje-cmimi/

23 “Hetimi, CEZ shperblente punonjesit qe mbifaturonin” http://time.ikub.al/2afad09e2d/44 5564cf92c2c-0259d0562e9238b8515/Lajm_Hetimi-CEZ-shperblente-punonjesit-qe-mbifaturo-nin-abonentet.aspx

24 “Prokurorët, hetim 14 mijë ankesave për mbifaturim energjie” dated 27.11.2011 – available at http://www.shqip-tarja.com/lajme/2706/prokuroret-hetim-14-mije-ankesave-per-mbifaturim-energjie-65833.html

Ovaj propis jasno utvrđuje da očitavanje i kazna moraju da se dese u prisustvu potrošača ili njihovih rođaka (uz fotografije, video snimke i bilo kakve druge dokaze koji potvrđuju da je bilo intervencije na strujomeru). U slučaju odsustva potrošača ili njihovih rođaka ili ukoliko potrošač odbije da potpiše službenu zabelešku sa očitavanja, zabelešku moraju da potpišu članovi drugog tima kompanije (NTL tim). Iz zabeleški sa očitavanja bilo je jasno da zabeleške nisu potpisali ni potrošač ni članovi NTL tima, u vreme kada su ispostavljeni previsoki računi ili kazne za ilegalno povezivanje na elektrodistributivnu mrežu. Ono što je indikativno je da su samo 21. oktobra 2010. zabeležene kazne za oko 17 ilegalnih povezivanja na elektrodistributivnu mrežu, i to sve u razmaku od po 2 minuta jedna iza druge ili čak istovremeno[25].

Više od 10 ljudi je osumnjičeno za učešće u ovoj šemi naplate previsokih računa. Još ovakvih šema je otkriveno posle ovog slučaja i sudski su procesuirane. Sud je već osudio nekoliko članova osoblja kompanije, dok se još uvek čeka na suđenja drugih članova osoblja. Iako je u iznad navedenom slučaju naplata previsokih računa vršena putem LDA uređaja, i u drugim slučajevima takođe postoje navodi o izmeni elektronskih podataka, nakon što su registrovani pomoću LDA uređaja[26].

Slučaj iz Albanije 4: Pronevera i falsifikovanje u knjigovodstvu

Ovaj slučaj se tiče službenice odgovorne za vođenje knjiga, koja je, tokom dugog niza godina, vršila proneveru novca kojim je raspolagala i deponovala ga na svom bankovnom računu.

Optužena g-dja M.K. je bila šef računovodstva Regimente komandosa u vojnoj bazi Zall-Herr u Tirani. Na ovoj poziciji, M.K. je vršila radnje u suprotnosti sa zakonom, otuđujući novčana sredstva i stavljajući ih na svoj bankovni račun, putem falsifkovanja dokumentacije i drugih podataka.

Godine 2009., Odsek unutrašnje revizije Ministarstva odbrane sproveo je „Tematsku reviziju implementacije legislative na snazi kojom se regulišu plate i dodaci platama zaposlenih u Regimenti komandosa Zall-Herr“. Revizija je otkrila da je M.K., na svojoj poziciji šefa računovodstva, falsifikovala dokumentaciju, konkretno platne spiskove zaposlenih Vojnog odseka 1200[27].

25 Odluka suda u Tirani br. 1633, datirana 30.06.2014.
26 “Prokuroria: Skema si CEZ vidhte 15 mijë konsumatorë” dated 15.04.2013 Dostupno na: http://gazeta-shqip.com/lajme/2013/04/15/prokuroria-skema-si-cez-vidhte-15-mije-konsu-matore/
27 Zasnovano na Odluci okružnog suda u Tirani br. 41 datiranoj 20.01.2012.

Forenzičkom istragom računovodstva utvrđeno je da je M.K. proneverila ukupno 8.668.886 ALL (61.920 evra), od kojih je 6.198.326 ALL bilo rezultat neto uvećanja plata, a ostalih 2.470.560 ALL dodataka na plate, dnevnice, usluge, itd. Sva novčana sredstva potekla su iz državnog budžeta i iz fonda namenjenog posebno za vojnu jedinicu br.1200 iz Zall-Herra u Tirani.

Način organizacije rada u kancelariji bio je takav da je finansijski specijalista policije vršio samo one dužnosti koje mu je naznačio šef računovodstva, konkretno izvođenje i priprema platnih spiskova. Međutim, finansijski specijalista nije nadgledao sumiranje platnih spiskova i neto zarade zaposlenih, pošto je ove platne spiskove pripremala šefica računovodstva, odnosno M.K.

Pošto su platni spiskovi pripremljeni, predaju se, putem i-mejla ili drugim elektronskim putem, na odobrenje i načelniku štaba i komandantu regimente. Ona je uspela da falsifikuje platni spisak i dobije odobrenje od načelnika štaba i komandanta tako što bi prvo dobijala pismeno odobrenje, a zatim menjala elektronske podatke koji su se odnosili i na platni spisak i na banku.

Banka ne snosi nikakvu odgovornost za neslaganja u platama, pošto banka nije bila u mogućnosti da kontroliše podatke ili da ima pregled plata, čak iako su se iznosi koji su prenošeni na račun M.K. činili višim od onoga što bi se moglo smatrati razumnim iznosom plate. Pošto bi sredstva legla na njen račun M.K. bi ih podizala sa računa i krila na razne načine.

M.K. je sud proglasio krivom i osudio na godinu dana zatvora[28].

28 Ibid.

Bosna i Hercegovina

Pripremili Aleksandra Martinović i Srđan Nogo

Slučaj iz Bosne i Hercegovine 1: Hakovanje i-mejla Glavnog tužioca

Svi relevantni domaći i međunarodni izveštaji o sistemu prvosuđa u Bosni i Hercegovini (BiH), uključujući i godišnje izveštaje o napretku Evropske komisije, ukazuju na to da pravosuđem dominira, da ga kontroliše i na njega utiče politička elita, sa konstantnim političkim pokušajima da se poveća uticaj na imenovanje sudija i tužilaca kroz čitavo pravosuđe BiH. Kompleksna i sumnjiva priroda pravosudnog sistema BiH i njegovi nedostaci u smislu nezavisnosti i nepristrasnosti mogu se dočarati kroz slučaj jednog od državnih tužilaca (dalje u tekstu: g.X), koji je optužen da je hakovao i-mejl bivšeg Glavnog tužioca (dalje u tekstu: g.Y) kako bi ga diskreditovao neposredno pre suspenzije sa dužnosti.

Mogući motiv zloupotrebe i-mejla g.Y od strane g.X može se naći u njegovoj izjavi po suspenziji g.Y, kada je zabeleženo da je rekao da će konkurisati za mesto Glavnog tužioca BiH. Takođe su postojale i glasine da je g.X štitio neke optužene koje je g.Y gonio po službenoj dužnosti.

Smatra se da su i g.X i g.Z bili povezani sa određenim političkim partijama u BiH. Konkretno, g.Y je navodno bio povezan sa Strankom nezavisnih socijaldemokrata (SNSD) koja je vodeća partija u Republici Srpskoj i jedna od najuticajnijih partija u BiH, dok je g.X u to vreme navodno bio povezan sa Socijaldemokratskom partijom BiH (SDP), najjačom partijom u Federaciji Bosne i Hercegovine, ali isto tako i sa Zajednicom za bolju budućnost BiH.

Tokom istrage koja je usledila potvrđeno je da se g.X ulogovao na i-mejl g.Y i poslao lažne „Opšte instrukcije“ na adrese zaposlenih u Tužilaštvu BiH i nekoliko medija u Federaciji BiH. „Opšte instrukcije“, koje su sadržavale kompromitujuće izjave, poslate su 29. juna 2011., u dokumentu sa zaglavljem kancelarije Tužioca BiH, sa falsifikovanim potpisom Glavnog tužioca.

U ovim „Opštim instrukcijama“ stajalo je da je strogo zabranjeno svim zaposlenima u Tužilaštvu BiH da daju bilo kakve komentare na negativne medijske izveštaje o Glavnom tužiocu, naročito o onima vezanim za, u to vreme, aktuelnim aferama „Prisluškivanje“, „Reket“ i druge, u koje je Glavni tužilac navodno bio umešan u to vreme.

„Instrukcije“ su takođe branile ljudima da čitaju časopise „Slobodna Bosna“, „Dani“, „Oslobođenje“, „Avaz“ i „San“, koji se izdaju u Federaciji BiH, ili da gledaju bilo koje programe koje je emitovala Federalna televizija (jedan od tri javna servisa u BiH), naročito TV program „60 minuta“, koji se emitutuje na ovoj televiziji.

U „Opštim instrukcijama“ takođe je stajalo da su *„tužioci koji misle da će se početi sa održavanjem redovnih mesečnih sastanaka, u smislu Člana 20, stav 2 Pravilnika, budale.“*

Pošto je saznao za ovaj i-mejl, Glavni tužilac BiH podneo je tužbu protiv nepoznatog počinioca Sudu BiH i Tužilaštvu BiH, posle čega je izdata naredba Federalnoj policiji (u okviru Ministarstva unutrašnjih poslova BiH) da započne istragu.

Tokom istrage, inspektor koji je vodio borbu protiv računarskog kriminala u federalnom Ministarstvu unutrašnjih poslova, utvrdio je da je i-mejl Glavnog tužioca zloupotrebljen putem mobilnog telefona (iPhone 4), registrovanog na majku g.X, ali koji je koristio isključivo on. Navodno je g.X nekako došao u posed lozinke za i-mejl Glavnog tužioca, a zatim je upotrebio da se uloguje na njegov i-mejl nalog sa udaljene lokacije i da pošalje instrukciju. Uprkos činjenici da su bile aktivne sve relevantne mere bezbednosti, kako bi se sprečila upravo ovakva vrsta zloupotrebe, izgleda da je ljudski faktor bio odlučujući u ovom slučaju. Po završetku istrage, izveštaj, koji je sadržavao detalje krivične optužbe protiv tužioca g.X za zloupotrebu položaja, falsifikat i prevaru, predat je nadležnoj kancelariji tužioca (tačnije Tužilaštvu BiH – Odseku za organizovani kriminal i korupciju).

Prema nekim medijskim izvorima, uprkos znatnim naporima kolega g.X, iz Tužilaštva, da zataškaju ovaj skandal bez presedana, kancelarija Disciplinskog saveta , u okviru Visokog sudskog i tužilačkog saveta (VSTS) BiH informisana je o slučaju.

Međutim, to nije bila jedina optužba protiv državnog tužioca g.X. On je isto tako optužen i za to da je počinio još dva disciplinska prekršaja. Konkretno, naredio je uništenje zabeleški o izjavama svedoka, u prisustvu tih istih svedoka i poslao je zahtev za informacije direktoru Federalne policijske uprave sa sadržajem koji nije bio prikladan za zvaničnu korespondenciju i funkciju koju je g.X obavljao u tom trenutku. Konkretno, g.X je zahtevao, na veoma neprikladan način, da direktor otkrije izvor informacije i pregleda zvaničnu policijsku zabelešku koja je optuživala g.X, visoke zvaničnike Vlade Federacije BiH i Socijaldemokratske Partije BiH za organizovanje zavere protiv direktora Federalne policijske uprave.

Više od godinu dana kasnije, 26. septembra 2012, kancelarija Disciplinskog saveta VSTS BiH došla je do zajedničke nagodbe sa g. X o određivanju disciplinske odgovornosti i disciplinskog postupka. On je tom prilikom priznao i prihvatio odgovornost za disciplinske prekršaje, a kancelarija Disciplinskog saveta je povukla zahtev za utvrđivanjem njegove disciplinske odgovornosti za određene stavke iz disciplinske žalbe.

Prilikom preporuke disciplinske mere, kancelarija Disciplinskog saveta imala je na umu to da je *„optuženi imao uspešnu karijeru kao javni tužilac i da je bio angažovan na kompleksnim slučajevima koji su zahtevali visok nivo stručnosti i posvećenosti“.* Činjenica da je bio porodičan čovek i otac malog deteta, kao i činjenica da je bio opterećen dugom, uzete su u obzir kao olakšavajuće okolnosti. Činjenica da je protiv njega u toku bio još jedan predistražni postupak u vezi sa optužbama za uzimanje mita nije čak ni uzeta u razmatranje.

Prvostepena Disciplinska komisija tužilaca VSTS prihvatila je nagodbu između g. X i kancelarije Disciplinskog saveta i odlučila da je g. X odgovoran za tri disciplinska prekršaja i za kršenje Etičkog kodeksa tužilaštva. To je ocenjeno kao ozbiljno kršenje službene dužnosti, koje je dovodilo u pitanje poverenje javnosti u kredibilitet Tužilaštva i štetilo ugledu Tužilaštva BiH. Kažnjen je sa umanjenjem plate od 10% tokom perioda od šest meseci.

Samo dan pošto je njegov i-mejl hakovan, g. Y, Generalni tužilac u tom trenutku, je suspendovan sa dužnosti zbog svojih „neprikladnih poznanstava“ sa međunarodnim krijumčarima oružja. Postojale su brojne službene zabeleške (fotografije i zvučni zapisi) njegovih sastanaka i telefonskih razgovora sa trgovcem oružjem stavljenim na crnu listu UN, koje su ukazivale na to da je g. Y primao novac i skupe poklone zato što je pomagao kriminalnoj mreži. Na kraju, korupcija nije dokazana. G.Y je izjavio da žali što su njegovi neprikladni sastanci naškodili ugledu Tužilaštva BiH te se i on nagodio sa VSTS i postavljen je na nižu poziciju – nastavio je da radi kao tužilac za ratne zločine u Tužilaštvu BiH, a njegova disciplinska kazna bila je umanjenje plate za 10% tokom perioda od tri meseca.

Slučaj iz Bosne i Hercegovine 2: Još jedno moguće kontroverzno zaposlenje u Vrhovnoj revizorskoj instituciji u Republici Srpskoj

Vrhovna revizorska institucija Republike Srpske (VRIRS) oglasila je upražnjena radna mesta sa stalnim zaposlenjem za „dva **mlađa** revizora“. Oglas je objavljen u Službenom glasniku Republike Srpske, 3. maja 2014., kao i na vebsajtu institucije (29. aprila 2014.) kao i u medijima. Krajnji rok za prijavu na oglas je bio 30 dana nakon dana objave.

Tokom tog perioda, ukupno 61 kandidat se prijavio za ova radna mesta, a oni koji su ispunjavali zahtevane opšte i posebne kriterijume i koji su podneli svu traženu dokumentaciju i potvrde pozvani su da polažu pismeni test.

Test je sproveden 18. juna 2014., u IT kabinetu Ekonomskog fakulteta u Banja Luci, elektronskim putem, uz korištenje računara u toj prostoriji.

Kao i prilikom prethodnih iskustava sa sprovođenjem takvih testova, radovi svih kandidata je trebalo da budu odštampani neposredno nakon završetka testa, kopirani na USB uređaj, koji pripada VRIRS, i izbrisani iz memorije računara na Ekonomskom fakultetu. Takođe, svaki kandidat koji je normalno polagao test imao je pravo da kopira svoj test na USB uređaj.

Ali ovog puta je nešto pošlo naopako. Iako nema zvanične potvrde za ovo, navodno su neki podaci izgubljeni zbog problema sa IT sistemom Ekonomskog fakulteta. Postoji nekoliko špekulacija unutar VRIRS-a da ili nisu bili odštampani svi testovi ili da nisu svi propisno

snimljeni tako da neki podaci nedostaju, ili čak da je sa tehničkom opremom sve u redu, ali da testove drži u tajnosti uprava VRIRS-a (uključujući članove komisije odgovorne za proceduru selekcije) kao izgovor za diskutabilan izbor jednog od kandidata.

U svakom slučaju, nisu postojale propisne mere bezbednosti i njihovo odsustvo je omogućilo da se ovo desi. Na primer, umesto da su kandidati prilikom testiranja koristili neki bezbedan softver, oni su svoje radove pisali u prostom Word formatu bez ikakve zaštite tako da je bilo koja osoba iz nadležne komisije imala priliku da napravi izmene na radovima. Štaviše, ovaj put kandidatima nije bilo dozvoljeno da prave kopije testova na svojim USB uređajima i testovi im nisu dati na pregled.

Uprkos tome što nikakvi rezultati testa nisu objavljeni, kandidati iz užeg izbora pozvani su na razgovor, 25. i 26. juna 2014. i, sudeći prema informaciji objavljenoj na veb sajtu VRIRS-a, *„komisija odgovorna za proceduru izbora odredila je listu uspešnih kandidata i poslala je glavnom revizoru“*. Na osnovu predložene liste, koja još uvek nije dostupna javnosti, glavni revizor je odabrao dva kandidata.

Dok za prvog kandidata nisu bile vezane nikakve kontroverze, već postoje neki napisi u medijima o kontroverzama vezanim za izbor drugog kandidata. Ovaj slučaj je privukao pažnju zbog sumnje drugih kandidata (pobuđenih manjkom transparentnosti u gore navedenim procedurama). Zbog toga su neki kandidati podneli žalbe VRIRS-u.

Što se tiče bezbednosnih mera za sprečavanje ovakvih problema u budućnosti, prema izvorima unutar VRIRS-a, još ništa nije urađeno. Uz činjenicu da odabrani kandidat ima istoriju ugrožavanja javnog reda i mira, njegov izbor na poziciju mlađeg revizora u 48. godini života je prilično diskutabilan. Propozicije za to radno mesto uključuju samo godinu dana potrebnog prethodnog radnog iskustva i nije eksplicitno navedeno da je neophodno iskustvo iz sektora revizije. U tim godinama, odabrani kandidat je verovatno previše kvalifikovan i mogao bi pre da bude izabran za neku drugu, višu poziciju.

Prema nekim medijskim spekulacijama, on je doveden na tu poziciju od strane izvesne političke partije, što bi moglo da ga učini podložnim uceni od samog početka njegovog novog radnog odnosa. Ukoliko se pojave neki dokazi koji bi potvrdili ove navode, za očekivati je da se od njega traži da za uzvrat učini neke kontrausluge – radi zaštite interesa političkih elita i da spreči otkrivanje informacija i dokaza o koruptivnim radnjama u javnim institucijama, koje podležu javnim revizijama, te da se odgovorni za te radnje sudski gone.

Uz ovu priču o kontroverznim imenovanjima i zapošljavanju u VRIRS-u, tokom poslednjih nekoliko godina, vredno je pomenuti i slučaj imenovanja novog glavnog revizora. Konkretno, prvi izbor za tu poziciju Komisije Skupštine Republike Srpske, nadležnog za odabir kandidata, bila je osoba koja je sumnjičena da je došla do lažne diplome fakulteta. Usled jakog pritiska medija, do njegovog imenovanja ipak nije došlo.

Slučaj iz Bosne i Hercegovine 3: Zloupotreba elektronskog sistema projekta CIPS

Projekat Sistem za zaštitu identifikacije građana (CIPS) započet je u Bosni i Hercegovini u aprilu 2002., kada je privremeno uspostavljena uprava za njegovu implementaciju. Glavni zadatak projekta bio je da uspostavi deo sistema uz pomoć kojeg bi se primenjivao Zakon o centralnoj evidenciji i razmeni podataka.

Godine 2008., u skladu sa strategijom za razvoj identifikacionih dokumenata, Uprava je postala Agencija za identifikacione dokumente, evidenciju i razmenu podataka (IDDEEA) Bosne i Hercegovine. Ova institucija prati, koordiniše i institucionalno upravlja oblašću identifikacionih dokumenata, primenjujući relevantne standarde i propise Evropske zajednice i razvijajući se u skladu sa takvim standardima. Odgovorna je za personalizaciju i tehničku obradu sledećih identifikacionih dokumenata: ličnih karti, ličnih karti za strance, vozačkih dozvola, putnih isprava, dokumenata za registraciju vozila i druga identifikaciona dokumenta uz pristanak nadležnih organa i uz Posebnu odluku Saveta ministara.

Od najranijih faza CIPS projekta, zabeležen je znatan broj pritužbi na zloupotrebu njegovog elektronskog sistema, naročito kod izdavanja ličnih karti i pasoša, u čitavoj zemlji.

Tužilaštvo BiH naredilo je sveobuhvatnu istragu, koja je sprovedena uz zajedničke napore nekoliko institucija u BiH: Državne agencije za istrage i zaštitu (SIPA), nekoliko odgovornih ministarstava unutrašnjih poslova i uprava policije i Policijske misije evropske zajednice (EUPM) u BiH.

Prva velika operacija sprovedena je 28. maja 2008., kada je uhapšeno 20 osoba iz nekoliko gradova u BiH. Za ovim je usledilo još nekoliko hapšenja, tokom 2009. Uhapšene osobe bile su uglavnom vršioci javnih funkcija, kao što su policajci, zaposleni u opštinskoj administraciji i arhivari, ali bilo je isto tako i osoba koje nisu bili vršioci javnih funkcija. Nekoliko vršilaca javnih funkcija su bili osumnjičeni da su bili uključeni u organizovani kriminal, kroz zloupotrebu svojih finansijskih i tehničkih resursa, omogućavajući tako čitavim organizovanim grupama da ostvare nezakonitu materijalnu korist.

Prvi u lancu bili su zaposleni u policiji, odgovorni za izdavanje ličnih dokumenata. Oni su imali pristup registru centralne evidencije, koji je deo sistema Agencije u kom se pohranjuju podaci o svim građanima BiH. Policajci su koristili svoje službene računare i ovlašćenja da uđu u sistem i izmene podatke. Uglavnom bi pronašli osobu u bazi podataka koja je imala državljanstvo BiH ali nikad nije dobila ličnu kartu (npr. ukoliko je osoba otišla u inostranstvo za vreme rata i nije se vraćala). Zatim su osobu koja je želela da dobije lažnu ličnu kartu slali u arhivu (drugi deo organizovane kriminalne grupe koja je operisala u okviru opštinske administracije) gde bi dobila izvod iz matične knjige rođenih i potvrdu o državljanstvu na lažno ime, što je bilo dovoljno da se započne procedura za dobijanje lične karte. Korišteni su čak i podaci preminulih osoba; umesto da zvanično zavedu nečiju smrt,

oni su prijavljivali da je preminula osoba izgubila postojeću, vežeću ličnu kartu, a zatim pokretali proceduru za izdavanje nove lične karte.

Kao što je izjavilo tužilaštvo BiH, *„osumnjičeni su optuženi za zloupotrebu sistema za izdavanje ličnih dokumenata u BiH na taj način što su građanima BiH i drugih država omogućili izdavanje originalnih ličnih dokumenata BiH, koja su sadržavala lažne informacije o identitetu osoba ili njihovoj nacionalnosti".*

Istraga je pružila dokaze da su nezakonito izdata lična dokumenta u znatnoj meri korištena za kriminalne aktivnosti u različitim delovima zemlje i regiona. Na primer, bilo je osumnjičenih koji su bili članovi Zemunskog klana, osumnjičenih za ubistvo bivšeg srpskog premijera, Zorana Đinđića, za pokušaj ubistva srpskog političara Vuka Draškovića, kao i nekoliko drugih članova kriminalnog podzemlja koji su dobili lažna idetifikaciona dokumenta BiH.

Takođe su postojale i sumnje da su uhapšene osobe prodavale originalne lične karte i pasoše BiH sa lažnim identitetima za 2.000 €. Samo u Banja Luci izdato je više od 200 nelegalnih ličnih karata i pasoša.

Ovaj krupni slučaj naneo je veliku štetu reputaciji javne službe u celoj zemlji. Kao rezultat toga, pokrenut je znatan broj izmena i procedura kako bi se sprečila pojava sličnih slučajeva u budućnosti. Na primer, procedure u kancelariji arhivara su znatno ojačane tako da nije više moguće izvaditi izvod iz matične knjige rođenih i potvrdu o državljanstvu za treću osobu bez odobrenja te osobe. Isto tako postoje i dodatne elektronske provere u kancelarijama arhivara, ministarstvima unutrašnjih poslova i u drugim nadležnim administrativnim organima za utvrđivanje identiteta, boravka i drugih relevantnih podataka o osobama kada im se izdaju lična dokumenta.

Hrvatska

Priredili Zorislav Petrović i Ivana Andrijašević

Slučaj iz Hrvatske 1: Poziv od doktora radi glasanja

Tokom kampanje za lokalne izbore, u maju 2013., građani Dubrovnika, koji su bolovali od dijabetesa, primili su pismo od dijabetologa u Opštoj bolnici u Dubrovniku, koji se kandidovao za gradonačelnika. Mnogi od njegovih pacijenata primili su pismo lično od njega, u kom ih on podseća na svoju kandidaturu, ističući istovremeno da je spreman da im pomogne: *„(...) moj prvi izbor je da vam budem na usluzi, dragi moji pacijenti“*. Takođe je podsetio svoje pacijente na veliki napredak ostvaren osnivanjem najmodernijeg centra za dijabetes i spomenuo da *„ove godine proslavljamo 20 godina Udruženja za dijabetes“*. Kada je jedna grupa aktivista otkrila ovo, momentalno su zahtevali istragu od Državnog tužilaštva Republike Hrvatske (DORH) u Dubrovniku.

Istraga je odmah pokrenuta i njome je otkriveno da je kol centar Hrvatske narodne stranke (HNS), čiji je doktor bio član, nazvao ukupno 3.133 fiksna telefonska broja u Dubrovačko-neretvanskoj županiji i da su 3.215 (98%) bili brojevi njegovih pacijenata. Svi ti brojevi, sa imenima i adresama, bili su pohranjeni u ličnim kartonima, u Klinici za dijabetes i endokrinologiju, gde je on radio. Za DORH u Dubrovniku tako visok procenat *„je bio jasna indikacija da je za izbornu kampanju dijabetologa upotrebljen registar pacijenata, koji je sadržavao njihove lične podatke“*. Međutim, on je porekao da je ikad od kog tražio da mu dostavi takve podatke za izbornu kampanju.

Tokom istrage, DORH je otkrio da su brojne osobe u Opštoj bolnici u Dubrovniku imale pristup spiskovima pacijenata i njihovim ličnim podacima. Štaviše, DORH je otkrio da je spisak koji je upotrebljen u kol centru HNS napravilo više osoba i da je korišteno više različitih izvora. Stoga „*nje bilo moguće utvrditi odakle i od koga su dobijeni podaci“* te zato nije ni bilo osnove za dalje gonjenje kandidata za gradonačelnika.

Tokom istrage, on je tvrdio da je koristio javno dostupne podatke za slanje pisama, a da je mogao jedino da dođe do podataka svojih pacijenata ali ne i pacijenata drugih doktora. Pa ipak, druga doktorka, koja je radila na istoj klinici gde i dijabetolog u pitanju, potvrdila je da je svako sa osnovnim poznavanjem sistema mogao da pristupi kompletnim registrima pacijenata. Ona je tvrdila da joj je on lično dostavio podatke o svim pacijentima za jednu studiju na kojoj je radila. Administrator je potvrdio da većina medicinskih sestara i doktora imaju ovlašćenje za pristup tim podacima. Administrator je isto tako potvrdio da je on dostavio podatke jednom drugom doktoru i sestri na njihov zahtev, jer su im trebali za „neku godišnjicu“.

Kao rezultat odluke DORH da ne goni kandidata za gradonačelnika, 5. marta 2014., Klub gradskih većnika „Srđ je naš“ obavestio je Hrvatsko udruženje za promociju prava pacijenata o ovom slučaju zloupotrebe podataka pacijenata. Cilj ovog obaveštenja bio je

da se zatraži od udruženja da upotrebi svoj uticaj i podrži zahtev većnika upućen DORH da prepusti ovaj slučaj kancelariji DORH van Dubrovnika.

Samo nekoliko dana kasnije, 7. marta 2014. udruženja su se okupila u „Platformu 112“ da podnesu tužbu protiv kancelarije DORH u Dubrovniku zbog sumnje na političku korupciju. Jedna od optužbi tvrdila je da je, uprkos dokazima, ova kancelarija neosnovano odbacila optužbe protiv dijabetologa. Isto tako su obavestili Hrvatskog narodnog ombudsmana o tome da nije bilo istrage ovog slučaja od strane Hrvatske agencije za zaštitu ličnih podataka i kritikovali Hrvatsku medicinsku komoru.

Postoje bar tri moguća scenarija zloupotrebe IT u ovom slučaju:

a) privatni podaci pacijenata pribavljeni su nezakonito od strane nekoga u dubrovačkoj Opštoj bolnici, verovatno nekoga bliskog kandidatu za gradonačelnika, isključivo u svrhu kreiranja mejling liste za lokalne izbore;

b) neko je spolja provalio u bazu podataka – bila je hakovana i niko iz bolnice ne bi mogao biti direktno odgovoran za to;

c) neko iz bolnice je uzeo podatke radi druge namene a zatim je neko blizak kandidatu za gradonačelnika isto tako došao do tih podataka.

Slučaj iz Hrvatske 2: Baza sa poverljivim podacima Hrvatske radio-televizije na crnom tržištu

Prema Zakonu o Hrvatskoj radio televiziji (HRT), svako fizičko i pravno lice u Hrvatskoj koje poseduje TV ili radio aparat obavezno je da plaća pretplatu. HRT vodi i upravlja registrom mesečnih pretplatnika HRT u Republici Hrvatskoj. Ovaj registar nije dostupan javnosti. Pošto sadrži lične podatke korisnika, kao što su ime i prezime, adresa, lični identifikacioni broj (Osobni identifikacioni broj - OIB), itd., upravljanje njime i njegovo korištenje zaštićeni su odredbama legislative koja se odnosi na zaštitu ličnih podataka. Prema informacijama iz javno dostupnog Centralnog registra, sa podacima o sistemima zbirki ličnih podataka u Agenciji za zaštitu ličnih podataka, registar HRT nalazi se na serveru kome fizički pristup imaju isključivo osobe sa ovlašćenjem. Ovlašteni korisnici koriste podatke iz registra unoseći svoje korisničko ime i lozinku ili sertifikat. Aplikacija je dostupna putem lokalne mreže i interneta, korištenjem zaštićenih tunela za podatke. Konačno, rezervne kopije(backup) se nalaze u serverskoj sobi.

Međutim, 2014, CD koji je sadržavao kopiju ove baze podataka pojavio se na crnom tržištu. Navodno, CD je napravio zaposleni u HRT-u, koji radi sa tom bazom podataka i ostvaruje profit od njene nelegalne prodaje.

U ovom slučaju, IT je zloupotrebljena u svrhu namernog kopiranja i prodaje podataka od strane zaposlenog u HRT-u, koji je ili imao pristup registru ili je znao nekoga sa pristupom registru. Kao rezultat, sve gore pomenute tehničke mere obezbeđenja su probijene, a isto tako su i prekršene odredbe Opštih pravila rada i ponašanja na HRT-u, prema kojima zaposleni HRT-a moraju da rade u skladu sa najvišim poslovnim standardima i osnovnim etičkim standardima, zasnovanim na nekoliko vrednosti, uključujući i poverljivost i zaštitu podataka, u skladu sa relevantnom legislativom i opštim pravlima. Očigledno, ovi standardi nisu bili primenjeni.

Član Upravnog odbora NVO „Potrošač" („The Consumer"), prijavio je ovaj slučaj Odelenju za privredni kriminal (OPK) Ministarstva unutrašnjih poslova. Zbog čestih žalbi od dalmatinskih pretplatnika koji su se osetili uznemiravanim od strane raznih kompanija koje nude svoje usluge putem kataloške ponude, koristeći adrese iz baze podataka HRT-a 2004. godine, HRT je organizovao internu istragu aktivnosti odseka za prikupljanje pretplate. Međutim, istraga nije dala rezultate i pretplatnici su i dalje bili meta za razne senzacionalne ponude kompanija.

Slučaj iz Hrvatske 3: U potrazi za veteranima

Godinama se jedna od najvećih rasprava u hrvatskom društvu vodila oko pokušaja utvrđivanja tačnog broja ratnih veterana. Uvek su postojale spekulacije da je mnogo više ljudi bilo uključeno u odbranu zemlje tokom Rata za nezavisnost nego što se to navodi u zvaničnoj evidenciji. Pošto zvanični podaci o ovom pitanju nisu nikad objavljeni, to je bila jedna od glavnih tema u političkim sučeljavanjima između vladajuće, nacionalističko-konzervativne partije HDZ (Hrvatska demokratska zajednica) i opozicije. HDZ nikad nije bila voljna da objavi registar veterana i opozicija ih je optuživala da kriju te podatke kako bi na taj način omogućili velikom broju ljudi, koji na to u stvari nisu imali pravo, da uživaju privilegije namenjene ratnim veteranima. Veteranima su omogućene brojne privilegije, počevši od visokih penzija, besplatnih stanova i privilegija prilikom kupovine vozila. Prema tvrdnjama opozicije, HDZ je na ovaj način kupovao podršku u narodu. 6. aprila 2010, veb sajt www.registarbranitelja.com iznenada je objavio nepotpuni spisak veterana[29]. Autori sajta bili su anonimni i, kako su napisali na sajtu, cilj im je bio da zaustave korupciju i da nateraju hrvatske vlasti da objave potpuni spisak veterana.

Ovo objavljivanje je izazvalo burne reakcije u čitavoj zemlji. Tadašnja premijerka, Jadranka Kosor, ga je nazvala „delom obaveštajnog podzemlja", a Ministarstvo unutrašnjih poslova je odmah objavilo da se radi o krivičnom delu za koje sledi kazna do tri godine zatvora. Ministarstvo odbrane i Ministarstvo za pitanja boraca zahtevali su hitnu istragu od strane

29 Veterani su bili uključeni u odbranu kroz Ministarstvo odbrane i Ministarstvo unutarnjih poslova – Ovaj spisak sadržao je samo lica uključena preko Ministarstva odbrane.

Državnog tužilaštva. MO je isto tako objavilo da njegov IT sistem nije ugrožen i da nije pretrpeo nikakav pokušaj računarskog napada.

Bivši Ministar za pitanja boraca tvrdio je da su mnoge osobe imale pristup takvim podacima. On je tvrdio da je 2003, kada je bio na dužnosti, primio te podatke na CD-ovima. Prema Pančićevim rečima Vlada je mogla da otkrije kada su podaci ukradeni prosto upoređujući objavljene informacije sa registrom postojećeg stanja. *„Kada sam ja bio Ministar, bilo je 430.000 veterana, a sada ih ima više od 500.000...možda je neko ukrao CD pre šest godina i objavio ga tek danas“*, rekao je Pančić

Nekoliko dana kasnije, policija je otkrila podatke kod četvorice bivših zaposlenih u Kancelariji za odbranu (ogranak Ministarstva odbrane) u Karlovcu i osumnjičila ih da su ukrali podatke. Istraga je pokazala da su zaista ova četvorica objavili podatke na internetu ali i da su zaposleni u Kancelariji za odbranu, njih ukupno 23 imali pristup istim podacima. Nisu podignute optužnice protiv četvorke iz Karlovca. Nadalje, nije bilo nikakvih drugih novosti u medijima o nekom drugom ko je optužen za upad. Hrvatska Vlada je zahtevala od kompanije koja je hostovala veb sajt www.registarbranitelja.com da skine informacije sa sajta ali je vlasnik kompanije to odbio. Registar veterana stajao je na veb sajtu do aprila 2012. kada je istekao domen. Zvanični registar je objavljen 19. decembra 2012. i uključivao je većinu podataka objavljenih na neoficijelnom sajtu.

Ovo je primer zloupotrebe položaja. Pošto su podaci objavljeni, možemo da pretpostavimo da je neko iz Kancelarije za odbranu uzeo podatke, objavio ih, ili ih dao, ili ih čak prodao nekom ko ih je onda objavio. Moglo bi da postoji mnogo različitih motiva za objavljivanje registra, počevši od političkih sukoba do plemenitih motiva, kao što je pokušaj da se poveća transparentnost. Ipak, nema sumnje da je glavni razlog zašto se to desilo bio manjak minimalnih bezbednosnih protokola prilikom rukovanja podacima kojima raspolažu kancelarije za odbranu u različitim hrvatskim gradovima.

Slučaj iz Hrvatske 4: Uz malu pomoć državnih službenika, 68 hrvatskih pasoša prodato kriminalcima

U združenoj akciji Ministarstva unutrašnjih poslova Republike Hrvatske (MUP) i Kancelarija za suzbijanje korupcije i organizovanog kriminala (USKOK), pod šifrovanim nazivom „Border“, identifikovano je sedam lica koja su optužena za falsifikovanje i prodaju hrvatskih pasoša kriminalcima iz Srbije, Bosne i Hercegovine i Crne Gore. Od 2006. do kraja 2010. grupa je prodala 68 pasoša po ceni od 10.000 € po komadu, zarađujući na taj način najmanje 680.000 €.

Jedna državna službenica iz Hrvatskog konzularnog ureda u Orašju, u Bosni i Hercegovini, nije izvedena pred sud jer se nagodila sa USKOK i prihvatila kaznu od jedne godine

zatvora. Druga, koja je radila kao viši službenik u pasoškom odeljenju Zagrebačke županijske policijske uprave, optužena je za zloupotrebu položaja i osuđena na 13 meseci zatvora. Pet drugih članova ove kriminalne organizacije još uvek čekaju suđenje.

Uloga glavnog vođe čitave operacije bila je da pribavi informacije o ljudima koji imaju hrvatsko državljanstvo ali nemaju pasoš. Ta osoba bi onda ugovorila falsifikovanje pasoša sa trećim licima (uglavnom kriminalcima), sakupila bi fotografije i polovinu dogovorene svote novca. Uloga dvojice policajaca i jednog višeg službenika iz pasoškog odelenja Zagrebačke županijske policijske uprave bio je da proveravaju tačnost podataka koje je prethodno prikupio njihov kolega o ljudima koji imaju hrvatsko državljanstvo ali nemaju pasoš. Ove podatke su proveravali u informacionom sistemu Ministarstva unutrašnjih poslova, konkretno u Evidenciji putnih isprava hrvatskih državljana, koja predstavlja jedan od registara u okviru informacionog sistema Ministarstva unutrašnjih poslova.

Oni su mogli obaviti ovaj zadatak pošto su obojica, u skladu sa svojim radnim mestima, imali korisničko ime i lozinku neophodne za pristup Evidenciji putnih isprava hrvatskih državljana. Iako je ova baza podataka bila namenjena samo za profesionalnu upotrebu, oni su zloupotrebili svoja ovlaštenja i pristupili bazi podataka u kriminalne svrhe.

Pošto su pribavili sve potrebne podatke o ljudima čije će pasoše koristiti, oni su onda falsifikovali ovlaštenje za podizanje pasoša. Sa ovim ovlaštenjem pasoši su mogli biti podignuti u diplomatskim i konzularnim misijama Republike Hrvatske u Bosni i Hercegovini i Srbiji. Taj deo posla dodeljen je državnom službeniku koji je radio u hrvatskom Konzulatu u Orašju, u Bosni i Hercegovini.

Slučaj iz Hrvatske 5: Policajac uhvaćen dok je unosio falsifikovane podatke u informacioni sistem policije

Godine 2005. policajac u Zagrebu je ubacio lažne podatke u zvaničnu evidenciju policije koji potvrđuju da je čovek iz Srbije, star 64 godine, prijavio gubitak svoje hrvatske lične karte, uprkos tome što nije imao ni hrvatsko državljanstvo ni hrvatsku ličnu kartu. Štaviše, odštampao je potvrdno pismo o gubitku lične karte, overio ga zvaničnim pečatom i ubacio ga u informatički sistem Ministarstva unutrašnjih poslova, konkretno u Evidenciju osobnih iskaznica, koja predstavlja jedan od registara u okviru informacionog sistema Ministarstva unutrašnjih poslova. On je mogao da izvrši ovaj zadatak pošto je, u skladu sa svojim radnim mestom, imao korisničko ime i loznku neophodne za pristup Evidenciji osobnih iskaznica. Tim postupkom je zloupotrebio svoja ovlaštenja, unoseći falsifikovane podatke u registar.

Tokom rutinskog procesa monitoringa, šef policijske stanice primetio je ovo potvrdno pismo u informatičkom sistemu i počeo da sumnja u njegovu autentičnost.

Posle procesa verifikacije, utvrđeno je da je ovo potvrdno pismo falsifikovano i da je osumnjičeni policajac zloupotrebio svoja ovlaštenja. Kao rezultat, policajac je udaljen iz službe, a policija je protiv njega podnela krivičnu prijavu.

Prema informacijama iz policije, osumnjičeni policajac nije primio mito od građanina Srbije i Crne Gore. Falsifikovao je potvrdno pismo o gubitku lične karte kao uslugu zajedničkom prijatelju kako bi popravio pravnu poziciju lica starog 64 godine koje je pokušavalo da dobije hrvatsko državljanstvo.

Slučaj iz Hrvatske 6: Policajci brisali saobraćajne prekršaje iz evidencije i otkrivali poverljive podatke: prihvatali čak i pečeno jagnje i 20 litara vina kao mito!

Posle dugog perioda prisluškivanja i praćenja, zajednička akcija Ministarstva unutrašnjih poslova Republike Hrvatske (MUP) i Kancelarije za suzbijanje korupcije i organizovanog kriminala (USKOK), izvedena pod šifrovanim nazivom „Kamion“, završena je hapšenjem 37 lica, od kojih su 11 bili policajci, pod sumnjom da su otkrivali poverljive podatke iz informacionog sistema Ministarstva unutrašnjih poslova. Policajci su osumnjičeni da su zloupotrebili svoja ovlaštenja i da su primali mito od vlasnika prevozničkih preduzeća, zanatlija i drugih. Isto tako su osumnjičeni i da su otkrivali informacije o lokaciji i vremenu kontrola transportnih vozila od strane Hrvatskih autocesta (HAC) u najmanje 80 slučajeva. HAC je jedna od četiri kompanije koje upravljaju hrvatskom putnom mrežom, nadzirući transport opasnih roba otkrivajući podatke o vozilima iz informacionog sistema Ministarstva unutrašnjih poslova. Primljena mita za pomenute usluge bila su u obliku novca, a u jednom slučaju i u obliku pečenog jagnjeta i 20 litara vina. U skladu sa svojim ovlaštenjima i potrebama kao saobraćajnih policajaca, imali su korisničko ime i lozinku koji su im omogućavali pristup različitim bazama podataka u okviru policijskog informacionog sistema, između ostalih i onoj sa podacima o lokaciji i vremenu kontrola transportnih vozila od strane HAC-a, nadzoru nad vozilima sa opasnim teretom, kao i podacima o vozilima. Iako je njihova primarna uloga bila da obezbede sigurnost svih učesnika u saobraćaju, oni su odlučili da zloupotrebe svoja ovlaštenja i pristupili su bazi podataka radi kriminalnih potreba.

Slučaj iz Hrvatske 7: Slučajno uhvaćeni u otkrivanju poverljivih podataka o automobilima i njihovim vlasnicima!

Tokom praćenja organizatora međunarodnog lanca prostitucije, tokom hrvatsko-španske policijske akcije, sa šifrovanim nazivom „Catalunya“, detektivi su slučajno otkrili krivično delo jednog saobraćajnog policajca i službenika administracije u Međimurskoj županijskoj policiji. Tokom perioda od dva meseca, policajac i službenik administracije su otkrivali poverljive podatke o automobilima i njihovim vlasnicima jednom od pritvorenih tokom akcije „Catalunya“. Pritvorenik, koji je bivši policajac, osim što je regrutovao devojke da rade u Lloret de Mar, u Španiji, gde su bile primoravane na prostituciju, isto tako se bavio i preprodajom automobila. Kada je kupovao polovna kola, saobraćajni policajac i službenik administracije su mu prosleđivali podatke, o automobilima i vlasnicima iz informacionog sistema Ministarstva unutrašnjih poslova, konkretno iz Evidencije registracije cestovnih vozila. Oni su mogli obaviti ovaj zadatak pošto su, u skladu sa svojim radnim mestima, imali korisničko ime i lozinku neophodne za pristup ovom registru. Tim postupkom, zloupotrebili su svoja ovlaštenja i prekršili zakone o zaštiti ličnih podataka.

Nije poznato da li je ovo učinjeno radi novčane koristi ili kao usluga bivšem kolegi. Protiv obojice su podnešene krivične prijave i suspendovani su iz policije do završetka disciplinske procedure.

Slučaj iz Hrvatske 8: Svake godine nestane 2 miliona evra sa naplatnih rampi

31. decembra 2013. ukupna dužina mreže autoputeva u Hrvatskoj iznosila je 1.288,5 km. Prilikom upotrebe autoputeva, vozači su obavezni da plate putarinu. Ukupni prihodi od putarine u 2013. iznosili su 296.688.044 evra (bez PDV)[30]. Međutim, prema rečima nekih od direktora Hrvatskih autocesta (HAC), 1% putarina, u vrednosti 1,7 do 2 miliona evra, nestane svake godine. Glavni osumnjičeni za ovaj gubitak su zaposleni u HAC-u koji rade na naplatnim rampama. HAC je primetio da neki od njihovih zaposlenih nakupe i deset puta više faktura koje onda bivaju otkazane i ponovo odštampane sa izmenjenim podacima. Npr. kada bi se kamion pojavio na naplatnoj rampi, zaposleni koji je radio u toj kabini bi tražio od vozača da plati regularnu putarinu za kamion (koja je viša nego za putnička vozila). Zatim bi pristupio informacionom sistemu, otkazao upravo izdatu fakturu, ubacio lažne podatke – to jest, ubeležio bi da vozilo koje je upravo prošlo nije kamion nego automobil - i zatim bi odštampao novu fakturu. Pošto je putarina bila (i još uvek je) viša za kamione nego za putnička vozila, zadržao bi višak novca za sebe.

30 HUKA – Hrvatsko udruženje koncesionara za autoputeve sa naplatom putarine. Nacionalni izveštaj o autoputevima u Hrvatskoj za 2013. Dostupan na: http://www.huka.hr/en/news/223-national- report-on-motorways-in-croatia-for-the-year-2013

U avgustu 2010.interna revizorska kontrola u kompaniji Autocesta Rijeka Zagreb d.d., drugoj koja upravlja Hrvatskom mrežom autocesta, otkrila je da je 22 zaposlenih kralo novac sa naplatnih rampi na Demerju i Lučkom. Prijavljeni su policiji i odmah zatim otpušteni. Vođeni principom *in dubio pro reo*, sudija je izjavio da sud sumnja da su zloupotrebili položaj i počinili krivično delo ali da nema dokaza za njihovo krivično delo. Dok je čitao oslobađajuću presudu, sudija ih je pozvao da pročitaju pesmu od E.A. Poa „Gavran" i da obrate posebnu pažnju na poslednju rečenicu svake strofe: Nikad više!

U ovom slučaju, kompanija Autocesta Rijeka Zagreb d.d upotrebila je internu reviziju IT sistema, kao zaštitnu meru protiv zloupotrebe IT u svrhe korupcije. Kao nastavak sudijinom poetskom postupku prilikom izricanja oslobađajuće presude, da bi predupredili slične slučajeve u budućnosti i kao zaštitnu IT meru, uprava HAC-a je odlučila da postavi kamere koje će da nadgledaju rad zaposlenih na naplatnim rampama. Ove kamere neće snimati lica zaposlenih ni njihove glasove već samo njihov radni prostor, ruke i proces naplate putarine. Ukupan iznos ove investicije bio je 354.000 evra.

Slučaj iz Hrvatske 9: Korumpirani policajci – policajci otkrivali poverljive podatke krijumčarima oružja

Tri policijska službenika iz Zagreba su slučajno uhvaćena kako krijumčarima oružja otkrivaju poverljive podatke iz informacionog sistema Ministarstva unutrašnjih poslova (MUP). Prilikom prisluškivanja razgovora između krijumčara oružja i policije, policijski istražitelji iz unutrašnje kontrole su čuli da se otkrivaju poverljivi podaci iz informacionog sistema MUP-a. Pored otkrivanja poverljivih podataka, policijski službenici su brisali krivične prijave; krivotvorili dokumentaciju; čak i davali savete nekim uhapšenim krminalcima kako da se brane tokom istrage i upozoravali ih u slučaju da su praćeni od strane policije.

Prvi osumnjičeni je otkrio razne informacije i podatke iz informacionog sistema MUP-a svojim prijateljima, od kojih su neki bili kriminalci. Otkrivene informacije su uključivale naloge za hapšenje, lične podatke o konobarici koju su angažovali u svom kafe baru, ili informacije o nećaku koji je pobegao od kuće. Druga dva policijska službenika su pomogla svom kolegi da dobije sve informacije i podatke iz informacionog sistema MUP-a.

Oni su bili u mogućnosti da odrade ovaj zadatak budući da su, zbog prirode svojih radnih mesta, imali korisnička imena i lozinke za pristupanje različitim evidencijama. Pristupanjem tim evidencijama i otkrivanjem podataka zloupotrebili su svoja ovlašćenja i prekršili zakone o zaštiti ličnih podataka.

Naime, *„tajnost, integritet, kontinuirana dostupnost i kontrola podataka i informacija iz informacionog sistema MUP-a, su implementirani kroz određeni broj organizacionih, sistemskih i programskih mera i procedura kao i raspodelom nadležnosti i ovlašćenja. Svi korisnici informacionog sistema MUP-a su u obavezi da primenjuju zaštitu podataka, pro-*

pisanu Pravilnikom o zaštiti informacionog sistema MUP-a na bazi elektronske obrade podataka, Pravilnikom o bezbednosti i zaštiti službenih podataka MUP-a i drugim internim direktivama i uputstvima kojima su uređene aktivnosti na zaštiti informacionog sistema MUP-a. Odgovornosti radnih mesta službenika definišu nivo dostupnosti podataka".

Kao rezultat istrage, policija je podigla optužbe protiv 23 lica, uključujući i tri policijska službenika. Među njima je trinaest lica priznalo krivicu i nagodilo se sa USKOK-om u zamenu za blažu kaznu. Prvooptuženi je pravosnažno osuđen na zatvorsku kaznu u trajanju od šest meseci, kazna koja je sada zamenjena sa kaznom od pedeset dana društveno korisnog rada. Sud mu je takođe izrekao zabranu rada u svojstvu policijskog službenika u trajanju od tri godine. Druga dva policijska službenika, pored osam lica koji su optuženi za dobijanje nelegalnih informacija od strane tri policijska službenika, i dalje čekaju suđenje.

Slučaj iz Hrvatske 10: Policajac osuđen na kaznu zatvora od godinu dana jer je omogućio prijatelju nelegalan ribolov

U maju 2012. godine Vijeće Županijskog suda u Rijeci je osudilo dva bivša policijska službenika i još jedno lice zbog zloupotrebe poverljivih policijskih podataka. Prvi bivši policijski službenik je otkrio informacije iz informacionog sistema Ministarstva unutrašnjih poslova (MUP) o registarskim brojevima vozila i profilima vlasnika svom poznaniku. Kako bi prikrio svoje pristupanje sistemu i dobijanje informacija, on je koristio korisnička imena i lozinke svojih kolega. Na taj način je zloupotrebio svoja ovlašćenja i prekršio zakone o zaštiti ličnih podataka.

Naime,"*tajnost, integritet, kontinuirana dostupnost i kontrola podataka i informacija iz informacionog sistema MUP-a, su implementirani kroz određeni broj organizacionih, sistemskih i programskih mera i procedura kao i raspodelom nadležnosti i ovlašćenja. Svi korisnici informacionog sistema MUP-a su u obavezi da primenjuju zaštitu podataka, propisanu Pravilnikom o zaštiti informacionog sistema MUP-a na bazi elektronske obrade podataka, Pravilnikom o bezbednosti i zaštiti službenih podataka MUP-a i drugim internim direktivama i uputstvima kojima su uređene aktivnosti na zaštiti informacionog sistema MUP-a. Odgovornosti radnih mesta službenika definišu nivo dostupnosti podataka"*.

Ovaj policijski službenik je osuđen na zatvorsku kaznu u trajanju od jedne godine zbog izvršenja tri krivična dela zloupotrebe ovlašćenja. Takođe mu je zabranjen rad u državnoj upravi u periodu od pet godina. Još jedan bivši policijski službenik je osuđen na zatvorsku kaznu u trajanju od 5 meseci zbog podsticanja drugog na vršenje krivičnih dela, dok je njihov poznanik osuđen na zatvorsku kaznu u trajanju od 4 meseca za isto krivično delo.

Od decembra 2007. godine do juna 2008. godine prvi osuđeni policijski službenik je takođe otkrio podatke iz informacionog sistema MUP-a svom kolegi u penziji. Te informacije su se odnosile na vremenski raspored patroliranja policijskih čamaca Porečkim akvatorijumom. Kao rezultat toga, on je znao kada je bezbedno ilegalno izlovljavati prstace (lat. Lithophaga lithophaga), školjke koja su strogo zaštićene Pravilnikom o proglašavanju divljih svojti zaštićenim i strogo zaštićenim (Narodne novine br. 7/06 i 99/09).

Slučaj iz Hrvatske 11: Viši inspektor zloupotrebio poverljive podatke kako bi pobedio na lokalnim izborima

Viši inspektor Poreske uprave u okviru Ministarstva finansija je pristupio informacionom sistemu poreske uprave 2010. godine, nameravajući da otkrije iznos poreskog duga njegovog rivala na izborima za predsednika opštinskog odbora Hrvatske demokratske zajednice (HDZ) u delu Zagreba koji se zove Špansko. Šta više, on je koristio podatke iz Evidencije poreskih obveznika koji su pokazivali poreski dug njegovog rivala kako bi pripremio brošuru za predstojeće izbore, koji su se održali 1. juna 2010. godine. U toj brošuri, odvojeno od informacija o poreskom dugu, on je napisao *"Da li ste sigurni da ćemo prosperirati sa onima koji izbegavaju plaćanje poreza državi?"* On je mogao ovo da uradi budući da je bio ovlašćen da pristupi određenim ličnim podacima poreskih obveznika uključujući, između ostalih, njegovog rivala. Na posletku, pobedio je na izborima.

Nakon toga je njegov rival podneo tužbe protiv njega zbog zloupotrebe ovlašćenja državnom sekretaru Poreske uprave. Sud državnih službenika ga je proglasio krivim za *„ozbiljno kršenje profesionalnih dužnosti"* i kažnjen je smanjenjem plate u iznosu od 15 procenata u periodu od 4 meseca. On se žalio Višem sudu državnih službenika, ali je žalba odbijena. Na bazi ove odluke, njegov rival je podneo prijavu protiv njega Sudu časti HDZ-a. Ipak, partija je bila popustljiva i samo ga je ukorila zbog onog što je učinio.

U skladu sa Članom 62 Zakona o porezu na prihod (Narodne novine 177/04, 73/08, 80/10, 114/11, 22/12, 144/12, Odluka USRH-120/13, 125/13, 148/13) u svrhu dostavljanja podataka neophodnih za poresku procenu, poreski obveznici su u obavezi da podnesu prijavu za upis u registar obveznika za porez na prihod u lokalnu ispostavu Poreske uprave koja je nadležna za njihovo mesto boravka ili prebivališta.

Član 8 Opšteg poreskog zakona (147/08, 18/11, 78/12, 136/12, 73/13) uvodi koncept poreske tajne. Svi podaci navedeni od strane poreskog obveznika i prikupljeni tokom postupka oporezivanja smatraju se poreskom tajnom. Ovo predstavlja jedan oblik zaštite od neovlašćenog korišćenja ili javnog objavljivanja takvih podataka. Obaveza čuvanja poreske tajne se primenjuje na sva službena lica, eksperte i druga lica uključena u postupak oporezivanja. Ipak, Član 8, stav 2 Opšteg poreskog zakona sadrži odredbu koja propisuje da se, u određenim okolnostima, neki podaci neće smatrati poreskom tajnom. To su: podatak

o datumu upisa ili ispisa iz sistema poreza na dodatnu vrednost, i podatak o poreskim obveznicima koji su davali lažne podatke o porezu na dodatnu vrednost. Stavovi 5, 6, 7 i 12 navode slučajeve u kojima obaveza čuvanja poreske tajne neće biti prekršena. Nadalje, u skladu sa odredbama Člana 9 Opšteg poreskog zakona, strane u poreskim odnosima su dužne postupati u dobroj veri; tj. savesno i pravično. U konkretnom, gore opisanom, slučaju viši inspektor Poreske uprave u okviru Ministarstva finansija je zloupotrebio svoja ovlašćenja. Manipulišući podacima iz registra poreskih obveznika kako bi diskreditovao svog političkog protivnika prekršio je poresku tajnu. Njegovo ponašanje nije bilo ni etičko ni u dobroj veri.

Slučaj iz Hrvatske 12: Ni dana svog života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!

Iako nikada nije radila, 2007. godine jedna starija gospođa je počela da prima svoju penziju. Tokom zadnje tri godine, primila je više od 20.000 evra. Od 2007. godine njena ćerka je radila u Hrvatskom zavodu za penziono osiguranje (HZPO) na mestu načelnice službe za internu reviziju. Njene kolege su sumnjale da je pristupila penzijskom informacionom sistemu i izmenila podatke svoje majke kako bi joj omogućila da postane korisnik penzije. U skladu sa tim, oni su prijavili sumnjivu proneveru upravi HZPO-a. Ona je bila u mogućnosti to da uradi budući da je imala pristup dvema evidencijama HZPO-a: matičnoj evidenciji o osiguranicima penzionog osiguranja i matičnoj evidenciji o korisnicima prava iz penzionog osiguranja.

Tokom istrage je otkriveno da je ona krivotvorila radnu knjižicu, pa su tako i protiv nje podnešene krivične prijave. Ipak, iako je istraga pokazala da njena majka nije imala pravo da prima penziju, policija nije mogla da dokaže da joj je njena ćerka pomogla da stekne to pravo. Na kraju, ona je preraspođena sa mesta načelnice službe interne revizije na mesto koordinatora sektora ekonomskih poslova. Njena majka, iako nije imala pravo da dobija penziju, nikada nije vratila nelegalno stečen novac.

Kosovo

Pripremili Hasan Preteni i Driart Elshani

Dostignuća u oblasti informacionih tehnologija (IT) su u velikoj meri pomogla modernizaciji nacionalnih institucija, omogućavajući veću efikasnost u njihovom radu. Ipak, ne ide sve u prilog poštenom i efektivnom radu. Na osnovu radne prakse Agencije za aktikorupciju, od 2006. godine na Kosovu je zabeležen veliki broj slučajeva kada informacione tehnologije nisu korišćene za svoju predviđenu namenu.

Svaki državni službenik ili službenica na Kosovu imaju svoju službenu i-mejl adresu na domenu @rks-gov.net. Ta i-mejl adresa treba da se koristi samo u zvaničnoj komunikaciji između službenika i drugih lica – i samo za službene potrebe. Svaki korisnik u okviru svog domena može lako naći i poslati i-mejl zaposlenima u drugim državnim institucijama. Oko 70.000 zaposlenih u institucijama Kosova koristi gore navedeni i-mejl domen. Ovaj broj uključuje nivo centralne, regionalne i lokalne vlasti, zvaničnike svih „jurisdikcija“ (zakonodavne, izvršne i sudske vlasti), Kabinet predsednika, i druge nezavisne mehanizme kao što su Policija Kosova i razne agencije uspostavljene od strane Skupštine Kosova ili preko drugih mehanizama.

Zvanične i-mejl adrese treba koristiti samo za zvaničnu komunikaciju. Ipak, česti su slučajevi kada se mreže koriste za privatne stvari ili za potrebe političke partije ili u komercijalne svrhe. Uticajni ljudi tokom izbornih kampanja često zloupotrebljavaju zvaničnu i-mejl adresu kako bi pozvali državne službenike da glasaju za njih ili njihovu političku partiju.

Neki državni službenici u saradnji za različitim firmama uspostavili su „profesionalne organizacije za obuku državnih službenika”, čiji su fondovi za obuku pronevereni. Nadalje, zloupotrebljavana je mreža računara institucija Kosova, slanjem raznih reklama koje pozivaju institucije (državne službenike) da putuju u inostranstvo na seminare, o trošku institucija. To je dovelo do toga da određeni zvaničnici prisustvuju neprofesionalnim obukama sa lošom organizacijom što nije bilo od koristi institucijama, ali je bilo veoma profitabilno za kompanije koje su organizovale obuku u saradnji sa IT zvaničnicima.

Flagrantno kršenje je zabeleženo jednom prlikom kada je direktor jednog sektora u nekom ministarstvu otvorio restoran van glavnog grada, Prištine, i preko @rks-ks.net i-mejl adrese reklamirao otvaranje, i koristio zvaničnu i-mejl adresu da pošalje pozivnice, čak i na adrese rukovodilaca u glavnim institucijama, da prisustvuju ceremoniji otvaranja. Ova reklama se pokazala štetnom za državnog službenika, budući da su par dana kasnije mediji otkrili da je on koristio službenu i-mejl adresu za oglašavanje i slanje privatnih pozivnica, njegov restoran je napadnut, spaljen do temelja i nikada više nije otvoren. Ipak, to se verovatno desilo zbog gneva javnosti jer je jedan državni zvaničnik otvorio restoran, a ne zbog sredstva komunikacije koje je on odabrao.

Sve Kosovske institucije imaju svoje zvanične veb sajtove na internetu. Ipak, kao rezultat nedovoljne računarske bezbednosti institucija, skoro sve institucije su barem jednom bile napadnute od strane „hakera“.

Nisu retki slučajevi kada državni službenici, tokom radnih sati, koriste svoje računare da komuniciraju sa raznim osobama na društvenim mrežama, i da zbog toga nisu efikasni tokom rada i zloupotrebljavaju tehnologiju institucije zbog ličnih potreba.

Takođe, utvrđeno je više slučajeva kada su zvaničnici koristili internet, nakon radnih sati, da gledaju pornografske materijale ili surfuju raznim mrežama koje propagiraju nemoral.

Pored ovih oblika neželjene upotrebe informacionih tehnologija, niže u tekstu će biti prikazani neki konkretni slučajevi koji su naštetili institucijama, a od kojih su pojedinci imali koristi.

Slučaj sa Kosova 1: Uništavanje dokaza

Nakon rata, na Kosovu se pojavio veliki broj zahteva da se stabilizuje situacija i omogući napredak za građane kroz otvaranje novih radnih mesta i uspostavljanje uslova za celokupan razvoj zemlje. Jedan od prioriteta Vlade u to vreme je bio da se poboljša putna infrastruktura. Znatna sredstva su opredeljena za asfaltiranje i lokalnih i regionalnih puteva. Zbog posleratnih okolnosti, veoma mali broj kompanija se specijalizovao za ovaj tip posla. Očekivanja građana su bila velika i zbog toga su građani pozdravljali sve aktivnosti. Ipak, javnost je uskoro shvatila da se radovi na renoviranju puteva ne rade po istim standardima po kojima se radilo pre rata.

Neki od zvaničnika centralne vlasti su zloupotrebili ovu situaciju. Zvaničnici, u saradnji sa vlasnicima građevinskih firmi su počeli da zloupotrebljavaju fondove i da krše zakone koji su na snazi. Državni službenici su počeli da traže mito od svake kompanije koja je željela da dobije ugovor za izvođenje radova.

Iznos koji je tražen za dobijanje posla je bio 10-20% od vrednosti tendera. Od svog osnivanja, Agencija za borbu protiv korupcije je dobila informacije o brojnim navodima korupcije u ovoj oblasti. Najkonkretniji slučaj je bio kada se vlasnik firme žalio da je, za potrebe dobijanja milionskog posla, državni službenik zatražio visoki, sedmocifreni iznos (ili 15%) ukupne vrednosti tendera.

Ovaj poslovni čovek je bio veoma zabrinut i odlučio je da kontaktira Agenciju za borbu protiv korupcije. Primljen je od strane zvaničnika Agencije, i imajući u vidu mandat Agencije i potpisani Memorandum o saradnji sa tužiteljima Evropske misije za vladavinu prava Evropske unije na Kosovu (EULEX), Agencija je odlučila da prosledi ovu informaciju EULEX-u. Vrednost tendera je bila veoma visoka, a visokog ranga su bila i lica osumnjičena za

traženje mita. Slučaj je bio veoma delikatan, i istraga je odmah započela. Sredinom 2007. godine, istražitelji su intervenisali u prostorijama gde su ti zvaničnici radili, prekontrolisali poslovne prostorije i prikupili veliku količinu fizičkog materijala, nešto računara i drugog elektronskog materijala, i uhapsili neke od zvaničnika.

Nekoliko dana kasnije, zvaničnici Agencije su zaplenili drugu elektronsku opremu koja se nalazila u Ministarstvu za državnu upravu. U skladu sa institucionalnim pravilima koja se primenjuju u celoj javnoj upravi na Kosovu, serveri za pohranjivanje podataka svih vladinih institucija su locirani u prostorijama ovog ministarstva. Tog istog dana, EULEX istražitelji su takođe uhapsili dva IT službenika. Otkriveno je da je sav materijal koji su istražitalji očekivali da nađu na serverima Ministarstva i koji bi dokazao sumnje Agencije za borbu protiv korupcije u vezi sa neregularnostima i kršenjima zakona, izbrisan sa vladinih servera. Isključiva namera ovih istražitelja je bila da omogući nalaženje dokaza protiv zvaničnika uključenih u korupciju. Zbog toga se pretpostavilo da su izbrisani i podaci koji sadrže dokaze o ponudama drugih kompanija sa nižim ponudama. Brisanjem takvih podataka sa servera, cilj je bio da tender dobije kompanija sa najskupljom ponudom. Istraga je trajala više godina, i sada slučaj ima epilog na sudu. Lista optuženih lica, pored zvaničnika iz sektora za puteve, takođe uključuje dva IT službenika iz Ministarstva za državnu upravu koji su omeli istragu brisanjem podataka sa glavnog servera. Ukupan broj optuženih zvaničnika je bio 8-10. Krivična dela za koja su optuženi su zloupotreba službenog položaja, prevara u službi i falsifikovanje dokumenata. Jedna od mera za sprečavanje budućih slučajeva ove vrste je da neko nezavistan kontroliše ove servere.

Slučaj sa Kosova 2: Dobijanje statusa „ratnog invalida“

U okviru Ministarstva rada i socijalnog staranja postoji poseban sektor za ratne invalide. U junu 1999. godine, nakon rata na Kosovu, veliki broj lica se prijavio za upis na spisak veterana rata. Kasnije, tokom 2003-2004. godine, počeo je rad na obradi spiska veterana rata. Postojao je veliki broj prijavljenih lica, i bilo je veoma podsticajno registrovati ljude da se nađu na spisku, jer pored materijalnih beneficija, oni bi stekli i druge beneficije kao što je preferencijalni medicinski tretman, kupovina vozila bez plaćanja carine i druge privilegije i beneficije za njih i članove njihovih porodica. Neki od njih su odmah stekli taj status, dok su neki drugi kasnije stekli status – i ti koji su kasnije stekli taj status su predstavljali problem.

Jedno lice je Agenciju za borbu protiv korupcije obavestilo i prijavilo drugo lice sa inicijalima F.M. da prima penziju ratnog invalida u iznosu od 200 evra mesečno, kao lice sa 30% invaliditeta. Doušnik je bio iz istog sela odakle je bio i F.M. a znao je sa sigurnošću da F.M. nema invaliditet u tom stepenu. Na Kosovu, postoje tri ratna udruženja: 1) Udruženje veterana; 2) Udruženje invalida; i 3) Udruženje nacionalnih mučenika. Agencija je otvorila slučaj, i na početku je tražila podatke iz tri udruženja. F.M. je bio registrovan kao veteran-učesnik u ratu, ali ne i kao lice sa invaliditetom. Agencija je zbog toga koristila svoja

zakonska prava i zatražila podatke i pripadajuću dokumentaciju iz Ministarstva rada i socijalnog staranja u vezi sa licem F.M. Nakon dobijanja dokumentacije, primećeno je da postoje znatne razlike. Osnovni dokument za dobijanje penzije nije bio original – bio je falsifikovan. Jedan IT službenik je bio odgovoran za falsifikovanje elektronskog dokumenta F.M. tako što je dostavio falsifikovanu skeniranu dokumentaciju za dobijanje invalidske penzije. Zaključak Agencije za borbu protiv korupcije je bio da postoji osnovana sumnja da su službenici iz te kancelarije falsifikovali elektronske podatke kako bi omogućili materijalne beneficije – invalidsku penziju. Agencija je ovaj slučaj predala Državnom tužilaštvu, koje je u periodu od tri meseca angažovalo policiju u postupku prikupljanja dokaza. Tokom krivične istrage utvrđen je veliki broj prekršaja. Više od 1500 lica je dobilo invalidsku penziju falsifikovanjem dokumentacije da su žrtve rata sa invaliditetom, iako u stvari ta lica nisu ni imala invaliditet. Bogatstvo lica koje je rukovodilo ovom kancelarijom se istovremeno, slučajno, takođe znatno povećalo. Trenutno je slučaj u procesu čekanja podizanja optužnica za dela sankcionisana krivičnim zakonikom: prevara u službi i falsifikovanje dokumentacije, dok su tri zvaničnika odseka za invalidske penzije u ovom ministarstvu suspendovani bez plate. Zloupotreba je počinejna tokom skeniranja, kada je falsifikovan lekarski izveštaj. F.M. je dostavio dokument kojim je dokazivao da je tokom rata na Kosovu imao zdravstvene probleme. Dokument nije iz ratnog perioda, već je sačinjen 5 godina kasnije. On sadrži datume kao da je sačinjen tokom rata. Ovaj slučaj pokazuje da nije dovoljno da se izvrše provere samo u IT sistemu, već se provere moraju proširiti i na dokumente u papiru koji se pohranjuju u sistemu. Na kraju, moguće slabosti u IT sistemu mogu otežati dokazivanje da su dokumenti skenirani i pohranjeni u sistem naknadno, pokrivajući čitavu šemu prethodnog datiranja.

Slučaj sa Kosova 3: Zloupotreba lozinke

Oglas za slobodno radno mesto za imenovanje direktora klinike na univerzitetskom kliničkom centru na Kosovu je propao više puta. Među medicinskim osobljem je postojala posebna zainteresovanost da budu rukovodioci klinika. U nekim slučajevima je Ministarstvo zdravlja a u drugim slučajevima nezavisni nadzorni komitet, kao telo koje nadgleda državne službenike i njihovo zapošljavanje i otpuštanje, poništio takve oglase za slobodna radna mesta. Godinama su najvećem broju klinika rukovodili vršioci dužnosti direktora, imajući na umu da je oglas za radno mesto zaključen u junu 2014. godine. Komisija za procenu kandidata je bila oformljena, pitanja za intervju pripremljena i sve neophodne pripreme za postupak zapošljavanja sprovedene. U nekim klinikama su imenovani direktori, ali u osam klinika nije došlo do imenovanja novih direktora. Jedan od kandidata za rukovođenje klinikom je dobio informacije da su pojedini kandidati dobili pitanja unapred, a pitanja su trebala da budu poverljiva do dana testiranja.

Član nadzorne komisije je obavestio[31], i mediji su objavili i-mejl adresu sa koje su pitanja poslata. Budući da je bio u nezgodnoj situaciji zbog svih tih činjenica i skandala koji je usledio, jedan član komisije za odabir direktora je organizovao konferenciju za medije, i priznao da su podaci poslati sa njegovog računara nekim od kandidata, ali da on lično nije bio odgovoran za to. Zvaničnik je pokušao da prebaci odgovornost na lice koje je optužio da mu je ukralo i zloupotrebilo lozinku, i koje je pristupilo računaru na neovlašćeni način, i naveo da je dao toj osobi svoju ličnu lozinku kada je otišao na odmor. Ipak, ishod ovog skandala je bio da je član komisije dao ostavku, oglas za radno mesto je morao ponovo biti objavljen, dok u vezi sa drugim merama koje je bilo potrebno preduzeti, Agencija za borbu protiv korupcije još uvek nema informacije.

Prošle godine, Agencija za borbu protiv korupcije je nezvanično obaveštena da je pomoćnica direktora jednog nezavisnog mehanizma koristila i-mejl adresu direktora na neovlašćeni način. Postoji više slučajeva kada su viši službenici ovlastili svoje pomoćnike da pristupaju njihovim i-mejl adresama kako bi komunicirali u njihovo ime. Ipak, ovaj slučaj predstavlja neetičko ponašanje pomoćnice koja je koristila i-mejl načelnika institucije kod svoje kuće, budući da je bila na porodiljskom odsustvu.

Slučaj sa Kosova 4: Falsifikovanje poreskih dokumenata

Jedno preduzeće koja pruža usluge čišćenja podnelo je ponudu i dobilo ugovor za čišćenje zgrade jednog ministarstva. Čitav postupak počeo je da se primenjuje u skladu sa zakonima koji su na snazi. Ime prvorangiranog sa najnižom cenom je objavljeno, ugovor je zaključen i implementacija počela. Nakon nekoliko meseci implementacije, došlo je do pogoršanja međuljudskih odnosa među zaposlenima izvođača. Vlasnik preduzeća je otpustio lice koje je pre toga radilo u ministarstvu duži niz godina i koje je bilo nadležno za finansije i nabavke. To lice, nezaposleno i razočarano čitavom situacijom, odlučuje da se „osveti" bivšem poslodavcu. Odlučuje da prijavi preduzeće. Jednog dana, Agencija za borbu protiv korupcije je dobila informacije od anonimnog lica putem i-mejla: preduzeće koje pruža usluge čišćenja je u vlasništvu lica sumnjive prošlosti, koje je dobilo veliki broj tendera za održavanje prostorija centralnih institucija Kosova. Doušnik je rekao Agenciji kako ovo preduzeće dobija sve tendere, zbog toga što ne plaća poreze i tako može da daje niže ponude.

Dokaz da se porez redovno plaća je jedan od osnovnih dokumenata koji ponuđač mora da dostavi u okviru tenderske ponude kada se nadmeće za dobijanje ugovora. Vlasnik kompanije je koristio svoje veze da zaobiđe tu obavezu, zbog dobrih odnosa koje je imao sa zvaničnicima poreskih vlasti. Nakon početne uplate poreza u visokom iznosu, za sva buduća nadmetanja je koristio istu priznanicu ali sa falsifikovanim datumima. Svi zvaničnici

31 Dnevni list Tribuna, sreda 14. avgust 2014. godine, br. 1538, godina 2014, strane 10-11 http://www.gazetatribuna.com/?FaqeID=1

iz institucija su mogli da zatraže originalni dokument, ali su nerado to činili, jer su osećali da posluju sa starijim licem i dali bi obrazloženje da je dokument skeniran i da ispunjava njihove uslove.

Agencija je zatražila pristup informacijama o ovom preduzeću od strane Poreske uprave. Sumnje su se pokazale tačnim. Porezi nisu plaćani na redovnoj osnovi, i dokumenti korišćeni od strane ovog preduzeća za dobijanje tendera su bili falsifikovani i kao takvi nisu trebali biti prihvaćeni. Agencija se bavila sa mnogim drugim tenderima koje je ovo preduzeće dobilo, i utvrdila da su tu još tri lokalne i jedna međunarodna institucija gde je to preduzeće pružalo usluge. Zanimljivo je da je ovo preduzeće takođe podnelo ponudu za održavanje zgrade Agencije za borbu protiv korupcije. Ipak, u zadnjem trenutku procene ponuda, ponuda je povučena bez ikakvog obrazloženja. Krivična prijava protiv ovog preduzeća je predata pre nekoliko meseci državnom tužiocu. Sve institucije su obaveštene o nalazima i dobile su zahtev od Agencije za borbu protiv korupcije za raskidanje ugovora sa ovim preduzećem. Ali i pored toga, to se nije svuda desilo. Međunarodna institucija je raskinula ugovor i predala slučaj EULEX tužiocu zbog naknade štete. Agencija je zatražila od tela za reviziju nabavki – Suda za tendere da stavi ovo preduzeće na crnu listu, kako ono više ne bi dobilo neki drugi posao kod vladinih institucija. Nažalost, Agencija još uvek nije dobila potvrdu da su sličnu aktivnost preduzele i lokalne institucije.

Makedonija

Pripremili Marjan Stoilkovski i Rozalinda Stojova

Makedonska definicija korupcije

U pravnoj terminologiji u Republici Makedoniji „korupcija označava korišćenje funkcije, javnog ovlašćenja, službene dužnosti i pozicije u svrhu sticanja dobiti za sebe ili drugo lice"[32].

Korupcija se dešava na svim nivoima vlasti, i žrtve mogu biti pojedinci, pa čak i čitave zajednice. Korupcija je složeno krivično delo koje često uključuje više od dve strane, te je stoga teško razlikovati korupciju od drugih oblika krivičnih dela; zbog toga, često se istraga nikada ne bavi korupcijom (uključujući korupciju putem manipulacije ili zloupotrebe IT sistema) kao nezavisnim krivičnim delom, već je uvek povezuje sa drugim krivičnim delima.

Rangiranje

Rezultati vezani za dva najnovija indeksa percepcije korupcije (IPK) organizacije Transparency International, pokazuju da je Makedonija rangirana na 69 i 67 mestu na rangiranju 2012 i 2013, što u regionalnom kontekstu stavlja Makedoniju na drugo mesto među ReSPA zemljama[33].

Ipak, sa kulturne i društvene tačke gledišta, značajno je da „Makedonski građani rangiraju korupciju kao najvažniji problem sa kojim se suočava njihova država nakon nezaposlenosti i siromaštva/niskog životnog standarda". (UNODC istraživanje, 2011)[34]

Godina	Rang države	Država/ Teritorija	IPK bodovanje
2012.	69	Makedonija	43
2013.	67	Makedonija	44

32 Zakon o sprečavanju korupcije, amandmani od 2. jula 2004. godine. Definicija korupcije, član 1-a: http://www.dksk.org.mk/en/images/stories/PDF/law/2004.pdf
33 2013. godine je drugo mesto podelila sa Crnom Gorom.
34 https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Corruption_report_fYR_Macedonia_FINAL_web.pdf

Slučaj iz Makedonije 1: Zloupotreba IT sistema na naplatnim rampama

Ovaj slučaj je presuđeni slučaj zloupotrebe službenog položaja a to se, u skladu sa makedonskim zakonom, smatra osnovnim činom korupcije. Uključuje manipulaciju IT sistema za naplatu putarine, koji se koristi za upravljanje procesom naplate putarine, upravljanje smenama zaposlenih i njihovim radnim postupcima na naplatnim rampama.

Ovaj slučaj je dodeljen Jedinici za borbu protiv korupcije i Jedinici za finansijski kriminal na dalju istragu. Na početku istrage, ove jedinice su zatražile da zvanično dobiju sve neophodne informacije o IT sistemu od preduzeća koje je razvilo i održavalo upravljanje sistemom naplate putarina.

Istraga je otkrila da je postojala kombinacija različitih tipova zloupotrebe IT sistema, izvršenih od strane zaposlenih:

- zloupotreba IT sistema upotrebom različitih korisničkih imena i upotreba korisničkih imena drugih zaposlenih,
- u kombinaciji davanja komande za puštanje vozila, ili
- manipulacija sa IT sistemom preko izmene plaćenog iznosa, ili
- neunošenje svakog vozila koje je prošlo naplatnu rampu, ili
- nedavanje priznanica i deljenje troškova sa vozačima vozila po principu 50:50, ili
- unošenje drugačije kategorije za vozila.

Da bi se prikupili relevantni dokazi primenjene su posebne istražne mere. Podaci i informacije prikupljene iz IT sistema tokom istrage su pomogli da se utvrde i dokažu nelegalne aktivnosti organizovane kriminalne grupe. Na kraju, i uglavnom kroz razne analize preduzete po pitanju podataka iz IT sistema, bilo je moguće proceniti i obračunati štetu načinjenu od strane ovog preduzeća.

Istraga je pokazala da je postojala zloupotreba službenog položaja prilikom upotrebe IT sistema, i na taj način se omogućilo zaposlenima da steknu nelegalnu imovinsku korist koja se u kasnijoj fazi oprala preko legalnih investicija u robu.

Krivične prijave za ovaj slučaj su podnešene 1. decembra 2011. godine, i 92 lica su osuđena za zloupotrebu službenog položaja, krivotvorenje, korupciju (primanje mita) i članstvo u organizovanoj kriminalnoj grupi. Vršenjem takvih nelegalnih aktivnosti, ogranizovana kriminalna grupa je ilegalno stekla više od 120 miliona makedonskih denara i zbog toga je preduzeće moralo da plati kaznu u istom iznosu.

Sudski postupak je okončan 23. maja 2013. godine sa presudama u rasponu od 3 do 6 godina zatvorske kazne za 86 lica, i sa presudama koje su uključivale nadoknadu štete prouzrokovanu preduzeću u iznosu od oko 107 miliona denara. Jedanaest osoba je osuđeno kaznom konfiskacije imovine u vrednosti od 5 miliona denara.

Nakon što je ovaj slučaj okončan, preduzeće koje je vlasnik naplatnih rampi u Republici Makedoniji je poboljšalo IT sistem za upravljanje naplate putarine i nadgledanja rada zaposlenih. Poboljšanja u sistemu su kreirana i razvijena kako bi se prevazišli identifikovani i očekivani problemi, i to putem automatizacije radnih procesa, izbegavanja unošenja podataka u IT sistem od strane zaposlenih, i interkacije sa samim procesom.

Slučaj iz Makedonije 2: Napad na IT sistem javnih nabavki

U Republici Makedoniji, počevši od 1. januara 2012. godine, u skladu sa Članom 8 Zakona o javnim nabavkama, naručioci su u obavezi da koriste elektronske aukcije u 100% slučajeva kod objavljenih poziva na otvoreni postupak, ograničeni postupak, pregovarački postupak sa prethodnom objavom i pojednostavljeni konkurentni postupak.

Elektronski sistem javnih nabavki je veb bazirana aplikacija gde se oglašavanja, obaveštenja i tenderi objavljuju u potpunosti elektronski, i gde učesnici na tenderu šalju svoje originalne ponude elektronskim putem.

Sistem je u vlasništvu Agencije za javne nabavke i hostuje ga lokalni pružalac usluga. U sistemu postoji zaštitni zid koji je instaliran i konfigurisan sa sistemom za detekciju upada (SDU), i koristi virtuelnu privatnu mrežu (VPN) radi pružanja bezbednog pristupa sistemu. Sami sistem koristi bezbedni https protokol, i SSL sertifikat.

Na nivou aplikacije, sistem registruje različite tipove korisnika, naručilaca, i privrednih subjekata (preduzeća). Sistem ima sopstveni nivo modula aplikacije i dodeljuje korisnicima odgovarajuća prava pristupa.

Naručioci imaju interne korisnike na nivou aplikacije, tj. lokalnog administratora, službu nabavki, komisiju za javne nabavke i odgovorno lice. Privredni subjekti (preduzeća) takođe imaju svoje interne korisnike, a svi imaju iste privilegije: mogućnost razmene elektronskih procedura, učešće na elektronskim aukcijama, postavljanje pitanja, itd. Jedna sesija od strane korisnika čija je autentičnost dokazana na nivou aplikacije traje 40 minuta. Ukoliko ne postoji korisnička aktivnost tokom tog perioda korisnik je odjavljen.

U avgustu 2012. godine, ponuda za nabavku automobila je objavljena uz korišćenje IT sistema javnih nabavki. Tenderskim postupkom je upravljao IT sistem javnih nabavki, i ponudu je podnelo više od jednog ponuđača. Tokom tenderskog postupka, IT sistem je funkcionisao dobro sve do zadnjih nekoliko minuta, kada se sistem srušio – nije bio u mogućnosti da prima dalje ponude tokom tog perioda, i pored činjenice da je bilo pokušaja podnošenja novih ponuda od strane korisnika.

Slučaj je prvo prijavljen kao upad u računarski sistem i kao slučaj računarskog kriminala. Ovo je proceduralna praksa, koja podrazumeva da se na početku slučajevi ove vrste istražuju kao računarski kriminal, a u narednoj fazi istrage i ukoliko postoji dokaz da su počinjena druga krivična dela, slučaj će biti istraživan paralelno sa drugim krivičnim delima. Budući da je ovaj incident bio slučaj koji uključuje javnu nabavku opreme visoke vrednosti, smatran je i tretiran kao slučaj računarskogkog kriminala, a istovremeno i kao neki oblik korupcije. Iako na početku nisu postojali dokazi i informacije da je u pitanju slučaj korupcije ili zloupotrebe, istraga je pokrila oba aspekta slučaja.

Jedinica za računarski kriminal je istraživala ovaj slučaj i tvrdila da je preduzela sve neophodne korake da sačuva dokaze i dobije relevantne informacije koje bi pomogle u istrazi. Na početku, osnovne informacije iz IT sistema, detaljne tehničke informacije, sve relevantne sistemske, sigurnosne i administrativne datoteke evidencije su zatražene od hosting firme i od Uprave za javne nabavke.

Jedinica za računarski kriminal je dobila inetpub datoteke evidencije sa servera koji sadrže evidencije IP adresa sa kojih je pristupano aplikaciji, datoteke evidencije aplikacije i datoteke evidencije tokom procesa aukcije. Nakon detaljne analize dobijenih informacija koristeći Linux operativni sistem i skripte za izvršavanje funkcija, otkriveno je da je u kritičnom periodu sistem pao zbog distribuiranog napada radi blokiranja usluga (DDoS napad) izvršenog sa brojnih IP adresa koje potiču iz stranih zemalja. Istraga je takođe utvrdila da je zadnja ponuda podnešena od strane komapnije A samo nekoliko sekundi pre nego što je sistem pao, i kada je kompanija B pokušala da podnese ponudu, sistem nije bio dostupan i zbog toga nije mogao da prihvati nove ponude.

Kompanija B je prijavila slučaj kao potencijalnu zloupotrebu i dostavila podatke koji su dokazali da je ova kompanija podnela novu ponudu tokom perioda kada je sistem za javne nabavke bio nedostupan, i da njihova ponuda nije registrovana i samim tim nije prihvaćena.

Kasnije je istraga otkrila da IT sistem za javne nabavke nije bio ciljani veb sajt za DdoS napad, već je cilj bila druga veb stranica (informativna veb stranica). Kako su oba sistema hostovana na istom serveru, obe veb usluge su bile nedostupne.

Na bazi dobijenih datoteka evidencije utvrđeno je da je tokom kritičnog perioda poslat veliki broj zahteva prema sistemu koji je bio predmet napada, a ne prema veb servisu koji je držao sistem javnih nabavki.

DDoS napad je jedna od metoda koje se koriste da se određene usluge učine nedostupnim na internetu. Slanjem velikog broja zahteva prema sistemu, sistem postaje nedostupan jer ne može da prihvati i obradi sve zahteve. Kada sistem dostigne tačku kada više nije u mogućnosti da prihvati sve poslate zahteve, on se obično sam ugasi. U većini slučajeva, ova vrstu napada se vrši uz korišćenje botnet mreža (mreža od velikog broja računara koje kontroliše jedan računar sa namerom vršenja određenih aktivnosti).

Ovaj tip napada ne prouzrokuje značajnu štetu napadnutom sistemu kao što je brisanje ili menjanje podataka. On samo čini uslugu nedostupnom, obično gašenjem određenih usluga sistema ili gašenjem sistema.

Na kraju nije dokazano da ovaj slučaj predstavlja zloupotrebu službenog položaja i korupciju, ali daje pregled postupaka i potencijalnih metoda za zloupotrebu IT sistema za korupciju, zloupotrebom službenog položaja ili kroz društveni inžinjering. Imajući na umu tehnologije koje se koriste za olakšavanje i poboljšavanje svakodnevnog rada i usluga, možemo da identifikujemo veliki broj načina zloupotrebe IT sistema.

Administrator sistema ima pune privilegije u sistemu tokom dužeg vremenskog perioda, i ako se njegove/njene aktivnosti ne prate i nadgledaju adekvatno, on/ona bi mogao/la da zloupotrebi sistem uništavanjem ili menjanjem digitalnih dokaza, i na posletku onemogući vršenje istrage u tom slučaju i dokazivanje zloupotrebe.

Slučaj iz Makedonije 3: Zloupotreba IT sistema i nelegalno otkrivanje ličnih podataka

Razvoj tehnologija i implementacija novih tehničkih rešenja kao alata za pružanje usluga u javnom sektoru povećavaju rizik od potencijalne zloupotrebe službenog položaja od strane zaposlenih u institucijama državne uprave.

Slučaj koji se ovde opisuje je slučaj zloupotrebe službenog položaja i dozvole pristupa IT sistemu u kojem se čuvaju podaci sa ograničenim pristupom koji mogu biti otkriveni samo pod posebnim uslovima. U skladu sa nacionalnim zakonima za zaštitu ličnih podataka, institucija koja čuva ili obrađuje lične podatke je u obavezi da sledi posebne procedure za otkrivanje ličnih podataka.

U ovom slučaju, jedno lice zaposleno u instituciji javnog sektora sa pristupom podacima o finansijskom prihodu je zloupotrebilo svoj položaj i otkrilo takve informacije. Iako procedure navode da takva informacija može biti otkrivena samo na lični zahtev građanina ili predstavnika agencije za sprovođenje zakona nakon sudskog naloga, u ovom slučaju, zaposleni nije poštovao procedure za otkrivanje ličnih podataka, i izdao je zvanični dokument koji je napravio IT sistem koji je sadržao lične podatke. Kasnije je taj zvanični dokument korišćen kao dokaz u građanskoj parnici.

Ovaj slučaj je istraživan sa tri tačke gledišta: zloupotreba ličnih podataka od strane zaposlenog i institucije (istragu je vršila Direkcija za zaštitu ličnih podataka), zloupotreba službenog položaja i usluga od strane poslodavca (moguća korupcija tj. primanje mita ili dobijanje drugih beneficija ili koristi) i zloupotreba ličnih podataka u skladu sa Nacionalnim krivičnim zakonikom, Član 149 o zloupotrebi ličnih podataka (istragu vršilo Ministarstvo unutrašnjih poslova).

Iz istrage koja je sprovedena za zloupotrebu ličnih podataka i zloupotrebu službenog položaja, prikupljeni su dokazi koji pokazuju da je zaposleni/a nelegalno izdao/la dokument iz IT sistema i da je on/ona počinio/la krivično delo. Dokazi su izvučeni i iz IT isistema i iz sistema video nadzora (CCTV). Iako u ovom slučaju, primanje mita ili dobijanje drugih beneficija ili koristi nije zakonski dokazano, činjenicu da je zaposleni/la imao/la dozvolu da koristi sistem, ali ne i ovlašćenje od vlasnika podatka da ih obelodani, istraga (policija i tužilaštvo) je smatrala da je u pitanju jedan oblik korupcije, definisan u skladu sa nacionalnim zakonodavstvom.

Ovaj slučaj je samo jedan primer zloupotrebe službenog položaja i postoji veliki broj sličnih primera kao što je ovaj tj. zloupotrebe službenog položaja radi otkrivanja informacija. Činjenica je da se često takvi slučajevi ne prijavljuju kao krivična dela, već se samo istražuju interno u okviru institucije.

Slučaj iz Makedonije 4: Zloupotreba sistema evidentiranja broja radnih sati

Tokom zadnje decenije, sistemi koji registruju radne sate su uključeni u svakodnevni rad velikog broja uprava, javnih preduzeća, bolnica i škola. Sistem evidentira dolazak i odlazak na radno mjesto, kao i službeno i privatno odsustvo, i pohranjeni podaci se koriste da se računa broj radnih sati za zaposlenog tokom određenog vremenskog perioda. Broj radnih sati se koristi da se obračunaju zarade zaposlenih, utvrdi period kontinuiranog izostanka sa posla određenog zaposlenog, i za druge analize. U skladu sa relevantnim zakonima, ostajanje na poslu nakon definisanog radnog vremena, ne znači samo po sebi prekovremeni rad.

Sa druge strane, učestalo kašnjenje na posao tokom kratkog vremenskog perioda je razlog za pokretanje disciplinskog postupka. Ovo je naročito primenjivo u institucijama koje rade u jednoj smeni, pogotovo imajući na umu da u Makedoniji ne postoji „klizno“ radno vreme u upravi.

U jednoj od institucija gde je takav sistem instaliran za evidenciju radnih sati, samo jedna osoba je imenovana za posao administratora nadležnog za upravljanje čitavim sistemom. Administratorske privilegije su uključivale mogućnost kontrole i pregleda evidencije prisustva na radu i izradu opštih izveštaja i konkretnih izveštaja za pojedinačna zaposlena lica, grupu zaposlenih ili izveštaje tokom određenog vremenskog perioda.

Nakon obavljanja funkcije administratora više od dve godine, zaposleni/a je prepoznao/la mogućnost korišćenja sistema u svoju korist, menjanjem vremena dolaska i odlaska, tako da odgovaraju zvanično definisanom radnom vremenu, a ne stvarnom vremenu dolaska i odlaska. Ovo lice je to radilo više od jedne i po godine a da nije otkriveno od strane kolega ili nadređenih. Jednog dana je iskrsla potreba da ovo lice promeni podatke za to jutro ili za zadnji radni dan, bez provere kako se podacima upravlja i kako se oni čuvaju u sistemu, posebno bez provere kako se pohranjuju aktivnosti administratora. Iako retko, povremeno, mogućnost za zloupotrebu sistema je korišćena ne samo za kasne dolaske na posao, već i za čitave dane.

Skoro dve godine nakon što je raspoređen na mesto administratora, institucija je izvršila preraspodelu zadataka među zaposlenima, što je kao rezultat imalo imenovanje druge osobe na mesto administratora. Novi administrator je slučajno otvorio datoteke evidencije (logove) i shvatio da su neka dešavanja označena, i time drugačija od drugih. Zainteresovan da vidi kako su se razlikovali od preostalih dešavanja, novi administrator je počeo detaljnu reviziju evidencije. Ubrzo je postalo jasno šta su označena dešavanja predstavljala i on/ona je o tome obavestio/la upravu.

Istražni postupak je počeo imenovanjem zvaničnog IT lica iz uprave, čiji glavni zadatak je bio da proveri sve izveštaje i datoteke evidencije na radu. Zaključak tokom ovog postupka se u potpunosti poklapao sa pretpostavkom novoimenovanog administratora.

Zbog priznanja zaposlenog/e, slučaj nije sudski procesuiran i rešen je interno. Postoji procena finansijske štete koju je on/ona počinio/la nedolaženjem na posao i zbog neizvršavanja zadataka, i za taj iznos je zaposleni/a kažnjen/a adekvatnom disciplinskom merom. Ipak, nije došlo do otkaza ugovora o radu sa zaposlenim/om.

Slučaj iz Makedonije 5: Zloupotreba prava administratora

U procesu izdavanja uvoznih dozvola, između ostalih potrebnih dokumenata, lice mora takođe podneti bankarsku garanciju u vrednosti srazmernoj vrednosti roba ili usluga koje se uvoze. Pravila su veoma striktna, što je veća bankarska garancija, veća je vrednost robe za koju je uvoz dozvoljen.

Sistem za proveru podataka na granici i izdavanje dozvola koristi podatke koji su uneseni, pohranjeni i čuvani u administrativnom centru uprave A. Pored toga što se određeni podaci pohranjuju po osnovu razmene između ovog sistema i sistema drugih uprava, iznose koji se odnose na same bankarske garancije unose administrativni službenici, a ne bankarski informacioni sistem.

Jedan od administratora, između premeštaja iz jednog administrativnog centra u drugi je otkrio način da iskoristi svoju poziciju. Nakon premeštaja iz administrativnog centra B u administrativni centar C, primetio je da su njegova pristupna prava i dalje ista, pa je kreirao za sebe novi korisnički nalog. Glavni administrator nije vršio redovne provere i revizije prava premeštenih administratora, i zbog toga je administrator bio u mogućnosti da počini veliki broj krivičnih dela korišćenjem novokreiranog korisničkog naloga.

Tokom perioda od dve godine, korišćenjem lažnog naloga u preko 100 navrata, i korišćenjm sopstvenog naloga u nekoliko desetina navrata, zaposleni je uneo više iznose bankarskih garancija pre kontrole na granici, i vratio prave vrednosti nakon izvršenih kontrola. Kada su granični službenici proverili svoj sistem, podaci koje je administrator izmenio su izgledali regularni. Ostao je u stalnom kontaktu sa upravom preduzeća da bi znao kada će roba prispeti na granicu. U najkraćem mogućem roku, podaci u instituciji A su sadržali deklaracije sa najvećim bankarskim garancijama.

Slučaj je otkriven internom kontrolom i revizijom sa ICT sektorom prilikom sprovođenja redovne revizije. Istražni tim je ustanovljen kako bi se razmotrio ovaj slučaj i utvrdilo da li je u pitanju zaista slučaj korupcije, da li su počinjena druga krivična dela, i u kom obimu su počinjena krivična dela.

Analiziranjem dešavanja u datotekama evidencije sistema, IT istražni tim je utvrdio IP adrese sa kojih su izvršene izmene, što ih je dovelo do računara administratora. Datoteke evidencije nisu mogle biti menjane, te je bilo veoma jednostavno napraviti listu aktivnosti koje je administrator odradio.

Dalje je otkriveno da je zbog izbora korisničkog imena i lozinke ovo delo učinjeno sa predumišljajem. Administrator je osigurao da, tokom redovnih provera, korisničko ime i lozinka budu među zadnjim koji bi se proveravali, a to su inače bili korisničko ime i lozinka koji se ni po čemu nisu isticali, i time je izbegnuta svaka sumnja.

Dokazano je samo da je on na ovaj način zloupotrebljavao sistem uprave A u saradnji sa jednom lokalnom kompanijom. Finansijska šteta za državu je procenjena na iznos od 10.614.779,00 denara.

Crna Gora

Pripremili Dušan Drakić i Ivan Lazarević

Slučaj iz Crne Gore 1: Zloupotreba službenog položaja i falsifikovanje zvaničnih dokumenata

Predmetni slučaj je primer nemara na radnom mestu i nelegalnog vršenja funkcije državnog organa tj. zloupotrebe funkcije i položaja od strane lica zaposlenih u državnom organu.

Pasoš lica „A" je istekao i on je dobio novi pasoš. Zvaničnici u nadležnom organu Ministarstva unutrašnjih poslova Crne Gore su odlučili da koriste stari pasoš u kriminalne svrhe. Koristeći pečat tog organa, oni su za pet godina produžili važenje starog pasoša na ime lice „A" koji je istekao, ali sa fotografijom trećeg lica „B".

Očigledno, lice „B" je bilo traženo od policije. Kao posledica toga, lice „A" je zadržano na putničkom terminalu aerodroma Lisabon, gde je bilo kako bi se ukrcalo na brod na kojem je trebalo da radi u narednom periodu. Nakon provere njegovih identifikacionih dokumenata, policijski istražni tim ga je predao (u lisicama) Emigracionom centru na aerodromu, gde je proveo 48 sati, nakon čega ga je policija (vezanog) stavila na let iz Portugala za Beograd preko Švajcarske. Ovo lice nije ni videlo svoja dokumenta do dolaska u Švajcarsku. Tretman od strane portugalskih vlasti i slika koju su o njemu kreirali kao o kriminalcu prouzrokovali su kod lica „A" mentalnu agoniju, dok mu je reputacija bila narušena u njegovom rodnom gradu, porodici, među prijateljima, itd.

Neizvršavanje obaveze ovlašćenog lica da uništi istekli pasoš, i aktivnosti preduzete na produžavanju roka važenja pasoša pod istim imenom ali sa fotografijom trećeg lica ("B") i potvrđivanje toga sa zvaničnim pečatom, predstavljaju aktivnosti koje čine krivično delo zloupotrebe položaja i istovremeno potvrđuju nelegalno ponašanje državnih organa.

U ovom slučaju, zvaničnici u nadležnom organu Ministarstva unutrašnjih poslova nisu uništili pasoš, koji je nakon izdavanja novog pasoša oduzet od lica „A", državljanina Crne Gore.

Prvostepeni sud u ovom krivičnom postupku je zaključio da neizvršavanje obaveze ovlašćenog lica da uništi istekli pasoš, i naredne aktivnosti objašnjene u pasusima iznad, predstavljaju aktivnosti koje čine krivično delo zloupotrebe službenog položaja, u skladu sa Članom 416, Stav 1 Krivičnog zakonika Crne Gore. Istovremeno, za krivično delo je zaprećena zatvorska kazna u trajanju od tri meseca do pet godina. U skladu sa Članom 416 Krivičnog zakonika Crne Gore, zloupotreba službenog položaja nastaje ako službeno lice protivpravnim iskorišćavanjem svog službenog položaja ili ovlašćenja, prekorači granice svog službenog ovlašćenja ili nevršenjem svoje službene dužnosti, pribavi sebi ili drugom korist, drugom nanese štetu ili teže povredi prava drugog.

Nakon podnošenja žalbe na odluku prvostepenog suda, Vrhovni sud Crne Gore je potvrdio presudu Osnovnog suda i u obrazloženju presude br. 902/13 od 12. aprila 2013. godine, jasno naveo sledeće:

"sve navedene činjenice takođe potvrđuju nelegalno činjenje optuženog – nadležne službe Ministarstva unutrašnjih poslova na Cetinju, što je dovelo do štete po tužioca, za koju je, u skladu sa odredbama člana 172, stav 1 prethodno važećeg zakona o obligacionim odnosima, optuženi odgovoran, a u skladu sa odredbama Člana 154 istog zakona optuženi će nadoknaditi nastalu štetu. U prezentovanju svojih zaključaka, Sud je takođe naveo sadržaje prethodno prezentovanih konkretnih aktivnosti u ovom slučaju koji predstavljaju nelegalno delovanje optuženog i sve druge okolnosti u slučaju, kao i činjenicu da je identitet trećeg lica, koje je zloupotrebilo prethodni zvanični dokument žrtve i njegove identifikacione podatke, potvrđen, i da je to lice optuženo za više krivičnih dela počinjenih na teritoriji druge države (Italije)."

Tokom postupka, žrtva je dokazala da je, zbog nelegalnog delovanja optuženog organa, pretrpela nematerijalnu štetu zbog povrede ugleda, časti, kršenja sloboda i prava ličnosti.

Takođe navodeći podatke dobijene od strane predmetnog brodskog prevoznika o iznosu zarada (po svim osnovama) tužioca, zarađenih tokom perioda boravka na brodu (i izuzetih za sporni period), i pravila koja se tiču štete u skladu sa kriterijumima koji važe na dan presude (Član 189 stav 2 Zakona o obligacionim odnosima), iznos povezane materijalne štete za tužioca je bio pravilno obračunat od strane finansijskog eksperta angažovanog od strane suda.

Zaključak 1

Gore navedeni primer pokazuje da postoji nedostatak ili propust u informacionom sistemu za izdavanje pasoša. Sistem bi trebao, ali ne uspeva, da eliminiše rizik od korišćenja ili izdavanja pasoša nakon isteka roka važenja. Takođe, jasno je da takav dokument ne bi bilo moguće produžiti bez naknadnog unošenja netačnih podataka u informacioni sistem za izdavanje putnih dokumenata. Interesantno je da ne postoje elektronski tragovi službenika koji je izdao takav dokument. Podaci o datumu, vremenu i imenu službenika koji je pristupio sistemu i obradio i izdao dokument bi trebali biti dostupni u informacionom sistemu. To takođe znači da sistemi za izdavanje i kontrolu putnih dokumenata, posebno na graničnim prelazima i aerodromima, moraju biti u mogućnosti da analiziraju i eliminišu takve falsifikovane dokumente ukoliko se pojave u sistemu. Identifikacioni brojevi takvih dokumenata treba da budu automatski identifikovani i za stalno izbačeni iz elektronskih evidencija, i sami IT sistem treba da bude u mogućnosti da ih prepozna kao nevažeće (čak iako bi ti podaci bili od koristi samo u Crnoj Gori, a ne i u stranim zemljama).

Da bi rešili ovaj i slične probleme, neophodno je da se sve IT baze podataka redovno ažuriraju i međusobno povezuju što je više moguće, kako bi identifikacioni broj takvih dokumenata bio elektronski eliminisan iz daljeg korišćenja i da ne bi bio predmet zloupotrebe od strane ljudskog faktora. Ipak, i dalje će postojati rizik da se takav dokument fizički prebaci

u treću zemlju, i koristi kao važeći dokument u toj zemlji, što postavlja pitanje potrebe regionalne IT saradnje, sa ciljem eliminisanja potencijalnih rizika.

Slučaj iz Crne Gore 2: Upotreba IT podataka sa ciljem nanošenja političke štete

Da bi se isprovocirala politička destabilizacija i diskreditovao određeni viši vladin zvaničnik/političar ili stekla lična korist, u medijima je objavljen navodni telefonski listing članova organizovane kriminalne organizacije, koji je sadržao telefonske brojeve viših vladinih zvaničnika/političara. Namera je bila da se utiče na javno mnenje preko indirektnog povezivanja zvaničnika sa tom organizovanom kriminalnom grupomkako bi se kreirala slika navodne veze između državnih organa i organizovanog kriminala.

Krajem 2011. godine, listing je poslat iz dve lokalne pošte dnevnom listu, kao i elektronskim putem sa IP adrese na bežičnoj mreži koja se nalazi u zgradi gde živi viši državni zvaničnik. Dnevni list je objavio navodni listig, u skladu sa kojim je šef kriminalne grupe, za kojeg je Interpol izdao nalog za hapšenje po optužbi za krijumčarenje narkotika, imao telefonsku komunikaciju sa više vladinih zvaničnika u Crnoj Gori. Ono što je posebno interesantno je da se listing odnosi na telefonsku komunikaciju šefa kriminalne grupe iz 2008. godine, i čuvan je tri godine pre nego što je objavljen. To je dalje produbilo sumnju i špekulacije da je neko iz operativne strukture policije/unutrašnjih poslova/sektora bezbednosti bio uključen u slučaj, vođen pohlepom ili željom za osvetom, da bi prouzrokovao političku destabilizaciju u zemlji, za svoj ili za račun još uvek nepoznatih lica.

Slučaj nije stigao do suda, budući da je istraga otkrila da nije postojala telefonska komunikacija između viših vladinih zvaničnika/političara i glavnog organizatora kriminalne grupe i da je listing krivotvoren i da nije bio policijski dokument, kako je predstavljeno u medijima. Zatim, telefonska kompanija je jasno navela da objavljeni listing, za koji je dnevni list tvrdio da je mobilni operater dostavio policiji za potrebe istrage, nije bio listing iz tog preduzeća, tj. nije u skladu ni sa oblikom niti sa sadržajem listinga u kojima se navode podaci o komunikacijama na zahtev ovlašćenog organa, u skladu sa važećim zakonodavstvom u Crnoj Gori. Utvrđeno je da je listing lica označenog kao glavnog organizatora kriminalne grupe, a koji je napravljen od strane uprave policije za njihove operativne/istražne potrebe naknadno krivotvoren, tj. sadržao je imena i brojeve viših vladinih zvaničnika i njihove adrese.

Ipak, i dalje je nejasno ko je dostavio originalni listing ili onaj koji policija koristi za operativne potrebe, niti ko je krivotvorio dokument tako da izgleda kao autentičan. Takođe nije jasno kako i po kom osnovu je Uprava policije dobila listing iz 2008. godine i kakva vrsta istrage je sprovođena protiv navedenog glavnog organizatora kriminalne grupe, niti šta je bio rezultat istrage i kakva vrsta dokaza je prikupljena u to vreme.

Takođe ostalo je nepoznato ko je osoba koja je poslala materijale, tj. i-mejl poruke sa gore pomenute IP adrese.

Ovaj slučaj predstavlja klasičan primer kršenja osnovnih ljudskih prava garantovanih Ustavom i međunarodnim konvencijama, kršenje prava na privatnost, moguću zloupotrebu ovlašćenja, budući da se listinzi sa razgovorima ne mogu dobiti bez sudske saglasnosti, niti objaviti u medijima. Takođe, veoma je verovatno da je ovaj slučaj povezan sa mitom i zloupotrebom službenog položaja, kao i falsifikovanjem podataka i zloupotrebom IT sistema.

Zaključak 2

Gore navedeni primer jasno pokazuje ranjivost IT sistema i mogućnost njihove zloupotrebe. Slučaj se primarno tiče ustavnog principa koji se primenjuje na nekršenje poverljivosti pisama, telefonskih razgovora, i ostalih sredstava komunikacije. Sa druge strane, tu je pitanje moguće odgovornosti nadležnih lica kod telefonskog operatera, pre svega u vezi sa poverljivošću i presretanjem, i zloupotrebom elektronske prepiske. Operater je u obavezi da obezbedi tehničke i organizacione preduslove koji omogućavaju presretanje komunikacija, tj. da omogući nadležnim državnim organima da dobiju pohranjene podatke o saobraćaju i lokacijama, ali samo u skladu sa sudskom odlukom, ukoliko je neophodno za sprovođenje krivičnih postupaka, ili iz razloga bezbednosti Crne Gore. Javnost nije dobila odgovore na pitanje da li je takvo odobrenje postojalo i kakav postupak je u to vreme vođen od strane policije i zbog čega. Slučaj se pokazao izuzetno komplikovanim, jer pored potencijalnih elemenata zloupotrebe ovlašćenja takođe ima elemente računarskog kriminala, za šta je potrebno veliko znanje, obuka i tehnički kapaciteti kao i kvalitetna međunarodna saradnja.

Ovaj slučaj nije imao sudski epilog niti je pružio odgovore na niz gore navedenih pitanja. Nikakva objektivna niti subjektivna odgovornost nije ustanovljena. Svakako, pored političke štete koja je prouzrokovana ovim dešavanjima, ono što je još važnije je činjenica da ukoliko se takav slučaj, nevezano za motive i razloge, mogao desiti najvišim državnim zvaničnicima, šta bi mogao da očekuje prosečan građanin Crne Gore, ukoliko se on/ona nađu u istoj ili sličnoj situaciji.

Takođe treba da navedemo neadekvatnu i nedovoljnu reakciju od strane državnih organa u vezi sa utvrđivanjem objektivne odgovornosti za rad institucija i mogućnost otkrivanja učinioca, što nesumnjivo prouzrokuje nemerljivu štetu za državu i opšti princip vladavine prava, a što se ogleda u gubitku poverenja građana u rad institucija. Potrebno je da preduzmemo dodatne napore i detaljno analiziramo postojeći sistem kako bi uspostavili jasne procedure za dobijanje i korišćenje operativnih podataka i za uspostavljanje jasnih i konkretnih preventivnih mera, uz korišćenje softvera i mogućnosti IT.

Konkretno, neophodno je nastaviti rad na poboljšavanju komunikacije sa javnošću i medijima u takvim slučajevima kako bi se povećalo poverenje javnosti u rad državnih organa.

Slučaj iz Crne Gore 3: Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre

Ovaj slučaj je povezan sa elektronskim izdavanjem lažnih dozvola ili drugih uverenja da bi se takva uverenja kasnije koristila u pravnim postupcima.

Odlukom Osnovog suda u Kotoru iz 2010. godine, dve osobe, službenik i rukovodilac opštinskog katastra u Crnoj Gori, su proglašeni krivim za krivčno delo zloupotrebe službenog položaja, u skladu sa Članom 416, stav 3 u vezi sa stavom 1 Krivičnog zakonika Crne Gore. Obrazloženje presude je glasilo da su koristili svoj položaj da steknu nelegalnu imovinsku korist, i prekoračili ograničenja svog službenog položaja tako što su doneli i objavili odluke za koje nisu imali ovlašćenja. Prvom odlukom su omogućili restituciju i prenos zemljišta u državnom vlasništvu navodnom prethodnom vlasniku zemljišta, a zatim prodali zemljište neposredno nakon registracije. Istovremeno, i na isti način su izdali drugu odluku sa lažnim sadržajem, kojom je neko drugo zemljište vraćeno svom navodnom prethodnom vlasniku. U ovom slučaju, navodni vlasnik je, uz pomoć i zahvaljujući potpisima optuženih lica, prodao zemlju odmah nakon neosnovane registracije, iako nije imao važeći vlasnički list. Sprovođenjem i omogućavanjem takvih aktivnosti i na osnovu restitucije zemljišta, optužena lica su stekla imovinsku korist u iznosu 571.307,32 evra.

Ta dva lica su osuđena na kaznu zatvora u trajanju od dve godine.

Dokazano je da su oba optužena u ovom konkretnom slučaju prekoračila svoja zvanična ovlašćenja. Takođe, dokazano je da postupku restitucije i vraćanja zemljišta nije prethodila odluka skupšitne opštine, kao i da je odluka donešena bez zahteva ovlašćenog lica, prethodnog vlasnika, i na taj način se izbegla procedura predviđena za upravni postupak. Naredne aktivnosti su kao rezultat imale usvajanje odluka u katastru, gde je bilo jasno da postupak nije bio ispoštovan, i da nije bio u interesu opštine.

Krivični zakonik Crne Gore definiše krivično delo zloupotrebe službenog položaja kao prekoračenje granica službenog ovlašćenja radi pribavljanja imovinske koristi veće od 30.000 evra.

Stoga, sud je presudio da su optuženi (službenik i rukovodilac u opštinskom katastru) delovali bez ovlašćenja u tim slučajevima. Oni su znali da nisu ovlašćeni za restituciju i nisu mogli da prenesu zemljište navodnim prethodnim vlasnicima. Oni su takođe znali da je zemljište pod nadležnošću drugog opštinskog organa. Pored toga, dokazi su pokazali da odluke donešene od strane optuženih nisu bile propraćene dokumentacijom koja bi dokazala vlasništvo navodnih prethodnih vlasnika kojima je zemljište vraćeno. Nadalje, naredni postupak restitucije je sproveden na usmeni zahtev lica koje je kupilo zemljište od navodnih prethodnih vlasnika i pored činjenice da je u pitanju nacionalizovano zemljište i da ga nije moguće prodati. Za sud je bilo nesporno da su oba optužena lica prekoračila svoja ovlašćenja, procedura predviđena za upravni postupak nije sprovedena, niti su zaštićeni interesi opštine, te su prema tome oba optužena lica počinila krivčna dela za koja su optužena.

Zaključak 3

Gore navedeni primer jasno pokazuje da podaci iz javnih registara, koji se čuvaju elektronskim putem, mogu biti podložni manipulaciji od lica koja su ovlašćena da im pristupaju i unose podatke.

Unošenju podataka u elektronsku katastarsku evidenciju je prethodilo usvajanje nezakonite odluke, pa bi ovaj slučaj mogao predstavljati ne samo krivično delo zloupotrebe službenog položaja naveden u Članu 416 stav 3 u vezi sa stavom 1 Krivičnog zakonika Crne Gore, već možda i neki od krivičnih dela vezanih za bezbednost kompjuterskih podataka. Zbog toga je jasno da potencijalni kupci zemljišta mogu biti u zabludi kada proveravaju podatke u katastarskim listovima, i zatim mogu biti izloženi naknadnim sporovima oko utvrđivanja prava vlasništva, kada i najmanji nedostatak savesti kupca imovine može prouzrokovati znatnu materijalnu štetu.

U ovom slučaju je jasno pokazano da su izmene napravljene u bazi katastarske evidencije, nakon odluke opštinskog katastra, koji inače nema ovlašćenja da donosi takve odluke. Slučaj dokazuje da je postojeći IT sistem i postupak čuvanja evidencije, konkretno način pristupa bazama podataka i IT sistemu, i mogućnost pravljenja izmene u evidencijama bez važeće zakonske osnove, nepotpun i neadekvatan. Od presudne je važnosti poboljšati IT sistem tako da se jasno i nedvosmisleno utvrdi procedura pristupa, kao i da se utvrde organi koji mogu doneti odluke o pristupanju i izmeni podataka u evidencijama

.

Slučaj iz Crne Gore 4: Nezakonito izdavanje putnih isprava

Jedna osoba zaposlena u Uprave policije Crne Gore u Podgorici, u svojstvu službenice u odseku za putna dokumenta i oružje je optužena za korišćenje službenog položaja kako bi omogućila drugim licima da steknu korist tokom 2004 i 2005. godine. Službenica je postupala u suprotnosti sa Zakonom o putnim ispravama i Odlukom o izdavanju pasoša, zajedničkog pasoša, putnog lista i vize, nakon dobijanja zahteva za izdavanje dve putne isprave (pasoša), i izradom dokumenata bez prethodne provere identiteta podnosioca zahteva za kojeg je zatraženo izdavanje putne isprave. Ona nije sprovela proveru u skladu sa gore navedenim uredbama. Stoga je počinila krivično delo zloupotrebe službenog položaja, Član 416, stav 1 Krivičnog zakonika.

Interesantno je da odluka prvostepenog suda, uzimajući u obzir optužbe, odbranu i sve dokaze, odlučila da optužena treba da bude izuzeta od gonjenja u skladu sa članom 363 stav 1 Zakona o krivičnom postupku – budući da krivično delo za koje je optužena ne predstavlja krivično delo u skladu sa zakonom. U presudi je naglasak stavljen na činjenicu da je optužena preduzela aktivnosti da bi omogućila sticanje koristi za ta lica, ali je činjenični opis krivične

radnje izostavio deo koji se odnosi na to da su predmetni pasoši izdati licima naznačenim u presudi, a sa tim u vezi izostavljen je deo koji se odnosi na sticanje koristi za ta lica.

Posebno intreresantan detalj iz presude je da je optužena navela da, iako je imala pristup predmetnim putnim ispravama, ne postoji evidencija putnih isprava, niti su nađeni zahtevi za izdavanje putnih isprava. Sve je nestalo. Kada je njen nadređeni naložio nalaženje dokumenata, otkrili su da je sva dokumenatcija nestala. Interna istraga nije mogla utvrditi ko je uključen u nestanak dokumentacije, niti šta se sa njom desilo. Činjenica je da su dokumenti čuvani u arhivi, koja se nalazi u podrumu centra bezbednosti, i da ih je čuvao poseban službenik. Ipak, svi zaposleni u odeljenju su imali pristup arhivi. Optužena je zbog toga špekulisala po kom osnovu je njen prethodni nadređeni zaključio da je od sedam kolega ona jedini prestupnik.

Tokom postupka, došlo je do izmene Krivičnog zakonika. Krivično delo za koje je ova službenica bila optužena više nije predstavljalo krivično delo u skladu sa izmenama. Saglasno Članu 133 stav 1 Krivičnog zakonika, sud je stoga bio u obavezi da primeni zakon koji je najblaži za optuženu.

U skladu sa tim optužena je oslobođena optužbi za predmetno delo i predmet je vraćen na ponovni postupak.

Novi postupak je započet. Uključio je ne samo gore navedenu službenicu, već i dva službenika iz Uprave policije/Ministarstva unutrašnjih poslova. Dva novooptužena su optužena za korišćenje službenog položaja za krivotvorenje i izdavanje velikog broj ličnih karti, vozačkih dozvola i pasoša u periodu između 2011 i januara 2013. godine. Oni su takođe optuženi za upisivanje lica kojima su izdali legitimacije u evidenciju državljana Crne Gore. Na posletku, optuženi su za primanje mita za svako izdavanje lažnih dokumenata u iznosu od 50 do 1.300 evra. Ukupno, optužba je obuhvatila 17 lica za korupciju, tj. davanje mita i krivotvorenje dokumenata.

Dva lica su optužena za posredovanje u primanju mita. Oni su tražili osobe kojima su takva dokumenta bila potrebna, a zatim ih uz nadoknadu povezivali sa optuženim službenicima.

Još jedno lice je bilo optuženo za krivotvorenje dokumenata. To je bio informatički inženjer koji bi, u dogovoru sa gore navedenim pomagačima, pravio lažna uverenja o položenim vozačkim ispitima.

Sedamnaest lica je optuženo za davanje mita i krivotvorenje dokumenata.

Čitav slučaj je sudski okončan u julu 2014. godine. Službenica, prvooptužena, je osuđena za primanje mita, vršenje protivzakonitog uticaja, i pomaganje u krivotvorenju dokumenata. Ona je osuđena na jedinstvenu zatvorsku kaznu od 4 i po godine.

Sve u svemu, provosnažnom presudom Specijalnog posebnog veća Višeg suda u Podgorici grupa od sedamnaest članova je osuđena na ukupno sedamnaest godina i četiri meseca zatvorske kazne zbog krivotvorenja dokumenata i davanja i primanja mita.

Zaključak 4

Gore navedeni primeri takođe pokazuju da postoji, ili je postojao, nedostatak ili propust u sistemu upravljanja dokumentima Ministarstva unutrašnjih poslova. Ne postoji elektronska evidencija skeniranih zahteva za izdavanje pasoša u informa—cionom sistemu, što bi eliminisalo rizik korišćenja i izdavanja krivotvorenih dokumenata. Takođe je očigledno da ne postoje elektronski tragovi koji bi pokazali ko je izdao takva dokumenta.

Moguće rešenje u ovom i sličnim slučajevima je uvođenje obaveznog skeniranja dokumenata ili uspostavljanja elektronske baze podataka svih dokumenata koji su podnešeni i izdati sa kopijom u papiru sa obaveznom opcijom dvostrukog bekapa, kako bi se osigurala bezbednost podataka u slučaju njihovog namernog ili slučajnog uništenja. Takođe, neophodno je poboljšati elektronski sistem praćenja fizičkog pristupa prostorijama gde se predmeti i zvanični dokumenti čuvaju.

Rezime

Na kraju, treba imati u vidu da što se tiče krivičnog pravnog sistema u Crnoj Gori, krivična dela korupcije u vršenju službene dužnosti su navedena u Glavama XXXIV i XXII Krivičnog zakonika. Kao takva, ta krivična dela ne predstavljaju ništa više od različitih tipova i odstupanja od zakonom definisanih načina vršenja službenih dužnosti. Zbog toga, krivična korupcija predstavlja veću pretnju po društvo pošto su prekršioci prvenstveno državni zvaničnici. Preko njihovih aktivnosti oni krše pravni i upravni sistem i smanjuju efikasnost države. Pored očiglednih materijalnih posledica nastalih po osnovnu takvih krivičnih dela, najštetnije posledice uključuju pretnje po integritet institucija i pad poverenja javnosti u rad državnih i lokalnih vlasti. To je na posletku, funkcionisanje države.

Krivični Zakonik Crne Gore (KZ) predviđa sledeća krivična dela sa obeležjima korupcije:

- Pranje novca (Član 268 KZ); Povreda ravnopravnosti u vršenju privredne delatnosti (Član 269 KZ);
- Zloupotreba monopolističkog položaja (Član 270 KZ);
- Zloupotreba položaja u privrednom poslovanju (Član 272 KZ);
- Prouzrokovanje stečaja (Član 273 KZ) i Prouzrokovanje lažnog stečaja (Član 274 KZ);
- Zloupotreba ovlašćenja u privredi (Član 276 KZ);
- Primanje mita u privrednom poslovanju (Član 276a KZ);
- Davanje mita u privrednom poslovanju (Član 276b KZ), Lažan bilans (Član 278 KZ);
- Zloupotreba procene (Član 279 KZ);
- Odavanje poslovne tajne (Član 280 KZ);
- Zloupotreba povlašćenih informacija (Član 281 KZ);
- Zloupotreba službenog položaja (Član 416 KZ);;
- Nesavestan rad u službi (Član 417 KZ);
- Prevara u službi (Član 419 KZ);
- Protivzakoniti uticaj (Član 422 KZ);
- Navođenje na protivzakoniti uticaj (Član 422A KZ);

- Primanje mita (Član 423 KZ);
- Davanje mita (Član 424 KZ).

Uopšteno gledajući, za takva krivična dela je predviđena zatvorska kazna, i zaplena imovine stečene istim kada je to moguće. Ipak, u praksi, ta krivična dela su često povezana sa drugim krivičnim delima, koja u osnovi nisu koruptivna krivična dela, već su sa njima blisko povezana. To uključuje krivotvorenje zvaničnih dokumenata i krivična dela vezana za bezbednost računarskih podataka. Čini se da sudskoj praksi još nema dovoljno primera krivičnih dela korupcije zbog zloupotrebe računarskih podataka, ali će praksa pokazati koliko su adekvatne pravne zaštitne mere i da li postoji potreba uvođenja novih krivičnih dela vezanih za računarski kriminal.

Svakako ostaje činjenica da je jedan od efektivnih mehanizama borbe protiv korupcije uspešno krivično gonjenje. To znači efektivne metode za otkrivanje i prikupljanje dokaza i postojanje efektivnih i adekvatnih kazni.

Nadležne institucije za otkrivanje, gonjenje i sankcionisanje u Crnoj Gori su policija, javni tužilac i sudovi. Ove institucije su funkcionalno povezane i svaka od njih, u okviru svojih nadležnosti, primenjuje zakonske institute u borbi protiv korupcije. Ipak, oni se ponekad suočavaju sa poteškoćama u primeni takvih instituta, što iziskuje potrebu za različitim stručnim diskusijama i izmenama zakona u oblasti korupcije. Policiji, kao organu nadležnom za otkrivanje krivičnih dela, je potrebna saradnja i uključivanje drugih institucija: primarno bankarskog sektora i drugih finansijskih institucija, Uprave za antikorupcijsku inicijativu, Uprave za sprečavanje pranja novca, nevladinog sektora, i samih građana. Sa jedne strane, policija ima ovlašćenje da primenjuje razne metode prikupljanja dokaza, tj. mere tajnog nadzora krivičnih dela korupcije, bez obzira na način vršenja krivičnih dela i propisane kazne. Sa druge strane, takvi metodi takođe postavljaju pitanje potencijalnog kršenja osnovnih ljudskih prava i privatnosti.

Nevezano za ove mere suzbijanja, sprečavanje korupcije je od najvećeg značaja. To u osnovi uključuje podizanje nivoa svesti, znanja, veština, kao i odgovornosti zaposlenih, sa jedne strane, i obezbeđenje adekvatnih fizičkih, tehničkih i finansijskih uslova za zaposlene sa druge strane.

Prema tome, jedna od modernih metoda prevencije za obezbeđenje i uspostavljanje zakonskog i etičkog kvaliteta rada u državnm organima je priprema plana integriteta za institucije. Oni predstavljaju interne preventivne antikorupcione dokumente, koji mapiraju ranjiva područja u institucijama, tj. predstavljaju analizu rizika radnih procesa u svakom državnom organu, organizaciji ili službi. Na posletku, plan integriteta treba shvatiti kao oblik strateškog dokumenta, kvaliteta i upravljanja rizikom, što kao rezultat treba da ima veći kvalitet usluga u javnom sektoru, smanjenje troškova i povećanje otpornosti institucija na nelegalne i neželjene efekte. To uključuje digitalizaciju i korišćenje IT kao jednog od ključnih elemenata.

Srbija

Pripremili Nemanja Nenadić i Bojan Cvetković

Sprovodeći istraživanje o koruptivnim delima koja su uključivala IT, za razgovor su kontaktirane sledeće institucije:

- Ministarstvo pravde
- Kancelarija poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti
- Direkcija za elektronsku upravu
- Ministarstvo unutrašnjih poslova
- Ministarstvo finansija
- Zaštitnik građana

Samo prva dva organa su odgovorila na pozive i zakazani su sastanci za dobijanje informacija. Direkcija za elektronsku upravu je odgovorila na poziv ali sastanak nikada nije bio organizovan.

Slučaj iz Srbije 1: Seks ispred Beogradske arene

Početkom marta 2011. godine, na internetu je objavljen video snimak koji prikazuje seksualni odnos ispred Beogradske arene. Sami snimak je nastao u jutarnjim časovima 24. aprila 2010. godine. Pošto je snimak nastao putem opreme za video nadzor koji koristi Ministarstvo unutrašnjih poslova (MUP) za potrebe kontrolisanja saobraćaja, to predstavlja jasan slučaj koruptivnog krivičnog dela „zloupotrebe službenog položaja".

Prvobitna reakcija ljudi koji se vide na originalnom snimku na internetu je bila relativno blaga, ali u mesecima koji su sledili nakon incidenta, postalo je prilično jasno da je snimak imao znatan uticaj na njhove živote i živote njihovih porodica. Identiteti Elizabete M. (22) i Milovana S. (24) su javno otkriveni, i oni su bukvalno morali da izbegavaju bilo kakvu vrstu javnog pojavljivanja i njihove porodice su, prema sopstvenim tvrdnjama, „prošle kroz pakao".

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Rodoljub Šabić (poverenik) podneo je krivičnu prijavu Višem tužilaštvu u Beogradu protiv „nepoznatog policijskog službenika" zbog objavljivanja snimka seksualnog odnosa između dve odrasle osobe na internetu, koristeći snimak sa video nadzora koji koristi Ministarstvo unutrašnjih poslova (MUP) za kontrolisanje saobraćaja u Beogradu. On je naveo da je jasno da MUP nije preduzeo sve tehničke, ljudske i organizacione mere predostrožnosti da zaštiti podatke sprečavajući moguću zloupotrebu snimaka video nadzora. U ovom konkretnom slučaju, IT je zloupotrebljen nelegalnim dobijanjem podataka kroz manipulaciju sa postojećim podacima i procedurama. U vreme kada se ovo dogodilo, jedina uredba koja široko pokriva

ovaj slučaj je interna uredba Saobraćajne policije MUP-a koja navodi da snimak video nadzora može biti korišćen samo interno u okviru MUP-a za potrebe istraživanja okolnosti saobraćajnih nezgoda. Važno je primetiti da nisu postojali nacionalni propisi koje pokrivaju ovaj slučaj. Takođe, izmanipulisana je ključna interna politika MUP-a *„ukoliko nešto nije jasno regulisano niti nacionalnim niti internim propisima MUP-a, zaposleni u MUP-u moraju da zatraže od MUP-a zvaničnu dozvolu a ne da pretpostavljaju da mogu nešto"* da preduzmu.

"Radi se o slučaju koji predstavlja veoma ozbiljno kršenje prava na privatnost i ozbiljno kršenje Zakona o zaštiti ličnih podataka", izjavio je poverenik, dodajući da je nepostojanje neophodnih procedura i postojanje sigurnosnih propusta dovelo do incidenta.

U skladu sa svojim dužnostima, poverenik je započeo kontrolu da utvrdi kako se sprovodi Zakon o zaštiti podataka o ličnosti od strane MUP-a, što je na kraju za posledicu imalo izdavanje upozorenja MUP-u, koje je sadržalo listu 14 mera koje je potrebno preduzeti na tehničkom, ljudskom i organizacionom nivou zbog zaštite podataka kako bi se izbegla bilo kakva vrsta zloupotrebe u budućnosti. Poverenik je takođe zatražio da ga MUP zvanično obavesti u zakonskom roku od 15 dana o planiranim merama koje namerava da usvoji i sprovede na eliminisanju neregularnosti. Ovom prilikom, poverenik je ponovo podsetio na činjenicu da u Srbiji ne postoji zakon o video nadzoru, iako je veoma veliki broj ljudi uključenih u video nadzor.

U prvom reagovanju MUP-a navedeno je da će biti veoma teško utvrditi ko je kopirao video snimak i objavio ga na internetu, budući da svi rukovodioci, operateri i administratori, u Komandno operativnom centru (KOC) imaju pristup snimcima video nadzora što, uz nedostatak procedura za pristup i bezbednost podataka, predstavlja jasnu slabost u administriranju sistema video nadzora KOC MUP-a.

Nakon upozorenja izdatog od strane poverenika, MUP je preduzeo konretne korake na kažnjavanju ljudi uključenih u incident. Interna istraga je utvrdila da je postojalo 10 kompjuterskih radnih stanica sa kojih je video zapis mogao biti kopiran (preuzet).

Disciplinski postupak za zloupotrebu ovlašćenja je pokrenut protiv policijskog službenika, koji je bio na dužnosti nadzornika u beogradskom KOC-u MUP-a na dan kada je video zapis snimljen. MUP je objavio detaljne instrukcije u zvaničnom uputstvu „Obavezni uslovi za korišćenje i održavanje video nadzora na gradskim ulicama i raskrsnicama u gradu Beogradu" kako bi premostio nedostatke u sistemu bezbednosti (kao što je činjenica da previše ljudi imaju pristup, nedostatak evidencije ko je pristupio kom delu sistema, itd.). ne samo za sistem video nadzora beogradskog KOC MUP-a već i za slične sisteme MUP-a širom zemlje. Ipak, MUP nije objavio detalje istrage i disciplinskog postupka tako da nemamo uvid u mogući motiv prekršioca.

Poverenik je odmah reagovao na aktivnosti MUP-a, dajući pohvale za konstruktivnu i korisnu reakciju na njegovo upozorenje izjavivši da, iako u skladu sa sadašnjim kriterijuma

za bezbednost i zaštitu podataka preduzeti koraci nisu ništa specijalno i smatraju se standardom, oni su, u specifičnim okolnostima u Srbiji, dobrodošli budući da nesumnjivo predstavljaju dobru i korisnu stvar.

Iako nije bilo sličnih incidenata u Srbiji u neko vreme nakon toga, u toku 2014. godine je dalje eskalirao problem sa sistemima za video nadzor.

Između 8. juna i 10. juna 2014. godine, pojavila su se dva snimka na sajtu youtube. Na prvom se vidi saobraćajna nesreća u noći 7. na 8. jun 2014. godine u Novom Sadu. Snimak pokazuje trenutak kada Audi kojeg vozi D.V. (21) bočno udara Polo, usmrtivši dve devojke, M.L. i V.M., i mladića A.M. (svi 20 godina starosti).

Drugi snimak koji je privukao pažnju javnosti je iz Niša i pokazuje pešaka, M.Z. (17 godina), kojeg je na pešačkom prelazu pokosio Audi, i koji je usled toga pretrpio teške povrede.

Oba snimka su emitovana od strane više medijskih kuća, uz objavljivanje ličnih podatka uključenih lica.

Nadležni poverenik je odmah sproveo kontrolu i nadzor u odseku saobraćajne policije u Novom Sadu, Javnom komunalnom preduzeću „Informatika" u Novom Sadu, čiji je javni sistem video nadzora snimio automobilsku nesreću u Novom Sadu, i Odseku saobraćajne policije MUP-a u Nišu. Poverenik je naglasio da „smo suočeni sa stvarnom opasnošću da se preveliki broj sistema video nadzora pretvore u snimanje užasa i skandala", urgirajući na medije da „dovedu u pitanje etičke standarde svoje profesije". U skladu sa mišljenjem poverenika, objektivna informacija može biti saopštena javnosti bez nepotrebnog uplitanja u privatnost uključenih lica, i bez otežavanja u gubitku njihovih najvoljenijih. Ponovo je podsetio policiju i druge državne organe na odredbe Člana 42, stav 3 Ustava, koji izričito zabranjuje i sankcioniše upotrebu podataka o ličnosti izvan svrhe za koju su prikupljeni — u ovom slučaju da doprinesu bezbednosti na putu i pomognu u otkrivanju i dokazivanju krivičnih dela.

Porodice žrtava iz Novog Sada i porodice ozbiljno povređenog maloletnika iz Niša su navele da je objavljivanje snimaka nesreće u kojoj su njihova deca snimljena veoma važno za javnost, ističući da ljudi moraju da vide kako su se te nesreće dogodile, ali i da smanje mogućnost bilo kakvog skrivanja istine.

Iako u trenutku pisanja ovog teksta, rezultati kontrola i nadzora još uvek nisu poznati, naučene lekcije iz ovog slučaja ukazuju i na potrebu da Srbija sačini i usvoji zakon o video nadzoru koji mora biti u skladu sa novom verzijom Zakona o zaštiti ličnih podataka[35] i EU direktivama u toj oblasti.

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

Slučaj iz Srbije 2: Kada IT izvođač „pusti korenje”

Aktuelno Ministarstvo pravde Republike Srbije (novo MP) je nasledilo dužnosti bivšeg Ministarstva pravde i državne uprave (MPDU) prilikom spajanja prethodnog ministarstva pravde (prethodno MP) i dela za državnu upravu iz prethodnog Ministarstva za državnu upravu, lokalnu samupravu i ljudska prava (MDULSLJP).

Mandat prethodnog MP je trajao do jula 2012. godine. MPDU je formirano u julu 2012. godine, i postojalo je do aprila 2014. godine kada je formirano novo MP.

Za skoro 10 godina državne uprave u Srbiji, sudska funkcija u vladi se nalazila u prethodnom MP, nakon čega je usledilo manje od dve godine zajedničkog upravljanja između funkcija pravde i državne uprave. Ipak, kao rezultat zadnje reorganizacije vlade, sudska funkcija je sada vraćena kao jedinstvena funkcija novog MP.

Sektor pravde sa svim svojim međusobno povezanim ali nezavisnim telima je veoma kompleksno okruženje, gde svako telo u okviru sektora ima jasno razdvojene funkcije, procese i nadležnosti i gde je interakcija sa drugim sektorskim telima detaljno regulisana. MPDU, kao i novo MP, je čvrsto verovalo da, u cilju uspešnog rukovođenja i upravljanja sektorom pravde, ICT treba koristiti samo kao alat za smanjenje složenosti sektora. Strategija prethodnog MP je bilo sasvim suprotna i usmerena na kreiranje kompleksnih ICT sistema koji mapiraju kompleksnost sektora, zahtevaju znatne budžetske investicije i za troškove korišćenja i održavanja. Takve aktivnosti dovode do velike raznolikosti hardvera, softvera i povezanih ICT sistema korišćenih u okviru ICT ekosistema sektora pravde, što još uvek pravi velike probleme vezane za rizike sa ICT izvođačima i mogućnostima za korupciju u tom delu.

Trenutno, u skladu sa mišljenjem pomoćnika ministra pravde zaduženog za IT, postoje tri različita glavna informaciona sistema u sektoru pravde, koji koriste dve različite softverske aplikativne platfome: dve različite platforme za baze podataka i jednu platformu operativnog sistema, iako svi pripadaju istoj porodici IT aplikacija – upravljanje dokumentima. Ukoliko bi neko izbrojao mnoge manje sisteme, kao na primer one korišćene u Ustavnom sudu, broj bi bio još i veći. Oni su zahtevali trošenje više od 10 miliona evra donatorskih sredstava, a takođe su uticali i na budžet Srbije sa troškovima korišćenja i održavanja od 1,5 miliona evra godišnje! To bi moglo biti prihvatljivo ukoliko bi celi sektor sudstva bio pokriven jednim ili sa sva tri glavna informaciona sistema; ipak, trenutna obuhvaćenost sektora je ispod 25%. Da bi se obuhvatio ostatak tela u sektoru pravde (tj. 75%), potrebna je nova investicija koja bi iznosila između 20 i 30 miliona evra. Takvo finansiranje nije dostupno novom MP, jer bi godišnji budžet za korišćenje i održavanje vrtroglavo skočio na više od 3 miliona evra. Jasno je iz gore navedenih činjenica, kao i zbog činjenice da je svetska ekonomska kriza takođe uticala na resurse dostupne nakon budžetskih rezova, da je nalaženje takvih sredstava teško. Novo MP ima znatne probleme što se tiče rizika vezanih za ICT izvođače, jer tu lako dolazi do pojave krivičnih dela korupcije.

Postojali su problemi tokom postupka javne nabavke mrežnih i komunikacionih usluga (Internet i VPN WAN), što potpada pod IT korupciju, i može biti konkretno opisano kao „zloupotreba službenog položaja“ „nepotizam i protekcionizam”, i „kršenje postupka nabavke” od strane zaposlenih u prethodnom MP, i u korist tog istog IT izvođača kojeg je prethodno MP koristilo kao pružalac mrežne i komunikacione usluge širom zemlje. Zaposleni u prethodnom MP zadužen za računarske mreže je manipulisao procedurama definisanim u ugovoru između prethodnog MP i IT izvođačaa u smislu da kontrolne i zaštitne procedure ili nisu poštovane ili su u velikoj meri pojednostavljene u korist IT ugovarača kako bi se smanjili njegovi troškovi. On je takođe zloupotrebio položaj sakrivanjem podataka (bili su nedostupni) koji se tiču pristupa IT ugovarača VPN WAN sistemu, i uništavanjem elektronske dokumentacije sistema tako da MPDU i novo MP nije moglo da kontroliše, nadgleda i vrši nadzor sistema.

Isti zaposleni prethodnog MP je pokazao nepotizam i protekcionizam kada je kršio pravila za nabavke koristeći podatke i informacije o sistemu koji nisu bili dostupni višim zvaničnicima novog MP za kreiranje tenderske dokumentacije za nabavku mrežnih i komunikacionih usluga. Ipak, Ministar pravde i državne uprave nije dozvolio da ova tenderska dokumentacija bude objavljena jer se plašio negativnih efekata tendera koji je možda namešten u korist jednog pružaoca internet usluga (ISP), IT izvođača, koji je u vreme tendera već 8 godina pružao mrežne i komunikacione usluge širom zemlje (Internet i VPN WAN). Umesto toga, Ministar pravde i državne uprave je dao nalog da se pripremi nova i pravična tenderska dokumentacija u skladu sa relevantnim zakonima i prema najboljim praksama.

Novom MP i sprskim poreskim obveznicima je nanešena finansijska šteta, jer IT izvođač nije želeo da iz početka ponovo ugovara cene i kvalitet usluga, niti da dozvoli novom MP da započne novi tenderski postupak. IT izvođač je uspeo da zaustavi novi tenderski postupak korišćenjem složene i opsežne šeme žalbi što je omogućeno zbog rupa u Zakonu o javnim nabavkama koji je tada bio na snazi. Službenik prethodnog MP je, kada je suočen sa situacijom, napustio radno mesto tokom mandata MPDU. MPDU je započelo zvaničnu istragu i predmet je završio na sudu (predstavnici novog MP trenutno se bave ovim predmetom).

Zaključak koji treba izvući iz ovog slučaja je da državne uprave ne smeju potceniti rizike vezane za IT izvođače. One moraju pravilno propisati procedure prilikom davanja ugovora eksternim saradnicima. Kako će privatni sektor pružati sve više IT usluga u budućnosti, a imajući u vidu da se budžeti za zaposlene u državnim organima smanjuju, značaj IT izvođača će sve više rasti.

Slučaj iz Srbije 3: Viši državni zvaničnik špijunira zaposlene

Da bi otkrila ko je govorio o njenom lošem učinku, generalna direktorica Agencije za privatizaciju (Agencija) je svojevremeno smenila IT direktora Agencije zato što je odbio da kopira i-mejl poruke zaposlenih, i nakon toga naredila drugom zaposlenom da to uradi time stičući pristup znatnom broju i-mejl poruka zaposlenih. Ovaj slučaj „zloupotrebe položaja“ je doveo do njene prevremene penzije i time kraja njenog mandata kao Generalne direktorice Agencije.

Sada već penzionisana generalna direktorka Agencije je zatražila kopije poslovnih i-mejl poruka svih zaposlenih u Agenciji bez njihovog znanja, time kršeći njihovu privatnost. U Srbiji trenutno ne postoji propis koji reguliše vlasništvo i pristup elektronskim komunikacijama koje zaposleni naprave tokom radnog vremena, i zbog toga se svaka vrsta takve komunikacije (i-mejl, čet, telefon, društveni mediji, itd.) smatra ličnim vlasništvom zaposlenog. Zbog toga veliki broj kompanija koje posluju u Srbiji primenjuju sopstvene interne politike i procedure vezane za prava, dužnosti i obaveze zaposlenih u vezi sa elektronskim komunikacijama. Tako da, iako su to bile poslovne i-mejl poruke i ona je bila generalna direktorica Agencije, nije joj bilo dozvoljeno da ih pročita jer Agencija nije imala takve politike i procedure. Nije poznato ko sada ima pristup stotinama hiljada i-mejl poruka od 300 zaposlenih koje su preuzimane nakon radnog vremena i vikendima. Takođe nije poznato da li ih je podelila sa nekim i, ako jeste, sa kim.

Razlog za takav zahtev je kritički članak o njoj koji je objavljen u novembru prošle godine u nedeljnom magazinu pod naslovom „Pljačka Srbije – kako su svi uvezani” sa podnaslovom koji je bio posvećen njoj „Ko je vratio kraljicu privatizacije na mesto zločina?”. U tekstu se citira i jedan od i-mejlova u kojem zaposleni u Agenciji obaveštava nekoliko ustanova da je uprava zabranila radne sastanke, i da im je dozvoljena jedino komunikacija i-mejlom.

Vršilac dužnosti IT direktora Agencije u to vreme je naveo da je objavljeni članak bio ključni razlog interesovanja generalne direktorice „da dokaže curenje informacija iz Agencije”, dok je u stvari želela da otkrije ko je novinarima dao informacije o njenom lošem rukovođenju Agencijom. U skladu sa usmenim iskazima, IT direktor se konsultovao sa svojim advokatom u vezi sa legalnošću kopiranja i-mejl poruka bez saglasnosti zaposlenog. Advokat mu je rekao da takav nalog nije u skladu sa Zakonom o zaštiti podataka o ličnosti i Krivičnim zakonikom. U stvari, advokat ga je informisao da su kazne za nedozvoljenu obradu podataka i povredu tajnosti od 50.000 do 1.000.000 dinara, ali i zatvor do dve godine.

IT direktor je naveo da kada je upitao generalnu direktoricu zbog čega su joj potrebne kopije, ona mu je rekla da to nije njegova briga. Takođe je naveo da su i lica koja nisu zaposlena niti angažovana, i koja nisu imala formalno-pravni odnos sa Agencijom, bila prisutna na sastanku o ovom pitanju.

U odgovoru medijima, generalna direktorica Agencije je navela da nikada nije tražila da se kopiraju i-mejl poruke, i porekla je da je kopiran ijedan i-mejl zaposlenih. Kada je upitana da li je IT direktor otpušten zato što se protivio tom činu, ona je odgovorila da je otpušten zato što posao nije obavljao u skladu sa ugovorom, ali nije išla dalje u pojedinosti. Bivša generalna direktorica je naglasila da nije bila svesna članka koji je magazin objavio o njoj, i da se nekoliko dana pre toga penzionisala sa pozicije generalne direktorice Agencije.

Nije poznato koje mere su preduzete da se premosti nedostatak u sigurnosnom sistemu Agencije, jer je IT sistem Agencije zloupotrebljen kroz formalni lanac komandovanja. Najbolji zaključak koji je moguće izvući iz ovog slučaja je da bi nedostatak etike i obuke vezane za korupciju vezanu za IT kao i svest državnih službenika mogao biti veliki problem jer su oni od presudne važnosti kao dugoročne mere zaštite od korupcije povezane sa IT.

Slučaj iz Srbije 4: „Drumska mafija"

Suđenje „Drumskoj mafiji" u Srbiji koje je počelo u maju 2007. godine je obuhvatilo 53 lica, uglavnom zaposlena u državnom preduzeću „Putevi Srbije", koja su elektronski preusmeravala plaćanje putarina. Ovo se opisuje se kao najveća elektronska pljačka u istoriji srpskog pravosuđa[36].

U novembru 2009. godine, Posebno odelenje Okružnog suda u Beogradu je osudilo 41 lice na ukupnu zatvorsku kaznu od 131 godine i 10 meseci. Optuženi su proglašeni krivim za zadržavanje dela novca od naplaćenih putarina, i time opljačkali državno preduzeće za puteve u Srbiji „Puteve Srbije" za oko 6,5 miliona evra. Devet optuženih je oslobođeno, dok su trojica počinila samoubistvo tokom sudskog postupka[37]. Milanu Jovetiću, zaposlenom u unutrašnjoj kontroli Puteva Srbije, koji bio označen kao organizator grupe, izrečena je najduža zatvorska kazna u trajanju od šest godina. Drugooptuženom, Živoradu Đorđeviću, za kojeg se takođe veruje da je bio jedan od vođa grupe, je izrečena zatvorska kazna od tri godine i dva meseca[38].

36 http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/newsbriefs/2007/05/29/nb-06
37 http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-years Ishod presude Apelacionog suda su malo niže kazne.
38 Ibid.

U javnim raspravama u Srbiji je prilično uobičajeno da se sumnja da su optužena i osuđena lica tek nešto više od „žrtvenih jaraca“, budući da korupcija na visokom nivou ne može funkcionisati bez ili aktivnog učešća, ili „prećutne saglasnosti“ sa političkog nivoa. Ipak, prilično je retko za takav scenario da bude skoro u celosti potvrđen od strane pravosudnih organa:

“Sud smatra da Jovetić i Đorđević nisu pravi organizatori grupe i da će pravi organizatori, na žalost, ostati nepoznati. Mi imamo dokaze... da su neka druga lica kriva.... Nije utvrđeno ko je bio organizator u Beogradu i ko je uzimao 40% novca[39].

Jedno osuđeno lice zaposleno u preduzeću „Micros Electronics”, kako presuda glasi, „je kreiralo i razvilo mehanizme i tehnička sredstva koja su omogućila nelegalni rad i naplatu novca”, putem „korišćenja konektorskih kablova, postojećih elektronskih uređaja i posebnog, neregularnog softvera”. Jedna garnitura kablova je povezala gornji i donji štampač na mašini za distribuciju kartica. Druga garnitura kablova, sa sklopkom, povezivala je (ili rastavljala) rampu za ulaz automobila i računar na naplatnoj rampi. Ovaj mehanizam je instaliran na naplatnim rampama „Bubanj Potok” i „Nais” (dva kraja autoputa Beograd – Niš). On je takođe ubacio neregularnu kopiju softvera „EMU-87” u postojeći operativni sistem za naplatu putarine. Time je, bez izmene elektronskog sistema, omogućena registracija kartica o plaćenoj putarini. Šefovi smena su pokrenuli nelegalni program pre nego što su odabrani radnici na platnim ramapma započeli svoje smene.

Regularni softver, uključujući originalnu datoteku „EMU 87” služi kao matematički korpocesor za aritmetičke operacije. Budući da stari raučunari nisu imali takav kopocesor, EMU 87 datoteka je provobitno služila samo da ga „simulira“. Treba imati na umu da je ta datoteka deo originalnog sistema. Radnik na održavanju je samo prekopirao orginalnu datoteku sa neregularnom. Razlika između originalne i neregularne EMU 87 bi se mogla videti prilikom otvaranja datoteke u tekst editoru. Dok originalna datoteka ima „hieroglife“ da bi bila nečitljiva, neregularna datoteka sadrži jasno čitljiv oblik kartice na kojoj je navedeno da je putarina naplaćena. U sistemu je bilo moguće videti osobine datoteke, datum pristupanja, itd. Kao što je jedan od kontrolora objasnio, provera i kontrola nisu utvrdile prevaru, jer se u sistemu nisu ostavljali tragovi.

Kombinacija kablova, posebnih elektronskih uređaja i neregularnog softvera je omogućavala radnicima na naplati (članovima grupe) da istovremeno odštampaju dva primerka kartice o plaćenoj putarini na autoputu sa identičmim serijskim brojevima, dok je elektronski sistem registrovao samo jednu. Kada je putarina, na osnovu prve duple kartice bila plaćena, softver je omogućio štampanje kartice bez registracije u elektronskom sistemu za naplatu. Istovremeno, nakon pritiska na sklopku, bilo je moguće da kamioni nastave dalje put nakon plaćanja, budući da je sklopka prekidala vezu između sistema za elektronsku kontrolu plaćanja, računara i rampe. Isti radnik preduzeća Micros Electronics, koji je instalirao neregularnu datoteku, je takođe održavao neregularni sistem kada je bilo potrebe za tim

39 Sudija Vladimir Vučinić, u izjavi za dnevni list „Politika”, http://www.balkaninsight.com/en/article/serbia-s-road-mafia-get-131-years.

(zamenjivao je kablove, skrivao neregularni softver po potrebi, obučavao druge kako da koriste sistem, itd.).

Razlog zbog kojeg je sistem mogao funkcionisati tako dugo je bio nedostatak efektivne kontrole i veoma raširene kriminalne mreže. Članovi grupe nisu čak ni uklonili neregularne kablove nakon svojih smena, šefovi smena ih nisu na to upozoravali, i ilegalno stečen novac je obično ostajao u kućicama naplatnih rampi gde je i naplaćivan. Kontrola je vršena obično nakon 18:00 (kada članovi grupe nisu radili), postojale su šifre upozorenja o nameravanim kontrolama, itd.

Interesantna je činjenica koja je navedena u sudskoj presudi, ali ne i dalje razrađena, da se u periodu obuhvaćenom presudom (između 2004. i 2006. god.) ukupan iznos nenaplaćenih putarina efektivno povećao, što je suprotno od očekivanog kao posledice pljačke. Ovo je ipak jasna naznaka da je sistem pronevere funkcionisao tokom mnogo dužeg vremenskog perioda, i da je istraga pokrila samo neke od aspekata i počinilaca pljačke.

Slučaj „drumske mafije“ je bio prvi slučaj sa kojim se javnost upoznala sa jednim od najpoznatijih zviždača[40] (insajdera) u Srbiji, licem koje je bilo privremeno zaposleno u preduzeću „Putevi Srbije“. Kada je ova osoba počela da razgovara o problemima sa drugim kolegama, reakcija je bila da se dozvoli isticanje njegovog ugovora početkom 2006. godine, koji nije obnavljan sa obrazloženjem „nedostatka potrebe za takvom uslugom“.

„Onda sam rešio da dokažem i sve sumnje koje sam imao u vezi sa krađom na naplatnim rampama, a o čemu niko nije smeo da priča zbog straha od otkaza. Tajno sam kamerom snimio prolazak vozila na niškoj i beogradskoj rampi, usput snimajući i kartice koje su dobijali vozači. Međutim, da bih kompletirao dokaz bio mi je potreban listing kartica na naplatnim rampama, jer bi se tako pokazalo da su izdavane duple kartice“, izjavio je.

Zviždač je snimio karticu koju je vozač kamiona dobio, uključujući komunikaciju sa vozačem. Zatim mu je bio potreban zvanični listing. Ipak, „Putevi Srbije“ su odbili zahtev za slobodnim pristupom informacijama. Poverenik za informacije je više puta govorio u javnosti o tom slučaju. Kada je insajder zatražio njegovu pomoć da bi dobio listing distribucije kartica putarine, poverenik je zatražio od „Puteva Srbije“ da objasne razloge za uskraćivanje traženih informacija. Poverenik nije prihvatio njihov argument da je to privredna tajna, i dostavio je nalog za javno objavljivanje listinga.

„Moja odluka je bila zakonski obavezujuća za preduzeće „Putevi Srbije“ ali oni nisu postupili u skladu sa njom. Vlada Srbije, koja mora sprovesti odluku poverenika ukoliko je to potrebno, nije to uradila.”

Osoba koja je skrenula pažnju javnosti na ovaj problem je takođe svedočila na suđenju koje je usledilo. Interesantno je da je njegova traka, jedan od potencijalnih dokaza kriminalnog udržívanja, nestala iz sudskih spisa pre glavnog pretresa.

40 Srbija još uvek nema zakon koji omogućava efektivnu zaštitu zviždača.

2. Mere zaštite od zloupotrebe IT u svrhe korupcije

Uvod

Pripremila Louise Thomasen

Primeri iz poglavlja 1 odnose se na razne zloubotrebe informaciono-komunikacione tehnologije (ICT) i krivična dela. Da bi iz ovih događaja utvrdili koje su zaštitne mere nedostajale i šta su zemlje iz tih primera naučile, autori iz pojedinačnih država će u ovom poglavlju za svoju zemlju opisati konkretne i opšte mere zaštite od zloubotrebe IT u svrhe korupcije.

U konkretne mere zaštite od zloupotrebe informacione tehnologije (IT) u svrhe korupcije spadaju:

- tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe ICT sistema
- organizacione i proceduralne mere zaštite kao što je „načelo više očiju"
- praćenje protoka podataka i pristupa zaposlenih sistemima podataka
- mere usavršavanja i podizanja svesti za državne službenike o rizicima od zloupotrebe ICT u svrhe korupcije i zaštitnim merama
- revizija sistema ICT (interne ili eksterne revizije; inicira ih državni organ ili se pokreću nakon nekog izveštaja ili prigovora građana ili medija)
- zakonodavne mere zaštite, kao što je sveobuhvatno upravno, građansko i krivično zakonodavstvo čiji je cilj da spreči i kazni zloupotrebu ICT u svrhe korupcije.

Pošto navedeni slučajevi opisuju zloupotrebu ICT u svrhe korupcije koja se već desila, nismo tražili primere sa nekim konkretnim ishodima koji su vodili do dodatnih ili planiranih zaštitnih mera. Primeri iz poglavlja 1 su stvarni slučajevi korupcije i kao takvi će dopuniti i obogatiti znanja koja možemo da steknemo o merama zaštite koje treba da postoje u borbi protiv korupcije koja zloupotrebljava ICT.

Pojedini primeri možda nisu proizveli nikakve posledice, npr. doveli do suđenja, a u nekim slučajevima je nejasno šta je ko uradio, gde i kako. Ono što je bitno je da iz tih primera možemo da naučimo - koje zaštitne mere su trebale da postoje, gde su sistemi IT osetljivi na zloupotrebu, kao i koliko su zemlje zapadnog Balkana koje su u mreži ReSPA odmakle u realizaciji i sprovođenju mera zaštite od zloupotrebe ICT i korupcije u javnom sektoru.

Albanija

Pripremili Edlira Nasi i Ened Kercini

U informatičkom dobu, dok postajemo sve više zavisni od složenih informacionih sistema, začuđuje koliko malo pažnje se posvećuje onima koji su zaduženi za funkcionisanje i administraciju tih sistema. U pitanju su osobe na pozicijama od značaja i poverenja bez presedana. Zlonamerne radnje od strane tih insajdera mogu imati teške posledice.

Ovi primeri ukazuju na nekoliko stvari vezanih za pretnju informacionim sistemima koja dolazi iznutra. Ipak, postaće jasno da su problemi iznutra već prisutni, uključujući policiju, vojsku, privatna preduzeća i sektor energetike. Takođe, pokazaćemo da postoji snažna tendencija da rukovodstva reše ove probleme brzo i tiho, te da izbegnu negativne lične i organizacione posledice i publicitet.

Nismo bili u mogućnosti da dokažemo koliko su ovi problemi zaista raširени. Ono o čemu ovde izveštavamo čini se da je samo vrh ledenog brega.

Osim toga, uprkos dokazanim internim problemima i posebnoj osetljivosti javne infrastrukture, paradoksalno je malo toga učinjeno na povećanju interne zaštite, dok su velike investicije kontinuirano namenjene otkrivanju i sprečavanju prodora spolja. Iako je zaštita od pretnji spolja zaista bitna, problemi sa ljudima ne mogu se rešiti tehničkim rešenjima.

Informacioni sistemi javne infrastrukture još dugo će biti osetljivi na zloupotrebe od strane onih koji jednostavno poznaju sistem: insajdera.

Ključni problemi koje smo evidentirali u našim slučajevima su nerazumevanje slabosti zaposlenih koji su izloženi riziku i nepostojanje standardizovanih pravila koja uređuju korišćenje informacionih sistema, pri čemu oba problema imaju eksplicitne posledice zloupotrebe.

Mere zaštite u slučajevima iz Albanije

Slučaj iz Albanije 1: Korupcija u TIMS sistemu granične kontrole

Ovaj slučaj predstavlja tipičnu zloupotrebu službenog položaja i podmićivanje službenika granične policije u vidu namernog unošenja lažnih podataka u informacioni sistem TIMS (Total Information Management System), s namerom da se izbegne plaćanje dažbina državi za korišćenje uvezenog vozila.

Glavni problem u ovom primeru predstavlja činjenica da je prisutna velika razlika u tome kako sistem u stvarnosti funkcioniše kod praćenja ljudi kada prelaze granicu i kako je osmišljen da prati registarske brojeve vozila.

Napredak koji je poslednjih godina postignut na planu identifikacionih dokumenata i namenskih uređaja za čitanje ugrađenih na svim graničnim prelazima u velikoj meri je unapredio postupak registrovanja ljudi, uz bolji kvalitet automatskog učitavanja podataka. Ceo postupak je zahvaljujući očitavanju informacija sa biometrijskih identifikacionih dokumenata smeštenih u elektronskom obliku u zaštitnom čipu sa aktivnim RFID postao lakši za korišćenje i transparentniji.

Isto se, međutim, ne može reći za praćenje registarskih brojeva vozila. U pitanju je još uvek manuelan postupak koji podrazumeva da ljudi čitaju odgovarajuću dokumentaciju, potvrđuju autentičnost informacija kao i da vrše poređenje sa jedinstvenim brojevima koji se nalaze na zavučenim, dobro poznatim mestima u vozilu.

Insajder je uspešno iskoristio upravo ovu slabost sistema, na način što je bio u mogućnosti da na osnovu lažnih informacija unetih u sistem TIMS izradi „originalni" dokument. Ovde moramo naglasiti da su same informacije bile tačne. Falsifikovano je bilo samo vreme prijema. Mnogo krupnije pitanje (koje izlazi iz okvira ove studije) predstavlja činjenica da je vozilo krajem 2009. godine prošlo carinu bez odgovarajuće evidencije.

U ovom slučaju nisu korišćeni specijalni ili sofisticirani IT instrumenti, jer je u pitanju jednostavno bila namerna zloupotreba informacionog sistema. Do zloupotrebe je prvi put došlo kada auto nije evidentiran u sistem TIMS kod prvog ulaska u zemlju, a zatim je ponovljena kada je, 4 godine kasnije, vlasnik konačno želeo da registruje taj auto.

Informacioni sistem TIMS ima veoma dobra ovlašćenja i administraciju na nivou korisnika. Propise i postupke su na odgovorajući način sprovodili pripadnici granične policije koji su unosili informacije i pojedinačno se potpisivali u tradicionalnim, štampanim knjigama evidencije. TIMS takođe poseduje dokazanu, ugrađenu mogućnost unošenja i praćenja ko šta radi, pa je na taj način bilo lako zapaziti „insajdera", kada su prikupljanjem drugih dokaza dobijene i potvrđene naznake. Kao takav, sistem TIMS je pokazao svoju sposobnost da podrži postupak revizije.

Nismo mogli da potvrdimo da je ovaj slučaj pokrenuo unapređenje sistema. Međutim, to ne isključuje brojna unapređenja sistemskog softvera, popravke softvera i druge proceduralne promene koje se povremeno sprovode. Razmotreno je praćenje i snimanje putem video nazora (CCTV), koji je zatim uspešno primenjen kao dobar način da se kršenje pravila svede na minimum i pomogne nadležnim organima da u slučaju sprovođenja istrage prepoznaju prestup.

Slučaj iz Albanije 2: Korupcija u elektronskom sistemu javnih nabavki

Ovaj slučaj se odnosi na krađu korisničkog identiteta radi pribavljanja ovlašćenja u sistemu javnih nabavki sa jasnom namerom izmene konačne odluke u postupku nabavke.

Albanija već godinama ima elektronski sistem javnih nabavki, koji se smatra uspešnim projektom. Sistem je pozitivno uticao na ukupne troškove koje je država imala za nabavku robe i usluga.

Ukratko, sistem omogućava objavljivanje tenderske dokumentacije. Ponuđači zatim mogu da unesu svoju dokumentaciju u sistem i podnesu finansijsku ponudu. Ovaj proces je šifrovan i ostaje takav do isteka roka za dostavljanje ponuda, a može se dešifrovati ako najmanje tri ili više prethodno ovlašćenih službenika unesu svoja „korisnička imena" i „lozinke" u definisanom vremenskom okviru. U određenom smislu, ovim se obezbeđuje dobar stepen transparentnosti dostavljanja ponuda. Sistem nabavke takođe može da razvrsta i automatski prikupi i šalje obaveštenja ponuđačima u potpunoj saglasnosti za zakonom o nabavkama, podzakonskim aktima i uredbama. Važno je napomenuti da postaje dobra praksa da Vrhovna državna revizorska institucija, pre nego što sprovede reviziju nekog javnog subjekta, dobije kompletan detaljan izveštaj iz sistema javnih nabavki o tom subjektu i periodu koji je predmet revizije.

Ovaj slučaj je pokrenut zahvaljući tome što je Vrhovna državna revizorska institucija bila u mogućnosti da utvrdi nepodudarnost između informacija koje je sakupio elektronski sistem javnih nabavki i tenderske dokumentacije u štampanom obliku koju je potpisala imenovana tenderska komisija.

Kako je to moglo da se desi? Na samom početku tenderskog postupka komisija za ponude unosi namensku oblast elektronskog sistema nabavki. Slično nekoj samouslužnoj aplikaciji, nakon početnog konfigurisanja, svaki član može da unese svoje „korisničko ime" i da izabere „lozinku".

Ovaj sistem nudi funkciju čuvanja podataka (failback) u slučaju potrebe da se resetuje sistem i može da je aktivira imenovani predsednik komisije za ponude. Ona šalje i-mejl sa linkom za resetovanje nazad izvornim korisnicima, pošto svaki korisnik mora imati registrovani i-mejl da bi pristupio sistemu. Sve to se čini prihvatljivim, ali u suštini smanjuje bezbednost na nivo korisnikove lozinke za i-mejl, pošto se generalno svi korisnici registruju putem zvanične i-mejl adrese koja se ponekad daje drugima ili čija lozinka je poznata ljudima. To znači da u stvarnosti oni svi znaju „lozinke" jedni drugih. Iako je ova praksa uvedena sa dobrim namerama rešavanja pitanja tokom rada, njome se u celini smanjuje bezbednost sistema.

Prepoznali smo još jedan interesantan problem. Čak i kada se usvoje procedure i propisi i kada se sprovode kroz funkcije informacionih sistema kao što je prihvatanje samo složenih lozinki, sa povremenim zahtevom za promenom lozinke, tada se javlja jedan drugi ljudski

faktor - veća „jednostavnost korišćenja”. Videli smo podatke koji to potvrđuju. Većini korisnika vremenom sve dosadi, naročito povremena promena složenih lozinki, pa koriste prečicu i ostavljaju lozinke nepromenjene uz zadatu verziju koju im je administrator sistema dao na početku za prvo prijavljivanje. Posle tri meseca njihovi nalozi su blokirani ali je mnogo lakše tražiti resetovanje lozinke na istu inicijalnu zadatu verziju koju administrator sistema uvek daje. Na kraju će skoro sve lozinke za i-mejl biti slične.

Bilo je zaista nemoguće dokazati šta se dešava, a datoteka evidencije nije bila dostupna da se ovaj problem dalje ispita. U očima Vrhovne državne revizorske institucije, jedina izvesna stvar bila je da je član tenderske komisije mogao da dokaže da nije ni bio u Albaniji.

Na kraju, dobro projektovanje sistema i procedure doživeće neuspeh, lanac je onoliko jak koliko je jaka njegova najslabija karika, a u ovom slučaju snažno verujemo da je zaista bilo previše lako oponašati identitet korisnika tako što se znalo za ovu slabost u vezi lozinke za i-mejl i iskoristila opcija za resetovanje šifre sistema za nabavke.

Verujemo da ne postoji način da se uspostavi odgovarajuća bezbednost i zaštita koristeći samo lozinke. Novi sistem mora biti ažuriran mogućnošću provere identiteta sa dva faktora, koji barem ne bi ostavio prostor za apstraktne i besmislene argumente za izvrdavanje kada je u pitanju identitet korisnika.

Slučaj iz Albanije 3: Zloupotreba IT u svrhe korupcije kod distributera električne energije

Ovaj slučaj predstavlja „insajdersku” manipulaciju informacionog sistema visokog profila. Sistem je bio programiran da daje sistematične promene vrednosti u nivoima potrošnje u okviru sistema izdavanja računa. To je manipulatoru omogućilo da poveća vrednosti računa za struju s namerom sticanja finansijske koristi za preduzeće.

Ovaj slučaj je takođe podrazumevao velike teškoće u sakupljanju informacija, zbog stručnog znanja upotrebljenog da se situacijom interno upravlja iz privatnog preduzeća, velike novčane vrednosti u pitanju i velike pažnje nezadovoljne javnosti.

U ovom slučaju nemamo uobičajene podatke koji bi dali dovoljno informacija da se shvati šta se zaista desilo sa informacionim sistemom. Međutim, bili smo u mogućnosti da na osnovu nespornih činjenica prikupljenih u to vreme donesemo dovoljno pretpostavki.

U mernim podacima LDA postoji petlja. Ti se podaci na osnovu određenih pokazatelja mogu filterisati i ne šalju se direktno sistemu za izdavanje računa, pošto može da prikaže problematične klijente, novčane kazne i druge neobične probleme izdavanja računa koje zaposleni treba dodatno da provere. Ima smisla da su ovi podaci filterisani zbog razmatranja ranijih problema sa plaćanjem ili u slučajevima kada su lica zadužena za

očitavanje strujomera posumljala da potrošači podešavaju svoju potrošnju električne energije. Činjenica da je postupak merenja obavljen, prema knjigama evidencije, kasno tokom dana i posle radnog vremena zaposlenih zaduženih za očitavanje strujomera, mogla bi da bude ključni pokazatelj da je prekomereno zaračunavanje potrošnje bilo namerno i štetno.

Vremenska oznaka transakcije je veoma sumnjiva i tokom istrage bila je jedno od glavnih upozorenja da nešto nije u redu. Operatori LDA na terenu su samo prekršili protokol u pogledu vremena uzimanja podataka, ali vremenske oznake ukazuju na učestalosti korišćenja koje nisu moguće za ljude. Dakle, reč je ili o manipulisanju podacima ili fiktivnom uzimanju podataka. Analiza podataka je ukazala na ovo drugo.

Ceo slučaj bi se mogao takođe smatrati sofisticiranim pokušajem prevare skoro 15.000 potrošača. Opet se može prepoznati isti obrazac, namerna zloupotreba informacionog sistema, ovog puta zbog povećanja profita preduzeća. Razlika je što ova intervencija ne može biti delo jedne osobe, a postoji i obaveza za odobrenjima da se takvo nešto uradi, a kako se profit sliva direktno u finansije preduzeća, ne ostaje ništa što bi podržalo opravdanja kao što su greška nastala u sistemu izdavanja računa ili greška napravljena od strane zaposlenih.

Slučaj iz Albanije 4: Pronevera i falsifikovanje u knjigovodstvu

Iako se čini poprilično bezazlenim, ovaj slučaj predstavlja sasvim jasnu zloupotrebu sistema od strane zaposlene osobe odgovorne za knjigovodstvo, koja je godinama vršila proneveru sredstava za čije knjiženje je bila zadužena.

Ključ za bolje razumevanje zašto je slučaj interesantan je činjenica da se u suštini ne odnosi na informacionu tehnologiju već na to što je blagajnica iskoristila nedostatak nadzora ili pažnje njenih nadređenih.

Kako se sve odvijalo? Kao prvo, finansijski sistem koji prihvata platne spiskove, i po njima isplaćuje plate kroz bankarski sistem, čini se nije bio u mogućnosti da istovremeno obradi pojedinačne detalje platnog spiska za celu državnu upravu i druge državne institucije, kao što je vojska o kojoj je ovde reč. Drugo, postojalo je ozbiljno pitanje poverenja koje se odnosilo na interno više rukovodstvo kao i nepostojanje provere različitih potpisanih dokumenata za platni spisak između finasijskih organa.

Može biti da je prva naznaka o ovim potencijalnim spornim pitanjima otkrivena slučajno, kao rezultat obične greške, nešto što bi moglo da skrene pažnju službenice koja radi sa finansijama na slabost sistema. Posle toga, službenica je namerno unela još jednu grešku u platni spisak da dokaže da finansijski sistem ne može na pravi način da otkrije grešku, te je time dobila potvrdu da se glavna finansijska provera obavlja na ukupnim troškovima

za isplatu plata, koji ne smeju premašiti određeni, unapred planirani budžetski limit koji se utvrđuje na početku fiskalne godine.

Jedina stvar koja je preostala da se reši da bi takva šema funkcionisala bila je potreba da se savršeno prilagodi nekoliko dokumenata u štampanoj formi povezanih sa platnim spiskovima. Ti platni spiskovi treba samo da ostanu sa istom ukupnom sumom na kraju meseca. Na taj način se tabelama moglo lako manipulisati sve dok pojedinačni detalji ostaju unutar onoga što je sistem trezora predviđao kao ukupni iznos, da se ne probudi nikakva sumnja. Istovremeno, javiće se manje negativne razlike kod većine pojedinaca na platnim spiskovima koje se mogu zbrojiti na jedan jedinstveni račun sa konačnim iznosom. To je bilo moguće pošto banke obično nisu zainteresovane koliki je pojedinačni iznos plate nekog lica. Ono što je bitno je da iznos koji je platio trezor predstavlja zbir svih plata. Sa različitim elementima i rasponima koji postoje u platnom spisku vojske, kao što su naknade i drugi dodaci, zaposlenima u trezoru i banci je još teže da uoči nešto sumljivo što bi predstavljalo odstupanje od uobičajenih iznosa za isplatu plata.

Upravo je to razlog zašto je pronevera bila moguća duži vremenski period. Sve dok ukupna suma nije premašivala iznos koji su odobravali načelnik generalštaba i komandant regimente šema je mogla da se odvija nesmetano.

Ovakva vrsta zloupotrebe sistema može se opisati kao napad „čovekom u sredini". U ovom slučaju, napad izvodi osoba unutar sistema koja je uživala poverenje svojih nadležnih, koji su potvrđivali platni spisak bez dodatne provere, i iskoristila interesantnu činjenicu da se između trezora i banke razmenjivala samo ukupna suma svih platnih spiskova.

Ova „rupa" je sada zatvorena, pošto je softver trezora modernizovan, a razmena sa bankama sada obuhvata više podataka iz sistema trezora.

Mere zaštite od zloupotrebe IT u Albaniji

Zakonske mere zaštite

Kada je reč o zakonodavnim merama zaštite, Albanija je nedavno izmenila svoj zakonski okvir i Krivični zakonik kako bi odražavali pojavu računarskog kriminala ili kriminala povezanog sa IT. Najznačajnije mere, koje se odnose i na zloupotrebu baza podataka ili IT resursa, spadaju Zakon br. 10023 od 27.11.2008. o izmenama i dopunama Zakona br. 7895, od 27.1.1995. godine. „Zakonikom Republike Albanije", uključujući njegove izmene i dopune, dodata su nova krivična dela u Krivični zakonik, uključujući računarsku prevaru[41],

41 Član -143/b - Računarska prevara - „Ko unese, izmeni, izbriše ili propusti unošenje računarskih podataka ili izvrši bilo kakvo ometanje rada računarskog sistema u nameri da sebi ili drugom, putem prevare, pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se zatvorom od šest meseci do šest godina. Ovo krivično delo, kada se učini sa saučesnicima, ili više od jedanput, ili kada uzrokuje velike materijalne posledice,

računarsko falsifikovanje[42], neovlašćeni pristup računaru[43], neovlašćeno povezivanje računarskih podataka[44], ometanje računarskih podataka[45], ometanje računarskih sistema[46], kao i zloupotreba opreme[47].

Dalje, nedavno je usvojen zakonski propis kojim se uređuju elektronske baze podataka, što predstavlja odgovor na potrebu za zakonskom osnovom za formiranjem elektronskih baza podataka u cilju unapređenja javnih usluga. Ova pravna akta utiču i na korišćenje i upravljanje informacijama iz baza podataka i postupke koje zaposleni treba da slede da bi ostvarili standarde propisane zakonom u pogledu bezbednosti podataka. Zakon br. 10325 od 23.09.2010. godine „O državnim bazama podataka" propisuje načine registrovanja i upravljanja državnim bazama podataka, kao i osnivanje nadležnog koordinacionog organa za regulisanje baza podataka i njihovo korišćenje.

Ministar inovacija i informaciono komunikacione tehnologije (koji je sada Državni ministar za inovacije i državnu upravu) predložio je Savetu ministara konkretne mere čiji je cilj bezbednost baza podataka. Konkretno, Odlukom Saveta ministara br. 961 od 4.11.2012. osniva se nadležni koordinacioni organ Nacionalna agencija za informaciono društvo, dok se Odlukom Saveta ministara br. 945 od 02.11.2012. usvaja uredba o adminstiranju baza podataka. Važan aspekt ove uredbe o administriranju baza podataka je specifikacija nivoa bezbednosti, na visoki, srednji i niski[48], pri čemu se nivo bezbednosti utvrđuje na osnovu parametara integriteta, poverljivosti i dostupnosti podataka[49]. Zatim se, na osnovu

kazniće se zatvorom od pet do petnaest godina."

42 Član 186/a - Računarsko falsifikovanje - „Ko nezakonito unese, izmeni, izbriše ili propusti unošenje računarskih podataka s namerom da kreira lažne podatke u cilju njihovog unošenja i korišćenja kao autentičnih, bez obzira da li su kreirani podaci jasno čitljivi ili razumljivi, kazniće se zatvorom od šest meseci do šest godina. Ovo krivično delo će se kazniti zatvorom od tri do deset godina kada ga učini lice zaduženo da čuva i administrira računarske podatke, i kada ga učini sa saučesnicima, više od jednom, ili kada to delo dovede do teških posledica po javni interes."

43 Član 192/b - Neovlašćeni pristup računaru - „Ko neovlašćeno pristupi ili prekorači ovlašćenja da bi pristupio računarskom sistemu kao celini ili nekom njegovom delu, kršeći mere zaštite, kazniće se novčanom kaznom ili zatvorom do tri godine. Kada se ovo krivično delo učini u računarskim sistemima vojske, nacionalne bezbednosti, javnog reda, civilne zaštite, zdravstvene zaštite ili u nekom drugom računarskom sistemu od javnog značaja, kazniće se zatvorom od tri do deset godina."

44 Član 293/a - Neovlašćeno povezivanje računarskih podataka - „Nezakonito povezivanje tehničkom opremom sa prenosima računarskih podataka, koji nisu javni, iz ili unutar računarskog sistema, uključujući elektromagnetske emisije iz jednog računarskog sistema koji sadrži takve računarske podatke, kazniće se zatvorom od tri do sedam godina. Kada se ovo krivično delo učini iz ili unutar računarskih sistema vojske, nacionalne bezbednosti, javnog reda, civilne zaštite, zdravstvene zaštite ili nekog drugog računarskog sistema od javnog značaja, kazniće se zatvorom od sedam do petnaest godina."

45 Član 293/b - Ometanje računarskih podataka - „Ko neovlašćeno ošteti, uništi, izmeni, izbriše, ili prikrije računarski podatak kazniće se zatvorom od tri meseca do jedne godine. Kada se ovo krivično delo učini sa računarskim podacima vojske, nacionalne bezbednosti, javnog reda, civilne zaštite, zdravstvene zaštite ili nekim drugim računarskim podacima od javnog značaja, kazniće se zatvorom od tri do deset godina."

46 Član 293/c - Ometanje računarskih sistema - „Ko unese, ošteti, uništi, izmeni, izbriše ili prikrije računarski podatak ili računarski sistem u nameri da napravi teške i neovlašćene prepreke u cilju ometanja rada računarskog sistema, kazniće se zatvorom od tri do sedam godina. Kada se ovo krivično delo učini u računarskim sistemima vojske, nacionalne bezbednosti, javnog reda, civilne zaštite, zdravstvene zaštite ili u nekom drugom računarskom sistemu od javnog značaja, kazniće se zatvorom od pet do petnaest godina."

47 Član 293/c - Zloupotreba opreme - „Proizvodnja, čuvanje, davanje radi korišćenja, distribuiranje ili bilo koja druga radnja da se na raspolaganje stavi oprema, uključujući računarski softver, računarsku lozinku, šifru za pristup ili drugi sličan podatak koji je kreiran ili prilagođen za pristup računarskom sistemu ili nekom njegovom delu, sa ciljem učinjenja krivičnih dela propisanih članovima 192/b, 293/a, 293/b i 293/c ovog Zakonika, kazniće se zatvorom od šest meseci do pet godina."

48 Član 17, Odluka Saveta ministara br. 945 od 2.11.2012. (Aneks 1)

49 Ibid, Član 18.

kategorizacije baza podataka, preduzimaju mere tehničke bezbednosti. Mere bezbednosti koje se preduzimaju nadgleda Nacionalna agencija za računarsku bezbednost. Međutim, agencija za računarsku bezbednost je relativno nova institucija sa ograničenim kadrovskim resursima i trenutno je u postupku povećanja svojih kapaciteta da bi ispunila zahteve koji su joj propisani zakonom.

Ostali relevantni zakonski propisi koji se odnose na pitanja IT obuhvataju sledeće zakone i dokumenta koja obezbeđuju odgovarajuću realizaciju i korišćenje IT sistema:

- Zakon br. 9880, od 25.02.2008. „O elektronskom potpisu"
- Zakon br. 9887, od 10.03.2008. izmenjen i dopunjen Zakonom br. 48/2012
- „O zaštiti ličnih podataka"
- Višesektorska strategija za informaciono društvo 2008-2013
- Zakon br. 72/2012, „O organizaciji i radu državne infrastrukture za geoprostorne informacije u Republici Albaniji"
- Zakon br 9918, od 19.05.2008. (sa izmenama i dopunama) „O elektronskoj komunikaciji u Republici Albaniji""
- Zakon br. 119/2014 „O pravu na informisanje" (izglasan krajem septembra 2014. i kojim je zamenjen Zakon br. 8503, od 30.06.1999. „O pravu na informisanje o službenim dokumentima")

Tehničke mere zaštite od korupcije

Uz manju pažnju posvećenu ljudima, strategije bezbednosti informacionih sistema su najvećim delom tehničke prirode. Dve glavne vladine agencije u Albaniji, NAID (Nacionalna agencija za informaciono društvo) i NARB (Nacionalna agencija za računarsku bezbednost), potpomognute sa AŠDU (Albanska škola za državnu upravu), uključene su u obuku tehničkih kadrova da bolje štite državne sisteme od mogućih zloupotreba u svrhe korupcije. Uloga Nacionalne agencije za računarsku bezbednost je posebno važna, ako uzmemo u obzir da se radi o instituciji koja treba da ponudi stručno znanje za reviziju bezbednosti i drugih mera kod baza podataka. Specifičnosti revizije baza podataka daju interesantnu pozadinu za bolje razumevanje kako se u IT uvode zaštitne mere. Prema Uredbi o administriranju državnih baza podataka, revizija sistema se vrši redovno, odnosno svake dve godine za baze podataka sa visokim nivoom bezbednosti, svake tri godine za one sa srednjim nivoom bezbednosti, te svake četiri godine za baze podataka sa niskim nivoom bezbednosti. Primenjenim postupkom se obezbeđuje da su tehničke mere zaštite primenjene, jer Uredba propisuje da revizija treba da obuhvati potvrdu usklađenosti sa popisom imovine sistema, proveru da li su mere bezbednosti odgovarajuće, kao i proveru da li se tehničke mere i mere bezbednosti adekvatno primenjuju[50]. Na osnovu izveštaja i zapisnika revizije, institucije su obavezne da preduzmu korake u cilju ispravljanja svih evidentiranih neusklađenosti.

50 Član 24 (3), Odluka Saveta ministara br. 945 od 02.11.2012.

Organizacione i proceduralne mere zaštite

Postupak uređen zakonom sada se primenjuje (Naredba br. 2 od 9. februara 2013. Ministra za ICT „za standardizaciju izrade projektnog zadatka u oblasti ICT u državnoj upravi"), na osnovu kojeg svaka državna institucija koja unapredi ili izgradi informacioni sistem mora da ima revidirani projekat i odobrenje za projektni zadatak od stručnih lica iz Nacionalne agencije za informaciono društvo. Reč je o albanskoj strategiji korišćenja najboljeg lokalnog stručnog znanja i iskustva, od početnog osmišljavanja javnog IT projekta do finalizovane tenderske dokumentacije.

Nova albanska Vlada, koja je usvojila plan borbe protiv korupcije, nedavno je uz podršku Nacionalne agencije za informaciono društvo uvela novi postupak za tehnički prijem informacionih sistema. Očekuje se drugačiji pristup kod tehničkog prijema informacionih sistema, na način što će se učešće u radnoj grupi, imenovanoj za tehnički prijem informacionog sistema, otvoriti za eksterne stručnjake. Nadanja su da će takav pristup u velikoj meri smanjiti probleme koji su se javljali kod projekata za informacione sisteme tokom perioda tehničkog prijema (previše tolerisanja i brojni nedovršeni radovi), a koji su uglavnom odnosili na tehničke i upravljačke kadrove.

Bilo bi netačno tvrditi da je bezbednost nešto što se može lako kupiti. Ljudski faktor može da pokaže i da su najpouzdanija očekivanja netačna.

Obuka i podizanje svesti

Albanija ima još jednu inicijativu koja je u toku i koja je potekla od Nacionalne agencije za računarsku bezbednost, u saradnji sa Albanskom školom za državnu upravu, a odnosi se na organizovanje obuka za skoro sve IT kadrove u javnim institucijama i drugim državnim subjektima. Obuke se organizuju na različite teme, kao što su bezbednost sistema, zaštita i eksterna i interna ocena rizika. To bi mogao da bude prvi znak pozitivnog razvoja u okviru kojeg se fokus pomera sa opreme na ljude koji je administriraju i koriste.

Zaključak

U zaključku, sigurni smo da je neophodno istražiti druge načine upravljanja bezbednošću informacionih sistema i sprečavanja korupcije unutar sistema, jer oni često zanemare društvene faktore rizika koji dolaze od „insajderske pretnje" i teškoća da se informacioni procesi prilagode neformalnim strukturama javnih institucija.

Bosna i Hercegovina

Pripremili Aleksandra Martinović i Srđan Nogo

Uvod u primere mera zaštite od zloupotrebe IT u svrhe korupcije

Kada IT instrumenti nanose štetu reputaciji pojedinaca ili institucija, onda upotreba tih instrumenata i tehnologija postaje neka vrsta krivičnog dela. Računarski kriminal u BiH je u mnogim slučajevima teško dokazati, a pravne posledice i kazne za ta dela su slabe. Da bi sprečila takve kriminalne aktivnosti, Bosna i Hercegovina je već preduzela korake u borbi protiv računarskog kriminala i to kroz realizaciju sledećih projekata:

- centralizovani sistem zaštite identiteta građana (IDDEEA),
- PKI infrastruktura (Zakon BiH o elektronskom potpisu),
- projekti centralizovanog krovnog sistema elektronske uprave za razmenu informacija između svih nivoa vlasti u BiH,
- projekti Kancelarije koordinatora za reformu državne uprave (PARCO) čiji je cilj unapređenje državne uprave.

Pored ovih, postoje i mnoge druge aktivnosti i projekti, koji se realizuju preko Europe Aid i drugih bilateralnih fondova, a koji predstavljaju značajnu pomoć u borbi protiv korupcije.

Bosna i Hercegovina je 2002. godine u Beogradu potpisala „e-SEE agendu za informaciono društvo", te postala član inicijative Elektronska jugoistočna Evropa. Tom je agendom dogovoreno da države članice moraju da izrade i usvoje politiku i strategiju razvoja informacionog društva u JIE i „Jedinstvenog informacionog prostora JIE - prioritetna oblast", koje definiše načine uspostavljanja javne infrastrukture za bezbedno poslovanje na osnovu kvalifikovanog elektronskog potpisa.

„Zakon o elektronskom potpisu" i „Zakon o elektronskom pravnom i poslovnom prometu" usvojeni su 2006. godine. Takođe su usvojene odluke koje uređuju oblast korišćenja elektronskih potpisa i sertifikovanje kako bi se obezbedio neophodan pravni okvir za implementaciju digitalnog potpisa.

Zaštitne mere u primerima iz Bosne i Hercegovine

Reč je o slučaju u kojem je Državni tužilac navodno hakovao i-mejl nalog bivšeg Glavnog tužioca da bi ga diskreditovao, neposredno pre njegove suspenzije sa mesta Glavnog tužioca.

Tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe IT sistema

Nadležna lica iz pravosuđa BiH su utvrdila da postojeće mere zaštite nisu bile dovoljne da spreče nameran, nezakonit pristup računarskom sistemu - naime, službenom i-mejl nalogu zaposlenog. Pravosuđe BiH je stoga unapredilo postupke bezbednosti na svim nivoima i primenila standard ISO / IEC 27001:2005.

Organizacione i proceduralne zaštitne mere poput „načela više očiju"

Iako je sve sprovedeno u skladu sa zakonom, već uspostavljene proceduralne mere zaštite bile su nedovoljne i neodgovarajuće da spreče grešku uzrokovanu ljudskim faktorom i nizak nivo svesti ljudi koji koriste infrastrukturni sistem IT o bezbednosti.

Praćenje prometa podataka i pristupa zaposlenih sistemima podataka

Zakoni i procedure pravosuđa BiH propisuju praćenje prometa podataka, kao i praćenje pristupanja zaposlenih sistemima podataka. Prema internim izveštajima, koje su izradile različite sudske instance, ovakav pristup je prepoznat kao neophodna mera opreza, i kao takva se koristi u zaštiti od korupcije i računarskog kriminala.

Mere obuke i podizanja svesti za državne službenike o rizicima od zloupotrebe IT u svrhe korupcije i zaštitnim merama

Da, Agencija za državnu službu Bosne i Hercegovine i slične agencije na nivou entiteta obučavaju svoje državne službenike da smanje rizik od nastanka sukoba interesa, kao i da unaprede kodeks ponašanja u državnoj upravi na svim državnim administrativnim nivoima.

Agencija za prevenciju korupcije i kordinaciju borbe protiv korupcije je institucija na nivou države, koja je takođe nadležna za razvoj i praćenje edukativnih obuka o prevenciji i borbi protiv različitih oblika korupcije. Zbog nedostatka političke volje da se zaposle svi potrebni kadrovi i obezbedi oprema, Agenciji nedostaju kapaciteti da u celosti sprovede sve zadatke koje za nju propisuju relevantni zakoni.

Revizija IT sistema

Organizacija sada sprovodi dodatne revizije IT sistema kako bi sprečila zloupotrebu IT sistema u budućnosti.

Zakonodavne mere zaštite

- Zakon o elektronskom potpisu
- Zakon o elektronskom poslovanju
- Zakon o elektronskom pravnom i poslovnom prometu
- Zakon o zaštiti tajnih podataka

Slučaj iz Bosne i Hercegovine 2: Još jedno moguće kontraverzno zaposlenje u Vrhovnoj revizorskoj instituciji u Republici Srpskoj

Slučaj pisanog testa za izbor dva mlađa revizora u Vrhovnoj revizorskoj instituciji Republike Srpske, kada su nestali podaci sa testa i gde postoji mogućnost da je jedan kandidat odabran pre objavljivanja rezultata testiranja.

Tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe IT sistema

Što se tiče mera zaštite (tehničkih) za sprečavanje ovakve vrste problema u budućnosti, prema izvorima iz VRIRS do sada ništa nije urađeno.

Organizacione i proceduralne mere zaštite poput „načela više očiju"

Ne samo da su postojale oblasti koje nisu adekvatno sprovedene u skladu sa zakonom, već su i neke od postojećih proceduralnih zaštitnih mera bile nedovoljne i neodgovarajuće. Kandidati treba da polažu testove koristeći bezbedan softver. Umesto toga, kandidati su svoj test radili u jednostavnom „Word" formatu bez ikakve zaštite, tako da je bilo ko iz nadležne komisije mogao da izvrši izmene u testu. Osim toga, ovog puta kandidatima nije bilo dozvoljeno da iskopiraju testove na svoje USB memorije i testovi im nisu dati da ih pogledaju.

Praćenje prometa podataka i pristup zaposlenih sistemima podataka

Organizacija nije naučila ništa iz ovog slučaja i ne postoji svest da je praćenje prometa podataka potrebno kao zaštitna mera.

Mere obuke i podizanja svesti za državne službenike o rizicima od zloupotrebe IT u svrhe korupcije i zaštitnim merama

Da, Agencija za državnu službu Republike Srpske obučava državne službenike da smanje rizik od nastanka sukoba interesa, kao i da unaprede kodeks ponašanja u državnoj upravi na svim administrativnim nivoima.

Revizija IT sistema

Organizacija treba da sprovede internu reviziju IT sistema i to je njihova obaveza u skladu sa zakonom.

Zakonodavne mere zaštite

Nije bilo dostupno.

Slučaj iz Bosne i Hercegovine 3: Zloupotreba elektronskog sistema projekta CIPS

Projekat Sistem za zaštitu identifikacije građana (CIPS) pokrenut je u Bosni i Hercegovini u aprilu 2002. godine kada je privremeno osnovana uprava za njegovu realizaciju. Glavni zadatak projekta bio je da uspostavi deo sistema kroz koji bi se primenio Zakon o centralnoj evidenciji i razmeni podataka. Još od ranih faza projekta CIPS evidentiran je veliki broj pritužbi o zloupotrebi njegovog elektronskog sistema, naročito prilikom izdavanja ličnih karata i pasoša u celoj zemlji.

Tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe IT sistema

IDDEEA je između 2012. i 2015. godine implementirala sledeće standarde: ISO/27001:2005 i ISO/90001:2008 (sa planiranim revizijama[51]).

Sistem upravljanja dokumentima (DMS) u okviru IDDEEA se koristi za čuvanje podataka o institucijama na nivou države i entiteta, kao i agencija koje su obavezne da svoj rad usklade sa visokim standardom bezbednosti i zaštite IT.

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

Organizacione i proceduralne zaštitne mere poput „načela više očiju”

- Nastaviti sa primenom relevantnijih standarda i redovno koristiti reviziju u skladu sa pravilima i zakonskim propisima EU, s posebnim osvrtom na standarde Upravljanja kvalitetom ISO 9001.
- Bezbednosna provera zaposlenih sprovedena kod nadležnog organa (Obaveštajno-bezbednosna agencija BiH) čime je omogućeno izbegavanje narušavanje bezbednosti IT i prikupljanje ličnih podataka svih zaposlenih pod ugovorom kako bi se izradio društveni profil za buduće namene.

Praćenje prometa podataka i pristup zaposlenih sistemima podataka

U smislu infrastrukture i bezbednosti prenosa podataka, institucije u BIH su uvele visoko sofisticiranu komunikacionu mrežu primenjujući tehnologiju Sinhrone digitalne hijerarhije (SDH) koja omogućava brzu, pouzdanu i efikasnu razmenu podataka, slika i zvuka. SDH mreža je zatvoren sistem, koji nije povezan sa internetom i koji radi u određenom opsegu frekvencija pokrivenih za tu svrhu. Institucija koja održava tehničku SDH mrežu, Agencija za identifikacione dokumente, evidenciju i razmenu podataka (IDDEEA), je nadležna za identifikaciona dokumenta, čuvanje, personalizaciju i prenos dokumenata, kao i za centralnu evidenciju i razmenu informacija između nadležnih organa u Bosni i Hercegovini.

IDDEEA[52] prati, koordiniše i reguliše institucionalno polje identifikacionih dokumenata, i kao takva je razvila elektronski potpis u zatvorenom sistemu – a njeno iskustvo u primeni elektronskog potpisa u zatvorenim sistemima je veoma bitno za sprovođenje Zakona o elektronskom potpisu BiH i otvorenih sistema.

U **ključne probleme** spadaju:

- nedostatak institucionalnih dogovora neophodnih za koordinaciju aktivnosti u oblasti usluga elektronske uprave (koje se pružaju na različitim nivoima i od strane različitih ministarstava),
- neracionalna iskorišćenost (neadekvatno raspoređenih) IT kadrova,
- neadekvatna politika IKT i zakonski okviri koje primenjujuju upravljački organi na nivou države i entiteta, i
- neizvršenje smernica IDDEEA.

Mere obuke i podizanja svesti za državne službenike o rizicima od zloupotrebe IT u svrhe korupcije i zaštitnim merama

Agencija za državnu službu BiH i slične agencije na nivou entiteta obučavaju svoje državne službenike da smanje rizik od nastanka sukoba interesa, kao i da unaprede kodeks ponašanja u državnoj upravi na svim državnim administrativnim nivoima.

52 http://www.iddeea.gov.ba/images/stories/PDF/law_on_agency_final.pdf

IDDEEA je implementirala platformu za elektronsko učenje u cilju kontinuirane edukacije i unapređenje veština svojih kadrova, što je neophodno da bi se postigli najveći standardi delotvornosti i profesionalizma.

Agencija za prevenciju korupcije i koordinaciju borbe protiv korupcije je institucija na državnom nivou koja je takođe nadležna za razvoj i praćenje edukativnih obuka o prevenciji i borbi protiv različitih oblika korupcije. Zbog nedostatka političke volje da se zaposle svi potrebni kadrovi i obezbedi oprema, Agenciji nedostaju kapaciteti da u celosti sprovede sve zadatke koje za nju propisuju relevantni zakoni.

Revizija IT sistema

Da, za IT informacioni sitem osnovano je interno odelenje za reviziju u cilju sprečavanje zloupotrebe IT sistema.

Zakonodavne mere zaštite

- Zakon o zaštiti lica koja prijavljuju korupciju u institucijama Bosne i Hercegovine („Službeni list Bosne i Hercegovine" br. 100/13)
- Zakon o upravi („Službeni list Bosne i Hercegovine" br. 32/02 i 102/09),
- „Smernice" o podnošenju internih izveštaja o sumnjama i bojaznima u vezi korupcije zaposlenih u Agenciji za identifikacione dokumente, evidenciju i razmenu podataka Bosne i Hercegovine, 31. mart 2014.

MERE ZAŠTITE OD ZLOUPOTREBE IT U BOSNI I HERCEGOVINI

Borba protiv korupcije

Svi relevantni domaći i međunarodni dokumenti o stanju korupcije u BiH ukazuju da je korupcija jedan od najvećih problema u društvu i najveća prepreka raznim reformama i ukupnom privrednom i društvenom napretku. U najnovijem izveštaju EU o napretku BiH se još jednom navodi da je zemlja u ranoj fazi borbe protiv korupcije[53]. Pored toga, ključni delovi antikorupcijskih zakonskih propisa su izmenjeni na način koji potkopava prethodna dostignuća. Korupcija je i dalje veoma rasprostranjena, sa nedovoljno rezultata po pitanju istraga i krivičnog gonjenja u slučajevima na viskom nivou.

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

Pravosudni sistem

Visoki sudski i tužilački savet (VSTS) je 2013. godine preduzeo niz mera i konkretnih radnji koje treba da doprinesu profesionalnijem i kvalitetnijem radu tužilaca. Slučaj br. 1, koji je opisan u poglavlju 1, po našem mišljenju, doprineo je bržoj automatizaciji i profesionalizaciji sistema. Znanje, veštine i razumevanje aktuelnih pitanja, od značaja za tužilački rad, unapređeni su kroz posebno angažovanje projekta „Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa" u oblasti edukacije. Ovi ciljevi su ostvareni izradom modula za obuku, organizacijom velikog broja edukativnih strategija, saradnjom sa CEST (centrima za edukaciju sudija i tužilaca), u cilju poboljšanja postojećeg modela edukacije tužilaca, i upravljenjem mrežama svih aktera u krivičnoj istrazi tokom edukativnog procesa. Tokom ovog procesa, više od 150 tužilaca je unapredilo svoje znanje u sledećim oblastima:

- krivični postupak protiv pravnih lica,
- imunitet svedoka,
- veštine proučavanja i istraživanja,
- posebne istrage,
- računarski kriminal,
- pranje novca i finansijske istrage,
- trgovina ljudima, i
- veštine i metode komunikacije.

Što se tiče gore navedenog, konstatovali smo brojne relevantne činjenice u pogledu zakonodavtsva i pokazali da poštovanje zakonskog okvira može u velikoj meri da spreči ovu vrstu kriminala i korupcije.

Pored redovnih revizija, Vrhovna revizorska kancelarija Bosne i Hercegovine (VRK BiH) je 2013. godine sprovela o reviziju učinka: „Telekomunikaciona rešenja u institucijama Bosne i Hercegovine". Navedeni izveštaj revizije je istakao pozitivne primere VSTS, koji je utrošio značajno manji iznos za internet usluge u odnosu na druge institucije iz uzorka revizije, iako VSTS ima značajno veći broj korisnika.

Poboljšana bezbednost pravosudnog informacionog sistema BiH i dalje je jedan od njegovih strateških prioriteta, kao što se navodi u Strategiji reforme pravosuđa u BiH 2014-2018[54]. Tu su i preporuke VSTS da kapitalne investicije u pravosuđu treba da obuhvate zamenu zastarele i nabavku nedostajuće računarske opreme, dalji razvoj informacionih sistema u pravosuđu, održavanje postojeće opreme i softverskih licenci i usavršavanje IT i drugih kadrova u pravosuđu.

U okviru procesa kompjuterizacije pravosuđa postavljen je sistem za elektronsku razmenu podataka između policijskih organa i tužilaštava, te zvanično stavljen u funkciju u junu 2013. godine. Tužioci u tužilaštvima širom zemlje sada imaju mogućnost da prate elektronsku evidenciju u nadležnosti policijskih organa, u skladu sa vežaćim zakonskim okvirom. Pored toga, policijski organi imaju mogućnost praćenja statusa policijskih izveštaja o krivičnim

54 http://www.mpr.gov.ba/aktuelnosti/propisi/konsultacije/SRSP%20u%20BiH.pdf

delima koji se dostavljaju tužilaštvima, a koji se čuvaju u njihovom sistemu za automatsko upravljanje predmetima (TCMS). Sistem je izgrađen u skladu sa Sporazumom zaključenim između VSTS, Ministarstva bezbednosti BiH, Državne agencije za istrage i zaštitu, granične policije i Ministarstava unutrašnjih poslova na svim nivoima vlasti. Podrška pravosuđu Bosne i Hercegovine (IPA 2009.) i IPA projekat „Podrška reformi policije" bila su dva glavna projekta koja su dovela do uspostavljanja ovog sistema.

Da bi se odgovorilo na sve veće potrebe sistema, naročito u pogledu novog automatskog sistema upravljanja predmetima za sudove i tužilaštva (CMS/TCMS) i da bi se obezbedila softverska rešenja kompatibilna sa važećim softverskim standardima, proces dogradnje svih hardverskih i softverskih komponenti sistema ICT (optimizacija i konsolidacija sistema ICT u pravosuđu BiH) nastavljen je 2013. godine. Ovaj proces je sproveden da bi se:

- na najmanji mogući nivo smanjio period nefunkcionisanja sistema koje nastaje zbog zastarelosti IT opreme i softvera;
- obezbedila najbolja iskorišćenost postojećeg servera u centrima sa podacima VSTS;
- omogućio normalan rad korisnika u pravosudnom sistemu i jednostavan pristup elektronskim uslugama pravosuđa, koje su preko interneta dostupne građanima;
- poboljšala bezbednost podataka pohranjenih u bazama podataka pravosudnog informacionog sistema; i
- obezbedilo da tehnički zahtevi za nesmetanu razmenu podataka sa eksternim sistemima budu ispunjeni (policija, poreski i drugi vladini elektronski registri), što je od ključnog značaja za borbu protiv korupcije i organizovanog kriminala.

Zaposleni u Odelenju VSTS za ICT su u okviru ovog projekta dogradili sistem za upravljanje digitalnim identitetima, kao i sisteme elektronske pošte u centrima za obradu i pohranjivanje podataka unutar VSTS.

Sve ove mere prepoznate su u najnovijem Izveštaju EU o napretku BiH. U izveštaju se ističe da je pravosudni informaciono-komunikacioni sistem u potpunosti funkcionalan. CMS/TCMS sadrži preko 3,4 miliona zavedenih predmeta i generiše automatske izveštaje o rezultatima rada pravosuđa, što pomaže kod odlučivanja o politikama i u strateškom planiranju. Pristupanje pravosudnom internet portalu značajno se povećalo, kao i pristupanje stranaka ili njihovih advokata informacijama o predmetima pred sudovima. Pravosudni dokumentacioni centar takođe beleži porast poseta preko interneta.

Centri za edukaciju sudija i tužilaca dva entiteta nude obuku za pravosuđe. U nastojanju da se unapredi i poveća izgradnja kapaciteta, oba centra uvode učenje na daljinu[55].

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

Policija

Kao što je potvrđeno u Izveštaju EU o napretku BiH, agencije i odbori formirani u skladu sa zakonima o reformi policije još uvek konsoliduju svoje poslove[56].

Formiran je međuresorski tim za praćenje koji je nadzirao realizaciju sistema za elektronsku razmenu podataka za registre policije i tužilaštva. Pojedine tehničke aspekte sistema još uvek treba rešiti, uključujući i činjenicu da Direkcija za koordinaciju policijskih tela još uvek nema pristup bazama podataka sistema. Europol je sproveo reviziju zaštite podataka.

Agencija za policijsku podršku se nalazi na istoj lokaciji kao i Direkcija za koordinaciju policijskih tela i izradila je Pravilnik o standardizaciji policijske opreme.

Izmene i dopune zakona o policijskim službenicima su u postupku usvajanja na nivou države. Federacija BiH, kantoni i Distrikt Brčko su pokrenuli inicijativu da usaglase svoje pojedinačne zakone. Izmene i dopune se odnose na tehnička i operativna pitanja, kao što su upotreba oružja i policijskih ovlašćenja i unapređenje zaštite ličnih podataka[57].

Zakon BIH[58] prepoznaje računarski kriminal kao oblik kriminalnog ponašanja u kojem se računarska tehnologija i informacioni sistemi koriste kao instrument ili meta izvršenja krivičnopravnih radnji sa odgovarajućim posledicama.

Osnovne karakteristike ili svojstva računarskog kriminala su:

- društveno opasno, nezakonito ponašanje za koje zakon propisuje krivične sankcije;
- poseban način izvršenja krivičnih dela sa ili putem računara;
- poseban predmet zaštite, bezbednost računarskih podataka ili informacionog sistema kao celine ili njegovih pojedinačnih segmenata; i
- namera samog učinioca ili nekog drugog lica je da za sebe obezbedi korist iz tog dela[59].

Krivična dela povezana sa računarima i internetom[60]:

- Računarsko krivotvorenje
- Računarska prevara
- Dečija pornografija
- Povrede intelektualne svojine

56 Proces sveobuhvatne reforme policije BiH, koji je započeo posle građanskog rata, podrazumevao je osnivanje nekoliko važnih institucija na državnom nivou, kao što su: Državna granična policija, Služba za poslove sa strancima Ministarstva bezbednosti BIH, Državna agencija za istrage i zaštitu (SIPA), Direkcija za koordinaciju policijskih tela BiH, itd.

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

58 Krivični zakon Federacije Bosne i Hercegovine - Član 393 do 398

59 http://www.fup.gov.ba/?p=1697 - Uprava policije Federacije

60 http://www.rs.cest.gov.ba/

Neovlašćeni pristup:

- nameran nezakonit pristup računarskom sistemu
- prouzrokavanje štete na računarskim sistemima i podacima
- otkrivanje poverljivih podataka

Zloupotreba uređaja:

- namerno, neovlašćeno delo proizvodnje, prodaje, nabavke ili distribucije
- uređaji za pristupanje (uključujući računarske programe)
- računarske lozinke
- CODE
- druge vrste pristupnih informacija za činjenje krivičnih dela iz oblasti računarskog kriminala

Neovlašćeno presretanje podataka:

- namerno, nezakonito presretanje podataka od strane računarskog sistema.
- zaštita privatnosti prenosa računarskih podataka koji nisu javni od praćenja i snimanja.

Ometanje podataka:

- namerno, neovlašćeno nanošenje štete, brisanje, uništavanje, izmena ili dela da se računarski podaci učine neupotrebljivim
- ubacivanje štetnog koda koji predstavlja pretnju integritetu ili mogućnosti korišćenja podataka i programa
- virusi koji ometaju podatke

Definitivno postoje mere za krivično gonjenje ovih i sličnih slučajeva povezanih sa zloupotrebom IT u svrhe korupcije, bez obzira da li je reč o krađi podataka ili „slušanje podataka" sa ciljem delenja „preslušanih" informacija sa zainteresovanim stranama.

IT sistemi i interne procedure povezane sa sistemom za upravljanje dokumentima, arhivom, predmetima tužilaca i drugim relevantnim dokumentima i materijalima, uključujući zaposlene koji rade na tim sistemima, predmet su redovne kontrole od strane nadležnih organa. U nekim institucijama je to definisano internim procedurama, u zavisnosti od profila institucije. U ovom slučaju, ključni detalj je implementacija ISO/IEC 27001:2005, sa ciljem da se osigura da je bezbednost podataka zadovoljavajuća.

Šta raditi

Nastaviti sa primenom još relevantnijih standarda i redovno koristiti usluge revizije u skladu sa pravilima i propisima EU, s posebnim osvrtom na ISO 9001 upravljanje kvalitetom ISO/27001:2005 i ISO/90001:2008 standarde.

Nastaviti sa bezbednosnim proverama zaposlenih koje sprovode nadležni organi, a kojima se omogućava izbegavanje narušavanja bezbednosti IT i prikupljanje ličnih podataka svih lica pod ugovorom i budućih kadrova kako bi se izradio društveni profil za buduće namene.

Borba protiv organizovanog kriminala i korupcije

Slabosti u sistematičnom prikupljanju, analizi i korišćenju obaveštajnih podataka od strane organa za sprovođenje zakona otežava strateško ciljanje grupa i poslova organizovanog kriminala. Sistematična razmena obaveštajnih podataka između organa za sprovođenje zakona u cilju zajedničkog operativnog planiranja ne postoji.

Pripremljene su izmene i dopune državnog Zakonika o krivičnom postupku, čiji je cilj delotvornija upotreba specijalnih istražnih mera, ali njihovo usvajanje tek predstoji.

U oblasti pravosudne saradnje u krivičnim stvarima, pripreme za zaključivanje sporazuma o saradnji sa Eurojust-om su u početnoj fazi, ali je ostvaren određeni napredak. Procena zakonskih propisa o zaštiti podataka je završena. Izmene i dopune Zakona o zaštiti tajnih podataka, kojima se zakon usaglašava sa relevantnim evropskim standardima i koje propisuju realizaciju bilateralnih sporazuma o bezbednosti, tek treba da se usvoje.

Računarski kriminal

Izveštaj Evropske unije o napretku Bosne i Hercegovine za 2013. godinu navodi nepostojanje strategije i institucija koje bi se borile protiv računarskog kriminala i pretnji:

„Bosna i Hercegovina nema ni strategiju ni institucije za rešavanje pitanja računarskog kriminala i računarskih bezbednosih pretnji. Savet ministara još nije usvojio Akcioni plan za formiranje BIH CERT-a (Computer Emergency Response/Readiness Team –Tim za odgovore na računarske incidente). Preduzete su aktivnosti za uspostavljanje CERT-a. Izveštaji o krivičnim delima koje pripremaju organi za sprovođenje zakona u Bosni i Hercegovini se ne odnose na računarski kriminal. Oni ne daju tačne podatke o broju slučajeva, istragama ili osumnjičenima. Digitalna forenzika i druga tehnička sredstva za borbu protiv računarskog kriminala na državnom i međunarodnom nivou su ograničena i nedovoljna. Direkcija za koordinaciju policijskih tela je određena kao stalno dostupna kontakt tačka u skladu s Konvencijom o računarskom kriminalu (Konvencija iz Budimpešte), ali za to nedostaju potrebni kapaciteti.” [61].

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

OSTALE MERE

Razmena podataka između organa državne uprave

Sa projektom „Podrška pravosuđu Bosne i Hercegovine" (IPA 2009) i IPA projektom „Podrška reformi policije", koji je počeo 2013. godine, uz zaokružen proces implementacije, i u skladu sa sporazumom kojim se uspostavlja sistem elektronske razmene podataka između policijskih organa i tužilaca - koji su zaključili VSTS, Ministarstvo bezbednosti BiH, Granična policija, Državna agencija za istrage i zaštitu (SIPA) i Ministarstvo unutrašnjih poslova - VSTS je započeo sa aktivnostima koje će nadamo se rezultirati novom generacijom razmene podataka u BiH. Tokom ovog procesa, potrebno je da svi gore navedeni standardi budu sprovedeni a sistemi podataka ažurirani da bi se izbegli primeri korupcije koji se navode u ovoj studiji. Da bi se to postiglo, u ovaj sistem biće ugrađeni instrumenti i zaštitne mere u koje spadaju: zaštitni zid (firewall), sistem za detekciju i prevenciju upada (IDS), testiranje penetracije i skeniranje osetljivosti, postupci za prenos osetljivih podataka, postupci i pravila za povezivanje sa eksternim sistemima, antivirus zaštita i „pro-defence" instrumenti, kontrole za daljinsko upravljanje, postupci i kontrole za ulazak i izlazak u prostorije, pravljenje rezervne kopije podataka na udaljenoj lokaciji u kombinaciji sa složenom zaštitom pomoću lozinke i fizičkom bezbednošću, kao i stalna edukacija zaposlenih o IT.

Agencija za identifikaciona dokumenta, evidenciju i razmenu podataka, bivši Sistem za zaštitu identifikacije građana (CIPS)[62], je dobar primer primene zaštitnih mera i bezbednosti. Međutim, iako je Agencija veoma dobro organizovana na državnom nivou, zloupotrebe nažalost postoje na nivou lokalnih vlasti.

Šta su naučili iz zloupotrebe elektronskog sistema projekta CIPS

U periodu od 2012. do 2015. godine sprovode ISO/27001:2005 i ISO/90001:2008 sa isplaniranim revizijama[63]. Njihov sistem upravljanja dokumentima, matični registar i interno okruženje Orakl, koje se koristi za čuvanje podataka svih institucija i agencija na državnom nivou, je veoma zaštićen i bezbedan. Problem u ovom slučaju, kao što je opisano u poglavlju 1, je taj što su nadležni organi (u Federaciji BiH to su bila kantonalna ministarstva unutrašnjih poslova, Ministarstvo unutrašnjih poslova Republike Srpske, i nadležni organ koji funkcionalno deluje kao državna institucija u Distriktu Brčko) imali stroge procedure za rad sa podacima, a istovremeno su menjali, dodavali, brisali i ažurirali lične podatke građana.

Kako propisuje zakon, nadležni organi su vlasnici podataka, dok je uloga Agencije IDDEEA u tom procesu samo da čuva i zaštiti podatke, kao i da primeni sve poznate zaštitne mere i dobre prakse bezbednosti[64]. Imajući tu činjenicu u vidu, nadležnost za takve slučajeve

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=105&Itemi d=97&lang=en

mora da se dodeli upravama policije u BiH i nadležnim organima koje će se baviti drugim sličnim situacijama, ako ih bude. To znači da njihovi standardi, procedure, te generalno način postupanja kod takvih problema nisu prihvatljivi.

IDDEEA je obezbedila potpunu bezbednost na svim nivoima zaštite podataka za nadležne policijske agencije i nadležne organe u Bosni i Hercegovini. Dakle, zloupotrebu IT tehnologije u svrhe korupcije treba tražiti na nivou nadležnog organa, gde će država osigurati i unaprediti informacionu bezbednost.

IDDEEA je primenila digitalne potpise za sve kanale komunikacije u okviru Agencije, kao i za eksternu komunikaciju prema nadležnim organima.

Međutim, nedostaje Tim za odgovore / pripremljenost na računarske incidente[65] (CERT). Iako je bila predviđena izrada akcionog plana za CERT[66], taj plan još uvek nije urađen.

Elektronski potpis

Tehnički opis Ključne javne infrastrukture (PKI)[67] je da se drastično podigne nivo bezbednosti za razmenu podataka u primarnoj tehničkoj komponenti na državnom nivou. To može da bude ili centralna infrastruktura sa jednim organom za izdavanje sertifikata i nižim telima koja izdaju sertifikate za elektronske potpise, ili nezavisna infrastruktura na nivou interoperativnosti.

U Bosni i Hercegovini ne postoji PKI za preduzeća i pojedince na državnom nivou. Međutim, postoji veliki broj samostalnih upotreba PKI, naročito u elektronskom bankarstvu i delimično u oblasti elektronske uprave, koje funkcionišu u zatvorenim sistemima. Dakle, tehnički problem se ne temelji toliko na nepostojanju PKI na državnom nivou. Umesto toga, problem je da se skupe i objedine postojeće PKI i informacioni sistemi. Povezivanje sa različitim PKI bi olakšalo proces poslovanja i rada u državnoj upravi.

Bezbednost bi bila pojačana, pošto bi svi učesnici u elektronskoj razmeni podataka ili obični građani imali identitet u ovom sistemu. Time se na najmanju moguću meru smanjuje mogućnost zloupotrebe i omogućava kontinuirano praćenje ljudskih aktivnosti. Svi sistemi koji su integrisani sa PKI, čime se u suštini stvara jedan veliki sistem, značajno smanjuju mogućnost zloupotrebe.

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

ZAKONODAVNI OKVIR

Direktiva 1999/93/EC o okviru Zajednice za elektronske potpise

Ova Direktiva uspostavlja pravni okvir za elektronske potpise i usluge sertifikovanja na evropskom nivou. Njena svrha je da olakša upotrebu elektronskih potpisa kao i da doprinese njihovom pravnom priznavanju u državama članicama.

Odluka 2003/511/EC Komisije od 14. jula 2003. godine o objavljivanju referentnih brojeva opšte priznatih standarda za proizvode elektronskih potpisa u skladu sa Direktivom 1999/93/EC

Bosna i Hercegovina se sa ovom odlukom Evropske komisije oslanja na tri opšte prihvaćena standarda za proizvode za elektronske potpise koji pretpostavljaju poštovanje kvalifikovanog elektronskog potpisa.

Odluka 2000/709/EC Komisije - novembar 2000. godine

U skladu sa članom 3 (4) Direktive 1999/93/EC Evropskog parlamenta i Saveta o okviru Zajednice za elektronski potpis, ova odluka propisuje kriterijume koje države članice moraju uzeti u obzir prilikom imenovanja tela koje će biti nadležno za ocenu usklađenosti sredstava za izradu elektronskog potpisa.

Zakonodavni okvir BiH

Na nivou države (BiH), trenutno su na snazi sledeći zakonski propisi:

- Zakon o elektronskom potpisu („Službeni list BiH", br. 91/06)
- Zakon o elektronskom pravnom i poslovnom prometu („Službeni list BiH", br. 88/07)
- Zakon o upravnom postupku („Službeni list" br. 29/02, 12/04, 88/07, 93/09)
- Odluka o osnovama upotrebe elektronskih potpisa i pružanja usluga overavanja („Službeni list BiH", br. 21/09)
- Odluka o elektronskom poslovanju i e-vladi („Službeni list" br. 07/10)
- Odluka o kancelarijskom poslovanju ministarstava, službi, institucija i drugih tela Saveta ministara („Službeni list BiH" br. 21/01, 29/03)
- Uputstvo o izradi i održavanju službenih Internet stranica institucija Bosne i Hercegovine (Službeni list br. 21/09)
- Zakon o zaštiti lica koja prijavljuju korupciju u institucijama Bosne i Hercegovine („Službeni list Bosne i Hercegovine" br. 100/13)
- Zakon o Agenciji za prevenciju korupcije i koordinaciju borbe protiv korupcije („Službeni list Bosne i Hercegovine", decembar 2009.).

Pored toga, trenutno su u izradi sledeća akta:

- Uredba o internoj organizaciji Ministarstva komunikacija i saobraćaja (osnivanje Kancelarije za praćenje i akreditaciju)
- Visoki sudski i tužilački savet (VSTS) preporučio je izvršnim vlastima BiH da Ministarstvo saobraćaja i komunikacija treba da usvoji odgovarajuća podzakonska akta i uspostavi institucionalne kapacitete kako bi se omogućila puna implementacija Zakona o elektronskom potpisu i Zakona o elektronskom poslovanju u pravosudni informacioni sistem, koja bi se primarno ogledala u mogućnosti dostavljanja podnesaka sudu u elektronskom obliku, kao i u dostavi sudskih odluka elektronskim putem (overenim kvalifikovanim digitalnim sertifikatom)[68].

Javne nabavke

Zakon o javnim nabavkama Bosne i Hercegovine[69] je, na jedinstven način, obuhvatio sve naručioce u skladu sa Direktivom EU 17/2004 i Direktivom EU 18/2004. Konkretna pravila EU o javnim nabavkama su obrađena kroz niz detaljnih direktiva u kojima se preciziraju sveobuhvatni zahtevi za regulisanje postupaka javnih nabavki. U Bosni i Hercegovini nema dovoljno preciznih propisa koji uređuju ovu oblast u skladu sa propisima EU.

Rešenje za prevazilaženje nedostataka u sistemu javnih nabavki bi moglo da bude omogućavanje jednom telu da sprovodi postupak nabavki za sve nadležne organe. To telo bi imalo, ako bi radilo analizu IT i korupcije, jedinstveni i centralizovani softver izrađen u skladu sa Zakonom o javnim nabavkama Bosne i Hercegovine koji bi se bavio potrebama svih nivoa vlasti, što bi mu omogućilo da sprovodi sve javne nabavke.

Naravno, preduslov bi bio uvođenje standarda i poznavanje tržišta od strane zaposlenih u smislu najnovijih informacija i kontakta sa dobavljačima. Takvo nešto je neophodno da bi se osiguralo da se kupuje samo neophodna roba i usluge, kao i da su ti proizvodi najbolji dostupni na tržištu.

68 http://www.hjpc.ba/intro/gizvjestaj/?cid=5889,2,133 http://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

Hrvatska

Pripremili Zorislav Petrović i Ivana Andrijašević

Glavni zakonodavni okvir za informacionu bezbednost

Zakonodavni okvir za obezbeđivanje informacione bezbednosti u informacionim sistemima državne uprave u Republici Hrvatskoj se oslanja na sledeće najvažnije zakone i podzakonska akta: Zakon o informacionoj bezbednosti, Zakon o tajnosti podataka, Zakon o zaštiti ličnih podataka, Zakon o bezbednosno-obaveštajnom sistemu, Zakon o elektronskoj ispravi, Zakon o elektronskom potpisu; Zakon o bezbednosnim proverama, Uredba o merama informacione bezbednosti, Uredba o sadržaju, izgledu, načinu ispunjavanja i postupanju sa upitnikom za bezbednosnu proveru i Pravilnik za uvođenje radnih mesta savetnika za informacionu bezbednost.

Zakon o informacionoj bezbednosti (Narodne novine, br. 79/07) utvrđuje pojam informacione bezbednosti, mere i standarde informacione bezbednosti, područja informacione bezbednosti, te nadležna tela za donošenje, sprovođenje i nadzor mera i standarda informacione bezbednosti. Ovaj se zakon primenjuje na državne organe, organe jedinica lokalne i regionalne samouprave te na pravna lica s javnim ovlašćenjima koja, u svom delokrugu, koriste klasifikovane i neklasifikovane podatke, kao i na pravna i fizička lica koje ostvaruju pristup ili postupaju sa klasifikovanim i neklasifikovanim podacima.

Zakon o tajnosti podataka (Narodne novine, br. 79/07, 86/12) utvrđuje pojam klasifikovanih i neklasifikovanih podataka, stepene tajnosti, postupak klasifikacije i deklasifikacije, pristup klasifikovanim i neklasifikovanim informacijama, zaštitu klasifikovanih i neklasifikovanih informacija i nadzor nad sprovođenjem ovoga zakona. Ovaj zakon se primenjuje na državne organe, organe jedinica lokalne i regionalne samouprave, pravna lica sa javnim ovlašćenjima te na pravna i fizička lica koja, u skladu sa ovim zakonom, ostvare pristup ili postupaju sa klasifikovanim i neklasifikovanim informacijama.

Zakon o zaštiti ličnih podataka (Narodne novine, br. 103/03, 118/06, 41/08, 130/11, 106/12) uređuje zaštitu ličnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korišćenjem ličnih podataka u Republici Hrvatskoj. Svrha zakona je zaštita privatnog života i ostalih ljudskih prava i osnovnih sloboda u prikupljanju, obradi i korišćenju ličnih podataka.

Zakonom o bezbednosno-obaveštajnom sistemu Republike Hrvatske (Narodne novine, br. 85/08, 86/12) se, radi sistematskog prikupljanja, analize, obrade i ocene podataka koji su od značaja za nacionalnu bezbednost, u cilju otkrivanja i sprečavanja radnji pojedinaca ili grupa koje su usmerene: protiv opstanka, nezavisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, na nasilno rušenje ustroja državne vlasti, ugrožavanje Ustava Republike Hrvatske i zakonima utvrđenih ljudskih prava i osnovnih sloboda te osnova privrednog sistema Republike Hrvatske i koji su nužni za donošenje odluka značajnih

za ostvarivanje nacionalnih interesa u području nacionalne bezbednosti, osnivaju bezbednosno-obaveštajne agencije: Sigurnosno-obaveštajna agencija (SOA) i Vojna sigurnosno-obaveštajna agencija (VSOA).

Zakon o elektronskoj ispravi (Narodne novine, br. 150/05) uređuje pravo fizičkih i pravnih lica na korišćenje elektronske isprave u svim poslovnim radnjama i delatnostima te u postupcima koji se vode pred telima javne vlasti u kojima se elektronska oprema i programi mogu primenjivati u izradi, prenosu, pohranjivanju i čuvanju informacija u elektronskom obliku, pravna valjanost elektronske isprave te upotreba i promet elektronskih isprava.

Zakon o elektronskom potpisu (Narodne novine, br. 10/02, 80/08, 30/14) uređuje pravo fizičkih i pravnih lica na korišćenje elektronskog potpisa u upravnim, poslovnim i drugim radnjama, te prava, obaveze i odgovornosti fizičkih i pravnih lica u vezi sa pružanjem usluga sertifikovanja elektronskog potpisa.

Zakon o bezbednosnim proverama (Narodne novine, br. 85/08, 86/12) utvrđuje pojam i stepene bezbednosne provere, bezbednosne prepreke te postupak sprovođenja bezbednosnih provera. U skladu sa ovim zakonom, bezbednosna provera je postupak kojim nadležna tela utvrđuju postojanje bezbednosnih prepreka za fizička i pravna lica.

Uredba o merama informacione bezbednosti (Narodne novine, br. 46/08) utvrđuje mere informacione bezbednosti za postupanje sa klasifikovanim i neklasifikovanim informacijama. Uredba se primenjuje na državna tela, tela jedinica lokalne i regionalne samouprave, te na pravna lica sa javnim ovlašćenjima, koja u svom delokrugu koriste klasifikovane i neklasifikovane informacije, kao i na pravna i fizička lica koja ostvaruju pristup ili postupaju sa klasifikovanim i neklasifikovanim informacijama.

Uredba o sadržaju izgledu, načinu ispunjavanja i postupanju sa upitnikom za bezbednosnu proveru (Narodne novine, br. 114/08) uređuje sadržaj, izgled, način ispunjavanja i postupanje sa upitnikom za bezbednosnu proveru za fizička i pravna lica.

Pravilnikom za uvođenje radnih mesta savetnika za informacionu bezbednost (Narodne novine, br. 100/08, 30/11) utvrđuju se kriterijimi za uspostavljanje radnih mesta savetnika za informacionu bezbednost.

Pored navedenih propisa, postoji veliki broj zakona i podzakonskih akata koji se samo delimično bave informacionom bezbednošću, kao što su Zakon o elektronskoj trgovini, Krivični zakonik, Zakon o arhivskoj građi, Zakon o bezbednosti i zaštiti, itd. Na kraju, važno je napomenuti da, kao članica NATO i EU, Hrvatska usklađuje svoje propise u oblasti informacijske bezbednosti sa drugim državama članicama NATO i EU.

Centralni državni organi nadležni za informacionu bezbednost

U centralne državne organe nadležne za informacionu bezbednost u Hrvatskoj spadaju:

- **Kancelarija Saveta za nacionalnu bezbednost**: centralno državno telo nadležno za informacionu bezbednost koordinira i usklađuje donošenje i primenu mera i standarda informacione bezbednosti u Republici Hrvatskoj, kao i za razmenu klasifikovanih i neklasifikovanih informacija između Republike Hrvatske i stranih država i organizacija (član 14 Zakona o informacionoj bezbednosti);
- **Zavod za bezbednost informacionih sistema**: centralno državno telo za tehnička područja bezbednosti informacionih sistema u organima i pravnim licima, tj. za: standarde bezbednosti informacionih sistema, bezbednosne akreditacije informacionih sistema, upravljanje kriptomaterijalima koji se koriste u razmeni tajnih podataka, koordinaciju prevencije i odgovora na računarske pretnje po bezbednost informacionih sistema (član 17 Zakona o informacionoj bezbednosti); i
- **Nacionalni CERT**: nacionalno telo za prevenciju i zaštitu od računarskih pretnji po bezbednost javnih informacionih sistema u Republici Hrvatskoj koje deluje u okviru Hrvatske akademske i istraživačke mreže (CARNet) – glavnog stuba interneta za državni sektor u Hrvatskoj. Najvažniji zadatak CERT-a je obrada incidenata na internetu, tj. očuvanje informacione bezbednosti u Hrvatskoj. Nacionalni CERT u okviru svog delovanja sprovodi proaktivne i reaktivne mere u cilju sprečavanja ili ublažavanja moguće štete. Korisnici Nacionalnog CERT-a su svi korisnici Interneta u Republici Hrvatskoj i pružaoci hosting usluga te usluga pristupa Internetu (ISP)[70].

Uopšteno o sistemu informacione bezbednosti

Zakon o informacionoj bezbednosti definiše pet područja informacione bezbednosti za koja su propisane mere i standardi informacione bezbednosti: bezbednosna provera, fizička bezbednost, bezbednost podataka, bezbednost informacionog sistema i bezbednost poslovne saradnje.

Područje informacione bezbednosti bitno za ovu studiju je bezbednost informacionog sistema. Prema stavu 1 člana 12 zakona o informacionoj bezbednosti, bezbednost informacionog sistema je „područje informacione bezbednosti u okviru kojeg se utvrđuju mere i standardi informacione bezbednosti klasifikovanog i neklasifikovanog podatka koji se obrađuje, pohranjuje ili prenosi u informacionom sistemu i zaštita celovitosti i raspoloživosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada informacionog sistema". Dalje, u skladu sa istim članom, „bezbednosna akreditacija informacionog sistema obavlja se za informacioni sistem u kojem se koriste klasifikovani podaci stepena POVERLJIVO, TAJNO i VRLO TAJNO. Osobe koje učestvuju u gore navedenom procesu treba da poseduju sertifikat nivoa VRLO TAJNO ili za jedan stepen viši od najvišeg nivoa klasifikovanih podataka koji se obrađuju, pohranjuju ili prenose u informacionim sistemima u njihovoj nadležnosti. Mere fizičke zaštite prostora u kojima

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

se nalaze informacioni sistemi će se preduzeti u skladu sa najvišim nivoom klasifikovanih podataka koji se u njima obrađuju, pohranjuju ili prenose. I na kraju, centralna državna tela nadležna za informacionu bezbednost su obavezna da uspostave registar sertifikovane opreme i uređaja koji se koriste u informacionom sistemu nivoa POVJERLJIVO, TAJNO i VRLO TAJNO. Registar sertifikovane opreme i uređaja se uspostavlja na osnovu preuzimanja odgovarajućih registara međunarodnih organizacija ili sopstvenim procesom sertifikovanja u skladu sa odgovarajućim međunarodnim normama."

U mere informacione bezbednosti za područje bezbednosti informacionog sistema, u skladu sa Uredbom o merama informacione bezbednosti, spadaju:

- mere zaštite informacionog sistema (zaštita hardvera, softvera i medija za pohranjivanje podataka, upravljanje konfiguracijom i sistemom korisničkog pristupa, kontrola povezivanja i upotrebe informacionih sistema, itd);
- svest o bezbednosti (donošenje pravila o bezbednosti za zaposlene i edukacija o bezbednosti); i
- planiranje delovanja u vanrednim okolnostima (definisanje postupaka koje treba sprovesti u slučaju incidenta i upravljanje poslovnim kontinuitetom).

Bezbednost informacionog sistema se sprovodi tokom celog životnog ciklusa informacionog sistema za sisteme sa klasifikovanim (putem bezbednosne akreditacije) i neklasifikovanim (usklađivanje sa HRN ISO/IEC 27001 i HRN ISO/IEC 17799 standardima) podacima[71].

Primeri hrvatskih mera zaštite od zloupotrebe IT

Slučaj iz Hrvatske 1: Poziv od doktora radi glasanja

Reč je o slučaju u kojem je doktor izvlačio podatke iz bolničkog sistema. Prema informacijama iz javno dostupnog Centralnog registra sa evidencijom o sistemu za podnošenje ličnih podataka koji vodi Agencija za zaštitu ličnih podataka, ta zaštita u okviru Zbirke o ličnim podacima pacijenata, koja je delom elektronska a delom na papiru, se obezbeđuje poštovanjem mera zaštite: zaključavanjem dokumentacije u ormariće, sistemom video nadzora, lozinkom i korisničkim imenom, te sistemom za zaštitu od požara. U ovom konkretnom slučaju, glavni problem je bila slaba zaštita podataka, uključujući činjenicu da je previše ljudi imalo pristup bazi podataka. Navodno, u sistemu baze podataka nije bilo funkcije koja bi evidentirala ko je je bila poslednja osoba koja je preuzela podatke. Stoga je nemoguće utvrditi ko je preuzeo informacije za pisma kandidata za gradonačelnika.

71 Službena internet stranica Zavoda za bezbednost informacionih sistema, dostupno na: https://www.zsis.hr/default.aspx?id=34

Slučaj iz Hrvatske 2: Baza sa poverljivim podacima Hrvatske radio-televizije na crnom tržištu

Prema Zakonu o Hrvatskoj radio-televiziji, sva fizička i pravna lica u Hrvatskoj koja poseduju TV ili radio prijemnik su obavezna da plaćaju pretplatu. HRT poseduje i vodi registar svojih mesečnih pretplatnika u Republici Hrvatskoj. Taj registar nije javno dostupan. Pošto sadrži lične podatke korisnika, kao što su ime i prezime, adresa, lični (osobni) identifikacioni broj (OIB), itd., vođenje i korišćenje tog registra su zaštićeni odredbama zakonskih propisa o bezbednosti ličnih podataka. Na osnovu informacija iz javno dostupnog Centralnog registra, sa podacima o sistemima zbirki ličnih podataka u Agenciji za zaštitu ličnih podataka, registar HRT se nalazi na serveru kome fizički mogu da pristupe samo ovlašćena lica. Ovlašćeni korisnici koriste podatke iz registra putem aplikacije, svog korisničkog imena i lozinke ili sertifikata. Aplikacija je dostupna preko lokalne mreže i interneta, a koriste se tuneli zaštićenih podataka. I na kraju, u sobi sa serverom nalaze se i rezervne kopije u sefu.

U ovom slučaju, IT je zloupotrebljena za namerno umnožavanje i nezakonitu prodaju podataka od strane zaposlenog u HRT koji je ili imao pristup registru ili je poznavao nekoga sa pristupom registru. Na taj način je došlo do kršenja svih gore navedenih mera zaštite, kao i odredbi Opštih pravila rada i ponašanja zaposlenih u HRT, prema kojem zaposleni u HRT moraju da rade u skladu sa najvišimposlovnim standardima i osnovnim etičkim standardima, koji se temelje na nekoliko vrednosti, uključujući poverljivost i zaštitu podataka, u skladu sa važećim zakonskim propisima i opštim pravilima. Ti standardi očigledno nisu primenjeni.

Slučaj iz Hrvatske 3: U potrazi za veteranima

Reč je o primeru zloupotrebe službenog položaja. Očigledno je neko iz Kancelarije za odbranu uzeo podatke, objavio ih, dao, ili čak prodao, nekome ko ih je potom objavio. Postoje brojni različiti razlozi za objavljivanje registra, od političkih sporenja do uzvišenih motiva, kao što je pokušaj da se poboljša transparentnost. Ipak, nema sumnje da je glavni razlog zašto se to desilo to što nije bilo minimuma protokola bezbednosti u postupku rada sa podacima koji su se dostavljali kancelarijama za odbranu u različitim hrvatskim gradovima.

Slučaj iz Hrvatske 4: Uz malu pomoć državnih službenika, 68 hrvatskih pasoša prodato kriminalcima; slučaj 5: Policajac uhvaćen dok je unosio falsifikovane podatke u informacioni sistem policije; slučaj 6: Policajci brisali saobraćajne prekršaje iz evidencije i otkrivali poverljive podatke: prihvatali čak i pečeno jagnje i 20 litara vina kao mito!; i slučaj 7: Slučajno uhvaćeni u otkrivanju poverljivih podataka o automobilima i njihovim vlasnicima!

„Tajnost, integritet, kontinuirana dostupnost i kontrola podataka i informacija iz informacionog sistema MUP-a, su implementirani kroz određeni broj organizacionih, sistemskih i programskih mera i procedura kao i raspodelom nadležnosti i ovlašćenja. Svi korisnici informacionog sistema MUP-a su u obavezi da primenjuju zaštitu podataka, propisanu Pravilnikom o zaštiti informacionog sistema MUP-a na bazi elektronske obrade podataka, Pravilnikom o bezbednosti i zaštiti službenih podataka MUP-a i drugim internim direktivama i uputstvima kojima su uređene aktivnosti na zaštiti informacionog sistema MUP-a. Odgovornosti radnih mesta službenika definišu nivo dostupnosti podataka".

Slučajevi kao ovi mogu se sprečiti praćenjem prometa podataka i pristupa zaposlenih sistemu podataka, kao i obukama i merama podizanja svesti o rizicima od zloupotrebe IT u svrhe korupcije i merama zaštite. Državni službenici treba da postanu svesni koliko je važno da njihove lozinke ostanu tajna, kao i činjenice da će se svako pristupanje bazi podataka pratiti. Najslabija karika u lancu zaštitnih mera je pojedinac, sa svim njegovim/njenim vrlinama i manama.

Slučaj iz Hrvatske 8: Svake godine nestane 2 miliona evra sa naplatnih rampi

U ovom slučaju, preduzeće Autocesta Rijeka Zagreb d.d. je koristilo internu reviziju IT sistema kao meru zaštite od zloupotrebe IT u svrhe korupcije. Nakon što je sudija doneo poetsku oslobađajuću presudu, a da bi sprečila slične slučajeve u budućnosti i uvela zaštitnu IT meru, uprava HAC-a je odlučila da se postave kamere koje će nadzirati rad zaposlenih na naplatnim rampama. Te kamere neće snimati ni lice niti glasove zaposlenih, već samo njihov radni prostor, ruke i postupak plaćanja/naplate cestarine. Ukupan iznos ove investicije iznosio je 354.000 evra.

Slučaj iz Hrvatske 9: Korumpirani policajci - policajci otkrivali poverljive podatke krijumčarima oružja; i slučaj 10: Policajac osuđen na kaznu zatvora od godinu dana jer je omogućio prijatelju nelegalan ribolov

Ova dva slučaja pokazuju da čak i precizno definisane mere zaštite od zloupotrebe IT u svrhe korpucije možda nisu dovoljne. Naime, u skladu sa važećim zakonskim propisima, Ministarstvo unutrašnjih poslova (MUP) je propisalo razne mere zaštite od zloupotrebe svog informacionog sistema, koji obuhvata veliki broj različitih registara[72]. U skladu sa politikom bezbednosti i činjenicom da su pojedina dokumenta, koja propisuju mere upotrebljene za zaštitu ovog sistema, samo za službenu upotrebu, nije moguće nabrojati sve mere zaštite. Međutim, neka od njih se mogu prepoznati iz raspoložive dokumentacije i medijskih izveštaja, kao što su:

- **Tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe IT sistema.** Ova zaštitna mera odnosi se na najčešću pretnju u umreženom sistemu. Prva linija odbrane od neovlašćenog pristupa i zloupotrebe IT sistema su lozinke. *„Svaki službenik policije ima svoju lozinku s kojom može da pristupi različitim bazama podataka u okviru informacionog sistema policije"*[73], izjavio je ekspert za kriminalistiku Željko Cvrtila. U skladu sa njihovim ovlašćenjima i potrebama, policijskim službenicima se dodeljuje pristup određenim nivoima tajnih podataka. Time dobijaju „pristup najvećem registru ličnih podataka u Republici Hrvatskoj"[74]. U skladu sa odredbama gore navedenh propisa o informacionoj bezbednosti, podaci iz ove baze podataka se mogu koristiti samo za poslovne potrebe.

- **Praćenje prometa podataka i pristupa zaposlenih sistemima podataka.** Međutim, *„jednostavno je vrlo teško to kontrolisati. Koliko ja znam, taj proces se veoma slabo nadzire"*, rekao je ekspert za kriminalistiku Željko Cvrtila. *„Dnevno se proverava nekoliko hiljada predmeta. Iako je zaštićena od hakiranja, ovu bazu nije teško probiti"*, zaključio je[75]. Kao što smo ranije naveli, svakom službeniku policije dodeljen je određeni nivo pristupa podacima putem lozinke koju koristi, ali niko posle ne poreverava sa zaposlenim zašto je tražio određenu informaciju, navodi Cvrtila.

- **Mere obuke i podizanja svesti za državne službenike o rizicima od zloupotrebe IT u svrhe korupcije i zaštitnim merama.** Zaposleni u Ministarstvu unutrašnjih poslova učestvuju u različitim projektima čiji je cilj obuka i podizanje svesti o rizicima od zloupotrebe IT u svrhe korupcije i zaštitnim merama. Primeri tih zaštitnih mera od zloupotrebe IT u svrhe korupcije su dva projekta čiji je cilj jačanje administrativnih

72 Spisak svih registara MUP-a je dostupan na: 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

74 Potrka, Nikola (2013) Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. Policijska sigurnost 22(4): 509-521

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

kapaciteta Ministarstva u oblasti zloupotrebe IT: Jačanje administrativnih kapaciteta Ministarstva unutrašnjih poslova u suzbijanju kibernetičkog kriminala (projekat vredan 700.000 evra) i Regionalna saradnja i krivično pravosuđe: jačanje kapaciteta u suzbijanju kibernetičkog kriminala (projekat iznosi 2.777.778 evra), kao i radionice o forenzičkim mrežama koje organizuju Ministarstvo unutrašnjih poslova i Hrvatska akademska i istraživačka mreža.

- **Etički kodeks.** Prema Etičkom kodeksu *„svaki zaposleni je odgovoran za etičko korišćenje datog ovlašćenja za pristup ličnim podacima iz baza podataka policije*"[76]. Zaposleni Ministarstva unutrašnjih poslova su obavezni da postupaju u skladu sa Etičkim kodeksom. Građani mogu da prijave neetičko ponašanje zaposlenih u državnoj upravi službenicima za etiku.

- **Revizija IT sistema**. U skladu sa Uredbom o internoj organizaciji Ministarstva unutrašnjih poslova (Narodne novine br. 70/12, 140/13), za revizije informacionog sistema policije zadužene su dve interne organizacije. Jedna je Samostalna služba za informacionu bezbednost, koja vrši praćenje organizacije, realizacije i efikasnosti propisanih mera i standarda informacione bezbednosti, a druga je Samostalna služba za internu reviziju, koja vrši revizije informacionog sistema.

- **Zakonodavne mere zaštite**. Članovi 266 do 273 Krivičnog zakonika (Narodne novine, br. 125/11, 144/12) definišu krivična dela protiv računarskih sistema, programa i podataka: neovlašćen i nezakonit pristup računarskim sistemima ili računarskim podacima (upad ili „hakovanje" računara), ometanje rada računarskog sistema; oštećenje računarskih podataka, neovlašćeno presretanje računarskih podataka, računarsko falsifikovanje, računarska prevara, i zloupotrena uređaja. Prema krivičnom zakoniku, teškim krivičnim delima protiv računarskih sistema, programa i podataka se smatraju ona koja su usmerena protiv računarskih sistema i računarskih podataka u vlasništvu državnih i lokalnih organa, kao i javnih preduzeća. I na kraju, Zakonik obuhvata krivična dela povezana sa dečijom pornografijom putem računarskih sistema i računarsko nasilje.

Još je jednom važno istaći da su gore navedene mere zaštite samo jedan deo mreže zaštitnih mera koje se primenjuju u Ministarstvu unutrašnjih poslova. Informacije o drugim merama nisu dostupne javnosti iz razloga bezbednosti.

Gore opisani slučajevi pokazuju da je, bez obzira na zakonodavni okvir, propisane procedure, Etički kodeks i razne mere zaštite, zloupotreba IT sistema i dalje moguća. Najslabija karika procesa zaštitnih mera je pojedinac sa svim svojim vrlinama i manama. Teško je čak i zamisliti zaštitnu meru koja bi mogla da garantuje ponašanje u kojem ne bi bilo korupcije.

76 Potrka, Nikola (2013) Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. Policijska sigurnost 22(4): 509-521

Slučaj iz Hrvatske 11: Viši inspektor zloupotrebio poverljive podatke kako bi pobedio na lokalnim izborima

U skladu sa važećim zakonskim propisima o informacionoj bezbednosti, Ministarstvo finansija je propisalo razne mere za zaštitu od zloupotrebe podataka poreskih obveznika iz svojih informacionih sistema. Ovde nije moguće navesti sve te mere, zbog politike bezbednosti i činjenice da su dokumenta, koja propisuju mere upotrebljene za zaštitu tog sistema od zloupotrebe, samo za službenu upotrebu, kao što smo naveli u prethodnim slučajevima. Međutim, one koje su saopštene već su navedene ranije u slučaju 10.

U ogromnom organizacionom sistemu, kao što je Ministarstvo finansija, koji zapošljava preko devet hiljada ljudi i sa organizacionim jedinicama raspoređenim širom zemlje, pitanjima politke bezbednosti se bavi nekoliko organizacionih jedinica:

- Sektor za informatiku u okviru Glavnog sekretarijata. Ovaj sektor, između ostalog, vrši poslove organizovanja, uspostavljanja i održavanja jedinstvenog informacionog sistema za sedište Ministarstva. Sektor vodi računa o delotvornom i tačnom korišćenju informaciono-komunikacionih resursa, organizuje i upravlja procesom razvoja, analize i vraćanja rezervnih kopija podataka, prati bezbednost komunikacija i sprovodi mere zaštite informacionog sistema.
- Služba za informacioni sistem u okviru Poreske uprave, između ostalog, obavlja planiranje, razvoj i korišćenje informacionog sistema i edukuje korisnike o sistemu IT.
- Služba za informacioni sistem u okviru Carinske uprave, između ostalog, vrši planiranje, upravljanje, nadzor i koordinaciju razvoja, nabavke i funkcionisanja poslovnih aplikacija, IT servisa i tehnologija, izrađuje i sprovodi politike zaštite i dodele prava za pristup informacionom sistemu, utvrđuje mere i kvalitet usluga, obezbeđuje izradu rezervnih kopija u informacionom sistemu, planira finansijska sredstva za licence, razvoj i održavanje informacionog sistema, izrađuje strategiju za razvoj IT sistema i edukuje korisnike o IT sistemu Carinske uprave.
- Služba za razvoj i podršku operativno-informacionom sistemu Državnog trezora, između ostalog, obezbeđuje kontinuitet i stabilnost te potreban nivo zaštite poslovnih procedura u Državnom trezoru, obavlja zadatke definisanja, optimizacije, analize, unapređivanja i standardizacije poslovnih procedura, kao i zadatke na autorizaciji, bezbednosti i zaštiti podataka.
- Odsek za strateške analize i informacioni sistem Kancelarije za sprečavanje pranja novca, između ostalog, projektuje i razvija informacione sisteme i podsisteme ove kancelarije, predlaže podzakonska akta i interne propise u oblasti sistemskih podataka i zaštite evidencije u kancelariji, održava i nadzire sistem podataka i zaštitu evidencije koju vodi Kancelarija.

Još jednom je važno istaći da su navedene zaštitne mere samo deo mreže zaštitnih mera koje primenjuje Ministarstvo unutrašnjih poslova ali koje, iz bezbednosnih razloga, nisu u potpunosti dostupne javnosti.

Međutim, kao i u prethodnim slučajevima, bez obzira na zakonodavni okvir, propisane procedure, Etički kodeks i razne mere zaštite, zloupotreba IT sistema je i dalje moguća. Najslabija karika procesa zaštitnih mera je pojedinac sa svim svojim vrlinama i manama. Teško je čak i zamisliti zaštitnu meru koja bi mogla da garantuje ponašanje u kojem ne bi bilo korupcije.

Slučaj iz Hrvatske 12: Ni dana svog života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!

Mere zaštite napravljene da spreče zloupotrebu registra lica koja imaju penzijsko osiguranje i glavnog registra korisnika prava iz penzijskog osiguranja u okviru HZPO su: 1) praćenje hronologije menjanja podataka (koristeći korisničko ime i datum); 2) politika odobrenja za pristup podacima u skladu sa radnim mestom, kao i korišćenje modernih, hardverskih i softverskih mera za zaštitu. Pored ovih glavnih zaštitnih mera, takođe postoje: 3) odredbe važećih zakonskih propisa o zaštiti ličnih podataka, i 4) odredbe Etičkog kodeka i interna revizija. Međutim, slučaj kao što je ovaj potvrđuje da sve ove zaštitne mere i dalje mogu prekršiti.

U protekle dvije godine, HZPO je postao jedna od prvih institucija koja učestvuje u projektu integracije sistema ličnog (osobnog) identifikacionog broja (OIB), zajedno sa Poreskom upravom Ministarstva finansija, Ministarstvom javne uprave i Ministarstvom unutrašnjih poslova. *„Cilj uvođenja OIB-a bio je da se stvori jedinstveni identifikator osoba, koji bi bio zakonski prihvaćen od strane svih javno-pravnih organa Republike Hrvatske. Stvaranjem jedinstvenog identifikatora osoba u svim službenim evidencijama kao rezultat se stvaraju i preduslovi za informatičku razmenu podataka između javno-pravnih organa. Jedino informatičkom razmenom podatka javno-pravni organi ekonomično i efikasno razmenjuju potrebne podatke iz službenih evidencija za pravovremeno i dosledno sprovođenje svih upravnih, poreskih i krivičnih postupaka"*[77]. Imajući to u vidu, OIB je prepoznat kao snažan instrument koji će, između ostalog, omogućiti sistematičnu borbu protiv korupcije.

Pre integrisanja u mrežu razmene OIB, HZPO je funkcionisao poput nekog ostrva unutar državne uprave. Imao je sopstvenu bazu podataka korisnika i redovno im je isplaćivao njihove penzije. Pošto razmena podataka između javno-pravnih tela nije bila moguća, nakon što bi član porodice preminuo ostali članovi porodice imali su obavezu da donesu izvod iz matične knjige umrlih u regionalnu podružnicu HZPO, organ koji bi isplatio peziju sada preminulom. Ovaj postupak stvarao je prostor za moguće prevare. Ako niko ne bi poneo izvod iz matične knjige umrlih u regionalnu podružnicu HZPO, porodica bi mogla da nastavi da prima penziju.

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

Međutim, od septembra 2013. godine, integracija HZPO u mrežu OIB je zatvorila ovu prazninu. Pošto je posedovanje OIB-a preduslov za rezmenu podataka između javno-pravnih organa, prvi korak HZPO-a je bio da obezbedi da svi njegovi korisnici imaju OIB. Na taj način je otkriveno da 125.867 penzionera, od ukupno 1,2 miliona, nije imalo OIB. Drugi korak je bio uskraćivanje mogućnosti primanja penzije preko pošte, već isključivo preko ličnog računa u banci. Ako su korisnici HZPO želeli da nastave da primaju penziju, bili su obavezni da HZPO dostave svoj OIB.

Broj penzionera bez OIB se u aprilu 2014. godine smanjio na 49.586 a reč je uglavnom o stranim korisnicima. Dodatnom razmenom podataka sa Poreskom upravom Ministarstva finansija, Ministarstva uprave i Ministarstva unutrašnjih poslova, 8. aprila 2014. godine obustavljena je isplata 9.593 penzije – 9.108 iz inostranstva i 485 iz Hrvatske. HZPO još uvek pokušava da utvrdi razloge zašto im ovi penzioneri nisu dostavili OIB. *„Jesu li ti korisnici uopšte u Hrvatskoj, jesu li uopšte među živima, podiže li neko umesto njih penziju i time nezakonito dobiva sredstva”*, izjavio je ministar rada i penzijskog sistema, g-din Mirando Mrsić i dodao: „*Je li tu ima prevara, jesu li oni uopšte u Hrvatskoj, gdje te penzije idu, tako da želimo da se te stvari srede. Napominjem da to nisu mala sredstva, to je* ***preko 127 miliona kuna*** *i želimo da se ta sredstva isplaćuju onima koji na to imaju pravo”*[78].

Integracija HZPO u mrežu OIB je do sada pokazala da je 26 porodica nastavilo da prima penzije pokojnih članova porodice. Među njima je bio slučaj u kojem je poštar redovno donosio penziju porodici čoveka koji je umro pre 20 godina! Samo zbog tog jednog slučaja država je pretrpela gubitak od 65.000 evra. Sa integracijom u sistem OIB, slučajevi kao što su ovi prethodno opisani nisu više mogući, pošto se razmenom podataka između javno-pravnih organa sakupljaju i upoređuju podaci i nadležni organi automatski obaveštavaju o neusklađenosti podataka.

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

Kosovo

Pripremili Hasan Preteni i Driart Elshani

Uvod u primere mera zaštite od zloupotrebe IT u svrhe korupcije

Organi i institucije iz javnog sektora se oslanjaju na sisteme informacione tehnologije (IT) za vršenje svojih operativnih poslova, a mnoge i za pružanje svojih usluga. Važno je obezbediti da informacije koje se održavaju u ovim sistemima budu tačne i potpune. Takođe je od suštinskog značaja da te informacije budu lako dostupne za legitimne namene i da istovremeno budu zaštićene od zloupotrebe. Na Kosovu postoji samo nekoliko elektronskih registara pa je stoga veoma malo slučajeva zloupotrebe IT u svrhe korupcije jer nema prostora za menjanje elektronskih podataka. Umesto toga, slučajevi koje smo odabrali uopšteno ilustruju nedostatak mera zaštite od zloupotrebe podataka i sistema IT.

Svi slučajevi izloženi u poglavlju 1 ove studije ukazuju na važnost da svaka odgovarajuća institucija uvede i primeni kako administrativne (ili zakonodavne) tako i tehničke mere zaštite. Štaviše, ono što smo naučili iz svakog od pomenutih slučajeva je da mere zaštite ili nisu bile uvedene ili se nisu poštovale. Čak i kada su propisane, zaštitne mere nisu bile potpune ili su im nedostajale jasne definicije postupaka i uloge da se ublaže rizici od zloupotrebe podataka i opštih sistema informacione tehnologije. Kosovo mora napornije da radi na utvrđivanju i realizaciji tih mera zaštite, naročito kad se ima u vidu da će Kosovo uvesti brojne IT sisteme u budućnosti, te stoga mora da smanji rizike od zloupotrebe podataka i sistema IT. Kosovo još uvek nije preduzelo konkretne radnje da pitanju zaštitnih mera pristupi na odgovarajući način.

Mere zaštite predstavljene u ovom tekstu bi ublažile te rizike i sprečile zloupotrebu sistema informacionih tehnologija. U budućnosti će sve biti digitalno, tj. upotreba papira biće ograničena, pa se otuda mogu javiti novi oblici zloupotrebe koje treba rešavati različitim metodama. Te metode bi se oslanjale na mere zaštite predstavljene ovde.

U ovoj studiji smo predložili konkretne mere za zaštitu integriteta podataka i integriteta IT sistema od moguće zloupotrebe od strane ljudi. Izneli smo predloge za opšte smernice i mehanizme za elektronske sisteme. Te mere zaštite i smernice treba primeniti u svim institucijama.

Ovi standardi i politike su kreirani da zaštite IT sisteme i podatke od uništenja, menjanja ili falsifikovanja. Zaštitne mere koje predlažemo u poglavlju 2 ove studije mogu da se usvoje u formi politike za ceo spektar institucija u cilju zaštite njihovih IT sistema od potencijalnih zloupotreba.

- U smislu tehničkih mera zaštite, pored centralizacije pojedinih IT sistema, sve ostale tehničke mere zaštite su očigledno nedostajale. Nemamo informacije da li su uvedene dodatne tehničke mere zaštite. Međutim, sada znamo da se u nekim institucijama i organima analiziraju i procenjuju opšta primena i postupci odobravanja.

- U smislu organizacionih i proceduralnih zaštitnih mera, one nisu uvođene. Na primer, uloge i nadležnosti su mogle da budu jasno utvrđene ili je moglo da se uvede načelo „više očiju". Dodatne zaštitne mere ovakve vrste nisu uvedene.
- U smislu praćenja pristupa zaposlenih sistemima podataka, organizacije su shvatile iz ovog slučaja da je takve mere potrebno uvesti. Neke od tih mera, kao što je praćenje ko pristupa sistemima podataka, su sada dostupne.
- U smislu obuke i mera na podizanju svesti, takve mere nisu postojale i ne postoje ni sada. Ne postoje čak ni planovi da se uvedu takve mere.
- U smislu revizije, većina organizacija nije imala nikakvu reviziju kada je ovaj slučaj otkriven i nemamo informacije da li takve mere postoje danas. Pojedine organizacije su od tada obavile ukupnu reviziju bezbednosti i sada su u postupku sprovođenja preporuka. Međutim, te se preporuke odnose samo na bezbednost kao što je odbrana od računarskih napada i ne bave se pitanjima koja su proizašla iz ovog slučaja.
- U smislu zakonodavnih mera zaštite, u vreme kada se desio ovaj slučaj nije ih bilo.

Osim toga, najznačajnija stvar koju smo naučili iz ovog slučaja je da razmena podataka može da bude od ključnog značaja u borbi da se spreči njegovo ponavljanje. Da su sistemi bili interoperabilni, to bi ubrzalo proces. Na primer, interoperabilni postupak potvrđivanja poreske dokumentacije bi značajno otežao njeno falsifikovanje.

Mere protiv zloupotrebe IT na Kosovu

Potrebno je uvesti zaštitne mere u cilju adekvatnog otkrivanja, praćenja i preduzimanja koraka protiv slučajeva korupcije. Te zaštitne mere treba da budu široke i različite, uključujući: tehničke mere zaštite, organizacione i proceduralne mere zaštite, praćenje prometa podataka i pristupa zaposlenih sistemima podataka, obuke i mere podizanja svesti, internu i eksternu reviziju i zakonodavne mere zaštite.

Štaviše, bilo bi preporučljivo da se osnuje posebno institucionalno telo u zemlji da bi se zaštitio integritet podataka i sistema informacione tehnologije i sprečila krivična dela. Važno je reći da takva institucija ne postoji na Kosovu. Na Kosovu postoji specijalizovana Agencija za zaštitu privatnosti i podataka, ali ova agencija deluje samo kao neka vrsta organizacije koja prati pitanja iz oblasti privatnosti. Njene nadležnosti nisu dovoljne i ne uključuju obavezu obezbeđivanja zaštitnih mera povezanih sa zloupotrebom informacione tehnologije.

Dakle, uopšte ne postoji institucija koja se bavi definisanjem i sprovođenjem zaštitnih mera i standarda iz ove oblasti. Brojni slučajevi zloupotrebe informacione tehnologije i dalje su prisutni, a često ne budu uopšte otkriveni. Kada govorimo o merama zaštite, vredi pomenuti da te mere mogu biti dvostruke: tehničke i administrativne.

Administrativne mere zaštite mogu da budu u obliku zakona, normativnih akata i administrativnih propisa koji sankcionišu sva nedela povezana sa integritetom podataka i

integritetom sistema informacione tehnologije uopšte. Sve institucije bi poštovale jasnu infrastrukturu propisa utvrđenu zakonom.

Tehničke mere zaštite bi mogle da budu u obliku Standardnih operativnih procedura (SOP) koje svaka institucija treba da primeni da bi se zaštitila od zloupotrebe podataka i opštih zloupotreba sistema informacione tehnologije. Svaka institucija bi radila po kontrolnoj listi SOP koja garantuje njenu maksimalnu zaštitu i otpornost na takva krivična dela. Postojeća administrativna uputstva ne sadrže nikakve SOP.

U smislu administrativnih mera zaštite, Kosovo je usvojilo set zakona, strategija i administrativnih uputstava (normativnih akata) koja se odnose na korišćenje informaciono-komunikacionih tehnologija, ali se zakonodavna infrastruktuara do sada nije na odgovarajući način bavila pitanjem integriteta podataka i zloupotrebom sistema informacione tehnologije u konkretnom ili opštem smislu.

Računarski kriminal

Kosovo još uvek nema Tim za odgovor na računarske incidente (CERT), koji bi takođe mogao da bude nadležan za zaštitu IT sistema. Predviđeno je da CERT bude formiran u bliskoj budućnosti. Međutim, CERT bi još uvek bio nedovoljan, jer po pravilu CERT bi delovao samo reaktivno u smislu zaštite od zloupotrebe, umesto da obezbeđuje proaktivne preventivne mere.

Ostale mere

U borbi protiv zloupotrebe IT u svrhe korupcije mogu se koristiti i druge mere. Na primer, razmena podataka između javnih organa i primena sveobuhvatnog okvira ineroperabilnosti mogle bi da pomognu u sprečavanju nekih slučajeva, na primer slučaja 2. Posebne mere u IT sistemima javnih nabavki, kao što su elektronske nabavke, mogle bi se takođe pokazati relevantnim. Kosovo je u procesu uvođenja elektronskog sistema javnih nabavki. Mere kao što su otvoreni vladini podaci možda bi takođe bile poželjne. To bi podstaklo razmenu podataka između javnih organa. Kosovo je u početnoj fazi ovog procesa.

ZAKONI, STRATEGIJE I ADMINISTRATIVNA UPUTSTVA U VEZI ICT NA KOSOVU

Zakoni

Zakoni o informaciono-komunikacionim tehnologijama (ICT) koji su se od 2009. do danas primenjivali na Kosovu su dati u sledećoj tabeli:

Tabela 2 Zakoni koji su primenjivani, menjani i dopunjavani od 2009. do 2014. godine[79]

Br.	Naziv zakona	U akcionom planu?	Zakon br.	Datum usvajanja	Akt i datum proglašenja
1	**Zakon o zaštiti ličnih podataka**	DA	**03/L-172**	29.04.2010.	Odluka br. DL-020-2010, od 13.05.2010.
2	**Zakon o sprečavanju i borbi protiv računarskog kriminala**	DA	**03/L-166**	10.06.2010.	Odluka br. DL-028-2010, od 02.07.2010.
3	**Zakon o pristupu javnim dokumentima**	DA	**03/L-215**	07.10.2010.	Odluka br. DL-063-2010, od 01.11.2010
4	**Zakon o uslugama informacionog društva**	DA	**04/L-094**	15.03.2012.	Odluka br. DL-010-2012, od 02.04.2012
5	**Zakon o sprečavanju sukoba interesa u vršenju javnih funkcija**	DA	**04/L-051**	31.08.2011.	Odluka br. DL-029-2011, od 31.08.2011
6	**Zakon o državnom arhivu**	DA	**04/L-088**	15.02.2012.	Odluka br. DL-007-2012, od 01.03.2012.
7	**Zakon o upravnim sporovima**	DA	**03/L-202**	16.09.2010.	Proglašen, u skladu sa članom 80.5 Ustava Republike Kosovo, od 06. 10.2010.
8	**Zakon o visokom obrazovanju u Republici Kosovu**	DA	**04/L-037**	29.08.2011.	Odluka br. DL-036-2011, od 31.08.2011.

79 Podaci Skupštine Kosova* - Odeljenje za pravnu podršku i postupak (AK – DSLP) (2014)

Strategije

Do sada su usvojene sledeće strategije:

- Nacionalna strategija za informaciono društvo 2006-2012
- Strategija za elektronsku upravu 2009-2015
- Strategija elektronskog učenja za Kosovo 2010-2015 sa glavnim ciljem da elektronsko učenje postane integralni deo celokupnog sistema obrazovanja
- Kosovski strateški plan obrazovanja 2011-2016, koji sadrži osam prioritetnih programa uključujući Izgradnju kapaciteta i Informaciono-komunikacionu tehnologiju
- Strategija razvoja douniverzitetskog obrazovanja 2007-2017

Međutim, nijedan od ovih zakona ili strategija ne bavi se konkretno integritetom podataka ili zloupotrebom sistema informacione tehnologije.

Administrativna uputstva

Na kraju, u oblasti IT do sada su usvojena sledeća administrativna uputstva (AU):

1. A.U. br. 02/2010 za upravljanje informacionom bezbednošću
2. A.U. br. 01/2010 o bezbednosti i pristupanju bazama podataka
3. A.U. br. 04/2010 za korišćenje službene elektronske pošte u institucijama Kosova
4. A.U. br. 01/2011 za upravljanje i korišćenje interneta u institucijama Kosova
5. A.U. br. 07/2008 za jačanje transparentnosti i standardizaciju internet stranica institucija Kosova
6. A.U. br. 03/2010 za korišćenje hardvera i softvera
7. A.U. br. 02/2011 za portal Vlade Republike Kosovo

Analiza sadržaja ovih dokumenata takođe otkriva sledeća pitanja:

- AU o informacionoj bezbednosti je formalno objavljeno 2010. godine ali nije bilo programa koji bi obezbedio da ga sve strane prihvate i shvate svoje nadležnosti i obaveze;
- AU o informacionoj bezbednosti opisuje tehničke politike, ali ne definiše okvir sistema upravljanja, uključujući uloge, nadležnosti i ovlašćenja;
- Ne postoji jasna veza između različitih administrativnih uputstava ili kako su definisana da bi se ispunili određeni zahtevi.

Osim toga, ova administrativna uputstva samo se delimično bave pitanjima kao što su prava pristupa bazama podataka i internetu, i umesto toga uglavnom su neodređena. Štaviše, njihovo sprovođenje je prilično složeno, pošto se nijedna konkretna institucija ne bavi pitanjem da li se ona poštuju. Najvažnije od svega, iako je opšte mišljenje da Kosovo ima dobru zakonsku infrastrukturu, vidi se da mnoge stvari još uvek nedostaju i/ili da su u velikoj meri nepotpune. Kosovo mora još uvek da se potrudi da zakonom propisane mere zaštite budu jasno napisane, usvojene i da se primenjuju u praksi.

Tehničke mere zaštite

Mere zaštite se do sada uglavnom svode na jednostavnu zaštitu lozinkom koju koriste pojedinačni korisnici, šifrovanje podataka u pojedinačnim slučajevima i pokušaje da se serveri zaštite od fizičkog ometanja. Kosovu trenutno nedostaju sofisticiranije strategije i standardi za tehničke mere zaštite IT koja se koristi u javnom sektoru.

Makedonija

Pripremili Marjan Stoilkovski i Rozalinda Stojova

Institucionalne mere zaštite

U skladu sa Zakonom o sprečavanju korupcije, 2002. godine osnovana je Državna komisija za sprečavanje korupcije (DKSK), kao nezavisno telo. U članu 1 zakona, DKSK je data nadležnost da primeni mere i sprovodi aktivnosti na sprečavanju korupcije u radu vlade, vršenju javnih ovlašćenja, obavljanju službene dužnosti i sprovođenju politike, zatim mere i aktivnosti na sprečavanju sukoba interesa, kao i mere i aktivnosti na sprečavanju korupcije u poslovima od javnog interesa u organima koji vrše javna ovlašćenja, kao i mere i aktivnosti na sprečavanju korupcije u preduzećima.

Takođe, 2008. godine osnovano je Odelenje za borbu protiv korupcije. Reč je o posebnoj organizacionoj jedinici u okviru Sektora za organizovani kriminal Ministarstva unutrašnjih poslova. U nadležnosti Odelenja za borbu protiv korupcije spada otkrivanje i sprovođenje istrage o svim oblicima korupcije u Republici Makedoniji.

Tehničke mere zaštite od neovlašćenog pristupa i zloupotrebe IT sistema i praćenje protoka podataka i pristupa zaposlenih sistemima podataka

U okviru tehničke specifikacije informacionih sistema, bez obzira da li je njihova izrada ugovorom poverena nekom preduzeću ili se izrađuju u okviru institucije, postoji nekoliko postupaka koje se koriste i primenjuju. Neki od tih postupaka su utvrđeni u skladu sa odgovarajućim zakonom, ali neki od najvažnijih su oni koji su nastali iz prakse umesto da su definisani zakonom. Njihov cilj je da spreče zloupotrebu IT u svrhe korupcije i smatraju se jednim od najvažnijih uslova koji se moraju ispuniti na samom početku provere za prijem radova. Tu spadaju:

- Vođenje evidencije o svakom pristupu, dodavanju, brisanju ili menjanju podataka i dostupnost datoteke evidencije na zahtev u svrhe analize i revizije. Pored vođenja i arhiviranja evidencije, druge aktivnosti nisu dozvoljene.

- Obezbeđivanje različitih nivoa identifikacije i autorizacije. Poverljivost nivoa podataka koji se obrade u sistemu utiče na nivo i složenost procesa identifikacije i autorizacije. U svim sistemima, različite korisničke uloge se definišu u zavisnosti od dodeljenih ovlašćenja, počev od jednostavnog korisničkog imena i lozinke za neke, dok za druge postoje zahtevi korišćenja digitalnih sertifikata ili čak omogućavanje pristupa podacima samo sa određene radne stanice i precizno utvrđene fizičke lokacije.
- U skladu sa Zakonom o elektronskom upravljanju, u slučaju da se razvoj sistemskog pohranjivanja i/ili obrade ličnih podataka ugovorom poveri nekom preduzeću, ali pritom ne isključujući slučajeve razvoja sistema u okviru institucije, jedan od zahteva je da se formiraju razvojna i probna okruženja i koriste probni podaci, dok se stvarni podaci pohranjuju samo u proizvodnom okruženju. Time je omogućen kanalisan i kontrolisan pristup podacima i to samo od strane službeno imenovanih zaposlenih lica.
- Izrada redovnih izveštaja o aktivnostima za različite vrste korisnika i uloga je takođe zahtev kojim se obezbeđuje redovno praćenje korisničkih aktivnosti. Ovi izveštaji se šalju glavnim administratorima i rukovodstvu.
- Jedna od najboljih praksi za većinu lokalnih sistema je slanje obaveštenja glavnom admnistratoru/ima i rukovodstvu putem elektronske pošte ili sms-a u slučajevima kada se otkriju sumljive aktivnosti ili u momentu njihovog izvršenja.
- Da bi se zaštitila internet konekcija sistema prilikom razmene podataka između dva sistema, kao i da bi se sprečilo ometanje razmene podataka, sve institucije uvode/uspostavljaju VPN konekcije koristeći šifrovane podatke.
- U skladu sa radom koji obavljaju, obični službenici koriste radne stanice koje imaju pristup samo podacima za koje je nadležna njihova institucija, te nemaju pristup internetu ili drugim sistemima.
- Sistemi IT u privatnom i javnom sektoru se testiraju na osetljivost i moguće upade u sistem. Iako se testiranje upada u sistem više primenjuje u privatnom finansijskom sektoru, često se dešava da i javni sektor angažuje sertifikovana preduzeća za testiranje upada i da koriste taj metod da spreče neovlašćeni pristup sistemima IT.

Organizacione i proceduralne mere zaštite kao što je „načelo više očiju”

- Prisutan je trend potpisivanja Ugovora o poverljivosti sa ekonomskim operaterima i izvršiocima. Ovi se ugovori dopunjuju izjavama o poverljivosti od obe strane, ugovarača i realizatora, za osobe koje imaju pristup sistemu.
- Fizički pristup u bilo kom trenutku, bez obzira da li tokom realizacije ugovora ili tokom održavanja, je moguć samo nakon dobijanja odobrenja Ministarstva unutrašnjih poslova za svaku osobu za koju se pristup traži.
- U institucijama postoji usvojena praksa dodeljivanja dve osnovne ključne uloge dvema različitim kategorijama zaposlenih lica: tehničkim administratorima i administratorima sadržaja. Tehnički administratori su nadležni za sistem na nivou aplikacije i pored upravljanja sistemom i bazom podataka, zaposleni sa ovom ulogom takođe upravljaju korisnicima i njihovim ovlašćenjima, ali ne i podacima pohranjenim/sačuvanim u bazama podataka. Administratori sadržaja su nadležni za upravljanje podacima pohranjenim u bazama podataka.

Obuka i mere podizanja svesti za državne službenike o rizicima od zloupotrebe IT i zaštitnim merama

Žrtve korupcije mogu biti pojedinačni građanin, preduzeće ili grupa subjekata, ali u nekim slučajevima žrtva je društvo u celini. Borba protiv korupcije je jedan od najvažnijih strateških ciljeva koji su usvojila ministarstva i druge institucije, pokazujući na taj način posvećenost Vlade Republike Makedonije (npr. pogledati Strategiju reforme javne uprave i njen Akcioni plan[80]). Dalje, javni sektor i građani igraju aktivnu ulogu u reformisanju društva, te time dokazuju značaj svoje volje i spremnosti da saznaju više o načinima kako da se spreči korupcija i mogućnostima koje stoje na raspolaganju u pogledu pravnog delovanja. Institucije i javni sektor (NVO) su, stoga, preduzeli sledeće radnje: češća obuka zaposlenih i građana u institucijama koje su osetljivije na korupciju, kampanje podizanja svesti preko različitih kanala, štampanje letaka, bilbordi, kratke TV reklame.

Revizija IT sistema (interne ili eksterne revizije, inicira ih državni organ ili se pokreću nakon nekog izveštaja ili pritužbe građana ili medija)

Iako se interne i eksterne revizije sprovode za veoma mali broj ICT sistema, reč je o jednoj od mogućih mera. Primenjuje se u veoma retkim slučajevima, kao na primer kada sistem obrađuje tajne podatke ili podatke od značaja za državu, i u slučajevima kada se za tu namenu opredeli dovoljan budžet i vreme.

Zakonodavne mere zaštite

Zakon o sprečavanju korupcije usvojen je 2002. godine, što je omogućilo primenu zakonskog okvira u borbi protiv korupcije. Poslednji put je izmenjen i dopunjen 2010. godine, a tim se zakonom:

„uređuju mere i aktivnosti na sprečavanju korupcije u vršenju vlasti, javnih ovlašćenja, službene dužnosti i politike, zatim mere i aktivnosti na sprečavanju sukoba interesa, kao i mere i aktivnosti na sprečavanju korupcije u poslovima od javnog interesa koje obavljaju pravna lica i koji se odnose na vršenje javnih ovlašćenja, kao i mere i aktivnosti na sprečavanju korupcije u trgovačkim preduzećima." (Član 1).

Zakon je uveo sistem integriteta (pakt o integritetu) i zaštitu lica koja prijavljuju korupciju.

- **Zakon o elektronskom upravljanju** opisuje standarde koje treba zadovoljiti prilikom razvoja informacionih sistema koji komuniciraju i razmenjuju podatke i dokumenta sa informacionim sistemima drugih institucija u cilju sprovođenja upravnog postupka[81]. Podzakonski akt za prepoznavanje jedinstvenog okruženja i elektronske komunikacije između institucija u cilju razmene podataka i dokumenata, sa kasnijim

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

smernicama za tehničke uslove, način rada, komunikaciju sa klijentom i preporukom za korišćenje sistema interoperabilnosti, opisuje:

- tehničke zahteve u pogledu hardverske i softverske infrastrukture klijenata koji međusobno komuniciraju;
- probno okruženje;
- održavanje i razvoj internet usluga;
- protokole elektronske pošte;
- pristupanje podacima koji su predmet razmene;
- bezbednost i integritet podataka, a sa sledećim smernicama su uvedene brojne kontrolne mere iz ISO 2700 serije standarda;
- strukturu podataka i dokumenta koji su predmet razmene; i
- planiranje osnovnih elemenata arhitekture za komunikaciju sa sistemom interoperabilnosti.

- **Zakon o elektronskoj komunikaciji** propisuje zaštitu prava korisnika, uključujući krajnje korisnike sa posebnim društvenim potrebama i obezbeđuje poverljivost komunikacija.
- **Zakon o zaštiti ličnih podataka**, poslednji put izmenjen i dopunjen 2012. godine, je usaglašen sa važećim direktivama EU i primenjuje se na potpuno ili delimično automatizovanu obradu ličnih podataka. Između ostalog, opisuje načine obrade ličnih podataka i utvrđene potrebne tehničke mere za zaštitu obrade ličnih podataka.
- **Zakon o upotrebi podataka iz javnog sektora**, koji je usvojen 2014. godine, je odraz aktivnosti preduzetih tokom Inicijative partnerstvo za otvorenu Vladu. Zakon je usklađen sa Direktivom 2003/98/EC Evropskog parlamenta i Evropskog saveta o ponovljenoj upotrebi informacija iz javnog sektora. „Ovaj zakon uvodi obavezu organa i institucija u javnom sektoru u pogledu javnog objavljivanja podataka koji nastanu tokom vršenja njihovih ovlašćenja u skladu sa zakonom, kako bi se omogućila upotreba tih podataka od strane preduzeća ili pojedinaca u cilju stvaranja novih informacija, sadržaja, aplikacija ili usluga.” Jedan od ciljeva je da se podstakne „povećana odgovornost i transparentnost javnog sektora”, što je jedan od instrumenata za sprečavanje korupcije.
- **Zakon o finansijskoj disciplini**, koji je usvojen 2013. godine, uređuje pravovremeno ostvarivanje finansijskih obaveza koje nastaju po osnovu realizacije poslovnih transakcija između ekonomskih operatera u privatnom sektoru ili između subjekata javnog sektora i ekonomskih operatera iz privatnog sektora, u cilju sprečavanja neispunjavanja predviđenih novčanih obaveza u skladu sa uslovima iz zakona. Za svakog ugovarača koji ne postupi u skladu sa ovom obavezom utvrđene su novčane kazne. Sprovođenje kontrolisanog plaćanja novčanih obaveza predstavlja snažnu podršku aktivnostima usmerenim na borbu protiv korupcije.
- Poslednje izmene i dopune **Zakona o javnim nabavkama** su usvojene 2014. godine i obuhvataju nekoliko velikih promena. Pre nabavke robe i usluga koje imaju veću procenjenu vrednost od one utvrđene na mesečnom nivou za male nabavke, naručioci su obavezni da obave istraživanje tržišta. To znači obezbeđivanje određenog broja dobavljača (u zavisnosti od procenjene vrednosti) koji mogu da prihvate ponuđene uslove. Ako je dobavljača sposobnih da isporuče traženu robu ili usluge,

a koji ispunjavaju uslove da učestvuju na tenderu, manje od propisanog broja naručilac mora da dobije pisanu saglasnost od Saveta za javne nabavke, tela koje je osnovano izmenama i dopunama zakona.

- U skladu sa nacionalnim zakonodavstvom o tajnim podacima, svaki IT sistem koji sadrži ili obrađuje tajne podatke mora biti akreditovan od strane lica iz Nacionalne direkcije za tajne podatke sertifikovanih za akreditaciju. Prilikom razvoja IT sistema za obradu tajnih podataka, usvajaju se posebne direktive za tehničke karakteristike hardvera i softvera koji će se koristiti u IT sistemu za poverljive informacije.
- Pored ostalih zakonskih akata, **Zakon o tajnim podacima** na nacionalnom nivou se koristi kao mera zaštite od neovlašćenog pristupa i zloupotrebe IT sistema.

OSTALE MERE

Mere zaštite u postupku javnih nabavki i za finansijsku disciplinu

Pored gore navedenih, uvedeni su i sledeći zahtevi koji pomažu u sprečavanju korupcije u postupcima javnih nabavki:

- Tehničke specifikacije ne smeju da sadrže nazive brendova, čak ni kada su povezani sa glavnim opisom, a detaljne zahteve iz specifikacije treba da zadovolji više od jednog dobavljača, osim u slučajevima propisanim zakonom kada se primenjuje prethodno definisan proces;
- Sve javne nabavke državnih i javnih institucija moraju se sprovesti kroz sistem javnih nabavki.

Karakteristična primena softvera kao zaštitna mera

Ministar rada i socijalne politike (MRSP) je izjavio da je Ministarstvo sprovelo niz aktivnosti i analiza u oblasti prava iz socijalne zaštite. Dodao je da su sa primenom novog softvera za socijalno staranje otkriveni slučajevi u kojima su korisnici zloupotrebljavali sistem i davali lažne informacije. Dublja analiza je otkrila da te zloupotrebe ne bi bile moguće da nije bilo saradnje sa nekoliko zaposlenih. Kao rezultat toga, pokrenute su interne revizije i praćenje rada centara za socijalni rad i u nekoliko slučajeva su pronađeni dokazi o zloupotrebi prava iz socijalne zaštite, a protiv svih koji su prekršili zakon podnete su krivične prijave. Dokazano je da je devet građana iz grada A, zaposlenih kao službenici u javnoj instituciji „Centar za socijalni rad" u gradu A, zloupotrebilo svoj službeni položaj i pomoglo određenom broju građana da nezakonito ostvare prava iz socijalne zaštite.

U slučajevima koji su pre bili osetljivi na korupciju, sada se koriste IT sistemi kojima se dele CEMT licence, socijalni stanovi, sobe u studentskim i učeničkim domovima, ili se pružaju druge usluge. Jedan od najvažnijih servisa je elektronska raspodela predmeta

sudijama, što je prepoznato i predstavljeno kao mera 11 u Strategiji reforme javne uprave sa Akcionim planom[82].

Za anonimno prijavljivanje korupcije, koja se desila ili je u toku, postoji elektronski obrazac na portalu Kancelarije za javne prihode (KJP). Reč je o najčešće korišćenom obrascu te vrste. Anonimnost pošaljioca je zagarantovana, jer je napravljeno da njegova ili njena IP adresa bude nevidljiva za korisnike KJP.

Otvorena Vlada kao zaštitna mera

Otvaranje javnih podataka i njihovo objavljivanje na portalima institucija u nekom od formata nivoa 5 zvezdica[83] je kratak opis Inicijative partnerstvo za otvorenu Vladu. Reč je o novom pristupu za aktivnosti usmerene na borbu protiv korupcije koji omogućava svakom subjektu da dobije aktivnu ulogu u sprečavanju i otkrivanju korupcije. Na primer, jedna vrsta podataka koji se objavljuju, ako ih podnesu, su podaci o finansijskom i imovinskom statusu visokih funkcionera.

Kao dodatni dokaz posvećenosti Vlade, 2014. godine usvojen je Zakon o upotrebi podataka iz javnog sektora. Ovaj zakon uvodi obavezu organa i institucija javnog sektora da javno objave podatke koji nastanu u obavljanju njihovih nadležnosti, kako bi se preduzećima i pojedincima omogućilo da koriste te podatke za kreiranje novih informacija, sadržaja, aplikacija i usluga. Zakon takođe propisuje ograničenja za ekskluzivne ugovore u institucijama.

Usaglašeni sa otvorenim podacima, zakoni koji se bave postupkom izdavanja stručnih licenci koji se završava testiranjem, tj. za izvršitelje, forenzičare, procenitelje, notare i druga stručna lica, su usaglašavani prema sledećim načelima: za svaku profesiju treba da postoji skup od 500 prethodno definisanih pitanja koja su javno dostupna na odgovarajućim portalima. Testiranje se vrši elektronskim putem i koristi se samo sistem elektronskog testiranja. Uzorak pitanja na pravom testiranju se bira nasumično u skladu sa određenim kriterijumima, čime se obezbeđuju jednake šanse za sve kandidate. Pored toga, testiranje može da se snima video kamerom ili prenosi putem interneta i može biti poništeno ako se primete ili dokažu nepravilnosti.

Ovo načelo treba primeniti i u postupku zapošljavanja državnih službenika, kao i tokom eksternog testiranja učenika/studenata, ali u tim slučajevima bez video nadzora i pripremom različitih pitanja za svakog učenika/studenta.

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

83 Plan otvorenih podataka od pet zvezdica, kako ga je predložio Tim Berners-Lee, pronalazač globalne računarske mreže (world wide web) i predlagač otvorenih podataka, dodeljuje zvezdice u zavisnosti od toga koliko je format podataka otvoren i kako se povezuje. Jedna zvezdica opisuje objavljivanje podataka na internetu (u bilo kom formatu) u okviru otvorene licence, ali podaci ne moraju da budu strukturirani, mogu da koriste vlastite formate, a ne moraju da koriste URI da se označe stvari i ne moraju da se povezuju sa drugim podacima da bi se dobio kontekst. Jedna zvezdica je najniži nivo otvorenosti podataka.

Crna Gora

Pripremili Dušan Drakić i Ivan Lazarević

Uvod u primere mera zaštite od zloupotrebe IT

Da bi se smanjila zloupotreba podataka moramo kontinuirano da pratimo i razvijamo određene aspekte ICT. Međutim, u užem smislu, zloupotreba podataka na državnom i ponekad na lokalnom nivou je verovatnije posledica moralnog statusa društva, kao i nespremnosti pojedinca da se potčini organizovanom redu i poštovanju propisa. Kvalitetni registri podataka u ICT, definisani u skladu sa međunarodnim standardima, nude priznavanje i zaštitu domaćih i stranih fizičkih i pravnih lica, kao i pokretne i nepokretne imovine na teritoriji države.

Odabrani slučajevi skreću pažnju na potrebu za većim brojem elektronskih registara, koji će nam omogućiti da odredimo mesto porekla podataka, kao i njihovo pohranjivanje u centralizovanu bazu podataka na internetu i omogućiti njihovo korišćenje.

Neophodno je kvalitetnom i pouzdanom ICT infrastrukturom poboljšati i standardizovati međusektorsku razmenu podataka. Važno je modernizovati državnu upravu i proširiti javne usluge namenjene korisnicima, i to povećanjem njihove dostupnosti i bezbednog pružanja kroz više kanala.

Slučajevi takođe ukazuju da postoji potreba da se uspostavi okvir interoperabilnosti koji će stvoriti uslove za unapređenje kvaliteta upravljanja informacijama i razmene informacija između državnih organa i institucija, te omogućiti automatsku razmenu i korišćenje podataka pohranjenih u javnim registrima i drugim informacionim sistemima.

Mere zaštite u primerima iz Crne Gore

Slučaj iz Crne Gore 1: Zloupotreba službenog položaja i falsifikovanje zvaničnih dokumenata

Slučaj falsifikovanog pasoša kome je istekao period važenja i koji je koristilo treće lice pokazuje nedostatke ili grešku u informacionom sistemu Ministarstva unutrašnjih poslova za izdavanje pasoša, koji treba da eliminiše rizike korišćenja i ponovnog izdavanja putničkih isprava kada period važenja istekne. Sistem nije povezao fizičku ispravu (pasoš) sa preslikanom evidencijom iz baze podataka koja sadrži potpuno iste informacije, uključujući fotografiju vlasnika pasoša. Dalje, nije bilo elektronskih tragova u sistemu koji bi identifikovali službenika koji je izdao falsifikovani pasoš.

Slučaj pokazuje nedostatak kako tehničkih tako i zaštitnih mera praćenja/revizije protiv zloupotrebe.

Putničke isprave se koriste u inostranstvu, a slučaj takođe ukazuje na potrebu za elektronskom razmenom podataka i verifikacijom između rezličitih zemalja, kao što je to slučaj između zemalja Šengen zone.

Slučaj iz Crne Gore 2: Upotreba IT podataka sa ciljem nanošenja političke štete

Reč je o slučaju kada je medijima poslat lažan spisak telefonskih poziva iz kojih se navodno vidi da su viši funkcioneri komunicirali sa članovima organizovane kriminalne grupe.

Gore navedeni primer jasno pokazuje da postoji pitanje moguće odgovornosti nadležnih lica u preduzeću operatoru, prvenstveno u pogledu tajnosti, presretanja i zloupotrebe elektronske pošte.

Podaci su ključna imovina nekog preduzeća. Gubitak podataka izlaže preduzeće tužbi i gubitku ugleda. Informacije koje se pohranjuju u bazi podataka su važne. Preduzeća rutinski pohranjuju osetljive, privatne i lične informacije kao što su jedinstveni matični brojevi, kreditne kartice, platni spiskovi i lične informacije, da navedemo samo neke. Preduzeća moraju da održavaju i zaštite ove informacije na poverljiv način, inače bi sebe izložila gubitku ugleda i/ili prihoda.

Operator je obavezan da obezbedi tražene tehničke i organizacione preduslove koji omogućavaju presretanje komunikacija, tj. da omogući nadležnom državnom organu da dođu do sačuvanih podataka o prometu i lokaciji, ali samo u skladu sa sudskim nalogom, ako je to neophodno za sprovođenje krivičnog postupka (u skladu sa Zakonikom o krivičnom postupku) ili iz razloga nacionalne bezbednosti Crne Gore (a naročiti u skladu sa zakonskim propisima koji uređuju rad obaveštajnih službi).

Slučaj nije imao sudski epilog, a nije utvrđena ni objektivna ni subjektivna odgovornost. Stoga nije moguće odrediti koje mere zaštite su nedostajale.

Slučaj iz Crne Gore 3: Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre

Ovaj slučaj se odnosi na nezakonit prenos državnog zemljišta iz opštinskog katastra na treće lice pomoću nezakonitih izmena u katastru. U ovom slučaju je izrađena lažna elektronska potvrda koja se kasnije mogla koristiti u sudskom postupku.

U Crnoj Gori postoji kombinacija različitih elektronskih i fizičkih zemljišnih knjiga. U svakom slučaju, svake godine broj registara se povećava. Pojedini registri su digitalizovani i u nekim slučajevima podaci se mogu deliti elektronskim putem. Ista dokumenta mogu biti različitog porekla, a ponekad je nemoguće utvrditi ko ih je kreirao i ko ima pun pristup dokumentima. U ovom slučaju postoji zahtev da se dokumentacija drži u elektronskom obliku, a pristup registrima je dozvoljen samo ovlašćenim licima.

Kao načelo bezbednosti, zaposleni službenici treba da imaju tačno onaj nivo ovlašćenja za pristup koji im je neophodan za obavljanje njihovih poslova ili zadataka. Dodeljivanje korisničkih ovlašćenja koja prevazilaze njihove potrebe je česta praksa, koja može da dovede do zloupotrebe tih prevelikih ovlašćenja.

Praćenje korisnika pomaže da se obezbedi:

- privatnost podataka, tako da samo autorizovane aplikacije i ovlašćeni korisnici mogu da pristupe osetljivim podacima.
- upravljanje podacima, tako da se ključne strukture i vrednosti baze podataka ne menjaju izvan kontrolnih procedura za njihovo menjanje u preduzeću.

Ovaj slučaj ilustruje šta se dešava kada je praćenje pristupanja sistemu od strane zaposlenih neadekvatno. Dalje, za promene u opštinskom katastru su nedostajale organizacione i proceduralne mere zaštite, kao što je „načelo više očiju”. Nisu vršene dodatne provere o statusu zemljišta i vlasništvu, ni u tehničkom smislu niti od strane drugog zaposlenog u opštinskom katastru ili od strane eksterne revizije.

Slučaj iz Crne Gore 4: Nezakonito izdavanje putnih isprava

U Centru bezbednosti u Podgorici dva zahteva za izdavanje novih pasoša nisu verifikovana od strane službenika koji je radio na njima. Međutim, istražitelji u informacionom sistemu nisu pronašli elektronsku evidenciju o izdavanju pasoša, a sva dokumentacija o skeniranim zahtevima za pasoše je nestala iz prostorije sa spisima.

Ovaj primer pokazuje da u informacionom sistemu nije bilo elektronske evidencije o skeniranim zahtevima za izdavanje pasoša, što bi inače eliminisalo rizik od korišćenja i

izdavanja falsifikovanih dokumenata. Takođe je neophodno poboljšati elektronski sistem bezbednosti koji snima fizički pristup prostorijama u kojima se drže spisi i službena dokumenta.

Računari za upravljanje bazom podataka i informacioni sistem (serveri) treba da budu opremljeni sa:

- sistemom za bezbedno prijavljijvanje i evidentiranje svih pristupa, tako da pristupanje serveru može da se kontroliše i ograniči; i
- mehanizmom za sprečavanje neovlašćenog skidanja i postavljanja prenosivih IT medija, komunikacionih portova ili konekcija za štampanje podataka.

Autentikacija je potvrđivanje identiteta od strane sistema ili baze podataka na osnovu unošenja jedinstvenih ovlašćenja u sistem. Autentikacija doprinosi tajnosti podataka i odgovornosti za aktivnosti obavljene na sistemu putem verifikacije jedinstvenog identiteta korisnika. Pristup telekomunikacijama, računaru i sistemima aplikacija za obradu podataka treba dozvoliti samo nakon unošenja pripadajućeg korisničkog imena i odgovarajuće lozinke.

Sve veći broj aplikacija i internet usluga elektronske uprave zahtevaju / omogućavaju autentikaciju i digitalni potpis koji koriste digitalni identitet. U tom slučaju, od ključnog je značaja da se sva značajna dokumenta nalaze na jednom mestu - elektronskom registru - dok pristup tom registru treba da bude dozvoljen samo ovlašćenim službenicima koji poseduju odgovarajući digitalni sertifikat.

Interno telo za sertifikaciju (TS) u Ministarstvu za informaciono društvo i telekomunikacije (GOV.ME) je formirano sa ciljem da se za bezbednu i pouzdanu razmenu dokumenata između državnih organa koriste digitalni sertifikati. Od samog početka Ministarstvo za informaciono društvo i telekomunikacije (MIDT) je aktivno promovisalo korišćenje i primenu digitalnih sertifikata. Usluge elektronske uprave, kako u MIDT tako i u drugim institucijama, imaju za cilj da povećaju korišćenje digitalnih sertifikata, uglavnom iz razloga bezbedne razmene podataka i identifikacije korisnika.

Mere protiv zloupotrebe IT u svrhe korupcije u Crnoj Gori

Svest o korupciji je porasla u Crnoj Gori tokom poslednje decenije, a borba protiv korupcije je postala važan prioritet u političkim planovima zemlje. Različiti sastavi Vlade Crne Gore su se jedan za drugim obavezivali da će se boriti protiv korupcije i preduzeti su ključni koraci na rešavanju tog pitanja, delom i zbog obaveza koje proističu iz procesa pristupanja Evropskoj uniji i potrebe da se nacionalno zakonodavstvo uskladi sa prevnom tekovinom EU, acquis communautaire.

Informaciono-komunikacione tehnologije su nezamenjiv deo modernog načina življenja. Integrisanje ICT u obavljenje dnevnih poslova i zadataka je postalo sve očiglednije. U tom smislu, pretnje za informaciono-komunikacionu infrastrukturu koje mogu da ugroze njenu pouzdanost, privatnost i integritet, mogu takođe da utiču na funkcionisanje društva u celini. Postoje brojni ICT instrumenti koji se mogu koristiti u različitim fazama borbe protiv korupcije, uključujući prevenciju, otkrivanje, analizu i korektivno delovanje.

ICT nije magični štapić kada je reč o obezbeđivanju veće transparentnosti i manje korupcije ili snažnije demokratije.

- ICT može da olakša deljenje informacija i u krajnjem obezbedi digitalne platforme na kojima građani mogu anonimno da prijavlju incidente.
- ICT može da olakša rad organizacija civilnog društva koje se zalažu za veću transparentnost i bore protiv korupcije podržavajući kombinaciju metoda vođenja kampanja o transparentnosti i edukacije građana o tome šta je korupcija i koja su njihova građanska prava.
- ICT može da poveća transparentnost u javnom sektoru na način što bi unapredila koordinaciju, pružanje informacija i administrativne kapacitete javnog sektora, te poboljšala pružanje usluga kroz primenu administrativnih sistema prilagođenih korisniku.

Međutim, ICT može i direktnije da utiče. Automatizovanjem procesa moguće je značajno smanjiti mogućnost pojave korupcije na način što će se na tačkama sakupljanja podataka i pružanja usluga ukloniti ljudski faktor – kada se ljudi upuste u elektronsko bankarstvo nema službenika koga treba podmititi..

ICT može, načelno, da pomogne u suzbijanju korupcije na neki od sledećih načina:

- Automatizacija: eliminisanje ljudskog elementa, a time i mogućnost pojave korupcije, iz radnog procesa;
- Transparentnost: eliminisanje mogućnost diskrecije;
- Otkrivanje tokom radnog procesa: oboje, i detalji i agregatne funkcije i podaci mogu da se prate u cilju otkrivanja anomalija i neočekivanih pojava u radu;
- Preventivno otkrivanje: društvene mreže na internetu i pojedinci mogu da budu praćeni da bi se otkrile pripreme koruptivnih radnji;
- Podizanje svesti: javnost može bolje da se odupre proizvoljnom odnosu kada je svesna vladinih pravila i procedura;
- Prijavljivanje: mobilisanje korisnika/zajednice da prijavljuju slučajeve će olakšati preduzimanje korektivnih radnji protiv pojedinaca i reorganizovanje sistema da se izbegnu „rupe”;
- Odvraćanje: objavljivanje informacija o prijavljenim slučajevima korupcije i pokazatelji (kao što je neusklađenost primanja i imovine) će odvratiti državne službenike od korupcije;
- Promovisanje etičkih stavova: uključivanje javnosti kroz vođenje diskusija na različitim internet forumima.

Veoma je važno uvesti proceduru bezbednosti podataka, da bi se izbegli svi problemi u oblasti zloupotrebe IT. Takođe je neophodno definisati mere zaštite od zloupotrebe IT s namerom činjenja koruptivnog dela.

Zakonodavni okvir

Pravni propisi koji čine osnovu za funkcionisanje i dalju nadogradnju modernog koncepta informacione bezbednosti u Crnoj Gori su:

- **Uredba o merama informacione bezbednosti** (Službeni list Crne Gore br. 14/10), propisuje primenu mera i standarda informacione bezbednosti, uključujući stepen poverljivosti, integritet i dostupnost podataka. Ova uredba odnosi se na državne organe, organe državne uprave, organe jedinica lokalne samouprave, pravna lica sa javnim ovlašćenjima i fizička lica koja ostvaruju pristup ili postupaju sa podacima. Ova uredba se ne odnosi na informacije koje su bitne za informacionu bezbednost, u skladu sa propisima koji uređuju poverljivost podataka;
- **Zakon o elektronskom potpisu** („Službeni list Republike Crne Gore", br. 55/03 i „Službeni list Crne Gore", br. 41/10) uređuje upotrebu elektronskog potpisa u pravnom prometu, upravnim, sudskim i drugim postupcima, kao i prava, obaveze i odgovornost pravnih i fizičkih lica u vezi sa elektronskim sertifikatima, ako posebnim zakonom nije drugačije uređeno;
- **Zakon o elektronskom dokumentu** uređuje način upotrebe elektronskog dokumenta u pravnim, sudskim i drugim postupcima, kao i prava, obaveze i odgovornosti privrednih društava, preduzetnika, pravnih i fizičkih lica, državnih organa, organa državne uprave, organa jedinica lokalne samouprave i organa koji vrše javna ovlašćenja u vezi sa elektronskim dokumentom;
- **Zakon o tajnosti podataka** - zakonski okvir o bezbednosnim procedurama za razmenu tajnih podataka je uspostavljen i sastoji se od Zakona o tajnosti podataka i Krivičnog zakonika, kao i od Uredbe o načinu i postupku označavanja tajnosti podataka i Uredbe o evidenciji tajnih podataka;
- **Zakon o potvrđivanju Konvencije o računarskom kriminalu** - Crna Gora je usvojila Zakon o potvrđivanju Konvencije o računarskom kriminalu 3. marta 2010. godine, a stupio je na snagu 1. jula 2010. Krivična dela obuhvaćena ovom Konvencijom obuhvataju širok opseg širenja virusa, neovlašćeni pristup računarskoj mreži od piraterije do pornografije i upad u bankarski sistem, zloupotrebu kreditnih kartica, kao i sva druga krivična dela za čije se izvršenje koriste računari.

U ostale važne propise koje treba pomenuti spadaju:

- Elaborat sa definisanim nadležnostima državnih organa u borbi protiv računarskog kriminala, uključujući procenu stanja i spremnost države u oblasti računarske bezbednosti;
- Uredba o bližim uslovima i načinu sprovođenja informatičkih mera zaštite tajnih podataka;
- Uredba o bližim uslovima i načinu sprovođenja mera zaštite tajnih podataka;

- Uredba o bližim uslovima i načinu sprovođenja industrijskih mera zaštite tajnih podataka;
- Uredba o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mera zaštite tajnih podataka.

Bezbednosni kontrolni elementi

Kada je reč o zloupotrebi IT u svrhe korupcije onda moraju postojati kontrolni elementi bezbednosti. „Kontrolni elementi informacione bezbednosti su tehničke, procesne i strateške mere osmišljene da zaštite osetljive podatke ublažavanjem prepoznatih i procenjenih rizika po njihovu tajnost, integritet i dostupnost"[84]. U Ministarstvu za informaciono društvo i telekomunikacije postoji Direktorat za informatičku infrastrukturu koji ima tri sektora: Direkciju za analizu, planiranje i praćenje projekata, Direkciju za infrastrukturne servise i Direkciju za zaštitu od računarskih i bezbednosnih incidenata na internetu – CIRT. Glavni ciljevi CIRT-a su:

Prevencija, obrada i otklanjanje posledica od računarskih bezbednosnih incidenata na internetu i drugih rizika po bezbednost informacionih sistema:

- Prevencija se ogleda u proaktivnom načinu delovanja, koji podrazumeva pružanje informacija i procenu stanja informacione bezbednosti, provere ranjivosti sistema, prikupljanje, evidentiranje i obradu podataka o incidentima, testiranje i primenu novih softverskih i hardverskih sistema za zaštitu IT resursa;
- Obrada podataka i otklanjanje posledica sastoji se od utvrđivanja pojave i težine incidenta, utvrđivanja uzroka incidenta, posredovanja u komunikaciji svih strana koje su uključene u incident, izveštavanja drugih CERT/CIRT/CSIRT timova, sastavljanja izveštaja i upozorenja za ostale korisnike, otklanjanja ranjivosti u sistemu, zaštite sistema od mogućih incidenta, forenzičke analize.

Edukacija korisnika po pitanju informacione bezbednosti obuhvata:

- Postavljanje publikacija, priručnika, softverskih alata i drugih korisnih informacija vezanih za sigurnije korišćenje informacionih tehnologija na web portal (www.cirt.me);
- Organizovanje kurseva i obuka na temu bezbednosti IT i mogućih načina zaštite i prevencije od računarsko-bezbednosnih incidenata.

Ministarstvo za informaciono društvo i telekomunikacije je izradilo nekoliko pravilnika:

- Pravilnik o merama i postupcima zaštite sertifikata i podataka vezanih za potpisnike. Ovaj pravilnik propisuje organizacione i tehničke mere za zaštitu sistema sertifikovanja u delu zaštite sertifikata i kvalifikovanih sertifikata, podataka vezanih za potpisnike, kao i uspostavljanje i primena sistema zaštite pristupa evidenciji sertifikata;

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

- Pravilnik o standardima informacione bezbednosti - utvrđuju se standardi informacione bezbednosti koji se primenjuju za sprovođenje mera informacione bezbednosti utvrđenih propisom Vlade Crne Gore;
- Pravilnik o upravljanju računarskim i bezbednosnim incidentima na internetu - CIRT izrađuje i vodi plan odgovora na računarske i bezbednosne incidente na internetu u vidu definisanja postupaka bitnih za upravljenje incidentima;
- Pravilnik o sadržaju i načinu vođenja evidencije i registra davalaca usluga sertifikovanja. Ovim pravilnikom propisuje se sadržaj i način vođenja evidencije davalaca usluga sertifikovanja, način vođenja registra akreditovanih davalaca usluga sertifikovanja, kao i najniži iznos osiguranja za rizik od odgovornosti za štete koje mogu nastati obavljenjem usluga sertifikovanja;
- Pravilnik o merama zaštite elektronskog potpisa i naprednog elektronskog potpisa. Ovim pravilnikom se uređuju mere zaštite elektronskog potpisa i naprednog elektronskog potpisa, mere provere identiteta potpisnika od strane potpisnika ili davaoca usluga sertifikovanja u Crnoj Gori, tehničko-tehnološki postupci za izradu naprednog elektronskog potpisa i uslovi koje treba da ispune sredstva za izradu naprednog elektronskog potpisa;
- Pravilnik o načinu rada i uslovima za administrativni pristup Web Portalu Vlade Crne Gore;
- Pravilnik o upotrebi računarsko-komunikacionih resursa na mreži državnih organa;
- Praktična pravila pružanja usluge sertifikacije (Certification Practice Statement – CPS).

Informaciona bezbednost mora takođe da zadovolji uslove poverljivosti, integriteta i dostupnosti podataka. Informaciona bezbednost je usmerena na podatke, bez obzira u kom su obliku: elektronskom, štampanom ili nekom drugom.

Zbog stalnog porasta broja usluga koje državni organi i privatni sektor pružaju građanima, kao i pravnim licima, potrebno je odrediti kritičnu informacionu infrastrukturu u Crnoj Gori i utvrditi procedure zaštite.

Ključne aktivnosti:
- Određivanje i zaštita kritične informacione infrastrukture;
- Jačanje otpornosti informacionih sistema na incidente;
- Analiza pretnji po IT infrastrukturu.

Zaštita podataka

U Ministarstvu za informaciono društvo i telekomunikacije formiran je Tim za odgovor na računarske incidente/Tim za odgovore na računarske i bezbednosne incidente - CERT/CSIRT (Direkcija za zaštitu od računarskih i bezbednosnih incidenata na internetu). Ministarstvo za informaciono društvo i telekomunikacije i Međunarodna telekomunikaciona unija potpisali su administrativni sporazum u cilju dobijanja specijalizovane tehničke pomoći za potrebe formiranja Nacionalnog tima za odgovor na računarske incidente – CIRT

(Nacionalni tim za obradu i zaštitu od računarskih incidenata) koji će delovati u saradnji sa CIRT mrežom koja je osnovana u okviru Međunarodnog multilateralnog partnerstva protiv računarskih pretnji (IMPACT).

Primena Zakona o informacionoj bezbednosti i Uredbe o merama informacione bezbednosti obezbeđena je kroz sistem inspekcijskog nadzora, što doprinosi sve većem nivou zaštite podataka.

Kao primarni korisnici CIRT.ME definisani su:

- svi državni organi u Crnoj Gori;
- kritična nacionalna informaciona infrastruktura.

CIRT Crna Gora je osnovan u skladu sa Zakonom o informacionoj bezbednosti Crne Gore, u okviru Ministarstva za informaciono drustvo i telekomunikacije (MIDT). Formiran kao zasebna organizaciona jedinica Ministarstva, CIRT posluje u okviru Direktorata za informatičku infrastrukturu i obuhvata nadležnosti nacionalnog CIRT-a. CIRT je angažovan na rešavanju incidenata iz oblasti informacione bezbednosti ako se jedna od strana umešanih u incident nalazi u Crnoj Gori (ako pripada domenu „.me" ili ako se nalazi unutar prostora pokrivenog crnogorskom IP adresom).

Misija CIRT-a:

- CIRT koordiniše i pomaže državnim organima u implementaciji proaktivnih servisa kako bi se smanjio rizik od računarskih incidenata, te reaguje na takve incidente u slučaju da se dogode;
- CIRT.ME organizuje kampanje podizanja svesti kako bi edukovali lokalno stanovništvo o negativnim uticajima računarskih pretnji i računarskog kriminala.

U okviru administracije mora postojati definisana organizaciona hijerarhija koja će biti najdelotvorniji i dugoročno održiv izvor odgovarajućih upravljanja informacionom bezbednošću.

Iako je pouzdanih podataka malo, postoje barem neki dokazi da ICT može da bude delotvoran instrument za borbu protiv korupcije. Međutim, potencijal ICT može se realizovati samo u kombinaciji sa stvarnom reformom državne uprave.

Tehničke mere zaštite

Reč je o hardverskim i softverskim kontrolnim elementima da se LAN i WAN zaštite od neovlašćenog pristupa ili zloupotrebe, da se pruži pomoć u otkrivanju zloupotreba i kršenja bezbednosti i obezbedi zaštita LAN aplikacija. U tehničke mere zaštite spadaju identifikacija i provera identiteta korisnika, kontrolni elementi autorizacije i pristupa, kontrolni elementi integriteta, mehanizmi praćenja prethodnih aktivnosti, kontrolni elementi poverljivosti i kontrolni elementi preventivnog održavanja hardvera.

Lozinke su primarni metod koji se koristi za kontrolu pristupa resursima i najčešće su upotrebljavani mehanizam provere identiteta[85]. Ministarstvo za informaciono društvo i telekomunikacije (MIDT) je nadležno za administraciju mreže državne uprave. MIDT obavlja praćenje i administriranje mreže. Zadatak funkcionisanja IT je dat u nadležnost kako bi se obezbedilo da se komunikacione veze održavaju i da se korisnicima obezbedi odobreni nivo pristupa mreži. Za celu mrežu državne uprave postoji politika korišćenja lozinki kojom je definisan metod kreiranja novih lozinki svakog meseca.

Prepoznavanje kontrolnih elemenata

Utvrđivanje odgovarajućeg skupa kontrolnih elemenata bezbednosti koji bi, ako se realizuju i pokažu delotvornim u svojoj primeni, bili u skladu sa navedenim zahtevima u pogledu bezbednosti na način što bi umanjivali posledice ili verovatnoću svake prepoznate pretnje, predstavlja izazov za organizacije. Za svaku kategoriju bezbednosti potrebno je imati niz različitih kontrolnih elemenata koji bi činili sveobuhvatan i robustan bezbednosni okvir.

Upotreba šifrovanja da se zaštite korisnički podaci od izvora do destinacije, koje se naziva šifrovanje „s kraja na kraj", je snažan instrument da se omogući bezbednost mreže.

Ministarstvo za informaciono društvo i telekomunikacije Vlade Crne Gore (MIDT) je upravljalo ključnom javnom infrastrukturom (GOV.ME-PKI) za unutrašnje potrebe državne uprave Crne Gore. U okviru MIDT, formirano je sertifikaciono telo kao jedinstveni Organ za sertifikaciju, koji sertifikuje državne službenike Ministarstva za informaciono društvo i zaposlene u Vladi Crne Gore. Sistem je sproveden u potpunosti u skladu sa važećim zakonskim propisima, uglavnom Zakonom o elektronskom potpisu.

Trenutno postoje planovi da se počne sa korišćenjem digitalnih sertifikata za prijavljivanje na svaki računar u državnoj upravi, ali je nedostatak sredstava još uvek problem i prepreka za sprovođenje takve mere.

Prenos podataka

Prenos osetljivih podataka, preko FTP, od sistema do sistema, ili podnošenjem Web obrazaca, treba obavljati samo bezbednim putem ili uređajem sa kontrolnim elementima koji obezbeđuju poverljivost, integritet i autentičnost sadržaja. Sve veze od nekog internog sistema ili baze podataka do drugih sistema van akreditacionih granica treba da budu odobrene isključivo kroz sistem sporazuma o konekciji i treba ih kontinuirano pratiti i kontrolisati.

Za zaštitu podataka tokom prenosa otvorenim, javnim mrežama treba da se koristi jako šifrovanje i bezbednosni protokoli. Prenos ličnih podataka od eksternih lica do organizacije,

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

obično preko internet stranice, treba realizovati preko zaštićenih servera uz korišćenje šifrovanja visokog nivoa.

Trenutno se prenos podataka, ili razmena podataka, obavlja preko zaštićenih web servisa za potrebe specijalizovanih IT sistema. Veza se obezbeđuje preko zaštićene mreže i šifruje digitalnim sertifikatima.

Specijalizovani sistem za razmenu podataka i dalje predstavlja izazov za Crnu Goru. Trenutno pripremamo projekat „Magistrala elektronskih sabirnica" (Enterprise Service Bus) koji će omogućiti državnim institucijama da bezbedno razmenjuju podatke među sobom. Ali, nedostatak finansijskih sredstava i dalje predstavlja problem za realizaciju ovog projekta.

Pristup sa daljine

Definicija pristupa sa daljine je svaki pristup informacionom resursu organizacije od strane korisnika ili sistema koji komuniciraju preko eksterne mreže ili veza koje ne kontroliše organizacija. Organizacija može da proceni da je neophodno da obezbedi pristup podacima i sistemu sa daljine za radnike koji rade na daljinu ili kao podrška poslovima koji se obavljaju na udaljenim lokacijama. U nekim slučajevima prodavci opreme zahtevaju povremeni pristup sa daljine zbog redovne ili hitne podrške sistemu.

U Vladi Crne Gore samo ministri i zamenici ministara mogu da dobiju pristup svojim računarima na GOV mreži sa daljine.

U Crnoj Gori je 88,3% ispitanih preduzeća navelo da su koristili računare u svom radu u januaru 2012. godine. Prema rezultatima istraživanja, 53,3% preduzeća (koja su koristila računare u svom radu) je u januaru 2012. svojim zaposlenima omogućavalo pristup sistemima elektronske pošte, dokumentima ili aplikacijama preduzeća sa daljine.

Kao rezultat povećanog rizika povezanog sa pristupom izvan zaštićenog opsega, organizacija treba da primeni politike i procese sa uslovima pod kojima se dodeljuje i ukida pristup na daljinu. Pristup na daljinu treba dodeliti na osnovu odobrenih poslovnih potreba, zatim ograničiti na minimum potrebnih ovlašćenja i tražiti odobrenje rukovodstva, a sva odobrenja treba periodično proveriti i obrazložiti.

Samo 27,9% preduzeća u Crnoj Gori ima pravilnik koji normativno uređuje pitanja informacione bezbednosti. Takođe, mali broj preduzeća, njih samo 26,9%, sprovodi procenu znanja svojih zaposlenih o merama informacione bezbednosti.

Koordinisana izgradnja organizacionih, institucionalnih i upravljačkih kapaciteta, poboljšanje zakona i propisa su važni elementi za prisustvo informacione bezbednosti u Crnoj Gori.

Srbija

Pripremili Nemanja Nenadić i Bojan Cvetković

Mere zaštite u primerima iz Srbije

Slučaj iz Srbije 1: Seks ispred Beogradske arene

Prema uputstvu Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, Ministarstvo unutrašnjih poslova (MUP) je sprovelo kratkoročne, srednjoročne i dugoročne mere zaštite od korupcije povezane sa IT.

Kratkoročne mere zaštite:

- Tehničke mere zaštite:
  - Bilo kakav tehnički pristup bilo kojoj vrsti IT sistema mora biti evidentiran za kasnije revizije i provere;
  - Uvedene su kodirane kartice da se ograniči pristup prostorijama sa instalacijama u kojima se pohranjuju podaci;
- Organizacione i proceduralne mere zaštite:
  - Pristup podacima mora biti praćen pisanim procedurama, koje definišu podatke kojima se može pristupiti, i ovlašćenjem za pristup;
  - Broj zaposlenih sa direktnim operativnim pristupom podacima je smanjen na minimum potreban za normalan radni proces;
  - Upotreba elektronskih prenosivih medija u prostorijama sa instalacijama u kojima se pohranjuju podaci je sada strogo ograničena konkretnim procedurama za pristup podacima ili je potpuno zabranjena (u zavisnosti od vrste instalacija);
- Zaštitne mere praćenja:
  - Instalirani su zasebni sistemi video nadzora koji direktno prate pristup IT podsistemima za pohranjivanje podataka.

Srednjoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Obuka i mere podizanja svesti;
  - Obuka službenika MUP o rizicima od zloupotrebe IT u svrhe korupcije;
- Revizija IT sistema;
  - MUP je izradio planove za uvođenje internet IT revizije kao i ISO 27001 standardizacije u bliskoj budućnosti.

Dugoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Zakonodavne mere zaštite:
  - Izmenjeni su i dopunjeni interni upravni propisi da bi se obezbedilo da neovlašćeni pristup bude definisan ne samo kao disciplinski prekršaj već i kao krivično delo;

- Izmenjeni su i dopunjeni interni upravni propisi kako bi obuhvatili konkretan stav MUP-a da se upotreba podataka za bilo koju drugu namenu osim one izvorne zbog koje su podaci prikupljeni sada smatra krivičnim delom (a ne samo disciplinskim prekršajem);
- Izmenjeni su i dopunjeni interni upravni propisi o upotrebi i primeni određenih vrta elektronskih prenosivih medija (optičkog diska, USB memorije, „pametnog" telefona, digitalnog fotoaparata, itd.) sa ciljem ograničavanja ili zabrane njihove upotrebe na lokacijama MUP-a u zavisnosti od vrste podataka koji se mogu zloupotrebiti;
- Član 42, stav 3 Ustava izričito zabranjuje i kažnjava korišćenje ličnih podataka za namene koje prevazilaze svrhu za koju su prikupljeni.

Slučaj iz Srbije 2: Kada IT izvođač „pusti korenje"

Stvarni slučaj koji je razotkrio zavisnost MP od njegovih IT izvođača i ukazao na veliki broj različitih vrsta rizika vezanih za IT izvođače. Mere zaštite koje su uvedene obuhvatile su kratkoročne, srednjoročne i dugoročne mere čiji je cilj značajno smanjenje rizika vezanih za IT izvođače.

Kratkoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Tehničke mere zaštite:
  - Bilo kakav tehnički pristup bilo kojoj vrsti IT sistema mora biti evidentiran;
  - Uvedeni su sistemi fizičke zaštite kao mera da se ograniči i kontroliše pristup centru sa podacima MP koje na jednom mestu pohranjuje sve podatke;
- Organizacione i proceduralne mere zaštite;
  - Pristup podacima mora biti propraćen službenim zahtevom i odobrenjem (dozvolom) od nadležnog suda (ili tužilaštva) za pristup određenom predmetu (predmetima);
  - Niko, čak ni zaposleni na najvišem nivou u MP, ne može imati pristup podacima bez prethodnog odobrenja (dozvole) suda (ili tužilaštva);
  - Sudovi (ili tužilaštva) mogu da pristupe samo svojim podacima - pristup podacima koji pripadaju drugim subjektima je zabranjen;
  - Zaposleni kod IT izvođača ne mogu da pristupe glavnom centru sa podacima niti samim podacima ako u njihovoj pratnji nisu najmanje dva službenika ministarstva;
  - Broj zaposlenih sa direktnim operativnim pristupom podacima je smanjen na minimum koji je potreban za normalno odvijanje radnog procesa;
  - Sve dogradnje i ažuriranja moraju da se obave iz glavnog centra za podatke - nikome nije dozvoljen pristup sa daljine;
  - Upotreba ektronskih prenosivih medija u prostorijama sa instalacijama u kojima se pohranjuju podaci je potpuno zabranjena;
- Zaštitne mere praćenja:

- Instaliran je zaseban sistem video nadzora koji direktno prati pristup glavnom centru podataka u koji se pohranjuju svi podaci.

Srednjoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Obuka i mere podizanja svesti:
  - Obuka službenika MUP-a o rizicima od zloupotrebe IT u svrhe korupcije;
- Revizija IT sistema:
  - MP je već uvelo eksternu reviziju IT;
  - MP planira da uvede ISO 27001 and ISO 20000 standarde u bliskoj budućnosti.

Dugoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Zakonodavne mere zaštite:
  - Izmenjeni su i dopunjeni interni upravni propisi da se zabrani neovlašćeni pristup podacima u MP;
  - Izmenjeni su i dopunjeni interni upravni propisi da se pristup podacima definiše u skladu sa „odvojenim nadležnostima" između ministarstva, sudova, tužilaštava i zatvora;
  - Izmenjeni su i dopunjeni interni upravni propisi o upotrebi i primeni određenih vrsta elektronskih prenosivih medija (optičkog diska, USB memorije, „pametnog" telefona, digitalnog fotoaparata, itd.) sa ciljem zabrane njihove upotrebe u glavnom centru za podatke MP;
  - Zakon o javnim nabavkama („Službeni list Republike Srbije", br. 124/12).

Slučaj iz Srbije 3: Viši državni zvaničnik špijunira zaposlene

Nije poznato koje su mere preduzete da se zatvori „praznina" u Agenciji za privatizaciju u pogledu sprečavanja zloupotrebe IT, pošto je opisani slučaj jasno ukazao na ljudski faktor kao slabost u Agenciji za privatizaciju koji je bio ključan i u samom središtu zloupotrebe IT.

Slučaj iz Srbije 4: „Drumska mafija"

Kao što je obrazloženo u presudi za „Drumsku mafiju", mere zaštite od zloupotrebe IT u svrhe korupcije nisu funkcionisale godinama. Članovi bande su na vreme bili informisani o proverama, pa su imali dovoljno vremena da prikriju dokaze o izvršenom krivičnom delu. Provere su se obavljale obično oko 18:00, kada banda nije delovala. Dalje, uprkos činjenici da je fajl EMU-87 bio lažan i da se razlikovao od originala, istina je godinama ostala sakrivena. Pošto je elektronski sistem za plaćanja i evidentiranje vozila radio „normalno", provere nisu otkrile ovaj upad. Zaposleni iz preduzeća koje je održavalo elektronski sistem

„Puteva Srbije" imao je administrativna ovlašćenja, a izgleda da niko iz „Puteva Srbije" nije nadgledao njegov rad.

Sistem registrovanja pojedinačnih službenika za naplatu putarine sa njihovom jedinstvenom identifikacijom nije funkcionisao u praksi. Identifikacioni brojevi su bili vidljivi kolegama, a šefovi smena često zamenjivali zaposlene.

Srednjoročne mere zaštite od zloupotrebe IT u svrhe korupcije bile su:

- Tehničke mere zaštite:
- Instaliran je dopunski ali zaseban IT sistem sa senzorima za praćenje vrste i broja vozila koja prolaze kroz kućice za naplatu (sada se statistički podaci iz originalnog sistema moraju poklopiti sa novim sistemom sa senzorima)
- Uvedeni su sistemi fizičke bezbednosti kao mera da se ograniči i kontroliše pristup prostorijama sa instalacijama u kojima se pohranjuju podaci korisnika.

Nemamo informacije jesu li i koje su mere u smislu organizacije, procedura i praćenja preduzete.

Nemamo informacije jesu li i koje su srednjoročne mere zaštite od zloupotrebe IT u svrhe korupcije preduzete.

Dugoročne mere zaštite od zloupotrebe IT u svrhe korupcije obuhvatile su uvođenje nove vrste naplate putarine poznatu kao „ENP" (elektronska naplata putarine) koja je u potpunosti zasnovana na elektronskom plaćanju putem NFC kartica da bi se izbegli svi direktni gotovinski transferi između strana kod plaćanja putarine.

Proaktivno objavljivanje informacija – instrument za sprečavanje zloupotrebe IT u svrhe korupcije

Srpski Zakon o slobodnom pristupu informacijama („Službeni list Republike Srbije", br. 120/04, 54/07, 104/09 i 36/10) propisuje obavezno objavljivanje „Informatora" za sve organe javne vlasti (koji se finansiraju iz budžeta), a reč je o dokumentu definisanom u „Uputstvu poverenika" (poslednji put objavljeno 2010. godine)[86]. Informator mora da se objavljuje na internetu i ažurira barem jednom mesečno. Cilj ove publikacije je da pruži veliku količinu korisnih informacija pomoću kojih javnost može da insistira na odgovornosti organa, kao što su podaci o javnim nabavkama, budžetu, donacijama i državnoj pomoći. Ostale informacije odnose se na strukturu državnih organa ili usluge koje pružaju građanima. Međutim, za svrhe ove analize, najinteresantniji delovi su odredbe članova 37, 38 i 39.

Član 37 se bavi „čuvanjem nosača informacija". Nosači informacija su mediji na kojima se pohranjuju podaci, kao što su papir, hard diskovi, baze podataka, video trake, itd. Državni organ mora da identifikuje različite vrste takvih medija koji se koriste za pohranjivanje

86 http://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/uputstvo-informator/uputstvoen.doc

informacija, po tipu, količini (tačnoj ili procenjenoj), kao i vrsti podataka koji se na njima pohranjuju. Dalje, organi moraju da utvrde gde se „nosači informacija" čuvaju (organizacione jedinice ili posebni delovi unutar organa, kao što su arhiva, biblioteka i elektronske baze podataka) kao i mesta za njihovo čuvanje unutar tih prostorija (npr. metalni ormari, police sa fasciklama, zajednički server ili pojedinačna računarska oprema). Državni organi su obavezni da ukratko opišu kako se nosači informacija čuvaju i održavaju u praksi (da li se vrši bezbedno snimanje podataka na drugi nosač podataka, da li su računari zaštićeni od virusa, da li još neko osim zaposlenih ima pristup nosaču informacija, da li postoji periodična procena usaglašenosti sa zahtevima za čuvanje nosača informacija, itd.), kao i da navedu da li su uslovi za čuvanje nosača u skladu sa propisima ili potrebom da se sačuvaju, ukoliko takvi propisi ne postoje.

Članovi 38 i 39 obavezuju državne organe da objave vrste informacija koje poseduju i vrste podataka za koje će biti dozvoljen pristup. Vrste informacija, na primer, mogu (kao što se navodi u Uputstvu) biti sledeće:

- • zbirka propisa
- objavljena mišljenja
- zapisnici sa sastanaka
- odluke
- žalbe
- zaključeni ugovori
- zvučni i video snimci sa događaja koje organizuje državni organ
- pisma građana
- razni oblici komunikacije sa javnošću
- dokumenta o isplatama, zaposlenima, javnim nabavkama
- nacrti dokumenata u pripremi
- službena evidencija
- zahtevi i molbe klijenata, itd.

Informacije o dostupnosti podataka treba predstaviti na takav način da je moguće izvršiti poređenje sa spiskom vrsta informacija koje organ poseduje. Ako su informacije tačne i sveobuhvatne, javnost može da insistira na odgovornosti organa i može da spreči, između ostalog, situacije u kojima državni službenici tvrde da neki organ ne poseduje određene informacije ili da su informacije izgubljene, itd. U praksi, međutim, većina organa ne postupa u skladu sa ovim odredbama i ne nude detalje niti o nosačima informacija niti informacije o vrstama podataka. Očekivanja su da će se ova situacija ubrzo promeniti sa najavljenim izmenama i dopunama Zakona o slobodnom pristupu informacijama koje će postupke nadzora i kažnjavanja učiniti delotvornijim.

Krivična dela propisana, primena nepoznata

Krivični zakonik Republike Srbije (Službeni list RS, br. 85/2005, 88/2005, 107/2005) sa izmenama i dopunama od 31. avgusta i 29. decembra 2009, 24. decembra 2012, propisuje sankcije u poglavlju XXVII za krivična dela protiv bezbednosti računarskih podataka.

Prvo krivično delo iz ove grupe je *„Oštećenje računarskih podataka i programa"* (Član 298). Lice može biti kažnjeno novčanom kaznom ili zatvorom do jedne godine ako *„neovlašćeno izbriše, izmeni, ošteti, prikrije ili na neki drugi način učini neupotrebllјivim računarski podatak ili program"*. Ako je prouzrokovana šteta veća, učinilac se može kazniti do pet godina zatvora. Uređaji i sredstva kojima je učinjeno krivično delo se oduzimaju.

„Računarska sabotaža" (Član 299) propisuje kaznu do pet godina za onoga:

„ko unese, uništi, izbriše, izmeni, ošteti ili prikrije ili na neki drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade ili prenos podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte".

„Pravljenje i unošenje računarskih virusa" (Član 300) utvrđuje kaznu do šest meseci za onog *„ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu"*. Ako učinilac *„unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu"* kazna je do dve godine zatvora. Uređaji i sredstva kojima je učinjeno krivično delo se oduzimaju.

„Računarska prevara" (Član 301) se definiše na sledeći način:
„Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine"

Za veće imovinske koristi ili štete, kazna može biti do deset godina zatvora.

„Neovlašćeni pristup računaru" i *„računarskoj mreži ili elektronskoj obradi podataka"* (Član 302) mogu se kazniti kaznom do tri godine zatvora, u zavisnosti od učinjene štete.

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (Član 303) se kažnjava do tri godine.

„Neovlašćeno korišćenje računara ili računarske mreže" (Član 304) propisuje:
„Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist kazniće se novčanom kaznom ili zatvrorom do tri meseca. Gonjenje za ovo delo preduzima se po privatnoj tužbi."

Najnovija izmena i dopuna iz ove grupe je *„Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka”* (Član 304a):

„Ko poseduje, pravi, nabavlja, prodaje ili daje drugom na upotrebu računare, računarske sisteme, računarske podatke i programe radi izvršenja krivičnih dela iz članova 298. do 303 ovog zakonika, kazniće se zatvorom od šest meseci do tri godine. Predmeti iz stava 1 ovog člana oduzeće se.”

Srbija takođe ima veliki raspon krivičnih dela koja mogu da se koriste za kažnjavanje korupcije (zloupotreba službenog položaja, uzimanje mita, davanje mita, protivzakoniti uticaj, itd.), koja su skoro u potpunosti usaglašena sa relevantnim međunardnim standardima. Mogao bi se izvući pogrešan zaključak da je krivičnopravni sistem za borbu protiv zloupotrebe IT u svrhe korupcije delotvoran. Međutim, to teško da je tačno. Ukupan broj slučajeva u kojima je korupcija (povezana sa IT ili neka druga) do kraja istražena i slučajevi finalizovani je i dalje prilično mali i takvi su slučajevi izuzetno retki, a naročito oni u koje su uključeni visoko rangirani funkcioneri ili visoke svote novca. Situacija nije mnogo bolja ni kada je genralno reč o istragama krivičnih dela povezanih sa IT. Srbija godinama ima posebnu tužilačko odelenje za borbu protiv računarskog kriminala. To odelenje, koje deluje od 2006. godine, još uvek ima internet stranicu koja je „u izradi”, a najnoviji statistički podaci su stari već tri godine[87].

Stečena znanja – Mere zaštite od korupcije koja zloupotrebljava ICT u javnom sektoru zemalja zapadnog Balkana

Pripremila Louise Thomasen

Pojedinačne mere zaštite nabrojane u uvodu i opisane kroz celo ovo poglavlje ukazuju kako jedna mera zaštite sama po sebi nije dovoljna. Zaštita od zloupotrebe ICT u svrhe korupcije zahteva uvođenje svih gore opisanih mera, jer one podržavaju i dopunjuju jedna drugu. Elektronska uprava se nikada ne svodi na čisto tehničko pitanje. Elektronska uprava se ne tiče samo tehnologije, već i državne uprave i kako obavljamo određene stvari, kako sarađujemo sa vladom, državnom upravom, zajednicom, privredom i društvom u celini. Elektronska uprava se nikada ne sme posmatrati izolovano i nezavisno od ostatka društva.

Borba protiv korupcije postaje prioritet za zemlje zapadnog Balkana u mreži ReSPA. Autori iz nekoliko zemalja su istakli kako se prikazanim primerima naglašava potreba za povećanom svešću o određenim pitanjima povezanim sa korupcijom i elektronskom upravom, bez obzira koliko se fokus i mere međusobno razlikuju. U Albaniji je nova albanska vlada inovirala svoj plan za borbu protiv korupcije, te je nedavno uvela novi postupak za tehnički

87 http://www.beograd.vtk.jt.rs/

prijem informacionih sistema. U nacionalnim izveštajima iz Bosne i Hercegovine se tvrdi da korupcija spada u najveće probleme društva, dok se u Izveštaju EU o napretku te zemlje za 2013. godinu navode nedostatak strategije i institucija za borbu protiv računarskog kriminala i pretnji. Autori iz Kosova su primetili da ne postoje nikakve institucije koje bi se bavile formulisanjem i sprovođenjem mera i standarda ICT zaštite, kao i da brojni slučajevi zloupotrebe ICT u svrhe korupcije prođu neopaženo. Autori iz Srbije ističu da je ukupan broj slučajeva u kojima je sprovedena puna istraga o korupciji (sa ili bez ICT) prilično mali, posebno slučajeva u koje su umešani visoko rangirani funkcioneri ili koji se odnose na velike novčane iznose. Iako Srbija ima posebno tužilačko odelenje za borbu protiv računarskog kriminala od 2006. godine, od tog odelenja nije dostupno puno informacija.

Autori iz Crne Gore primećuju da se svest o korupciji povećala i da je korupcija postala važan prioritet u političkim planovima zemlje, i to ne samo za postojeću vladu. U Ministarstvu za informaciono društvo i telekomunikacije Crne Gore sada postoji Direktorat za informacionu infrastrukturu sa tri direkcije: Direkcija za analizu, planiranje i praćenje projekata, Direkcija za infrastrukturne servise i CIRT (Tima za odgovor na računarske i bezbednosne incidente). Autori iz Crne Gore takođe ukazuju na nekoliko studija i propisa o borbi protiv računarskog kriminala i zaštiti informacija u Crnoj Gori. I u Crnoj Gori je borba protiv korupcije jedan od najvažnijih strateških ciljeva za Vladu. Pored toga, Crnogorci takođe organizuju kampanje podizanja svesti, obuku zaposlenih i građana o načinima da se spreči korupcija, informisanje o mogućnostima u pogledu preduzimanja zakonskih mera i utvrđuju obaveze Vlade u Strategiji reformi javne uprave i njenom Akcionom planu. U Hrvatskoj postoji skup zakonskih propisa o informacionoj bezbednosti, kao i državni organi nadležni za zaštitu „integriteta i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izrade, korišćenja i prestanka rada informacionog sistema".

Ne možemo napraviti direktno poređenje između zemalja da bi utvrdili koliko su one odmakle u borbi protiv zloupotrebe ICT u svrhe korupcije, jer nemamo statističkih podataka da nas u tome podrže. Međutim, na osnovu analiza autora iz pojedinačnih zemalja, možemo uslovno raspoznati napore zemalja, te izgleda da Hrvatska, Makedonija i Crna Gora više rade na zaštiti ICT u javnom sektoru od zloupotrebe i korupcije od drugih zemalja iz ove studije.

Tehničke mere zaštite - pristup podacima

ICT u javnom sektoru može da omogući veću transparentnost u smislu ko pristupa i koristi podatke javnog sektora. Ali, isto tako može da omogući i mnogo širu zloupotrebu nego što je moguća bez ICT, kao što je falsifikovanje podataka, nezakonito pribavljanje podataka i uništavanje podataka.

Dozvolite da još jednom naglasimo da naši primeri ne predstavljaju reprezentativan uzorak, ali ono što je očigledno iz tabele 3 je da ima više slučajeva falsifikovanja podataka od nezakonitog pribavljanja podataka, dok se najmanje slučajeva odnosi na stvarno uništavanje podataka.

Tabela 3 Slučajevi zloupotrebe koji su bili mogući zbog pristupa podacima

Falsifikovanje podataka	Nezakonito pribavljanje podataka	Uništavanje podataka
Slučaj iz Bosne i Hercegovine 3: Zloupotreba elektronskog sistema projekta CIPS	Slučaj iz Hrvatske 1: Poziv od doktora radi glasanja	Slučaj iz Bosne i Hercegovine 2: Još jedno kontraverzno zaposlenje u Vrhovnoj revizorskoj instituciji Republike Srpske
Slučaj iz Hrvatske 8: Svake godine nestane 2 miliona evra sa naplatnih rampi	Slučaj iz Hrvatske 11: Viši inspektor zloupotrebio poverljive podatke kako bi pobedio na lokalnim izborima!	Slučaj iz Hrvatske 6: Policajci brisali saobraćajne prekršaje iz evidencije i otkrivali poverljive podatke: prihvatali čak i pečeno jagnje i 20 litara vina kao mito!
Slučaj iz Hrvatske 12: Ni dana života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!	Slučaj iz Hrvatske 2: Baza sa poverljivim podacima Hrvatske radio televizije na crnom tržištu	Slučaj iz Hrvatske 8: Svake godine nestane 2 miliona evra sa naplatnih rampi
Slučaj sa Kosova 1: Uništavanje dokaza	Slučaj iz Hrvatske 3: U potrazi za veteranima	Slučaj sa Kosova 1: Uništavanje dokaza
Slučaj sa Kosova 2: Dobijanje statusa „ratnog invalida"	Slučaj iz Hrvatske 4: Uz malu pomoć državnih službenika, 68 hrvatskih pasoša prodato kriminalcima	
Slučaj sa Kosova 4: Falsifikovanje poreskih dokumenata	Slučaj iz Hrvatske 6: Policajci brisali saobraćajne prekršaje iz evidencije i otkrivali poverljive podatke: prihvatali čak i pečeno jagnje i 20 litara vina kao mito!	
Slučaj iz Makedonije 1: Zloupotreba IT sistema na naplatnim rampama	Slučaj iz Hrvatske 7: Slučajno uhvaćeni u otkrivanju povreljivih podataka o automobilima i njihovim vlasnicima!	
Slučaj iz Makedonije 3: Zloupotreba IT sistema i nelegalno otkrivanje ličnih podataka	Slučaj iz Crne Gore 2: Korišćenje podataka iz IT sistema za nanošenje političke štete	
Slučaj iz Makedonije 4: Zloupotreba sistema evidentiranja broja radnih sati	Slučaj iz Makedonije 3: Zloupotreba IT sistema i nelegalno otkrivanje ličnih podataka	
Slučaj iz Crne Gore 1: Zloupotreba službenog položaja i falsifikovanje zvaničnih dokumenata	Slučaj iz Srbije 1: Seks ispred Beogradske arene	
Slučaj iz Crne Gore 2: Upotreba IT podataka sa ciljem nanošenja političke štete		
Slučaj iz Crne Gore 3: Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre		
Slučaj iz Crne Gore 4: Nezakonito izdavanje putnih isprava		
Slučaj iz Srbije 4: Drumska mafija		

Zaštita pristupa podacima stoga postaje od najvećeg značaja, i obuhvata ne samo kontrolu pristupa već i korišćenje odgovarajućih nivoa pristupa.

Kontrola pristupa - lozinke i upravljanje identitetom korisnika

Kontrola i ograničenje pristupa sistemu se sprovode dodeljivanjem korisničkog imena i lozinke korisnicima. Većina sistema, koji razmenjuju podatke ili opslužuju više od jednog korisnika, ima neku vrstu kontrole pristupa, korisničkog imena i lozinke. Kod samostalnih sistema, podatke i računarske porograme treba zaštititi kontrolom pristupa samom računaru. Može se činiti logičnim da pristup treba ograničiti na ovlašćene korisnike, ali u praksi nije uvek tako.

U slučaju iz Srbije 4 (Drumska mafija) sistem registrovanja pojedinačnih službenika za naplatu putarine sa njihovim jedinstvenim korisničkim imenom nije funkcionisao u praksi. Identifikacioni brojevi su bili vidljivi kolegama, a šefovi smena su često vršili zamene zaposlenih. U slučaju iz Makedonije 5 (Zloupotreba prava administratora - bankarske garancije/uvozne kvote), zaposleni sa administratorskim pravima je otkrio da je posle prelaska iz jednog administrativnog centra u drugi zadržao ovlašćenje za pristup. Potom je kreirao lažni korisnički nalog i iskoristio ga da privremeno promeni podatke o bankarskoj garanciji i u dosluhu sa lokalnim preduzećem počini prevaru na granici. Glavni administrator nije vršio redovne provere i revizije ovlašćenja administratora koji su premešteni na druga mesta, pa je administrator stoga mogao da počini krivična dela koristeći novi korisnički nalog. U drugim primerima, zloupotreba ili krađa lozinki, kao u slučaju sa Kosova 3 (Zloupotreba lozinke), slučaju iz Bosne i Hercegovine 1 (Najpoznatiji bosanski haker istovremeno i tužilac) i slučaju iz Albanije 2 (Korupcija u elektronskom sistemu javnih nabavki), stvaraju mogućnost za pojavu korupcije. Iako se činilo da su u elektronskom sistemu javnih nabavki ispoštovane sve mere opreza i zaštite, zbog sistema elektronske pošte koji je korišćen kao podrška elektronskom sistemu nabavki su propale sve dobre namere, kao što je otkriveno kada je procenu javnih nabavki izvršilo treće lice nakon promene lozinke. U praksi, svi korisnici su imali lozinke jedni drugih. Iako je cela ova aktivnost realizovana sa dobrim namerama da se reše problemi u radu, bezbednost sistema je u generalno time umanjena.

Lozinka i korisničko ime treba uvek da budu lični i tajni. Ono što započne kao prikladan način da se svakodnevni posao pojednostavi, kao što je davanje lozinki kolegama ili podređenima da bi se neki zadatak što pre obavio, ili resetovanje lozinki u standardnu verziju koju znaju drugi pa time više nije tajna, može da se zloupotrebi, kao što su pokazali gore navedeni primeri. Ako je potrebno kolegi poveriti pristup sistemima i podacima, onda sistemi treba to da dozvoljavaju, ali na način: 1) da zaposleni koristi svoje korisničko ime kada se prijavljuje na sistem; 2) da se o pristupu sistemu i podacima vodi datoteka evidencije, i 3) da bude odobren samo ograničen i ciljani pristup i da njegovo trajanje posle određenog vremena istekne.

Odgovarajući nivo pristupa podacima i sistemima

Nekoliko navedenih slučajeva eksplicitno ilustruje šta se može desiti kada nivoi pristupa podacima nisu odgovarajući, tj. kada se dodeli veći pristup sistemima i podacima nego što je potrebno da zaposleni obave neodložive zadatke.

U slučaju iz Makedonije 5 (Zloupotreba prava administratora (bankarske garancije/uvozne kvote)) i slučaju iz Crne Gore 3 (Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre), zaposleni su imali mnogo veći pristup menjanju i unošenju podataka nego što im je zaista bilo potrebno da obave svoj posao. U oba slučaja su zloupotrebili svoje službene položaje i omogućili prikazivanje podataka / dokumenata koji su izgledali zakoniti drugim stranama.

Fizički pristup podacima i dokumentima

Fizički pristup instalacijama na kojima se pohranjuju podaci ili fizičkim kopijama podataka zbog verifikacije, potvrđivanja zakonitosti, itd. treba da bude ograničen naa ovlašćene službenike, čiji se pristup evidentira i prati.

U slučaju iz Hrvatske 2 (Baza sa poverljivim podacima Hrvatske radio televizije na crnom tržištu), kopija baze podataka Hrvatske radio-televizije o pretplatama (registar HRT) je prodata na crnom tržištu. Fizički pristup prostoriji sa serverom na kojem se nalazi registar HRT-a daje se isključivo ovlašćenim licima, ali je pristup bazi podataka moguć i kroz lokalnu mrežu i internet koji koriste tunele za zaštićene podatke. Bez obzira da li je baza podataka kopirana direktno sa servera u prostoriji u kojoj se on nalazi ili sa daljine, autori iz Hrvatske napominju da standardi kojima se ograničava fizički pristup nisu bili primenjeni.

U slučaju iz Crne Gore 4 (Nezakonito izdavanje putnih isprava) autori navode da je neophodno uvesti skeniranje dokumenata ili formirati elektronsku bazu podataka o svim dokumentima koji se podnose i izdaju u štampanom obliku sa obaveznom dvostrukom opcijom rezervne kopije, kako bi se obezbedila zaštita podataka u slučaju njihovog namernog ili slučajnog uništenja. Takođe, potrebno je unaprediti elektronski sistem video nadzora koji beleži fizički pristup prostorijama u kojima se drže spisi i službena dokumenta. Situacija je još složenija u slučaju iz Crne Gore 3 (Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre), gde se javlja kombinacija različitih elektronskih i fizičkih katastara. Ista dokumenta možda potiču iz različitih izvora i ponekad je nemoguće utvrditi ko je tačno kreirao dokumenta i ko ima pun pristup tim dokumentima. U ovom slučaju, postoji zahtev da se dokumenta drže u elektronskom obliku, a pristup kako fizičkim tako i elektronskim regsitrima je dozvoljen samo ovlašćenim licima.

U slučaju iz Srbije 1 (Seks ispred Beogradske arene) sada su uvedene kodirane kartice da se ograniči pristup prostorijama sa instalacijama na kojima se pohranjuju podaci. Upotreba elektronskih prenosivih medija unutar tih prostorija je sada strogo ograničena i praćena

konkretnim procedurama za pristup podacima, ili je u potpunosti zabranjena (u zavisnosti od vrste prostorije i instalacija).

U Crnoj Gori je danas za fizički pristup sistemima, tokom instalacije ili održavanja, za svako angažovano lice neophodno dobiti odobrenje Ministarstva unutrašnjih poslova.

Procedure i standardi bezbednosti

Autori iz Bosne i Hercegovine, Makedonije, Crne Gore i Srbije ukazali su na ISO 27001 standard o upravljanju informacionom bezbednošću i ISO 9001 standard za upravljanje kavlitetom kao konkretne mere zaštite primenjene kao procedure bezbednosti čiji je cilj da se osigura zaštita i integritet podataka. U Bosni i Hercegovini pravosuđe je unapredilo procedure bezbednosti, poput onih što se navode u procedurama ISO 27001, na svim nivoima i primenilo standard ISO/IEC 27001:2005. U Srbiji, Ministarstvo unutrašnjih poslova i Ministarstvo pravde zasebno planiraju da uvedu ISO 27001 u bliskoj budućnosti. U Crnoj Gori, Pravilnik o standardima informacione bezbednosti propisuje standarde informacione bezbednosti koji se primenjuju u okviru realizacije mera informacione bezbednosti propisanih uredbom Vlade Crne Gore. U Makedoniji, Zakon o elektronskom upravljanju propisuje standarde koji moraju da budu zadovoljeni prilikom izrade ICT sistema koji komuniciraju, razmenjuju podatke i dokumenta u javnoj upravi. Dodatne smernice o sprovođenju brojnih kontrolnih elemenata iz serije ISO 27000 uvedene su podzakonskim aktom.

Rezervna kopija (backup) i datoteka evidencije

Datoteka evidencije omogućava da se sistem kasnije proveri i da se utvrdi ko je tačno šta radio i kada. Isto važi i za rezervnu kopiju, pošto su rezervne kopije snimci kako su podaci izgledali u određenom trenutku.

U slučaju sa Kosova 1 (Uništavanje dokaza) svi materijali, koje su istražitelji očekivali da nađu na serverima Ministarstva za javnu upravu i koji bi dokazali sumnje Agencije za borbu protiv korupcije u pogledu neregularnosti i kršenja zakona, bili su izbrisani sa vladinih servera. Dodatnu otežavajuću okolnost u ovom slučaju predstavljala je činjenica da su se serveri za pohranjivanje podataka za cijelu državnu upravu na Kosovu, za sve državne institucije nalazili u ovom ministarstvu. Ti su podaci izbrisani iz okruženja za koje se pretpostavljalo da je jedno od najzaštićenijih za čuvanje podataka na Kosovu.

U slučaju iz Makedonije 4 (Zloupotreba sistema evidentiranja broja radnih sati) istraga datoteke evidencije bila je od ključnog značaja za otkrivanje zloupotrebe. Autori iz Makedonije primećuju da su sada uvedene prakse u skladu sa važećim zakonom, ali pojedine prakse su uvedene bez formalnog uporišta u zakonu ili podzakonskim aktima. Jedna od tih praksi je i vođenje datoteke evidencije za svako pristupanje, dodavanje, brisanje ili izmenu podataka. Ujedno, datoteka evidencije je na zahtev postala dostupna za provere i revizije. Osim vođenja i arhiviranja evidencije, ostale aktivnosti nisu dozvoljene.

I na kraju, tu je slučaj IDDEEA-e (Agencije za identifikaciona dokumenta, evidenciju i razmenu podataka) u Bosni i Hercegovini koja je nadležna za uvođenje razmene podataka između policijskih organa i tužilaca, čime je započela aktivnost koja je dovela do nove generacije razmene podataka u BiH. Jedan od zahteva je pravljenje rezervne kopije podataka na udaljenoj lokaciji sa dobrom lozinkom kao zaštitom, u kombinaciji sa fizičkim obezbeđenjem.

Interoperativnost između ICT sistema javnih organa i formiranje baznih registara

Interoperativnost je termin koji se koristi da opiše sposobnost različitih sistema i organizacija da zajedno rade (uzajamno deluju). Da bi sistemi bili interoperativni potrebno je da razmenjuju podatke. U prepreke za razmenu podataka obično spadaju tehničke, semantičke, organizacione i zakonske barijere, ali bi se tu mogao dodati još jedan element - poverenje. Da bi jedna organizacija svoje podatke otkrila drugoj mora postojati određeni stepen poverenja između strana u toj razmeni. U suprtonom, kako nam govori iskustvo, saradnje više neće biti. Garantovanje integriteta i zaštita podataka od zloupotrebe je od velikog značaja za ineroperativnost, i ključno za realizovanje potencijala elektronske uprave da smanji administrativno opterećenje kroz integraciju instrumenata elektronske uprave: pametnog korišćenja informacija koje građani i preduzeća moraju da daju organima državne uprave da bi završili administrativne procedure, definisanja elektronskih procedura kao dominantnog kanala za pružanje usluga elektronske uprave i načela „samo jednog" evidentiranja potrebnih podataka. Ovim poslednjim se obezbeđuje da građani i preduzeća daju određene standardne informacije samo jednom, jer službe državne uprave preduzimaju radnje da interno razmenjuju te podatke, tako da za građane i preduzeća nema dodatnog opterećenja.

Od posebnog je značaja zaštita integriteta nacionalnih baznih registara. Bazni registri su kameni temeljci moderne elektronske uprave u zemlji i sve više između zemalja. Sastoje se od glavnih baza podataka koje sadrže najnovije kategorije svega što je potrebno vladi i javnom sektoru da postanu efikasna administracija koja nudi dobre usluge (kako elektronske tako i one obične) građanima i preduzećima, kao i da izrađuju i sprovode delotvorne politike. Bazni registri su otelotvorenje načela „samo jedanput". Registri koje najviše srećemo sadrže detalje o svim građanima (datum rođenja, bračni status, datum smrti, adrese, jedinstvene matične brojeve, brojeve pasoša/ličnih karti, itd.) i svim preduzećima (veličinu, godinu osnivanja, broj zaposlenih, sektor poslovanja, dospeli i plaćeni porez, što je često povezano sa registrima koji pokazuju godišnji promet, profit, itd.). Postojanje katastara zemljišta i objekata je takođe uobičajeno, kao i registara vozila, saobraćajne mreže, plovnih puteva, itd. Bazni registri mogu da smanje dupliranje posla koje se javlja kod organa državne uprave i da smanje verovatnoću pravljenja greške. Izrada baznih registara, kao i sistema interoperativnosti koji je za njih potreban da bi ga međusobno delila odgovarajuća ministarstva i agencije, je stoga glavni temelj elektronske uprave.

Međutim, ukoliko su javni ICT sistemi ugroženi ili osetljivi na zloupotrebu, posledice mogu biti dalekosežne i imati teške ekonomske, društvene i pravne implikacije za sve, bez obzira da li se radi o državnoj upravi, građanima, preduzećima, itd.

U slučaju iz Hrvatske 12 (Ni dana života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!) integracijom podataka i konsolidacijom baznih registara između organa, koristeći nacionalni lični identifikacioni broj (mreža za razmenu „OIB"), primenjuje se zaštitna mera „načelo više očiju" te rešavaju problemi opisani u slučaju u trenutku kada je Hrvatski zavod za penzijsko osiguranje (HZPO) integrisan u mrežu za razmenu OIB i kada je sprovedena revizija podataka o penzijama.

Slučajevi iz poglavlja 1 sadrže oba primera onoga što čini sastavni deo baznih registara, kao što su slučaj iz Bosne i Hercegovine 3 (Zloupotreba elektronskog sistema projekta CIPS) i slučaj iz Crne Gore 3 (Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre).

U slučaju iz Bosne i Hercegovine se navodi da je od početka projekta Sistem za zaštitu identifikacije građana (CIPS) 2002. godine bilo dosta pritužbi, naročito kod izdavanja ličnih karata i pasoša, u celoj zemlji. Veoma je opasno da takav, centralni registar bude ugrožen, a autori iz Bosne i Hercegovine primećuju da iako je Agencija za identifikaciona dokumenta, evidenciju i razmenu podataka (IDDEEA), koja je sada nadležna za CIPS, primenila niz različitih mera zaštite i zadovoljava standarde veoma visokog stepena ICT bezbednosti i zaštite, još uvek postoje problemi u pogledu razmene podataka sa drugim organima, nedostatak dogovora između institucija o koordinaciji aktivnosti u okviru elektronske uprave i neprimenjivanja smernica IDDEEA-e u celoj državnoj upravi. Na taj način se slabi ne samo sistem CIPS, već i spremnost organa javne uprave da svoje sisteme učine interoperabilnim.

Slučaj iz Crne Gore 3 odnosi se na opštinski katastar, gde su nedozvoljene izmene podataka omogućile nezakonit prenos zemlje u vlasništvu države iz opštinskog katastra na treće lice. Slučaj je podrazumevao izradu lažne elektronske potvrde koja je kasnije mogla da se koristi u sudskom postupku. U ovom slučaju se ne navode stečena znanja i primena dodatnih mera zaštite. Međutim, ovaj slučaj pokazuje šta se dešava kada je praćenje pristupa zaposlenog neadekvatno i kako može da ugrozi celi registar.

Slučaj iz Makedonije 5 (Zloupotreba prava administratora (bankarske garancije/uvozne kvote)) pokazuje šta se dešava kada jedan organ državne uprave- granična služba - zavisi od informacija i podataka od drugog organa kao garanta za informacije o trećoj strani (bankarska garancija) i gde administrativni službenik unosi vrednost, koja je ograničena stvarnom bankarskom garancijom, umesto da se dobije direktno iz informacionog sistema banke. Autori ne navode da je bilo nekih posledica po saradnju organa državne uprave koji su u ovaj slučaj uključeni, ali se može očekivati da su preduzete mere opreza i da se zahteva integritet podataka.

Praćenje i revizija

Rezervne kopije i datoteke evidencije „tehnički" omogućavaju zaštitne mere praćenja i revizije, ali postoji nekoliko dodatnih pitanja kad se tumači potreba za praćenjem i revizijom ICT sistema.

Između sistema i procesa – najslabija karika

Nekoliko slučajeva iz poglavlja 1 predstavlja primer kako organizacija mora da zaštiti sve svoje procese, ali i pojedinačne korake, kako od elektronske tako i od fizičke zloupotrebe. Čak i „savršeni" ICT sistemi su onoliko bezbedni a podaci pouzdani koliko su to njihove ulazne informacije. Ako se u ICT sisteme unesu lažni podaci, ugrožen je integritet celog sistema. Praćenje i revizija se moraju proširiti na sve poslovne procese i sisteme, bez obzira da li su oni fizički ili elektronski.

U slučaju iz Albanije 4 (Pronevera i falsifikovanje u knjigovodstvu) službenica nadležna za knjigovodstvo je proneverila novac tako što je falsifikovala platni spisak. Nakon što bi (u štampanom obliku) dobila pisano odobrenje, menjala je elektronske podatke na platnom spisku kao i podatke koje su slali banci. Pošto nije bilo revizije usaglašenosti odštampanog primerka i elektronske evidencije, između ova dva „postupka" postojala je slaba veza. Autori iz Albanije takođe navode nedostatak provera od strane finansijskog sistema, koji nije mogao istovremeno da obradi pojedinačne detalje sa platnog spiska i uporedi ih sa ukupnim iznosom. Dalje, između finansijskih organa nije bilo ni uzajamne provere različitih potpisanih dokumenata za potrebe isplate plata.

U slučaju sa Kosova 2 (Dobijanje statusa ratnog invalida) zloupotreba je izvršena tokom skeniranja, kada je falsifikovan medicinski dokument. Učinilac F.M. je dostavio dokument pomoću kojeg je tvrdio da je tokom rata na Kosovu imao zdravstvenih problema. Dokument nije bio iz ratnog perioda, već je izrađen 5 godina kasnije. Na njemu su bili datumi kao da je napisan tokom rata.

Primer falsifikovanog pasoša, kome je istekao period važenja i koji je koristilo treće lice u slučaju iz Crne Gore 1 (Zloupotreba službenog položaja i falsifikovanje zvaničnih dokumenata), pokazuje grešku ili problem u informacionom sistemu Ministarstva unutrašnjih poslova (MUP) za izdavanje pasoša, koji bi trebao da eliminiše rizike od korišćenja ili ponovnog izdavanja putnih isprava kada im istekne period važenja. Sistem nije povezao fizičku ispravu (pasoš) sa preslikanom evidencijom iz baze podataka koja sadrži potpuno iste informacije, uključujući fotografiju vlasnika pasoša. Dalje, nije bilo elektronskih tragova u sistemu koji bi identifikovali službenika koji je izdao falsifikovani pasoš. Osetljivost sistema u ovom slučaju ogledala se u nekoherentnosti između stvarnog i dokumentovanog pasoša sa jedne strane i sistema MUP-a sa druge.

I na kraju, slučaj sa Kosova 4 (Falsifikovanje poreskih dokumenata) ilustruje šta se dešava kada niko ne proverava da li postoji neka slaba tačka ili veza. U ovom slučaju, vlasnik preduzeća koje je imalo ugovor sa javnim institucijama za usluge čišćenja je iskoristio svoju

„snagu" zahvaljujući dobrim odnosima koje je imao sa poreskim službenicima. Nakon jedne inicijalne uplate poreza na visoku vrednost, u svim ostalim javnim nadmetanjima je koristio istu potvrdu, ali sa falsifikovanim datumima. Svi službenici institucija mogu da zatraže originalni dokument, ali u ovom slučaju nisu želeli to da urade, jer su videli da im se obraća starija osoba, pa su naveli da je skenirani dokument zadovoljavao uslove. Međutim, to niko nije proverio, pa stoga takvo nešto predstavlja osetljivost sistema. Ovde imamo slučaj u kojem su službenici mogli da zaštite postupak javnih nabavki tako što bi tražili uvid u poreski dokument, ali niko to nije uradio.

Praćenje i revizija, kao i zakonske i proceduralne mere zaštite, treba da se prošire i obuhvate sve sisteme i procese (elektronske i fizičke) koje sprovode javne institucije.

Problemi sa izdvajanjem poslova (outsourcing) i rizici vezani za IT izvođače

Slučaj iz Makedonije 2 (Napad na IT sistem javnih nabavki) predstavlja interesantan slučaj u kojem elektronski sistem javnih nabavki primenjuje sve moguće tehničke mere zaštite, ali postane osetljiv na DDoS napad zbog toga što je smešten u zajedničkom okruženju sa ISP. Iako makedonske vlasti nisu dokazale zloupotrebu službenog položaja i korupciju, slučaj nudi pregled postupka i moguće načine zloupotrebe IT sistema u svrhe korupcije, kroz zloupotrebu službenog položaja ili društveni inženjering. Administrator sistema ima puna ovlašćenja u sistemu duži vremenski period i ako se njegove ili njene aktivnosti ne kontrolišu ili ne prate na odgovarajući način, može da zloupotrebi sistem na način što će uništiti ili izmeniti digitalne dokaze, zbog čega je nemoguće sprovesti istragu i dokazati zloupotrebu.

Slučaj iz Srbije 2 (Kada IT izvođač „pusti korenje") predstavlja slučaj u kome IT izvođač ima internu kontakt osobu koja manipuliše podacima i postupcima u korist izvođača na način što mu produžava povoljan ugovor o izdvajanju poslova. Zakoni i propisi o javnim nabavkama u Srbiji su od tada promenjeni, ali je ozloglašeni službenik iskoristio svoje poznavanje sistema i zahteva da bi favorizovao određenog IT izvođača i smanjio troškove tog izvođača. Službenik je sakrio ili učinio nedostupnim podatke o pristupu IT izvođača VPN WAN sistemu i uništio elektronsku dokumentaciju u sistemu tako da državni organi (MPDU, a kasnije novo MP) nisu mogli da kontrolišu, prate i nadziru sistem.

U slučaju iz Albanije 3 (Zloupotreba IT u svrhe korupcije kod distributera električne energije), distributer električne energije je većim delom bio privatizovan. Koristeći šemu većih računa za struju, lažnih očitavanja strujomera pomoću PDA uređaja radnika, i na osnovu navoda za druge slučajeve da su elektronski podaci menjani u IT sistemu preduzeća nakon što bi bili uneti pomoću PDA, oni su potrošačima naplaćivali veće račune za utrošenu električnu energiju. Cilj upotrebe PDA uređaja i postupaka za očitavanje strujomera je u početku bio da obezbede izdavanje tačnog računa za utrošenu energiju. Međutim, neovlašćen pristup i falsifikovanje podataka, možda (još uvek nije dokazano) čak uz pomoć rukovodstva, uništava poverenje koje je javnost imala u pošten postupak očitavanja strujomera.

I na kraju, naša zbirka slučajeva zloupotrebe ICT u svrhe korupcije obuhvata i tri primera prevare i pronevere u preduzećima za naplatu putarine (slučaj iz Hrvatske 8, slučaj iz Makedonije 1 i slučaj iz Srbije 4)[88]. U slučajevima iz Hrvatske i Makedonije, naplata putarine je bila izdvojena i poverena privatnim preduzećima, dok je u Srbiji preduzeće bilo u potpunosti u vlasništvu države. Uz postojanje različitih šema, od jednostavne prevare koju su počinili zaposleni u slučajevima iz Makedonije i Hrvatske, do razrađene i sofisticiranije šeme u primeru iz Srbije, rizik od prevare i pronevere je uvek prisutan tamo gde postoji direktna naplata a nema odgovarajućeg praćenja rada zaposlenih. U slučajevima iz Hrvatske i Makedonije, slučajevi zloupotrebe su otkriveni internom revizijom. U slučaju iz Srbije, javilo se interno lice koje je prijavilo korupciju i ukazalo na zloupotrebu. U sva tri slučaja kasnije su primenjene pojačane tehničke mere zaštite i praćenje rada zsposlenih.

Kada se ICT sistemi izdvoje i povere nekome drugome, državni organi i institucije moraju u ugovoru sa IT izvođačem obezbediti da mogu da prate i vrše reviziju sistema na isti način na koji bi to radili da je u pitanju neki interni sistem, ali u još većoj meri, jer izdvajanje poslova i njihovo poveravanje privatnim preduzećima generalno podrazumeva gubitak kontrole nad sistemima.

Organizacione i proceduralne mere zaštite

U Albaniji, svaki državni organ ili institucija koja menja ili postavlja informacioni sistem sada mora da dobije ocenu projekta i da stručnjaci iz Nacionalne agencije za informaciono društvo nemaju primedbe na opis posla. Dalje, primopredaja sistema od strane izvođača naručiocu iz javnog sektora kroz postupak „prijema radova na informacionom sistemu" ima za cilj da obezbedi bolji integritet i kvalitet informacionih sistema u javnom sektoru. U Bosni i Hercegovini, IT sistemi policije i službenici koji rade na njima se sada redovno proveravaju od strane nadležnih organa. U skladu sa Uredbom o merama informacione bezbednosti, u Hrvatskoj je sada propisano planiranje postupaka u vanrednim situacijama (definisanje postupaka koje treba slediti u slučaju bezbednosnog incidenta i za obezbeđivanje kontinuiteta funkcionisanja). Autori iz Makedonije su zapazili trend potpisivanja ugovora o poverljivosti između ekonomskih operatora i izvršilaca u kojem se obe strane slažu da ne objavljuju informacije o licima koja imaju pristup sistemu. Pored toga, u makedonskim institucijama sada je prihvaćena praksa razdvajanja uloga tehničkih administratora i administratora sadržaja (podataka). Tehnički administratori su nadležni za sistem na nivou aplikacija i upravljanja ovlašćenjima i pristupom korisnika. Administratori sadržaja su nadležni za upravljanje podacima pohranjenim u bazama podataka, ali ne i za upravljanje samim sistemima. U Crnoj Gori, Ministarstvo za informaciono drustvo i telekomunikacije je izradilo nekoliko pravilnika koji propisuju standarde, zaštitu podataka, upravljanje incidentima, sadržaj i način vođenja evidencije o sertifikaciji pružaoca usluga, elektronski potpis, pristup portalu elektronske uprave i korišćenje interne mreže državnih organa. I na kraju, u Srbiji su Ministarstvo unutrašnjih poslova i Ministarstvo pravde sad sproveli procedure kojima se

88 Slučaj iz Hrvatske 8 (Svake godine nestane 2 miliona evra sa naplatnih rampi), slučaj iz Makedonije 1 (Zloupotreba IT sistema na naplatnim rampama) i slučaj iz Srbije 4 („Drumska mafija")

uređuje pristup podacima, u cilju zaštite od zloupotrebe. Osim toga, u Ministarstvu pravde niko ne može pristupiti podacima bez prethodnog odobrenja od strane suda ili tužilaštva, čak ni visoko rangirani službenici.

Zaštita primenom načela „više očiju"

Pojedini primeri iz poglavlja 1 ilustruju „jednostavnu" primenu načela „više očiju". Na primer, slučaj iz Hrvatske 5 (Policajac uhvaćen dok je unosio falsifikovane podatke u informacioni sistem policije) u kojem je šef policijske stanice primetio potvrdno pismo u informacionom sistemu Ministarstva unutrašnjih poslova, ili slučaj iz Makedonije 4 (Zloupotreba sistema evidentiranja broja radnih sati) u kojem je preraspodela zadataka dovela do toga da je novi administrator pogledao datoteku evidencije iz sistema za registrovanje radnog vremena, te na taj način sproveo reviziju koristeći „načelo više očiju" i otkrio nedoslednost.

U slučaju iz Hrvatske 12 (Ni dana života niste bili zaposleni? Nema problema, i dalje možete dobiti punu penziju!), konsolidacijom podaka u registru OIB (OIB = lični (osobni) identifikacioni broj) postiže se primena „načela više očiju". U slučaju sa Kosova 4 (Falsifikovanje poreskih dokumenata) je to načelo moglo biti ostvareno da su službenici u različitim državnim institucijama, koje su bile naručioci, samo insistirale na potvrđivanju tačnosti poreskog dokumenta, a zloupotreba bi bila otkrivena mnogo ranije i postupak javne nabavke bi bio zaštićen načelom „više očiju". Isti nedostatak uzajamne provere važi i za slučaj iz Crne Gore 3 (Zloupotreba službenog položaja i unošenje netačnih podataka u javne registre) u kojem su za izmene opštinskog katastra nedostajale organizacione i proceduralne mere zaštite, kao što je „načelo više očiju". Uzajamna provera statusa zemljišta i vlasništva nije obavljena ni tehnički, ni od strane drugog zaposlenog lica u opštinskom katastru niti od strane eksterne revizije.

Etički kodeks

Kao mogući ishod slučaja iz Hrvatske 9 i 10 o zloupotrebi IT u svrhe korupcije od strane policajaca i slučaja iz Hrvatske 11 (Viši inspektor zloupotrebio poverljive podatke kako bi pobedio na lokalnim izborima!), za državne službenike usvojen je Etički kodeks, a zaposleni u Ministarstvu unutrašnjih poslova i Ministarstvu finansija su obavezni da ga poštuju. Ono što je jednako važno je da građani mogu da prijave neetičko ponašanje zaposlenih u javnoj upravi nadležnim službenicima za etiku.

Otvoreni podaci i vlada, omogućavanje javnosti da pomogne u zaštiti integriteta i tačnosti podataka

Autori iz Makedonije navode otvorenu vladu i otvorene podatke kao primer aktivnosti usmerenih protiv korupcije koje omogućavaju građanima da igraju aktivniju ulogu u sprečavanju i prepoznavanju korupcije. Otvaranjem vladinih podataka se može omogućiti pri-

mena „načela više očiju" kroz učešće građana u proveri podataka, na primer konačnog i imovinskog statusa funkcionera. Znamo iz prethodne studije ReSPA-e iz 2012. godine[89] da su u to vreme Hrvatska, Srbija i Makedonija počinjale sa sprovođenjem određenih inicijativa u oblasti otvorenih podataka.

Obuka, etika i svest o integritetu

U Albaniji je u toku realizacija inicijative Nacionalne agencije za računarsku bezbednost koja u saradnji sa Albanskom školom za javnu upravu organizuje obuke za skoro sve službenike zadužene za IT u javnim institucijama. Usavršavanje obuhvata računarsku bezbednost, zaštitu i procenu rizika. U Bosni i Hercegovini danas postoje moduli obuke za tužioce na temu npr. računarskog kriminala i veština komuniciranja.

U Hrvatskoj, Uredba o merama informacione bezbednosti propisuje podizanje svesti o računarskoj bezbednosti, na primer prilikom definisanja bezbednosnih pravila i edukacije zaposlenih. Zaposleni u Ministarstvu unutrašnjih poslova učestvuju u raznim obukama i projektima podizanja svesti o rizicima od zloupotrebe ICT u svrhe korupcije i merama zaštite. Primeri su dva projekta čiji je cilj jačanje administrativnih kapaciteta Ministarstva unutrašnjih poslova u suzbijanju kibernetičkog kriminala, kao i projekat Regionalna saradnja i krivično pravosuđe: jačanje kapaciteta u borbi protiv kibernetičkog kriminala. Projekat takođe obuhvata organizovanje radionica o forenzičkim mrežama od strane Ministarstva unutrašnjih poslova i Hrvatske akademske i istraživačke mreže.

U Srbiji, Ministarstvo pravde i Ministarstvo unutrašnjih poslova sada obučavaju svoje zaposlene o rizicima od zloupotrebe ICT u svrhe korupcije.

U Makedoniji, Strategija reforme javne uprave i Akcioni plan za njeno sprovođenje propisuju obuku i kampanje podizanje svesti o korupciji i za državne službenike i za građane. Crna Gora nudi edukaciju korisnika u oblasti informacione bezbednosti i sprečavanja računarskih bezbednosnih incidenata.

Samo se za Kosovo navodi da ne postoje mere ili planovi za organizaciju obuka i podizanje svesti državnih službenika o rizicima i merama zaštite od zloupotrebe ICT u srvhe korupcije.

Lica koja prijavljuju korupciju (zviždači)

Neka krivična dela će biti otkrivena samo zahvaljujući internim izvorima koji „zvone na uzbunu" da bi ukazali na pravo stanje stvari, što posebno važi ako je rukovodstvo uključeno u korupciju. Slučaj sa Kosova 4 (Falsifikovanje poreskih dokumenata) i slučaj iz Srbije 4 (Drumska mafija) ilustruju da rukovodstvo i/ili cela organizacija mogu da se ne obaziru na

89 ReSPA, Regionalna uporedna studija o elektronskoj upravi (2012), dostupna na: http://respaweb. eu/download/doc/Regional+comparative+eGov+study+-+web.pdf/dfab3d5a78e0d10e9-a6a80827e36a277.pdf

zloupotrebu službenog položaja, prevaru na radu, proneveru i organizovani kriminal, čime se stvara kultura u kojoj su svi „umešani" u zloupotrebu, ne usuđuju se da nešto po tom pitanju urade i prihvataju takvu situaciju, zbog toga što se ili boje odmazde zbog otkrivanja zloupotrebe ili nemaju od toga nikakve koristi.

Ljudski faktor

Čak i kada se ispoštuju sve mere zaštite od zloupotrebe ICT u svrhe korupcije, nema garancije da sistemi neće biti zloupotrebljeni. Uvek će postojati situacije kao što je nezakonit nalog rukovodioca da se izvuče elektronska pošta u slučaju iz Srbije 3 (Viši državni zvaničnik špijunira zaposlene) ili u slučaju iz Albanije 2 (Korupcija u elektronskom sistemu javnih nabavki) u kojem je većina korisnika bila nezadovoljna, naročito periodičnim promenama složenih lozinki, zbog čega su tražili prečice i ostavljali lozinke nepromenjene sa standardnom verzijom koju bi im na početku, kod prvog prijavljivanja, obezbedio administrator.

Svest među zaposlenima o ozbiljnosti pretnji koje ugrožavaju sisteme će biti od ključnog značaja da se ti sistemi zaštite i sačuvaju. Tu spada svest ne samo o implikacijama po bezbednost, već i o dimenzijama državne službe koje se odnose na etiku i integritet. Državni službenici moraju biti svesni kako svojih prava tako i svojih obaveza, a zemlje pojedinačno moraju da utvrde modalitete koji podržavaju etičko ponašanje.

Zakonodavne mere zaštite

Autori iz pojedinačnih zemalja navode celi niz zakonskih propisa i državnih strategija iz oblasti kao što su: administrativne procedure, elektronska dokumenta, tajni podaci, elektronski potpis, zaštita ličnih podataka, javne nabavke, korupcija i krivični zakonici. Ovom studijom nije predviđena izrada komparativne analize mera zaštite propisanih u svakoj od obuhvaćenih zemalja, jer su navedeni kao dodatak da se pokažu zakonske mere zaštite bitne za pojedinačne navedene slučajeve.

Interesantna stvar koju smo saznali iz ove studije je činjenica da ima slučajeva u kojima su zakonom propisane mere bile neodgovarajuće kao zaštita od zloupotrebe ICT u svrhe korupcije.

Autori sa Kosova su naveli da: „U smislu administrativnih mera zaštite, Kosovo je usvojilo set zakona, strategija i administrativnih uputstava (normativnih akata) koja se odnose na korišćenje informaciono-komunikacionih tehnologija, ali se zakonodavna infrastruktuara do sada nije na odgovarajući način bavila pitanjem integriteta podataka i zloupotrebom sistema informacione tehnologije u konkretnom ili opštem smislu."

Svega je nekoliko primera u ovoj studiji koji opisuju neodgovarajuće zakonske mere za zaštitu od zloupotrebe ICT u svrhe korupcije, a time i saznanja koja treba izvući. U slučaju

iz Makedonije 2 (Napad na IT sistem javnih nabavki), pravila javnih nabavki izgleda ne uzimaju u obzir situaciju u kojoj je elektronski postupak dostavljanja ponuda prekinut iz „tehničkih razloga". U drugom primeru koji se ticao nabavki, slučaj iz Srbije 2 (Kada IT izvođač „pusti korenje"), navodi se da je IT izvođač zaustavio novi tenderski postupak koristeći složeni i dugotrajni proces podnošenja žalbi koji je moguć zbog „rupa" u Zakonu o javnim nabavkama. Zakon je od tada izmenjen („Službeni list Republike Srbije", br. 124/12).

U slučaju iz Srbije 1 (Seks ispred Beogradske arene) interni administrativni propisi su dopunjeni i sada obuhvataju: 1) neovlašćen pristup podacima Ministarstva unutrašnjih poslova je sada propisan ne kao disciplinski prekršaj, već kao krivično delo; i 2) upotreba podataka za bilo koju drugu namenu osim one izvorne zbog koje su podaci prikupljeni je sada propisana kao krivično delo (a ne samo disciplinski prekršaj).

Slučajevi u ovoj studiji su samo primeri. Nema reprezentativnih informacija na osnovu kojih bi se mogli izvući bilo kakvi zaključci u pogledu opštih nedostataka u merama zaštite propisanim zakonima.

3. Preporuke u pogledu politike za smanjenje rizika od zloupotrebe ICT

Pripremili Tilman Hoppe i Louise Thomasen

Deo 1 – Preporuke namenjene ekspertima za borbu protiv korupcije

Svaki akter uključen u sprečavanje korupcije treba da prihvati ICT ne samo kao instrument u borbi protiv korupcije, već i kao rizik da se počini korupcija. U tom smislu, za eksperte za borbu protiv korupcije su potrebne sledeće mere:

1. Eksperti za borbu protiv korupcije treba blisko da sarađuju na prepoznavanju i sprečavanju rizika od zloupotrebe ICT u svrhe korupcije.

2. Organi za sprečavanje korupcije treba u svoje kataloge standardnih rizika od korupcije da uključe i mogućnost zloupotrebe ICT u svrhe korupcije. Procene rizika u državnoj upravi treba da obuhvate bezbednost IT od zloupotrebe u svrhe korupcije. Procene rizika treba da anliziraju i provere sve IT elemente nabrojane kasnije u tekstu (Deo 2 preporuka).

3. Rukovodioci javnih organa i institucija kao i funkcioneri treba da budu svesni rizika koji postoje u ICT u pogledu korupcije. Organi za sprečavanje korupcije treba aktivno da nude savete o popunjavanju bezbednosnih praznina u IT sistemu državne uprave.

4. Organi za sprečavanje korupcije i centri za profesionalno usavršavanje treba da nude obuke o rizicima povezanim sa zloupotrebom ICT u svrhe korupcije i u te obuke treba uključiti eksperte za IT.

5. Nacionalnim strategijama i akcionim planovima treba dodati poglavlje o sprečavanju korupcije koja je povezana sa zloupotrebom IT. Ako se neke druge strategije (npr. o elektronskoj upravi ili reformi državne uprave) već detaljno i sveobuhvatno bave jačanjem IT u cilju sprečavanja zloupotrebe, politika borbe protiv korupcije treba onda barem da uključi upućivanje na druge strategije i da obezbedi koordinaciju između eksperata za borbu protiv korupcije i IT eksperata o reformskim merama.

6. Organi za sprovođenje zakona i sprečavanje korupcije treba da sakupe statističke podatke o zloupotrebi IT u svrhe korupcije, da analiziraju obrasce ponašanja i u skladu sa tim usvoje reformske mere.

Deo 2 – Preporuke namenjene ekspertima za elektronsku upravu

1. Pristup svim sopstvenim podacima i sistemima mora da bude zaštićen kontrolom pristupa uz korišćenje privatnih korisničkih imena i lozinki.

2. U nadležnosti je rukovodstva svakog javnog organa i institucije da obezbedi da je pristup podacima na odgovarajućem nivou. Pristup sopstvenim podacima treba dozvoliti kada je to potrebno za hitno obavljanje radnih zadataka.

3. Fizički pristup prostorijama sa instalacijama na kojima se pohranjuju podaci ili fizičke kopije treba ograničiti i omogućiti ovlašćenim licima čiji se pristup i evidentira i prati.

4. Javne organizacije moraju da primene standarde informacione bezbednosti, kao što si ISO 27001 kako bi se podaci zaštitili i obezbedio njihov integritet.

5. Za svaku javnu organizaciju treba izraditi planove za oporavak od otkazivanja sistema i kontinuitet rada u slučaju bezbednosnih incidenata. Planovi moraju da definišu procedure koje treba slediti u slučaju incidenta, kako upravljati poslovnim kontinuitetom, da utvrde nadležnosti u pogledu organizacije aktivnosti u hitnim situacijama i budu usaglašeni u tom pogledu.

6. Sve javne organizacije treba da sprovedu postupke pravljenja rezervne kopije (back-up) sa periodičnom izradom rezervene kopije za sve sisteme i podatke. Tu spadaju i desktop i prenosivi računari. Rezervne kopije treba fizički smestiti negde van organizacije.

7. Datoteka evidencije je deo strukture praćenja i nadzora u organizaciji, a predstavlja i važan instrument za reviziju. Kopije datoteke evidencije takođe treba držati na nekoj lokaciji van organizacije i/ili odvojeno od same aplikacije. Lica zadužena za menjanje sadržaja (podataka) ne treba da budu (tehnički) administratori datoteke evidencije.

8. Javni organi i institucije moraju da obezbede da nijedan njihov proces, bez obzira da li je fizički ili elektronski, ne bude osetljiv na zloupotrebu u svrhe korupcije. Ugroženi proces ili korak u procesu će uticati na sve druge procese sa kojima je povezan. ICT sistemi koji se oslanjaju na ulazne informacije iz drugih sistema ili procesa su onoliko bezbedni od korupcije koliko i sistemi i procesi sa kojima su povezani.

9. Bazni registri zahtevaju posebne i strože mere zaštite jer su oni, u suštini, kameni temeljci koherentne interoperabilne elektronske uprave.

10. Izdvajanje poslova (outsourcing) razvoja, održavanja ili postavljanja IT zahteva povećan oprez javne organizacije koja izdvaja te poslove i poverava ih drugima. Odgovornost se nikada ne može izdvojiti. Prilikom izdvajanja ovih poslova, obezbedite

da je pristup podacima dozvoljen samo ovlašćenim imenovanim licima i da se oni prate i proveravaju.

11. Potrebno je razdvojiti uloge službenika zaduženih za podatke (sadržaj) i službenika zaduženih za sisteme (tehnologiju).

12. Revizije sistema i praćenje proteklih aktivnosti nikada ne treba da prati i administrira isti IT administrator.

13. Nadzor i primena načela „više očiju" treba da bude sastavni deo, ne samo tokom projektovanja i razvoja sistema, već i u svakodnevnom radu.

14. Otvoreni podaci vlade i učešće građana u proveravanju podataka iz javnog sektora mogu da obezbede i „proveru stvarnog stanja" i poboljšanje kvaliteta podataka, ali i da otkriju nepravilnosti i zloupotrebu. U ovom kontekstu, takođe je važno građanima ponuditi kanale kojima će vladi i javnom sektoru davati povratne informacije. U slučaju korupcije/nepravilnosti, službenici za etiku kojima građani mogu da prijave neetičko ponašanje državnih službenika mogu da budu takav kanal.

15. Potrebno je obezbediti da obukama i podizanjem svesti o etici i integritetu budu obuhvaćeni i kadrovi zaduženi za ICT.