VODIČ ZA IKT SISTEME OD POSEBNOG ZNAČAJA:

INFORMACIONA BEZBEDNOST

SHARE FONDACIJA

oebs Organizacija za evropsku bezbednost i saradnju Misija u Srbiji

Шведска Sverige

РЕПУБЛИКА СРБИЈА РАТЕЛ РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Република Србија Министарство трговине, туризма и телекомуникација

VODIČ ZA IKT SISTEME OD POSEBNOG ZNAČAJA:

INFORMACIONA BEZBEDNOST

VODIČ ZA IKT SISTEME OD POSEBNOG ZNAČAJA: INFORMACIONA BEZBEDNOST
SHARE FONDACIJA
NOVEMBAR 2019.
UREDNICI: DANILO KRIVOKAPIĆ, NATALIJA RADOJA
AUTORI: DANILO KRIVOKAPIĆ, ANDREJ PETROVSKI, DUNJA TASIĆ, SONJA KOLUNDŽIJA
OBRADA TEKSTA: BOJAN PERKOV
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: BEOPRINT
TIRAŽ: 1000

Publikacija je izrađena uz finansijsku podršku Švedske agencije za međunarodnu razvojnu saradnju, u okviru projekta Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji.

LISTA POJMOVA I SKRAĆENICA

LISTA POJMOVA I SKRAĆENICA

IKT sistem - informaciono-komunikacioni sistem

MTTT - Ministarstvo trgovine, turizma i telekomunikacija Republike Srbije

Nacionalni CERT - Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima

NIS direktiva - Direktiva EU o merama za visok nivo bezbednosti mrežnih i informacionih sistema u EU br. 2016/1148

Poseban CERT - Poseban centar za prevenciju rizika u IKT sistemima

RATEL - Regulatorna agencija za elektronske komunikacije i poštanske usluge Republike Srbije

CERT - Centar za prevenciju bezbednosnih rizika u IKT sistemima (eng. *Computer Emergency Response Team*)

CERT organa vlasti - Centar za bezbednost IKT sistema u organima vlasti

CERT samostalnog operatora IKT sistema - Centri za prevenciju bezbednosnih rizika IKT sistema Ministarstva odbrane, Ministarstva unutrašnjih poslova, Ministarstva spoljnih poslova i službi bezbednosti

PREDGOVOR

PREDGOVOR

Nove tehnologije menjaju svet i nesumnjivo omogućavaju koristi za društvo i građane, ali paralelno sa tehnološkim razvojem dolaze i novi, sve opasniji i zahtevniji bezbednosni izazovi.

Republika Srbija je na vreme prepoznala značaj zaštite informacija i digitalne infrastrukture i 2016, na predlog Ministarstva trgovine, turizma i telekomunikacija, donet je Zakon o informacionoj bezbednosti. Godine 2019. usvojene su i izmene i dopune ovog zakona, kojima je uspostavljena još bolja povezanost svih relevantnih aktera u oblasti informacione bezbednosti, jačanje kapaciteta Nacionalnog CERT-a i kontinuirana saradnja CERT-ova u Republici Srbiji. U 2017. godini, takođe na predlog ovog ministarstva, doneta je Strategija razvoja informacione bezbednosti i Akcioni plan, kojima su usvojene mere koje se odnose na bezbednost IKT sistema, informacionu bezbednost građana, borbu protiv visokotehnološkog kriminala i informacionu bezbednost Republike Srbije.

Ministarstvo trgovine, turizma i telekomunikacija uspostavilo je jedinstveni sistem za prijem informacija o incidentima koji su u isto vreme vidljivi u Nacionalnom CERT-u. Takođe, ovo ministarstvo osnovalo je inspekciju za informacionu bezbednost, koja osim što nadzire rad IKT sistema od posebnog značaja, pruža i savetodavnu pomoć u implementaciji propisa.

Budući da je saradnja ključna u ovoj oblasti, jedan od najznačajnijih mehanizama koji je uspostavljen jeste Telo za koordinaciju informacione bezbednosti, osnovano od strane Vlade Republike Srbije, koje čine predstavnici relevantnih organa i kojim rukovodi Ministarstvo trgovine, turizma i telekomunikacija.

Iako je na ovom polju mnogo učinjeno, predstoji još dosta rada u nadogradnji kapaciteta i jačanju relevantnih institucija. Izgradnja poverenja između privatnog i javnog sektora je još jedan od imperativa za razvoj sajber bezbednosti. Neophodno je podizanje svesti ne samo zaposlenih u javnom i privatnom sektoru, već i stanovništva, kako bi se rizici koji u ovoj oblasti prete smanjili na najmanju moguću meru.

Saradnja i poverenje, međuresorno, međusektorsko, kao i međunarodno, su ključne reči kada je u pitanju oblast informacione bezbednosti i u tom pravcu svakako bi trebalo da se nastavi i ubuduće. Ovaj vodič, koji objedinjuje sve neophodne informacije za IKT sisteme od posebnog značaja, nesumnjivo doprinosi pregledu stanja kao osnove za razvoj informacione bezbednosti.

Tatjana Matić, državni sekretar u Ministarstvu trgovine, turizma i telekomunikacija Republike Srbije

UVOD

UVOD

Razlozi donošenja Zakona o informacionoj bezbednosti

Zaštita informaciono-komunikacionih sistema konačno je našla svoje mesto u pravnom poretku Srbije, usvajanjem prvog Zakona o informacionoj bezbednosti[1] 26. januara 2016. godine. Pre donošenja ovog Zakona, materija informacione bezbednosti kod nas nije bila regulisana, što je dovodilo do brojnih propusta i sajber incidenata. Jedan od najozbiljnijih sajber incidenata u skorijoj prošlosti kod nas je svakako kompromitovanje matičnih brojeva građana Srbije na sajtu Agencije za privatizaciju 2014. godine, kada je utvrđeno da je na ovom sajtu 10 meseci javno dostupan bio dokument sa ličnim podacima preko pet miliona građana.[2]

Propusti poput ovakvog ukazali su na ozbiljnu potrebu da se donese nacionalni zakon koji bi regulisao materiju informacione bezbednosti, naročito informacionih sistema koji kontrolišu kritičnu infrastrukturu (tzv. IKT sistemi od posebnog značaja) u eri sofisticiranih tehničkih napada i ubrzanog razvoja sajber oružja. Informaciona bezbednost je ništa drugo do skup mera koji omogućavaju da podaci kojima se rukuje putem informaciono-komunikacionih sistema budu zaštićeni od neovlašćenog pristupa, odnosno da se zaštite njihovi integritet i autentičnost.

Predmet Zakona o informacionoj bezbednosti

Zakon o informacionoj bezbednosti reguliše mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima (u daljem tekstu: IKT sistemi), odgovornosti pravnih lica prilikom upravljanja i korišćenja IKT sistema, nadležne organe za sprovođenje mera zaštite i reguliše koordinaciju između tela nadležnih za sprovođenje mera zaštite.

Zakon je, između ostalog, regulisao osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika (Nacionalni CERT) kao tela zaduženog za koordinaciju prevencije i zaštite od bezbednosnih rizika u IKT sistemima na nacionalnom nivou, a u velikoj meri se pozabavio regulisanjem tzv. IKT sistema od posebnog značaja i njihovim merama zaštite. Predviđeno je i osnivanje Tela za koordinaciju poslova informacione bezbednosti sa ciljem ostvarivanja saradnje u okviru nacionalne bezbednosti i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti, kao i uspostavljanje Inspekcije za informacionu bezbednost koja bi trebalo da vrši inspekcijski nadzor nad primenom Zakona.

Donošenjem Zakona nametnuta je jasna obaveza privatnim i javnim subjektima da primene odgovarajuće mere zaštite informacionih sistema, što se naročito odnosi na IKT sisteme od posebnog značaja kao sisteme koji se koriste za poslove državnih organa, obradu posebnih vrsta podataka o ličnosti i obavljanje delatnosti od opšteg interesa, poput elektronskih komunikacija.

Zakon o informacionoj bezbednosti je usvojen u periodu pre usvajanja Direktive EU o merama za visok nivo bezbednosti mrežnih i informacionih sistema u EU br. 2016/1148 (eng. *Network and Information Security Directive*, tzv. NIS direktiva), koja je usvojena jula 2016. godine. Uprkos činjenici da je naš zakon donet pre usvajanja NIS direktive, u velikoj meri je bio usklađen sa njom.

Izmene i dopune Zakona iz 2019. godine

Krajem oktobra 2019. godine, Skupština je usvojila Zakon o izmenama i dopunama Zakona o informacionoj bezbednosti[3] iz 2016. godine, kako bi se Zakon dodatno uskladio sa NIS direktivom, kao i da bi

1 Zakon o informacionoj bezbednosti ("Sl. glasnik RS", br. 6/2016)
2 SHARE Fondacija, Agencija za privatizaciju – jedinstven slučaj, 24. mart 2016. Dostupno na: resursi.sharefoundation.info
3 Zakon o izmenama i dopunama Zakona o informacionoj bezbednosti ("Sl. glasnik RS", br. 77/2019)

se postojeća zakonska rešenja unapredila u skladu sa potrebama koje je pokazala dosadašnja praksa u primeni takvih rešenja.

Izmenama Zakona menjaju se, proširuju i dopunjuju pojmovi značajni za informacionu bezbednost, osnažuju se kapaciteti Nacionalnog CERT-a; jača se institucionalna saradnja između Nacionalnog i posebnih CERT-ova; u Telo za koordinaciju poslova informacione bezbednosti uključuje se i Narodna banka Srbije; uspostavlja se obaveza vođenja evidencija IKT sistema od posebnog značaja od strane nadležnog organa itd.

Međutim, treba napomenuti da do momenta donošenja navedenih izmena Zakona, Inspekcija za informacionu bezbednost nije započela svoj rad u punom kapacitetu, tako da ne postoji ni statistika njihovih aktivnosti, pa samim tim ni statistika kako su relevantni subjekti uskladili svoje delovanje sa Zakonom.

Donošenje podzakonskih akata

Nakon donošenja Zakona 2016. godine, Vlada Republike Srbije je donela četiri uredbe kojima detaljnije uređuje same IKT sisteme od posebnog značaja, mere zaštite, sadržaj opšteg akta, te postupanje u slučaju incidenata, čime je pravni okvir za postupanje operatora IKT sistema od posebnog značaja zaokružen.

U "Službenom glasniku RS", broj 94/2016 od 24. novembra 2016. godine, objavljene su sledeće uredbe:

1) Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja;
2) Uredba o bližem uređenju mera zaštite IKT sistema od posebnog značaja;
3) Uredba o utvrđivanju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste IKT sistemi od posebnog značaja, i
4) Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u IKT sistemima od posebnog značaja.

Kome je namenjen ovaj Vodič?

Ovaj Vodič namenjen je pre svega **operatorima IKT sistema od posebnog značaja** - pravnim licima, organu vlasti ili organizacionoj jedinici organa vlasti koji koristi IKT sistem od posebnog značaja u obavljanju poslova iz svoje nadležnosti, i to sledećim kategorijama lica radno angažovanih kod operatora IKT sistema od posebnog značaja:

1) Rukovodiocima operatora IKT sistema od posebnog značaja koji moraju imati osnovna znanja o značaju informacione bezbednosti, naročito s obzirom na to da su upravo oni prekršajno odgovorni u slučaju nepoštovanja odredbi Zakona i Uredbi, a u slučaju ozbiljnijih propusta mogu građanski i krivično odgovarati;
2) Tehničkim ekspertima koji su zaduženi za informacionu bezbednost IKT sistema od posebnog značaja, te je u tom smislu posebno obrađena svaka od 28 mera zaštite koje se moraju primeniti; kao i
3) Rukovodiocima pravnih službi u čijoj je nadležnosti izrada i donošenje Akta o bezbednosti koji je bilo potrebno doneti do najkasnije do 2. marta 2017. godine.

NAČELA - OSNOVNI ZAKONSKI KONCEPTI

NAČELA - OSNOVNI ZAKONSKI KONCEPTI

Zakon uspostavlja temelje sistema informacione bezbednosti sa četiri načela i propisuje da se prilikom planiranja i primene mera zaštite IKT sistema treba rukovoditi sledećim načelima:

1) **Načelo upravljanja rizikom –** podrazumeva da se izbor i nivo primene mera se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanja posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti.

Rizici u kontekstu informacione bezbednosti su svi **potencijalni događaji** koji mogu da ugroze integritet informacionog sistema. Oni mogu biti različite prirode i porekla, kao što su ljudski faktor, greške, hakerski napad, gubljenje podataka, različite pretnje po fizički integritet opreme, itd. Procena rizika se obavlja aktivno u svim fazama životnog ciklusa IKT sistema - od projektovanja, do tranzicije u novi IKT sistem.

2) **Načelo sveobuhvatne zaštite –** podrazumeva da se mere primenjuju na svim organizacionim, fizičkim i tehničko-tehnološkim nivoima, kao i tokom celokupnog životnog ciklusa IKT sistema.

Mere zaštite IKT sistema se primenjuju u svim fazama životnog ciklusa IKT sistema i u svim njegovim aspektima. Sistem je bezbedan koliko i njegova najslabija karika, pa je stoga podjednako važna implementacija mera zaštite u centralnom i perifernim delovima sistema, te svih sistema koji direktno komuniciraju sa IKT sistemom od posebnog značaja.

Kada su u pitanju distribuirani sistemi, mere se primenjuju na sve pojedinačne instance sistema, ali i na komunikacione kanale koji ih povezuju. Implementacija se sprovodi sveobuhvatno i jednovremeno za sve delove sistema.

3) **Načelo stručnosti i dobre prakse –** podrazumeva da se mere primenjuju u skladu sa stručnim i naučnim saznanjima i iskustvima u oblasti informacione bezbednosti.

Dinamika implementacije i revizije uslovljena je promenama u sferi informacione bezbednosti koje su praktično svakodnevne. Komunikacija sa tačkama kao što su CERT-ovi ključna je u prevenciji napada, te u pristupu bazi znanja i pozitivnih praksi. Ekspertiza industrije i akademije neophodan je resurs za operatore IKT sistema od posebnog značaja.

4) **Načelo svesti i osposobljenosti –** podrazumeva da sva lica koja svojim postupcima efektivno ili potencijalno utiču na informacionu bezbednost treba da budu svesna rizika i poseduju odgovarajuća znanja i veštine.

Sva lica koja su povezana sa IKT sistemom od posebnog značaja moraju imati znanje i svest o rizicima i incidentima. Inicijalne i periodične edukacije koje sprovode eksperti za informacionu bezbednost doprinose podizanju svesti o samom sistemu, rizicima, prevenciji, blagovremenom prijavljivanju incidenata i potencijalnih rizika, te unapređuju ličnu i profesionalnu odgovornost prilikom upravljanja incidentima i rizicima.

NADLEŽNI ORGANI

NADLEŽNI ORGANI

Organi nadležni za sprovođenje Zakona o informacionoj bezbednosti su: Ministarstvo trgovine, turizma i telekomunikacija; Nacionalni CERT; Ministarstvo odbrane, CERT organa vlasti; CERT samostalnog operatora IKT sistema; Telo za koordinaciju poslova informacione bezbednosti i posebni CERT-ovi.

MINISTARSTVO TRGOVINE, TURIZMA I TELEKOMUNIKACIJA

Nadležni organ koji vrši nadzor nad primenom zakona je ministarstvo nadležno za poslove informacione bezbednosti, odnosno **Ministarstvo trgovine, turizma i telekomunikacija.**

MTTT vrši poslove inspekcije za informacionu bezbednost preko Inspekcije za informacionu bezbednost, utvrđuje da li su IKT sistemi ispunili uslove propisane Zakonom i nalaže mere IKT sistemima. Dodatno, MTTT vodi veb stranicu i jedinstveni sistem za prijem obaveštenja o incidentima operatora IKT sistema od posebnog značaja, nadzire rad Nacionalnog CERT-a, ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema i preduzima preventivne mere za bezbednost i zaštitu dece na internetu (edukacija, informisanje, davanje saveta i slično).

Izmenama i dopunjama Zakona iz 2019. godine uvedena je obaveza MTTT-a da uspostavlja i vodi evidenciju IKT sistema od posebnog značaja i stavlja je na raspolaganje Nacionalnom CERT-u. Ova evidencija bi trebalo da sadrži osnovne identifikacione podatke IKT sistema od posebnog značaja. Postojeći operator IKT sistema od posebnog značaja ima obavezu da se upiše u evidenciju u roku od 90 dana od dana usvajanja Pravilnika o upisu u registar koji donosi MTTT, odnosno u roku od 90 dana od uspostavljanja novog IKT sistema od posebnog značaja.

NACIONALNI CERT

Nacionalni CERT je telo koje obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou.

Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL). Ovakvo telo postoji u 102 zemlje sveta, odnosno u gotovo svim evropskim zemljama.

Nadležnosti nacionalnih CERT-ova se, u zavisnosti od specifičnosti infrastrukture, razlikuju od države do države, ali to je uvek ekspertska organizacija čija je glavna nadležnost koordinacija i komunikacija na nacionalnom i međunarodnom nivou, radi prevencije i upravljanja rizicima u ovoj oblasti.

Nacionalni CERT je nadležan da prati incidente na nacionalnom nivou, da pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima, da reaguje po prijavljenim ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja.

Ovo telo takođe prati prijavljene incidente na nacionalnom nivou i na osnovu prikupljenih podataka kontinuirano izrađuje analize rizika i incidenata, podiže svest kod građana, privrednih subjekata i organa javne vlasti o značaju informacione bezbednosti, vodi evidenciju Posebnih CERT-ova, te izveštava MTTT kao Nadležni organ na kvartalnom nivou o preduzetim aktivnostima. Bitno je razumeti da Nacionalni CERT najčešće neće biti u po-

ziciji da reaguje i pomogne IKT sistemima u kriznim i hitnim situacijama, s obzirom na to da su njegove nadležnosti u ovom momentu prevashodno preventivnog karaktera.

Izmene i dopune Zakona iz 2019. godine uređuju i obradu podataka o ličnosti lica koje se obrati Nacionalnom CERT-u, te nabraja koje konkretno lične podatke Nacionalni CERT može tom prilikom obrađivati, a svrha takve obrade je evidentiranje podnetih prijava, informisanje podnosioca o statusu predmeta i eventualno upućivanje prijave nadležnim organima radi daljeg postupanja.

POSEBNI CERT-OVI

Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica, upisana u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT.

Poseban CERT (Poseban centar za prevenciju rizika u IKT sistemima) takođe obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima, ali u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično. Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica sa sedištem na teritoriji Republike Srbije. Za razliku od Nacionalnog CERT-a koji ima ulogu podizanja svesti o mogućim bezbednosnim rizicima, pruža upozorenja, prati incidente na nacionalnom nivou i koordiniše informacije koje dobija, posebni CERT-ovi imaju operativniju ulogu da konkretno brane IKT sisteme na koje su fokusirani, odnosno u okviru kojih su formirani. Na taj način, posebni CERT-ovi se specijalizuju za određenu oblast ili grupu, te prate stanje i reaguju u slučaju incidenata samo za tu oblast ili grupu. Na ovaj način posebni CERT-ovi stiču posebna znanja i iskustva za određene oblasti i spremniji su da pruže specijalizovanu pomoć. U toku 2017. godine doneti su poseban Pravilnik koji utvrđuje uslove za upis u evidenciju posebnih CERT-ova[4] i Procedura za upis u evidenciju posebnih CERT-ova,[5] koja propisuje uslove za upis.

CERT ORGANA VLASTI

CERT organa vlasti (Centar za bezbednost IKT sistema u organima vlasti) obavlja poslovne koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti, osim IKT sistema samostalnih operatora. Poslove CERT-a organa vlasti obavlja organ nadležan za projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa, odnosno Kancelarija za informacione tehnologije i elektronsku upravu.

CERT organa vlasti je zadužen za zaštitu Jedinstvene informaciono-komunikacione mreže elektronske uprave i koordinaciju i saradnju sa operatorima IKT sistema koje povezuje ova mreža u cilju prevencije incidenata, otkrivanja i prikupljanja informacija o incidentima i otklanjanju njihovih posledica, kao i davanje stručnih preporuka za zaštitu IKT sistema organa vlasti, osim kada su u pitanju IKT sistemi za rad sa tajnim podacima.

CERT SAMOSTALNOG OPERATORA IKT SISTEMA

Samostalni operatori IKT sistema su Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo spoljnih poslova i službe bezbednosti. Navedena ministarstva i službe su u obavezi da for-

4 Pravilnik o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima ("Sl. glasnik RS", br. 12/2017)

5 Procedura za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima (RATEL, br. 1-05-031-9/17, 26. maj 2017). Dostupno na: ratel.rs

miraju **sopstvene centre za bezbednost IKT sistema radi upravljanja incidentima u svojim sistemima**, koji mogu razmenjivati informacije o incidentima, kao i sa Nacionalnim CERT-om i sa CERT-om organa vlasti, a po potrebi i sa drugim organizacijama.

TELO ZA KOORDINACIJU POSLOVA INFORMACIONE BEZBEDNOSTI

Ovo telo radi na ostvarivanju saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti.

Vlada Republike Srbije je osnovala Telo za koordinaciju poslova informacione bezbednosti 3. marta 2016. godine, a čine ga predstavnici institucija čije su nadležnosti povezane sa poslovima informacione bezbednosti. Telom rukovodi predstavnik MTTT-a, dok su u njegovom sastavu predstavnici Ministarstva odbrane, Ministarstva unutrašnjih poslova, Ministarstva spoljnih poslova, Ministarstva pravde, Bezbednosno-informativne agencije, Vojno-obaveštajne agencije, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Direkcije za elektronsku upravu, Generalnog sekretarijata Vlade, CERT-a organa javne vlasti (Kancelarija za informacione tehnologije i elektronsku upravu) i Nacionalnog CERT-a (RATEL). U skladu sa izmenama Zakona iz 2019. godine, u sastav Tela za koordinaciju poslova informacione bezbednosti će ulaziti i predstavnici Narodne banke Srbije.

U skladu sa obaveštenjem MTTT-a, *"zadatak Tela za koordinaciju je da ostvaruje saradnju između organa i usklađuje obavljanje poslova u funkciji unapređenja informacione bezbednosti, inicira i prati preventivne i druge aktivnosti u oblasti informacione bezbednosti, predlaže mere za unapređenje informacione bezbednosti u Republici Srbiji, daje sugestije i predloge koji se odnose na pripremu strateških dokumenata, podzakonskih akata i politika informacione bezbednosti u Republici Srbiji, i utvrđuje međusobnu saradnju u slučaju incidenata koji mogu da imaju znatan uticaj na narušavanje informacione bezbednosti u Republici Srbiji."*[6]

Značajno je napomenuti da Zakon predviđa i formiranje stručnih radnih grupa u koje se uključuju i predstavnici drugih organa javne vlasti, privrede, akademske zajednice i nevladinog sektora. Telo za koordinaciju je u skladu sa Odlukom o obrazovanju Tela za koordinaciju poslova informacione bezbednosti[7] donelo poslovnik o svom radu koji nije dostupan onlajn. Odluka predviđa i obavezu Tela za koordinaciju da Vladi podnosi izveštaje o svom radu jednom godišnje, koji takođe nisu dostupni onlajn.

MINISTARSTVO ODBRANE

Ministarstvo odbrane nadležno je za poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih prozvoda, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja i druge poslove predviđene Zakonom.

6 Ministarstvo trgovine, turizma i telekomunikacija RS, Obrazovano Telo za koordinaciju poslova informacione bezbednosti, 7. mart 2016. Dostupno na: mtt.gov.rs

7 Odluka o obrazovanju Tela za koordinaciju poslova informacione bezbednosti ("Sl. glasnik RS", br. 24/2016, 53/2017, 79/2017, 112/2017 i 93/2018)

IKT SISTEMI OD POSEBNOG ZNAČAJA

IKT SISTEMI OD POSEBNOG ZNAČAJA

IKT sistemi od posebnog značaja su informaciono-komunikacioni sistemi koji su od velike važnosti za državu, jer u slučaju hakerskog napada ili drugog kompromitovanja takvih sistema, to može imati direktan nepovoljan uticaj na veliki broj građana. Dakle, IKT sistemi od posebnog značaja su sistemi koji se koriste u obavljanju poslova u organima vlasti, za obradu tzv. posebnih podataka o ličnosti kao najosetljivijih podataka, odnosno koji se koriste u obavljanju delatnosti od opšteg interesa.

Preciznije, Zakon o informacionoj bezbednosti u članu 6 definiše 3 osnovne kategorije IKT sistema od posebnog značaja i to:

1) Sistemi koji se koriste u obavljanju poslova u organima vlasti

Ukoliko imate status organa vlasti, vaša informaciona infrastruktura će imati status IKT sistema od posebnog značaja.

Zakon daje definiciju organa vlasti - to su državni organi, organi autonomne pokrajine, organi jedinice lokalne samouprave, organizacije i drugo pravno ili fizičko lice kome je povereno vršenje javnih ovlašćenja.

2) Sistemi koji se koriste za obradu posebnih vrsta podataka o ličnosti

Određeni podaci o ličnosti su "ličniji" od drugih, a njihovom obradom se dublje zadire u privatnost građana kao osnovno ljudsko pravo, te je stoga ovim podacima potrebno dati drugačiji status kako bi mere njihove zaštite bile strože u odnosu na ostale podatke o ličnosti. Novi Zakon o zaštiti podataka o ličnosti (ZZPL)[8] u skladu s tim definiše posebne vrste podataka o ličnosti i to su: podaci kojima se oktriva rasno i etničko poreklo, političko mišljenje, versko ili filozofsko uverenje, članstvo u sindikatu, genetski podaci, biometrijski podaci u cilju jedinstvene identifikacije lica, podaci o zdravstvenom stanju, seksualnom životu i seksualnoj orjentaciji lica.

Zakon o informacionoj bezbednosti propisuje da se u slučaju obrade podataka o ličnosti (u koje spadaju i posebne vrste podataka o ličnosti) prilikom vršenja nadležnosti i ispunjenja obaveza iz ovog Zakona, mora postupati u skladu sa ZZPL-om, koji propisuje niz obaveza u vezi sa obradom i zaštitom integriteta podataka o ličnosti od strane lica koja obrađuju takve podatke.

3) Sistemi koji se koriste u obavljanju delatnosti od opšteg interesa i drugim delatnostima

Zakon izričito definiše oblasti u kojima se obavljaju delatnosti od opšteg interesa dok su ovi poslovi i delatnosti precizno definisani Uredbom o utvrđivanju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja:

1) u oblasti proizvodnje, prenosa i distribucije električne energije

1 - proizvodnja, prenos i distribucija električne energije;

2 - proizvodnja i prerada uglja;

3 - istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata;

4 - istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa.

8 Zakon o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 87/2018)

2) saobraćaj:

1 - železnički, poštanski, vodni i vazdušni saobraćaj.

3) zdravstvo:

1 - zdravstvena zaštita.

4) bankarstvo i finansijska tržišta:

1 - poslovi finansijskih institucija;

2 - poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;

3 - poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta.

5) digitalna infrastruktura:

1 - razmena internet saobraćaja;

2 - upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS).

6) dobra od opšteg interesa:

1 - korišćenje, upravljanje zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja).

7) usluge informacionog društva:

1 - usluge informacionog društva u smislu zakona kojim se uređuje elektronska trgovina.

8) ostale oblasti:

1 - elektronske komunikacije;

2 - izdavanje službenog glasila Republike Srbije;

3 - upravljanje nuklearnim objektima;

4 - proizvodnja, promet i prevoz naoružanja i vojne opreme;

5 - upravljanje otpadom;

6 - komunalne delatnosti;

7 - proizvodnja i snabdevanje hemikalijama.

Obaveze operatora IKT sistema od posebnog značaja

Izmenama i dopunama Zakona o informacionoj bezbednosti iz 2019. godine predviđen je novi član koji utvrđuje obaveze operatora IKT sistema od posebnog značaja.

U skladu sa navedenim, svaki operator IKT sistema od posebnog značaja ima obavezu da:

1 - upiše IKT sistem od posebnog značaja u evidenciju operatora IKT sistema od posebnog značaja;

2 - preduzme mere zaštite IKT sistema od posebnog značaja;

3 - donese akt o bezbednosti IKT sistema;

4 - vrši proveru usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje;

5 - uredi odnos sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom, ukoliko poverava aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima;

6 - dostavlja obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema;

7 - dostavi tačne statističke podatke o incidentima u IKT sistemu.

MERE ZAŠTITE IKT SISTEMA OD POSEBNOG ZNAČAJA

MERE ZAŠTITE IKT SISTEMA OD POSEBNOG ZNAČAJA

Operator IKT sistema od posebnog značaja odgovara za bezbednost IKT sistema i preduzimanje mera zaštite IKT sistema. Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

Mere zaštite IKT sistema su detaljno propisane Uredbom o bližem uređenju mera zaštite IKT sistema od posebnog značaja:

1. USPOSTAVLJANJE ORGANIZACIONE STRUKTURE (ČLAN 2 UREDBE)

Organizaciona struktura operatora IKT sistema od posebnog značaja treba da se reflektuje u IKT sistemu. Preciznije, pristup IKT sistemu od posebnog značaja treba da bude uslovljen radnim zaduženjima i obavezama koje svako od zaposlenih ima u opisu svog radnog mesta, s ciljem da se smanji rizik od zloupotreba, neovlašćenih pristupa, narušavanja integriteta podataka u IKT sistemu i ljudske greške.

Sam IKT sistem od posebnog značaja treba da se bazira na principima "*Security by design*" i "*Privacy by design*".

Sistem takođe treba da ima mogućnost praćenja aktivnosti zaposlenih kako bi se, ukoliko je to potrebno, mogla utvrditi odgovornost prilikom zloupotreba. Specifična odgovornost zaposlenih jeste da prijave zabeležene bezbednosne incidente u okviru IKT sistema od posebnog značaja svojim nadređenima, u skladu sa Zakonom o infomacionoj bezbednosti. "*Security by design*" i "*Privacy by design*" predstavljaju principe razvoja informacionih sistema na takav način da se u svakoj fazi razvoja imaju u vidu bezbednost sistema i integritet podataka. Drugim rečima, to znači da su tokom celog životnog ciklusa IKT sistema premise bezbednosti i privatnosti validne. Principi se takođe primenjuju na sve nadogradnje, promene i postupke prestanka korišćenja bilo kog dela IKT sistema.

2. BEZBEDAN RAD NA DALJINU I BEZBEDNA UPOTREBA MOBILNIH UREĐAJA (ČLAN 3 UREDBE)

Najčešći oblici IKT sistema su distribuirani i imaju više korisnika, što znači da obuhvataju više različitih uređaja koji su na neki način umreženi. Dinamika i potrebe rada često zahtevaju da se unos, obrada ili prikaz podataka u okviru IKT sistema vrši sa više lokacija, a ponekad i dinamički (kroz mobilne uređaje) sa terena. Korišćenje mobilnih uređaja i pristup na daljinu mogu biti izazov u bezbednosti IKT sistema budući da koriste javne mreže (internet, GSM) kako bi komunicirali sa centralnim IKT sistemom. Uspostavljanjem veze između centralnog sistema, mreže ili servera i spoljašnjeg računara ili mobilnog uređaja, otvara se mogućnost za MitM (*Man in the Middle*) napade.

MitM je vrsta tehničkog napada u kom klijent i server nisu nužno izloženi opasnosti, ali napadač koristi nedostatke veze kako bi pristupio njihovoj komunikaciji i izvršio krađu podataka.

Bezbedan način za rad na daljinu je povezivanje putem VPN-a (*Virtual Private Network* - virtuelna privatna mreža). Reč je o usluzi stvaranja izdvojenog tunela između dva računara na javnoj mreži, koji se posebno kodira radi zaštite.

Pored same veze između mobilnog uređaja ili računara uspostavljene putem javnih mreža, kroz VPN, treba voditi računa i o terminalnoj opremi, odnosno o samim računarima i mobilnim uređajima koji se koriste za pristup IKT sistemu. Za ove uređaje važe svi bezbednosni standardi koji su na snazi za uređaje u okviru centralnog IKT sistema.

3. EDUKACIJA O NAČINU FUNKCIONISANJA I ODGOVORNOSTI ZAPOSLENIH KOJI KORISTE IKT SISTEM (ČLAN 4 UREDBE)

Operatori IKT sistema od posebnog značaja trebalo bi da posvete pažnju konstantnoj edukaciji zaposlenih u oblasti bezbednosti IKT sistema.

Pre svega, potrebno je usvojiti Akt o bezbednosti informacionog sistema od posebnog značaja koji bliže uređuje oblast bezbednosti IKT sistema, a koji će u potpunosti biti u skladu sa zahtevima Zakona o informacionoj bezbednosti, Uredbe o bližem uređenju IKT sistema od posebnog značaja, Uredbe o bližem sadržaju akta o bezbednosti IKT sistema od posebnog značaja i drugih podzakonskih akata. Istovremeno, treba da sadrži i bliže odrednice o primeni propisa u delatnosti kojom se operator IKT sistema od posebnog značaja bavi.

Vrste i načine za sprovođenje edukacije najpogodnije je klasifikovati u odnosu na radni staž zaposlenog i to:

1. Prilikom započinjanja radnog odnosa:

- Novozaposleni treba da se upozna sa internim aktom o bezbednosti IKT sistema od posebnog značaja, te da potpiše izjavu o tome, čime formalno preuzima odgovornost za postupanje sa IKT sistemom u skladu sa internim aktima, odnosno Zakonom o informacionoj bezbednosti.

- Novozaposleni treba da potpiše izjavu o poverljivosti informacija do kojih dolazi u toku obavljanja redovnih i vanrednih radnih aktivnosti.

2. U toku radnog odnosa:

- Interni akt o bezbednosti IKT sistema od posebnog značaja mora biti stalno dostupan svim zaposlenima na internom portalu IKT sistema od posebnog značaja;

- U definisanim vremenskim intervalima treba organizovati obuke za zaposlene koji rade u okviru IKT istema od posebnog značaja. Suština ovih obuka bi trebalo da bude ne samo u objašnjavanju pravnih propisa, već u analizi konkretnih primera kršenja zakona i loše prakse.

U definisanim vremenskim intervalima bi takođe trebalo organizovati testiranje zaposlenih iz oblasti bezbednosti IKT sistema. Testiranje bi, pored čisto teorijskih pitanja, trebalo da bude zasnovano na studiji slučaja iz delokruga rada IKT sistema od posebnog značaja, gde bi se od zaposlenih očekivalo da odgovore na pitanje šta bi uradili, odnosno kako bi postupili u konkretnoj situaciji.

U slučaju odgovornosti zaposlenog za narušavanje bezbednosti IKT sistema od posebnog značaja, operator je dužan da pokrene odgovarajući postupak.

4. ZAŠTITA OD RIZIKA KOJI NASTAJU PRI PROMENAMA POSLOVA ILI KADROVSKIM PROMENAMA (ČLAN 5 UREDBE)

Operator IKT sistema od posebnog značaja ima obavezu da ugovorom ili drugim internim pravnim aktom preciznije uredi dužnosti i obaveze zaposlenog ili na drugi način angažovanog lica koje radi u IKT sistemu od posebnog značaja, a koje ostaju na snazi pri promeni poslova ili nakon prestanka radnog odnosa ili angažovanja.

Zaposleno ili na drugi način angažovano lice nakon prestanka ili promene radnog angažovanja nema pravo da otkriva poverljive ili druge informacije koje mogu da utiču na bezbednost IKT sistema od posebnog značaja.

5. IDENTIFIKACIJA I KLASIFIKACIJA INFORMACIONIH DOBARA U OKVIRU IKT SISTEMA (ČLAN 6 UREDBE)

Operator IKT sistema je dužan da formira bazu informacionih dobara, opreme i softvera koji se koriste za izradu, obradu, čuvanje, prenos, brisanje i unošenje podataka u okviru IKT sistema od posebnog značaja.

Baza mora da odražava realno stanje IKT sistema i da svaki unos u bazu bude označen sa adekvatnim nivoom osetljivosti i kritičnosti. Takođe, za svaki segment IKT sistema, uređaj, softver ili podatak treba da bude naznačena osoba koja je odgovorna za njegovu bezbednost, odnosno integritet.

6. KLASIFIKOVANJE PODATAKA (ČLAN 7 UREDBE)

Nivo zaštite podataka u okviru IKT sistema od posebnog značaja mora da odgovara osetljivosti i važnosti podataka, te štete koja može nastati usled neovlašćenog otkrivanja, izmene, brisanja ili uništenja podataka i da bude u skladu sa propisima koji uređuju pitanja zaštite podataka kao što su poslovna tajna, tajni podaci i podaci o ličnosti. Operator IKT sistema od posebnog značaja ima obavezu da izradi sistem klasifikacije podataka kojim će se odrediti njihov nivo zaštite u skladu sa navedenim principima, a nakon izvršene procene rizika u okviru IKT sistema od posebnog značaja i u skladu sa propisima koji regulišu tajne, odnosno osetljive podatke.

Prilikom procene rizika u okviru IKT sistema, treba voditi računa o naročito ranjivim delovima sistema, kao što su delovi IKT sistema koji su iz legitimnih razloga dostupni trećim licima, te o nastalim rizicima i prevenciji budućih rizika, kao i o vanrednim okolnostima.

7. ZAŠTITA NOSAČA PODATAKA (ČLAN 8 UREDBE)

Nosači podataka su sve vrste memorijskih predmeta i uređaja koji se koriste za skladištenje i prenos podataka. Ovaj segment opreme obuhvata diskove koji su fiksni deo IKT sistema, ali i uređaje i nosače koji se koriste za prenos podataka, kao što su USB *Flash* memorije, eksterni

diskovi, CD, DVD i ostali predmeti i komponente koji imaju mogućnost čuvanja i prenosa podataka.

Prvi korak u zaštiti nosača podataka je definisati koji nosači mogu da se koriste u okviru IKT sistema, a u zavisnosti od operativnih potreba. Takođe, treba propisati da lica koja rade u okviru IKT sistema ne mogu da koriste svoje lične ili uređaje i medije trećih lica kako bi skladištili ili prenosili podatke unutar i izvan IKT sistema od posebnog značaja.

Upotreba neproverenih uređaja i medija predstavlja veliki bezbednosni rizik koji otvara mogućnost unošenja malicioznog softvera u IKT sisteme od posebnog značaja. Dalje, treba jasno definisati da uređaji koji se koriste u okviru IKT sistema od posebnog značaja ne mogu da se koriste u drugim IKT sistemima dok se podaci koji su na njima bili zapisani trajno ne unište.

Procedura skladištenja podataka u okviru IKT sistema od posebnog značaja, u skladu sa nivoom osetljivosti i kritičnosti podataka, treba da inkorporira mehanizme enkripcije i zaštite integriteta podataka. Ovaj princip se primenjuje i prilikom prenosa podataka sa jednog uređaja na drugi, odnosno prenos podataka treba da se vrši putem enkriptovanih kanala (VPN) ukoliko ne postoji mogućnost da se uređaji fizički povežu.

Kontrola pristupa podacima koji se nalaze na određenom uređaju ili mediju, u skladu sa nivoom osetljivosti i kritičnosti, treba da bude regulisana korisničkim imenom i sigurnosnom lozinkom, dok u okviru IKT sistema od posebnog značaja mora da postoji sistem beleženja događaja i aktivnosti, kako bi postojao pregled o ''životnom veku'' podataka, od trenutka nastanka do trajnog brisanja ili uništenja.

8. KONTROLA PRISTUPA IKT SISTEMU OD POSEBNOG ZNAČAJA (ČLANOVI 9, 10 I 11 UREDBE)

Obavljanje osnovne delatnosti operatora IKT sistema od posebnog značaja povezano je sa rukovanjem podacima koji se nalaze u IKT sistemu. Zbog toga je neophodno da zaposlenima bude omogućen pristup različitim podacima u okviru sistema. Međutim, pristup zaposlenih ovim podacima treba da bude usaglašen sa procesnom strukturom organizacionog sistema. Zaposlenima je potrebno obezbediti pristup samo onim podacima i delovima IKT sistema koji su im potrebni za realizaciju aktivnosti za koje su nadležni, a ne kompletnom IKT sistemu. Stoga je potrebno prilagoditi prava pristupa IKT sistemu opisima poslova iz važećeg pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mesta. Takođe, ukoliko je operator IKT sistema od posebnog značaja implementirao sistem upravljanja kvalitetom, potrebno je usaglasiti prava pristupa zaposlenih sa njihovim ulogama u procedurama.

Neophodno je osigurati da je pristup IKT sistemu od posebnog značaja omogućen samo onima koji za to imaju pravni osnov, uz odgovarajuću evidenciju svakog pristupa i eventualnog ažuriranja. Zbog toga je neophodno implementirati sistem korisničkih rola, kojim će biti definisani odgovarajući nivoi prava pristupa prikupljenim podacima u IKT sistemu od posebnog značaja. Sistem rola mora precizno da definiše najpre kojim podacima korisnik kome je dodeljena određena rola uopšte može da pristupi, a zatim i na koji sve način može da ih obrađuje. Operator IKT sistema od posebnog značaja mora da uspostavi mehanizam kreiranja i ukidanja korisničkih naloga, te da vodi evidenciju svih korisničkih naloga u okviru IKT sistema, kako aktivnim, tako i ukinutim nalozima. Operator propisuje procedure

dodele i ukidanja naloga, te provere adekvatnog nivoa pristupa i dodele jedinstvene identifikacione oznake svakog naloga.

Pristup IKT sistemu od posebnog značaja se bazira na podacima za autentifikaciju, kao što su lozinke, kriptografski ključevi i tokeni. Distribuciju i čuvanje ovih podataka reguliše operator, kako bi se sprečile bezbednosne pretnje poput otkrivanja podataka za autentifikaciju zaposlenih (kolegama, porodici ili trećim licima) ili zapisivanje šifre u notesu ili na nalepnici.

Osnovno pravilo pri kreiranju lozinke jeste izbegavanje podataka iz privatnog života kao što su datum rođenja, ime kućnog ljubimca, omiljeno mesto i slično, kao i bilo kakve reči prirodnog jezika. Klasične metode probijanja lozinke danas podrazumevaju automatizovane pretrage po spiskovima reči (*dictionary attack*) a koji mogu obuhvatati na milione pojmova iz različitih jezika.

Šifra od 12 brojeva ima 1.000.000.000.000 kombinacija, preciznije 10^12, šifra od 12 znakova koja sadrži cifre, velika i mala slova i specijalne karaktere ima 475.920.310.000.000.000.000.000 kombinacija, imajući u vidu da je ukupan broj svih alfanumeričkih i specijalnih karaktera 94.

Šifra od 12 brojeva ili manje, može se razbiti za manje od sat vremena. Sa tehnologijom u slobodnoj prodaji, potrebno je oko pet miliona godina da bi se probila šifra iste dužine koja, osim brojeva, sadrži velika i mala slova i specijalne karaktere.

Kod informacionih sistema predviđenih za veliki broj korisnika, administratori uobičajeno automatski generišu inicijalne lozinke. Neretko, lozinke se korisnicima šalju elektronskom poštom, što nije bezbedan kanal komunikacije. Da bi se eliminisao rizik od presretanja poruke koja sadrži lozinke, ne treba ih slati mejlom. Prilikom razvoja IKT sistema, sistem treba postaviti tako da administrator kreira naloge samo sa korisničkim imenima, a da se korisnicima prepusti mogućnost da sami postave lozinku prilikom prve prijave u sistem, koristeći adekvatan digitalni sertifikat ili token kako bi potvrdili svoj identitet.

Sve lozinke se čuvaju u bazama ili datotekama koje se nalaze na serverima. Takve baze se moraju enkriptovati, tako da ni sam sistem administrator ne može da ih pročita. Iz praktičnih razloga administratoru treba ostaviti mogućnost da resetuje lozinke.

Jak sistem autentifikacije podrazumeva više od jednog zahteva prilikom pristupa - ne samo korisničku lozinku, već i kvalifikovani sertifikat. Dvostruka provera podrazumeva zahtev za potvrdu identiteta lozinkom i sertifikatom. Prednost korišćenja ovakvog sistema nalazi se u dodatnoj prepreci, u slučaju da je lozinka ukradena.

Pored IKT sistema od posebnog značaja, dvostruku proveru bi trebalo koristiti i za ostale naloge zaposlenih (mejl, nalozi na društvenim mrežama, finansijske aplikacije i slično). Digitalni sertifikati se mogu primeniti na više načina, ali je najjednostavnije distribuirati ih u obliku smart kartica ili USB tokena. Ukoliko se koriste sertifikati u obliku kartica, za njihovu upotrebu neophodni su odgovarajući čitači, dok se USB tokeni koriste preko postojećeg USB ulaza na računaru.

9. ENKRIPCIJA (ČLAN 12 UREDBE)

Zaštitu podataka u IKT sistemu od posebnog značaja omogućava enkripcija, odnosno šifrovanje podataka tako da ih je nemoguće rastumačiti bez šifre. Budući da računar sve sadržaje tretira kao brojeve, bez obzira da li je reč o tekstu ili slikama, proces šifrovanja praktično prevodi podatke u veliki skup besmislenih znakova koji se obrnutim procesom, uz pomoć jedinstvenog ključa, vraćaju u prvobitni oblik.

Korišćenje mehanizama (algoritama) za enkripciju mora da bude standardizovano na nivou operatora IKT sistema od posebnog značaja, te je potrebno voditi računa o kripto ključevima i "*hash*" vrednostima koji se koriste za ovu vrstu zaštite.

Operator mora da propiše adekvatne načine generisanja, čuvanja, distribucije, povlačenja i brisanja kripto ključeva. Ključevi se moraju čuvati u enkriptovanoj bazi sa visoko restriktivnim pristupom, a osoba koja je zadužena za bezbednost sistema i ima visok nivo pristupa IKT sistemu, treba da bude ovlašćena za njihovu administraciju, sa posebno visokim nivoom odgovornosti.

10. FIZIČKA ZAŠTITA SISTEMA OD POSEBNOG ZNAČAJA (ČLANOVI 13 I 14 UREDBE)

Prostorije operatora IKT sistema od posebnog značaja treba da imaju adekvatnu fizičku zaštitu u vidu alarmnih sistema i sistema za kontrolu pristupa (korišćenjem identifikacionih kartica i sl). Prostorije u kojima se nalaze oprema i dokumenti koji su sastavni deo IKT sistema od posebnog značaja treba da budu bezbedne zone u okviru objekta operatora.

Svi serveri treba da budu smešteni u posebnoj server sali, u kojoj se poštuju određene sigurnosne mere. Pristup sali mora biti ograničen na službenike iz IT sektora koji su zaduženi za održavanje sistema, servera, mreže i telekomunikacija.

Takođe, sala se mora zaključavati sigurnosnom bravom. Na serverima treba da bude jasno označena njihova namena, odnosno funkcija i broj pod kojim su zavedeni u bazu informacionih dobara. Serveri treba da budu zaštićeni od svih vrsta udara i fizičkih oštećenja, od preterano visokih ili niskih temperatura, elektromagnetnih zračenja, kao i od suviše visoke ili niske vlažnosti vazduha. Serveri se uobičajeno nalaze na regalima iznad patosa kako bi se izbegla oštećenja u slučaju poplave. U sali treba da postoji klima uređaj koji ventilira vazduh. Takođe, veoma je važno koristiti uređaje za neprekidno napajenje električnom energijom (*Uninterruptible Power Supplies* - UPS). Svu potrebnu opremu za bezbednost fizičkog okruženja treba redovno održavati.

11. ISPRAVNO I BEZBEDNO FUNKCIONISANJE IKT SISTEMA OD POSEBNOG ZNAČAJA (ČLANOVI 15 I 25 UREDBE)

Pristup IKT sistemu treba omogućiti samo licima koja održavaju sistem. Osim ovlašćenih lica, pristup sistemu treba obezbediti licima kojima je pristup potreban zbog pojedinačnog slučaja (npr. na zahtev IKT sistema od posebnog značaja).

Takođe, za pristupe s ciljem unapređenja i razvoja IKT sistema, treba napraviti testno okruženje koje je odvojeno od operativnog i ne sadrži osetljive podatke iz IKT sistema od posebnog značaja. Korisnički pristup sistemu treba da bude na najnižem nivou, odnosno da poseduje minimalne privilegije i to isključivo delu sistema koji je korisniku potreban za rad.

Takođe, sistem administator treba da konfiguriše sistem tako da se nakon određenog vremena neaktivna sesija prekine. Ovo podešavanje treba da bude na nivou celog sistema, odnosno da važi za svakog korisnika. Softver treba ažurirati blagovremeno i uspostaviti redovnu šemu pravljenja rezervnih kopija. Svaki server treba da sadrži određene mere zaštite sistema kao što su anti-virus i zaštitni zid (*firewall*). Početak zaštite od zlonamernog softvera je kontrola unosa podataka, softvera i uređaja u IKT sistem od posebnog značaja.

12. ZAŠTITA OD ZLONAMERNOG SOFTVERA (ČLAN 16 UREDBE)

Pre svega, na nivou hardvera treba blokirati sve portove koji nisu potrebni za operativni rad na konkretnim uređajima, te propisati pravila o korišćenju uređaja koji nisu u vlasništvu operatora IKT sistema od posebnog značaja.

Arhitektura sistema može da sadrži komponente kao DMZ (*demilitarised zone*) za delove sistema koji treba da budu dostupni javnosti ili tzv. honeypot servere, čija je namena da privuku napade na sebe kako bi ostatak sistema ostao bezbedan. Takođe se preporučuje upotreba bastion servera, koji su namenjeni prepoznavanju i sprečavanju napada i zaštitnih (*firewall*) servera koji filtriraju ulaz u IKT sistem. Softverska rešenja za zaštitu od zlonamernog softvera su anti-virus ili anti-malver softver na svakom uređaju u okviru IKT sistema, te softverski zid (*firewall*) koji filtrira saobraćaj u okviru mreže. Kad je u pitanju elektronska komunikacija, dobra anti-spam i anti-malver konfiguracija smanjuje rizik da zaposleni iz neznanja unesu zlonameran softver u IKT sistem. Administrator IKT sistema je zadužen za instalaciju i automatsko ažuriranje softvera za zaštitu od zlonamernog softvera. Takva podešavanja su od ključnog značaja kako bi sistem bio zaštićen od novih vrsta zlonamernog softvera koje se distribuiraju gotovo svakodnevno. Takođe, softver za zaštitu treba da bude konfigurisan za monitoring sistema u realnom vremenu i skeniranje svakog novonastalog podatka u okviru IKT sistema.

13. ZAŠTITA OD GUBITKA PODATAKA (ČLAN 17 UREDBE)

Stvaranje rezervne kopije (*backup*) ne utiče na stepen bezbednosti samog sistema, ali je od ključnog značaja kada se posle bezbednosne krize javi potreba da se izgubljeni podaci povrate. Ponekad je na osnovu rezervne kopije moguće utvrditi uzrok pada sistema - rekonstrukcijom sigurnosnih propusta ili grešaka u sistemu, i slično.

Preporučeno je i eksterno i interno čuvanje kopija. Eksterni backup se odnosi na čuvanje datih kopija podataka na posebnim diskovima u posebnim sefovima koji su zaštićeni od mogućih nezgoda (primer: vatrostalni sefovi). Interni *backup* podrazumeva čuvanje kopija baze podataka u okviru sistema, odnosno na različitim serverima ili na serveru koji je posebno namenjen za backup.

Servere treba kopirati noću. Diferencijalna kopiranja (*backup* promena) treba obavljati svake noći, dok celokupni backup treba obavljati jednom u sedam dana.

Dnevne izrade kopije treba čuvati jednu sedmicu, dok bi sedmični trebalo čuvati jedan mesec. Mesečne bezbednosne kopije treba čuvati jednu godinu, dok bi godišnje trebalo čuvati zauvek. Podrazumeva se da te rezervne kopije treba zaštiti od svih vrsta fizičkih povreda. Treba imati u vidu da se izbrisani podaci ponekad ne mogu povratiti.

D	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
N	1							2							3							4						
M	1																											
G	... x 12																											

Oznaka	Opis	Period čuvanja
D	Dnevni *backup*	7 dana
N	Nedeljni *backup*	1 mesec
M	Mesečni *backup*	1 godina

14. LOGOVANJE (ČLAN 18 UREDBE)

Log je registar svih događaja u okviru jednog sistema, odnosno svih aktivnosti korisnika - od prijave, preko unosa podataka do njihovih promena, štampanja, brisanja i drugih postupaka.

Logovi mogu beležiti aktivnosti u različitim delovima sistema. Osnovni oblik je pristupni log (access log), a njegovu strukturu, kao i strukturu svih logova, podešava administrator IKT sistema od posebnog značaja. Prilikom podešavanja treba imati na umu da log treba da bude dovoljno detaljan da omogući jasno utvrđivanje zloupotreba (neovlašćeni pristupi i druge aktivnosti) ali da ne bude previše kompleksan za analizu ili skladištenje.

Svaki pristupni log bi trebalo da sadrži konkretne informacije:

- korisnik koji je pristupio bazi podataka;
- datum i vreme pristupa;
- IP adresa sa koje je pristupljeno bazi podataka;
- resurs kome je pristupljeno;
- vrsta obrade podatka (pregled/unos/izmena/brisanje/izvoz/štampa).

Logove je potrebno čuvati najmanje godinu dana, a ukoliko postoji mogućnost i duže. Pored toga, informacioni sistem je neophodno projektovati tako da se za svaki njegov segment (aplikacije, podaci, ostali resursi) od trenutka nastanka, pa sve do trenutka brisanja, pamte sve izmene.

Dakle, prilikom svake izmene potrebno je čuvati konkretne informacije:

- korisnik koji je izvršio izmenu;
- vrsta izmene (unos, izmena, brisanje podataka, nadogradnja softvera, instaliranje novih aplikacija itd);
- datum i vreme izmene;
- vrednost podatka.

Operator je dužan da nadgleda razvojni proces kako bi imao saznanja o tome da li se naloženi standardi implementiraju u sistem. Kako bi to bilo moguće, operator, zajedno sa trećim licem koje razvija IKT sistem, mora da dokumentuje, sistematizuje i kvantifikuje sve vrste bezbednosnih zahteva i standarda koje IKT sistem treba da sadrži, još pre početka projektovanja. Kasnije, tokom naprednijih faza razvoja, implementaciju ovih standarda takođe treba dokumentovati.

15. INTEGRITET SOFTVERA (ČLANOVI 19, 20 I 21 UREDBE)

Kako bi se smanjio rizik od greške ljudske prirode koja bi potencijalno ugrozila bezbednost IKT sistema, administraciju softvera treba da vrši ovlašćeno lice sa adekvatnim obrazovanjem, sistem administrator, koji treba da vodi računa o svim segmentima IKT sistema. Njegove aktivnosti podrazumevaju ažuriranje softvera, vođenje računa o rezervnim kopijama, uniformno konfigurisanje softvera, uspostavljanje mehanizama za povratak na prehodno stanje IKT sistema i čuvanje starije verzije softvera neophodne u slučaju greške ili bezbednosnog incidenta.

Sistem administrator treba da vrši periodične testove bezbednosti IKT sistema (*penetration testing*) kako bi identifikovao slabosti u bezbednosnim procedurama IKT sistema. Ovi testovi obuhvataju sve segmente IKT sistema, a pre svega pristup spolja kroz "*brute force*" napade ili preko grešaka u softverskom kodu koje su nastale slučajno ili namerno, a koje omogućavaju napadačima neprimetan ulaz u sistem (*backdoors*).

Kao preventivnu meru, sistem administrator treba da konfiguriše sistem tako da instalacije dodatnog softvera ne mogu da vrše zaposleni ili druga lica bez odobrenja. Prilikom sprovođenja aktivnosti testiranja bezbednosti IKT sistema, administrator treba da vodi računa da ove aktivnosti ne utiču na normalno funkcionisanje sistema, ili da njihov uticaj bude minimalizovan. Praktično, najbolje je da obim testova bude ograničen, ili da se oni sprovode van radnog vremena ili tokom vikenda, kad je to moguće.

16. ZAŠTITA KOMUNIKACIONIH KANALA (ČLANOVI 22 I 23 UREDBE)

Prilikom uspostavljanja kanala komunikacije koji se koriste za prenos podataka u okviru IKT sistema od posebnog značaja, kao i između IKT sistema od posebnog značaja i drugih IKT sistema koji imaju legitimno pravo da dobijaju podatke, moraju se poštovati najviši nivoi tehničke zaštite. Najbolje je da se koristi "end to end" enkripcija, što bi značilo da se podaci enkriptuju na izvoru, a dekriptuju na destinaciji, odnosno da oni ni u jednom trenutku nisu jasno vidljivi (plain text) prilikom prenosa kroz javne mreže.

Operator IKT sistema treba da izvrši segmentaciju mreže, odnosno da mrežu koja se koristi za prenos tajnih i osetljivih podataka odvoji od mreže koja ima druge namene, tako da zaštićenoj mreži mogu pristupiti samo ovlašćena lica. Mediji za prenos podataka i kablovi za napajanje električnom energijom treba da budu adekvatno zaštićeni od elektromagnetnih zračenja i drugih fizičkih rizika koji bi mogli da utiču na integritet i bezbednost podataka.

Kad je u pitanju razmena podataka sa drugim IKT sistemima, ugovorom treba predvideti da drugi IKT sistem poštuje iste standarde bezbednosti podataka, te da postoji odredba o tajnosti podataka. U slučaju da su predmet prenosa podaci o ličnosti, primenjuju se odredbe Zakona o zaštiti podataka o ličnosti.

17. ŽIVOTNI CIKLUS IKT SISTEMA OD POSEBNOG ZNAČAJA (ČLAN 24 UREDBE)

Standarde informacione bezbednosti potrebno je postaviti u okviru svake faze razvoja IKT sistema od posebnog značaja. Razvoj novog ili zamena postojećeg IKT sistema svakako mora da se bazira na konceptima "*Privacy by design*" i "*Security by design*", te da se prilikom projektovanja detaljno razmotre svi rizici i potencijalne slabosti sistema koje model poslovanja samog operatora IKT sistema od posebnog značaja nalaže. Značajno je korigovati procedure na samom početku primene, kako bi se ubuduće izbegle skupe i teške korekcije sistema.

Ukoliko sistem u bilo kom segmentu i udelu razvijaju treća lica (hardver ili softver), operator je dužan da nadgleda razvojni proces kako bi imao saznanja o tome da li se naloženi standardi implementiraju u sistem. Kako bi to bilo moguće, operator, zajedno sa trećim licem koje razvija IKT sistem, mora da dokumentuje, sistematizuje i kvantifikuje sve vrste bezbednosnih zahteva i standarda koje IKT sistem treba da sadrži, još pre početka projektovanja. Kasnije, tokom naprednijih faza razvoja, implementaciju ovih standarda takođe treba dokumentovati.

18. UGOVORI SA PRUŽAOCIMA USLUGA (ČLANOVI 26 I 27 UREDBE)

Ukoliko postoji potreba da IKT sistem od posebnog značaja bude dostupan pružaocima usluga koji će koristiti određeni segment IKT sistema, kao što su podaci ili specifične funkcije sistema, operator IKT sistema od posebnog značaja treba da odredi nivo i način pristupa u zavisnosti od legitimnih potreba pružalaca usluga.

Obaveze pružalaca usluga, odnosno bezbednosni standardi neophodni kako bi se pružaocima usluga omogućio pristup IKT sistemu, regulišu se sporazumom između operatora IKT sistema od posebnog značaja i pružalaca usluga. Operator je obavezan da vrši nadzor i kontrolu pristupa pružalaca usluga, te da obezbedi pružanje poverenih usluga u skladu sa aktom o bezbednosti IKT sistema.

Operator IKT sistema od posebnog značaja treba da utvrdi procedure pristupa i da naznači lice koje će vršiti nadzor i kontrolu nad pristupima pružalaca usluga IKT sistemu od posebnog značaja.

19. PREVENCIJA I REAGOVANJE NA BEZBEDNOSNE INCIDENTNE PRETNJE (ČLAN 28 UREDBE)

I pored primene najviših bezbednosnih standarda, rizik od incidenta uvek postoji. Kad do njega dođe, bitno je da postoji **procedura upravljanja incidentima**, kako bi sistem postao funkcionalan što pre, te da bi se razlog nastanka incidenta brzo locirao.

Operator IKT sistema od posebnog značaja treba da razvije protokole koji se sastoje od pravila i odgovornih lica koja će znati šta tačno treba da rade kad primete da se desio, ili da će se desiti incident u oblasti bezbednosti IKT sistema. Pre svega, potrebno je definisati ko su lica koja će biti zadužena da incident prijave nadležnim organima, posebnom CERT-u, Nacionalnom CERT-u, Odeljenju za borbu protiv VTK u MUP-u, Posebnom tužilaštvu za VTK, Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti, Ombudsmanu i slično.

Takođe, odgovorna lica treba da vode evidenciju o aktivnostima pre, tokom i nakon kraja bezbednosnog incidenta, da koordinišu kanale komunikacije, te da obezbede procese za identifikaciju, prikupljanje i čuvanje informacija koje mogu predstavljati dokazni materijal u daljem disciplinskom, prekršajnom ili krivičnom postupku.

20. KONTINUITET OBAVLJANJA POSLA U VANREDNIM OKOLNOSTIMA (ČLAN 29 UREDBE)

Od kritične važnosti je da nakon bezbednosnog incidenta sistem bude vraćen u funkciju što pre. Operator IKT sistema od posebnog značaja treba da ima razvijene procedure koje regulišu funkcionisanje sistema u takvim slučajevima, a kojima će se zadržati nivo informacione bezbednosti sistema, definisati zaduženja i odgovornosti, planovi za upravljanje krizom i procedura za oporavak IKT sistema.

Značajno je da čitav set procedura i dokumenata bude razvijen i funkcionalno testiran tokom redovnog stanja IKT sistema, kako bi njegova implementacija u vanrednim okolnostima bila jasna svim odgovornim licima. Takođe, treba razmotriti upotrebu redundantnih sistema i paralelnih arhitektura, ukoliko postojeća infrastruktura ne može da garantuje dovoljan nivo upotrebljivosti tokom vanrednih situacija.

OBAVEŠTENJE O INCIDENTIMA

OBAVEŠTENJE O INCIDENTIMA

Incident je svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema.

Svaki operator IKT sistema od posebnog značaja vrši obaveštavanje o incidentima koji mogu imati značajan uticaj na narušavanje informacione bezbednosti preko veb stranice Nadležnog organa (MTTT) ili preko veb stranice Nacionalnog CERT-a (RATEL) u jedinstveni sistem za prijem obaveštenja o incidentima.

Ukoliko se radi o incidentima u IKT sistemima poslova finansijskih institucija i poslova vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama, obaveštenje o incidentu se upućuje Narodnoj banci Srbije. Ukoliko se radi o incidentima u IKT sistemima poslova iz oblasti elektronskih komunikacija, obaveštenje o incidentu se upućuje RATEL-u. U oba slučaja će ova tela dostaviti primljeno obaveštenje u jedinstveni sistem za prijem obaveštenja o incidentima.

Nakon prijave incidenta, ukoliko je incident i dalje u toku, operatori IKT sistema od posebnog značaja dostavljaju obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta organu kome su u skladu sa ovim zakonom prijavili incident. Takođe, operatori IKT sistema od posebnog značaja dostavljaju završni izveštaj o incidentu organu koga su obaveštavali o incidentu, u roku od 15 dana od dana prestanka incidenta, a koji obavezno sadrži vrstu i opis incidenta, vreme i trajanje incidenta, posledice koje je incident izazvao, preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge relevantne informacije.

Izmenama i dopunama Zakona takođe su predviđena dva slučaja prosleđivanja informacija o incidentima nadležnim organima i to:

1) Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje odbrane Republike Srbije, organ kome je upućeno obaveštenje o incidentu obaveštava Vojno-bezbednosnu agenciju.

2) Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje nacionalne bezbednosti, organ kome je upućeno obaveštenje o incidentu obaveštava Bezbednosno-informativnu agenciju.

Ako je incident od interesa za javnost, organ kome je upućeno obaveštenje o incidentu može objaviti informaciju o incidentu, nakon što se posavetuje sa operatorom IKT sistema od posebnog značaja kome se incident dogodio.

Nakon donošenja Zakona 2016. godine a pre usvajanja njegovih izmena i dopuna 2019. godine, doneta je Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, kojom se bliže uređuje sam postupak dostavljanja podataka o incidentima u IKT sistemima od posebnog značaja. U skladu sa Uredbom, operator IKT sistema od posebnog značaja obaveštenje o incidentu dostavlja MTTT-u kao Nadležnom telu, Narodnoj banci Srbije, odnosno RATEL-u, u roku od jednog dana od dana saznanja za incident. Takvo obaveštene mora sadržati vrstu, opis, vreme trajanje i posledice incidenta, kao i preduzete aktivnosti radi ublažavanja incidenta i druge informacije ukoliko su one relevantne.

Operator IKT sistema od posebnog značaja dužan je, najkasnije jedan dan od dana saznanja, da prijavi relevantnom organu sledeće incidente:

1) incidente koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;

2) incidente koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period;

3) incidente koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;

4) incidente koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;

5) incidente koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose;

6) incidente koji su nastali kao posledica incidenata u sistemu poslova usluga informacionog društva, kada IKT sistem od posebnog značaja u svom poslovanju koristi usluge informacionog društva.

Operator IKT sistema od posebnog značaja dužan je da, pored obaveštenja o incidentu, dostavi Nacionalnom CERT-u statističke podatke o svim incidentima u IKT sistemu u prethodnoj godini, i to najkasnije do 28. februara tekuće godine.

Prilikom određivanja vrste incidenta, operatoru IKT sistema od posebnog značaja na raspolaganju je definisana lista:

1. provaljivanje u IKT sistem – napad na računarsku mrežu i serversku infrastrukturu u okviru koga je, kršenjem mera zaštite, ostvaren pristup koji omogućava neovlašćen uticaj na rad IKT sistema;
2. oticanje podataka – dostupnost zaštićenih podataka van kruga lica ovlašćenih za pristup podacima;
3. neovlašćena izmena podataka;
4. gubitak podataka;
5. prekid u funkcionisanju sistema ili dela sistema;
6. ograničavanje dostupnosti usluge (*denial of service*);
7. instaliranje zlonamernog softvera u okviru IKT sistema;
8. neovlašćeno prikupljanje podataka putem neovlašćenog nadzora nad komunikacijom ili socijalnim inženjeringom;
9. neprestani napad na određene resurse;
10. zloupotreba ovlašćenja pristupa resursima IKT sistema;
11. ostali incidenti.

Trenutno je, u skladu sa izmenama i dopunama Zakona, u pripremi nova Uredba o postupku obaveštavanja o incidentima u IKT sistemima od posebnog značaja, kojom se predviđa izmena gore navede liste incidenata i definisanje značaja incidenata prema nivou opasnosti, kao i postupanje i razmena informacija o incidentima između nadležnih organa.

AKT O BEZBEDNOSTI I PROVERA BEZBEDNOSTI IKT SISTEMA OD POSEBNOG ZNAČAJA

AKT O BEZBEDNOSTI I PROVERA BEZBEDNOSTI IKT SISTEMA OD POSEBNOG ZNAČAJA

DONOŠENJE AKTA O BEZBEDNOSTI

Svi operatori IKT sistema od posebnog značaja bili su dužni da donesu Akt o bezbednosti zaključno sa 2. martom 2017. godine. U suprotnom, čine prekršaj iz člana 30 Zakona o informacionoj bezbednosti zbog čega mogu novčano odgovarati. Međutim, do momenta donošenja izmena i dopuna Zakona iz 2019. godine, ne postoji zvanična statistika koliko je operatora IKT sistema od posebnog značaja ispunilo svoju zakonsku obavezu i usvojilo Akt o bezbednosti.

Akt o bezbednosti uređuje mere zaštite, principe, način i procedure postizanja održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja. Operator sistema od posebnog značaja dužan je da vrši proveru usklađenosti primenjenih mera IKT sistema sa Aktom o bezbednosti najmanje jednom godišnje.

Sadržaj Akta o bezbednosti bliže je propisan Uredbom o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja.

Mere zaštite

Mere zaštite treba definisati tako da one budu usklađene i grupisane u 28 odeljaka koji se podudaraju sa tačkama i nazivima iz Zakona o informacionoj bezbednosti i Uredbe o određenju mera. Svaka od mera bi trebalo da bude što detaljnije opisana.

Primer mera – Zaštita od gubitka podataka (član 17):

Operator IKT sistema od posebnog značaja štiti IKT sistem od gubitka podataka saglasno procedurama o rezervnim kopijama. Operator IKT sistema od posebnog značaja smatra da je primenom ovih procedura minimalizovan rizik od gubitka podataka.

Principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema

Pored osnovnog opisa, mera bi trebalo da sadrži principe i procedure koje će se primenjivati prilikom njenog sprovođenja.

Primer procedura:

Operator IKT sistema od posebnog značaja vrši eksterno i interno čuvanje kopija. Eksterni backup se odnosi na čuvanje datih kopija podataka na posebnim diskovima u posebnim sefovima koji su zaštićeni od mogućih nezgoda (npr. sefovi otporni na toplotu). Interni backup podrazumeva čuvanje kopija baze podataka u okviru sistema, odnosno na različitim serverima ili na serveru koji je namenjen za *backup*.

Rezervne kopije se rade noću, diferencijalna kopiranja (backup promena) se obavljaju svake noći, dok se celokupni *backup* obavlja jednom u sedam dana. Dnevne izrade kopije se čuvaju jednu nedelju, dok

se nedeljni čuva jedan mesec. Mesečne bezbednosne kopije se čuvaju jednu godinu, dok se godišnje čuvaju zauvek. Podrazumeva se da su rezervne kopije zaštićene od svih vrsta fizičkih povreda.

Ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja

Nakon opisa mera i upućivanja na principe i procedure, Akt o bezbednosti bi za svaku meru trebalo da propiše i odgovorna lica za njeno poštovanje.

Primer

Odgovorno lice za sprovođenje procedura o rezervnim kopijama je zaposleni u sektoru za IT poslove, odnosno sistem administrator. Njegova je odgovornost da vodi računa o tome da li automatizovani sistem rezervnih kopija funkcioniše kako treba, te u slučaju problema u funkcionisanju, prijavi ove probleme svom nadređenom, direktoru sektora za IT poslove, koji je obavezan da obavesti generalnog direktora. Sistem administrator je takođe obavezan da proverava uništenje nepotrebnih, odnosno zastarelih rezervnih kopija.

Ukoliko je operator IKT sistema određene mere, procedure ili odgovornost lica već uredio svojim internim aktima i pre stupanja na snagu Zakona i Uredbe, to ga ne oslobađa dužnosti da donese Akt o bezbednosti. U ovom slučaju, Akt će morati da sadrži svih 28 odeljaka, a ukoliko su određena pitanja uređena drugim aktima operatora IKT sistema, navode se upućujuće odredbe na ta akta.

Dodatno, ukoliko određenu meru zaštite nije moguće primeniti ili je analiza rizika pokazala da se ta mera ne mora primeniti u punom obimu, potrebno je to obrazložiti u Aktu o bezbednosti.

PROVERA IKT SISTEMA

Informacione tehnologije su izuzetno dinamična kategorija i zbog toga je neohodno konstantno pratiti promene vlastitog informacionog sistema, ali i digitalnog okruženja, s obzirom na to da se novi rizici po informacionu bezbednost svakodnevno pojavljuju. U skladu s tim, Uredba o merama propisuje obavezu operatora da najmanje jednom godišnje vrši proveru IKT sistema, te da o tome sačini izveštaj.

Ovaj postupak predstavlja proveru usklađenosti primenjenih mera zaštite, procedura i odgovornosti utvrđenih Aktom o bezbednosti, sa realnim rizicima po informacionu bezbednost IKT sistema.

Samu proveru mogu vršiti stručna lica operatora IKT sistema samostalno ili uz angažovanje spoljnih eksperata.

Elementi izveštaja koji je potrebno izraditi nakon postupka provere, posebno su definisani:

1. naziv operatora IKT sistema koji se proverava;
2. vreme provere;
3. podaci o licima koja su vršila proveru;
4. izveštaj o sprovedenim radnjama provere;
5. zaključci po pitanju usklađenosti Akta o bezbednosti IKT sistema sa propisanim uslovima;
6. zaključci po pitanju adekvatne primene predviđenih mera zaštite u operativnom radu;
7. zaključci po pitanju eventualnih bezbednosnih slabosti na nivou tehničkih karakteristika komponenti IKT sistema;
8. ocena ukupnog nivoa informacione bezbednosti;
9. predlog eventualnih korektivnih mera;
10. potpis odgovornog lica koje je sprovelo proveru IKT sistema.

IZMENA AKTA O BEZBEDNOSTI

U skladu sa proverom IKT sistema i izveštajem, operator je dužan da konstantno vrši izmene Akta o bezbednosti kako bi mere, procedure i odgovornosti prilagodio izveštaju o proveri IKT sistema, odnosno novim rizicima koji mogu narušiti informacionu bezbednost.

ODGOVORNOST OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA

ODGOVORNOST OPERATORA IKT SISTEMA OD POSEBNOG ZNAČAJA

Operatori IKT sistema od posebnog značaja mogu snositi različite posledice u slučaju da ne primenjuju propisane mere, odnosno da u drugim slučajevima ne poštuju Zakon i podzakonske akte.

PREKRŠAJNA ODGOVORNOST

Zakon u članovima 30 i 31 propisuje prekršajnu odgovornost i kazne:

- **pravno lice** kao operator IKT sistema može se kazniti novčanom kaznom od 50.000 do 2.000.000 dinara, odnosno **fizičko lice**, odgovorno lice u operatoru IKT sistema od posebnog značaja, može se kazniti novčanom kaznom od 5.000 do 50.000 dinara ukoliko se ne upiše u evidenciju operatora IKT sistema od posebnog značaja u zakonskom roku; ne donese Akt o bezbednosti IKT sistema u zakonskom roku; ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema; ne izvrši proveru usklađenosti primenjenih mera ili ne postupi po nalogu inspektora za informacionu bezbednost; ne dostavi Nacionalnom CERT-u statističke podatke o incidentima iz prethodne godine.
- **pravno lice kao operator IKT sistema** može se kazniti novčanom kaznom od 50.000 do 500.000 dinara, odnosno **fizičko lice**, odgovorno lice u operatoru IKT sistema od posebnog značaja, može se kazniti novčanom kaznom od 5.000 do 50.000 dinara ukoliko o incidentima u IKT sistemu ne obavesti nadležne organe, odnosno ne dostavi nadležnom organu izveštaj o incidentu u zakonskom roku.

GRAĐANSKO-PRAVNA ODGOVORNOST

Ukoliko usled neadekvatnog rukovanja IKT sistemom od posebnog značaja, drugo lice pretrpi materijalnu štetu (npr. gubitak prihoda) ili nematerijalnu štetu (duševni bol usled povrede časti i ugleda), to lice može po opštim pravilima građanskog prava pokrenuti parnični postupak za naknadu štete.

Lica koja nadoknađuju štetu u ovom slučaju bi bila:

- **operator IKT sistema kao pravno lice**, ukoliko je štetu prouzrokovao njegov zaposleni u radu ili u vezi sa radom;
- **zaposleni kod operatora IKT sistema**, ukoliko je štetu prouzrokovao namerno.

KRIVIČNA ODGOVORNOST

Neadekvatno rukovanje IKT sistemom od posebnog značaja može za sobom povući i krivičnu odgovornost lica koja su zaposlena u operatoru IKT sistema od posebnog značaja, a u određenim slučajevima može postojati i odgovornost samog operatora kao pravnog lica.

U slučaju da je operator organ vlasti, krivičnu odgovornost će uvek snositi fizičko lice, a nikada organ vlasti, imajući u vidu član 3 Zakona o odgovornosti pravnih lica za krivična dela. S druge strane,

ukoliko operator IKT sistema od posebnog značaja nije organ vlasti, on kao pravno lice može odgovarati pod uslovima iz člana 6 Zakona o odgovornosti pravnih lica za krivična dela, odnosno ako odgovorno lice počini krivično delo u nameri da za operatora ostvari korist ili ako je krivično delo nastalo zbog nepostojanja nadzora odgovornog lica.

Ovom prilikom ćemo skrenuti pažnju samo na neke članove Krivičnog zakonika (KZ) relevantne za rukovanje IKT sistemom od posebnog značaja:

- Član 303 KZ-a predviđa **krivično delo sprečavanja i organičavanja pristupa javnoj računarskoj mreži** za koje se lice koje neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži može kazniti novčanom kaznom ili zatvorom do jedne godine. Dodatno, u istom članu je predviđen kvalifikovani oblik ovog krivičnog dela ukoliko ga je učinilo službeno lice u vršenju službe, te se takvo lice može kazniti zatvorom do 3 godine.
- Član 304 KZ-a predviđa **krivično delo neovlašćenog korišćenja računara ili računarske mreže** za koje se lice koje neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, može kazniti novčanom kaznom ili zatvorom do tri meseca.

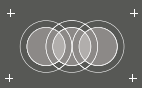
DISCIPLINSKA ODGOVORNOST

Zaposleni koji nije poštovao odredbe Zakona i podzakonskih akata uvek treba i disciplinski da odgovara u Zakonom i internim aktima predviđenom disciplinskom postupku. Posledice po zaposlenog zavise od vrste povrede:

- novčana kazna;
- određivanje neposredno nižeg platnog razreda;
- zabrana napredovanja;
- premeštaj na radno mesto u neposredno niže zvanje;
- prestanak radnog odnosa.

RESURSI I LINKOVI

- Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima Republike Srbije (NCERT), dostupno na: cert.rs
- SHARE CERT - prvi poseban centar u Srbiji za prevenciju rizika u IKT sistemima onlajn medija i organizacija civilnog društva, dostupno na: sharecert.rs
- Agencija EU za mrežnu i informacionu bezbednost – ENISA (European Union Agency for Network and Information Security), dostupno na: enisa.europa.eu
- Tim za brze reakcije u slučajevima sajber kriminala Evropske unije (CERT – EU), dostupno na: cert.europa.eu
- Forum za timove za brze reakcije i bezbednost (Forum for Incident Response and Security Teams), dostupno na: first.org
- Međunarodna telekomunikaciona unija (International Telecommunication Union - ITU), dostupno na: itu.int
- Trusted Introducer, dostupno na: trusted-introducer.org
- SANS Institute, dostupno na: sans.org
- Nacionalni institut za standarde i tehnologije SAD (National Institute of Standard and Technology - NIST), dostupno na: nist.gov
- Međunarodna organizacija za standardizaciju (International Organization for Standardization - ISO), dostupno na: iso.org


2019