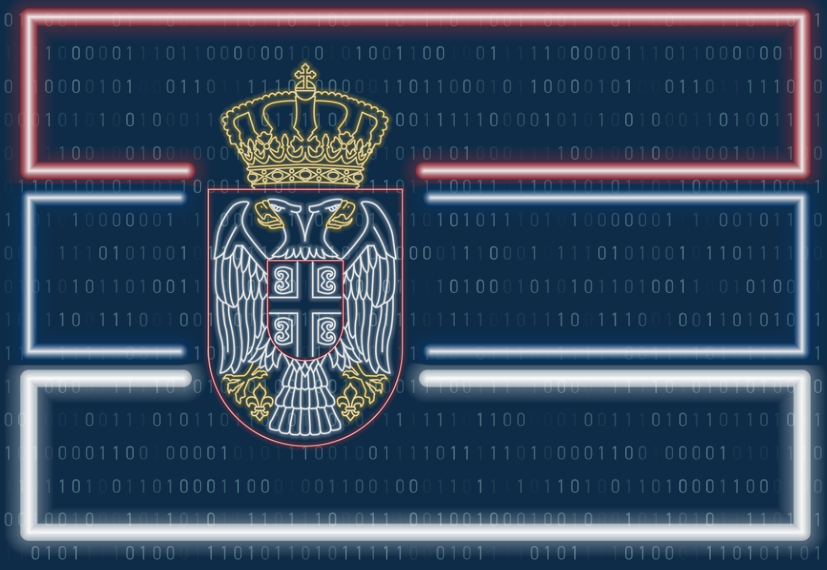
British Embassy Belgrade

UK International Development
Partnership | Progress | Prosperity

TAG International
Securing lives and livelihoods

NALED

Smernice za informacionu bezbednost za lokalne samouprave u Srbiji



Smernice za informacionu bezbednost za lokalne samouprave u Srbiji

© 2024 NALED. Ovu publikaciju je pripremio stručni tim NALED-a u okviru projekta „Jačanje informacione bezbednosti“ koji sprovodi NALED u partnerstvu sa organizacijom TAG International i uz podršku Britanske ambasade u Beogradu. Analize, tumačenja i zaključci izneti u ovoj publikaciji ne moraju nužno odražavati stavove članova Izvršnog odbora i drugih organa NALED-a, ili organizacija koje su podržale njenu izradu. Svi napori su učinjeni kako bi se osigurala pouzdanost, tačnost i ažurnost informacija iznetih u ovoj publikaciji. NALED ne prihvata bilo kakav oblik odgovornosti za eventualne greške sadržane u publikaciji ili nastalu štetu, finansijsku ili bilo koju drugu, proisteklu u vezi sa korišćenjem ove publikacije. Korišćenje, kopiranje i distribucija sadržaja ove publikacije dozvoljeno je isključivo u neprofitne svrhe i uz odgovarajuće naznačenje imena, odnosno priznavanje autorskih prava NALED-a.

Uvod

Napredak informacionih i komunikacionih tehnologija u poslednje tri decenije doneo je do sada nezabeležene promene u svim oblastima života i rada, ali istovremeno i mnogo problema od kojih je bezbednost verovatno najveći.

Zlonamerni korisnici imaju velike mogućnosti da sprovode svoje namere. Sajber kriminal,[1] ali i drugi oblici zloupotreba sajber prostora su u stalnoj ekspanziji, pri čemu se povećava i broj i sofisticiranost napada, ali i štete koje ovi napadi prouzrokuju. Mogućnosti za ispravnu identifikaciju počinilaca napada na internetu nisu dovoljno velike, kao ni mogućnosti da se počinioci privedu pravdi i kazne, a šteta nadoknadi.

> Jedinice lokalne samouprave, kao i svi ostali, prilagođavaju svoj rad promenama u tehnologiji. Kako ove promene za posledicu imaju da su jedinice lokalne samouprave sve više zavisne od tehnologije dok je sajber kriminal u porastu, pri čemu sofisticiranost napada takođe raste, može se izvući jasan zaključak da raste i verovatnoća da će neka jedinica lokalne samouprave postati meta sajber napada, ali i rizik da takav napad prouzrokuje veliku štetu. Jedinice lokalne samouprave su nivo vlasti sa kojim građani ostvaruju najviše kontakata. Prateći način na koji se ti kontakti realizuju i ocenjujući efikasnost u sprovođenju nadležnosti.

Kao i u drugim sektorima, povećanje zavisnosti od informaciono-komunikacionih tehnologija dovodi i do većeg rizika za poremećaje u radu u slučaju incidenata u IKT sistemima.

Incidenti u IKT sistemima se ne mogu u potpunosti sprečiti, ali je moguće zaustaviti neke ili većinu od njih i napraviti okruženje u kojem će jedinica lokalne samouprave biti spremna na eventualni napad i u kojem će posledice takvog napada biti minimalne, a poslovanje normalizovano u najkraćem roku. vJedan od značajnih faktora za postizanje tog cilja je da svaki službenik razume i sledi propisane mere bezbednosti kako bi se smanjila mogućnost da jedinica lokalne samouprave postane žrtva napada.

Ove Smernice su namenjene službenicima u jedinicama lokalne samouprave, koje su u poslednje vreme česta meta napada. Smernice su namenjene svim kategorijama zaposlenih, jer napadači koriste svaku ranjivost da bi realizovali svoj cilj. Smernice su takođe namenjene i predavačima koji realizuju obuke iz oblasti informacione bezbednosti za jedinice lokalne samouprave.

1 U Srbiji je u zvaničnoj upotrebi pojam „visokotehnološki kriminal“. U tekstu Smernica ova dva pojma imaju isto značenje.
2 Zakon o informacionoj bezbednosti nije definisao pojam pretnje. Navedena definicija preuzeta je iz Nacrta zakona o informacionoj bezbednosti iz jula 2024. godine.

Osnovne informacije

Radi boljeg razumevanja teksta koji sledi potrebno je poznavati značenje nekoliko osnovnih pojmova.

U bilo kojem aktivnom IKT sistemu u svakom trenutku dešava se mnogo različitih aktivnosti. U tom smislu, pod pojmom događaj podrazumevamo bilo koju uočljivu pojavu u sistemu ili mreži, kao što su slanje elektronske pošte, logovanje korisnika, preusmeravanje paketa u ruteru i slično. Ipak, postoje pojave koje imaju negativne posledice pa takve pojave nazivamo neželjeni događaji. S tim u vezi, pretnja predstavlja svaku okolnost, događaj ili radnju koja može da ugrozi, poremeti ili na drugi način štetno utiče na IKT sistem, korisnike sistema i druga lica.[2]

Incident

Incident je svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema. Pojam sajber napad odnosi se na incidente koji su namerno izazvani.

Informaciona bezbednost

Informaciona bezbednost obuhvata skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

Pojam informacione bezbednosti nije eksplicitno definisan u NIS 2 Direktivi niti u Aktu o sajber bezbednosti EU, ali se podrazumeva da informaciona bezbednost označava zaštitu tajnosti, integriteta i raspoloživosti, u skladu sa definicijom iz publikacije „Pregled sajber bezbednosti i srodnih termina“4 koji je objavila Agencija EU za sajber bezbednost ENISA i sa definicijom iz standarda ISO 270005.

Sajber bezbednost

Zakonom o informacionoj bezbednosti nije definisan pojam sajber bezbednosti, mada se on često upotrebljava u svakodnevnom govoru i ponekad poistovećuje sa pojmom informacione bezbednosti. U legislativi Evropske Unije češće se upotrebljava pojam sajber bezbednost koji označava aktivnosti neophodne za zaštitu mrežnih i informacionih sistema, korisnika tih sistema i drugih osoba na koje utiču sajber pretnje.[3] Pojam informacione bezbednosti nije eksplicitno definisan u NIS 2 Direktivi niti u Aktu o sajber bezbednosti EU, ali se podrazumeva da informaciona bezbednost označava zaštitu tajnosti, integriteta i raspoloživosti, u skladu sa definicijom iz publikacije „Pregled sajber bezbednosti i srodnih termina“[4] koji je objavila Agencija EU za sajber bezbednost ENISA i sa definicijom iz standarda ISO 270005.[5]

3 Akt o sajber bezbednosti (Uredba EU 2019/881)
4 https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
5 https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Izvori pretnji

Izvori pretnje mogu se svrstati u četiri kategorije:

- **ambijentalni** – katastrofalni događaji i infrastrukturni poremećaji na koje organizacija ne može uticati (požari, zemljotresi, nestanci struje...),
- **strukturni** – poremećaji u radu opreme (kvarovi uređaja, greške u softveru...),
- **slučajni** – slučajne ljudske greške tokom rada i
- **namerni** – zlonamerno delovanje pojedinaca, grupa, organizacija ili država.

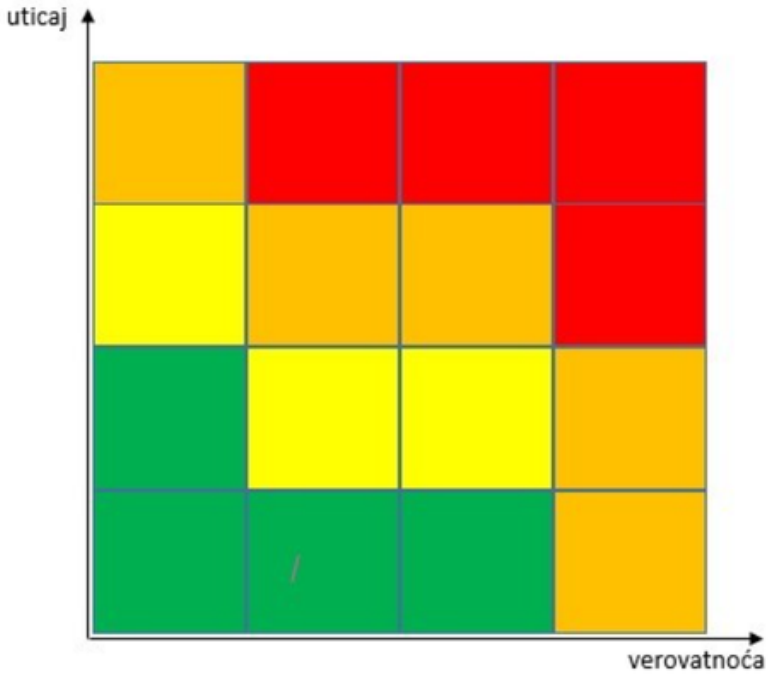
Ranjivost i rizik

Ranjivost označava neku slabost koja postoji u sistemu i koja potencijalno može dovesti do problema.

Slabosti mogu postojati u komponentama računarskog sistema (hardveru), operativnim sistemima, korisničkim i drugim programima (sistemskom i aplikativnom softveru i firmveru), bezbednosnim procedurama i kontrolama, poslovnim procesima, implementaciji itd. Često su ranjivosti nepoznate čak i proizvođačima uređaja i softvera, pa iz tog razloga oni vrše stalno ispitivanje svojih proizvoda i prate da li postoje informacije o probijanjima zaštite njihovih proizvoda. Ako na bilo koji način dođu do saznanja o ranjivosti svojih proizvoda, proizvođači pripremaju korekcije koje se u vidu bezbednosnih zakrpa stavljaju na raspolaganje korisnicima koji treba da ih instaliraju.

Zakonom o informacionoj bezbednosti defnisano je da rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema. Uopšteno, rizik predstavlja meru u kojoj je neka organizacija (na primer, jedinica lokalne samouprave) ugrožena nekim potencijalnim događajem ili okolnošću i funkcija je verovatnoće takvog događaja ili okolnosti i uticaja koji bi nastao ako se taj događaj ili okolnost desi. Da bi verovatnoća da se događaj ili okolnost desi uopšte postojala, moraju postojati i ranjivost i pretnja.

Jedna od mera koje sve organizacije, uključujući jedinice lokalne samouprave treba da preduzimaju je da povremeno utvrđuju postojanje rizika i na osnovu poznatih informacija i iskustva određuju njegovu veličinu. Ako je verovatnoća štetnog događaja velika i ako bi uticaj takvog događaja bio veliki po organizaciju, onda se moraju hitno preduzimati mere kako bi se takav događaj sprečio. Sa druge strane, ako je verovatnoća mala i ako bi uticaj bio od male važnosti onda se može doneti i odluka da se ne troše resursi radi suzbijanja takvog rizika.



Na Slici 1 prikazan je jedan od modela određivanja rizika. Rizike koji se prema verovatnoći i uticaju svrstaju u crvenu zonu treba odmah rešavati, dok oni koji su u zelenoj zoni mogu da čekaju dok se reše svi ostali ili čak da se tolerišu.

Upravljanje rizikom je sistematičan skup mera koji uključuje planiranje, organizovanje i usmeravanje aktivnosti kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima.

Slika 1: Određivanje rizika

U suštini, na utvrđeni rizik može se odgovoriti na neki od sledećih načina:

- **prihvatanje rizika** – kada se identifikovani rizik može tolerisati (na primer, ne preduzimaju se nikakve dodatne mere),
- **izbegavanje rizika** – kada je identifikovani rizik neprihvatljiv a nema mogućnosti za njegovo prihvatljivo ublažavanje pa se preduzimaju mere odustajanja od rizičnih aktivnosti ili primene rizičnih tehnologija (na primer, odustane se od upotrebe nekog softvera),
- **podela rizika** – kada se deo odgovornosti za rizik prebacuje na organizacije koje su kvalifikovanije da se bave određenom delatnošću (na primer, čuvanje podataka organizacije u specijalizovanom data centru),
- **prenos rizika** – kada se celokupna odgovornost za rizik prebacuje na drugu organizaciju (na primer, osiguranje kod osiguravajućeg društva) i
- **ublažavanje (slabljenje) rizika** – kada se primene dodatne bezbednosne mere kojima se smanjuju verovatnoća ili uticaj (na primer, korišćenje čistog mobilnog uređaja kada zaposleni putuje u inostranstvo).

Strateški, pravni i institucionalni okvir informacione bezbednosti u Republici Srbiji

Strategija razvoja informacionog društva i informacione bezbednosti[6]

Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine je međusektorska strategija kojom se utvrđuju ciljevi i mere za razvoj informacionog društva i informacione bezbednosti.

U oblasti informacione bezbednosti, želja je da se realizacijom Strategije postigne informaciono bezbedno okruženje u kome postoji dovoljan nivo svesti o rizicima, ali i prednostima koje nove tehnologije pružaju građanima, javnoj upravi i privredi.

Opšti cilj Strategije je razvijeno informaciono društvo i elektronska uprava u službi građana i privrede i unapređena informaciona bezbednost građana, javne uprave i privrede. Opšti cilj Strategije ostvaruje se kroz tri posebna cilja:

1. Unapređenje digitalnih znanja i veština građana, podizanje kapaciteta zaposlenih u javnom i privatnom sektoru za korišćenje novih tehnologija i unapređanje digitalne infrastrukture u obrazovnim ustanovama.
2. Digitalizacija usluga i poslovanja u javnom i privatnom sektoru.
3. Unapređenje informacione bezbednosti građana, javne uprave i privrede.

Strategijom je predviđeno da se unapređenje informacione bezbednosti građana, javne uprave i privrede ostvaruje kroz realizaciju sledećih mera:

- podizanje svesti i znanja u oblasti informacione bezbednosti građana, javnih službenika i privrede,
- podizanje kapaciteta IKT sistema od posebnog značaja za primenu mera zaštite,
- podizanje kapaciteta Nacionalnog CERT-a, CERT-a organa vlasti i CERT-ova samostalnih operatora IKT sistema,
- podizanje kapaciteta inspekcije za informacionu bezbednost,
- podsticanje javno-privatnog partnerstva u oblasti informacione bezbednosti i
- unapređenje regionalne i međunarodne saradnje.

6 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/strategija/2021/86/1/reg

Akcionim planom za realizaciju Strategije za period od 2024. do 2026. godine,[7] usvojenim u avgustu 2024. godine, predviđeno je više aktivnosti koje imaju za cilj jačanje kapaciteta državnih organa, uključujući i jedinice lokalne samouprave:

- organizovanje i koordinisanje kampanja za podizanje svesti građana, javnih službenika, malih i srednjih preduzeća u cilju podizanja svesti o značaju informacione bezbednosti, o rizicima i merama zaštite (Aktivnost 1.3.1.1),
- Razvoj i sprovođenje obukaza javne službenike na temu informacione bezbednosti (Aktivnost 1.3.1.3),
- Unapređenje edukativnih sadržaja za službenike u javnoj upravi (Aktivnost 1.3.1.6),
- Unapređenje sadržaja na platformi za podizanje svesti i znanja o informacionoj bezbednosti kroz interaktivne programe (Aktivnost 1.3.1.7),
- Analiza stanja informacionih sistema i informacione bezbednosti u jedinicama lokalne samouprave (Aktivnost 1.3.1.8),
- Podizanje svesti o značaju informacionih tehnologija, digitalizacije, informatičke pismenosti i informacione bezbednosti (Aktivnost 1.3.1.9),
- Obuke za zaposlene u IKT sistemima od posebnog značaja o primeni mera zaštite i postupanju u slučaju incidenata u IKT sistemima (Aktivnost 1.3.2.1),
- Izrada brošura, preporuka i drugih materijala u cilju podizanja svesti o važnosti primene mera zaštite (Aktivnost 1.3.2.4),
- Unapređenje platforme za razmenu podataka između Nacionalnog CERT-a i IKT sistema od posebnog značaja u cilju informisanja o aktuelnim rizicima i pretnjama u oblasti informacione bezbednosti i promovisanja primera dobre prakse (Aktivnost 1.3.2.5),
- Izrada obrasca za samoprocenu IKT sistema od posebnog značaja (Aktivnost 1.3.2.8),
- Uspostavljanje sistema za rana upozorenja (Aktivnost 1.3.2.10),
- Izrada metodologije procene rizika i kataloga pretnji (Aktivnost 1.3.2.15).

7 https://www.srbija.gov.rs/extfile/sr/806566/akc_pl_strat_razvoja_IDrustva_IBezbedn_2021-2026_per_2024- 2026_020_cyr.zip

Zakon o informacionoj bezbednosti[8]

Zakonom o informacionoj bezbednosti[9] uređene su mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određeni su nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

Odredbe Zakona o informacionoj bezbednosti usklađene su sa Direktivom EU o osnovnim merama mrežne i informacione bezbednosti (NIS Direktiva) usvojenom 2016. godine.[10]

Na osnovu Zakona o informacionoj bezbednosti doneti su sledeći podzakonski akti:

- Uredba o bližem sadržaju Akta o bezbednosti IKT sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja,
- Uredba o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja,
- Uredba o bližem uređenju mera zaštite IKT sistema od posebnog značaja,
- Uredba o utvrđivanju liste delatnosti u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja,
- Uredba o kriptobezbednosti i zaštiti od kompromitujućeg elektromagnetnog zračenja,
- Pravilnik o bližim uslovima za upis u Evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima,
- Pravilnik o vrsti, formi i načinu dostavljanja statističkih podataka o incidentima u informaciono-komunikacionim sistemima od posebnog značaja,
- Pravilnik o podacima koje sadrži evidencija operatora informaciono-komunikacionih sistema od posebnog značaja.

7 https://www.srbija.gov.rs/extfile/sr/806566/akc_pl_strat_razvoja_IDrustva_IBezbedn_2021-2026_per_2024- 2026_020_cyr.zip 8 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg 9 Prvi Zakon o informacionoj bezbednosti Republike Srbije usvojen je početkom 2016. godine, da bi 2019. godine bio usvojen Zakon o izmenama i dopunama Zakona o informacionoj bezbednosti čime je legislativa Republike Srbije u ovoj oblasti usaglašena sa legislativom Evropske Unije. 10 U decembru 2022. godine Evropska Unija usvojila je Direktivu o merama za visoki nivo sajber bezbednosti (NIS 2 Direktiva) kojom je dodatno uredila ovu oblast u EU. Republika Srbija, u skladu sa svojim opredeljenjem o pristupanju EU, pripremila je novi Nacrt zakona o informacionoj bezbednosti kojim bi se legislativa Republike Srbije uskladila sa ovom novom Direktivom. Očekuje se da novi Zakon o informacionoj bezbednosti u Republici Srbiji bude usvojen tokom 2024. godine.

Najvažnije odredbe Zakona o informacionoj bezbednosti

Ovim zakonom definisano je da informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica. Zakonom su definisana sledeća svojstva podataka:

- tajnost znači da podatak nije dostupan neovlašćenim licima,
- integritet znači očuvanost izvornog sadržaja i kompletnosti podatka,
- raspoloživost znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban,
- autentičnost znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio i
- neporecivost znači sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći.

Zakonom o informacionoj bezbednosti definisana je kategorija IKT sistema od posebnog značaja koji su neophodni za pružanje usluga od vitalne važnosti. Zakonom je propisano da se u IKT sisteme od posebnog značaja svrstaju sistemi koji se koriste:

- u obavljanju poslova u organima vlasti,
- za obradu posebnih vrsta podataka o ličnosti,
- u obavljanju delatnosti od opšteg interesa i drugih delatnosti u sledećim oblastima:
- energetika,
- saobraćaj,
- zdravstvo,
- bankarstvo i finansijska tržišta,
- digitalna infrastruktura,
- dobra od opšteg interesa,
- usluge informacionog društva,
- ostale oblasti:
- elektronske komunikacije,
- izdavanje službenog glasila Republike Srbije,
- upravljanje nuklearnim objektima,
- proizvodnja, promet i prevoz naoružanja i vojne opreme,
- upravljanje otpadom,
- komunalne delatnosti,
- proizvodnja i snabdevanje hemikalijama, i
- u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti navedenih u prethodnoj tački.

U skladu sa ovim odredbama, jedinice lokalne samouprave i pravna lica i ustanove čiji je osnivač jedinica lokalne samouprave i koje obavljaju delatnosti u navedenim oblastima spadaju u kategoriju IKT sistema od posebnog značaja, te stoga moraju ispuniti obaveze koje Zakon o informacionoj bezbednosti nalaže ovoj kategoriji.

Obaveze IKT sistema od posebnog značaja

Zakonom o informacionoj bezbednosti propisano je da operator IKT sistema od posebnog značaja[11] ima posebne obaveze iz domena informacione bezbednosti.:

1. upisivanje u evidenciju IKT sistema od posebnog značaja,
2. preduzimanje mera zaštite IKT sistema od posebnog značaja,
3. donošenje akta o bezbednosti IKT sistema,
4. provera usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema,
5. u slučaju da se aktivnosti u vezi sa IKT sistemom poveravaju trećim licima, uređivanje odnosa sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema,
6. dostavljanje obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema, i
7. dostavljanje tačnih statističkih podataka o incidentima u IKT sistemu.

Upisivanje u evidenciju IKT sistema od posebnog značaja

Evidenciju IKT sistema od posebnog značaja vodi Nadležni organ.[12] Operator IKT sistema od posebnog značaja ima obavezu da Nadležnom organu dostavi sledeće podatke:

1. naziv i sedište operatora IKT sistema od posebnog značaja,
2. ime i prezime, službenu adresu za prijem elektronske pošte i službeni kontakt telefon administratora IKT sistema od posebnog značaja,
3. ime i prezime, službenu adresu za prijem elektronske pošte i službeni kontakt telefon odgovornog lica IKT sistema od posebnog značaja i
4. podatak o vrsti IKT sistema od posebnog značaja (osnov za svrstavanje u IKT sistem od posebnog značaja).

Nadležni organ može propisati da evidencija IKT sistema od posebnog značaja može sadržati i dopunske podatke. Evidencija IKT sistema od posebnog značaja na raspolaganju je i Nacionalnom CERT-u.

Podaci koje sadrži Evidencija IKT sistema od posebnog značaja propisani su Pravilnikom o podacima koje sadrži evidencija operatora informaciono-komunikacionih sistema od posebnog značaja.[13] Zahtev za upis podataka u Evidenciju podnosi se elektronskim putem.[14]

11 Zakonom o informacionoj bezbednosti je propisano da je operator IKT sistema pravno lice, organ vlasti ili organizaciona jedinica organa vlasti koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti

12 Zakonom o informacionoj bezbednosti propisano je da je nadležni organ ministarstvo nadležno za informacionu bezbednost. U daljem tekstu detaljnije su objašnjene nadležnosti Nadležnog organa.

Nadležnom organu na Obrascu 115 u formi elektronskog dokumenta u originalu ili u formi overenog digitalizovanog akta, u skladu sa propisima kojima se uređuje elektronski dokument. Zahtev se može podneti i pisanim putem na popunjenom Obrascu 1, neposredno ili poštom, na elektronsku adresu Ministarstva. Nadležnom organu na Obrascu 115 u formi elektronskog dokumenta u originalu ili u formi overenog digitalizovanog akta, u skladu sa propisima kojima se uređuje elektronski dokument. Zahtev se može podneti i pisanim putem na popunjenom Obrascu 1, neposredno ili poštom, na elektronsku adresu Ministarstva.

U slučaju da dođe do promene podataka upisanih u Evidenciju IKT sistema od posebnog značaja, jedinica lokalne samouprave je dužna da u roku od osam dana od nastanka promene podnese Zahtev za promenu podataka na Obrascu 216.

- tajnost znači da podatak nije dostupan neovlašćenim licima,
- integritet znači očuvanost izvornog sadržaja i kompletnosti podatka,
- raspoloživost znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban,
- autentičnost znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio i
- neporecivost znači sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći.

Preduzimanje mera zaštite IKT sistema od posebnog značaja

Mere zaštite IKT sistema spadaju u preventivne mere kojima se sprečava nastanak incidenta, odnosno onemogućuje ili umanjuje šteta od incidenta. Mere zaštite bazirane su na međunarodnim standardima u oblasti informacione bezbednosti i odnose se na:

1. uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema;
2. postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja;
3. obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost;
4. zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema;
5. identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu;

13 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/ministarstva/pravilnik/2020/9/2/reg
14 Na adresu evidencijaiktsistema@mit.gov.rs
15. https://mit.gov.rs/extfile/sr/184/Obrazac%201%20%20Zahtev%20za%20upis%20podataka%20u%20evidenciju%20IKT%20sistema%20od%20posebnog%20zna%C4%8 Daja1.docx
16 https://mit.gov.rs/extfile/sr/188/Obrazac%202%20-%20Zahtev%20za%20promenu%20podataka%20u%20evidenciji%20IKT%20sistema%20od%20posebnog%20znacaj a1.docx

6. klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom; [17]
7. zaštitu nosača podataka;
8. ograničenje pristupa podacima i sredstvima za obradu podataka;
9. odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža;
10.utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju;
11. predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti i integriteta podataka;
12. fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu;
13. zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem;
14. bezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka;
15. zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera;
16. zaštitu od gubitka podataka;
17. čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema;
18. obezbeđivanje integriteta softvera i operativnih sistema;
19. zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;
20. obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema;
21. zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove;
22. bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema;
23. ispunjenje zahteva za informacionu bezbednost u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;
24. zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema;
25. zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga;
26. održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;
27. prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama;
28. mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima.

Bliže uređenje mera zaštite propisano je Uredbom o bližem uređenju mera zaštite IKT sistema od posebnog značaja.[18] Ovom Uredbom detaljnije je razrađena svaka od navedenih mera zaštite.

17 Član 3. Zakona o informacionoj bezbednosti
18 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2016/94/2/reg

Donošenje Akta o bezbednosti IKT sistema

Jedna od obaveza je usvajanje Akta o bezbednosti IKT sistema, koji treba da sadrži opis mera bezbednosti koje se primenjuju u jedinici lokalne samouprave.

Detaljniji sadržaj i okvir za sprovođenje ovog Akta propisani su Uredbom o bližem sadržaju Akta o bezbednosti IKT sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja.[19]

Aktom o bezbednosti IKT sistema određuju se mere zaštite, principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja. Akt o bezbednosti IKT sistema treba da sadrži detaljniji opis primene za svaku od 28 mera propisanih Zakonom o informacionoj bezbednosti u jedinici lokalne samouprave (odnosno, potrebno je u Aktu o bezbednosti IKT sistema napisati obrazloženje u slučaju da je neka od predviđenih mera neprimenljiva ili je analiza rizika pokazala da je nepotrebna).

Model akta o bezbednosti IKT sistema kojim su obuhvaćene sve mere zaštite predviđene Zakonom o infomacionoj bezbednosti, Uredbom o bližem sadržaju akta o bezbednosti IKT sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja i Uredbom o bližem uređenju mera zaštite IKT sistema od posebnog značaja dostupan je na internet stranici Nacionalnog CERT-a.[20]

Akt o bezbednosti IKT sistema potrebno je revidirati uvek kada postoje promene u okruženju koje mogu dovesti do povećanog rizika (tehničko-tehnološke, kadrovske ili organizacione promene u IKT sistemu, kao i događaji na globalnom i nacionalnom nivou koji mogu narušiti informacionu bezbednost), ili kada postoje mogućnosti za unapređenje mera zaštite.

19 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2016/94/1/reg
20 https://www.cert.rs/files/shares/Model%20Akta%20o%20bezbednosti.pdf

Provera usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema

Jedinica lokalne samouprave je u obavezi da barem jednom godišnje vrši proveru IKT sistema, odnosno proveru usklađenosti primenjenih mera zaštite sa Aktom o bezbednosti, merama zaštite propisanim Zakonom o informacionoj bezbednosti i Uredbom o bližem uređenju mera zaštite IKT sistema od posebnog značaja.

Svrha provere je da se utvrdi ugroženost ili narušavanje informacione bezbednosti koja nastaje korišćenjem neodgovarajućih postupaka i tehničkih sredstava. Provera se vrši na sledeći način:

1. proverava se da li su mere zaštite, procedure, ovlašćenja i odgovornosti u IKT sistemu predviđene Aktom o bezbednosti IKT sistema usklađene sa propisanim uslovima u jedinici lokalne samouprave,
2. putem razgovora sa zaposlenima, posmatranja procesa rada, simulacija i uvida u predviđene evidencije i drugu dokumentaciju proverava se da li se u operativnom radu adekvatno primenjuju predviđene mere zaštite i procedure u skladu sa utvrđenim ovlašćenjima i odgovornostima,
3. putem uvida u izabrane proizvode, arhitekture rešenja, tehničke konfiguracije, tehničke podatke o statusima, zapise o događajima (logove) kao i metodom testiranja postojanja poznatih bezbednosnih slabosti u sličnim okruženjima vrši se provera bezbednosnih slabosti na nivou tehničkih karakteristika komponenti IKT sistema.

Jedinica lokalne samouprave proveru može izvršiti samostalno ili angažovati spoljne eksperte.

Nakon izvršene provere izrađuje se izveštaj koji mora sadržati sledeće podatke:

Nakon izvršene provere izrađuje se izveštaj koji mora sadržati sledeće podatke:

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

Uređivanje odnosa sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema

Ako jedinica lokalne samouprave poveri aktivnosti u vezi sa IKT sistemom trećem licu, u obavezi je da uredi odnos sa tim licem na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa propisima. Pod aktivnostima u vezi sa IKT sistemom podrazumevaju se sve aktivnosti koje uključuju obradu, čuvanje i mogućnost pristupa podacima kojima raspolaže jedinica lokalne samouprave, kao i razvoj i održavanje komponenti IKT sistema od kojih zavisi vršenje poslova iz nadležnosti jedinice lokalne samouprave. Pod trećim licem podrazumevaju se i organizacije i privredni subjekti čiji je osnivač jedinica lokalne samouprave.

Poveravanje aktivnosti trećem licu vrši se na osnovu ugovora zaključenog između jedinice lokalne samouprave i lica kome se te aktivnosti poveravaju. Poveravanje aktivnosti trećem licu može se izvršiti i na osnovu posebnog propisa, pri čemu se tim propisom mogu drugačije urediti obaveze i odgovornosti jedinice lokalne samouprave u vezi poverenih aktivnosti.

Dostavljanje obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema

Jedinice lokalne samouprave u obavezi su da blagovremeno dostavljaju informacije o incidentima koji mogu značajno da ugrožavaju informacionu bezbednost.

Pod incidentima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti smatraju se:

1. incidenti koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga,
2. incidenti koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period,
3. incidenti 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. incidenti koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije,
5. incidenti koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose,
6. incidenti koji su nastali kao posledica incidenta u IKT sistemu koji pruža usluge informacionog društva, kada jedinica lokalne samouprave u svom poslovanju koristi informacione usluge IKT sistema koji pruža usluge informacionog društva.

Način na koji se ove informacije dostavljaju propisan je Uredbom o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja.[21] Uredbom je propisano da se obaveštenja o incidentima koji mogu imati značajan uticaj na narušavanje informacione bezbednosti dostavljaju bez odlaganja, a najkasnije narednog radnog dana od dana saznanja o nastanku incidenta. Obaveštenja se dostavljaju preko internet stranice Nadležnog organa (ministarstvo nadležno za infiormacionu bezbednost[22]) ili Nacionalnog CERT-a[23] u jedinstven sistem za prijem obaveštenja o incidentima. U slučaju hitnosti, pored dostavljanja podataka preko internet stranice, obaveštenje o incidentu može se prijaviti i putem telefona, elektronske pošte ili na drugi odgovarajući način.

21 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2020/11/3/reg
22 https://mit.gov.rs/tekst/3228/prijava-incidenata-u-oblasti-informacione-bezbednosti.php
23 https://www.cert.rs/rs/prijava.html

Neophodno je da obaveštenje o incidentu sadrži sledeće podatke:

1. naziv podnosioca prijave, broj telefona i adresu elektronske pošte,
2. vrstu i opis incidenta,
3. datum i vreme početka incidenta i trajanje incidenta,
4. posledice koje je incident izazvao,
5. preduzete aktivnosti radi ublažavanja posledica incidenta.

Po potrebi, obaveštenje o incidentu može sadržati i druge relevantne podatke.

Jedan od podataka koji treba uneti u obaveštenje o incidentu je klasifikacija incidenta prema grupi i vrsti incidenta. Lista incidenata prema vrstama nalazi se u Prilogu 1 ovih Smernica.

Ako je incident u toku i nakon prijave incidenta, jedinica lokalne samouprave ima obavezu da organu kome je prijavljen incident dostavlja obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta.

Nakon prijema obaveštenja o incidentu, Nacionalni CERT prikuplja, analizira i razmenjuje informacije o incidentu i obaveštava, pruža podršku, upozorava i savetuje jedinicu lokalne samouprave i vrši druge poslove iz svoje nadležnosti. Na osnovu izvršene analize, Nacionalni CERT vrši klasifikaciju prema nivou opasnosti, pri čemu se uzimaju u obzir posledice incidenta. Klasifikacija incidenata prema nivou opasnosti nalazi se u Prilogu 2 ovih Smernica.

U slučaju incidenta nivoa opasnosti „nizak“, Nacionalni CERT po potrebi priprema predlog preporuka za postupanje i stupa u kontakt sa jedinicom lokalne samouprave u kojoj se desio incident.
U slučaju incidenta nivoa opasnosti „srednji“, Nacionalni CERT priprema predlog preporuka za postupanje i stupa u kontakt sa jedinicom lokalne samouprave u kojoj se desio incident u cilju primene predloženih preporuka za postupanje.

U slučaju incidenta nivoa opasnosti „visok“, Nacionalni CERT obaveštava ministarstvo nadležno za poslove informacione bezbednosti, organizuje sastanak sa predstavnicima ministarstva, drugih CERT-ova i drugih lica u cilju koordinacije reagovanja na incident, a u slučaju da je neophodno, inspektor za informacionu bezbednost može da zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost u jedinici lokalne samouprave i za to ostavi rok.

U slučaju incidenta nivoa opasnosti „veoma visok“, Nacionalni CERT obaveštava ministarstvo nadležno za poslove informacione bezbednosti, koje potom obaveštava Republički štab za vanredne situacije koji postupa u skladu sa svojim nadležnostima.

Uz saglasnost ministarstva nadležnog za poslove informacione bezbednosti Nacionalni CERT može upozoriti i savetovati javnost o incidentima koji mogu imati značajan uticaj na narušavanje informacione bezbednosti IKT sistema od posebnog značaja u Republici Srbiji.

Dostavljanje tačnih statističkih podataka o incidentima u IKT sistemu

> Jedinica lokalne samouprave je u obavezi da najkasnije do 28. februara tekuće godine Nacionalnom CERT-u dostavi elektronskim putem statističke podatke o svim incidentima u IKT sistemu u prethodnoj godini. Bliži način dostavljanja statističkih podataka propisan je Pravilnikom o vrsti, formi i načinu dostavljanja statističkih podataka o incidentima u informaciono-komunikacionim sistemima od posebnog značaja24.

Statistički podaci o svim incidentima u IKT sistemu za prethodnu godinu dostavljaju se Nacionalnom CERT-u preko veb forme koja je dostupna registrovanim korisnicima.[25] Vrsta statističkih podataka o svim incidentima sadržana je u obrascu ISP – Izveštaj o statističkim podacima o svim incidentima u IKT sistemima od posebnog značaja, koji se nalazi u Prilogu 3 ovih Smernica.

Nacionalni CERT vrši obradu dostavljenih statističkih podataka i objavljuje ih na svojoj internet stranici u formi godišnjeg izveštaja.[26] Godišnji izveštaj ne sadrži pojedinačne podatke ni ocenu bezbednosti bilo kojeg pojedinačnog operatora IKT sistema od posebnog značaja, već samo agregirane i anonimizovane podatke. Nacionalni CERT može trećim licima ustupati pojedinačne podatke iz ISP obrasca isključivo uz izričitu saglasnost operatora IKT sistema od posebnog značaja koja se daje u formi pisane izjave zakonskog zastupnika.

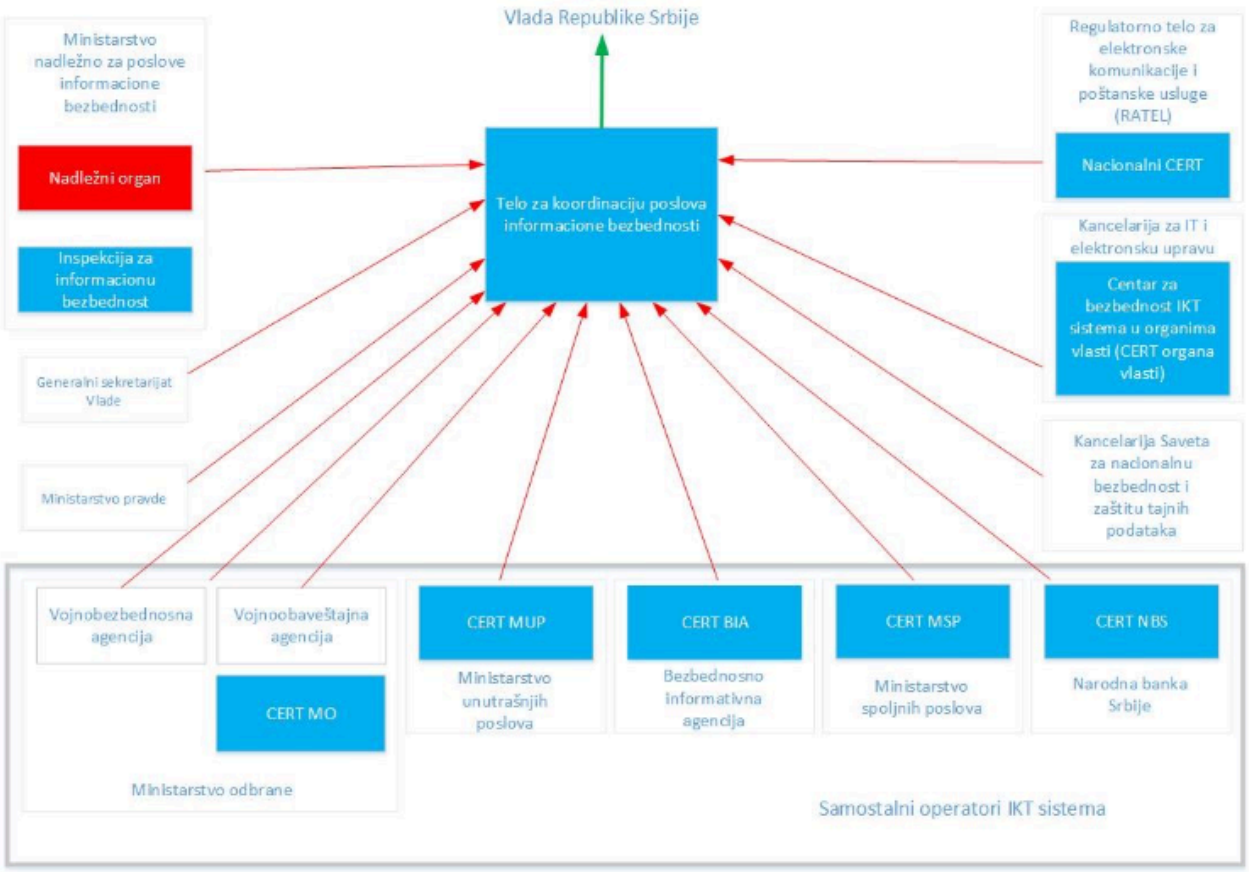
Listu operatora IKT sistema od posebnog značaja koji nisu dostavili statističke podatke o incidentima u IKT sistemu Nacionalni CERT dostavlja Nadležnom organu najkasnije do kraja drugog tromesečja tekuće godine.

24https://www.ratel.rs/uploads/documents/empire_plugin/Pravilnik%20o%20vrsti%2C%20formi%20i%20na%C4%8Dinu%20dostavljanja%20statisti%C4%8Dkih%20podataka%20o%20incidentima%20u%20informacionokomunikacionim%20sistemima%20od%20posebnog%20zna%C4%8Daja.pdf
25 Adresa za logovanje je https://www.cert.rs/rs/login.html, a registrovani korisnici se za sve informacije u vezi sa pristupom i unosom podataka u veb formu mogu obratiti elektronskom poštom na statistika@cert.rs.
26 https://www.cert.rs/rs/izvestaji.html

Institucionalni okvir

Zakonom o informacionoj bezbednosti propisan je i institucionalni okvir za informacionu bezbednost u Republici Srbiji i nadležnosti institucija.

Na slici ispod prikazane su institucije Republike Srbije koje su ovim Zakonom dobile određenu nadležnost.



Slika 2: Institucionalni okvir za informacionu bezbednost u Republici Srbiji

Plavim pravougaonicima predstavljene su organizacione celine čije je uspostavljanje propisano Zakonom o informacionoj bezbednosti, crvenim pravougaonikom uspostavljanje nadležnosti Nadležnog organa, crvenim strelicama učešće u radu Tela za koordinaciju poslova informacione bezbednosti i zelenom strelicom izveštavanje Vlade Srbije u vezi sa informacionom bezbednošću.

Nadležni organ

Važećim Zakonom o informacionoj bezbednosti propisano je da organ državne uprave nadležan za bezbednost IKT sistema bude ministarstvo nadležno za poslove informacione bezbednosti.[27]

Ovo ministarstvo, između ostalog, obavlja poslove koji se odnose na:

- štitu podataka i informacionu bezbednost,
- pripremu predloga propisa iz oblasti informacione bezbednosti,
- preventivno delovanje i vršenje inspekcijskog nadzora nad primenom zakona i drugih propisa kojima se uređuje informaciona bezbednost,
- preduzimanje propisanih upravnih i kaznenih mera u vršenju inspekcijskog nadzora u odnosu na procenjeni rizik, u skladu sa zakonom kojim se uređuje inspekcijski nadzor,
- nadzor nad radom IKT sistema od posebnog značaja,
- nadzor nad radom Nacionalnog CERT-a,
- uspostavljanje i vođenje evidencije IKT sistema od posebnog značaja,
- prijem obaveštenja o incidentima u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti,
- međunarodnu saradnju u oblasti bezbednosti IKT sistema,
- proveru usklađenosti mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema Ministarstva,
- planiranje rada, koordinaciju i sprovođenje aktivnosti Nacionalnog kontakt centra za bezbednost dece na internetu.

Ministarstvo nadležno za poslove informacione bezbednosti ima nadležnost po pitanjima međunarodne saradnje u oblasti bezbednosti IKT sistema i pruža upozorenja o rizicima i incidentima koji ispunjavaju barem jedan od sledećih uslova:

1. brzo rastu ili imaju tendenciju da postanu visokorizični,
2. prevazilaze ili mogu da prevaziđu nacionalne kapacitete ili
3. mogu da imaju negativan uticaj na više od jedne države.

Nadležni organ vrši nadzor nad radom Nacionalnog CERT-a tako što najmanje jednom godišnje proverava da li Nacionalni CERT raspolaže odgovarajućim resursima, vrši poslove propisane Zakonom o informacionoj bezbednosti i kontroliše učinak uspostavljenih procesa za upravljanje bezbednosnim incidentima.

Zakonom o informacionoj bezbednosti propisano je i da Nadležni organ preduzima preventivne mere za bezbednost i zaštitu dece na internetu putem edukacije i informisanja dece, roditelja i nastavnika o prednostima, rizicima i načinima bezbednog korišćenja interneta, kao i putem jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, i upućuje prijave nadležnim organima radi daljeg postupanja.

27 Zakonom o ministarstvima propisano je da Ministarstvo informisanja i telekomunikacija obavlja poslove državne uprave koji se odnose na zaštitu podataka i informacionu bezbednost.

Inspekcija za informacionu bezbednost

Ministarstvo nadležno za poslove informacione bezbednosti obavlja poslove inspekcije za informacionu bezbednost preko inspektora za informacionu bezbednost.

Nadležnost inspekcije za informacionu bezbednost je da vrši inspekcijski nadzor nad primenom Zakona o informacionoj bezbednosti i radom IKT sistema od posebnog značaja. U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi propisani Zakonom o informacionoj bezbednosti i propisima donetim na osnovu ovog zakona. Prilikom sprovođenja nadzora inspektor za informacionu bezbednost je, pored opštih ovlašćenja, ovlašćen da naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok i da zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok.

Kontrola IKT sistema od posebnog značaja obavlja se korišćenjem Kontrolne liste KL-001-03/09[28] koja sadrži sledeća pitanja:

1. Da li je donet Akt o bezbednosti?
2. Da li je Akt o bezbednosti donet u skladu sa postojećim propisima?
3. Da li su primenjene mere zaštite?
4. Da li je izvršena godišnja provera usklađenosti primenjenih mera zaštite?
5. Da li je u skladu sa propisima sačinjen izveštaj o godišnjoj proveri IKT sistema od posebnog značaja?
6. Da li je izvršen upis u Evidenciju operatora IKT sistema od posebnog značaja?
7. Da li su Nacionalnom CERT-u dostavljeni tačni statistički podaci o incidentima u IKT sistemu u skladu sa članom 11b Zakona o informacionoj bezbednosti?

Odgovori na navedena pitanja donose određen broj bodova, a prema ukupnom zbiru bodova određuje se stepen rizika koji može biti neznatan, nizak, srednji, visok ili kritičan.

Jedinica lokalne samouprave može i samoinicijativno zahtevati službenu savetodavnu posetu u svrhu preventivnog delovanja, koja se organizuje van inspekcijskog nadzora i tokom koje inspekcija pruža stručnu i savetodavnu podršku. Inspekcija je dužna da u roku od 15 dana od dana prijema zahteva za stručnu savetodavnu posetu postupi po zahtevu ili obavesti jedinicu lokalne samouprave o razlozima za nepostupanje po zahtevu. Ako tokom stručne savetodavne posete uoči propust, inspekcija je dužna da u roku od osam dana jedinici lokalne samouprave putem dopisa dostavi preporuke kako i u kom roku da taj propust, odnosno nedostatak ili nepravilnost ispravi. Jedinica lokalne samouprave je obavezna da postupi po preporukama i da u roku navedenom u dopisu o tome obavesti inspekciju za informacionu bezbednost. U slučaju nepostupanja po preporukama ili neobaveštavanja u zadatom roku, inspekcija za informacionu bezbednost može pokrenuti postupak inspekcijskog nadzora.

28 https://mit.gov.rs/extfile/sr/1794/Kontrolna%20lista%2001%20-%20zakon%20o%20informacionoj%20bezbednosti%20oktobar%202022%20(1)%20(2).docx

Telo za koordinaciju poslova informacione bezbednosti

Telo za koordinaciju poslova informacione bezbednosti je koordinaciono telo Vlade Republike Srbije sastavljeno od predstavnika ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnika službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije, Centra za bezbednost IKT sistema u organima vlasti i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima.

Zadatak Tela za koordinaciju poslova informacione bezbednosti je ostvarivanje saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti, iniciranje i praćenje preventivnih i drugih aktivnosti u oblasti informacione bezbednosti, predlaganje mera za unapređenje informacione bezbednosti u Republici Srbiji, davanje sugestija i predloga koji se odnose na pripremu strateških dokumenata, podzakonskih akata i politika informacione bezbednosti u Republici Srbiji i utvrđivanje međusobne saradnje u slučaju incidenata koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti u Republici Srbiji.

Pored redovnih sastanaka, Telo za koordinaciju poslova informacione bezbednosti sastaje se i u slučajevima incidenata nivoa opasnosti „veoma visok“ i „visok“, a po potrebi i u slučajevima incidenata nivoa opasnosti „srednji“.

Telo za koordinaciju poslova informacione bezbednosti može u funkciji unapređenja pojedinih oblasti informacione bezbednosti formirati stručne radne grupe u koje se uključuju i predstavnici drugih organa javne vlasti, privrede, akademske zajednice i nevladinog sektora.

Nacionalni CERT

Nadležnost da obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou ima Nacionalni CERT, koji je uspostavljen u okviru Regulatornog tela za elektronske komunikacije i poštanske usluge. Zakonom o informacionoj bezbednosti propisano je da u nadležnosti Nacionalnog CERT-a spadaju:

- aćenje stanja o incidentima na nacionalnom nivou,
- pružanje ranih upozorenja, uzbuna i najava i informisanje relevantnih lica o rizicima i incidentima,
- pružanje saveta i preporuka po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i po prijavama fizičkih i pravnih lica, i preduzimanje drugih potrebnih mera iz svoje nadležnosti,
- izrada analiza rizika i incidenata,
- podizanje svesti kod građana, privrednih subjekata i organa vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti,
- vođenje evidencije Posebnih CERT-ova,
- izveštavanje Nadležnog organa o preduzetim aktivnostima.

Radi ispunjavanja svojih nadležnosti, Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema i sa CERT-om organa vlasti. Posebna saradnja uspostavlja se između Nacionalnog CERT-a, CERT-a organa vlasti i CERT-ova samostalnih operatora IKT sistema koji održavaju međusobne sastanke najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji. Ovim sastancima prisustvuju i predstavnici Nadležnog organa, a po potrebi i predstavnici Posebnih CERT-ova i druga lica.

Centar za bezbednost IKT sistema u organima vlasti (CERT organa vlasti)

CERT organa vlasti uspostavljen je u okviru Kancelarije za IT i elektronsku upravu i obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti, izuzev u IKT sistemima samostalnih operatora. Zakon o informacionoj bezbednosti propisuje da CERT organa vlasti ima sledeće nadležnosti:

- zaštita Jedinstvene informaciono-komunikacione mreže elektronske uprave,
- koordinacija i saradnja u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata sa operatorima IKT sistema koje povezuje Jedinstvena informaciono-komunikaciona mreža elektronske uprave,
- izdavanje stručnih preporuka za zaštitu IKT sistema organa vlasti, osim IKT sistema za rad sa tajnim podacima.

Više informacija o nadležnostima i uslugama koje pruža CERT organa vlasti može se naći na internet stranici Kancelarije za IT i elektronsku upravu.[29]

Samostalni operatori IKT sistema

Zakon o informacionoj bezbednosti propisuje da određeni IKT sistemi od posebnog značaja imaju drugačije obaveze u odnosu na ostale IKT sisteme od posebnog značaja. Ova grupa IKT sistema od posebnog značaja naziva se samostalni operatori IKT sistema i u nju spadaju ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove i službe bezbednosti.

Samostalni operatori IKT sistema imaju sledeće obaveze:

- da formiraju sopstvene centre za bezbednost IKT sistema radi upravljanja incidentima u svojim sistemima,
- da odrede posebna lica, odnosno organizacione jedinice za internu kontrolu sopstvenih IKT sistema koja izveštaj o izvršenoj internoj kontroli podnose rukovodiocu samostalnog operatora IKT sistema.

29 https://www.ite.gov.rs/tekst/88/cert.php

Samostalni operatori IKT sistema nemaju obavezu prijavljivanja incidenata koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti u jedinstveni sistem za prijem obaveštenja o incidentima.

Centri za bezbednost u samostalnim operatorima IKT sistema upravljaju incidentima u svojim sistemima i razmenjuju informacije o incidentima međusobno, sa Nacionalnim CERT-om, CERT-om organa vlasti i, po potrebi, sa drugim organizacijama. Pored toga, Centri za bezbednost u samostalnim operatorima IKT sistema mogu imati i druge nadležnosti kao što su:

1. izrada internih akata u oblasti informacione bezbednosti,
2. izbor, testiranje i implementacija tehničkih, fizičkih i organizacionih mera zaštite, opreme i programa,
3. izbor, testiranje i implementacija mera zaštite od KEMZ,[30]
4. nadzor implementacije i primene bezbednosnih procedura,
5. upravljanje i korišćenje kriptografskih proizvoda,
6. analiza bezbednosti IKT sistema u cilju procene rizika,
7. obuka zaposlenih u oblasti informacione bezbednosti.

Narodna banka Srbije ima obaveze kao i samostalni operatori IKT sistema, sa tom razlikom da ima zakonsku obavezu da prijavljuje incidente, kao i svi ostali IKT sistemi od posebnog značaja.

Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima (Posebni CERT-ovi)

Pravna lica sa sedištem na teritoriji Republike Srbije imaju mogućnost da u svom okviru formiraju posebno pravno lice ili organizacionu jedinicu radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika u IKT sistemima. Ovo posebno pravno lice ili organizaciona jedinica stiče status Posebnog CERT-a upisom u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT.

Upis u evidenciju posebnih CERT-ova regulisan je Pravilnikom o bližim uslovima za upis u Evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima.[31] Prijava za upis podnosi se u pismenom obliku (neposredno ili poštom), ili elektronskim putem na internet stranici Nacionalnog CERT-a.

Upis u evidenciju može biti izvršen ako Poseban CERT ispunjava sledeće uslove:

1. ima sedište na teritoriji Republike Srbije,
2. ima status pravnog lica ili organizacione jedinice u okviru pravnog lica,
3. u trenutku podnošenja prijave za upis u Evidenciju obavlja poslove prevencije i zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

30 Kompromitujuće elektromagnetno zračenje
31 https://www.ratel.rs/uploads/documents/empire_plugin/Pravilnik%20o%20sadr%C5%BEaju%2C%20na%C4%8Din u%20upisa%20i%20vo%C4%91enja%20evidencije%20posebnih%20centara%20za%20prevenciju%20bezbednosnih %20rizika%20u%20informaciono-komunikacionim%20sistemima.pdf

Jedinica lokalne samouprave može angažovati Poseban CERT za prevenciju bezbednosnih rizika i reagovanje na incidente u svom informaciono-komunikacionom sistemu, u skladu sa propisanim uslovima za uređivanje odnosa sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema.
Evidencija Posebnih CERT-ova nalazi se na internet stranici Nacionalnog CERT-a.[32]

Zakon o elektronskoj upravi[33]

Zakon o elektronskoj upravi uređuje obavljanje poslova uprave državnih organa i organizacija, organa i organizacija pokrajinske autonomije, organa i organizacija jedinica lokalne samouprave, ustanova, javnih preduzeća, posebnih organa preko kojih se ostvaruje regulatorna funkcija i pravnih i fizičkih lica kojima su poverena javna ovlašćenja upotrebom informaciono-komunikacionih tehnologija, odnosno uslovi za uspostavljanje, održavanje i korišćenje interoperabilnih informaciono-komunikacionih tehnologija organa. Ovim Zakonom nije obuhvaćeno postupanje sa aktima koji su, saglasno zakonu kojim se uređuje tajnost podataka, određeni kao tajna i označeni određenim stepenom tajnosti. Zakonom je propisano da informacioni sistemi, elektronske komunikacione mreže i oprema koja se koristi za vršenje elektronskog upravnog postupanja moraju da ispunjavaju uslove i standarde informacione bezbednosti, u skladu sa propisima.

Poslove koji se odnose na zaštitu od incidenata u okviru Jedinstvene informaciono-komunikacione mreže elektronske uprave obavlja Centar za bezbednost informaciono-komunikacionih sistema republičkih organa (CERT organa vlasti).

Na osnovu Zakona o elektronskoj upravi doneti su sledeći podzakonski akti:

- Uredba o bližim uslovima za uspostavljanje elektronske uprave [34]
- Uredba o organizacionim i tehničkim standardima za održavanje i unapređenje Jedinstvene informaciono-komunikacione mreže elektronske uprave i povezivanje organa na tu mrežu[35]
- Uredba o načinu vođenja Metaregistra, načinu odobravanja, suspendovanja i ukidanja pristupa servisnoj magistrali organa i načinu rada na Portalu eUprava [36]
- Uredba o načinu rada Portala otvorenih podataka [37]
- Uredba o bližim uslovima za izradu i održavanje veb prezentacije organa [38]

Jedinstvena informaciono-komunikaciona mreža elektronske upraveje informaciono-komunikaciona mreža koja omogućava prenos podataka između organa kojom upravlja ministarstvo nadležno za razvoj elektronske uprave.[39]
Jedinica lokalne samouprave zahtev za priključenje na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave podnosi ovom Ministarstvu, koje omogućava pristup u skladu sa organizacionim i tehničkim standardima.

Jedinica lokalne samouprave je dužna da poslove elektronske uprave obavlja preko Jedinstvene informaciono-komunikacione mreže elektronske uprave ili na drugi bezbedan način, u skladu sa propisima kojima se uređuje pitanje informacione bezbednosti.

32 https://www.cert.rs/rs/evidencija-certova.html 33 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/27/4/reg
34 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2018/104/1/reg
35 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2018/104/2/reg
36 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2018/104/3/reg
37 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2018/104/4/reg
38 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2018/104/5/reg
39 Zakonom o ministarstvima propisano je da je Ministarstvo državne uprave i lokalne samouprave nadležno za razvoj elektronske uprave.

Izuzetno, ako je zbog prirode poslova, razloga bezbednosti ili drugih opravdanih razloga utvrđenih posebnim zakonom propisano, jedinica lokalne samouprave može koristiti internu računarsku mrežu za obavljanje poslova elektronske uprave.

Radi uspostavljanja elektronske uprave jedinica lokalne samouprave je dužna da:

1. uspostavi odgovarajuću organizaciju poslova i radnih zadataka za elektronsku upravu,
2. obezbedi kadrove koji imaju neophodnu stručnost, iskustvo i kvalifikacije za primenu administrativnih i upravljačkih procedura koje odgovaraju standardima i koji su prošli odgovarajuću obuku u oblasti korišćenja informaciono-komunikacionih tehnologija, informacione bezbednosti, zaštite podataka o ličnosti, informacija od javnog značaja i otvorenih podataka,
3. obezbedi odgovarajuću opremu i softverska rešenja za poslove koje obavlja,
4. uspostavi mehanizam za autorizovani pristup sistemu,
5. omogući prijem podnesaka i dostavljanje elektronskim putem kao i praćenja statusa podneska,
6. omogući odlaganje priloga i elektronski potpisanih dokumenata u elektronske arhive, automatsko računanje roka čuvanja, upravnu statistiku i različite pretrage i preglede,
7. omogući prijem elektronske pošte, automatsko potvrđivanje primljenih poruka, povezivanje sa elektronskim adresama ovlašćenih službenih lica i mogućnost automatskog slanja poruka,
8. razvija servise za pribavljanje i ustupanje podataka iz registara i evidencija u elektronskom obliku,
9. omogući elektronsko plaćanje taksi i naknada u elektronskoj upravi,
10. uspostavi interoperabilnost informacionih sistema koji se koriste u elektronskoj upravi, u skladu sa Listom standarda interoperabilnosti,
11. ispuni uslove informacione bezbednosti u skladu sa zakonom,
12. vodi evidenciju o korisnicima usluga elektronske uprave,
13. omogući utvrđivanje tačnog datuma i vremena podnošenja elektronskih podnesaka,
14. obezbedi mogućnost elektronske identifikacije korisnika usluge elektronske uprave,
15. vodi evidenciju o podnetim elektronskim podnescima u elektronskoj upravi,
16. uspostavlja i vodi registar u skladu sa Zakonom o elektronskoj upravi i drugim propisima,
17. omogući čuvanje elektronskih podataka i dokumenata u propisanom vremenu kako bi se mogli obezbediti dokazi u upravnom i sudskom postupku,
18. osigura čuvanje i zaštitu elektronskih podataka i dokumenata i trajno čuvanje i zaštitu arhivske građe u elektronskom obliku, njeno održavanje, prebacivanje na savremene nosače u propisanim formatima sve do predaje nadležnom arhivu,
19. omogući pristup sadržaju i uslugama elektronske uprave svakome, u skladu sa standardima pristupačnosti,
20. omogući pristup sadržaju i uslugama elektronske uprave i na mobilnim uređajima.

Uredba o bližim uslovima za uspostavljanje elektronske uprave uređuje uslove za uspostavljanje elektronske uprave, odnosno izvršavanje dužnosti organa i organizacija jedinica lokalne samouprave radi uspostavljanja elektronske uprave. Između ostalog, jedinica lokalne samouprave je dužna da:

- uspostavi odgovarajuću organizaciju poslova i radnih zadataka,
- imenuje administratora za poslove koje obavlja elektronskim putem,
- obezbedi kadrove koji imaju neophodnu stručnost, iskustvo i kvalifikacije za primenu administrativnih i upravljačkih procedura,
- obezbedi odgovarajuću obuku u oblasti korišćenja informaciono-komunikacionih tehnologija, primenu standarda informacione bezbednosti i u oblastima otvorenih podataka i informacija od javnog značaja,
- obezbedi odgovarajuću opremu i softverska rešenja za poslove koje obavlja, poštujući propise i odgovarajuće standarde informacione bezbednosti,
- uspostavi mehanizme za autentifikaciju i autorizovani pristup sistemu u skladu sa propisima kojima se uređuje informaciona bezbednost i elektronska identifikacija.

Zakon o zaštiti podataka o ličnosti [40]

Zaštita podataka o ličnosti propisana je Zakonom o zaštiti podataka o ličnosti. Imajući u vidu da su jedinice lokalne samouprave organ vlasti koji je u neposrednom kontaktu sa građanima, pri čemu se u velikoj meri vrši obrada njihovih podataka, neophodno je da zaposleni u jedinicama lokalne samouprave poznaju propise koji regulišu mere zaštite koje se primenjuju prilikom obrade ove vrste podataka.

Zakonom o zaštiti podataka o ličnosti definisano je da je podatak o ličnosti svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta. Zakonom je takođe definisano da je obrada podataka o ličnosti svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima, kao što su prikupljanje, beleženje, razvrstavanje, grupisanje, odnosno strukturisanje, pohranjivanje, upodobljavanje ili menjanje, otkrivanje, uvid, upotreba, otkrivanje prenosom, odnosno dostavljanjem, umnožavanje, širenje ili na drugi način činjenje dostupnim, upoređivanje, ograničavanje, brisanje ili uništavanje.

Rukovalac, u smislu Zakona o zaštiti podataka o ličnosti, je fizičko ili pravno lice, odnosno organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade. Obrađivač je fizičko ili pravno lice, odnosno organ vlasti koji obrađuje podatke o ličnosti u ime rukovaoca. Pod povredom podataka o ličnosti podrazumeva se povreda bezbednosti podataka o ličnosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneseni, pohranjeni ili na drugi način obrađivani.

40 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg

Podaci o ličnosti moraju se obrađivati na način koji obezbeđuje odgovarajuću zaštitu podataka o ličnosti, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera. Rukovalac je prilikom određivanja načina obrade i u toku obrade, uzimajući u obzir nivo tehnoloških dostignuća i troškove njihove primene, prirodu, obim, okolnosti i svrhu obrade, kao i verovatnoću nastupanja rizika i nivo rizika za prava i slobode fizičkih lica koji proizilaze iz obrade, dužan da:

1. primeni odgovarajuće tehničke, organizacione i kadrovske mere, kao što je pseudonimizacija,[41] koje imaju za cilj obezbeđivanje delotvorne primene načela zaštite podataka o ličnosti, kao što je smanjenje broja podataka,
2. obezbedi primenu neophodnih mehanizama zaštite u toku obrade, kako bi se ispunili propisani uslovi za obradu i zaštitila prava i slobode lica na koja se podaci odnose.

Bezbednosni incidenti u IKT sistemima

Prethodno je objašnjeno da je incident svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema, dok sajber napadi označavaju podskup incidenata u IKT sistemu koji su namerno izazvani. U nastavku će pažnja biti posvećena objašnjenju i upravljanju ovoj grupi incidenata, ali predložene mere služe za smanjenje efekata i suzbijanje i svih ostalih vrsta incidenata.

Motivi i kategorije napadača

Namerno izazivanje bezbednosnih incidenata i zloupotrebe sajber prostora uopšte sprovode se uvek sa određenim razlogom. Motivi za ovakve aktivnosti mogu pripadati nekoj od sledećih kategorija:

1. finansijska dobit,
2. krađa identiteta,
3. urušavanje kritičnih IKT sistema,
4. špijunaža (državna i industrijska),
5. umanjenje poslovne sposobnosti,
6. krađa ličnih podataka,
7. manipulisanje javnim mnjenjem,
8. urušavanje ličnog integriteta,
9. urušavanje poslovne reputacije,
10. dokazivanje itd.

41 Pseudonimizacija označava obradu na način koji onemogućava pripisivanje podataka o ličnosti određenom licu bez korišćenja dodatnih podataka, pod uslovom da se ovi dodatni podaci čuvaju posebno i da su preduzete tehničke, organizacione i kadrovske mere koje obezbeđuju da se podatak o ličnosti ne može pripisati određenom ili odredivom licu.

Napadači koji pokreću i realizuju ove aktivnosti, odnosno izvori namernih pretnji mogu biti:

- države, koje mogu sprovoditi političku ili ekonomsku špijunažu, voditi kampanje dezinformisanja ili urušavati kritičnu infrastrukturu druge države,
- kompanije, čiji motiv može biti ekonomska špijunaža ili podrivanje sposobnosti ili reputacije konkurencije,
- kriminalci, koji su vođeni finansijskom dobiti,
- teroristi, koji nastoje da promovišu svoju ideologiju ili urušavaju kritičnu infrastrukturu,
- haktivisti, čiji je cilj da naude pojedincima, organizacijama ili državama sa kojima se ideološki ne slažu,
- radoznali korisnici, koji žele da dokažu svoje umeće sebi ili drugima i
- insajderi, koji iz osvete, besa, finansijskih razloga ili čiste nebrige izazivaju incidente u IKT sistemu organizacije u kojoj rade ili su ranije radili, ili su spoljni saradnici sa pravima pristupa.

Prema motivima i izvorima namerne pretnje se mogu podeliti u pet velikih kategorija:

- sajber kriminal,
- sajber špijunaža,
- sajber terorizam,
- sajber ratovanje i
- haktivizam (ili sajber vandalizam).

Sajber kriminal je daleko najzastupljenija kategorija u koju se može svrstati preko 80% svih zabeleženih napada.

Karakteristike namerno izazvanih bezbednosnih incidenata

Namerno izazvani bezbednosni incidenti (napadi) u IKT sistemima imaju jedinstvenu osobinu da i napadač i žrtva mogu biti bilo ko u tom trenutku povezan na taj IKT sistem. Ako je IKT sistem povezan na internet, napadač se može geografski nalaziti bilo gde. Sam napad se obično realizuje brzo, ali priprema za napad može trajati duži vremenski period, posebno ako je potencijalna žrtva veoma primamljiva i ako se neće ukazati druga prilika u slučaju da žrtva primeti pripreme za napad ili otkrije napad na vreme. U početnoj fazi napada tokom koje napadač izviđa svoju potencijalnu žrtvu (koja može biti i bilo ko zaposlen u jedinici lokalne samouprave) često se primenjuju tehnike socijalnog inženjeringa, od kojih su neke navedene u okviru ovih Smernica. Nakon izbora i prikupljanja informacija o svojoj potencijalnoj žrtvi napadač analizira uočene ranjivosti i vrši izbor metoda i tehnika napada. Kada smatra da je spreman, napadač pokušava da iskoristi ranjivosti i prodre u IKT sistem žrtve kako bi ostvario svoje namere.

Vrste incidenata

Postoje različite kategorizacije bezbednosnih incidenata i veliki broj različitih vrsta incidenata. U prilogu Uredbe o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja definisane su vrste incidenata koje su svrstane u sledeće grupe:

- Instaliranje zlonamernog softvera u okviru IKT sistema, u koju spadaju virus, crv, ransomver, trojanac, špijunski softver, rutkit;
- Neovlašćeno prikupljanje podataka, u koju spadaju skeniranje portova, presretanje podataka između računara i servera, socijalni inženjering (lažno predstavljanje i drugi oblici), kompromitovanje ili curenje podataka;
- Prevara, u koju spadaju fišing, neovlašćeno korišćenje resursa;
- Pokušaji upada u IKT sistem, u koju spadaju pokušaj iskorišćavanja ranjivosti sistema, pokušaj otkrivanja kredencijala;
- Upad u IKT sistem, u koju spadaju otkrivanje ili neovlašćeno korišćenje privilegovanih naloga, otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga, neovlašćeni pristup aplikaciji, mreža zaraženih uređaja;
- Nedostupnost ili ograničena dostupnost IKT sistema, u koju spadaju napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema, distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema, sabotaža, prekid u funkcionisanju sistema ili dela sistema;
- Ugrožavanje bezbednosti podataka, u koju spadaju neovlašćen pristup podacima, neovlašćena izmena ili brisanje podataka, kriptografski napad;
- Operativni incidenti, u koju spadaju otkazivanje hardverskih komponenti, problemi u radu sa softverskim komponentama;
- Incidenti fizičko-tehničke bezbednosti, u koju spadaju krađa hardverskih komponenti, požar, poplava;
- Ostali incidenti, u koju spadaju incidenti koji ne spadaju u gore navedene kategorije.

Neke od navedenih vrsta incidenata ukratko su objašnjene u narednom tekstu. Socijalni inženjering i fišing su detaljnije obrađeni, s obzirom da su usmereni ka osobama i da ih napadači veoma često primenjuju u praksi.

Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl. „malware")

Malver je zajedničko ime za svaki računarski kôd[42] napisan sa ciljem da izvrši neku zlonamernu aktivnost u informaciono-komunikacionom sistemu u kojem je pokrenut. Da bi ispunio svoj cilj napadač mora izvršiti dve radnje, a to je da prvo taj kôd unese u sistem (računar, mobilni telefon) potencijalne žrtve, a zatim i da pokrene njegovo izvršavanje. Realizacija ovih radnji nije jednostavna ako napadač nema pristup sistemu potencijalne žrtve, pa u tom cilju napadač pokušava da iskoristi ranjivosti koje postoje u sistemu ili da prevari nekog od zaposlenih da preuzme zaraženi fajl i pokrene ga (na primer, slanjem zaraženog fajla putem fišing mejla ili snimanjem zaraženog fajla na neki prenosni medij kao što je USB memorija i podešavanjem da se automatski pokrene prilikom povezivanja na računar). U nastavku su date osnovne karakteristike nekih podvrsta malvera.

Virus

Virus je vrsta malvera kojem je neophodan legitimni fajl domaćin na koji se zakači (doda svoj kôd na kôd tog fajla), pa se pokrene kad i taj fajl.[43] Prilikom izvršavanja traži druge potencijalne domaćine i pravi svoje kopije koje zakači na te fajlove. Ako su prilikom izvršenja ispunjeni i drugi uslovi predviđeni kôdom, sprovode se i druge zlonamerne aktivnosti kao što su brisanje podataka, slanje informacija napadaču preko interneta i slično.

Crv (engl. „worm")

Crvima nije potreban fajl domaćin, nego se kôd crva izvrši na nekom računaru i onda samostalno ispituje okruženje i mogućnost pristupa nekom drugom računaru sa kojim je povezan putem informaciono-komunikacionog sistema. Ako postoje ranjivosti u mrežnim ili informacionim sistemima, crv kopira svoj kôd na drugi računar gde se kopija izvrši i radi isti postupak. Na ovaj način za veoma kratko vreme može biti zaraženo puno računarskih sistema. Ostale karakteristike crva su slične kao kod virusa.

Ransomver (engl. „ransomware")

Ovaj tip malvera nakon aktivacije onemogućava pristup određenim resursima korisnika, a zatim obavesti korisnika (na primer, putem poruke na ekranu) o sprovedenim aktivnostima i načinu na koji može da plati otkup da bi ponovo bio u mogućnosti da raspolaže resursima. Ransomver može da blokira pristup nekim hardverskim resursima, ali najčešće su mu meta korisnički dokumenti, slike, video zapisi i slično, koje šifruje i zahteva otkup u zamenu za ključ za dešifrovanje. Ovu vrstu malvera napadači veoma često koriste poslednjih nekoliko godina. Redovna i sistemska izrada i provera kopija podataka je najbolja odbrana od ransomvera.

---

42 Računarski kôd je skup instrukcija napisanih u nekom programskom jeziku koje računar može da prepozna i izvrši. 43 Jedna od kategorija fajlova su izvršni fajlovi, koji sadrže instrukcije i podatke kojima se računaru zadaje izvršavanje određenih radnji (prikaz na ekranu, štampanje, snimanje na hard disk, brisanje iz memorije, slanje i prijem podataka sa interneta itd.). Instrukcije u izvršnom fajlu se izvršavaju po zadatom redosledu, a virusi i drugi malveri takođe sadrže instrukcije koje nastoje da dodaju u kôd odgovarajućih izvršnih fajlova kako bi se izvršile zajedno sa ostalim instrukcijama iz originalnog fajla. Instrukcije koje sadrže malveri mogu se odnositi na traženje mogućnosti za dalje širenje, uspostavljanje prikrivene komunikacije sa napadačem putem interneta, pretragu računara na kojem su aktivni, brisanje i šifrovanje fajlova na računaru i na druge zlonamerne aktivnosti. Izvršni fajlovi u koje malver doda svoje instrukcije (u žargonu se koristi izraz „na koje se zakači") nazivaju se fajlovi domaćini (engl. „host files").

Trojanac

Trojancima je potreban fajl domaćin kao i virusima, ali prilikom izvršenja ne prave svoju kopiju. Fajl domaćin je obično neki legitiman program koji je žrtva pokrenula ne znajući za zlonamerni dodatak u tom programu. Nakon pokretanja trojanac sprovodi definisane zlonamerne aktivnosti slično kao virusi i crvi.

Špijunski softver (engl. „spyware")

Ova vrsta malvera omogućava napadaču da dobije informacije o aktivnostima žrtve. Špijunski softver može beležiti stranice na internetu koje korisnik posećuje, snimati korisnička imena i lozinke za pristup i prikupljati druge podatke i slati ih napadaču.

Rutkit (engl. „rootkit")

Rutkitovi su vrsta malvera koju je napadač uspeo da smesti u deo memorije u kojem se nalaze programi koji se automatski izvršavaju prilikom pokretanja računara. Instaliranje malvera u taj deo memorije je veoma teško, ali je takođe teško i programima za zaštitu da otkriju takav malver zbog ekskluzivnosti tog dela memorije. Zbog velikih prava pristupa koje operativni sistem uobičajeno daje programima koji se nalaze u tom delu memorije, rutkitovi mogu bez posebnih prepreka da sprovode zlonamerne aktivnosti kao što su špijunuranje korisnika ili krađa podataka.

Neovlašćeno prikupljanje podataka

Postoje dve osnovne kategorije podataka koje napadači prikupljaju: podaci koji se mogu prodati i podaci koji se mogu upotrebiti za dalje faze napada. Svaki ozbiljniji napad započinje prikupljanjem podataka o potencijalnoj žrtvi, a u dosta slučajeva krajnji cilj napada je krađa osetljivih podataka žrtve.

Skeniranje portova

Jedna od metoda koju napadači koriste prilikom pripreme napada je skeniranje otvorenih portova na sistemu potencijalne žrtve u potrazi za ranjivostima koje mogu iskoristiti za upad u sistem.[44] Ako napadači pronađu takve ranjivosti, u sledećoj fazi napada primenjuju tehnike za iskorišćavanje ranjivosti i ostvaruju pristup sistemu.

44 Da bi bilo moguće sa jednog računara preko jednog internet priključka uspostaviti mnogobrojne konekcije ka različitim sistemima u različite svrhe (npr. štampanje, istovremeni pristup različitim veb sajtovima, kontrola i preuzimanje slika sa sistema video nadzora itd.) uvedena je tehnika kreiranja portova za svaku od tih konekcija. Portovi su u ovom slučaju određene numeričke vrednosti koje su poznate za dve strane koje komuniciraju preko interneta. Za određene aplikacije ove numeričke vrednosti su unapred određene, pa napadači skeniranjem portova proveravaju koje aplikacije su aktivne i pokušavaju da iskoriste poznate ranjivosti tih aplikacija. Pojam port odnosi se i na fizičke interfejse na uređajima pomoću kojih se povezuju drugi uređaji, ali u ovom slučaju napadači ne targetiraju taj tip portova.

Presretanje podataka između računara i servera (engl. „sniffing")

Prilikom ovog napada, koji je usmeren prema nezaštićenim ili loše zaštićenim komunikacijama, napadač korišćenjem podesnog uređaja ili softvera vrši pasivno snimanje (prisluškivanje) saobraćaja[45] u nekoj tački informaciono-komunikacionog sistema. Napadač je u mogućnosti da snimljeni saobraćaj naknadno analizira u potrazi za kredencijalima, osetljivim informacijama ili drugim informacijama koje će mu omogućiti dalji prodor u sistem.

Socijalni inženjering

Socijalni inženjering je pojam koji se odnosi na tehnike koje se primenjuju na pojedinca kako bi se naveo da učini nešto što nije u njegovom interesu. Na ovu temu treba posebno obratiti pažnju zbog masovnosti primene metoda socijalnog inženjeringa od strane napadača.

Tehnike socijalnog inženjeringa koriste ljudske osobine kao što su pohlepa, strah, nesigurnost, povodljivost, zavist, ali i dobrotu, plemenitost i druge pozitivne osobine. Socijalni inženjeri procenjuju koji pristup može biti najbolji kod određene osobe i realizuju ga, uz moguće stvaranje okvira koji će doprineti boljem efektu, kao što su uspostavljanje odnosa poverenja, vremenski pritisak da neka odluka mora brzo da se donese, stvaranje osećaja nestašice ili privida velikog broja istomišljenika i slično. Socijalni inženjering se u velikom broju slučajeva koristi u početnoj fazi kompleksnijeg sajber napada, pri čemu informacije dobijene od žrtve ili aktivnost koju žrtva izvrši otvaraju mogućnosti za ozbiljnije ugrožavanje nekog IKT sistema.

Postoje dve kategorije napada primenom metoda socijalnog inženjeringa:

- direktni napadi, kod kojih se napadač mora fizički približiti žrtvi i
- indirektni napadi, kod kojih napadač komunicira sa žrtvom korišćenjem nekog komunikacionog sredstva ili platforme za komunikaciju.

U direktne napade spadaju gledanje preko ramena dok neko unosi svoju lozinku ili PIN kod, prisluškivanje razgovora, prekopavanje tuđeg smeća u potrazi za traženim informacijama, lažno predstavljanje radi stvaranja autoriteta kod sagovornika ili neautorizovanog ulaska u određeni prostor i slično. Najčešći oblik indirektnih napada su razne varijante fišinga. Detaljnije tehnike fišinga objašnjene su u daljem tekstu.

Socijalni inženjering se može primenjivati istovremeno prema velikom broju potencijalnih žrtava korišćenjem različitih komunikacionih sredstava, a može se primenjivati i ad-hoc prema ljudima koji su se zadesili na određenom mestu u određenom trenutku. U slučaju da je krajnji cilj napada dovoljno unosan, kriminalci će socijalnom inženjeringu posvetiti koliko god vremena je potrebno da bi došli do neophodne informacije ili da bi ubedili žrtvu da uradi nešto što će im omogućiti dalje akcije.

45 Prilikom komunikacije između dva uređaja u informaciono-komunikacionom sistemu ne razmenjuju se samo informacije koje su razumljive za korisnike, nego postoji i značajna komunikacija kojom se uređaji i aplikacije automatski dogovaraju o načinu uspostavljanja konekcije, izboru protokola, proveri uspešnosti konekcije i slično. Sva komunikacija koja se odvija kroz jedan komunikacioni kanal naziva se saobraćaj.

U ovakvim situacijama socijalni inženjering se usmerava ka odabranom pojedincu i sastoji se od četiri faze:

> • istraga, tokom koje napadači biraju žrtvu, proučavaju je koristeći sve dostupne izvore (društvene mreže, objave na internetu itd) i osmišljavaju metodu socijalnog inženjeringa koju će koristiti, • udica, tokom koje napadači ostvaruju početni kontakt sa žrtvom, • igra, tokom koje napadači uvlače žrtvu u planirani kontekst i navode je da otkrije željenu informaciju ili da izvrši određenu aktivnost i • izlaz, koju napadači sprovode nakon što je žrtva uradila što su napadači planirali i tokom koje se prekida kontakt između napadača i žrtve na način da žrtva ne posumnja da je bila iskorišćena.

Napadači koji primenjuju socijalni inženjering su veoma vešti i u stanju su da prepoznaju odgovarajuću tehniku kojom treba da pristupe potencijalnoj žrtvi, ili da koriste kombinacije različitih tehnika da bi postigli uspeh. Svest o tehnikama koje se primenjuju prilikom ovakvih napada i oprez prilikom komunikacije sa nepoznatima može pomoći meti socijalnog inženjeringa da ne postane žrtva.

Kompromitovanje ili curenje podataka (engl. „data breaches")

Kompromitovanje ili curenje podataka u opštem smislu označava neovlašćeni pristup podacima. Cilj napadača je pristup tajnim, osetljivim i na bilo koji način interesantnim podacima koji im mogu doneti materijalnu dobit ili pomoću kojih mogu realizovati neke više ciljeve.[46] Kompromitovanje ili curenje podataka je po pravilu posledica grešaka i slabosti u tehnologiji ili ljudskom ponašanju.

Prevara

Prevara je opšti termin koji se koristi za opisivanje kriminalnih radnji koje se sprovode preko interneta u cilju nezakonitog sticanja informacija i njihovog korišćenja radi materijalne dobiti.

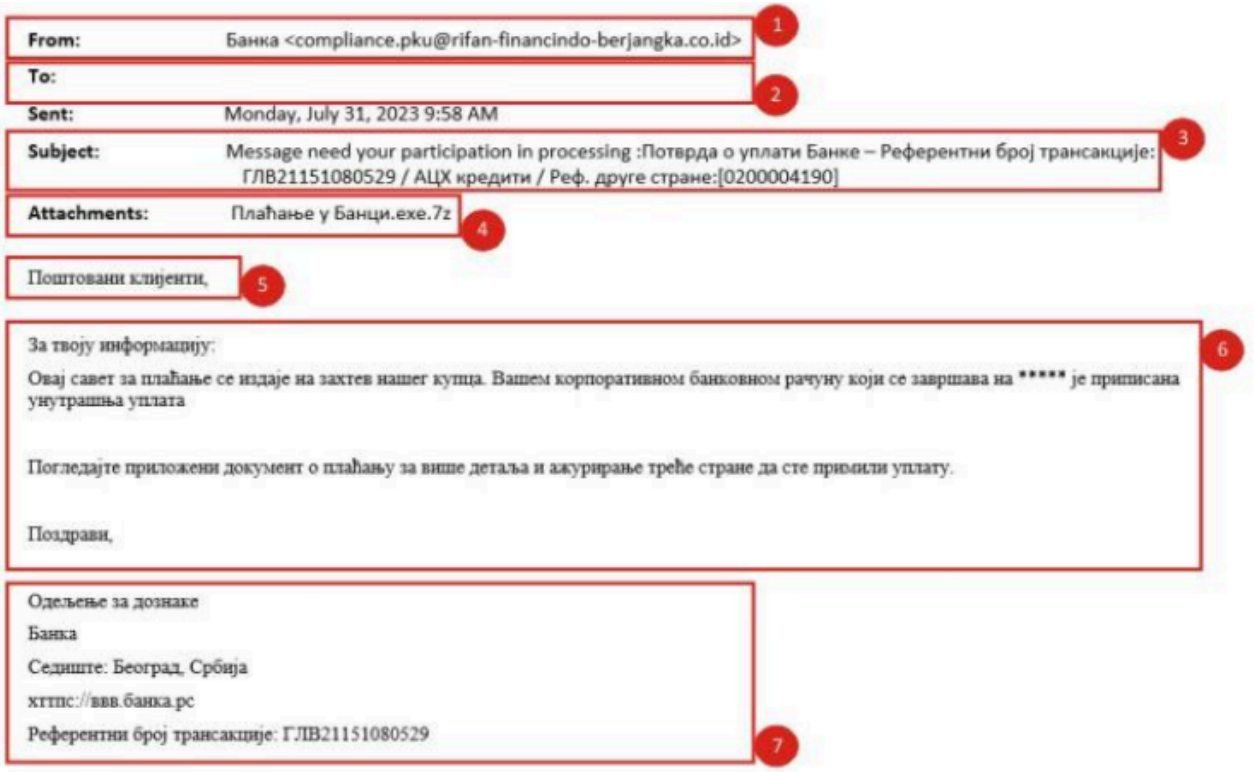
Fišing (engl. „phishing")

Fišing u opštem smislu označava vrstu napada primenom metoda socijalnog inženjeringa tokom kojeg napadač primenom nekog sredstva komunikacije pokušava da navede potencijalnu žrtvu da učini nešto što će napadaču biti od koristi. Postoje različite varijante fišinga:

46 Među najopasnije pretnje na internetu svrstavaju se napredne trajne pretnje (engl. Advanced Persistent Threat – APT). Ovaj termin se koristi za vrstu napada (i za organizovanu grupu napadača koja stoji iza napada) koji ima za cilj da se izvrši upad u IKT sistem i ostane neotkriven koliko god je moguće. Posebna karakteristika ovakvog napada je njegova složenost koja od napadača zahteva vrhunske specijalnosti u različitim oblastima. APT napadi se sprovode u nekoliko faza tokom kojih napadači razvijaju svoje mogućnosti pristupa i kontrole sistema, da bi došli u poziciju da neopaženo prikupljaju i preuzimaju osetljive podatke, intelektualnu svojinu i lične informacije, kao i da steknu mogućnosti da izbrišu podatke u sistemu žrtve ili unište sposobnost žrtve da nastavi sa radom (ako je to jedan od ciljeva napada). Zbog veštine napadača, neophodne logistike i velikih finansijskih troškova koje ovakvi napadi zahtevaju, često se smatra da su sponzorisani od strane država. Prema istraživanjima kompanije IBM Security, prosečno vreme otkrivanja APT napada od momenta upada napadača u sistem je oko 200 dana, nakon čega je u proseku potrebno još oko 70 dana da se ova pretnja potpuno eliminiše iz sistema žrtve.

- običan phishing, kada napadači na veliki broj adresa šalju identične poruke elektronske pošte u kojima se nalazi link ka stranici na internetu ili prilog, sa očekivanjem da određeni procenat primalaca neće biti dovoljno oprezan i da će kliknuti na link ili otvoriti prilog čime će zaraziti svoj računar, • spear phishing, kada napadači odaberu jednu žrtvu o kojoj imaju ograničen skup informacija koje iskoriste u poruci elektronske pošte kako bi naveli žrtvu da poveruje u sadržaj poruke i klikne na link ili otvori prilog,
- whaling, kada je ciljana osoba rukovodilac u nekoj organizaciji pa napadači posvećuju više vremena pripremi za napad i pažljivo i detaljno pripremaju tekst poruke jer očekuju veći dobitak,
- vishing, kada napadači primenjuju metode socijalnog inženjeringa u telefonskom razgovoru,
- smishing, kada se kao platforma za komunikaciju napadača sa žrtvom koriste SMS poruke,
- quishing, kada se žrtva navodi da otvori QR kod koji vodi na zlonamerni link.

Fišing može naneti štetu kako jedinici lokalne samouprave, tako i svakom pojedincu koji postane žrtva. Otvaranjem priloga ili klikom na link mogu se aktivirati malveri, pa je veoma važno da zaposleni prepoznaju elemente u elektronskoj poruci koji upućuju na prevaru. Na slici ispod je primer jedne elektronske poruke sa označenim delovima pomoću kojih se prepoznaje fišing.



Napadači koji šalju fišing poruke na veliki broj adresa nadaju se da određeni procenat primalaca neće biti dovoljno oprezan ili dovoljno vešt da prepozna fišing. Zbog toga je potrebno da se svakoj prispeloj poruci posveti malo pažnje i izvrši kratka analiza.

1. Obavezno proveriti adresu pošiljaoca, jer nelogične adrese sa kojih je mejl stigao upućuju da se radi o prevari. Prilikom provere treba biti pažljiv jer napadači umeju da se potrude da adresa bude slična originalnoj.
2. Proveriti da li je poruka upućena na ličnu ili službenu adresu elektronske pošte. Prazna lista primalaca ukazuje da je ista poruka poslata na veliki broj adresa, pa ako se u takvom slučaju tekst poruke odnosi na pojedinca, onda je to siguran pokazatelj pokušaja prevare.
3. Proveriti temu poruke jer nelogičnosti takođe mogu ukazivati na prevaru. Ako su napadači stranci, dešava se da prilikom prevođenja pomešaju jezike ili ekavicu i ijekavicu.
4. Prilog ili link u poruci uvek je razlog za dodatnu opreznost. Uvek treba razmisliti da li je baš neophodno da se otvori fajl ili klikne na link.
5. Način obraćanja takođe može ukazati na pokušaj prevare. Proveriti da li je način obraćanja u skladu sa običajima organizacije koja je navodno poslala poruku i da li je saglasan tekstu poruke, na primer da li se u obraćanju i tekstu meša jednina i množina.
6. U tekstu poruke mogu da se nalaze mnoge nelogičnosti. Napadači pokušavaju da namame potencijalnu žrtvu mogućnošću da ostvari finansijsku dobit, pritiskaju je ograničenim vremenom za reagovanje i primenjuju druge metode socijalnog inženjeringa kako bi je omeli da razmisli o mogućim posledicama. Uvek kada u poruci postoji neka ponuda treba razmisliti da li je previše povoljna da bi bila istinita.
7. Potpis takođe može biti pokazatelj prevare. Treba uočiti svaku nelogičnost, na primer ćirilično ispisivanje naziva stranice na internetu.

Osnovna mera zaštite koju svi treba da primenjuju je da dobro razmisle pre nego što kliknu na linkove u porukama ili otvore fajlove u prilozima (ovo se odnosi i na elektronsku poštu i na druge komunikacione platforme kao što su SMS, Viber, Whatsapp i slično). Napadači su sve veštiji u kreiranju fišing poruka i sve češće koriste sisteme veštačke inteligencije, pa se elementi koji ukazuju na prevaru teže prepoznaju. Iz tih razloga, pored provere prethodno navedenih elemenata, prilikom prijema poruke treba postaviti nekoliko pitanja:

- Da li je prijem ovakve poruke očekivan?
- Da li je tekst poruke u korelaciji sa pošiljaocem i dosadašnjim načinom komunikacije?
- Da li je zahtev da se klikne na link ili otvori prilog opravdan (ako u poruci postoje linkovi ili prilozi)?
- Da li u poruci ima bilo šta sumnjivo?

Ako postoji bilo kakva sumnja iz bilo kojeg razloga, pre bilo kakvih daljih akcija (a naročito kliktanja na link ili otvaranja priloga) potrebno je kontaktirati pošiljaoca putem neke druge komunikacione platforme i proveriti sve sumnjive elemente.

Neovlašćeno korišćenje resursa (engl. "cryptojacking" i drugi oblici)

Neovlašćeno korišćenje tuđih resursa naročito je zastupljeno u svrhu rudarenja kriptovaluta. Za ovakve napade koriste se specijalni malveri koje napadači ubace u računar ili mobilni telefon žrtve, koja ne samo što u tom slučaju ima znatno sporije performanse svog uređaja nego i troši znatno veće količine energije (i posledično dobija veće račune). Zbog ogromne procesorske snage koja je portrebna za kripto rudarenje, napadači često pokušavaju da zaraze što više računara, formiraju botnet mrežu i distribuiraju zadatke kripto rudarenja podjednako na svaki „zombi" uređaj.[47]

Pokušaji upada u IKT sistem

Napadi na informaciono-komunikacione sisteme ostavljaju tragove, ali je za zaštitu sistema neophodno da postoje uređaji za zaštitu koji će prepoznati pokušaje napada i podići alarme sa ciljem da nadležna lica sprovedu dodatne mere zaštite koje će suzbiti napad.

Pokušaj iskorišćavanja ranjivosti sistema

U početnim fazama napada napadači istražuju sistem u potrazi za ranjivostima koje bi mogli da eksploatišu. Ako se takva ispitavanja primete na vreme moguće je primeniti dodatne mere zaštite (kao što je, na primer, instaliranje odgovarajućih zakrpa) koje će sprečiti upad napadača u sistem.

Pokušaj otkrivanja kredencijala (engl. „brute force attack", „dictionary attack" i sl.)

Imajući u vidu činjenicu da značajan procenat korisnika nikada ne menja fabričke lozinke na uređajima, koristi jednostavne lozinke ili koristi iste lozinke za različite naloge, napadači kreiraju liste (rečnike – engl. „dictionary") najčešće korišćenih lozinki (koje mogu sadržati milione različitih lozinki) i uz pomoć specijalizovanih programa pokušavaju pristup ciljanim sistemima koristeći jednu po jednu lozinku sa liste dok ne uspeju da pristupe sistemu ili dok ne iscrpe listu.

47 Pojmovi zombi i botnet biće objašnjeni kasnije u tekstu

1. Obavezno proveriti adresu pošiljaoca, jer nelogične adrese sa kojih je mejl stigao upućuju da se radi o prevari. Prilikom provere treba biti pažljiv jer napadači umeju da se potrude da adresa bude slična originalnoj.
2. Proveriti da li je poruka upućena na ličnu ili službenu adresu elektronske pošte. Prazna lista primalaca ukazuje da je ista poruka poslata na veliki broj adresa, pa ako se u takvom slučaju tekst poruke odnosi na pojedinca, onda je to siguran pokazatelj pokušaja prevare.

Napadači koji primenjuju socijalni inženjering su veoma vešti i u stanju su da prepoznaju odgovarajuću tehniku kojom treba da pristupe potencijalnoj žrtvi, ili da koriste kombinacije različitih tehnika da bi postigli uspeh. Svest o tehnikama koje se primenjuju prilikom ovakvih napada i oprez prilikom komunikacije sa nepoznatima može pomoći meti socijalnog inženjeringa da ne postane žrtva.

Upad u IKT sistem

Upad u IKT sistem se odnosi na incident kod kojeg je napadač bez ovlašćenja ostvario pristup sistemu ili određenim resursima sistema.

Otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl. „privileged account compromise")

Administratori IKT sistema zbog prirode svog posla koriste naloge koji imaju širok ili neograničen pristup resursima sistema. Ovakvi nalozi se nazivaju privilegovani nalozi i moraju biti posebno zaštićeni. U slučaju da napadač kompromituje takav nalog i dobije prava pristupa kakva ima administrator, u mogućnosti je da izazove ogromnu štetu u IKT sistemu (krađa, brisanje i izmena podataka, instaliranje malvera itd.).

Otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl. „unprivileged account compromise")

Neovlašćeni pristup aplikaciji

Neovlašćeni pristup nekoj aplikaciji može se ostvariti ako ta aplikacija poseduje neku ranjivost. Napadači mogu iskoristiti te ranjivosti da preko aplikacije sprovedu druge zlonamerne aktivnosti.

Mreža zaraženih uređaja (engl. „botnet")

Računar u koji je napadač ubacio specijalizovan malver koji mu omogućava kontrolu nad tim računarom naziva se zombi, a u velikom broju slučajeva korisnici takvih računara nisu svesni aktivnosti koje napadač sprovodi u pozadini. Pojam botnet odnosi se na mrežu takvih zaraženih računara koje napadač može kontrolisati bez znanja njihovih vlasnika. Ovakve mreže računara napadači koriste za DDoS napade ili slanje fišing poruka.

Nedostupnost ili ograničena dostupnost IKT sistema

Među osnovne ciljeve primene mera informacione bezbednosti je očuvanje raspoloživosti pristupa informacijama. Da bi narušili ovo svojstvo napadači pribegavaju različitim tehnikama koje imaju za cilj da informacije i uređaji postanu nedostupni legitimnim korisnicima.

Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. "denial–of–service attack" – DoS)

Prilikom napada ove vrste napadači šalju veliki broj zahteva na odabrani sistem kako bi doveli taj sistem u situaciju da troši vreme obrađujući te zahteve, dok legitimni zahtevi drugih korisnika čekaju da dođu na red. Obično zahtevi napadača budu formulisani sa namernim greškama ili budu nepotpuni, pa napadnuti sistem troši više vremena na obradu tih zahteva.

Distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. "distributed denial–of–service attack" – DDoS)

Efikasnost napada koji imaju za cilj uskraćivanje usluge zavisi od mogućnosti napadača da broj zahteva koje šalje prema napadnutom sistemu bude veći od broja zahteva koje taj sistem može da obradi. Ovakav kapacitet u realnim okolnostima ne može da se postigne sa jednog računara, pa napadači koriste više računarskih sistema sa kojih istovremeno izvode napad ka ciljanom sistemu. U tu svrhu napadači moraju na internetu stvoriti mrežu računara koje su prethodno zarazili i koje mogu kontrolisati bez znanja njihovih vlasnika i korisnika.

Napadi na lanac snabdevanja

Veće organizacije, koje su željena meta napadača, obično primenjuju jače bezbednosne mere pa prodor u takve sisteme i druge zlonamerene aktivnosti nisu jednostavan zadatak. Atraktivnost takvih organizacija zbog mogućnosti za veću zaradu ili izvlačenje vrednih informacija predstavlja stimulans za napadače da traže ranjivosti gde god postoje i pokušaju da ih iskoriste. Jedna od mogućnosti je da se izvrši napad na manje kompanije koje isporučuju uređaje ili softver većim organizacijama jer se pokazalo da one imaju blaže bezbednosne kriterijume (ili nemaju dovoljnu bezbednosnu kulturu) i nemaju resurse za primenu jakih bezbednosnih mera. Ako napadači uspeju da naprave proboj u sistem takve manje kompanije i umetnu svoj malver u proizvod koji će se isporučiti većoj organizaciji, onda će ta veća organizacija u svoj sistem implementirati i zlonamerni kôd koji će napadaču omogućiti dalji pristup. Ovakvi napadi nazivaju se napadi na lanac snabdevanja za koje postoji nekoliko primera poslednjih godina, od kojih su neki napravili izuzetno veliku štetu. Zbog toga se ulažu veliki napori da se uspostavi okvir i metode za verifikaciju i sertifikaciju proizvoda kako bi se smanjili rizici od ovakve vrste napada.

Primena mera bezbednosti

Potrebno je štititi sve što ima vrednost za jedinicu lokalne samouprave. To mogu biti informacije, hardver, softver i druga imovina. Što je neka imovina vrednija to je treba više čuvati, ali pri tome treba primenjivati princip da vrednost primenjenih mera bezbednosti ne sme prevazići vrednost imovine.

Svakako treba imati na umu da se vrednost ne odnosi samo na cenu koštanja nekog uređaja ili podatka, jer i reputacija organa javne uprave zavisi od njegove mogućnosti da svoje obaveze izvršava na vreme i zaštiti podatke građana i privrede koji su mu na raspolaganju. Reputacija i poverenje se grade godinama a mogu biti narušeni za kratko vreme, pa je i taj aspekt potrebno uzeti u obzir prilikom procene rizika.

Kategorije i pregled mera bezbednosti

Mere bezbednosti mogu se svrstati u tri velike grupe: fizičke, organizacione i tehničke.
U fizičke mere bezbednosti spadaju sve mere kojima se neovlašćena lica sprečavaju ili odvraćaju da pristupe nekom prostoru ili kontroliše fizičko prisustvo. U ove mere spadaju fizičko obezbeđenje, ograde, sistemi video nadzora, alarmni sistemi, sistemi za fizičku kontrolu pristupa i slično.

U organizacione (administrativne) mere spadaju sve procedure, pravila, politike i drugi dokumenti kojima se organizuje bezbednost u nekoj organizaciji ili, u ovom slučaju, jedinici lokalne samouprave, uspostavljanje posebnih organizacionih jedinica ili određivanje osoba nadležnih za informacionu bezbednost, uspostavljanje prakse prijavljivanja narušavanja informacione bezbednosti, izrada procene rizika, ranjivosti i pretnji, primena najboljih praksi, praćenje trendova, obuke i podizanje svesti zaposlenih, uključivanje informacione bezbednosti u proces planiranja, klasifikacija i označavanje osetljivih podataka i slično.

U tehničke (logičke) mere spadaju svi tehnički sistemi namenjeni očuvanju bezbednosti, kao što su sistemi za identifikaciju, autentifikaciju i autorizaciju48, razni uređaji za zaštitu računarskih mreža (mrežne barijere, IPS, IDS, WAF, ruteri itd), softveri namenjeni bezbednom korišćenju računara (anti-malver, VPN, softveri za enkripciju i bezbedno brisanje itd) i slično.

Treba imati na umu da savršena zaštita ne postoji, jer postoje nesavršenosti u uređajima i protokolima, kao i mogućnosti da zaposleni odnosno službenici prave greške. U IKT sistemima postoje mnoge bezbednosne ranjivosti kojih ni proizvođači uređaja i softvera nisu svesni. Zbog toga treba po pitanjima bezbednosti stalno biti oprezan, pratiti informacije o otkrivenim ranjivostima, uspostaviti redovne obuke za zaposlene, pripremati se i u slučaju potrebe reagovati brzo i efikasno.

Kratak pregled uređaja i softvera za zaštitu

Mrežna barijera

Mrežna barijera (engl. „firewall“) je uređaj koji se nalazi na granici između mreže (na primer, između interneta i interne računarske mreže) i koji ima svrhu da filtrira saobraćaj prema definisanim pravilima. Ovaj uređaj ima unapred definisane kriterijume za blokiranje paketa, ali pored toga i ugrađenu logiku koja prepoznaje određene tipove napada i može da ih spreči. Uvakvi uređaji se veoma često sreću zbog svoje jednostavnosti i primenljivosti, a mogu biti izvedeni i u harderskoj i u softverskoj verziji.

Napadi na lanac snabdevanja

Veće organizacije, koje su željena meta napadača, obično primenjuju jače bezbednosne mere pa prodor u takve sisteme i druge zlonamerene aktivnosti nisu jednostavan zadatak. Atraktivnost takvih organizacija zbog mogućnosti za veću zaradu ili izvlačenje vrednih informacija predstavlja stimulans za napadače da traže ranjivosti gde god postoje i pokušaju da ih iskoriste. Jedna od mogućnosti je da se izvrši napad na manje kompanije koje isporučuju uređaje ili softver većim organizacijama jer se pokazalo da one imaju blaže bezbednosne kriterijume (ili nemaju dovoljnu bezbednosnu kulturu) i nemaju resurse za primenu jakih bezbednosnih mera. Ako napadači uspeju da naprave proboj u sistem takve manje kompanije i umetnu svoj malver u proizvod koji će se isporučiti većoj organizaciji, onda će ta veća organizacija u svoj sistem implementirati i zlonamerni kôd koji će napadaču omogućiti dalji pristup. Ovakvi napadi nazivaju se napadi na lanac snabdevanja za koje postoji nekoliko primera poslednjih godina, od kojih su neki napravili izuzetno veliku štetu. Zbog toga se ulažu veliki napori da se uspostavi okvir i metode za verifikaciju i sertifikaciju proizvoda kako bi se smanjili rizici od ovakve vrste napada.

Primena mera bezbednosti

> Potrebno je štititi sve što ima vrednost za jedinicu lokalne samouprave. To mogu biti informacije, hardver, softver i druga imovina. Što je neka imovina vrednija to je treba više čuvati, ali pri tome treba primenjivati princip da vrednost primenjenih mera bezbednosti ne sme prevazići vrednost imovine.

Svakako treba imati na umu da se vrednost ne odnosi samo na cenu koštanja nekog uređaja ili podatka, jer i reputacija organa javne uprave zavisi od njegove mogućnosti da svoje obaveze izvršava na vreme i zaštiti podatke građana i privrede koji su mu na raspolaganju. Reputacija i poverenje se grade godinama a mogu biti narušeni za kratko vreme, pa je i taj aspekt potrebno uzeti u obzir prilikom procene rizika.

Kategorije i pregled mera bezbednosti

Mere bezbednosti mogu se svrstati u tri velike grupe: fizičke, organizacione i tehničke.
U fizičke mere bezbednosti spadaju sve mere kojima se neovlašćena lica sprečavaju ili odvraćaju da pristupe nekom prostoru ili kontroliše fizičko prisustvo. U ove mere spadaju fizičko obezbeđenje, ograde, sistemi video nadzora, alarmni sistemi, sistemi za fizičku kontrolu pristupa i slično.

U organizacione (administrativne) mere spadaju sve procedure, pravila, politike i drugi dokumenti kojima se organizuje bezbednost u nekoj organizaciji ili, u ovom slučaju, jedinici lokalne samouprave, uspostavljanje posebnih organizacionih jedinica ili određivanje osoba nadležnih za informacionu bezbednost, uspostavljanje prakse prijavljivanja narušavanja informacione bezbednosti, izrada procene rizika, ranjivosti i pretnji, primena najboljih praksi, praćenje trendova, obuke i podizanje svesti zaposlenih, uključivanje informacione bezbednosti u proces planiranja, klasifikacija i označavanje osetljivih podataka i slično.

U tehničke (logičke) mere spadaju svi tehnički sistemi namenjeni očuvanju bezbednosti, kao što su sistemi za identifikaciju, autentifikaciju i autorizaciju,[48] razni uređaji za zaštitu računarskih mreža (mrežne barijere, IPS, IDS, WAF, ruteri itd), softveri namenjeni bezbednom korišćenju računara (anti-malver, VPN, softveri za enkripciju i bezbedno brisanje itd) i slično.

Treba imati na umu da savršena zaštita ne postoji, jer postoje nesavršenosti u uređajima i protokolima, kao i mogućnosti da zaposleni odnosno službenici prave greške. U IKT sistemima postoje mnoge bezbednosne ranjivosti kojih ni proizvođači uređaja i softvera nisu svesni. Zbog toga treba po pitanjima bezbednosti stalno biti oprezan, pratiti informacije o otkrivenim ranjivostima, uspostaviti redovne obuke za zaposlene, pripremati se i u slučaju potrebe reagovati brzo i efikasno.

Kratak pregled uređaja i softvera za zaštitu

Mrežna barijera

Mrežna barijera (engl. „firewall“) je uređaj koji se nalazi na granici između mreže (na primer, između interneta i interne računarske mreže) i koji ima svrhu da filtrira saobraćaj prema definisanim pravilima. Ovaj uređaj ima unapred definisane kriterijume za blokiranje paketa, ali pored toga i ugrađenu logiku koja prepoznaje određene tipove napada i može da ih spreči. Uvakvi uređaji se veoma često sreću zbog svoje jednostavnosti i primenljivosti, a mogu biti izvedeni i u harderskoj i u softverskoj verziji.

48 Identifikacija se odnosi na predstavljanje korisnika sistemu (na primer, korisničkim imenom). Autentifikacija (ponekad se koristi i izraz autentikacija) znači pruženje dokaza sistemu o identitetu korisnika (na primer, unošenjem lozinke). Nakon toga, sistem proverava šta taj korisnik ima prava da radi u sistemu i autorizuje ga (omogućava mu da koristi određene uređaje ili da pristupi određenim aplikacijama i podacima u sistemu).

WAF

Web Application Firewall (WAF) je uređaj koji ima namenu da zaštiti veb stranicu od specijalizovanih napada koji imaju za cilj pristup restriktivnim delovima sajta, izmenu veb stranica, postavljanje zlonamernih sadržaja i slično. Ovim uređajem se štiti kako sadržaj veb stranice tako i korisnici koji pristupaju stranici.

IPS i IDS

Intrusion Prevention System (IPS) i Intrusion Detection System (IDS) su uređaji koji se postavljaju u sistem kako bi otkrili uljeze na osnovu predefinisanih modela i na osnovu informacija o ponašanju korisnika sistema u prethodnom periodu. Ovi uređaji po postavljanju u neki sistem moraju da prođu neki period učenja kako bi prepoznali uobičajeno ponašanje korisnika sistema i u tom periodu im je potrebna asistencija nekog administratora. Razlika između IPS i IDS je u tome što se IPS postavlja na liniju toka saobraćaja i poseduje i mogućnost prekida saobraćaja u slučaju da identifikuje neregularno ponašanje, dok se IDS postavlja paralelno liniji toka saobraćaja i samo daje alarme u slučaju detekcije neregularnog ponašanja.

SIEM

Security Incident and Event Management (SIEM) je platforma u koju se u realnom vremenu slivaju podaci sa različitih uređaja, ne samo uređaja koji su implementirani iz razloga bezbednosti već i sa različitih servera, računara krajnjih korisnika i mrežnih uređaja. SIEM sistem vrši obradu svih informacija i pravi njihovu korelaciju po vremenu i iz svih dobijenih informacija izvlači zaključke o incidentima ili pretnjama sistemu.

Anti-malveri (engl. „anti-malware“)

Služe za detekciju i uklanjanje ili onemogućavanje dejsta raznih vrsta malvera (virusa, crva, trojanaca itd). Osnovni režim rada im je da upoređuju podatke iz memorije (operativne ili masovne) sa svojom bazom podataka i ako nađu poklapanje sprovode zadatu aktivnost (na primer, stavljaju malver u karantin ili ga brišu). Postoji i drugi režim rada anti-malver softvera koji proverava da li u sistemu postoje obrasci ponašanja tipični za malvere i ako pronađu takve obrasce uključuju alarm i sprovode zadate aktivnosti. Ovaj režim rada naziva se heuristički ili bihejvioralni.

Kako se svakodnevno pojavi veoma veliki broj novih malvera i njihovih varijanti i podvarijanti, neophodno je redovno raditi ažuriranje baze anti-malver softvera.

Često se za ovaj proizvod upotrebljava i termin anti-virus.

Anti-spajveri (engl. „anti-spyware“)

Kao što je već objašnjeno, špijunski softveri su specijalizovani malveri koji, kad se aktiviraju na računaru žrtve, prikupljaju informacije o njenom ponašanju i aktivnostima i šalju te informacije napadaču koji kontroliše špijunski softver. Anti-spajver softveri prepoznaju malvere ovog tipa i onemogućavaju njihovo delovanje.

Mere bezbednosti na radnom mestu

Razdvajanje poslovnog i privatnog

Veoma često se službene i privatne informacije mešaju, što predstavlja rizik jer kompromitacijom privatnih uređaja i naloga napadač ima pristup i službenim informacijama i obrnuto.

Čuvanje tajnosti lozinki

Službenici imaju običaj da međusobno dele korisnička imena i lozinke ili da ih ostavljaju zapisane na papirićima na lako dostupnim mestima. Na ovaj način dolaze u rizik da njihovi nalozi budu zloupotrebljeni.

Zaključavanje računara prilikom izlaska iz kancelarije

Računar se može zaključati jednostavnom kombinacijom tastera, nakon čega je potrebno uneti lozinku radi otključavanja. Ovu meru službenici treba da primenju čak i kada iz kancelarije izlaze na kratko.

Jasno označavanje dokumenata

Svi službenici treba striktno da primenjuju propise koji važe za dokumente sa oznakama tajnosti. Označavanjem dokumenta daje se svim ostalim radnicima jedinice lokalne samouprave jasna poruka kako sa tim dokumentom treba postupati.

Politika „čistog stola“

Pre napuštanja kancelarije sa stola treba skloniti sve papirne dokumente koji sadrže osetljive informacije. Time se sprečava da neko ko ima pristup stolu bude u mogućnosti da dođe do važnih informacija.

Brisanje prenosnih medija

Sa svakog prenosnog medija koji treba da se upotrebi van jedinice lokalne samouprave prethodno moraju biti obrisani podaci na bezbedan način. Kao što postoje dostupni alati koji mogu da vrate podatke koji nisu bezbedno obrisani, tako postoje i dostupni alati za bezbedno brisanje koji onemogućavaju takve akcije.

Pažljiva upotreba tuđih i nepoznatih prenosnih medija

Prenosni mediji mogu biti opasni jer se na njima mogu nalaziti malveri.[49] Na svoj uređaj sme se povezivati samo prenosni medij za koji se zna poreklo, a i u tom slučaju potrebno ga je proveriti nekom anti-malver softverom pre korišćenja. Takođe je potrebno isključiti opciju automatskog izvršavanja prilikom povezivanja eksternih uređaja.[50]

Primena principa „potrebno da zna”

Princip „potrebno da zna” odnosi se na davanje drugim osobama onoliko informacija koliko je potrebno da znaju da bi mogle da realizuju neku aktivnost. Ovaj princip se naročito odnosi na davanje informacija saradnicima van jedinice lokalne samouprave.

Zaštita službene adrese elektronske pošte

Službena adresa elektronske pošte ima svoju ulogu samo za službenu komunikaciju i za pristup nalozima koji se koriste za službene potrebe. Službena adresa elektronske pošte ne koristi se za privatne potrebe.

Pažnja prilikom vođenja službenih razgovora

Vođenje razgovora o službenim stvarima u situacijama kada treća lica mogu da čuju razgovor može dovesti do odavanja osetljivih informacija. Uvek kada se vode službeni razgovori, bez obzira da li se razgovor vodi na fizičkoj lokaciji ili putem nekog sredstva komunikacije, treba biti oprezan i ne iznositi informacije koje mogu ugroziti bezbednost.

49 Jedan od načina na koji kriminalci pokušavaju da instaliraju malver u neki računarski sistem je da ga snime na prenosni medij i pokušaju da prevare nekog od službenika da taj medij (najčešće USB memoriju) ubaci u svoj računar, nakon čega malver treba automatski da se izvrši. Često kriminalci pribegavaju metodi da USB memoriju ostave na mestu na kojem će ga pronaći neki od službenika (na primer, bace ga na pod u hodniku u jedinici lokalne samouprave ili ostave na stolu u pekari u koju često svraćaju službenici) u nadi da će ga neko povezati na računar u svojoj kancelariji da proveri da li pripada nekom od kolega. 50 Zbog velikog rizika u nekim organizacijama je zabranjena upotreba USB memorija na uređajima koji su povezani na IKT sistem.

Mere bezbednosti tokom službenog putovanja

Zaštita kartica

Uvek, a posebno u nepoznatoj sredini treba voditi računa prilikom korišćenja kartica i unošenja PIN-a kako ne bi došlo do mogućnosti zloupotrebe. Kriminalci pokušavaju da aktiviraju beskontaktne kartice i snime podatke kako bi ih zloupotrebili, pa je korisno držati kartice u futrolama koje sprečavaju njhovo aktiviranje i vaditi ih iz futrola samo prilikom upotrebe.

Nošenje samo neophodnih podataka

Mobilni uređaji su uvek u riziku od krađe, a posebno je opasno ako sa uređajem budu ukradeni osetljivi podaci koji se na njima nalaze. Na put treba nositi samo zaista neophodne podatke i dodatno ih zaštititi šifrovanjem.

Mere bezbednosti na javnom mestu

Isključivanje bluetooth konekcije

Bluetooth konekcija je pogodna za brzu organizaciju razmene podataka, ali je i podložna raznim vrstama napada. Zbog malog dometa Bluetooth konekcije napadači moraju prići blizu svojoj potencijalnoj žrtvi, pa je jedna od mera bezbednosti da se na javnim mestima na kojima se okuplja veći broj ljudi ova vrsta konekcije isključi.

Izbegavanje korišćenja otvorenih bežičnih mreža

Za pristup otvorenim bežičnim mrežama nije potrebno posedovanje bilo kakvih kredencijala, ali je i komunikacija svih povezanih korisnika otvorena i dostupna bilo kome ko se nalazi u dometu pristupne tačke. Na otvorene mreže na javnim mestima treba se povezivati samo ako je povezivanje neophodno i ako nema drugih mogućnosti, a i tada ne treba pristupati nalozima i unostiti lozinke.

Bezbednost podataka

Primenjene mere bezbednosti imaju za cilj da obezbede tri osnovna bezbednosna svojstva:

- tajnost – podrazumeva da su podaci ili drugi resursi dostupni samo ovlašćenim osobama,
- integritet – podrazumeva da podatke mogu menjati samo ovlašćene osobe i
- raspoloživost – podrazumeva da ovlašćene osobe podacima ili drugim resursima mogu pristupati uvek kada su im potrebni.

Za ova tri bezbednosna svojstva se često koristi naziv CIA trijada prema akronimu na engleskom jeziku (confidentiality, integrity i availability).

Klasifikacija podataka

Podaci se razlikuju po značaju. Dok neki podaci mogu slobodno da se objavljuju javno, postoje podaci koje je potrebno da zna samo mali broj ovlašćenih lica i koji se moraju dodatno štititi.

Iz tih razloga primenjuje se klasifikacija podataka – svrstavanje podataka u određenu kategoriju, pri čemu svaka kategorija podrazumeva primenu određenih mera zaštite.

Mere zaštite koje će se primeniti zavise od značaja podatka i oblika u kojem se nalazi (elektronskom ili fizičkom – npr. papirnom) i primenjuju se u procesima obrade, čuvanja i prenosa podataka, a najčešće se primenjuju mere kriptozaštite (šifrovanje) prilikom prenosa i čuvanja, kontrola pristupa, obrada i čuvanje na odvojenim ili zaštićenim uređajima i slično.

Zakonom o tajnosti podataka[51] uređeno je određivanje i zaštita tajnih podataka. Po ovom Zakonu, tajni podatak je podatak od interesa za Republiku Srbiju koji je određen i označen određenim stepenom tajnosti, a čijim otkrivanjem neovlašćenom licu bi nastala šteta po interese Republike Srbije. Određivanje tajnosti podatka vrše ovlašćena lica, između ostalih rukovodioci organa javne vlasti (uključujući rukovodioce organa jedinica lokalne samouprave) i lica zaposlena u organu javne vlasti koja je za određivanje tajnosti podataka pismeno ovlastio rukovodilac tog organa.

Tajni podatak može imati jedan od sledećih stepena tajnosti:

- „DRŽAVNA TAJNA", koji se određuje radi sprečavanja nastanka neotklonjive teške štete po interese Republike Srbije;
- „STROGO POVERLJIVO", koji se određuje radi sprečavanja nastanka teške štete po interese Republike Srbije;
- „POVERLJIVO", koji se određuje radi sprečavanja nastanka štete po interese Republike Srbije;
- „INTERNO", koji se određuje radi sprečavanja nastanka štete za rad, odnosno obavljanje zadataka i poslova organa javne vlasti koji ih je odredio.

Pristup tajnim podacima dozvoljen je licima koja poseduju odgovarajući bezbednosni sertifikat, koji se dobija nakon bezbednosne provere koju sprovodi nadležni organ.

51 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2009/104/7

Sajber higijena

Koncept sajber higijene odnosi se na rutinsko sprovođenje preventivnih bezbednosnih mera, kao što se rutinski peru ruke radi očuvanja zdravlja. U suštini, sajber higijena obuhvata osnovne bezbednosne prakse koje treba redovno da sprovode sva službena lica koja imaju pristup IKT sistemu, od službenika sa neprivilegovanim nalozima, preko administratora IKT sistema do rukovodilaca, kako bi se smanjile mogućnosti za bezbednosne incidente koji mogu naneti štetu jedinici lokalne samouprave.

U nastavku su navedene neke od mera sajber higijene, koje nisu komplikovane i ne zahtevaju veliko tehničko znanje, ali je bitno da se sprovode uvek kada je potrebno. Cilj je da primena ovih mera uđe u naviku i postane normalna praksa, a ne da se o njima posebno razmišlja i prave planovi. Ako se ovaj cilj ostvari kod svih službenika koji imaju pristup IKT sistemu jedinice lokalne samouprave onda će i taj sistem biti mnogo bezbedniji, ali će biti bezbedniji i ovi službenici, jer će stečene navike primenjivati i prilikom upotrebe privatnih uređaja i podataka.

Isključivanje bluetooth konekcije

Poizvođači softvera i uređaja su u stalnom procesu preispitivanja bezbednosti njihovih proizvoda i izrade poboljšanja kako bi se eliminisale uočene ranjivosti. Ova poboljšanja se korisnicima njihovih proizvoda isporučuju u obliku zakrpa (engl. „patches“) ili ažuriranja (engl. „updates“), pri čemu se zakrpe obično izrađuju za rešavanje jednog problema (po pravilu bezbednosne prirode), dok ažuriranja sadrže veći broj poboljšanja uključujući i rešavanje bezbednosnih ranjivosti.

Objavljene zakrpe i ažuriranja treba što pre instalirati jer je sa zakrpama i ažuriranjima objavljena i informacija o ranjivostima, pa napadači nakon toga kreću u potragu za sistemima koji ih još uvek nisu instalirali kako bi ih napali. Za najveći broj korisnika najbolja opcija je uključivanje automatskog ažuriranja, kada sistem samostalno proverava postojanje zakrpe ili ažuriranja i automatski ih instalira.

Redovno pravljenje rezervih kopija podataka (engl. backup)

Redovno pravljenje rezervnih kopija važnih podataka je jedna od osnovnih mera sajber higijene. Pri pravljenju rezervnih kopija treba voditi računa o načinu i lokaciji njihovog čuvanja, kao i redovno proveravati upotrebljivost rezervnih kopija. Rezervne kopije se nikada ne čuvaju na istoj lokaciji sa podacima koji su u upotrebi.

Korišćenje jakih i posebnih lozinki

Definisanje i dosledna primena politike bezbedne upotrebe lozinki je veoma bitna za jedinicu lokalne samouprave jer smanjuje mogućnosti za bezbednosni incident, ali je bitna i za svakog pojedinca u zaštiti ličnih podataka. Politikom bezbedne upotrebe lozinki definišu se:

- minimalna (a po potrebi i maksimalna) dužina lozinke,
- zahtevana snaga lozinke (upotreba malih i velikih slova, brojeva i specijalnih karaktera),
- maksimalni period do izmene lozinke,
- period u kojem korisnik ne može prilikom izmene uneti lozinku koju je već koristio itd.

Primena navedenih ograničenja može se tehnički kontrolisati, ali postoje i mere bezbednosti koje se ne mogu kontrolisati i za koje službenici moraju imati svest da treba da ih primenjuju (na primer, da ne koriste istu lozinku za pristup službenom nalogu i privatnom nalogu na internetu).

Korišćenje multifaktorske autentifikacije

Još bezbedniji način za kontrolu pristupa sistemu ili prostoru je upotreba multifaktorske autentifikacije. Kod ovakvog koncepta potrebno je sistemu pružiti dokaze iz više skupova faktora na osnovu kojih će sistem utvrditi da je službenik koji želi da ostvari pristup zaista onaj za kojeg se predstavlja korisničkim imenom.

Faktori mogu pripadati nekom od sledećih skupova:

- šta znam (lozinke, PIN-ovi i drugo se može zapamtiti),
- šta imam (pametna kartica, token, mobilni telefon i drugo što se može posedovati) i
- šta jesam (biometrijske karakteristike osobe kao što su otisak prsta, sken lica, određeni pokret, glas i slično).

Kod multifaktorske autentifikacije dokazi se mogu pružiti iz dva ili tri skupa faktora (pa shodno tome postoje dvofaktorska i trofaktorska autentifikacija), ali nije dozvoljeno koristiti dva ili više dokaza samo iz istog skupa (na primer, ne smatra se bezbednim ako se u procesu autentifikacije traži samo unos lozinke i PIN-a).

Odgovornost i priprema službenika

Prvu liniju odbrane svake jedinice lokalne samouprave drže njeni službenici. Službenici su najčešće i meta prve faze napada tokom koje napadači nastoje da instaliraju malver u IKT sistem organizacije ili da dobiju informacije koje će omogućiti nastavak i proširenje napada na tu organizaciju.

Kako bi se smanjile mogućnosti za nastanak bezbednosnog incidenta i povećale sposobnosti da se na njega pravovremeno i adekvatno reaguje, službenici u jedinicama lokalnih samouprava moraju redovno sprovoditi osnovne mere zaštite, znati da prepoznaju kada dođe do incidenta i znati kako da postupaju nakon toga. Mere zaštite IKT sistema propisane Zakonom o informacionoj bezbednosti odnose se, između ostalog, i na:

- uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema,
- obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost,
- identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu,
- utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentifikaciju.

Zbog toga je važno da svaka jedinica lokalne samouprave, ma koliko bila mala ili velika, pripremi plan za reagovanje u slučaju incidenata, obuči svoje zaposlene i redovno im podiže bezbednosnu svest.

Od svakog službenika se očekuje da na svaki problem koji primeti obrati dužnu pažnju i preduzme razumne mere radi otklanjanja problema koji bi mogli imati negativan uticaj ako se ne otklone blagovremeno i na odgovarajući način. Od službenika se takođe očekuje da pokažu dužnu marljivost u otkrivanju uzroka problema i preduzimanja svih potrebnih aktivnosti kako bi se slični problemi sprečili u budućnosti.

Ključnu ulogu u pripremi službenika imaju obuke i radionice za podizanje bezbednosne svesti. Ove aktivnosti nemaju veliki efekat ako se sprovedu samo jednom, već moraju biti organizovane kao kontinuiran proces. Obuke i radionice moraju biti obavezne za službenike i obuhvatiti sve koji imaju pristup IKT sistemu. Jedino takvom organizacijom će se znanje i spremnost službenika obnavljati i unapređivati na sistemski način.

Odgovornost rukovodilaca i odgovornih lica

Rukovodioci i odgovorna lica[52] imaju obavezu da primenjuju sve propisane bezbednosne mere kao i svi ostali službenici, ali njihova odgovornost je veća jer će zaposleni slediti njihov primer i revnost – ako oni ne primenjuje propisane bezbednosne mere, ni ostali službenici neće to smatrati neophodnim već samo kao jednu od mnogih obaveza. Ako dođe do bezbednosnog incidenta radnici će od rukovodioca tražiti mišljenje, savet i odluku u situaciji kada je potrebno brzo donositi odluke i delovati smireno. Jedinica lokalne samouprave može imati velike posledice ako u toj situaciji rukovodilac ne može da ostvari dobru komunikaciju sa svojim radnicima i nema pravo rešenje zbog svog lošeg odnosa prema bezbednosnim merama i neadekvatne pripremljenosti za krizne situacije.

52 Rukovodilac i odgovorno lice mogu biti ista osoba

Zakon o informacionoj bezbednosti propisuje i kaznene odredbe prema jedinicama lokalne samouprave i odgovornim licima u njima i to u sledećim slučajevima:

- ako se ne izvrši upis u evidenciju IKT sistema od posebnog značaja u predviđenom roku,
- ako se ne donese Akt o bezbednosti IKT sistema,
- ako se ne primene mere zaštite određene Aktom o bezbednosti IKT sistema,
- ako se ne izvrši provera usklađenosti primenjenih mera zaštite određenih Aktom o bezbednosti IKT sistema,
- ako se ne dostave statistički podaci o incidentima,
- ako se ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku,
- ako se ne dostavi obaveštenje o incidentu u IKT sistemu,
- ako se ne dostavljaju obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta,
- ako se ne dostavi završni izveštaj o incidentu u predviđenom roku.

Zadaci i nadležnost tehničkih lica

U svakoj organizaciji tehnička lica su uključena u procese zaštite IKT sistema i informacija koje se u njemu nalaze. U slučaju bezbednosnog incidenta u IKT sistemu, tehnička lica su prva koja će zaposleni kontaktirati kako bi se problem rešio. Njihov zadatak u tom slučaju je da sagledaju pravo stanje stvari i odmah reaguju sa primenom osnovnih mera radi sprečavanja daljeg širenja incidenta.[53] Istovremeno, treba da procene razmere i vrstu incidenta i o incidentu obaveste koga treba, ako je potrebno.

Ne mogu se sva tehnička lica smatrati ekspertima za sajber bezbednost i u većini slučajeva ona to i nisu, ali sva tehnička lica u svom poslu moraju redovno primenjivati bezbednosne mere, kao i ostali službenici. Time oni štite sistem, ali i daju primer drugima kako treba da razmišljaju i rade.

53 Aktivnosti koje mogu sprovesti tehnička lica u takvim situacijama su izolacija uređaja obuhvaćenih incidentom, izrada njihovih sistemskih kopija radi kasnije analize, njihova reinstalacija sa prethodno urađenih bezbednih sistemskih kopija i slično.

Bezbednosni plan (Plan reagovanja na incidente)

Jedna od mera zaštite propisana Zakonom o informacionoj bezbednosti je prevencija i reagovanje na bezbednosne incidente. Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema propisuje sledeće obaveze jedinici lokalne samouprave po pitanju ove mere:

- utvrđivanje procedura kojima se definišu odgovorna lica zadužena za prevenciju i reagovanje, plan postupanja u slučaju opasnosti od nastanka bezbednosnih incidenata ili nastanka bezbednosnih incidenata, obavezu vođenja evidencije o preduzetim aktivnostima, obavezu izveštavanja i razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama,
- obavezivanje svih zaposlenih i pružalaca usluga da odgovornom licu zaduženom za prevenciju i reagovanje bez odlaganja prijavljuju bezbednosne slabosti, pretnje i incidente u IKT sistemu,
- određivanje odgovornog lica za obaveštavanje nadležnih organa o incidentima u IKT sistemu koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti,
- definisanje i primena procedura koje treba da obezbede procese za identifikaciju, prikupljanje i čuvanje informacija koje mogu da posluže kao dokaz radi pokretanja disciplinskog, prekršajnog ili krivičnog postupka.

Model Akta o bezbednosti IKT sistema koji je pripremio Nacionalni CERT predlaže usvajanje sledećih procedura:

- procedura za pripremu i planiranje odgovora na incidente,
- procedura za nadgledanje, detekciju, analizu i izveštavanje o događajima i incidentima u vezi sa bezbednošću informacija,
- procedura za zapisivanje aktivnosti u okviru upravljanja incidentima,
- procedura za postupanje sa sudskim dokazima,
- procedura za ocenjivanje i odlučivanje o događajima u okviru bezbednosti informacija i ocenjivanje slabosti u pogledu bezbednosti informacija,
- procedura za odgovaranje na incidente, oporavak od incidenta i komunikaciju sa eksternim ili internim osobama ili organizacijama.

Sve navedeno može biti uključeno u jedinstven bezbednosni plan. Ovaj plan mora biti odobren od strane rukovodioca jedinice lokalne samouprave i redovno, a po potrebi i vanredno proveravan i unapređivan. Zaposleni u jedinici lokalne samouprave moraju biti upoznati sa ovim planom i moraju se organizovati redovne vežbe kako bi svaki službenik znao svoje dužnosti i odgovornosti. Često se dešava da prilikom reagovanja na bezbednosne incidente nastupe situacije mimo okvira bezbednosnog plana, pa se u tim slučajevima moraju brzo donositi i sprovoditi odluke uz preciznu komunikaciju svih koji su uključeni u proces reagovanja.

Praksa pokazuje da u slučajevima bezbednosnih incidenata planiranje, kreiranje svesti o rizicima i potrebnim postupcima i uvežbavanje imaju krucijalnu važnost za saradnju zaposlenih i uspešno reagovanje na situacije koje bezbednosni plan ne predviđa.

U vezi sa bezbednosnim planom potrebno je pomenuti i mere zaštite koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima i koje u skladu sa Zakonom o informacionoj bezbednosti treba da budu definisane u Aktu o bezbednosti IKT sistema. Ove mere se odnose na pripremu i postupanje u vanrednim situacijama kao što su zemljotresi, požari, velike havarije i slično, ali i uspešni sajber napadi koji imaju uticaj na podatke u IKT sistemu jedinice lokalne samouprave u meri da ti podaci više nisu dostupni, upotrebljivi ili pouzdani. Neke od mera kojima se obezbeđuje kontinuitet poslovanja su:

- izrada Plana za obezbeđenje kontinuiteta poslovanja i Plana oporavka od neželjenih događaja,
- određivanje odgovornih lica,
- uspostavljanje rezervnih lokacija za rad,
- obezbeđenje rezervnih komunikacija i napajanja,
- nabavka i priprema rezervnih uređaja,
- priprema kopija potrebne dokumentacije u vezi IKT sistema,
- izrada i čuvanje sistemskih kopija,
- izrade i čuvanje rezervnih kopija podataka,
- definisanje procedure za instalaciju i konfigurisanje uređaja i servisa itd.

Samoprocena spremnosti

U Prilogu 4 je dat upitnik koji služi za samostalnu procenu ispunjenosti zakonskih obaveza i spremnosti za upravljanje incidentima u IKT sistemu.[54] Upitnik služi i kao podsetnik na obaveze koje lokalna samouprava ima, ali može i dati smernice za planiranje najnužnijih aktivnosti za zaštitu IKT sistema.

Upitnik je namenjen internoj upotrebi u jedinici lokalne samouprave. Popunjeni upitnici ne smeju se objavljivati i deliti sa licima van jedinice lokalne samouprave.

54 Napomena: ovaj upitnik nije u vezi sa obrascem za samoprocenu IKT sistema od posebnog značaja čija je izrada predviđena Strategijom razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine

Reagovanje u slučaju incidenta

Identifikacija incidenta

Neke incidente je jednostavno primetiti, kao na primer DDoS napad tokom kojeg se ne može pristupiti internet stranici ili ransomver napad kada se na ekranu pojavi poruka kojom napadači obaveštavaju žrtvu da su fajlovi šifrovani i da će ključ za dešifrovanje poslati nakon uplate otkupa. Druge napade je veoma teško primetiti, kao na primer delovanje APT grupa[55] koje raspolažu značajnim znanjem i resursima, a čiji je cilj da što duže ostanu neprimećeni u napadnutom sistemu i preuzimaju informacije iz njega.

Službenici mogu posumnjati da je bezbednosni incident u toku ako se na njihovom uređaju dešava nešto od sledećeg:

- nemogućnost pristupa uređaju ili podacima na njemu,
- neočekivano gašenje ili blokiranje uređaja,
- usporen rad uređaja,
- isključivanje programa za zaštitu (anti-malver programa i sličnih),
- smanjenje slobodnog memorijskog prostora,
- porast količine saobraćaja ka internetu,
- učestalo pojavljivanje reklamnih poruka,
- izmene u konfiguraciji pretraživača itd.

Navedeni indikatori nisu siguran znak da je zaista u pitanju bezbednosni incident, ali svakako treba da podstaknu službenika da ih ispita i potraži pomoć stručne osobe u slučaju potrebe.

Reagovanje nakon uočenog incidenta

Po utvrđivanju da je incident u toku treba odmah krenuti sa postupcima kojima će se zaustaviti njegovo dalje širenje i ograničiti šteta. Osnovno pravilo za reagovanje na incidente, posebno u prvim trenucima nakon saznanja da se nešto loše dešava u sistemu, jeste da se ne sme paničiti jer je tada neophodno da se razmisli i donesu ispravne odluke za kratko vreme. U tim situacijama mnogo pomaže napisan i uvežban bezbednosni plan, jer daje jasne smernice službenicima kako da reaguju i svoje zadatke obave na efikasan način, čime će se stvoriti uslovi da se funkcionisanje vrati u normalan tok za najkraće moguće vreme.

Reagovanje na incident ne sme da bude sporo i konfuzno, jer može da dovede do širenja incidenta i veće štete, ali ne sme da bude ni prebrzo i panično (na primer, neselektivno isključivanje napajanja svim uređajima, neselektivno brisanje fajlova sa diskova ili instaliranje neproverenih programa za zaštitu sistema ili vraćanje podataka). Komunikacija i koordinacija mora da postoji u slučaju incidenta i korisnici IKT sistema ne smeju samostalno donositi i sprovoditi odluke bez konsultacija sa odgovornim i stručnim licima nadležnim za reagovanje na incident.

55 Napredne trajne pretnje (engl. „Advanced Persistent Threat“ – APT). Objašnjenje je dato ranije u tekstu.

Treba voditi računa i o izboru sredstva za komunikaciju u slučaju bezbednosnog incidenta, jer neki od ustaljenih načina komunikacije (na primer, poruke elektronske pošte) mogu biti kompromitovani i praćeni od strane napadača.

Prijava incidenta

Veoma je bitno da nakon uočenog incidenta brzo bude obavešteno odgovorno lice za prevenciju i reagovanje, koje od tog trenutka koordinira realizaciju svih predviđenih aktivnosti u skladu sa usvojenim planom.

U tekstu je već objašnjeno da su jedinice lokalne samouprave u obavezi da određene bezbednosne incidente u svojim IKT sistemima prijavljuju Nadležnom organu ili Nacionalnom CERT-u i način na koji se ove prijave dostavljaju. Takođe, navedena je i obaveza dostavljanja obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta.

Mogućnosti za podršku i pomoć

Po prijemu prijave incidenta, Nacionalni CERT u skladu sa svojim nadležnostima prikuplja, analizira i razmenjuje informacije o incidentu, nakon čega stupa u kontakt sa jedinicom lokalne samouprave u kojoj se desio incident i, po potrebi, priprema predlog preporuka za postupanje. U slučaju incidenata nivoa opasnosti „visok“ i „veoma visok“, koordinacija reagovanja na incident vrši se u saradnji sa Nadležnim organom i drugim organima.

Jedinica lokalne samouprave može angažovati treća lica za pomoć u rešavanju incidenta ako nema dovoljno internih kapaciteta da samostalno reši incident. Ova pomoć može uključivati konsultacije o načinima za rešavanje incidenta, ili daljinsko povezivanje ili izlazak stručnih osoba na lice mesta radi neposrednog rešavanja incidenta.

Najčešće se pomoć traži od drugih organizacija sa kojima jedinica lokalne samouprave već ima ugovorenu ili je u prošlosti imala uspešnu saradnju, a pre svih od onih koji su jedinici lokalne samouprave isporučili opremu za zaštitu IKT sistema ili uređaje koji su napadnuti. Ako ni te organizacije ne mogu da reše incident, potrebne usluge mogu pružiti Posebni CERT-ovi registrovani kod Nacionalnog CERT-a i druge specijalizovane kompanije koje se bave zaštitom IKT sistema.

Odluke se svakako moraju doneti brzo jer postoji mogućnost da neke posledice ne mogu da se otklone ako prođe dovoljno dugo vremena.

Saradnja sa nadležnim organima

U Krivičnom zakoniku Republike Srbije[56] postoji posebna glava koja se odnosi na krivična dela u oblasti bezbednosti računarskih podataka. U krivična dela koja pripadaju ovoj oblasti spadaju:

- Oštećenje računarskih podataka i programa
- Računarska sabotaža
- Pravljenje i unošenje računarskih virusa
- Računarska prevara
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka
- Sprečavanje i organičavanje pristupa javnoj računarskoj mreži
- Neovlašćeno korišćenje računara ili računarske mreže
- Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka

Pored navedenog, krivična dela koja spadaju u visokotehnološki kriminal mogu se odnositi i na druge oblasti kao što su sloboda i prava čoveka i građanina, polne slobode, javni red i mir, ustavno uređenje i bezbednost Republike Srbije, intelektualna svojina, imovina, privreda i pravni saobraćaj, ako se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, ili ako se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.

U slučaju da se bezbednosni incident može kvalifikovati kao krivično delo, potrebno je podneti prijavu u policijskoj stanici, Odeljenju za suzbijanje visokotehnološkog kriminala MUP-a ili Posebnom tužilaštvu za viokotehnloški kriminal.[57]

Analiza nakon sajber incidenta

Nakon što je incident završen, veoma je bitno napraviti analizu kako se dogodio incident, kako je uticao na poslovanje jedinice lokalne samouprave i kakve je posledice ostavio, šta je bilo dobro, a šta loše tokom reagovanja na incident i kakva poboljšanja treba napraviti. Ova analiza treba da pokaže i da li je potrebno menjati proceduru reagovanja na incidente i bezbednosni plan. Najčešće se ovakva analiza radi na posebnom sastanku kojem prisustvuju oni koji su bili uključeni u rešavanje incidenta.

Procedurama je potrebno predvideti ko saziva i ko prisustvuje ovakvom sastanku. Najlogičnije rešenje je da obavezu sazivanja sastanka im odgovorno lice za prevenciju i reagovanje, ali dobro rešenje je i da ovu obavezu ima rukovodilac organa. Sastanak treba sazvati u roku od najkasnije nekoliko dana od prestanka incidenta, a praksa je da sastanku prisustvuju lica koja su učestvovala u rešavanju incidenta i, u slučaju potrebe, i druga lica.

56 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg
57 https://www.beograd.vtk.jt.rs/lt/default.html

Prilog 1: Lista incidenata prema vrstama

LISTA INCIDENATA PREMA VRSTAMA	
Grupa incidenata	Vrsta incidenta
Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl. „malware")	Virus
	Crv (engl. „worm")
	Ransomver (engl. „ransomware")
	Trojanac
	Špijunski softver (engl. „spyware")
	Rutkit (engl. „rootkit")
Neovlašćeno prikupljanje podataka	Skeniranje portova
	Presretanje podataka između računara i servera (engl. „sniffing")
	Socijalni inženjering (lažno predstavljanje i drugi oblici)
	Kompromitovanje ili curenje podataka (engl. „data breaches")
Prevara	Fišing (engl. „phishing")
	Neovlašćeno korišćenje resursa (engl. „cryptojacking" i drugi oblici)
Pokušaji upada u IKT sistem	Pokušaj iskorišćavanja ranjivosti sistema
	Pokušaj otkrivanja kredencijala (engl. „brute force attack", „dictionary attack" i sl)
Upad u IKT sistem	Otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl. „privileged account compromise")
	Otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl. „unprivileged account compromise")

Upad u IKT sistem	Neovlašćeni pristup aplikaciji
	Mreža zaraženih uređaja (engl. „botnet")
Nedostupnost ili ograničena dostupnost IKT sistema	Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. „denial-of-service attack" – DoS)
	Distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. „distributed denial-of-service attack" – DDoS)
	Sabotaža
	Prekid u funkcionisanju sistema ili dela sistema (engl. „outage")
Ugrožavanje bezbednosti podataka	Neovlašćen pristup podacima
	Neovlašćena izmena ili brisanje podataka
	Kriptografski napad
Operativni incidenti	Otkazivanje hardverskih komponenti
	Problemi u radu sa softverskim komponentama
Incidenti fizičko-tehničke bezbednosti	Krađa hardverskih komponenti
	Požar
	Poplava
Ostali incidenti	Incidenti koji ne spadaju u gore navedene kategorije

Prilog 2: Klasifikacija incidenta prema nivou opasnosti

KLASIFIKACIJA INCIDENTA PREMA NIVOU OPASNOSTI	
Nivo opasnosti	Posledice incidenta
Veoma visok	U slučaju nastupanja okolnosti ugrožavanja, ometanja rada ili onemogućavanja rada IKT sistema od posebnog značaja, a kada su rizici, pretnje ili nastale posledice incidenta po stanovništvo, materijalna dobra ili životnu sredinu takvog obima i intenziteta da njihov nastanak ili posledice nije moguće sprečiti ili otkloniti redovnim delovanjem nadležnih organa i službi, zbog čega je za njihovo ublažavanje i otklanjanje neophodno upotrebiti posebne mere, dodatne snage i sredstva uz pojačan režim rada.
Visok	Kada su rizici i pretnje ili nastale posledice incidenta po stanovništvo, materijalna dobra ili životnu sredinu takvog obima i intenziteta da je njihov nastanak ili posledice moguće sprečiti ili otkloniti redovnim delovanjem nadležnih organa i službi.
Srednji	Kada su rizici, pretnje ili nastale posledice incidenta takvog obima i intenziteta da mogu biti otklonjena zajedničkim delovanjem IKT sistema od posebnog značaja u kome se incident desio i Nacionalnog CERT-a.
Nizak	Kada su rizici, pretnje ili nastale posledice incidenta takvog obima i intenziteta da mogu biti otklonjene delovanjem IKT sistema od posebnog značaja.

Prilog 3: Obrazac ISP

IZVEŠTAJ O STATISTIČKIM PODACIMA O SVIM INCIDENTIMA U IKT SISTEMIMA OD POSEBNOG ZNAČAJA

PODACI O OPERATORU IKT SISTEMA OD POSEBNOG ZNAČAJA

Puno poslovno ime operatora	
Sedište operatora	
Matični broj operatora	
Adresa internet stranice operatora	
Ukupan broj IP uređaja*	

* upisati ukupan broj svih uređaja koji koriste IP protokol za komunikaciju, a koji su u mreži operatora IKT sistema od posebnog značaja

PREGLED INCIDENATA PREMA VRSTAMA

Grupa incidenata	Vrsta incidenta	Broj incidenata
Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl.„malware“)	virus	
	crv (engl.„worm“)	
	ransomver (engl.„ransomware“)	
	trojanac	
	špijunski softver (engl.„spyware“)	
	rutkit (engl.„rootkit“)	
Neovlašćeno prikupljanje podataka	skeniranje portova	
	presretanje podataka između računara i servera (engl.„sniffing“)	
	socijalni inženjering (lažno predstavljanje i drugi oblici)	
	kompromitovanje ili curenje podataka (engl.„data breaches“)	
Prevara	fišing (engl.„phishing“)	
	neovlašćeno korišćenje resursa (engl.„cryptojacking“) i drugi oblici	
Pokušaj upada u IKT sistem	pokušaj iskorišćavanja ranjivosti sistema	
	pokušaj otkrivanja kredencijala (engl.„brute force attack“, „dictionary attack“ i sl.)	
Upad u IKT sistem	otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl.„privileged account compromise“)	
	otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl.„unprivileged account compromise“)	
	neovlašćeni pristup aplikaciji	
	mreža zaraženih uređaja (engl.„botnet“)	

Nedostupnost ili ograničena dostupnost IKT sistema	napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl.„denial-of-service attack“- DoS)	
	distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl.„distributed denial-of-service attack“- DDoS)	
	sabotaža	
	prekid u funkcionisanju sistema ili dela sistema (engl.„outage“)	
Ugrožavanje bezbednosti podataka	neovlašćen pristup podacima	
	neovlašćena izmena ili brisanje podataka	
	kriptografski napad	
Operativni incidenti	otkazivanje hardverskih komponenti	
	problemi u radu sa softverskim komponentama	
Incidenti fizičko-tehničke bezbednosti	krađa hardverskih komponenti	
	požar	
	poplava	
Ostali incidenti	incidenti koji ne spadaju u gore navedene kategorije	

Prilog 4: Samoprocena spremnosti

* NAPOMENA: Popunjen upitnik ne objavljivati i ne deliti sa licima van jedinice lokalne samouprave!

Da li je IKT sistem prijavljen kod nadležnog organa?

- ☐ Ne, jer još uvek ne postoje svi elementi
- ☐ Ne, ali sve je pripremljeno i samo treba poslati prijavu
- ☐ Da

Da li je određeno odgovorno lice za IKT sistem?

- ☐ Ne
- ☐ Da

Da li je određen administrator IKT sistema?

- ☐ Ne
- ☐ Da

Da li je izrađen Akt o bezbednosti IKT sistema?

- ☐ Ne
- ☐ Da, ali nije odobren od strane rukovodioca
- ☐ Da

Da li su odredbe Akta o bezbednosti IKT sistema proverene od strane nezavisnog stručnjaka izvan organizacije?

- ☐ Ne
- ☐ Stručnjaci izvan organizacije su konsultovani oko pojedinih odredbi tokom pisanja Akta
- ☐ Da, urađena je verifikacija ili je Akt izrađen od strane nezavisnog stručnjaka izvan organizacije

Ako je IKT sistem poveren trećim licima ili ga održavaju treća lica, da li su definisane mere bezbednosti? (na ovo pitanje ne treba odgovarati ako jedinica lokalne samouprave samostalno upravlja IKT sistemom)

- ☐ Ne, u ugovoru nisu definisane mere bezbednosti
- ☐ Da, u ugovoru su definisane mere bezbednosti ali ne postoji definisan način provere ili se provera ne vrši
- ☐ Da, u ugovoru su definisane mere bezbednosti i način provere koja se vrši redovno

Da li se vrši redovna provera bezbednosti IKT sistema?

- ☐ Ne
- ☐ Provera se vrši po potrebi, a ne u skladu sa rokovima propisanim Aktom o bezbednosti IKT sistema
- ☐ Da, određena je nadležna osoba, provera se vrši u skladu sa rokovima propisanim Aktom o bezbednosti IKT sistema i izrađuje se izveštaj koji se dostavlja rukovodiocu

Da li se mere informacione bezbednosti primenjuju u svim fazama projekata koji se pokreću u jedinici lokalne samouprave?

- ☐ Ne, nego se u nekoj fazi realizacije projekta sagledava šta može biti primenjeno od raspoloživih mera
- ☐ Da, ali se razmatra samo primena mera koje su na raspolaganju bez dodatnih investicija
- ☐ Da, uključujući specifičnosti projekta koje zahtevaju dodatne mere bezbednosti

Da li postoji procena rizika po bezbednost IKT sistema?

- ☐ Ne
- ☐ Da, ali je rađena pre više od godinu dana
- ☐ Da

Da li se sprovode mere za prevenciju od rizika po bezbednost IKT sistema?

- ☐ Ne
- ☐ Da, ali mere se sprovode samo kada se utvrdi ili dobije informacija o riziku (ad-hoc)
- ☐ Da, mere se sprovode sistemski na osnovu redovno rađenih procena rizika

Da li postoji plan izrade rezervnih kopija i da li se redovno izrađuju rezervne kopije?

- ☐ Ne
- ☐ Ne postoji odobren plan izrade rezervnih kopija, ali zaposleni koji su nadležni za IKT sistem rade rezervne kopije u skladu sa svojim znanjem i najboljim mogućnostima
- ☐ Plan izrade rezervnih kopija postoji ali se ne sprovodi ili se sprovodi parcijalno
- ☐ Rezervne kopije se izrađuju redovno prema odobrenom planu

Da li postoji i primenjuje se politika lozinki?

- ☐ Ne postoji propisana politika lozinki, nego svaki službenik postupa u skladu sa svojom savešću
- ☐ Postoji propisana politika lozinki u jedinici lokalne samouprave, ali nije implementirana u IKT sistem ili je delimično implementirana
- ☐ Politika lozinki je propisana i sistemski implementirana

Da li se u jedinici lokalne samouprave primenjuje zaštita ličnih podataka?

- ☐ Ne, ličnim podacima skladištenim u IKT sistemu mogu pristupiti svi koji imaju pristup IKT sistemu
- ☐ Da, ali službenici nisu upoznati sa odredbama Zakona o zaštiti ličnih podataka
- ☐ Da, podaci su u IKT sistemu zaštićeni u skladu sa propisima i zaposleni su upoznati sa odredbama Zakona o zaštiti ličnih podataka

Da li u jedinici lokalne samouprave postoji razrađen sistem zaštite tajnih podataka u IKT sistemu?

- ☐ Ne, tajni podaci se obrađuju samo u papirnom obliku
- ☐ Tajni podaci se čuvaju u IKT sistemu, ali primenjene mere zaštite nisu u skladu sa Zakonom o tajnosti podataka
- ☐ Da, tajni podaci se čuvaju u IKT sistemu sa primenjenim merama zaštite u skladu sa Zakonom o tajnosti podataka

Da li u jedinici lokalne samouprave postoji razrađen sistem čuvanja bezbednosnih zapisa (logova)?

- ☐ Ne, bezbednosni zapisi ostaju sačuvani na uređajima koji su ih generisali
- ☐ Da, bezbednosni zapisi se čuvaju centralizovano

Da li je određeno odgovorno lice za prevenciju i reagovanje u slučaju incidenata?

- ☐ Ne
- ☐ Odgovorno lice je formalno određeno, ali službenici nisu upoznati
- ☐ Da, i službenici su upoznati kome treba da prijave incident

Da li postoji organizovano praćenje stanja u IKT sistemu u cilju brzog otkrivanja incidenta?

- ☐ Ne
- ☐ Postoje odgovarajući resursi (uređaji i aplikacije), ali ne postoje obučeni radnici koji bi mogli na zadovoljavajući način da ih koriste
- ☐ Postoje obučeni radnici ali ne postoje odgovarajući resursi ili nisu upotrebljivi (istekle licence, zastareli uređaji i slično)
- ☐ Za ove aktivnosti angažovana su treća lica
- ☐ Da, postoje odgovarajući resursi i obučeni radnici

Da li je utvrđen plan (ili procedura) za postupanje u slučaju opasnosti od nastanka bezbednosnih incidenata ili nastanka bezbednosnih incidenata (bezbednosni plan)?

- ☐ Ne
- ☐ Plan je pripremljen ali nije odobren
- ☐ Da, ali službenici nisu upoznati sa planom
- ☐ Da, službenici su upoznati sa planom ali nikad nije sprovedena vežba
- ☐ Da, službenici su upoznati sa planom i vežbe se sprovode redovno

Da li je određeno odgovorno lice za obaveštavanje nadležnih organa o incidentima u IKT sistemu?

- ☐ Ne
- ☐ Da

Da li je definisana procedura za identifikaciju, prikupljanje i čuvanje informacija koje mogu da posluže kao dokaz radi pokretanja disciplinskog, prekršajnog ili krivičnog postupka?

- ☐ Ne
- ☐ Da, ali se ne primenjuje
- ☐ Da, i primenjuje se prilikom incidenata

Da li se sprovode obuke zaposlenih u oblasti informacione bezbednosti i radionice za podizanje bezbednosne svesti?

- ☐ Ne
- ☐ Povremeno se organizuju ali njima nisu obuhvaćeni svi zaposleni u jedinici lokalne samouprave niti postoji plan organizacije
- ☐ Da, redovno se organizuju u skladu sa planom

Da li službenici prijavljuju bezbednosne incidente odgovornom licu u jedinici lokalne samouprave?

- ☐ Ne, jer prijavljivanje bezbednosnih incidenata nije organizovano u jedinici lokalne samouprave
- ☐ Postoji definisana procedura i određeno je odgovorno lice, ali praksa nije uspostavljena
- ☐ Praksa prijavljivanja incidenata je uspostavljena, ali poznati su slučajevi da službenici nisu prijavili incidente
- ☐ Nisu poznati slučajevi da službenici nisu prijavili incidente

Da li se organizuju stručne obuke u oblasti informacione bezbednosti za tehnička lica?

- ☐ Ne
- ☐ Tehnička lica se povremeno upućuju na ponuđene obuke, ali ne postoje zahtevi po ovom pitanju niti plan realizacije
- ☐ Da, tehnička lica se redovno upućuju na obuke u skladu sa planom

Da li se organizuju stručne obuke za tehnička lica za teme od interesa za jedinicu lokalne samouprave (van oblasti informacione bezbednosti)?

- ☐ Ne
- ☐ Tehnička lica se povremeno upućuju na ponuđene obuke, ali ne postoje zahtevi po ovom pitanju niti plan realizacije
- ☐ Da, tehnička lica se redovno upućuju na obuke u skladu sa planom