British Embassy Belgrade

UK International Development
Partnership | Progress | Prosperity

TAG International
Securing lives and livelihoods

NALED

Smernice za informacionu bezbednost za mala i srednja preduzeća u Srbiji

Smernice za informacionu bezbednost za mala i srednja preduzeća u Srbiji

Sadržaj

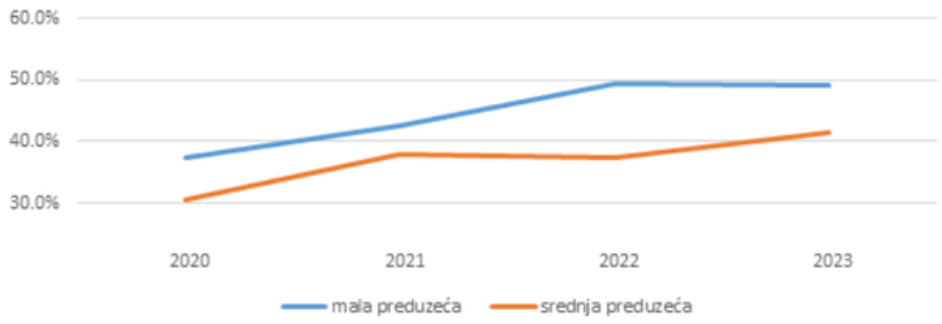
Uvod

Mala i srednja preduzeća, kako na globalnom nivou tako i u Srbiji, su daleko najbrojniji vid poslovnih subjekata. Prema dostupnim podacima mala i srednja preduzeća čine gotovo 99,5% srpske privrede i učestvuju sa gotovo 60% u ukupnom prometu i sa preko 51% u ukupnoj bruto dodatoj vrednosti u Srbiji.[1]

Kriterijume za razvrstavanje pravnih lica i preduzetnika propisuje Zakon o računovodstvu, ali u ovu kategoriju mogu spadati, na primer, i male radnje sa nekoliko zaposlenih i fabrike sa par stotina radnika, a i poslovni prihodi po zaposlenom u preduzećima koja spadaju u ovu kategoriju mogu biti veoma različiti.

> Promene koje je doneo razvoj informacionih i komunikacionih tehnologija poslednjih godina i decenija nije zaobišao ni mala i srednja preduzeća bez obzira kojom delatnošću se bave. U publikaciji Republičkog zavoda za statistiku „Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji" objavljeni su statistički podaci značajni za sagledavanje trenutne situacije po pitanju upotrebe informaciono-komunikacionih tehnologija u malim i srednjim preduzećima.[2]

Pregledom podataka može se utvrditi da je upotreba informaciono-komunikacionih tehnologija u stalnom porastu. U poslednjih nekoliko godina značajno je porastao procenat zaposlenih koji upotrebljavaju internet u poslovne svrhe, kako u malim tako i u srednjim preduzećima.



Slika 1: Procenat preduzeća u kojima internet za poslovne potrebe koristi više od 75% zaposlenih

1 Publikacija „Preduzeća u Republici Srbiji, prema veličini 2023" Republičkog zavoda za statistiku Srbije
2 Publikacija „Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji" objavljuje se jednom godišnje. U trenutku pisanja ovih Smernica poslednja objavljena publikacija bila je iz 2023. godine, ali upitnikom nisu obuhvaćena pitanja iz oblasti IKT bezbednosti pa su iz tog razloga za ovu oblast korišćeni statistički podaci iz publikacije za prethodnu godinu.

Veliki procenat malih i srednjih preduzeća koristi internet (veb) sajtove u svom poslovanju. 82,4% malih i 94,2% srednjih preduzeća poseduje veb sajt, a preko njega pružaju sledeće usluge:

	Mala preduzeća	Srednja preduzeća
Opis robe ili usluga, cenovnik	86,9%	84,7%
Onlajn naručivanje	18,5%	19,3%
Detaljnije informacije o proizvodima	55,2%	59,7%
Praćenje ili status porudžbina	10,0%	11,1%
Sadržaj prilagođen redovnim posetiocima	62,0%	67,6%
Usluga korisničke podrške	11,7%	12,4%
Oglašavanje otvorenih radnih mesta ili onlajn prijava za posao	14,3%	18,7%
Sadržaj dostupan na najmanje dva jezika	48,0%	51,5%

Tabela 1: Pružanje usluga putem veb sajta

Mala i srednja preduzeća u sve većoj meri koriste i društvene mreže kao podršku poslovanju, i to:

	Mala preduzeća	Srednja preduzeća
Društvene mreže (Meta, Linkedin, Xing, Yammer)	51,3%	59,4%
Blog (Twitter/X)	8,2%	12,1%
Multimedijalni sajtovi za razmenu sadržaja (Youtube, Flickr, Picassa)	13,4%	22,7%

Tabela 2: Korišćenje društvenih mreža

Analizu podataka primenjuje 18,1% malih i 39,4% srednjih preduzeća, a upotreba klauda u različite svrhe je zastupljena u značajnoj meri:

	Mala preduzeća	Srednja preduzeća
Mejl (elektronska pošta)	80,9%	80,9%
Office paket	50,6%	64,5%
Softverske aplikacije za finansije ili računovodstvo	38,3%	48,7%
Bezbednosne softverske aplikacije (anti-virus, kontrola mrežnog pristupa i slično	33,8%	47,4%
Hosting baze podataka preduzeća	51,6%	46,6%
Skladištenje fajlova	41,8%	48,2%
Računari za pokretanje softvera koji koristi preduzeće	13,9%	18,4%

Tabela 3: Korišćenje klaud servisa

Zabeležena je i primena tehnologije veštačke inteligencije, i to kod 1,8% malih i kod 2,4% srednjih preduzeća.

Po pitanjima stručne radne snage u oblasti informaciono-komunikacionih tehnologija, 18,3% malih i 40,6% srednjih preduzeća zapošljava stručnjake u oblasti IKT. U 2021. godini 4,9% mailh i 14,9% srednjih preduzeća imalo je potrebu za zapošljavanjem IKT stručnjaka, ali u 49,9% slučajeva kod malih i u 59,1% slučajeva kod srednjih preduzeća suočili su se sa teškoćama da nađu adekvatnu radnu snagu.

U takvim okolnostima, u 32,8% malih preduzeća održavanje IKT infrastrukture, podršku za Office softver, razvoj ili podršku za softver za upravljanje poslovanjem i druge poslove vezane za informaciono-komunikacione tehnologije obavlja neko od zaposlenih (većina od njih ima i druga zaduženja, a ove poslove obavlja kao dodatnu obavezu), dok 67,1% malih preduzeća za takve poslove angažuje treća lica (eksterne dobavljače). Kod 51,2% srednjih preduzeća poslove vezane za IKT obavljaju zaposleni u preduzeću, a 65,7% angažuje treća lica.[3]

Po pitanju obuka u oblasti informaciono-komunikacionih tehnologija, 6,7% malih i 22,8% srednjih preduzeća upućuje svoje IKT stručnjake na obuke iz ove oblasti, dok 15,7% malih i 29,2% srednjih preduzeća na obuke iz informaciono-komunikacionih tehnologija upućuje i ostale zaposlene.

3 Deo preduzeća angažuje i sopstvene zaposlene i treća lica pa je zbog toga zbir veći od 100%.

Kada je reč o bezbednosti IKT sistema može se primetiti da postoji izvesna razlika u angažovanju trećih lica, u smislu da se ona angažuju u nešto manjoj meri. Zaposleni su zaduženi za sprovođenje aktivnosti u vezi sa bezbednošću IKT sistema kod 35,4% malih i kod 50,7% srednjih preduzeća, dok 61,7% malih i 54,9% srednjih preduzeća i za ovu vrstu poslova angažuje treća lica.

U kolikom procentu se pojedine bezbednosne mere primenjuju u malim i srednjim preduzećima prikazano je sledećom tabelom:

	mala preduzeća	srednja preduzeća
Autentifikacija preko jake lozinke	76,3%	88,0%
Autentifikacija putem biometrijskih metoda	3,4%	7,2%
Autentifikacija zasnovana na kombinaciji najmanje dva mehanizma	15,7%	19,8%
Šifrovanje podataka, dokumenata ili mejlova	40,2%	42,2%
Pravljenje rezervne kopije podataka na odvojenoj lokaciji (uključujući klaud)	61,2%	77,8%
Kontrola pristupa mreži (upravljanje korisničkim pravima)	51,4%	72,4%
Korišćenje virtuelne privatne mreže (VPN)	34,2%	55,7%
Korišćenje sistema za nadzor koji otkriva sumnjive aktivnosti u IKT sistemu (ne uključujući anti-virus softver)	23,2%	37,7%
Održavanje fajlova za logovanje koji omogućavaju analizu bezbednosti	20,5%	37,0%
Izrada procene rizika	13,1%	24,8%
Sprovođenje bezbednosnih testova u IKT sistemu	19,5%	30,7%
Bezbednosne smernice za vođenje onlajn sastanaka	55,3%	71,6%
Uputstva za bezbednost za daljinski pristup (zaštita onlajn sastanaka, zabrana korišćenja javnog Wi-Fi, korišćenje VPN, zahtevi koji se odnose na privatnost podataka itd.)	41,5%	49,1%

Tabela 4: Primena mera bezbednosti u IKT sistemima malih i srednjih preduzeća

U 51,8% malih i 63,5% srednjih preduzeća postoje izrađeni dokumenti o merama, praksi ili procedurama o bezbednosti u IKT sistemu. Ažurnost ovih dokumenata predstavljena je sledećom tabelom:

	mala preduzeća	srednja preduzeća
Dokumenti ažurirani u prethodnih 12 meseci	62,4%	70,5%
Dokumenti ažurirani između 12 i 24 meseca	20,8%	17,1%
Dokumenti ažurirani pre više od 24 meseca	16,8%	12,4%

Tabela 5: Ažuriranje dokumenata o merama, praksi ili procedurama o bezbednosti IKT sistema

U većini malih i srednjih preduzeća postoji svest o potrebi za zaštitom IKT sistema i informacija, ali nemaju sva preduzeća mogućnosti da organizuju obuke iz ove oblasti pa zaposleni često moraju sami da nalaze načine za dobijanje potrebnih informacija.

	mala preduzeća	srednja preduzeća
Dobrovoljna obuka ili interno dostupne informacije (sa interneta i slično)	51,6%	55,1%
Obavezni kursevi ili gledanje obaveznog materijala	9,5%	17,1%
Obavezivanje ugovorom (npr. ugovorom o radu)	22,9%	26,7%

Tabela 6: Upoznavanje zaposlenih o obavezama po pitanju bezbednosti

* Napomena: Podaci o primeni mera bezbednosti, radnoj snazi i obukama su iz publikacije „Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji“ za 2022. godinu

Istraživanje sprovedeno u Evropskoj Uniji identifikovalo je sedam najvećih izazova za mala i srednja preduzeća u oblasti informacione bezbednosti:

- nizak nivo svesti zaposlenih o rizicima,
- neodgovarajuća zaštita kritičnih i osetljivih informacija,
- nedostatak budžeta,
- nedostatak stručnjaka za informacionu bezbednost,
- nedostatak odgovarajućih smernica za informacionu bezbednost za mala i srednja preduzeća,
- pomeranje rada u IKT okruženju van kontrole preduzeća i
- slaba podrška menadžmenta.

Istraživanje je takođe pokazalo i da mnoga preduzeća iz ove kategorije veruju da je zaštita implementirana u uređaje u IKT sistemu dovoljna i da nije potrebno da primenjuju dodatne mere bezbednosti. [4]

Uzimajući u obzir prethodno navedene statističke podatke i rezultate istraživanja može se zaključiti da u malim i srednjim preduzećima, u opštem slučaju, nije dovoljno razvijena svest o pretnjama i rizicima koji postoje prilikom upotrebe informaciono-komunikacionih tehnologija, ili se rizici svesno zanemaruju zbog nedostatka sredstava ili nemogućnosti obezbeđenja ljudskih resursa. Deo ovih nedostataka može se uspešno kompenzovati, a rizici smanjiti, dobrim pristupom i podizanjem svesti zaposlenih.

Ove Smernice su namenjene zaposlenima u malim i srednjim preduzećima, koji su posebno osetljivi na sajber napade, jer obim i šteta koju sajber napad prouzrokuje mogu biti takvi da preduzeće nakon toga ne bude u mogućnosti da se vrati normalnom poslovanju. Smernice su namenjene svim kategorijama zaposlenih, od pripravnika do vlasnika preduzeća, jer napadači koriste svaku ranjivost da bi realizovali svoj cilj.

Smernice su takođe namenjene i predavačima koji realizuju obuke iz oblasti informacione bezbednosti za mala i srednja preduzeća. Njima Smernice mogu poslužiti za pripremu predavanja i kao izvor primera iz prakse.
Napomena: u tekstu se reč „preduzeće“ uvek upotrebljava u smislu „malo i srednje preduzeće“.

Izvor: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Osnovne informacije[5]

U ovim Smernicama, a takođe i u drugim dokumentima i u svakodnevnom govoru, često se upotrebljava pojam informaciono-komunikacioni sistem (ili IKT sistem).

Pod ovim pojmom podrazumeva se tehnološko-organizaciona celina koja obuhvata:

1. elektronske komunikacione mreže,
2. uređaje ili grupe međusobno povezanih uređaja, takve da se u okviru barem jednog iz grupe uređaja vrši automatska obrada podataka korišćenjem računarskog programa,
3. podatke koji se vode, čuvaju, obrađuju, pretražuju ili prenose putem sredstava iz prethodne dve tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja,
4. organizacionu strukturu putem koje se upravlja IKT sistemom i
5. sve tipove sistemskog i aplikativnog softvera i softverske razvojne alate.

U svakom trenutku u IKT sistemu dešava se mnoštvo različitih aktivnosti. Svaka takva aktivnost u sistemu, kao na primer uključivanje računara, snimanje Word ili Excel fajla, pristup stranici na internetu i slično, naziva se događaj. Ipak, postoje pojave koje imaju negativne posledice. 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.

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

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.

Sajber bezbednost označava aktivnosti neophodne radi zaštite IKT sistema, korisnika tih sistema i drugih osoba obuhvaćenih sajber pretnjama.

Pojam haker se u literaturi često koristi isključivo u negativnom kontekstu za osobe koje neovlašćeno upadaju u IKT sisteme, što nije u potpunosti korektno. Zajedničko za sva tumačenja ovog pojma je da hakeri poseduju značajne veštine u oblasti informacionih tehnologija, uključujući znanja i sposobnosti da zaobiđu mere bezbednosti, ali neki od njih svoje veštine koriste za ispitivanje bezbednosti informacionih sistema i rešavanje problema dok ih drugi koriste u kriminalne svrhe. Kako bi se istakla pozitivna konotacija često se koristi pojam etički hakeri koji označava stručnjake u domenu informacione bezbednosti koji proveravaju mere zaštite i traže ranjivosti u IKT sistemima kako bi ih uklonili pre nego što ih otkrije neko sa lošim namerama. Iz navedenih razloga, u ovim Smernicama se za one koji imaju loše (zle) namere i izazivaju bezbednosne incidente koriste termini napadači ili kriminalci.

5 Definicije IKT sistema, incidenta i informacione bezbednosti preuzete su iz važećeg Zakona o informacionoj bezbednosti, dok je definicija pretnje preuzeta iz Nacrta zakona o informacionoj bezbednosti objavljenog u okviru javne rasprave u julu 2024. godine (do završetka pisanja ovih Smernica zakon još uvek nije bio usvojen). Definicije sajber napada i sajber bezbednosti ne postoje u Zakonu o informacionoj bezbednosti (ni u važećem, ni u nacrtu novog zakona) i preuzete su iz dokumenata Evropske Unije, a razlog njihovog navođenja je što preciznije objašnjavaju pojmove koji se često koriste u ovim Smernicama i u svakodnevnom govoru.

Izvori pretnji

Kao što je prethodno navedeno, pretnja je nešto što može da napravi štetu informaciono-komunikacionom sistemu ili korisnicima sistema (a posredno i onima koji nisu korisnici sistema). Izvori pretnje mogu se svrstati u četiri kategorije:

- ambijentalni – katastrofalni događaji i infrastrukturni poremećaji na koje preduzeće 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.[6]

Sa druge strane, IKT sistemi nisu savršeni i mogu posedovati određene slabosti. Najčešće se slabostima smatraju greške u računarskom kôdu (softveru) napravljene prilikom programiranja, ali one mogu postojati i u uređajima (hardveru), a takođe i u bezbednosnim procedurama i kontrolama, poslovnim procesima, implementaciji itd. Pojam ranjivost označava neku slabost koja postoji u IKT sistemu i koja potencijalno može dovesti do bezbednosnog problema.[7] 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.

Rizik predstavlja meru u kojoj je preduzeće ugroženo nekim potencijalnim događajem i zavisi od verovatnoće da će se nešto takvo desiti i uticaja (posledica) koji bi nastao ako se taj događaj desi. Pri tome, da bi takav događaj uopšte mogao da se desi, moraju postojati i ranjivost i pretnja vezani za taj događaj.

Radi prevencije incidenata potrebno je da preduzeća povremeno utvrđuju postojanje rizika i na osnovu poznatih informacija i iskustva određuju koliki je rizik. Ako je verovatnoća štetnog događaja velika i ako bi uticaj takvog događaja bio veliki po preduzeće, 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.

Uzimajući u obzir verovatnoću i uticaj, na utvrđeni rizik može se odgovoriti na neki od sledećih načina:

- prihvatanje rizika – kada se utvrđeni rizik može tolerisati (odnosno, zbog male verovatnoće i/ili uticaja donosi se odluka da se ne preduzimaju bilo kakve dodatne mere),
- izbegavanje rizika – kada je utvrđeni 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 mogućnosti pristupa osetljivim podacima preduzeća izvan interne računarske mreže),

6 Prethodno je već navedeno da se bezbednosni incidenti u IKT sistemima koje izazivaju namerni izvori pretnje nazivaju sajber napadi. U tekstu ovih Smernica često će se koristiti skraćeni izraz napadi koji podrazumeva sajber napade.

7 Razliku između pojmova slabosti i ranjivosti možemo objasniti pomoću sledećeg primera: programer je napravio program koji jednom dnevno pravi novu rezervnu kopiju podataka iz sistema, ali je greškom izostavio da se prethodne kopije brišu pa se kao posledica toga raspoloživi memorijski prostor nepotrebno popunjava. Ako se parametri ovog programa ne mogu menjati i ako IKT sistem ima dovoljno memorijskog prostora ova slabost neće uticati na performanse sistema. Međutim, ako postoji mogućnost podešavanja da se rezervna kopija izrađuje svakog minuta, za kratko vreme može doći do popunjavanja raspoloživog memorijskog prostora i prestanka funkcionalnosti programa ili dela sistema. U ovom primeru je slabost dovela do ranjivosti koja može biti iskorišćena za izazivanje bezbednosnog incidenta.

- podela rizika – kada se deo odgovornosti za rizik prebacuje na organizacije koje su kvalifikovanije da se bave određenom delatnošću (na primer, čuvanje podataka preduzeća u specijalizovanom centru za čuvanje podataka – 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, nabavka i implementacija bezbednosnih uređaja u IKT sistem).

Ko, zašto i kako napada?

U prethodnom delu je objašnjeno da sajber napadi označavaju namerno izazvane bezbednosne incidente u IKT sistemu. U nastavku će pažnja biti posvećena objašnjenju i upravljanju ovom vrstomincidenata, ali predložene mere služe za smanjenje efekata i suzbijanje i svih ostalih vrsta incidenata.

Ko su napadači i zašto to rade?

Napadačima nazivamo pojedince, grupe ili organizacije (bilo koje vrste) koje izazivaju bezbednosne incidente u IKT sistemima. Motivi za izazivanje bezbednosnih incidenata mogu biti:

- finansijska dobit,
- krađa identiteta,
- urušavanje kritičnih IKT sistema,
- špijunaža (državna i industrijska),
- umanjenje poslovne sposobnosti,
- krađa ličnih podataka,
- manipulisanje javnim mnjenjem,
- urušavanje ličnog integriteta,
- urušavanje poslovne reputacije,
- dokazivanje itd.

Pojedinci, grupe ili organizacije koje izazivaju bezbednosne incidente mogu biti:

- države, koje mogu sprovoditi političku ili ekonomsku špijunažu 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 (u ovu kategoriju spadaju i spoljni saradnici sa pravima pristupa).

Imajući u vidu motive i tipove napadača namerne pretnje se mogu podeliti u pet velikih kategorija:

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

Sajber kriminal[8] je daleko najzastupljenija kategorija u koju se može svrstati preko 80% svih zabeleženih napada.

Kao što i mnogi pojedinci smatraju da su suviše mali i neinteresantni za kriminalce, tako i mnoga mala i srednja preduzeća misle da su kriminalci orijentisani na velike kompanije i da neće trošiti vreme na nešto što im može doneti male finansijske dobitke. Oba ova stava su pogrešna. Kriminalaca u sajber prostoru ima mnogo i svi traže žrtve koje će odgovarati njihovim sposobnostima i raspoloživim resursima. Mala i srednja preduzeća su logičan izbor za jedan sloj kriminalaca koji nemaju kapacitet za napad na velike kompanije, ali su vođeni razmišljanjem da se u tako velikom skupu poslovnih subjekata nalazi dosta onih koji imaju slabu svest o pretnjama i ne primenjuju adekvatne mere zaštite. Motivi ovih kriminalaca ne moraju biti neposredno finansijske prirode (u smislu da ukradu novac sa računa nekog preduzeća), već mogu pokušati upad u IKT sistem u potrazi za finansijskim i drugim podacima klijenata, rezultatima istraživanja i razvoja ili intelektualnom svojinom, odnosno svim podacima koje mogu prodati na crnom tržištu ili iskoristiti za napade na neke druge žrtve. Iz tih razloga preduzeća moraju razmišljati i o zaštiti tuđih podataka koji se nalaze u njihovim IKT sistemima. Preduzeće može imati posledice i u slučaju uspešnog napada na neku drugu organizaciju ili pojedinca tokom kojeg su korišćeni ukradeni podaci iz IKT sistema tog preduzeća.

Osnovne osobine sajber napada

Za sajber napade je karakteristično da geografska lokacija ne igra nikakvu ulogu – napadač i žrtva se mogu nalaziti u istoj prostoriji, a mogu biti i na različitim kontinentima. Sajber napadi mogu biti prilično jednostavni, ali i veoma sofisticirani, a napadači mogu biti početnici koji prate neko uputstvo za napad koje su našli na internetu, ali i vrhunski stručnjaci koji svoje znanje koriste u kriminalne svrhe.

8 U Srbiji je u zvaničnoj upotrebi pojam „visokotehnološki kriminal". U tekstu Smernica ova dva pojma imaju isto značenje.

Poseban problem predstavlja mogućnost iznajmljivanja usluga sajber napada zahvaljujući čemu i potpune tehničke neznalice mogu izazvati velike probleme ako svoje poznavanje nekog IKT sistema ili lozinke za pristup stave na raspolaganje nekome ko pruža ovakve usluge.[9] Ozbiljniji napadi se realizuju u nekoliko faza, a počinju tako što napadač bira i proučava svoju potencijalnu žrtvu, 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 da bi ostvario svoje planove.

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 i sprovede mere zaštite koje će sprečiti dalje posledice. U početnoj fazi napada tokom koje napadač izviđa svoju potencijalnu žrtvu često se primenjuju tehnike socijalnog inženjeringa, od kojih su neke navedene u okviru ovih Smernica.

Kako se izazivaju bezbednosni incidenti?

Postoji mnogo načina na koje nastaju bezbednosni incidenti u IKT sistemima. U daljem tekstu će biti opisani neki od najčešćih načina, objašnjeni neki pojmovi koji se često koriste u medijima i stručnoj literaturi i dati primeri napada koji su se dogodili u prošlosti.

Malver (engl. „malware")

Malver je zajedničko ime za svaki računarski kôd 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.

9 Veliki deo interneta (po nekim procenama više od 99%) nije dostupan za pristup putem standardnih pretraživača. Ovaj deo interneta, koji se često naziva Duboki veb (eng. „Deep web"), obuhvata razne podmreže kojima sa inteneta mogu pristupiti samo ovlašćeni korisnici, naloge zaštićene lozinkama, neindeksirane baze podataka i slično. Ove lokacije na internetu se u velikoj većini slučajeva koriste u legalne svrhe i uz upotrebu standardnih protokola, ali namena im nije da budu javno dostupni i korisnici bez odgovarajućih prava ili bez odgovarajućih parametara im ne mogu pristupiti. Ipak, postoji deo Dubokog veba koji čine sajtovi sa izuzetno restriktivnim pristupom i sajtovi kojima se može pristupiti samo uz korišćenje posebnih protokola koji obezbeđuju anonimnost i zaštitu sadržaja komunikacije, što ih čini pogodnim za kriminalne aktivnosti. Ovaj deo Dubokog veba se naziva Dark net, a među sajtovima koji spadaju u ovaj deo interneta mogu se naći i oni na kojima se na prodaju nudi droga, oružje ili nelegalni softver, ali i ukradeni identiteti, ukradene informacije, usluge hakovanja itd. Treba napomenuti da protokole koji obezbeđuju anonimnost i štite sadržaj komunikacije ne koriste samo kriminalci, nego i pojedinci, organizacije i vladine agencije koje imaju potrebu da sakriju komunikaciju i identitet.

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.[10] 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.

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.

> Jedna kompanija iz Kalifornije postala je žrtva kriminalaca koji su uspeli da instaliraju trojanca u IKT sistem ove kompanije i dođu do kredencijala korišćenih za finansijske transakcije. Kriminalci su zatim inicirali više finansijskih transakcija ka inostranim bankama u ukupnoj vrednosti od 1,5 miliona američkih dolara. Kompanija je uspela da blokira prenos oko trećine od ove sume, ali je oko 1,1 milion dolara nepovratno izgubljeno. Regulatorno telo države Kalifornije, nakon saznanja o napadu, naložilo je ovoj kompaniji da u roku od tri dana nadoknadi sredstva svojim klijentima, a kako se to nije dogodilo kompanija je zatvorena.

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.

---

10 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 na koje se „zakači“ malver nazivaju se fajlovi domaćini (engl. „host files“).

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.

> Proizvod jedne IT kompanije je softver za koji je kompanija svojim klijentima obezbedila usluge ažuriranja koristeći 15 servera smeštenih u data centru. Do izbijanja pandemije Kovid-19, pristup ovim serverima bio je dozvoljen samo iz interne mreže kompanije, ali su onda zaposleni morali biti usmereni na rad od kuće. Kako bi usluga ažuriranja mogla i dalje da se pruža, kompanija je omogućila programerima da pristupaju serverima u data centru korišćenjem RDP protokola.[11] Međutim, kompanija nije zaštitila RDP konekcije i kriminalci su uspeli da iskoriste taj propust i enkriptuju podatke na 14 od 15 servera, nakon čega su tražili otkup u zamenu za ključ za dekripciju. Kompanija je tako postala žrtva ransomvera, ali je imala veliku sreću što je preostali server, koji nije bio enkriptovan, služio za čuvanje rezervnih kopija svih ostalih servera. Kompanija je zahvaljujući tome brzo vratila sistem u normalno funkcionisanje i zaštitila svoje RDP konekcije.[12]

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“)

Rutkit je ime za vrstu malvera koju je napadač uspeo da smesti u deo memorije u kojem se nalaze programi koji se automatski izvršavaju prilikom pokretanja računara. Ubacivanje 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, rutkit može bez posebnih prepreka da sprovodi zlonamerne aktivnosti kao što su špijunuranje korisnika ili krađa podataka.

Malveri za rudarenje kripto valuta (engl. „cryptojacking")

Rudarenje kriptovaluta zahteva velike računarske resurse, pa kriminalci pribegavaju i prikrivenom korišćenju tuđih resursa u ovu svrhu.

11 Protokol za daljinsko upravljanje drugim računarom (engl. Remote Desktop Protocol – RDP)
12 Izvor: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

. Za ovakve napade koriste se specijalni malveri koje napadači ubace u računar ili mobilni telefon žrtve, koja ne samo što 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.[13]

Prevara

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

Socijalni inženjering (lažno predstavljanje i drugi oblici)

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. Zbog masovnosti primene metoda socijalnog inženjeringa od strane napadača na ovu temu treba posebno obratiti pažnju.

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 kasnijem 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.

13 Pojmovi botnet i zombi će biti objašnjeni kasnije u tekstu.

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.

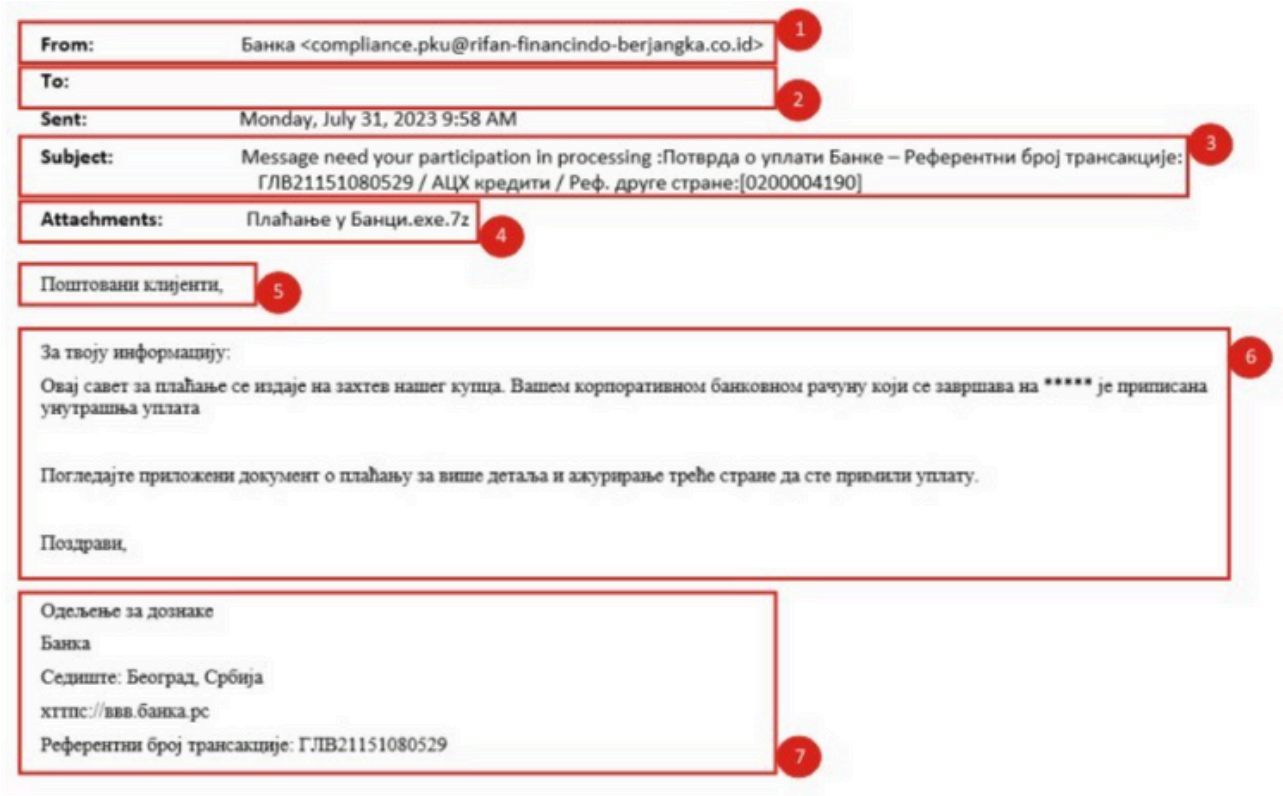
Napadači koji primenjuju socijalni inženjering su veoma vešti i u stanju su da prepoznaju odgovarajuću tehniku kojom treba da pristupe potencijalnoj žrtvi, ili da koriste kombinacije različitih tehnika da bi postigli uspeh. Svest o tehnikama koje se primenjuju prilikom ovakvih napada i oprez prilikom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

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:

- 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 preduzeću, 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.



Slika 2: Fišing poruka

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 kako na elektronsku poštu tako 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.

Jedna kompanija za marketing prešla je sa sopstvenog mejl servera na mejl sistem u klaudu. U toku prelaznog perioda jedan od zaposlenih naseo je na fišing mejl kojim su kriminalci tražili verifikaciju naloga, lažno se predstavljajući kao provajderi usluge u klaudu. Sa tog preuzetog naloga kriminalci su zatim slali mejlove klijentima kompanije, tražeći im da buduća plaćanja vrše na drugi račun (kontrolisan od strane kriminalaca) ili da zbog navodno neizmeirenog računa kliknu na link ka lažnom sajtu na kojem su im traženi kredencijali za pristup. Jedan od klijenata marketinške kompanije prepoznao je da je u pitanju lažni (fišing) sajt i obavestio marketinšku firmu, ali je i otkazao buduće poslove zbog zabrinutosti za bezbednost (u vrednosti između 200.000 i 300.000 evra godišnje).[14]

14 Izvor: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Kompromitacija poslovne pošte (engl. „Business Email Compromise“ – BEC)

Kompromitacija poslovne pošte je vrsta napada koja može napraviti veliki finansijski gubitak organizaciji, a kompanije koje spadaju u kategoriju malih i srednjih preduzeća uništiti ili dovesti na rub opstanka.

Napad se može ostvariti ako kriminalac ima mogućnost da prati komunikaciju koji imaju potencijalni kupac i potencijalni prodavac putem elektronske pošte (što je moguće ako, na primer, neko od ove dvojice ima kompromitovanu lozinku za pristup svojem nalogu). Potencijalni kupac i potencijalni prodavac se dogovaraju o ceni, rokovima isporuke i drugim aspektima kupoprodaje, dok napadač prati način pisanja, obraćanje i druge elemente komunikacije kako bi u određenom trenutku mogao da kreira verodostojnu poruku.

Kada su se prodavac i kupac dogovorili o svim aspektima kupoprodaje, prodavac kupcu šalje dokument (predračun) po kojem uplata treba da se izvrši. To je trenutak kada kriminalac stupa u akciju i šalje kupcu novi mejl. Koristeći znanje o njihovom načinu komunikacije, kriminalac se predstavlja kao prodavac i izvinjava se što je došlo do greške i moli kupca da prethodni dokument zanemari, a uplatu izvrši prema dokumentu koji se nalazi u prilogu tog mejla. U tom novom dokumentu, koji predstavlja prerađeni originalni dokument, nalaze se instrukcije za plaćanje sa promenjenim brojem računa i drugim podacima značajnim za uplatu.

Ako kupac ne posumnja i postupi po mejlu napadača, uplatiće novac na pogrešan račun. Ako nakon toga brzo ne shvati da je naseo na prevaru i urgira kod banke da se transfer zaustavi, kriminalci će novac prebaciti na druge račune i žrtva prevare će ostati bez novca.

Direktorska prevara (engl. „CEO fraud“)

Direktorska prevara je vrsta usmerenog fišinga („spear phishing“) koja se realizuje tako što kriminalci pošalju mejl radniku preduzeća lažno se predstavljajući kao direktor i tražeći da se hitno izvrši neka uplata. Da bi ovakav napad bio uspešan kriminalci moraju imati uvid u imena i pozicije radnika u preduzeću i u uobičajen način komunikacije. Kriminalci napad pokreću kada je direktor odsutan i u fišing mejlu traže od radnika kome je upućen da izvrši nalog odmah i bez obaveštavanja drugih radnika jer je u pitanju osetljiv posao, a način komunikacije pravdaju lošom internet konekcijom.

Jabuka na putu (engl. „Road apple“)

Jedan od načina na koji kriminalci pokušavaju da instaliraju malver u računarski sistem preduzeća je da ga snime na neki prenosni medij i pokušaju da prevare nekog od zaposlenih 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 zaposlenih (na primer, bace ga na pod u hodniku u preduzeću ili ostave na stolu u pekari u koju često svraćaju zaposleni) u nadi da će ga neko povezati na računar u svojoj kancelariji da proveri da li pripada nekom od kolega.

Napadi na internet sajtove

Ova vrsta napada usmerena je na veb sajtove i posetioce sajtova, a cilj napada je ubacivanje malvera u računare i mobilne uređaje posetilaca, dolaženje do informacija o njihovim kredencijalima i drugim podacima, neovlašćen pristup, izmena ili brisanje podataka sa veb sajtova i slično.

SQL injekcije (engl. „SQL Injections“)

U ovim slučajevima na meti napadača su baze podataka kojima pokušavaju neovlašćeno da pristupe putem unošenja neočekivanih parametara prilikom prijave. Ako uspeju, napadači dobijaju mogućnost da pristupe, menjaju, dodaju ili brišu podatke u bazi podataka. Ove napade je relativno lako sprečiti ograničavanjem podataka koje korisnik može da unese u veb obrazac i ograničavanjem privilegija naloga.

Cross-Site Scripting (XSS)

Kod ove vrste napada napadač ubacuje malver u sadržaj kojem pristupaju posetioci veb sajta. Prilikom posete veb lokacije kompromitovane XSS napadom, posetioci preuzimaju i malver zajedno sa drugim sadržajem veb sajta. Kada se malver pokrene na računaru žrtve napadač može biti u mogućnosti da preuzme kredencijale žrtve i pristupi drugim nalozima, ili da kontroliše njen računar i da ga koristi za napade na druge sisteme.

Cross-Site Request Forgery (XSRF ili CSRF)

Dok je napad korišćenjem prethodno opisanog XSS-a fokusiran na ubacivanje malvera u veb sajt, XSRF/CSRF se primenjuje da bi prevario veb pretraživače da izvrše radnje koje korisnik nije pokrenuo, kao što su onlajn kupovina, kreiranje sesije, preuzimanje kolačića itd. U nekim varijantama XSRF napada malver ostaje neaktivan dok se ne pristupi određenoj veb lokaciji.

Farming (engl. „Pharming“)

Farming se odnosi na lažnu kopiju regularne veb stranice kojom se pokušava navođenje korisnika da unesu svoje kredencijale. Deo ovoga napada je i usmeravanje korisnika na lažnu veb stranicu, na primer pomoću fišing mejla sa linkom. Žrtve tada unose svoje kredencijale misleći da su na regularnoj stranici.

Izmena izgleda veb stranice (engl. „Web Defacement“)

Kod ovog tipa napada, napadač ostvaruje pristup veb sajtu i menja ga iz različitih razloga, uključujući ponižavanje i diskreditaciju žrtve. Da bi se ovakav napad realizovao napadači moraju savladati mere zaštite veb servera i doći u poziciju da postojeću veb stranicu zamene nekom svojom.

Napadi u bežičnim mrežama

Bezbednosni problem kod svih bežičnih mreža je što se saobraćaj između pristupne tačke (engl. „access point“) i korisničkog uređaja odvija na način da svako ko je u blizini može da prati taj saobraćaj. Korisnici koji na ovaj način pristupaju internetu ili privatnim mrežama ne znaju ko je prisutan u bežičnoj mreži i ko pasivno snima saobraćaj. Takođe, korisnici ne mogu znati ko kontroliše pristupnu tačku u javno dostupnim bežičnim mrežama. Iz tih razloga je veoma bitno da se bežična komunikacija zaštiti, pa se u praksi regularno primenjuju različite varijante kontrole pristupa i enkripcije saobraćaja.

Lažne bežične mreže

Ovaj tip napada je relativno jednostavno izvesti ako napadač ima mogućnosti da postavi svoju pristupnu tačku na željenu lokaciju. Postoje dve podvarijante ovog napada, prva kod koje je naziv bežične mreže (SSID) identičan nekoj postojećoj mreži (ovaj tip napada zove se Evil Twin) i druga kod koje je naziv bežične mreže drugačiji od postojeće (ali može biti sličan; ovaj tip napada zove se Rogue Access Point). Saobraćaj u lažnim bežičnim mrežama je po pravilu otvoren, a napadač proverava sadržaj komunikacije u nadi da će neki korisnik ostaviti kredencijale za povezivanje na neki nalog ili podatke o kreditnoj kartici, što će napadaču omogućiti izvođenje daljih napada.

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 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.
Ako ne uspe da na ovaj način pristupi ciljanom sistemu, napadaču ostaje na raspolaganju mogućnost da isproba svaku moguću kombinaciju malih i velikih slova, brojeva i specijalnih karaktera. Ova metoda naziva se brutalna sila (engl. „brute force“) i može zahtevati nerealno veliku količinu potrebnog vremena u slučaju jakih lozinki (praktično je nemoguće otkriti jaku lozinku korišćenjem ove metode).
Ovakve napade je jednostavno sprečiti uvođenjem adekvatne politike pristupa sistemu.

Neovlašćeno korišćenje naloga

Administratori 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.).

Neprivilegovani nalozi su korisnički nalozi koji imaju ograničene mogućnosti u IKT sistemu. Kompromitacija ovakvih naloga može da dovede do ograničene štete u IKT sistemu, ali ako se ne primeti na vreme i ako postoje druge ranjivosti napadač može iskoristiti pristup takvom nalogu da poveća svoje priilegije i učini veću štetu.

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.[14] Kompromitovanje ili curenje podataka je po pravilu posledica grešaka i slabosti u tehnologiji ili ljudskom ponašanju.

> Kompanija IBM Security svake godine objavljuje izveštaj o napadima koji rezultuju curenjem podataka. U izveštaju objavljenom sredinom 2024. godine navodi se da je prosečan iznos štete izazvane curenjem podataka oko 4,88 miliona dolara, od čega se u proseku 1,47 miliona odnosi na izgubljene poslove. U preko 30% od zabeleženih slučajeva uzrok curenja podataka bio je fišing napad ili ukradeni i na drugi način kompromitovani kredencijali.

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.

---

15 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 mogućnosti za pristup i kontrolu sistema sa ciljem da dođu 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 troškove 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.
16 https://www.ibm.com/reports/data-breach

Uskraćivanje usluge (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.

Distribuirano uskraćivanje usluge (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. [17]

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 ne predstavljaju jednostavne zadatke. 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 snabdevaju veće organizacije jer se pokazalo da manje kompanije imaju blaže bezbednosne kriterijume (ili nemaju dovoljnu bezbednosnu kulturu) i nemaju resurse za primenu jakih bezbednosnih mera. Cilj napada je da se malver prvo unese u sistem manje kompanije, pa da se putem redovne komunikacije posredno implementira u IKT sistem veće organizacije. 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.

Kako incidenti utiču na poslovanje?

Bezbednosni incidenti u IKT sistemu preduzeća svakako utiču na poslovni proces. U nekim slučajevima taj uticaj je odmah vidljiv kroz nemogućnost obavljanja delatnosti ili krađu sredstava sa računa, ali postoje i slučajevi kod kojih incidenti utiču na ugled koji preduzeće ima kod svojih klijenata i saradnika.

17 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.

Direktan uticaj incidenata na poslovanje

Incidenti u IKT sistemu mogu direktno uticati na poslovanje preduzeća na nekoliko načina:

- krađa finansijskih sredstava,
- krađa intelektualne svojine,
- krađa ličnih podataka,
- onemogućavanje rada.

Krađa finansijskih sredstava

Preduzeća koja u okviru svog poslovanja imaju istraživanje i razvoj moraju izuzetno da paze da informacije o proizvodima koje razvijaju budu dostupne samo ovlašćenim radnicima. Investicije u istraživanje i razvoj su obično veoma velike, proces je dugotrajan, a očekivani prihod treba da pokrije sve troškove i obezbedi pristojnu zaradu. Konkurenciji ili kriminalcima koji informacije mogu unovčiti ovakvi projekti predstavljaju veliki mamac, a cilj im je da dođu do informacija pre završetka projekta kako bi proizvod plasirali pre preduzeća koje je radilo razvoj. Ako se desi takva situacija, preduzeće koje je investiralo velika finansijska sredstva i vreme u projekat ne može očekivati značajne prihode i veoma lako može doći u poziciju da ne može da opstane na tržištu.

Krađa ličnih podataka

Jedan od ciljeva kriminalaca je i prikupljanje ličnih podataka koje mogu iskoristiti za druge zlonamerne aktivnosti kao što su lažno predstavljanje (u svim mogućim varijantama), neovlašćeni pristup nalozima itd. U IKT sistemu preduzeća mogu se nalaziti lični podaci zaposlenih, ali i lični podaci kupaca i saradnika koji kriminalcima mogu biti interesantni. Upadi u IKT sistem koji dovedu do krađe ličnih podataka smeštenih u tom sistemu mogu da dovedu do krivičnih prijava protiv preduzeća i velikog nepoverenja klijenata.

Agencija Ešli Medison pokrenula je 2002. godine veb sajt za upoznavanje, ali sa specifičnom namenom da bude prvenstveno namenjen osobama koje su u braku i traže poznanstva van braka. Provokativna marketinška kampanja agencije naišla je na mnoge osude, ali je bez obzira na to broj članova rastao i dostigao broj od nekoliko desetina miliona širom sveta. Hakerska grupa „The Impact Team“ uspela je 2015. godine da upadne u IKT sistem agencije i ukrade podatke za 37 miliona članova, uključujući njihova imena, kućne adrese, mejl adrese, brojeve kreditnih kartica i prijavljene seksualne fantazije. Hakerska grupa je tražila od agencije da prestane sa radom, a kako se to nije dogodilo počeli su da objavljuju ukradene podatke, ali i da ucenjuju neke od članova. Posledice ovog upada u sistem i krađe podataka bile su velike tužbe i nekoliko samoubistava.

Onemogućavanje rada

Za preduzeća koja svoje poslovanje oglašavaju ili obavljaju preko veb sajta na internetu od ogromne važnosti je da sajt uvek bude raspoloživ i ažuran za klijente. Kriminalci koji imaju na raspolaganju resurse za DDoS napade (ranije opisane u ovim Smernicama) mogu ucenjivati preduzeća preduzimanjem ovakvih napada u pokazne svrhe i zahtevima za otkup da takve napade ne vrše. Takođe i konkurencija može angažovati kriminalce da sprovode ovakve napade.

Strateški i zakonski okvir

Informaciona bezbednost u Republici Srbiji je uređena Zakonom o informacionoj bezbednosti i podzakonskim aktima donetim na osnovu ovog Zakona, kao i drugim propisima koji sadrže odredbe vezane za bezbednost informacija i informaciono-komunikacionih sistema. Strateški pravci razvoja informacione bezbednosti zadati su Strategijom razvoja informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine.

Strategija razvoja informacionog društva i informacione bezbednosti[18]

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 unapređenje 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.

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

Prva od navedenih mera, podizanje svesti i znanja u oblasti informacione bezbednosti građana, javnih službenika i privrede, posebno je značajna za mala i srednja preduzeća jer predviđa više aktivnosti u cilju podizanja svesti o rizicima koji postoje za poslovanje preduzeća i znanja o načinima kako da se ovi rizici smanje na najmanju moguću meru:[19]

- 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,
- obuke za mala i srednja preduzeća o potebi i načinu primene mera zaštite i važnosti kontinuiranog podizanja kapaciteta zaposlenih, u skladu sa nacionalnim i međunarodnim standardima,
- promocija vodiča sa preporukama o osnovnom nivou mera zaštite malih i srednjih preduzeća,
- unapređenje sadržaja na platformi za podizanje svesti i znanja o informacionoj bezbednosti kroz interaktivne programe,
- podizanje svesti o značaju informacionih tehnologija, digitalizacije, informatičke pismenosti i informacione bezbednosti.

Zakon o informacionoj bezbednosti[20]

Krovni zakon u oblasti informacione bezbednosti u Republici Srbiji je Zakon o informacionoj bezbednosti. Ovim zakonom uređene su mere zaštite od bezbednosnih rizika u IKT sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja IKT 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.[21]

Najvažnije odredbe Zakona o informacionoj bezbednosti

Zakonom o informacionoj bezbednosti 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 svojstva podataka:

- tajnost – svojstvo koje znači da podatak nije dostupan neovlašćenim licima,
- integritet – očuvanost izvornog sadržaja i kompletnosti podatka,
- raspoloživost – svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban,
- autentičnost – svojstvo koje 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 – sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći.

19 Akcioni plan za realizaciju Strategije razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2024. do 2026. godine usvojen je u avgustu 2024. godine i može se naći na linku https://www.srbija.gov.rs/extfile/sr/806566/akc_pl_strat_razvoja_IDrustva_IBezbedn_2021-2026_per_2024-2026_020_cyr.zip.
20 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg

Postojećim Zakonom o informacionoj bezbednosti propisano je da se organizacije i institucije koje pružaju usluge od vitalne važnosti svrstaju u IKT sisteme od posebnog značaja.

Zakonom je propisano da se u IKT sisteme od posebnog značaja svrstaju sistemi koji se koriste:

1. u obavljanju poslova u organima vlasti,
2. za obradu posebnih vrsta podataka o ličnosti,
3. 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
4. pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti navedenih u prethodnoj tački.

Za preduzeća koja spadaju u IKT sisteme od posebnog značaja, Zakon o informacionoj bezbednosti propisuje sledeće 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.

21 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

Zakonom o informacionoj bezbednosti nisu propisane obaveze za preduzeća koja ne spadaju u IKT sisteme od posebnog značaja. Ipak, primena mera bezbednosti je važna za svako preduzeće, pa se dodatne informacije o Aktu o bezbednosti IKT sistema i merama zaštite mogu naći u dve uredbe koje su donete na osnovu Zakona o informacionoj bezbednosti:

- 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[22] i
- Uredba o bližem uređenju mera zaštite IKT sistema od posebnog značaja.[23]

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.[24]

Zakon o zaštiti podataka o ličnosti[25]

Zaštita podataka o ličnosti propisana je Zakonom o zaštiti podataka o ličnosti. Ovim Zakonom 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.

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[26] 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[27], 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.

22 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2016/94/1/reg
23 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2016/94/2/reg
24 https://www.cert.rs/files/shares/Model%20Akta%20o%20bezbednosti.pdf
25 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg

Preduzeća koja prikupljaju podatke o ličnosti (kupaca, klijenata, saradnika) u obavezi su da poštuju odredbe Zakona o zaštiti podataka o ličnosti i da primenjuju mere informacione bezbednosti u cilju smanjenja rizika.

Preduzeća koja posluju sa EU moraju biti upoznata i sa odredbama Uredbe EU o zaštiti fizičkih osoba sa osvrtom na obradu ličnih podataka i slobodnom prenosu ovih podataka (GDPR)[28]. Ova Uredba je bitna jer propisuje okvir za obradu ličnih podataka građana EU i preduzećima koja su van EU ali obrađuju podatke subjekata koji imaju prebivalište u EU. Uredbom je, između ostalog, propisano da za obradu podataka mora biti dobijena saglasnost subjekta, kao i da prava subjekta moraju biti jasno objašnjena pre dobijanja saglasnosti za obradu, a povlačenje saglasnosti mora biti jednostavno.

Kako se pripremiti i smanjiti rizik od incidenta?

Šta treba da se štiti?

Bilo šta što ima vrednost za preduzeće treba štititi. To mogu biti informacije, uređaji i mašine koje preduzeće koristi u svom radu, računarski programi (softver) i druga imovina preduzeća (za sve što ima vrednost za preduzeće koristi se naziv aset). Što je neka imovina vrednija za preduzeće to je treba više čuvati, ali pri tome treba primenjivati princip da vrednost primenjenih mera bezbednosti ne sme prevazići vrednost imovine.

Vrednost se ne odnosi samo na cenu koštanja nekog uređaja ili podatka, jer i reputacija preduzeća zavisi od njegove mogućnosti da na vreme isporuči usluge ili proizvode garantovanog kvaliteta. Kao što je već navedeno, reputacija nekog preduzeća gradi se godinama a može biti narušena za kratko vreme, pa je ona jedna od meta koje ciljaju napadači prilikom planiranja svojih aktivnosti.

Mere bezbednosti

Mere bezbednosti mogu se svrstati u tri velike grupe: fizičke, organizacione i tehničke. Mala i srednja preduzeća se uglavnom oslanjaju na tehničke mere zaštite (na primer, postavljanjem mrežnih barijera ili instaliranjem anti-virus programa) i prepuštaju sve poslove oko informacione bezbednosti tehničkim licima zaduženim za IKT sistem, što ne može biti zadovoljavajući nivo. U malim i srednjim preduzećima najčešće je zapostavljen ljudski i organizacioni faktor u smislu da ne postoje adekvatne procedure i da zaposleni nemaju potrebnu svest i nisu obučeni kako da postupaju u kriznim situacijama.

U fizičke mere bezbednosti spadaju sve mere kojima se neovlašćena lica sprečavaju ili odvraćaju da pristupe nekom prostoru ili se kontroliše fizičko prisustvo. U ove mere spadaju fizičko obezbeđenje, ograde, sistemi video nadzora, alarmni sistemi, sistemi za fizičku kontrolu pristupa i slično.

---

26 Rukovalac 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.
27 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.
28 https://eur-lex.europa.eu/eli/reg/2016/679/oj

U organizacione (administrativne) mere spadaju sve procedure, pravila, politike i drugi dokumenti kojima se organizuje bezbednost u nekom preduzeću, 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 spada primena svih tehničkih sistema namenjenih očuvanju bezbednosti, kao što su sistemi za identifikaciju, autentifikaciju i autorizaciju,[29] razni uređaji za zaštitu računarskih mreža (mrežne barijere (firewall), 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 mogućnost grešaka zaposlenih u preduzeću. U IKT sistemima postoje 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.

Organizacija i priprema zaposlenih

Prvu liniju odbrane svakog preduzeća drže njegovi zaposleni. Zaposleni su najčešće i meta prve faze napada tokom koje napadači nastoje da instaliraju malver u IKT sistem preduzeća ili da dobiju informacije koje će omogućiti nastavak i proširenje napada na preduzeće.

Kako bi se smanjile mogućnosti za sajber napad i povećale sposobnosti da se na njega pravovremeno i adekvatno reaguje zaposleni moraju redovno sprovoditi osnovne mere zaštite, znati da prepoznaju kada dođe do incidenta i znati kako da postupaju nakon toga. Zbog toga je važno da svaka organizacija, ma koliko bila mala ili velika, pripremi plan za reagovanje u slučaju sajber incidenata, obuči svoje zaposlene i redovno im podiže bezbednosnu svest.

Od svakog zaposlenog 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 zaposlenih se takođe očekuje da pokažu dužnu marljivost u otkrivanju uzroka problema i preduzimanja svih potrebnih aktivnosti kako bi se slični problemi sprečili u budućnosti.

Odgovornost rukovodilaca

Od rukovodilaca sve počinje i oni su ključni faktor uspešne organizacije informacione bezbednosti u preduzeću. Njihova podrška i svest o potrebi obezbeđivanja resursa, organizacije obuka za zaposlene ili izrade procedura predstavlja izuzetan podsticaj za radnike kojima je informaciona bezbednost u opisu posla da budu više posvećeni tim nadležnostima. Prisustvo rukovodilaca na obukama i radionicama za podizanje bezbednosne svesti daje motivaciju zaposlenima da budu pažljiviji slušaoci i primenjuju stečena znanja i veštine.

29 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).

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

Podržavanjem inicijativa, davanjem primera i uvođenjem jasnih pravila kroz politike i procedure rukovodioci u praksi pridobijaju podršku zaposlenih za efikasnu informacionu bezbednost u preduzeću.

Određivanje nadležne osobe

Za preduzeće je veoma bitno da odredi osobu nadležnu za informacionu bezbednost koja će imati i ulogu kontakt tačke za sva pitanja i aktivnosti u ovoj oblasti. Poslovi ove osobe mogu obuhvatati:

- procenu pretnji i rizika,
- izbor i primenu mera bezbednosti,
- organizaciju obuka za zaposlene,
- nadzor nad primenom mera zaštite,
- izradu internih propisa i procedura,
- koordinaciju reagovanja u slučaju incidenata,
- evidenciju i analizu incidenata,
- komunikaciju sa spoljnim saradnicima u vezi informacione bezbednosti i drugo.

Za ovu nadležnost ne mora se otvarati novo radno mesto nego se ti poslovi mogu dodeliti nekome od postojećih radnika, pri čemu je neophodno da taj radnik dobije potrebne obuke, resurse i budžet, kao i dovoljno vremena za implementaciju svih potrebnih mera.

Ako ove nadležnosti nije moguće ili nije pogodno dodeliti nekom od postojećih radnika, postoji i mogućnost da se nadležnost za informacionu bezbednost dodeli trećem licu koje nije zaposleno u preduzeću, na primer kompaniji specijalizovanoj za informacionu bezbednost ili kompaniji koja održava IKT sistem preduzeća. U tom slučaju neophodno je da preduzeće sa trećim licem ima ugovor o pružanju usluga u oblasti informacione bezbednosti (ili da postoji deo posvećen informacionoj bezbednosti u ugovoru o održavanju IKT sistema) sa jasno definisanim obavezama i odgovornošću, obavezom pružanja dokaza o kvalitetu pruženih usluga, brzini i načinu reagovanja u slučaju incidenata i kontakt osobama sa obe strane. U slučaju da ta kompanija u okviru ugovorenih poslova ima mogućnost pristupa ličnim podacima koji se nalaze u IKT sistemu preduzeća potrebno je obezbediti poštovanje odredbi Zakona o zaštiti podataka o ličnosti, a ako ima mogućnost pristupa osetljivim podacima preduzeća onda u ugovor treba uključiti i obavezu potpisivanja sporazuma o neotkrivanju podataka (engl. „Non-Disclosure Agreement“ – NDA).

Politika preduzeća u oblasti informacione bezbednosti

Politika preduzeća u oblasti informacione bezbednosti je kratak dokument u kojem se navode osnovni ciljevi primene mera zaštite i osnovna pravila ponašanja zaposlenih prilikom korišćenja IKT sistema preduzeća i postupanja sa podacima. Politika treba da sadrži i posledice po zaposlene ako se ne pridržavaju navedenih pravila. Sa politikom preduzeća treba da budu upoznati svi zaposleni i da nemaju bilo kakve dileme, zbog čega je potrebno da bude napisana jednostavnim i razumljivim jezikom.

Politiku preduzeća u oblasti informacione bezbednosti je potrebno povremeno proveravati i eventualno menjati i dopunjavati. Pravila ponašanja napisana u politici moraju biti jedna od tema na obukama za zaposlene.

Bezbednosni plan (plan reagovanja na incidente)

Poželjno je i neophodno izbegavati bezbednosne incidente u IKT sistemu i u tom cilju je primena bezbednosnih mera od izuzetnog značaja, ali se dešava da neki napad uspe i pored implementacije najboljih praksi. Preduzeće mora biti pripremljeno i za takve situacije i umeti da efikasno reaguje kako bi se brzo sprečilo širenje napada i ograničila šteta, između ostalog i zbog toga što će poverenje klijenata i saradnika zavisiti od načina na koji je preduzeće reagovalo i posledica napada, a ne od same informacije da je preduzeće bilo napadnuto. Efikasno reagovanje na sajber napad u kojem učestvuju svi zaposleni i izbegnute posledice mogu čak i da učvrste poverenje i doprinesu povećanju broja klijenata.

Radi pripreme za reagovanje na bezbednosne incidente preduzeće treba da izradi bezbednosni plan u kojem treba da opiše postupke i obaveze zaposlenih. Bezbednosni plan treba uvežbati kako bi zaposleni shvatili svoja zaduženja, stekli rutinu u primeni tih zaduženja i bili spremni da ih primene u slučaju potrebe.

Bezbednosni plan treba da sadrži:

- podatke o osobi nadležnoj za reagovanje na incidente,
- način prijave incidenta,
- aktivnosti koje treba preduzeti po primećenom incidentu (u formi standardne operativne procedure),
- uloge zaposlenih u reagovanju na incidente,
- koordinaciju i komunikaciju tokom rešavanja incidenta,
- način prikupljanja i čuvanja dokaza za krivičnu prijavu,
- nadležnu osobu i način komunikacije sa klijentima i saradnicima u slučaju potrebe,
- nadležnu osobu i način komunikacije sa nadležnim organima (policijom, tužilaštvom, Poverenikom za zaštitu podataka o ličnosti) u slučaju potrebe,
- nadležnu osobu i način komunikacije sa medijima u slučaju potrebe.

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.[30]

30 Dvajt Ajzenhauer (predsednik SAD 1953.–1961.): „Pripremajući se za bitku uvek sam otkrivao da su planovi beskorisni, ali da je planiranje neophodno“

Edukacija i podizanje bezbednosne svesti

Informaciona bezbednost mora biti utkana u delatnost preduzeća kao normalna i uobičajena aktivnost koju svi zaposleni shvataju i sprovode rutinski. Postoje mišljenja da je informaciona bezbednost tehničko pitanje i da zbog toga njome treba da se bave samo tehnička lica, ali to je potpuno pogrešan pristup. Informaciona bezbednost se tiče svih zaposlenih jer jedna greška može da utiče na sve ostale. Veoma je važno uspostaviti bezbednosnu kulturu u preduzeću, što se postiže radionicama za podizanje svesti o rizicima od bezbedosnih incidenata i edukacijama o merama zaštite koje treba preduzimati, uključujući mere koje spadaju u sajber higijenu. Obuke i radionice nije dovoljno organizovati jednom i za deo zaposlenih u preduzeću, već moraju biti kontinualan proces sa periodičnim aktivnostima u koje su uključeni svi zaposleni koji imaju pristup IKT sistemu preduzeća. Veoma je bitno da se kroz edukacije zaposlenima objasne bezbednosni planovi i procedure u slučaju incidenata, kao i da se organizuje uvežbavanje procedura.

Obuke, između ostalog, treba da uključuju:

- upoznavanje sa internim propisima i procedurama u preduzeću,
- mere sajber higijene koje treba da primenjuju svi zaposleni,
- metode socijalnog inženjeringa,
- kako prepoznati fišing,
- kome i kako prijaviti incident,
- kako reagovati u slučaju incidenta itd.

U slučaju da postoji potreba program obuke može biti različit za različite organizacione jedinice u okviru preduzeća. Nedostatak sredstava za angažovanje spoljnog predavača može se rešiti tutorijalima i lekcijama u video formatu koje se mogu besplatno naći na internetu.

Obuke za tehnička lica

Problem sa tehničkim licima koja održavaju IKT sisteme malih i srednjih preduzeća je što ona često nisu adekvatno obučena za primenu mera zaštite, zbog čega može doći do loše konfiguracije uređaja ili grešaka koje napadači mogu iskoristiti. Zbog toga je potrebno predvideti odgovarajuće stručne obuke za ova lica, a ako je održavanje IKT sistema povereno nekoj spoljnoj kompaniji onda ugovor o pružanju usluga obavezno treba da sadrži i deo koji se odnosi na zahtevani nivo informacione bezbednosti.

Provere primenjenih mera bezbednosti

Provere primenjenih mera informacione bezbednosti sprovode se u cilju identifikacije ranjivosti i rizika koji nisu primećeni u svakodnevnom radu. Ove provere treba organizovati povremeno (u redovnim vremenskim intervalima, nakon implementacije značajnih izmena u IKT sistemu i vanredno u slučaju određenih sumnji), a za njihovo izvođenje preporučivo je angažovati profesionalca van preduzeća i van kompanije sa kojom preduzeće ima ugovor iz oblasti informacione bezbednosti (sa napomenom da profesionalci prilično skupo naplaćuju svoje usluge).

Provere, pored tehničkih kontrola, mogu obuhvatiti i propise i procedure preduzeća, svest, znanje i ponašanje zaposlenih, mere fizičke zaštite, a po dogovoru sa rukovodstvom preduzeća i prikrivene napade prema zaposlenima metodama socijalnog inženjeringa i ciljanih fišinga, penetracione testove i slično.

Tehničke mere bezbednosti koje preduzeće može implementirati

Pravljenje rezervnih kopija (bekap, engl. „back-up“)

Rezervne kopije daju mogućnost preduzeću da relativno brzo i jednostavno nastavi sa poslovanjem nakon bilo koje vrste incidenta u kojem su podaci u aktivnom IKT sistemu oštećeni ili nedostupni, ne samo kao posledica sajber napada.[31] Pravljenje rezervnih kopija treba da bude automatizovano i redovno, pri čemu se period izrade rezervnih kopija proračunava na osnovu količine podataka, maksimalne tolerancije po pitanju perioda za koji neće postojati rezervna kopija,[32] raspoloživog memorijskog prostora i drugih parametara.

Rezervne kopije treba držati odvojeno od aktivnog IKT sistema preduzeća. Često se za čuvanje rezervnih kopija primenjuje pravilo „3-2-1“ koje znači da se prave tri rezervne kopije, od kojih se dve kopije čuvaju na dva različita medija, a treća van lokacije preduzeća (najčešće u klaudu). Radi bezbednosti rezervne kopije treba enkriptovati i sprovoditi periodične provere upotrebljivosti.

Redovno ažuriranje

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 preduzeća treba što pre da instaliraju 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 preduzeća najbolja opcija je uključivanje automatskog ažuriranja, kada sistem samostalno proverava postojanje zakrpe ili ažuriranja i automatski ih instalira.[33]

31 Na primer, u slučaju fizičkog oštećenja ili kvarova uređaja.
32 Na primer, ako je sistem podešen da pravi rezervne kopije u ponoć a incident se dogodi u 18h sledećeg dana, period u trajanju od 18 časova neće biti moguće rekonstruisati.
33 Mogućnost automatskog ažuriranja nije uvek dostupna, pa treba identifikovati softver koji zahteva ručno pokretanje ažuriranja i način na koji ažuriranje treba izvršiti.

Enkripcija (šifrovanje, engl. „encryption“)

Enkripcija ili šifrovanje je proces transformacije čitljivih informacija u oblik nečitljiv za sve osim za one koji poseduju odgovarajući ključ za dekripciju (dešifrovanje). Enkripciju treba primenjivati za sve osetljive podatke preduzeća prilikom čuvanja u IKT sistemu, kao i prilikom prenosa preko interneta. Enkripciju je preporučivo koristiti i za druge namene, a posebno se preporučuje enkripcija mobilnih uređaja kao što su laptopovi i mobilni telefoni, čime se sprečava mogućnost da u slučaju krađe osetljivi podaci preduzeća postanu dostupni neovlašćenim licima.

Prilikom korišćenja interneta potrebno je koristiti protokole sa enkripcijom uvek kad je to moguće.[34]

Kontrola pristupa IKT sistemu

Lozinke (engl. „passwords“) su osnovni metod autentifikacije korisnika u velikoj većini IKT sistema i samim tim ključni faktor za zaštitu tih sistema od neovlašćenog pristupa. Definisanje i dosledna primena politike bezbedne upotrebe lozinki je veoma bitna za preduzeća jer smanjuje mogućnosti za bezbednosni incident, ali je bitna i za svakog pojedinca u zaštiti ličnih podataka. Politikom bezbedne upotrebe lozinki definišu se:

- minimalna[35] (a po potrebi i maksimalna) dužina lozinke,
- zahtevana snaga lozinke (upotreba malih i velikih slova, brojeva i specijalnih karaktera),[36]
- maksimalni period do izmene lozinke,
- period u kojem korisnik ne može prilikom izmene uneti lozinku koju je već koristio itd.

Primenu navedenih ograničenja preduzeće može tehnički kontrolisati, ali postoje i mere bezbednosti koje se ne mogu kontrolisati i za koje zaposleni mora imati svest da treba da primenjuje (na primer, da ne koristi istu lozinku za pristup nalogu na poslu i na privatnom nalogu na internetu, da je ne zapisuje na papirićima koje drži istaknute na svom radnom mestu, da je ne deli sa drugima i slično).
Prilikom kreiranja lozinke svakako treba izbegavati neke očigledne nizove kao što su „12345“, „987“, „abcd“ ili „qwerty“, lična imena, brojeve od ličnog značaja (rođendani, brojevi telefona), imena kućnih ljubimaca i slično. Što više slučajnosti ima u lozinki to je ona bolja.

Jedna od preporuka je da se kao lozinka koristi pristupna fraza (engl. „passphrase“) koja se sastoji od nekoliko spojenih reči po slučajnom izboru. Prilično jaka lozinka može se napraviti ako se pojedina slova u tim rečima zamene brojevima, neka druga specijalnim karakterima a ostatak uredi da lozinka sadrži i velika i mala slova. Primer pravljenja takve pristupne fraze može biti skup od sledeće tri nasumice izabrane reči:

zona pelikan zelen

Sa ovim se možemo igrati na bilo koji način – menjati slova brojevima i specijalnim karakterima, menjati mala slova u velika, premeštati ih, menjati ih drugim slovima i raditi bilo šta što nam padne na pamet, na primer:

z%Na1peKiLan!z6LeN

34 Protokol TLS namenjen je zaštićenoj komunikaciji sa sajtom na internetu na način da neko ko ima mogućnost da snima saobraćaj ne može da razume sadržaj komunikacije. Protokol IPSec često se koristi za enkripciju komunikacije u virtuelnim privatnim mrežama (VPN).
35 Ne postoji konsenzus oko minimalne dužine lozinke, ali retko ko preporučuje lozinku kraću od 12 karaktera.
36 U specijalne karaktere spadaju !"#$%&'()*+,-./:;<=>?@[\]^_{|}~. Neki sistemi ne dozvoljavaju upotrebu svih navedenih karaktera u lozinkama.

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 osoba koja želi da ostvari pristup zaista ona za koju se predstavlja korisničkim imenom.

Faktori mogu pripadati nekom od sledećih skupova:

- šta znam (lozinke, PIN-ovi i drugo što 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).

Primena alata za zaštitu mejlova

U ranijem tekstu opisano je šta znači fišing i kakav rizik predstavlja po preduzeće. Jedan od načina da se ovaj rizik smanji je obuka zaposlenih kako da prepoznaju takve poruke, ali i uspostavljanje procedura verifikacije pre izvršenja uplate za koju je nalog stigao mejlom (na primer, korišćenjem drugog sredstva komunikacije za dobijanje potvrde od strane nadležne osobe).

Pored toga, postoje alati koji se dodaju mejl serverima sa namenom da filtriraju prispele mejlove i uklanjaju one sa prilozima koji sadrže malvere, mejlove sa linkovima ka sajtovima koji su sumnjivi ili označeni kao zlonamerni i sve druge mejlove koji se po određenim kriterijumima mogu smatrati neželjenima. Na ovaj način se korisnici unapred štite od mejlova koji mogu nauditi preduzeću i njima lično. Ipak, ovi alati nisu svemogući i dešava se da do zaposlenih stignu i mejlovi sa zlonamernim sadržajem, pa u svakom trenutku treba biti oprezan i sprovoditi osnovna pravila provere da li je prispeli mejl fišing.

Većina usluga mejl servera koje se nude u klaudu poseduje implementirane alate za zaštitu.

Kratak pregled uređaja i softvera za zaštitu

Mrežna barijera (engl. „firewall“)

Mrežna barijera je uređaj koji se nalazi na granici između pojedinih delova mreže (a najčešće između interne mreže i interneta) i koji ima svrhu da filtrira saobraćaj prema definisanim pravilima. Ovaj uređaj ima unapred definisane kriterijume za blokiranje paketa, a 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 hardverskoj i u softverskoj verziji.

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 specijalizovanih uređaja za zaštitu već i sa različitih servera, računara krajnjih korisnika i mrežnih uređaja. Ovi podaci dolaze u formi bezbednosnih zapisa (logova) koje ti uređaji formiraju o događajima koji mogu imati bezbednosni značaj. SIEM sistem vrši obradu svih dobijenih podataka, pravi njihovu korelaciju po vremenu i izvlači zaključke o incidentima ili pretnjama sistemu.

Anti-malveri

Služe za detekciju i uklanjanje ili onemogućavanje dejstva 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 pojavljuje veoma veliki broj novih malvera i njihovih varijanti i podvarijanti, neophodno je redovno raditi ažuriranje baze anti-malver softvera.

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 koje sprovode zaposleni

Mere bezbednosti na radnom mestu

Razdvajanje poslovnog i privatnog

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

> Mala pravna kancelarija dozvoljava svojim zaposlenima da rade od kuće i da koriste svoje lične laptopove. Zaposleni imaju mogućnost i da sa ličnih uređaja pristupaju internoj mreži firme. Jednom od zaposlenih provalnici su provalili u kuću i ukrali vredne stvari, između ostalog i lični laptop koji je koristio za daljinski rad, a na kojem su se nalazile sve informacije o klijentima i kopije mejlova koje je razmenjivao sa klijentima. Sadržaj hard diska na laptopu nije bio enkriptovan, tako da su osetljivi podaci na njemu postali dostupni svakome ko je nakon toga došao u posed tog laptopa.[37]

Čuvanje tajnosti lozinki

Zaposleni 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 radi otključavanja potrebno uneti lozinku. Ovu meru zaposleni treba da primenju čak i kada iz kancelarije izlaze na kratko.

37 Izvor: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Jasno označavanje dokumenata

Svaki zaposleni treba striktno da primenjuje politiku preduzeća po pitanju osetljivih informacija. Označavanjem dokumenata daje se svim ostalim zaposlenim u preduzeću 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 preduzeća prethodno moraju biti obrisani podaci na bezbedan način. Kao što postoje alati koji mogu da vrate podatke koji nisu bezbedno obrisani, tako postoje i dostupni su alati za bezbedno brisanje koji onemogućavaju takve akcije.

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 preduzeća.

Zaštita službene mejl adrese

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

Mere bezbednosti prilikom rada od kuće

Zaposleni u preduzećima često imaju potrebu da poslove obavljaju od kuće. Ovaj način rada je bio naročito rasprostranjen tokom pandemije korona virusa, ali i danas se masovno primenjuje zbog svojih dobrih strana kao što su uštede ili brzina obavljanja poslova. Međutim, ovakav način rada nosi sa sobom i određene rizike, pa je potrebno primenjivati mere bezbednosti kako bi se oni umanjili.

Upotreba virtuelnih privatnih mreža (VPN)

Virtuelne privatne mreže se koriste za zaštitu komunikacija preko interneta između dve geografski različite lokacije. Postoje različite mogućnosti za realizaciju virtuelnih privatnih mreža, ali u slučaju rada od kuće štiti se komunikacija koju zaposleni sa neke lokacije van sedišta preduzeća ostvaruje sa IKT sistemom u preduzeću. Rad u virtuelnoj privatnoj mreži daje zaposlenom sve mogućnosti kao da radi na poslu, a primenjeni protokoli obezbeđuju zaštićeno prijavljivanje na mrežu i enkriptovanu komunikaciju.

Veoma je važno da se virtuelna privatna mreža uspostavi direktno između zaposlenog koji je van preduzeća i IKT sistema preduzeća, za šta je neophodno da na obe strane postoji instaliran odgovarajući softver i da su generisani i dodeljeni odgovarajući kredencijali za pristup. Na internetu se mogu naći ponude za korišćenje (često i besplatno) virtuelnih privatnih mreža, ali treba obratiti pažnju da te virtuelne privatne mreže štite komunikaciju između korisnika i provajdera ove usluge, dok je komunikacija kroz ostatak prenosnog puta (između provajdera i IKT sistema preduzeća) nezaštićena. Takođe, u ovom slučaju je sva komunikacija između zaposlenog i IKT sistema preduzeća otvorena za tog provajdera na njegovoj strani komunikacije.

Zaštita kućne bežične mreže

Uređaji koji se nalaze na istoj kućnoj bežičnoj mreži su međusobno mnogo više izloženi nego prema nekom uređaju van te mreže. To je jedan od razloga zbog kojih treba uključiti protokole zaštite bežične mreže (WPA2), redovno menjati lozinku za pristup i paziti kome se dozvoljava pristup mreži.

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 enkripcijom.

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 kriminalci 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 poznavanje bilo kakvih podataka, 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.

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.

Pažljivo i ograničeno deljenje ličnih podataka

Jedna od polaznih tačaka kriminalaca koji se pripremaju za napad je istraživanje svih podataka o potencijalnoj žrtvi korišćenjem svih raspoloživih izvora, a najviše društvenih mreža (Facebook/Meta, Twitter/X, LinkedIn, Instagram itd). Opreznost prilikom objavljivanja ličnih podataka i selekcija onih koji mogu imati pristup takvim informacijama značajno sužava mogućnosti za uspešan napad socijalnim inženjeringom.

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 sve osobe povezane na informacione i komunikacione mreže, od običnih korisnika preko administratora IKT sistema do rukovodilaca, kako bi se smanjile mogućnosti za uspešne sajber napade.

Mere sajber higijene nisu komplikovane i ne zahtevaju veliko tehničko znanje, ali je bitno da se sprovode redovno. 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 zaposlenih koji imaju pristup poslovnom IKT sistemu onda će i taj sistem biti mnogo bezbedniji, ali će biti bezbedniji i ovi zaposleni jer će stečene navike primenjivati i prilikom upotrebe privatnih uređaja i podataka.

Neke od mera sajber higijene (koje se zaposlenima preporučuju da ih primenjuju i u privatne svrhe) su:

- pravljenje rezervnih kopija,
- redovno ažuriranje operatinog sistema i aplikacija,
- enkripcija osetljivih podataka i mobilnih uređaja,
- implementacija anti-malver rešenja,
- instalacija mrežnih barijera,
- zaštita bežičnih mreža,
- postavljanje bezbednih konfiguracija internet pretraživača,
- zaštita mobilnih uređaja od krađe,
- korišćenje jakih lozinki i multifaktorske autentifikacije.

Bezbednost informacija

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

Nemaju svi podaci isti značaj za jedno preduzeće. Dok neki podaci mogu slobodno da se objavljuju javno, postoje podaci koje je potrebno da zna samo mali broj ljudi i koji se moraju dodatno štititi (ugovori, finansijski detalji, podaci o istraživanju, razvoju i proizvodnji, lični podaci zaposlenih, klijenata i dobavljača i slično). 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 enkripcija prilikom prenosa i čuvanja, kontrola pristupa, obrada i čuvanje na odvojenim ili zaštićenim uređajima i slično.
Preduzeća sama određuju u koliko kategorija će svrstati svoje podatke, a obično su to tri ili četiri kategorije. Jedan od često korišćenih je model sa tri kategorije tajnosti:

- poverljivo, za podatke koje treba da zna samo određen krug osoba i koji se štite na način koji preduzeće odredi,
- interno, za podatke koje treba da poznaju zaposleni u preduzeću ali ne i osobe van preduzeća i koji se obično čuvaju u internoj računarskoj mreži preduzeća i
- javno, za sve ostale podatke koji se mogu deliti bez ograničenja.

Standardizacija

Kao i u mnogim drugim oblastima, i u oblasti informacione bezbednosti postoje međunarodno priznati standardi kojima se ukazuje na mere koje treba preduzeti da bi određena delatnost bila dobro uređena i da bi organizacija koja primenjuje te standarde bila prepoznata kao ozbiljan i poželjan partner. Standardi u oblasti informacione bezbednosti služe preduzeću da identifikuje potrebne mere kako za zaštitu IKT sistema i podataka koji se u njima nalaze, tako i za reagovanje i oporavak od bezbednosnih incidenata. Standardi se, u najvećem broju slučajeva, mogu primeniti u preduzećima bez obzira na njihovu veličinu ili delatnost kojom se bave.

Postoji nekoliko značajnih međunarodnih standarda u oblasti informacione bezbednosti (BS 7799, NIST CSF, BSI IT-Grundschutz, NCSC Cyber Essentials itd.) ali najpoznatiji standard u ovoj oblasti je ISO/IEC 27001 za upravljanje bezbednošću informacija.[38]

Standard ISO/IEC 27001

Ovaj standard je jedan od standarda iz familije ISO/IEC 27000. Standardi iz ove familije pokrivaju informacionu bezbednost, zaštitu privatnosti, tajnost podataka i druge aspekte bezbednosti. Neki od predstavnika familije ISO/IEC 27000 su:

- ISO/IEC 27000 – pregled i rečnik,
- ISO/IEC 27001 – zahtevi za sistem upravljanja informacionom bezbednošću,
- ISO/IEC 27002 – katalog kontrola u informacionoj bezbednosti,
- ISO/IEC 27003 – vodič za implementaciju sistema za upravljanje informacionom bezbednošću,
- ISO/IEC 27004 – nadzor, merenje, analiza i evaluacija,
- ISO/IEC 27005 – vodič za upravljanje rizicima u informacionoj bezbednosti,
- ISO/IEC 27021 – zahtevi po pitanju kompetencija profesionalaca za sisteme upravljanja informacionom bezbednošću,
- ISO/IEC 27032 – vodič za sajber bezbednost,
- ISO/IEC 27033 – serija od nekoliko standarda u oblasti bezbednosti mreža,
- ISO/IEC 27034 – serija od nekoliko standarda u oblasti bezbednosti aplikacija,
- ISO/IEC 27039 – prevencija upada u sistem,
- ISO/IEC 27040 – bezbednost skladištenja podataka,
- ISO/IEC 27043 – istraživanje incidenata itd.

Standard ISO/IEC 27001 postavlja okvir zahteva za sisteme upravljanja informacionom bezbednošću i najvažniji je predstavnik familije ISO/IEC 27000. Zahtevi koje standard postavlja odnose se na politike, procedure, uloge, odgovornosti, resurse, provere i drugo što jedna organizacije treba da ima uspostavljeno u oblasti informacione bezbednosti. Mere zaštite koje preduzeće mora implementirati putem politika, procesa i procedura da bi bilo u saglasnosti sa standardom nazivaju se kontrole kojih u najnovijoj verziji standarda[39] ima 93 svrstanih u četiri tematske celine:[40]

- organizaciona,
- ljudska,
- fizička i
- tehnološka.

Preduzeće može imati potrebu za sertifikatom za standard ISO/IEC 27001 kojim dokazuje nivo primenjenih mera zaštite i posedovanje potrebnih sposobnosti za upravljanje informacionom bezbednošću. Sertifikat se dobija nakon uspešnog procesa provere ispunjenosti uslova koju vrše akreditovani proveravači.

38 Standard ISO/IEC 27001:2013 poslužio je kao osnova za mere zaštite koje su u obavezi da primenjuju IKT sistemi od posebnog značaja prema važećem Zakonu o informacionoj bezbednosti.
39 Najnovija verzija standarda je ISO/IEC 27001:2022
40 Prethodna verzija standarda ISO/IEC 27001:2013 sadržala je 114 kontrola svrstanih u 14 domena.

Šta raditi u slučaju incidenta?

Indikatori na koje treba obratiti pažnju

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

Zaposleni mogu posumnjati na bezbednosni incident 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 (antivirus 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 sajber incident, ali svakako treba da podstaknu zaposlenog da ih ispita i potraži pomoć stručne osobe u slučaju potrebe.

Prve aktivnosti nakon uočenog incidenta

VPo utvrđivanju da je sajber incident u toku treba odmah krenuti sa postupcima kojim će se zaustaviti njegovo dalje širenje i ograničiti šteta. Osnovno pravilo za reagovanje na sajber incidente, posebno u prvim trenucima nakon saznanja da se nešto loše dešava u sistemu, jeste da se ne sme paničiti jer je tada najbitnije da se razmisli i donesu ispravne odluke za kratko vreme. U tim situacijama mnogo pomaže napisan i uvežban bezbednosni plan čijim sprovođenjem će se stvoriti uslovi da se funkcionisanje preduzeća 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 sajber incidenta i korisnici IKT sistema ne smeju samostalno donositi i sprovoditi odluke bez konsultacija sa stručnim licima nadležnim za reagovanje na incident.

Komunikacija, a naročito ona koja dolazi od rukovodilaca i stručnih lica, mora biti jasna, sažeta i precizna. Na taj način će se kod zaposlenih smanjiti napetost prouzrokovana incidentom i svako će biti motivisaniji da ispuni svoje zadatke u reagovanju na incident.

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.

Veoma je bitno da nakon uočenog incidenta brzo budu obaveštene osobe nadležne za sprovođenje procedure reagovanja na incidente, koje trebaju hladne glave i efikasno da koordiniraju realizaciju svih predviđenih aktivnosti.

Mogućnosti za podršku i pomoć

Eksternu pomoć treba pozvati ako bezbednosni incident ima veće razmere i postoji rizik da bude izazvana veća šteta, ili ako preduzeće nema dovoljno internih kapaciteta da samostalno reši incident. Ova pomoć može uključivati konsultacije o načinima za rešavanje incidenta ili angažovanje stručnih osoba (dolaskom na lice mesta ili radom sa daljine) radi neposrednog rešavanja incidenta.

Preduzeće može imati ugovor sa trećim licem o pružanju usluga u domenu informacione bezbednosti i u slučaju bezbednosnih incidenata prvo se poziva to treće lice u skladu sa odredbama ugovora. Ako preduzeće nema takav ugovor, može se za pomoć obratiti drugim organizacijama sa kojima je već imalo saradnju, a pre svih onima koji su preduzeću isporučili neku 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[41] i druge specijalizovane kompanije koje se bave zaštitom IKT sistema.

Odluke se svakako moraju doneti brzo, jer postoji mogućnost da neke posledice neće biti moguće otkloniti ako prođe dovoljno dugo vremena.

Prijava nadležnim organima

U Krivičnom zakoniku Republike Srbije[42] 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 ograničavanje 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.

41 Evidencija Posebnih CERT-ova koju vodi Nacionalni CERT nalazi se na adresi https://www.cert.rs/rs/evidencija-certova.html
42 https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg

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 visokotehnloški kriminal.[43]

Šta raditi nakon završenog incidenta?

Posle stresa izazvanog incidentom i utrošenog vremena na njegovo rešavanje i vraćanje poslovnog okruženja u normalno (ili upotrebljivo) stanje, zaposlenima je najvažnije da završe aktivnosti započete pre incidenta i nastave sa ustaljenim načinom rada. Međutim, to što je do incidenta došlo znači da postoje određene ranjivosti koje treba rešiti. Zbog toga je potrebno napraviti analizu i to najkasnije nekoliko dana nakon završetka incidenta, dok su utisci još sveži. Ova analiza se može napraviti kroz sastanak zaposlenih i spoljnih saradnika koji su učestvovali u rešavanju incidenta, na kojem treba sagledati:

- kako se dogodio incident,
- kako je uticao na poslovanje preduzeća,
- kakve je posledice ostavio,
- šta je bilo dobro, a šta loše tokom reagovanja na incident,
- da li je potrebno menjati proceduru reagovanja na incidente i bezbednosni plan.

43 https://www.beograd.vtk.jt.rs/lt/default.htm

Zaključak

Prema svim dostupnim podacima može se zaključiti da većina malih i srednjih preduzeća primenjuje manje rigorozne bezbednosne mere nego što je potrebno i ima ograničene resurse za prevenciju, detekciju i reagovanje na incidente.

Primena novih tehnologija u poslovanju donosi uštede kao što su brza i jednostavna razmena informacija i mogućnosti za rad od kuće, ali sva ova unapređenja nose sa sobom i bezbednosne izazove. U takvim okolnostima, mala i srednja preduzeća su posebno ranjiva na napade na IKT sistem, a treba imati u vidu da se broj i sofisticiranost napada na internetu povećava, ali i štete koje ovi napadi prouzrokuju.

> Treba biti svestan da se ne mogu sprečiti svi sajber napadi i da će ih svakako biti, ali jeste moguće zaustaviti neke ili većinu od njih i pripremiti se tako da posledice uspešnog napada budu minimalne a poslovanje normalizovano u najkraćem roku. Jedan od bitnih faktora za postizanje tog cilja je da svaki zaposleni razume i sledi propisane mere bezbednosti, jer greška jednog zaposlenog može uticati na sve ostale i na preduzeće u celini.

Nadamo se da će ove Smernice doprineti boljem razumevanju opasnosti i pomoći da preduzeća unapred onemoguće veći broj pokušaja napada, da se dobro pripreme za bezbednosne incidente i da spreče ili minimizuju štetu od incidenta.

Prilog: Pregled preporuka za informacionu bezbednost malih i srednjih preduzeća

1. Kreirajte politiku informacione bezbednosti preduzeća

- Odredite koje ciljeve želite da postignete
- Odredite osnovna pravila ponašanja zaposlenih
- Odredite posledice po zaposlene u slučaju kršenja pravila
- Postavite dokument tako da bude stalno dostupan zaposlenima

2. Izgradite kulturu informacione bezbednosti u preduzeću

- Primenjujte pozitivan i prepoznatljiv odnos rukovodstva prema informacionoj bezbednosti
- Motivišite zaposlene da primenjuju mere informacione bezbednosti

3. Kreirajte pravila za klasifikaciju osetljivih podataka u preduzeću

- Odredite nivoe klasifikacije
- Odredite kriterijume za klasifikaciju podataka
- Odredite načine zaštite osetljivih podataka
- Učinite dokument dostupnim zaposlenima

4. Postavite pravila za prikupljanje i obradu ličnih podataka

- Odredite nivoe klasifikacije
- Odredite kriterijume za klasifikaciju podataka
- Odredite načine zaštite osetljivih podataka
- Učinite dokument dostupnim zaposlenima

5. Napravite inventar uređaja i programa

- Napravite popis svega što ima vrednost
- Odredite šta ima veći značaj, a šta je od vitalne važnosti za vaš posao
- Odredite mere zaštite u zavisnosti od važnosti

5. Napravite inventar uređaja i programa

- Napravite popis svega što ima vrednost
- Odredite šta ima veći značaj, a šta je od vitalne važnosti za vaš posao
- Odredite mere zaštite u zavisnosti od važnosti

6. Napravite inventar osetljivih podataka

- Napravite popis podataka ili grupa podataka koji spadaju u osetljive
- Primenite mere zaštite

7. Primenite mere fizičke zaštite objekata i prostora

- Odredite šta je potrebno da ima zaštitu od fizičkog pristupa
- Odredite načine fizičke zaštite objekata
- Odredite načine zaštite od fizičkog pristupa unutrašnjim prostorima od značaja

8. Primenite mere tehničke zaštite IKT sistema

- Sagledajte potrebe i implementirajte uređaje za zaštitu IKT sistema (mrežne barijere, IPS, IDS i drugo)
- Sagledajte potrebe i implementirajte programe za zaštitu IKT sistema (anti-malver, anti-spajver i drugo)
- Sagledajte i implementirajte enkripciju
- Primenjujte alate za zaštitu mejl komunikacije
- Definišite kriterijume za korišćenje i način zaštite mobilnih uređaja
- Definišite i implementirajte bezbedne konfiguracije
- Implementirajte sistem za nadzor IKT sistema
- Uspostavite mehanizam za čuvanje bezbednosnih zapisa (logova)
- Uspostavite mehanizam za čuvanje master lozinki za slučaj nedostupnosti administratora

9. Zaštitite bežičnu mrežu preduzeća

- Primenite najbolje protokole za enkripciju saobraćaja
- Uspostavite kriterijume za pristup bežičnoj mreži
- Uspostavite odvojenu bežičnu mrežu za goste

10. Uspostavite politiku i sistem kontrole pristupa IKT sistemu

- Odredite kriterijume za dobijanje prava pristupa IKT sistemu
- Odredite načine autentifikacije (politika lozinki, multifaktorska autentifikacija)
- Odredite kriterijume za gubljenje prava na pristup sistemu
- Uspostavite mehanizam za brzo blokiranje pristupa IKT sistemu za radnike kojima prestanu obaveze u preduzeću

11. Uspostavite redovno ažuriranje

- Uspostavite automatsko ažuriranje gde je moguće
- Odredite način za ručno ažuriranje gde automatsko nije moguće
- Odredite nadležne radnike

12. Uredite daljinski pristup sistemu

- Definišite način pristupa sistemu
- Odredite način zaštite uređaja kojima se daljinski pristupa sistemu
- Odredite način kontrole daljinskog pristupa sistemu

13. Uredite poslovanje u klaudu

- Odredite usluge koje se koriste i način korišćenja
- Primenite mere enkripcije za sve podatke koji se čuvaju u klaudu
- Uredite čuvanje podataka o ličnosti u skladu sa propisima

14. Uspostavite redovno pravljenje rezervnih kopija

- Definišite način izrade rezervnih kopija
- Odredite način čuvanja rezervnih kopija
- Odredite nadležne radnike

15. Uredite poslovanje na internetu

- Sagledajte način i važnost poslovanja na internetu
- Zaštitite komunikaciju koja se obavlja preko interneta
- Zaštitite veb sajt preduzeća

16. Uredite odnos sa trećim licima u vezi održavanja IKT sistema

- Napravite ugovore sa eksplicitno definisanim obavezama obe strane
- Odredite nivo usluge i obaveze u slučaju incidenata u IKT sistemu
- Odredite kontakt osobe sa obe strane za sprovođenje ugovora

17. Napravite procene pretnji i rizika

- Napravite procene pretnji po informacionu bezbednost preduzeća
- Sagledajte ranjivosti
- Napravite procene rizika po bezbednost

18. Napravite bezbednosni plan za slučaj incidenta u IKT sistemu

- Odredite nadležnog radnika
- Odredite način prijave incidenata
- Napravite standardnu operativnu proceduru u slučaju incidenta

19. Obučite radnike

- Odredite teme koje je potrebno pokriti obukama
- Napravite plan obuka i redovno ga sprovodite
- Organizujte radionice za podizanje bezbednosne svesti
- Organizujte stručne obuke za tehnička lica

20. Sprovodite redovne provere informacione bezbednosti

- Uspostavite redovan ciklus provera
- Sprovodite i vanredne provere
- Proveravajte i unapređujte dokumenta preduzeća iz domena informacione bezbednosti
- Proveravajte i unapređujte primenjene mere zaštite
- Angažujte spoljne saradnike