4. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija

---

Na temelju članka 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i Poglavlja 3. Odluke o usvajanju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine ("Službeni glasnik BiH", broj 38/17), na prijedlog Ministarstva komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine, na 3. sjednici, održanoj 23. veljače 2023. godine, donijelo je

ODLUKU
O USVAJANJU SMJERNICA O UPRAVLJANJU SIGURNOSNIM ZAKRPAMA, SMJERNICA O KLASIFIKACIJI INFORMACIJSKIH RESURSA, SMJERNICA O INFORMATIČKOJ SIGURNOSTI RADNOG MJESTA I SMJERNICA O UPRAVLJANJU SIGURNOSNIM INCIDENTIMA

Članak 1.
(Predmet Odluke)

Ovom Odlukom usvajaju se Smjernice o upravljanju sigurnosnim zakrpama, Smjernice o klasifikaciji informacijskih resursa, Smjernice o informatičkoj sigurnosti radnog mjesta i Smjernice o upravljanju sigurnosnim incidentima, koje su sastavni dio ove Odluke.

Članak 2.
(Praćenje realiziranja)

Za praćenje realiziranja ove Odluke zadužuju se Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine.

Članak 3.
(Stupanje na snagu)

Ova Odluka stupa na snagu danom donošenja i objavljuje se u "Službenom glasniku BiH".

VM broj 60/23	Predsjedateljica
23. veljače 2023. godine	Vijeća ministara BiH
Sarajevo	**Borjana Krišto**, v. r.

SMJERNICE
O UPRAVLJANJU SIGURNOSNIM ZAKRPAMA

UVOD

Na temelju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje od 2017. do 2022. godine (u daljnjem tekstu: Politika), a sukladno Poglavlju 3. - Zakon i podzakonski akti za realiziranje Politike - Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine su zaduženi za izradu i dostavu Vijeću ministara Bosne i Hercegovine na razmatranje prijedloga zakona i dokumenata definiranih Politikom.

SVRHA

Svrha *Smjernica o upravljanju sigurnosnim zakrpama* je reguliranje procesa otklanjanja skrivenih pogrešaka operativnih sustava i programskih paketa.

Pravodobno otklanjanje postojećih pogrešaka operativnih sustava i programskih paketa sprečava moguću štetu zbog širenja virusa, crva, zlonamjernih kodova i ostalih napada na sigurnost, koji za posljedicu imaju smanjenje operativnosti, integriteta i povjerljivosti informacijskog sustava.

UPRAVLJANJE SIGURNOSNIM ZAKRPAMA

Redovito pregledavanje i pravodobna instalacija sigurnosnih zakrpa jedan je od temeljnih uvjeta za uspostavu sigurnog i pouzdanog informacijskog sustava. Sve veći broj sigurnosnih propusta unutar različitih programskih paketa i operativnih sustava predstavlja ozbiljnu prijetnju za informacijske sustave ako se ne poduzmu odgovarajuće preventivne mjere koje će omogućiti zaštitu potencijalno ranjivih sustava. Problem redovitog praćenja sigurnosnih upozorenja i instalacije pripadajućih sigurnosnih zakrpa dodatno je naglašen u većim, heterogenim okruženjima, gdje je potrebno voditi računa o velikom broju klijentskih i serverskih računara s različitim operativnim sustavima i servisima. Jedno od rješenja koje mrežnim administratorima olakšava proces pregledavanja računara te instalacije odgovarajućih zakrpa su tzv. patch management alati, kojima je temeljni cilj automatizirati i olakšati postupak upravljanja sigurnosnim zakrpama.

Administrator je odgovoran brinuti osobno ili oformiti skupinu zaduženu za upravljanje programskim zakrpama.

Zadatak upravljanja programskim zakrpama je redovita kontrola ažurnosti verzija operativnih sustava i kritičnih programskih paketa te dokumentiranje zatečenog stanja. Sukladno provedenoj kontroli, potrebno je poduzeti adekvatne mjere pomoću postojećih mehanizama za primjenu programskih zakrpa i/ili instalaciju novih verzija. Privremeno rješenje može uključivati ukidanje nepotrebnog servisa i/ili promjenu konfiguracijskih parametara.

Preporuka redovitih kontrola je svakih mjesec dana za Windows okruženje, svaka tri mjeseca za mrežne uređaje i centralne računare i/ili češće, ovisno o pokazateljima na neispravan rad nekih servisa ili dobivenim/objavljenim upozorenjima od proizvođača i odgovarajućih izvora.

Ako postoji mogućnost, poželjno je da se instalacija zakrpa provodi centralizirano – s jednog računara istodobno na sve računare informacijskog sustava. Ako ovakav način instalacije zakrpa nije moguć, potrebno je osmisliti mehanizme kojima će se osigurati instalacija zakrpa na svaki računar sustava.

Administrator prije odobrenja treba proučiti pripadajuću dokumentaciju i, po mogućnosti, testirati programsku zakrpu na izdvojenoj testnoj okolini koja je što sličnija produkcionoj okolini.

Za kritične računare (serveri i računari na kojima su instalirane aplikacije neophodne za normalni tijek poslovnih procesa) je prije same instalacije programske zakrpe potrebno napraviti sigurnosnu kopiju koja osigurava povratak na staro.

Administrator (odgovorna osoba/e) je obvezan voditi ažurnu i jedinstvenu evidenciju primijenjenih programskih zakrpa na računarima. U evidenciju se upisuju i one programske zakrpe koje se nisu mogle primijeniti na računare zbog neadekvatne verzije instaliranog softvera i/ili posebnosti instaliranih aplikacija, čija funkcionalnost, nakon primjene istih, ne bi bila moguća.

Evidencija o programskim zakrpama treba sadržavati sljedeće informacije:

- ime zakrpe,
- datum izdavanja zakrpe,
- maximum severity (critical, important)
- veličinu paketa,
- status zakrpe (Currently Approved, Not Approved, Updated, New),
- kratak opis (namjena zakrpe),
- veza na web stranicu s dodatnim informacijama o zakrpi,

- informacija o tome da li zakrpa zahtjeva ponovno pokretanje računara (reboot),
- informacija o ovisnosti o drugim zakrpama,
- lista platformi za koje je zakrpa primjenjiva.

Iako proces instalacije sigurnosnih zakrpa na prvi pogled djeluje prilično jednostavno i logično, praksa i iskustvo pokazuje da postoje brojni problemi i ograničenja koja otežavaju provedbu ovih zadataka. Kao najbolji pokazatelj može se uzeti svakodnevna pojava novih sigurnosnih incidenata koji su najčešće posljedica iskorištavanja poznatih sigurnosnih problema za koje zakrpe nisu pravodobno instalirane.

Upravljanje sigurnosnim zakrpama moguće je provesti nekom od sljedećih metoda:

- pojedinačnom instalacijom sigurnosnih zakrpa nakon što su javno objavljene,
- korištenjem specijaliziranih programa ugrađenih u sam operativni sustav ili programski paket,
- korištenjem specijaliziranih aplikacija neovisnih proizvođača.

Koji će se od navedenih pristupa koristiti ovisi o specifičnosti okruženja u kojem se sustav koristi, potrebama i raspoloživom proračunu institucije te o brojnim drugim čimbenicima.

ZAKLJUČAK

Sukladno Politici i Smjernicama o upravljanju sigurnosnim zahtjevima preporučuje se institucijama BiH da donesu svoj interni akt u kojem će definirati **pravilo/proceduru o upravljanju sigurnosnim zakrpama**.

LITERATURA

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustavi za upravljanje sigurnošću informacija – Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija

SMJERNICE
O KLASIFICIRANJU INFORMACIJSKIH RESURSA

UVOD

Na temelju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017-2022. godine (u daljnjem tekstu: Politika), a sukladno s Poglavljem 3. Zakon i podzakonski akti za realiziranje politike, Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine su zaduženi za izradu i dostavu Vijeću ministara Bosne i Hercegovine na razmatranje prijedlog zakona i dokumenata definiranih Politikom.

SVRHA

Svrha *Smjernica o klasifikaciji informacijskih resursa* je uputiti korisnike na koji način rukovati pojedinim resursom. Budući da nije moguće za svaki resurs definirati na koji način se prema njemu odnositi u smislu zaštite, nastao je pojam klasificiranja. Cilj klasificiranja je svrstati svaki resurs u pojedinu klasu ovisno o kriterijima klasificiranja. Klasa resursa jednoznačno određuje na koji način je korisnik dužan koristiti resurs, sa kolikom pažnjom i odgovornošću.

KLASIFICIRANJE IMOVINE

Vlasnik resursa dužan je prije njegova puštanja u uporabu klasificirati informaciju. Klasifikacija je postupak procjene informacije prema:

- vrijednosti,
- osjetljivosti,
- dostupnosti,
- tajnosti,
- važnosti za Instituciju,
- zakonodavnim zahtjevima.

Ovisno o izvršenoj procjeni svakoj imovini dodjeljuje se klasa. Institucija klasificira imovinu prema 3 postojeće klase:

- Javno dostupno
- Interna uporaba
- Povjerljivo

Javno dostupno

Klasa javno dostupno predstavlja podatke:

- čija je uporaba otvorena za sve korisnike,
- koji nisu tajna,
- dijeljenje i objavljivanje ovih podataka ni na koji način ne štete Instituciji,
- ne postoje zakonodavni zahtjevi za "skrivanjem" podataka.

Interna upotreba

Interna upotreba označava one podatke prema kojima se zbog zakonodavnih zahtjeva, moralnih obveza, prava privatnosti i sl. mora pažljivo i odgovorno odnositi sa ciljem zaštite podataka od neovlaštenog pristupa, modificiranja, kopiranja, prijenosa i ostalih načina zlouporabe. Podaci klasificirani kao *interna upotreba* namijenjeni su isključivo zaposlenicima Institucije koji imaju legitimno pravo pristupa ovakvim podacima.

Podaci klase interna uporaba:

- moraju biti zaštićeni od neovlaštenog pristupa,
- podaci moraju biti pohranjeni na sigurnim mjestima u smislu fizičke zaštite,
- ukoliko podaci više nisu potrebni, moraju biti uništeni prema pravilima o uklanjanju medija i brisanja informacija.

Povjerljivo

Sukladno Zakonu o zaštiti tajnih podataka ("Službeni glasnik BiH", br. 54/05 i 12/09) i podzakonskim aktima proizašlim iz Zakona.

PRAVILA KLASIFICIRANJA

Svi resursi Institucije moraju zadovoljavati sljedeće kriterije:

- vlasnik je dužan provesti klasificiranje resursa prije njegova puštanja u uporabu,
- svaki resurs (CD, DVD, papirnati dokumenti, web stranice i sl.) mora imati jasno istaknutu oznaku stupnja klasificiranja, osim ukoliko je riječ o javno dostupnim podacima,
- prije usmenog priopćavanja klasificiranih podataka drugim osobama (koje imaju pravo pristupa tim podacima) obvezno se daje prethodno upozorenje o stupnju njihove klasifikacije,
- povjerljivi podaci ne smiju se dijeliti ni na koji način (usmeno, pismeno, elektroničkim putem itd.) osobama koje nemaju pravo pristupa tim podacima,
- svaku uočenu nepravilnost (neovlašteni pristup, promjene, brisanje, dijeljenje informacija i sl.) korisnik je dužan prijaviti odgovornoj osobi,
- klasificirane podatke dobivene od treće strane potrebno je klasificirati prema pravilima klasificiranja Institucije; ukoliko ne postoji mogućnost klasifikacije prema internim pravilima, potrebno je proširiti postojeća pravila sukladno ukazanim potrebama,

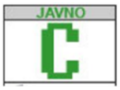
- odgovorna osoba dužna je uspostaviti metode vođenja evidencije o pristupu *povjerljivim* podacima.

KLASIFIKACIJSKE OZNAKE

Klasifikacijska oznaka pojedinog informacijskog sustava trebala bi bit jedinstvena zbog toga što u suprotnome može doći do miješanja nejednakih klasifikacijskih oznaka više informacijskih sustava.

Prijedlog klasifikacijskih oznaka Institucije:

Javno dostupno



Interna upotreba

Povjerljivo

Klasifikacijske oznake važno je što bolje označiti (npr. različitim bojama, oblicima) i istaknuti ih na uočljivim mjestima kako bi bili sigurni da su ih korisnici uočili (posebno ako je riječ o povjerljivim resursima).

ZAKLJUČAK

Sukladno s Politikom i Smjernicama o klasificiranju informacijskih resursa preporučuje se Institucijama BiH da donesu svoj interni akt u kojem će definirat **pravilo/proceduru o klasifikaciji informacijskih resursa.**

LITERATURA

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017. - 2022. godina ("Službeni glasnik BiH " broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija – Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija
4. Zakon o zaštiti tajnih podataka ("Službeni glasnik BiH", br. 54/05 i 12/09)

SMJERNICE
O INFORMATIČKOJ SIGURNOSTI RADNOG MJESTA

UVOD

Na temelju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017-2022. godine (u daljnjem tekstu: Politika), a sukladno s Poglavljem 3. Zakon i podzakonski akti za realiziranje politike, Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine su zaduženi za izradu i dostavu Vijeću ministara Bosne i Hercegovine na razmatranje prijedlog zakona i dokumenata definiranih Politikom.

SVRHA

Smjernice o informatičkoj sigurnosti radnog mjesta namijenjene su korisnicima informacijskih sustava Institucija Bosne i Hercegovine (u daljem tekstu: Institucije BiH) sa ciljem pobude svijesti o IT sigurnosti kroz obavljanje svakodnevnih zadataka na računalu, korištenju Interneta, uporabi elektroničke pošte, postupanja sa osjetljivim podacima, korištenjem aplikacija. Korisnici također moraju biti svjesni da upravo oni imaju kritičnu ulogu u održavanju uspješne informatičke sigurnosti.

RUKOVANJE ZAPORKAMA

Upravljanje sigurnošću informacionih sustava sastoji se od nekoliko komponenti od kojih svaka ima za cilj opisati razvitak, dokumentiranje i implementiranje određenih sigurnosnih procedura i kontrola kojima će ostvarivat zahtijevanu razinu zaštite. Jedan od aspekata informacijske sigurnosti kojem se ne pridaje dovoljno pažnje jest upravljanje zaporkama (engl. password management). Upravljanje zaporkama obuhvata procedure koje se odnose na razvijanje, dokumentiranje i efektivno implementiranje zaporki kako bi se osiguralo zadovoljavanje sigurnosnih zahtjeva definiranih od strane organizacijske sigurnosne politike. Problem kvalitetnog upravljanja zaporkama posebno je važan za održavanje visoke razine sigurnosti s obzirom da se kod većine Internet servisa danas upravo zaporke koriste kao temeljni način autentikacije korisnika.

Korištenje zaporki je vrlo dobro uhodan način sigurnosne kontrole, iako nedovoljno siguran. Upravljanje zaporkama za svoj prvi cilj ima definiranje preporuka po kojima se odabiru jake zaporke. Jaka zaporka definira se kao zaporka koja nije laka za otkrivanje bilo kojem programskom alatu u razumnom vremenskom razdoblju (otprilike sedam dana), koja je lako pamtljiva, koja je privatna (koristi je samo jedan korisnik) i koja je tajna. Samim isticanjem važnosti odabira zaporke, apsulutno se odbacuje mogućnost korištenja praznih zaporki (engl. null password), tj. zaporki koje uopće ne postoje, što znači da je korisnik, prilikom kreiranja zaporke, umjesto upisa zaporke pritisnuo tipku Enter. Osim odabira zaporke, aktualno je i pitanje broja zaporki koje se koriste. Ukoliko se koristi jedna zaporka za pristupe, u slučaju otkrivanja zaporke napadač ima pristup svim korisničkim resursima. U slučaju korištenja zaporke za pojedine pristupe povećana je mogućnost zaboravljanja ili njihova zapisivanja pri čemu je neizbježno lako otkrivanje zaporki. Kao kompromisno rješenje među navedenim slučajevima preporučljiv je odabir zaporki prema domenima korisničkog pristupa (elektronička pošta, aplikacije, mrežni pristup, web servisi, itd.). Pri odabiru zaporke aktualna su dva načina. Prvi način je samostalan odabir zaporke, a drugi način je korištenje programskih proizvoda za generiranje zaporki. Oba načina imaju svoje prednosti i mane.

Korisnici često smatraju kako ne moraju brinuti o sigurnosti jer njihovo računalo ne sadrži vrijedne informacije. No kompromitiranjem jednog personalnog računala u lokalnoj mreži ili jednog korisničkog računa na serveru napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dešifrovat jednostavne zaporke, dok u isto vrijeme većina korisnika ne može pamtiti složene zaporke dugačke osam znakova. Stoga je svaki korisnik dužan pridržavat se pravila korištenja zaporki, te bit svjestan da nepridržavanjem pravila nije moguća uapostava kvalitetne zaštite cjelokupnog sustava.

Pravila korištenja zaporki

Samostalan odabir zaporke je za većinu korisnika najjednostavniji način. Sigurno je da će korisnik takvu zaporku lako zapamtiti, ali je isto tako sigurno da će ona biti lako otkrivena, jer je u većini slučajeva sastavljena od osobnih podataka. Kako bi se kod korisnika promijenio ustaljeni način odabira zaporki, navedene su preporuke koje upućuju na način odabira jake zaporke koja će korisniku biti pamtljiva.

Zaporka koja će zadovoljiti prethodno navedene karakteristike da neće biti laka za otkrivanje, da je lako pamtljiva, privatna i tajna treba biti odabrana slijedom i kombinacijom ovih preporuka:

- omogućiti centralno administriranje zaporki (naprimjer putem domenskih servisa)
- minimalna dužina zaporke za korisnički nalog je 9 znakova,
- minimalna dužina zaporke za nalog sa administrativnim privilegijama je 13 znakova
- admnistrativne zaporke ne smiju bit identične na svim računalima
- treba sadržavati kombinaciju malih i velikih slova,
- treba sadržavati slova i brojeve,
- treba sadržavati minimalno jedan specijalni znak,
- treba imati minimalno četiri različita znaka (koja se ne ponavljaju),
- treba se mijenjati određenom frekvencijom,
- treba biti različita od prethodno korištene zaporke,
- treba biti lako pamtljiva samo korisniku i treba predstavljati parafrazu koja mu je lako pamtljiva.
- preporučljivo je izbjegavati afrikate
- preporučljivo je koristiti znakove/karaktere koji se nalaze na istom mjestu i na ENG tastaturi i na B/H/S tastaturi
- "Account Lockout"; zaključavanje naloga usljed pogrešno upisane zaporke treba bit uključen

Također postoje i preporuke koje upućuju na to kakva zaporka ne smije biti. To su:

- ne koristiti korisničko ime ili bilo koji njegov dio,
- ne koristiti osobne podatke (datum rođenja, JMB, itd.),
- ne koristiti prethodne zaporke ili bilo koji njihov dio,
- ne koristiti slijedna slova ili brojeve (npr. *abcdefg* ili *234567*)
- ne koristiti susjedna slova na tastaturi (npr. *asdfghjk*).

Kako bi se korisnicima olakšao odabir zaporki koje zadovoljavaju prethodno navedene stavke koriste se različite metode. Jedna od metoda je korištenje mnemotehnike. Od rečenice koja ima određeno značenje za korisnika uzmu se prva slova svake riječi koja će činiti zaporku. Ukoliko se koriste parafraze zgodno je koristiti izmislenu parafrazu iz realnog života u kojoj se pojedina slova zamjene brojevima ili specijalnim karakterima. Naprimjer: *VolimGolf2*, pretvaramo u *V0l!m6olif2* što je puno pamtljivije od $prAodR567

Administrativne zaporke moraju biti različite na računarima. Unificiranost administrativnih zaporki omogućava jednostavno širenje kripto virusa. "Account Lockout" treba uključiti (4 – 10 pogrešeno unesenih zaporki, zaključan nalog ostaje minimalno 60 minuta)

U sigurnosti informacijskih sustava nema mjesta za mit o savršenoj sigurnosti. Bitna je procjena rizika za određeni informacijski resurs te njegovo smanjivanje uvođenjem odgovarajuće sigurnosne procedure. Korištenje zaporki je, koliko jednostavan, toliko i nesiguran način sigurnosne kontrole. Iako je najrasprostranjenija metoda autentikacije, predložena su i implementirana, te se i dalje razvijaju razna druga rješenja koja će jednako jednostavno, ali sa većim stupnjem sigurnosti nuditi istu uslugu. Za korisnike na svim razinama preporučljiv je odabir zaporke koja je jaka, po samostalno odabranoj metodi te pokušaj probijanja zaporke s ciljem provjere njezine efikasnosti. Institucijama se preporučuje provođenje procesa podizanje svjesnosti korisnika te njihovo obrazovanje o sigurnosnim problemima, a preporučljivo je i uvođenje sigurnosne politike upravljanja zaporkama u kojima će biti propisan postupak odabira te čuvanja zaporki, kao i uvjeti koji omogućavaju probijanje zaporke. Takva sigurnosna politika mora se zasnivati na poslovnim procesima, identificiranim resursima, te procjenom rizika jer cilj politike nije ometati kontinuitet poslovnih procesa, već osigurati odgovarajuću razinu zaštite.

ANTIVIRUSNA ZAŠTITA

Maliciozni programi (u koje spadaju virusi, crvi, trojanski konji itd.) su svi oni programi kojima je svrha zlonamjeran učinak na računalo (računarski sistem) ili koji obavljaju akcije na računalu bez znanja (pristanka) korisnika.

Maliciozni programi svakim danom postaju sve složeniji i sofisticiraniji te ih je teže otkriti i spriječiti u izvršavanju zloćudnih aktivnosti. Antivirusne kompanije razvijaju nove, naprednije, tehnologije kako bi se uspjele nositi sa najnovijim oblicima zlonamjernih programa. Da bi se utvrdila uspješnost novih tehnologija važno je antivirusne alate redovno ispitivati i evaluirati njihov kvalitet. Da bi se izbjegli nekvalitetni testovi potrebno je postaviti standarde struke prema kojima će se svi ravnati i koje će poštivati. Upravo na ovom osjetljivom i važnom području ispitivanja antivirusnih alata takve smjernice dugo nisu postojale. To je bio jedan od glavnih razloga nastanka brojnih loše dizajniranih testova koji su korisnike često krivo informirali i tako im u biti odmagali prilikom odabira antivirusnog alata. Baš iz tih razloga stručnjaci iz struke odlučili su osnovat organizaciju AMTSO (Anti-Malware Testing Standards Organization), koja je zadužena za razvoj standarda i smjernica za ispitivanje antivirusnih alata, te podsticanje diskusija vezanih uz ovo područje. AMTSO organizacija također je zadužena za reviziju postojećih i budućih postupaka evaluacije antivirusnih alata. Ova inicijativa trebala bi u doglednoj budućnosti rezultirati kvalitetnijim testovima i realnijim pregledom mogućnosti brojnih antivirusnih alata na tržištu. Time bi u konačnici najviše trebali profitirati krajnji korisnici koji će dobivati točne informacije o proizvodima koje odabiru, što je posebno važno za podizanje globalne svjetske računarske sigurnosti na višu razinu.

Na koji način se zaštititi

Da bi računalo bilo zaštićeno od malicioznih programa, korisnik je dužan pridržavat se nekoliko bitnih i jednostavnih pravila:

- na svakom računalu mora biti instaliran antivirusni program,
- baza podataka sa informacijama o novim virusima mora biti redovito ažurirana,
- korisnik mora provodit provjere na prisustvo virusa kod svih datoteka na elektroničkim medijima nesigurnog ili neautoriziranog porijekla ili datoteka nabavljenih preko neprovjerenih mreže (uključujući Internet),
- raditi provjeru na prisustvo virusa kod svih dodataka elektroničke pošte i preuzetih datoteka,
- antivirusni program mora vršit aktivnu kontrolu web browsera u realnom vremenu, kako bi se spriječila zaraza sa web-a,
- korisnik ne smije svojevoljno isključivati antivirusnu zaštitu,
- korisnik ne smije otvarati datoteke sumnjivog sadržaja,
- u programu za pregled pošte treba isključit mogućnost automatskog otvaranja primljene pošte.

FIREWALL/VATROZID

Većina modernih operativnih sustava kao jednu od temeljnih sigurnosnih zaštita posjeduju firewall/vatrozid. Korisnik je dužan pridržavati se sljedećih pravila:

- ne smiju se mjenjati postavke firewalla/vatrozida niti isti neovlašteno isključivati,
- postavke firewalla/vatrozida se prilagođavaju poslovnom okruženju (po potrebi se otvaraju određeni portovi).

SIGURNOST RADNE OKOLINE

Da bi sigurnost radne okoline bila zadovoljena potrebno je pridržavati se "*čistog stola"*. Između ostalog korisnik je dužan pridržavati se sljedećih pravila:

- važne informacije moraju biti fizički nedostupne svim osobama koje im nemaju pristup,
- kada nije u blizini radnog mjesta korisnik mora onemogućiti pristup sadržaju računala.

UPOTREBA ELEKTRONIČKE POŠTE

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne, no njeno korištenje može ozbiljno ugroziti sigurnost informacijskog sustava.

Pod zlouporabom elektroničke pošte, odnosno e-mail-a, mogu se smatrati sljedeće aktivnosti :

- prikupljanje i krađa ličnih i poslovnih informacija drugih korisnika elektroničke pošte,
- zlouporaba podataka i propaganda u komercijalne svrhe putem elektroničke pošte,
- lažno predstavljanje i krađa identiteta putem elektroničke pošte,
- korištenje elektroničke pošte kao načina distribucije zlonamjernog softvera (raznih varijanti virusa, crva, trojanaca, keylogger-a …).

Potencijalne prijetnje i ranjivosti elektroničke pošte:

Virusi

Elektronička pošta može bit malicioznog karaktera – u dodatku je datoteka koja sadrži virus.

Nesigurnost protokola

Poruke putuju kao običan tekst te ih je lako pročitati ili izmijeniti sadržaj.

Lako je krivotvorit adresu pošiljaoca.

Nezgode

Pritiskom na pogrešnu tipku ili odabirom pogrešnog korisnika u adresaru poruka može doći neželjenom korisniku (ili više njih).

Da bi prijetnje informacijskom sustavu izazvane neprimjerenom uporabom elektroničke pošte sveli na minimum, potrebno je pridržavat se sljedećih pravila:

- elektronička pošta ne smije se koristiti za slanje uvredljivih, omalovažavajućih, seksualno uznemiravajućih i drugih poruka sličnog sadržaja,
- nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi,
- svaka napisana poruka smatra se dokumentom. Nemate pravo poruke koju su poslane korisniku osobno proslijediti dalje bez odobrenja autora,
- svaku poruku koja sadrži dodatak sumnjivog sadržaja obvezno provjeriti antivirusnim programom,
- institucija ima pravo filtriranja poruka sa namjerom da zaustavi neželjenu elektroničku poštu (eng. *spam*),
- u slučaju incidenta, institucija ima pravo pregleda svih podataka (uključujući elektroničku poštu),
- poruke koje su dio poslovnog procesa nužno je arhivirati i čuvati propisano vremensko razdoblje,
- korisnik ne smije slat masovne poruke, bez obzira na njihov sadržaj.

SOCIJALNI INŽENJERING

Postoje mnoge tehnike i ranjivosti koje zlonamjerni korisnici mogu iskoristiti za proboj informacijske sigurnosti neke institucije. Jednu od njih predstavljaju i ljudske ranjivosti, koje je moguće iskoristiti preko raznih metoda socijalnog inženjeringa. Cilj napada je dobit povjerenje žrtve kako bi se ostvarila krađa podataka ili identiteta te upad u mrežu ili sustav s namjerom narušavanja rada ili uzrokovanja štete. Socijalni inženjering ima određene specifičnosti, ali svima je zajedničko usmjeravanje na ljudski faktor sigurnosti nekog sustava.

Ove metode iskorištavaju ljudske pogreške ili slabosti kako bi se ostvarila prava pristupa sustavu bez obzira na razinu sigurnosti koju je institucija uvela. Usmjerenost na ljudske osobine poput povjerenja, želje za pomoći ili nemarnosti zasnovana je prednost ovih napada. Također, svaka osoba može postati socijalni inženjer i primijeniti neku od brojnih taktika napada. Socijalni inženjering uključuje razne tehnike, od jednostavne krađe zapisanih zaporki do stvaranja i izvođenja složenih scenarija. Jedna od najraširenijih i najpoznatijih, je izvođenje *phishing* napada. Riječ je o procesu prijevare u kojem se napadač predstavlja kao povjerljiva strana kako bi došao do osjetljivih podataka žrtve.

Cilj socijalnog inženjeringa

Temeljni cilj socijalnog inženjeringa je povećati prava pristupa sustavu ili informacijama sa mogućnošću:

- Izvođenja prijevare – dobivanje zaporki legitimnih korisnika najčešće se koristi za izvođenje prevara koje nanose novčanu štetu.
- Upada u mrežu – poznavanje osjetljivih korisničkih podataka (korisničko ime i zaporka) omogućuje prijavu na sustav sa jednakim pravima koja su dodijeljena legitimnom korisniku.
- Industrijskog špijuniranja – otkrivanje povjerljivih podataka neke organizacije moguće je iskoristiti za razne svrhe poput ostvarivanja konkurentnosti na tržištu ili prodaje ideja konkurentskim organizacijama.
- Krađe identiteta – dobivanjem korisničkih imena, zaporki ili drugih kredencijala napadač se može predstaviti kao korisnik.
- Jednostavnog narušavanja sustava ili mreže – dobivanje pristupa sustavu omogućuje napadaču nanošenje štete te izvođenje svih akcija koje su dozvoljene korisniku čije je podatke otkrio. To može uključivati brisanje, izmjenu ili pregled datoteka, umetanje lažnih podataka, blokiranje mreže, stvaranje nepotrebnih konekcija i sl.

Najčešće metode prijevare:

- **Lažno predstavljanje** – najčešća metoda napada, postupak u kojem se napadač predstavlja kao neka druga osoba,
- **Uvjeravanje/Nagovaranje** – nagovaranje ili uvjeravanje je postupak pri kojem napadač nagovara i uvjerava žrtvu da obavi postupke koje mu nalaže napadač,
- **Stvara odgovarajuće situacije** – napadač stvara "plodno tlo" za izvršenje napada na način da iskoristi žrtvine slabost; primjer takvog napada je zbližavanje sa žrtvom kako bi došao do informacija, iskorištavanje nespremnost ili nepažnju žrtve kako bi učinila pogrešan potez i sl.,

- **Moralna odgovornost** – žrtva pokuša pomoći napadaču jer osjeća da je to njena moralna obveza; žrtve nisu svjesne da na taj način odaju korisne informacije napadaču,
- **Želja za pomaganjem** – iskorištavanje želje žrtve da pomogne drugima; čest je slučaj da napadač uvjeri žrtvu da će on postupiti isto u situaciji kada žrtvi bude trebala pomoć,
- **Iskorištavanje starih veza i korupcije** – napadač stvara odnos koji je dovoljan za stjecanje povjerenja ili potkupljuje korisnika koji mu odaje željene informacije.

Načini izvršenja napada:

- **Telefonski inženjering** – jedan od najčešćih i najlakših načina izvršavanja socijalnog inženjeringa; napadač naziva npr. jednog od zaposlenika te svojim komunikacijskim vještinama lako stječe njegovo povjerenje,
- **Pretraživanje otpada** – jedan od načina sakupljanja informacija je pretraživanje otpada pri čemu se saznaje mnogo korisnih informacija za izvođenje napada,
- **Korištenjem Interneta** – brojni su načini prikupljanja informacija putem Interneta, a najčešći je slanjem lažnih poruka elektroničkom poštom. Na taj način moguće je doći do vrlo tajnih informacija kao što su zaporke i osobni podaci,
- **Zavirivanje** – tip socijalnog inženjeringa pri kojemu napadači pokušavaju očitati žrtvine pokrete kako bi dobili željene podatke. Primjer ove tehnike je gledanje pokreta ruke prilikom ukucavanja PIN-a na bankomatu ili pri upisivanju zaporke prilikom prijave na sustava,
- **Forenzička analiza** – do korisnih informacija napadač može doći pregledom nepažljivo odbačenih medija (CD, DVD, memorijske kartice, diskovi, USB memorije i sl).

Phishing

Jedna od tehnika socijalnog inženjeringa je *phishing* napad, koji se koristi kako bi se prevarilo korisnike i iskoristilo loše implementiranje i uporabu tehnologija za sigurnost web stranica. *Phishing* napad, je proces prevare u kojem se pokušavaju otkriti osjetljivi podaci (poput korisničkih imena, zaporki, brojeva kreditnih kartica i sl.) predstavljanjem kao povjerljivi entitet u elektroničkoj komunikaciji. Napadači se obično usmjeravaju na komunikaciju preko popularnih socijalnih mreža te web stranica sa aukcijama ili online naplatom. Napad se najčešće provodi preko poruka elektroničke pošte ili poruka koje se prenose u stvarnom vremenu (eng. instant messaging), a cilj je usmjeriti korisnika na lažnu web stranicu koja izgleda identično kao i originalna, legitimna stranica. Često je vrlo teško uočiti razliku između lažne i originalne stranice čak i kada se koriste napredne tehnike autentikacije korisnika.

Ukoliko napadač uspješno obavi napad i prikupi željene informacije, pruža mu se mogućnost pristupa informacijskim sustavima financijskih ustanova ili nekim drugim sustavima preko kojih može steći određenu financijsku korist.

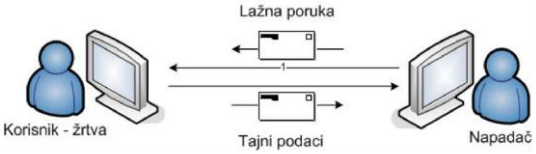
Tijek provođenja *phishing* napada moguće je podijeliti u tri faze:

- osmišljavanje i pripremanje napada,
- provođenje napada,
- prikupljanje povjerljivih informacija i njihovo iskorištavanje.

Prva faza, osmišljavanje i pripremanje napada najvažniji je dio napada. U toj fazi napadač pokušava skupiti što više informacija o žrtvi, o detaljima žrtvinog operativnog sustava i informacijskog sustava itd. Što više informacija posjeduje, napadač će sa većom vjerojatnošću uspješno obaviti napad i ostati neotkriven.

Druga faza je provođenje napada. Način provođenja napada ovisit će o prikupljenim podacima u prvoj fazi.

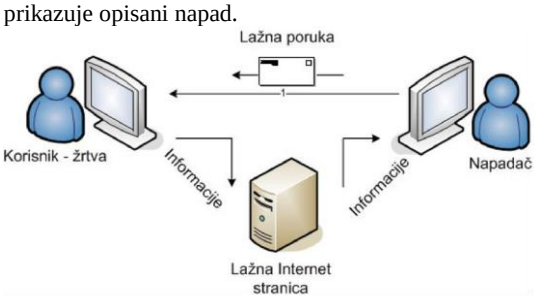
Slika 1. shematski prikazuje napad elektroničkom poštom:



Slika 1. – Primjer *phishing* napada elektroničkom poštom

Napad elektroničkom poštom realizira se tako da napadač slanjem elektroničke pošte potakne korisnika na odavanje željenih informacija. Jedan od primjera ovog napada prikazan je slikom: napadač šalje korisniku žrtvi lažnu poruku tako da se predstavi kao financijska ustanova. U poruci traži da žrtva hitno pošalje tajne podatke zbog provjere ili gubitka dijela podataka. Ukoliko korisnik ne primijeti prijevaru, šalje napadaču poruku u kojoj su sadržani tajni podaci. Napad je uspješno realiziran i napadač dolazi do željenih podataka. Ovaj napad je najjednostavniji, a realiziranje ovisi o needuciranosti korisnika žrtve. Ukoliko je žrtva naivna, vjerojatnost uspješnosti napada je relativno velika.

Druga metoda napada elektroničkom poštom je pozivanje korisnika žrtve na lažne Internet stranice. Slika 2. shmatski prikazuje opisani napad.



Slika 2. – Primjer *phishing* napada lažnom Internet stranicom

Primjer toka napada: korisnik žrtva dobiva lažirani e-mail. U poruci se poziva da zbog određenog razloga posjeti Internet stranice financijske ustanove. Iako žrtva ne sumnja u vjerodostojnost, Internet stranice navedene u poruci su lažirane. Naime, lažne stranice vrlo je teško uočiti. Izuzev sličnosti u nazivu, lažirane stranice vizualno su identične originalnim Internet stranicama, stoga korisnici ne sumnjaju u bilo kakav oblik prijevare. Cilj napadača je da se korisnik pokuša prijaviti na sustav na lažnoj Internet stranici. Ukoliko se korisnik pokuša prijaviti, vjerojatno će dobiti poruku o trenutnom nefunkcionisanju sistema. No napadaču to više nije važno. Unosom podataka od strane korisnika napadač je dobio željene podatke za pristup originalnom sustavu banke ili bilo kog drugog informacijskog sustava.

Opisani oblici napada su napadi u kojima rezultat napada ovisi o reakciji korisnika. Ostali oblici napada baziraju se na sposobnostima napadača da iskoriste propuste u komunikacijskim protokolima, operativnim sustavima, softveru, sigurnosnim kontrolama itd., te ne ovise o reakcijama korisnika.

Metode zaštite

Sigurnosna politika i standardi

Dobro dokumentirana i dostupna sigurnosna politika i standardi ključ su dobre sigurnosne strategije neke institucije. Politika treba jasno definirati svoj opseg i sadržaj za svako

područje na koje se odnosi. Zajedno sa svakom politikom potrebno je specificirati standarde koje treba uvesti kako bi se provele odredbe politike. Neki od uobičajenih dijelova sigurnosne politike u borbi protiv socijalnog inženjeringa su:

- upotreba računarskog sustava – upravljanje korištenjem sustava, upotreba hardvera i programa koji nisu u vlasništvu institucije i sl.,
- klasificiranje i rukovanje informacijama – osigurati pravilnu klasifikaciju povjerljivih informacija kako bi one bile zaštićene od neovlaštenog pristupa,
- osobna sigurnost – provjera novih zaposlenih kako bi se osiguralo da ne predstavljaju sigurnosnu prijetnju,
- fizička sigurnost – osigurati objekte znakovima, video kamerama i sigurnosnim uređajima i sl.,
- pristup informacijama – procesi za generiranje sigurnih zaporki, udaljeni pristup i sl.,
- zaštita od virusa – provesti mjere zaštite sustava od virusa i drugih zlonamjernih prijetnji,
- treninzi za podizanje svijesti zaposlenih o informacijskoj sigurnosti – informirati zaposlene o prijetnjama i mjerama,
- upravljanje usklađenošću – osiguravanje usklađenosti sa zakonima i standardima,
- politika o zaporkama – definiranje standarda za osiguravanje zaporki,
- reagovanje na incident – definiranje postupka reakcije i prijave incidenta,
- distribuiranje dokumentacije – rukovanje sa povjerljivim podacima.

Jednom definirana politika mora biti lako dostupna svim zaposlenima. Također, potrebno je provoditi stalno ažuriranje i provjeravanje sigurnosne politike kako bi se načinile nužne promjene sukladno novim odredbama ili prijetnjama.

Educiranje zaposlenih i osoblja

Kako bi sigurnosna politika bila efikasna potrebno je provesti postupke educiranja. Stvaranje svijesti o prijetnjama, ponašanju koje napadači iskorištavaju te metodologijama čini važan dio strategije zaštite od istih prijetnji. Najbolji način za postizanje toga je predstavljanjem stvarnih primjera hakiranja institucija putem metoda socijalnog inženjeringa. Postoje mnogi alati koji se mogu iskoristiti pri educiranju poput video zapisa, brošura, znakova (natpisa na radnom mjestu, displeja, podsjetnika i dr.) i slično. Programi educiranja imaju ulogu:

- upoznavanja zaposlenih sa sigurnosnom politikom,
- stvaranje svijesti o rizicima i mogućim gubicima,
- treniranja sa ciljem prepoznavanja tehnika socijalnog inženjeringa.

Znači, nije dovoljno zaposlenim ukazati što i kako, činiti nego ih je potrebno upoznati sa posljedicama koje donose prijetnje socijalnog inženjeringa. Budući da educiranje zaposlenih o rizicima socijalnog inženjeringa predstavlja jednu od temeljnih metoda zaštite, to je vrlo zahtjevan zadatak. Dobar program obuke mora biti raznovrstan što znači da je potrebno iskoristiti svaku mogućnost i alat kako bi se postiglo povećanje svijesti i razumijevanje prijetnja koje donose socijalni inženjeri.

Drugi postupci zaštite

Jedan od ključnih postupaka zaštite od socijalnog inženjeringa je pravilno upravljanje zaporkama. Organizacija mora imati jedinstveni identifikator za svakog zaposlenika koji će biti povezan sa pravima pristupa tog zaposlenika. Znači, identifikatorom se zaposlenom određuju prava pristupa informacijama na sustavu. U tome se vidi prednost korištenja posebnog identifikatora za svakog zaposlenog. U slučaju da napadač sazna identifikator nekog korisnika, on ima pravo pristupa samo onim informacijama koje su dodijeljene tom korisniku dok su ostali dijelovi sustava zaštićeni. Definiranje operativnih postupaka također ima važnu ulogu u zaštiti institucije od napada socijalnih inženjera. Pri tome se prvenstveno misli na procedure povezane sa odobravanjem pristupa i izdavanjem dozvola. Takvi postupci zahtijevaju višestruku provjeru točnosti i vjerodostojnosti podataka. Osnovna svrha je smanjiti rizike napada oponašanjem zaposlenih.

Zaštita običnih korisnika

Svaki korisnik Interneta može provesti određene mjere zaštite od napada socijalnim inženjeringom poput:

- upoznavanja sa vrijednostima podataka – napadači se obično usmjeravaju na korisnička imena i zaporke te brojeve kreditnih kartica pa je potrebno posebno oprezno rukovanje sa tim podacima,
- provjeravanja identiteta sagovornika – socijalni inženjeri obično se usmjeravaju na stjecanje povjerenja korisnika uvjeravajući ih kako se radi o njima poznatim osobama, suradnicima, nadležnim osobama, vladinim službenicima i sl.,
- zadržavanja zaporki tajnim – zaporke treba čuvati u tajnosti te izbjegavati njihovo zapisivanje ili dijeljenje sa drugim osobama,
- provjeravanja poruka elektroničke pošte – provjeriti izvor poruke, provesti skeniranje antivirusnim alatom i sl.,
- izbjegavanja upisivanja zaporki u nesigurne stranice – provjeriti valjanost web stranica prije upisa zaporke preko URL niza i drugih indikatora sigurnosti,
- ne otkrivanja puno informacija o sebi – saznavanjem informacija o nekom korisniku socijalni inženjer se može fokusirati na njegove navike i hobije kako bi ga naveo na posjećivanje lažnih web stranica,
- korištenja *anti-phishing* zaštite – postoje alati koji provjeravaju poruke elektroničke pošte kako bi otkrili izraze koji su karakteristični za *phishing* poruke.

SIGURNOST MEDIJA

Mediji su resursi institucija koji služe za pohranu podataka. Kao takvi igraju veliku ulogu u sigurnosti. Dolaskom do medija na kojem su pohranjeni povjerljivi podaci ili podaci za internu upotrebu, napadaču mogu biti otvorena vrata za obavljanje zlonamjernih radnji.

Pitanje trajnosti zapisa na medijima najznačajnije je pitanje kada se govori o životnom vijeku podataka. Međutim, jednako je važno i pitanje smisla dugog čuvanja zapisa na tehnologijama današnjice. Činjenica je da tehnologija iznimno brzo napreduje i za očekivati je značajne promjene u bližoj budućnosti na svim poljima pa tako i na polju pohrane podataka. Sukladno s tim, može se uočiti da na medije za pohranu trajnost podataka nije jedini uvjet, važnije je odrediti ispravna i funkcionalna pravila koja će se primjenjivati kod pohranjivanja podataka.

Potreba za povećanjem kapaciteta uređaja, odnosno medija za pohranu podataka je neupitna pa je vrlo lako formulirat predviđanja za budućnost vezana uz kapacitete – očekuje se nastavak rasta kapaciteta, a pri tome smanjivanje veličine medija i samih uređaja. Također, realno je očekivati i povećanja brzine prenosa podataka.

Osnovne karakteristike uređaja za pohranu podataka su sljedeće:

- kapacitet,
- brzina prijenosa podataka i

- prosječno vrijeme pristupa.

Poželjne karakteristike su:

- postojanost podataka,
- jednostavno rukovanje i male dimenzije te
- pristupačnost cijene.

Uređaji koji zadovoljavaju date karakteristike zasnivaju se na magnetnoj i optičkoj tehnologiji.

Kapacitet

Kapacitet uređaja za pohranu mjeri se u oktetima (bajtima) – iz čega slijede sledeće jedinice:

- B – bajti (okteti)
- KB – kilobajti
- MB – megabajti
- GB – gigabajti
- TB – terabajti

Na primjer, 1 KB iznosi 1024 B. Iako nije potpuno ispravno, radi jednostavnosti ove mjere često se zaokružuju na 1000, npr. 1 MB se poistovjećuje s 1000 KB, odnosno 1 000 000 B, pri čemu relativna greška iznosi oko 5%.

Prosječno vrijeme pristupa

Radi se o vremenu potrebnom da upravljačka jedinica pristupi podatku na datoj adresi na mediju. Mjeri se u milisekundama pri čemu je manje bolje.

Uprkos visokoj pouzdanosti današnjih medija i uređaja za pohranu podataka, poznata preporuka korisnicima i dalje vrijedi: vaši podaci su onoliko dobri koliko je dobar vaš posljednji *backup*.

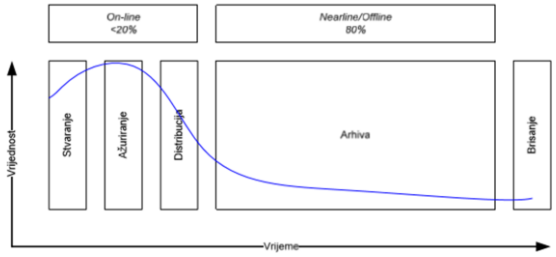
Pravilnik o sigurnosti medija treba definirati da:

- svi mediji moraju biti pohranjeni na sigurnom i zaštićenom mjestu,
- svi mediji moraju biti čuvani prema specifikacijama proizvođača,
- mediji sa povjerljivim podacima ne smiju se davati na korištenje neovlaštenim korisnicima,
- svako dijeljenje medija sa povjerljivim podacima mora biti dokumentirano,
- potrebno je tražiti ovlaštenje za uklanjanje medija iz institucije te se mora sačiniti zapisnik o takvim aktivnostima,
- ako više nisu potrebni, treba obrisati prijašnje sadržaje svakog ponovno iskoristivog medija koji će biti uklonjen iz institucije,
- svi prijenosni mediji bazirani na flash-memoriju (USB-stikovi) i prenosni tvrdi diskovi moraju biti kriptovani dostupnim softverskim alatima kako bi bili nedostupni trećim osobama u slučaju da budu izgubljeni/ukradeni,
- svi službeni "pametni" uređaji (smartphone/tablet) moraju biti kriptovani odgovarajućim alatima koje osigurava proizvođač uređaja.

Upravljanje životnim ciklusom podataka i informacija

Među podacima razlikuju se aktivni i neaktivni podaci, odnosno informacije. Životni ciklus podataka počinje njihovim prikupljanjem. Aktivni podaci označavaju podatke koji se upotrebljavaju svakodnevno u uobičajenim poslovnim procesima korisnika. S vremenom ti podaci gube svoju važnost. Učestalost pristupa opada uz postupno gubljenje poslovne vrijednosti pa informacije svoj životni vijek konačno završavaju arhiviranjem ili njihovim odlaganjem.

Aktivni podaci nose poslovnu korist instituciji, poduzeću, odnosno korisniku. Svaki uspješan i efikasan poslovni proces zahtjeva jednostavan i neometan pristup aktivnim podacima. Upravljanje podacima zasniva se na vrlo jednostavnom načelu: prenosu podatka iz sloja u sloj kroz vrijeme, prema prikazu na slici 1.



Slika 3. Vremenski tijek podataka

Razumijevanjem načina na koji se podaci prenose, odnosno zadržavaju u pojedinom sloju korisnici razvijaju strategije i obrasce korištenja kako bi optimizirali upotrebu medija za pohranu. Na taj se način optimizira ukupna cijena spremanja podataka tokom njihovog životnog ciklusa.

Sličan, ali složeniji, pristup primjenjuje se kod pohrane podataka u relacionu bazu podataka (eng. *Relational Database*). Kompleksnost u ovom slučaju povećava inherentna međuovisnost podataka. Relacione baze podataka jedni su od čestih i velikih korisnika prostora za pohranu podataka, a ujedno su, zbog prirode korištenja, jedan od najsloženijih mehanizama pristupa podacima. Složenost upravljanja relacionim bazama podataka čini upravo ta međuovisnost podataka. Zbog toga je vrlo važno razviti efikasne mehanizme upravljanja kako baza ne bi izašla van granica nadzora. U protivnom bi svaki dohvat podataka iz baze postajao sve skuplji što bi u konačnici rezultiralo lošim performansama čitavog sustava.

Nakon što podaci više nisu potrebni za poslovni proces korisnika, oni postaju **neaktivni**. Ipak, to ne znači da su i nepotrebni te da ih se može izbrisati sa medija na kojemu su pohranjeni. Pojam upravljanje životnim ciklusom podataka (eng. *DLM - Data Life Cycle Management*) odnosi se na koordiniranje prolaskom informacija kroz informacijski sustav; od njihovog nastanka i inicijalne pohrane sve do trenutka kada isti podaci postaju nepotrebni i slijedi im brisanje. Ovakvi sustavi automatiziraju procese uključene u upravljanje podacima, a radi se o organizaciji podataka u međusobno odvojene slojeve zasnovanoj na unaprijed određenim pravilima (eng. Policy), te automatizaciji prenosa podataka iz jednog sloja u drugi, zasnovanoj također na uspostavljenim pravilima. Primjer pravila može se ilustrirati situacijom kada se podaci kojima se češće pristupa spremaju na skuplje, ali i brže medije, dok se podaci s manjim značajem spremaju na jeftinije i sporije medije.

Izraz upravljanje životnim ciklusom informacija (eng. ILM – Information Life Cycle Management) nije isti upravljanju ciklusom podataka, iako se nerijetko ta dva pojma koriste ravnopravno. Osustavi orjentirani na podatke koriste atribute datoteka (vrstu, veličinu, datum nastanka, uređivanja i sl.) za dohvat podataka na zahtjev korisnika. Sustavi zasnovani na upravljanju informacijama uveliko su složeniji i omogućavaju pretragu, odnosno dohvat podataka korištenjem složenih upita poput konkretnih vrijednosti pojedinih parametara spremljenih u datotekama.

Hijerarhijsko upravljanje pohranom podataka (eng. HSM – Hierarchical Storage Management) jedan je od mogućih načina upravljanja podacima. Radi se o tehnici koja omogućuje automatski prenos podataka između medija različitog cjenovnog ranga. Razlog potrebi za takvim upravljanjem je prvenstveno u cijeni uređaja za pohranu. Očito je kako bi najjednostavnije i najefikasnije rješenje bilo korištenje uređaja

visokih performansi. Ipak, cijena je ta koja uslovljava korištenje uređaja lošijih karakteristika. Nakon uspostave konačnog skupa pravila o prenosu podataka između različitih korištenih uređaja, odgovornost za ispravno funkcioniranje preuzima HSM sustav nadzirući način korištenja podataka i pravilnim raspoređivanjem podataka.

Uklanjanje medija

Svrha pravilnika o uklanjanju medija je smanjiti rizik od "curenja" osjetljivih informacija koje može nastati nepravilnim odbacivanjem medija ukoliko medij više nije potreban. Kako bi se rizik "curenja" sveo na minimum potrebno je uspostaviti formalne smjernice za sigurno uklanjanje medija.

Sve medije kvalificirane kao osjetljive, koji više nisu za upotrebu, potrebno je ukloniti tako da niko ni na koji način nije u mogućnosti doći do podataka (ili dijela podataka) pohranjenih na mediju, papirnate i optičke medije potrebno je ukloniti pomoću aparata za uklanjanje medija, USB i ostale memorije potrebno je ukloniti prema pravilima proizvođača ili fizičkim djelovanjem na medij, ostale medije potrebno je ukloniti fizičkim djelovanjem, posebnim uređajima ili na treći način prema preporukama stručnjaka.

Lista dokumenata koji mogu zahtijevati sigurno uklanjanje:

- optički mediji (CD, DVD..),
- prenosni tvrdi diskovi
- USB memorije,
- papirnati dokumenti,
- snimljeni glas,
- indigo papir,
- traka za printer,
- sustavska dokumentacija itd.

Osim definiranja smjernica, važno je naglasiti da je uklanjanje osjetljivih medija treba biti provjereno i dokumentirano.

ZAKLJUČAK

Sukladno s Politikom i Smjernicama o informatičkoj sigurnosti radnog mjesta preporučuje se Institucijama BiH da donesu svoje interne akte u kojima će definirati:

- **Pravila/procedure o korištenju antivirusne zaštite,**
- **Pravila/procedure o upotrebi elektroničke pošte,**
- **Pravila/procedure o metodama zaštite,**
- **Pravila/procedure o sigurnosti medija.**

LITERATURA

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za period 2017. -2022. godina ("Službeni glasnik BiH " broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sistemi za upravljanje sigurnošću informacija – Zahtjevi
3. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija

SMJERNICE
O UPRAVLJANJU SIGURNOSNIM INCIDENTIMA

UVOD

Na temelju Politike upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine (u daljnjem tekstu: Politika), a sukladno Poglavlju 3. - Zakon i podzakonski akti za realiziranje Politike - Ministarstvo komunikacija i prometa Bosne i Hercegovine i Ministarstvo sigurnosti Bosne i Hercegovine su zaduženi za izradu i dostavu Vijeću ministara Bosne i Hercegovine na razmatranje prijedlog zakona i dokumenata definiranih Politikom.

SVRHA

Smjernice o upravljanju sigurnosnim incidentima namijenjene su korisnicima računarskih sustava u institucijama Bosne i Hercegovine (u daljnjem tekstu: institucije BiH) u svrhu upravljanja sigurnosnim incidentima na sustavima koje koriste, ako do njih dođe. Bez obzira na sve veća sredstva i napore koji se ulažu u postizanje i održavanje sigurnosti informacijskih sustava, sigurnosni incidenti i dalje su česta pojava. Svaki sigurnosni incident, bez obzira na veličinu i trajanje, za instituciju predstavlja gubitak, zbog čega je vrlo važno da se adekvatna pozornost posveti razvoju strategije i planiranju aktivnosti u slučaju pojave sigurnosnih incidenata.

Incident se može definirati kao svaki događaj koji nije standardna operacija usluge, a može prouzrokovati ili uzrokuje prekide ili smanjenje kvaliteta IT usluge. Cilj procesa upravljanja incidentima je omogućiti korisniku što je prije moguće povrat do normalne razine usluga s najmanjim mogućim utjecajima na poslovanje. Proces upravljanja incidentima mora identificirati i snimati nastale incidente, budući da je to važno za mjerenje i kontrolu kvalitete procesa, ali i za identifikaciju uzroka incidenata te poduzimanje korektivnih mjera i daljnjih poboljšanja.

Računarski sigurnosni incidenti su česta pojava u moderno doba. Računarski sigurnosni incident je posredno ili neposredno ugrožavanje sigurnosne politike, pravila i procedura. Razvoj tehnologije i računarske znanosti omogućio je i razvoj novih metoda napada i ugrožavanja računarskih sustava i mreža. Kako bi se ograničilo djelovanje zlonamjernih napadača potrebno je uspostaviti postupak za rješavanje sigurnosnih incidenata. Odgovor na sigurnosne incidente postao je važan dio informacijske tehnologije, a sigurnosne prijetnje brojne i raznovrsne, ali, što je najvažnije, i sve razornije (npr. napad uskraćivanja usluga može napadnutoj instituciji stvoriti velike financijske troškove). Aktivnosti za sprečavanje sigurnosnih prijetnji utemeljene na rezultatima procjene rizika (npr. primjena sigurnosne metrike) mogu smanjiti broj incidenata, ali ne mogu spriječiti sve incidente. Institucija treba imati sposobnost rješavanja sigurnosnog incidenta u smislu ljudstva i primjene sigurnosnih mjera zaštite. Za potrebe odgovora na sigurnosne incidente osnivaju se posebne skupine za njihovo rješavanje. One su potrebne za brzo otkrivanje incidenata i saniranje štete nastale sigurnosnim incidentom.

AKTIVNOSTI U PROCESU UPRAVLJANJA INCIDENTIMA

Aktivnosti u procesu upravljanja incidentima su:

- identifikacija i zapis incidenata: incidenti se identificiraju, detektiraju i zapisuju,
- incident se klasificira i daje se početna potpora za njegovo rješavanje,
- uspoređivanje (usklađivanje) incidenata: traži se kompatibilnost s već poznatim incidentima radi lakšeg rješavanja postojećeg incidenta, a zatim se provjerava mogućnost korištenja već postojeće solucije za incident,
- istraživanje i dijagnoza: ako je incident nepoznat, potrebno je detaljnije istraživanje i dodjela kompetentnije skupine za potporu,
- rješavanje incidenta i zatvaranje: nakon zatvaranja incidenta, incident slog (zapis) mora biti potpuno ažuriran (navedena kategorija i prioritet, usluga/korisnik na koje se negativno odrazio incident, konfiguracijski detalji identificirani kao uzroci incidenta),

- praćenje incidenata: komunikacija s korisnicima o statusu incidenata.

Kritični čimbenici uspjeha za proces upravljanja incidentima su:

- procjena incidenta s aspekta utjecaja na posao i potrebi vremenskog rješavanja,
- baza znanja u potpori prepoznavanja incidenata i njihovog rješavanja,
- adekvatni automatski sustavi za zapis i praćenje incidenata,
- dobra povezanost s procesom upravljanja stupnjem usluga koja će utjecati na prioritete i vrijeme rješavanja incidenata.

Indikatori performansi za proces upravljanja incidentima su:

- ukupan broj incidenata,
- prosječno vrijeme rješavanja incidenata,
- % incidenata riješenih unutar SLA ciljeva,
- % incidenata riješen prvom linijom potpore,
- prosječni troškovi podrške po incidentu,
- % incidenata s početnom korektnom klasifikacijom,
- % incidenata u korektno realiziranom ciklusu aktivnosti.

U svrhu kvalitetnog ustrojstva upravljanja sigurnosnim incidentima potrebno je definirati:

- odgovornosti i uloge,
- potencijalno opasne radnje,
- procedure u slučaju incidenta,
- procedure za pravodobnu detekciju,
- procedure za analizu incidenta i uklanjanje posljedica,
- procedure za vraćanje sustava u inicijalno stanje.

Upravljanje sigurnosnim incidentima važan je segment poslovanja svake institucije. Ako se unaprijed definiraju zaštitne mjere i koraci u slučaju pojave incidenta, znatno se mogu umanjiti gubici i utjecaj incidenta na poslovanje institucije.

DEFINIRANJE ODGOVORNOSTI I ULOGA

Glavna odgovorna osoba dužna je inicirati provedbu politike upravljanja sigurnosnim incidentima. Odgovornost u instituciji i provedbi politike može imati jedna osoba, ali i više njih. Važno je da hijerarhija odgovornosti bude jasno definirana i dokumentirana.

Inicijalnu odgovornost nad upravljanjem sigurnosnim incidentima ima glavna odgovorna osoba. Glavna odgovorna osoba odgovornost ili dio odgovornosti može prenijeti na drugu osobu/osobe, uz obvezno jasno definiranje i dokumentiranje odgovornosti.

PRAVODOBNA DETEKCIJA

Kako bi se potencijalne prijetnje i incidenti pravodobno detektirali, potrebno je osposobiti sljedeće mehanizme:

- softversko praćenje dnevnika zapisa s mogućnošću alarmiranja kod detekcije potencijalno opasnih radnji (DDoS napadi, *brute force* napadi, uporaba resursa informacijskog sustava za slanje neželjene pošte itd.),
- periodički pregled dnevnika zapisa odgovorne osobe s ciljem uočavanja potencijalno opasnih radnji koje softver nije detektirao,
- pregled prijava korisnika o incidentima korisnika,
- pregled prijava korisnika o ranjivostima sustava.

Odgovorne osobe koje pregledavaju prijave korisnika dužne su voditi evidenciju primljenih zahtjeva i akcija koje su poduzete. Dnevnik, između ostalog, mora sadržavati sljedeće podatke:

- kada je napravljena prijava korisnika,
- kada je odgovorna osoba pregledala prijavu,
- zapis prijave,
- koje su akcije poduzete u vezi s prijavom,
- da li je opasnost otklonjena ili ne.

KAKO REAGIRATI U SLUČAJU INCIDENTA

U slučaju incidenta odgovorna osoba dužna je reagirati tako da spriječi daljnje činjenje zlonamjernih radnji i pokuša prikupiti dodatne informacije o napadu (dokazni materijal), lokaciji s koje je kazneno djelo izvršeno, vremenu izvršenja itd.

Ako odgovorna osoba primijeti ili dobije prijavu korisnika o potencijalnoj ranjivosti sustava, dužna je učiniti sljedeće:

- napraviti evidenciju zahtjeva na isti način kao kod prijema prijave o incidentu,
- inicirati rješenje problema tako da obavijesti vlasnika resursa o propustu,
- u evidenciju dodati tko je odgovoran, datum i vrijeme kada je primio obavijest o ranjivosti i kada je ranjivost uklonjena,
- obavijestiti Tim za odgovor na računarske incidente (CERT) za institucije Bosne i Hercegovine i slijediti obvezujuće mjere i standarde za upravljanje sigurnosnim računarskim incidentima koje propisuje CERT za institucije Bosne i Hercegovine.

ANALIZA INCIDENTA I UKLANJANJE POSLJEDICA

Nakon obavljanja inicijalnih procedura u slučaju incidenta i nakon što je napad (opasnost) prošao, potrebno je napraviti analizu stanja kako bi se utvrdilo šta je sve obuhvaćeno incidentom i šta je njegov cilj.

Neki od mogućih ciljeva napada su:

- iskorištavanje sustava za obavljanje zlonamjernih radnji (slanje neželjene elektroničke pošte, izvršavanje napada odbijanja usluge itd.),
- napadi na sustav odbijanja usluge, *brute force* napadi,
- krađa resursa,
- mijenjanje resursa,
- uništavanje resursa itd.

Bitan dio rješavanja incidenta su učenje i poboljšavanje. Svaka institucija BiH treba učiti na riješenim incidentima kako bi mogla što bolje djelovati u budućnosti koja donosi nove prijetnje i profinjenije napade. Pitanja na koja treba dati odgovore prilikom analize nastalog incidenta su:

- Šta se točno dogodilo i u koje vrijeme?
- Koliko su dobro osoblje i menadžment izveli svoj zadatak i nosili se s incidentom?
- Jesu li procedure dokumentirane i jesu li bile odgovarajuće?
- Koje je informacije trebalo doznati ranije?
- Jesu li poduzeti svi koraci ili akcije koje mogu usporiti oporavak?
- Šta bi osoblje i menadžment učinili drugačije idući put kada se dogodi sličan incident?
- Koje je mjere potrebno poduzeti za sprečavanje sličnih incidenata u budućnosti?
- Koji su dodatni resursi i alati potrebni za otkrivanje, analizu i ublažavanje posljedica budućih incidenata?

Za male incidente nije potrebno obavljati opsežne analize, osim onih incidenata kod kojih su korištene nove metode napada kako bi se slični napadi brže i učinkovitije sanirali u budućnosti. Analiza riješenog sigurnosnog incidenta dobar je materijal za obnavljanje sigurnosnih politika i procedura za suzbijanje sigurnosnih incidenata.

Kritični čimbenici uspjeha su:

- dobro definirane aktivnosti, ciljevi, odgovornosti i ostali resursi dokumentirane procedure,
- dobra koordinacija između procesa upravljanja incidentima i procesa upravljanja problemima budući da su podaci o incidentu (kategorija incidenta, prioritet, status, konfiguracijski detalji, korisnik i usluga čija je isporuka spriječena) važni za definiranje, istraživanje problema i traženje uzroka u cilju njegove eliminacije.

Indikatori performansi su:

- smanjen broj incidenata upravljanjem i rješavanjem problema,
- smanjeno vrijeme za rješavanje problema,
- smanjenje troškova potrebnih za eliminiranje poremećaja u isporuci IT usluga.

Predviđanje budućnosti u industrijskoj grani kao što je računarska tehnologija gotovo je nemoguć zadatak. Samo kratki pogled u prošlost otkriva koliko je situacija postala ozbiljna. Računarski kriminal toliko je uznapredovao da je važnost provedbe najosnovnijih sigurnosnih mjera veća nego ikada. Proteklo razdoblje obilježilo je značajno povećanje sigurnosnih prijetnji na webu te iskorištavanje ranjivosti novih tehnologija (web 2.0, mobilni telefoni nove generacije…). Iako je poprilično nezahvalno detaljnije predviđati razvoj događaja na sceni računarskog kriminala, stručnjaci se slažu o sljedećem:

- raznovrsnost napada i njihova učestalost nastavit će svoj rast eksponencijalnom brzinom, vođeni željom napadača za provaljivanje u tuđe računarske sustave zbog krađe identiteta, resursa ili osjetljivih informacija,
- curenje podataka postat će sve veći problem, prvenstveno zbog sve većeg korištenja mobilnih tehnologija u poslovnim okruženjima,
- kompromitirani personalni računari i dalje će, kao dio *botnet* mreža, biti glavni izvor spam poruka elektroničke pošte. Botnet mreže novim načinom komuniciranja, putem P2P mreža, vješto izbjegavaju otkrivanje,
- zlonamjerne poruke će u budućnosti sadržavati sve više raširenih vrsta dokumenata poput PDF i DOC datoteka za koje napadači svakodnevno pronalaze nove ranjivosti.

Kako internet postaje svakodnevnica i u životu običnih ljudi a ne samo informatičkih stručnjaka, očekuje se da će i napadači i dalje svoje aktivnosti usmjeriti najviše na "mrežu svih mreža" - internet. Kako bi se sigurnosni incidenti smanjili na najmanju moguću razinu važno je konstantno educirati korisnike računara kako bi koristili što više sigurnosnih mjera i time učinili svoj računar, ali i računar drugih korisnika, sigurnijim. Upravno je ljudski čimbenik uzrok mnogim sigurnosnim incidentima, ali naša sposobnost da učimo i mijenjamo svoje ponašanje predstavlja područje s najvećim mogućnostima za razvoj i napredak globalne računarske sigurnosti.

ZAKLJUČAK

Sukladno Odluci o određivanju Tima za odgovor na računarske incidente za institucije Bosne i Hercegovine, Politici i Smjernicama o upravljanju sigurnosnim incidentima preporučuje se institucijama BiH da donesu svoje interne akte u kojima će definirati:

- **pravila/procedure kako prijaviti sigurnosni incident i potencijalne ranjivosti sustava,**
- **pravila/procedure o načinu sprečavanja daljnjih zlonamjernih radnji,**
- **pravila/procedure o načinu na koji se mogu prikupiti dodatni dokazni materijali koji su izazvali incident,**
- **pravila/procedure za vraćanje sustava u inicijalno stanje nakon saniranog incidenta.**

Institucije BiH su u obvezi slijediti obvezujuće mjere i standarde za upravljanje sigurnosnim računarskim incidentima koje propisuje Tim za odgovor na računarske incidente (CERT) za institucije Bosne i Hercegovine.

LITERATURA:

1. Odluka o određivanju Tima za odgovor na računarske incidente za institucije Bosne i Hercegovine ("Službeni glasnik BiH", broj 25/17)
2. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za razdoblje 2017-2022. godine ("Službeni glasnik BiH", broj 38/17)
3. Standard ISO/IEC 27001 - Sigurnosne tehnike - Sustavi za upravljanje sigurnošću informacija – Zahtjevi
4. Standard ISO/IEC 27002 - Sigurnosne tehnike - Pravilo dobre prakse za kontrole sigurnosti informacija

346

На основу члана 30. став (1) тачка г) и став (2) и члана 37. став (1) Закона о платама и накнадама у институцијама Босне и Херцеговине ("Службени гласник БиХ", бр. 50/08, 35/09, 75/09, 32/12, 42/12, 50/12, 32/13, 87/13, 75/15, 88/15, 16/16, 94/16, 72/17, 25/18, 32/20, 65/20 и 59/22), члана 50. става 4. тачка м) Закона о раду у институцијама Босне и Херцеговине ("Службени гласник БиХ", бр. 26/04, 7/05, 48/05, 60/10, 32/13 и 93/17) и члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08), на приједлог Министарства финансија и трезора Босне и Херцеговине, Савјет министара Босне и Херцеговине, на другом дијелу 5. сједнице одржане 15.3.2023. године, донио је

ОДЛУКУ
О ИЗМЈЕНАМА И ДОПУНИ ОДЛУКЕ О НАЧИНУ И ПОСТУПКУ ОСТВАРИВАЊА ПРАВА ЗАПОСЛЕНИХ У ИНСТИТУЦИЈАМА БОСНЕ И ХЕРЦЕГОВИНЕ НА ТРОШКОВЕ СМЈЕШТАЈА, НАКНАДУ ЗА ОДВОЈЕНИ ЖИВОТ И НАКНАДУ ЗА ПРИВРЕМЕНО РАСПОРЕЂИВАЊЕ

Члан 1.

У Одлуци о начину и поступку остваривања права запослених у институцијама Босне и Херцеговине на трошкове смјештаја, накнаду за одвојени живот и накнаду за привремено распоређивање ("Службени гласник БиХ", бр. 42/12, 78/12, 51/13, 68/18 и 79/22) у члану 3. став (1) тачка б) износ од: "300,00 КМ" замјењује се ријечима: "60% основице за обрачун плате запосленим у институцијама Босне и Херцеговине која се примјењује у мјесецу за који се врши обрачун накнаде."

У тачки ц) износ од: "250,00 КМ" замјењује се ријечима: "50% основице за обрачун плате запосленим у институцијама Босне и Херцеговине која се примјењује у мјесецу за који се врши обрачун накнаде."

У тачки д) износ од: "150,00 КМ" замјењује се ријечима: "30% основице за обрачун плате запосленим у институцијама Босне и Херцеговине која се примјењује у мјесецу за који се врши обрачун накнаде."