

KORPORACIJSKA ISTRAGA KOMPJUTERSKOG KRIMINALA SA IMPLEMENTACIJOM SIGURNOSNE POLITIKE

Msc. Vladan Nikačević, dipl. inž.
Vojska Srbije
vladan.milnik@gmail.com

Izvod: Kompjuterski kriminal, iz godine u godinu, postaje sve sofisticiraniji i efikasniji. Napadi su sve više usmereniji prema korporacijama, a sve sa ciljem pribavljanja osetljivih podataka.

U ovom radu se, na bazi usvojenih modela istrage kompjuterskog kriminala na mrežnim uređajima, definišu postupci i metodi utvrđivanja validnih digitalnih dokaza na mrežnim uređajima, od strane tima za upravljanje kompjuterskim incidentom.

Izvršena je eksperimentalna verifikacija primene forenzičkih tehnika i alata na scenariju napada na ruter. Na osnovu analize modela istrage kompjuterskog kriminala i eksperimentalnih rezultata predložena je sigurnosna politika korporacije sa skupom relevantnih pravila, sa ciljem sprečavanja (smanjenja) posledica kompjuterskog kriminala, trajnog oporavka od napada i olakšanja korporacijske forenzičke istrage računara i računarskih mreža.

Ključne reči: analiza, mrežni uređaj, log datoteka, kompjuterski incident, politike.

UVOD

Krađa osetljivih podataka i dalje je glavni uzrok nastajanja kompjuterskih incidenata u korporacijama.

Sigurnosni incidenti se sve češće događaju od strane zaposlenih u korporaciji, što ukazuje da je potrebno uvesti niz efikasnih i jasno određenih pravila koja će osigurati i zaštititi materijalne i intelektualne vrednosti organizacije od krađe i uništavanja.

Prilikom istrage kompjuterskog kriminala na računarskim mrežama, u toku prikupljanja, analize i prezentacije digitalnih dokaza moraju se poštovati određeni principi. Najbolja forenzička praksa dokazala je da je najbolje formirati tim sačinjen od profesionalaca: zvaničnog organa istrage, tužioca, eksperta u oblasti informaciono komunikacionog sistema, eksperta u oblasti računarskih mreža, digitalnog forenzičara i dr. po potrebi. U slučaju kompjuterskog kriminala česta je praksa da se zahteva ekspertsko svedočenje ili veštačenje.

U ovom radu predmet istraživanja je pronalaženje digitalnih dokaza na mrežnim uređajima koji se koriste u korporacijama u cilju forenzičke akvizije na računarskim mrežama i izrada sigurnosne politike za korporaciju sa težištem na rešavanju kompjuterskih incidentata i digitalnu forenzičku istragu kompjuterskog kriminala..

Uvođenje sigurnosne politike može biti skup i dugotrajan proces u kojem je potrebno prilagoditi sve delove organizacije da rade sinhronizovano. Korporacijama i institucijama se preporučuje uvođenje sigurnosne politike radi podizanja nivoa sigurnosti kako informacionog sistema, tako i njihovih korisnika.

1. PROCES KORPORACIJSKE ISTRAGE

Korporacijska istraga se može smatrati predistražnim postupkom zvanične istrage kompjuterskog kriminala.

„Odvija se u tri faze:

- pokretanje istrage,
- određivanje karaktera kompjuterskog incidenta i
- analiza prikupljenih digitalnih podataka.“¹

Praksa je pokazala da se efikasni rezultati dobijaju izvršavanjem 6 *Rosenblattovih* koraka:

- eliminisanje očiglednosti,
- postavljanje hipoteze o napadu,
- rekonstruisanje krivičnog dela,
- otkrivanje traga do osumnjičenog računara,
- analiza izvornog, ciljnog i posrednog računara i
- prikupljanje dokaza,

nakon čega predati nalaze i dokazne materijale korporacijskim ili zvaničnim organima istrage za dalji postupak.

Rekonstrukcija traga napada predstavlja čitanje log datoteka na celom putu napada, pri čemu se javljaju sledeći problemi:

- log datoteke su izmenjene, ne postoje ili su neadekvatne,
- isprekidana zaustavljanja između izvora napada i računara žrtve,
- uskraćena saradnja administratora posrednih računara,
- lažiranje IP adresa,
- izmenjeni log datoteka napadnutog računara ili primenjeni drugi trikovi za maskiranje neovlašćenog pristupa,
- samo jedan neovlašćeni pokušaj pristupa.

Prikupljanje dokaza i predavanje dokaznog materijala korporacijskim ili zvaničnim organima istrage, vrši se isključivo po odobrenju vlasnika napadnutog sistema i odluci korporacije.

2. SIGURNOSNA POLITIKA

Skup jasno definisanih pravila koja obuhvataju sva područja na kojima je moguće izvršiti neku vrstu napada naziva se sigurnosnom politikom. Sigurnosnom politikom jasno se određuju pravila

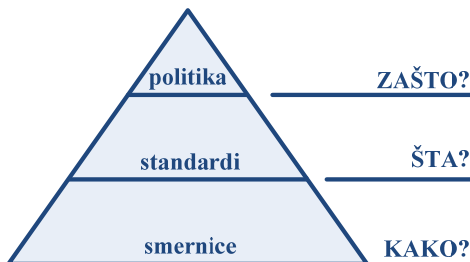
¹ Milosavljević M., Grubor G. „Istraga kompjuterskog kriminala“, Beograd, 2009, str. 37

ponašanja i odgovornosti vezane uz informacijski sistem kako bi se minimizovala šteta nastala namernim ili nenamernim delovanjem.

Sigurnosna politika korporacije ili institucije prilagođava se potrebama i nije jednaka za sve.

Standard je obavezni postupak ili pravilo koje je izrađeno kako bi učinilo politiku delotvornom, a mora uključivati jedan ili više tehničkih opisa za komponente računara, programe i njihovo rukovanje.

Smernice su uopštene izjave, preporuke ili administrativna uputstva koja daju okvirna uputstva za sprovođenje sigurnosne politike konstruisane kako bi se ostvarili ciljevi sigurnosne politike.

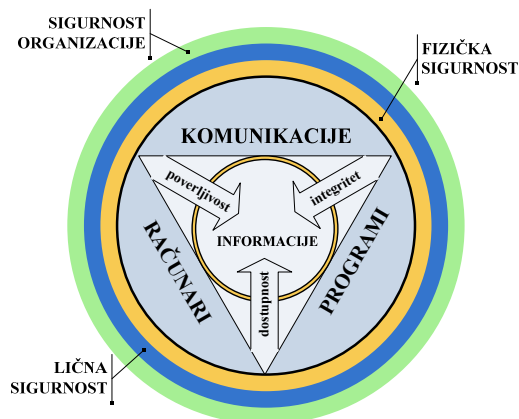


Slika 2.1. Prikaz uklapanja smernica, standarda i sigurnosne politike

Uspostavom sigurnosne politike korisnicima su nametnuta obavezujuća pravila ponašanja koja ograničavaju slobodu pri pregledu poverljivih informacija, kao i pravila za ispravno korišćenje računarske opreme koja je korisniku data na korišćenje.

Sigurnosnom politikom osiguravaju se tri svojstva informacija koje sadrži neki sistem (Slika 2.2.):

- poverljivost (*confidentiality*),
- integritet (*integrity*) i
- dostupnost (*availability*).



Slika 2.2. Sigurnosne informacione komponente

Da bi se zadovoljili propisani standardi sigurnosti informacijski sistemi se dele na tri glavna dela:

- računarsku opremu,
- programe i
- komunikacije.

Mehanizmi zaštite i sprečavanja su podeljeni na tri osnovna nivoa:

- fizička sigurnost, pod kojom se smatra sigurnost računarske opreme i podataka,
- lična sigurnost je zaštita korisnika i poverljivih informacija o korisniku i
- sigurnost organizacije, koja zavisi od prva dva nivoa.

3. SIGURNOSNI STANDARDI

Standardi iz ISO/IEC 27000 serije korporacijama pružaju smernice za konstruisanje, primenu i proveru informacionih sistema čime se osigurava poverljivost, integritet i dostupnost informacionog sadržaja, sistema i procesa unutar organizacije.

Za područje sigurnosti informacionih sistema najčešće se koriste dva standarda:

- ISO/IEC 27001 i
- ISO/IEC 27002 (pre 2007. godine poznat kao ISO/IEC 17799:2005).

ISO/IEC 27001

ISO/IEC 27001² je službeni skup specifikacija na bazi kojih korporacije imaju pravo zatražiti postupak sertifikacije, ukoliko su primenile taj standard na sistem upravljanja sigurnošću informacija. Ovaj standard propisuje zahteve za uspostavljanje, sprovođenje, nadgledanje, ispitivanje, održavanje i poboljšanje sistema za upravljanje sigurnošću informacija.

Standard se sastoji od 5 delova:

1. Sistem za zaštitu informacija,
2. Odgovornost rukovodećih ljudi,
3. Unutrašnje provere sistema za zaštitu informacija,
4. Provera valjanosti sistema za zaštitu informacija i
5. Poboljšanja na sistemu za zaštitu informacija.

ISO/IEC 27002 (ISO/IEC 17799)

ISO/IEC 27001 standard definiše koje zahteve neki sistem za zaštitu informacija mora imati, pa za primerene provere navodi upotrebu ISO/IEC 27002 standarda. ISO/IEC 27002³ je službeni standard, ali se tumači kao skup smernica koje je moguće upotrebiti.

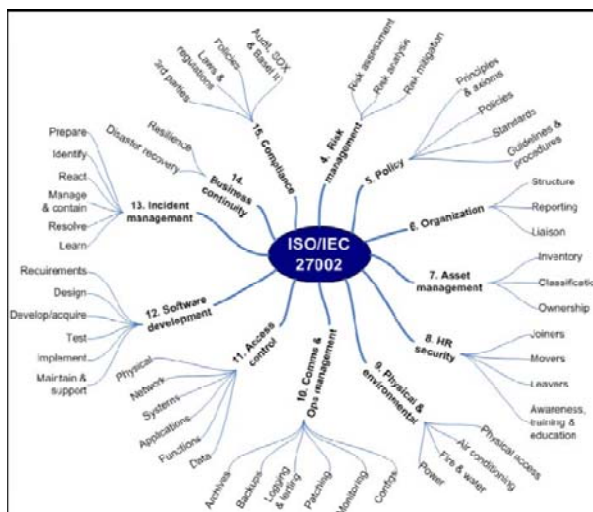
Standard sadrži 39 ciljeva i sastoji se od 12 delova:

1. Procena rizika,
2. Sigurnosna politika,
3. Organizacija informacione sigurnosti,
4. Upravljanje imovinom,
5. Zaštita od zaposlenih,
6. Fizička zaštita i zaštita od okoline,
7. Upravljanje komunikacijama i operacijama,
8. Provera pristupa,
9. Nabavka, razvoj i održavanje informacionih sistema,
10. Upravljanje incidentima u informacionom sistemu,
11. Upravljanje poslovnim kontinuitetom i

² www.iso27001security.com/html/27001.html, februar 2010

³ www.iso27001security.com/html/27002.html, februar 2010

12. Usklađivanje.



Slika 3.1. Prikaz strukture ISO/IEC 27002 standarda

4. EKSPERIMENTALNI REZULTATI

Uz saglasnost sa administratorom mreže lokalnog internet servis provajdera izvršen je eksperiment na bežičnom ruteru, baziran na Linux operativnom sistemu, Mikrotik verzija 2.9.

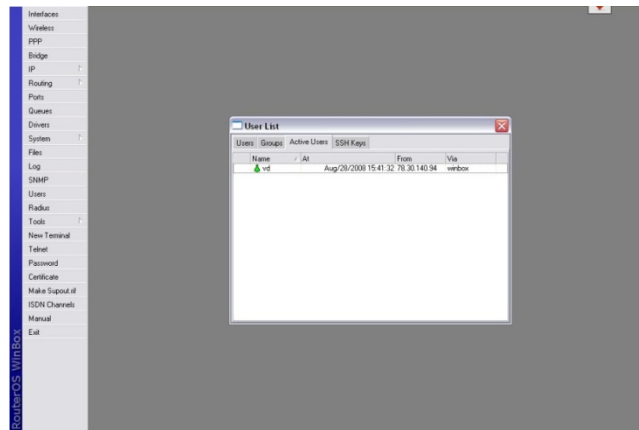
Bežični korisnici se priključuju na ruter biranjem SSID provajdera, kojim putem DHCP servisa dodeljuje IP adrese. Internet servis, korisnici dobijaju putem zaštićene VPN konekcije. Prilikom eksperimenta, podaci sa rutera su snimljeni „na živo“, tj. dok je ruter u radu.

Scenario:

Napadač je “upao” u korisnički kompjuter koji je priključen na bežični internet. Korisnik putem bežične mreže i VPN konekcije ostvaruje internet saobraćaj.

Eksperimentom su prikupljeni sledeći podaci:

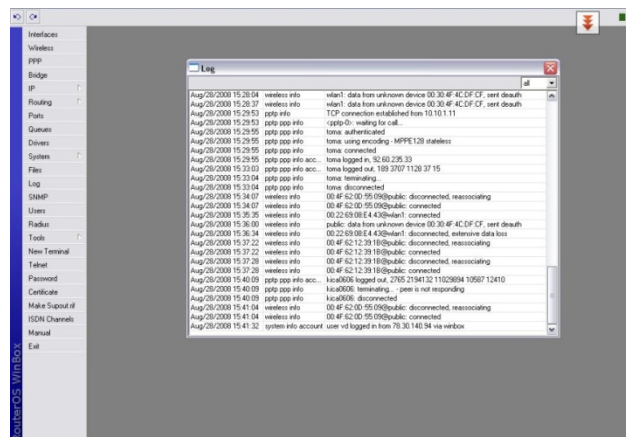
- prikaz aktivnog korisnika (vd) koji je pristupio ruteru, korišćenjem programa “winbox”, sa datumom i vremenom pristupa. Aktivni korisnik se može priključiti na ruter putem bežične ili žične mreže. Datum i vreme pristupa su prema podešavanjima na ruteru te se prilikom forenzičke analize, moraju konsultovati.



Slika 4.1. Prikaz aktivnog korisnika

Podatak je bitan za administriranje rutera. Ukoliko je neko pristupio ruteru, u zavisnosti od vrste naloga (admin, user i dr.), može vršiti izmene konfiguracionih podataka na ruteru. Ukoliko nema prava izmena, može vršiti pregled podataka i time sakupiti informacije o korisnicima ili o konfiguraciji mreže, koje može upotrebiti za sledeće korake u napadu.

- prikaz aktivnosti bežičnih korisnika, konektovanje na bežičnu mrežu i na VPN uz prikaz MAC adrese korisnika,



Slika 4.2. Prikaz log datoteke

Analiza napada:

Analizom log datoteke, koja se nalazi na ruteru, mogu se videti korisnici u bežičnoj mreži, sa svojim MAC adresama sa vremenom konektovanja na mrežu.

Napad iz scenaria je mogao izvršiti:

- interni korisnik koji je priključen na isti ruter ili
- napadač preko Interneta

Analizom log datoteke može se utvrditi da li je napadnuti korisnik u trenutku napada bio korisnik Internet servisa. Info poruka (*pptp pptp info*) daje informaciju o tome koji se korisnik mreže

konektovao na zaštićenu VPN konekciju.

Ukoliko se u log datoteci, analizom info poruka utvrdi da korisnik nije koristio Internet servisa, istraga se sužava na lokalne korisnike na ruteru.

Log datoteke rutera se mogu analizirati na samom ruteru, a najbolje je kada se log datoteke šalju i skladište na izdvojenoj lokaciji na posebnom računaru.

Prilikom logovanja događaja i saobraćaja upotrebljavaju se filteri, te se tako samo bitni elementi loguju. Naravno, takvi logovi ne daju potpune informacije o svim događajima na ruteru, obavljenom saobraćaju, kao i odbačenim paketima usled postavljenih pravila logičkih (mrežnih) barijera.

Mogu se koristiti i specijalizovani programi za pregled log datoteka, kao što je *PyFlag*, za bržu i lakšu akviziciju.

- trenutni pregled saobraćaja koji ostvaruje VPN korisnik sa prikazanim izvornim i odredišnim IP adresama

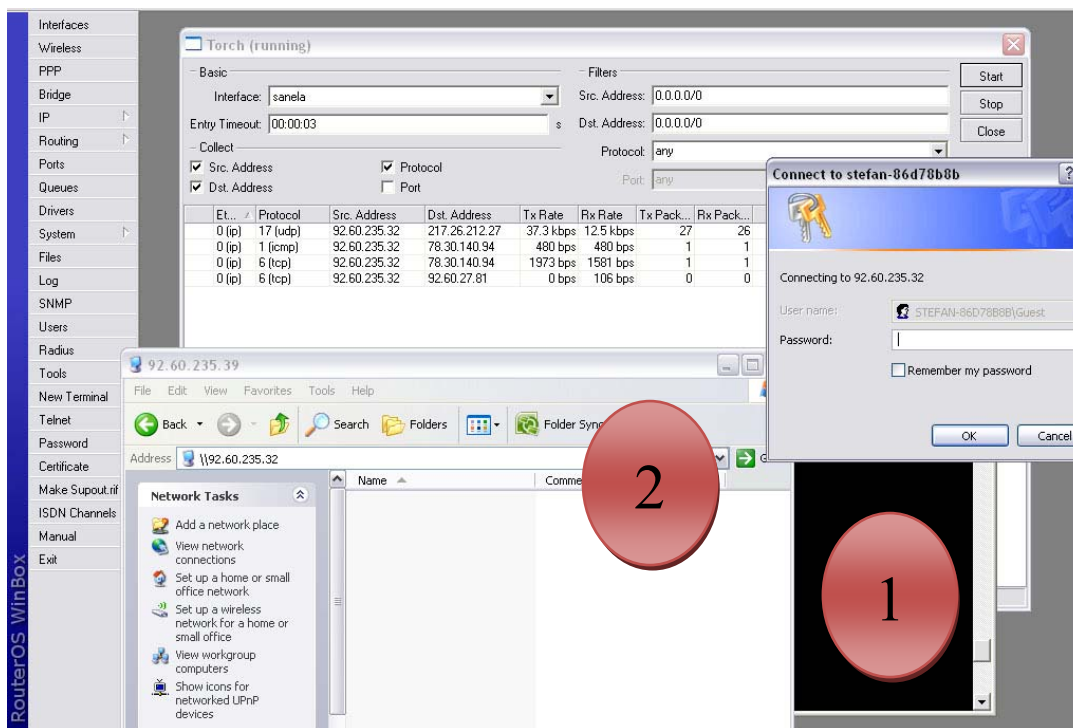
Src. Address	Dst. Address	Tx Rate	Rx Rate	Tx Pack.	Rx Pack.
92.60.225.30	79.116.54.174	0 bps	256 bps	0	0
92.60.225.30	92.60.225.237	600 bps	0 bps	1	0
92.60.225.30	24.147.22.195	0 bps	128 bps	0	0
92.60.225.30	89.164.168.81	0 bps	128 bps	0	0
92.60.225.30	91.136.44.9	200 bps	256 bps	0	0
92.60.225.30	78.145.62.38	0 bps	128 bps	0	0
92.60.225.30	94.0.120.105	300 bps	256 bps	0	0
92.60.225.30	93.139.79.37	296 bps	128 bps	0	0
92.60.225.30	62.223.191.62	280 bps	128 bps	0	0
92.60.225.30	79.119.93.111	560 bps	354 bps	0	0
92.60.225.30	92.60.238.35	560 bps	354 bps	0	0
92.60.225.30	84.232.176.161	280 bps	0 bps	0	0
92.60.225.30	89.172.14.139	280 bps	0 bps	0	0
92.60.225.30	173.21.41.243	560 bps	354 bps	0	0
92.60.225.30	89.143.191.131	280 bps	0 bps	0	0
92.60.225.30	89.142.152.42	300 bps	0 bps	0	0
92.60.225.30	213.89.216.143	304 bps	0 bps	0	0
92.60.225.30	95.63.127.164	540 bps	340 bps	0	0
92.60.225.30	189.95.63.122	280 bps	0 bps	0	0
92.60.225.30	90.40.76.103	0 bps	152 bps	0	0

Total Tx: 9.0 kbps Total Rx: 4.4 kbps Total Tx Packet: 6 Total Rx Packet: 3

Slika 4.3. Pregled saobraćaja korisnika

Prikazuje se trenutni saobraćaj koji korisnik ostvaruje. Uključeni su filteri za IP adrese, a može se analizirati saobraćaj i po protokolu i portu.

- analizom saobraćaja na priključku otkriven je napadač koji je pokušao “upad” u računar



Slika 4.4. Otkrivanje napadača

Napad “upada” u kompjuter simuliran je sa računara sa IP adresom 78.30.140.94, na taj način što je ka računaru sa IP adresom 92.60.235.32, VPN korisnik “*sanela*”, pušten stalni ping (označen brojem 1) i otvaranje deljenih foldera na računaru (označen brojem 2).

Na ruteru, analizom saobraćaja koji ostvaruje korisnik “*sanela*” nedvosmisleno se utvrđuje:

- destinaciona adresa 78.30.140.94 (sa napadnutog računara), protokol 1 (icmp), predajni i primljeni paketi, po 1. Ovaj podatak se odnosi na aktivnu komandu ping sa napadačevog računara, broj 1. i
- ista destinaciona adresa, protokol 6 (tcp), predajni i primljeni paket po 1. Ovaj podatak je usled otvaranja deljenih foldera na računarima, broj 2.

Eksperimentom je potvrđeno da se u saradnji sa administratorom mreže i pristupom ruteru, može utvrditi ilegalna aktivnost napadača, koja se odnosi na određene napade, a može se ogledati kroz:

- neovlašćeni pristup ruteru,
- krađu sesije,
- povećanog protoka u saobraćaju i drugi napadi prikazani u pristupnom radu.

5. PREDLOG SIGURNOSNE POLITIKE RAČUNARSKE MREŽE

Zašto sigurnosna politika?

Kao odgovor na porast kompjuterskih incidenata, primenjuje se kompjuterska forenzika, koja sadrži tehnike za otkrivanja i prikupljanja informacija o kompjuterskim incidentima, na takav način da budu prihvatljivi na sudu.

Primenom kompjuterske forenzike na kompjuterski incident se deluje preventivno sa ciljem sprečavanja incidenata i poboljšanja oporavka od učinjenog napada.

Bilo koja korporacija ili institucija koja koristi računare i računarske mreže treba da ima uspostavljene mere bezbednosti i sposobnost za sprovođenje forenzičkih aktivnosti.

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definiše sigurnosna politika važe za:

- Svu računarsku opremu (kao i pripadajuće programe), koja se nalazi u prostorima Korporacije,
- Administratore informacionih sistema,
- Davaoce usluge, zaposleni u Odseku za informatiku koji obezbeđuju potrebne servise Korporaciji,
- Korisnike, u koje spadaju: zaposleni, spoljni saradnici i članovi Korporacije i
- Spoljne institucije koje po ugovoru rade na održavanju opreme ili softvera.

Specijalisti za sigurnost

Kako bi se osiguralo upravljanje sigurnošću, potrebno je oformiti je Tim za upravljanje kompjuterskim incidentom. Direktor Korporacije imenuje menadžera sigurnosti čija je prvenstvena briga sigurnost informacionih sistema.

Sastav tima za upravljanje bezbednosnim kompjuterskim incidentima:

- menadžer zaštite informacija,
- administrator računarskog sistema i mreža,
- specijalisti za upravljanje i kontrolu bezbednosnog rizika,
- kontrolor sistema kvaliteta,
- predstavnici drugih timova (za vanredne događaje, usaglašenost standarda i sl.),
- digitalni forenzičar,
- pravnik korporacije,
- menadžer za upravljanje ljudskim resursima.

Postupci za rešavanje incidenata dati su u pratećem dokumentu pod nazivom Pravilnik o rešavanju sigurnosnih incidenata.

Tim sagledava celokupno stanje u korporaciji sa aspekta kompjuterskog incidenta i predlaže mere za preventivno delovanje na incident, uključujući nabavku opreme, organizaciju obrazovanja korisnika i specijalista.

Menadžer tima daje odobrenje za sprovođenje istrage u slučajevima incidenata.

Po učinjenom kompjuterskom incidentu i završenoj forenzičkoj istrazi, tim podnosi izveštaj upravi Korporacije sa predlogom mera da li se podnosi krivična prijava i protiv koga ili ne. Takođe u izveštaju se navodi koji su podaci ukradeni, oštećeni i da li su oporavljeni.

U skladu sa mogućnostima, korporacija može oformiti tim za hitne intervencije, obučenu za postupanje u slučaju incidentnih situacija, koju čine specijalisti različitih usmerenja, na primer za mreže, Unix, Microsoft Windows, baze podataka itd. U tom slučaju razrađuju se procedure za postupanje u incidentnim situacijama, i obučavaju se članovi ekipe kako bi mogli izvršiti istragu i što pre vratiti informacioni sistem u redovno stanje.

Obuka tima za upravljanje kompjuterskim incidentima

Procedure za istragu kompjuterskog incidenta koje slede napad treba da budu pažljivo sprovedene i u tome tim treba da bude uvežban, a naročito lica koja se bave računarima i računarskim mrežama.

Tokom istrage, tim utvrđuje da li se napad dogodio, a ako je moguće identifikovati kompjuterski incident kako je učinjen, ko je učinio i naći dokaze koje je ostavio. Da bi se navedene radnje sprovele, tim treba da razume učinjene korake napadača da bi mogao da ga prati.

Tim mora znati gde je moguće naći dokaze. Od ključne je važnosti da digitalni forenzičar bude ekspert za kompjutersku i mrežnu administraciju. Potrebno je da završi obuku u hakerskim tehnikama i da se poznaje generičke ranjivosti sistema.

Digitalni forenzičar mora da bude dobro verziran u prikupljanju dokaza. Mnoge klasične tehnike prikupljanja dokaza se ne mogu koristiti na računaru forenzičara zbog prirode kompjutera i informacionih sistema. Glavna karakteristika je brza promena stanja. Na primer, datoteka dnevnika može biti promenjena stotinu puta dnevno.

Da bi bila upotrebljiva na sudu, forenzičar mora nesumnjivo pokazati, kroz sve ispravke, da je dnevnička datoteka validna i da predstavlja:

- sadržaj koje se odnosi na incident i
- da nije neovlašćeno prikupljena.

Nadzor nad informacionim sistemima

Korporacija zadržava pravo nadzora nad instaliranim softverom, podacima koji su sačuvani na umreženim računarima i nad načinom korišćenja računara.

Nadzor se sme sprovoditi radi:

- Osiguranja integriteta, poverljivosti i dostupnosti informacija i resursa,
- Sprovođenja istrage u slučaju sumnje da se dogodio sigurnosni incident i
- Provere da li su informacioni sistemi i njihovo korišćenje usklađeni sa zahtevima sigurnosne politike.

Nadzor obavljaju samo osobe iz sastava tima za upravljanje kompjuterskim incidentima. U slučajevima kada je zaposleni prekršio pravila sigurnosne politike, ne može se više osigurati poverljivost informacija otkrivenih u istrazi, pa se one mogu koristiti u sudskom postupku.

Sprovođenje

Korisnici su dužni pomoći osobama iz tima za upravljanje kompjuterskim incidentima, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi sprovođenja nadzora.

Reference:

- Standard ISO/IEC 27001 i
- Standard ISO/IEC 27002

PRAVILNIK O REŠAVANJU SIGURNOSNIH INCIDENATA

Svrha

Svrha ovog dokumenta je da se ustanovi obaveza prijavljivanja problema prilikom rada sa računarskom opremom. Prosečan korisnik nemože znati da li je njegov računar žrtva sigurnosnih incidenata.

Svaki problem sa računarskom opremom treba biti prijavljen, a tehničko osoblje Odseka za informatiku, vrši opravku, podešavanje opreme i dr. U slučaju sumnje na sigurnosni incident prijavljuje timu za upravljanje kompjuterskim incidentima.

Sigurnosne incidente rešava tim za upravljanje kompjuterskim incidentima sprovodeći tehnike kompjuterske i mrežne forenzike koje se koriste da otkriju digitalne dokaze u raznim kompjuterskim zločinima kao što su krađe poslovne tajne i uopšte zloupotreba računa i računarskih mreža u cilju zaštite intelektualne svojine.

Prijava incidenta

Svaki zaposleni, korisnik ili saradnik Korporacije dužan je prijaviti:

- usporeni rad računara,
- usporeni ili onemogućeni pristup mrežnom servisu,
- nemogućnost pristupa, gubitka ili neovlašćene izmene datoteke,
- pojave virusa ili nepoznatih ikonica na računaru,
- sumnju da se događa kompjuterski incident.

Tim za upravljanje kompjuterskim incidentima izrađuje i ažurira listu kontakt osoba kojima se prijavljuju problemi u radu računara i servisa i obrazac za prijavu incidenta. Lista se deli svim zaposlenima i objavljuje se na internim web stranicama Korporacije.

Svaki incident se dokumentuje. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac sa opisom incidenta i preduzetih mera pri rešavanju problema.

Procedure i uputstva za rešavanje incidenata

Prilikom primena forenzičkih akcija tim za upravljanje kompjuterskim incidentima sprovodi sledeće procedure:

- informacioni sistem sačuvati u zatečenom stanju, odnosno ne činiti izmene koje bi otežale ili onemogućile dijagnostifikovanje,
- pravljenje dve kopije oštećenog hard diska, korišćenjem alata za kreiranje slike diska,
- dokumentovanje svake radnje, tako da se ponavljanjem zabeleženih akcija može rekonstruisati tok istrage,
- o istrazi se sačinjava izveštaj, kako bi u slučaju potrebe mogli poslužiti kao dokaz u eventualnim krivičnim ili sudskim procesima,
- izveštaji o oncidentu smatraju se poverljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlašćene osobe.

Tim za upravljanje kompjuterskim incidentima ima ovlašćenja:

- praćenje svih korisničkih procesa na računaru i izlistavanja sadržaja korisničkog direktorijuma, ako sumnja da se računar koristi na nedozvoljen način,

- pristupa svakoj datoteci u računarskom sistemu korporacije i
- pristupa sistemski uskladištenih podataka na serveru i rezervnih kopija podataka lokalnih korisnika,

bez dozvole zaposlenog kome je računarska oprema data na upotrebu, koji je kreirao datoteku ili napravio rezervnu kopiju podataka i ne smatraju se napadom na privatnost.

Podaci mogu biti upotrebljeni i na sudu.

Korporacija može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja poverljivih i personalnih informacija.

Obuka

Svi zaposleni se moraju obučiti za primenu procedura odgovora na kompjuterski incident.

Tim za upravljanje kompjuterskim incidentima planiraće simulaciju incidenta i testirati postupak u realnim situacijama.

Po završetku testa upoznati sve zaposlene sa iskustvima.

Sankcije

Svrha istrage je da se odredi uzrok nastanka problema i da se iz toga izvuku zaključci o tome kako sprečiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bila greška čoveka, protiv odgovornih se mogu preduzeti sankcije.

Korporacija može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.

Ukoliko je incident izazvao zaposleni spoljne firme, korporacija može zatražiti od nje da ga ukloni sa liste osoba ovlašćenih za obavljanje posla u Korporaciji.

U slučaju teže povrede pravila sigurnosne politike korporacija može pokrenuti krivični postupak.

PRAVILNIK ZA DIGITALNU FORENZIČKU ISTRAGU KOMPJUTERSKOG INCIDENTA

Svrha

U postojanju napora da se obezbede kompjuterski sistemi u sprečavanju incidenata, forenzičke tehnike su potrebne da se otkriju počinioci i da se omogući povratak imovine ili prihoda izgubljenih u incidentu.

Krajnji cilj računarske forenzike je da se obezbedi dovoljno dokaza da bi se otkriveni kompjuterski incident uspešno procesuirao.

Taksonomija kompjuterskog napada

Hakerski napadi dolaze od različitih izvora i od različitog nivoa umeća rada sa kompjuterima, od početnika do kompjuterskog eksperta. Najčešći koraci u izvođenju napada su:

- Upornost – predstavlja napadačevo prepoznavanje žrtve. U ovom koraku, napadač kreira profil organizacione strukture, mrežne mogućnosti, komponente mreža i sigurnosne mere. U trajanju ove faze napadač pronalazi svoje željene ciljeve i smišlja plan za zaobilazanje bezbednosnih mehanizama,
- Penetracija - je sledeći korak u napadu. Njom se obezbeđuje dovoljno podataka da bi se pristupilo meti i ciljanom sistemu. Na primer, ako sistem ima konfiguracionu grešku, i pristup FTP serveru preko protokla TFTP, do pristupa sistema, tada se napad razvija u pravcu korišćenja slabosti u protokolu TFTP,
- Sticanje ovlašćenja - cilj ovog koraka je da se iskoriste konfiguracione greške i propusti za sticanje dodatnih privilegija, kao što je pribavljanje administratorskog naloga,
- Delovanje - kada dobije dovoljan nivo ovlašćenja, napadač ispoljava cilj u vršenju nedozvoljenih radnji. Koristi ih za instalaciju trojanaca, zapisivanja lozinki, brisanja datoteka, ili bilo koje zlonamerno ponašanje koje ima na umu,
- Prikriivanje tragova - pre povlačenja, napadač pokušava da prikrije svoje tragove, brisanjem ili sakrivanjem datoteka koje je ostavio za sobom.

Ispitivanje ovih koraka daje vredne informacije u pronalaženju načina da se zaustavi napad. Oni takođe, pružaju uvid u stvari koje se mogu uraditi za poboljšanje sposobnosti hvatanje napadača koji je probio bezbednosni mehanizam.

Kompjuterska i mrežna forenzika

Srž delatnosti kompjuterske i mrežne forenzike je prikupljanje dokaza, koji se akumuliraju iz različitih komponenti sistema i služe za pronalaženje tragova o kompjuterskom incidentu. Informacija ne postaje dokaz dok incident nije potvrđen. Iz tog razloga, podaci se prikupljaju sa sistema kao potencijalni dokazi.

Postoji mnogo potencijalnih izvora dokaza u računarima i mrežnim komponentama.

Datoteke su očigledan izvor potencijalnih dokaza. Aplikativna dokumenta word, excel, itd. su skoro uvek dragoceni potencijalni dokazi, kao i skrivene aplikacione datoteke koje sadrže informacije o istoriji, kešu, bekapu i log datoteka u kojima su upisane promene i događaji na računaru.

Pošto prikupljanje potencijalnih dokaza i pronalaženje aplikacionih datoteka na kompjuteru, nije lako, zahteva se angažovanje stručnjaka koji su posebno obučeni u neophodnim veštinama za uspešno obavljanje forenzičke istage. Forenzički stručnjak mora da ima istražiteljske veštine detektiva, pravne veštine advokata i kompjuterske veštine hakera. Čak i sa ovim veštinama, digitalna forenzika ne garantuje da će forenzički stručnjak naći dovoljno dokaza. Međutim, iskusni forenzički stručnjaci mogu naći više potencijalnih dokaza nego što najbolji haker očekuje.

Za razliku od klasičnog forenzičkog ciklusa, gde forenzička aktivnost počinje posle učinjenog dela ili kasnije, pošto je delo otkriveno, u digitalnoj forenzici računarskih mreža, forenzičke aktivnosti prikupljanja potencijalnih dokaza počinju pre nego što je kompjuterski incident učinjen. Po učinjenom incident digitalna forenzika se odnosi na analizu dokaza koji su već prikupljeni.

Pravila za sprovođenje kompjuterske i mrežne forenzike

- U korporaciji vršiti sistematsko skladištenje i zadržavanje sadržaja aplikacija i korisničkih datoteka kao potencijalne dokaze, po sledećem:
 - na serveru, za korisnike koji su priključeni na domensku računarsku mrežu, prilikom svakog odjavljivanja sa računarske mreže vršenjem sinhronizacije i
 - na lokalnim računarima, koji nisu priključeni na računarsku mrežu, pravljenjem rezervnih kopija podataka, u skladu sa Pravilnikom o izradi kopija podataka.
- Obrisane, skrivene i šifrovane datoteke, koje se nalaze na računarima su vlasništvo korporacije,
- Tim za upravljanje kompjuterskim incidentima ima prava pristupa svakoj datoteci u sistemu bez dozvole onoga koji je datoteku kreirao,
- Korisničke računare konfigurisati na taj način da se vrši praćenje i evidencija sistemskih, aplikacionih i mrežnih informacija, u vidu dnevnčkih (log) datoteka,
- Mrežne uređaje konfigurisati tako da se log datoteke šalju na centralni log server. Oni uređaji koji ne omogućavaju slanje log datoteka, periodično, preuzimati datoteke i skladištiti na centralni log server,
- Sistemska vremena na mrežnim uređajima koja imaju tu mogućnost, podesiti po centralnom log serveru,
- Pratiti sledeće mrežne aktivnosti:
 - prijavljivanje i odjavljivanje računara sa domenske računarske mreže,
 - pristup mrežnim servisima (daljinski Telnet, FTP sesija),
 - internet servisi (e-mail i web pristup),
 - za bežične korisnike, prijavljivanje na pristupnu tačku i dr.
- Obezbediti pravljenje vremenske linije, prikupljanjem informacija na navedene načine i informacijama dobijenih od svedoka i fizičkih dokaza,
- Vršiti analizu TCP/IP paketa i njegovog zaglavlja koji sadrži informacije o izvornom i ciljnom računaru. IP adrese pružaju informacije o identitetu napadača i meti unutar računarske mreže korporacije,
- Prilikom konfigurisanja rutera i mrežnih barijera, sve odbačene pakete, koji nisu u skladu sa pravilima, preusmeriti na sigurno mesto i voditi evidenciju o njima,
- Konsultovati tehničku dokumentaciju, pisane instrukcije i priručnike o računarskoj opremi i specifičnim programima.

Planiranje odgovora na kompjuterski incident

Iako se politikom dešinišu pravila i uputstva za prikupljanje potencijalnih dokaza, usled oklevanja ili neuspeha u otkrivanju dokaza, može se izazvati veća šteta nego da se dogodio kompjuterski incident. Takođe, može se izgubiti prilika da se otkrije počinioc i povrati nastala šteta.

Digitalna forenzika zahteva efikasan Plan odgovora na napad, da se odgovori, ko, šta, kada i gde.

Uspostavljanje tima za upravljanje bezbednosnim kompjuterskim incidentima

U glavom tekstu predloga sigurnosne politike računarske mreže, određen je sastav i zadaci tima za upravljanje bezbednosnim kompjuterskim incidentima.

Procedure odgovora na napad

Pravila za zaposlene

Data su u Pravilniku o rešavanju sigurnosnih incidenata.

Procedure i uputstva za rešavanje incidenata

Prilikom primena forenzičkih akcija tim za upravljanje kompjuterskim incidentima sprovodi sledeće procedure:

- određivanje tačne prirode kompjuterskog incidenta ili zloupotrebe i dali je u toku ili je završen,
- informacioni sistem sačuvati u zatečenom stanju, odnosno ne činiti izmene koje bi otežale ili onemogućile dijagnostifikovanje,
- pravljenje dve kopije oštećenog hard diska, korišćenjem alata za kreiranje slike diska,
- kopiranje kompjuterskih i mrežnih dnevnika,
- ograničavanje pristupa oštećenom sistemu,
- eliminisanje očiglednosti,
- postavljanje hipoteze o napadu:
 - razumevanje kako je napadač izvršio incident, ušao u računarsku mrežu ili računar. Teoretski se analizira napad, mapiranjem svih mogućih vektora napada tj. pristupnih putanja računaru,
 - testiranje hipotetičkih putanja i ACL (lista kontrole pristupa) svih korisnika i administratora koji imaju pristup računaru i mrežnim uređajima u cilju utvrđivanja da li su oni izvršioci napada. U ovom koraku se određuje vreme, datum i okolnosti napada,
- dokumentovanje svake radnje, tako da se ponavljanjem zabeleženih akcija može rekonstruisati tok istrage,
- rekonstruisanje krivičnog dela - vrši se testiranjem uspostavljene hipoteze napada gde se saznaje kojim putem je napadač pristupio sistemu. Upotrebljavaju se forenzički računari za simulaciju sa fizičkom slikom HD (bit-po-bit) napadnutog računara, po potrebi mrežni uređaji sa konfiguracionim podešavanjima koji su korišćeni u slučaju incidenta i drugo,
- otkrivanje traga do osumnjičenog računara - traženje logičkih grešaka napadača na log datotekama računara i mrežnih uređaja u cilju utvrđivanja identiteta napadača,
- analiza izvornog, ciljnog i posrednog računara,
- prikupljanje dokaza, markiranje, obeležavanje i pakovanje fizičkih dokaznih materijala
- šifrovanje datoteka PKI sistemom koji se koriste kao digitalni dokaz i zaštita od izmena, korišćenjem hash programa (SHA-256, SHA-512 i sl.),

- obezbeđenje dokaza o vremenskoj liniji incidenta,
- izrada izveštaja o istrazi, koji sadrži:
 - kratak sadržaj incidenta (opis incidenta),
 - metod istraživanja,
 - generalni zaključci po redosledu izvedenih dokaza,
 - opis navedenih zaključaka sa ukazivanjem na čvrste dokaze,
 - preporuka o sprečavanju ponavljanja incidenta,
 - predlog za dalji postupak.

Izveštaji o incidentu su poverljiva dokumenta i čuvaju se na taj način da im pristup imaju samo ovlašćene osobe.

Korporacija može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja poverljivih i personalnih informacija.

Obuka

Tim za upravljanje kompjuterskim incidentima treba biti uvežban za donošenje raznih odluka koje treba sprovesti. Potrebno je pratiti i predviđati moguće kompjuterske incidente i davati rešenja za sprečavanje.

Timu treba izgraditi veštine da identifikuje da li se kompjuterski incident dogodio ili, ne, a u slučaju da jeste, način na koji je učinjen, ko je izvršio incident i naći dokaze koje je ostavio.

Digitalnog forenzičara obučiti za:

- računarsku i mrežnu administraciju koja se koristi u korporaciji,
- generičke ranjivosti svih sistema koji su na upotrebi u korporaciji,
- hakerske tehnike i
- legalno prikupljanje digitalnih dokaza, koji se koriste na sudu, čime se nesumnjivo potvrđuje da dokaz sadrži informaciju o učinjenom incidentu i da je legalno prikupljen.

Ubrzanje istrage

- Forenzičku istragu zaključiti što je brže moguće. Istraga ometa korporacijske aktivnosti, naročito po pitanju korišćenja opreme koja neće biti dostupna za upotrebu. Pored toga, duga istraga, daje veće šanse da potencijalni dokazi budu uništeni ili ugroženi. Šteta učinjena incidentom treba da se ispravi što je pre moguće, omogući oporavak svega što je izgubljeno i spreči buduće napade,
- Prilikom rada sa log datotekama, koje su uskladištene na centralnom log serveru, koristiti indeksiranje podataka i po potrebi vršiti upoređivanje sa originalnim informacijama,
- Digitalne dokaze kao što su dnevničke (log) datoteke, IDPS (Intrusion Detection and Prevention Systems) izlazi, kao i indeksi podataka, šifrovati i zaštititi sa jakim autentifikacijom,
- Imati jaku proveru identiteta i integriteta administrativnog pristupa mrežnim uređajima i
- Periodično (na 10 dana) proveravati integritet prikupljenih podataka.

Sankcije

U glavom tekstu predloga sigurnosne politike, korisnicima je zabranjeno da instaliraju programe, bez odobrenja administratora računara, što uslovljava da se usled pojavljivanja drugih programa,

zaposleni pozove na odgovornost.

Svrha istrage je da se odredi uzrok nastanka problema i da se iz toga izvuku zaključci o tome kako sprečiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bila greška čoveka, protiv odgovornih se mogu preduzeti sankcije.

Korporacija može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.

Ukoliko je incident izazvao zaposleni spoljne firme, korporacija može zatražiti od nje da ga ukloni sa liste osoba ovlašćenih za obavljanje posla u korporaciji.

U slučaju teže povrede pravila sigurnosne politike korporacija može pokrenuti krivični postupak.

ZAKLJUČAK

Kriminal na računarskim mrežama raste brzo i razvija se kao i Internet.

Cilj eksperimentalnog istraživanja je prikaz gde i kako naći digitalne dokaze koji potvrđuju kompjuterski kriminal koji se može realno dogoditi u korporaciji koja ima računarsku mrežu i pristup Internetu.

Kao rezultat i zaključak eksperimentalnog istraživanja predložena je sigurnosna politika koja definiše digitalnu forenzičku istragu kompjuterskog incidenta i rešavanje sigurnosnih incidenata, skupom pravila, koja omogućavaju i olakšavaju oporavak sistema posle incidenta i time smanjuju uticaj i sprečavaju ponavljanje kompjuterskog incidenta.

Postupci i metodi koji su sprovedeni tokom eksperimentalnog istraživanja sublimirani su u Pravilniku za digitalnu forenzičku istragu kompjuterskog kriminala, a u Pravilniku o rešavanju kompjuterskih incidenta date su smernice za zaposlene u korporaciji.

Kompjuterska forenzika je mnogo šira od samog pružanja izvora potencijalnih dokaza. Ozbiljna korporacija uspostavlja tim za upravljanje kompjuterskim incidentima i planira obuku, zajedno sa sigurnosnim politikama i procedurama za forenzičku istragu.

Preventivne i reaktivne mere zaštite nisu više dovoljne održavanje računarskih sistema i mreža na prihvatljivom nivou rizika. Potrebno je pronaći način da se maliciozni napadi proaktivno spreče, uspešni napadi identifikuju, a posledice i uzroci trajno otklone, kao i da se identifikuje, uhvati i procesuiru kompjuterski kriminalac koji je izvršio napad, što je ključno pitanje kompjuterske forenzike.

LITERATURA

- [1] McClure S, Scambray J, Kurtz G., *Hakerske tajne: zaštita mrežnih sistema, prevod petog izdanja*, Mikro knjiga, Beograd, 2006.
- [2] Milosavljević M., Grubor G. *Istraga kompjuterskog kriminala metodološko – tehnološke osnove*, Univerzitet Singidunum, Beograd, 2009.
- [3] Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd, 2009.
- [4] Pleskonić D., Maček N. Đorđević B. Carić M. *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007.
- [5] Standard ISO/IEC 27001, www.iso27001security.com/html/27001.html
- [6] Standard ISO/IEC 27002, www.iso27001security.com/html/27002.html
- [7] Udruženje javnih tužioca i zamenika javnih tužilaca Srbije, 2010. *Suzbijanje visokotehnološkog kriminala*, Narodna biblioteka Srbije, Beograd.

Internet izvori:

- [8] NIST SP 800-31, Intrusion Detection Systems, www.csrc.nist.gov/publications/nistpubs/index.html (Visited February 2010)
- [9] NIST SP 800-44, Guidelines on Securing Public Web Servers, www.csrc.nist.gov/publications/nistpubs/index.html (Visited February 2010)
- [10] NIST SP 800-61, Computer Security Incident Handling Guide, www.csrc.nist.gov/publications/nistpubs/index.html (Visited February 2010)
- [11] NIST SP 800-83, Guide to Malware Incident Prevention and Handling, www.csrc.nist.gov/publications/nistpubs/index.html (Visited February 2010)
- [12] www.e-evidence.info/index.html (Visited February 2010)
- [13] www.forensics.nl (Visited February 2010)
- [14] www.forensicfocus.com/ (Visited February 2010)

ABSTRACT

Computer crime, from year to year is getting more sophisticated and efficient. Attacks are aimed at the corporations, in order to collect sensitive data.

On the basis of established models of computer crime investigations on network devices, the aim of research is to define methods and procedures to determine valid digital evidences on network devices by the Computer Incident Response Team, CIRT, according to which the proposed corporate security policies to prevent computer crime, recovery of attacks and facilitate computer forensics and computer networks.

Performed experimental verification of application of forensic techniques and tools to attack the router scenario. Based on the analysis of models of computer crime investigations and experimental results suggested the security policy of the corporation with a set of relevant rules, to prevent (reduce) a result of computer crime, a lasting recovery from attacks and to facilitate corporate forensic investigations of computers and computer networks.

Key words: analysis, network device, log file, computer incident, policies.