REAGOVANJE NA INCIDENTE U INFORMACIONIM SISTEMIMA

Boško Rodić, VP 1122-54 Beograd
rbosko@eunet.yu

Sažetak: Incident ne mora biti samo posledica namere već i nehata ili delovanja više sile, elementarne nepogode. Incident može da bude posledica greške inetrmitentnog karaktera. Svaki incident mora da bude saniran. Prvi korak u sanaciji je takozvana **forenzična (sudska) obrada incidenta**. Istražuje se, pre svega, eventualna odgovornost za incident. Dijagnosticira se i otklanja uzrok u sistemu koji je, eventualno, dozvolio da dođe do incidenta. Nakon toga saniraju se posledice incidenta, IS se vraća u stanje koje garantuje bezbedno funkcionisanje sistema.
Ključne reči: bezbednost, informacioni sistem, incident, sanacija.

Summary: An incident may not be just a matter of intent but also an ordinary fault or vis major, natural catstrophe. An incident may be a result of an intermittent error. Every incident must be reconstructed. The first step in reconstruction is so called **forensic processing of the incident**. Possible responsibility for the incident is investigated first. The possible system error which is probable cause of the incident is diagnosed and repaired. After that, the reconstruction takes place and information system is turned back into the state which guarantees safe operation of the system.
Key words: security, information system, incident, reconstruction.

Prema [Kuk02] incidenti se dešavaju u informacionim sistemima (IS) i u najbezbednijim okruženjima. Incident izaziva stanje IS u kom je narušena bezbednost IS.

Bezbednost − engl. ***security***, rus. ***безопасность***, nem. ***sicherheit*** je ***je stanje sistema*** u odnosu na okolinu ali i na samog sebe. Bezbednost [Pra70] (javna) − ***stanje*** u kome su isključeni protivpravni akti, naročito oni uz upotrebu fizičke sile...ili ukoliko ovakvi akti i postoje, oni su vrlo retki i protiv njih se preduzimaju energične efikasne sankcije. Nasuprot ovome, (javne − u originalu) bezbednosti nema gde su ovakvi akti česti, odnosno gde se oni ne sankcionišu. Takođe, **bezbednost**, u odnosu na suštinu i stvarno značenje može se definisati **kao stanje**, organizacija i funkcija. Bezbednost kao ***stanje*** predstavlja zaštićenost nekog dobra, vrednosti, tekovine, društva...". Prema [Mat76] bezbednost ***je stanje*** onog koji je bezbedan, onog štoje bezbedno. Takođe, prema [Mat76], bezbedan je onaj koji je osiguran od opasnosti, zaštićen.

Sigurnost − prema [Mat76], je stanje, osobina onoga koji je siguran, onoga što je sigurno, u kome nekome ili nečemu ne preti opasnost, odsutnost opasnosti, bezbednost. Prema tome, u kontekstu *stanja* sistema prihvatimo da sigurnost ima isto značenje kao i bezbednost. Zaključujemo da se, sa jedne strane, radi o sinonimima. U zapadnoj varijanti srpskohrvatskog jezika, sada hrvatski jezik, reč sigurnost upravo označava bezbednost u smislu: javna sigurnost (bezbednost), državna sigurnost (bezbednost).

Sa druge strane, engl. ***reliable, dependable, trustworthy***, rus. siguran − ***верный***, ***надежный, достоверный***, nem. sigurnost − ***gewi'sheit*** − izvesnost. Prema tome, sigurnost u kontekstu na primer ***gewi'sheit*** − izvesnost(i) "Siguran sam, izvesno je, da sam

siguran (bezbedan)", može da se tumači kao stav − ubeđenje. Prilog sigurno, prema [Mat76], bi značio − sa najvećim pouzdanjem, stalno bez prekida, čvrsto, odlučno, bez kolebanja itd.
Za informacioni sistem bezbednost bi bila stanje koje obezbeđuje[1]:
poverljivost;
integritet;
raspoloživost;
pouzdanost;
neporicljivost informacija, odnosno podataka;
proverenost.

Poverljivost; stanje sistema u kome informacija nije na raspolaganju drugima ili pružena onima koji nisu ovlašćeni da je prime. Informacija u ovom slučaju uključuje kako onu koja može da se izvuče iz podataka (informacija je protumačeni podatak) koji se prenose tako i onu koja može da bude zaključena posmatranjem saobraćaja.

Integritet; stanje sistema u kome podaci nisu izmenjeni ili uništeni na neovlašćeni način. Prema [IBM85] ovaj atribut znači stanje sistema u kom je moguće pravovremeno reagovanje i ponovno osposobljavanje sistema kod nastupa štenog događaja.

Raspoloživost; stanje sistema u kome podacima i drugim resursima može da se pristupa i da se koriste kada je to neophodno.

Pouzdanost; sposobnost komponente, uređaja ili sistema da obavlja svoju zadatu funkciju u određenim uslovima eksploatacije i da zadržava svoje parametre (osobine) u datim tolerancijama.

Neporicljivost; stanje sistema takvo da strane u transakciji ne mogu naknadno da poriču učestvovanje u svim ili delovima transakcije.

Proverenost; [IBM85] kao atribut bezbednosti IS je stanje u kom je omogućena provera rada IS i svih njegovih komponenti u svrhu pravovremenog otkrivanja eventualne povrede njegove bezbednosti.

Prema [Kuk02] predlažemo 10 (delimično izmenjenih) **zlatnih pravila** forenzičnog računarstva.

1. Osigurati i izolovati mesto gde se desio incident.
2. Izvršiti sistematičnu potragu za dokazima.
3. Treba delovati blagovremeno, ali ne treba dizati paniku.
4. Ne dirati tastaturu ukoliko to nije neophodno.
5. Ukoliko je to moguće, isključiti računar iz mreže.
6. Loša zamena za isključivanje računara iz mreže može biti isključivanje što je više moguće mrežnih usluga.
7. Zapisati sve važne podatke na papir.
8. Utvrditi vreme otkrivanja incidenta.
9. Utvrditi ko je otkrio problem, na koji način.
10. Ne dirati ništa na računaru!? Idealno bi bilo da računar u ovoj fazi bude ugašen.

[1] Prema ISO IEC 17799 bezbednost (sigurnost) informacije se tretira kao čuvanje: integriteta, raspoloživosti i poverljivosti.

1. Metodologija za opis tipičnih scenarija potencijalnih incidentnih situacija

Prema [Cer97a], razvijena je metodologija za opis potencijalnih incidentnih situacija u IS. "Prijava", koja je osnova ove metodologije, je razvijena na osnovama klasifikacije potencijalnih izvora narušavanja integriteta IS prema [Rod01a].

Red. br.	Pitanja za opis incidenta
Opšti podaci	
1.	Matični broj preduzeća:
2.	R. br. incidenta u tekućoj godini:
3.	- odg. lice - prezime i ime, funkcija:
4.	- adresa:
5.	- telefon na poslu:
6.	- telefon kod kuće:
7.	- broj faksa:
8.	- broj mobilnog telefona:
9.	- broj pejdžera:
10.	- e-mail:
11.	- ovl. lice - prezime i ime, funkcija:
12.	- adresa:
13.	- telefon na poslu:
14.	- telefon kod kuće:
15.	- broj faksa:
16.	- broj mobilnog telefona:
17.	- broj pejdžera:
18.	- e-mail:

Da li ste još nekom (izuzev Centra[2]) prijavili incident	
1.	- firma:
2.	- odgovorno lice - prezime i ime, funkcija:
3.	- adresa:
4.	- telefon na poslu:
5.	- telefon kod kuće:
6.	- broj faksa:
7.	- broj mobilnog telefona:
8.	- broj pejdžera:
9.	- e-mail:
10.	- datum prijave:

Organ bezbednosti kome ste (ako ste) prijavili incident	
1.	- organ bezbednosti (unitrašnjih poslova):
2.	- odgovorno lice - prezime i ime, čin:
3.	- adresa:
4.	- telefon na poslu:
5.	- telefon kod kuće:

[2] Podrazumeva se postojanje "Centra" kojem se prijavljuju incidenti.

6.	- broj faksa:
7.	- broj mobilnog telefona:
8.	- broj pejdžera:
9.	- e-mail:
10.	- datum prijave:

Servis kome ste (ako ste) prijavili incident	
1.	- naziv firme:
2.	- adresa firme:
3.	- odgovorno lice - prezime i ime:
4.	- adresa:
5.	- telefon na poslu:
6.	- telefon kod kuće:
7.	- broj faksa:
8.	- broj mobilnog telefona:
9.	- broj pejdžera:
10.	- e-mail:
11.	- datum prijave:

Stradala lica		
	Broj stradalih lica (smrtno - S, teško - T, lako - L)	
1.	Osoblje IS	
2.	Osoblje van IS	
3.	Ostali	

Štete na infrastrukturi			
	Vrsta i stepen štete (teška - T, srednja - S, laka - L) na:		Cena
1.	Objekat		
2.	Elektroenergetska oprema (instalacije)		
3.	Klima uređaj(i)		
4.	Ostalo		

Štete na informatičkoj tehnologiji			
	Vrsta i stepen štete (teška - T, srednja - S, laka - L) na:		Cena
1.	Hardver		
2.	Mrežna oprema		
3.	Aplikativni softver		
4.	Uslužni - licencni softver		
5.	Operativni sistem		

6.	Podaci		

Obzirom da se ocena stepena štete može relativizirati, kao orjentaciju kod ocenjivanja uzimati sledeći kriterijum[3], na primer:

- ako je funkcionalnost IS (zbog neispravnosti hardvera ili softvera ili gubljenja podataka) bila narušena do, 8 radnih sati štetu treba smatrati lakom - L, ako je funkcionalnost IS bila narušena više od 8 i manje od 24 sata tada štetu treba smatrati srednjom - S, narušenu funkcionalnost IS od 24 sata i više smatrati teškom (katastrofalnom) štetom - T;
- kod ljudstva teškim stradanjem podrazumevati svako ono koje je za posledicu imalo bilo koji stepen invaliditeta, lako stradavanje je ono koje nije smrtno i teško.

Aktuelnost računarskih mreža zahteva da se posebno tretiraju kad su u pitanju incidenti. Prijavu incidenta proširujemo detaljnijim prikazom degradacije računarske mreže.

Podaci o HOST računaru(ima) - ako postoji(e) - odgovore ponoviti za svaki HOST[4] posebno		
1.	Broj oštećenih vaših HOST-ova	
2.	Ime HOST-a ili njegov identifikator	
3.	Adresa HOST-a	
4.	Tip HOST-a, prodavac, OS	
5.	Funkcija(e) HOST(ova)	
6.	Jednokorisnička radna stanica (da/ne)	
7.	Višekorisnička radna stanica (da/ne)	
8.	Mrežni "fajl" server (da/ne)	
9.	Ruter (da/ne)	
10.	Terminal server (da/ne)	
11.	Ostale funkcije (npr. mail hub, informacioni server, interni DNS, eksterni DNS i td.) (da/ne)	
12.	Gde je u mreži oštećeni host (npr. bekbon, podmreža, ispred vatrenog zida i td.)	
13.	Funkcija HOST-a (npr. privatni, za kadrovske poslove, finansijski)	
14.	Da li je HOST izvor - žrtva ili oboje	
15.	Da li je kompromitacija HOST-a nastupila kao rezultat napada (da/ne)	
16.	Da li je kontaktiran (ili se planira kontakt) sistem administrator u vezi oštećenih HOST-ova na drugim adresama? (da/ne)	

Podaci o HOST računaru(ima) - ako postoji(e) - odgovore ponoviti za svaki HOST posebno		
11.	Broj oštećenih ostalih HOST-ova	

[3] Neki sistemi ne smeju nikako prestajati sa radom.

[4] HOST - ili matični računar koji je izvor informacija ili signala. Ovaj termin je referisao na bilo koju vrstu računara od matičnog na koji se vezuju terminali (PC računari sa emulacijom) do servera koji je matični za njegove klijente. U mrežnoj arhitekturi klijentska radna stanica (korisnička mašina) može da se tretira kao HOST obzirom da je ona (ponekad) izvor informacija za razliku od rutera ili recimo sviča koji su (samo) prenosnici informacija.

12.	Ime HOST-a ili njegov identifikator	
13.	Tip mreže	
14.	Adresa(e) HOST(ova)	
15.	Tip HOST-a, prodavac, OS	
16.	Da li je kompromitacija HOST-a nastupila kao rezultat napada (da/ne)	
17.	Da li je kompromitacija HOST-a nastupila kao rezultat napada (da/ne)	
18.	Da li je kontaktiran (ili se planira kontakt) sistem administrator u vezi oštećenih HOST-ova na drugim adresama? (da/ne)	

Kategorija incidenta		
1.	Napad na javni (*anonymous*) FTP servis (*File Transfer Protocol*) (da/ne)	
2.	Provala u sistem (da/ne)	
2.1.	Nametljivac je dobio privilegovani pristup (da/ne)	
2.2.	Nametljivac je instalirao program "Trojanski konj" (da/ne)	
2.3.	Nametljivac je instalirao sistem za analizu saobraćaja na mreži *(packet sniffer*[5]) (da/ne)	
2.3.1.	Koji je(su) puni *pathname*(ovi) za izlazne datoteke njuškala?	
2.3.2.	Koliko puta je "njuškalo" testiralo pakete na mreži?	
2.4.	Provaljen *password* (da/ne)	
2.5.	Lako provaljiv *password* (da/ne)	
2.6.	FTP napad (da/ne)	
2.7.	NIS[6] - *Network Information System* (*yellow pages*) (da/ne)	
2.8.	NFS - *Network File System* napad (da/ne)	
2.9.	*Rlogin*[7] ili RSH - *Remote/Restricted Shell* napad (da/ne)	
2.10.	*Telnet*[8] napad (da/ne)	
2.11.	TFTP - *Trivial File Transfer Protocol* napad (da/ne)	
3.	Greška u konfiguraciji (da/ne)	
3.1.	Tip greške u konfiguraciji (specificirati)	

[5] *Sniffer* - lovac, hvatač - njuškalo. Programi koji se instaliraju u čvorovima mreža i u stanju su da elektronski nadziru saobraćaj koji se odvija kroz mrežu. *Sniffer* programi, u legalnoj upotrebi, služe za dijagnosticiranje problema koji se mogu pojaviti u toj mreži i raspoloživi su za svaku mrežnu platformu. Nelegalna upotreba ovih programa predstavlja ekstremno visok nivo rizika jer omogućava izuzetno visok nivo kompromitacije.

[6] NIS (*Network Information System*) tekuće ime ranije poznato pod YP (*Yellow Pages*). Ovim se daje mogućnost da se daju informacije o mnogim mašinama u računarskoj mreži (RčM) uključujući i *password*-e u RčM. NIS nije dizajniran da promoviše bezbednosni sistem.

[7] *Rlogin* - *Remote* LOGIN, UNIX komanda za udaljeno priključenje - "logovanje" korisnika na server u mreži kao da je terminal direktno uključen na sam server. *Rlogin* je sličan *Telnet* komandi samo što se prilikom logovanja prosleđuje i informacija o klijent računaru koji se priključuje na *Rlogin* server (tip klijent računara itd.). Rsh (*Remote SHell*) je UNIX komanda kojom se udaljeni korisnik loguje na server ali se istovremeno dozvoljava i prosleđivanje jedne ili više komandi ka tom serveru koje će biti izvršene interaktivno ili neinteraktivno.

[8] *Telnet* je protokol za komunikaciju kojim se *Telnet* klijent prijavljuje na *Telnet* server preko TCP/IP mreže i dobija mogućnost da pokreće programe na udaljenom računaru kao da se nalazi i na terminalu priključenom na taj računar.

4.	Prekid fukcionisanja servisa (da/ne)	
4.1.	Koji je servis prekinut	
4.2.	Kako je servis prekinut	
5.	E-*mail* bombradovanje (SPAM) (da/ne)	
5.1.	Da li je e-*mail* bombardovanje bilo uspešno (da/ne)	
6.	Slanje e-*mail* sa lažnom adresom pošiljaoca (*fake mail*) (da/ne)	
7.	IP lažno predstavljanje (da/ne)	
8.	Zloupotreba resursa *host*-a (da/ne)	
9.	Neslana šala (da/ne)	
10.	Pokušaj (da/ne)	
11.	Servis je ranjiv (da/ne)	
11.1.	Da li je ranjivost eksploatisana (specificiarati)?	
12.	Prevara (da/ne)	
13.	Osmatranje (da/ne)	
14.	Napad na *mail* server (*Sendmail*) (da/ne)	
14.1.	Da li je ovaj napad rezultovao kompromiracijom (da/ne)	
15.	Infiltracija u sistem (da/ne)	
16.	Nešto drugo (molimo specificirati)	

Detaljan opis incidenta		
1	Pretpostavke o vrsti napada (npr. ime virusa, naziv korišćenog teksta i sl.)	
1.1.	Kako ste otkrili incident	
1.2.	Opis slabosti sistema koje su zloupotrebljene ali nisu istaknute u prethodnim sekcijama	
1.3.	Izvor napada (ako vam je poznat)	
1.4.	Preduzeti koraci da se incident više ne ponovi (na primer, reinstalacija osetljivog softvera, popravka (patch) ugrožene aplikacije)?	
1.5	Ukoliko postoje, koji su planirani postupci da bi se incidenti prevazišli?	
1.6.	Da li planirate korišćenje nekog alata iz sledeće sekcije?	
1.6.1.	Navedite alate koje će te koristiti.	
2.	Aspekti incidenta koji nisu obrađeni napred	
2.1.	Da li je nešto od sledećeg softvera nametljivac ostavio na vašem sistemu?	
2.2.	Log fajl kao posledica delovanja incidentnog softvera (npr. *sniffer* programa)	
2.3.	Alati/skriptovi koji su koristili slabosti (da/ne)	
2.4.	Sors kod programa kao npr. programi za "Trojanca", programi za njuškanje (da/ne)	
2.5.	Binarni kod programa za npr. "Trojanca" ili programe za njuškanje. (da/ne)	
2.6.	Sakriveni fajlovi/direktoriji (da/ne)	
2.7.	Virus je inficirao fajlove (da/ne)	
2.8.	Drugi fajlovi, molimo specificirati.	

Bezbednosni alati

1.	U vreme incidenta, koje ste, od sledećih sigurnosnih alata, koristili?	
1.1.	Alati za password-e i autentičnost	
1.1.1.	*Crack*[9] (da/ne/kako često) - CERT®[10]	
1.1.2.	*Kerberos* (da/ne)	
1.1.3.	*One-time passwords* (da/ne)	
1.1.4.	*Proactive password checkers* (da/ne)	
1.1.5.	*Shadow passwords*[11] (da/ne)	
1.2.	Alati za proveru integriteta fajlova	
1.2.1.	MD5[12] (da/ne/kako često)	
1.2.2.	*Tripwire*[13] (da/ne/kako često)	
1.3.	Višenamenski alati	
1.3.1.	C2[14] "*security*" (da/ne)	
1.3.2.	COPS[15] (da/ne/kako često)	
1.3.3.	TAMU "*Tiger*"[16] (da/ne/kako često)	

[9] *Crack* je javno dostupan program koji omogućava predstavljanje šifrovanih *password*-a u obliku prostog teksta (*clear text presentation*). U cilju povećanja bezbednosti sistema *Crack* se koristi radi provere kvaliteta šifara koje se koriste na sistemu i upozorenja na one koje bi eventualni napadač mogao, zbog svoje jednostavnosti, lako probiti. *Crack* je dostupan *na ftp://coast.cs.purdue.edu/pub/tools/unix/crack/*.

[10] CERT predpostavlja korišćenje konkretnih alata, to su alati od 1.1.1. do 1.1.5, zatim 1.2.1. do 1.2.2. itd.

[11] *Shadow passwords* - skrivene šifre su šifre sistema koje se, za razliku od običnih, čuvaju u fajlovima koji nisu javno dostpuni, ili za njihovu poziciju zna samo administrator sistema.

[12] MD5 je program koji jedinstveno potpisuje nekakav objekat (fajl, skup falova i sl.) pri čemu potpis nije moguće ponoviti novim objektom (sem ukoliko nije isti kao originalni). MD5 se može naći u RFC 1321 (RFC - *Request For Comments* (Internet)). Pogledajte sajt - *ftp://coast.cs.purdue.edu/pub/tools/unix/md5*.

[13] *Tripwire* je program koji proverava integritet fajlova i direktorijuma potpisujući svaki od nih posebnim MD5 potpisom i čuvajući te potpise u svojoj tajnoj bazi. U trenutku eventualne promene nekog fajla, *Tripwire* će primetiti razliku jer će se i MD5 potpisi razlikovati, te će moći i da prijavi promenu nekom predefinisanom licu. *Tripwire* je dostupan na mnogim sajtovima koji uključuju *ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire/*.

[14] C2 - NCSC - *National Computer Security Center pri NSA* - *National Security Agency*, je definisao kriterijume bezbednosti za informacione sistemet poznate pod imenom *Trusted Computer Systems Evaluation Criteria* (TCSEC), standard Ministarstva odbrane 5200.28, takođe poznat kao "narandžasta knjiga" - *Orange Book*. Crvena knjiga - *Red Book*, je odgovarajući deo za računarske mreže. Prema ovom kriterijumun, na primer, nivo D je minimalna zaštita, C je diskretna zaštita, a C2 je zaštita kontrolisanim pristupom.

Bezbednosne osobine koje se zahtevaju na nivou C2 podrazumevaju:

- *Mandatory identification of all users on sytem* - sposobnost sistema da identifikuje tzv. korisnike i samo njima dozvoli pristup resursima;
- *Discretionary access control* - mogućnost da korisnici zaštite sopstvene podatke prema sopstvenim potrebama;
- *Accountability and auditing* - sposobnost sistema da detaljno prati i beleži sve akcije korisnika a i samog sistema;
- *Object Reuse* - sposobnost sistema da onemogući korisnicima pristup informacijama iz resursa koji su prethodno korišćeni od strane drugih korisnika ili sistema - memorije koja je ispražnjena ili obrisanih fajlova.

Kvalitativna kontrola na nivou C2 uključuje:

- ispitivanje izvornog koda;
- ispitivanje detaljne projektne dokumentacije;
- ponovno testiranje kao potvrda da su greške pri evaluaciji ispravljene.

[15] COPS (*Computer Oracle and Password System*) - je sistem programa koji se mogu upotrebiti radi provere sigurnosti/ranjivosti UNIX sistema. Sistem programa COPS ne popravlja nepravilnosti nego samo pravi izveštaj uočenih bezbednosnih nedostataka. COPS je dostupan na *ftp://coast.cs.purdue.edu/pub/tools/unix/cops.*

[16] TAMU *Security Tools* - sistem programa/skriptova kojima se proverava bezbednost UNIX sistema u mrežnom okruženju napravljenih od strane *Texas A&M University*. Uočene probleme ne popravlja nego pravi izveštaj (report). Alati su publikovani i dostupni su na *www.net.tamu.edu/ftp/security/TAMU/*.

1.4.	Alati za monitoring mreže (da/ne)	
1.5.	Alati za filtriranje (da/ne)	
1.6.	Alati za otkrivanje "slabih tačaka" (da/ne)	
1.7.	Razni i ostali alati (da/ne)	
2.	Šta ste radili u vreme dešavanja incidenta?	
3.	Da li će biti sačuvani poslovi koji su prekinuti zbog incidenta?	

Ostale informacije		
1.	Datum dešavanja incidenta	
2.	Sat dešavanja incidenta	
3.	Datum prijave incidenta Centru	
4.	Sat prijave incidenta Centru	

Ako postoje pretpostavke da je učinjeno zlonamerno (kriminalno) delo tada [Pet00], u slučaju prijave incidenta, za dalji uspešan rad od izuzetnog značaja bi bilo da se pripremi i jedan broj indicijalnih činjenica. To su tzv. "crveni signali (lampice - u originalu)" - činjenice koje svojim značenjem upućuju na mogućnost postojanja delikta i učinioca ili upućuju na uzrok kriminalnog dela.

Ili, prema [Mar85a], definisani su indikatori bezbednosti - pokazatelji, pojmovne definicije koje ukazuju na nešto, upućuju na nešto, skreću pažnju na postojanje nečega ili na mogućnost postojanja nečega. U istraživanju društvenih pojava, među koje svakako spadaju bezbednosne pojave, indikatori su metodološko sredstvo kojim se služimo da u stvarnosti otkrijemo dokaze postojanja nečeg.

Prema [Rod01a] aktiviraju se po potrebi (ako postoje) DAT (*Disaster Assesiment Team*) tim za procenu katastrofe (štete) i DDT (*Disaster Development Team*) tim - grupa(e) ljudi koji će realizovati plan obnove.

2. METODOLOGIJA ZA OPIS TIPIČNIH SCENARIJA KOJIMA SE ODGOVARA U PROCESU SPREČAVANJA NAPADA

Aktivnosti u procesu sprečavanja napada sprovode se:
- pre (eventualnog) napada;
- u toku (eventualnog) napada;
- nakon izvršenog napada.

Svakako da se pre napada sprovode aktivnosti preventive, a nakon izvršenog napada sprovode se aktivnosti sanacije.

Univerzalna procedura za odbranu u toku napada ne postoji. Osnovni cilj je da se onemogući veća šteta od onog trenutka kada se shvatilo da se radi o napadu na sistem. Izuzetno je važno da administrator dobro poznaje svoj sistem, da poznaje način funkcionisanja servisa na njemu i eventualne slabe tačke te da bude dobro obavešten o mogućim napadima koji mogu biti preduzeti protiv tog sistema.

Očigledno je da se u vezi sa ovim problemom mora baviti vrhunski stručnjak.

Izuzetna je zavisnost od *Windows* OS i proizvođača softvera u slučaju napada na *Windows* OS. Prema tome za očekivati je napade čak i od samog proizvođača OS - *Microsofta.* Ovo se odnosi, pre svega, na one koji nemaju legalan softver.

Preporučuje se da se korisnici za konekciju na javne računarske mreže opredeljuju za na primer OS Linux koji mogu kontrolistai, odnosno za koji imaju izvorni kod.

U toku utvrđivanja havarije na sistemu, treba blagovremeno reagovati. Pri ovome treba znati da se napad, vrlo često, realizuje korišćenjem različitih alata, za koje se čeka otvaranje nekih sporednih vrata, kroz koja oni mogu da deluju. Na neke napade treba (svesno) reagovati sa zadrškom, ako je u pitanju npr. preticanje. Špijuna treba pustiti da obavlja opservaciju i polako ga uvoditi u nevažne ili čak lažne podatke i sl. Ne sme se dozvoliti, ako se otkrije da je napd u toku, da uljez, eventualno, dođe u posed zaštićenih informacija. Najbolja reakcija je da se konkretni računar ili celi sistem isključi mreže, ako se napad realizuje preko mreže. Međutim, to treba raditi sa pažnjom, jer potpunim isključenjem sistema prekida se i rad korisničkih servisa čime se ugrožava ugled i poverenje korisnika u sistem.

3. OPIS KOREKTIVNIH AKTIVNOSTI KOJIM SE OTKLANJAJU POSLEDICE EVENTUALNOG NAPADA.

Scenario napada (štete) u odnosu na način i posledice može da bude u raznim varijantama, tabela, [Rod01a], podrazumeva se da će i scenario, skup aktivnosti, za otklanjanje posledica eventualnog napada biti, takođe, u raznim varijantama.

U svakom slučaju scenario za otklanjanje posledica eventualnog napada, zvaćemo ga SANACIJA, mora da ima sledeće karakteristike, ciljeve:

1. Smanjiti štetu[17]
   1.1.Sanirati ljudstvo
      1.1.1.Sprečiti dalje stradavanje ljudstva

Sprečiti stradavanje ljudstva koje je (bilo) ugroženo neposredno u IS kao i ljudstva koje se angažuje na sanaciji štete u IS. Ljudstvo može biti ugroženo [Mil75], pre svega, mehanički, asfiktički - pri poremećaju gasne razmene, fizički napose - zbog dejstva toplote, hemijski pod uticajem otrova i najposle psihički. Svi navedeni slučajevi su, teoretski, mogući i kad je u pitanju ljudstvo angažovano u IS. U svim ovim slučajevima treba skloniti uzrok ugrožavanja zdravlja i života ljudstva.

      1.1.2. Ukazati ljudstvu prvu pomoć

Shodno vrsti ugroženosti zdravlja i života preduzeti mere prve pomoći. Prioritet u davanju prve pomoći imati prema kritičnosti ugroženosti života i zdravlja. Najpre sprečiti, na primer, krvarenje a zatim pristupiti ostalim merama prve pomoći.

      1.1.3. Na najbolji mogući način dugoročno sanirati posledice stradavanja ljudstva.
      1.1.4. Pokrenuti (po potrebi) disciplinski, prekršajni ili krivični postupak.
   1.2. Sanirati informatičku tehnologiju
      1.2.1. Sprečiti uništavanje (degradaciju) podataka bez obzira na medij[18].
      1.2.2. Sprečiti dalje uništavanje[19] informatičke tehnologije (softver i hardver).

[17] Poznato je da se zbog nestručnosti, i neblagovremenosti, u sanaciji šteta u IS, štetne posledice mogu i - uvećati. Tipičan primer je diletantskog postupanja sa licem stradalim od strujnog udara - lice se zakopava "da bi zemlja izvukla struju"!?

[18] Magnetni mediji (sadržaj) u vatrostalnoj kasi mogu da se unište ako se kasa naglo otvori, pre izjednačavanja temperatura - hlađenja okoline kase.

1.2.3. Osposobiti IT za dalji rad uz maksimalni nivo pouzdanosti rada.
1.3. Sanirati infrastrukturu
1.3.1. Sprečiti uništavanje (degradaciju) infrastrukture.
1.3.2. Osposobiti infrastrukturu za korišćenje.
1.4. Sačuvati dokaze

U cilju utvrđivanja uzroka pojave štete neophodno je sačuvati dokazni materijal. Pre svega, kad je ljudstvo u pitanju, bitno je da se omogući, putem dokaza, da se izvede zaključak da li je do narušavanja života i zdravlja došlo na pririodan način ili nasilnim putem. Ako je u pitanju nasilno oštećenje bitan je odgovor da li je ono bilo zadesno [Mil75], samoranjavanjem (samoubistvom) ili ranjavanjem (ubistvom) od strane drugog lica.

Kada je reč o štetama na IT (kompjuterskim kriminalnim delima (3), u originalu) mora se imati u vidu da "kompjuterizovani elektronski dokazi" često nisu jednaki ostalim oblicima fizičkih dokaza. Isto tako, neki od problema vezanih za utvrđivanje činjenica u oblasti kompjuterskog kriminala zasnivaju se na prolaznoj prirodi obrade podataka i kratkom vremenu zadržavanja u računaru mnogih datoteka i zapisa, zbog čega, ako se kriminalni akt ne otkrije već u toku izvršenja ili neposredno nakon toga, verovatno će do momenta otkrivanja nestati mnogi tragovi i dokazi, pa krivac, iako je opravdano sumnjiv, neće moći biti uspešno krivično gonjen.

2. Utvrditi uzrok pojave štete

Odgovorima na Upitnik u vezi prevencije u zaštiti IS [Rod01a], zajedno sa prijavom incidenta, uz uslov da su sačuvani dokazi, stvaraju se uslovi za zaključivanje o mogućem uzroku incidenta. Utvrđivanje uzroka, u postupku sanacije, presudno je zbog (najmanje) tri razloga:

- utvrđivanja odgovornosti i u tom cilju pokretanja adekvatnog (disciplinskog, prekršajnog ili krivičnog) postupka;
- "izvlačenja pouke" - kod revitalizacije sistema da se na najbolji mogući način izvede *backup*. Ovo je karakteristično kod *batch* obrada, iz tih razloga se vodi dnevnik obrade da se lakše locira "mesto" prekida u obradi i da bi se obrada bez ponavljanja mogla nastaviti od momenta prekida;
- "izvlačenja pouke" - kod revitalizacije sistema (ili u radu sistema) u buduće se ne sme dozvoliti ponavaljanje uočenog uzroka - greške.

U sledećem primeru CERT [Cer97b], je dao dokument koji u grubim crtama sugeriše korake u oporavku sistema ukoliko je došlo do njegove kompromitacije. Sistem administrator(i) mogu koristiti ovaj dokument za nekoliko tipova provala u sistem. Prvenstvena namena ovog dokumenta je da korisnici modifikuju svoj sistem u cilju oporavka potencijalnih slabosti sistema ili "krpljenja rupa" kako se to popularno kaže, bilo lično, bilo preko prodavca opreme koji treba da vam obezbedi dopunu i/ili izmenu softvera.

A) Potražite znake kompromitacije (ugrožavanja bezbednosti) vašeg sistema.

Vodite računa da sve akcije, koje preduzmete tokom ispitivanja potencijalne kompromitacije konkretnog sistema, budu usklađenje sa pravilima organizacije u kojoj je kompromitovani IS.

---

[19] I u ovom slučaju poznati su primeri brzoplete sanacije, gašenje požara na elktronici vodom npr, koja je još više povećala postojeću štetu.

1. Ispitajte "log fajlove" da bi uočili eventualne netipične konekcije, ili neke druge neuobičajene aktivnosti, sa neočekivanih lokacija u kompromitovani IS. Treba pogledati "logove" o prijavama lokalnih korisnika na sistem u nekom periodu vremena, sistemske "logove" kreirane od posebnog sistemskog procesa (*syslog*) kao i ostale relevantne log fajlove u kojim bi mogla biti zabeležena informacija o nedozvoljenim aktivnostima. Ukoliko *firewall* računar ili ruter beleže svoje logove na nekom drugom računaru, koji nije (bio) ugrožen, treba proveriti i njih. Treba uočiti da ovo nije potpuno pouzdan metod sem ukoliko postoji sistem sa log fajlovima koji se naknadno ne mogu menjati nego sistem samo dodaje nove informacije na njihov kraj (*append-only logs*). Mnogi nametljivci dodatno edituju i menjaju informacije u log fajlovima koji nisu *append-only* da bi sakrili tragove svog prisustva i nedozvoljenih aktivnosti na sistemu.

2. Potražite sve *setuid/setgid* fajlove na sistemu (posebno *setuid* fajlove sa *root* privilegijama). Napadači često ostavljaju kopije programa */bin/sh* ili */bin/time*, koje imaju *setuid* karakteristike, želeći da i kasnije imaju administrativne privilegije na sistemu na koji su jednom nedozvoljeno upali. UNIX komanda za pretražiavnje (*find*(1)) omogućava jedno takvo pretraživanje. Na primer, sledećim komandama mogu se pronaći svi *setuid* fajlovi na sistemu sa administrativnim (*root*) privilegijama i svi *setgid* fajlovi gde je pripadna grupa *kmem*.

   ```
   find / -user root -perm -4000 -print
   find / -group kmem -perm -2000 -print
   ```

   Još jedan program koji može da pretražuje diskove i particije na njima, u potrazi za fajlovima, sa navedenim karakteristikama je program *ncheck* [Emw00]. Na primer pretraživanje *setuid* fajlova na disk particiji */dev/rsd0g* moguće je izvršiti komandom:
   ncheck -s /dev/rsd0g

3. Provera sistemskog softvera da bi se uočile eventualne nedozvoljene izmene. Poznati su slučajevi izmene programskog koda na primer sledećih programa:

   login, su, telnet, netstat, ifconfig, ls, find, du, df, libc, sync

kao i ostali programi koje poziva "*smart*" server (*inetd*) kao i razne deljive sistemske biblioteke. Obavezna je provera sistemskog softvera sa originalnim na instalacionom disku. Ne treba previše verovati samim kopijama svih programa (*backup copies*) koje su jednom napravljene, jer i one mogu da sadrže "Trojanca". Po povratku takvih podataka na disk Trojanac ima ulogu da predstavi sistemu ili korisniku kao da je sve u redu i da se na sistemu nalaze stari programi iako su u stvari menjani. Trojanac ima tu sposobnost da zavara sistemske pozive za proveru identiteta softvera, te je neophodno koristiti druge preventivne programe i tehnologije kao što je MD5, Tripwire i sl, koji informaciju o verziji programa čuvaju u svojoj, "samo sebi znanoj" zaštićenoj zoni. Uz dodatno korišćenje PGP programa, kojim se jednoznačno može potpisati rezultat rada prethodno navedenih programa (izlazni fajl sa rezultatima), može se smatrati da je sistem preventivno dobro obezbeđen.

4. Provera sistema u cilju preventive na preslušavanje saobraćaja u mreži nekim od poznatih *sniffer* programa čime bi se omoglo doći u posed, recimo informacija o korisničkim šiframa i nalozima na sistemu. Više informacija o ovim programima i zaštiti od njih može da se nađe na Internet adresi:

   ftp://info.cert.org/pub/cert_advisories/CA-01.netnjork.monitoring.attacks

5. Proverite sve programe koji se startuju iz "*cron*" ili "*at*" aplikacije jer je česta pojava da nametljivac ostavi dodatni prolaz (*back door*) unutar tih aplikacija koje se startuju pod kontrolom navedenih server procesa. Time se dobija mogućnost da se pristupi sistemu i dobiju se administratorske privilegije i to naknadno, po izvršenoj analizi sistema od strane administratora. Sam administrator može biti dalje u uverenju da je posle uklanjanja bitnih programskih celina, koje je nametljivac ostavio, sada bezbedan, ali to, zapravo, ne mora biti istina. Zato je ova provera neophodna.

6. Provera aktivnih servisa na sistemu podrazumeva kontrolu svih aplikacija koje se startuju kao serveri i koje omogoćavaju pristup preko mreže. Kontrolom u sistemskom fajlu */etc/inetd.conf* može se uočiti da li su aktivni baš oni servisi koje smo želeli da aktiviramo ili je aktiviran i neki dodatni. Takođe, čak i ako izgleda da je sve u redu, potrebno je proveriti ponaosob svaku od startovanih aplikacija, jer je moguće da je nametljivac ostavio svoju zamenu za originalnu aplikaciju koja ćemu dopustiti pristup sistemu kad se najmanje nadamo. Takođe, moguće je da da nametljivac nije dirao ni jednu od serverskih aplikacija, ali da je ostavio Trojanca kao sam glavni kontrolni server proces (inetd) čime bi omogućio da se sistem otvara prema ostalom delu mreže onako kako je on zamislio.

7. Provera sistemskih i korisničkih fajlova sa lozinkama na sistemu *(/etc/passwd*) je neophodna da bi se uočile promene tipa dodavanje novog korisnika, promena grupnog broja ili jedinstvenog korisničkog broja u tim fajlovima kao i postavljanje korisnika bez šifre što su sve primeri pripreme sistema za destruktivno nelegalno delovanje nametljivca.

8. Provera da li u sistemskim i mrežnim fajlovima postoje celine koje su naknadno i bespravno dodate. Posebno treba obratiti pažnju da li u konfiguracionim fajlovima tipa */etc/hosts.eljuiv .rhosts* i */etc/hosts.lpd* postoje linije koje sadrže znak "+". Takođe, treba proveriti da li su neki od konfiguracionih fajlova postojali od ranije, ili ih je dodao nametljivac u sistem.

9. Provera da li u sistemu postoje skriveni ili neuobičajnei fajlovi, koji pre nisu postojali. Obično postoji mogućnost da je nametljivac sakrio svoje programe pod fajl ili direktorijum sa imenom "..." ili ".." ili "..^G" i sl. Takvi fajlovi, kao i fajlovi čija imena počinju sa tačkom "." ne mogu se na prvi pogled uočiti. Običnom komandom za pretraživanje mogu se uočiti i takve strukture:

```
find / -name ".. " -print -xdev
```

10. Ispitivanje svih računara na mreži da bi se našli dodatni znaci znaci provale u sistem. Obično kada nametljivac razbije zaštitu jednog sistema, onda je vrlo verovatno da su i drugi računari koliko-toliko zloupotrebljeni. Ovo je posebna karakteristika sistema u kojima je aktivan servis NIS. Zbog toga je neophodno proveriti sve računare koji bi na bilo koji način koristili resurse napadnutog sistema, npr. preko one koji koriste *.rhosts* ili/i */etc/hosts.equiv* datoteke na sistemu koji je postao nesiguran.

B) Proučiti ostale CERT dokumente:

Za nove informacije o napadima koji su prijavljeni na na CERT pogledati sajt:

ftp://info.cert.org/pub/cert_summaries/

Ukoliko se sumnja da je sistem posednut od strane nametljivca treba pogledat dokument "Kako se oporaviti od napada na UNIX sistem".

ftp://info.cert.org/pub/tech_tips/root_compromise

Treba pogledati i ostale dokumente na tom istom sajtu. Incident možete prijaviti CERT-u popunjavanjem formulara dostupnog na adresi:

ftp://info.cert.org/pub/incident_reporting_form.

4. LITERATURA

[Cer97a] CERT© Coordination Center, *Incident Reporting Form - Version 4.3.3*, Dec. 15, 1997. godina.

[Cer97b] CERT© Coordination Center, *Intruder Detection Checklist - Version 1.2*, ftp://info.cert.org/pub/tech_tips/intruder_detection_checklist, October 3, 1997. godina.

[Emw00] EMWAC server: http://www1.sica.com/IMS/index.htm, 2000. godina.

[IBM85] IBM – Intertrade, Tehnike osiguranja računskog centra i zaštite podataka, Radovljica,1985. godina.

[Kuk02] Milan Kukrika, Upravljanje sigurnošću informacija - zaštita informacionih sistema prema standardu ISO 17799, INFOhome Press, Beograd, 2002002. godina.

[Mar85a] Vidan Marković, *Bezbednosni informacioni sistemi*, Birotehnika Zagreb, 1985. godine,

[Mat76] ***, *Rečnik srpskohrvatskog književnog jezika*, Matica srpska, Novi Sad, 1976. godina.

[Mil75] M. Milovanović, *Sudska medicina*, "Medicinska knjiga", Beograd - Zagreb, 1975. godina.

[Pet00] Slobodan Petrović, *Kompjuterski kriminal*, Ministarstvo unutrašnjih poslova Republike Srbije – Uredništvo časopisa "Bezbednost" i lista "Policajac", Beograd, 2000. godine.

[Pra70] ***, *Pravni leksikon (drugo izmenjeno i dopunjeno izdanje),* "Savremena administracija" Beograd, 1970. godina.

[Rod01a] Boško Rodić, *Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija* – doktorska disertacija, Vojnotehnička akademija Beograd, 2001. godina.