CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje sigurnosnim incidentima

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Računalni sigurnosni incidenti su česta pojava u moderno doba. Općenita definicija računalno sigurnosnog incidenta jest posredno ili neposredno ugrožavanje sigurnosne politike, pravila i procedura. Razvoj tehnologije i računalne znanosti omogućio je i razvoj novih metoda napada i ugrožavanja računalnih 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. Sigurnosne su prijetnje brojne i raznolike, ali i sve razornije (npr. napad uskraćivanja usluga može napadnutoj tvrtki stvoriti velike financijske troškove) Aktivnosti za sprečavanje sigurnosnih prijetnji temeljene na rezultatima procjene rizika (npr. primjena sigurnosne metrike) mogu smanjiti broj incidenata, ali ne mogu spriječiti sve incidente. Zbog toga je potrebno da organizacija ima sposobnost rješavanja sigurnosnog incidenta u smislu ljudstva i primjene sigurnosnih mjera zaštite. Za potrebe odgovora na sigurnosne incidente osnivaju se posebne grupe za rješavanje istih. One su potrebne za brzo otkrivanje incidenata te za saniranje štete nastale sigurnosnim incidentom. Grupe za rješavanje sigurnosnih incidenata obično su dio CERT (eng. Computer Emergency Response Team) organizacije zadužene za pružanje potpore u slučaju narušavanja sigurnosti neke tvrtke ili organizacije. Sigurnosni incidenti, CERT organizacije i grupe za rješavanje incidenata opisani su u prva dva poglavlja ovog dokumenta.

Osim postojanja organizacija za upravljanje incidentima potrebno je definirati postupak rješavanja sigurnosnih incidenata. Životni ciklus postupka rješavanja sigurnosnog incidenta je također opisan u dokumentu, kao i specifičnosti vezane uz opasnije sigurnosne incidente, kao što su DoS (eng Denial of Service) napad i pokretanje zlonamjernog programskog koda. DoS napad je opasan za organizaciju jer je posljedica napada velika novčana šteta za napadnutu organizaciju. Pokretanjem proizvoljnog programskog koda napadač može uzrokovati još i veću štetu organizaciji (krađa podataka, stanje uskraćivanja usluga, a time i veliki novčani gubici).

2. Sigurnosni incidenti

Računalni sigurnosni incident je, prema definiciji iz Pravilnika o koordinaciji prevencije i odgovora na računalne sigurnosne incidente (*www.pak.hr/lgs.axd?t=16&id=2611*), svaki događaj koji ugrožava bilo koji aspekt računalne sigurnosti, odnosno koji za posljedicu ima gubitak povjerljivosti, cjelovitosti i raspoloživosti podatka, zlouporabu ili oštećenje informacijskog sustava ili informacija, uskraćivanje usluge ili onemogućavanje rada informacijskog sustava te svaka nezakonita radnja čiji se dokazi mogu pohraniti na računalni medij. Dakle, sigurnosni incident je čin narušavanja propisanih ili podrazumijevanih sigurnosnih normi. Kako bi određenu aktivnost mogli proglasiti incidentom bitno je da se radi o ciljanoj ilegalnoj aktivnosti. Incidenti se mogu podijeliti u dvije glavne skupine: prema vrsti i težini incidenta.

Podjela prema vrsti incidenta:

- neželjeni prekid ili uskraćivanje usluga (eng. Denial of Service),
- neovlaštena uporaba sustava i
- prijevare putem Interneta.

Podjela prema težini incidenta:

- računalni sigurnosni incidenti koji imaju utjecaj na ključne sustave, servise ili informacije,
- računalni sigurnosni incidenti koji imaju utjecaj na sustave, servise ili informacije koji nisu definirani kao ključni i
- incidenti čije rješavanje nije vremenski osjetljivo.

Sigurnosni događaj je bilo koja pojava u sustavu ili računalnoj mreži. To može biti na primjer povezivanje korisnika na računalo s dijeljenim datotekama (eng. file share), primanje zahtjeva za web stranicom, slanje poruka elektroničke pošte, sprečavanje neželjenih veza putem vatrozida i slično. Zlonamjerni događaji su oni čije su posljedice negativne, kao što su rušenje sustava, preopterećenje mreže paketima, neovlaštena uporaba administratorskih ovlasti, neovlašten pristup osjetljivim podacima ili pokretanje proizvoljnog programskog koda koji uništava podatke. Na web stranicama CERT-a objavljeni su dokumenti koji detaljno opisuju pojedini tip sigurnosnog incidenta.

Primjeri incidenata sa primjerima zlonamjerne aktivnosti su:

- uskraćivanje usluga (eng. Denial of Service):
  - napadač može slati posebno oblikovane pakete ili veliki broj mrežnih paketa web poslužitelju što za posljedicu ima prekid usluga poslužitelja.
  - napadač može izvesti DDoS (eng. Distributed Denial of Service) napad i u tu svrhu usmjeriti stotine vanjskih nezaštićenih radnih stanica da šalju što je više moguće ICMP (eng. Internet Control Message Protocol) zahtjeva računalnoj mreži organizacije čiju mrežu želi srušiti.
- zlonamjerni programski kod:
  - napadač može koristiti zlonamjerni programski kod, kao što je računalni crv za napad na organizaciju. Računalni crvi su programi koji umnožavaju sami sebe i pri tome koriste računalne mreže da bi se kopirali na druga računala, često bez sudjelovanja čovjeka. Crvi otežavaju rad mreže, mogu oštetiti podatke i ugroziti sigurnost računala.
- neovlašteni pristup:
  - napadač može koristiti posebni programski alat kako bi neovlašteno pristupio datoteci s zaporkama pohranjenoj na poslužitelju.
  - napadač može neovlašteno pristupiti sustavu upotrebom ukradenog administratorskog korisničkog računa. Pri tome može ukrasti ili kriptirati osjetljive podatke koji su vrlo važni za napadnutu organizaciju. Napadač zatim ucjenjuje organizaciju objavom ukradenih podataka u javnosti ukoliko organizacija ne plati određenu svotu novaca. Ovakvi su napadi vrlo rašireni u današnje vrijeme i imaju naziv *ransomware*. Jedan od posljednjih napada izveden je upotrebom trojanskog konja TROJ_FAKEALE.BG. Zlonamjerni program kriptira otvorene datoteke i traži od korisnika da kupi program za dekriptiranje.
- neprimjerena uporaba:
  - korisnik može postavljati na Internet ilegalne kopije programskog paketa i raširiti ih ostalim korisnicima putem P2P (eng. peer-to-peer) mreže.

– napadač može slati žrtvi prijetnje putem elektroničke pošte.

2.1. Poznati sigurnosni incidenti u 2009. godini

DDoS napad koji je uzrokovao probleme s pristupom Internetu više milijuna korisnika u Kini dogodio se u svibnju 2009. godine. Napad na kineski registrator domena DNSPod uzrokovao je veća zagušenja u mreži te je pristup Internetu bio onemogućen ili značajno usporen u barem pet provincija. Među stranicama koje ovise o DNSPodu je i Baofeng.com, popularno sjedište za prikazivanje video sadržaja. Brojni korisnički pokušaji otvaranja sadržaja na web sjedištu Baofeng.com uzrokovali su pojavu mnogo neodgovorenih DNS upita, što je pak dovelo do još većeg zagušenja u regionalnoj mreži. U isto vrijeme, zahtjevi slani prema web sjedištu Baofeng.com dodatno su pojačali intenzitet napada uskraćivanja usluge na DNSPod. Zbog svega navedenog korisnici iz provincija Shanxi, Guangxi, Zhejiang, Jaingsu i Hebei na više su sati u potpunosti izgubili pristup Internetu.

U travnju 2009. godine otkrivena je nova botnet mreža (objašnjeno u poglavlju 4) koja se sastoji od, procjenjuje se, oko 1,9 milijuna računala s upravljačkim poslužiteljem koji se nalazi u Ukrajini. U botnetu se nalaze i računala iz mreža vlada Sjedinjenih Američkih Država i Ujedinjenog Kraljevstva, zatim Kanade, Njemačke i Francuske, objavili su sigurnosni stručnjaci iz tvrtke Finjan. Za neovlašteno preuzimanje kontrole nad korisničkim računalima korišteni su razni sigurnosni propusti u web preglednicima Internet Explorer i Firefox te preglednicima PDF dokumenata. Skupina koja kontrolira botnet ostvaruje zaradu nudeći kontrolu nad zaraženim računalima po cijeni koja se kreće oko 100$ za tisuću računala.

U studenom 2008. godine pojavio se opasan crv Conficker, također poznat kao Downup, Downadup i Kido. Conficker je računalni crv koji napada operacijski sustav Microsoft Windows i pri tome koristi napredne tehnike zlouporabe ugroženih računala što ga čini otpornim na uklanjanje. Crv se vrlo brzo proširio i smatra se da je to najveća zaraza crvom od 2003. godine i crva SQL Slammer. Napadi crvom zabilježeni su uglavnom u Europi, i to u Francuskoj, Ujedinjenom Kraljevstvu i Njemačkoj.

U siječnju 2009. crv je zarazio računalnu mrežu Francuske mornarice Intramar i neke od glavnih sustava Ministarstva obrane Ujedinjenog Kraljevstva. Crv se širio putem administrativnih ureda do računala u ratnim brodovima i podmornicama te bolnicama grada Sheffild. U veljači 2009. crv je napao računala oružanih snaga Republike Njemačke. U svibnju 2009. crv se proširio Windows poslužiteljima sveučilišta Southamptom i onemogućio računala na kampusu, kao i pristup Internetu te požarne alarme. Conficker za svoje širenje koristi različite tehnike i to ga čini vrlo otpornim. Uz to, njegovi dizajneri pomno prate aktualna rješenja za uklanjanje crva i prikladno ga nadograđuju. Poznato je pet inačica crva Conficker, poznatih kao inačice A, B, C, D i E. Inačice su otkrivene 21.studenog 2008., 29. prosinca 2009.,20. veljače 2009, 4. ožujka 2009. i 7. travnja 2009. godine respektivno.

Simptomi zaraze crvom Conficker uključuju:

- automatsko resetiranje politike zaključavanja korisničkih računa
- onemogućavanje nekih servisa operacijskog sustava Windows, kao što su Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender i Windows Error Reporting
- spor odgovor glavnog upravljačkog servisa domene (eng. Domain controllers) na zahtjeve klijenata
- zagušenje lokalnih računalnih mreža (eng. Local Area Network – LAN),
- nedostupnost web stranica čiji je sadržaj vezan uz antivirusne programe i servis Windows Update i
- zaključavanje korisničkih računa

Zanimljivo je da tvrtka Microsoft od 13.veljače 2009. nudi 250 000 američkih dolara za informacije koje će dovesti do uhićenja i osude pojedinaca zaslužnih za stvaranje i dizajn te distribuciju crva Cinficker.

2.2. Sigurnosni incident u Hrvatskoj

Najveći prijavljeni sigurnosni incident u Hrvatskoj bio je DDoS napad i dogodio se 21.travnja 2001. godine. Napadnuti su hrvatski Internet poslužitelji što je za posljedicu imalo nemogućnost korištenja Interneta u Hrvatskoj. Napad je odmah prijavljen policiji koja je kontaktirala CERT kako bi se otkrio identitet napadača i sanirao incident. Počinitelj ili počinitelji su DDoS napadom na tadašnje HT-ove (danas T-com) usmjerivače otežali pristup sadržajima web stranica izvan Hrvatske. Nakon što je prvi napad zaustavljen, pola sata iza ponoći, kasnije je uslijedilo još nekoliko napada. Prema istraživanjima napadi su pristigli iz 23 zemlje svijeta. Nakon što je u subotu napadnut HT, već u nedjelju je proveden DDoS napad i na drugi najveći hrvatski ISP, Iskon. No, kako su tada i Iskon i ostali domaći ISP-ovi (osim CARNet-a) svoje Internet usluge pružali preko HT-ove veze, svaki napad na HT-ov Hinet bio je na štetu i svim ISP-ovima. Neki od poznatijih DDoS napada na hrvatske web stranice su napadi na dvije popularne web stranice: www.auti.hr i www.oglasnik.hr. Napade je navodno izvela grupa maloljetnika iz Tuzle tražeći određeni novčani iznos kako bi prestali s ometanjem rada web stranica.

3. CERT organizacije

CERT organizacije su zadužene za pružanje potpore i obrane od napada na računalne sustave, kao i za razmjenu informacija te surađivanje s vladom, industrijom i međunarodnim partnerima.

Osim CERT organizacije, postoji i CERT koordinacijski centar (CERT Coordination Center – CERT/CC)) koji predstavlja opširniji CERT program. Program je usredotočen na identificiranje i rješavanje postojećih i potencijalnih sigurnosnih prijetnji, uključujući obavještavanje i obrazovanje administratora i drugog tehničkog osoblja organizacije, koordinaciju sa skupinama za rješavanje sigurnosnih incidenata u svijetu.

CERT/CC je glavni centar za rješavanje računalnih sigurnosnih problema. Prvi je osnovan u studenom 1988. godine u Sjedinjenim Američkim Državama, nakon napada crva „Morris Worm“ koji je srušio velik dio Internet mreže i ukazao na mnoge propuste u mrežnoj sigurnosti. Ubrzo nakon tog događaja DARPA (eng. Defense Advanced Research Projects Agency) je osnovala institut SEI (eng. Software Engineering Institute) koji je imao sposobnost brzo i učinkovito koordinirati komunikaciju među stručnjacima u slučaju sigurnosnog incidenta. CERT/CC osoblje pruža tehničke savjete i koordiniraju odgovore na sigurnosne incidente, identificiraju trendove u napadačkim metodama, analiziraju ranjivosti programskih paketa te pružaju načine rješavanja sigurnosnih problema u budućnosti. Zbog rasta Interneta i pojave profinjenih tehnika napada javlja se potreba za dodatnim resursima i mogućnostima rješavanja sigurnosnih problema. Kako bi se ostvarili dodatni resursi i mogućnosti CERT/CC je postao dio CERT programa. Ostala područja CERT programa uključuju edukaciju, istraživanje i razvoj, obavještavanje javnosti, forenziku i globalnu suradnju.

CERT organizacija postoji i u Hrvatskoj. CARNet je +CERT.hr osnovao 1996. godine s ciljem posredovanja u rješavanju računalno-sigurnosnih incidenata u kojima je uključena strana iz Hrvatske.

Razlozi formiranja CARNet CERT-a su:

- uspostava odgovarajuće koordinacije i suradnje u rješavanju sigurnosnih incidenata u kojima je barem jedna uključena strana iz Hrvatske,
- edukacija korisnika i rad na sprečavanju sigurnosnih incidenata i
- suradnja s mjerodavnim ustanovama na izradi odgovarajućeg zakonodavstva koje bi moglo pratiti razvoj informatizacije društva.

CARNet CERT je mjesto od povjerenja na području sigurnosti računalnih mreža i sustava Republike Hrvatske namijenjen akademskoj zajednici. Ciljevi rada CARNet CERT-a su:

- prikupljanje i analiza informacija o sigurnosnim incidentima te koordinacija i posredovanje između zainteresiranih strana pri rješavanju sigurnosnih incidenata,
- prikupljanje i distribucija sigurnosnih savjeta, preporuka i alata,
- edukacija i informiranje korisnika i javnosti o značaju i poboljšanju sigurnosti računalnih sustava,
- pokretanje projekata i uspostava timova o sigurnosnim problemima i objavljivanje rezultata rada,

- suradnja s relevantnim tijelima (Ministarstvo znanosti, obrazovanja i športa, Ministarstvo pravosuđa, Ministarstvo unutarnjih poslova,...) na uspostavi odgovarajuće pravne regulative na području sigurnosti računalnih sustava i
- međunarodna suradnja s ostalim CERT-ovima preko članstva u Forum of Incident Response and Security Teams

CARNet CERT već duže vrijeme održava i koordinira komunikaciju s predstavnicima pravosuđa i policije Republike Hrvatske. 31. ožujka ove godine na sjednici Vlade Republike Hrvatske osnovan je Nacionalni program informacijske sigurnosti u Republici Hrvatskoj te usvojen plan provedbe Nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj. Ovi dokumenti CARNet CERT postavljaju u poziciju vršnog nacionalnog CERT-a i središnjeg tijela u nacionalnoj hijerarhiji državnih i privatnih tijela odgovornih za sigurnosne incidente na Internetu i drugima mrežama temeljenim na javnoj komunikacijskoj infrastrukturi.

U slučaju da otkriju sigurnosni incident korisnici mogu prijaviti incident CARNet CERT-u. Prijava incidenta treba sadržavati osnovni skup podataka nužnih za uspješnu obradu incidenta. Podaci koje prijava mora sadržavati su:

- IP adresa i/ili ime računala koje je napadnuto,
- izvod iz dnevničke datoteke ili slični podaci iz kojih je moguće rekonstruirati o kakvoj se vrsti neželjene mrežne aktivnosti radi,
- datum, točno vrijeme i vremenska zona napada,
- ako se prijavljuje prijem spama, hoaxa ili e-mail poruke s virusom tada tu poruku priložite prijavi zajedno s cjelokupnim zaglavljem (eng. header).

Incident se prijavljuje CARNet CERT-u ako postoji potreba da se kontaktiraju nadležne osobe u domeni izvora incidenta u čemu posreduje CARNet CERT te ako se pojedini incident ponavlja kroz duže vremensko razdoblje. Incidenti se mogu prijaviti na adresu elektroničke pošte ccert@cert.hr.

3.1. CSIRT (eng. Computer Security Incident Response Team)

CERT je naziv koji se dodjeljuje stručnim grupama koje se bave sigurnosnim incidentima. Većina grupa svojem nazivu dodjeljuje kraticu CERT ili CSIRT. CSIRT je organizacija koja je odgovorna za primanje, pregledavanje i odgovaranje na prijave sigurnosnih incidenata. Organizacija može pružati svoje usluge korporaciji, vladi, edukacijskoj ustanovi, regiji ili državi, istraživačkoj mreži ili privatnim klijentima. CSIRT može biti formalizirana grupa ili *ad hoc* grupa koja stvara rješenje specifično za određeni sigurnosni problem. Formalizirana skupina je oblikovana za rješavanje većine sigurnosnih incidenata, a *ad hoc* skupina se oblikuje posebno za rješavanje određenog sigurnosnog incidenta.

Čak i najbolja sigurnosna računalna infrastruktura ne može jamčiti da se neće dogoditi napadi na sustav. Kada se dogodi sigurnosni incident, bitno je da organizacija ima učinkovit način rješavanja problema. Zbog toga je potrebno da organizacija ima CSIRT. Brzina kojom se može prepoznati, analizirati i riješiti incident ograničit će štetu i smanjiti troškove oporavka od incidenta. CSIRT može biti na licu mjesta događaja, upoznat s ugroženim sustavom i provesti brzi odgovor na sigurnosni incident. Veze s drugim CSIRT i sigurnosnim organizacijama mogu olakšati podjelu strategija rješavanja problema i odmah ukazati na potencijalne probleme. Komunikacijom s ostalim CSIRT organizacijama mogu saznati koja su rješenja primijenjena za slične incidente što može utjecati na učinkovitost saniranja sigurnosnog incidenta. Također, CSIRT surađuje s ostalim područjima organizacije (npr. dijelovima organizacije zahvaćenim sigurnosnim incidentom, upravom i slično) u kojoj djeluje i osigurava da su novi sustavi koji se postavljaju zaštićeni i u skladu sa sigurnosnim politikama. Pomaže identificirati ranjiva područja i obaviti procjene ranjivosti i otkrivanje incidenata. CSIRT organizacija se može osnovati unutar neke druge organizacije, može biti dio postojeće IT (eng. Information technology) grupe, zatim može postojati kao dio neke druge sigurnosne grupe ili kao samostalna organizacija. Gdje god da se CSIRT nalazi, bitno je da ima upravljačku strukturu i potporu za posao koji obavlja.

3.2. Dužnosti CSIRT organizacije

Dužnosti CSIRT organizacije su pružanje pomoći, zaštita i osiguravanje kritičnih dijelova računalne mreže organizacije. Svaka CSIRT grupa odabire koje će usluge pružati u ovisnosti o tome gdje se nalazi. Koje god usluge CSIRT skupina odluči pružati, njezini se ciljevi moraju temeljiti na poslovnim ciljevima organizacije kojoj pružaju svoje usluge. CSIRT mora omogućiti potporu kritičnim poslovnim procesima i sustavima organizacije kojoj pruža usluge.

CSIRT se može usporediti sa vatrogasnom službom. Na isti način kao što vatrogasci gase požare, CSIRT pomaže organizacijama suzbijanje i oporavljanje od sigurnosnih napada i prijetnji. Proces koji CSIRT koristi za rješavanje sigurnosnih incidenata je upravljanje incidentima (o čemu će biti riječi u jednom od idućih poglavlja). Kao što vatrogasna služba trenira i obrazuje svoje zaposlenike, tako i CSIRT nudi usluge obrazovanja osoblja organizirajući osnovne i napredne tečajeve o sigurnosnim incidentima i prijetnjama, kako bi proaktivno djelovali na sigurnosne incidente. Tipovi proaktivnih usluga mogu biti:

- osvješćivanje osoblja u smislu računalne sigurnosti,
- otkrivanje upada u sustav,
- provjera sustava na ranjivosti i/ili
- dokumentiranje i razvoj programa.

Nabrojane proaktivne usluge mogu pomoći organizaciji u sprečavanju sigurnosnih incidenata i smanjiti vrijeme potrebno za odgovor na sigurnosni incident.

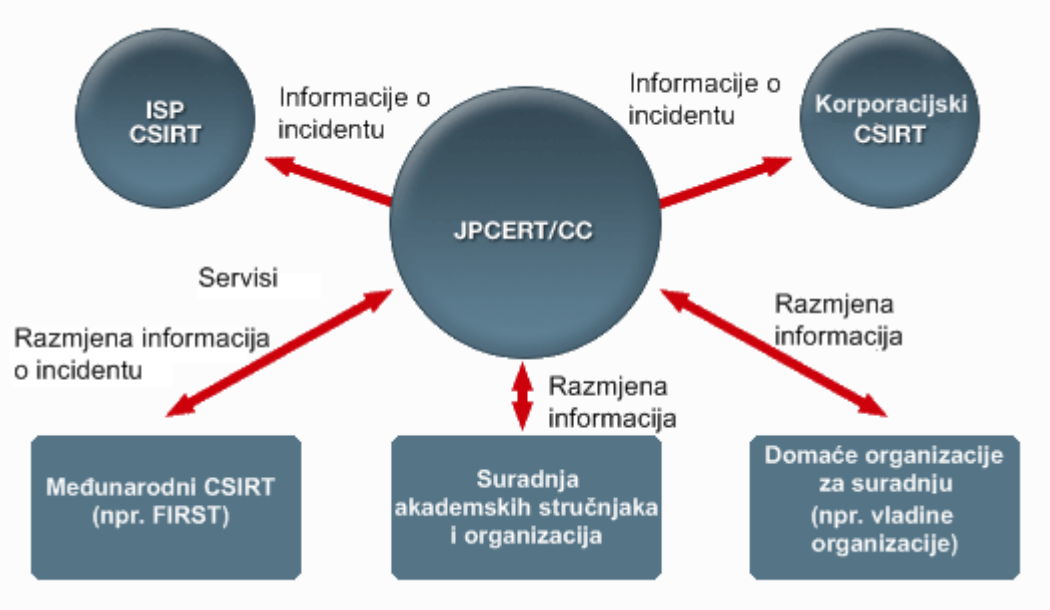
3.3. Tipovi CSIRT organizacija

Postoje različiti tipovi CSIRT organizacija. Neke su namijenjene pružanju potpore cijelim državama. Na primjer Japanski CERT (eng. Japan Computer Emergency Response Team Coordination Center - JPCERT/CC) je jedna od takvih organizacija. Osim toga, postoje i one CSIRT organizacije koje pružaju pomoć određenoj regiji u svijetu, kao što je AusCERT za Azijsko-Pacifičko područje, te one koje pružaju svoje usluge sveučilištima i komercijalnim organizacijama. Postoje i korporacijske grupe koje nude CSIRT usluge klijentima uz proviziju.

Neke od glavnih skupina CSIRT organizacija uključuju slijedeće:

- **Unutarnji CSIRT** – pruža usluge rukovanja incidentima svojim partnerskim organizacijama. To može biti CSIRT za banku, tvornicu, sveučilište ili vladinu agenciju.
- **Nacionalni CSIRT** – pruža usluge rukovanja incidentima državi. Na primjer, Japanski CERT (JPCERT/CC) ili Singapurski CERT (SingCERT).
- **Koordinacijski centri** – koordiniraju i olakšavaju upravljanje incidentima među raznim CSIRT organizacijama. Na primjer CERT koordinacijski centar (CERT/CC) ili US-CERT (eng. United States – CERT).
- **Centar za analizu** – usredotočen je na prikupljanje podataka iz različitih izvora i utvrđivanje trendova i uzoraka u pojavi sigurnosnih incidenata. Prikupljene se informacije mogu koristiti za predviđanje budućih incidenata te za rana upozorenja.
- **Prodavačke skupine** – upravljaju izvještajima o ranjivostima u svojim programskim paketima i uređajima. Mogu se formirati unutar organizacije i određivati jesu li proizvodi ranjivi te u slučaju da jesu razviti strategije koje uklanjaju problem i smanjuju posljedice.
- **Organizacije za rješavanje incidenta** - pružaju usluge upravljanja incidentima uz proviziju drugim organizacijama.

Slijedeća slika prikazuje primjer koordinacije i razmjene informacije JPCERT-a:



Slika 1. Suradnja JPCERT -a s CSIRT ostalim organizacijama

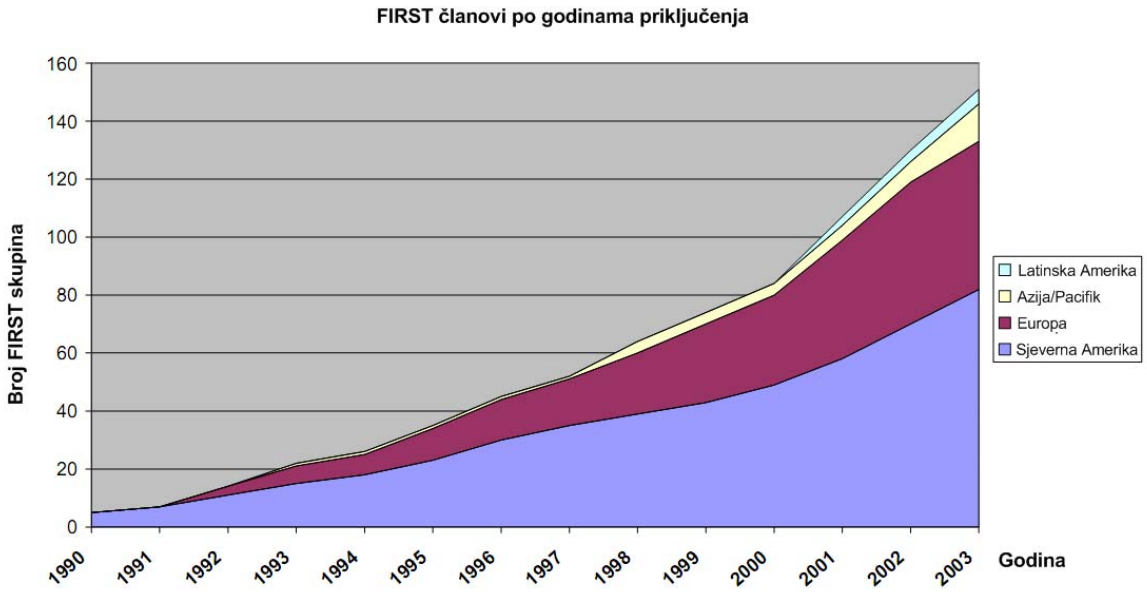
Postoji mnogo akronima za skupine koje se bave uklanjanjem sigurnosnih incidenata, a neke od njih su:

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Tablica 1. Popis skupina za rješavanje sigurnosnih incidenata

3.4. FIRST (eng. Forum of Incident Response and Security Teams)

FIRST je međunarodni forum za skupine i rješavanje incidenata osnovan 1990. godine (http://www.first.org/). To je organizacija koja okuplja različite sigurnosne grupe , kao što su skupine za odgovor na sigurnosne incidente koje rade za vladu, komercijalni sektor, akademske organizacije, i druge. Cilj FIRST-a je promicanje koordinacije i suradnje u sprečavanju incidenata, promicanje brze reakcije u slučaju incidenta te poticanje razmjene informacija među članovima i u globalnoj zajednici. FIRST broji više od 150 članova. Slika 2 prikazuje rast članova FIRST-a od 1991. godine do 2003. godine.



Slika 2. Rast broja članova FIRST-a

FIRST organizira godišnje konferencije (http://www.first.org/conference/) na kojima sigurnosne grupe razmjenjuju nove informacije o sigurnosnim prijetnjama, novim tehnikama i strategijama za pružanje pomoći u slučaju incidenta i produbljuju međusobnu suradnju. FIRST-ova konferencija je jedinstvena na svojem području. U svrhu prepoznavanja globalnog širenja računalnih mreža i zajedničkih problema s kojima su suočeni korisnici osobnih računala, konferencija se održava u različitim dijelovima svijeta. Prezentacije na konferenciji održavaju predstavnici iz različitih dijelova svijeta i uključuju posljednje prijavljene incidente, odgovore na njih i sprečavanje takvih incidenata u budućnosti. Uz to, incidenti koji se spominju u prezentacijama postaju osnova za poboljšanje računalne sigurnosti u cijelom svijetu. Prezentacije se mogu preuzeti sa FIRST-ovih web stranica, neke od njih se mogu naći na adresi http://conference.first.org/podcasts.aspx. Tu se nalaze prezentacije koje će se održati na 21. godišnjoj konferenciji u Kyotu 28.lipnja do 3. srpnja 2009. godine.

4. Postupak u slučaju sigurnosnog incidenta

Postupak u slučaju sigurnosnog incidenta ima nekoliko faza. Početna faza uključuje uspostavljanje i obrazovanje skupine za rješavanje incidenta, te pribavljanje potrebnih alata i resursa. Tijekom pripreme, organizacija također pokušava ograničiti broj incidenata koji će se dogoditi. To čine odabirom i primjenom niza sigurnosnih mjera temeljenih na rezultatima procjene rizika. Procjena rizika uključuje:

- otkrivanje općenitih prijetnji,
- otkrivanje specifičnih prijetnji,
- otkrivanje potrebne razine zaštite i
- usklađivanje potrebne razine zaštite.

Otkrivanje sigurnosnih propusta je potrebno kako bi se prijavio sigurnosni incident. Uzimajući u obzir ozbiljnost incidenta organizacija može poduzeti odgovarajuće mjere u smislu smanjivanja posljedica i oporavka od incidenta. Nakon što je incident riješen, organizacija objavljuje izvještaj koji detaljno opisuje sigurnosni incident. U izvještaju se navodi uzrok i trošak incidenta te koraci koje organizacija treba poduzeti kako bi spriječila takve incidente u budućnosti. Izvještaj se izrađuje radi prikupljanja dokaza i razmjene s ostalim CSIRT organizacijama. Često se u izvještaju mogu naći osjetljive informacije kao što su podaci koji su ugroženi sigurnosnim incidentom. Zbog toga je potrebno ograničiti pristup izvještajima o sigurnosnim incidentima i samo bi ovlaštene osobe trebale imati pristup takvim podacima. Osim toga, radi očuvanja povjerljivih podataka u izvještaju potrebno je kriptirati poruke elektroničke pošte vezane uz incident.

Glavne faze postupka u slučaju incidenta su:

1. priprema,
2. otkrivanje i analiza,
3. obuzdavanje, iskorjenjivanje i oporavak i
4. aktivnosti nakon incidenta.

Slika 3. Životni ciklus postupka u slučaju sigurnosnog incidenta

U slijedećim poglavljima opisani su koraci postupka u slučaju sigurnosnog incidenta.

4.1. Priprema

Priprema je jedna od najvažnijih faza postupka u slučaju sigurnosnog incidenta. Ako je skupina za rješavanje sigurnosnih incidenata pripremljena, moći će brzo i učinkovito ustanoviti je li se dogodio incident, analizirati ga, potpuno ga ukloniti, osigurati da se takav incident više neće dogoditi te postaviti bolju zaštitu na računalnu mrežu i programa na računalima.

Mnogo skupina za rješavanje sigurnosnih incidenata u sklopu pripreme grupira skupinu alata i materijala koji će biti potrebni u slučaju sigurnosnog incidenta. Svaka takva skupina alata i materijala obično sadrži prijenosno računalo na kojem se nalaze prikladni programi (npr. forenzički alati, osluškivači mrežnog prometa i drugi), uređaji za stvaranje sigurnosnih kopija, prazni mediji, osnovna mrežna oprema, žice, zakrpe za operacijski sustav i programske pakete. Važno je da je skupina alata i materijala uvijek ažurna.

Također, potrebno je održavati broj incidenata u sustavu niskim. Ako su metode zaštite sustava neprimjerene, pojavit će se mnogo incidenata i grupa za rješavanje incidenata neće moći pružiti kvalitetnu uslugu, odnosno incidenti će se rješavati sporo. To znači da posljedice napada mogu biti katastrofalne jer se problem neće ukloniti na vrijeme. Dok grupa za rješavanje incidenata odredi koji je od gomile prijavljenih incidenata pravi sigurnosni incident i koji predstavljaju veliku opasnost za

organizaciju, napadač će obaviti svoje zlonamjerne akcije i nanijeti štetu organizaciji. Prema tome potrebno je poboljšati sigurnosnu zaštitu organizacije, na primjer postavljanjem sigurnosne politike (više u dokumentu „Sigurnosna politika", dostupnom na adresi http://www.cert.hr/documents.php?id=381) i prije nego što se incident dogodio. U tu svrhu potrebno je provoditi periodične procjene rizika (više o upravljanju rizikom može se pročitati u dokumentu „Upravljanje sigurnosnim rizicima, dostupnom na http://www.cert.hr/documents.php?id=2).

4.1.1. Osnovni forenzički alati

Računalna forenzička analiza je postupak utvrđivanja činjenica nad digitalnim medijima primjenom različitih metoda. Najčešće se koristi u postupcima sudskog dokazivanja, a sastoji se od niza analitičkih metoda za otkrivanje, prikupljanje, ispitivanje i skladištenje podataka, te često podrazumijeva ispitivanje računalnih sustava kako bi se utvrdilo njihovo korištenje u ilegalnim ili neovlaštenim aktivnostima poput krađe poslovnih tajni, uništavanja intelektualnog vlasništva ili prijevare. Za otkrivanje, prikupljanje i ispitivanje podataka prilikom rješavanja sigurnosnog incidenta i forenzičke analize obično se koriste forenzički računalni programi i uređaji. U nastavku su forenzički alati podijeljeni u nekoliko osnovnih skupina.

- **Programski paketi za stvaranje preslika čvrstog diska (eng. Disk imaging software)** – bilježe strukturu i sadržaj čvrstog diska. Njihovom upotrebom moguće je kopirati podatke i sačuvati način na koji su datoteke organizirane, kao i njihove međusobne veze. Poznatiji alati ove skupine su: Acronis True Image, Paragon Drive Backup i FarStone Drive Clone.

  Pregled alata moguće je naći na web stranici http://disk-imaging-software-review.toptenreviews.com/.
- **Alati za rekonstrukciju programskih paketa i sklopovlja** – takvim je alatima moguće kopirati i rekonstruirati čvrste diskove bit po bit. Alati ne mijenjaju, odnosno ne uništavaju, postojeće podatke u procesu rekonstrukcije. Primjer forenzičkog alata koji nudi ovu opciju je EnCase.
- **Alati za rukovanje sažetcima poruka (eng. hash)** – koriste se za uspoređivanje izvornih podataka sa kopijama, analizu podataka te dodjelu jedinstvene oznake. Ako su sažetci izvornika i kopije jednaki, kopija npr. čvrstog diska je savršena replika izvornika. Alat koji nudi opciju rukovanja sažetcima poruka je ProDiscover.
- **Programi za dohvaćanje obrisanih podataka** – koriste se za otkrivanje lokacije podataka na računalu koji su označeni za brisanje, ali još uvijek nisu prepisani. Podaci koji nisu prepisani mogu se dohvatiti, no takvi podaci ne moraju uvijek biti cjeloviti i pohranjeni na istom mjestu. Primjeri spomenutih programa su DT Utilities Digital Rescue, Recover My Files, a detaljan popis alata koji pripadaju ovoj kategoriji moguće je pronaći na web stranici http://data-recovery-software-review.toptenreviews.com/.
- **Programi za dekriptiranje i otkrivanje zaporki** – primjeri takvih programa su FileZilla, CryptoTools i drugi.

4.2. Otkrivanje i analiza sigurnosnih incidenata

Za sve organizacije najizazovniji dio odgovora na sigurnosni incident je precizno otkrivanje i procjena mogućih incidenata te utvrđivanje je li se incident dogodio, ako jest, koja vrsta incidenta se dogodila i koliki mu je utjecaj na cijeli sustav. Tri su faktora koja čine ovaj postupak važnim:

1. Incidente je moguće otkriti na mnogo načina s različitom razinom detalja i povjerenja u alate i metode koje se koriste. Automatsko otkrivanje uključuje mrežno orijentirane i računalno orijentirane sustave za otkrivanje i sprečavanje napada (eng. Intrusion and detection prevention system – IDPS, još i IDS/IPS, u dokumentu će se koristiti kratica IDPS), programe za analizu računalnih dnevnika (eng. log) te antivirusne programe. IDPS može otkriti kada je napadač uspješno ugrozio sustav iskorištavanjem neke ranjivosti sustava. Osim toga, može bilježiti informacije o otkrivenim upadima u sustav u posebne dnevnike. Incidente je moguće otkriti i metodama koje nisu automatske (npr. korisnička prijava problema). Neke je incidente lako otkriti jer imaju očite naznake jasno vidljive dok je druge gotovo nemoguće otkriti bez upotrebe alata za automatsko otkrivanje incidenata.

2. Količina potencijalnih znakova incidenta je velika. Na primjer, nije neuobičajeno da organizacija primi tisuće, čak milijune prijava senzora za otkrivanje napada. Pregled web stranice alatom za otkrivanje ranjivosti može stvoriti stotine prijava na mrežnim i poslužiteljskim IDPS sustavima. Ukoliko napadač provodi takav pregled na deset web stranica, može preplaviti sustav tisućama IDPS prijava iz kojih je vrlo teško utvrditi koje su stvarne prijetnje, a koje nisu.
3. Potrebno je specijalističko znanje i opsežno iskustvo za valjanu i efikasnu analizu podataka vezanih uz incident. U većini organizacija mali je broj ljudi koji imaju spomenutu razinu znanja.

Znakovi napada mogu se svrstati u jednu od dvije kategorije:

- prethodnici i
- pokazivači napada.

Prethodnik napada ukazuje da bi se incident mogao dogoditi u nekoj bliskoj budućnosti, dok pokazivač napada ukazuje da se incident već dogodio ili da se upravo događa. Postoji mnogo tipova pokazatelja incidenta, a neki od njih su:

- mrežni senzor za otkrivanje napada koji prijavljuje pojavu prepisivanja spremnika na FTP (eng. File Transfer Protocol) poslužitelju,
- antivirusni program koji prijavljuje zarazu računala crvom,
- žalbe korisnika na spor pristup računalima i Internetu,
- administrator sustava otkrije datoteku s neobičnim znakovima u nazivu,
- korisnik zatraži pomoć od korisničke službe u vezi prijeteće poruke elektroničke pošte,
- poslužitelj pohranjuje zapise o promjenama u konfiguracijskim datotekama,
- program sadrži zapise o mnogim pokušajima prijava na nepoznati udaljeni sustav,
- administrator elektroničke pošte prijavljuje veliki broj odbačenih poruka elektroničke pošte sa sumnjivim sadržajem i
- mrežni administrator primjećuje promjene u obujmu mrežnog prometa.

U puno slučajeva organizacija može otkriti aktivnosti koje prethode sigurnosnom incidentu. Na primjer mrežni IDPS senzor bilježi neuobičajeno skeniranje priključaka (eng. port) usmjeren na grupu računala. Takav se događaj obično javlja prije napada uskraćivanja usluga (eng. Denial of Service) i pripada u kategoriju prethodnika napada. Drugi primjeri prethodnika napada su:

- zapisi web poslužitelja pokazuju upotrebu programa za pregled ranjivosti web stranica,
- najava novog načina zlouporabe ranjivosti poslužitelja elektroničke pošte i
- prijetnja skupine napadača.

Nije moguće otkriti svaki napad putem prethodnika napada. Neki napadi nemaju prethodnika, dok druge organizacija ne uspije otkriti na vrijeme. Ukoliko se otkriju prethodnici napada, organizacija ima priliku spriječiti incident upotrebom automatske obrane, odnosno IDPS sustava ili na primjer promjenama u postavkama vatrozida. U slučajevima kada prethodnici napada ukazuju na ozbiljni napad (kao što je DDoS napad i pokretanje zlonamjernog programskog koda), organizacija se može ponašati kao da se napad već dogodio te na taj način smanjiti rizik. Najmanje što organizacija može učiniti je pobliže pratiti određenu aktivnost.

4.2.1. Izvori prethodnika i pokazatelja napada

Prethodnici i pokazatelji napada prepoznaju se upotrebom različitih izvora, kao što su obavijesti antivirusnih programa, dnevnički zapisnici, javno dostupne informacije i korisnici. Sljedeća tablica sadrži popis uobičajenih izvora prethodnika i pokazatelja.

Izvor prethodnika ili pokazivača	Opis
Obavijesti računalnih programa	
Mrežni i računalni IDPS	IDPS proizvodi su osmišljeni za prepoznavanje sumnjivih događaja i za bilježenje bitnih podataka vezanih uz takve događaje. Zapisi sadrže podatke o vremenu, tipu, izvorišnim i odredišnim IP adresama te o korisničkom imenu (ako je primjenjivo i poznato). Većina IDPS proizvoda korisni niz uzoraka napada kako bi identificirali zlonamjernu aktivnost. Uzorci napada su neke pojave i događaji karakteristični za određeni napad.
Antivirusni programi	Antivirusni programi otkrivaju različite oblike zlonamjernog programskog koda i sprečavaju njihovo pokretanje na korisničkim računalima. Antivirusni su programi efikasni ako se njihove baze zlonamjernih programa redovito ažuriraju. Antivirusni bi se programi trebali primjenjivati na razini mreže i na razini osobnih računala.
Programi za provjeru besprijekornosti (integriteta) datoteka	Tokom incidenta napadač može promijeniti podatke u važnim datotekama. Programi za provjeru integriteta datoteka koriste *hash* algoritme (algoritmi za izračunavanje sažetka kao ulaz primaju poruku i proizvode jedinstveni izlaz koji se naziva sažetak poruke) za izračunavanje kriptografskog zbroja za provjeru dodijeljenog svakoj datoteci. Ako je datoteka promijenjena i zbroj za provjeru ne odgovara, vrlo je velika mogućnost da je datoteka neovlašteno promijenjena.
Zapisnici (eng. logs)	
Zapisnici operacijskih sustava, servisa i programa	Zapisi operacijskih sustava, usluga i programa pružaju obilje informacija, kao što su podaci o korisnicima koji su se prijavljivali na sustav i akcijama koje je pojedini korisnik izvodio. No u mnogim slučajevima zapisi u dnevnicima ne sadrže dokaze o napadu jer su ili izmijenjeni ili onemogućeni. Svaki sustav bi trebao imati omogućeno bilježenje događaja kako bi se olakšalo rukovanje incidentom. Na svim sustavima potrebno je periodički provjeriti besprijekornost zapisnika. Dnevnici se koriste za analizu i povezivanje informacija o događaju. Ovisno o informacijama o događaju utvrđuje se je li se ili nije pojavio incident.
Zapisnici mrežnih uređaja	Zapisnici vatrozidova i usmjerivača (eng. router) se ne koriste kao primarni izvor prethodnika i pokazivača. Pružaju informacije o blokiranim pokušajima spajanja. Mogu se koristiti za otkrivanje učestalog povezivanja na određene priključke, što može ukazivati na pripremu napada uskraćivanja usluga.
Javno dostupne informacije	
Informacije o novim ranjivostima i metodama zlouporabe	Praćenjem sigurnosnih preporuka te pojava novih metoda napada moguće je spriječiti pojavu nekih sigurnosnih incidenata. Upotrebom spomenutih informacija lakše je obaviti analizu novih metoda napada. Nacionalna baza ranjivosti (eng. National Vulnerability Database – NVD) je jedna od mnogih baza koje sadrže javno dostupne podatke o otkrivenim sigurnosnim ranjivostima. Organizacija kao što je CERT (eng. Computer Emergency Readiness Team) pruža svakodnevne novosti o računalnim prijetnjama i sigurnosnim ranjivostima. Sigurnosne preporuke na hrvatskom jeziku objavljuju se svakodnevno na web stranici CARNet CERTa: http://www.cert.hr/advs.php?lang=hr.

	Ljudi
Ljudi u organizaciji i izvan nje	Korisnici, administratori, mrežni administratori, mogu prijaviti znakove incidenta. Važno je provjeriti svaku prijavu jer često korisnici, ali i administratori ne posjeduju dovoljno znanja za utvrđivanje je li neki događaj znak pojave incidenta ili nije. Ljudi izvan organizacije također mogu pomoći u otkrivanju incidenta (na primjer prijavom neispravne web stranice).

Tablica 2. Izvori prethodnika i pokazatelja sigurnosnih incidenata

4.2.2. Analiza incidenta

Otkrivanje i analiza incidenta bio bi lagan posao kada bi se moglo jamčiti da su svaki prethodnik i pokazivač napada točni. Nažalost to nije slučaj. Na primjer, žalbe korisnika kojima izjavljuju da je poslužitelj nedostupan obično su netočne. Sustavi za otkrivanje napada često proizvode mnogo lažno pozitivnih (netočnih) pokazatelja napada. Spomenuti primjeri pokazuju kako otkrivanje i analiza incidenata mogu biti vrlo teški.

Za svakog bi se pokazatelja napada trebala utvrditi njegova valjanost. No problem je u tome što svi izvori znakova napada (prethodnika i pokazatelja) stvaraju dnevno milijune prijava. Pronalazak pravih sigurnosnih prijetnji u takvoj gomili informacija je zamoran posao. Čak i ako je pokazatelj napada ispravan, ne mora značiti da se dogodio incident. Neki pokazatelji napada, kao što su nedostupnost web poslužitelja ili izmjena kritičnih podataka mogu se dogoditi iz drugih razloga, od kojih je jedan ljudska pogreška. Općenito, ljudi zaduženi za sigurnosne incidente trebaju pretpostaviti da se incident dogodio sve dok se ne dokaže suprotno.

Utvrđivanje je li neki događaj incident ili nije katkad je stvar procjene. U mnogim slučajevima situaciju treba riješiti na isti način bez obzira je li potvrđeno da je vezana uz računalnu sigurnost ili ne. Na primjer, ako organizacija gubi vezu na Internet svakih 12 sati i nitko ne zna razlog zašto se to događa, potrebno je riješiti problem jednako brzo kao da se radi o sigurnosnom incidentu i upotrijebiti iste resurse za dijagnozu problema bez obzira na njegov uzrok. Neke incidente, kao što je neispravna web stranica, lako je otkriti. Međutim, mnogi incidenti nemaju jasnih simptoma. Mali znakovi, kao što je promjena u jednoj konfiguracijskoj datoteci, mogu biti naznaka sigurnosnog incidenta.

U rukovanju incidentima, otkrivanje incidenta najteži je zadatak. Ljudi odgovorni za analizu dvosmislenih, nejasnih, proturječnih i nepotpunih simptoma trebaju utvrditi što se točno dogodilo. Iako postoje tehnička rješenja, najbolja je opcija formirati grupu iskusnih i stručnih ljudi koji mogu efikasno analizirati prethodnike i pokazatelje napada i poduzeti primjerene akcije.

4.2.3. Dodjeljivanje prioriteta incidentima

Dodjeljivanje prioriteta incidentima najkritičnija je točka odluke u postupku upravljanja incidentima. Incidenti se ne bi smjeli rješavati prema pravilu „tko prvi njegovo“ nego je potrebno dodijeliti prioritete incidentima na osnovi dva faktora:

1. **Trenutni i potencijalni tehnički efekt na incident** – prilikom rješavanja incidenta potrebno je uzeti u obzir ne samo trenutni negativni efekt koji sigurnosni incident ima (npr. neovlašten pristup podacima), već i efekt koji će imati u budućnosti ako se brzo ne sanira (npr. ugrožavanje administratorskog korisničkog računa). Na primjer, crv koji se širi računalima u mreži nema velikog utjecaja na pojedina računala, ali promet kojeg će stvoriti unutar nekoliko sati mogao bi za posljedicu imati uskraćivanje usluga.
2. **Kritičnost resursa na koje utječe incident** – računalni resursi na koje utječe incident, kao što su vatrozidovi, web poslužitelji, Internet veza, korisnička računala i programi, imaju različitu značajnost u organizaciji. Kritičnost resursa temelji se na podacima ili uslugama, korisnicima, međuovisnosti s drugim resursima i vidljivosti (npr. javni web poslužitelj je izloženiji od unutarnjeg odjelnog web poslužitelja). Obično se propisuju SLA (eng. Service Level Agreement) dokumenti koji određuju vrijeme u kojem svaki ključni resurs mora biti saniran.

Kako bi se odredilo ocjenjivanje ozbiljnosti sigurnosnog incidenta potrebno je prvo utvrditi ocjene utjecaja za incident. Slijedeća tablica sadrži primjer dodjele takvih ocjena:

Vrijednost	Ocjena	Definicija
0.00	Ništa	Nema utjecaja na jednu organizaciju, odnosno agenciju, skupinu agencija ili kritičnu infrastrukturu
0.10	Minimalno	Zanemarivi utjecaj na jednu agenciju
0.25	Nisko	Srednji utjecaj na jednu agenciju
0.50	Srednje	Veliki utjecaj na jednu agenciju ili zanemariv utjecaj na skupinu agencija ili kritičnu infrastrukturu.
0.75	Visoko	Srednji utjecaj na više agencija ili kritičnih infrastruktura.
1.00	Kritično	Veliki utjecaj na više agencija ili kritičnih infrastruktura

Tablica 3. Ocjene utjecaja incidenta

Nakon postavljanja ocjena utjecaja organizacije trebali bi koristiti slijedeću tablicu za dodjelu ocjena kritičnosti na sustave koji su zahvaćeni incidentom.

Vrijednost	Ocjena	Definicija
0.10	Minimalno	Sustav ili infrastruktura koji nisu ključni (npr. osobna računala zaposlenika).
0.25	Nisko	Sustavi koji pružaju potporu za jedan zadatak (npr. DNS poslužitelji), ali nisu ključni za obavljanje te zadaće.
0.50	Srednje	Sustavi koji su ključni za obavljanje neke zadaće (npr. sustav za plaće) za jednu agenciju.
0.75	Visoko	Sustavi koji pružaju potporu više agencija ili sektora kritične infrastrukture (npr. korijenski DNS poslužitelji).
1.00	Kritično	Sustavi sa značajnom zadaćom za više agencija ili kritičnih infrastruktura.

Tablica 4. Ocjene kritičnosti incidenta

Navedena dva sustava ocjenjivanja trebaju se definirati za svaki incident kako bi se mogle odrediti ukupne ocjene utjecaja. Za utvrđivanje ukupnih ocjena utjecaja za pojedini incident organizacije bi trebale slijediti formulu:

```
ukupna ocjena utjecaja =
(trenutna ocjena utjecaja*2.5)+(predviđena ocjena utjecaja*2.5)+(ocjena kritičnosti sustava*5))
```

Upotrebom rezultata navedene formule, organizacije mogu primijeniti ukupne ocjene utjecaja incidentu, kao što pokazuje slijedeća tablica:

Vrijednost	Ocjena
00.00 – 00.99	Ništa
01.00 – 02.49	Minimalno
02.50 – 03.74	Nisko
03.75 – 04.99	Srednje
05.00 – 07.49	Visoko
07.50 – 10.00	Kritično

Tablica 5. Ukupne ocjene utjecaja incidenta

4.3. Suzbijanje, potpuno uklanjanje i oporavak od sigurnosnog incidenta

Nakon što je incident prošao fazu otkrivanja i analize, važno ga je ograničiti prije nego što se počne širiti i preopteretiti sustave i resurse te uzrokovati još veću štetu. Većinu je incidenata potrebno ograničiti pa se zbog toga metode suzbijanja incidenta moraju razmatrati još u ranim fazama postupka rješavanja sigurnosnog incidenta. Osnovni dio ove faze je donošenje odluka, kao što su gašenje sustava, isključivanje iz računalne mreže, onemogućavanje određenih funkcionalnosti i druge. Takve je odluke mnogo lakše donijeti ako su već određene strategije i procedure za ograničavanje incidenta. Organizacije bi trebale definirati prihvatljivi rizik u slučaju incidenta i razviti prikladne strategije. Strategije ograničavanja razlikuju se prema tipu incidenta. Na primjer, općenita strategija za ograničavanje širenja virusa koji se prenosi porukama elektroničke pošte je drugačija od one za rješavanje incidenta nastalog napadom uskraćivanja usluga u raspodijeljenoj računalnoj mreži. Kriterij za određivanje strategije uzima u obzir:

- potencijalnu štetu i krađu resursa,
- potrebu za očuvanjem dokaza,
- dostupnost usluga (npr. povezanost mreže računala),
- vrijeme i resurse potrebne za primjenu strategije,
- učinkovitost strategije(npr. djelomično ograničava širenje incidenta, potpuno ograničava incident i sl.) i
- trajnost rješenja (npr. privremeno zaobilaženje problema, trajno rješenje i sl.).

U pojedinim slučajevima organizacije mogu odgoditi ograničavanje širenja posljedica incidenta tako da mogu pratiti aktivnosti napadača. To se obično radi zbog prikupljanja dodatnih dokaza. Ako organizacija zna da je sustav ugrožen i dozvoljava da se incident širi, može se držati tu organizaciju neposredno odgovornom za napade koje napadač izvede upotrebom njihovog ugroženog sustava. Strategija koja uključuje odgađanje suzbijanja incidenta je vrlo opasna jer napadač može povećati razinu pristupa i ugroziti ostale sustave u vrlo kratkom vremenu. Obično se koristi zbog prikupljanja dokaza i otkrivanja identiteta napadača u slučajevima kada je moguće kontrolirati akcije napadača te kada je napad ograničen.

Tijekom postupka suzbijanja sigurnosnog incidenta, vlasnici sustava obično žele saznati identitet napadača. Iako su takve informacije bitne, pogotovo ako organizacija želi tužiti napadača na sudu, bitno je da se grupa za rješavanje sigurnosnog incidenta usredotoči više na suzbijanje incidenta nego na pronalazak napadača. Traženje napadača je proces koji grupi za suzbijanje sigurnosnog incidenta oduzima dragocjeno vrijeme u kojem trebaju ograničiti širenje incidenta (tj. štetu koju incident čini).

Nakon što je incident obuzdan, vrlo je vjerojatno da će biti potrebno iskorijeniti dijelove sustava kompromitirane incidentom. Takav postupak uključuje brisanje zlonamjernog programskog koda i onemogućavanje kompromitiranog korisničkog računa. Za neke incidente iskorjenjivanje nije potrebno, ili je već učinjeno tokom oporavka kada administratori vraćaju sustav u normalni rad i osiguraju sustav od sličnih incidenata. Oporavak se obično sastoji od akcija vraćanja i oporavka sustava. Takve akcije uključuju upotrebu neugroženih sigurnosnih kopija, ponovno izgrađivanje sustava, zamjenu ugroženih datoteka sa novim inačicama, promjenu zaporki i slično. Jednom kada se u nekom sustavu dogodi incident, taj je sustav ranjiv i na druge vrste napada jer su nakon prvog uspješnog napada mnogi resursi tog sustava dostupni na Internetu.

4.4. Specifičnosti vezane uz DoS napad

Napad uskraćivanja usluga (eng Denial of Service – DoS) je akcija koja sprečava ili onemogućuje ovlaštenu upotrebu računalne mreže, sustava ili programa iskorištavanjem resursa kao što je procesor (CPU), memorija, propusnost mreže i prostor na tvrdom disku. Primjeri DoS napada su:

- zagušenje propusnosti računalne mreže stvaranjem neuobičajeno velikog broja mrežnih paketa,
- slanje posebno oblikovanih TCP/IP paketa poslužitelju s namjerom rušenja operacijskog sustava poslužitelja,
- slanje ilegalnih zahtjeva aplikaciji u svrhu rušenja programa,

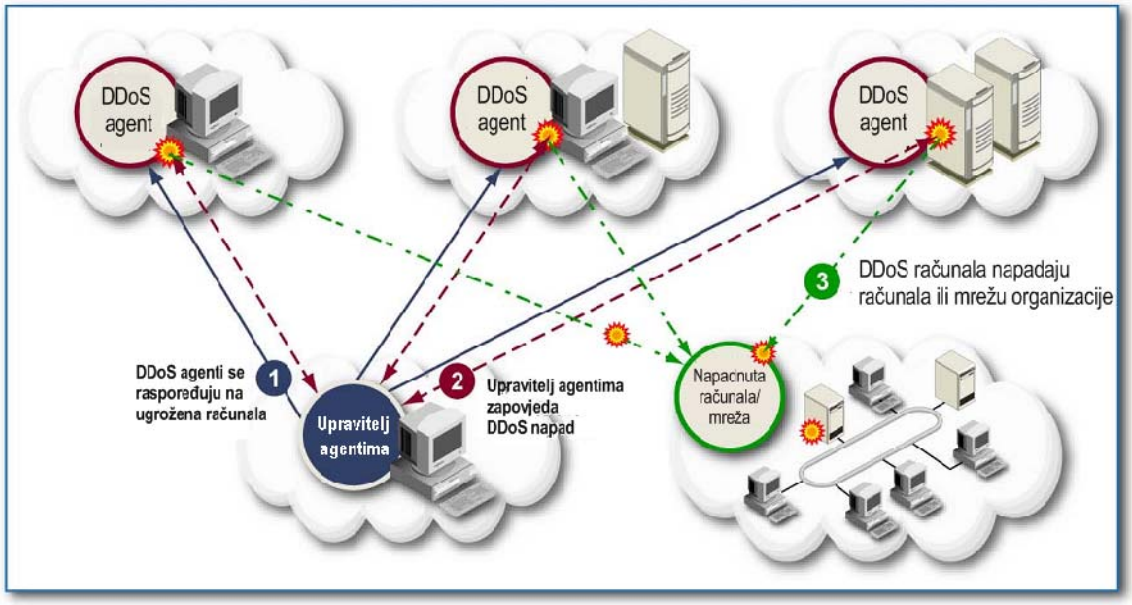
- slanje zahtjeva procesoru za koje mu treba puno vremena da ih obradi (npr. slanje zahtjeva za kriptiranjem svakog odgovora poslužitelja),
- uspostavljanje velikog broja sjednica za prijavu na poslužitelj u svrhu sprečavanja korisnika od započinjanja sjednica za prijavu,
- slanje signala na istoj frekvenciji na kojoj radi bežični Internet u svrhu onemogućavanja pristupa legitimnih korisnika i
- zauzimanje prostora na tvrdom disku stvaranjem velikih datoteka i slično.

Mrežna propusnost koju organizacije koriste je uglavnom vrlo velika te je nemoguće uzrokovati uskraćivanje usluga upotrebom jednog računala koje stvara velik promet. Umjesto upotrebe jednog računala, napadač izvodi raspodijeljeni napad uskraćivanja usluga (eng. Distributed Denial of Service – DDoS) i koordinira napad upotrebom više računala. Ako napadač koristi dovoljno računala, opseg stvorenog mrežnog prometa može iskoristiti ne samo resurse ciljanog računala, već i blokirati propusnost mreže za cijelu organizaciju. DDoS napadi su postali popularni i njihove posljedice mogu uzrokovati velike financijske gubitke za napadnutu organizaciju.

U DDoS napadima napadači tipično koriste dva tipa komponenti:

- agente - posebni programski kod koji se pokreće na ugroženim računalima i obavlja stvarni napad i
- upravitelje agenata (eng. handler) – program koji upravlja agentima, govori im kada trebaju obaviti napad, što trebaju napasti i na koji način trebaju izvesti napad.

Agenti se još nazivaju botovima, a skupina računala na kojima se pokreću agenti nazivaju se botnet mreže. U nekim slučajevima napadač ne mora koristiti upravitelja agenata već može izravno davati naredbe botovima. Napadači često koriste velike botnet mreže računala koje se sastoje od tisuća agenata koji izvode napad. Slijedeća slika prikazuje tri koraka DdoS napada.



Slika 4. DDoS napad

Na slici je moguće vidjeti da prvo napadač raspoređuje svoje botove (agente) na ugrožena računala, zatim upotrebom upravitelja agenata zapovijeda botovima što, kada i kako da napadnu te konačno botovi obavljaju zadane instrukcije i napadaju ciljanu organizaciju.

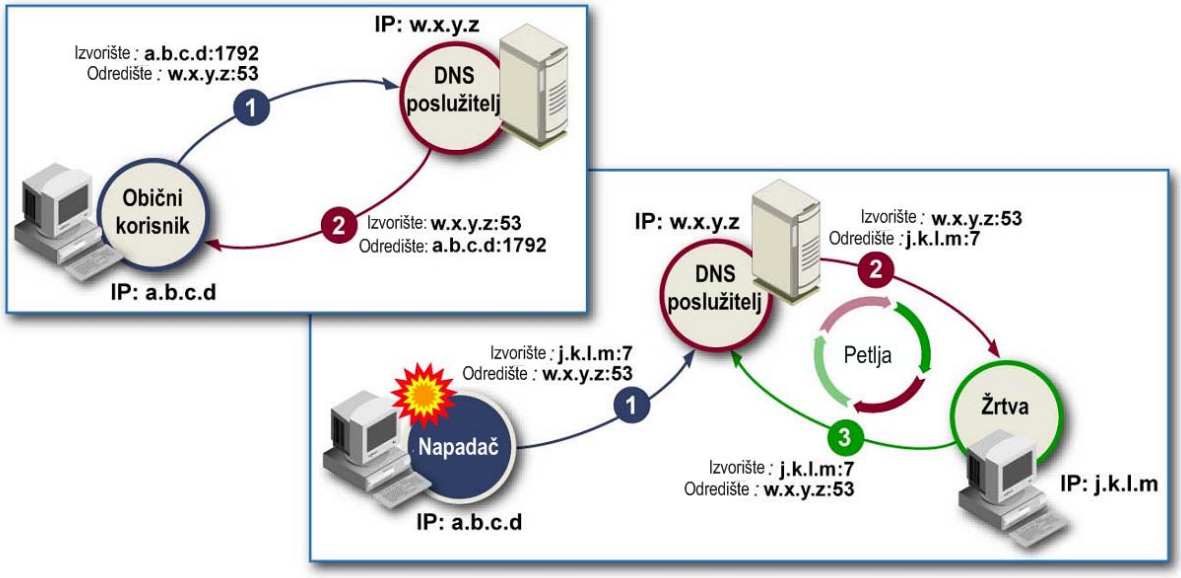
4.4.1. Reflektivni DoS napad

Kod izvođenja reflektivnog napada, napadač šalje velik broj zahtjeva s promijenjenom izvorišnom adresom servisu na posrednom računalu. Servis koji se napada obično koristi UDP (eng User Datagram Protocol) protokol, što olakšava napadačima prikladnu promjenu izvorišne adrese zahtjeva u svrhu sakrivanja pravog izvora napada. Posredno računalo svoje odgovore šalje na promijenjenu izvorišnu adresu. Kako posredno računalo zapravo izvodi napad, računalo s kojeg

napadač šalje zahtjeve naziva se reflektor. Tokom reflektivnog napada, uskraćivanje usluga se javlja na računalu čija je adresa podmetnuta, a često i na posrednom računalu. Servisi koji se obično napadaju spomenutom metodom su na priključnicama 7 (echo), 19 , 53 - DNS (eng. Domain Name System), 161 - SNMP (eng. Simple Network Management Protocol), 500 - ISAKMP (eng. Security Association and Key Management Protocol).

U nekim slučajevima napadač može koristiti dva reflektora kako bi ograničio nastanak stanja uskraćivanja usluga. Napadač može slati zahtjeve reflektoru koristeći kao podmetnutu izvorišnu adresu, IP adresu nekog drugog računala, umjesto adrese računala s kojeg šalje zahtjeve. U tom slučaju kada posredno računalo šalje odgovore, slat će ih na adresu drugog reflektora. Ako se ispravno izabere kombinacija reflektivnih računala, napadač može stvoriti petlju između dva reflektivna računala. Dakle, napadač može stvoriti petlju između echo i DNS usluga te onemogućiti njihovo korištenje.

Većina se reflektivnih napada može spriječiti vatrozidom koja odbacuju sumnjive kombinacije izvorišnih i odredišnih priključaka. Slijedeća slika skicira tijek reflektivnog napada.



Slika 5. Reflektivni DoS napad

Prvi dijagram pokazuje uzorak mrežnog prometa normalnog DNS upita i odgovora. DNS klijent šalje upit sa svojeg UDP priključka 1792 na poslužiteljev DNS priključak 53. DNS poslužitelj odgovara na upit slanjem UDP paketa klijentu na priključak 1792.

Drugi dijagram pokazuje reflektivni napad na DNS poslužitelja. Napadač šalje paket DNS poslužitelju, međutim, šalje i posebno oblikovani paket koji koristi kao izvorišnu adresu računala koji je žrtva napada, dakle **j.k.l.m** IP adresu. Ako računalo koje je žrtva napada nudi uslugu echo, može stvoriti paket koji vraća primljene podatke natrag DNS poslužitelju. U tom slučaju nastaje petlja između DNS poslužitelja i računala koje je žrtva napada.

4.4.2. Prethodnici i pokazatelji DoS napada

DoS napad je moguće otkriti putem specifičnih prethodnika i pokazatelja koji su prikazani u tablicama 6 i 7. Tablica 6 daje popis mogućih prethodnika DoS napada s objašnjenjima svake moguće akcije i pruža preporučeni odgovor za sprečavanje pojave sličnog incidenta. Tablica 7. sadrži popis zlonamjernih akcija, kao što su mrežni DoS, DoS napad na operacijski sustav i DoS napad na program te moguće pokazatelje spomenutih akcija. Svaka organizacija može stvoriti vlastite tablice koje će uključivati prethodnike i pokazatelje specifične za sustav pojedine organizacije te na taj način olakšati i ubrzati proces rješavanja sigurnosnog incidenta.

Prethodnici	Odgovor
DoS napadu obično prethodi izviđanje – stvaranje prometa u svrhu utvrđivanja najbolje metode napada	Ako administrator otkrije neobičnu aktivnost za koju je procijenio da bi mogla biti priprema za DoS napad, organizacija može blokirati napad postavljanjem vatrozida da sprečava upotrebu određenog protokola na ranjivom računalu.
Novi alat za stvaranje DoS stanja može biti prijetnja organizaciji	Proučavanje novog alata i postavljanje sigurnosnih mjera tako da alat ne može naštetiti sustavu.

Tablica 6. Prethodnici DoS napada

Zlonamjerna akcija	Pokazatelji
Mrežni DoS napad na određeno računalo	• korisnik javlja nedostupnost sustava • neobjašnjivi gubitci mrežne povezanosti • prijave upada u mrežu • prijave upada u klijentska računala • zauzimanje većeg opsega mrežnog prometa nego uobičajeno • pojava velikog broja veza na jedno računalo • asimetrični uzorak mrežnog prometa (dolazni promet je veći od odlaznog) • promjene u dnevničkim zapisima vatrozidova i usmjerivača • pojava paketa s neobičnom izvorišnom adresom
Mrežni DoS napad na određenu mrežu računala	• prijave nedostupnosti sustava i mreže • neobjašnjivi gubitci mrežne povezanosti • prijave upada u mrežu • zauzimanje većeg opsega mrežnog prometa nego uobičajeno • pojava velikog broja veza na jedno računalo • asimetrični uzorak mrežnog prometa (dolazni promet je veći od odlaznog) • promjene u dnevničkim zapisima vatrozidova i usmjerivača • pojava paketa s neobičnom izvorišnom adresom • pojava paketa s nepostojećom odredišnom adresom
DoS napad na operacijski sustav određenog računala	• prijave nedostupnosti programa i sustava • prijave upada u mrežu i računalo • promjene dnevničkih zapisa operacijskog sustava • pojava paketa s neobičnom izvorišnom adresom

DoS napad na program na određenom računalu	• prijave nedostupnosti programa • prijave upada u mrežu i računalo • promjene dnevničkih zapisa programa • pojava paketa s neobičnom izvorišnom adresom

Tablica 7. Pokazatelji DoS napada

Iako ove tablice mogu biti korisne u analiziranju incidenata, nedostaju im pokazatelji koji se mogu povezati s bezazlenim akcijama. Bezazlene i zlonamjerne akcije mogu imati slične simptome, što otežava utvrđivanje je li se dogodio sigurnosni incident ili nije. Prema tome, u tablicu 7. bi trebalo dodati i bezazlene aktivnosti. Na primjer, u slučaju kada organizacija izgubi vezu na Internet, mnogi simptomi, ali ne i svi mogu biti slični DDoS napadu.

4.5. Specifičnosti vezane uz napade pokretanjem zlonamjernog programskog koda

Kada se govori o zlonamjernim programima, misli se na programe ili dijelove programskog koda koje napadač podmetne i pokrene s namjerom promjene ili uništavanja podataka, ili nekim drugim razlogom ugrožavanja računala, kao što je narušavanje povjerljivosti, besprijekornosti i dostupnosti podataka, programa i operacijskog sustava. Postoji mnogo vrsta zlonamjernih programa, a neki od njih su virusi, crvi, trojanski konji, zlonamjerni programski kod i drugi. Zlonamjerni programi također uključuju alate kao što su Backdoor i rootkit, programi za praćenje pritisaka tipki na tipkovnici, programi za praćenje cookie datoteka i slično.

Virusi su programi koji se sami umnožavaju, odnosno prave kopije samog sebe, i šalju vlastite kopije drugim datotekama, programima i računalima. Virusi se umetnu u određeni program i šire se kada se program pokrene, npr. otvaranje određene datoteke. Virusi imaju različite svrhe, neki su osmišljeni kao bezazlene pošalice, a neki kao uništavači podataka. Neki se virusi pretvaraju da su pošalice dok zapravo uništavaju određene podatke. Dva su glavna tipa virusa, sastavljeni (eng. compiled) virusi, namijenjeni operacijskom sustavu, i interpretacijski virusi namijenjeni određenoj aplikaciji.

Crvi su programi koji se umnožavaju kopiranjem i nije im, kao kod virusa, potreban posredni program da zaraze računala. Crvi se sami šire i mogu stvoriti potpuno funkcionalne kopije koje se pokreću bez pomoći korisnika. Crvi iskorištavaju ranjivosti programa i postavki sustava, kao što je nezaštićena veza za dijeljenje datoteka. Većina crva ima namjenu iskorištavanja i preopterećenja resursa sustava. Osim toga, mnogi crvi nanose štetu sustavima instaliranjem *backdoor* programa i izvođenjem DDoS napada. Postoje dvije glavne vrste crva, crvi namijenjeni mrežnim uslugama i crvi namijenjeni elektroničkoj pošti.

Trojanski konji su programi koji se ne mogu sami umnožavati. Oni se pretvaraju da su bezazleni programi, no zapravo imaju zlonamjernu svrhu, kao što je zamjena postojećih datoteka zlonamjernim. Teško ih je otkriti jer se obično pretvaraju da obavljaju neku korisnu akciju (npr. zaštitu od virusa).

4.5.1. Prethodnici i pokazatelji napada

Organizacije trebaju težiti brzom otkrivanju zlonamjernih programa jer se zaraze mogu proširiti sustavom u vrlo kratkom roku (u pitanju su minute). Rano otkrivanje zlonamjernog programskog koda može pomoći organizaciji da smanji broj zaraženih računala, što je važno za fazu oporavka od incidenta. Zlonamjeran programski kod ima mnogo oblika te ga je moguće otkriti preko različitih prethodnika i pokazatelja incidenta. Tablice 8 i 9 sadrže popis čestih prethodnika i pokazatelja napada zlonamjernim programima.

Prethodnici	Odgovor
Objava o pojavi novog zlonamjernog programa (virusa, crva…) namijenjenog programimama koje koristi organizacija	Proučavanje novog zlonamjernog programa kako bi se utvrdilo je li objava o pojavi stvarna. Ako se utvrdi da se zaista pojavio novi zlonamjerni program, potrebno je ažurirati bazu Uzorka zlonamjernih programa antivirusnog alata. Ako uzorak zlonamjernog programa nije dostupan, potrebno je pokušati spriječiti napad na druge načine, kao što je postavljanje poslužitelja elektroničke pošte tako da blokiraju poruke s određenim sadržajem.
Antivirusni program otkrije i uspješno ukloni ili stavi u karantenu zaraženu datoteku	Utvrđivanje kako je zlonamjerni kod ušao u sustav i koju je ranjivost iskoristio, te nakon toga uklanjanje utvrđenih ranjivosti.

Tablica 8. Prethodnici napada zlonamjernim programima

Zlonamjerna akcija	Pokazatelj
Virus koji se širi putem elektroničke pošte zarazio je računalo	• Antivirusni program prijavljuje zaražene datoteke • Iznenadan porast broja primljenih i poslanih poruka elektroničke pošte • promjene u predlošcima za određene dokumente i tablice • pojava obrisanih, djelomičnih i nedostupnih datoteka • pojava neobičnih prozora, poruka i grafičkih prikaza • sporo pokretanje programa • nestabilnost sustava • pristupanje podacima s administratorskim ovlastima
Crv koji se širi putem ranjive usluge zarazio je računalo	• Antivirusni program prijavljuje zaražene datoteke • pojava skeniranja priključaka i neuspjelih uspostava veze na ranjiv servis • povećana upotreba računalne mreže • usporeno pokretanje programa i nemogućnost pokretanja određenih programa • nestabilnost sustava • pristupanje podacima s administratorskim ovlastima
Instalacija i pokretanje trojanskog konja	• Antivirusni program prijavljuje datoteke s trojanskim konjima • prijava upada u mrežu i komunikacije trojanskog konja s poslužiteljima • pojava dnevničkih zapisa u vatrozidu i usmjerivaču o komunikaciji trojanskog konja s klijentima i poslužiteljima • uspostavljanje veza između računala i nepoznatih udaljenih sustava

	• neočekivano otvaranje pojedinog priključaka • pokretanje nepoznatih procesa • porast mrežnog prometa prema vanjskim računalima • sporo i onemogućeno pokretanje programa • nestabilnost sustava • preuzimanje administratorskih ovlasti
Zlonamjerni mobilni kod na web stranici se koristi za kopiranje virusa, crva ili trojanskog konja na računalo	• pokazatelji spomenuti do sada • pojava neobičnih prozora sa zahtjevima za dozvolom obavljanja nekih akcija • pojava neobičnih grafičkih prikaza, kao što je preklapanje prozora s spomenutim porukama
Zlonamjerni mobilni kod na web stranici iskorištava ranjivosti računala	• pojava neobičnih prozora sa zahtjevima za dozvolom obavljanja nekih akcija • pojava neobičnih grafičkih prikaza, kao što je preklapanje prozora s spomenutim porukama • iznenadni porast broja primljenih i poslanih poruka elektroničke pošte • uspostava veza između računala i nepoznatih udaljenih sustava • preuzimanje administratorskih ovlasti
Korisnik primi lažnu dojavu o virusu (eng. hoax)	• Izvorište poruke nije ovlašteni centar za sigurnost, kao CERT, već vladina agencija ili važna službena osoba • ne pojavljuje se u drugim izvorima • terminologija poruke izaziva paniku i osjećaj hitnosti • potiče primatelje poruke na brisanje određenih datoteka i slanje poruke drugim korisnicima

Tablica 9. Pokazatelji napada

4.6. Specifičnosti vezane uz neovlašteni pristup

Neovlašteni se pristup sustavu javlja kada napadač preuzme ovlasti i pristupi sustavima kojima inače ne bi smio pristupiti. Napadač obično preuzima korisničke ili administratorske ovlasti iskorištavanjem ranjivosti operacijskog sustava ili programa. Kako bi to učinio, napadač krade korisnička imena i zaporke. Do tih podataka može doći, osim zlouporabom sigurnosnih ranjivosti i socijalnim inženjeringom (više o ovim oblicima napada moguće je pronaći u dokumentima: dokumentima „Socijalni inženjering“ i „Socijalni inženjering putem VoIP tehnologije“, dostupnim na službenim stranicama CERTa). Primjeri neovlaštenog pristupa su:

- preuzimanje administratorskih ovlasti poslužitelja elektroničke pošte,
- postupci koji mijenjaju ili brišu sadržaje web stranica organizacije,
- pogađanje ili razbijanje zaporki,
- neovlašteno pregledavanje ili kopiranje osjetljivih podataka, kao što su zapisi o plaćama, medicinske informacije, brojevi kreditnih kartica,

- pokretanje programa za prisluškivanje paketa na radnoj stanici u svrhu krađe korisničkih imena i zaporki,
- iskorištavanje dojave o zabrani pristupa na anonimni FTP poslužitelj u svrhu širenja piratskih programa i glazbenih datoteka,
- lažno predstavljanje putem telefona, resetiranje zaporki elektroničke pošte i
- upotreba tuđih radnih stanica

4.6.1. Prethodnici i pokazatelji incidenta

Sigurnosni se incidenti neovlaštenog pristupa javljaju u mnogo oblika i moguće ih je otkriti preko različitih tipova prethodnika i pokazatelja incidenta. Tablica 10 sadrži popis mogućih prethodnika napada neovlaštenim pristupom, objašnjava razloge zašto se izvodi pojedina akcija i preporuča prikladni odgovor. Tablica 11 daje popis zlonamjernih akcija, kao što su neovlaštena uporaba korisničkog računa, i pokazatelje tih akcija. Spomenute tablice svaka organizacija prilagođuje svojim sustavima.

Prethodnici	Odgovor
Neovlaštenom pristupu obično prethode aktivnosti kao što su mapiranje računala i usluga u svrhu otkrivanja ranjivosti, skeniranje priključaka, računala, izvođenje naredbi ping i traceroute i slično. Spomenuta aktivnost otkriva se IDPS programima i analizom dnevničkih zapisa.	Potrebno je potražiti uočljive promjene u sustavu, kao što su iznenadni porast interesa za određeni priključak ili računalo. Ako ova aktivnost ukazuje na ranjivost koju napadač može iskoristiti, organizacija možda može na vrijeme spriječiti napad uklanjanjem ranjivosti.
Objavljen je u javnosti novi način za neovlašteno pristupanje sustavu organizacije što predstavlja veliku prijetnju organizaciji.	Organizacija bi trebala proučiti tu novu metodu i sukladno primijeniti sigurnosne mjere.
Korisnici prijavljuju pokušaje socijalnog inženjeringa – napadači ih pokušavaju prevariti na otkrivanje osjetljivih informacija, kao što su zaporke, ili ih potiču na preuzimanje i pokretanje programa u privitcima poruka elektroničke pošte.	Skupina za rješavanje incidenta treba poslati obavijest svim korisnicima sa savjetima kako se oduprijeti socijalnom inženjeringu. Također, potrebno je otkriti za koje resurse su zainteresirani napadači jer je moguće da socijalni inženjering prethodi napadu na te resurse.
Osoba ili sustav mogu zabilježiti fizički pokušaj pristupa resursima (npr. osoba koja nije zaposlena u organizaciji pokuša otvoriti ormarić sa žicama, nepoznata osoba koristi poništenu identifikacijsku karticu i slično).	Ako je moguće, osiguranje bi trebalo zadržati i ispitati tu osobu te pojačati osiguranje ako se utvrdi da je to potrebno.

Tablica 10. Prethodnici neovlaštenog pristupa

Zlonamjerna akcija	Pokazatelj
Preuzimanje administratorskog korisničkog računa za pristup računalu u organizaciji	• postojanje neovlaštenih alata vezanih uz sigurnost • neobičan promet između računala u organizaciji (npr. napadač može iskoristiti jedno računalo za napad na druga računala) • promjene u postavkama sustava, kao što su promjene ili dodaci u procesima i/ili servisima, otvaranje neočekivanih priključaka, ponovno pokretanje sustava, promjene u dnevničkim zapisima i podacima, postavljanje mrežne kartice da prisluškuje promet, stvaranje nove administratorske grupe korisnika • promjene osjetljivih datoteka, oznaka vremena i ovlasti izvođenja programa, sustavnih i konfiguracijskih datoteka • neobična upotreba korisničkih računa (npr. slanje neočekivanih naredbi nekog korisnika, pojava velikog broja zaključanih računa, istovremena pojava upotrebe istog računa na različitim računalima) • značajne promjene u iskorištenosti resursa (npr. procesora, računalne mreže) • prijave korisnika o nedostupnosti sustava • prijave upada u sustav • pojava novih datoteka i direktorija s neobičnim imenima • napadač kontaktira organizaciju i izjavljuje da je ugrozio sustav
Neovlaštena izmjena podataka (npr. promjena sadržaja web stranica)	• prijave provala u sustav • povećana upotreba resursa • prijave promjene podataka (npr. sadržaja web stranica) • promjene u osjetljivim datotekama • pojava novih datoteka i direktorija s neobičnim imenima • povećana upotreba resursa
Neovlaštena uporaba korisničkih računa	• pokušaji pristupa osjetljivim datotekama (npr. datotekama sa zaporkama) • neobična upotreba korisničkih računa (npr. slanje neočekivanih naredbi nekog korisnika, pojava velikog broja zaključanih računa, istovremena pojava upotrebe istog računa na različitim računalima) • zapisi na posrednim web poslužiteljima pokazuju preuzimanje napadačkih alata
Fizička provala u organizaciju	• prijave korisnika o nedostupnosti sustava • neočekivane promjene u statusu sustava

	(npr. ponovno pokretanje sustava, nestabilnost sustava) • nedostaju računalni uređaji (npr. ukradeni čvrsti diskovi i druge komponente) • pojava neovlaštenih novih uređaja u mreži
Neovlašten pristup podacima (npr. datotekama sa zaporkama, bazi podataka i slično)	• prijave pokušaja upada u sustav korištenjem FTP, HTTP i drugih protokola • postojanje zapisa o pokušajima pristupa osjetljivim datotekama

Tablica 11. Pokazatelji neovlaštenog pristupa

Neovlašteni pristup napadača obično se odvija u nekoliko koraka. Napadač će prvo obaviti izviđanje kako bi mapirao mrežu, identificirao računala u organizaciji, odredio koji je operacijski sustav u upotrebi, koje se programi i usluge nalaze na računalima. Zatim utvrđuje koje su sigurnosne ranjivosti sustava prisutne i na koji ih način može iskoristiti. Nakon što je upoznao sustav, napadač će izvesti svoj napad. Zbog toga je važno da organizacije obrate pažnju na izviđačke aktivnosti napadača i prepoznaju ih kao takve.

4.7. Aktivnosti nakon incidenta

Bitan dio rješavanja incidenta su učenje i poboljšavanje. Svaka grupa za suzbijanje incidenata treba učiti na riješenim incidentima kako bi mogli što bolje djelovati u budućnosti koja donosi nove prijetnje i profinjenije napade. Mnoge organizacije održavaju sastanke na kojima se raspravlja o riješenim incidentima i lekcijama koje se mogu iz tih incidenata naučiti. Pitanja na koja se odgovara na takvim sastancima su:

- Što se točno dogodilo i u koje vrijeme?
- Koliko su dobro osoblje i uprava 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?
- Što bi osoblje i uprava učinila 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. Izvještaji sa sastanaka vezanih uz riješeni sigurnosni incident dobar su materijal za učenje novih članova grupe, kao i za obnavljanje sigurnosnih politika i procedura za suzbijanje sigurnosnih incidenata.

5. Zaključak

Razvojem tehnologije i računalne znanosti nastaju i nove metode napada i ugrožavanja sustava i računalnih mreža. Ti su napadi sve opsežniji i razorniji. Organizacije osim provođenja procjena rizika i poboljšavanja zaštite sustava trebaju grupe za rješavanje sigurnosnih incidenata jer je neke sigurnosne incidente i napade nemoguće spriječiti. Zaštitom i osiguravanjem kritičnih dijelova računalne mreže bave se CSIRT organizacije. Postoje različiti tipovi CSIRT organizacija koje pružaju svoje usluge zemljopisnim regijama, državama, korporacijama ili privatnim osobama. Kako bi se ograničilo djelovanje i širenje sigurnosnih incidenata utvrđeni su postupci za rješavanje sigurnosnih incidenata koji čine četiri faze (priprema, otkrivanje i analiza, obuzdavanje/iskorjenjivanje i oporavak) te aktivnosti nakon incidenta. Nakon suzbijanja incidenta potrebno je detaljno proučiti okolnosti nastanka incidenta, pregledati prikupljene podatke tokom obuzdavanja sigurnosnog incidenta te utvrditi što se može poboljšati te kako spriječiti slične incidente u budućnosti.

Sigurnosni incidenti su neizbježni i prema tome treba ih prihvatiti kao takve. Primjenom utvrđenih postupaka za rješavanje sigurnosnih incidenata moguće je u većini slučajeva ukloniti nastalu štetu i poboljšati sigurnost napadnutog sustava.

6. Reference

[1] Computer security incident handling guide, Karen Scarfone, Tim Grance, Kelly Masone, ožujak 2008., http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

[2] CSIRT FAQ, http://www.cert.org/csirts/csirt_faq.html

[3] CARNet CERT, http://www.cert.hr/plainhtmlpage.php?id=1&lang=hr

[4] ZSIS, http://www.zsis.hr/site/CERTZSISa/Ra%C4%8Dunalnosigurnosniincidenti/tabid/107/Default.aspx

[5] CERT FAQ, http://www.cert.org/faq/cert_faq.html

[6] FIRST konferecije, http://conference.first.org/ CERT, http://www.cert.hr

[7] FIRST, http://www.first.org/

[8] JPCERT, http://www.jpcert.or.jp/english/ir/

[9] Računalni napad u Hrvatskoj, http://www.vjesnik.hr/pdf/2004%5C05%5C02%5C39A39.PDF