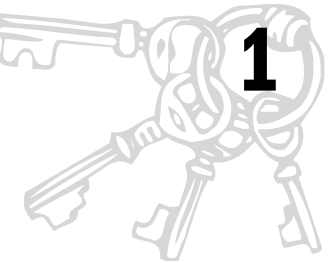


1 Pretnje, napadi, sigurnost i metode zaštite

Zbog ubrzanog razvoja i sve većeg značaja računarskih i komunikacionih tehnologija neophodnih za savremeno poslovanje, problemu sigurnosti mora se posvetiti posebna pažnja. Zahtevi koji se odnose na sigurnost informacija unutar neke organizacije značajno su se promenili u nekoliko poslednjih decenija. Pre nego što su se počeli masovno primenjivati uređaji za obradu podataka, podaci koji su smatrani značajnim za jednu organizaciju, štitili su se fizičkim i administrativnim merama.

Sa uvođenjem računara, pojavila se potreba i za novim i automatizovanim alatima za zaštitu datoteka i drugih informacija smeštenih na računar. To je posebno značajno za deljene sisteme, kao što su sistemi s deljenjem datoteka, kojima se pristupa preko javnih računarskih mreža. Važna promena koja je takođe uticala na sigurnost jeste pojava i širenje distribuiranih sistema, kao i širenje primene računarskih mreža i komunikacija. Opšte ime za skup alata, procedura, pravila i rešenja čija je namena da umreženi sistem odbrane od napada, glasi **sigurnost računarskih mreža** (engl. *computer network security*).

U ovom poglavlju opisani su osnovni pojmovi koji se odnose na sigurnost računarskih mreža. Najpre se definišu pojmovi napad, rizik, pretnja, ranjivost i vrednost imovine, pri čemu se posebna pažnja posvećuje sistematizaciji pretnji i napada. Zatim su – kroz opis velikog trojstva sigurnosti – navedeni ciljevi koje zaštitom treba postići, navedene su i ukratko opisane sigurnosne usluge, modeli i strategije ostvarivanja sigurnosti. Na kraju poglavlja klasifikovane su i ukratko analizirane različite metode zaštite.

Sadržaj poglavlja:

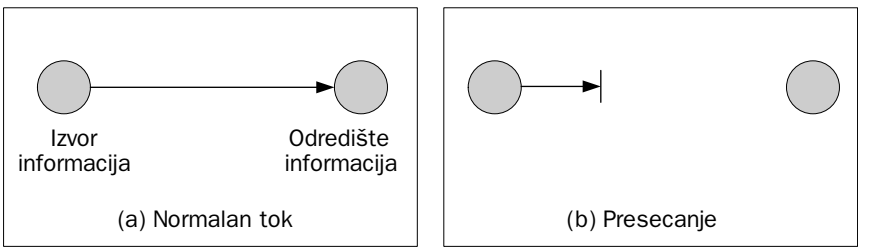
1.1 Napadi i pretnje

Da bi se efikasno procenile sigurnosne potrebe neke organizacije i da bi se odabrali različiti sigurnosni proizvodi, pravila, procedure i rešenja, rukovodiocu u firmi koji je zadužen za sigurnost potreban je sistematičan način definisanja zahteva u pogledu sigurnosti i kategorizacije pristupa koji obezbeđuju da se ti zahtevi zadovolje. Jedan pristup je da se razmotre tri aspekta sigurnosti informacija:

- **napad na sigurnost** (engl. *security attack*) – bilo koja akcija koja ugrožava sigurnost informacija;
- **sigurnosni mehanizam** (engl. *security mechanism*) – mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada;
- **sigurnosna usluga** (engl. *security service*) – usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.

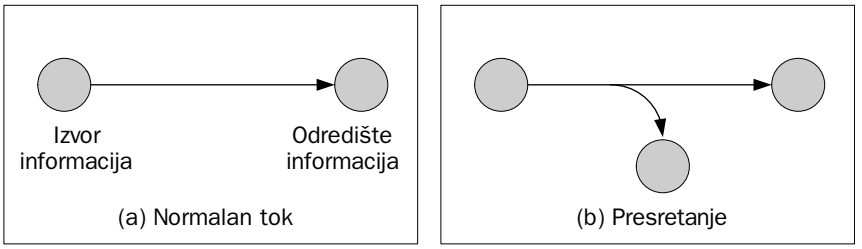
U osnovi, napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža. Postoje različite vrste napada, ali se oni generalno mogu klasifikovati u četiri osnovne kategorije.

- **Presecanje**, tj. **prekidanje** (engl. *interruption*) predstavlja napad na **raspoloživost** (engl. *availability*). Presecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcionisanje nekog sistema (slika 1.1). Ovakav napad je aktivan.



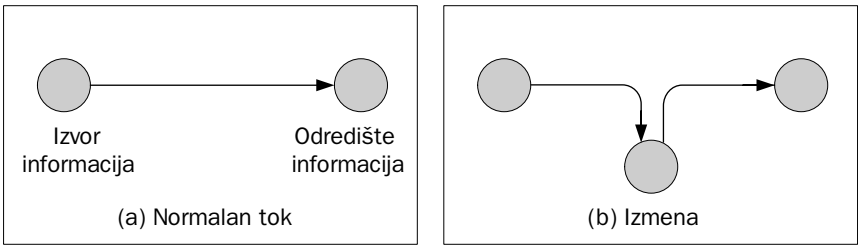
Slika 1.1 *Presecanje*

- **Presretanje** (engl. *interception*) predstavlja napad na **poverljivost** (engl. *confidentiality*). Presretanje (slika 1.2) može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično. Kao pasivan napad, teško se otkriva jer ne menja podatke tj. ne utiče na unutrašnje funkcionisanje sistema. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.
- **Izmena** (engl. *modification*), slika 1.3, predstavlja napad na **integritet** (engl. *integrity*). Po svojoj prirodi, to je aktivan napad. Ukoliko se dešava na prenosnom putu, može se, na primer, ispoljiti kao napad „čovek u sredini“ (engl.



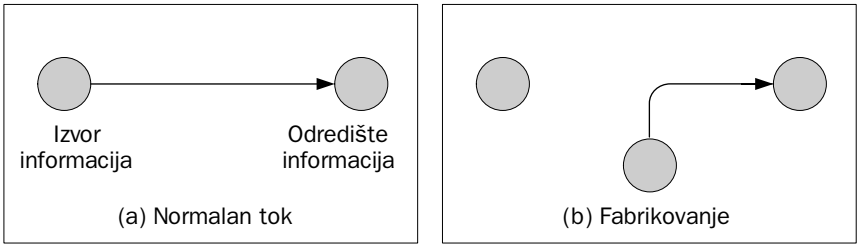
Slika 1.2 *Presretanje*

man in the middle). Napad se može obaviti i unutar nekog računarskog sistema – u tom slučaju radi se o izmeni podataka, pristupnih prava, načina funkcionisanja programa ili sistema i slično. Iako menja podatke ili sistem, često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.



Slika 1.3 *Izmena*

- **Fabrikovanje** (engl. *fabrication*), slika 1.4, predstavlja napad na **autentičnost** (engl. *authenticity*). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlaštene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.

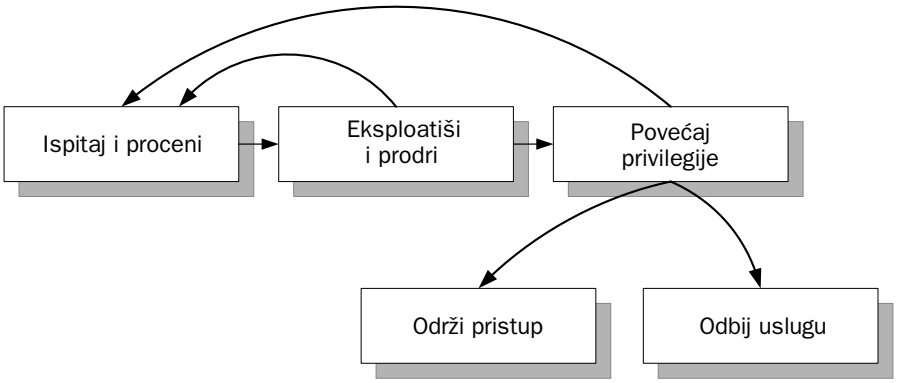


Slika 1.4 *Fabrikovanje*

Anatomija napada

Ako razumemo osnovni pristup koji napadači koriste da „osvoje“ neki sistem ili mrežu, lakše ćemo moći da preduzmemo odbrambene mere znaćemo šta je primenjeno i protiv čega. Osnovni koraci napadačeve metodologije ilustrovani su slikom 1.5 i ukratko su opisani.

[1] **Ispitaj i proceni** (engl. *survey and assess*). Prvi korak koji napadač obično preduzima jeste istraživanje potencijalne mete i identifikovanje i procena njenih karakteristika. Te karakteristike mogu biti podržani servisi, protokoli s mogućim ranjivostima i ulaznim tačkama. Napadač koristi informacije prikupljene na ovaj način kako bi napravio plan za početni napad.[1]



Slika 1.5 *Osnovni koraci napada*

[2] **Eksploatiši i prodri** (engl. *exploit and penetrate*). Nakon što je istražio potencijalnu metu, napadač pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem. Ako su mreža ili umreženi računar (najčešće server) potpuno osigurani, aplikacija postaje sledeća ulazna tačka za napadača – napadač će najlakše upasti u sistem kroz isti ulaz koji koriste legitimni korisnici. Na primer, može se upotrebiti stranica za prijavljivanje ili stranica koja ne zahteva proveru identiteta (engl. *authentication*).

[3] **Povećaj privilegije** (engl. *escalate privileges*). Nakon što napadač uspe da ugrozi aplikaciju ili mrežu – na primer, ubacivanjem (engl. *injecting*) koda u aplikaciju ili uspostavljanjem legitimne sesije na operativnom sistemu – odmah će pokušati da poveća svoja prava. Posebno će pokušati da preuzme administratorske privilegije tj. da uđe u grupu korisnika koji imaju sva prava nad sistemom. Definisanje najmanjeg nužnog skupa prava i usluga koji je neophodno obezbediti korisnicima aplikacije, primarna je odbrana od napada povećanjem privilegija.

[1] Na primer, napadač može primetiti ranjivost tipa *cross-site scripting* (XSS) tako što će ispitati da li neki upravljački element Web strane vraća eho na izlaz.

[4] **Održi pristup** (engl. *maintain access*). Kada prvi put uspe da pristupi sistemu, napadač preduzima korake da olakša buduće napade i da prikrije tragove. Čest način olakšavanja budućih pristupa jeste postavljanje programa sa „zadnjim vratima“ (engl. *back-door*) ili korišćenje postojećih naloga koji nisu strogo zaštićeni. U prikrivanje tragova često spada brisanje dnevničkih datoteka (engl. *log files*) i skrivanje napadačevih alata. Uzevši u obzir da su dnevničke datoteke jedan od objekata koje napadač želi da modifikuje kako bi prikrio tragove, one treba da budu osigurane i da se redovno analiziraju. Analiza dnevničkih datoteka često može otkriti rane znakove pokušaja upada u sistem, i to pre nego što nastane šteta.

[5] **Odbij uslugu** (engl. *deny service*). Napadači koji ne mogu da pristupe sistemu ili računarskoj mreži i da ostvare svoj cilj, često preduzimaju napad koji prouzrokuje odbijanje usluge (engl. *Denial of Service attack*, DoS), kako bi sprečili druge da koriste aplikaciju.[2] Za druge napadače, DoS napad je cilj od samog početka.

Pretnje i jednačina rizika

Rizik je, u kontekstu sigurnosti računarskih sistema i mreža, mera opasnosti, tj. mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda. Rizik treba definisati eksplicitno, na primer, „rizik od narušavanja integriteta baze klijenata“ ili „rizik odbijanja usluga od strane *on-line* portala banke“. Rizik se obično izražava u obliku jednačine rizika, gde je:

- Rizik = Pretnja × Ranjivost × Vrednost imovine

Pretnja (engl. *threat*) jeste protivnik, situacija ili splet okolnosti s mogućnošću i/ili namerama da se eksploatiše ranjivost. Ova definicija pretnje stara je nekoliko decenija i konsistentna je s opisom terorista.

Pretnja može biti strukturirana ili nestrukturirana. Strukturirane pretnje su protivnici s formalnom metodologijom, finansijskim sponzorom i definisanim ciljem. Takve pretnje su karakteristične za ekonomsku špijunažu, organizovani kriminal, strane obaveštajne službe i takozvane „informatičke ratnike“. Pretnje se dele na pasivne i aktivne.

- **Pasivne pretnje** ne utiču neposredno na ponašanje sistema i njihovo funkcionisanje. U pasivne pretnje spadaju otkrivanje sadržaja poruka (na primer, prisluškivanje) i analiza saobraćaja.
- **Aktivne pretnje** mogu uticati na ponašanje i funkcionisanje sistema ili na sadržaj podataka. U aktivne pretnje spadaju: maskiranje, tj. pretvaranje, lažiranje (engl. *masquerade*), reprodukcija, tj. ponavljanje mrežnog saobraćaja (engl. *replay*), izmena sadržaja poruke i odbijanje usluge.

[2] Primer ovakvog napada je *SYN flood attack*; napadač koristi program koji šalje veliki broj TCP SYN zahteva da bi zagušio red dolazećih konekcija na serveru, onemogućavajući tako druge korisnike da se povežu na server i iskoriste njegove usluge.

Ranjivost (engl. *vulnerability*) predstavlja slabost u nekoj vrednosti, resursu ili imovini koja može biti iskorišćena, tj. eksploatisana. Ranjivosti su posledica lošeg projektovanja, implementacije ili „zagađenja".

- **Loše projektovanje** je greška projektanta sistema. Proizvođač koji piše loš kôd – kôd koji sadrži greške (engl. *bugs*), kao što je prekoračenje bafera na steku ili u dinamičkoj memoriji (engl. *heap memory*) – pravi osetljiv proizvod koji se može lakše „razbiti". Pametni napadači će iskoristiti slabosti u arhitekturi softvera.
- **Implementacija** je odgovornost klijenta koji instalira proizvod. Iako proizvođači treba da pripreme dokumentaciju o bezbednom korišćenju svojih proizvoda, korisnik mora biti vrlo oprezan.
- **„Zagađenje"** se odnosi na mogućnost da se dostigne stepen „iza" predviđene upotrebe proizvoda. Dobro projektovan softverski proizvod treba da obavlja predviđenu funkciju i ništa više od toga. Na primer, ne sme postojati mogućnost da se iz mrežne usluge ili aplikacije koja se izvršava s privilegijama korisnika *root* na Linux sistemu, otvori instanca komandnog interpretera, jer će, u tom slučaju korisnik dobiti na „poslužavniku" komandni interpreter sa svim pravima administratora sistema. Odluke koje ponekad donesu proizvođači i korisnici, mogu da prouzrokuju „zagađenje" tj. da stvore mogućnost za prekoračenje predviđene upotrebe proizvoda.

Vrednost imovine je mera vremena i resursa potrebnih da se neka imovina zameni ili vrati u prethodno stanje. Zato se kao ekvivalentan termin može koristiti i „cena zamene". Server baze podataka na kome se čuvaju informacije o kreditnim karticama klijenata, podrazumevano je vredniji, tj. ima veću cenu zamene nego radna stanica u nekoj laboratoriji za ispitivanje softverskih proizvoda.

Modelovanje pretnji

Modelovanje pretnji ne treba da bude jednokratan proces. To treba da bude iterativan proces koji počinje u ranoj fazi projektovanja aplikacije i traje tokom celog životnog ciklusa aplikacije. Za to postoje dva razloga. Prvo, nemoguće je da se u jednom prolazu identifikuju sve moguće pretnje. Drugo, s obzirom na to da su aplikacije retko statičke, već treba da budu proširive i prilagodljive tako da odgovaraju promenljivim poslovnim zahtevima, proces modelovanja pretnji treba da se ponavlja kako aplikacija evoluira. **Proces modelovanja pretnji** odvija se u šest faza, a može se primeniti i za postojeće aplikacije i za aplikacije koje se tek razvijaju.

[1] **Identifikovanje vrednosti.** U ovom koraku identifikuju se vrednosti i utvrđuje se šta sistem treba da zaštiti.

[2] **Izrada pregleda arhitekture.** Korišćenjem jednostavnih dijagrama i tabela, dokumentuje se aplikacija, uključujući podsisteme, granice poverenja i tokove podataka.

[3] **Dekompozicija aplikacije.** Arhitektura aplikacije se dekomponuje, uključujući osnovnu arhitekturu mreže i računara/servera, kako bi se napravio sigurnosni profil aplikacije. Namena sigurnosnog profila je da otkrije ranjivosti u arhitekturi, implementaciji, instalaciji i konfigurisanju aplikacije.

[4] **Identifikovanje pretnji.** Imajući u vidu ciljeve napadača i poznajući arhitekturu i moguće ranjivosti aplikacije, identifikuju se pretnje koje mogu da ugroze aplikaciju.

[5] **Dokumentovanje pretnji.** Pretnje se dokumentuju korišćenjem zajedničkog šablona (engl. *template*); on definiše centralni skup atributa kojim se može uhvatiti svaka pretnja.

[6] **Rangiranje**, tj. **procena pretnji.** Pretnje se rangiraju po prioritetu kako bi se prvo rešavale najznačajnije pretnje, tj. one koje predstavljaju najveći rizik. U procesu rangiranja meri se verovatnoća pretnje u odnosu na štetu koju može prouzrokovati napad, ako se dogodi. Rangiranje može pokazati da određene pretnje ne opravdavaju nikakvu akciju kada se rizik od te pretnje uporedi s troškovima ublažavanja pretnje.

Rezultat procesa modelovanja pretnji je dokument koji članovima projektnog tima omogućava da jasno razumeju pretnje i moguće pristupe u rešavanju. Model pretnji se sastoji od definicije arhitekture aplikacije i liste pretnji za različite scenarije primene aplikacije.

Najčešće primenjivani napadi i pretnje

Računarski sistem i računarska mreža mogu se napasti na mnogo načina. Najčešće korišćene metode eksploatacije slabosti jesu DoS, lažiranje IP adresa i njuškanje.

- **Odbijanje usluga** (engl. *Denial of Service*, DoS). DoS izaziva prestanak rada servisa ili programa, čime se drugima onemogućava rad s tim servisima ili programima. DoS napad se najlakše izvršava na transportnom sloju – slanjem velikog broja SYN paketa (TCP CONNECTION REQUEST) – a zaštita se postiže kontrolisanjem broja SYN paketa u jedinici vremena.
- **Lažiranje IP adresa** (engl. *spoofing*). Napadač prati IP adrese u IP paketima i predstavlja se kao drugi računar. Kako DNS ne proverava odakle dolaze informacije, napadač može da izvrši napad lažiranjem tako što DNS servisu daje pogrešnu informaciju (ime računara od poverenja). Najbolja zaštita od ovog napada je sprečavanje rutiranja paketa sa adresama izvorišta (engl. *source address*) za koje sigurno znamo da su neispravne – na primer, odbacivanje paketa koji stižu na javni interfejs rutera, a imaju adresu lokalne mreže.
- **Njuškanje** (engl. *sniffing*). Napadač specijalnim programima presreće TCP/IP pakete koji prolaze kroz određeni računar i po potrebi pregleda njihov sadržaj. Kako se kroz mrežu obično kreću nešifrovani podaci, program za njuškanje (snifer) lako može doći do poverljivih informacija.

Osim toga, program koji je napisao jedan korisnik (programer), a kojim se služe drugi korisnici, može da predstavlja pretnju i da dovede do uspešnog napada na sistem. Pretnje ovakvog tipa zovu se **programske pretnje**; u njih se ubrajaju trojanski konji, klopke i prekoračenje, tj. prelivanje bafera.

- **Trojanski konj** (engl. *trojan horse*) ilegalan je segment koda, podmetnut u kôd nekog programa, a cilj mu je da promeni funkciju ili ponašanje originalnog programa. Na primer, u editor teksta može biti podmetnut potprogram koji pretražuje otvorenu datoteku i – u slučaju da pronađe željenu sekvencu – kopira datoteku na mesto dostupno programeru koji je napisao taj editor. Specijalna varijanta trojanskog konja je program koji oponaša proceduru prijavljivanja na sistem ili mrežu; napadač koristi programe ovog tipa – a i neznanje korisnika – kako bi obezbedio pristup računarskom sistemu ili mreži s tuđim akreditivima.[3]
- **Klopka** (engl. *trap door*). Autor programa može slučajno ili namerno ostaviti prazna mesta u svom kodu (klopku) – uljez koji zna za ta mesta može da podmetne svoj kôd i time ostvari neku dobit. Osim toga, autor programa može izmeniti deo koda tako da se izmena ne može jednostavno primetiti. Na primer, zaokruživanje iznosa transakcije na neku celobrojnu vrednost u određenim trenucima, predstavlja klopku ukoliko se ostatak zaokruživanja prenosi na račun programera. Klopke se teško otkrivaju, jer treba analizarati celokupan kôd sumnjivog programa.
- **Prekoračenje**, tj. **prelivanje bafera** (engl. *buffer overrun*, *buffer overflow*) na steku ili u dinamičkom delu memorije. Prekoračenje bafera je najčešći napad s mreže pri pokušaju neovlašćenog pristupanja sistemu. Ovlašćeni korisnici takođe mogu da odaberu ovu vrstu napada kako bi prevarili sistem i ostvarili veća prava od onih koja imaju. Po pravilu, napadač koristi grešku u programu, to jest, neodgovarajuću kontrolu razdvajanja steka, podataka i koda. Tada napadač šalje više ulaznih podataka nego što program očekuje, prepunjava ulazno polje, argumente komandne linije ili ulazni bafer – sve dok ne dođe do steka. Potom preko važeće adrese u steku upisuje adresu svog koda, puni deo steka svojim kodom, koji – na primer – izvršava neku komandu (kopira neke podatke ili pokreće komandni interpreter). U slučaju uspešnog napada, umesto nedovoljno zaštićenog programa izvršiće se ilegalan kôd, ubačen zahvaljujući prekoračenju bafera.

[3] Programi ovakvog tipa presreću legitimnu proceduru prijavljivanja na sistem i prikazuju odzivnik za prijavljivanje, identičan onom pravom, koji čeka da korisnik unese korisničko ime i lozinku. Korisnik unosi korisničko ime i lozinku koje trojanski konj smešta u neku datoteku dostupnu napadaču, a potom obaveštava korisnika da je pogrešno uneo lozinku. Trojanski konj, zatim, predaje kontrolu pravoj proceduri prijavljivanja na sistem. Korisnik smatra da je uneo pogrešnu lozinku, unosi je ponovo i prijavljuje se na sistem. Napadač proverava datoteku i prijavljuje se na sistem pod tuđim imenom. Korisnik najčešće nije svestan da je na ovaj način kompromitovao svoje akreditive.

Mnogi operativni sistemi imaju mehanizam pomoću kojeg procesi mogu da generišu druge procese. U takvom okruženju moguće je zlonamerno korišćenje datoteka i sistemskih resursa. Pretnje ovog tipa nazivaju se **sistemske pretnje**. Dve metode kojima se one mogu postići jesu crvi i virusi.

- **Crvi** su samostalni zlonamerni programi koji se šire s računara na računar. Uobičajene metode prenošenja na žrtvu jesu upotreba elektronske pošte i Internet servisa. Crv eksploatiše ranjivost žrtve (na primer, prekoračenje bafera nekog mrežnog servisa) ili koristi metode prevare i obmanjivanja, poznate kao društveni inženjering (engl. *social engineering*), kako bi primorao korisnika da ga pokrene. Crv degradira performanse, a ponekad nanosi i dodatnu štetu.
- Za razliku od crva, koji su samostalni programi, **virusi** su fragmenti koda koji se ubacuju u druge legitimne programe. Dakle, virus zahteva nosioca u vidu izvršne datoteke. Posle pokretanja, virus obično inficira i druge izvršne datoteke na sistemu. Virusi su, najčešće, vrlo destruktivni i teško se uklanjaju ukoliko administrator zaraženog sistema nema zdrave kopije izvršnih datoteka. Zbog svega navedenog, virusi su jedan od glavnih problema pri korišćenju personalnih računara.

1.2 Šta je sigurnost?

Sigurnost je proces održavanja prihvatljivog nivoa rizika. Znači, sigurnost je proces, a ne završno stanje, tj. nije konačni proizvod. Organizacija ili institucija ne može se smatrati „sigurnom“ ni u jednom trenutku posle izvršene poslednje provere usklađenosti s vlastitim sigurnosnim pravilima. Jednostavno rečeno, ako vas šef pita: „Da li smo mi sigurni?“, trebalo bi da odgovorite: „Sačekajte da proverim“. Ako vas pita: „Da li ćemo biti sigurni sutra?“, trebalo bi da odgovorite: „Ne znam“. Takvi iskreni odgovori nisu popularni, ali – uz takvo poimanje stvarnosti – preduzeća ili organizacije biće uspešnije zaštićeni. Rukovodioci koji shvataju koncept po kome je sigurnost proces održavanja prihvatljivog, tj. razumnog nivoa rizika, verovatno će odrediti vreme i resurse koji su potrebni da se ti zahtevi i odgovornosti ostvare.

Neretko se dešava da velike svetske kompanije, uključujući i tržišne lidere, reklamiraju u raznim medijima svoje proizvode kao svemoćna rešenja ili „srebrni metak“. Oni koji veruju da sigurnost može biti jednom „dostignuta“ i da će posle toga sistem ostati siguran, voljni su da kupe proizvode i usluge koji se na taj način reklamiraju. Treba vrlo oprezno razmotriti tako oglašenu ponudu.

Kada se kaže da je sigurnost proces, onda se misli na činjenicu da se sigurnost ne može kupiti kao proizvod ili usluga, već da je to proces u kome se koriste različiti proizvodi i usluge, procedure i pravila, ali se smatra i to da postoje drugi bitni elementi kao što su edukacija, podizanje svesti i stalno praćenje stanja u ovoj oblasti. Ostvarivanje sigurnosti takođe podrazumeva održavanje sistema u stanju prihvatljivog rizika, tj. kompromis između potrebnih ulaganja i smanjenja mogućnosti da nastane šteta koje se tim ulaganjem postiže.

Dakle, kada se govori o sigurnosti i zaštiti informacionih sistema i mreža, nekoliko principa danas važe kao osnovni postulati.

- Sigurnost je proces. Sigurnost nije proizvod, usluga ili procedura, već skup koji ih sadrži – uz još mnogo elemenata i mera koje se stalno sprovode.
- Ne postoji apsolutna sigurnost.
- Uz različite metode zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

Uopšteno govoreći, veće ulaganje u sigurnost smanjuje izloženost sistema ili računarske mreže riziku. S druge strane, ono izlaže vlasnika sistema ili računarske mreže većim troškovima i smanjuje profitabilnost. Zato je veoma značajno da se odredi tačka u kojoj se postiže ravnoteža između ulaganja u sigurnost i postignutih efekata.

Treba takođe imati u vidu sledeće: kao i u drugim sistemima i oblastima, sigurnosni mehanizmi ili procedure vrlo često smanjuju udobnost rada ili pogoršavaju performanse sistema. Kratkoročno gledano, to može negativno uticati na opšte efekte rada; dugoročno, ove mere pozitivno utiču na uspeh u radu, to jest, na profit komercijalnih organizacija. To se ogleda i kroz materijalne pokazatelje, i kroz pokazatelje koji nisu direktno materijalni, kao što su rast ili gubitak reputacije tj. ugleda, zavisno od toga da li se dešavaju ili ne dešavaju incidenti.

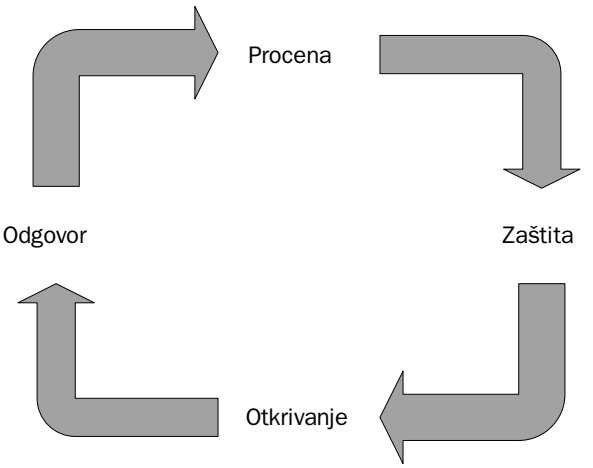
Najvažniji faktori uspeha su sledeći:

- aktivnosti koje se odnose na ceo sigurnosni proces moraju biti zasnovane na zahtevima posla i moraju ih voditi poslovna rukovodstva;
- neophodno je dobro razumeti rizike od potencijalnih pretnji i ranjivosti sistema;
- osnovni koncepti zaštite moraju biti izloženi svim rukovodiocima i zaposlenima kako bi svi shvatili koliko je zaštita važna;
- kompanijska ili insitucionalna uputstva za primenu pravila i standarda zaštite moraju se dostaviti svim zaposlenima i svim saradnicima koji nisu stalno zaposleni.

Sigurnost kao proces (slika 1.6) zasniva se na četiri osnovna koraka: procena, zaštita, otkrivanje i odgovor. U ovom modelu, neki autori koriste izraz planiranje (engl. *planning*) umesto izraza izraza procenjivanje, i sprečavanje ili prevencija (engl. *prevention*), a ne zaštita.

[1] **Procena** (engl. *assessment*). Procena je priprema za ostale tri komponente. Smatra se posebnom akcijom, zato što je u vezi s pravilima, procedurama, pravnom i drugom regulativom, određivanjem budžeta i drugim upravljačkim dužnostima, i još je povezana s tehničkom procenom stanja sigurnosti. Greška u proceni bilo kog od ovih elemenata, može naškoditi svim operacijama koje slede.

[2] **Zaštita** (engl. *protection*). Zaštita, tj. sprečavanje ili prevencija, podrazumeva primenu protivmera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primenjuje se sledeći korak – otkrivanje.



Slika 1.6 *Sigurnost kao proces*

[3] **Otkrivanje** (engl. *detection*). Otkrivanje, ili detekcija predstavlja proces identifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost. Neki autori definišu incident kao svaki „nezakonit, neovlašćen ili neprihvatljiv postupak koji je preduzet, a odnosi se na računarski sistem ili mrežu".

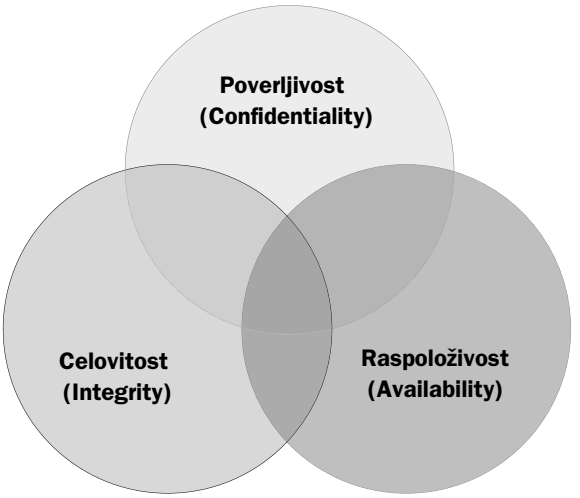
[4] **Odgovor** (engl. *response*). Odgovor ili reakcija predstavlja proces oporavka, tj. lečenja posledica upada. U aktivnosti reakcije spadaju postupci „zakrpi i nastavi", ili „goni i sudi". Ranije se na prvo mesto stavljalo oporavljanje funkcionalnosti oštećenih resursa, kao što je korišćenje rezervnih kopija podataka za vraćanje sistema u stanje pre izvršenog napada. U novije vreme sve češće se koriste pravna sredstva (sudski proces protiv onoga ko ugrožava sigurnost), među koja spada prethodno prikupljanje dokaza metodama digitalne forenzike pomoću kojih se potkrepljuje tužba.

Sigurnosni ciljevi

Poverljivost, celovitost (integritet) i raspoloživost čine takozvano „veliko trojstvo" sigurnosti (slika 1.7). Na engleskom jeziku, skraćenica za ova tri termina je CIA (*Confidentiality*, *Integrity*, *Availability*), što se poklapa sa akronimom koji se koristi za najpoznatiju američku obaveštajnu agenciju.

Ovaj koncept predstavlja tri fundamentalna principa informacione sigurnosti. Sve što se odnosi na sigurnost informacija i mehanizme obezbeđenja, zatim sve pretnje, ranjivosti i sigurnosni procesi, predmet su procenjivanja prema ova tri (CIA) kriterijuma.

- **Poverljivost** (engl. *confidentiality*). Koncept poverljivosti obuhvata pokušaje da se spreči namerno ili nenamerno neovlašćeno otkrivanje sadržaja poruka. Poverljivost se može izgubiti na mnogo načina, kao što su namerno otkrivanje privatnih podataka u vlasništvu kompanije ili, recimo, pogrešnim definisanjem i sprovođenjem prava pristupa mreži.



Slika 1.7 *Veliko trojstvo sigurnosti*

- **Integritet** (celovitost, engl. *integrity*). U okviru sigurnosti informacija, koncept integriteta obezbeđuje sledeće:
  - podatke ne smeju menjati neovlašćena lica ili procesi,
  - ovlašćena lica ili procesi ne smeju obavljati neovlašćene promene podataka,
  - podaci su interno i eksterno konsistentni, što znači da su interni podaci međusobno konsistentni u svim potcelinama (delovima), kao i s realnim svetom, tj. spoljnim okruženjem.
- **Raspoloživost** (engl. *availability*). U okviru sigurnosti informacija, koncept raspoloživosti obezbeđuje da odgovarajuće osoblje pouzdano i pravovremeno može da pristupa podacima ili računarskim resursima. Drugim rečima, raspoloživost označava da su sistemi podignuti i da rade kao što je predviđeno. Osim toga, ovaj koncept garantuje da funkcionišu sigurnosne usluge koje zahtevaju stručnjaci za sigurnost.

Postoji i svojevrsna igra rečima: DAD je skraćenica koju čine reči suprotnog značenja od onih reči koje čine skraćenicu CIA – *disclosure* (otkrivanje, obelodanjenje), *alteration* (izmena) i *destruction* (uništenje). Ova skraćenica se na engleskom jeziku čita „ded“, što znači mrtav.

Sigurnosne usluge

Kao što je već rečeno, **sigurnosna usluga** (servis) jeste usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosni servis podrazumeva upotrebu jednog ili više sigurnosnih mehanizama, tj. mehanizama koji treba da detektuju ili preduprede napad na sigurnost, ili da oporave sistem od napada. Sigurnosni mehanizmi su rešenja, tehnologije, pravila i procedure koje možemo implementirati na sistemu. Sigurnosni mehanizmi se menjaju i unapređuju uvođenjem novih

tehnologija. Da bi se izabrao odgovarajući mehanizam, stanje na tržištu mora se proveriti kad god se projektuju ili poboljšavaju servisi. Za razliku od mehanizama, servisi se ređe menjaju, a komponente CIA trijade ostaju konstantne.

U sigurnosne usluge spadaju:

- **Poverljivost**, **privatnost** (engl. *confidentiality*, *privacy*). Međunarodna organizacija za standardizaciju, ISO, definisala je poverljivost kao „uslugu obezbeđivanja pristupa informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe". Poverljivost je veoma značajna sigurnosna usluga, a takođe i jedan od ciljeva projektovanja mnogih savremenih šifarskih sistema. Privatnost se najopštije može definisati kao sposobnost pojedinca ili grupe ljudi da sakriju sve ono što ne treba da bude javno dostupno, tj. da spreče „curenje" informacija u javnost. Privatnost se u nekim slučajevima vezuje za pojam anonimnosti, iako je najviše cene baš pojedinci i grupe koji su izloženi javnosti. Drugim rečima, privatnost je sigurnosna usluga koja obezbeđuje da informacija ostane dostupna onom krugu korisnika kome je namenjena i nikom više. Privatnost je od fundamentalnog značaja kada postoje dve suprotstavljene interesne grupe, koje na neki način moraju da sakriju komunikaciju između svojih članova. Dakle, podaci se ne smeju otkriti neovlašćenim klijentima. Podaci se moraju štititi kad su uskladišteni, tokom obrade i prilikom prenosa.
- **Provera identiteta** (engl. *authentication*) – usluga kojom se od svakog korisnika zahteva da se predstavi sistemu pre nego što nešto uradi, i koja obezbeđuje način da svaki objekat (neko ili nešto) koji tvrdi da ima određen identitet (korisničko ime ili kodirani ID) to i dokaže. Provera identiteta, u sprezi s dnevnikom događaja, obezbeđuje uvid u „istorijsko" činjenično stanje (na primer, uvid u to ko je napravio ili izmenio određenu datoteku na disku servera, ko je preuzeo podatke ili ih poslao van mreže itd.).
- **Integritet** (engl. *integrity*) – usluga koja obezbeđuje celovitost podataka, tj. obezbeđuje da napadač ne može da izmeni podatke, a da to ostane neprimećeno. Dakle, integritet je usluga zaštite od neovlašćenog, nepredviđenog ili nenamernog modifikovanja. Što se tiče podataka, oni moraju biti zaštićeni od neovlašćenih izmena tokom skladištenja, obrade ili transporta, a sistem treba da neometano izvršava predviđene operacije (usluge) bez neovlašćenog manipulisanja.[4]
- **Neporicanje**, **priznavanje** (engl. *non-repudiation*) – usluga koja obezbeđuje da korisnik koji pošalje poruku ili izmeni neki podatak ne može kasnije tvrditi da on to nije uradio. Na primer, korisnik koji digitalno potpiše dokument svojim privatnim ključem kasnije neće moći da tvrdi kako on nije napravio i potpisao taj dokument, jer se potpis lako može proveriti. Uopšteno govoreći, sporovi

[4] Na primer, jednosmerna heš funkcija obezbeđuje integritet dokumenata. Ukoliko neko izmeni makar jedan znak u dokumentu, izmeniće se i heš. Samim tim, korisnici će postati svesni da je dokument izmenjen.

mogu nastati oko određenog događaja: da li se desio, kada je bio zakazan, koje su strane bile uključene i koje su informacije bile relevantne. Cilj ove usluge je da obezbedi neoboriv dokaz koji omogućava brzo rešavanje sporova.

- **Kontrola pristupa** (engl. *access control*) – usluga koja treba da predupredi zloupotrebu resursa. Pomoću kontrole pristupa dozvoljava se objektu s proverenim identitetom i sa odgovarajućim ovlašćenjima da koristi određene usluge sistema ili određene operacije definisane u takozvanim matricama pristupa, u čijim se vrstama nalaze operacije sistema, a u kolonama – korisnici. Kontrola pristupa, najjednostavnije rečeno, određuje ko ima pravo da pristupi resursima, i na kakav način.
- **Raspoloživost**, **upotrebljivost** (engl. *availability*) – usluga kojom se obezbeđuje dostupnost podataka i raspoloživost sistema koji pruža neke usluge. Primeri takvih usluga su sprečavanje DoS napada i sprečavanje infekcije virusima koji brišu ili oštećuju datoteke.

Strategije ostvarivanja sigurnosti

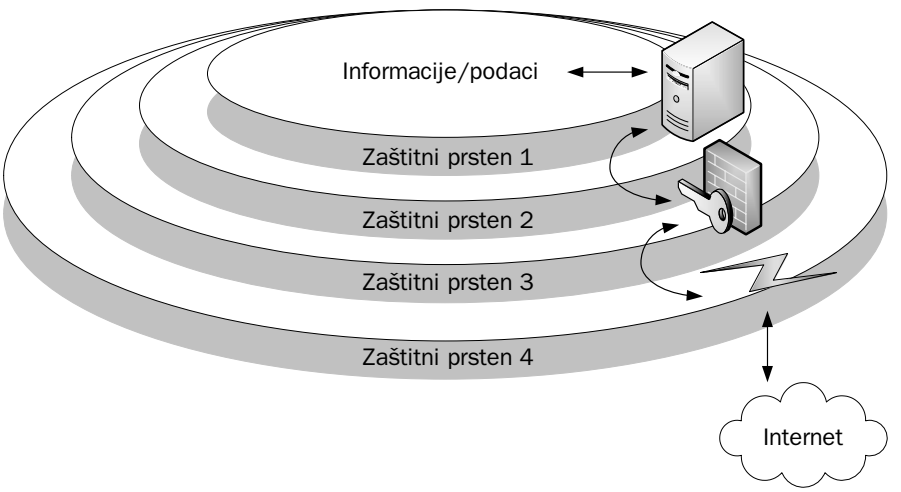
Servisi i mehanizmi, sami po sebi, ne znače ništa ukoliko nema odgovarajuće strategije ostvarivanja sigurnosti. **Strategija ostvarivanja sigurnosti** je plan koji pokazuje pravac ostvarivanja usluga, tj. određuje ko je odgovoran za koji aspekt sigurnosti i kojim će se resursima taj aspekt ostvariti; drugim rečima, određuje koje sigurnosne mehanizme koriste određene usluge (na primer, provera identiteta ili kontrola pristupa). Da bi strategija bila uspešna, moraju se projektovati pravila i procedure, dodeliti uloge i odgovornosti, i mora se obučiti osoblje (korisnici i administratori sistema). Strategija obuhvata uspostavljanje fizičke sigurnosti i sistema ličnog obezbeđenja, u cilju kontrole i praćenja pristupa infrastrukturi i bitnim elementima informatičkog sistema.

Slojevita zaštita

Jedna od najefikasnijih i najraširenijih strategija je **slojevita zaštita,** koja se zasniva na formiranju zaštitnih slojeva (ili prstenova) oko sistema. Korisnik sistema koji prolazi kroz slojeve zaštite mora zadovoljiti dodatne sigurnosne mehanizme koji zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima. Slojevit pristup treba da obezbedi kombinaciju sigurnosnih mehanizama i tehničkih rešenja koji obuhvataju dovoljno široku lepezu sigurnosnih zahteva. Uz to, treba da onemogući da probijanje jednog sloja ima katastrofalne posledice po sigurnost celog sistema. Naime, verovatnoća da budu probijeni svi slojevi mnogo je manja od verovatnoće probijanja jednoslojne zaštite. Slojevitu zaštitu ilustrovaćemo na primeru četiri prstena, prikazanih na slici 1.8.

- Spoljašnji sloj je granica između sistema i spoljašnjeg sveta (najčešće Interneta). U ovom sloju, sigurnosni mehanizmi su mrežne barijere (engl. *firewalls*) i provera identiteta rutera i DNS servera. Ovom sloju zaštite odgovara demilitarizovana zona, tj. javno dostupan deo privatne mreže.

- Treći zaštitni sloj štiti sistem od mreže u kojoj se nalazi i sadrži mehanizme PKI (infrastruktura javnih ključeva), VPN (virtuelne privatne mreže) i mrežne barijere.
- Drugi sloj implementira CIA koncepte koristeći mehanizme na sistemskom nivou. Ovi mehanizmi su implementirani na radnim stanicama, serverima ili *mainframe* računarima na nivou operativnih sistema koji su na njima instalirani. Instalirani operativni sistemi moraju imati najnovije zvanične zakrpe i moraju biti adekvatno administrativno i fizički zaštićeni.
- Unutrašnji sloj štiti same informacije i podatke koji se čuvaju na sistemu. U sigurnosne mehanizme na ovom sloju spadaju kontrola pristupa na aplikativnom nivou (lozinke ili drugi način provere identiteta), kontrola pristupa podacima na osnovu matrica pristupa, šifrovanje i digitalno potpisivanje podataka (datoteka), te praćenje (engl. *auditing*) operacija i objekata koji su pristupili sistemu.



Slika 1.8 *Slojevita zaštita*

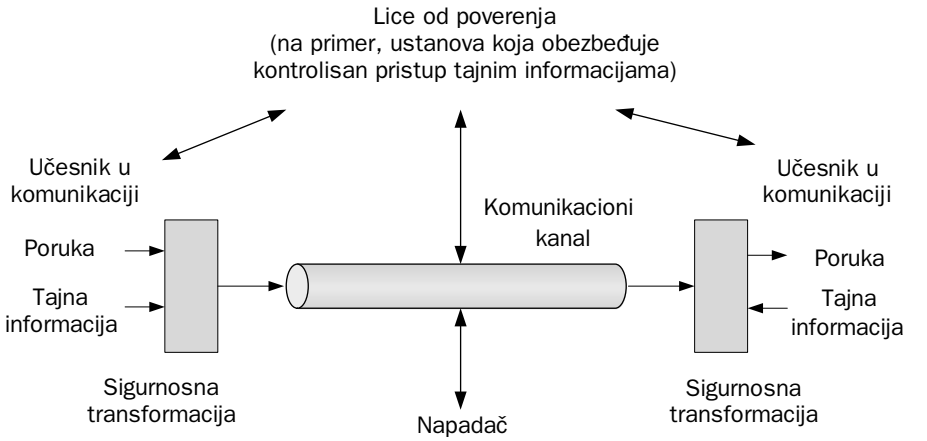
Sigurnosni modeli

Shodno mestu sigurnosne transformacije[5] i funkciji koju ta transformacija obavlja (na primer, šifrovanje ili digitalno potpisivanje) i koja obezbeđuje sigurnosnu uslugu privatnosti, neporicanja, ili integriteta, izdvajamo dva sigurnosna modela.

Prvi model (slika 1.9) pokazuje protok informacija između dva učesnika preko nesigurnog komunikacionog kanala, uz postojanje protivnika, tj. napadača. Oba učesnika primenjuju odgovarajuću sigurnosnu transformaciju sa odgovarajućim tajnim informacijama koje obezbeđuje „lice od poverenja", tj. strana kojoj veruju oba

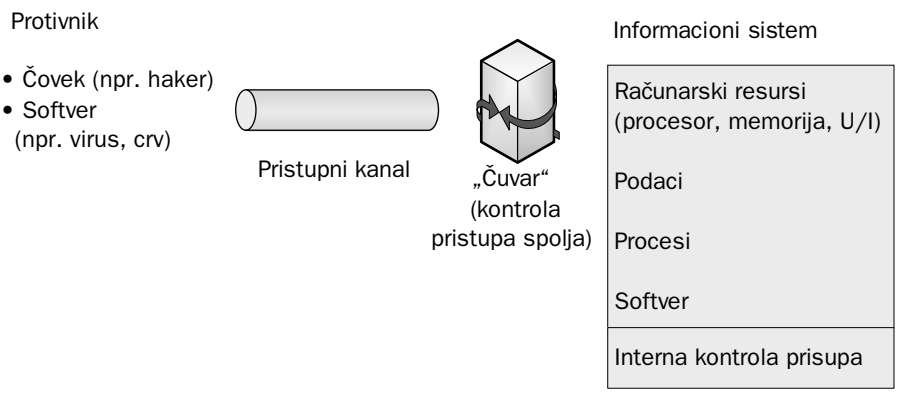
[5] Sigurnosna transformacija je operacija pomoću koje je implementiran neki sigurnosni mehanizam. Jednostavnije rečeno, to je operacija „radi nešto" s podacima kako bi ih zaštitila.

učesnika u komunikaciji. Na ovaj način se komunikacioni kanal štiti od napadača, jer napadač ne zna i ne može da dobije skrivenu informaciju. Na primer, sigurnosna transformacija može biti šifrovanje s javnim ključem, a lice od poverenja neka ustanova koja će učesnicima u komunikaciji distribuirati javne ključeve i obezbeđivati potvrdu usaglašenosti identiteta učesnika i ključa (na primer, pomoću sertifikata).



Slika 1.9 *Model s nesigurnim komunikacionim kanalom*

Drugi model (slika 1.10) odnosi se na kontrolisan pristup podacima ili resursima računarskog sistema, u prisustvu potencijalnih napadača. Ovaj model je zasnovan na odgovarajućoj kontroli pristupa unutar samog sistema (na primer, liste za kontrolu pristupa datotekama na disku, prava dodeljena korisnicima nad nekom bazom podataka) i na takozvanom „čuvaru" (engl. *gatekeeper*), tj. zaštitnom mehanizmu koji kontroliše pristup sistemu spolja (na primer, mrežna barijera koja obezbeđuje pristup samo određenim mrežnim servisima) kako bi se obezbedila odgovarajuća sigurnost. U ovom modelu se mogu koristiti i neke od kriptografskih tehnika zaštite.



Slika 1.10 *Model sigurnog pristupa mrežnim resursima*

1.3 Klasifikovanje informacija

Jedan od najbitnijih koncepata politike zaštite informacija jeste koncept **vlasništva**. Ovim konceptom se obezbeđuje da svi računarski resursi – glavni informacioni entiteti (informacioni podsistemi, baze podataka, uređaji, datoteke, prenosni putevi) – moraju imati vlasnika, tj. nekoga ko je zadužen za njih. Vlasnik treba da:

- klasifikuje informacije u jednu od raspoloživih klasa;
- deklariše ko može da pristupi podacima;
- bude odgovoran za podatke i za njihovu zaštitu.

Informacije koje su proizvedene ili se obrađuju u nekoj organizaciji, moraju biti klasifikovane u skladu s tim koliko je bitno da ne budu izgubljene ili otkrivene (obelodanjene). Vlasnici podataka su odgovorni za definisanje nivoa osetljivosti. Ovaj pristup omogućava da upravljanje sigurnošću bude izvedeno kako treba, saglasno šemi klasifikacije.

Postoji nekoliko pristupa klasifikaciji tajnosti informacija. Broj, nazivi i karakteristike klasa informacija zavise od namene (komercijalne organizacije, državne institucije, vojska, policija) i od zemlje u kojoj se koriste. Značajan uticaj na klasifikaciju imaju pravni sistem i regulativa zemlje. Ovde su izneti neki od najrasprostranjenijih načina klasifikacije.

Klasifikovanje tajnosti informacija

Prema jednoj od dominantnih klasifikacija, karakterističnoj za zemlje koje svoje metode zaštite definišu na bazi predinformatičkog doba, informacije se dele u četiri osnovne klase: javne, interne, poverljive i tajne informacije.

[1] **Javne informacije**. Podaci nisu poverljivi i mogu postati javni bez ikakvih štetnih posledica po kompaniju. Integritet podataka nije važan za ovu klasu informacija. Nedostupnost usluga zbog napada zlonamernog napadača, prihvatljivo je opasna. Primeri: usluge ispitivanja bez poverljivih podataka ili neke javne usluge pružanja informacija.

[2] **Interne informacije**. Interni pristup je selektivan. Klasifikacioni nivo treba da bude napisan na dokumentima. Preventivno bi trebalo sprečiti javno objavljivanje ovih podataka (interni podaci ne bi trebalo da se iznose van kompanije), iako neki od njih mogu biti namenjeni za javno objavljivanje. Primer: podaci u razvojnim grupama, produkcioni javni servisi, radni dokumenti i projekti, interni telefonski imenici.

[3] **Poverljive informacije**. U ovu klasu spadaju kompanijski poverljivi podaci koji su zaštićeni od spoljašnjeg pristupa. Računski centri sadrže poverljive podatke. Računari moraju da budu u prostorijama koje se zaključavaju. Dokumenti se takođe čuvaju pod ključem. Sadržaj dokumenta se mora šifrovati ukoliko se prenose preko Interneta. Kada više nisu potrebni, dokumenti se

uništavaju. Pristup poverljivim podacima može prouzrokovati značajan finansijski gubitak za datu kompaniju, doneti dobitak konkurentskoj kompaniji, smanjiti poverenje korisnika usluga ili potrošača proizvoda. Primer: podaci o platama, podaci o zaposlenima, projektna dokumentacija, računovodstveni podaci, poverljivi ugovori.

[4] **Tajne informacije**. Neovlašćen spoljašnji ili unutrašnji pristup ovim podacima mogao bi biti poguban za preduzeće ili instituciju. Integritet podataka je izuzetno važan. Ovim podacima trebalo bi da sme pristupati izuzetno malo ljudi i pri tom moraju da se poštuju veoma stroga pravila. Podatke bi trebalo čuvati u šifrovanom obliku ili u uređajima s hardverskom zaštitom. Osim toga, potrebno je zaključavati prostorije u kojima se čuvaju tajni podaci. Primer: vojni podaci, podaci o reorganizaciji, o većim finansijskim transakcijama i dr.

Drugi načini klasifikacije

U sledećih nekoliko definicija opisani su nivoi klasifikacije sigurnosti državnih informacija, rangirani od najnižeg do najvišeg:

[1] **Neklasifikovano** (engl. *unclassified*). Informacije koje nisu označene ni kao osetljive niti kao klasifikovane. Javno pokazivanje ovih informacija neće povrediti poverljivost.

[2] **Osetljivo ali neklasifikovano** (engl. *sensitive but unclassified*, *SBU*). Informacije koje su označene kao male tajne, ali neće nastati ozbiljna šteta ako se otkriju. Rešenja testova i ispita, kao i informacije iz oblasti zdravstvene zaštite, primeri su osetljivih, ali neklasifikovanih informacija.

[3] **Poverljivo** (engl. *confidential*). Informacije koje su označene kao poverljive po svojoj prirodi. Neovlašćeno otkrivanje ovih informacija može izazvati štetu po nacionalnu sigurnost, tj. sigurnost zemlje. Ovaj nivo zaštite koristi se za dokumente koji su između osetljivih ali neklasifikovanih i tajnih.

[4] **Tajna** (engl. *secret*). Informacije koje su označene kao tajne po svojoj prirodi. Neovlašćeno otkrivanje ovih informacija može da prouzrokuje ozbiljnu štetu za nacionalnu bezbednost.

[5] **Strogo poverljivo** (engl. *top secret*). Najviši nivo klasifikacije informacija po sigurnosti. Neovlašćeno otkrivanje ovog tipa informacija može da nanese izuzetno ozbiljnu štetu po nacionalnu bezbednost.

U svim navedenim kategorijama, za pojedinca ili proces, uz neophodnost da imaju odgovarajuću dozvolu za pristup informacijama, važi princip da mogu da pristupaju takozvanim „*treba-da-zna*“ *informacijama*. Saglasno tome, lice koje ima dozvolu za pristup informacijama stepena tajna ili nižeg, nije ovlašćeno da pristupi materijalu tog stepena (stepena tajna) ako mu taj materijal nije nužan za obavljanje njemu poverenih poslova.

Sledeća terminologija koristi se za klasifikaciju informacija namenjenih privatnom sektoru:

[1] **Javne** (engl. *public*). Informacije slične neklasifikovanim informacijama; sve kompanijske informacije koje ne spadaju u neku od niženavedenih kategorija, mogu se smatrati javnim. Takve informacije verovatno ne bi trebalo da budu otvorene. Međutim, ako su otvorene, ne očekuje se da imaju ozbiljan ili nepovoljan uticaj na kompaniju.

[2] **Osetljive** (engl. *sensitive*). Informacije za koje se zahteva viši nivo klasifikacije od onog za obične podatke. Ovakve informacije treba da budu zaštićene od otkrivanja da bi se očuvalo poverenje u kompaniju. Takođe treba da budu zaštićene i od gubitka integriteta usled neovlašćene izmene.

[3] **Privatne** (engl. *private*). Informacije za koje se smatra da su lične ili privatne prirode; namenjene su za korišćenje samo unutar firme. Njihovo otvaranje može se nepovoljno odraziti na kompaniju i/ili njene zaposlene. Na primer, iznosi plata ili medicinske informacije smatraju se privatnim.

[4] **Poverljive** (engl. *confidential*). Informacije koje se smatraju vrlo osetljivim i namenjene su samo za internu upotrebu. Ove informacije su izuzetak od obaveze javnog otvaranja tj. saopštavanja prema Aktu o slobodi informacija (*Freedom of Information Act*). Njihovo neovlašćeno otkrivanje može se ozbiljno i negativno odraziti na kompaniju. Na primer: informacije o razvoju novog proizvoda, poslovne tajne ili pregovori o spajanju s drugom firmom, smatraju se poverljivim informacijama.

Postoji i jednostavnija klasifikacija informacija koje se koriste u privatnom i komercijalnom sektoru:

[1] **Javna upotreba**. Informacije koje se mogu otkriti javnosti;

[2] **Samo interna upotreba**. Informacije koje je bezbedno interno otkriti, ali ne u javnosti;

[3] **Informacije poverljive za preduzeće**. Osetljive informacije koje se daju na uvid samo onome ko mora da zna za njih.

1.4 Metode zaštite

Za metode zaštite takođe postoji nekoliko pristupa i podela. S vremenom ove klasifikacije evoluiraju i menjaju se kako se razvijaju tehnologije i primene računarskih sistema i mreža. Prema nekim autorima, postoje četiri grupe metoda zaštite:

- kriptografske metode,
- programske metode,
- organizacione metode i
- fizičke metode.

Mnogi autori ovu podelu smatraju prevaziđenom i sve češće se koristi šema zasnovana na **deset domena sigurnosti** koje je definisala organizacija (ISC)2. Neki autori, takođe, definišu takozvane metode odbrane, klasifikujući ih na sledeći način:

- šifrovanje;
- softverska kontrola pristupa (pristupna ograničenja u bazi podataka ili operativnom sistemu);
- hardverska kontrola pristupa (pametne kartice – *smartcards*, biometrijske metode);
- zaštitne polise tj. pravila zaštite (poput insistiranja da se često menjaju lozinke),
- fizička kontrola pristupa.

Kao što je već rečeno, kontrola pristupa je sigurnosna usluga kojom se dozvoljava objektu proverenog identiteta da koristi određene usluge sistema, tj. određuje ko ima pravo da pristupi resursima i na kakav način. Za kontrolu pristupa u opštem smislu, najčešće važi sledeće:

- kontrola pristupa je obavezna i neizostavna;
- svi korisnici moraju biti ovlašćeni da bi mogli da pristupe nekom objektu;
- svi korisnici mogu da prava nad objektima koji njima pripadaju dodele drugim korisnicima;
- korisnici sistema ne smeju neovlašćeno da upotrebljavaju tuđa prava niti da menjaju tuđa prava nad entitetima koji im ne pripadaju.

Različiti aspekti zaštite

Aspekti zaštite se vrlo često definišu u odnosu na položaj mehanizama zaštite u računarskom ili informacionom sistemu ili računarskoj mreži. Pod ovim se često podrazumevaju sledeći nivoi:

- **Zaštita na nivou aplikacije**. Zaštita na nivou aplikacije može da obuhvati, na primer, sledeće elemente: softversku zaštitu aplikacije (recimo, zaštitu od prekoračenja bafera), izolovanje bitnih aplikacija na namenskim serverima i umreženim računarima, primenu specifičnih protokola (na primer, kriptografski zaštićenog protokola SSH umesto nezaštićenog protokola Telnet).
- **Zaštita na nivou operativnog sistema**. Kada se govori o zaštiti na nivou operativnog sistema, ulazi se u veoma složeno i obimno područje koje na neki način dotiče sve slojeve operativnog sistema. Zaštita na nivou operativnog sistema obuhvata i vezu operativni sistem – aplikacije, kao i odnos prema mrežnoj arhitekturi tj. vezama sa drugim sistemima.[6]

[6] Prema nekim preporukama, minimalna zaštita obuhvata: blokiranje nepotrebnih servisa (finger, ftp, telnet), obezbeđivanje sveobuhvatne i obavezne kontrole pristupa na nivou korisnika, obezbeđivanje integriteta softvera koji čini operativni sistem (većina sigurnosnih napada usmerena je na operativne sisteme bez primenjenih zakrpa, pa je zato potrebno redovno – čitaj: što češće – ažurirati sve elemente sistema najnovijim „zakrpama“). Međutim, ovim nije iscrpljen ni minimum realnih zahteva, tako da će o ovoj temi biti više reči u 10. poglavlju.

- **Zaštita na nivou mrežne infrastrukture**. Kada se govori o zaštiti na nivou mrežne infrastrukture, obično se misli na sledeće osnovne elemente: primenu mrežnih barijera (engl. *firewalls*), blokiranje nepotrebnih portova (priključaka), šifrovanje putanje, izolovanje putanje pomoću rutera i komutatora ili pomoću posebne infrastrukture.
- P**roceduralna i operaciona zaštita**. Ovaj nivo zaštite obuhvata sledeće elemente: definisanje i sprovođenje pravila zaštite, politike i procedure, detekciju napada, proaktivno delovanje tj. sprovođenje preventivnih mera u cilju zaštite i smanjivanja ranjivosti sistema, upravljanje konfiguracijom sistema, podizanje svesti o sigurnosnim problemima i obrazovanje korisnika.

Posebne segmente u metodama zaštite čine zaštita od elementarnih nepogoda (požara, poplava, zemljotresa) i zaštita od terorizma ili drugih destruktivnih i rušilačkih akcija. Treba voditi računa i o pravnim, etičkim, društvenim i psihološkim aspektima.

Nekoliko primera iz prakse

U ovom delu navedeni su neki praktični primeri i situacije u kojima se koriste različite metode i tehnike zaštite. Sve ove ideje i primeri biće detaljno analizirani u ostalim poglavljima knjige.

- Formiranje demilitarizovane zone (DMZ). DMZ je neutralna zona između privatne mreže i javne mreže, formirana pomoću računarskog hardvera i softvera. Koristi se kombinacija rutera, mrežnih barijera, posredničkih servera (engl. *proxy servers*) i softverskih sistema za detekciju i sprečavanje napada.
- Ispitivanje softvera. Pre instaliranja bilo kog softvera u bilo kom proizvodnom ili operativnom okruženju, potrebno je detaljno ispitivati taj softver u razvojnom okruženju. U ispitivanje softvera spada i instaliranje, npr. Web servera, ftp servera, servera za e-poštu i sistema za upravljanje bazama podataka (obavezno uključiti sve potrebne zakrpe, koje se vrlo često odnose na sigurnost rada).
- Zaštita vitalnih kompanijskih podataka. Posebno osetljive datoteke (podaci o klijentima, podaci o uplatama i isplatama, podaci o platama, podaci o dokumentima) čuvaju se u bazama podataka koje imaju ograničenu mogućnost povezivanja sa spoljašnjim mrežama. Čuvanje pojedinih vitalnih podataka na odvojenom mestu ili medijumu, sa ograničenim pristupom, izuzetno je važno je, na primer, pri skladištenju podataka o kreditnim karticama.
- FTP i Telnet. Blokirati FTP i Telnet kako bi se sprečilo da neovlašćeni korisnici preko ovih servisa pristupe štićenom sistemu. Ovi servisi se lako konfigurišu da budu dostupni onda kada su stvarno potrebni.

- Korišćenje lozinki. Obavezno upotrebljavati korisničke lozinke i često ih menjati. Ne koristiti „očigledne“ lozinke kao što su imena članova porodice, datumi rođenja, telefonski brojevi, imena kućnih ljubimaca i slično. Paradoks: korišćenje složenih lozinki može ponekad u praksi povećati opasnost, jer ih treba zapisivati, a to povećava sigurnosni rizik.
- Ažuriranje softvera. Pravovremeno ažurirati verzije softvera. Starije verzije softvera često sadrže sigurnosne propuste koje napadači mogu da iskoriste. Postoje timovi koji prate sigurnosne probleme i izdaju odgovarajuće savetodavne izveštaje (engl. *advisory reports*) o primećenim problemima.
- Politika zaštite informacija. Organizacija mora da proceni rizike. Potrebno je razviti jasnu politiku pristupanja informacijama i njihove zaštite.

Ljudi su, uglavnom, najosetljivije mesto u svakoj bezbednosnoj šemi. Ljudski faktor (na primer, zlonameran ili nepažljiv radnik, ili radnik koji nije svestan važnosti zaštite informacija) može da poništi i najbolju zaštitu.

Pristup organizacije (ISC)2

Nekoliko severnoameričkih profesionalnih udruženja koja čine (ISC)2 – *International Information Systems Security Certification Consortium* ustanovilo je postupak CISSP sertifikacije. (ISC)2 je neprofitna organizacija čija je jedina funkcija da razvija i administrira programe sertifikacije. Značenje titule CISSP je „sertifikovani profesionalac za sigurnost informacionih sistema“ (*Certified Information Systems Security Professional*). Uloga ove organizacije je da formira i održava Zajednički skup osnovnih znanja (engl. *Common Body of Knowledge*, CBK), koji obuhvata sledećih deset oblasti zaštite:

- sistemi za kontrolu pristupa,
- sigurnost razvoja aplikacija i sistema,
- planiranje oporavka od napada i obezbeđivanje kontinuiranog poslovanja,
- kriptografija,
- pravni i etički aspekti sigurnosti,
- fizička sigurnost,
- sigurnost operative,
- upravljanje sigurnosnim sistemima,
- sigurnosne arhitekture i modeli,
- sigurnost komunikacionih i računarskih mreža.

Ovih deset oblasti danas se često koriste prilikom klasifikacije zaštitnih metoda. (ISC)2 organizuje i vodi seminare i ispite za praktičare u oblasti sigurnosti koji žele da dobiju sertifikat CISSP. Kandidati za ispit moraju dokazati da imaju od 3 do 5 godina iskustva u oblasti sigurnosti i moraju potpisati Etički kodeks udruženja – *(ISC)2 Code of Ethics*.

Projektovanje sistema zaštite

Zaštitni mehanizam treba da bude jednostavan, dosledan (na isti način primenjen u celom sistemu) i primenjen na najnižim nivoima u sistemu.

Prilikom projektovanja sistema zaštite potrebno je odrediti sledeće:

- lice odgovorno za projekat,
- metode identifikacije korisnika i terminala,
- strukture šema ovlašćenja,
- načine detekcije nedozvoljenih pristupa,
- načine integrisanja zaštite u sistemske programe,
- postupke oporavka zbog oštećenja datoteka,
- postupke oporavka zbog otkaza sistema,
- metode nadzora,
- da li treba koristiti kriptografiju ili ne,
- koje kontrole treba ugraditi radi analize i korišćenja statističkih datoteka,
- koje kontrole treba ugraditi u operacije pregledanja datoteka.

Principi projektovanja sistema zaštite su sledeći:

- ekonomičnost zaštite (projekat treba da je što jednostavniji),
- pouzdanost zaštite,
- potpuna provera (inicijalizacija, radni režim, oporavak, isključivanje i održavanje),
- javnost projekta (mehanizmi zaštite ne bi trebalo da zavise od neznanja potencijalnih napadača),
- razdvajanje prava,
- najmanja prava,
- redukcija zajedničkih mehanizama,
- psihološka prihvatljivost (sprega između računara i čoveka),
- radni faktor,
- evidencija ugrožavanja.

Osim toga, prilikom projektovanja zaštite treba uzeti u obzir uticaj primene zaštitnih metoda na cenu i performanse računarskog sistema (mreže). Što je stepen zaštite veći, to je i cena veća, a performanse su obično slabije. Na primer, korišćenje jednokratne beležnice[7] (engl. *one-time pad*) u nekom kriptografskom protokolu, značajno će povećati nivo sigurnosti, ali će performanse biti upola lošije. Ukoliko se ovakav šifarski sistem koristi za komunikaciju preko Interneta, a kompanija plaća pristup Internetu na osnovu ostvarenog protoka, troškovi će biti dvaput veći.

[7] Kada se koristi jednokratna beležnica, neophodno je da se dvostruko veća količina podataka – tj. šifrat i ključ koji je dugačak kao otvoreni tekst – prenese kroz dva različita komunikaciona kanala. Šifrat se dobija primenom operacije ekskluzivno ILI nad otvorenim tekstom i ključem. Na mestu prijema primeni se operacija ekskluzivno ILI nad šifratom i ključem i dobije se otvoreni tekst.

Prilikom projektovanja zaštite treba uzeti u obzir i funkciju cene gubitaka podataka: C = f(D, I, P), gde je:

- C – cena gubitaka,
- D – tip datoteke kojoj pripadaju podaci,
- I – vrsta napadača za koju je zaštita projektovana (neupućena lica, obučena lica, lica koja žele da ostvare dobit, dobro opremljeni kriminalci, finansijski jake organizacije, viša sila),
- P – vrsta posledica po integritet podataka.

Jedno od pitanja na koje projektant takođe treba da odgovori glasi: da li je bolje koristi hardversku ili softversku zaštitu? Univerzalan odgovor na ovo pitanje ne postoji. Šta ćete koristiti, zavisi od konkretne situacije. U praksi se, međutim, najčešće koristi kombinacija softverske i hardverske zaštite. Na primer, ukoliko nekoliko zaposlenih u kompaniji treba povremeno da šifruje neke datoteke, odabraćete softverski paket koji pruža tu funkcionalnost (na primer, GnuPG). Ako se identitet svih zaposlenih proverava pomoću biometrijske metode, kupićete čitače za otisak prsta. Ukoliko treba da obezbedite rutiranje i kontrolu pristupa određenim mrežnim resursima, kupićete ruter sa ugrađenom mrežnom barijerom. U slučaju da svi zaposleni treba da šifruju elektronsku poštu koristeći infrastrukturu javnih ključeva, nabavićete čitače pametnih kartica (hardver) i odgovarajući softver za šifrovanje i potpisivanje pošte.