P O G L A V L J E 1

Opšti koncepti umrežavanja i bezbednosti

O ovom poglavlju

Ovo poglavlje pruža opšti pregled bezbednosnih problema. Prolazeći kroz ostatak knjige, naučićete više o svakoj ovoj temi. Kada završite knjigu i položite ispit Security+, moći ćete da razumete koncepte, probleme i jezik stručnjaka za bezbednost.

Napomena Kroz knjigu ćete nailaziti na upute na RFC dokumenta (*Request for Comment*), dokumenta NIST-a (*National Institute for Standards and Technology*) i CC dokumenta (*Common Criteria*) koja dopunjuju temu o kojoj se diskutuje. Ukoliko nije drugačije napomenuto, ova dokumenta možete naći na sledećim veb stranicama:

CC: *http://www.commoncriteria.org*

NIST: *http://www.csrc.nist.gov/publications*

RFC: *http://www.icann.rfceditor.org*

Da bi vam bilo zgodnije, neka ključna RFC, NIST i CC dokumenta su dodata na CD sa dopunskim materijalom za kurs. Ova dokumenta su data kao dopunske informacije. Međutim, preporučujemo vam da odete na navedene veb stranice da biste dobili najnovija dokumenta, ukoliko nameravate da koristite te informacije u donošenju odluka o bezbednosti.

Pre nego što počnete

Predznanje koje se očekuje da kandidat poseduje za sertifikat Security+, su sertifikati CompTIA A+ i Network+ ili ekvivalentno znanje, kao i znanje i iskustvo sa TCP/IP protokolom. Ne postoje preduslovi za ovo poglavlje, ali se u knjizi pretpostavlja da ispunjavate ove uslove koje je odredila CompTIA.

Lekcija 1: Opšti pregled

Mreža predstavlja dve ili više mašina koje su međusobno povezane radi komunikacije. Ovo je vrlo uprošćen pogled na mrežu, ali pomaže za sticanje opšte slike o mrežnom i poslovnom okruženju današnjice.

Kompanije povezuju računare radi deljenja informacija i resursa, obezbeđujući veću efikasnost i produktivnost uz niže troškove. Serveri su moćni računari a velikog kapaciteta za čuvanje podataka, tako da mogu da odgovore na zahteve klijentskih računara na mreži. Štampači su primer pomoćnih uređaja koji se mogu dodati mreži i kojima se može upravljati sa servera.

Računari klijenti se mogu povezati sa serverima, tako da zaposleni u kompaniji mogu da čuvaju i pozivaju podatke, i štampaju informacije na mrežnim štampačima. Na serveru se čuva rezervna kopija podataka, i u slučaju gubitka podataka, informacije se mogu rekonstruisati sa tog rezervnog medijuma. Radnici tako dobijaju alat koji im je potreban da urade posao, i sa razumnim troškovima se obezbeđuje efikasno, pouzdano radno okruženje u kome se poslovni podaci bezbedno čuvaju i donekle su zaštićeni od kvara opreme ili grešaka korisnika.

Da bi zaposleni bili produktivniji, konfiguriše se pristup Internetu. Time im se omogućuje da komuniciraju sa ljudima iz drugih kompanija koristeći instant poruke, e-poštu i mnoge druge metode. I druge kompanije su povezane sa Internetom i osetljivi podaci se prenose tamo-amo. Internet pruža brz i prilično jeftin način za obavljanje poslova, tako da se kompanije trude da preko njega obavljaju što je više moguće posla.

U procesu rada, važni podaci se čuvaju i prenose, i odvijaju se osetljive komunikacije. Neki oportunisti mogu pokušati da poremete taj proces, ukradu ili unište podatke, ili iskoriste komunikacije.

Kao osoba zadužena za računare u manjoj kompaniji, član grupe informacionih sistema (IS) u većoj kompaniji, ili jednostavno korisnik koji uživa u krstarenju Internetom i slanju e-pošte porodici i prijateljima, morate biti svesni osnovne bezbednosti informacija. Iako ne radite posao vezan za visoku tehnologiju, ukoliko se povežete sa Internetom važni podaci koje čuvate na vašem sistemu se mogu zaraziti virusom i tako ugroziti njegov rad.

Ako trenutno radite u oblasti visoke tehnologije ili želite tamo da se zaposlite, morate razumeti kako da zaštitite resurse vaše firme (uključujući i podatke koji su sačuvani u računarima), da zaposlenima obezbedite alat koji im je potreban za izvršavanje njihovog posla, i obezbedite vezu za komunikaciju sa drugim kompanijama i izvorima podataka. Jedan od vaših prvih koraka je da shvatite informacionu bezbednost, njene uslove i koncepte.

Po završetku ove lekcije, moći ćete da:

- razumete šta je u opasnosti;
- razumete kako da vrednujete svoja raspoloživa sredstva;
- razumete ciljeve informacione bezbednosti;
- razumete kako da kontrolišete rizik.

Vreme potrebno za lekciju: 20 minuta

Šta rizikujete

Možda mislite da su napadi malo verovatni i da oni ne prouzrokuju veliku štetu. Prema članku koji je objavljen na Newsfactor.com u februaru 2001. godine, Frank Bernhard sa Kalifornijskog univerziteta sproveo je istraživanje u 3000 američkih kompanija, i došao do zaključka da hakerski i drugi upadi koštaju kompanije skoro 6 centi za svaki dolar prihoda. To je velika šteta.

Informacija je dragocena

Za svaku kompaniju podaci su bogatstvo. Kada bi svaki proizvođač bezalkoholnih pića imao recept za Coca-Colu svako bi mogao da je napravi, i kompanija Coca-Cola bi teže prodavala svoj proizvod. U slučaju proizvođača aviona, može biti reči o novom mlaznom avionu koji će napraviti revoluciju u avionskoj industriji. Koja god da je kompanija i kakva god delatnost da je u pitanju, postoje podaci koji moraju biti zaštićeni i bezbedni.

Koliko su važne i vredne informacije vaše kompanije? Slede neka pitanja koja vam mogu pomoći da shvatite vrednost:

- Koliki je gubitak za moju kompaniju ukoliko se njeni podaci ugroze?
- Kolika je vrednost gubitka intelektualne svojine za moju kompaniju?
- Koliki je gubitak prihoda ili udela na tržištu?
- Kolika je vrednost gubitka tajnosti?
- Kolika je vrednost pokvarene reputacije moje kompanije?

Vrednost informacije je drugačija za svaku kompaniju. Za većinu, informacija je jedna od najbitnijih, ako ne i najbitnija vrednost. Ako se nešto od hardvera pokvari ili se ošteti zgrada u kojoj se nalazi kompanija, troškovi mogu biti veliki ali se oprema može zameniti a oštećenje se najčešće može popraviti. Međutim, ako se informacije unište, one nestaju zauvek. Ovo može naneti nepopravljivu štetu. Takođe, morate shvatiti da se vrednost informacije menja tokom njenog života. Ta vrednost takođe može biti realna ili procenjena.

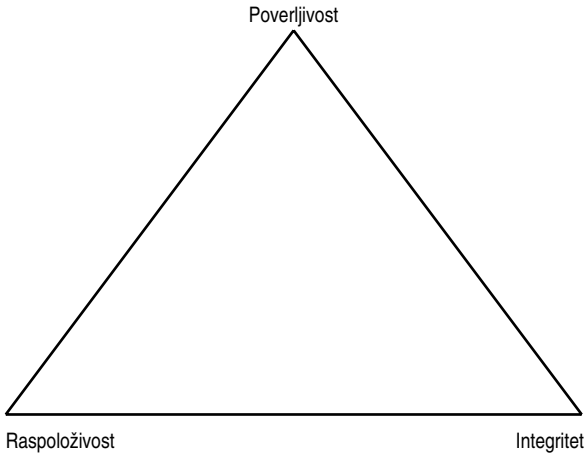
- **Realna vrednost.** Zamislite da radite za kompaniju koja proizvodi čaj. Ako vaša kompanija ima formulu za specijalnu mešavinu čija godišnja prodaja donosi 5 miliona dolara, onda možete reći da ta formula vredi 5 miliona dolara. Pet godina kasnije, može se desiti da kafa bude popularnija, tako da godišnja prodaja čaja može da padne na vrednost od 2 miliona dolara. Vrednost formule bi pala sa 5 miliona na 2 miliona dolara. Informacija se nije promenila, ali jeste njena vrednost.
- **Procenjena vrednost.** Kompanija za proizvodnju čaja ima veoma pametno rukovodstvo i grupu koja se bavi marketingom. Tim rukovodilaca ima plan za saradnju sa distributerima, da bi povećali zastupljenost čaja širom sveta. Marketinški tim ima ideju za reklamnu kampanju koja će popularisati čaj i mogla bi da uspori rast popularnosti kafe.

  Dobijanje pristupa informacijama rukovodećeg i marketinškog tima bi imalo vrednost, ali ona nije opipljiva, ona je procenjena. Bez obzira na to da li informacija ima opipljivu ili procenjenu vrednost, vaša je obaveza da je zaštitite. Što je veća realna ili procenjena vrednost, to je bolja meta za krađu.

Razumevanje cilja bezbednosti

C-I-A trojstvo, prikazano na slici 1-1, je uobičajen termin u razgovorima o bezbednosti informacija. C-I-A je na engleskom skraćenica od:

- **Confidentiality** (***Poverljivost***). Obezbeđuje da samo ovlašćeno osoblje ima pristup informacijama.
- **Integrity** (***Integritet***). Obezbeđuje da samo ovlašćeno osoblje modifikuje informacije.
- **Availability** (***Raspoloživost***). Obezbeđuje ovlašćenom osoblju pristup informacijama i sistemima kad god je to potrebno.



Slika 1.1 C-I-A trojstvo (trojstvo poverljivost-integritet-raspoloživost)

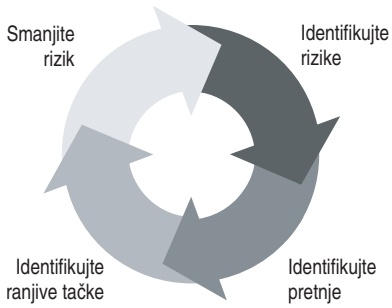
Kada napore da obezbedite poverljivost, integritet i raspoloživost podataka udružite sa fizičkom bezbednošću, možete pružiti vrlo efikasno bezbednosno rešenje.

Kroz celu knjigu su predstavljene odbrane od opisanih pretnji. Posao specijaliste za informacione sisteme, a naročito stručnjaka za bezbednost, jeste da pruži pouzdane podatke samo onima koji treba da imaju pristup i to kada im je pristup potreban.

Kontrola rizika

Informacije imaju vrednost, i moraju biti dostupne ovlašćenom osoblju za upotrebu kada i gde je to potrebno. Vaš posao kao stručnjaka za bezbednost je da svedete na minimum šanse da se C-I-A trojstvo sruši.

Kontrola rizika, prikazana na slici 1-2, je celokupan proces koji se koristi da se otkrije, kontroliše i ublaži moguća šteta. Pošto je nemoguće potpuno eliminisati rizik, cilj kontrole rizika je da ga umanji i održi C-I-A trojstvo. Ovo se postiže tako što se prvo utvrde rizici, otkriju pretnje i ranjive tačke i zatim se one svode na minimum.



Slika 1.2 Kontrola rizika

Rizik svodite na minimum tako što otkrijete rizike i napravite plan za njihovo ublažavanje. *Ublažavanje* se definiše kao pravljenje nečega manje štetnim ili manje bolnim; stoga vi planirate smanjivanje rizika. Za kompaniju koja proizvodi čaj, plan za ublažavanje mogao bi biti ograničenje broja kopija formule i broja lokacija na kojima je ona memorisana. Plan bi mogao da uključi i ograničenje broja ljudi koji imaju pristup formuli i kako joj oni pristupaju.

Da biste smanjili rizik prvo identifikujte potencijalne rizike, pretnje i ranjive tačke sa kojima se vaša kompanija suočava.

- *Rizik* je izloženost gubitku ili mogućem oštećenju. Kada govorimo o bezbednosti informacija, pod rizikom podrazumevamo mogućnost da spoljni faktori ugroze podatke, što bi vašoj firmi prouzrokovalo gubitak u vremenu, novcu i reputaciji.

  Kod kompanije koja proizvodi čaj, rizik je ako se formula zbog izloženosti otkri jer druge kompanije mogu početi da prave veoma sličan čaj. To bi ovoj kompaniji prouzrokovalo gubitak udela na tržištu. Ako je formula čaja opšte poznata a vrednost je bila u njegovoj jeftinoj proizvodnji, onda rizik gubljenja formule ne bi bio tako veliki. Vrednost je onda u procesu proizvodnje.
- *Pretnja* po bezbednost informacija je svaka aktivnost koja predstavlja moguću opasnost po vaše informacije. Pretnje mogu da imaju različite oblike, ali svaka predstavlja opasnost za C-I-A trojstvo. U primeru kompanije za proizvodnju čaja, druga kompanija bi mogla ukrasti formulu čaja, ili je neki radnik može prodati drugoj kompaniji.
- *Slaba tačka* je propust u zaštiti informacija odnosno u bezbednosti vašeg sistema i mreže, procesima i procedurama. Kod kompanije za proizvodnju čaja, formula čaja je vredna informacija. Ljudi moraju da imaju pristup formuli kako bi napravili čaj, i ta formula se mora negde čuvati.

Slabe tačke mogle bi biti lokacija na kojoj se čuva formula, broj ljudi koji moraju da imaju pristup formuli, i način na koji joj se pristupa.

Sve zajedno

Radi bezbednosti informacija morate štititi C-I-A trojstvo, ali ga ne možete štititi po svaku cenu, niti je to uvek potrebno. Na primer, ako vaša kompanija prodaje flaširanu vodu prečišćenu procesom inverzne osmoze, taj proces je dobro poznat i stoga nema nikakve svrhe štititi tu informaciju. S druge strane, bilo bi logično obezbediti informaciju o revolucionarnom procesu koji bi prepolovio troškove i vreme potrebno za prečišćavanje vode. Postoji izvesna granica vrednosti za ostvarivanje zaštite, i stoga bi trebalo da kombinujete svoje znanje o vrednosti, pretnjama, ranjivim tačkama i rizicima kako bi sastavili izvodljiv plan. Da biste to uradili pratite sledeći plan:

- Odredite vrednost informacije.
- Utvrdite što je moguće više rizika kao i pretnji i slabih tačaka vezanih za iste.
- Ublažite otkrivene rizike.
- Budite svesni da uvek postoji nešto što ste prevideli.

Rizik se može ublažiti samo do izvesne mere, a ponekad će njegovo smanjenje koštati više nego sam rizik. Na primer ako radite u kompaniji koja proizvodi čaj i imate datoteku sa podacima o svim sastojcima koji se koriste za proizvodnju čitave linije proizvoda, možda nije vredno vremena, novca i napora da se ta informacija zaštiti, jer je to jednostavno spisak sastojaka. Ali ako imate recept za čaj koji se najviše prodaje, a vaša kompanija je jedina koja ga proizvodi, onda za čuvanje te informacije vredi utrošiti znatno vreme, napor i novac. Svaki plan o rizicima je drugačiji jer se svaka kompanija nalazi u drugačijim okolnostima, ima drugačiji budžet i radnu snagu koje koristi da bi umanjila rizik. Neka od pitanja koje treba da postavite da biste bolje utvrdili sa kojim ograničenjima posluje vaša firma, su sledeća:

- Koju informaciju treba zaštititi?
- Kolika je vrednost te informacije?
- Kakvi su izgledi da ta informacija bude ugrožena?
- Koliki je gubitak za kompaniju ako ta informacija bude ugrožena?
- Na koji način se pristupa informaciji?
- Koliko ljudi ima pristup informaciji?
- Da li je informacija slabo obezbeđena?

Bez obzira na to da li odlučite da ublažite rizik, treba da otkrijete što je više moguće potencijalnih rizika i da razvijete plan za ublažavanje koji obuhvata svaki od njih. Kada identifikujete sve rizike i odredite troškove (vreme i novac) kojima obezbeđujete informaciju, uporedite ih sa vrednošću informacije da biste odredili koje su mere bezbednosti razumne. U svakoj situaciji će biti drugačija kontrola rizika i kompromisa. Koristeći primer kompanije koja proizvodi čaj možete utvrditi sledeće:

- Vrednost formule čaja je 5 miliona dolara jer prodaja čaja toliko donosi.
- Rizik je da bi konkurenti mogli dobiti tu formulu.
- Pretnja je da bi neko spolja mogao da locira formulu čaja i pristupi joj, ili da neki radnik dobije pristup formuli i proda je ili je preda konkurenciji.
- Slaba tačka je to što se formula čuva na pet različitih lokacija i mnogi mogu da joj pristupe.
- Da biste ublažili rizik, formulu možete čuvati na jednom mestu i ne dozvoliti nikome pristup, ali to je nepraktično. Bolji plan za ublažavanje rizika bio bi da se smanji broj lokacija na tri i ograniči pristup na broj od 25 osoba.
- Stvari o kojima možda niste razmišljali bile bi ograničenje pristupa na oblast u kojoj se formula koristi za pravljenje čaja, objavljivanje spiska osoba koje imaju pristup i provera identiteta ljudi koji imaju pristup formuli.

Verovatno postoji još nekoliko pretnji, slabih tačaka, rizika i ublaženja koje možete otkriti. Od dobrog specijaliste za bezbednost se zahteva da ih otkrije što je više moguće.

Vežba: Pravljenje plana za kontrolu rizika

Vi ste stručnjak za bezbednost u maloj kompaniji koja proizvodi i prodaje mirišljave sveće. Vaša kompanija prodaje ove sveće maloprodajnim radnjama, ali ih takođe prodaje preko Interneta. Sirovine koje koristite za proizvodnju sveća se nabavljaju preko Interneta od četiri različita snabdevača. Vaša kompanija ima osoblje za daljinski sistem prodaje koji funkcioniše širom sveta, i oni preko Interneta pristupaju vašoj internoj mreži. Takođe, imate radnike kojima je dozvoljeno da rade kod kuće i imaju daljinski pristup mreži kompanije.

Kompanija prodajom ostvaruje 12 miliona dolara godišnje, i to 3 miliona prodajom običnih sveća u maloprodaji, 2 miliona prodajom specijalnih mirišljavih sveća koje se mogu nabaviti samo preko Interneta, i 7 miliona dolara prodajom sirovina za pravljenje sveća.

U ovom vežbanju treba da:

- Odredite vrednost svakog dela posla.
- Identifikujete što više pretnji.
- Identifikujete što više ranjivih tački.
- Identifikujete što više rizika.
- Napravite plan kontrole rizika.

U ovoj vežbi ne postoje konačni odgovori. Ona je napravljena kako bi vas ohrabrila da razmišljate o mogućim rizicima i o načinu da ih ublažite. Kroz knjigu ćete sticati vredne informacije koje možete iskoristiti da u ovoj vežbi date bolji i detaljniji odgovor. Zabeležite svoj sadašnji odgovor, a kada završite sa udžbenikom vratite se na ovu vežbu da biste uvideli koliko ste znanja i veštine stekli.

Pregled lekcije

Sledeća pitanja su sačinjena sa namerom da se utvrdi ključno gradivo predstavljeno u ovoj lekciji. Ukoliko niste u stanju da odgovorite na neko pitanje, pročitajte ponovo lekciju, a zatim opet pokušajte da odgovorite na pitanje. Odgovore na pitanja možete naći u dodatku A „Pitanja i odgovori”.

1. Iako postoji potreba za bezbednošću informacija, i postoji mala verovatnoća da neko hakeriše vaš sistem, obično nema nikakve štete i trošak kompanije koja je pretrpela hakerski napad je relativno mali. (Tačno ili netačno?)

2. Radite za kompaniju koja prodaje čaj i sirovine za proizvodnju čaja. Ukupna godišnja prodaja iznosi 5 miliona dolara. Prodaja čaja donosi 2 miliona, a prodaja sirovina 3 miliona dolara. Čaj ima veoma neobičan ukus i ne može se kopirati. Šta od navedenog treba uzeti u obzir pri utvrđivanju vrednosti formule čaja i zašto?
   a. Kako se čaj proizvodi
   b. Kolika je ukupna godišnja prodaja čaja
   c. Gde je sačuvana formula
   d. Koliko osoba u kompaniji ima pristup formuli

3. Radite za kompaniju koja prodaje čaj i sirovine za proizvodnju čaja. Ukupna godišnja prodaja iznosi 5 miliona dolara. Prodaja čaja donosi 2 miliona, a prodaja sirovina 3 miliona dolara. Čaj ima veoma neobičan ukus i ne može se kopirati. Grupa zadužena za marketing ima plan od koga se očekuje da udvostruči prodaju čaja, sa 2 na 4 miliona dolara. Koja je realna vrednost formule čaja? Koja je procenjena vrednost marketinškog plana?

4. Kada se govori o bezbednosti informacija, koja su tri kamena temeljca C-I-A trojstva?

5. Napišite redosled po kome se izvršavaju sledeći koraci kada se pravi plan kontrole rizika.
   a. Identifikujte ranjive tačke vašeg C-I-A trojstva.
   b. Odredite vrednost vašeg C-I-A trojstva.
   c. Identifikujte pretnje vašem C-I-A trojstvu.
   d. Utvrdite kako možete da ublažite rizike.

Rezime lekcije

Iz ove lekcije ste naučili da se bezbednost informacija svodi na osiguravanje poverljivosti, integriteta i raspoloživosti podataka. Ključne tačke koje treba da zapamtite su:

- Poverljivost znači osigurati da su informacije bezbedne, sa pristupom koji je dozvoljen samo odgovarajućim ljudima.
- Integritet znači osigurati da informacije ne budu slučajno ili zlonamerno promenjene ili uništene.
- Raspoloživost znači obezbediti da informacije i komunikaciona sredstva budu spremna za upotrebu kada je to potrebno

- Da biste osigurali da vaš plan održava poverljivost, integritet i raspoloživost, neophodna je bezbednost. Morate identifikovati moguće pretnje i tačke upada, slabe tačke, rizik koji postoji ako vaš plan obezbeđenja propadne, i načine da ublažite te rizike postavljanjem odbrane. Da biste ublažili rizike morate odrediti vrednost informacije koju štitite, i šta bi bila moguća posledica ako bi informacija dospela u pogrešne ruke. Dok ovo radite morate da shvatite pravne posledice toga što radite, i da osigurate da nit dokaza ostane netaknuta da bi sudska vlast mogla da skupi potrebne podatke i goni odgovorne.
- C-I-A trojstvo je način da zapamtite da su poverljivost, integritet i raspoloživost informacije briga svakog stručnjaka za informacione sisteme, a naročito stručnjaka za bezbednost.

Lekcija 2: Identifikacija pretnji

Pretnje možete kategorizovati da bi ih bilo lakše identifikovati. One nisu uvek zasnovane na principu da neko napada vaše računarske sisteme ili mrežu. Na primer, zamislite da radite u kompaniji za proizvodnju čaja kojoj ljudi naručuju čaj preko Interneta, a zaposleni popunjavaju narudžbine pristupom bazi podataka na serveru koji vi održavate. Ako je server pao, zaista nije bitno da li je prostorija u kojoj se on nalazi poplavljena, ili je server zaražen virusom koji je privremeno uništio sve podatke. Informacija nije na raspolaganju ljudima kojima je potreban pristup njoj.

Po završetku ove lekcije, moći ćete da:

- identifikujete izvor pretnje;
- razumete šta je napad;
- razumete šta je zlonameran kod;
- razumete ko napada;
- razumete šta je društveni inženjering.

Vreme potrebno za lekciju: 25 minuta

Izvori pretnji

Da biste pretpostavili pretnju ili da biste reagovali na nju, morate razumeti njenu prirodu. Na primer, ako štitite svoje datoteke tako što instalirate softver koji blokira komunikaciju sa Internetom, tako štitite pristup preko spoljašnjih izvora, ali ste vrlo malo uradili da sprečite da neko iz kompanije pristupi podacima. Postoji mnogo načina da se kategorizuju pretnje, ali važno ih je identifikovati što je više moguće, i napraviti plan kontrole rizika za svaku od njih.

Pri identifikovanju izvora pretnje, treba da postavite nekoliko pitanja koja pomažu u otkrivanju tipa pretnje, a zatim je ublažite. Neka od pitanja koja možete postaviti su sledeća:

- Da li je pretnja rezultat neke vrste katastrofe ili napada?
- Ako je u pitanju napad, da li pretnja potiče od nekog ko radi u kompaniji, ili od nekog izvan nje?
- Ako preti napad, da li je napad dobro poznat?
- Ako preti napad, da li možete da ge identifikujete pregledanjem kontrolnih datoteka?
- Ako preti napad, da li je taj napad usmeren na posao?

Što više znate o tipovima pretnji koje mogu da se jave, možete bolje da planirate i umanjite rizik. Što više kategorija ili načina za identifikovanje pretnji imate, utoliko je više pretnji koje ćete moći da identifikujete i napravite plan.

Pretnje od katastrofe

Katastrofa se definiše kao iznenadna ili velika nesreća. Neke katastrofe su prirodne, a ima i prouzrokovanih. Na primer, požar može biti prirodni događaj (kao šumski požar) ili prouzrokovan (kao požar koji je podmetnuo neki palikuća). Neke stvari se ne smatraju katastrofama, ali sigurno mogu biti porazne za C-I-A trojstvo vaše kompanije.

- **Elementarne nepogode.** Na C-I-A trojstvo mogu uticati prirodne katastrofe kao što su zemljotresi ili uragani. Morate identifikovati one prirodne katastrofe koje će najverovatnije uticati na vašu kompaniju, i da napravite plan za ublažavanje mogućih gubitaka.
- Da bi vaš plan obuhvatio prirodne katastrofe morate identifikovati tipove katastrofa koje su najverovatnije, morate da utvrdite koliko se često te stvari događaju (istorijski), i zatim da napravite plan za ublažavanje koji minimizuje uticaj na vašu kompaniju. Taj plan možda neće biti ostvaren, ali ga ipak treba utvrditi.
- **Katastrofe koje čovek prouzrokuje.** Katastrofe koje prouzrokuje čovek ili prouzrokovane katastrofe, koje mogu da utiču na C-I-A trojstvo, uključuju požar, nestanak struje ili pad strukture. Pošto je definicija katastrofe iznenadna ili velika nesreća, taj događaj bi bio veliki i ne bi uticao samo na bezbednost informacija. Glavna briga i prioritet je bezbednost ljudi zahvaćenih katastrofom, ali dobro planiranje će pomoći kompaniji da se brže oporavi od nedaće.
- **Nezgoda.** *Nezgoda* se definiše kao nesrećni slučaj. Ako server padne a stručnjaci koji ga popravljaju i obnavljaju su odsutni, tada je C-I-A trojstvo ugroženo. Razmotrite ozbiljnost i verovatnoću tog događaja, bez obzira na to da li je katastrofa epskih razmera ili manji nesrećni slučaj, tako da možete da minimizujete rizik.

Pretnje od napada

Pretnje od napada su prepoznatljiviji događaji, i obično ih je teže predvideti od katastrofa i nezgoda, jer se ovaj tip pretnji konstantno menja. Zlonamerni korisnici stalno prerađuju metode napada da bi iskoristili različitu tehnologiju i specifične ranjive tačke koje se otkriju. Da biste razumeli kako da se branite od napada, morate da razumete tehnologiju koja je napadnuta. Mnoge pretnje spadaju u više kategorija, ali cilj nije da kategorizujemo napade; cilj je napraviti određen broj kategorija koje nam pomažu da identifikujemo pretnje.

- **Pretnje po posao.** Neke pretnje su direktno povezane sa poslom kojim se bavi vaša kompanija; stoga napadi koji su najverovatniji mogu biti bolje određeni. Na primer, ako vaša kompanija ima specijalnu formulu čaja, onda će pretnja verovatno stići od nekoga ko pokušava da ukrade formulu. Ako vaša kompanija održava veb lokacije drugim kompanijama, onda bi pretnja verovatno bila da se ugase veb lokacije, da se ljudi preusmere na drugu veb lokaciju, ili da se prikupe neki poverljivi podaci pridruženi toj lokaciji.
- **Pretnje koje mogu biti proverene.** Proverljive pretnje se mogu identifikovati pomoću podataka koji su uhvaćeni. Na primer, ako imate veb lokaciju koju neko želi da ishakeriše, možda možete da pogledate datoteke dnevnika ili postavite alarm da identifikujete tip napada, vreme u koje se dogodio i druge specifične podatke. Ovo vam možda neće pomoći da umanjite rizik od uspešnog napada, ali će vam pomoći da identifikujete tip napada i pripremite svoje obezbeđenje da se bori protiv njega. I što je još važnije, omogućiće vam da se bolje pripremite za sledeći sličan napad u budućnosti.
- **Opšte poznate pretnje.** Neke pretnje su opšte poznate i možete da čitate o njima. Ovaj tip pretnji obično je fokusiran na određenu aplikaciju ili tehnologiju, i može a ne mora biti zlokoban. Primer ovog tipa pretnje je virus ILOVEYOU koji je zarazio sisteme za e-poštu. Virus je slao e-poštu svima iz adresara zaraženog korisnika. Iako virus nije uništio sistemske podatke, preopteretio je servere za e-poštu širom sveta i pokazao da se može naneti šteta i računarima primaoca e-pošte. Iako podacima nije naneta šteta, servis e-pošte (servis od presudnog značaja) bio je neraspoloživ i stoga je C-I-A trojstvo bilo prekinuto.
- **Unutrašnje pretnje.** Morate biti svesni i unutrašnjih pretnji koje mogu da utiču na C-I-A trojstvo. Na primer, ako koristite kablove da povežete sve sisteme u mrežu, postoji verovatnoća da neko stekne pristup vašoj mreži i beleži komunikaciju koja se odvija preko lokalne mreže. Ukoliko ne koristite neki metod provere identiteta internih korisnika, onda je integritet vaših informacija ugrožen.
- **Spoljašnje pretnje.** Spoljašnje pretnje nastaju izvan vaše kompanije. Na primer, ako se povezujete sa veb lokacijom na Internetu, ta veb lokacija bi mogla daljinski da učita aplikaciju na vaš računar koja bi pristupila adresaru u vašem programu za e-poštu. S druge strane, neko bi mogao da uhvati komunikaciju između vas i veb lokacije sa kojom ste se povezali da biste kupili novi auto. Uradivši to, zlonamerni korisnik može da sazna vaše ime, adresu i druge lične informacije kao što su broj kreditne kartice ili računa u banci. Ovaj tip pretnje bio bi spoljašnja pretnja.

Napadi

Napad je pokušaj da se zaobiđu bezbednosne kontrole na računaru. Napad može da promeni, objavi ili odbije podatke. Tipovi napada se menjaju skoro brzinom svetlosti, ali većina ima ime koje dobro opisuje tip napada.

Napadi su detaljno obrađeni u kasnijim poglavljima, ali sledi kratka lista tipova napada sa kratkim opisom, da biste videli neke od tehnika koje se danas koriste:

- **Odbijanje servisa (***Denial of Sevice***,** DoS**).** Ovaj tip napada čini servis neoperativnim. Na primer, DoS napad može da učini da popularna veb lokacija bude neko vreme nedostupna. Distribuirano odbijanje servisa (*Distributed Denial of Service,* DDoS) ima isti uticaj, ali je napad raspodeljen kroz više napadajućih računara.
- **Lažiranje adrese (**engl. *spoofing***).** U informacionoj bezbednosti, *lažiranje adrese* označava pretvaranje da ste neko drugi tako što ćete imitirati, maskirati se ili podražavati tu osobu. Ako obezbedite korisničko ime i lozinku, adresu internet protokola ili bilo koji akreditiv koji nije vaš, da biste dobili pristup mreži, sistemu ili aplikaciji, onda vi zavaravate taj sistem. Postoji više tehnika lažiranja koje se danas koriste, ali najčešća je lažiranje IP-a koja predstavlja falsifikovanje informacija u IP paketu.
- **Posrednik (**engl. *man-in-the-middle***).** U mrežama, računar uhvati komunikaciju između dva računara i imitira oba. Na primer, klijentski računar se poveže sa serverom da bi preuzeo izveštaj o mesečnim transakcijama. Računar posrednik bi igrao ulogu servera u komunikaciji sa klijentom, a ulogu klijenta u komunikaciji sa serverom. Ovo računaru posredniku omogućuje da uhvati svu komunikaciju između računara klijenta i servera.
- **Pogađanje lozinke.** Ovaj tip napada podrazumeva pogađanje korisničkog imena i lozinke pri pokušaju da se pridobije pristup mreži ili sistemu. Postoje programi koji pokušavaju da provale lozinku koristeći tehniku grube sile, i drugi koji proveravaju lozinku uz pomoć rečnika. Ovi napadi po rečniku mogu ne samo da porede reči sa rečnikom, nego i da koriste velika i mala slova ili menjaju slova brojevima u pokušaju da provale lozinku.

Zlonameran kôd

Zlonameran kôd je softver ili firmver koji se namerno postavlja u sistem iz neovlašćenih razloga. Primeri za to su parazitski program Morris i virus Melissa. O ovim napadima možete naći dosta informacija na Internetu, a takođe su detaljnije obrađeni kasnije u ovoj knjizi. Neki od osnovnih tipova su:

- **Virus.** *Virus* je program koji može sam da se umnožava, ali ne i da se sam rasprostire. Zahteva instalacioni vektor, kao što je izvršna datoteka priložena uz e-poštu ili disketu. Virus će zaraziti druge programe na tom sistemu, a može se preneti sa mašine na mašinu pomoću priloženih datoteka uz e-poštu, ili pomoću nekog medijuma kao što je disketa. Virus može da uništi podatke, sruši sistem, a može biti i bezopasan.
- **Parazitski program, crv.** *Parazitski program* je program koji može sam i da se umnožava *i* da se rasprostire. Rasprostire se tako što zarazi druge programe na istom sistemu, a takođe se preko mreže širi na druge sisteme, bez potrebe za instalacionim vektorom. Parazitski program vam takođe može uništiti podatke, srušiti sistem, ili može biti bezopasan.
- **Trojanski konj.** Uopšteno, program *Trojanski konj* izgleda poželjno i bezopasno, ali zapravo nanosi štetu. Na primer, možete preuzeti nešto za šta mislite da je igra, ali kada to pokrenete, otkrijete da vam briše sve izvršne datoteke diska.

Ko napada?

Da biste se zaštitili od napada morate da znate ko napada i kako. Neki napadi su pokušaji da se stekne pristup vašim informacijama, dok su drugi prevare. Citiramo šta je rekao vojni strateg i general Sun Tzu Wu: „Spoznaj svog neprijatelja i spoznaj sebe, i dobićeš stotinu bitaka.” Slede neki tipovi napadača:

- **Haker.** Termin *haker* ima dve definicije, u zavisnosti od toga sa kim razgovarate. Za programera, haker može biti osoba koja sastavlja kôd koji pruža brzo rešenje za težak problem. Kôd ne mora da bude tečno napisan, ali je funkcionalan i efikasan. Za ostale ljude, haker je neko ko probija zaštitu na automatizovanom informacionom sistemu ili mreži. Ovaj tip hakera (poznat i kao *razbijač*, engl. *cracker*) je obično štetan i zlonameran, iako možda pokušavaju da provale u sistem zbog nečega što smatraju dobrim i višim ciljem, oni ipak provaljuju u sistem.
- **Novajlija.** *Novajlija* je neko ko teži da postane haker, ali nije dovoljno ovladao tehnologijom. Obično novajlija ide na veb lokaciju koju je napravio haker, i pokreće program koji napada mrežu ili računarski sistem. Iako se napadi novajlija obično lako otkriju i odbiju, mogu da proizvedu dovoljno „belog šuma” koji sakriva dokaze da haker pokušava ozbiljniji napad na sistem ili mrežu.

Društveni inženjering

Jedan od napada od koga je najteže odbraniti se jeste *društveni inženjering*, odnosno iskorićavanje tuđe pristojnosti i lakovernosti da bi se prevarom stekao pristup obezbeđenim podacima. Na primer, neko može da vas nazove i kaže da on ili ona popravlja vaš sistem, i treba mu lozinka da se prijavi na sistemu i proveri da li je popravka završena. Druga smicalica bi mogla biti da neko dođe do obezbeđenih vrata koja zahtevaju posebnu pristupnu karticu, i zamole vas da zadržite otvorena vrata da bi on ili ona ušli.

Postoji nekoliko načina na koji društveni inženjering može da podrije i najbolji plan bezbednosti. Jedno od najboljih rešenja za ublažavanje rizika od društvenog inženjeringa je obuka korisnika. Ona će vašim korisnicima pomoći da shvate koja informacija se nikada ne sme dati drugoj osobi, pružiće najbolje vežbe za rad sa osetljivim informacijama, kao i postavljanje lozinki i druge svakodnevne zadatke.

Pregled lekcije

Sledeća pitanja su sačinjena sa namerom da se utvrdi ključno gradivo predstavljeno u ovoj lekciji. Ukoliko niste u stanju da odgovorite na neko pitanje, pročitajte ponovo lekciju, a zatim opet pokušajte da odgovorite na pitanje. Odgovore na pitanja možete naći u dodatku A „Pitanja i odgovori”.

1. Zaduženi ste za pravljenje plana za ublažavanje pretnji informacionom sistemu vaše kompanije. Šta od navedenog bi vaš plan trebalo da identifikuje kao napravljene pretnje i elementarne nepogode? (Izaberite sve što važi.)
   a. Nepotpune rezervne kopije
   b. Nestanci struje
   c. Zgrada vam je poplavljena
   d. Serveri vaše kompanije su zaraženi virusom
   e. Požar u zgradi

2. Pri određivanju rizika izazvanog pretnjom, spoljašnje pretnje su opasnije od unutrašnjih. (Tačno ili netačno?)

3. Izaberite napade koji su bazirani na upotrebi zlonamernog koda:
   a. Trojanski konj
   b. Društveni inženjering
   c. Virus
   d. Novajlija
   e. Parazitski program

Rezime lekcije

- Pretnje su sve što ugrožava C-I-A trojstvo, i mogu dospeti iz brojnih izvora. Primeri pretnji uključuju sledeće:
  - hakere (ili provalnike u sistem) koji pokušavaju da provale u vašu mrežu ili računare;
  - zlonamerni kôd kao što je računarski virus ili trojanski konj;
  - ljude koji rade za vašu kompaniju ali su nezadovoljni ili plaćeni da skupe i prodaju informacije vaše kompanije;
  - požar, poplavu, kvar hardvera ili elementarnu nepogodu.
- Pretnje mogu doći i od spoljašnjih izvora, kao što su hakeri i e-pošta, ali mogu doći i od izvora koji su unutar kompanije, kao u slučaju nezadovoljnog radnika ili nekoga ko je stekao fizički pristup vašim računarima.