CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosna metrika

CCERT-PUBDOC-2008-07-235

+CERT.hr u suradnji s LSS

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

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

CARNet CERT, www.cert.hr

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

LS&S, www.LSS.hr

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

Sadržaj

1. Uvod

U današnje se vrijeme za sigurnost informacijskih sustava često nude rješenja koja su polovična i vezana uz samo neke dijelove sustava. Zbog toga je procjena sigurnosti takvih sustava nesigurna i nepouzdana. Često se za sustav kaže da ima dobru ili lošu sigurnost no to nije dobra mjera za procjenu sigurnosti, odnosno rizika od napada na sustav.

Sigurnost cijelog sustava je uvijek proporcionalna sigurnosti njegove najslabije točke. Kako bi bilo moguće kvalitetno odrediti sigurnosni rizik sustava i ostvariti pouzdano upravljanje sigurnošću u organizaciji, koristi se sigurnosna metrika. Proces upravljanja rizikom sve je važniji u procesu zaštite informacijskih resursa i poslovnih procesa jer predstavlja temelj izgradnje sigurne i pouzdane informatičke infrastrukture. Kako bi se omogućilo kvalitetnije i ekonomičnije donošenje odluka vezanih uz unapređenje i poboljšanje sigurnosti potrebno je identificirati kritične dijelove sustava i odrediti pripadne sigurnosne rizike. Bez kvalitetnih analiza i procjena rizika informacijskih sustava vrlo je teško razviti i implementirati siguran sustav.

Kad se govori o sigurnosnoj metrici treba pripaziti na značenje pojma metrika, odnosno na razliku između metrike i mjerenja. Mjerenja se odnose na podatke koji su pohranjeni u sustavu, a metrika može biti objektivna ili subjektivna interpretacija podataka dobivenih mjerenjima. Metrika nastaje analizom podataka i ukazuje do kojeg su stupnja ostvareni sigurnosni ciljevi, kao što je npr. povjerljivost podataka. Iz analize je moguće zaključiti koje je akcije potrebno poduzeti kako bi se uklonio sigurnosni rizik i poboljšala cjelokupna organizacija sigurnosti informacijskog sustava.

U dokumentu je opisana sigurnosna metrika, zašto se koristi te na koji se način primjenjuje. Također, opisani su načini provođenja mjerenja, tipovi i metode sigurnosnih metrika, intenzitet i vrijednosti rizika.

2. Definicija sigurnosne metrike

Metrika nastaje analizom podataka dobivenih mjerenjima i predstavlja objektivnu ili subjektivnu interpretaciju tih podataka. Oblikuje se prikupljanjem i analizom podataka vezanih uz sigurnost i radni učinak informacijskog sustava. Svrha mjerenja sigurnosti i performansi sustava je uspostava nadzora nad mjerenim događajima i aktivnostima te ispravljanje otkrivenih propusta u sigurnosti sustava, kao i poboljšanje pouzdanosti sustava na temelju promatranih podataka.

Široko uvriježen princip upravljanja je da se nekom aktivnošću ne može upravljati ako se ona ne može mjeriti. Isti princip vrijedi za sigurnost informacijskih sustava. Sigurnosna metrika može biti moćno oruđe za raspoznavanje učinkovitosti različitih komponenti sigurnosnih programa, sustava i procesa te osoblja i dijelova organizacije zaduženih za rješavanje sigurnosnih problema. Metrikom se, također, može identificirati razina rizika kod poduzimanja određenih akcija te u tom smislu pružiti smjernice u prvenstvu ispravljanja problema. Uz to, koristi se i za podizanje razine svjesnosti o sigurnosti informacijskih sustava u organizaciji.

Korištenjem sigurnosne metrike za procjenu sigurnosti sustava moguće je odgovoriti na pitanja kao što su:

- Je li informacijski sustav tvrtke sigurniji danas nego što je bio jučer?
- Kako se možemo usporediti s drugima na području sigurnosti?
- Je li sustav tvrtke siguran od potencijalnih sigurnosnih napada?

Sigurnosna se metrika informacijskog sustava treba temeljiti na ciljevima koji se žele postići u smislu povećanja radnog učinka i sigurnosti. Metrika omogućava postizanje ovih ciljeva identifikacijom i provedbom preporučenih sigurnosnih postupaka. Postupci se definiraju sigurnosnim politikama i procesima koji vode konzistentnoj implementaciji sigurnosnih postupaka u cijeloj organizaciji. Neki primjeri ciljeva koji se žele postići i vezani su uz poboljšavanje učinkovitosti sigurnosnog sustava su:

- „Obrazovanje zaposlenika uključuje sažetak pravila ponašanja."
- „Obrazovanje zaposlenika uključuje sažetak i reference vezane uz sigurnosnu politiku organizacije."

Primjenom sigurnosne metrike kvantitativno se određuju podaci koji se mogu koristiti za usporedbe, analize i praćenje promjena u sustavu. Također, izračunavaju se postoci i prosječne vrijednosti vezane uz rizik sustava u smislu postojanja sigurnosnih propusta. Podaci koji se prikupljaju za izračunavanje metrike moraju biti lako dostupni i promatrani proces mora biti mjerljiv. Trebaju se razmatrati samo procesi koji su konzistentni i ponovljivi. Rezultati učinkovite sigurnosne metrike pružaju korisne podatke za upravljanje sigurnosnim resursima i omogućuju pojednostavljenje pripreme izvještaja o radnom učinku. Uspješna primjena sigurnosne metrike u organizaciji podiže razinu sigurnosti informacijskih sustava u toj organizaciji te omogućuje efektivno upravljanje rizicima.

Svrha upravljanja rizicima je omogućavanje organizacijama (tvrtkama) ispunjenje svojih poslovnih zadaća pomoću sigurnijeg informacijskog sustava u smislu pohrane, razvoja ili isporučivanja informacija, omogućavajući vodstvu izradu dobrih strategija upravljanja rizicima i opravdanje izdataka koji su dio proračuna.

3. Razlozi provođenja sigurnosne metrike

Sigurnosna metrika omogućuje upravljanje rizicima u organizaciji. Sigurnosni rizici uključuju različite prijetnje te mogućnosti ugrožavanja informacijskog sustava od strane vanjskih napadača, ali i internih korisnika. Kod upravljanja rizicima potrebno je najprije identificirati kritične informacijske resurse te prema tome odrediti potrebni stupanj zaštite pojedinih resursa. Upravljanje rizicima i sigurnosna metrika su relativno nove discipline na području informacijskih sustava. Proizašle su iz potrebe za standardizacijom postupaka vezanih uz upravljanje sigurnošću čime se u konačnici može uvelike utjecati na troškove poslovanja. Proces analize podataka o sigurnosti sustava te upravljanje rizicima podrazumijevaju prepoznavanje čimbenika koji mogu negativno utjecati na povjerljivost, raspoloživost i integritet informacijskih resursa. Također, sigurnosna metrika uključuje i vrednovanje pojedinih resursa i troškova njihove zaštite. Krajnji korak procesa je poduzimanje odgovarajućih mjera zaštite koje svode sigurnosni rizik na prihvatljivu razinu u skladu s poslovnim ciljevima organizacije. Proces upravljanja rizicima sastoji se od tri faze :

1. procjena rizika (eng. Risk Assessment),
2. umanjivanje rizika (eng. Risk Mitigation) i
3. ispitivanje i analiza (eng. Evaluation and Assessment).

Ciljeve postizanja prihvatljivog sigurnosnog rizika određuje uprava, kao i u kojoj mjeri i na kojim će se mjestima primijeniti sigurnosna metrika. Također, potrebno je postići kompromis između budžeta organizacije i primjene sigurnosne metrike. Sigurnosni se rizik može razmatrati na nekoliko načina: moguće ga je prihvatiti onakvim kakvim jest, pristupiti njegovom smanjivanju ili ga ignorirati i prebaciti u neku drugu organizaciju. U nastavku su objašnjene sigurnosne prijetnje i zahtjevi koje treba ispuniti informacijski sustav.

3.1. Sigurnosne prijetnje i zahtjevi

Svaka organizacija posjeduje informacije koje treba zaštititi od zlouporabe. Primjenom određenih sigurnosnih postupaka potrebno je zaštititi ranjive podatke jer posljedice zlouporabe mogu biti katastrofalne i odraziti se na poslovanje organizacije (tvrtke). Sigurnosne su prijetnje uvijek prisutne i definiraju se kao svaki događaj koji može poništiti ili smanjiti učinkovitost sustava, odnosno ograničiti ili onemogućiti ispunjenje cilja sustava ili procesa.

Kako bi se smanjila mogućnost iskorištavanja sigurnosnih propusta potrebno je postaviti određene sigurnosne zahtjeve. Oni ovise o vrsti podataka koji se žele zaštititi i postavljaju se u skladu s važnosti podataka koje ima organizacija. Podjela sustava koji se moraju zaštititi po važnosti:

- vojni informacijski sustavi,
- bankovni informacijski sustavi,
- zdravstveni informacijski sustavi,
- informacijski sustavi državnih institucija,
- informacijski sustavi osiguravajućih organizacija i
- poslovni informacijski sustavi.

Sigurnost računalnih sustava moguće je ugroziti na više načina, a neki od njih su:

- vanjski utjecaji – mehaničko uništenje uređaja, oštećenje nastalo elementarnim nepogodama, krađa medija s informacijama,
- sučelje prema korisniku,
- neodgovarajući unutarnji zaštitni mehanizmi – postupak autentikacije, ovlasti, autorizacija i
- komunikacijski mehanizmi - informacije se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim kanalima

Napadač može iskoristiti sigurnosne propuste različitim vrstama napada te narušiti sigurnost informacijskog sustava na mnogo načina. Neki od njih su:

- prisluškivanje – napadač može čitati pakete koji su namijenjeni nekom drugom te na taj način doći do osjetljivih informacija. Ovaj je napad pasivan i djeluje se na povjerljivost (tajnost) podataka.
- prekidanje – uljez može prekinuti komunikacijski kanal između izvorišta i odredišta. Narušava se raspoloživost podataka.
- promjena sadržaja poruka – uljez može prekinuti komunikacijski kanal i lažno se predstavljati kao izvorište podataka te promijeniti sadržaj poruka. Narušava se integritet (besprijekornost) podataka.
- izmišljanje poruka – napadač može uspostaviti komunikacijski kanal s odredištem, lažno se predstavljati kao izvor i slati izmišljene poruke ili stare snimljene poruke. Narušava se integritet informacija.
- lažno predstavljanje – napadač se predstavlja kao neki drugi korisnik ili može podesiti računalo tako da se ono pretvara da je neko drugo te se lažno predstavlja i vara druga računala.
- poricanje – nakon što je poruka poslana korisnik se može predomisliti i poricati autorstvo poruke te tvrditi krađu identiteta.

Prema opisanim napadima zaključuje se da se sigurnost računalnih sustava zasniva na ispunjavanju tri osnovna sigurnosna zahtjeva:

- povjerljivost – podaci u sustavu smiju biti dostupni samo ovlaštenim korisnicima,
- raspoloživost – podaci moraju uvijek biti na raspolaganju ovlaštenim korisnicima usprkos mogućim neočekivanim događajima, kao što je nestanak struje i
- integritet – podatke u informacijskom sustavu mogu mijenjati samo za to ovlašteni korisnici. Potrebno je osigurati jamstvo da su informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku.

Navedeni zahtjevi mogu biti ugroženi na različite načine, kao što su namjerna ili nenamjerna ljudska pogreška, vanjski utjecaji (požar, poplava, kvarovi opreme itd.) ili neki drugi nepredvidljivi događaji. Osim ovih osnovnih zahtjeva koje proces upravljanja sigurnošću informacijskog sustava treba zadovoljiti, potrebno je spomenuti zahtjeve vezane uz implementaciju sigurnosnih postupaka:

- autentičnost – ovlašteni se korisnici moraju moći jednoznačno prepoznati,
- autorizacija – dodatno se za osiguranje integriteta autenticiranim i ovlaštenim korisnicima dozvoljava ili zabranjuje pristup nekim sadržajima, odnosno određenim računalnim resursima i
- neporecivost – ovlašteni korisnik ne smije moći opovrgnuti poruku koju je ranije poslao tvrdnjama da ju je poslao uljez.

Informacijski su resursi sva ona sredstva koja organizacija koristi kako bi ostvarila svoje poslovne ciljeve. Svaka komponenta računalnog sustava može utjecati na ispunjavanje ili neispunjavanje sigurnosnih zahtjeva.

3.2. Utjecaj pojedinih komponenti računalnih sustava na sigurnost

Kad se razmatra sigurnost nekog informacijskog sustava potrebno je, osim identifikacije sigurnosnih prijetnji i zahtjeva, proučiti i utjecaj pojedinih komponenti računalnog sustava na sigurnost organizacije. Komponente računalnog sustava uključuju sklopovlje računala, programe, podatke i komunikaciju. Svaki nabrojani resurs može različito utjecati na ispunjavanje sigurnosnih zahtjeva.

- Sklopovlje računala može najviše utjecati na raspoloživost podataka i najviše je podložno vanjskim utjecajima. Unapređenje sustava se može postići odgovarajućim održavanjem sustava i ograničavanjem pristupa. Također, moguće je izgraditi sustav sa zalihošću te na taj način povećati raspoloživost podataka.
- Programi mogu utjecati na sva tri osnovna sigurnosna zahtjeva (povjerljivost, raspoloživost, integritet). Zlouporaba ili krađa programa može utjecati na tajnost podataka, a neovlaštena izmjena programa može djelovati na integritet i raspoloživost. Najpoznatiji način neovlaštenog djelovanja na programe su napadi računalnim virusima. Virusi su programski odsječci koji se komunikacijom ili razmjenom medijima za pohranu podataka unose u računalni sustav. Obično su izgrađeni tako da se sami pridodaju u neke postojeće programe i pri pokretanju djeluju štetno. Jedanput zaraženo računalo teško je vratiti u prvobitno normalno radno stanje te je stoga djelotvornije djelovati preventivno. Uz viruse poznati zloćudni programi su crvi i trojanski konji. Crvi su cjeloviti programi koji samo sebe prenose kroz komunikacijsku mrežu s računala na računalo i pri tome djeluju destruktivno. Trojanski konj je program koji obavlja neki koristan posao, ali mu je pridodana neka funkcija koja djeluje štetno. Na primjer, trojanski konj može djelovati tako da se uspostavi slobodan pristup datotekama koje su inače zaštićene.
- Podaci pohranjeni u bazama podataka ili datotekama podložni su svim oblicima narušavanja sigurnosti. Raspoloživost se može ugroziti brisanjem datoteka, tajnost neovlaštenim čitanjem sadržaja datoteka i besprijekornost (integritet) neovlaštenom promjenom sadržaja.
- Komunikacije su sa stanovišta sigurnosti najosjetljiviji dio računalnih sustava (iz razloga što brojni korisnici mogu pristupiti korisnikovom sustavu i podacima na njemu) i podložni su narušavanju svih oblika sigurnosti.

3.3. Koristi sigurnosne metrike

Upravljanje rizicima i sigurnosna metrika pružaju mnogo organizacijskih i financijskih koristi. Organizacija može poboljšati ukupnu sigurnost kao i uspostaviti odgovornost za ostvarenje sigurnosnih zahtjeva računalnog sustava. Proces prikupljanja podataka i procjena rizika omogućuju upravi da točno definira metode i akcije za ispravnu implementaciju sigurnosnih mjera. Sigurnosnom se metrikom može analizirati svaki aspekt informacijske sigurnosti u organizaciji. Na primjer, rezultati procjene rizika testiranja na moguće upade u sustav i ostale aktivnosti vezane uz sigurnost mogu se kvantificirati i koristiti kao podaci za stvaranje sigurnosne metrike. Upotrebom rezultata analiza moguće je točno odrediti problematične dijelove sustava koji zahtijevaju poboljšanje te opravdati zahtjeve za investicijama u sigurnost. Oskudnost ekonomskih resursa, fiskalna ograničenja i stanje tržišta prisiljavaju vladu i industriju da djeluje s reduciranim budžetom. U takvom okružju teško je opravdati visoka ulaganja u sigurnost informacijskih sustava. U prošlosti su se kao argumenti protiv ulaganja u sigurnost koristili nedostatak detalja i specifičnosti, što je rezultiralo povećanom ugroženosti informacijskih sustava. Upotreba sigurnosne metrike omogućava organizacijama procjenu uspjeha i neuspjeha sigurnosnih ulaganja u prošlosti i sada. Prikupljeni se podaci i analize koriste za planiranje budućih ulaganja u sigurnost. Također, sigurnosna se metrika koristi za utvrđivanje učinkovitosti ostvarenih sigurnosnih procedura i postupaka.

4. Primjena sigurnosne metrike

Sigurnosna metrika ima široku primjenu, a sama implementacija nije vremenski ograničena nego uglavnom ovisi o stupnju zaštite koji se želi uvesti. Jedna od primjena je i dijagnosticiranje sigurnosnih problema u organizacijama. Kod primjene metrike obično se postavljaju dva pitanja:

- Koje se hipoteze vezane uz učinkovitost sigurnosnih postupaka mogu oblikovati?
- Koji dokazi podupiru ili opovrgavaju hipotezu?

Na području sigurnosti metrika pomaže organizacijama:

- definirati sigurnosne rizike,
- uočiti postojeće probleme,
- djelovati na propuste u sustavima,
- mjeriti performanse implementiranih protumjera i
- preporučiti poboljšavanje tehnologija i procesa

4.1. Tipovi metrika

Postoji mnogo vrsta sigurnosnih metrika, a u nastavku dokumenta slijedi opis dvije najvažnije:

1. Tehnička (dijagnostička metrika)

   Ova metrika idealna je za dijagnostiku stanja sustava, a budući da je izražena brojevima njeni se parametri mogu izračunavati svakodnevno. Ovaj tip metrike mjeri:

   - Perifernu obranu: efektivno upravljanje rizicima zahtijeva razumijevanje otkud vrebaju potencijalne opasnosti te organizacije mjere učinkovitost sigurnosnih mjera elektroničke pošte, antivirusnih programa, antispam sustava, vatrozidne zaštite i sustava za detekciju upada.
   - Zaštitu i kontrolu sustava: metrikom se ustanovljuje raspon zaštite i doseg kontrola (od strane pojedinih korisnika) kao što su konfiguracija, zakrpe i sustavi za rukovanje ranjivostima.
   - Dostupnost i pouzdanost: organizacije (tvrtke) se oslanjaju na raspoloživost informacijskih sustava te oni trebaju biti otporni na vanjske utjecaje, kao što je srednje vrijeme oporavka i postoci koji izražavaju vrijeme koje je sustav bio u pogonu pokazuju ovisnosti između sigurnosti i profita. Razmatraju se, dakle, sustavi koji osiguravaju kontinuiranost i omogućuju oporavak od neočekivanih sigurnosnih incidenata.

2. Aplikacijska sigurnosna metrika

   Ovaj tip metrike predstavlja potpuno odvojenu domenu mjerenja i ima svoju dijagnostiku. Aplikacije se koriste za automatizaciju procesa poduzeća, kao što su plaćanje računa, korisnička služba i sl. Koliko god su aplikacije važne za poslovanje organizacija, mogu postati njihova slaba točka. Mjerenje relativne sigurnosti programskog koda nije jednostavan zadatak. Sigurnosna industrija još uvijek nije postigla dogovor u vezi značenja pojma izgradnje sigurne aplikacije. Iako postojeće definicije variraju, tri su osnovna načina mjerenja sigurnosti aplikacija, a to su:

   - oni koji se temelje na prebrojavanju sigurnosnih propusta koje mogu iskoristiti udaljeni ili lokalni napadači bez poznavanja programskog koda aplikacije,
   - brojanje pogrešaka u dizajnu i implementaciji koda i
   - stvaranje kvalitativne procjene rizika upotrebom težinskog sustava bodovanja (gdje se definiraju parametri koji se mjere obzirom na njihov ukupni značaj u sustavu)

4.2. Primjeri metrike

Za primjer općenite dijagnostičke metrike poslužit će izmišljena organizacija u kojoj se šef pita „Jesu li podaci u mojoj tvrtki sigurni od udaljenih napada?“. Neka je postavljena hipoteza da su podaci u tvrtki vrlo ranjivi na udaljene napade. Kako bi se ova izjava potvrdila konstruira se podhipoteza koja se može potvrditi ili opovrgnuti postavljanjem posebnih pitanja. Odgovori na ta pitanja se mogu precizno mjeriti i empirički izraziti. Slijedeća tablica daje primijenjenu dijagnostiku:

Podhipoteza	Dijagnostičko pitanje
Računalna mreža sadrži propuste i pruža jednostavan pristup bilo kome.	Koliko je web stranica povezano direktno s jezgrom mreže bez vatrozidova? Koliko računala može bežično pristupiti takvim stranicama? Počevši bez ikakvog predznanja koliko je vremena potrebno da se dobije potpuni pristup domenskim kontrolama?
Napadač može lako dobiti pristup unutarnjim sustavima jer su sigurnosne politike vezane uz zaporke neodgovarajuće.	Koji će postotak korisničkih računa biti ugrožen u roku od 15 minuta ili manje?
Nakon što je napadač pristupio mreži, može jednostavno preuzeti administratorske ovlasti.	Koliko će administrativnih zaporki biti ugroženo u roku od 15 minuta ili manje?
Uljez koji je otkrio propust negdje u mreži može pristupiti jezgri transakcijskih sustava.	Koliko ima internih zona koje odjeljuju korisnike, poslužitelje, transakcijske sustave i poslužitelje sa sučeljima za pristup Internetu,
Radne su stanice izložene riziku napada virusima ili crvima.	Koliko zakrpa nedostaje operacijskom sustavu?
Virusi i crvi mogu brzo zaraziti velik broj računala.	Koliko je mrežnih vrata (eng. prot) otvoreno na svakom računalu? Koliko je vrata riskantno?
Sigurnost aplikacija je slaba i ovisna je o tvorničkim postavkama.	Koliko je sigurnosnih propusta u svakoj poslovnoj aplikaciji? Kako se ranjivosti jedne aplikacije odnose naspram druge aplikacije?

Tablica 1. Primjena dijagnostičke metrike

Kako bi se odgovorilo na postavljena pitanja može se oblikovati npr. četveromjesečni plan i program za tvrtku (vrijeme se određuje prema specifičnostima sustava i različito je za sve ustanove koje žele primijeniti sigurnosnu metriku). U tom se periodu ocjenjuje periferna obrana, interna računalna mreža, najvažniji aplikacijski sustavi i povezana infrastruktura. Nakon toga se stvara sigurnosna metrika kojom se dokazuju hipoteze. Na temelju sigurnosne metrike moguće je oblikovati program sigurnosnih ispravaka koji se trebaju implementirati te odlučiti koliki će se budžet uložiti u provedbu ispravaka.

Drugi primjer sigurnosne metrike je primjena anketnih upitnika:

1. Imate li mogućnost otkriti neovlaštene ulaze u računalni sustav ?

Da Ne

Ako je odgovor pozitivan, objasnite način na koji to provodite.

_____

_____

_____

2. Jeste li otkrili pokušaje neovlaštenog ulaza u računalni sustav proteklih 12 mjeseci?

Da Ne Ne znam

Ako je odgovor pozitivan, objasnite način na koji ste to otkrili.

_____

_____

3. Ako ste otkrili ulaze u sustav koji je oblik aktivnosti izvršio napadač (upisati broj)?

__Promjena podataka
__Prijenos datoteka
__Krađa lozinke
__Unos virusa
__krađa novca
__Onemogućavanje rada servisa
__Otkrivanje poslovnih tajni
__Oštećenje podatak

__nešto drugo, navesti _____

4. Što je poduzeto kao sigurnosna mjera (upisati broj)?

__usmena opomena
__pismeni ukor
__otkaz
__ništa
__nagodba van suda
__suspenzija

__nešto drugo, navesti _____

Slika 1. Anketa

Neka organizacija provodi procjenu rizika od neovlaštenog upada u računalni sustav. Potrebno je odrediti dosadašnja iskustva u zaštiti od napada. Kako bi se prikupili podaci o trenutnom stanju moguće je ispitati zaposlenike i proučiti postojeću dokumentaciju. Najpogodnije prikupljanje podataka je anketom. Na temelju odgovora na anketu oblikuje se odgovarajuća sigurnosna metrika. Pritom treba voditi računa o tome da podaci iskazani anketom budu vjerodostojni. (tj. da zaposlenici iskreno odgovaraju na pitanja).

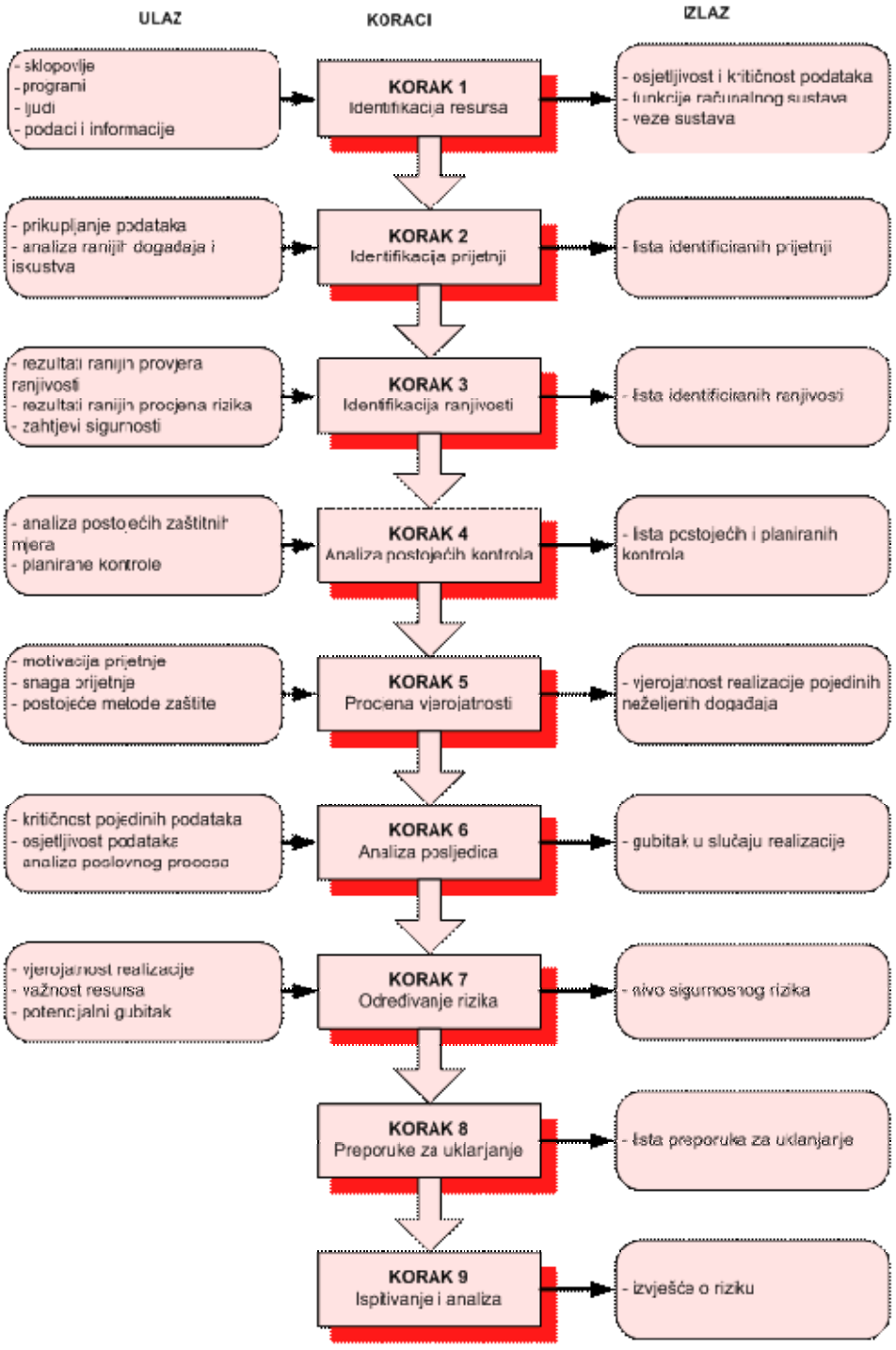
4.3. Metode metrika

Postoje četiri najpopularnija okvira (standarda) metrika, a to su:

- U.S.NIST (The Unites States National Institute of Standards and Technology) – određuju sedamnaest obitelji sigurnosnih kontrola visoke razine.
- ISO 17799 (ili ISO standard) – definirao je British Standards Institute i postoji deset glavnih hijerarhija od kojih svaka sadrži trideset i šest kontrola visoke razine s više od dvjesto preporučenih sigurnosnih politika i standarda.
- COBIT (Control Objectives for Information Technology) – definira ciljeve informacijskih i sigurnosnih sustava za organizacije koje implementiraju upraviteljske programe. Uključuje trideset i četiri cilja u domenama planiranja, organizacije, dohvata, implementacije, dostave, podrške i praćenja.
- ITIL (Information Technology Infrastructure Library) – koncentrirana je na široki raspon tehnologija i definira osam skupina ustaljenih postupaka za informacijske sustave.

4.3.1. NIST-ov pristup

Proces uključuje identifikaciju, analizu, uklanjanje rizika kao i periodičko ispitivanje. Procjena rizika je vezana uz konkretno određivanje sigurnosnog rizika i pojedini resurs. Sigurnosna se metrika koristi za procjenu rizika kako bi se odredila veličina potencijalnih prijetnji. Ovaj proces sadržava analizu svih ranjivosti i prijetnji, vjerojatnost realizacije rizika i moguće posljedice kao i analizu troškova/koristi. Rezultati provedenog postupka procjene rizika daju se na uvid upravi organizacije, kao i podaci koji su neophodni za donošenje odluka vezanih uz ulaganje u sigurnosna rješenja i proizvodnje. Na temelju tih podataka organizacija odlučuje o primjeni sigurnosne metrike. Proces procjene rizika je vrlo složen i najbolje ga mogu provoditi stručnjaci sa iskustvom i koji dobro poznaju sustav. Proces se sastoji od devet koraka, kao što je prikazano na slici 2.



Slika 2. Slijed faza u procjeni rizika

Određivanje sigurnosnog rizika zahtijeva provođenje svih koraka u procesu procjene rizika.

Sigurnosni rizik se može izraziti kao funkcija koja ovisi o tri parametra: prijetnja, ranjivost i vrijednost resursa.

```
Rizik = f (Prijetnja, Ranjivost, Vrijednost resursa)
```

Resursi se mogu razmatrati na dva načina, kao vrijednost u novcima i kao potencijalni gubitak za organizaciju u slučaju gubitka ili neraspoloživosti resursa.

U nastavku slijedi detaljno objašnjenje NIST-ovog pristupa:

1. Definiranje domene djelovanja obuhvaća identifikaciju i klasifikaciju informatičkih resursa. Identificiraju se svi resursi koji su značajni za organizaciju za koju se stvara sigurnosna metrika i pridjeljuje im se odgovarajuća novčana vrijednost, ako je to moguće (vrijednost opreme ili pojedine informacije). Za informacijski sustav u razvoju definiraju se odgovarajuće sigurnosne mjere, pravila i svojstva. Za prikupljanje tehničkih podataka se koriste različite metode, a neke od njih su ankete vezane uz upravljanje i plan kontrolnih operacija postojećeg sustava, razgovori s osobljem za potporu informacijskog sustava i vodstvom, razmatranja na licu mjesta (prikupljaju se podaci o fizičkom okruženju i operacijskoj sigurnosti informacijskog sustava). Osim toga, koriste se i dokumenti o strategiji, dokumentacija politike (zakonski dokumenti) administracija sustava, dizajn sustava te dokumentacija o sigurnosnim elementima te različiti alati za automatsko skeniranje sustava vezano uz pronalazak sigurnosnih ranjivosti.
2. Identifikacija prijetnji čiji je cilj otkriti izvore mogućih prijetnji i pribavljanje liste prijetnji koje mogu ugroziti postojeći informacijski sustav, kao i poslovanje organizacije. Izvori prijetnji se mogu podijeliti na namjerne (ciljana zlouporaba sigurnosnih nedostataka) i nenamjerne (izvori koji slučajno iskorištavaju ranjivosti, kao što su prirodne nepogode). Također potrebno je odrediti povezanost sa resursima organizacije i moguće motive napada.
3. Identifikacija ranjivosti gdje se pod pojmom ranjivosti podrazumijevaju svi propusti u sigurnosti koje napadač može iskoristiti za neovlaštene aktivnosti. Na primjer, ranjivosti su pogreške i propusti u programskom kodu, površno dizajnirani i implementirani programi i dijelovi sustava i drugi. Važno je da se ranjivost analizira u kombinaciji s identificiranim prijetnjama jer su dva parametra usko povezana. Implementiraju se samo ona zaštitna sredstva koja se mogu opravdati u smislu zaštite poslovnih ciljeva i budžeta organizacije.
4. Analiza postojećih kontrola koje su ostvarene ili se planiraju ostvariti kako bi se informacijski sustav što bolje zaštitio. Za kvalitetno određivanje vjerojatnosti zlouporabe pojedine ranjivosti potrebno je uzeti u obzir sve postojeće sigurnosne postupke ugrađene u sustav. Ako je zaštita ostvarena kvalitetno, vrlo je mala vjerojatnost da će se moći ugroziti sustav. Kontrole mogu biti ugrađene u obliku sklopovlja, programa (antivirusna zaštita, kriptografske metode) ili se mogu odnositi na sigurnosne politike, preporuke i postupke koji se stječu iskustvom.
5. Kod utvrđivanja vjerojatnosti pojave neželjenih događaja razmatraju se slijedeći čimbenici:
    - motivacija i sposobnost izvora prijetnji,
    - značajke određene ranjivosti i
    - postojanje i djelotvornost postojećih kontrola
6. Analiza posljedica podrazumijeva procjenu negativnog učinka koji može nastati u slučaju uspješne zlouporabe ranjivosti. Potrebno je voditi računa o svrsi resursa, kritičnosti resursa (značaju za organizaciju) i osjetljivosti podataka.
7. Nakon analize posljedica provodi se određivanje rizika. U ovom se koraku procjenjuje rizik kojem je izložen informatički sustav. Rizik se određuje za sve parove prijetnja-ranjivost, pri čemu se razmatraju vjerojatnost iskorištavanja ranjivosti u odnosu na pripadnu prijetnju, posljedice u slučaju uspješne zlouporabe te kvaliteta i učinkovitost planiranih ili već postojećih sigurnosnih postupaka.
8. Stvaranje preporuka za uklanjanje, odnosno umanjivanje rizika. Cilj je analizirati moguće načine zaštite i svođenje sigurnosti sustava na prihvatljivu razinu. Prilikom predlaganja sigurnosnih mjera treba razmotriti čimbenike kao što su pouzdanost i efikasnost preporučenih postupaka, troškovi ostvarenja i održavanja, utjecaj na poslovne procese i informacijski sustav, pravna ograničenja i slično.
9. Posljednji korak u stvaranju sigurnosne metrike je ispitivanje i analiza danih preporuka te njihova implementacija prema prioritetu i mogućnostima organizacije. Osim toga, analiziraju se faktori koji utječu na funkcionalnost, ostvarivost i isplativost sigurnosnih mjera. Na kraju se formira izvještaj koji treba biti jasan i pregledan te jednostavan za interpretaciju.

4.3.2. Metode ISO standarda

Tri su najpopularnije metode ISO standarda:

1. CRAMM (CCTA Risk Analysis and Method Managemen)
2. COBRA (Consultative, Objective and Bi-functional Risk Analysis)
3. RuSecure

Metoda CRAMM je prvenstveno napravljena za procjenu rizika državnih sustava, no može se upotrijebiti i u tržišnim organizacijama. Tri su osnovne faze ove metode:

- identifikacija i vrednovanje imovine (fizičke, programa, podataka i pomoćne imovine koja čini informatički sustav),
- procjena prijetnja i ranjivosti (virusa, pogrešaka na opremi i programima, terorizma, ljudskih pogrešaka i sl.) i
- izbor i preporuka mjera zaštite (izračunava razinu trenutačnog rizika)

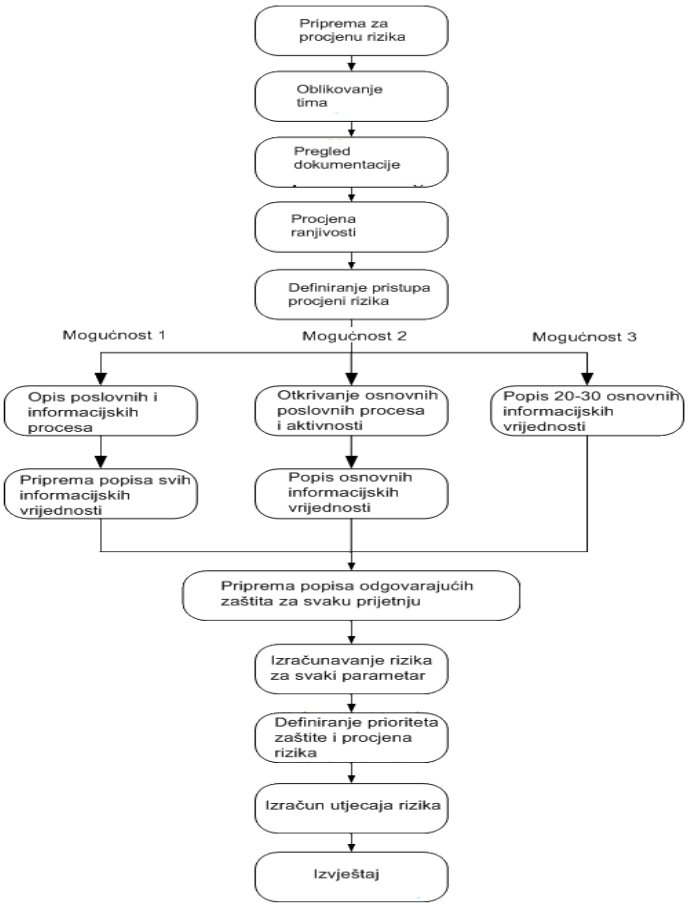
Mogući nedostaci metode su cijena i potreba angažiranja konzultantske tvrtke bar u početnoj fazi procjene.

Metoda COBRA je oblikovana za pomoć i podršku poslovnim organizacijama koje uvode ISO norme. Ovom se metodom pružaju upute za procjenu informacijskih sustava i stvaraju se alati koji se isporučuju u obliku programskog paketa. Za prikupljanje podataka koriste se strukturirani upitnici koji se ispunjavaju na računalu. Evaluacija se odvija u tri koraka:

- izgradnja upitnika,
- procjena rizika i
- izrada izvješća

U izvješćima se detaljno definiraju protumjere i zaštita za pojedine dijelove informacijskog sustava. Prednosti ove metode su velika baza prijetnji, mogućnost evaluacije pojedinih modula, a nedostaci su slaba strukturiranost, nepreglednost i dugotrajnost procesa procjene te ograničene mogućnosti prilagodbe izvješća.

RuSecure metoda (slika 3) se temelji na upitima u obliku priručnika kojima se savjetuje procjenitelja o pitanjima vezanim uz proces stvaranja sigurnosne metrike. Priručnik sadrži praktične savjete o izvedbi pojedinih dijelova u procesu procjene rizika. Metoda je jednostavna za implementirati, a koraci metode su pregledni i prikaz procjene je razumljiv neupućenom korisniku.



Slika 3. Koraci procjene rizika po metodi RuSecure

Sigurnosna metrika koja se ostvaruje ovom metodom uključuje procjenu ranjivosti, vrednovanje imovine, prijetnje, utjecaj prijetnji na imovinu, učestalost djelovanja i sve komponente se izražavaju kvalitativno. Mjernim se ljestvicama podaci prilagođuju u veličine pogodne za numeričko prikazivanje rezultata. Prednosti metode su preglednost i strukturiranost kriterija, jednostavnost, brzina provedbe i cijena, a nedostaci su nedovoljna preciznost podataka koji se mjere (što ovisi o tome koliko je detaljno izrađen upitnik), nepostojanje podrške programskog alata i necjelovitost.

4.3.3. COBIT

Metoda COBIT se temelji na istraživanju, razvoju, objavi i promoviranju općenito prihvaćenih ciljeva nadzora informacijske tehnologije za svakodnevnu uporabu.

Metoda obuhvaća metriku četiriju domena:

- Planiranje i organizacija – definiranje strateških sigurnosnih planova, razmatranje cjelokupnog budžeta i razina ulaganja, procjena rizika i rukovanje organizacijskim i ljudskim resursima.
- Prikupljanje i ostvarenje – identifikacija, prikupljanje, razvoj i ugradnja sigurnosnih rješenja.
- Dostava i potpora – definiranje sigurnosnih razina, ovlasti i pristupa, podučavanje korisnika, rješavanje incidenata i upravljanje programima u svrhu zaštite podataka, objekata i operacija.
- Nadzor – odnosni se na praćenje sustava, procjenu učinkovitosti sigurnosnih kontrola i potporu za procese.

Nabrojane domene ugrubo odgovaraju tipičnim fazama u životnom ciklusu razvoja sustava: strategija, planiranje, implementacija, održavanje i potpora.

COBIT je kontrolni model koji zadovoljava potrebe upravljanja informacijskim sustavom i osigurava cjelovitost informacija i drugih elemenata informacijskog sustava. Metoda COBIT objavljena je u 6 dijelova koji zajedno s programskim alatom čine jedinstven okvir i metodu procjene rizika. U središtu zanimanja osnovne metode COBIT veliki su sustavi s dnevno intenzivnom i raspodijeljenom obradom podataka.

Slika 4. Metoda COBIT i njene domene

4.4. Intenzitet i vrijednosti rizika

4.4.1. Kvantitativna procjena

Koriste se egzaktne numeričke vrijednosti, tj. vrijednosti resursa se prikazuju se u novčanim jedinicama. Na području kvantitativne procjene rizika standardna je upotreba metode ALE (eng. Anualized Loss Expectancy). ALE je novčana vrijednost gubitka koji se može očekivati za neki resurs u ovisnosti o riziku u roku od jedne godine. Definira se kao:

$$ALE = SLE * ARO$$

U formuli je SLE (eng. Single loss expectancy) utjecaj pojave u financijskim veličinama, a ARO (eng. anualized rate of occurence) učestalost pojave.

Metoda kombinira veličinu potencijalnog gubitka i vjerojatnost gubitka. Dobiveni iznos gubitka koristi se kao temelj za mjere zaštite troškova koji iz toga proizlaze.

Financijski se gubici otkrivaju za :

- informacije - metodama koje omogućuju kombiniranu procjenu (kvantitativno ili kvalitativno),
- opremu - financijsko izražavanje i
- procese - procjena troška vremenske odgode, prekida i obnove njihova rada kao i financijski gubici koji iz toga proizlaze.

Važno svojstvo ALE metode je da se može koristiti direktno u analizi troškova. Na primjer, ako prijetnja ili rizik imaju vrijednost ALE = 5000$, možda nije potrebno potrošiti 10 000$ godišnje na sigurnosne mjere koje će eliminirati prijetnju. Neka je SLE = 10 000$ i ARO = 0.5, tada je ALE = 5000$, što može predstavljati prihvatljivi novčani gubitak. Na temelju prikupljenih podataka upotrebom na

primjer *Poissonove* distribucije moguće je izračunati vjerojatnost za određeni broj pojave gubitaka godišnje.

Broj gubitaka godišnje	Vjerojatnost	Iznos godišnjeg gubitka
0	0.3679	$0
1	0.3679	$10,000
2	0.1839	$20,000
3	0.0613	$30,000
4	0.0153	$40,000
>4	0.0727	>$50,000

Tablica 2. Proračun rizika metodom ALE

Iz tablice je moguće vidjeti da je vjerojatnost gubitka 20 000$ jednaka 0.1839 ili 18.39%, vjerojatnost gubitka 50 000$ je veća ili približno jednaka 0.0727 ili 7.27%. Pokazatelj gubitaka je pokazatelj rizika pa je to osnova i za potrebne mjere smanjenje rizika. Ovakav je pristupe koristan i zbog toga što procjenitelj neposredno vidi kolika su potrebna ulaganja u zaštitu koja ne smiju biti veća od potencijalnih gubitaka. U ovisnosti o toleranciji rizika u organizaciji i mogućnosti podnošenja većih gubitaka, može se formirati metrika kojom se, na primjer, ulaže 10 000$ godišnje u implementaciju sigurnosnih mjera.

4.4.2. Kvalitativna procjena

Kvalitativna procjena rizika ne koristi apsolutne numeričke vrijednosti parametara već kvalitativno gleda njihov utjecaj na rizik (pri čemu Uprava kompanija odlučuje o tome koji su podaci kritičniji od ostalih te se kao takvi trebaju primjereno zaštititi). Ovakav pristup ne zahtijeva iskustvo, stručnost ili sposobnost osobe koja pristupa procjeni rizika. Procjena se provodi kvalitativno, no za lakše rukovanje podacima oni se ipak kvantificiraju prema provedenim ispitivanjima i mjerenjima. Tako dobivene numeričke vrijednosti nisu apsolutne već relativne. Kako se parametri subjektivno procjenjuju kvalitativni pristup je nepouzdan.

5. Zaključak

Kako je uklanjanje svih rizika kojima je izložen informacijski sustav gotovo nemoguće, organizacije trebaju poduzeti sve zaštitne mjere kako bi smanjile rizik. Na koji način i u kojoj mjeri smanjiti rizik ovisi o upravi organizacije i donosi se na temelju detaljne evaluacije ponuđenih rješenja. Cilj je implementirati ona rješenja koja su financijski prihvatljiva i ona koja će ujedno rezultirati što kvalitetnijim i što pouzdanijim sigurnosnim postupcima i kontrolama s minimalnim utjecajem na poslovanje organizacije. Kako bi se ispunili sigurnosni zahtjevi i postigao kompromis između uloženog novca i ostvarenja odgovarajuće sigurnosne zaštite potrebno je objektivno procijeniti rizik sustava, trenutnu zaštitu sustava te postaviti dijagnostiku. To se može postići postavljanjem hipoteza i podhipoteza te njihovim opovrgavanjem ili potvrđivanjem te anketiranjem zaposlenika organizacije. Nakon provedenih ispitivanja i procjena oblikuju se sigurnosne metrike za ugrožene sustave. Primjenjuju se metode sigurnosnih metrika te se na temelju procjena rizika i vjerojatnosti implementira odgovarajuća sigurnosna zaštita.

6. Reference

[1] Security metrics, Adison Wesley

[2] Upravljanje sigurnosnim rizicima: http://os2.zemris.fer.hr/ISMS/rizik/2006_zorcec/marinjo_diplomski.html#4

[3] A Guide to Security Metrics, Shirley C. Payne, lipanj 2006.

[4] Computer security, NIST, 2003.

[5] Usklađivanje IT-a s poslovnim sustavom, Silvana Tomić Rotim, 2006.

[6] The risk assessment of information system security, Miroslav Baća,

[7] Bilješke s predavanja i auditornih vježbi iz Operacijskih sustava 2, 2006