Sigurnost računalnih sustava

Computer Systems Security

Upravljanje informacijskom sigurnošću

Marin Golub

Sadržaj

- Uvod: osnovni pojmovi, norme, domene i kontrole
- Kontrola pristupa
- Biometrijska identifikacija
- Upravljanje rizicima
- Sigurnosna politika
- Preporučene sigurnosne kontrole
- Uspostava sustava upravljanja sigurnošću informacija
- Primjer sigurnosnih normi iz skupa normi PKCS

Osnovni pojmovi I

Spam - neželjena pošta

Malware - zlonamjerni programi

Spyware - špijunski programi

Programi koji potajno skupljaju različite podatke o korisniku i njegovim navikama te ih bez njegovog znanja šalju na unaprijed određenu adresu.

- Adware (*Advertising Supported Software*) - neželjene reklame
- Browser hijackers - nametnute početne Web stranice
- Dialers - preusmjerivači telefonskih poziva
- Monitoring cookies - *kolačići* koji se sami instaliraju prilikom pretraživanja weba, snimaju aktivnosti na računalu i šalju ih napadaču
- Key loggers - zlonamjerni programi koji snimaju tipkanje
  - Scumware - mijenjaju izgled i funkcionalnost web stranica

IPS (*Intrusion Prevention System*) - sustav za sprječavanje napada

IDS (*Intrusion Detection System*) - sustav za otkrivanje napada

Osnovni pojmovi II

Exploit - metoda ili program koji zloupotrebljava pogreške, propuste, odnosno ranjivosti računalnog sustava

Rootkit - zlonamjerni program koji se skriva (izbjegava detekciju) tako da nadomješćuje sustavske procese i podatke, odnosno datoteke operacijskog sustava

Pentesting - ispitivanje ranjivosti

Honeypot – mamac, tj. sredstvo koje služi da ga se skenira, napada ili kompromitira

Vulnerability – ranjivost, tj. nedostatak ili slabost u dizajnu sustava, implementaciji, ili operativnoj uporabi i upravljanju koji može biti iskorišten kako bi se prekršila sigurnosna politika sustava [11]

Phishing - pokušaj prikupljanja osobnih podataka s ciljem krađe identiteta koja nastaje kada netko koristi tuđe osobne podatke bez dozvole kako bi počinio prijevaru ili neki drugi zločin

Računalni sustav je siguran kada

1. se na sustavu mogu obavljati samo autorizirane radnje
2. ga koriste samo autorizirani korisnici i to samo u predviđene svrhe
3. je raspoloživ autoriziranim korisnicima

Ranjivost

- pogreška ili slabost u dizajnu/implementaciji/uporabi/upravljanju sustava koja se može iskoristiti za narušavanje sigurnosti

Prijetnja

- je bilo kakva mogućnost da dođe do povrede sigurnosne politike
- je napadač koji je motiviran i sposoban iskoristiti ranjivost

Napad

- je djelovanje s namjerom da se zaobiđe sustav zaštite, tj. da se iskoriste ranjivosti sustava kako bi se sustav iskoristio u nedopuštene svrhe
- Napadač mora imati
  - motiv i
  - priliku te znati
  - slabosti sustava.

Primjer napada: *Phishing*

šalje:**"FER - Sveučilište u Zagrebu"** <ecotou@hcmr.gr>

Pažnja:

Pokušaj je napravljen da se prijavite s novog computer. For sigurnosti vaš račun, spremna smo otvoriti upit. Ljubazno kliknite na link, http://bit.ly/2nlwWmW, za dobre sigurnosne prakse na svoj račun.

Hvala ti

FER - Sveučilište u Zagrebu

Phishing ili krađa identiteta

- nastaje kada netko koristi tuđe osobne podatke bez dozvole kako bi počinio prijevaru ili neki drugi zločin

Zakon o telekomunikacijama

Članak 111. stavak 4

Nije dopušteno, u svrhu izravne promidžbe, slanje elektroničke pošte u kojoj se pogrješno prikazuje ili prikriva identitet pošiljatelja u čije ime se šalje priopćenje, ili bez ispravne elektroničke adrese na koju primatelj može, bez naknade, poslati zahtjev za onemogućavanje takvih priopćenja.

Članak 116. (Teže povrede odredaba ovoga Zakona)

Novčanom kaznom od 5.000,00 do 1.000.000,00 kuna kaznit će se za prekršaj pravna osoba:

...

40. ako upotrebljava pozivne sustave s i bez ljudskog posredovanja, telefaks uređaje ili elektroničku poštu u svrhu izravne promidžbe protivno odredbama iz članka 111. ovoga Zakona.

Primjer narušavanja tajnosti i privatnosti

Istraživači s MITa su kupili 158 rabljenih tvrdih diskova (2007):

- Bez detaljne forenzičke analize na njima su pronašli:
  - važne korporacijske dokumente
  - povjerljive medicinske podatke
    - dokument u kojem se otac sedmogodišnjeg djeteta žali na liječnički tretman (dijete boluje od raka)
    - povjerljive dokumete California children's hospital
  - ljubavna pisma
  - pornografiju
  - 3800 brojeva kreditnih kartica
  - oko 10 000 e-mailova

Drugi primjer narušavanja tajnosti i privatnosti

Tvrtka (koja je davala uslugu arhiviranja podataka) je prodala poslužitelj (eBay) na kojem su bili povjerljivi osobni podaci više od milijun korisnika te banke:

- brojevi računa,
- lozinke,
- telefonski brojevi, itd.

Pošteni kupac je alarmirao *Britain's Information Commissioner's Office*.

[News Briefs, Security & Privacy, vol.6, num.5, 2008]

Primjer: Kako ljudski mozak percipira sigurnost

Što će ljudi izabrati ako im se dade na izbor:

- dobitak od 5000 kn ili
- bacanje novčića i mogućnost dobitka od 10 000 kn ili ništa?

- 5000 kn kazne ili
- bacanje novčića i mogućnost kazne od 10 000 kn ili ništa?

Ljudi različito reagiraju na primjerice sljedeće vijesti
(obje vijesti nose istu informaciju):

- "200 od 600 ljudi je spašeno.";
- "400 od 600 ljudi je poginulo." ?

Sigurnosne prijetnje

- samo 3% prijetnji dolazi izvan promatranog sustava
- 97% prijetnji dolazi unutar sustava

Istraživanje "dajte mi svoju lozinku", izvor RSA, 2007.:

- 70% za čokoladicu (London)
- 34% ni za što (London)
- 67% za kavu u Starbucksu (Italija)

Istraživanje na Sveučilištu u Zagrebu: "CIP traži mailom lozinku", izvor CARNet, 2010.

- 22% djelatnika jednog fakulteta je ispunilo obrazac

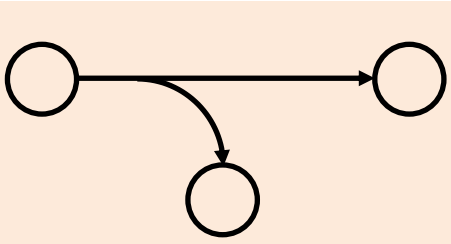
Definicije informacijske i kibernetičke sigurnosti

- Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i normi informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda [Zakon o informacijskoj sigurnosti, 2007].
  - usmjerena je na zaštitu informacija
- Kibernetička sigurnost obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru kojeg čine Internet i svi sustavi povezani na njega [Strategija kibernetičke sigurnosti, 2015].
  - usmjerena je na zaštitu kibernetičkog prostora kao i zaštiti ljudi u kibernetičkom prostoru i bilo koje imovine koja se može dosegnuti putem kibernetičkog prostora
  - kibernetički prostor
    - okruženje u kojem uz pomoć tehnoloških uređaja i mreže je omogućena inetrakcija ljudi, programa i usluga
    - ne postoji u fizičkom obliku

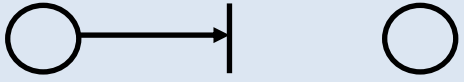
Zakonski i podzakonski akti o informacijskoj sigurnosti

- Zakon o informacijskoj sigurnosti, NN 79/07, 2007.
- Zakon o tajnosti podataka, NN 79/07, 86/12, 2007.
- Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/18, 2018.
- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/18, 2018.

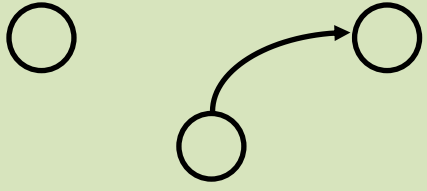
Prijetnje i napadi



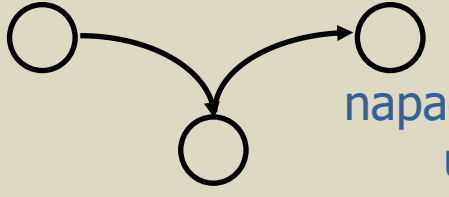
1. prisluškivanje
2. prekidanje



3. lažno predstavljanje



4. ponovno odašiljanje snimljenih starih paketa
5. modifikacija paketa



napad čovjek u sredini

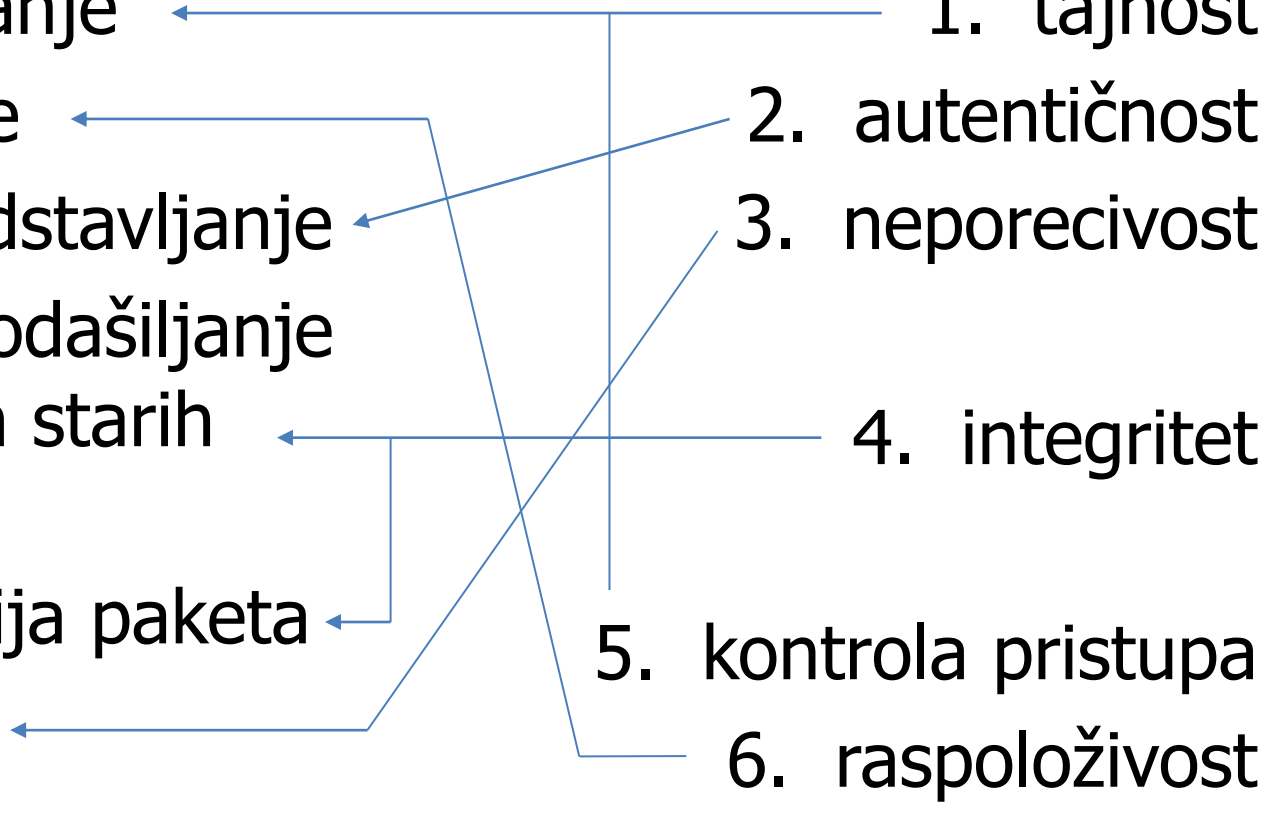
6. poricanje

Prijetnje i napadi

1. prisluškivanje
2. prekidanje
3. lažno predstavljanje
4. ponovno odašiljanje snimljenih starih paketa
5. modifikacija paketa
6. poricanje

Sigurnosni zahtjevi

1. tajnost
2. autentičnost
3. neporecivost
4. integritet
5. kontrola pristupa
6. raspoloživost



Sigurnosni zahtjevi

Osnovni sigurnosni zahtjevi

1. tajnost
2. autentičnost
3. neporecivost
4. integritet

Dodatni sigurnosni zahtjevi

5. kontrola pristupa
6. raspoloživost

Sigurnosne prijetnje i zahtjevi

1. prisluškivanje
2. prekidanje
3. lažno predstavljanje
4. ponovno odašiljanje snimljenih starih paketa
5. modifikacija paketa
6. poricanje

1. tajnost
2. autentičnost
3. neporecivost
4. integritet
5. kontrola pristupa
6. dostupnost

1.+2. = povjerljivost

1.+2.+3.+4. = osnovni sigurnosni zahtjevi

CIA = 1.+2.+5. + 4.+6. = povjerljivost, integritet i dostupnost
(engl. *Confidentiality, Integrity and Availability*)

Sigurnosni zahtjevi

povjerljivost

štiti informacije od neautoriziranog pristupa

1. tajnost
2. autentičnost

Osnovni sigurnosni zahtjevi

3. neporecivost
4. integritet

Dodatni sigurnosni zahtjevi

5. kontrola pristupa
6. raspoloživost

Sigurnosni zahtjevi

povjerljivost
Confidentiality

1. tajnost
2. autentičnost

Integrity

4. integritet

Availability

5. kontrola pristupa
6. raspoloživost

Sustav je siguran kada se njegovi resursi koriste i pristupa im se na za to predviđen način u svim okolnostima.

- nedostižno

Primjeri napada na sigurnost sustava

- neautorizirano čitanje podataka – narušena povjerljivost
- neautorizirana modifikacija podataka – narušen integritet
- neautorizirano brisanje podataka – narušena raspoloživost
- napad uskračivanjem usluge – narušena raspoloživost
- krađa usluge – narušeni povjerljivost i integritet

Povjerljivost

- sigurnosni zahtjev koji štiti informacije od neautoriziranog pristupa
  - tj. samo autorizirani korisnici smiju pristupiti osjetljivim podacima
- Što znači „1.+2. = povjerljivost”?
- ostvaruje se kombinacijom autentičnosti i tajnosti ali i provjerom prava pristupa
- povjerljivost ≠ tajnost
  - mada se ta dva pojma često poistovjećuju
  - povjerljivost se može ostvariti uz pomoć tajnosti
- može se ostvariti i bez tajnosti
  - samo uz pomoć autentičnosti i provjere prava pristupa

Neporecivost

- ostvaruje se uz pomoć asimetrične kriptografije i to kriptiranjem privatnim ključem
  - time se ostvaruje i autentičnost
- autentičnost se može ostvariti i bez asimetrične kriptografije
  - MAC
  - autentifikacijsko kriptiranje
  - međutim, time NIJE ostvarena neporecivost

Taksonomija prema Bishopu kaže da se sigurnost sastoji od tri komponente:

- sigurnosni zahtjevi koji definiraju sigurnosne ciljeve
  - Što se očekuje od sigurnosti?
- sigurnosne politike
  - Što treba poduzeti kako bi se ostvarili zadani sigurnosni ciljevi?
- sigurnosni mehanizmi koje nameće sigurnosna politika
  - Koje alate, procedure i ostale sigurnosne mehanizme treba pritom primijeniti?

[M.Bishop, "What Is Computer Security?", IEEE Security&Privacy, 2003.]

Upravljanje informacijskom sigurnošću

- Konzorcij pod nazivom (ISC)^2 (*International Information Systems Security Certification Consortium*) provodi ispitivanje i certifikaciju stručnjaka koji se bave računalnom sigurnošću.
- Kandidati koji polože ispit postaju certificirani stručnjaci iz područja sigurnosti informacijskih sustava (CISSP - *Certified Information System Security Professional*).
- Ispitivanje se provodi u okviru desetak domena [6].

Deset domena

1. Kontrola pristupa (*Access control*)
2. Mrežna sigurnost (*Network and Internet Security*)
3. Upravljanje rizikom (*Risk Management*)
4. Sigurnost primjenskih programa (*Application Program Security*)
5. Kriptografija
6. Sigurnosna arhitektura (*Security Arhitecture*)
7. Sigurnost računalnih operacija (*Computer Operations Security*)
8. Planiranje postupaka u slučaju incidenta
9. Pravni aspekti
10. Fizička sigurnost (*Phisical Security*)

Zaštitne mjere

- tehničke,
- administrativne i
- fizičke

Djelotvorna implementacija i nadzor svih potrebnih mjera zaštite i sigurnosnih kontrola zahtjeva dobro osmišljen sustav upravljanja sigurnošću.

1. Kontrola pristupa

- Identifikacija, autentifikacija i autorizacija.
- Smije li autentificirana osoba ili proces koristiti određeno sredstvo i ako smije, što može sa sredstvom raditi?
- Samo djelomična zaštita od *najvećih i najljućih* protivnika računalnih sustava: ovlaštenih korisnika. ☺
- Ponovimo: sustav upravljanja računalnom sigurnošću treba osigurati sljedeće sigurnosne zahtjeve (CIA):
  - povjerljivost,
  - integritet i
  - raspoloživost informacija.

Neki primjeri prijetnji

- *hakeri / crackeri*
- zamaskirani korisnici (*masqueraders*) - korisnici koji su dobili lozinku od nekog drugog korisnika (ili koriste tzv. dijeljene lozinke).
- autorizirani korisnici koji pristupaju podacima koji nisu njima namijenjeni zbog slabe kontrole pristupa (*unauthorized user activity*)
- nezaštićene kopije datoteka (*unprotected downloaded backup files*)
- lokalne mreže - podaci koji putuju lokalnom mrežom su vidljivi svim korisnicima lokalne mreže
- trojanski konji

Kako zadovoljiti sigurnosne zahtjeve?

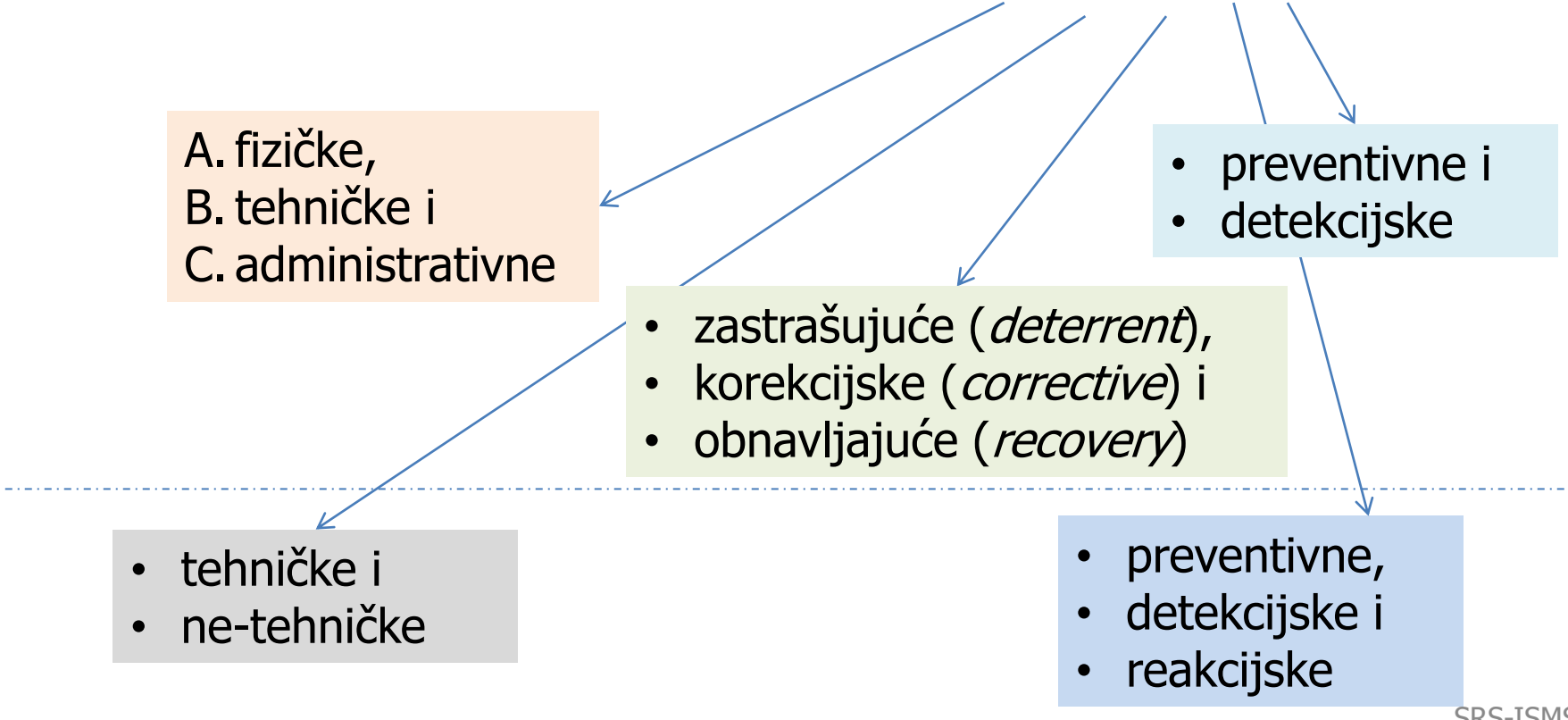
- Povjerljivost: modeli za uspostavu povjerljivosti
  - dozvole (najpoznatiji model *Bell-LaPadula*) ili
  - pravila (*MS rules*)
- Integritet: modeli za uspostavu integriteta
  - npr. *Biba*, *Clark-Wilson*
- Raspoloživost: zaštita od prijetnji koji je narušavaju, kao primjerice
  - DoS (*Denial of Service*) napada
  - prirodnih nepogoda (poplava, požar, grom, potres)
  - ljudskih *nepodopština* (rat, terorizam)

Zaključne napomene o sigurnosnim zahtjevima

- Nisu uvijek svi sigurnosni zahtjevi podjednako zastupljeni:
  - Kontrola leta – nema potrebe za osiguranjem tajnosti (povjerljivosti podataka), već moraju biti zadovoljeni integritet i raspoloživost podataka.
  - Automobilska industrija – najvažnije je sačuvati podatke tajnim (kako bi se prikrili novi modeli vozila), dok raspoloživost i integritet nisu toliko važni.
  - Vojska – sva tri zahtjeva moraju biti ispunjena.
- Povijesno se najviše pažnje posvećivalo povjerljivosti (vojska, špijuni).
- U novije vrijeme puno se pažnje posvećuje integritetu i raspoloživosti
  - modeli i sustavi za zaštitu integriteta
  - uređaji i sustavi za osiguravanje raspoloživosti (*UPS, hot swap, disaster recovery, error detection and correction, high-availability (HA) clusters ...*)

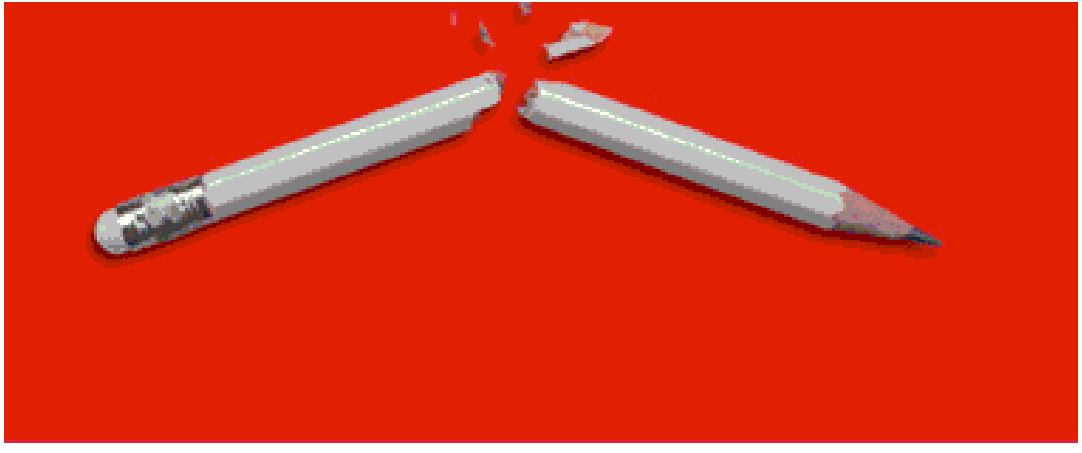
Kako ostvariti sigurnost računalnih sustava?

Odgovor: primjenom sigurnosnih kontrola.



- Preventivnim kontrolama nastoji se izbjeći neželjene događaje.
- Detekcijskim kontrolama nastoji se identificirati neželjene događaje nakon što su se već dogodili. Primjerice:
  - provjera tragova (*audit trails*),
  - detekcija upada u sustav *(intrusion detection methods*)
  - provjera sume (*checksums*)
- Zastrašivanje (*deterrent control*) – obeshrabruje korisnika od pokušaja namjernog kršenja sigurnosnih politika i procedura
  - primjerice prijetnje raznim kaznama: npr. prijetnja sramoćenjem imena - ime na oglasnoj ploči
- Korektivna kontrola (*corrective control*)
  - primjerice nakon ekscesa se može ustanoviti da su prava pristupa u danim okolnostima bila pogrešno podešena pa ih treba ispraviti.
- Obnavljanje (*recovery control*) – ponovno uspostavljanje (obnavljanje) izgubljenih računalnih resursa te pomoć organizaciji da nadoknadi izgubljena materijalna dobra.

Primjer zastrašivanja



Matični broj korisnika:

PIN korisnika:

Potvrda

Uputa za prijavu u aplikaciju:

1. U polje označeno s Matični broj korisnika utipkajte svoj matični broj.
2. U polje označeno s PIN korisnika utipkajte svoj PIN.
3. Potvrdite unos klikom na tipku Potvrda.

Usluga je namijenjena samo registriranim korisnicima. Pokušaj neovlaštenog pristupa je kazneno djelo.

1.A. Fizičke kontrole

- brave, zaštitari, znakovi, oznake, alarmi ...
- štite se računala i računalna oprema te sadržaj pohranjen u njima od
  - špijunaže
  - krađe
  - uništavanja
  - slučajnih oštećenja koja se mogu dogoditi zbog požara ili prirodnih katastrofa (poplava, potres)

1.A.i. Preventivne fizičke kontrole

Cilj preventivnih fizičkih kontrola je onemogućiti neovlaštenim osobama pristup računalnoj opremi te pomoć u zaštiti od prirodnih nepogoda.

- Sigurnosne kopije podataka i dokumentacije
  - moraju biti pohranjeni na nekom drugom mjestu kako isti nepoželjni događaj ne bi uništio i sigurnosne kopije
- Ograde
- Zaštitari
- Oznake i značke (bedževi)
- Dvostruka vrata
- Brave i ključevi
- Dodatna napajanja (UPS, dizelski/benzinski agregati)
- Biometrijska kontrola pristupa (zasebno potpoglavlje)
  - ostvarivo u okruženjima gdje su veliki zahtjevi na sigurnost, ali manji promet

1.A.ii. Detekcijske fizičke kontrole

Cilj je upozoriti zaštitnu službu da je narušena fizička sigurnost.

- Detektori pokreta
- Detektori požara i dima
- Nadgledanje prostora uz pomoć kamera
- Senzori
- Alarmi

1.B. Tehničke kontrole

- uključuju korištenje sigurnosnih mehanizama ugrađenih u sklopovlje, komunikacijske protokole i programe

1.B.i. Preventivne tehničke kontrole

Cilj preventivnih tehničkih kontrola je onemogućiti neovlaštenim osobama i procesima udaljeni pristup računalima.

- Programska rješenja
  - operacijski sustavi, sigurnosne zaštitne stijene, …
- Antivirusni alati
- kontrola i zapisivanje svih promjena u sustavu
- Lozinke
  - promjena lozinki nakon određenog vremena
  - dinamičke lozinke uz pomoć tablica ili tokena
  - koristiti velika i mala slova, brojeve, specijalne znakove...
  - za primjer vidjeti implementacijske smjernice kontrole "Uporaba lozinki" prema normi ISO/IEC 27002 unutar domene "Kontrola pristupa"
- Pametne kartice
- Kriptiranje
- Sustav za preventivnu zaštitu od napada (*IPS - Intrusion Prevention System*)

1.B.ii. Detekcijske tehničke kontrole

Cilj je upozoriti zaštitnu službu da je narušena ili da je bilo pokušaja narušavanja tehničke sigurnosti.

- Provjera tragova, tj. zapisa u dnevnicima (*audit trails*)
  - omogućuje rekonstrukciju događaja i ispitivanje pojedinih događaja (transakcija)
- Sustav za otkrivanje napada (*IDS - Intrusion Detection System*)
  - otkrivanje "neobičnih" akcija na računalu

1.C. Administrativne kontrole

- bave se osobljem kako bi se osigurala povjerljivost, integritet i raspoloživost podataka i aplikacija

- ograničenja u upravljanju (*management constraints*),
- operacijske procedure (*operational procedures*),
- procedure kojima se određuju odgovornosti (*accountability procedures*)
- procedure kojima se provjeravaju potrebne dozvole osobama koje imaju pristup računalnim resursima

1.C.i. Preventivne administrativne kontrole

- Razvoj svijesti o potrebi za računalnom sigurnošću i izobrazba
- Podjela zaduženja (*separation of duties*)
- Sigurnosne politike i protokoli (*security policies and procedures*).
- Pravilni odabir kadrova i otpuštanje
  - prilikom zapošljavanja treba voditi računa
    - jesu li potencijalni zaposlenici bili skloni kršenju zakona i imaju li kriminalni dosje
    - tražiti reference i doznati gdje su kandidati dosada radili
    - kakav im je karakter i kako podmiruju svoje financijske obveze (krediti)
  - prilikom otpuštanja radnika ili prijelaska na drugi posao treba voditi računa o
    - oduzimanju sigurnosnih povlastica
    - revidiranju svih ovlasti ako je zaposlenik imao mogućnost autoriziranja drugih djelatnika
    - treba promijeniti sve zaporke koje je znao bivši zaposlenik
- Nadziranje (*supervision*)
  - Novozaposlene treba nadzirati kako bi se na vrijeme otkrilo sumnjivo/neprikladno ponašanje.
- Oporavak od katastrofe, nepredviđenih situacija i planovi u izvanrednim slučajevima
- Registracija korisnika

1.C.ii. Detekcijske administrativne kontrole

- služe za ispitivanje provode li se sigurnosne politike i procedure, za detekciju prijevara i za izbjegavanje izlaganja zaposlenika nepotrebnim rizicima

- Pregled i provjera sigurnosti (*security reviews and audits*)
  - Koji dijelovi sigurnosne politike i procedura se ne provode kako treba?
- Vrednovanje djelotvornosti ugrađenih sigurnosnih kontrola (*performance evaluations*)
- Dani odmora (dopust) (*required vacations*)
  - zaposlenici koji duže vremena nisu bili na odmoru skloniji su propustima i greškama pa ih je potrebno poslati na odmor
  - tijekom odmora su moguće prevare
- Istraga (*background investigations*)
  - Prilikom prelaska na osjetljivija radna mjesta potrebno je provesti istragu o proteklim aktivnostima kandidata.
- Rotacija zaduženja (*rotation of duties*)
  - Nasumično razmještanje zaposlenika pomaže detekciji prevara.

Biometrijska identifikacija
Obilježja biometrijskih sustava 1/2

- Točnost (sustav nema smisla ako ovo svojstvo nije ispunjeno)
- Vjerojatnost lažnog odbacivanja (*FRR - False Reject Rate ili Type I error*)
- Vjerojatnost lažnog prihvaćanja (*FAR - False Accept Rate ili Type II error*)
  - najvažnije svojstvo i trebalo bi biti jednaka nuli
- Stanje jednake vjerojatnosti greške (*CER - Crossover Error Rate ili Equal Error Rate*)
  - Stanje u kojem su vjerojatnosti lažnog odbacivanja i prihvaćanja jednake.
  - Podesimo li sustav tako da on bude osjetljiviji, vjerojatnost lažnog prihvaćanja će pasti, ali će zato vjerojatnost lažnog odbacivanja porasti. I obrnuto.
- Brzina i propusnost (*Speed and Throughput Rate*)
- Pouzdanost (*Reliability*).
- Jedinstvenost
  - Samo nekoliko načina biometrijske identifikacije osiguravaju jedinstvenost identifikacije: npr. otisak prsta, šarenica oka i DNK.

Biometrijska identifikacija
Obilježja biometrijskih sustava 2/2

- Otpornost na krivotvorenje (*Resistance to Counterfeiting*)
  - mogućnost detekcije lažnih pokušaja identifikacije (plastikom, gumom, i sl.)
- Postojanost – nije poželjno da se svojstvo mijenja (lice)
- Svojstva spremnika za pohranu podataka (*Data Storage Requirements*).
- Trajanje upisa u sustav (*Enrollment Time*)
- Nametljivost prikupljanja podataka (*Intrusiveness of Data Collection*)
  - Je li štetno skeniranje šarenice crvenom svjetlošću?
- Prihvatljivost korisnicima (*Acceptability to Users*)
- Potreba za dodirivanjem (*Subject and System Contact Requirements*)
  - Mnogi ljudi dodiruju istu opremu…je li to prihvatljivo korisnicima?

Pregled biometrijskih metoda

Svojstvo	jedinstvenost (*universality*)	postojanost (*permanence*)	prikupljivost (*collectibility*)	prihvatljivost (*acceptability*)	izbjegavanje (*circumvention*)	jeftino
	(*accurate*)		(*easy to use*)		(*secure*)	(*cheap*)
Otisak prsta (fingerprint)	H	H	M	M	M (H)	H
DNK	H	H	L	L	L	L
Šarenica (iris)	H	H	M	L	L (H)	
Mrežnica (*retina*)	H	M	L	L (M)	L	
Uho (*ear*)	M	H	M	H	M	
Lice (*face*)	M	**M**	H	H	**M**	**M**
Thermogram	H	**L**	H	H	**H**	
Ruka (*hand geometry*)	M	M	H	M	M	
Keystroke dynamics	L	L	M	M	M	H
Miris (*smell*)	H	H	L	M	L	
Potpis (*signature*)	L	L	H	H	H (L)	H
Glas (*voice*)	M	L	M	H	**L**	
Vene (*vein*)	H		H		H	H
EEG						

Implementacija kontrole pristupa

- Podjela prema zaduženjima (*separation of duties*)
  - Ako su potrebna najmanje dva koraka pri izvršavanju kritične operacije, tada najmanje dvije osobe trebaju obaviti te korake. (Npr. programer ne treba biti taj koji i instalira program.)
- Podjela prema privilegijama (*least privilege*)
  - korisnik/program/proces ima minimalne privilegije, a koje su dovoljne za obavljanje njegovog posla

Kategorizacija resursa

4 stupnja tajnosti i 5 stupnjeva sigurnosti

- vrlo tajno, VT (strogo povjerljivo) (*top secret*)
- tajno, T (*secret*)
- povjerljivo, POV (*confidential*)
- ograničeno, OGR
- neklasificirano (*unclassified*) ili javno

Modeli za uspostavu povjerljivosti

- *Lattice*
  - temelji se na vojnoj podjeli dokumenata na: vrlo tajni (strogo povjerljivi), tajni, povjerljivi, ograničeni i neklasificirani.
- *Bell-LaPadula* (autori David Bell i Len LaPadula, 1973)
  - temelji se također na vojnom sustavu i imao je utjecaj na ostale modele.
- Objekti su klasificirani prema sigurnosnom nivou (strogo povjerljivi, tajni, povjerljivi, ograničeni i neklasificirani).
- Subjekti imaju sigurnosna dopuštenja (*clearance*).
- Cilj je spriječiti subjektima pristup onim objektima koji su višeg sigurnosnog nivoa od onog koji im je dopušten.

Bell-LaPadula model povjerljivosti

vrlo tajno	Marko, Mirko	tajni dokumenti
tajno	Ana, Vlado	e-mail
povjerljivo	Domagoj	dnevnik
neklasificirano	ostali	telefonski imenik

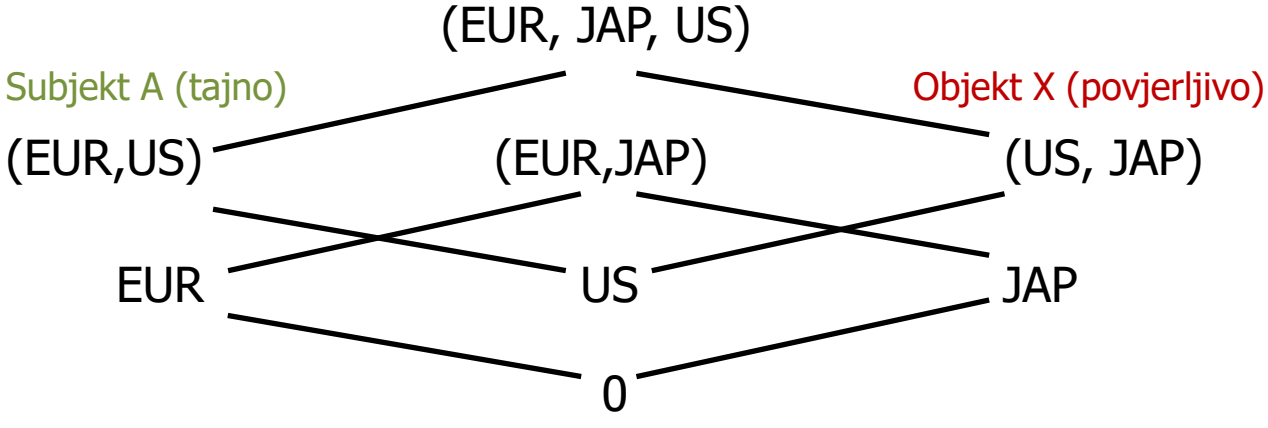
- *Lattice* model nije otporan na napad trojanskim konjem koji kopira fajlove određene razine u fajlove niže razine i na taj način fajlovi postaju dostupni osobama nižeg ranga.
- *Bell-LaPadula* model je riješio taj problem onemogućivši pisanje fajlova niže razine od one koja je dodijeljena određenoj osobi.
- Opisan je frazom: "*no read up, no write down*".
  - *no read up* : "secret researchers can view public or secret files, but may not view top-secret files"
  - *no write down* : "secret researchers can create secret or top-secret files but may not create public files"

- dokumenti (objekti) mogu biti dodatno klasificirani po kategorijama
  - dokument može spadati u više kategorija.

Primjer: 3 kategorije EUR, US, JAP čine rešetku (*lattice*):

{0, EUR, US, JAP, (EUR,US), (EUR,JAP), (US,JAP), (EUR,JAP,US)}

Primjer rešetke s dva nivoa za tri kategorije:



- Neka subjekt A ima dopuštenje za sigurnosni nivo {tajno, (EUR,US)}, a objekt X je klasificiran kao {povjerljiv, (US, JAP)}.
- Subjekt A ne može pristupiti, primjerice, {*, EUR}, niti {vrlo tajno, (EUR,US)}, ali može {tajno, (US)}, jer je na istom sigurnosnom nivou.
- Može li subjekt A pristupiti objektu X?

Modeli za uspostavu integriteta

- *Biba* model
  - usmjeren prema integritetu podataka i sadrži više nivoa integriteta za objekte i subjekte
  - radi po principu "*no write up, no read down*"
  - korisnici mogu stvarati (pisati) sadržaj na svojem i nižim sigurnosnim nivoima, a čitati sadržaj sa svojeg nivoa ili višeg:
    - "a monk may write a prayer book that can be read by commoners, but not one to be read by a high priest"
    - "a monk may read a book written by the high priest, but may not read a pamphlet written by a lowly commoner"
- *Take - Grant* model
  - specificira koja prava može neki subjekt drugom subjektu dati, odnosno oduzeti.
- *Clark - Wilson* model
  - zasniva se na integritetu transakcija: iz konzistentnog u konzistentno stanje

2. Mrežna sigurnost (*Network Security)*

- zaštita od zlonamjernih programa (*antivirus*, ...)
- sigurnosna stijena (*firewall*)
- sustavi za otkrivanje i zaštitu od napada (*IPS*, *IDS*)
- kriptografski programi (*PGP*, *kriptiranje sadržaja diska*, ...)
- sigurna administracija poslužitelja
- razvoj programa bez sigurnosnih propusta
- ispitivanje postojanja sigurnosnih propusta (*pentesting*)
- ... veliko područje (zaseban predmet)

Značajniji mrežni alati za otkrivanje ranjivosti računalnog sustava

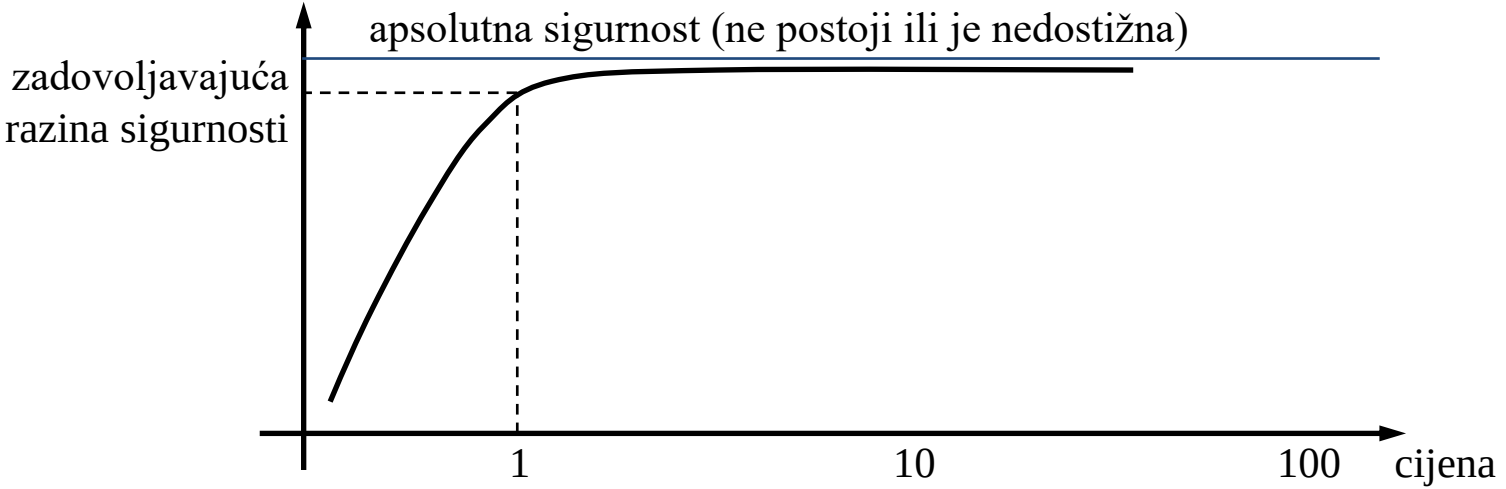
- nmap - alat za pregledavanje otvorenih pristupa (*portova*)
- Wireshark – alat za analizu mrežnog prometa i za razvoj mrežnih protokola
- metasploit – alat za ispitivanje ranjivosti
- John the Ripper – alat za otkrivanje slabih zaporki
- p0f - alat za pasivno prisluškivanje upita (iz kojih se primjerice određuje vrsta OSa na računalu koje šalje upit)
- nessus - komercijalni alat (od verzije 3) za ispitivanje ranjivosti sustava, koristi skriptni jezik NASL
- OpenVAS - nastavak razvoja nessusa od verzije 2 otvorenog koda (reakcija na komercijalizaciju nessusa)
- SNORT - sustav za otkrivanje napada (IDS) otvorenog koda

Baze ranjivosti

- *NVD (National Vulnerability Database)*
  http://nvd.nist.gov/
- *SecurityFocus*
  http://www.securityfocus.com/vulnerabilities
- *IBM X-Force Exchange*
  https://exchange.xforce.ibmcloud.com/
- *OSVDB (The Open Source Vulnerability Database)* je ugašena 2016. g.

3. Upravljanje rizikom
(*Risk Management*)

- Rizik je očekivani gubitak izražen kao vjerojatnost da će odredena prijetnja iskoristiti određenu ranjivost i pritom načiniti određenu štetu [11].
- Upravljanje rizikom je proces kojim se opravdavaju sigurnosna rješenja.
- Isplati li se ulagati u (skupu) računalnu sigurnost? Koliko?



Upravljanje sigurnosnim rizicima

Rizik se može

- smanjiti
  - implementacijom odgovarajućih sigurnosnih kontrola koje umanjuju rizik
- prenijeti
  - osigurati se i troškove ostvarenih prijetnji prenijeti na osiguravajuće društvo
- prihvatiti
  - kada su troškovi implementacije odgovarajuće kontrole veći od vrijednosti resursa
- odbaciti ili negirati ili izbjegavati
  - svjesno ignorirati rizik u nadi da se napad neće dogoditi - neprihvatljivo rješenje

Proces upravljanja rizikom

- ciklički proces koji se sastoji od tri faze:

A. Procjena rizika
   - identifikacija rizika
   - identifikacija mjera za smanjenje rizika
   - Kakve će posljedice na budžet imati
     - smanjenje,
     - prihvaćanje,
     - izbjegavanje ili
     - prenošenje rizika?

B. Provođenje mjera za smanjenje rizika

C. Ispitivanje i analiza rezultata

Ključna pitanja u procesu upravljanja rizikom

A. Procjena rizika

- Što se može dogoditi? Koja se prijetnja može ostvariti? (*threat event*)
- Ako se dogodi, koja će biti šteta? (*threat impact*)
- Kako se često može dogoditi? (*threat frequency, annualized*)
- Koliko su pouzdani odgovori na prethodna tri pitanja? (*recognition of uncertainty*)

B. Provođenje mjera za smanjenje rizika

- Što se može učiniti? Koji rizik mogu umanjiti? (*risk mitigation*)
- Koliko će to koštati? (*annualized*)
- Je li isplativo? (*cost/benefit analysis*)

3.A. Procjena rizika (*Risk Assessment*)

- identifikacija rizika
  - Identificirati vrijednosti imovine, odnosno sredstava (*Identifying the assets*)
  - Identificirati prijetnje (*Identifying the threats*)
- identifikacija mjera za smanjenje rizika

- Kvantitativna
  - opisuje se numerički, financijski pristup
- Kvalitativna
  - opis i subjektivna procjena
  - preferiraju ga norme (ISO/IEC 27001, 27002 i 27005) i praksa
- Kombinacija obje metode daje najbolje rezultate

Općenito, matematički, rizik *R* je određen funkcijom:

$$R = f(AV, V, T, P, I)$$

- *AV* = procjenjena vrijednost (*asset value*)
- *V* = ranjivost (*vulnerability*)
- *T* = prijetnja (*threat*)
- *P* = vjerojatnost događaja (*probability*)
- *I* = posljedice (*impact*)

Rezultati procjene su valjani ukoliko proces procjene zadovoljava sljedeće kriterije:

- jednoznačnost
- objektivnost
- pouzdanost
- ukoliko se ponovi procjena, mora dati iste rezultate

Kvantitativni pristup

$$R = AV \times EF_{I,V,T} \times P_{V,T}$$

- AV = procjenjena vrijednost resursa
- ranjivost (V), prijetnja (T) i posljedice (I) promatraju se kao **faktor izloženosti** $EF_{I,V,T}$ (engl. *Exposure Factor*)
- P = vjerojatnost ostvarenja prijetnje

Primjer: resurs vrijedi 20 000 KN, faktor izloženosti je 15% i vjerojatnost ostvarenja prijetnje neka je 0.02 u godini dana, tada rizik iznosi:

R = 20 000 KN x 0.15 x 0.02 / god = 60 KN/god

Nedosatci kvantitativnog pristupa

- AV se određuje iz knjigovodstvenih vrijednosti koje uopće ne moraju odražavati pravo stanje (primjer s bazom podataka na starom poslužitelju koji nema knjigovodstvene vrijednosti),
- EF je gotovo nemoguće odrediti niti približno
- P se određuje iz statistika koje također ne moraju odražavati stvarno stanje

$\Rightarrow$ Rezultat R je nepouzdan pa kvantitativni pristup nije prikladan.

Kvalitativni pristup

- Subjektivni pristup koji se oslanja na iskustvo, stručnost i sposobnost osoba koje obavljaju procjenu rizika.
- Parametri se kvantificiraju, a rezultat nije apsolutan, već relativan.

- Nedostaci:
  - subjektivan pristup je nepouzdan
  - kvantifikacija
  - reinterpretacija dobivenih vrijednosti

Prvi primjer metode za kvalitativnu procjenu rizika

Matrica predefiniranih vrijednosti

$$R = f(AV_I, V_{I,P}, T_{I,V,P})$$

AV = procjenjena vrijednosti
V = ranjivost
T = prijetnja
P = vjerojatnost događaja
I = posljedice

Jedna od varijacija: $R = AV + V + T$

$AV \in [0\text{-mala}, 4\text{-velika}]$ $V,T \in [0\text{-niska}, 2\text{-visoka razina}]$

$R \in [0\text{-najmanji rizik}, 8\text{-najveći rizik}]$

- svi parametri i rezultat poprimaju cjelobrojne vrijednosti

Nedostaci:

- vjerojatnost ostvarenja prijetnje se nigdje eksplicitno ne koristi, koristi se samo implicitno pri procjeni veličina parametara
- *V* i *T* je u praksi teško promatrati odvojeno.

Drugi primjer Metode za kvalitativnu procjenu rizika

Rangiranje prijetnji prema procjeni rizika

$$R = f(I_{AV,T}, P_{V,T})$$

AV = procjenjena vrijednosti
V = ranjivost
T = prijetnja
P = vjerojatnost događaja
I = posljedice

Jedna od varijacija: $R = I \times P$

$I, P \in$ [1-mala, 5-vrlo velika]

$R \in$ [1-najmanji rizik, 25-najveći rizik]

- svi parametri i rezultat poprimaju cjelobrojne vrijednosti

Nedostatak:

- *R* se procjenjuje na temelju samo dva parametra koji su implicitno funkcije više varijabli

Treći primjer Metode za kvalitativnu procjenu rizika

Procjena vjerojatnosti ostvarenja i mogućih posljedica

$$R = f(AV_{I,T}, P_{V,T})$$

AV = procjenjena vrijednosti
V = ranjivost
T = prijetnja
P = vjerojatnost događaja
I = posljedice

Jedna od varijacija: $R = AV + P$

za $P = V + T$ $R = AV + V + T$

$AV \in$ [0-mala, 4-velika] $V,T \in$ [0-niska, 2-visoka razina]

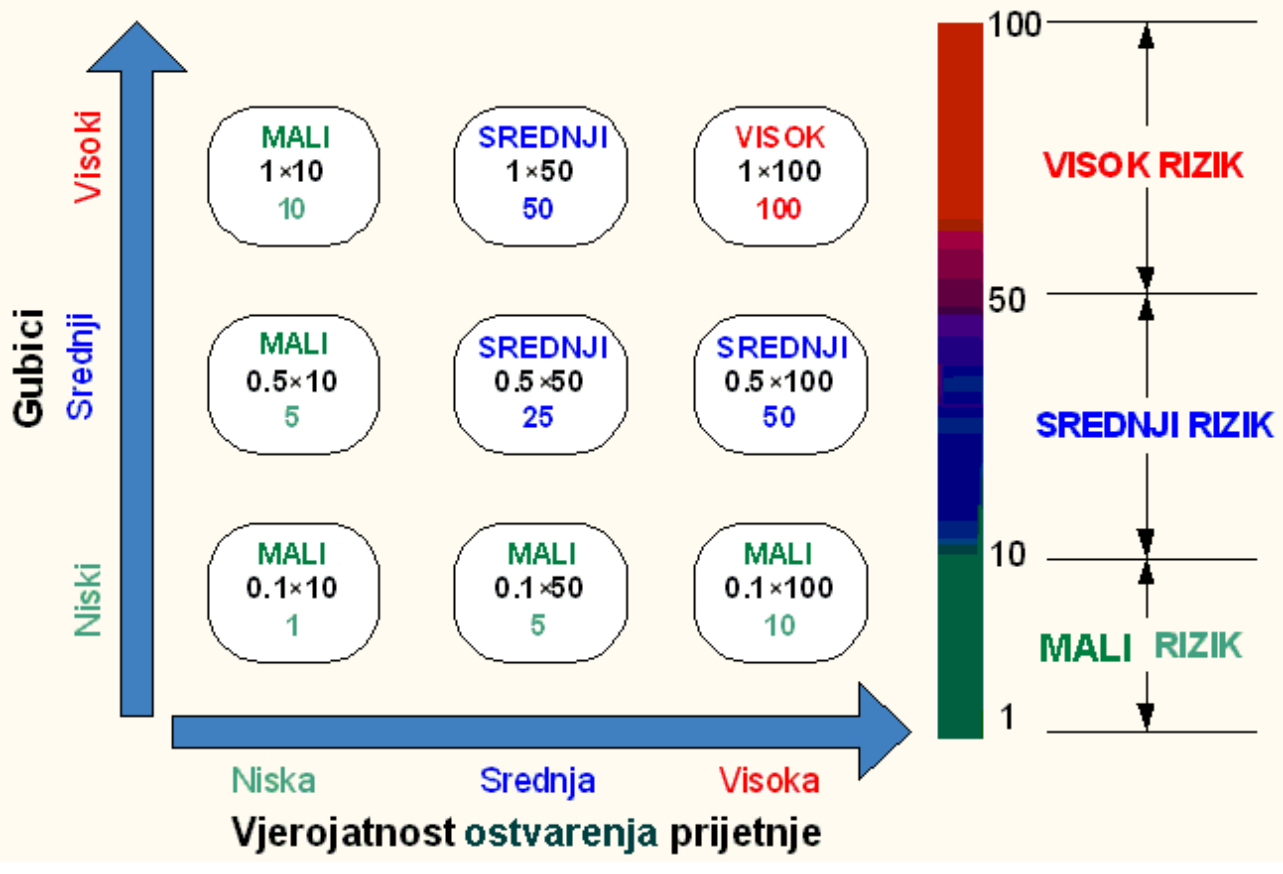
$R \in$ [0-najmanji rizik, 8-najveći rizik]

- formalno je ova metoda ista kao i prva metoda samo što se u prvoj metodi prilikom procjene ranjivosti i prijetnji implicitno odražava vjerojatnost ostvarenja dok se u ovoj metodi obavlja upravo obrnuti postupak: vjerojatnost ostvarenja prijetnje se izračunava na temelju procijenjenih ranjivosti i prijetnji

Nedostatak:

- problematična nezavisna procjena prijetnje i ranjivosti

Primjer granulacije rizika



Koraci procjene rizika prema NIST-u

1. Identifikacija resursa. Klasificirati resurse prema povjerljivosti i osjetljivosti (kritični resursi). Odrediti im vlasnika i po mogućnosti vrijednost.
2. Identifikacija prijetnji. Namjerni i nenamjeni izvori prijetnji.
3. Identifikacija ranjivosti. Koje su slabosti i propusti u sustavu? (iskustvo, *pentesting*, …)
4. Analiza postojećih kontrola.
5. Procjena vjerojatnosti ostvarenja prijetnje. $P = f$(prijetnja, ranjivost)
   Odrediti razinu (npr. visoka, srednja, niska).
6. Analiza mogućih posljedica.
7. Određivanje rizika za svaku kombinaciju ranjivost/prijetnja. Kvalitativna i/ili kvantitativna.
8. Preporuke za umanjenje rizika. Predložiti sigurnosne mjere ili kontrole koje će umanjiti rizik.
9. Izvještaj i dokumentacija. Jasni i pregledni. Rezultate prilagoditi upravi (tablice, grafikoni…).

Kako odabrati sigurnosne mjere?

Pregled skupa normi ISO/IEC 27000

ISO/IEC 27000:2018 - uvod, pregled normi i rječnik (slobodno dostupno!)

ISO/IEC 27001:2013 - zahtjevi za ostvarenje sustava upravljanja informacijskom sigurnošću (ISMS)

ISO/IEC 27002:2013 - praktična primjena sigurnosnih kontrola

ISO/IEC 27003:2017 - upute za implementaciju ISO/IEC 27001

ISO/IEC 27004:2016 - procjena ISM (*information security management measurement*)

ISO/IEC 27005:2018 - upravljanje rizikom

ISO/IEC 27006:2015 - upute za certifikaciju

ISO/IEC 27007:2017 - nadzor (*a guide to auditing ISMS management system elements*)

Evolucija norme ISO/IEC 27001:2013

- 1995. BS7799
- 2000. ISO/IEC 17799:2000
- 2005. ISO/IEC 27001:2005
- 2013. ISO/IEC 27001:2013

Norma ISO/IEC 27002

- definira upravljački okvir, ali ne zadire u konkretnu tehničku implementaciju
- pokriva sve vrste organizacija (gospodarske, državne, neprofitne...)
- sadrži
  - 14 domena ili skupova sigurnosnih mjera (kontrola), koje zajedno sadrže 35 sigurnosnih kategorija i ukupno 114 kontrola
- u procesu upravljanja rizikom treba navesti na koji način je moguće umanjiti rizik primjenom određenih mjera
  - poželjno je sastaviti poseban dokument sadrži popis svih mjera, informaciju jesu li primijenjene i za svaku mjeru "izjavu o primjenjivosti"

14 domena prema normi ISO/IEC 27002:2013

1. Politike informacijske sigurnosti
   Information security policies (2)
2. Organizacija informacijske sigurnosti
   Organization of information security (5+2)
3. Sigurnost ljudskih resursa
   Human resource security (2+3+1)
4. Upravljanje impovinom
   Asset management (4+2+3)
5. Kontrola pristupa
   Access control (2+6+1+5)
6. Kriptografija – *Cryptography* (2)
7. Fizička sigurnost
   Physical and environmental security (6+9)
8. Sigurnost računalnih operacija
   Computer Operations Security (4+1+1+4+1+2+1)
9. Mrežna sigurnost
   Communications security (3+4)
10. Nabava, razvoj i održavanje sustava
    System acquisition, development and maintenance (3+9+1)
11. Odnosi s dobavljačima
    Supplier relationships (3+2)
12. Upravljanje sigurnosnim incidentima
    Information security incident management (7)
13. Upravljanje kontinuitetom poslovanja
    Information security aspects of business continuity management (3+1)
14. Usklađenost s pravnim propisima
    Compliance (5+3)

- broj kontrola svrstane u kategorije

Sigurnosna kategorija

- sadrži
  - kontrolni cilj koji je potrebno ostvariti
  - jednu ili više mjera koje se mogu primijeniti kako bi se ostvario kontrolni cilj
- opis svake mjere (kontrole) je strukturiran:

Mjera

Definira određenu kontrolu koja treba zadovoljiti kontrolni cilj.

Implementacijske smjernice

Pruža *detaljnije* informacije kako implementirati kontrolu.

Dodatne informacije

Primjer sigurnosne mjere unutar sigurnosne kategorije *Upravljanje pristupom korisnika* (iz norme ISO/IEC 17799)

Mjera Upravljanje lozinkama

Dodjeljivanje lozinki treba biti kontrolirano kroz formalni proces.

Implementacijske smjernice

Proces upravljanja lozinkama treba uključivati sljedeće:

a) korisnici moraju potpisati izjavu o čuvanju lozinki te dijeljenju grupnih lozinki isključivo s ostalim članovima grupe;
b) kada korisnici sami čuvaju svoju lozinku, tada im se dodjeljuje inicijalna privremena lozinka koju odmah trebaju promijeniti;
c) utemeljiti procedure za provjeru identita korisnika prije nego što im se dodjeli nova, zamjenska ili privremena lozinka;
d) privremene lozinke se korisnicima trebaju dodijeliti na siguran način; izbjegavati posredstvo treće strane ili elektroničkih poruka;
e) privremene lozinke trebaju biti jedinstvene i teške za pogađanje;
f) korisnici trebaju potvrditi primitak lozinke;
g) lozinke nikad ne bi smjele biti sačuvane u nezaštićenom obliku u sustavu;
h) inicijalne lozinke proizvođača opreme trebaju biti promijenjene prije instalacije sustava ili programa.

Dodatne informacije

Ponekad je potrebno razmotriti druge načine identifikacije i autentifikacije korisnika, poput biometrijskih značajki (primjrice, otisak prsta) i uporabe sklopovskih tokena (pametne kartice).

Sigurnosna politika

ili preciznije

Politika informacijske sigurnosti

- riječ "politika" u ovom kontekstu znači planiranje i način upravljanja
- može biti dio opće politike organizacije pa ne mora nužno biti poseban dokument
- cilj sigurnosne politike je dati smjernice za upravljanje informacijskom sigurnošću u skladu s poslovnim zahtjevima organizacije i relevantnim zakonima i propisima
- treba je podržati uprava
- je skup dokumenata kojima se utvrđuju mjere informacijske sigurnosti za zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka te raspoloživosti i cjelovitosti informacijskog sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose
- treba je provjeravati i dorađivati u unaprijed određenim vremenskim intervalima

Dokument sigurnosne politike treba sadržavati:

- definiciju informacijske sigurnosti, njezine glavne ciljeve i opseg te važnost sigurnosti;
- izjavu o namjerama uprave koje će podupirati ciljeve informacijske sigurnosti u skladu s poslovnom strategijom;
- okvir za uvođenje kontrola, kao i strukturu procjene rizika i upravljanja rizikom;
- objašnjenje sigurnosne politike, principe, norme i zahtjeve od posebnog interesa koje organizacija treba usvojiti;
- definiciju odgovornosti u procesu upravljanja sigurnošću, uključujući i prijavu sigurnosnih incidenata;
- reference na dokumente koji podupiru sigurnosnu politiku

Sigurnosna politika

Sigurnosni zahtjevi

Djelatnici Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave pohranjuju i razmjenjuju informacije. Za kvalitetan rad nužno je zaštiti informacije od:

- neovlaštenih izmjena - osigurati **integritet**,
- objavljivanja tajnih informacija (primjerice ispitni zadaci) - osigurati **povjerljivost**,
- uskraćivanja dostupnosti informacija ovlaštenim korisnicima - osigurati **dostupnost**.

Sigurnosni incidenti nisu samo problem pojedinca (onog koji je izazvao incident) već su prijetnja cijelom Zavodu.

Najčešći izvori i oblici prijetnji

Ljudski faktor, nenamjerne prijetnje: nepažnja, nemar, nedisciplina, neznanje, neadekvatna ogranizacija, ...
Ljudski faktor, namjerne prijetnje: neautorizirani pristup, krađa, zlonamjerni programi, prisluškivanje, uništavanje, ...
Oprema: tehnička pogreška, prestanak napajanja, prekid komunikacije, ...
Prirodne nepogode: oluja, potres, požar, ...

Svrha

Svrha ovog dokumenta je definirati sigurnosne postupke koji će održati odgovarajuću razinu sigurnosti informacijskog sustava Zavoda. Sigurnosne postupke provode korisnici sustava nad mrežnom infrastrukturom, poslužiteljima, stolnim i prijenosnim računalima s dodatnom opremom, operacijskim sustavima, primjenskim programima te podacima.

Osnovni pojmovi

Zavodski **informacijski sustav** prikuplja, pohranjuje, čuva, obrađuje i pruža informacije tako da su one uvijek dostupne svim članovima Zavoda s odgovarajućim ovlastima (pravima pristupa) i sastoji se od mrežne infrastrukture i računala (računala u vlasništvu Fakulteta i privatna računala).
Korisnici se dijele u tri skupine: djelatnici, studenti i ostali.
Administrator je korisnik s administratorskim privilegijama.
Voditelj sigurnosti je osoba zadužena za nadgledanje i provođenje sigurnosnih mjera.

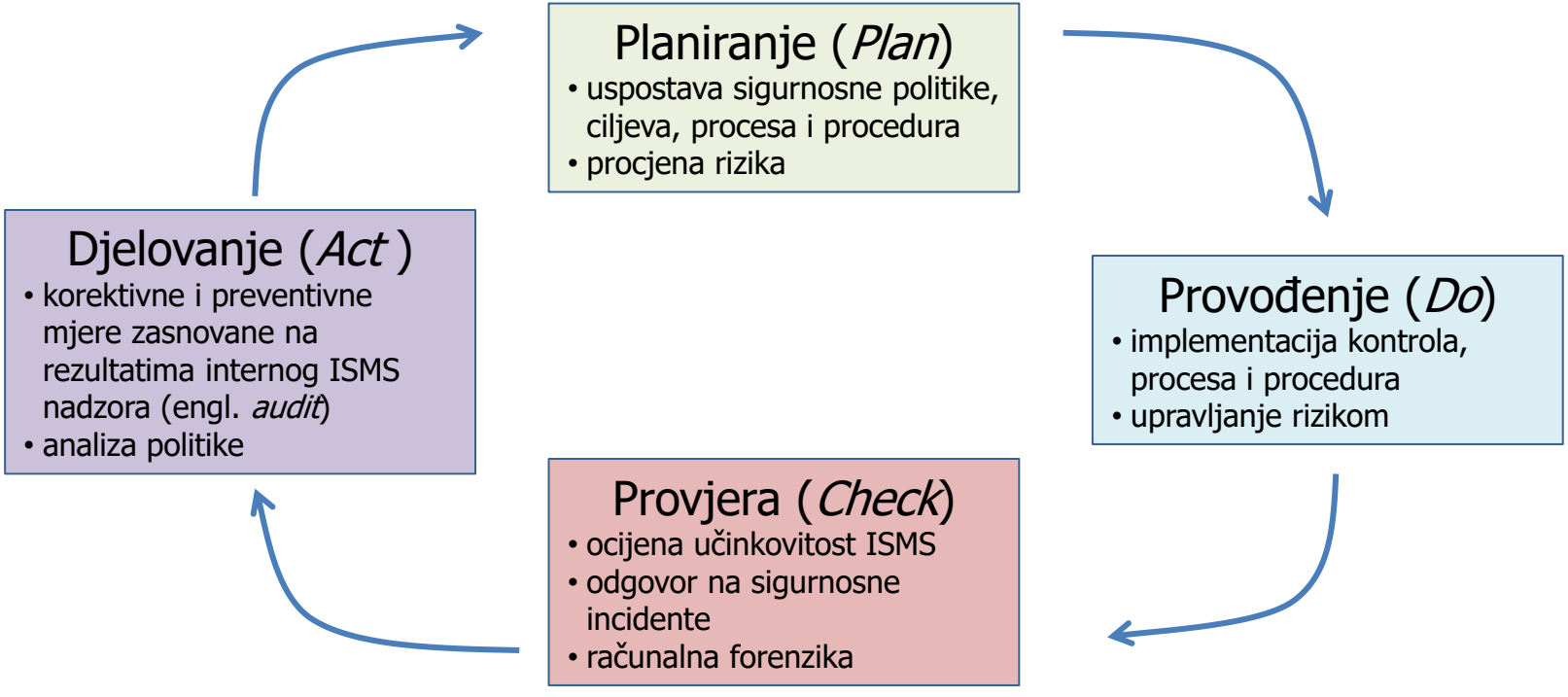
Popis dodatnih dokumenata

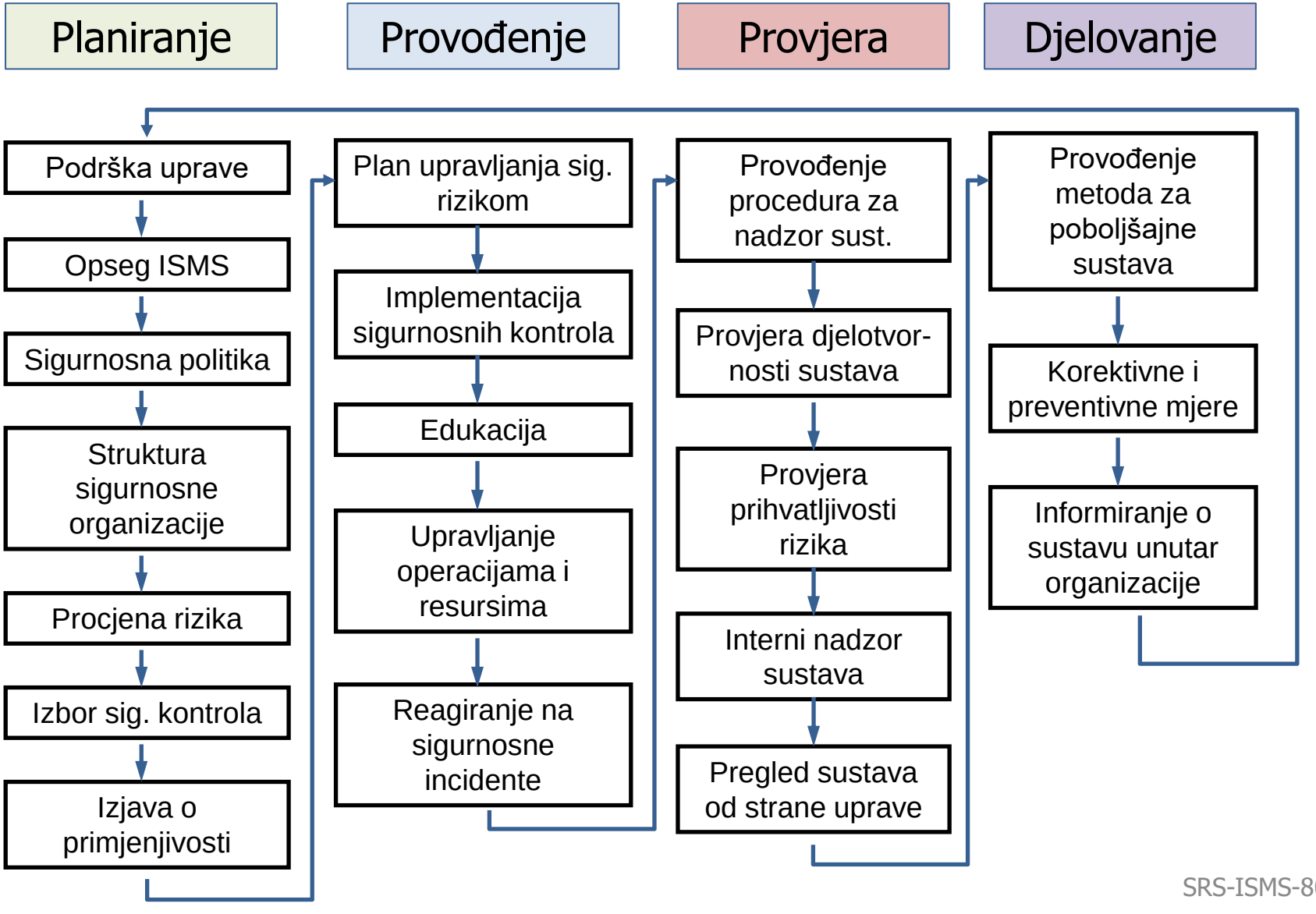
Pravilnik o sigurnosti radnog mjesta - dokument namijenjen korisnicima.
Pravilnik namijenjen administratorima i voditelju sigurnosti - dokumenti namijenjeni voditelju sigurnosti.

Sustav upravljanja sigurnošću informacija

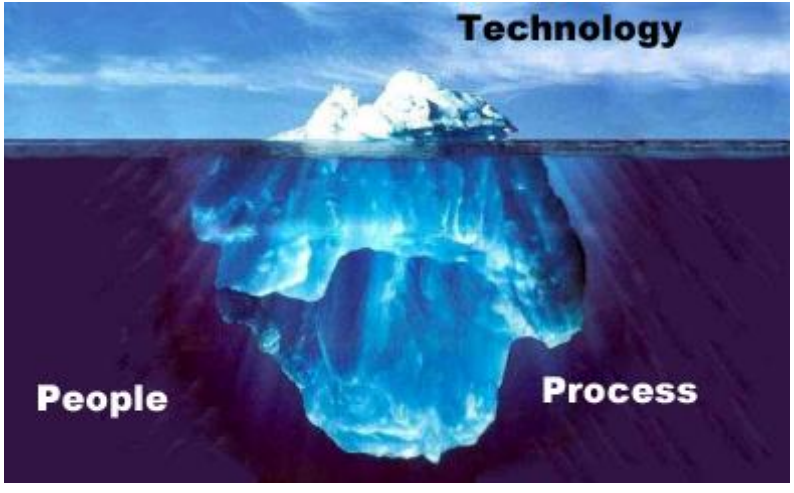
prema normi ISO/IEC 27001

PDCA model upravljanja




Planiranje
Provođenje
Provjera
Djelovanje
Podrška uprave
Opseg ISMS
Sigurnosna politika
Struktura sigurnosne organizacije
Procjena rizika
Izbor sig. kontrola
Izjava o primjenjivosti
Plan upravljanja sig. rizikom
Implementacija sigurnosnih kontrola
Edukacija
Upravljanje operacijama i resursima
Reagiranje na sigurnosne incidente
Provođenje procedura za nadzor sust.
Provjera djelotvor-nosti sustava
Provjera prihvatljivosti rizika
Interni nadzor sustava
Pregled sustava od strane uprave
Provođenje metoda za poboljšajne sustava
Korektivne i preventivne mjere
Informiranje o sustavu unutar organizacije

Umjesto zaključka



Dodatni slajdovi

Primjer kriptografskih normi iz skupa normi

PKCS

- skup normi koje podržavaju kriptografiju javnog ključa (*Public-Key Cryptography Standards*)
- osmišljen ranih 1990.-tih
- vlasnik, autor tvrtka *RSA Laboratories* kako bi promovirala svoj algoritam RSA
- numerirane norme od PKCS#1 do PKCS#15
- primjerice PKCS#1 specificira kako na siguran način koristiti algoritam RSA za kriptiranje i digitalni potpis
- s vremenom se gubi interes, no
- postaje dio novijih normi poput ANSI X9, SSL/TLS pa se ipak i dalje razvija

Popis trenutno važećih normi

Norma	Opis
PKCS#1	Kriptografska norma algoritma RSA
PKCS#2,4	*- ugrađeno u PKCS#1*
PKCS#3	Norma za razmjenu ključeva prokolom Diffie-Hellman
PKCS#5	Norma za kriptografiju zasnovanu na lozinkama (engl. *Password-Based Cryptography*)
PKCS#6	Norma koja definira sintaksu certifikata
PKCS#7	Norma koja definira sintaksu kriptografskih poruka
PKCS#8	Norma koja definira sintaksu privatnih ključeva
PKCS#9	Definicija atributa i klasa (eng. *Selected Object Classes and Attribute Types*)
PKCS#10	Norma koja definira sintaksu zahtjeva za certifikatom
PKCS#11	Norma koja definira programsko sučelje za rad s kriptografskim tokenima (engl. *CRYPTographic TOKen Interface standard , CRYPTOKI*)
PKCS#12	Norma koja definira sintaksu i načine razmjene osobnih podataka
PKCS#13	*- rezervirano za ECC - nije objavljeno*
PKCS#14	*- rezervirano za generatore pseudoslučajnih brojeva – nije objavljeno*
PKCS#15	Definicija sintakse i načina pohrane informacija (certifikata, ključeva) u kriptografske tokene

PKCS#1

- specificira kako na siguran način koristiti algoritam RSA za kriptiranje i digitalni potpis
- definira nadopunu bloka podataka *M* (engl. *padding*) i to na početku poruke, a ne na kraju kako je uobičajeno kod simetričnih algoritama i funkcija za izračunavanje sažetka

00 II BT II PS II M

  - prvi bajt je 00 kako bi se osiguralo da je broj koji se kriptira manji od *n*
  - BT = tip bloka
    - 02 - kada se kriptira javni ključem (najčešće)
    - 00 ili 01 – ako se kriptira privatnim ključem
  - PS = slučajna nadopuna (engl. *padding stream*)
    - minimum 8 slučajnih bajtova

PKCS#11

- norma koja definira programsko sučelje za rad s kriptografskim tokenima
- CRYPTOKI (izgovara se kao "*crypto-key*")
  - engl. *CRYPTographic TOKen Interface*
  - programsko sučelje prema kriptografskim uređajima (engl. *cryptographic token*) koji
    - čuvaju kriptografske informacije i
    - mogu obavljati kriptografske funkcije
  - objektno orjentirano programsko sučelje koje ne ovisi ni o vrsti:
    - uređaja, kao ni o vrsti
    - programa
  - cilj je sakriti programeru detalje uređaja

Kriptografski uređaj

- engl. *cryptographic token* ili samo *token*
- općeniti model kriptografskog uređaja

pametne kartice

PCMCIA kartice

sklopovski sigurnosni modul (engl. *hardware security module*, *HSM*)

USB kriptografski uređaj

PKCS#11

- normira, odnosno, specificira
  - strukture podataka i
  - funkcije

  koje su dostupne programima u programskom jeziku ANSI C
- programeri koriste podatke i funkcije čiji su prototipovi definirani u zaglavljima (*C header files*), a ostvarene su u biblioteci programa *Cryptoki*
- programsko sučelje *Cryptoki* definira najčešće korištene strukture podataka tj, tipove objekata kao što su
  - RSA ključevi
  - certifikati X.509
  - DES/3DES ključevi itd.

  te funkcije koje ih stvaraju, mijenjaju i brišu.

PKCS#11

- krajem 2020.g. izašla verzija norme 3.0
  - predzadnja verzija norme 2.40 je iz 2015.g.
- podržava sljedeće algoritme i protokole:
  - asimetrični: RSA, EC
  - razmjena ključa: DH, ECDH
  - simetrični: DES, 3DES, AES, Blowfish, Twofish, Camellia (Japan), ARIA i SEED (Južna Koreja), OTP i GOST
  - načini kriptiranja: ECB, CBC, OFB, CTR, GCM (autentifikacijsko kriptiranje), CTS (*ciphertext stealing*), MAC, HMAC
  - funkcije za izračunavanje sažetaka *(hash*): MD2, MD5, SHA-1, SHA-2 (224, 256, 384, 512), RIPE-MD 128/160
  - digitalni potpis: DSA, ECDSA
  - SSL, TLS

Za kraj ponovimo najznačajnije preporuke

- Simetrični algoritmi: AES
  - u bliskoj budućnosti algoritmi prilagođeni ugrađenim računalima i Internetu stvari, tj. algoritmi koji su manje zahtjevni na računalne resurse
- Asimetrični algoritmi:
  - za sada RSA-2048 i ECC
  - u bliskoj budućnosti bit će raspoloživi „post-kvantni” algoritmi koji se neće koristiti sve dok klasični asimetrični algoritmi ne budu kompromitirani
- Funkcije za izračunavanje sažetka poruke: SHA-3