CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosna politika

CCERT-PUBDOC-2009-05-265

+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

Učestalost napada na informacijske sustave tvrtki i institucija koji sadrže povjerljive i/ili osjetljive podatke (npr. osobni podaci korisnika, korisnička imena i lozinke, povjerljivi dokumenti, itd.), pokazala je potrebu za propisivanjem pravila kojima će se zaštititi materijalne i intelektualne vrijednosti neke organizacije. Jasno je da napade nije moguće predvidjeti, a ponekad niti spriječiti, ali moguće je poduzeti sve mjere opreza kako bi se šteta koju je napad prouzročio smanjila na najmanju moguću razinu. Najčešći motiv napada je stjecanje financijske koristi. Međutim, u velikom broju slučajeva financijska šteta je manja u odnosu na štetu nanesenu otkrivanjem informacija koje neki sustav sadrži.

Skup jasno definiranih pravila koja obuhvaćaju sva područja na kojima je moguće izvršiti neku vrstu napada naziva se sigurnosnom politikom. Sigurnosnom politikom jasno se određuju pravila ponašanja i odgovornosti vezane uz informacijski sustav kako bi se minimizirala šteta nastala namjernim ili nenamjernim djelovanjem. Dakle, ukoliko neka organizacija ima uvedenu formalnu sigurnosnu politiku smatra se da su sigurnost i zaštita informacijskog sustava na visokoj razini. Sigurnosna politika također ima ulogu osvještavanja zaposlenika o važnosti informacijske sigurnosti, ali i edukacije o sigurnosti te mogućim rizicima i posljedicama sigurnosnih incidenata.

U nastavku dokumenta moguće je saznati više o prijetnjama sa kojima su suočeni informacijski sustavi kako bi se korisnicima dočarao stvarni opseg zlonamjernih djelatnosti ili manjka pažnje i opreza pri korištenju računala, te njihov utjecaj na poslovanje organizacije. Također, moguće je saznati više o standardima na temelju kojih je moguće izraditi sigurnosnu politiku organizacije. Standardi predstavljaju samo smjernice za izradu sigurnosne politike (jer ponekad imaju preopćenit sadržaj), tj. ne odgovaraju specifičnim potrebama organizacija. Naposljetku, opisan je primjer uspostave sigurnosne politike prema smjernicama standarda ISO/IEC 27002.

2. Sigurnosna politika

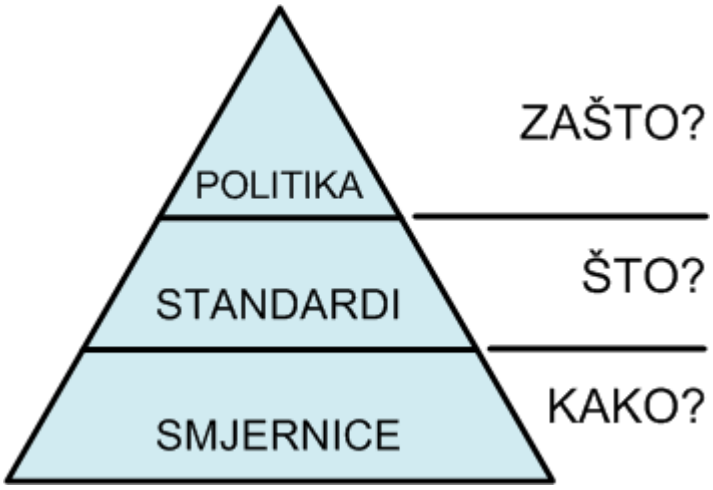
Informacijski sustavi u tvrtkama ili institucijama sadrže velik broj osjetljivih i povjerljivih podataka koje je potrebno zaštititi od zlonamjernih aktivnosti bilo da se radi o pokušaju krađe, izmjene ili brisanja podataka. Tvrtke, poput banaka, i institucije, poput sveučilišta ili onih koje sadrže velike baze povjerljivih podataka, moraju svojim korisnicima omogućiti pristup željenim podacima. Međutim, uz sve prijetnje koje mogu ugroziti korisnike i podatke, putem Interneta ili prijenosnih medija, potrebno je obratiti pažnju na sigurnost cijelog sustava.

Sigurnosna politika je skup pravila i postupaka kojima se određuje razina sigurnosti nekog informacijskog sustava, istovremeno pridajući pažnju sigurnosti tehnologije i informacija koje informacijski sustav sadrži. Sigurnosnom politikom korisniku se nameću obvezna pravila ponašanja i odgovornosti kako bi se zaštitilo informacijski sustav, tj. informacije pohranjene u informacijskom sustavu, od vanjskih utjecaja (udaljenih napada, zlonamjernih programa, itd.), ali također i korisnika (neovlašteni pristup podacima, krađa podataka, izmjena podataka, itd.). Sigurnosna politika tvrtke ili institucije prilagođava se potrebama, te nije jednaka za sve.

Sigurnosnu politiku predstavlja službena izjava ili plan organizacije koji obuhvaća ciljeve, smjernice i prihvatljive postupke. Ona uključuje sljedeće zahtjeve:

- potrebno je poštovati pravila definirana sigurnosnom politikom,
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija,
- potrebno je usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike i
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima i smjernicama.

Standard je obvezni postupak ili pravilo koje je izrađeno kako bi učinilo politiku suvislom i učinkovitom, a mora uključivati jedan ili više tehničkih opisa za komponente računala, programe i rukovanje istima. Smjernice su općenite izjave, preporuke ili administrativne upute koje daju okvirne upute za provođenje sigurnosne politike konstruirane kako bi se ostvarili ciljevi sigurnosne politike. Smjernice nisu obvezujuće, one služe više kao pomoć pri uspostavljanju sigurnosne politike.



Dijagram 1. Prikaz uklapanja smjernica, standarda i sigurnosne politike

Izvor: SANS

Dijagram 1. prikazuje odnose između smjernica, standarda i sigurnosne politike. Smjernice navode najbolje primjere *kako* izvesti nešto, npr. na koji način poboljšati sigurnost nekog informacijskog sustava. Standardi navode koji su osnovni zahtjevi za različite tehnologije i postavke, tj. *što* je potrebno kako bi se sustav postavio prema smjernicama. Sigurnosna politika opisuje kako i *zašto* je potrebno djelovati. Pri oblikovanju sigurnosti nekog informacijskog sustava prvi je postupak uspostavljanje sigurnosne politike,

potom slijedi odabir standarda prema kojem će se sigurnosna politika uspostaviti, te na kraju pronalazak smjernica koje će omogućiti učinkovit način provedbe sigurnosne politike.

Sigurnosnu politiku je važno dati svim korisnicima na uvid kako bi je znali primijeniti i kako bi znali ispravno koristiti tehnologije koje su im na raspolaganju. Kao prijetnja nameće se nanošenje štete na informacijskom sustavu, stoga se pravila određena sigurnosnom politikom primjenjuju na:

- raspolaganje računalnom opremom koja uključuje sama računala i programe - ispravno korištenje računala, periferne opreme, te programa koji su ugrađenih na računalu,
- osobe odgovorne za nadgledanje informacijskog sustava - uspostavljanje procedura koje osobe odgovorne za nadgledanje informacijskog sustava moraju izvršavati kako bi se povećala sigurnost informacijskog sustava,
- sve zaposlenike i korisnike sustava, tj. sve osobe koje imaju pravo pristupa informacijskom sustavu - postavljanje ograničenja pristupa određenim podacima (svaki zaposlenik/korisnik ima svoje područje djelatnosti, te mu je na temelju toga dodijeljen pristup podacima koji su potrebni kako bi mogao vršiti svoju poslovnu dužnost) i
- vanjske suradnike (npr. zaposlenici službe održavanja informacijskog sustava) - potrebno je uspostaviti nadzor vanjskih suradnika kako ne bi došlo do krađe ili oštećenja materijalnog ili intelektualnog vlasništva organizacije.

Sigurnosnu politiku tvrtke potrebno je dati na uvid svakom korisniku prije uporabe dostupne računalne opreme kako bi znao koje su dopuštene i nedopuštene radnje. Naravno, većina korisnika sigurnosnu politiku ne pročita dovoljno pažljivo, stoga je potrebno dokument sažeti i jasno odrediti pravila bez uporabe stručnih termina koji nisu razumljivi svima. Sigurnosna politika mora sadržavati odgovore na sljedeća pitanja:

- Tko ima pristup povjerljivim informacijama?
- Kako će se povjerljive informacije pohranjivati i prenositi u komunikaciji? (da li će se šifrirati, kako će se šifrirati, da li će se komprimirati, itd.)
- Na kojim informacijskim sustavima se smiju pohranjivati povjerljive informacije?
- Koja se razina tajnosti povjerljivih informacija smije ispisivati?
- Kako se osjetljive i povjerljive podatke smije uklanjati sa nekog informacijskog sustava?

2.1. Uloga sigurnosne politike

Zaštita različitim alatima i tehnologijama u informacijskim sustavima često nije dovoljna kako bi se zaštitili povjerljivi i osjetljivi podaci. Sigurnosti informacijskih sustava pridonosi ispravna uporaba svih dijelova informacijskog sustava i poštivanje pravila propisanih sigurnosnom politikom organizacije. Sigurnosnom politikom propisuju se dozvoljene i nedozvoljene radnje kako bi se osigurala postojanost računalne opreme (*eng. hardware*), programa (*eng. software*) i podataka koje informacijski sustav sadrži.

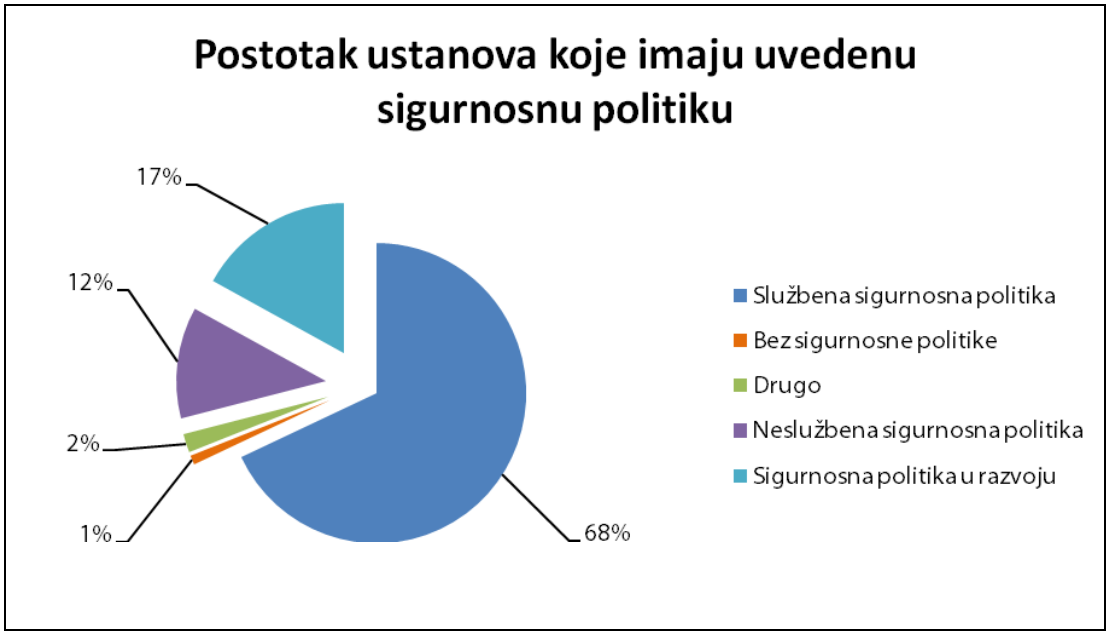
Uspostavom sigurnosne politike korisnicima su nametnuta obvezujuća pravila ponašanja koja ograničavaju slobodu pri pregledavanju povjerljivih informacija, te pravila za ispravno korištenje računalne opreme koja je korisniku dana na korištenje.

Uvođenjem i provođenjem sigurnosne politike tvrtka smanjuje mogućnost gubitka podataka što u velikoj mjeri utječe na učinkovito poslovanje. Međutim, nije u pitanju samo gubitak podataka, već i vremena i novaca. Uništavanjem, kopiranjem ili mijenjanjem povjerljivih podataka, tvrtka može izgubiti poziciju na tržištu. Primjerice, u slučaju da razvija novi proizvod, otkrivanjem podataka o njemu široj javnosti ili konkurentskim tvrtkama dovodi se do gore navedenih problema. Smatra se da uvođenje sigurnosne politike osigurava stabilno poslovanje neke tvrtke.

2.2. Statistika

Statistički pokazatelji iz izvješća Computer Security Institute "CSI Computer Crime and Security Survey" za 2008. godinu upućuju na činjenicu da je većina ustanova svjesna vrijednosti podataka koje njihovi informacijski sustavi sadrže, ali isto tako i prijetnji koje ih ugrožavaju. Navedeno je da čak 68% ustanova ima uvedenu službenu sigurnosnu politiku, a još 18% ustanova ju razvija ili prilagođava. Neslužbenu sigurnosnu politiku ima 12% ustanova, dok samo 1% ustanova u primjeni

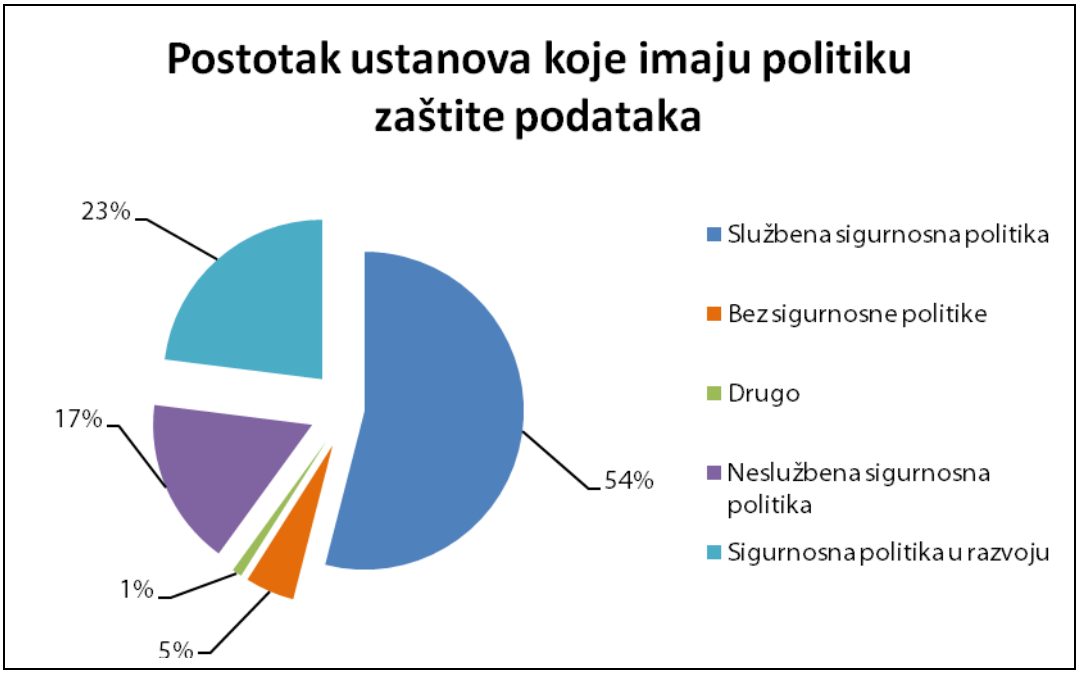
nema nikakvu sigurnosnu politiku. Iz Dijagrama 2. je vidljivo da velik broj ustanova ima uvedenu službenu ili neslužbenu sigurnosnu politiku, a taj postotak iznosi čak 80%. Također, u Dijagramu 2. navedena je kategorija „Drugo" pod koju spadaju neformalna pravila koja ne obuhvaćaju sva područja koja sigurnosna politika podrazumijeva.



Dijagram 2. Prikaz postotka ustanova koje imaju uvedenu sigurnosnu politiku

Izvor: CSI Computer Crime and Security Survey

Drugi podatak koji je važno izdvojiti svakako je udio organizacija koje imaju uvedenu politiku zaštite podataka (*eng. data retention policy*). Politika zaštite podataka u današnjici dobiva sve veći i veći značaj, stoga podaci prikazani u Dijagramu 3. ne iznenađuju. Udio organizacija koje imaju uveden neki oblik politike zaštite podataka iznosi 71%. Pod službenom politikom zaštite podataka podrazumijeva se izdavanje službenog dokumenta politike, dok kod neslužbene politike nije izdan službeni dokument ali su na neki način definirana pravila korištenja informacijskog sustava (usmeno, drugim dokumentima i sl.).



Dijagram 3. Prikaz postotka ustanova koje imaju politiku zaštite podataka

Izvor: CSI Computer Crime and Security Survey

3. Prijetnje informacijskim sustavima

Informacijski sustavi izloženi su velikom broju sigurnosnih prijetnji koje mogu utjecati na integritet podataka i otuđivanje istih, ali jednako tako i financijsku štetu. Razmjeri štete nastale neželjenim aktivnostima mogu biti različitog opsega, od uništenja jedna datoteke, pa do nestajanja cijele baze podataka. Uzročnici neželjenih aktivnosti mogu biti napadači ili legitimni korisnici, zlonamjerni programi, itd.

Prijetnja sigurnosti nekog informacijskog sustava je svaki događaj koji može ishoditi narušavanjem integriteta, pouzdanosti i dostupnosti podataka. Također, važno je spomenuti da svaka prijetnja i neovlašteni pristup informacijskom sustavu, imaju različite posljedice, npr. uništavanje podataka (točnosti, dostupnosti, itd.) ili narušavanje ispravnog rada cijelog informacijskog sustava.

Postoji nekoliko klasifikacija prijetnji informacijskim sustavima, međutim upitno je jedino da li svaka klasifikacija dovoljno detaljno razmatra sve uvjete i mogućnosti nastanka štete na informacijskom sustavu. Važnost detaljne klasifikacije je u pronalasku primjerenih načina zaštite, te standardizaciji klasifikacije. Prema klasifikaciji NIST-a (**N**ational **I**nstitute of **S**tandards and **T**echnology) prijetnje informacijskim sustavima se mogu podijeliti na:

1. *Greške i kvarove* - ovu se vrstu prijetnji često podcjenjuje, ali mogu nanijeti značajnu štetu informacijskom sustavu. Najčešći uzrok greškama i kvarovima su ljudske radnje. Mogu ih uzrokovati zaposlenici, proizvođači programskih paketa ili administratori informacijskih sustava. Vjeruje se da je gotovo 65% napada uzrokovano greškama i kvarovima.
2. *Prijevare i krađe* - zlonamjerna aktivnost kojom napadač pokušava steći financijsku ili neki drugi oblik koristi. Prijevare i krađe se mogu dogoditi aktivnostima unutar (zaposlenik) ili izvan (udaljeni napad) organizacije. Međutim, češći su slučajevi aktivnosti prijevare i krađe unutar organizacije koji se događaju u čak 74% slučajeva. Primjerice, zaposlenik ima pristup određenim financijskim podacima i lako može upravljati iznosima koje je potrebno obraditi. Vrlo lako je navesti razloge zbog kojih se prijevare i krađe događaju češće od strane zaposlenika nego udaljenim napadima:
    - zaposlenici imaju pristup podacima i informacijskom sustavu,
    - zaposlenici znaju koje podatke sustav sadrži i koje su sigurnosne provjere i
    - zaposlenici znaju koje su prilike za prijevaru i krađu, te kolika je vrijednost mogućeg plijena.
3. *Sabotažu od strane zaposlenika* - koja je česta prijetnja sigurnosti i podacima informacijskog sustava. Kao što je već naglašeno, zaposlenici imaju pristup, te znaju u kojim dijelovima sustava je moguće prouzročiti najveću štetu. Ako je u pitanju nezadovoljstvo zaposlenika, sabotaža je vrlo čest slučaj, bilo da se radi o sadašnjem ili bivšem zaposleniku. Najčešći primjeri sabotaže su:
    - fizičko uništavanje dijelova informacijskog sustava,
    - postavljanje logičke bombe (*eng. logic bomb*), tj. zlonamjernog programskog koda čija je namjena izbrisati, premjestiti ili izmijeniti podatke,
    - namjerni unos neispravnih podataka,
    - „rušenje“ informacijskih sustava,
    - brisanje i uništavanje podataka,
    - krađa podataka i ucjena pod prijetnjom otkrivanja tih podataka široj javnosti ili konkurenciji ili
    - namjerno mijenjanje podataka.
4. *Gubitak fizičke i infrastrukturne potpore* - je vrsta prijetnje koju nije moguće u potpunosti provjeriti, ponekad niti spriječiti, a može nanijeti veliku štetu sustavima. Takvi slučajevi mogu biti npr. prekid u opskrbi električnom energijom, prekid komunikacija, poplava, požar, potresi, itd.
5. *Hakere* (*eng. hackers*) - koje se smatra relativno novom vrstom prijetnje informacijskim sustavima koja se nameće kao najopasnija zbog razvoja Interneta i komunikacija, poslovanja i drugih

aktivnosti putem Interneta. Napadačem se smatra osoba koja svoje računalno znanje koristi kako bi ugrozila sigurnost računala ili podataka na istom. Više o napadačima moguće je saznati u dokumentu „Računala mamci i ponašanje napadača“ (CCERT-PUBDOC-2008-09-241) objavljenog na službenim stranicama CERT-a.

6. *Zlonamjerne programe (eng. malware)* - vrsta prijetnje koja narušava sigurnost informacijskog sustava zlonamjernim programima poput crva, virusa, trojanskih konja, logičkih bombi i drugih. Među najčešćim i najopasnijim prijetnjama su virusi, trojanski konji i crvi.
7. *Prijetnje privatnosti korisnika* - postaje vrlo česta prijetnja s obzirom da sve veći broj informacijskih sustava sadrži velik broj osobnih podataka korisnika. Primjeri takvih ustanova su banke, državne institucije i sve veći broj tvrtki.

Također, vrijedno je spomenuti i klasifikaciju prema ISO/IEC 17799:2000 standardu (*Code of Practice for Information Security Management*) koji definira ispravne i sigurne načine upravljanja nekim informacijskim sustavom. Prijetnje su podijeljene obzirom na uzroke nastanka:

1. *prirodne katastrofe* - sve pojave koje su nepredvidive ili ih je nemoguće provjeriti, npr. potresi, poplave, oluje, zagađenja, požari, itd.
2. *tehnički uzroci* - tehničke greške, kvarovi, komunikacijske greške, različiti oblici zračenja, itd.
3. *nenamjerne ljudske radnje* - neposlušnost, kršenje pravila, upotreba neprimjerenih programa, itd.
4. *namjerne ljudske radnje* - uništavanje, sabotaža, špijunaža, ratna razaranja, prijevara, krađa, zlonamjerni programi, itd.

Computer Security Institute (nadalje CSI) je naveo vrlo jednostavnu klasifikaciju prijetnji, obzirom na poziciju prijetnje u odnosu na poziciju informacijskog sustava, tj. prijetnje je podijelio na unutarnje i vanjske. Unutarnjim prijetnjama smatraju se sve namjerne i nenamjerne radnje korisnika koji imaju izravan pristup informacijskom sustavu. Vanjske prijetnje su definirane kao svi pokušaji nanošenja bilo kakvog oblika štete udaljenim napadima ili ubacivanjem zlonamjernih programa u informacijski sustav sa udaljenih lokacija.

3.1. CSI/FBI Computer Crime and Security Survey

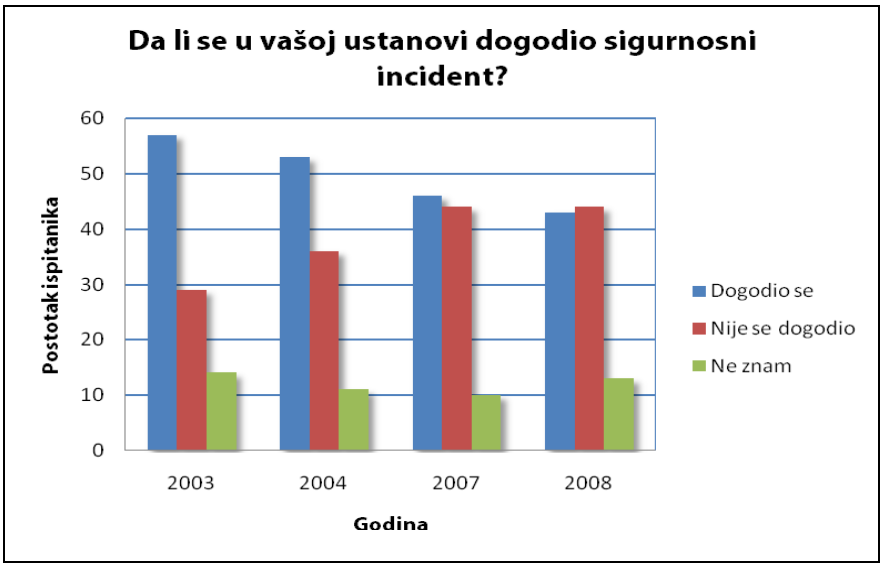
Prema zajedničkom izvješću CSI i FBI (Federal Bureau of Investigation) odjela za računalne zločine nazvanom „CSI/FBI Computer Crime and Security Survey“ vidljivo je da su provale u informacijske sustave u stalnom opadanju. Anketa je provedena na uzorku od 522 ispitanika, tj. stručnjaka za sigurnost informacijskih sustava iz američkih tvrtki, državnih, financijskih i zdravstvenih institucija, te sveučilišta. Izvješće je moguće preuzeti sa sljedeće adrese uz prethodnu registraciju:

http://www.gocsi.com/forms/csi_survey.jhtml

Iz Dijagrama 4 vidljivo je da se broj sigurnosnih incidenata u posljednjih pet godina smanjuje. U 2003. godini je čak 57% ispitanika odgovorilo da se u njihovoj ustanovi dogodio sigurnosni incident dok u sljedećim godinama taj postotak bilježi određen pad, za što se smatra da je rezultat uvođenja sigurnosnih mjera za zaštitu informacijskih sustava. Broj sigurnosnih incidenata bilježi pad od 7% u 2004. godini (13.2% u 2007. godini) te 6.5% u 2008. godini. Prosječan godišnji pad broja sigurnosnih incidenata iznosi 5.4%.

	Dogodio se sigurnosni incident	Nije se dogodio sigurnosni incident	Ne znam
2003	57%	29%	14%
2004	53%	36%	11%
2007	46%	44%	10%
2008	43%	44%	13%

Tablica 1. Prikaz udjela ispitanika po godinama



Dijagram 4. Učestalost događanja sigurnosnih incidenata

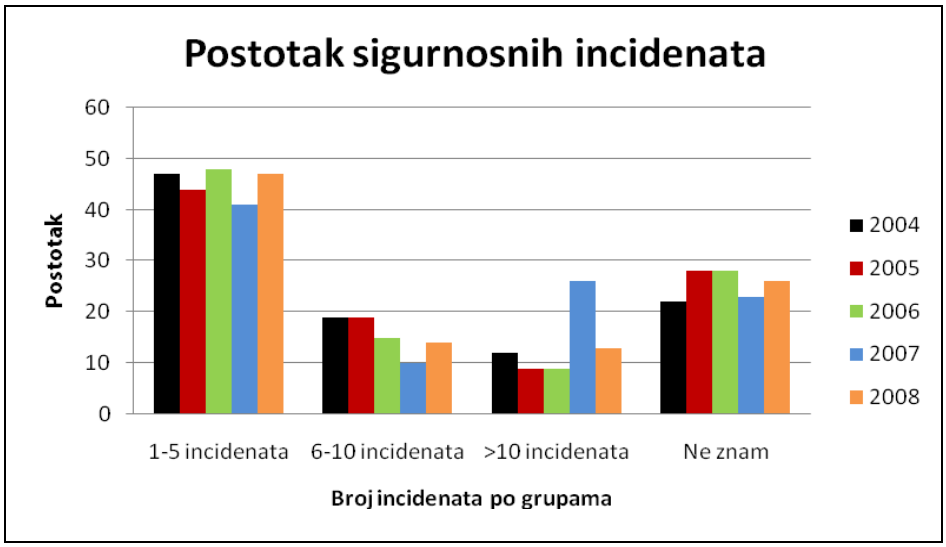
Izvor: CSI Computer Crime and Security Survey

Isto tako, broj ispitanika u čijim institucijama se nisu dogodili sigurnosni incidenti, zbog uvođenja naprednijih metoda zaštite, sigurnosne politike ili zato što nisu bili meta napada, je u stalnom porastu. Tako je, primjerice, u 2003. godini 29% ispitanika odgovorilo da se nije dogodio sigurnosni incident, u 2004. godini 36% ispitanika, te u 2007. i 2008. godini 44% ispitanika (razlike su male). Broj ustanova u kojima se nije dogodio sigurnosni incident bilježi rast od 24.1% u 2004. godini, te u narednim godinama rast od otprilike 7.4%.

Međutim, podatak koji zabrinjava je da jedan dio ustanova nije u potpunosti svjestan prijetnji, pa stoga niti ne zna da li se dogodio sigurnosni incident. Ova grupa ispitanika smatra se najrizičnijom jer nisu u potpunosti pripremljeni na incidente ili neprilike koje se mogu dogoditi, te ugroziti nesmetan rad ustanove. Također, ovakvim ponašanjem mogu ugroziti korisnike svojih usluga i svoje podatke.

U Dijagramu 3. ustanove su podijeljene u četiri grupe:

- ustanove kod kojih je dogodilo od 1 do 5 incidenata,
- ustanove kod kojih se dogodilo od 6 do 10 incidenata,
- ustanove kod kojih se dogodilo više od 10 incidenata i
- ustanove koje ne znaju točan broj incidenata koji se dogodio.



Dijagram 5. Postotak sigurnosnih incidenata po grupama

Izvor: CSI Computer Crime and Security Survey

Vidljivo je da je većina ustanova, u 2008. godini njih 47%, svrstana u grupu od 1 do 5 incidenata, što upućuje da velik broj ustanova ima zaštitu. Međutim, uslijed pojave novih vrsta zlonamjernih programa ili način zloupotrebe od strane zaposlenika incidenti se ipak javljaju. U grupi od 6 do 10 sigurnosnih incidenata nalazi se manji broj ustanova (u 2008. godini njih 14%) dok u grupi od 10 i više incidenata prema statistici za 2008. godinu incident je zabilježeno u 13% ustanova. U 2008. godini 26% ustanova se izjasnilo da ne zna koliki se broj sigurnosnih incidenata dogodio u njihovim informacijskim sustavima.

U Tablici 2. prikazane su različite vrste napada na informacijske sustave i incidenti do kojih dovode. Postotak u pojedinoj ćeliji prikazuje koliki je broj ispitanika izjavio da se u njihovoj instituciji dogodila određena vrsta napada, tj. incidenta. Iako je istraživanje provedeno na ograničenom broju ispitanika, podaci vrlo dobro prikazuju stvarnu situaciju. Prema podacima navedenima u tablici vidljivo je da su svega četiri kategorije zabilježile porast:

- neovlašteni pristup, sa 25% u 2007. godini na 29% u 2008. godini,
- krađa/gubitak zaštićenih informacija, sa 8% u 2007. godini na 9% u 2008. godini,
- zlouporaba Internet alata, sa 9% u 2007. godini na 11% u 2008. godini i
- DNS napadi, sa 6% u 2007. godini na 8% u 2008. godini.

Zabilježeni porast je rezultat uvođenja pravila ponašanja, te procedura u izvještavanju o incidentima. U prijašnjim godinama, povećao se broj organizacija koje provode sigurnosnu politiku, stoga je i broj zabilježenih incidenata veći (ali neznatno!).

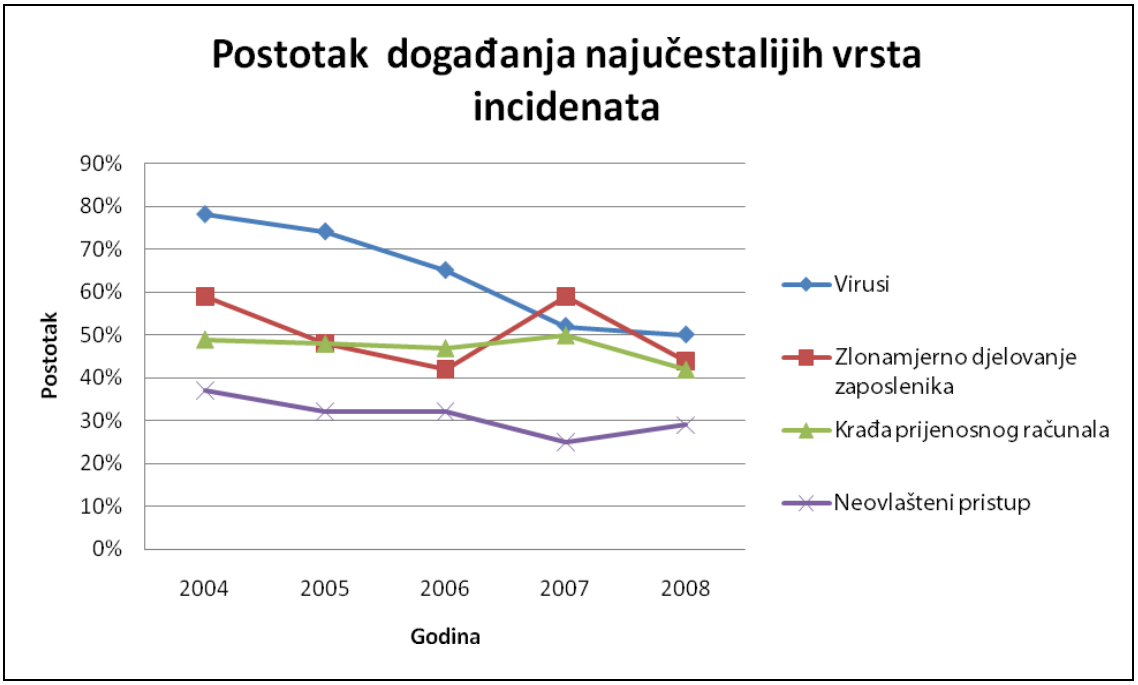
Zanimljivo je spomenuti da od četiri navedene kategorije, unutarnje prijetnje bilježe manji porast (12.4%) u odnosu na porast (21.6%) vanjskih prijetnji (zlouporaba Internet alata i DNS napadi).

	2004	2005	2006	2007	2008
DoS napad	39%	32%	25%	25%	21%
Krađa prijenosnog računala	49%	48%	47%	50%	42%
Telekomunikacijska prijevara	10%	10%	8%	5%	5%
Neovlašteni pristup	37%	32%	32%	25%	29%
Virusi	78%	74%	65%	52%	50%
Financijske prijevare	8%	7%	9%	12%	12%
Zlonamjerno djelovanje zaposlenika	59%	48%	42%	59%	44%
Proboj u sustav	17%	14%	15%	13%	13%
Sabotaža	5%	2%	3%	4%	2%
Krađa/gubitak zakonom zaštićenih informacija	10%	9%	9%	8%	9%
Putem mobilnih telefona	-	-	-	-	4%
Drugim načinima	-	-	-	-	5%
Zloupotreba bežičnih mreža	15%	16%	14%	17%	14%
Mijenjanje izgleda web stranice	7%	5%	6%	10%	6%
Zloupotreba Internet alata	10%	5%	6%	9%	11%
Bot programi	-	-	-	21%	20%
DNS napadi	-	-	-	6%	8%
Zloupotreba programa za komunikaciju	-	-	-	25%	21%
Krađa lozinki	-	-	-	10%	9%
Krađa/gubitak podataka o klijentima	-	-	-	17%	17%
Putem mobilnih telefona	-	-	-	-	8%
Drugim načinima	-	-	-	-	8%

Tablica 2. Prikaz postotka različitih vrsta napada i incidenata

Izvor: CSI Computer Crime and Security Survey

Također, vrijedi spomenuti da se najčešće događaju napadi virusima, zlonamjerno djelovanje zaposlenika, krađa prijenosnog računala i neovlašteni pristup sustavu. Čak 50% ispitanika izjasnilo se kako se u njihovoj ustanovi 2008. godine dogodio sigurnosni incident vezan uz viruse. Druga najučestalija vrsta sigurnosnih incidenata je zlonamjerno djelovanje zaposlenika sa 44%, a slijede krađa prijenosnog računala sa 42% i neovlašteni pristup sustavu sa 29%.



Dijagram 6. Prikaz postotka događanja najučestalijih incidenata

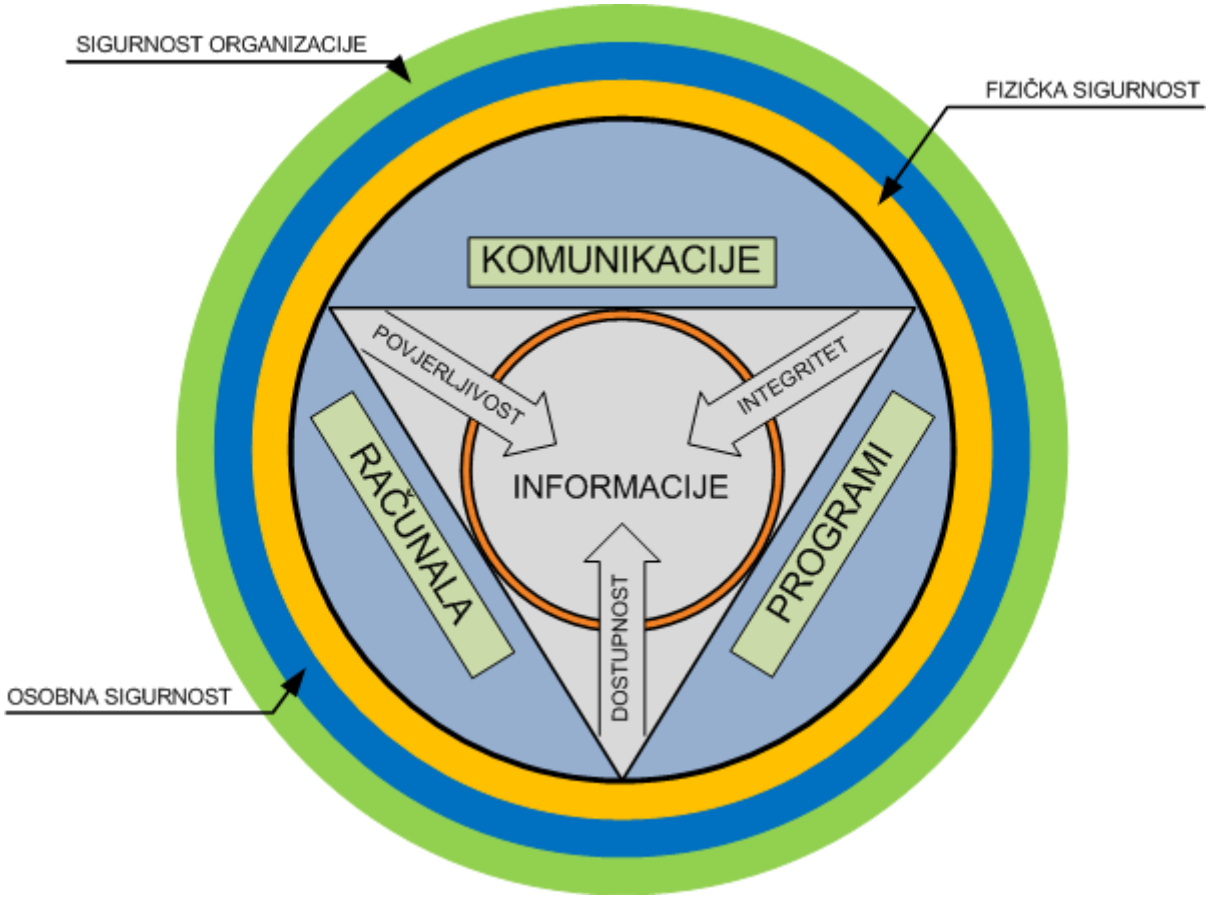
Izvor: CSI Computer Crime and Security Survey

Postotak sigurnosnih incidenata uzrokovanih virusima je u stalnom padu, od 78% u 2004. godini do 50% u 2008. godini. Sigurnosni incidenti uzrokovani zlonamjernim djelovanjem zaposlenika se mijenjaju iz godine u godinu, od 59% u 2004. godini do 44% u 2008. godini. Međutim, broj incidenata uzrokovanih krađom prijenosnih računala se zadržava na otprilike istoj razini, tj. u 2008. godini (42%) bilježi maleni pad u odnosu na 2007. godinu (50%). Zbog neovlaštenog pristupa u 2008. godini 29% ustanova zabilježilo sigurnosni incident.

4. Što štitimo sigurnosnom politikom

Sigurnosnom politikom osiguravaju se tri svojstva informacija koje sadrži neki sustav:

- povjerljivost (*eng. confidentiality*),
- integritet (*eng. integrity*) i
- dostupnost (*eng. availability*).



Dijagram 7. Sigurnosne informacijske komponente - CIA (***C**onfidentiality, **I**ntegrity, **A**vailability*)
Izvor: Wikipedia (*autor: John M. Kennedy T.*)

Da bi se zadovoljili propisani standardi sigurnosti informacijski sustavi dijele se na tri glavna dijela:

- računalnu opremu,
- programe i
- komunikacije.

Jednako tako, kao što je vidljivo na dijagramu 7., mehanizmi zaštite i sprječavanja su podijeljeni na tri osnovne razine:

1. kao prva i najvažnija je fizička sigurnost, pod kojom se smatra sigurnost računalne opreme i podataka,
2. osobna sigurnost je zaštita korisnika i povjerljivih informacija o korisniku i
3. sigurnost organizacije, koja ishodi iz prvih dviju razina.

4.1. Povjerljivost

Povjerljivost je zaštita informacija kod koje je potrebno spriječiti otkrivanje informacija od strane neovlaštenih osoba ili sustava. Ukoliko se informacijama koje su označene kao povjerljive ne rukuje na pravilan način, može doći do povrede povjerljivosti, tj. otkrivanja povjerljivih informacija (usmenim putem, ispisom, kopiranjem, slanjem informacija e-poštom, itd.). Najčešće prijetnje povjerljivim informacija su:

- **napadači** - korištenjem sigurnosnih propusta pokušavaju otkriti povjerljive informacije, zbog vlastite koristi ili kako bi te informacije javno prikazali putem Interneta,
- **lažno predstavljanje** - dobivanje pristupa povjerljivim informacijama putem lozinke drugog korisnika,
- **neovlaštena aktivnost** - korisnik sustava koristi (mijenja, briše, kopira, itd.) podatke za koje nema ovlasti,
- **kopiranje podataka na nezaštićene** lokacije - ugrožavanje povjerljivosti pri kopiranju podataka na sustave s nedovoljnom razinom zaštite,
- **zlonamjerni programi** - programi kojima je moguće ostvariti pristup sustavu koji sadrži povjerljive podatke ili otuđiti povjerljive podatke.

4.2. Integritet

Očuvanje integriteta podataka znači da korisnik podatke ne može izmijeniti bez odobrenja, tj. da su podaci potpuni i ispravni. Od velike je važnosti zaštititi povjerljive podatke od neovlaštenih izmjena, jer se u velikim sustavima često mogu dogoditi namjerni ili nenamjerni slučajevi narušavanja integriteta podataka. Očuvanjem integriteta podataka osigurava se točnost i ispravnost tih podataka, npr. podataka o građanima, platnim listama, itd. Kako bi se očuvao integritet podataka u velikim sustavima, važno je utvrditi identitet korisnika nekom vrstom autentikacije (npr. jednokratnim lozinkama, pametnim karticama, biometrijskim čitačima, itd.). Više o tehnikama autentikacije moguće je saznati u dokumentu „Tehnike generiranja jednokratnih lozinki“ (CCERT-PUBDOC-2009-04-262) objavljenog na službenim stranicama CERT-a.

Također, pri rukovanju podacima potrebno je obratiti oprez kako se ne bi dogodile slučajne izmjene u povjerljivim podacima. Međutim, oprez često nije dovoljan, stoga je potrebno kod rukovanja povjerljivim podacima osigurati strogo povjerljivu okolinu koja umanjuje mogućnost namjernih i nenamjernih izmjena.

4.3. Dostupnost

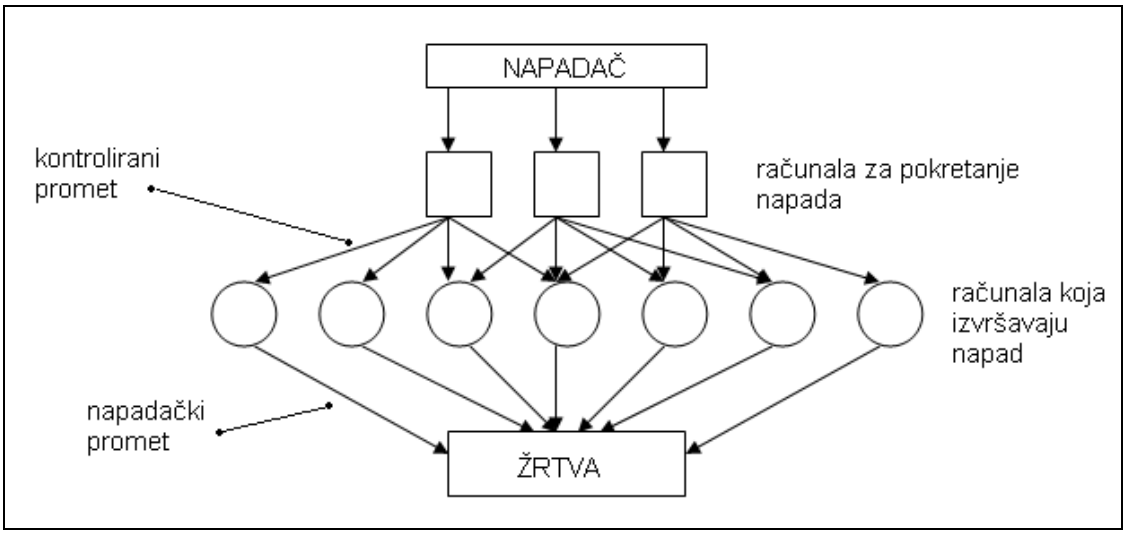
Kako bi informacijski sustav služio svojoj svrsi, sadržane informacije moraju u svakom trenutku biti dostupne. Dostupnost se može definirati kao garancija ovlaštenim korisnicima da će im informacijski sustav biti na raspolaganju kada ga imaju potrebu koristiti. Kako bi informacijski sustav bio dostupan u svakom trenutku podrazumijeva se ispravan rad:

- sustava za pohranu i obradu informacija,
- zaštitnog sustava i
- komunikacijskih veza putem kojih se pristupa informacijama.

Dostupnost informacija najčešće je upitna zbog:

- DoS napada (*eng. Denial of Service attack*) i
- gubitka mogućnosti obrade podataka.

DoS napad, tj. napad uskraćivanjem usluge je svaki napad kojem je cilj onemogućiti korištenje poslužitelja ovlaštenim korisnicima. Jedan od načina DoS napada je da napadač pokušava onesposobiti informacijski sustav na način da sa velikog broja računala informacijskom sustavu šalje veliki broj zahtjeva, što onemogućava informacijski sustav da radi ispravno i ovlaštenim korisnicima onemogućava pristup podacima.



Slika 1. Primjer DoS napada

Izvor: Sigurnosna politika, Damir Kovačević

Napadač putem Interneta uspostavlja izravnu vezu sa računalima za pokretanje napada i preuzima ovlasti nad njima. Nakon preuzimanja računala za pokretanje napada, napadač uspostavlja izravnu vezu sa računalima koja izvršavaju napad i također preuzima ovlasti nad njima. Napadač putem računala za izvršavanje napada poslužitelju istovremeno šalje velik broj zahtjeva, tj. šalje poslužitelju veliku količinu podataka, koje poslužitelj nije u mogućnosti obraditi u normalnom vremenskom roku. Pošto poslužitelj nije u mogućnosti obraditi sve zahtjeve i ne može znati koje je od računala napadač, odbija sve zahtjeve, pa tako i zahtjeve ovlaštenih korisnika. Napadač također može i sa vlastitog računala izvršiti DoS napad. Više o DoS napadima je moguće doznati iz dokumenata „DDoS napad" (CCERT-PUBDOC-2008-09-240) i „Napadi uskraćivanjem resursa" (CCERT-PUBDOC-2006-07-162) objavljenih na službenim stranicama CERT-a.

Gubitak mogućnosti obrade podataka može biti posljedica prirodnih katastrofa ili zlonamjernog djelovanja ljudi na sustav. Prirodne katastrofe uzrokuju prestanak normalnog rada sustava, npr. potresi, požari, poplave, itd. Ljudsko djelovanje, namjerno ili nenamjerno, također može prouzročiti jednaku štetu kao i prirodne katastrofe.

Sigurnosne mjere kojima se osigurava dostupnost su:

- *fizičke mjere* - kojima se uspostavlja provjera pristupa, tj. sprječava se pristup neovlaštenih osoba sklopovlju informacijskog sustava, te drugim sustavima koji kao posljedicu mogu imati nedozvoljenu promjenu u radnom okruženju.
- *tehničke mjere* - kojima se osigurava ispravnost rada cijelog informacijskog sustava. Primjerice, tehnička mjera je zrcaljenje tvrdih diskova čime se osigurava više kopija istih podataka. Ukoliko se dogodi da se jedan od tvrdih diskova pokvari, drugi, identični će preuzeti njegovo mjesto. Također, tehnička mjera je i stalna provjera ispravnosti rada programa, te izrada sigurnosnih kopija u slučaju prestanka napajanja električnom energijom.
- *administrativne mjere* - podrazumijevaju uspostavljanje provjere pristupa, provjere izvršavanja procedura i edukaciju korisnika (koja se pokazuje sve važnijom radi ispravnog korištenja informacija dostupnih u sustavu).

5. Sigurnosni standardi

Kao što je prije napomenuto, pri uspostavi sigurnosne politike organizacije primjenjuju se određeni standardi vezani uz sigurnost informacijskih sustava. Uspostava sigurnosne politike prema raspoloživim standardima osigurava pridavanje pažnje svim aspektima zaštite nekog informacijskog sustava te dokazuje kvalitetu uspostavljenih mjera sigurnosti.

Mjerodavne institucije za izdavanje ovakvih standarda u području zaštite informacijskih sustava su ISO (International Organization for Standardization) i IEC (International Electrotechnical Commission). Standardi iz ISO/IEC 27000 serije organizacijama pružaju smjernice za konstruiranje, primjenu i provjeru informacijskih sustava čime se osigurava povjerljivost, integritet i dostupnost informacijskog sadržaja, sustava i procesa unutar organizacije. Za područje sigurnosti informacijskih sustava najčešće se koriste dva standarda:

- ISO/IEC 27001 i
- ISO/IEC 27002 (prije 2007. godine poznat kao ISO/IEC 17799:2005).

Pri izradi sigurnosne politike preporuča se upotreba oba standarda. U nastavku je pobliže opisan standard ISO/IEC 27001, isto kao i ISO/IEC 27002.

5.1. ISO/IEC 27001

ISO/IEC 27001 standard, punim imenom „ISO/IEC 27001:2005 Informacijske tehnologije - Tehnike zaštite - Specifikacije za sustav upravljanja informacijskim sustavima“ je standard izrađen 2005. godine, a nastao je na temelju standarda BS 7799 (British Standards). Sadašnji standard je pod revizijom, jer su se donošenjem novih standarda iz iste ISO/IEC 27000 serije, neka pravila preklopila. Kako bi se izbjegle zabune, očekuje se da će ISO i IEC 2010. godine izdati ispravljeni standard.

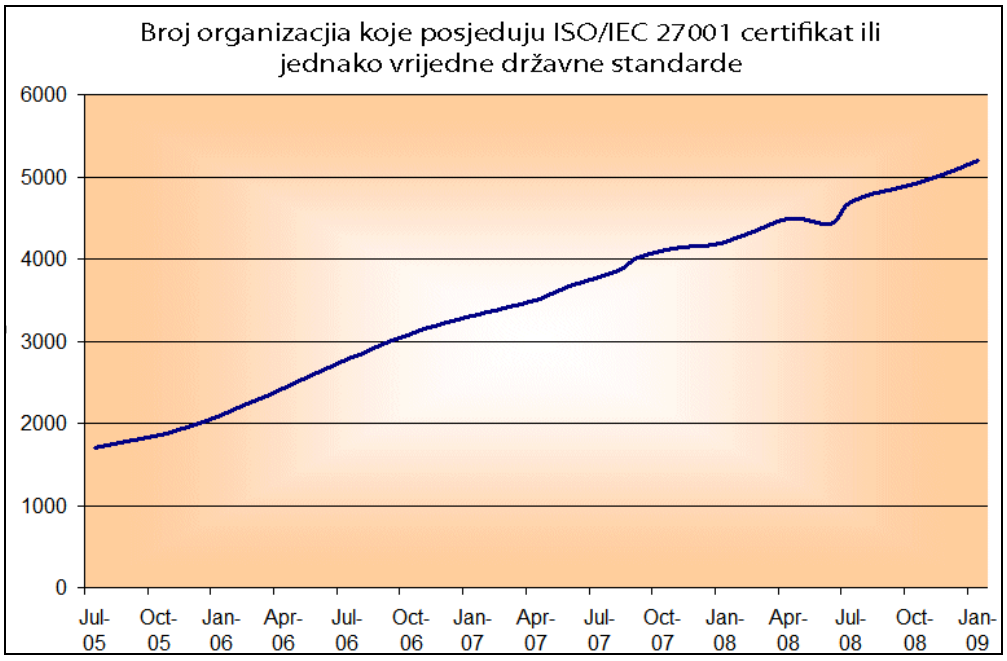
ISO/IEC 27001 je službena skupina specifikacija na temelju kojih organizacije imaju pravo zatražiti postupak certifikacije, naravno ukoliko su primijenile taj standard na sustav upravljanja sigurnošću informacija. Ovaj standard propisuje zahtjeve za uspostavljanje, provođenje, nadgledanje, ispitivanje, održavanje i poboljšanje sustava za upravljanje sigurnošću informacija. Standard je primjenjiv na sve vrste organizacija (komercijalne, neprofitne, državne institucije, itd.) i sve veličine organizacija, od malih pa do velikih svjetskih organizacija.

Standard se sastoji od 5 dijelova:

1. Sustav za zaštitu informacija
2. Odgovornost rukovodećih ljudi
3. Unutarnje provjere sustava za zaštitu informacija
4. Provjera valjanosti sustava za zaštitu informacija
5. Poboljšanja na sustavu za zaštitu informacija

U standardu su također navedeni ciljevi provjere koje je potrebno ostvariti i provjere koje je potrebno provesti kako bi se ostvarili ti isti ciljevi.

Postoji veliki broj ustanova ovlaštenih za certifikaciju prema ISO/IEC 27001 standardu, ali također i velik broj organizacija koje su certificirale svoje informacijske sustave prema ISO/IEC 27001 standardu ili jednako vrijednim standardima pojedine države. Certifikacija je stvar izbora organizacije, ali vrijedi spomenuti da poslovni partneri ponekad traže da organizacija s kojom surađuju ima certifikat. U nastavku se nalazi grafički prikaz broja organizacija koji posjeduje ISO/IEC 27001 certifikat ili jednako vrijedne državne certifikate u vremenskom razdoblju od lipnja 2005. godine do siječnja 2009. godine.



Dijagram 8. Prikaz broja certificiranih organizacija

Izvor: ISO27001 Security

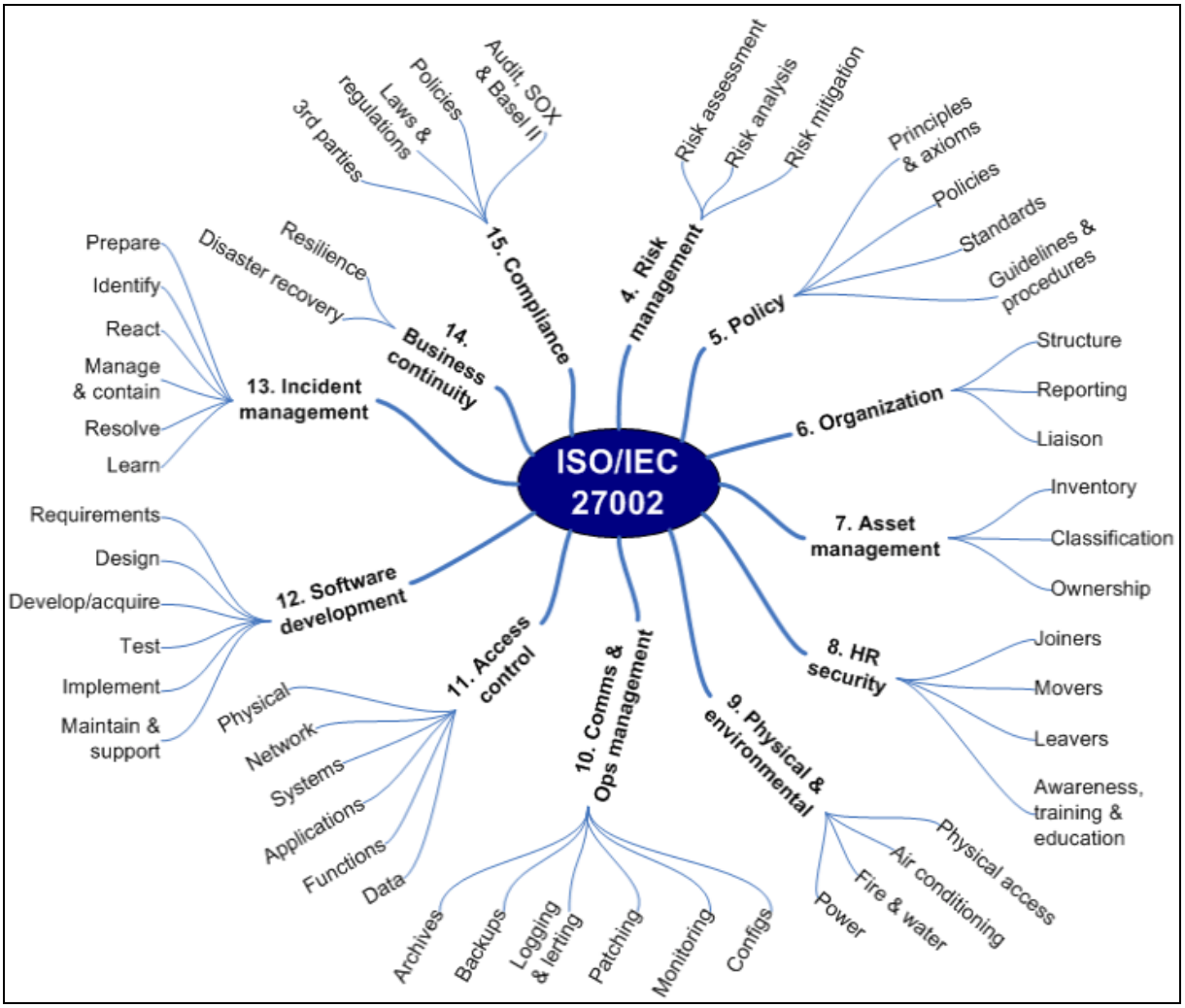
5.2. ISO/IEC 27002 (ISO/IEC 17799)

ISO/IEC 27002 standard također je nastao na temelju BS 7799 standarda. ISO/IEC 27001 standard definira koje zahtjeve neki sustav za zaštitu informacija mora imati, te za primjerene provjere navodi uporabu ISO/IEC 27002 standarda. ISO/IEC 27002 jest službeni standard, ali bolje ga je protumačiti kao skup smjernica koje je moguće upotrijebiti. Trenutačno je također pod revizijom, kako bi se čim bolje u budućnosti mogao primijeniti sa izmijenjenim standardom ISO/IEC 27001. Standard sadrži 39 ciljeva što ga čini vrlo detaljnim i temeljitim.

Standard se sastoji od 12 dijelova:

1. *Procjena rizika* - organizacija mora na temelju zahtjeva odrediti koje su moguće prijetnje informacijskom sustavu
2. *Sigurnosna politika* - rukovodeći ljudi organizacije bi trebali odrediti skup pravila i zahtjeva kako bi se stekla jasna vizija o dozvoljenim i nedozvoljenim radnjama
3. *Organizacija informacijske sigurnosti* - rukovodeći ljudi organizacije bi trebali odrediti ljude odgovorne za provođenje primjerene zaštite informacija, kako zaštite od unutarnjih, tako i od vanjskih prijetnji
4. *Upravljanje imovinom* - organizacija mora biti svjesna koliko su vrijedne informacije koje posjeduje, te znati njima ispravno raspolagati
5. *Zaštita od zaposlenika* - organizacija mora postaviti i dodijeliti potrebnu razinu pristupa svakom zaposleniku, među zaposlenicima uspostaviti određenu razinu svijesti, te ih primjereno obrazovati
6. *Fizička zaštita i zaštita od okoline* - vrijedna računalna oprema mora biti fizički zaštićena od zlonamjernih ili nenamjernih oštećenja i gubitaka
7. *Upravljanje komunikacijama i operacijama* - uspostavljanje sigurnosnih provjera za sustave i mrežnu komunikaciju
8. *Provjera pristupa* - pristup računalima, mreži i podacima mora biti pod nadzorom kako bi se spriječilo neovlašteno korištenje
9. *Nabava, razvoj i održavanje informacijskih sustava* - potrebno je odrediti specifikacije opreme koju je potrebno nabaviti, smjer mogućeg razvoj informacijskog sustava, te primjeren način održavanja kako ne bi došlo do gubitka ili oštećenja

10. *Upravljanje incidentima u informacijskom sustavu* - sigurnosne incidente koji su se dogodili potrebno je odmah prijaviti nadležnoj ustanovi, te voditi računa o upravljanju sustavom ukoliko se sigurnosni incident dogodi
11. *Upravljanje poslovnim kontinuitetom* - potrebno je provesti analizu utjecaja informacijskog sustava na kontinuirano poslovanje organizacije kako bi se umanjila šteta nastala sigurnosnim incidentom
12. *Usklađivanje* - informacijski sustav potrebno je uskladiti sa propisanim standardima i zakonima



Slika 2. Prikaz strukture ISO/IEC 27002 standarda

Izvor: ISO27001 Security

Svaki od dijelova sadrži određeni broj glavnih sigurnosnih kategorija, a pod sigurnosnim kategorijama navodi se cilj provjere koji je potrebno ostvariti i provjere koje je moguće primijeniti radi ostvarivanja cilja. ISO/IEC 27002 sadrži prijedloge ustroja sustava za zaštitu informacija isto kao i sustava provjere. U standardu nije naglašeno koje specifične sigurnosne provjere je potrebno raditi, već samo kako sustav za upravljanje mora funkcionirati jer:

- od svake organizacije se očekuje da provede detaljnu procjenu rizika kako bi se odredile specifične potrebe prije odabira sustava provjere,
- nemoguće je nabrojati sve moguće provjere u standardu za opću primjenu.

6. Opis procesa uspostave sigurnosne politike

Organizacija može svoju sigurnosnu politiku temeljiti na unaprijed izrađenim standardima, čime se uvelike smanjuju operativni troškovi i vrijeme potrebno za provedbu sigurnosne politike. Također, sigurnosnu politiku organizacije moguće je izraditi samostalno, procjenom mogućih prijetnji informacijskom sustavu, te procjenom i zaštitom slabih točki sustava. Ovaj je proces dakako dugotrajniji i skuplji, ali osigurava način zaštite koji potpuno odgovaraju potrebama organizacije. Iako se na prvi pogled samostalna izrada sigurnosne politike čini kao bolje rješenje, preporuča se izrada sigurnosne politike organizacije na temelju standarda kako bi se pri uspostavi sigurnosne politike obratila pažnja na sve moguće prijetnje koje mogu ugroziti informacijski sustav.

Kao što je u prethodnom poglavlju naznačeno, sigurnosna politika organizacije može se temeljiti na ISO/IEC 27001 standardu. Međutim, potrebno je spomenuti da ISO/IEC 27001 standard opisuje sve *što* je potrebno napraviti, ali ne i *kako* je potrebno napraviti. Da bi se odgovorilo na pitanje *kako* se koristi standard ISO/IEC 27002 (koji daje potrebne smjernice), razrađen je upravo primjer sigurnosne politike na temelju tog standarda. Kako bi se jasnije dočarao sam pojam sigurnosne politike u nastavku će biti opisan proces uspostave sigurnosne politike, koraci i postupci koje je potrebno napraviti.

6.1. Procjena rizika

Procjena rizika je vrlo važan faktor pri uspostavi sigurnosne politike. Bez procjene rizika organizacija može uvesti sigurnosnu politiku sa sasvim općenitim pravilima, koji ne uzimaju u obzir moguće rizike specifične za područje djelatnosti. Međutim, organizacija može definirati sigurnosnu politiku detaljno ili manje detaljno, samo je pitanje na koju će se razinu sigurnosti informacijskog sustava odlučiti.

Procjena rizika se sastoji se od:

- otkrivanja općenitih prijetnji,
- otkrivanja specifičnih prijetnji,
- otkrivanja potrebne razine zaštite i
- usklađivanja potrebne razine zaštite sa mogućnostima.

6.2. Sigurnosna politika

Sigurnosnom politikom uspostavlja se niz pravila i smjernica dobivenih od strane rukovodećih ljudi neke organizacije kako bi se osigurala povjerljivost, integritet i dostupnost informacija. Kako bi sigurnosna politika bila učinkovita potrebno ju je primijeniti na svaki dio organizacije.

6.2.1. Dokument sigurnosne politike

Dokument sigurnosne politike je službeni dokument organizacije i moraju ga odobriti vodeći ljudi unutar te organizacije. Dokument je potrebno objaviti i poslati svim zaposlenicima i korisnicima kojima je namijenjen. Sigurnosnu politiku potrebno je napisati kako bi bila razumljiva svim stranama kojih se tiče. Dokument sigurnosne politike mora sadržavati:

- definicije sigurnosti informacija, ciljeve i opseg te važnost sigurnosti,
- stavove rukovoditelja kojima se podržavaju ciljevi i principi informacijske sigurnosti,
- okvire uspostave ciljeva i provjera,
- objašnjenje sigurnosne politike, načela i standarda,
- suglasnost sa zakonodavnim, nadzornim i ugovornim zahtjevima,
- zahtjeve o educiranju po pitanju sigurnosti,
- posljedice nepridržavanja pravila sigurnosne politike,
- definicije općih i specifičnih odgovornosti rukovoditelja informacijske sigurnosti i
- reference na literaturu koja podržava uvedenu sigurnosnu politiku.

6.2.2. Provjera sigurnosne politike

Pojavom novih prijetnji informacijskim sustavima, ugradnjom nove opreme u informacijski sustav, te drugim radnjama mijenjaju se parametri na kojima je uspostavljena sigurnosna politika. Kako bi postojeća sigurnosna politika bila jednako učinkovita kao i u trenutku kada je uvedena, potrebno je uzeti u obzir promjene koje su se dogodile, te prilagoditi pravila i procedure. Međutim, nastale promjene nisu nužan uvjet za poboljšanje sigurnosne politike. Sigurnosnu politiku potrebno je prilagođavati na godišnjoj bazi čak i ako se niti jedan parametar u okruženju organizacije nije promijenio jer je moguće da uvedena sigurnosna politika ne odgovara organizaciji u potpunosti. Provjeru sigurnosne politike preporučeno je izvoditi u razmaku od godinu dana, ali u slučaju incidenata, otkrivanja ranjivosti i ugradnje nove opreme čak i češće. Provjera sigurnosne politike ne uvjetuje nužno i promjenu, ali je potrebno uzeti nove okolnosti u obzir kako bi informacijski sustav bio primjereno zaštićen.

Neke od činjenica koje treba uzeti u obzir pri provjeri sigurnosne politike su:

- rezultati neovisnih ispitivanja,
- promjene koje mogu pozitivno utjecati na sigurnost informacija,
- promjene vezane uz ranjivosti i prijetnje informacijskim sustavima,
- izvješća o sigurnosnim incidentima i
- preporuke stručnih organizacija.

6.3. Organizacija informacijske sigurnosti

Pri organizaciji informacijske sigurnosti potrebno je jasno odrediti sve odgovornosti u informacijskoj sigurnosti u skladu s sigurnosnom politikom. Rukovodeći ljudi organizacije trebaju podržavati učinkovito provođenje sigurnosne politike, te na propisan način kažnjavati one koji krše pravila. Također je bitno ispravno koordinirati zaposlenike kako bi provedba sigurnosne politike bila uspješna. Daljnji koraci koji se poduzimaju pri organizaciji informacijske sigurnosti su:

- *proces autorizacije* - odnosi se na procjenu razine sigurnosti nekog dijela opreme, npr. prijenosnog računala.
- *ugovor o povjerenju* - popisivanje vrijednosti koje organizacija posjeduje na način da se svako korištenje dokumentira s ciljem zaštite vrijednosti od kopiranja, uništavanja i zamjene od strane zaposlenika, partnera ili treće strane.
- *savjeti stručnjaka za informacijsku sigurnost* - potrebno je savjetovati se sa organizacijama koje se bave računalnom sigurnosti kako bi se u slučaju sigurnosnih incidenata dobili primjereni savjeti i smjernice koje upućuju kako djelovati.
- *suradnja s drugim organizacijama* - održavanje kontakta sa drugim organizacijama zbog unaprjeđenja znanja o sigurnosti informacijskih sustava ili brzih obavijesti u slučaju sigurnosnog incidenta.
- *provjera sigurnosti sustava* - potrebno je redovito provjeravati sigurnost informacijskog sustava zbog osiguranja da sustav zaštite ispravno funkcionira.
- *sigurnost pristupa treće stane* - održati jednaku razinu sigurnosti i kod informacija kojima treća strana ima pristup.
- *identifikacija rizika kod pristupa treće strane* - prije dodjele prava pristupa trećoj strani potrebno je provjeriti moguće rizike kako bi se moglo informacijski sustav primjereno zaštititi.
- *zahtjevi sigurnosti u ugovorima s trećom stranom* - ukoliko postoji dogovor sa trećom stranom koja ima pristup informacijskom sustavu, potrebno je formalnim dokumentom odrediti pravila zaštite koja su u skladu sa sigurnosnom politikom organizacije.

6.4. Upravljanje imovinom

Kako bi se osigurala zaštita imovine organizacije potrebno je provesti sljedeće korake:

- *popis imovine* - identifikacija imovine organizacije u svrhu procjene vrijednosti i važnosti, te shodno tome primjerene razine zaštite.
- *vlasništvo nad imovinom* - kako ne bi došlo do mijenjanja ili otuđivanja imovine, potrebno je odrediti vlasnika, tj. osobu odgovornu za sigurnost i zaštitu imovine.
- *prihvatljivo korištenje imovine* - definiranje jasnih pravila ispravnog korištenja imovine kako ne bi došlo do gubitke informacija ili sigurnosnog incidenta.
- *klasifikacija informacija* - primjena odgovarajuće razine zaštite na informacije.
- *smjernice za klasifikaciju* - klasifikacija se izvodi na temelju vrijednosti, osjetljivosti, važnosti za organizaciju i zakonodavnih zahtjeva.
- *označavanje i rukovanje informacijama* - definiranje procedura za označavanje i rukovanje informacijama, npr. procedure za kopiranje, pohranu, prijenos, itd.

6.5. Zaštita od zaposlenika

Zaposlenici često rade nesvjesne greške, ali jednako tako i svjesne zlonamjerne radnje. Kako bi se zaštitile informacije i imovina organizacije potrebno je uzeti u obzir sljedeće stavke:

- *uloge i odgovornosti* - potrebno je definirati uloge i odgovornosti zaposlenika, ugovornih djelatnika i treće strane.
- *provjera* - provjeravaju se potencijalni zaposlenici, ulagači ili poslovni partneri kako bi se povećala sigurnost informacijskog sustava.
- *uvjeti zaposlenja* - prije zapošljavanja ili ugovaranja posla sa ulagačima ili trećom stranom potrebno je u ugovor uključiti dio koji sve strane obvezuje na poštivanje sigurnosne politike organizacije.
- *odgovornosti rukovoditelja* - informiranje zaposlenika o ulogama i odgovornostima u provedbi sigurnosti
- *edukacija o informacijskoj sigurnosti* - zaposlenika ili treće strane kako bi se postigli zadovoljavajući rezultati, tj. kako bi svi bili svjesni važnosti zaštite informacijskog sustava
- *raskid ugovora* - potrebno je jasno definirati procedure koje je potrebno izvršiti po raskidu radnog odnosa, ili ugovora, tj. odrediti pravila o vraćanju sve imovine organizacije koja je zaposleniku dana na korištenje, ukidanje prava pristupa informacijskom sustavu, itd.

6.6. Fizička zaštita i zaštita od okoline

Cilj definiranja ovog poglavlja unutar sigurnosne politike je sprječavanje nastanka fizičke štete od stane zaposlenika ili bilo kojeg pojedinca koji je s organizacijom potpisao ugovornu obavezu. Potrebno je odrediti sljedeće:

- *područje fizičke zaštite* - dijelovi organizacije koji sadrže povjerljive informacije moraju biti zaštićeni nekom vrstom prepreke, npr. zidovima, vratima, autentikacijskim spravama, itd,
- *fizička provjera ulaska* - kako bi se osiguralo da pravo pristupa određenim prostorijama unutar organizacije imaju samo ovlaštene osobe potrebno je postaviti odgovarajuće metode provjere ulaska,
- *sigurnost opreme* - kako ne bi došlo do gubitaka, štete ili prekida poslovnih aktivnosti potrebno je osigurati primjerenu zaštitu vrijednostima organizacije,
- *smještaj i zaštita opreme* - opremu je potrebno primjereno smjestiti u skladu sa uputama proizvođača opreme,
- *sigurnost instalacija* - kako ne bi došlo do oštećenja informacijskog sustava potrebno je voditi računa o ispravnosti instalacija u prostorijama organizacije,
- *sigurnost kod kabliranja* - kablovi za opskrbu električnom energijom ili telekomunikacijski kablovi moraju biti primjereno zaštićeni u skladu s propisima i

- *održavanje opreme* - potrebno je redovito održavati opremu prema uputama proizvođača, a održavanje smiju raditi samo ovlaštene osobe.

6.7. Upravljanje komunikacijama i operacijama

Komunikacije i operacije (aktivnosti) organizacije su vrlo važni procesi. Stoga je potrebno jasno definirati pravila upravljanja komunikacijama i operacijama. Područja koja je potrebno obraditi su:

- *procedure rada i odgovornosti* - potrebno je odrediti procedure i odgovornosti za ispravno upravljanje i rad jedinica za obradu informacija čime se smanjuje rizik od namjerne i nenamjerne greške,
- *dokumentirane procedure rada* - operativne procedure moraju biti dokumentirane, održavane i dostupne svim korisnicima kojima su potrebne,
- *nadzor promjena u operativnim sustavima i objektima* - promjene vezane uz objekte i sustave moraju biti provjerene,
- *odvajanje dužnosti* - postupak odvajanja obveza i odgovornosti zaposlenika kako bi se mogućnosti obavljanja neovlaštenih i neželjenih radnji svele na minimum,
- *razdvajanje objekata za razvoj, ispitivanje i operativni rad* - potrebno je odvojiti razvojne i aktivnosti vezane za ispitivanje, isto kao i aktivnosti vezane uz operativni rad. Npr. program koji se provjerava ili razvija može biti opasan za ispravno funkcioniranje informacijskog sustava, pa je potrebno odvojiti sustave na kojima se obavlja razvoj i ispitivanje od onih na kojima se radi,
- *planiranje i prihvaćanje sustava* - radi osiguranja dostupnosti potrebnih kapaciteta te računalnih i drugih resursa,
- *zaštita od zlonamjernih programa* - potrebno je uvesti zaštitu koja će odgovorne ljude u organizaciji upozoriti da je informacijski sustav ugrožen zlonamjernih programom kako bi se zaštitio integritet podataka,
- *provjere protiv zlonamjernih programa* - ugraditi određene alate i mjere koji će redovito pregledavati da li u sustavu postoje zlonamjerni programi,
- *izrada sigurnosnih kopija* - potrebno je redovito izrađivati sigurnosne kopije podataka radi očuvanja integriteta i dostupnosti istih,
- *upravljanje sigurnošću mrežnog sustava* - potrebno je osigurati zaštitu informacija koje mrežni sustav sadrži, te zaštititi sam mrežni sustav,
- *rukovanje i sigurnost medija* - potrebno je uspostaviti procedure za zaštitu dokumenata, računalnih medija i dokumentacije od krađe, neovlaštenog pristupa, uništavanja, itd.,
- *upravljanje prijenosnim medijima* - uspostava pravila za rukovanje prijenosnim medijima i podacima koje sadrže,
- *uklanjanje medija* - ukoliko više nisu potrebni, medije se može uništiti, ali na ispravan način kako treća strana ne bi otkrila informacije koje medij sadrži,
- *procedure za rukovanje informacijama* - odrediti pravila za ispravno rukovanje informacijama kako bi se zaštitile od neovlaštenog otkrivanja i zloupotrebe,
- *razmjena informacija* - osigurati zaštitu pri razmjeni podataka i programa unutar organizacije ili izvan nje i
- *nadgledanje* - kako bi se pravovremeno uočile neovlaštene aktivnosti.

6.8. Provjera pristupa

Važno je odrediti koji će korisnik imati pristup određenim informacijama. Stoga je potrebno definirati sljedeće:

- *provjera pristupa u skladu s poslovnim zahtjevima* - pristup informacijama treba odgovarati zahtjevima poslovnih dužnosti kako bi se spriječilo neovlašteni pristup podacima,
- *politika provjere pristupa* - potrebno je uspostaviti niz pravila kojima će se odrediti razine pristupa zaposlenika,
- *upravljanje pristupom korisnika* - kako bi se spriječio neovlašteni pristup informacijama,

- *registracija korisnika* - uspostavljanje formalnog registracijskog postupka radi dobivanja prava pristupa višenamjenskim informacijskim sustavima,
- *upravljanje privilegijama* - potrebno je odrediti razinu privilegija u informacijskom sustavu koju je potrebno osigurati pojedinom zaposleniku,
- *upravljanje korisničkim lozinkama* - potrebno je izraditi formalnu izjavu kojom se korisnici obvezuju da dobivene lozinke čuvaju tajnima, te zabranu odavanja lozinke tijekom bilo kakvog oblika komunikacije (e-mailom, telefonom, pismeno),
- *odgovornost korisnika* - potrebno je potaknuti svijest korisnika o odgovornosti vezanoj uz lozinke i opremu koja im je dana na korištenje radi smanjenja mogućnosti neovlaštenog pristupa,
- *provjera pristupa mreži* - potrebno je uspostaviti provjeru mrežnih servisa i usluga kako bi se zaštitio mrežni sustav od nedozvoljenih aktivnosti,
- *provjera pristupa operacijskom sustavu* - kako bi se spriječio neovlašteni pristup računalnim resursima potrebno je uspostaviti sigurnosne mehanizme unutar operativnog sustava,
- *praćenje pristupa i korištenja sustava* - kako bi se pravovremeno uočili pokušaji nedozvoljenih aktivnosti potrebno je dokumentirati i provjeriti pristup te korištenje sustava,
- *bilježenje događaja* - u slučaju pojave sigurnosnog incidenta potrebno je bilježiti prethodne aktivnosti u sustavu kako bi se moglo odrediti što se zapravo dogodilo i
- *praćenje uporabe sustava* - kako bi se osiguralo da korisnici sustava izvode samo one aktivnosti za koje su ovlašteni potrebno je pratiti koliko i kako ga koriste.

6.9. Razvoj i održavanje sustava

Kako bi se osigurala primjerena i ispravna oprema, informacijski je sustav potrebno održavati. Također je potrebno definirati sve sigurnosne zahtjeve koji se nameću, uključujući niz postupaka za slučaj sigurnosnih incidenata. Sve zahtjeve je potrebno dokumentirati.

Provjerom ulaznih podataka moguće je spriječiti namjerno ili nenamjerno unošenje netočnih podataka. Provjera se može provoditi uzimajući u obzir:

- nedozvoljene vrijednosti,
- nedopuštene znakove u pojedinim poljima,
- nepotpune podatke ili
- prekoračenje količine podataka za unos.

Najvažnija kategorija koju ovo poglavlje obuhvaća je svakako provjera i održavanje operativnog dijela sustava od kojeg se zahtjeva neprekidan i ispravan rad.

6.10. Upravljanje incidentima u informacijskom sustavu

Svrha ovog poglavlja je dati smjernice na koji način u slučaju sigurnosnog incidenta brzo i učinkovito djelovati. Također, potrebno je sve zaposlenike educirati kako bi znali prepoznati da se radi o nekoj vrsti sigurnosnog incidenta, te da odmah upozore nadležne. Definirani su sljedeći koraci:

- *prijava sigurnosnih incidenata* - sigurnosni incident potrebno je prijaviti prema unaprijed određenoj proceduri u što kraćem vremenskom roku,
- *prijava ranjivosti sustava* - po otkrivanju sigurnosnog propusta u informacijskom sustavu potrebno je prijaviti ranjivost u što kraćem vremenskom roku,
- *upravljanje sigurnosnim prijavama* - potrebno je unaprijed definirati procedure u slučaju sigurnosnih incidenata ili ranjivosti kako bi se u što kraćem vremenskom roku iste mogle riješiti i
- *odgovornosti i procedure* - potrebno je definirati procedure koje će obuhvatiti različite vrste učestalih sigurnosnih incidenata, postupke koji će sustav zaštititi od ponavljanja istog sigurnosnog incidenta, te pohraniti i zaštititi dokumentaciju o incidentu kako bi se npr. otkrilo napadača ili kako bi se upotrijebila kao dokaz u sudskom postupku.

6.11. Upravljanje poslovnim kontinuitetom

Uslijed prekida rada u informacijskom sustavu, organizacija može doživjeti znatne financijske gubitke. Stoga je vrlo važno odrediti:

- *proces upravljanja kontinuitetom poslovanja* - organizacija se mora suočiti s rizicima poslovanja i biti spremna primjereno reagirati ukoliko se dogodi incident koji može uzrokovati zastoj u poslovanju,
- *kontinuitet poslovanja i analiza učinka* - potrebno je identificirati i analizirati događaje, tj. incidentne situacije, koji mogu prekinuti poslovni proces te definirati plan za kontinuirano poslovanje organizacije,
- *ispitivanje i održavanja* - potrebno je kontinuirano provoditi ispitivanja kako bi se pravovremeno otkrili propusti uslijed promjena u sustavu,
- *identifikacija rizika* - potrebno je odrediti potencijalne prijetnje informacijskom sustavu organizacije,
- *analiza rizika* - potrebno je odrediti koje je mjere moguće primijeniti kako bi se smanjili rizici kojima je izložen informacijski sustav,
- *prirodne katastrofe* - primjena provjera za minimiziranje štete nastale prirodnim katastrofama (potresi, poplave, požari, itd.) i
- *korisnici* - potrebno je poduzeti sve mjere zaštite i opreza kako korisnici sustava ne bi mogli uzrokovati prestanak ispravnog rada informacijskog sustava.

6.12. Usklađivanje

Važno ja da su sigurnosna politika i pravila koja se primjenjuju na informacijski sustav neke organizacije usklađena sa zakonskim i ugovornim zahtjevima. Stoga je potrebno uspostaviti pravila vezana uz:

- *intelektualno vlasništvo, autorska prava* - potrebno je definirati odgovarajuća pravila koja će biti u skladu sa zakonskim odredbama koje su vezane uz ugovore o intelektualnom vlasništvu i autorskim pravima,
- *čuvanje zapisa organizacije* - zapise je potrebo primjereno zaštititi od gubitka, oštećenja i krivotvorenja,
- *sprječavanje zlouporabe uređaja za obradu informacija* - korištenje računalnih resursa u neposlovne ili neovlaštene svrhe potrebno je dokumentirati kao neprikladno i
- *nadgledanje korisnika* - ukoliko zakon tako nalaže, korisnike je potrebno izvijestiti o pravilima o nadgledanju.

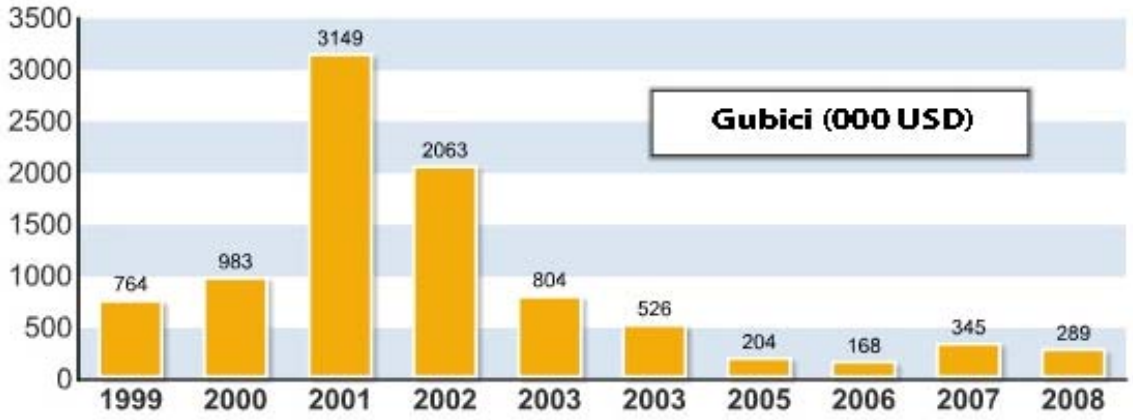
7. Važnost sigurnosne politike

Kao što je vidljivo iz statističkih podataka navedenih u poglavlju 3 uspostava nekog oblika sigurnosne politike u svakoj organizaciji je postala preporučljiva. Međutim, unatoč ispravnom provođenju sigurnosne politike sigurnosni incidenti se događaju. Materijalna, intelektualna ili druga šteta nastala incidentom poprima velike razmjere i ozbiljno ugrožava stabilno poslovanje organizacije.

Velike tvrtke često dožive sigurnosne incidente, bilo zbog materijalne koristi ili narušavanja poslovanja krađom povjerljivih podataka. Tvrtke koje svoje informacijske sustave ne zaštite sukladno rizicima koji im prijete vrlo su česta meta napadačima ili zlonamjernim zaposlenicima. U današnjici, tvrtke se bore za tržišne pozicije, stoga im gubitak podataka(npr. podataka o novom proizvodu) može ozbiljno naštetiti. Uvođenjem i provođenjem sigurnosne politike tvrtke osiguravaju zaštitu podataka na primjeren način, a u slučaju incidenta imaju pravo na zakonski progon izvršitelja ukoliko je to sigurnosnom politikom definirano.

Institucije koje imaju velike baze povjerljivih podataka moraju na primjeren način zaštititi podatke jer u protivnom osobe čiji se podaci nalaze u bazi mogu doživjeti financijsku štetu, krađu identiteta, te cijeli niz neugodnosti ukoliko povjerljive informacije dospiju u krive ruke. Uspostava sigurnosne politike smanjuje mogućnost otkrivanja povjerljivih podataka, ali i uspostavlja strogi nadzor nad svakim područjem djelatnosti organizacije.

U svrhu prikazivanja važnosti uspostave sigurnosne politike u organizaciji, još jednom se vrijedi pozvati na „CSI Computer Crime and Security Survey" izvješće iz 2008. godine u kojem je naznačeno kako je prosječni gubitak uzrokovan sigurnosnim incidentima u 2008. godini iznosio gotovo 1.550.000 kn (289.000 USD) što predstavlja iznos koji bi velik broj tvrtki doveo u neugodnu poziciju. U 2008. godini je zabilježen pad prosječnog gubitka uzrokovanog sigurnosnim incidentima u odnosu na 2007. godinu kada je iznosio 1.850.000 kn (345.000 USD. Iz prethodno navedenih statističkih podataka vidljivo je da je uspostavom sigurnosne politike u nekoj organizaciji smanjen broj incidenata, pa su stoga i nastale štete smanjene za određen iznos.



Dijagram 9. Prikaz iznos prosječnog gubitka uzrokovanog sigurnosnim incidentom

Izvor: CSI Computer Crime and Security Survey

Gornji prikaz vrlo dobro ukazuje na važnost uspostave sigurnosne politike u organizaciji, međutim financijski gubici ne trebaju biti jedini pokazatelj.

8. Zaključak

Svakim danom javlja se sve veći broj potencijalnih prijetnji, kako za korisnike osobnih računala, tako i za velike informacijske sustave. Zaštita podataka nužna je u bilo kojem okruženju pa je zato potrebno primijeniti odgovarajuće mjere zaštite. Kroz vrijeme se pokazalo da zaštita uobičajenim alatima većinom nije dovoljna kako bi se spriječilo nanošenje štete. Informacijski sustavi sadrže veliku količinu povjerljivih podataka, npr. podaci o građanima, bankovnim računima, tvrtkama, proizvodima, itd.

Iz statističkih podataka navedenih u dokumentu vidljivo je da se sigurnosni incidenti sve češće događaju od strane zaposlenika što ukazuje da je potrebno uvesti niz učinkovitih i jasno određenih pravila koja će osigurati i zaštititi materijalne i intelektualne vrijednosti organizacije od krađe, uništavanja i krivotvorenja. Iz navedenog primjera uspostave sigurnosne politike vidljivo je da je potrebno obratiti pažnju na svaki dio zaštite informacijskog sustava. Sigurnosna politika mora biti dokument prilagođen specifičnim potrebama organizacije i ne mora nužno sadržavati sve stavke iz ISO/IEC 27002 standarda. Navedene stavke samo su smjernice koje upućuju do koje razine sigurnosna politika može, a u nekim slučajevima i mora biti razrađena.

Razmatranjem potencijalnih prijetnji svaka će organizacija doći do jednakog zaključka - podatke je potrebno zaštititi. Međutim, uvođenje sigurnosne politike može biti skup i dugotrajan proces u kojem je potrebno prilagoditi sve dijelove organizacije da rade sinkronizirano. Usporedbom uloženog i dobivenog, rezultat je sasvim jasan, sigurnosna politika je dobro ulaganje. Tvrtkama i institucijama preporuča se uvođenje sigurnosne politike radi podizanja razine sigurnosti kako informacijskog sustava, tako i korisnika istog.

9. Reference

[1] Sigurnosna politika, http://os2.zemris.fer.hr/ISMS/2008_kovacevic/sigurnostIS.html, veljača 2008.

[2] Michele D. Guel: Kratak udžbenik za razvijanje sigurnosne politike, http://www.sans.org/resources/policies/Policy_Primer.pdf, 2007.

[3] S. Gerić, Ž. Hutinski: Information System Security Threats Classifications, Sveučilište u Zagrebu, Fakultet organizacije i informatike, Varaždin, 2007.

[4] CSI/FBI Computer Crime and Security Survey 2004

[5] R. Richardson: CSI Computer Crime and Security Survey, 2008.

[6] ISO 27001 Security, http://www.iso27001security.com/, svibanj 2009.

[7] Standardi iz serije ISO/IEC 27000, http://en.wikipedia.org/wiki/ISO/IEC_27000-series, svibanj 2009.

[8] ISO/IEC 27001 standard, http://en.wikipedia.org/wiki/ISO_27001, svibanj 2009.

[9] ISO/IEC 27002 standard, http://en.wikipedia.org/wiki/ISO_17799, svibanj 2009.