INFORMACIJSKA SIGURNOST U POSLOVNIM ORGANIZACIJAMA

Badžim, Antonio

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, Faculty of economics Split / Sveučilište u Splitu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:124:592683

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

REFST - Repository of Economics faculty in Split

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

INFORMACIJSKA SIGURNOST U POSLOVNIM ORGANIZACIJAMA

Mentor:

doc. dr. sc. Mario Jadrić

Student:

Antonio Badžim

Split, srpanj 2016.

SADRŽAJ:

SAŽETAK

1. UVOD…….. 3

2. INFORMACISJKA SIGURNOST- PREGLED STANDARDA, ZAKONA I POLITIKA O INFORMACIJSKOJ SIGURNOSTI …. 5

2.1. Sigurnosna politika…….. 5

2.2. Sigurnosni standardi…… 7

2.2.1. ISO/IEC 27001……. 8

2.2.2. ISO/IEC 27002……. 12

2.2.3. Veza i razvoj ISO/IEC 27001//27002……. 15

2.3. Zakon o informacijskoj sigurnosti…….. 16

3. OBLICI PRIJETNJI TE METODE I MJERE ZAŠTITE INFORMACIJSKIH RESURSA ORGANIZACIJE……. 24

3.1. Sigurnosne prijetnje…… 24

3.2. Procjena ranjivosti…… .. 28

3.3. Procjena rizika…… 30

3.4. Mjere zaštite informacijskih resursa……. 30

3.4.1. Organizacijske mjere zaštite……. 30

3.4.2. Fizičke mjere zaštite…….. 31

3.4.3. Programske mjere zaštite……. 33

4. EMPIRIJSKO ISTRAŽIVANJE RAZINE INFORMACIJSKE SIGURNOSTI U POSLOVNIM ORGANIZACIJAMA…….. 35

5. ZAKLJUČAK…….. 41

Sažetak

Svaka moderna organizacija ima razvijen informacijski sustav, a jedan od najvažnijih ciljeva organizacije je osiguranje kontinuiteta poslovanja. Za održavanje neometanosti poslovnog kontinuiteta bitno je da resursi informacijskog sustava u svako vrijeme budu dostupni i cjeloviti, a da povjerljivost podataka i informacija ne bude dovedena u pitanje. Kako bi sustav informacijske sigurnosti bio učinkovito zaštićen potrebno je uspješno uskladiti, implementirati i nadzirati sve potrebne mjere zaštite. Danas je u velikoj mjeri prepoznata potreba za uspješnim upravljanjem sigurnošću informacija, te se razvijaju brojni standardi koji daju preporuke za uspostavljanje sustava upravljanja sigurnošću informacija. Taj sustav uz nesmetanost obavljanja djelatnosti organizacije pomaže da se organizacija u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente.

Ključne riječi: sigurnosna politika, sigurnosni standardi i norme, upravljanje sigurnošću

Summary

Every modern organization has developed information system, and one of the most important goals of the organization is to ensure business continuity. To sustain business continuity it is important that information system resources at all times are available and complete, and that the confidentiality of data and information is not compromised. To be effectively protected, information security system is necessary to be successfully align, implement and supervise all necessary protection measures. Today there is widely recognized need for successful management of information security, and many standards are developing to provide recommendations for establishing information security management system. This system with a leeway to perform the activities of the organization helps the organization at any time to deal with the latest security threats and the time to react to any possible security incidents.

Keywords: security policy, security standards and norms, security management

UVOD

Informacijska sigurnost postaje važna infrastruktura u suvremenom poslovanju. Suvremeni državni i gospodarski subjekti ovise o računalnoj i komunikacijskoj infrastrukturi. Pod pojmom informacijske sigurnosti podrazumijeva se zaštita informacija od pojavnih oblika prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat uloženih investicija.

Cilj ovog rada je prikazati osnove uspostave sustava upravljanja sigurnošću informacija, koje su od neposredne važnosti za uspješnost i kontinuiranost poslovanja organizacije. Istovremeno, organizacije moraju biti svjesne činjenice da je uvijek prisutna određena razina nesigurnosti, što zahtjeva spremnost i sposobnost organizacije da u svakom trenutku može odgovoriti najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente.

Pojam informacijske sigurnosti se ne odnosi isključivo na tehničke mjere zaštite, već podrazumijeva administrativne i fizičke mjere. Stoga informacijsku sigurnost promatramo kao: način razmišljanja, beskonačan proces, upravljanje rizikom, jamstvo poslovnog uspjeha i kao odgovornost svakog zaposlenika. Informacija je imovina i kao takvu ju je potrebno prikladno zaštititi, kako bi se postiglo uspješno poslovanje organizacije. Bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti prikladno zaštićena, sigurnosno osigurana i namjenski korištena.

Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, špijunaže, sabotaže i sl. Šteta nanesena organizaciji u obliku računalnog hakiranja i uskraćivanja usluge je novi pojavni oblik kriminala u poslovanju. Informacijska sigurnost je jednako važna javnim i privatnim organizacijama. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Upravljanje i usklađenost poslovanja kroz organizacijski i upravljački sklad podržavan informacijskom sigurnošću zahtjeva učešće svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan organizacije. Sigurnost informacijskih sustava obuhvaća primjenu mjera i radnji za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te radi sprječavanja

gubitaka cjelovitosti ili raspoloživosti samih sustava. Sigurnosne mjere uključuju mehanizme i procedure koje trebaju biti implementirane u svrhu odvraćanja, prevencije, detektiranja i oporavka od utjecaja incidenata koji djeluju na povjerljivost, cjelovitost i raspoloživost podataka i pratećih sustavnih servisa i resursa, uključujući i izvještavanje o sigurnosnim incidentima. To je zapravo proces upravljanja rizikom koji se koristi za procjenu, nadgledanje, ukidanje, izbjegavanje, prijenos ili prihvaćanje rizika.

2. INFORMACISJKA SIGURNOST- PREGLED STANDARDA, ZAKONA I POLITIKA O INFORMACIJSKOJ SIGURNOSTI

Prvo pitanje koje se postavlja je što je to uopće informacijska sigurnost. Postoji nekolicina definicija, a jedna od njih je da predstavlja multidisciplinarno područje koje čini temelje razvoja suvremenog informacijskog društva, na sličan način kao što je sigurnost temelj tradicionalnog društva i odnosa u njemu. Upravo zbog toga svi segmenti društva imaju svoju ulogu, bilo u razvoju, bilo u provedbi informacijske sigurnosti.

Zahtjevi informacijske sigurnosti proizlaze iz tradicionalnih zahtjeva zaštite klasificiranih podataka u državnom sektoru. Razvojem i globalizacijom društva, informacije i informacijski sustavi postali su vrijednosni potencijal ne samo državnog sektora i ne samo u uskom okviru tajnih podataka. Tako je danas u sklopu informacijske sigurnosti nužno promatrati cjelokupno društvo i informacijski prostor u cjelini, usklađujući razlike i potrebe informacijske sigurnosti u različitim sektorima društva od pojedinih gospodarskih sektora do međunarodnih normi.

Područja informacijske sigurnosti za koje se propisuju mjere i standardi informacijske sigurnosti su:

- Sigurnosne provjere
- Sigurnost podataka
- Sigurnost informacijskih sustava
- Fizička sigurnost
- Sigurnost poslovne suradnje

2.1. Sigurnosna politika

Sigurnosnu politiku informacijskog sustava temeljimo na organizacijskom i upravljačkom skladu, gdje se točno zna tko je za što odgovoran. Politiku provode stručna tijela za upravljanje sigurnošću preko korisnika informacijskih sustava, korisnici informacijskih sustava dijele se na one koji koriste usluge i oni koji pružaju usluge.

Informacijski sustavi sadrže podatke kojima se služe ovlašteni korisnici i koji služe kako bi korisnicima bilo omogućeno korištenje sustavom. Budući da takvi podaci ne smiju biti javno dostupni odnosno moraju biti tajni, ne smiju se mijenjati bez odobrenja i biti nedostupni korisnicima, važno je provesti određene korake sigurnosti kako bi navedeni uvjeti uvijek bili zadovoljeni.

Sigurnosna politika predstavlja 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. Politikom ne određujemo na koji način zaštititi informacijski sustav već samo što zaštititi. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sustav. Stoga definiranje općenite sigurnosne politike za informacijske sustave nije moguće i jednom napisana politika mora se redovito pregledavati, mijenjati i nadopunjavati u skladu s potrebama. 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
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima smjernicama.

Sigurnosnom politikom definirana su pravila koja se odnose na:

- svu računalnu opremu institucije
- osobe odgovorne za administraciju informacijskog sustava
- sve zaposlenike i korisnike sustava
- vanjske suradnike

Zbog korisnika kojima je sigurnosna politika namijenjena i koji moraju s njom biti upoznati potrebno je definirati politiku tako da bude kratka i jasna, napisana na način da ju korisnici mogu

razumjeti. Politiku napisanu opširno i stručnim jezikom običan korisnik ne razumije i površno ju ili nikako ne analizira, pa je stoga ne može niti primijeniti.

Ljudi su oni na kojima se temelji sigurnost sustava stoga je primarna uloga sigurnosne politike određivanje načina ponašanja koje je prihvatljivo i neprihvatljivo, sve u svrhu zaštite vrijednosti informacijskog sustava.

Na temelju pravila definiranih u dokumentu, njen je zadatak osigurati tri jedinstvena svojstva informacija:

- povjerljivost
- integritet
- dostupnost

2.2. Sigurnosni standardi

Nakon uspostavljanja sigurnosne politike potrebno je odabrati standard prema kojem će se sigurnosna politika uspostaviti. Standardi su se pojavili na tržištu kako bi olakšali implementaciju sigurnosti u organizacije. Mjerodavne institucije za izdavanje ovakvih standarda u području zaštite informacijskih sustava su **ISO** (International Organization for Standardization) i **IEC** (International Electrotechnical Commission) i one zajedno čine sustav za međunarodnu standardizaciju. Organizacija ISO objavila je veći broj standarda vezanih uz zaštitu i sigurnost informacijskog sustava:

- ISO 27000 – Pregled normi iz ISO 27k serije;
- ISO 27001 – (2006) Sustav upravljanja informatičkom sigurnošću (ISMS);
- ISO 27002 – (2007) Kodeks postupaka za upravljanje sustava informacijske sigurnosti;
- ISO 27003 – Vodič za uvođenje sustava informacijske sigurnosti;
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti;
- ISO 27005 – (2006) Upravljanje rizicima informacijske sigurnosti;
- ISO 27006 – (2007) Zahtjevi za postupkom analize i certificiranja standarda;

- ISO 27011 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru.

U pripremi je još standarda koje reguliraju pitanja sustava informacijske sigurnosti.

ISO norma prihvaćena je i od Hrvatskog zavoda za norme 2006. godine, pa je točan naziv HRN ISO/IEC 27001:2006 i može se nabaviti direktno od dotičnog zavoda. Ona propisuje na koji način organizirati informacijsku sigurnost u bilo kojoj vrsti organizacije. Smatra se da je ovo temeljna norma za upravljanje informacijskom sigurnošću.

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).

Pri izradi sigurnosne politike preporuča se upotreba oba standarda.

2.2.1 ISO/IEC 27001

ISO/IEC 27001:2005 je standard objavljen u listopadu 2005. godine, razvijen je na temeljima BS 7799 standarda, točnije njegovog drugog dijela. Namjena ovog standarda je kvalitetna uspostava sustava upravljanja sigurnošću informacija (ISMS), a sadrži skup zahtjeva koje organizacija mora ispuniti da bi se priznao certifikat za informacijsku sigurnost. Iako standard 27001 obuhvaća izradu sigurnosne politike, njegova prvenstvena uloga je način implementacije sigurnosnih kontrola i samim time nije prikladan kao temelj pisanja sigurnosne politike.

Norma ISO 27001:2013 je izdana 2013. nakon revizije starije norme zbog preklapanja nekih od pravila koji su morali biti zadovoljeni. Svrha norme ISO 27001:2013 je da prikaže na

koji način uvesti informacijsku sigurnost u neku organizaciju. Norma pruža organizaciji mogućnost dobivanja certifikata koji služi kao potvrda da je sigurnost u organizaciji provedena na najbolji mogući način. Norma ISO 27001:2013 znači za informacijsku sigurnost isto ono što ISO 9001:2008 znači za sustav upravljanja kvalitetom. Vrijednost ove norme dodatno naglašava činjenica da su mnoga zakonodavstva uzela tu normu kao temelj za pisanje raznih regulativa iz područja zaštite osobnih podataka, zaštite tajnosti podataka, zaštite informacijskih sustava i sl. Standardi informacijske sigurnosti razvijaju se na osnovi zahtjeva kupaca. Norma ISO 27001:2013 napravljena je kako bi osigurala adekvatnu i razmjernu sigurnosnu kontrolu koja štititi podatkovnu imovinu i daje povjerenje korisnicima.

Kako bi se uveo sustav upravljanja informacijskom sigurnošću potrebno je provoditi ciklus od 4 faze koje postavlja norma ISO 27001. Te faze su:

- **Faza planiranja** koja služi za planiranje osnovne organizacije za informacijsku sigurnost i odabir mjere zaštite koja je najprimjerenija. Postoji niz koraka koje je potrebno ispuniti za završetak faze:
  - Određivanje opsega ISMS- a
  - Pisanje politike ISMS- a
  - Identificiranje metodologije za procjenu rizika i određivanje kriterija za prihvaćenje rizika
  - Identifikacija resursa, ranjivosti i prijetnji
  - Ocjenjivanje veličine rizika
  - Identifikacije i procjena opcija za ovladavanje (umanjivanje) rizika
  - Odabir mjera zaštita za ovladavanje (umanjivanje) rizika
  - Pribavljanje odobrenja uprave za preostale rizike
  - Pribavljanje odobrenja uprave za implementaciju ISMS- a
  - Pisanje izvješća o primjenjivosti koje popisuje primjerene mjere zaštite, koje su od njih već provedene, i koje mjere zaštite nisu primjerene

- **Faza implementacije** u kojoj se sve isplanirano u prethodnoj fazi provodi u djelo. Ova faza također sadrži niz koraka za provedbu:

- Pisanje plana ovladavanja rizikom – opisuje tko, kako, kada i sa kojim budžetom treba provesti primjerene mjere zaštite
- Implementirati plan ovladavanja rizikom
- Implementirati primjene mjere zaštite
- Odrediti kako će mjeriti učinkovitost mjera zaštite
- Provesti osvješćivanje i obuku djelatnika
- Upravljanje normalnim radom ISMS- a
- Upravljanje resursima ISMS- a
- Provedba procedure za detekciju i upravljanje sigurnosnim incidentima.

- **Faza nadzora i pregledavanja** sa svrhom da se kroz ovu fazu vrši nadgledanje funkcioniranja ISMS-a:
  - Provedba procedura i ostalih kontrola za nadzor i pregledavanje kako bi se ustanovila sva kršenja pravila, krivo procesiranje podataka, da li se sigurnosne aktivnosti provode kako je očekivano i sl.
  - Poduzimanje redovitog pregledavanja učinkovitosti ISMS- a
  - Mjerenje učinkovitosti mjera zaštite
  - Pregledavanje procjene rizika u redovitim intervalima
  - Poduzimanje internih audita u planiranim intervalima
  - Poduzimanje pregleda od strane uprave kako bi se osiguralo da ISMS funkcionira i da se identificiraju mogućnosti za poboljšanja
  - Ažuriranje sigurnosnih planova kako bi se uzele u obzir ostale aktivnosti nadzora i pregledavanja
  - Vođenje zapisa aktivnosti i incidenata koji mogu imati utjecaj na učinkovitost ISMS- a.
- **Faza održavanja i poboljšavanja** je završna faza i njena svrha je poboljšanje svega što je u prethodnoj fazi identificirano kao neadekvatno:
  - Implementacija identificiranih poboljšanja u ISMS- u
  - Poduzimanje korektivnih i preventivnih mjera; primjena vlastitih i tuđih sigurnosnih iskustava

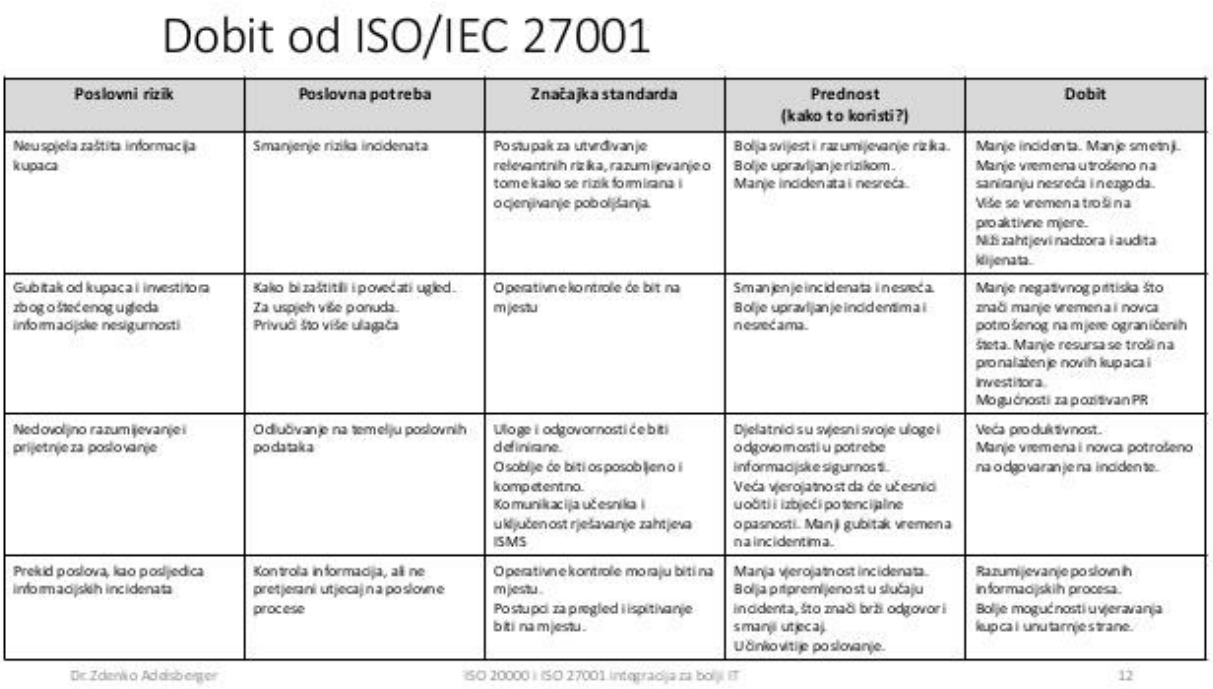
- Komuniciranje aktivnosti i poboljšanja svim zainteresiranim stranama
- Osiguravanje da poboljšanja postižu željene ciljeve.

Implementacija standarda **ISO/IEC 27001** u organizaciju odvija se kroz dvije faze:

1. Administrativna faza u kojoj menadžment donosi stratešku odluku da se ide u taj projekt, odnosno osigurava punu podršku implementaciji.

2. Druga faza odvija se kroz nekoliko koraka: određivanje opsega i granice ISMS, definiranje politike ISMS, evidencija imovine (za čuvanje, prijenos i obradu informacija), procjena rizika, donošenje dokumenta „Izjava o prihvatljivosti“ (SoA), prihvaćanje i odobrenje uprave, priprema dokumentacije, implementacija ISMS, izrada procedura za upravljanje incidentima, provođenje monitoringa, identifikacija i implementacija poboljšanja itd.

Ključni dokument koji se u cijelom projektu implementacije koristi kao temelj za donošenje odluke uprave o konačnom prihvaćanju strukture ISMS je „Izjava o prihvatljivosti“ (SoA – eng. Statement of Applicability). Kroz taj dokument točno se definira što sve treba od kontrola primijeniti u organizaciji kako bi se uspostavio željeni ISMS. Ukoliko se kontrola ne primjenjuje tada se mora u dokumentu SoA detaljno navesti razlog zašto se ta kontrola ne koristi u okviru konkretnog ISMS. Osnove za definiranje dokumenta SoA su sigurnosna politika organizacije, definirana na početku, te u skladu s njom izvršena procjena rizika. To drugim riječima znači, da rezultati procjene rizika na imovini određuju sve kriterije za bilo kakve potrebne kontrole i aktivnosti vezane za uspostavu ISMS.



Slika 1. Dobit od ISO/IEC 27001

Izvor: http://image.slidesharecdn.com/zlatibor-integracijaiso27001iiso20000-140428000004-phpapp02/95/zlatibor-integracija-iso27001-i-iso20000-12-638.jpg?cb=1398643443

2.2.2 ISO/IEC 27002

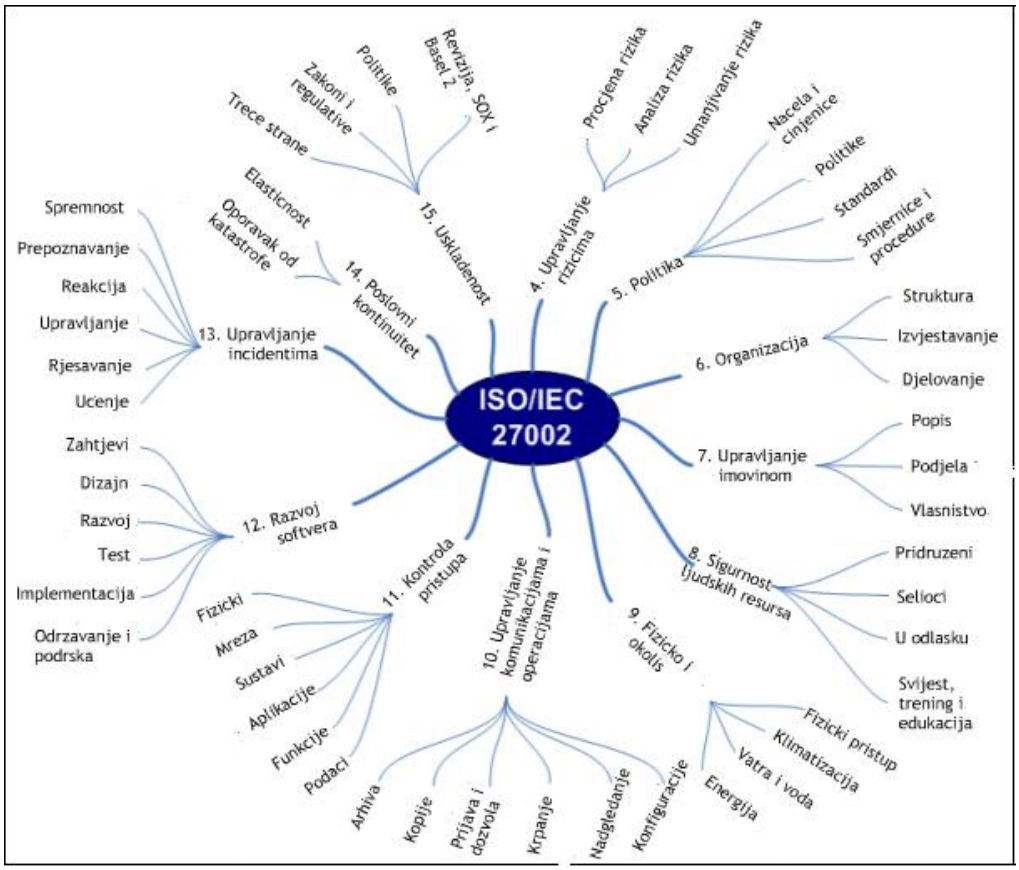
Ovaj Međunarodni standard je dizajniran da bi ga organizacije mogle koristiti kao referencu za odabir kontrola u procesu provedbe sustava upravljanja sigurnošću informacija (ISMS) temeljen na ISO/IEC 27001, kao vodič za organizacije koje provode opće prihvaćene informacije sigurnosne kontrole ili pak razvijaju svoj vlastiti vodič za upravljanje informacijskom sigurnošću. Organizacije svih vrsta i veličina (uključujući javni i privatni sektor, komercijalne i neprofitne) prikupljaju, obrađuju, pohranjuju i prenose podatake u mnogim oblicima, uključujući elektroničke, fizičke i verbalne (na primjer razgovora i prezentacija).

Vrijednost informacija nadilazi pisane riječi, brojeve i slike: znanje, koncepti, ideje i marke su primjeri nematerijalne oblike informacija. U povezanom svijetu, informacije i povezani postupci, sustavi, mreže i osoblje koji su uključeni u njihov rad, rukovanje i zaštita su sredstva koja, kao i druga važna poslovna imovina, su vrijedni za poslovne organizacije i time zaslužuju ili

zahtijevaju zaštitu od raznih opasnosti. Imovina podliježu namjernim i slučajnim prijetnjama, a povezani procesi, sustavi, mreže i ljudi su nerazdvojive slabosti. Promjene poslovnih procesa i sustava ili drugih vanjskih promjena (kao što su novi zakoni i propisi) mogu stvarati nove rizike informacijske sigurnosti. Stoga, s obzirom na mnoštvo načina na koje prijetnje mogu iskoristiti ranjivosti i naškoditi organizaciji, rizici informacijske sigurnosti su uvijek prisutni. Učinkovita informacijska sigurnost smanjuje ove rizike štiteći organizaciju protiv prijetnji i ranjivosti, a time se smanjuje utjecaj na imovinu.

Informacijska sigurnost se postiže primjenom odgovarajućeg skupa kontrola, uključujući i pravila, procesa, postupaka, organizacijske strukture i softver/hardverske funkcije. Te kontrole moraju biti uspostavljene, provođene, praćene, pregledavane i poboljšavane, gdje je to potrebno, kako bi se osiguralo ispunjavanje posebnih sigurnosnih i poslovnih ciljeva organizacije. ISMS kao što je navedeno u ISO / IEC 27001 zahtjeva holistički, koordiniran pogled na rizik informacijske sigurnosti organizacije u cilju provođenja cjelokupnog paketa kontrola informacijske sigurnosti u okviru cjelovitog sustava upravljanja. Mnogi informacijski sustavi nisu dizajnirani da budu zaštićeni u smislu ISO / IEC 27001 i ovog standarda. Sigurnost koja se može postići putem tehničkih sredstava je ograničena i treba biti podržana od strane odgovarajućeg upravljanja. Prepoznavanje kontrola koje se trebaju koristiti zahtijeva pažljivo planiranje i obraćanje pažnje na detalje.

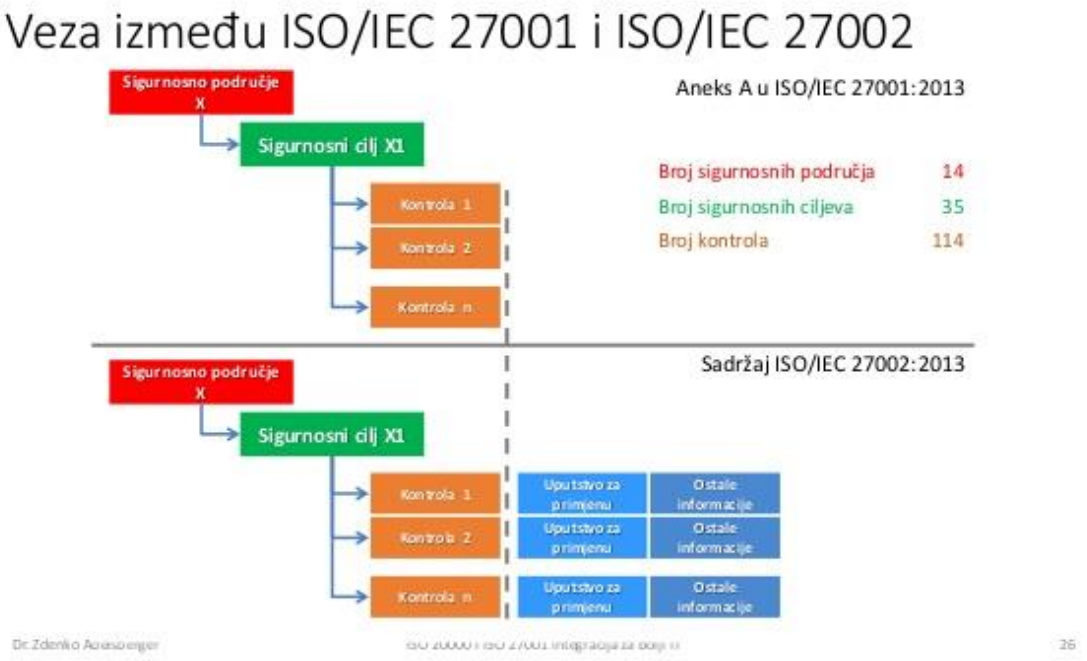
Uspješan ISMS zahtijeva podršku od strane svih zaposlenika u organizaciji. On također može zahtijevati sudjelovanje dioničara, dobavljača ili drugih vanjskih sudionika. Specijalistički savjet od vanjskih sudionika također može biti potreban. U općenitijem smislu, učinkovita informacijska sigurnost također uvjerava rukovodstvo i druge zainteresirane strane da je imovina organizacije prilično sigurna i zaštićena.



Slika 2. Komplet preporučene primjene informacijske sigurnosti

Izvor: https://pkab.wordpress.com/2009/03/13/peta-konsep-isoiec-27002/

2.2.3 VEZA I RAZVOJ ISO/IEC 27001 // 27002

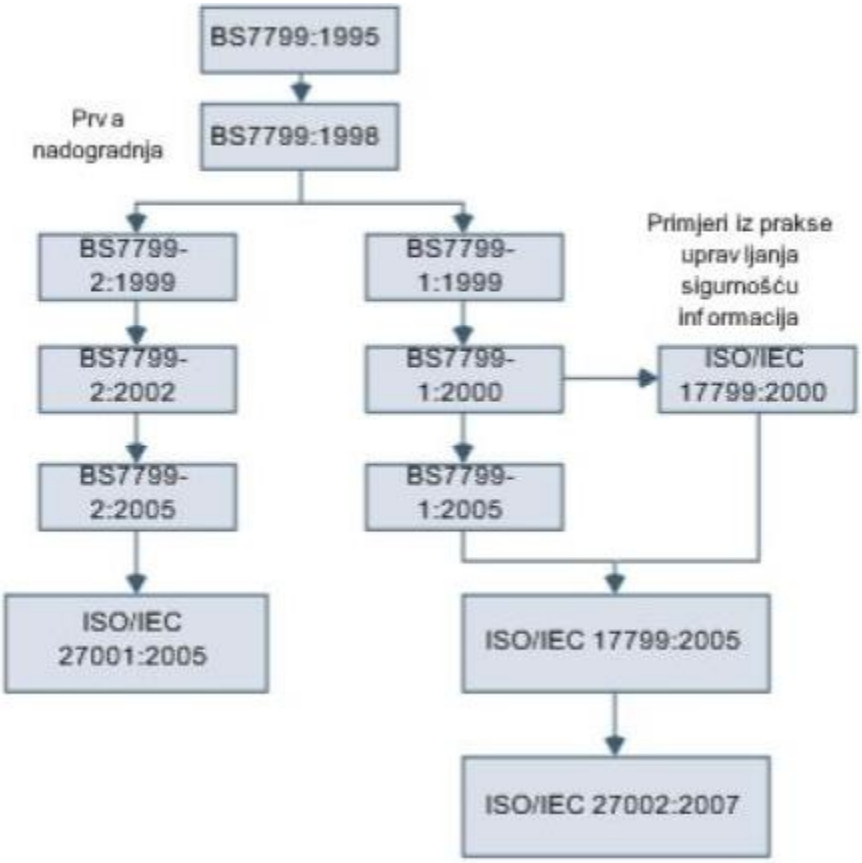


Slika 3. Veza između ISO/IEC 27001 i ISO/IEC 27002

Izvor: httpimage.slidesharecdn.comzlatibor-integracijaiso27001iiso20000-140428000004-phpapp0295zlatibor-integracija-iso27001-i-iso20000-26-638.jpgcb=1398643443

Nakon revizije ISO/IEC 27001:2013 i usporedbom sa revizijom iz 2005 godine došlo je do nekih promjena tako da je sada 113 kontrola umjesto 133, te 14 sigurnosnih područja umjesto 11. Niz kontrola nije promijenjeno u odnosu na reviziju iz 2005, neke su obrisane, nekima je mijenjan tekst, neke su pregrupirane, a neke spajane. Razlog za takve promjene proizlazi iz iskustva i opravdanih prijedloga koji su dolazili s terena tijekom više od 7 godina primjene prethodne revizije. Te promjene imaju utjecaj i na novu reviziju ISO/IEC 27002:2013 koja u vidu smjernica najbolje prakse prati promjene standarda ISO/IEC 27001.

Jedna od najvećih promjena u ISO/IEC 27002:2013 je potpuno uklanjanje poglavlja o procjeni i obradi rizika.



Slika 4. Razvoj standarda ISO/IEC 27001 do 2005. odnosno ISO/IEC 27002 do 2007. godine

Izvor:http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustava_2_dio.pdf

2.3. Zakon o informacijskoj sigurnosti

Postojeća zakonska regulativa koja regulira pitanja informacijske sigurnosti, a koja se odnosi na tijela državne uprave:

- Zakon o informacijskoj sigurnosti (NN 79/07)
- Uredba o mjerama informacijske sigurnosti (NN 46/08)
- Zakon o tajnosti podataka (NN 79/07)
- Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima (NN 72/07)

- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (NN 102/07)

Zakon o informacijskoj sigurnosti donesen je u srpnju 2007. godine i time se na jednom mjestu utvrđuju pojam informacijske sigurnosti, mjere i standardi, područja informacijske sigurnosti te tijela koja su nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

Neki od dijelova i članaka Zakona o informacijskoj sigurnosti:

I. OSNOVNE ODREDBE[1]

Članak 2.

Pojedini pojmovi u smislu ovoga Zakona imaju sljedeće značenje:
– Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.
– Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.
– Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.
– Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.
– Sigurnosna akreditacija informacijskog sustava je postupak u kojem se utvrđuje osposobljenost tijela i pravnih osoba iz članka 1. stavka 2. ovoga Zakona za upravljanje sigurnošću informacijskog sustava, a provodi se utvrđivanjem primijenjenih mjera i standarda informacijske sigurnosti.

[1] Zakon o informacijskoj sigurnosti NN 79/07 (http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti)

– Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike.

II. MJERE I STANDARDI INFORMACIJSKE SIGURNOSTI

Članak 5.

Mjere i standardi informacijske sigurnosti obuhvaćaju:
– nadzor pristupa i postupanja s klasificiranim podacima,
– postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka,
– planiranje mjera prilikom izvanrednih situacija,
– ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.

Članak 6.

(1) Mjere i standardi informacijske sigurnosti za zaštitu neklasificiranih podataka utvrđuju se u skladu s mjerama i standardima zakonom propisanim za zaštitu osobnih podataka građana.
(2) Mjere i standardi informacijske sigurnosti za zaštitu stupnja tajnosti »Ograničeno« utvrđuju se u skladu sa stavkom 1. ovoga članka, uz:
– prethodnu provjeru primjene propisanih mjera i standarda za neklasificirane podatke,
– primjenu mjera i standarda propisanih za stupanj tajnosti »Ograničeno«.

III. PODRUČJA INFORMACIJSKE SIGURNOSTI

Članak 8.

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:
– sigurnosna provjera,
– fizička sigurnost,

– sigurnost podatka,
– sigurnost informacijskog sustava,
– sigurnost poslovne suradnje.

Sigurnosna provjera

Članak 9.

(1) Sigurnosna provjera je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima.
(2) Osobe iz stavka 1. ovoga članka obvezne su ishoditi uvjerenje o sigurnosnoj provjeri osobe (certifikat).
(3) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, dužni su ustrojiti:
– popis osoba koje imaju pristup klasificiranim podacima,
– registar zaprimljenih certifikata s rokovima važenja certifikata.

Fizička sigurnost

Članak 10.

(1) Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci.
(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, izvršit će kategorizaciju objekata i prostora na sigurnosne zone, propisane mjerama i standardima informacijske sigurnosti.

Sigurnost podatka

Članak 11.

(1) Sigurnost podatka je područje informacijske sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.
(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane i neklasificirane podatke u svom djelokrugu, dužni su primijeniti procedure o postupanju s klasificiranim i neklasificiranim podacima, o sadržaju i načinu vođenja evidencije o izvršenim uvidima u klasificirane podatke te nadzoru sigurnosti podataka, propisanim mjerama i standardima informacijske sigurnosti.

Sigurnost informacijskog sustava

Članak 12.

(1) Sigurnost informacijskog sustava je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.
(2) Sigurnosna akreditacija informacijskog sustava provodi se za informacijski sustav u kojem se koriste klasificirani podaci stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«.
(3) Osobe koje sudjeluju u procesu iz stavka 1. ovoga članka trebaju posjedovati certifikat razine »Vrlo tajno« ili za jedan stupanj više od najviše razine tajnosti klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijskim sustavima pod njihovom nadležnosti.
(4) Mjere fizičke zaštite prostora u kojima se nalaze informacijski sustavi poduzet će se sukladno najvišoj razini tajnosti klasificiranih podataka koji se u njima obrađuju, pohranjuju ili prenose.
(5) Središnja državna tijela za informacijsku sigurnost ustrojavaju registar certificirane opreme i uređaja koji se koriste u klasificiranom informacijskom sustavu razine »Povjerljivo«, »Tajno« i »Vrlo tajno«.
Registar certificirane opreme i uređaja ustrojava se na temelju preuzimanja odgovarajućih

registara međunarodnih organizacija ili vlastitim certificiranjem u skladu s odgovarajućim međunarodnim normama.

Sigurnost poslovne suradnje

Članak 13.

(1) Sigurnost poslovne suradnje je područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe iz članka 1. stavka 3. ovoga Zakona.
(2) Pravne i fizičke osobe koje pristupaju provedbi natječaja ili ugovora iz stavka 1. ovoga članka, obvezne su ishoditi uvjerenje o sigurnosnoj provjeri pravne osobe (certifikat poslovne sigurnosti).
(3) Pravne i fizičke osobe iz stavka 1. ovoga članka za osoblje, objekte i prostore obvezne su primijeniti utvrđene mjere i standarde informacijske sigurnosti za određeni stupanj tajnosti klasificiranih podataka.
(4) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, ovlašteni su za podnošenje zahtjeva za izdavanje certifikata poslovne sigurnosti za pravne i fizičke osobe kojima dostavljaju klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«.
(5) Pravne i fizičke osobe koje sudjeluju u međunarodnim poslovima za koje je obvezan certifikat poslovne sigurnosti, ovlaštene su za podnošenje zahtjeva za izdavanje certifikata.
(6) Certifikat poslovne sigurnosti izdaje središnje državno tijelo za informacijsku sigurnost.

IV. SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

Ured Vijeća za nacionalnu sigurnost

Članak 14.

Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u

Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.

Članak 15.

(1) Ured Vijeća za nacionalnu sigurnost donosi Pravilnik o standardima sigurnosne provjere, Pravilnik o standardima fizičke sigurnosti, Pravilnik o standardima sigurnosti podataka, Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava te Pravilnik o standardima sigurnosti poslovne suradnje.
(2) Ured Vijeća za nacionalnu sigurnost trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

Zavod za sigurnost informacijskih sustava

Članak 17.

(1) Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavka 2. ovoga Zakona.
(2) Tehnička područja sigurnosti informacijskih sustava su:
– standardi sigurnosti informacijskih sustava,
– sigurnosne akreditacije informacijskih sustava,
– upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka,
– koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

Članak 18.

(1) Zavod za sigurnost informacijskih sustava pravilnikom će regulirati standarde tehničkih područja sigurnosti informacijskih sustava iz članka 17. stavka 2. ovoga Zakona.
(2) Zavod za sigurnost informacijskih sustava trajno usklađuje standarde tehničkih područja sigurnosti informacijskih sustava u Republici Hrvatskoj s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.

Članak 19.

Zavod za sigurnost informacijskih sustava obavlja poslove sigurnosne akreditacije informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost.

V. NACIONALNI CERT

Članak 20.

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.
(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet).
(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.
(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

3. OBLICI PRIJETNJI TE METODE I MJERE ZAŠTITE INFORMACIJSKIH RESURSA ORGANIZACIJE

Informacijski sustavi (IS) su izloženi različitim vrstama sigurnosnih prijetnji koje mogu rezultirati sa značajnim financijskim gubicima i šteti na resursima informacijskog sustava. Vrste oštećenja uzrokovanih sigurnosnim prijetnjama su različiti, npr. narušavanja sigurnosti integriteta baze podataka, fizičko uništenje cjelokupnog informacijskog sustava objekta uzrokovanih požara, poplave itd. Izvor tih prijetnji može biti neželjene aktivnosti "pouzdanih" zaposlenika, hakerskih napada, slučajnog propusta u unosu podataka i slično.

Financijski gubici uzrokovani narušavanjem sigurnosti često se ne može točno definirati jer je činjenica da znatan broj manjih razmjera sigurnosnih incidenata nikada nisu otkriveni, dio incidenata su opisani kao slučajne pogreške, a sve to je rezultat sklonosti kako bi se smanjila odgovornost osoba odgovornih za sigurnosni incident. Sigurnosna prijetnja može se definirati kao svaki događaj koji može rezultirati povredom informacijske povjerljivosti, cjelovitosti i dostupnosti ili bilo kojeg drugog oblika štete resursima informacijskog sustava. Posljedice sigurnosne prijetnje su različite, tako da neke sigurnosne prijetnje utječu na povjerljivost i pouzdanost pohranjenih podataka, a neke prijetnje utječu na funkcionalnost i učinkovitost cjelokupnog informacijskog sustava.

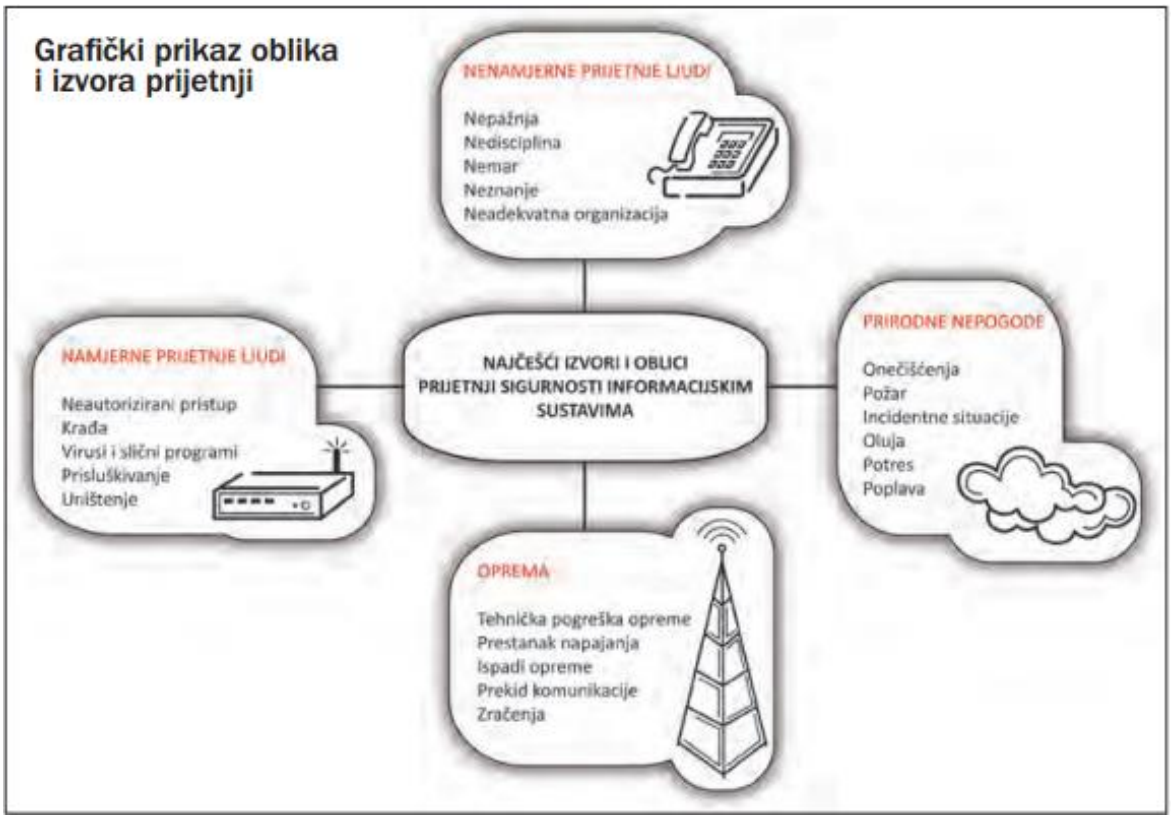
3.1. Sigurnosne prijetnje

Prijetnja i ranjivost nisu jedno te isto. Prijetnja je osoba ili događaj koji ima potencijal da utječe na vrijedan resurs na negativan način. Ranjivost je osobina resursa ili njegove okoline koja omogućuje prijetnji da se realizira. Postoji mnogo klasifikacija prijetnji s obzirom na različite kriterije.

Tako na primjer klasifikacija sigurnosnih prijetnje koja se pojavila iz međunarodne norme ISO / IEC 17799: 2000 razlikuje sigurnosne prijetnje prema vrsti njihovih izvora. Na temelju toga kriterija mogu se definirati četiri glavne skupine sigurnosnih prijetnji:

- prirodne nepogode (potresi, poplave, požari, oluje,…)

- tehničke prijetnje (tehničke greške, kvarovi, komunikacijske pogreške,…)
- ljudi – nenamjerne prijetnje (nedisciplina, nemar, neprimjeren softver ili organizacija,…)
- ljudi – namjerne prijetnje (sabotaža, diverzija, špijunaža, prijevara, krađa, virusi)



Slika 5. Izvori i oblici prijetnji sigurnosti informacijskim sustavima

Izvor: http://www.generalsecurity.hr/radovi/SIGURNOST%20INFORMACIJA-ENIMARK%20PONJEVIC-GENERAL%20SECURITY%20ZA%20POSLOVNI%20SAVJETNIK.pdf

Također kao kriterij se koristi područje na koje je određena prijetnja usmjerena. S obzirom na taj kriterij imamo podjelu:

- Udar na fizičku sigurnost
  - Ear tapping
  - DoS
  - Trash digging
- Udar na osobnu sigurnost
  - User's password guessing
  - Masquerading (false identity)
  - Social engineering
  - Extortions
  - Software piracy
- Udar na komunikaciju i sigurnost podataka
  - Attacks on data
  - Attacks on software
- Udar na operativnu sigurnost
  - Data frauds
  - Spoofing
  - Sniffing
  - Searching
  - Privileged access

Utjecaj prijetnji na sustav se može manifestirati kroz narušenost integriteta, dostupnosti ili povjerljivosti, a ta 3 svojstva osigurava sigurnosna politika.

Integritet predstavlja zaštitu podataka od namjernog ili slučajnog neovlaštenog mijenjanja. Kao i povjerljivost, integritet može biti ugrožen od hakera, lažnog predstavljanja, neovlaštenih aktivnosti i nedozvoljenih pristupa i drugih aktivnosti koje mogu dovesti do neovlaštenog mijenjanja podataka.

Tri su temeljna principa uspostave kontrola integriteta:

- Dodjela samo nužnih prava pristupa (engl. need-to-know basis) - korisnicima treba dodijeliti pravo pristupa samo na one datoteke i programe koji su im potrebni da bi obavljali svoju poslovnu funkciju u organizaciji.
- Odvajanje dužnosti i obveza (engl. separation of duties) - dobro je osigurati da nijedan zaposlenik nema kontrolu nad transakcijom od početka do kraja. Dvoje ili više ljudi trebaju biti odgovorni za izvođenje transakcije
- Rotacija dužnosti (engl. rotation of duties) - poslovni zadaci bi se trebali mijenjati periodički tako da korisnicima bude otežano zlonamjerno preuzimanje kontrole nad transakcijom. Ovaj princip je učinkovit kad se koristi u kombinaciji s odvajanjem dužnosti.

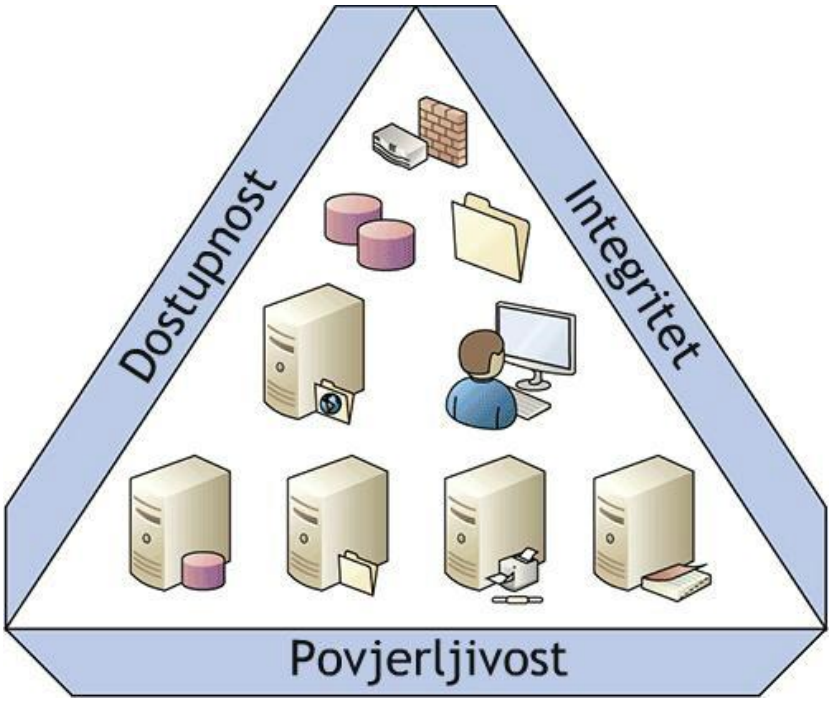
Dostupnost je garancija ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku kad za njim imaju potrebu.

Dva su najčešća uzroka neraspoloživosti sustava:

- Uskraćivanje usluge (eng. Denial Of Service) - vrsta napada u kojem se namjernim generiranjem velike količine mrežnog prometa nastoji zagušiti mrežna oprema i poslužitelji i na taj način onemogućava pružanje usluga hosta spojenog na internet
- Gubitak sposobnosti procesuiranja podataka kao rezultat prirodnih katastrofa ili ljudskih akcija – oni se prate planiranjem nepredviđenih situacija što omogućava minimiziranje vremena nedostupnosti sredstava za procesuiranje podataka. Planiranje može uključivati planiranje oporavka, obnove poslovnih procesa, itd., a osigurava alternative procesuiranja podataka odnosno dostupnosti

Povjerljivost je zaštita podataka koja sadrži sustav sigurnosti od neovlaštenog pristupa koji može biti narušen na razne načine od kojih se izdvajaju oni koji se najčešće događaju:

- Hakeri
- Lažno predstavljanje
- Nezaštićeno preuzimanje podataka
- Trojanski konji



Slika 6. Osnovni elementi informacijske sigurnosti

Izvor: https: //www.linkedin.com/pulse/kako-se-za%C5%A1titi-od-zlonamjernog-software-i-podataka-jasmin-kahriman.

3.2. Procjena ranjivosti

Ranjivost (eng. vulnerability) sustava podrazumijeva sve propuste i slabosti sustava sigurnosti koji omogućavaju ostvarivanje sigurnosnih prijetnji. Ranjivost može biti uvjetovana propustima ili pogreškama u operativnom provođenju sigurnosnih pravila i procedura.

Uz sigurnosne prijetnje, ranjivost je drugi ključni kriterij procjene vjerojatnosti sigurnosti rizika te ih uvijek treba promatrati povezano. Ukoliko ne postoji prijetnja koja bi iskoristila ranjivost tada ne postoji ni sigurnosni rizik pa te ranjivosti ne treba ni razmatrati. Za procjenu sigurnosnog rizika, a samim tim i za djelotvornu zaštitu ključna je detaljna procjena ranjivosti. Mjere koje treba poduzeti radi smanjena rizika ovise o broju i vrsti ranjivosti.

Potrebne informacije za određivanje ranjivosti prikupljaju se iz različitih izvora, a neki od njih su:

- Razgovor sa odgovarajućim zaposlenicima unutar prostorija organizacije pomaže prikupljanju informacija o fizičkoj i operativnoj sigurnosti IT sustava
- Pretraživanje javnih baza o ranjivosti informacijskih sustava
- Provođenje specijaliziranih istraživanja ranjivosti
- Pregledavanje sigurnosnih politika, sustavne dokumentacije i ostalih dokumenta koji se odnose na sigurnost može pružiti uvid u sigurnosne kontrole i pomoći pri identifikaciji ranjivosti.
- Uporaba alata za skeniranje sustava - proaktivne tehničke metode daju kvalitetnu sliku o sustavu i vrlo su efikasne u prikupljanu podatka o ranjivostima sustava. Najčešće korištene metode su penetracijska testiranja, ST&E (engl. Security Test & Evaluation) i automatizirani alati za skeniranje ranjivosti.

Osim indetifikacije ranjivosti važna je i procjena vjerojatnosi realizacije, a pri tome postoje nekoliko osnovnih stavki koje se uzimaju u obzir:

- motiviranost i interes izvora
- priroda ranjivosti
- učinkovitost sustava sigurnosti

Nivo vjerojatnosti	Definicija vjerojatnosti
Visoki	Prijetnja je visoko motivirana i ima dovoljno mogućnosti za realizaciju, a kontrole koje bi trebale spriječiti iskorištavanje ranjivosti su neefektivne.
Srednji	Prijetnja je motivirana i ima mogućnosti za realizaciju, ali postoje kontrole koje mogu spriječiti uspješno izvođenje prijetnje.
Nizak	Prijetnja nije motivirana ili nema dovoljno mogućnosti za realizaciju, ili postoje kontrole koje mogu spriječiti iskorištavanje ranjivosti

Slika 7. Tablica vjerojatnosti prijetnje

Izvor: http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

3.3 Procjena rizika

Sigurnosni zahtjevi se identificiraju metodičkom procjenom sigurnosnih rizika. Proširenje sigurnosnih kontrola mora biti proporcionalno šteti koju sigurnosni propusti nanose organizaciji. Rezultati procjene rizika pomažu u određivanju prioriteta i prikladnih akcija kod upravljanja sigurnosnim rizicima. Procjena rizika se mora provoditi periodički kako bi se u procjenu uključile bilo kakve promjene koje bi mogle utjecati na rizik, implementaciju i održavanje sustava i sl.

Bez adekvatne analize ranjivosti, gotovo je nemoguće pouzdano odrediti sigurnosni rizik. Sama logika nas navodi na to da tamo gdje nema rizika nema smisla ulagati u zaštitna sredstva, implementiraju se samo ona zaštitna sredstva koja će biti opravdana i smislena u pogledu zaštite poslovnih ciljeva organizacije.

3.4. Mjere zaštite informacijskih resursa

Mjere zaštite predstavljaju skup aktivnosti, postupaka, implementacije zaštitnih mehanizama i naprava, s ciljem ostvarenja zaštite informacijskog sustava od različitih sigurnosnih rizika i prijetnji, a to sve u skladu sa sigurnosnom politikom i na temelju odgovarajućih standarda i preporuka.

Zaštitne mjere:

- Organizacijske mjere zaštite
- Fizičke mjere zaštite
- Programske mjere zaštite

3.4.1. Organizacijske mjere zaštite

Ove mjere se odnose na opće mjere zaštite informacijskih resursa, a koje su sastavni dio osnovnog sustava sigurnosti cjelokupnog poslovnog sustava. One se ne bave specifičnostima zaštite informacijskih resursa već osiguravaju okvir za provođenje specifičnih mjera zaštite.

Podrazumijevaju osiguravanje točnosti, ažurnosti i pravilnosti obavljanja poslova, a također i sprječavanje neovlaštenog izmjenjivanja podataka, dokumentacije te neovlaštenog korištenja mreže i informatičke opreme.

Organizacijskim mjerama se određuje:

- Program edukacije zaposlenika
- Odgovorna osoba za provedbu sigurnosti
- Organizacija prostora
- Kretanje unutar organizacije

Nakon adekvatne organizacije prostora, određuje se i imenuje osoba ili više njih za provedbu organizacijskih mjera unutar organizacije. Organizacijske mjere također podrazumijevaju definiranje i upravljanje kontrolom kretanja zaposlenika na radnome mjestu i klijenata unutar organizacije, u cilju zaštite informacijskih resursa. Na primjer u bankarskom sustavu propisuju se posebna pravila i upute za zaposlenike koji obavljaju financijske transakcije i upravljaju isplatama i uplatama novca. Najbitniji dio organizacijskih mjera zaštite odnosi se na edukaciju zaposlenika, korištenjem računalnih i informacijskih sustava, tehničke opreme i raznih uređaja potrebnih za uspješno izvršavanje radnih zadataka. Svaki informacijski sustav organizacije koji korisnicima omogućuje svoje usluge putem interneta, poput internet bankarstva,internet trgovine i sl., obvezan je na određeni način svoje korisnike redovito obavijestiti o mogućim propustima i napadačima, te izdavati brošure i naputke s mjerama sigurnosti koje korisnici mogu sami ostvariti u cilju opće sigurnosti i poslovanja.

3.4.2. Fizičke mjere zaštite

Ove mjere se odnose na onemogućavanje pristupa neovlaštenim osobama pojedinim informacijskim resursima. Za provođenje ovih mjera uglavnom se koriste tehnička sredstva te u manjoj mjeri i ljudi. Mjere fizičke zaštite moraju uzeti u obzir sve pristupne putove informacijskim resursima, a ne samo one koji se uobičajeno koriste.

Kako bi se uspostavila adekvatna zaštita potrebno je uzeti u obzir 3 aspekta, i to:

- kontrola fizičkog pristupa
- zaštita informacijskih uređaja i opreme
- zaštita okoline

Kontrolom fizičkog pristupa želi se ograničiti pristup opremi odnosno računalnim resursima ili određenim prostorima koji sadrže povjerljive informacijske resurse. Razina zaštite ovisi o povjerljivosti i vrijednosti informacija te razini određene prijetnje. Prema tome postoje različiti oblici kontole pristupa, a to su:

- pristupne kartice i čitači
- biometrijski čitači (otisak prsta, prepoznavanje lica, prepoznavanje šarenice, prepoznavanje glasa)
- kontrolni uređaji i programski paketi
- nadzorne kamere
- alarmni sustav

Pod okolinom se podrazumijeva okolina računala poslužitelja odnosno server te u njima pohranjenih osjetljivih podataka. Ovaj aspekt obuhvaća sve mjere potrebne za zaštitu od vanjskih nepovoljnih utjecaja na sustav.

Najbitniji dio informatičke opreme u sustavu su ti serveri jer u njima je sve pohranjeno i upravljaju svim infomracijama u sustavu. Stoga je potrebno da su server fizički odvojeni od ostalih uređaja i opreme. Pohranjuju se u posebne prostorije, a unutar prostorije u posebna kućišta koja ne bi trebala odolijevati vanjskim utjecajima.

Uz server računala fizička zaštita uređaja i opreme se odnosi na one kojima se služe zaposlenici u izvršavanju određenih funkcija i zadataka kao na primjer osobna računala koja se mogu zaštiti lozinkom i sl. Kako bi se osigurala učinkovita zaštita potrebno je provoditi edukaciju zaposlenika i korisnika o pravilnom načinu korištenja uređaja i opreme.

3.4.3. Programske mjere zaštite

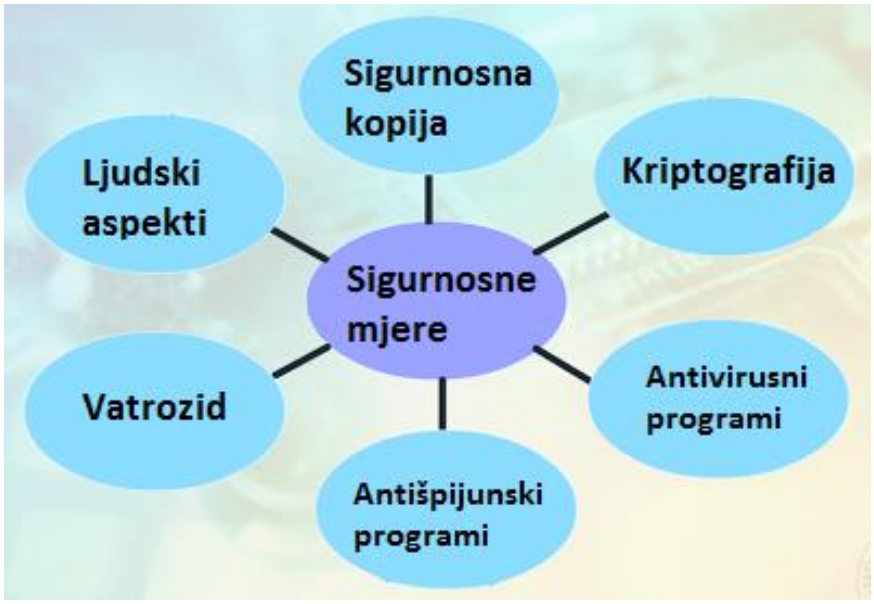
Programske mjere zaštite karakteristične su samo za dio informacijskih resursa i to podatke kao najvažniji informacijski resurs. Ove mjere se provode pomoću softvera. Mogu se podijeliti po nekoliko kriterija:

1. Prema funkciji:
    - Softverske kontrole pristupa radnoj okolini i informacijskim sadržajima predstavljaju osnovni mehanizam programske zaštite. Može se provoditi na više razina i od strane različitih softverskih komponenti, a za to koriste postupke identifikacije, autentifikacije i autorizacije
    - Kontrole formalne i logičke ispravnosti podataka koje se unose u baze podataka radi sprječavanja unosa pogrešnih podataka koji bi mogli imati negativan učinak na sustav
    - Osiguravanje tajnosti podataka posebice u mrežnom okruženju pri razmjeni podataka, odnosno u situacijama kada se ne provode mjere kontrole pristupa
    - Sigurnosne aktivnosti koje se provode u informatičkom sustavu kao povremeni i periodični poslovi radi analize stanja, preventive ili otklanjanja posljedica štetnih djelovanja
2. Prema softverskim sredstvima realizacije:
    - Pomoću sistemskog softvera koji se može raščlaniti na mjere zaštite pomoću:
        - operacijskih sustava
        - komunikacijskog softvera
        - pomoćnog softvera
        - sustava za upravljanje bazom podataka
    - Pomoću korisničkog softvera koji je bio najzastupljeniji do razvoja sistemskog softvera

Ove mjere se mogu realizirati na više načina i to:

- kriptiranjem
- Firewall
- antivirusnom zaštitom

- izradom sigurnosnih kopija i sl.



, *Slika 8. Načini realizacije mjera programske zaštite*

Izvor: http://panitiaictsmktp.blogspot.hr/2012/04/computer-security-security-measure.html

4. EMPIRIJSKO ISTRAŽIVANJE RAZINE INFORMACIJSKE SIGURNOSTI U POSLOVNIM ORGANIZACIJAMA

Za empirijski dio rada korištena je anketno istraživanje. Cilj ankete bio je utvrditi stanje informacijske sigurnosti u hrvatskim organizacijama. Postavljenim pitanjima utvrđivana je vrsta i veličina organizacije te neke osnovne informacije o stanju sigurnosti u tim organizacijama, pitanja će biti prikazana u nastavku.

Želja je bila ostvariti što veći odaziv na anketu, zbog statističke značajnosti rezultata, međutim zbog "osjetljivosti" ispitivanog područja na anketu se odazvalo 64 organizacije i to najviše trgovačkih društava, a zatim tijela državne uprave.

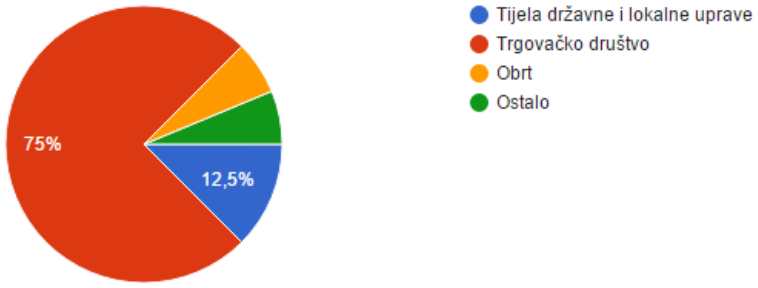
Od trgovačkih društava najveći dio predstavljaju srednja poduzeća (44%), a zatim mala poduzeća (25%). Oko 31% njih stanje informacijske sigurnosti ocjenjuje sa dobro, a po 25% sa vrlo dobro i izvrsno. Čak 37% bilo je na neki način napadnuto. Provjera ranjivosti sustava kod 56% ispitanih provodi se prema potrebi, a u slučaju incidenta 44% napad rješava samostalno dok ostatak traži pomoć vanjskih stručnjaka. Većina smatra da je najveća opasnost, za sigurnost organizacije, ponašanje zaposlenika, a dio da je to stanje informatičkog sustava i napad na sustav. Polovica ispitanih kao ključni faktor za zaštitu sustava smatra novac, a 31% svijest zaposlenih. Što se tiče sigurnosnih politika, njih 37.5% smatra da su one u njihovim organizacijama jasne i precizne, 37.5% da su prilično šture, a 20% da su osrednje definirane. Polovica smatra da je primjena tih politika zadovoljavajuća, 25% da je slaba, a oko 20% smatra da je izvrsna. Republika Hrvatska ima zakone kojima se regulira informacijska sigurnost, ali da su zakonski propisi u RH dobro osmišljeni, ali provedba nije zadovoljavajuća smatra 62.5%. Kada je riječ o ulaganjima u informacijsku sigurnost unutar organizacije, jako mali dio ulaže preko 50% sredstava namijenjenih za informatiku dok najveći dio (56%) ulaže 10-35%, a slijede ih oni koji ulažu manje od 10% i to čak 31% ispitanih.

Unatoč digitalizaciji i informatizaciji poslovanja u hrvatskoj se još uvijek informacijska sigurnost ne shvaća ozbiljno. Nedovoljno se ulaže u njen razvoj i nedovoljno se kontrolira. Trenutno stanje u svijetu je slično, ali prema rezultatima istraživanja provedenog od strane DNV GL- Business Assurance organizacije u budućnosti planiraju sve više ulagati u sigurnost, neće

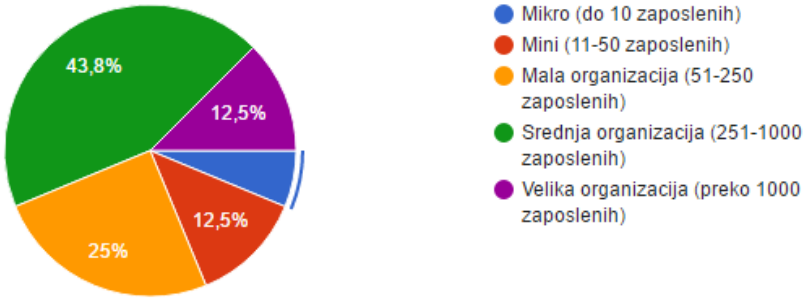
zanemariti zaštitu informacija i da će usvajati sustavni pristup kontrole i upravljanja sigurnošću. Sigurnost i zaštita informacija bi trebale biti ugrađene u kulturu organizacija i na tome bi trebalo raditi.

U nastavku slijede pitanja sa rezultatima:

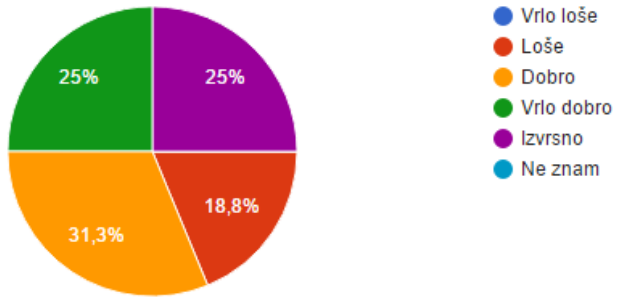
Odaberite vrstu organizacije u kojoj radite (64 odgovora)



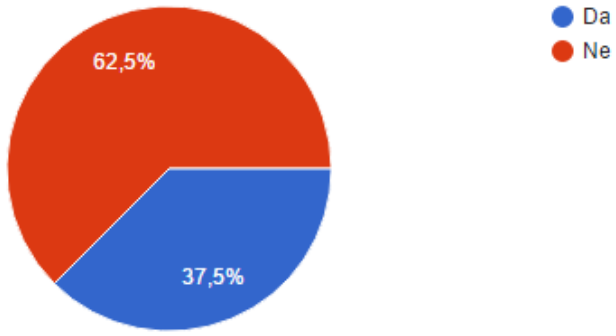
Veličina Vaše organizacije (64 odgovora)



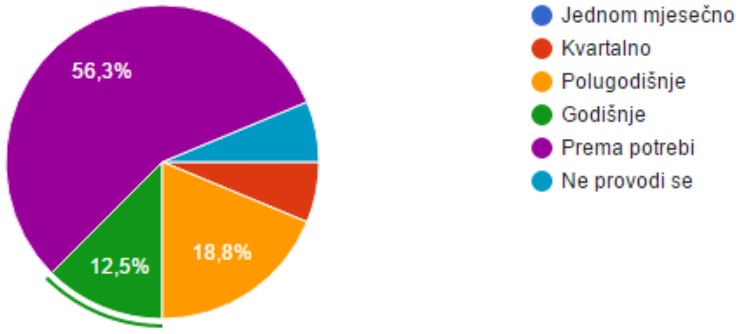
Ocjena stanja informacijske sigurnosti u Vašoj organizaciji (64 odgovora)



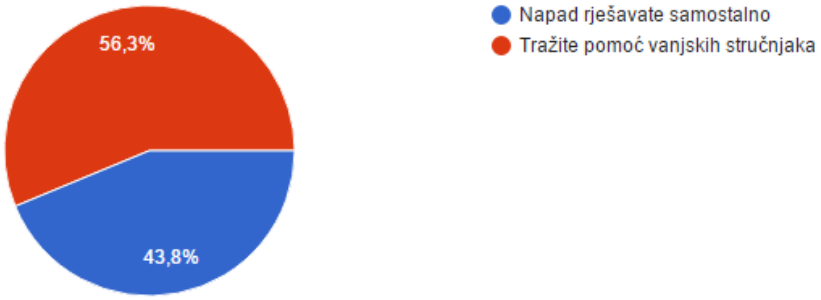
Jeste li Vi ili Vaša organizacija bili napadnuti? (64 odgovora)



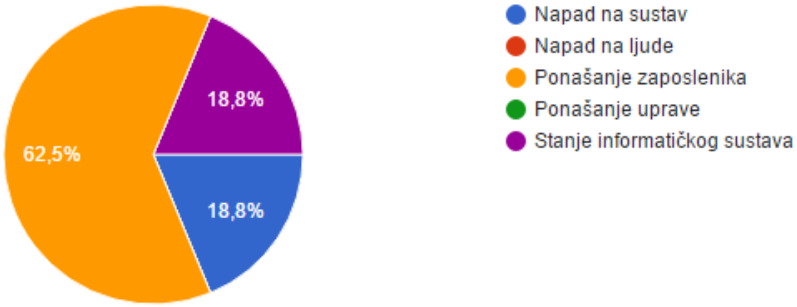
Provjera ranjivosti IT sustava u vašoj organizaciji provodi se: (64 odgovora)



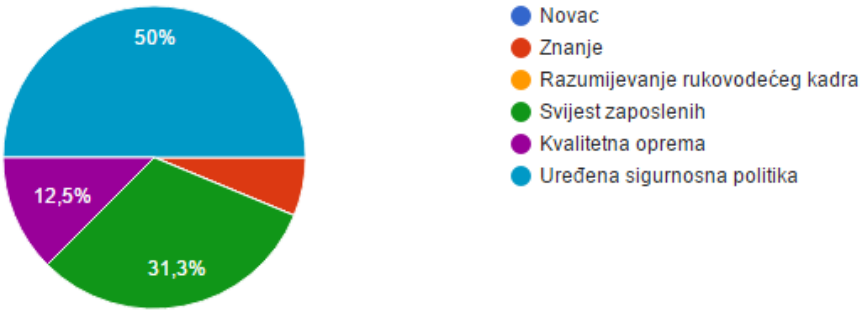
U slučaju većeg incidenta: (64 odgovora)



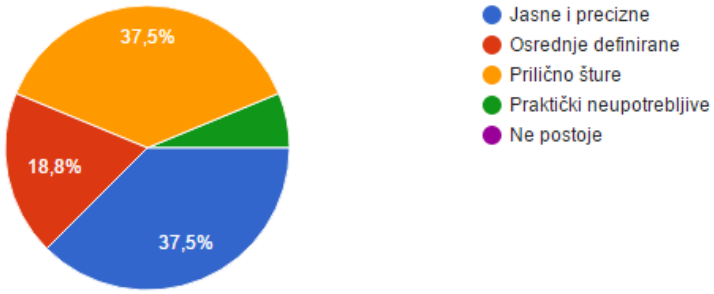
Po Vašem mišljenju, najveća opasnost za sigurnost Vaše organizacije je:
(64 odgovora)



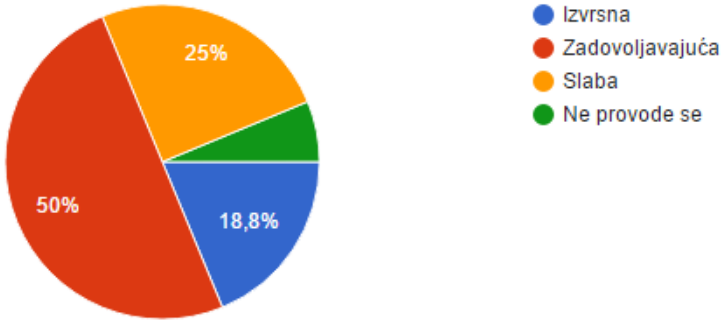
Ključni faktor za kvalitetnu zaštitu Vaših informacijskih sustava je: (64 odgovora)



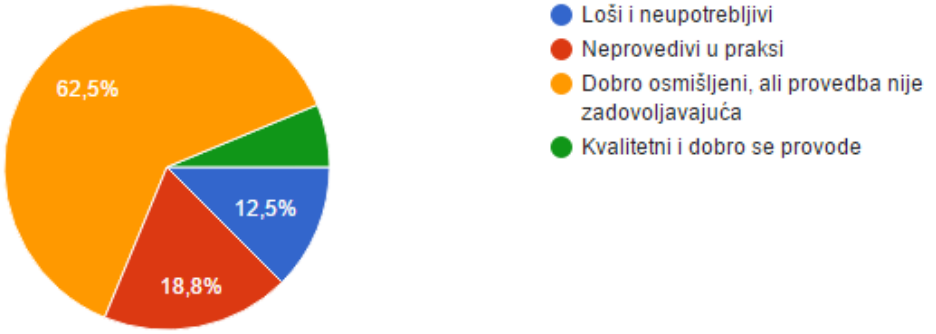
Politike vezane uz informacijsku sigurnost u Vašoj organizaciji su: (64 odgovora)



Primjena sigurnosnih politika u Vašoj organizaciji je: (64 odgovora)

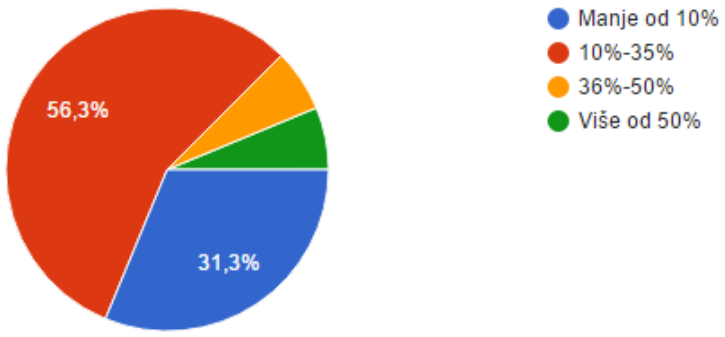


Zakoni i drugi propisi u RH vezani uz informacijsku sigurnost su: (64 odgovora)



Od ukupnih ulaganja unutar organizacije u informatiku, procijenite postotak ulaganja u informacijsku sigurnost

(64 odgovora)



5. ZAKLJUČAK

U današnjem poslovanju informacijski sustavi se smatraju sastavnim dijelom poslovanja. Svaki poslovni sustav se sastoji od niza informacija potrebnih za poslovanje kojima upravlja informacijski sustav. Prikupljanjem i obradom podataka postiže se temelj za donošenje odluka koji utječu na cjelokupno poslovanje.

Ovim radom se željelo prikazati osnove za uspostavu i zaštitu informacijskog sustava. Činjenica je da postoji određena razina opasnosti za sustav pogotovo u suvremenom poslovanju pa organizacije moraju biti toga svjesne i biti spremne na reakciju protiv mogućih prijetnji.

Postoji mnogo vrsta informacijskih sustava, najšira podjela je na informacijske sustave prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija. Samim time što je toliko podjela, a još više podjela unutar tih glavnih vidi se važnost funkcioniranja tog dijela u poslovnom sustavu. Odabirom pravog I odgovarajućeg informacijskog sustava za poslovanje bitno utječe na cjelokupno poslovanje neke organizacije, ali je potrebno konstantno provjeravati rad sustava radi održavanja prihvatljive razine rizika.

Modernizacijom i informatizacijom poslovanja sigurnosni rizik se povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi konkurentnost poslovne organizacije.

Zanemareni sustav informacijske sigurnosti, u smislu ne kontroliranja problema sigurnosti, vrlo lako može postati žrtvom napada. Sigurnost sustava bi se trebala periodično kontolirati, tražiti načine kako sustav učiniti još sigurnijim, otpornijim te implementirati dodatne sigurnosne kontrole koje savjetuju stručnjaci za informacijsku sigurnost.

U Republici Hrvatskoj postoji velik broj zakona, pravila, procedura kojima se upravlja informacijskom sigurnošću, ali su zaposlenici slabo odnosno nedovoljno educirani pa se informacije ne štite na prikladne načine.

LITERATURA:

1. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, http://www.iso27001security.com/html/27002.html
2. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems, http://www.iso27001security.com/html/27001.html
3. http://advisera.com/27001academy/hr/sto-je-iso-27001/
4. http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-003.pdf
5. Zakonski i podzakonski propisi i sigurnost informacijskih sustava, Biljana Cerin, dr.sc. Goran Vojković, http://www.snt.hr/boxcontent/news/Propisi_sigurnost.pdf
6. Sigurnosna politika CCERT-PUBDOC-2009-05-265, Nacionalni CERT, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf
7. Information technology- Security techniques- Code of practice for information security controls, 2013., http://www.slideshare.net/YounessFarah/iso-iec-270022013-code-of-practice-for-is-management-original
8. https://www.techopedia.com/definition/25830/cia-triad-of-information-security
9. https://www.qualys.com/solutions/compliance/iso-iec_27002/
10. Zakon o informacijskoj sigurnosti, Klasa: 650-05/07-01/01, Zagreb, srpanj 2007., http://narodne-novine.nn.hr/clanci/sluzbeni/298919.html
11. https://www.cerias.purdue.edu/assets/pdf/k-12/infosec_newsletters/03threats.pdf
12. https://msdn.microsoft.com/en-us/library/cc723507.aspx#XSLTsection127121120120
13. Osnove upravljanja rizikom informacijskog sustava, dr. sc. Suzana Stojaković, http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf
14. Fizička zaštita informacijskih sustava NCERT-PUBDOC-2010-06-304, Nacionalni CERT, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf
15. Identifying Information Security Threats; Timothy R. Stacey, Ronald E. Helsley, Judith V. Baston; http://www.ittoday.info/AIMS/DSM/82-10-41.pdf
16. Information Technology Threats and Vulnerabilities, http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm
17. Sustavi kontrole pristupa, Aleksandar Pašagić, http://www.generalsecurity.hr/radovi/Sustavi%20kontrole%20pristupa%20META%20br%209%20god%201%20svibanj%202009.pdf

18. Security and protection system, https://www.britannica.com/technology/security-and-protection-system
19. Security Intelligence https://securityintelligence.com/cyber-security-challenges-how-do-retailers-protect-the-bottom-line/#.VcxXnPkVjIU
20. https://books.google.hr/books?id=hbQIAAAAQBAJ&pg=SA1-PA19&lpg=SA1-PA19&dq=eps+electronic+physical+security&source=bl&ots=aRKzXXSs9f&sig=qNg6b738bpu58WYyCfR63fMBLlY&hl=hr&sa=X&ei=FZEEVLCIB4fmyQPT2ILgBw#v=onepage&q=eps%20electronic%20physical%20security&f=false
21. Laboratorij za Sustave i Signale, http://security.lss.hr/arhiva-dokumenata/fizicka-sigurnost-informacijskog-sustava.html
22. Information security is information risk management, Bob Blakley, Ellen McDermott, Dan Geer; http://ns2.datacontact.dc.hu/~mfelegyhazi/courses/EconSec/readings/03_Blakley2001infosec.pdf
23. http://net.hr/tehnoklik/vijesti-tehnoklik/informacijska-sigurnost-vise-od-trecine-globalnih-organizacija-trazi-metode-za-otkrivanje-cyber-napada/
24. DNV LG https://www.dnvgl.hr/news/sigurnost-informacija-organizacije-u-svijetu-planiraju-obranu-54323