Upravljanje rizicima informacijskog sustava

Marić, Andreja

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
SMJER INFORMATOLOGIJA
Ak. god. 2018./ 2019.

Andreja Marić

Upravljanje rizicima informacijskog sustava

Diplomski rad

Mentor: prof. dr. sc. Krešimir Pavlina

Zagreb, svibanj 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

1. Uvod

Danas je sigurnost informacijskih sustava od osobitog značaja. Razlog tomu je sve veća primjena informacijsko-komunikacijskih tehnologija u svim područjima javnog i privatnog života, zbog čega se organizacije i privatne osobe pojačano oslanjaju na informacijske sustave. Za svaku organizaciju koja primjenjuje informacijsko-komunikacijske tehnologije informacijski sustav postao je neizostavan dio. Iz tog je razloga sigurnost informacijskog sustava vrlo važna te se treba promatrati kao podloga za efikasno i uspješno poslovanje.

Svaka organizacija mora biti svjesna problema sigurnosti informacijskog sustava. Organizacija koja se služi digitalnim tehnologijama ima problema sa sigurnošću informacija i informacijskog sustava te je uvelike izložena različitim rizicima. Nije bitno gdje se informacija nalazi, ako ona i informacijski sustav nisu dovoljno zaštićeni, štete koje mogu nastati mogu biti ozbiljne. Iako se nijedan informacijski sustav ne može 100% zaštiti, uvijek se mogu poduzeti mjere koje će pridonijeti što većem stupnju zaštite. Bilo da se radi o maloj ili velikoj prijetnji, prijetnja je prijetnja i ne treba nijednu zanemariti. Pravovremeno uočavanje prijetnje omogućuje organizaciji da ublaži ili spriječi nastanak štete.

Iako proces upravljanja rizicima nije jednostavan proces, on predstavlja važnu komponentu za uspješno funkcioniranje informacijskog sustava, a time i same organizacije.

2. Svijet informacija

Pojam informacijskog sustava je povezan s druga dva pojma; *informacije* i *sustav.* Informacije čine ne samo ključni resurs informacijskog sustava već i najvažniji resurs 21. stoljeća. U današnjem svijetu, digitalnom svijetu, svijetu tehnologija raspoloživost informacijama je veća nego ikada. Svijet je preplavljen informacijama i ljudski mozak prima više informacija nego što može preraditi. Brzom širenju informacija pridonio je razvoj i napredovanje informacijsko-komunikacijske tehnologije. Bilo putem WWW-a[1], društvenih mreža ili pametnog mobitela, dovoljan je jedan klik i možemo doći do željene/tražene informacije. Međutim problem nije doći do informacija, nego čovjekova moć, sposobnost i znanje da njima ovlada. Promatrajući informacije kao fenomen i kao izvor znanja o nečemu, čovjek treba naučiti pomoću njih stjecati znanje i spoznaje te ih iskoristiti kao djelotvorno sredstvo na svim područjima ljudskog zanimanja.[2]

Komunikacija je dio svakodnevnog života, a to znači svakodnevno slanje i primanje informacija. Čak i kroz jednostavan razgovor dviju osoba, razmjenjuju se informacije. Čovjek prati događaje i procese, uočava i prikuplja podatke, očitava činjenice, stvara zabilješke i informacije, razmjenjuje i koristi ih, te na temelju svega toga praktično djeluje i posluje.[3] Vidimo kako se spominju i podaci i informacije. Ta dva pojma ponekad su zbunjujuća te se u praksi često poistovjećuju, no podatak nije isto što i informacija. Podaci se sastoje od skupa kvantitativnih parametara koji opisuju neku činjenicu ili zbivanje, oni sami za sebe nemaju nikakvo značenje, niti određuju svoj relativni značaj.[4] Tek obrađeni podatak, odnosno znanje o podatku, događaju ili pojavi predstavlja informaciju, te se iz informacije dobije potpunija slika o podatku.[5] Jednostavnije rečeno podaci se prikupljaju, a informacije stvaraju.

Informacija ima mnogobrojne definicije, kako u praksi tako i u teoriji. Jedna od njih je da je informacija skup podataka s pripisanim značenjem, osnovni element komunikacije koji,

[1] engl. *World Wide Web*: svjetska mreža, najčešće korišten internetski servis, koji korisnicima omogućava pregledavanje mnoštva digitalnih dokumenata danih na raspolaganje preko umreženih računala diljem svijeta (hrvatska online enciklopedija)

[2] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 9.

[3] Ibid., str. 27.

[4] Leksikografski zavod Miroslav Krleža (2019.) Hrvatska enciklopedija [online].
Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=27405

[5] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 29.

primljen u određenoj situaciji, povećava čovjekovo znanje.[6] Definicija informacije najčešće ovisi o pristupu, potrebi i interesu autora, ali i o načinu na koji se u pojedinoj znanosti ona može izraziti, ali zahvaljujući mogućnosti digitalnog oblikovanja i iskazivanja, one se svode na isti oblik prikazivanja, što omogućuje njihovu objektivizaciju.[7]

Vrste informacije prema različitim kriterijima:[8]

- prema nastanku (izvorne, izvedene)
- prema učinku (korisne, nekorisne)
- prema izvoru (unutarnje, vanjske)
- prema podrijetlu (vlastite, tuđe)
- prema pojavnom obliku (glasovne, pisane, zvučne, slikovne, zvukovne, znakovne)
- prema vjerodostojnosti (istinite, neistinite)
- prema otvorenosti (javne, tajne)
- prema sadržaju (osobne, opće, poslovne/funkcionalne)
- prema području djelovanja
- prema dospijeću (pravovremene, zastarjele)

Kao što vidimo postoji mnogo kriterija prema kojima se informacija može podijeliti, ali ne postoji kriterij koji svrstava informacije u dobre ili loše. Ona je onakva kakav joj je sadržaj i kakvom je učini onaj tko se njome koristi.[9] Jednoj osobi može biti korisna, dok drugoj beskorisna.

U demokratskim sustavima informacije su otvorene i kao takve predstavljaju temelj društva i društvenih odnosa. Izvori informiranja su disperzirani, a informacijski sustavi djeluju kao vrlo složene i otvorene mreže kroz koje informacije teku u svim smjerovima. Veliki dio društvenog i političkog djelovanja je usmjeren na ovladavanje informacijama, na otvaranje sustava informiranja i slobodan pristup informacijama.[10] Iako je cilj omogućiti građanima i institucijama slobodan pristup informacijama, važno je spomenuti kako nisu sve informacije uvijek otvorene i dostupne. Neke informacije je potrebno zaštiti kako ne bi došlo do

[6] Leksikografski zavod Miroslav Krleža (2019.) Hrvatska enciklopedija [online].
Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=27405
[7] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 32.
[8] Ibid., str. 33.
[9] Ibid., str. 41.
[10] Ibid., str. 42.

zlouporabe. Demokratska društva stoga zahtijevaju da se na području informacija poštuju određena načela u oblikovanju i upotrebi informacija kao što su:[11]

- Javnost informacija, što podrazumijeva dostupnost informacija građanima i institucijama kojima su podaci potrebni
- Objektivnost, kojom se izbjegava pristranost i prikazivanje informacija kako nekome odgovara
- Istinitost i točnost, čime se izbjegava poluistina
- Jasnoća i potpunost, čime se izbjegava dvosmislenost
- Pravodobnost, što omogućuje pravodobno procjenjivanje i donošenje odluka
- Sigurnost i zaštićenost, čime treba postići da informacija do korisnika dođe nepromijenjena, da ne dođe u ruke nekome tko bi ih mogao zloupotrijebiti, te da se spriječi štetno manipuliranje

Informacije čine podlogu za učenje, stjecanje znanja, predviđanje, donošenje odluka, bolje rezultate, poslovno djelovanje, veću sigurnost, natjecanje i drugo, a važne su jer omogućuju napredovanje u znanosti i tehnologiji, razvijanje poslovnih djelatnosti, bolje iskorištavanje prirodnih i drugih resursa, zbližavanje ljudi i naroda, razvoj komunikacija, osvajanje svemira, ovladavanjem genetskim kodom i temeljima života te jačanje opće i globalne sigurnosti svijeta.[12] A narušavanje načela, prvenstveno onih koji se odnose na dostupnost, cjelovitost i sigurnost informacija, predstavlja rizik kako za informacijski sustav tako i za organizaciju.

Vidimo kako informacije zaista predstavljaju jedan od najvažnijih resursa suvremenog svijeta. Ali u svijetu informacija pojavljuje se i problem. Na primjer: Ako se čovjek nalazi pred velikom nepreglednom količinom knjiga, a potrebna mu je jedna određena. Prvi korak koji će napraviti je postaviti si pitanje kako i gdje početi tražiti. Slično je i s informacijama. Svaki čovjek ima svoje ciljeve, interese i potrebe, koje želi postići i zadovoljiti, a kako je današnji svijet preplavljen informacijama, postavlja se pitanje kako doći do informacija koje su potrebne za ostvarenje upravo tih ciljeva i interesa. Da bi se pojedincu ili bilo kojoj drugoj društvenoj strukturi ili organizaciji to omogućilo, informacije treba stalno prikupljati, sređivati i skladištiti, te stvoriti sustav koji će omogućiti brz pristup skladištima (informacijskim bazama), pretragu i izbor, a potom i njihovu korisničku obradu koja će

[11] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 43
[12] Ibid.

olakšati donošenje potrebnih odluka.[13] Skladišta podataka pružaju integrirani i cjeloviti pogled na organizaciju i predstavljaju fleksibilan i interaktivan izvor informacija.[14]

Spominje se sustav, no što je uopće sustav i kako ga definirati. Definicija sustava najčešće ovisi o njegovoj vrsti i ulozi, no bez obzira na to, vrijedi; svaki sustav je skup elemenata ustrojen na određenoj jedinstvenoj ideji (koncepciji, teoriji, zakonu), s odgovarajućom strukturom i povratnim vezama između elemenata i ulazno-izlaznim vezama s okruženjem, definiranim funkcijama djelovanjem kojih ostvaruje svrhu i cilj svojega postojanja, a strukturu čine:[15]

- Stvaraoci
- Ideja
- Organizacijske cjeline
- Odnosi i veze
- Funkcije i poslovi
- Informacije i upravljanje

Svaki sustav predstavlja uređenu cjelinu, koja se sastoji od međusobno povezanih elemenata i koji međusobnim djelovanjem izvršavaju neku funkciju. Kako bi se olakšalo prikupljanje, pretraživanje, obrađivanje i pohranjivanje informacija razvili su se informacijski sustavi.

[13] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 75.

[14] Garača, Ž., Ćukušić, M. (2011.) Višedimenzijski informacijski sustavi. Skladištenje i analitička obrada podataka. Split: Ekonomski fakultet, str. 5.

[15] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 75.

3. Informacijski sustav

Informacijski sustav (eng. *Information System* ili *IS*, akronim koji će se koristiti dalje u tekstu) je organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podaci i informacije značajne za neku organizaciju, ustanovu, društvo ili državu.[16] Promatrajući definiciju može se reći kako suvremeni IS nije samo organizirani skup postupaka, već se sastoji od različitih komponenti koje zajedno čine informacijski sustav. Informacijski sustav kao organizacijsko-funkcijski sustav predstavlja sustav sastavljen od niza komplementarnih komponenti koji koordiniranim djelovanjem omogućuju prikupljanje (ulaz), obradu, pohranjivanje i distribuciju (izlaz) informacija za potrebe provedbe poslovanja i upravljanja nekim subjektom.[17] Bez obzira radi li se o općem, funkcionalnom ili poslovnom informacijskom sustavu svaki od njih ima isti zadatak, a to je pružiti što kvalitetniju, pravu i relevantnu informaciju i omogućiti da protok informacija bude što brži, lakši i sigurniji.[18]

3.1. Funkcije informacijskog sustava

Gledajući informaciju kao glavni resurs IS-a, njegove osnovne funkcije mogu se podijeliti na:[19]

- Prikupljanje i upis podataka u bazu podataka
- Obradu (procesiranje) podataka
- Prikaz i ispostavljanje podataka iz baze podataka
- Čuvanje (dokumentiranje, trajno pohranjivanje) podataka.

Podatak je glavni sadržaj informacije i svaki podatak u informacijskom sustavu zapravo je informacija, a model podataka zapravo model informacija zapisan na što kraći način. Informacijski sustavi teže tomu da u najkraćemu mogućem obliku zapišu podatke u bazu podataka kako bi njima lakše i brže manipulirali, te da svakom korisniku pri pogledu na bilo koji dio IS-a uvijek bude jasna informacija.[20]

[16] Leksikografski zavod Miroslav Krleža (2019.) Hrvatska enciklopedija [online].
Dostupno na: http://www.enciklopedija.hr/Natuknica.aspx?ID=27410
[17] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 18., str. 37.
[18] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 76.
[19] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 30.
[20] Ibid.

Osim temeljnih funkcija (prikupljanje, obrada, prikaz i čuvanje podataka i informacija) IS podrazumijeva i sljedeće funkcije:[21]

- Stvaranje bogatih informacijskih baza, koje će biti dostupne svim zainteresiranim korisnicima
- Omogućavanje brzog pristupa informacijskim bazama, njihovog djelotvornog pretraživanja i brzog pronalaska informacija
- Pružanje informacijskih usluga
- Informatičku i informacijsku korisničku obradu podataka i informacija i njihovu odgovarajuću prezentaciju
- Poboljšavanje i razvijanje informacijske djelatnosti te
- Uključivanje u informacijsko-komunikacijske mreže, posebno na internet.

Svaki informacijski sustav upisuje ulazne podatke u bazu podataka iz koje generira izvješća (proces transformacije podataka iz baze podataka u podatke potrebne korisnicima).[22] Postoje različite vrste baza podataka, ali se uvijek radi o sustavno uređenim podacima i informacijama u skladu s namjenom i pravilima prema kojima se baza organizira i podaci spremaju i prema kojima će se uzimati kada zatrebaju.[23] Prije otkrića računala bazu podataka predstavljali su papirnati arhivi, a ulazni i izlazni dokumenti bili su dio te baze podataka. Otkrićem računala i na osnovi informacijskih i komunikacijskih tehnologija omogućena je izgradnja automatiziranog informacijskog sustava, tako da se automatiziraju funkcije IS-a.[24]

3.2. Komponente suvremenog informacijskog sustava

Kako se suvremeni informacijski sustavi posebno oslanjaju na informacijsku i digitalnu tehnologiju, ona postaje sastavnim dijelom suvremenih IS-a, koji kao složeni sustavi sastavljeni od više cjelina čine informacijsku infrastrukturu. Sve komponente (cjeline) aktivno i trajno djeluju jedna na drugu kao uzrok i istodobno posljedica.[25]

[21] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 81.
[22] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 35.
[23] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 81.
[24] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 35.
[25] Panian, Ž., Strugar, I. (2013.) Informatizacija poslovanja. Zagreb: Ekonomski fakultet, str. 28.

Osnovne komponente (cjeline) suvremenog informacijskog sustava su:[26]

- Hardver (*eng. Hardware)* predstavlja materijalnu osnovicu IS-a, to jest ukupnost materijalne opreme IS-a. Hardver obuhvaća elektroničko računalo, ulazno-izlazne uređaje, dio uređaja i sredstava za komuniciranje i prenošenje podataka na daljinu, a koji je posredni dio računala i ostalu računalnu opremu za obradu podataka.
- Softver (*eng. Software)* obuhvaća nematerijalne elemente IS-a, odnosno ukupnost programske opreme IS-a. Softver obuhvaća sve sustavne i aplikativne programe i programske pakete. Programi koji pomažu korištenju IS-a, korisničku uvježbanost i korištenje svih metoda vezanih uz organizaciju, upravljanje, obrađivanje i korištenje rezultata obrade podataka i informacija.
- Netver (*eng. Netware)* čini mrežnu osnovicu IS-a, odnosno ukupnost mrežne opreme IS-a. Netver se sastoji od komunikacijsko hardversko-softverske opreme, mrežno ulazno-izlaznih uređaja, uređaja i sredstava za komuniciranje i prenošenje podataka na daljinu, a koji nisu dio računala, te od ostale komunikacijske opreme za olakšavanje daljinske obrade podataka.
- Lajfver (*eng. Lifeware)* je kadrovska ljudska osnovica IS-a. Lajfver predstavlja ekipu informatičkih stručnjaka (organizatora elektroničke obrade podataka, sustavnih analitičara, programer, operatera, te laika korisnika IS-a, sa svim njihovim specijaliziranim informacijskim znanjima, a koja su relevantna tijekom određenog životnog ciklusa IS-a.
- Orgver (*eng. Orgware)* predstavlja ukupnost svih organizacijskih postupaka, metoda, mjera, postupaka aktivnosti i načina usklađivanja te povezivanja svih komponenti IS-a u jedinstvenu, sustavnu, skladnu, funkcionalnu, ekonomičnu, i djelotvornu cjelinu.

Kako je IS povezan sa svojom okolinom, povezan je i s komponentama u toj okolini, odnosno komponentama koje ga okružuju kao na primjer drugi organizacijski sustavi i njihovi informacijski sustavi, korisnici, dobavljači, kupci, institucija i vlada.[27]

Kao korisnike informacijskog sustava smatraju se sve pravne i fizičke osobe, koje kao zaposlenici subjekta, vanjski suradnici, klijenti, regulatorne institucije ili u bilo kojoj drugoj

[26] Šimović, V., Ružić-Baf, M. (2013.) Suvremeni informacijski sustavi. Pula: Sveučilište Jurja Dobrile u Puli, str. 227.
[27]Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 39.

ulozi sudjeluju u procesima podataka.[28] Korisnik informacijskog sustava je osoba, organizacija ili neki drugi entitet (uključujući računalo i računalni sustav), koji se koristi računalom, servisnim uslugama i slično.[29] Osoba (pravna ili fizička) koristi IS kako bi obavila funkciju organizacijskog sustava u postizanju cilja, a koja nije računalni stručnjak, odnosno nije dio tehničkog tima za održavanje ili izgradnju informacijskog sustava.[30] Osoba koja nije dio organizacijskog sustava, a koristi se funkcijama informacijskog sustava u postizanju svojih ciljeva, predstavlja vanjskog korisnika (klijenti, revizori, porezni službenici, kontrolni i nadzorni inspektori).[31]

Sve komponente IS-a međusobno su povezane i u interakciji i temelje se uglavnom na računarskim mrežama. Računala povezana prema određenim načelima i pravilima čine mrežu. Mreže se stvaraju na lokalnim (LAN – eng. *Local Area Network*), nacionalnim i međunarodnim mrežama (MAN – eng. *Metropolitan Area Network*, WAN – eng. *Wide Area Network*), koja udružuje njihove potencijale, stavljajući ih na dohvat svakom dijelu mreže.[32] Računarske mreže omogućuju računalima jednostavno i brzo međusobno razmjenjivanje podataka i informacija.

3.3. Vrste informacijskog sustava

Postoje raznovrsni informacijski sustavi i ne bi bilo kraja njihovom nabrajanju i opisivanju. Općenita podjela IS-a mogla bi biti prema osnovnoj namjeni, načinu prikupljanja i obradi informacija te prema tipu upravljanja.

Prema osnovnoj namjeni informacijski sustavi mogu se podijeliti na:[33]

- Sustave za prikupljanje i obradu podataka (informatički sustavi),
- Informirajuće sustave – sustave informiranja (1 – za vanjsko informiranje, informiranje javnosti, građana, poslovnih partnera; 2 – za unutarnje informiranje, informiranje zaposlenika i organizacijskih jedinica; 3 – za informiranje informatora,

[28]Hrvatska agencija za nadzor financijskih usluga (2014.) Smjerniceza primjereno upravljanje rizicima informacijskih sustava subjekata nadzora [online]. Dostupno na: https://www.hanfa.hr/objave-sa-sjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/ , str. 2. [28. veljače 2019.]

[29] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 57.

[30] Ibid.

[31] Ibid.

[32] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 96.

[33] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT, str. 82.

- sustave informacija koji su podloga svim informacijskim, poslovnim i drugim upravljivim sustavima,
- integralne (cjelovite) informacijske sustave, koji funkcionalno i organizacijski obuhvaćaju cjelinu informacijskih funkcija i poslova.

Prema načinu prikupljanja informacija, IS-i dijele se na formalne i neformalne. Formalni IS sadržava informacije prikupljene na pravilan i unaprijed definiran način, nužne za funkcioniranje organizacije. Dok se informacije neformalnih IS-a sastoje od razgovora radnika, uvjeravanja kupaca, ideja, osobnih podataka i slično.[34]

S obzirom na tip upravljanja, informacijski sustavi se mogu podijeliti na izvršne i upravljačke. Izvršni IS je sustav o temeljnim poslovnim procesima organizacije, dok upravljački osigurava informacije za upravljanje organizacijom, kao na primjer sustavi za potporu odlučivanja.[35]

S obzirom na sredstva za obradu informacija, IS dijeli se na mehanografski, računalni i ručni. Računalni informacijski sustav je onaj sustav koji se oslanja i koristi informacijsku tehnologiju. Mehanografski IS je sustav zasnovan na strojevima koji u svojoj konstrukciji nemaju mikroprocesor, a ručni informacijski sustavi se za obradu i čuvanje podataka koriste ljudskim radom.[36] Ručni informacijski sustavi iako zastarjeli danas još uvijek postoje, međutim u praksi na njih vrlo rijetko nailazimo.

IS se organiziraju kao javni i "privatni" te opći i funkcionalni. Javni su usmjereni prema svim građanima i strukturama društva i organizirani na regionalnoj, nacionalnoj i međunarodnoj razini, dok su "privatni" informacijski sustavi sustavi privatnih organizacija.[37] Opći informacijski sustavi se bave svim vrstama informacija i okrenuti su raznim korisnicima, a za razliku od općih, funkcionalni IS organiziraju se s točno utvrđenom namjenom i ciljem i bave se samo informacijama koje služe provedbi postavljenog cilja ili programa.[38] Funkcionalni informacijski sustavi danas su sve češći, a posebnu ulogu među njima igraju poslovni informacijski sustavi.

[34] Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d., str. 40.
[35] Ibid.
[36] Ibid.
[37] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT, str. 82.
[38] Ibid.

3.4. Informacijski sustav kao dio poslovnog modela

"Digitalan", svojstvo koje opisuje današnji (poslovni) svijet. Današnji svijet obilježava digitalno doba i okruženje digitalne ekonomije. Digitalna ekonomija podrazumijeva nove modele poslovanja, proizvoda usluga, tržišta i brzo rastućih sektora ekonomije, koja se temelji na intenzivnoj primjeni digitalnih tehnologija, prvenstveno informacijsko-komunikacijske tehnologije, u neprekidnom procesu inovacije, kreativnosti stvaranja nove vrijednosti.[39] Novi modeli poslovanja se gotovo pa u potpunosti oslanjaju na informacijsku i digitalnu infrastrukturu, a kako su informacije izvor znanja i predstavljaju temelj poslovne snage i moći, novi modeli poslovanja se prije svega oslanjaju na funkcioniranje njihovih informacijski sustava,[40] stoga nije pogrešno reći kako je informacijski sustav danas gotovo pa neizostavan dio neke poslovne organizacije.

Informacijski sustav koji prikuplja, obrađuje, pohranjuje i čuva informacije važne za potrebe provedbe poslovanja i upravljanja nekim poslovnim subjektom (poslovne informacije) naziva se poslovni informacijski sustav. Poslovne informacije su sve informacije u funkciji unutarnjeg i vanjskog djelovanja poslovnog subjekta za ostvarivanje poslovnih interesa i ciljeva.[41] Svaka poslovna organizacija svojom djelatnošću stvara određene podatke. Ti podaci mogu proizaći iz prirode djelatnosti kao na primjer prodaja ili nabava, iz zakona i drugih propisa ili iz unutarnjih poslova kao što su odnosni među radnicima.[42] Izvori poslovnih informacija su informacijski obrađeni poslovni podaci spremljeni u određene informacijske baze ili druge nositelje informacija (primjerice poslovna knjiga).[43] Informiranje unutar organizacije značajno je i sa stajališta motivacije zaposlenih i način informiranja i sadržaj informacija vrhovni menadžment prilagođava svojim potrebama, a informacije bi se trebale odnositi na:[44]

- Opće ciljeve organizacije,
- Stupanj pouzdanosti odvijanja poslovnih procesa,

[39] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 6.
[40] Ibid., str. 37.
[41] Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga, str. 116.
[42] Ibid., str. 117.
[43] Ibid.
[44] Drljača, M. (2006.) Model informacijskog sustavaza upravljanje poslovnim -procesom. Kvaliteta: Časopis za unapređenje kvaliteta [online]., 16 (5-6): str. 47-51. Dostupno na: https://bib.irb.hr/prikazi-rad?&rad=520681 [10. ožujka 2019.]

- Stupanj zadovoljstva kupaca/korisnika kvalitetom proizvoda ili usluga organizacije i
- Poslovni rezultat organizacije

3.4.1. Poslovni informacijski sustavi

Poslovni informacijski sustav (*eng. Enterprise Information System, EIS)* je informacijski sustav koji podržava i informacijski poslužuje poslovne procese i operacije, poslovno odlučivanje te razvijanje i implementaciju kompetetivnih strategija poslovanja.[45]

Osnovne funkcije IS-a kao dio poslovne organizacije su:[46]

- Provoditi poslovne transakcije
- Dokumentirati poslovne transakcije i pohranjivati podatke i
- Izvještavati o stanju poslovanja

Poslovni informacijski sustav sastoji se od tri sloja (izvršni, upravljački i suradnički). Provođenje poslovnih transakcija i transakcijski procesi dio su izvršnog sloja. Transakcija (engl. *Transaction*), uvijek označava dvosmjerna davanja – razmjenu vrijednosti između dviju ili više strana.[47] Transakcijski sustav je dio poslovnog informacijskog sustava koji obrađuje poslovne transakcije IS-a, te može imati materijalne (na primjer novčanice s bankomata) i informacijske (podaci na potvrdi o izdanom novcu) ulaze i izlaze.[48] Svaku provedenu transakciju potrebno je dokumentirati, a podatke pohraniti.

Kako bi poslovanje bilo što efikasnije i djelotvornije te kako bi se ostvarili postavljeni ciljevi, informacije kojima informacijski sustav raspolaže moraju biti kvalitetne, jer su one potrebne za donošenje dobre poslovne odluke. Odlučivanje i upravljanje (operativno, strateško, taktičko) dio su upravljačkog sloja IS-a, koji pruža potporu svima koji donose odluke, predočavajući potrebne informacije.[49]

S druge strane suradnički sloj čine sudionici unutar i izvan organizacije, koji međusobno surađuju i komuniciraju i na različite načine obrađuju podatke.[50] Sustav za komunikaciju i suradnju (podsustav IS-a) koristi informacijsku tehnologiju za obavljanje različitih

[45] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT, str. 3.
[46] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 37.
[47] Poslovni dnevnik-Leksikon [online]. Dostupno na: http://www.poslovni.hr/leksikon/transakcija-1895
[48] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT, str. 17.
[49] Ibid., str. 20.
[50] Ibid., str. 24.

administrativnih poslova kao na primjer elektroničko glasovanje, priprema podataka za prezentaciju, pretraživanje dokumenata.[51]

Ovisno o vrsti poduzeća/organizacije za koji je poslovni IS izrađen, oni mogu biti standardni ili složeni. Standardni poslovni IS obuhvaća samo minimum nužnih funkcija i prema potrebi pridodaju mu se oni elementi (podsustavi) koji proizlaze iz mogućih posebnosti konkretnog poslovanja. Na primjer informacijski sustav fakulteta morat će pružati potporu – osim standardnim funkcijama – i funkciji evidencije studenata, koja nije karakteristična za ostala poduzeća/organizacije.[52] Ako je IS dio poduzeća, radi se o složenom sustavu, broj elemenata (podsustava) se uvelike povećava te dolazi do raščlanjivanja cjelovitog informacijskog sustava na:[53]

- Informacijski podsustav analize i planiranja poslovanja,
- Informacijski podsustav upravljanja trajnom poslovnom imovinom,
- Informacijski podsustav upravljanja ljudskim resursima,
- Informacijski podsustav računovodstva i upravljanja financijama,
- Informacijski podsustav nabave i ulazne logistike
- Informacijski podsustav proizvodnje
- Informacijski podsustav prodaje i izlazne logistike

Uzimajući broj podsustava u obzir, vidimo kako poslovni IS pridonosi uvelike normalnom odvijanju poslovanja poduzeća. Sada zamislimo da dođe do napada na informacijski sustav, poslovanje bi u tom trenutku vrlo vjerojatno stalo i nastao bi trenutni kaos. Iz tog razloga informacijska sigurnost i sigurnost informacijskog sustava je od osobitog značaja. Sigurnosni incidenti imaju sve veći utjecaj na poslovanje, a narušavanje sigurnosti (poslovnog) informacijskog sustava može uzrokovati financijske i druge štete. Stoga je vrlo važno posvetiti pažnju upravljanju rizicima IS-a, kako bi se opasnosti koje mu prijete svele na minimum.

[51] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT, str. 24.
[52] Ibid., str. 61.
[53] Ibid., str. 62.

4. Pojam rizika i proces upravljanja rizicima

Moglo bi se reći da se čovjek svaki dan suočava s nekom vrstom rizika, primjerice odlazak s autom na posao. U posljednje vrijeme broj automobilskih nesreća sve je veći i odlučimo li s autom ići na posao izlažemo se riziku od prometne nesreće, odnosno pitamo se kolika je vjerojatnost da će se zaista dogoditi nesreća.

Etimologija riječi i porijeklo rizika su nepoznati, međutim smatra se da potječe iz srednjovjekovne Italije te znači opasnost, štetu i slično. U Italiji u srednjem vijeku kulturna i ekonomska revolucija izazvala je pojavu brojnih financijskih inovacija kao knjigovodstvo, osiguranje, ugovori o kupnji, terminski ugovori i slično, a sve kako bi se izbjegao rizik.[54] Tada je rizik predstavljao potencijalnu opasnost gubitka nečega što ima vrijednost, te su se sukladno tome pojavljivale prve znanstvene analize upravljanja rizicima, pokrenute iz ekonomskih razloga.[55] Za razliku od prošlih vremena, danas se u rizik ubrajaju i situacije iz svakodnevnog života. Čovjek je tijekom svog života gotovo pa prisiljen birati između alternativa, a tijekom donošenja odluka postavljat će si uvijek iznova pitanje: što će se dogoditi, ako...? Prema tome rizik sam po sebi predstavlja vjerojatnost da je neki ishod nepovoljan/štetan. U kojoj je mjeri ishod povoljan ili nepovoljan vrlo je subjektivno i ovisi o situaciji, što znači da isti ishod za nekoga može predstavljati dobit, dok za drugoga gubitak.

Rizik prati i neizvjesnost. No za razliku od neizvjesnosti rizik se može mjeriti, na primjer bacanje kocke; vjerojatnost da će se prilikom bacanja pojaviti šestica je 1:6, kod neizvjesnosti takvo mjerenje ne postoji, jer je ishod u potpunosti nepoznat. Na temelju toga se može zaključiti da je rizik rezultat nekog budućeg događaja iz kojeg se očekuju različiti međusobno isključivi rezultati s poznatom (pretpostavljenom) vjerojatnošću, dok je neizvjesnost rezultat nekog budućeg događaja kod kojega ne postoji takva vjerojatnost, uzimajući to u obzir, svaki budući događaj može biti:[56]

- siguran
- rizičan
- nemoguć i
- neizvjestan

[54] Vukičević, M., Odobašić, S. (2012.) Upravljanje rizicima. Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti "Baltazar Adam Krčelić", str. 15.
[55] Ibid.
[56] Ibid., str. 29.

4.1. Klasifikacija rizika

Ne postoji jedinstvena podjela rizika, te se mogu klasificirati na različite načine. Klasifikacija rizika (eng. *Class of risk, Classification of risks*) je razvrstavanje rizika u pojedine skupine.[57] Rizici općenito mogu imati pozitivan (rizik predstavljen kao prilika), negativan (rizik predstavljen kao gubitak) ili neutralan ishod.[58] Postoje razne vrste i podjele svih pojavnih oblika rizika kao što su čisti, špekulativni, temeljni, zajednički, pojedinačni, objektivni, subjektivni i tako dalje.[59] Primjer čistog (hazardnog) rizika je krađa ili požar. Čisti rizici čine osnovni predmet osiguranja, te je organizacija u mogućnosti napraviti planove i programe odgovarajuće tolerancije tih rizika.[60] Rizici mogu isto tako biti poslovni, financijski, informatički, bankarski i drugi, no ne uzimajući u obzir veličinu entiteta i djelatnost, rizici se mogu podijeliti s obzirom na:[61]

- Pristup – opći i specifični rizici (na primjer: čisti rizik)
- Vezivanje – poslovni (vezan za ostvarivanje bruto financijskog rezultata poduzeća) i neposlovni rizik
- Porijeklo – unutarnji (nastaju u samoj organizaciji) i vanjski (svi utjecaji koji dolaze izvan organizacije) rizik
- Očekivanja – realni i oportunitetni rizik (sa stajališta predviđanja očekivanih poslovnih rezultata)
- Stvaranje dobiti – špekulativni i hazardni (isključivo ostvarenje gubitka) rizici
- Prenošenje – prenosivi (mogućnost prenošenja na drugu stranu) i neprenosivi rizici
- Mjerenje – mjerljivi (moguće izračunati eventualnu štetu) i nemjerljivi rizici
- Utjecaj – subjektivni (vezani uz poslovne odluke) i objektivni rizici
- nastup – direktni i indirektni rizici
- Pojavnost – tipični i atipični (pojavljuju se naglo) rizici
- Brzinu – katastrofični (npr. elementarne nepogode) i puzajući (stalno prisutni unutar poduzeća) rizici

[57] Andrijanić, I., Gregurek, M., Merkaš, Z. (2016.) Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada, str. 43.
[58] Ibid.
[59] Vukičević, M., Odobašić, S. (2012.) Upravljanje rizicima. Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti "Baltazar Adam Krčelić", str. 29.
[60] Andrijanić, I., Gregurek, M., Merkaš, Z. (2016.) Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada, str. 44.
[61] Ibid., str. 45.

4.2. *Cyber* rizici

Suvremeni informacijski sustavi izloženi su najčešće informatičkim rizicima, ponajprije *cyber* rizicima. Takvi rizici mogu izazvati financijske štete, štete unutar i na okruženje organizacije.

Informatički rizici predstavljaju vjerojatnost nastanka nekoga neželjenoga događaja (prijetnje) koja u danim okolnostima može uzrokovati štetu, zastoj ili umanjenje intenziteta rada IS-a ili štetu nad informacijama koje su u njemu pohranjene.[62] *Cyber* rizici su one vrste informatičkih rizika koje se odnosne na intenzivnu primjenu digitalnih tehnologija u poslovanju i što organizacije više koriste suvremene informacijske i digitalne tehnologije, to će biti i više izložene *cyber* i informatičkim rizicima.[63]

Postoje različite vrste informatičkih rizika, a to su:[64]

- Strateški informatički rizici; rizici neusklađenosti poslovanja i informatike, odnosno svi rizici kojima se ugrožavaju strateški poslovni interesi
- Rizici provedbe informatičkih programa i projekata; rizici da ulaganja u informatiku neće biti ispravno vođena, te rizici da provedba tih ulaganja kroz informatičke programe i projekte neće biti učinkovita ili neće doprinijeti stvaranju nove vrijednosti
- Rizici provedbe poslovnih procesa (operativni ili transakcijski); rizici izmjene informacijske tehnologije u redovitoj provedbi poslovnih procesa
- Infrastrukturni informatički rizici; rizici rada informatičke infrastrukture i opreme i svi ostali rizici koji se odnose na redovito funkcioniranje informatičke infrastrukture

Informatički rizici su uvijek prisutni, te imaju dvojnu narav:[65]

- dobro vođene informatičke inicijative stvaraju novu vrijednost, nove poslovne prilike i održivu konkurentsku prednost
- loše vođene informatičke inicijative uništavaju poslovanje, ne stvaraju nove vrijednosti, a troše resurse i stvaraju gubitke.

Što se tiče napada na informacijski sustav, najčešće se radi o napadima koji su usmjerni na krađu identiteta korisnika (phishing, društveni inženjering, keystroke loggers i drugi) i

[62] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 74.
[63] Ibid., str. 38.
[64] Ibid., str. 63.
[65] Ibid., str. 62.

napadima osmišljenima s ciljem krađe podataka i izmjene sadržaja (prisluškivanje, nasilni i neovlašteni upadi u računalne mreže, presretanje poruka, zlonamjerni računalni kôd).[66]

Društveni inženjering (eng. *Social Engineering*) obuhvaća brojne i raznovrsne načine pribavljanja lozinki za neovlašteni pristup sustavu, najpoznatiji su *Shoulder surfing* (otkrivanje lozinke neposrednim fizičkim uvidom, pri čemu žrtva nije svjesna) i *Scavenging* (traženje po tuđem smeću kako bi se našla lozinka za pristup sustavu).[67] Tehnike koje koristi društveni inženjering su sve zapravo tehnike pasivnog prikupljanja informacija i tehnike napada ostalih grana sigurnosti kao na primjer iskorištavanje ranjivosti računalnog sustava.[68] Razvijanje odnosa i povjerenja čini srž socijalnog inženjeringa. Cilj napadača je stjecanje povjerenja žrtve, te kasnije iskorištavanje istoga. Napadač najprije prikupi informacije koje su javno dostupne (novine, vijesti, web portali i slično), a zatim se lažno predstavi i pomoću prikupljenih informacija učini priču uvjerljivom.[69]

Phishing je tehnika društvenog inženjeringa. Odnosi se na aktivnosti kojima prevaranti i računalni kriminalci slanjem lažnih elektroničkih poruka, koje izgledaju kao da su ih poslale izvorne institucije, dobiju pristup povjerljivim korisničkim podacima.[70] *Phishing* koristi tehnike obmane i općenite tehnike napada na računalnu sigurnost. Kako bi obmana uspjela, poruka mora biti uvjerljiva, a prvi korak ka tome je lažno predstavljanje. Napadač se predstavlja ili kao već postojeća osoba/organizacija ili kao nepostojeća, ali relevantna osoba/organizacija.[71] Tehnike *phishing*a se mijenjaju sukladno s ljudskim navikama kao i socijalnim normama, a danas bi se mogao podijeliti u kategorije:[72]

- Uvjerljivost *phishing* poruke
- Napadi kroz web stranice
- Napadi zlonamjernim softverom
- Ostali napadi (npr. lažno predstavljanje kao osoblje IT kompanije)

[66] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 49.
[67] Dragičević, D. (2004.) Kompjutorski kriminalitet i informacijski sustavi. Zagreb: IBS, str. 52.
[68] Nacionalni CERT (2018.) Uvod u socijalni inženjering. CERT.hr-PUBDOC-2017-11-349 [online]. Dostupno na: https://www.cert.hr/32749/, str. 6. [22. ožujka 2019.]
[69] Ibid., str. 7.
[70] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 49.
[71] Nacionalni CERT (2018.) Phishing. NCERT-PUBDOC-2018-5-361 [online].
Dostupno na:https://www.cert.hr/phish, str. 9. [26. ožujka 2019.]
[72] Ibid.

Keyloggers su softveri ili hardverski uređaji kojima se bilježi svaki udarac na tipkovnici. Uređaju su nevidljivi za korisnika, a prate i bilježe sve što korisnici upisuju, a prikupljeni podaci naprednim algoritmima šalju se kriminalcima.[73]

Kod prisluškivanje (eng. *Wiretapping, Eavesdropping*) radi se o prisluškivanju telefonskih linija za prijenos podataka radi pribavljanja lozinki ili ugrađivanju prislušnih uređaja na telefonske linije unutar samog kompjutorskog centra.[74]

Zlonamjerni kôd ili zlonamjerni softver (eng. *Malware)* je program koji se umeće u sustav s namjerom kompromitiranja ili ometanja povjerljivosti, integriteta ili dostupnosti podataka, aplikacija ili operativnog sustava žrtve.[75] Zlonamjerni softveri predstavljaju jednu od većih prijetnji računalima i mrežama. Postoje različite vrste zlonamjernog softvera, no svi rade na sličan način i imaju slične ciljeve:[76]

- Prikupljanje i krađa važnih informacija (krađa identiteta i drugih podataka)
- Omogućavanje daljinskog pristupa napadaču kako bi preuzeo kontrolu nad zaraženim/kompromitiranim računalom i njegovim resursima.
- Izvođenjem napada odbijanjem usluga preplavljivanjem mreže ili usporavanjem veze.
- Šifriranje diska i zahtijevanje otkupnine za dešifriranje
- Skrivanje što je duže moguće
- odupiranje nastojanjima da se ukloni od računala.

Kada zlonamjerni softver jednom napravi štetu teško ju je popraviti. Potrebni su veliki napori da se zaraženo računalo ili mreža vrati u normalu. Neki od zlonamjernih softvera su:[77]

- Špijunski program
- Crvi
- Trojanci (trojanski konj)
- Rootkitmalvare
- Virusi
- Ransomeware i dr.

[73] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 49.
[74] Dragičević, D. (2004.) Kompjutorski kriminalitet i informacijski sustavi. Zagreb: IBS, str. 54.
[75]Datt, S. (2016.) Mrežna forenzika: zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan, str. 198.
[76] Ibid., str. 199.
[77] Ibid., str. 198.

Već iz samog naziva zlonamjernog softvera može se ustanoviti na koji način radi. Tako je na primjer cilj špijunskih programa tajno prikupljanje povjerljivih informacija, a crvi se s druge strane ukopavaju u sustav računala i potom ga uništavaju.[78] Trojanci su dobar primjer kombinacije već prije spomenutog socijalnog inženjeringa i zlonamjernog softvera. Napadač predstavlja zlonamjerni softver (trojanski konj) kao legitiman softver, te se trudi da tako i funkcionira, samo kako bi u pozadini zapravo izvršavao zlonamjerni kôd.[79]

Jedan od opasnijih zlonamjernih softvera i danas sve češći je ucjenjivački softver (eng. *Ransomware)*. Radi se o malicioznom softveru dizajniran tako da šifrira podatke, a zatim traži otkupninu. Šifriranje je dovoljno jako da spriječi dešifriranje u razumnom vremenu.[80] Žrtva ima samo dvije mogućnosti ili da plati otkupninu ili da zaboravi na podatke u slučaju da je dešifriranje bilo neuspješno.

Osim napada usmjerenih na krađu podatka, česti su i napadi na onemogućavanje rada IS-a. Napad uskraćivanjem usluga (eng. *Denial of Service, DoS*), odnosi se na nedopuštene aktivnosti sprječavanja ili onemogućavanja ovlaštene uporabe računalne mreže, sustava ili programa iskorištavanjem njihovih resursa.[81]

Sve spomenute tehnike *cyber* napada predstavljaju veliku opasnost informacijskim sustavima te ih je potrebno od njih zaštiti. Spomenuto je kako su napadi na informacijski sustav najčešće usmjerni na krađu identiteta korisnika. Krađe identiteta korisnika danas su vrlo česte, a nekoliko godina unazad se dogodila vjerojatno najveća krađa podataka u povijesti.

[78] Datt, S. (2016.) Mrežna forenzika: zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan, str. 202-204.
[79] Nacionalni CERT (2018.) Socijalni inženjering i zlonamjerni softver. CERT.hr-PUBDOC-2018-11-369 [online]. Dostupno na:https://www.cert.hr/NCSocIZS, str. 34. [31. ožujka 2019.]
[80] Datt, S. (2016.) Mrežna forenzika: zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan, str. 208.
[81] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 50.

4.2.1. Yahoo! – *Data breach*

Yahoo! je jedan od većih svjetski web portala koji uz pružanje najnovijih vijesti, zabave i sporta, omogućuje i pristup drugim Yahoo uslugama kao što su Yahoo Mail (usluge besplatne elektroničke pošte), Yahoo! Search (tražilica), Yahoo! Maps (karte), Yahoo! Finance (financije) i druge. Kompanija Yahoo pretrpjela je 2013. i 2014. godine dva veća hakerska napada. Naime radi se o najvećoj krađi podataka (eng. *Data Breach*) ikada. U rujnu 2016. godine Yahoo je razotkrio hakerski napad iz 2014., ukradeni su podaci 500 milijuna korisničkih računa. Napadači su imali pristup osobnim podacima korisnika, adresi elektroničke pošte, te broju telefona kao i nešifriranim sigurnosnim pitanjima i odgovorima. Koliko je tijekom napada korisničkih računa bilo aktivno nije poznato. 500 milijuna zvuči jako puno i je, ali u odnosu na krađu podataka koja se dogodila godinu prije, čini se malo. Tri mjeseca nakon razotkrivanja hakerskog napada koji datira iz 2014., Yahoo je razotkrio hakerski napad iz 2013., koji je bio nekoliko puta veći i time ušao u povijest krađe podataka. Prvo je bila riječ o napadu na milijardu korisničkih računa, samo kako bi se 2017. godine otkrilo da se zapravo radilo o tri milijarde. Drugim riječima, tijekom napada 2013. ukradeni su podaci svih korisničkih računa, koji su se do tada ikada otvorili. Kasnije se otvorilo pitanje zašto Yahoo nije prije razotkrio napade. Sukladno tome američka komisija za vrijednosne papire (SEC) otvorila je istragu protiv Yahooa kako bi utvrdila je li ranije trebao obavijestiti investitore o dvije ozbiljne krađe podataka, te je u prosincu od tehnološke kompanije zatražio dokumentaciju vezanu uz *Cyber* napad. Prema američkom zakonu, kompanije-žrtve takvih napada dužne su što prije dostaviti informacije jer takvi napadi obično utječu na vrijednost dionica kompanije.[82] Hakerski napadi odrazili su se na vrijednost dionica i kompanije, a vjerojatno i na povjerenje njegovih korisnika. Naime tijekom razotkrivanja hakerskih napada, telekomunikacijska kompanija Verizon već je bila u pregovorima s Yahoo o otkupu i preuzimanju kompanije. Nakon razotkrivanja napada, originalna cijena otkupa se smanjila za 350 milijuna dolara.[83] Napad 2013. godine je bio dokaz, a ujedno i upozorenje kompaniji da korisnički računi nisu bili dovoljno zaštićeni. Prema tome Yahoo je trebao poduzeti nove, bolje mjere zaštite, ali kako se ispostavilo Yahoo je samo godinu dana nakon, pretrpio novi hakerski napad s istim ciljem.

[82] Welt [online]. Dostupno na: https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/article169293837/Alle-Yahoo-Accounts-von-Datenklau-im-Jahr-2013-betroffen.html , zimo-NovaTV [online]. Dostupno na: https://zimo.dnevnik.hr/clanak/yahoo-pod-istragom-zbog-kradje-podataka---464556.html [4. travnja 2019.]

[83] The New York Times [online]. Dostupno na: https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html [4. travnja 2019.]

4.3. Proces upravljanja rizicima

Rizici su više manje stalno prisutni, a kako bi se smanjile opasnosti koje prijete organizaciji, društvu ili instituciji, te kako bi se rizik sveo na minimum potrebno je znati kako njime upravljati. Ovisno o vrsti rizika, ali i djelatnosti, procesi upravljanja rizikom se razlikuju. Međutim svaki bi trebao obuhvatiti:

- Identifikaciju i analizu rizika (identifikacija prijetnji i ranjivosti)
- Procjenu rizika te
- Poduzimanje koraka da se rizik smanji na prihvatljivi nivo.

Procjena rizika definira se kao sveukupni proces identifikacije, analize i vrednovanja rizika. Identifikacija rizika obuhvaća pronalaženje, prepoznavanje i opisivanje rizika, analiza razumijevanje prirode rizika i određivanje njegove razine, a vrednovanje obuhvaća usporedbu rezultata analize rizika i postavljenih kriterija, kako bi se odredilo je li razina rizika prihvatljiva ili nije.[84]

Upravljanje rizicima je faza njegove modifikacije, a može uključiti:[85]

- izbjegavanje rizika
- preuzimanje ili povećanje rizika
- mijenjanje vjerojatnosti njegove pojave
- mijenjanje posljedica
- prenošenje rizika na treću stranu
- svjesno prihvaćanje rizika

Kako se procesi upravljanja rizikom razlikuju (ovisno o vrsti rizika), korake procesa upravljanja rizikom neće se posebno opisivati, što bi također bilo teško, nego će biti detaljnije objašnjeni na primjeru informacijskog sustava.

[84] Krakar, Z., Tomić Rotim, S., Žgela, M., Arbanas, K., Kišasondi, T. (2014.) Korporativna informacijska sigurnost. Varaždin: Fakultet organizacije i informatike Sveučilišta u Zagrebu, str. 281.
[85] Ibid.

5. Informacijska sigurnost

Svaka organizacija koja se služi digitalnim tehnologijama ima problema sa sigurnošću informacija i informacijskog sustava te je uvelike izložena različitim rizicima, ponajprije, kao što smo vidjeli, informatičkim rizicima. Nije bitno nalazi li se informacija na papiru ili nekom drugom mediju, ako ona i informacijski sustav nisu dovoljno zaštićeni, štete koje mogu nastati mogu biti velike i u konačnici dovesti do trenutnog zastoja poslovanja. Primjena digitalne i informacijske tehnologije u svim industrijskim granama sve je veća, prvenstveno jer ima pozitivan učinak na poslovanje. Ali s druge strane to znači da je potrebno ulagati u informatiku, a to pak znači veću izloženost informatičkim rizicima.

Informacijska sigurnost se odnosi na sigurnost informacija, a time i na sigurnost informacijskog sustava. Sigurnost informacija i informacijskog sustava skup je metoda i zaštitnih mjera (kontrola) kojima se informacije i IS štite od neovlaštenog pristupa, uporabe, otkrivanja, prekida rada, promjena ili uništenja.[86] Zahtjevi informacijske sigurnosti proizlaze iz tradicionalnih zahtjeva zaštite klasificiranih podataka u državnome sektoru.[87] Razvojem i globalizacijom društva informacije i IS postali su vrijednosni potencijal ne samo državnog sektora već i ostalih, te je potrebno promatrati cjelokupno društvo i informacijski prostor u cjelini, usklađujući razlike i potrebe informacijske sigurnosti u različitim područjima društva.[88]

Tri osnovna sigurnosna zahtjeva su:[89]

- Zahtjev sigurnosti – obuhvaća povjerljivost i sigurnost podataka i informacija, to znači uspostavljanje uvjeta za neometano i stalno funkcioniranje IS-a.
- Zahtjev raspoloživosti – odnosi se na dostupnost podataka i informacija samo ovlaštenim osobama.
- Zahtjev tajnosti – odnosi se na pojedinačne i privatne podatke koji smiju biti dostupni isključivo ovlaštenim korisnicima.

[86] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 53.
[87] Andrijanić, I., Gregurek, M., Merkaš, Z. (2016.) Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada, str. 132.
[88] Ibid.
[89] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 57.

Pogreške ili sigurnosni propusti, te narušavanje sigurnosnih zahtjeva mogu imati negativne posljedice na organizaciju.

6. Upravljanje rizicima informacijskog sustava

Kako bi se opasnosti, bilo vanjske ili unutarnje, koje prijete informacijskom sustavu svele na minimum, potrebno ih je identificirati, procijeniti, te poduzeti mjere zaštite. Rizik IS-a predstavlja opasnost ili vjerojatnost da će odgovarajući izvor prijetnje u određenim okolnostima iskoristiti ranjivost (slabost) sustava, čime se posljedično, može počiniti neka šteta.[90] Proces upravljanja rizicima predstavlja važnu komponentu za uspješno funkcioniranje informacijskog sustava, a da bi upravljanje rizikom zaista bilo efikasno i kako bi procijenjeni rizik odgovarao stvarnom stanju sustava potrebno ga je integrirati u životni ciklus informacijskog sustava (eng. *SDLC*).[91]

Životni ciklus IS-a sastoji se od pet faza:[92]

- Prva faza – faza pokretanja/uvođenja sustava (potreba za sustavom)
- Druga faza – faza razvoja/izgradnje sustava (dizajniranje i programiranje sustava)
- Treća faza – faza implementiranja sustava (testiranje sustava)
- Četvrta faza – faza održavanja sustava
- Peta faza – faza dispozicije sustava

Upravljanje rizicima informacijskog sustava može se svesti na dva glavna koraka; sveukupni proces procjene rizika (identifikacija, analiza i procjena rizika) i proces ublažavanja rizika (odabir zaštitnih kontrola i njihova implementacija). Osnovni cilj jest otkriti i identificirati slabosti u organizaciji ili sustavu, procijeniti razinu opasnosti kojom su izloženi (poslovni) resursi i ponuditi racionalan, izvediv i troškovno učinkovit način smanjivanja njihova intenziteta.[93]

[90] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 61.

[91] Hrvatska agencija za nadzor financijskih usluga (2014.) Smjerniceza primjereno upravljanje rizicima informacijskih sustava subjekata nadzora [online]. Dostupno na: https://www.hanfa.hr/objave-sa-sjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/, str. 23. [9. travnja 2019.]

[92] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 5. [11. travnja 2019.]

[93]Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 70.

6.1. Procjena rizika

Kako bi se spriječilo nastupanje nekog budućeg neželjenog događaja, potrebno je napraviti analizu opasnosti koje prijete IS-u u skladu s njegovim slabostima. Procjena rizika informacijskog sustava sastoji se od ukupno devet koraka, a to su:[94]

- Karakterizacija informacijskog sustava
- Identifikacija prijetnji
- Identifikacija ranjivosti
- Analiza kontrola
- Određivanje vjerojatnosti
- Analiza utjecaja
- Određivanje rizika
- Preporuka kontrola
- Dokumentiranje rezultata

6.1.1. Karakterizacija informacijskog sustava

Određivanje obilježja IS-a definira opseg procesa procjene rizika. Za identifikaciju rizik potrebno je razumjeti sam sustav i njegovo okruženje. Pri određivanju obilježja IS-a potrebno je definirati resurse i informacije o sustavu:[95]

- Hardver
- Softver
- Sistemska sučelja
- Podaci i informacije
- Korisnici i IT stručnjaci
- Svrha sustava

[94] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST[online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 8. [11. travnja 2019.]
[95] Ibid., str. 10.

- Važnost i osjetljivost sustava i podataka

Dodatne informacije koje mogu poslužiti pri određivanju obilježja IS-a povezane su s operativnim okruženjem informacijskog sustava kao na primjer informacije o funkcionalnoj potrebi, topologiji mreže, internim aktima vezanim za IS, fizičkoj zaštiti, arhitekturi sigurnosti sustava i drugo.[96] Potrebne informacije se mogu prikupiti na različite načine kao na primjer anketnim upitnikom (ispitanike bi činilo menadžersko osoblje koje koristi i podržava IS), intervjuom ili pregledavanjem dokumenata (pravna dokumentacija, dokumentacija o IS-u, rezultati testiranja sustava i slično).[97] Nakon određivanja obilježja IS-a pomoću prikupljenih informacija slijedi identifikacija mogućih opasnosti koje mu prijete.

6.1.2. Identifikacija prijetnji

Prijetnja je potencijal određenog izvora prijetnja da iskoristi određenu ranjivost (slabost) informacijskog sustava. Međutim izvor prijetnje ne predstavlja rizik, ako ne postoji ranjivost koju može iskoristiti.[98] Prilikom identifikacije prijetnji stručnjak za sigurnost usmjerava se na potencijalne napadače ili događaje koji mogu negativno djelovati na sustav, oslanjajući se na prethodno prikupljene podatke i informacije o sustavu.[99] Događaj koji može na bilo koji način negativno utjecati na sustav, smatra se prijetnjom. Prijetnje mogu biti prirodne (poplave, zemljotresi, požari i druge prirodne nepogode), ljudske (hackeri, računalni kriminalci, nezadovoljni zaposlenici i slično) i prijetnje okoline (nestanak struje, kemikalije i slično).[100] Među prijetnjama ljudske su danas najčešće. Ljudska motivacija i volja za izvršavanjem napada predstavlja potencijalan i opasan izvor prijetnje. Već prije spomenuti *cyber* rizici su dobar primjer, jer iza svakog *cyber* napada stoji čovjek.

[96] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 10. [11. travnja 2019.]
[97] Ibid., str. 12.
[98] Ibid.
[99] Panian, Ž., Spremić, M. (2007.) Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri, str. 82.
[100] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 13. [11. travnja 2019.]

S obzirom na motivaciju i izvor prijetnji, ljudske prijetnje mogu se podijeliti na:[101]

- Hakeri
    - motivacija: pobuna, izazov, ego
    - aktivnost: hakiranje, socijalni inženjering, neovlašteno pristupanje sustavu
- Računalni kriminalci
    - motivacija: uništenje informacija, ilegalno razotkrivanje informacija, novčana dobit, izmjena sadržaja informacija
    - aktivnost: upad u sustav, lažiranje podataka ili IP adrese (eng. *Spoofing*), podmićivanje
- Teroristi
    - motivacija: uništenje, osveta, iskorištavanje, odavanje informacija (eng. *Blackmail*)
    - aktivnost: informacijsko ratovanje, penetracija, DoS napad
- Špijuni (kompanije, strana vlada)
    - motivacija: konkurentska i ekonomska prednost
    - aktivnost: krađa podataka, socijalni inženjering, penetracija
- Nezadovoljni djelatnici
    - motivacija: znatiželja, inteligencija, ego, osveta, novčana dobit
    - akcija: krađa, podmićivanje, obmana, sabotaža, zlonamjerni kôd, prodaja informacija, neovlašteni pristup

Sve nabrojane aktivnosti su namjerne, te imaju cilj napraviti štetu, no postoje i aktivnosti koje su nenamjerne. Radi se o situacijama koje su se slučajno dogodile, a mogu uzrokovati slabost sustava kao na primjer bilo kakva nehotična aktivnost korisnika (brisanje podataka, promjena svojstava sustava, pogreške u radu i slično). U ovu kategoriju se također mogu ubrojiti i prirodne nepogode.[102]

[101] Ibid., str. 14.
[102] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 73.

6.1.3. Identifikacija ranjivosti

Nakon identifikacije prijetnji slijedi korak identifikacije ranjivosti. Ranjivost sustava se odnosi na njegove slabosti, koje izvor prijetnje može iskoristiti, i time napraviti štetu, stoga je cilj ovog koraka utvrditi (ako je moguće) sve slabosti informacijskog sustava. Ranjivost IS-a je slabost u sigurnosnim procedurama sustava, njegovu dizajnu, implementaciji ili unutarnjim kontrolama, koja može biti iskorištena, te negativno rezultirati.[103] Radi se o nedostatku ili slabosti sustava, njegovih ključnih dijelova, ili internih kontrola koji namjernim ili nenamjernim djelovanjem mogu uzrokovati sigurnosni incident ili povredu sigurnosne politike.[104] Za identifikaciju ranjivosti sustava također pomažu i prikupljene informacije u prvom koraku. Primjeri ranjivosti sustava su:[105] nepostojanje zaštite od zlonamjernog softvera, neprimjerena konfiguracija vatrozida, nepostojanje autentifikacije prilikom pristupa, nepostojanje sustava za besprekidnu opskrbu električnom energijom i tako dalje.

Razina ranjivosti sustava uvelike ovisi o ugrađenim kontrolama, koje sprječavaju da se neka prijetnja dogodi. Međutim implementacija kontrolnih mehanizama zahtijeva određena financijska sredstva, te je potrebno utvrditi njihovu financijsku vrijednost.[106] Jedna od tehnika koja se ispostavila kao djelotvorna u identifikaciji ranjivosti IS-a je penetracijsko testiranje.

6.1.3.1. Penetracijsko testiranje

Penetracijsko testiranje je tehnika procjene sigurnosti računalnog sustava ili mreže koja se temelji na oponašanju stvarnog napada.[107] Jednostavno rečeno, osoba koja provodi testiranje izvršava napade na sustav, onakve kakve bi stvarni napadač napravio. Ovlašteni ispitivač naziva se još i etičan haker (eng. *Ethical Hacker, White hat*). On je stručnjak u području računarstva i računalnih mreža, a napada računalne sustave pokušavajući iskoristiti njihove slabosti, ali, on to čini prema nalogu vlasnika ciljanog sustava i upravo s ciljem identifikacije

[103] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 15. [11. travnja 2019.]

[104] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 74.

[105] Ibid., str. 63.

[106] Ibid., str. 74.

[107] CARNet CERT, L&LS (2010.) Metodologija penetracijskog testiranja. CCERT-PUBDOC-2008-02-219 [online]. Dostupno na: https://www.cis.hr/www.edicija/MetodologijapenetracijskogtestiranjaHTML.html, str. 5. [16. travnja 2019.]

ranjivosti i sprečavanja djelovanja zlonamjernih hakera.[108] Penetracijsko testiranje sastoji se od pet faza, a to su:[109]

- prikupljanje informacija: uključuje prikupljivanje informacija su ključne i osiguravaju potrebne preduvjete za nastavak testiranja.
- mapiranje mreže: uključuje pronalazak aktivnih računala, pretraživanje priključaka i servisa, određivanje vanjskih rubova mreže, utvrđivanje informacija o operacijskom sustavu i slično.
- identificiranje ranjivosti: detektiraju se točke sustava pogodne za napad.
- penetracija: pokušava se dobiti neovlašteni pristup zaobilaženjem sigurnosnih ograničenja
- dobivanje pristupa i povećanje ovlasti

6.1.4. Analiza kontrola

Kontrola je sustav kojim se spriječavaju, otkrivaju i ispravljaju neželjeni događaji i procesi u informacijskom sustavu.[110] Cilj ovog koraka je analizirati implementirane kontrole ili kontrole koje se planiraju implementirati. Kontrola obuhvaća skup međusobno povezanih komponenti koje potpomažu ostvarivanju utvrđenih ciljeva IS-a. Drugim riječima primjenjuju se da bi se spriječili (preventivne kontrole), otkrili (detektivne kontrole) ili ispravili (korektivne kontrole) neželjeni događaji.[111] Na primjer upute za ispunjavanje obrasca putem kojeg će se podaci unositi u sustav tiskaju se na samom obrascu, kako bi se sprječilo njegovo pogrešno popunjavanje (preventivne kontrole). Svrha kontrola je smanjenje očekivanih gubitaka do kojih bi došlo kod pojave neželjenih događaja ili ostvarenja neželjenih procesa u sustavu.[112]

[108] Ibid., str. 4.
[109] Ibid.
[110] Panian, Ž. (2001.) Kontrola i revizija informacijskih sustava. Zagreb: Sinergija, str. 19.
[111] Ibid.,, str. 20.
[112] Ibid.

6.1.5. Određivanje vjerojatnosti

Kako bi se utvrdila vjerojatnost da identificirana ranjivost bude iskorištena u okruženju izloženom prijetnji potrebno je uzeti u obzir sljedeće čimbenike:[113]

- Motivaciju i sposobnost izvora prijetnje
- Obilježja ranjivosti
- Postojanje i efikasnost postojećih kontrola

Vjerojatnost iskorištavanja ranjivosti može se iskazati pridruživanjem neke empirijske vrijednosti kao na primjer visoka (izvor prijetnji je vrlo motiviran i suviše sposoban, a kontrole nedjelotvorne), srednja (izvor prijetnji je motiviran i sposoban, ali su kontrole djelotvorne) i mala (izvor prijetnji ima manjak motivacije i kontrole su dovoljno efikasne da spriječe napad) vjerojatnost.[114]

6.1.6. Analiza utjecaja

Cilj ovog koraka je procijeniti negativan učinak ako prijetnja uspješno iskoristi ranjivost sustava. Prije analize potrebno je prikupiti informacije o svrsi sustava, te o važnosti i osjetljivosti sustava i podataka. Negativan učinak događaja može se opisati kao narušavanje funkcionalnosti ili bilo kojeg temeljnog načela informacijskog sustava. Temeljni parametri informacijske sigurnosti su:[115]

- Povjerljivost (eng. *Confidentiality*) – siguran pristup informaciji i IS-u isključivo za to ovlaštenoj osobi.
- Cjelovitost (eng. *Integrity*) – zaštita ispravnosti i cjelovitosti podataka i informacija.
- Raspoloživost ili dostupnost (eng. *Availability*) – ovlaštenoj osobi omogućiti pravodoban i stalan pristup informacijama i IS-u.

---

[113] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 21. [11. travnja 2019.]

[114] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 21. [11. travnja 2019.]

[115] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 53.

Posljedice koje mogu nastati narušavanjem temeljnih načela mogu biti gubitak konkurentske prednosti (otkrivanje informacija o novim proizvodima konkurenciji), gubitak povjerenja klijenata (curenje osobnih podataka klijenata u javnost), nepoštivanje mjerodavnih propisa (na primjer kršenje regulative u području zaštite osobnih podataka), financijski gubici, donošenje pogrešnih poslovnih odluka (zbog neispravnosti informacija), nemogućnost isporuke proizvoda i usluga klijentima (zbog nedostupnosti informacija ugovornim odnosima s klijentima, nemogućnost ispunjavanja ugovornih obveza.[116]

Učinke je moguće mjeriti kvantitativno u obliku financijskih sredstava i vremena koje je potrebno uložiti kako bi se popravio sustav ili riješili problemi ili opisati kvalitativno (odnosi se na učinke koji se ne mogu mjeriti kao na primjer gubitak povjerenja).[117]

6.1.7. Određivanje rizika

Cilj ovog koraka je procijeniti razinu rizika kojem je izložen informacijski sustav. Utvrđivanje rizika izloženosti određenoj kombinaciji prijetnje i ranjivosti može se izraziti kao funkcija:[118]

- Vjerojatnosti da će određeni izvor prijetnje iskoristiti ranjivost sustava
- Jačina učinka u slučaju uspješnog izvršenja prijetnje
- Adekvatnost planiranih ili postojećih kontrola za smanjivanje ili sprječavanje rizika.

Jedna od metoda pomoću koje se može utvrditi razina rizika je matrica procjene rizika.

6.1.7.1. Matrica razine rizika

Razina rizika može se izračunati pomoću matrice, tako da se pomnoži ocjena koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost IS-a s ocjenom učinka. Matrica razine rizika (eng. *Risk-Level Matrix*) može biti različitih dimenzija (3 x 3, 4 x 4, 5 x 5) i sadržavati različite dodijeljene brojčane vrijednosti. Tablica br. 1 jednostavan je prikaz matrice 3 x 3.

[116] Ibid.
[117] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 23. [11. travnja 2019.]
[118] Ibid., str. 24.

Vjerojatnost prijetnje	Učinak		
visoka (1.0)	mali 10 X 1.0 = 10	srednji 50 X 1.0 = 50	veliki 100 X 1.0 = 100
srednja (0.5)	srednji 10 X 0.5 = 5	srednji 50 X 0.5 = 25	srednji 100 X 0.5 = 50
niska (0.1)	mali 10 X 0.1 = 1	mali 50 X 0.1 = 5	mali 100 X 0.1 = 10

Tablica br. 1: Matrica razine rizika (prema Stoneburner i sur.)

Svakoj razini se dodaje vrijednost, u ovom slučaju 1.0 za visoku, 0.5 za srednju i 0.1 za nisku vjerojatnost prijetnje, te 100 za veliki, 50 za srednji i 10 za mali učinak. Gledajući tablicu br. 1 skala razine rizika bila bi: visoka ako je dobivena vrijednost >50 do 100, srednja ako je >10 do 50 i niska ako je 1 do 10. Ako je procijenjeni rizik veći od 51, potrebno ga je hitno smanjiti i plan korektivnih mjera u što kraćem roku sastaviti. Ako je rizik procijenjen kao srednji (>10 do 50), plan korektivnih mjera se treba u razumnom vremenu sastaviti i provesti. Ako se rizik ispostavi kao nizak (1 do 10), treba procijeniti je li potrebno provođenje korektivnih mjera ili je rizik kao takav prihvatljiv.[119]

6.1.8. Preporuka kontrola

Nakon određivanja rizika slijedi preporuka kontrola. U ovom koraku predlažu se kontrole (kasnije detaljnije opisane) i alternativna rješenja koja bi mogla smanjiti ili eliminirati već prije identificirane rizike. Cilj je pomoću predloženih kontrola smanjiti razinu rizika informacijskog sustava i podataka na prihvatljivu razinu, a čimbenike koje treba prilikom predlaganja uzeti u obzir su: djelotvornost predloženih kontrola, važeće propise, interne akte, te utjecaj na poslovne procese i sigurnost IS-a.[120] Prilikom predstavljanja mogućih kontrola osobi zaduženoj za prihvaćanje rizika sigurnosni stručnjak odnosno analitičar treba ponuditi

[119] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 25. [11. travnja 2019.]

[120] Ibid., str. 26.

kao opciju barem dva različita paketa protumjera, te za svaku opciju navesti očekivane troškove i količinu rizika koju će prihvatiti donositelj odluke.[121]

6.1.9. Dokumentiranje rezultata

Nakon provedbe svih prethodnih koraka, odnosno nakon što je proces procjene rizika IS-a završen, potrebno je dokumentirati rezultate u obliku službenog izvješća. Izvješće o procjeni rizika pomaže upravi i ostalim odgovornim osobama u donošenju odluka o promjenama internih akata i proračuna te o operativnim i upravljačkim promjenama. Izvješće treba imati sistematski i analitički pristup procjeni rizika. Takav pristup omogućava upravi da razumije rizike i raspodijeli resurse potrebne za smanjenje potencijalnog gubitka.

6.2. Ublažavanje rizika

Nakon procesa procjene rizika potrebno je razviti scenarije upravljanja rizicima. Tipični scenariji upravljanja su:[122]

- Prihvaćanje rizika – organizacija je upoznata s intenzitetom rizika, nadzire ga i, u skladu s korporativnim pravilima, procjenjuje njegov utjecaj na poslovanje i poslovne procese. U slučaju da razina rizika postane neprihvatljiva poduzimaju se protumjere.
- Smanjivanje intenziteta rizika – organizacija poduzima odgovarajuće aktivnosti kojima se smanjuje utjecaj rizika na poslovanje ili vjerojatnost njegova nastanka.
- Izbjegavanje rizika – u skladu s korporativnim pravilima organizacije ili u potpunosti ili djelomično izbjegava rizik.
- Podjela rizika – organizacija rizik transferira na neku drugu ili treću stranu (na primjer kupnja police osiguranja).

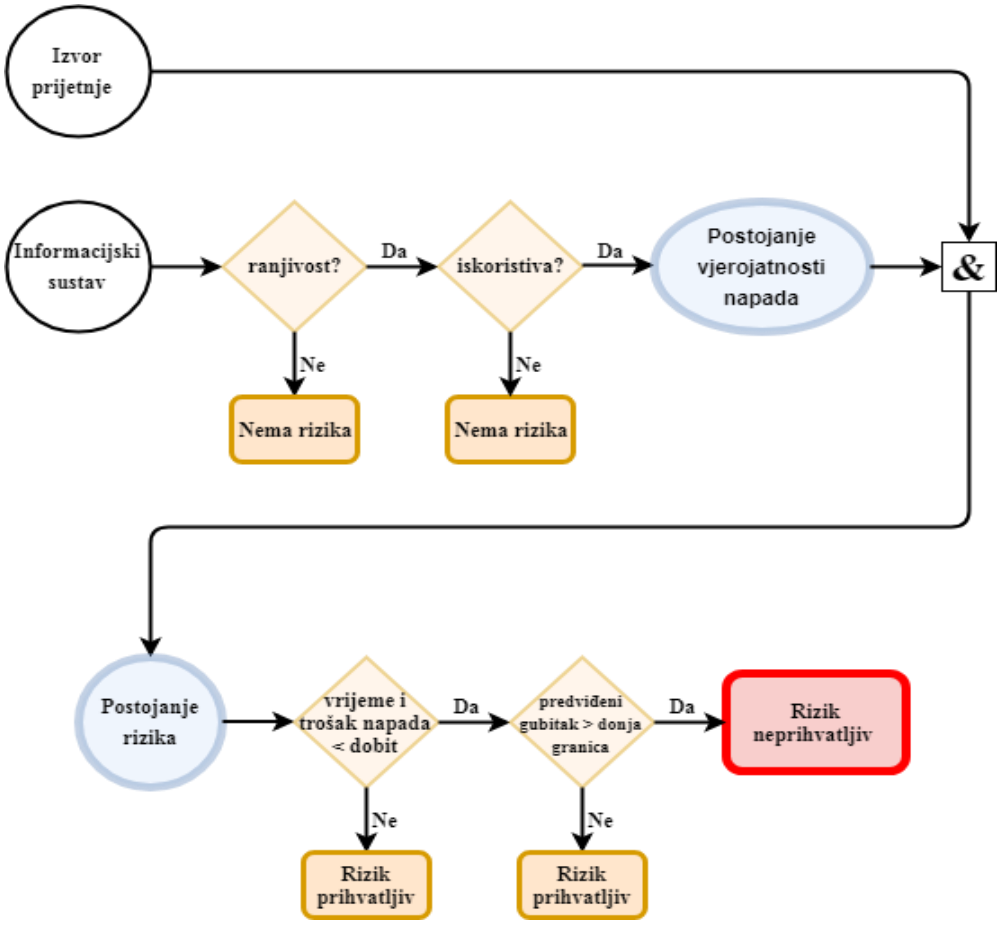
Ovisno o rezultatima procjene rizika, odabire se najprikladniji scenarij. Ako se ispostavi da je rizik veliki, odnosno da postoji visoka vjerojatnost da će ranjivost informacijskog sustava biti iskorištena i time negativno utjecati na poslovanje, potrebno je pod hitno poduzeti odgovarajuće protumjere (jer učinkovite kontrole ne postoje), te se zahtijeva promptna reakcija najviših razina menadžmenta (strategija smanjenja intenziteta rizika). Ako je rizik

[121] Panian, Ž., Spremić, M. (2007.) Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri, str. 88.

[122] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 79.

poznat, odnosno identificiran, prati se njegov utjecaj na poslovanje i nisu potrebne trenutne akcije.[123] Ovisno o stanju informacijskog sustava odabire se najprikladnija strategija. Prilikom odabira scenarija za upravljanje rizicima, postavljaju se pitanja poput: kada je rizik prihvatljiv, a kada nije? ili je li i kada je potrebno provođenje protumjera?

Kako donijeti odluku može se jednostavno prikazati pomoću dijagrama stablo odlučivanja (dijagram br. 1).



Dijagram 1: Ispitivanje stanja informacijskog sustava (prema Stoneburner i sur.)

Ako ranjivost (slabost) IS-a postoji, potrebno je povečati njegovu sigurnost (zaštitu) kako bi se smanjila vjerojatnost iskorištavanja njegove ranjivosti. U slučaju da ranjivost može biti iskorištena, potrebna je višeslojevita zaštita kao i uključivanje administrativnih kontrola kako bi se smanjio ili spriječio rizik. U slučaju da je vrijeme i trošak napada manji od potencijalnog dobitka, potrebno je tada smanjiti napadačevu motivaciju tako da se njegov trošak poveća. Ustanovi li se da predviđeni gubitak organizacije nadmašuje donju granicu,

[123] Ibid.

potrebno je poduzeti tehničke i netehničke protumjere (implementacija odgovarajućih kontrola).[124]

6.2.1. Kontrole informacijskog sustava

Ako se na temelju rezultata procesa procjene rizika došlo do zaključka da je informacijski sustav izložen riziku, te da je vjerojatnost iskorištavanja ranjivosti sustava visoka, potrebno je implementirati nove ili modificirati postojeće kontrole. Scenariji upravljanja rizicima odnose na određivanje odgovarajućih vrsta informatički kontrola, odnosno ručnih, automatskih i poluautomatskih kontrola IS-a.[125] Informatičke kontrole su kontrole ugrađene u rad informacijskog sustava, koje predstavljaju sustav (skup) međusobno povezanih komponenti koje, djelujući jedinstveno i usklađeno, potpomažu ostvarivanje ciljeva IS-a, a usmjeruju se na neželjene događaje ili procese u IS-u koji mogu nastati iz različitih razloga koji se odnose na unutarnje djelovanje IS-a (netočni podaci, nedjelotvorni procesi, neučinkoviti ulazi u sustav i slično) ili uzroke iz njegova okruženja[126]. Jednostavnije rečeno svrha kontrola je smanjiti vjerojatnost nastanka neželjenog događaja kao i smanjivanje očekivanih gubitaka do kojih bi došlo kod pojave ili ostvarenja neželjenog događaja/procesa.[127] Što su kontrole informacijskog sustava djelotvornije, to je manji rizik kojem je on izložen.

Kontrole IS-a mogu se podijeliti s obzirom na način primjene (automatske, ručne), s obzirom na svrhu (već prije spomenute preventivne, detektivne i korektivne), s obzirom na hijerarhiju (korporativne, upravljačke, operativne) i s obzirom na način funkcioniranja (organizacijske, tehnološke, fizičke).[128]

Automatske kontrole predstavljaju zaštitne mehanizme poslovnih procesa, te su najčešće ugrađene u automatizam funkcioniranja IS-a. Ručne kontrole se odnose na ručne provjere funkcioniranja IS-a. Organizacijske se odnose na interne akte kojima se propisuju željena ponašanja prilikom korištenja IS-a, tehnološke odnose se na mrežnu infrastrukturu, podatke i

[124] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 28. [11. travnja 2019.]

[125] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 79.

[126] Ibid., str. 87.

[127] Ibid.

[128] Ibid., str. 88.

opremu, a fizičke na opipljivi dio imovine informacijskog sustava.[129] Kako fizički zaštiti informacijski sustav i njegovu okolinu bit će detaljnije kasnije opisano.

Kako bi se smanjio rizik kojem je IS izložen, te povećala učinkovitost kontrola za rad IS-a i organizacije, organizacija treba uzeti u obzir korporativne, upravljačke i operativne sigurnosne kontrole ili njihovu kombinaciju.[130]

6.2.1.1. Korporativne kontrole

Korporativne kontrole (eng. *Technical controls*) odnose se na najvažnije politike, pravila i metodologije koje pomažu u uspješnom vođenju poslovanja i konkurentskom nadmetanju.[131] Korporativne kontrole osiguravaju sigurnost važnih i osjetljivih podataka, informacija i funkcioniranja IS-a. Primjeri korporativnih kontrola su:[132]

- Kontrole vezane u korporativno upravljanje informatikom (politike, pravila i metodologije vezane za planiranje, organiziranje, vođenje i kontrolu IS-a, mjerenje učinka IS-a na poslovanje, sposobnost kompanije za digitalnu transformaciju poslovanja, kontrole procesa upravljanja rizicima primjene informacijskih sustava, kontrole planova ulaganja u informatiku, vođenja i upravljanja informatičkim programima i projektima, ustrojavanje i funkcioniranje ključnih tijela zaduženih za upravljanje informatikom i druge).
- Strateške kontrole rada IS-a (kontrole životnoga ciklusa IS-a, dokumentacijski standardi, metodologije razvoja IS-a, standardi učinka IS-a, kontrole prekida ili otežanog odvijanja kritičnih poslovnih procesa uz dodjele odgovornosti, kontrole procesa financijskog izvještavanja i druge).
- Kontrole provedbe sigurnosne informacijske politike (sigurnosna informacijska politika predstavlja opsežan i izrazito važan dokument kojim se propisuju svi aspekti upravljanja sigurnošću IS-a)

[129] Ibid., str. 90.
[130] Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems, str. 32. [11. travnja 2019.]
[131] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 94.
[132] Ibid.

6.2.1.2. Upravljačke kontrole

Upravljačke kontrole se odnose na organizacijske te razne tehnološke, fizičke, preventivne, detektivne i druge kontrole.[133] Upravljačke kontrole se mogu podijeliti u tri glavne skupine:[134]

- Kontrole u postupku razvoja i uspostavljanja informacijskog sustava (definicije bitnih elemenata problema, identifikacija novih mogućnosti, identifikacija potrebnih promjena, učinak uvedenih promjena, odabir razvojnog modela, temeljne postavke organizacije rada, definicije obveza izvršitelja posla, vremenske usklađenosti poslova, integracija elemenata sustava za obradu informacija s ostalim komponentama IS-a, postupak izbora najpovoljnije ponude, rezultati testiranja sustava i tako dalje).
- Kontrole podataka (utvrđivanje prioriteta pristupa podacima, ispravnost definicije podataka, kvaliteta i pravodobnost informiranja korisnika, kvalitete sadržaja baze podataka, postojanje/nepostojanje nadzora nad okruženjem baze podataka, pridržavanje discipline pristupa bazi podataka i tako dalje).
- Sigurnosne upravljačke kontrole (kontrole usmjerene na politiku i organizaciju informacijske sigurnosti, sigurnost ljudskog potencijala, fizičku sigurnost i sigurnost okruženja, upravljanje komunikacijama i operacijama, upravljanje sigurnosnim incidentima, upravljanje kontinuitetom poslovanja i drugo).

Važno je napomenuti kako se upravljačke kontrole podataka u praksi prvenstveno usmjeravaju na pristup poslu, način izvršenja zadataka i rezultate osobe zadužene za brigu o njima, a ne izravno na podatke.[135]

6.2.1.3. Operativne kontrole

Operativne kontrole zadužene su za neometano odvijanje poslovnih transakcija, informatičke opreme, resursa, objekata i usluga. One se provode kako bi se spriječile neautorizirane transakcije i osigurala njihova potpunost, točnost i ispravnosti odnosno kako bi informatička

[133] Ibid., str. 98.
[134] Panian, Ž., Spremić, M. (2007.) Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri, str. 133.
[135] Ibid., str. 138.

oprema mogla neometano i ispravno opsluživati njihov rad (primjerice autorizacija, provjera identiteta, dodjela ovlasti rada).[136]

6.2.1.4. Kontrole pristupa informacijama i informacijskom sustavu

U prijašnjim poglavljima spomenuti su *cyber* rizici i napadi. Između svih rizika koje prijete (suvremenom) informacijskom sustavu oni su vjerojatno među najčešćima. Ciljevi takvih napada su krađa i izmjena sadržaja podataka/informacija. Kako bi se informacije i informacijski sustavi zaštitili (što je više moguće) od takvih napada primjenjuju se kontrole pristupa svim resursima IS-a. Kontrole pristupa se ubrajaju među najvažnije zaštitne mehanizme jer ograničavaju i kontroliraju pristup svim resursima IS-a te sprječavaju njihovu neovlaštenu uporabu (metode identifikacije, metode provjere ovlaštenja, metode zaštite u prijenosu i kriptografske metode).[137]

Identifikacija se odnosi na postupak prijave korisnika na IS korištenjem identifkacijskih oznaka i provjere njihove vjerodostojnosti. Korisnik unosi informacije poput svog imena, ili broja računa pod kojim je prijavljen. Identifikacija se može ostvariti fizički (na primjer posjedovanje nekog predmeta) i logički (na primjer poznavanje nekog pojma). Nakon identifikacije slijedi postupak autorizacije odnosno dodjela ovlasti korisniku za rad s resursima IS-a. Autorizacijom se pojedinom korisniku dodjeljuje određena ovlast rada nad resursima IS-a, a ovisi o potrebama posla, sistematizaciji dužnosti i razini odgovornosti.[138] Identifikacija može se postići na različite načine.

Najpoznatija metoda identifikacije i vjerojatno najrasprostranjenija je korisničko ime i lozinka (primjerice društvene mreže). Korisnik upisuje podatke, nakon toga ih sustav uspoređuje s pohranjenim podacima, ako se podaci podudaraju sustav odobrava pristup, ako ne uskraćuje ga. Nadalje, ako je identifikacija bila uspješna slijedi autorizacija. Druge metode identifikacije koje se danas koriste su certifikati (korištenje fizičkih uređaja kao na primjer elektronički čitaći kartica), sigurnosni tokeni (slični certifikatima), biometrijski uređaju (uređaji za skeniranje prsta, lica, dlana, oka i slično) i višestruka identifikacija.[139]

Metode zaštite u prijenosu štite podatke tijekom napuštanja zone sigurnosti, a postiže se primjenom standardnih komunikacijskih protokola (skup pravila za razmjenu informacija

[136] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 115.
[137] Ibid., str. 129.
[138] Ibid., str. 135.
[139] Ibid., str. 134.

između dva entiteta), dok kriptografske metode štite tajne i vrlo povjerljive podatke/informacije koje posjeduje svaka organizacija.[140]

Kriptografija (eng. *Cryptography*) je znanost o prikrivanju informacijskih sadržaja i onemogućivanju njihova razumijevanja, modificiranja i uporabe od strane neovlaštenih subjekata. Tajne i vrlo povjerljive informacije smiju biti dostupne samo određenom broju ovlaštenih korisnika i nikako neovlaštenima. A kako bi se tajni podaci ili informacije zaštitile tijekom njihovog prijenosa između ovlaštenih korisnika, njihov sadržaj će se nastojati učiniti nerazumljivim neovlaštenim osobama.[141]

6.2.1.5. Fizičke kontrole

Osim spomenutih metoda, koje se uglavnom odnose na unutarnju zaštitu informacijskog sustava, bitna je i njegova fizička zaštita, kao i zaštita njegovog okruženja. Fizička sigurnost opisuje mjere koje sprječavaju neovlašten pristup resursima ili informacijama pohranjenim na fizičkim medijima. Radi se o skupu smjernica za dizajniranje strukture koja je otporna na razne zlonamjerne radnje.[142] Već su prije spomenute prijetnje koje mogu ugroziti informacijski sustav i njegovu okolinu. One na koje čovjek ne može utjecati niti spriječiti, ali može poduzeti zaštitne mjere, su prirodne nepogode. Osim prirodnih nepogoda, javljaju se i prijetnje poput (dugotrajnog) nestanka struje, prašine, poplava uzrokovane slučajnim kvarovima ili puknućem cijevi, elektromagnetske radijacije (elektromagnetski valovi mogu uzrokovati kvarove na drugim uređajima), ali i ljudske prijetnje poput neovlaštenog pristupa podacima/informacijama i imovini, pogrešnog rukovanja, pa čak i krađe.[143]

U takvim okolnostima potrebno je poduzeti mjere koje će omogućiti nastavak neprekidnog rada informacijskog sustava i time spriječiti gubitak (važnih) informacija.[144] Fizičke kontrole su kontrole kojima se neovlaštenim osobama sprječava pristup uredima, radnim prostorima, postrojenjima, podacima, važnoj informatičkoj opremi, uređajima ili infrastrukturi. Drugim

[140] Ibid.,, str. 138.
[141] Panian, Ž. (2001.) Kontrola i revizija informacijskih sustava. Zagreb: Sinergija, str. 107.
[142] Nacionalni CERT, L&LS (2010.) Fizička zaštita informacijskih sustava. NCERT-PUBDOC-2010-06-304 [online]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf, str. 5. [27. travnja 2019.]
[143] Ibid., str. 8-10.
[144] Ibid., str. 7.

riječima fizičkim kontrola se štite svi oni dijelovi informatičkih i poslovnih resursa koji su vidljivi i opipljivi, a time i mogu ukrasti.[145]

Kako bi se zaštitio IS potrebno je najprije zaštiti njegovu okolinu i prostor. Takva zaštita se može postići na različite načine, primjerice postavljanjem lokota, kojima se onemogućuje ulazak neovlaštenih osoba, postavljanjem zaštitara kako bi se provodila identifikacija osoba na ulazu te poboljšao nadzor okoline, ili postavljanjem nadzornih kamera i alarmnih sustava (krađa, požari i slično).[146] U prostorijama koje sadrže važne poslužitelje ili skupocjene uređaje potrebno je primijeniti veći stupanj zaštite te uvesti veće mjere sigurnosti kao postavljanje gumba za slučaj opasnosti, instalacija protuprovalnog alarma, implementacija sustava protiv upada (zaštita na prozorima i vratima) i slično.[147]

Osim prostorija potrebno je zaštiti i opremu i uređaje. Najviše pažnje se pridaje poslužitelju i osobnim računalima, budući da oni sadrže najviše osjetljivih podataka, međutim ne treba zanemariti ostale uređaje kao na primjer prijenosni mediji. Njih treba pohraniti na sigurna mjesta, a stare adekvatno uništiti.[148]

Poslužitelje najbolje je smjestiti u posebne prostorije koje omogućuju dobro nadziranje, i smjestiti ga tako da se spriječi njegovo pomicanje i premještanje, kako ne bi došlo do kvarova. Osobna računala treba zaključavati i nadzirati, te rasporediti ih tako da niti jedan zaposlenik nema pristup podacima drugog zaposlenika. A da bi se spriječila krađa mogu se postaviti lokoti za zaključavanje kabela te sustavi za praćenje i otkrivanje lokacije ukradenih ili izgubljenih stvari. Sigurnost IS-a može se povećati i implementacijom zaključavanja USB priključaka da bi se spriječilo preuzimanje podataka ili onemogućilo umetanje zlonamjernih programa.[149]

[145] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb, str. 91.
[146] Nacionalni CERT, L&LS (2010.) Fizička zaštita informacijskih sustava. NCERT-PUBDOC-2010-06-304 [online]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf, str. 13. [27. travnja 2019.]
[147] Ibid., str. 14.
[148] Ibid., str. 15.
[149] Ibid., str. 16.

7. Standardi i okviri informacijske sigurnosti

Za organizacije i institucije standardi i okviri predstavljaju važnu podlogu za razvijanje novih ili proširenje već poznatih tematskih područja. Kako bi se podržala informacijska sigurnost, razvili su se tijekom povijesti različiti standardi i okviri. Primjenom takvih sigurnosnih standarda i okvira želi se osigurati uvođenje općepriznatih i jedinstvenih metoda za realizaciju informacijske sigurnosti.[150] Primjena pojedinih standarda upravljanja informacijskim sustavima je u određenim djelatnostima obavezna te je propisana regulatorna obveza primjene nekih normi.[151] U Hrvatskoj to su na primjer HNB-ova regulativa vezana za Odluku o primjerenom upravljanju informacijskim sustavima u svrhu smanjenja operativnih rizika (online dostupno[152]) i HANFA-ine Smjernice za upravljanje rizicima primjene informacijskih sustava (smjernice online dostupne[153]).

Među najpoznatijim standardima i okvirima za informacijsku sigurnosti i upravljanje informacijskim sustavima su obitelj ISO 27000 normi, CobiT 5 i ITIL.

7.1. Obitelj ISO 27000 normi

Međunarodna organizacija za standardizaciju (eng. *International Organization for Standardization*) je 2005. godine uvela ISO/IEC 27001 standard, koji je danas najrašireniji standard upravljanja informacijskom sigurnošću. ISO 27001 norma izravno se odnosi na sigurnost informacija i predstavlja minimalne zahtjeve i mjere koje organizacije/institucija treba poduzeti da bi se uspostavio sustav upravljanja informacijskom sigurnošću (eng. *Information Security Management System – ISMS*).[154] Obitelj ISO 27000 normi obuhvaćaju popis kontrola koje treba implementirati u informacijski sustav kako bi se sigurnosni rizik sveo na prihvatljivu razinu. Novije norme obitelji ISO 27000 su ISO 27002 do 27005, koje bi osim sigurnosti trebale i pokriti i područja upravljanja informatičkim rizicima i provedbe mehanizama kontrole na informacijskim sustavima u svrhu ostvarivanja sigurnosnih i drugih

[150] Bundesamt für Sicherheit in der Informationstechnik (2009.) Informationssicherheit Ein Vergleich von Standards und Rahmenwerken [online]. Dostupno na: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.html, str. 7. [30. travnja 2019.]

[151] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 200.

[152] https://www.hnb.hr/-/smjernice-za-upravljanje-informacijskim-sustavom-u-cilju-smanjenja-operativnog-rizika

[153] https://www.hanfa.hr/objave-sa-sjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/

[154] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 211.

rizika.[155] Najčešći razlog implementiranja ISO 27001 norme je certificiranje, jer propisuje zahtjeve prema kojima je organizaciju moguće certificirati, međutim bez ISO standarda 27002, koji predstavlja skup dobrih praksi za implementaciju kontrola vezanih uz sigurnost informacijskih sustava, certifikacija teško je izvediva.[156]

7.2. CobiT 5

CobiT (eng. *Control Objectives for Information and Related Technology*) je krovni okvir za korporativno upravljanje informatikom, a propisuje područja, procese i pojedinačne kontrole za korporativno i operativno upravljanje informatikom.[157] Također su naglašeni procesi upravljanja, planiranja i usklađivanja IT ciljeva s poslovnim ciljevima organizacije. Standard je izdao ITGI (*IT Governance Institut*), a o njemu se brine međunarodna udruga profesionalaca ISACA (eng. *Information Systems Audit and Control Association*).[158] CobiT predstavlja smjernice za analizu, mjerenje i kontrolu primjene IS-a i pripadne tehnologije u poslovanju, te sadrži 37 ciljeva kontrole i preko 300 informatičkih kontrola i uputa za njihovu primjernu.[159] CobiT definira radni okvir tako da su poslovni procesi organizacije u skladu s arhitekturom i funkcijom IS-a, smanjeni rizici koji nastaju neispravnim ili nepotpunim postavkama IS-a i da je omogućeno upravljanje rizicima IS-a na zadovoljavajući način i korištenje informacijskih resursa na racionalan i učinkovit način.[160]

7.3. ITIL

ITIL (eng. *Information Technology Infrastructure Library*) jedan je od najopširnijih standarda. Iako je nastao prije trideset godina danas se nametnuo kao koristan, praktičan i u svjetskim razmjerima gotovo neizostavan skup preporuka i najbolje prakse pri upravljanju informatičkim uslugama (eng. *IT Service Managment, ITSM*). Prva verzija ITIL-a nastala je 1986., a sastojala se od 40 knjiga i vrijedila do 1999., nakon toga izašla je druga verzija koja

[155] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 212.
[156] Uremović, D. (2012.) Gorak okus revizionizma. Mreža:Revizija informacijskih sustava [online], 11/2012: str. 61-72. Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, str. 66. [2. svibnja 2019.]
[157] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 201.
[158] Uremović, D. (2012.) Gorak okus revizionizma. Mreža:Revizija informacijskih sustava [online], 11/2012: str. 61-72. Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, str. 65. [2. svibnja 2019.]
[159] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 220.
[160] Centar informacijske sigurnosti (2012.) Cobit Framework 5. CIS-DOC-2012-06-051 [online]. Dostupno na: https://www.cis.hr/dokumenti/cobitframework-5.html, str. 6. [4. svibnja 2019.]

se sastojala od 8 knjiga.[161] Posljednja inačica (v3) organizirana je u pet knjiga i u potpunosti usmjerena na pitanje pružanja IT usluga u svrhu ostvarivanja poslovnih ciljeva. Prve tri knjige obrađuju osnovne IT procese, ali i operativne IT procese poput upravljanja incidentima, a preostale dvije razmatraju upravljački dio planiranja, nadzora i kontinuiranog poboljšavanja rada informacijskog sustava.[162] ITIL pruža poslovno usmjeren pristup menadžmentu informatike koji stavlja poseban naglasak na stratešku poslovnu vrijednost informatike i potrebu da se isporuči njezina visokokvalitetna usluga.[163]

[161] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 210.

[162] Uremović, D. (2012.) Gorak okus revizionizma. Mreža:Revizija informacijskih sustava [online], 11/2012: str. 61-72. Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155, str. 66. [2. svibnja 2019.]

[163] Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb. str. 210.

8. Zaključak

Zbog sve bržeg razvoja informacijskih i komunikacijskih tehnologija dostupnost i raspoloživost informacijama sve je veća. Informacije su postale jedan od ključnih resursa današnjice, a primjena digitalnih tehnologija u poslovanju sve je veća. Informacijski sustavi postali su neizostavan dio svakog poduzeća/organizacije. Suvremeni informacijski sustavi i informacijski sustavi uopće uvelike pridonose normalnom odvijanju poslovanja te imaju pozitivan učinak na poslovanje, zbog čega je upravljanje rizicima informacijskog sustava izrazito bitan i potreban dio svake organizacije.

Ponekad se shvaćanje rizika uzima olako i ne posvećuje mu se dovoljna pažnja, osobito jer se radi o složenom i dugotrajanom procesu. No ako organizacija ne posveti dovoljno pažnje tom aspektu, štete koje mogu nastati mogu biti ponekad i nepopravljive. Štetni učinci rizika informacijskog sustava rezultiraju narušavanjem svojstava informacija, a proizlaze iz djelovanja prijetnji koje iskorištavaju ranjivosti resursa informacijskog sustava.

Da bi zaštita informacijskog sustava bila što bolja potrebno je uključiti sve korake procesa upravljanja rizikom, što znači, od razumijevanja samog informacijskog sustava, identifikacije mogućih prijetnji sve do poduzimanja odgovarajućih kontrola (protumjera). Kada se spominje zaštita informacijskog sustava često se misli na njegovu logičku zaštitu, no važno je reći kako je fizička zaštita informacijskog sustava jednako važna kao i njegova logička.

Paralelno s razvojem informacijskih i komunikacijskih tehnologija i primjenom informacijskih sustava u poslovanju i uopće, razvila se i svijest o važnosti informacijske sigurnosti. Kao rezultat toga razvili su se standardi i okviri koji danas čine podlogu za učinkovito upravljanje informacijskom sigurnošću i informacijskim sustavima.

9. Literatura

Knjige:

1. Andrijanić, I., Gregurek, M., Merkaš, Z. (2016.) Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada
2. Datt, S. (2016.) Mrežna forenzika: zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan
3. Dragičević, D. (2004.) Kompjutorski kriminalitet i informacijski sustavi. Zagreb: IBS
4. Garača, Ž., Ćukušić, M. (2011.) Višedimenzijski informacijski sustavi. Skladištenje i analitička obrada podataka. Split: Ekonomski fakultet
5. Javorović, B., Bilandžić, M. (2007.) Poslovne informacije i business inteligence. Zagreb: Golden marketing-Tehnička knjiga
6. Krakar, Z., Tomić Rotim, S., Žgela, M., Arbanas, K., Kišasondi, T. (2014.) Korporativna informacijska sigurnost. Varaždin: Fakultet organizacije i informatike Sveučilišta u Zagrebu
7. Panian, Ž. (2001.) Kontrola i revizija informacijskih sustava. Zagreb: Sinergija
8. Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. (2010.) Poslovni informacijski sustavi. Zagreb: ELEMENT
9. Panian, Ž., Spremić, M. (2007.) Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri
10. Panian, Ž., Strugar, I. (2013.) Informatizacija poslovanja. Zagreb: Ekonomski fakultet
11. Pavlić, M. (2011.) Informacijski sustavi. Zagreb: Školska knjiga d.d.
12. Šimović, V., Ružić-Baf, M. (2013.) Suvremeni informacijski sustavi. Pula: Sveučilište Jurja Dobrile u Puli
13. Spremić, M. (2017.) Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski fakultet – Zagreb
14. Vukičević, M., Odobašić, S. (2012.) Upravljanje rizicima. Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti "Baltazar Adam Krčelić"

Internetski izvori:

15. Bundesamt für Sicherheit in der Informationstechnik (2009.) Informationssicherheit Ein Vergleich von Standards und Rahmenwerken [online]. Dostupno na:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.html

16. CARNet CERT, L&LS (2010.) Metodologija penetracijskog testiranja. CCERT-PUBDOC-2008-02-219 [online]. Dostupno na: https://www.cis.hr/www.edicija/Metodologijapenetracijskogtestiranja.html
17. Centar informacijske sigurnosti (2012.) Cobit Framework 5. CIS-DOC-2012-06-051 [online]. Dostupno na: https://www.cis.hr/dokumenti/cobitframework-5.html
18. Drljača, M. (2006.) Model informacijskog sustavaza upravljanje poslovnim - procesom. Kvaliteta: Časopis za unapređenje kvaliteta [online]., 16 (5-6): str. 47-51. Dostupno na: https://bib.irb.hr/prikazi-rad?&rad=520681
19. Hrvatska agencija za nadzor financijskih usluga (2014.) Smjerniceza primjereno upravljanje rizicima informacijskih sustava subjekata nadzora [online]. Dostupno na: https://www.hanfa.hr/objave-sa-sjednica/24102014_-66-sjednica-upravnog-vijeca-hanfe/
20. Nacionalni CERT (2018.) Phishing. NCERT-PUBDOC-2018-5-361 [online]. Dostupno na:https://www.cert.hr/phish
21. Nacionalni CERT (2018.) Socijalni inženjering i zlonamjerni softver. CERT.hr-PUBDOC-2018-11-369 [online]. Dostupno na:https://www.cert.hr/NCSocIZS
22. Nacionalni CERT (2018.) Uvod u socijalni inženjering. CERT.hr-PUBDOC-2017-11-349 [online]. Dostupno na: https://www.cert.hr/32749/
23. Nacionalni CERT, L&LS (2010.) Fizička zaštita informacijskih sustava. NCERT-PUBDOC-2010-06-304 [online]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf
24. Stoneburner, G., Goguen, A., Feringa, A. (2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30. Dostupno na:https://www.nist.gov/publications/risk-management-guide-information-technology-systems
25. The New York Times [online]. Dostupno na: https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html

26. Uremović, D. (2012.) Gorak okus revizionizma. Mreža: Revizija informacijskih sustava [online], 11/2012: str. 61-72. Dostupno na: http://alterinfo.hr/fullpage.aspx?PartID=155
27. Welt [online]. Dostupno na: https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/article169293837/Alle-Yahoo-Accounts-von-Datenklau-im-Jahr-2013-betroffen.html
28. Zimo-NovaTV [online]. Dostupno na: https://zimo.dnevnik.hr/clanak/yahoo-pod-istragom-zbog-kradje-podataka---464556.html

Upravljanje rizicima informacijskog sustava

Sažetak

Težište ovog rada je na informacijskim sustavima i upravljanju rizicima informacijskog sustava. Zbog sve bržeg razvoja informacijskih i komunikacijskih tehnologija sve se više organizacija oslanja na informacijske sustave. Radi se o sustavima dizajnirani za prikupljanje, obradu, pohranjivanje i distribuciju informacija. Oni potpomažu organizaciji u ostvarivanju postavljenih ciljeva i donošenju pravih odluka. Iz tog razloga proces upravljanja rizicima igra važnu ulogu u zaštiti informacija i organizacije od IT-rizika. Djelotvorno upravljanje rizicima čini važnu komponentu za uspješno funkcioniranje informacijskog sustava, a sastoji se od dva glavna koraka; procjene rizika i ublažavanje rizika. Upravljanje rizicima ne omogućuje samo prepoznavanje slabosti i ranjivosti sustava nego i predviđanje, a time i sprječavanje nastanka štete. Kako bi se podržala informacijska sigurnost razvili su se različiti standardi i okviri, a među najpoznatijima su Obitelj ISO 27000 normi, CobiT i ITIL.

Ključne riječi: informacije, informacijski sustav, upravljanje rizicima, standardi

Risk management for information systems

Summary

The focus of this paper are information systems and their risk management. Information systems are systems designed to collect, process, store and distribute information. The rapid growth of information and communication technology has led organizations to rely on information systems more than ever. In this digital age almost every organization uses information systems to process their information. They support the organization to achieve their mission and to make better decisions. Therefore, risk management plays a critical role in protecting an organization's information assets and thus its mission from IT-related risks. An effective risk management process is an important component of a successful information system and includes two main steps; risk assessment and mitigation. With risk management its not only possible to notice system weaknesses and vulnerability, but also to predict and prevent a possible harmful event. Therefore, standards and frameworks were developed to help organizations manage information systems and security. Some of the most popular are ISO/IEC 27000 family, CobiT and ITIL, which also will be briefly presented.

Keywords: informations, information system, risk management, standards