SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE U VARAŽDINU

Dino Alagić, Mario Vagner i Vedran Branković

Pojednostavljenje primjene metode procjene rizika uz regionalizaciju prijetnji informacijskom sustavu

Varaždin, 2011.

Ovaj rad je izrađen na Fakultetu organizacije i informatike u Varaždinu, pod vodstvom prof. dr. sc. Željka Hutinskog i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2010/2011.

SADRŽAJ

Popis grafikona:

Popis slika:

Popis tablica:

Sažetak

U današnjim tržišnim okolnostima neizbježna je činjenica da se sve veći dio poslovanja odvija uz potporu informacijskih sustava. Kako se oni sve više koriste, sve su veći i sigurnosni rizici koji im prijete. Zbog toga je sigurnost informacija u nekom sustavu realnost i potreba. Pretpostavka njihove sigurnosti je provedba procjene rizika u poslovnom sustavu. Kroz istraživanja u ovom radu provedena je usporedba metoda procjene rizika, selekcija najprikladnije te njena nadogradnja. Kroz drugi dio istraživanja kreiran je prvi hrvatski javno dostupni katalog napada na sigurnost koji je zatim integriran u aplikaciju koja je razvijena u sklopu rada. Time je stvorena mogućnost procjene rizika i sigurnosno needuciranim korisnicima, i to besplatno. Krajnji cilj ovog rada je svojim doprinosom povećati razinu sigurnosti u poslovnim sustavima kroz povećanje svijesti za to odgovornih osoba u organizacijama. Kroz sve navedeno stvoreni su svi potrebni uvjeti za ispunjenje tog cilja.

Ključne riječi

Sigurnosni rizici, informacijski sustav, sigurnost informacija, metode za procjenu rizika, Octave Allegro, katalog napada na sigurnost, prijetnje, ranjivost, aplikacija za procjenu rizika

Abstract

In today's market circumstances, the inevitable fact is that more and more growing portion of business is being conducted with the support of information systems. With its greater use comes a greater security risk that threatens them. Therefore, information security is not just a need, it's a necessity. To insure its safety, companies must conduct security risk assessments for their information systems. Through research conducted in this paper, comparison of methods for risk assessment, and selection of the most appropriate methods has been made. Through the second part of the paper we created the first Croatian publicly available catalog of security attacks and threats, which was then integrated into the application that was developed within this research. This created the possibility for users weakly educated in this area to conduct risk assessments, and for free. The ultimate goal of this paper is to contribute to the potential increase of levels of concern about security in companies through increasing awareness for security of the responsible persons in the organization. Through all of the above all necessary conditions for achieving that goal were created.

Key words

Security risks, information system, security of information, risk assessment methods , Octave Allegro, catalog of security threats, threats, vulnerability, application for risk assessment

1. Uvod

Danas se poslovni procesi u poslovnim sustavima sve više oslanjaju na informacijsku potporu kako bi se povećala učinkovitost poslovanja i prilagodilo zahtjevima iz okoline. Kako se poslovni procesi usmjeravaju sve više prema korisnicima tako poslovni sustavi povećavaju dostupnost informacijskog sadržaja javnosti i svojim korisnicima. Time sa druge strane bitni podaci i informacije postaju dostupniji neovlaštenim korisnicima i postoji mogućnost narušavanja njihovog integriteta, povjerljivosti i dostupnosti. Navedene tvrdnje podupiru podaci o napadima na sigurnost koje prikupljaju poslovni sustavi i institucije koje se bave sigurnošću računalnih i informacijskih sustava.

Napadi na sigurnost se provode pronalaženjem sigurnosnih propusta u aplikacijama i informacijskim sustavima. Ovisno o tipu napada i namjerama napadača proizlaze različite posljedice koje će utjecati na poslovanje poslovnih sustava. Realizacijom napada na sigurnost može doći do neovlaštenog prikupljanja, mijenjanja i brisanja podataka, uskraćivanja usluga te gubitka ili oštećenja podataka uzrokovanog nekim vanjskim utjecajima zbog lošeg upravljanja i planiranja u poslovnom sustavu.

Većina korisnika informacijskih sustava i aplikacija u poslovnim sustavima nije dovoljno educirana za korištenje informacijske tehnologije i načinom na koji ona funkcionira, te samim time nisu svjesni ranjivosti kojima se izlažu njenim korištenjem. Kako bi poslovni sustavi odgovorili na sve veće zahtjeve tržišta, ona uvode u poslovanje nove i složene informacijske tehnologije za koje nije moguće odmah otkriti potencijalne ranjivosti. Uz to napadi na sigurnost se s vremenom sve više razvijaju i predstavljaju time sve veću opasnost za sigurnost informacijskih sustava i krajnje korisnike. Podaci o napadima na sigurnost koji su prikupljeni u bazama podataka kao što su: CVE, CWE, Bugtrack i DatalossDB idu u prilog prethodnim tvrdnjama. Oni pokazuju kako se broj napada na sigurnost u zadnjih deset godina značajno povećao.

Stoga bi poslovni sustavi trebali posvetiti određenu pažnju sigurnosti informacijskog sustava, ne samo zbog zaštite svoga poslovanja nego i zbog svojih klijenata. Ukoliko se tome ne posveti dovoljno pažnje korisnički podaci koji su prikupljeni u poslovnom sustavu mogu biti neautorizirano prikupljeni, distribuirani, obrađivani ili uništeni.

U sklopu rada je izrađena besplatna aplikacija za procjenu rizika kako bi se olakšala i približila procjena rizika sigurnosno needuciranim korisnicima. Aplikacija je izdana pod GNU GPL v3 licencom što znači da je otvorenog koda. Smatramo da smo time napravili veliki društveni doprinos kako je to **prva besplatna aplikacija za procjenu rizika u svijetu** koliko je opće poznato i javno je dostupna. Ova aplikacija ne samo da omogućuje provođenje Octave Allegro metode nego ju i nadopunjuje primjerima te prijedlozima za napade na sigurnost do čijeg smo kataloga došli vlastitim istraživanjem. Smatramo da naša aplikacija ima potencijala za promjenu sadašnjeg stava prema procjeni rizika u informacijskim sustavima: „To je presloženo“ ili „Mi to ne znamo“ ili pak „Alati za provedbu metoda su preskupi“!

1.1. Problem i predmet istraživanja

Prilikom razvoja sigurnosti informacijskih sustava potrebno je provesti procjenu rizika kako bi se moglo odlučiti na koji način će se upravljati rizicima. Postoji mnogo različitih metoda i metodologija za procjenu rizika stoga je u radu napravljeno istraživanje dostupnih metodologija i metoda za procjenu rizika kako bi se odabrala najprikladnija. Na temelju usporedbe odabrana je metoda Octave Allegro.

U radu su definirana tri temeljna cilja na temelju kojih su se postavile hipoteze. Kroz njih su se željeli prikazati problemi koji se mogu pojaviti upotrebom informacijske tehnologije u poslovanju. Kao doprinos rješavanju navedenih problema izrađena je aplikacija za procjenu rizika pomoću Octave Allegro metode. Cilj aplikacije je približiti i olakšati procjenu rizika sigurnosno needuciranom korisniku i stručnjacima iz područja sigurnosti informacijskih sustava. Kako bi se to ostvarilo aplikacija je napravljena tako da je dostupna putem Interneta i može se besplatno koristiti. Kako bi se olakšala procjena rizika unutar aplikacije je integriran katalog najčešćih napada na sigurnost.

Kako nije postojao jedinstveni katalog najčešćih napada na sigurnost trebalo ga je sastaviti u sklopu rada. Tijekom prikupljanja podataka o najčešćim napadima na sigurnost zaključeno je kako se zastupljenost i intenzitet napada na sigurnost ne odnosi jednako za sve zemlje. Zbog toga je prije svega kreiran katalog najčešćih napada na sigurnost na temelju svih dostupnih izvora koji su bili na raspolaganju. U Hrvatskoj ne postoje javno dostupni izvori iz kojih bi se prikupili podaci o napadima na sigurnost. Kako bi se došlo do podataka koji se odnose na Hrvatsku provedena je anketa na temelju koje je kreiran jedinstveni katalog podataka napada na sigurnost.

Nakon izrade aplikacije provedeno je njezino testiranje na primjeru iz prakse. Testiranje je proveo stručnjak iz područja sigurnosti informacijskih sustava i korisnik koji nema dovoljno znanja iz područja sigurnosti informacijskih sustava. Uočeno je kako naše istraživanje pomaže u određenoj mjeri i profesionalcima i prosječno informatičko obrazovanim korisnicima što i je glavni cilj ovog rada.

1.2. Ciljevi istraživanja

1. Pokazati ovisnost poslovnog sustava o informacijskom sustavu koji unutar sebe sadrži određene ranjivosti čime se povećava sigurnosni rizik.
2. Pokazati kako povećanje sigurnosnog rizika može negativno utjecati na poslovanje poslovnog sustava i njegove rezultate poslovanja.
3. Pokazati način na koji se postojeći rizici u informacijskom sustavu poslovnog sustava mogu svesti na najmanju moguću mjeru, uz sustavno uvođenje sigurnosti informacijskog sustava pri čemu je neophodno provesti procjenu i izračun rizika.
4. Istražiti dostupne metode i metodologije za procjenu rizika i postaviti kriterije za odabir najpogodnije metode za procjenu rizika.
5. Usporediti metode za procjenu rizika prema odabranim kriterijima kako bi proučili odabranu metodu.
6. Dokazati prvu hipotezu.
7. Razviti aplikaciju uz pomoću koje će se dokazati druga hipoteza.

1.3. Hipoteze istraživanja

Za izradu i postizanje ciljeva rada postavljene su dvije hipoteze:

Prva hipoteza (H1) u radu je:

Katalozi napada na sigurnost koji postoje u svijetu nisu primjenjivi na svim regionalnim područjima već se popis napada na sigurnost treba lokalizirati da bi se mogao primijeniti u procjeni rizika.

Metodologija koja je korištena kod dokazivanja prve hipoteze objašnjena je u *devetom poglavlju*.

Druga hipoteza (H2) u radu je:

Razvijenu aplikaciju za procjenu rizika mogu zadovoljavajuće koristiti i slabo sigurnosno educirani korisnici.

Metodologija koja je korištena kod dokazivanja druge hipoteze objašnjena je u *jedanaestom poglavlju*.

2. Zavisnost poslovnog sustava o informacijskom sustavu

Informacijski sustav predstavlja uređeni skup elemenata, odnosno komponenata koje u interakciji obavljaju funkcije prikupljanja, obrade, pohranjivanja i diseminacije (izdavanja na korištenje) informacija. Drugim riječima informacijski sustav djeluje unutar nekog poslovnog sustava, omogućavajući mu da komunicira unutar sebe i sa svojom okolinom. Informacijski sustav preuzima informacije, obrađuje ih i prerađene prezentira poslovnom sustavu ili okolini. Dakle, informacijski sustav predstavlja podsustav poslovnog sustava. [62, 63]

Informacijski sustavi podupiru rad poslovnih informacijskih sustava. Kako bi ovaj sustav funkcionirao, podatke je potrebno prikupiti iz različitih izvora, zatim pohraniti ih na prikladne medije kako bi bile raspoložive na duži rok ili trajno. Nakon što su podaci prikupljeni, slijedi njihova obrada koja se može opisati kao primjena aritmetičko-logičkih postupaka, odnosno operacija kojima se podaci pretvaraju (transformiraju) iz izvornog u neki drugi, željeni oblik. Tako preoblikovane informacije nerijetko će se pohranjivati iz razloga sličnih onima zbog kojih se to čini i s izvornim informacijama. Konačno, izlazne podatke treba dostaviti, odnosno dostaviti korisnicima (konzumentima). Imajući u vidu sve navedeno, može se definirati i širi pojam informacijskog sustava. [62][63]

U poslovnim sustavima, informacijski sustavi podržavaju i podacima poslužuju poslovne procese i operacije, poslovno odlučivanje te razvijanje i implementaciju kompetitivnih strategija poslovanja. U tom smislu može se govoriti o poslovnim informacijskim sustavima. [62, 63]

Razvojem ICT tehnologije informacijski sustavi se sve više oslanjaju na nove tehnologije koje su ranjive. Tijekom razvoja aplikacija nije moguće potpuno testirati kod i uvidjeti sve moguće propuste je kasnije lako iskoristiti za narušavanje sigurnosti poslovnog sustava.

Prema Gartner i Standish Group istraživanju prosječan financijski gubitak uslijed prekida odvijanja poslovnih procesa jedan sat iznosio je:

- ✓ Investicijsko posredništvo 6,5 milijuna USD,
- ✓ Kartičarsko poslovanje (autorizacija kreditnih kartica) oko 2,6 milijuna USD,
- ✓ Logistika i paketna distribucija oko 150.000 USD,
- ✓ Rezervacijski sustavi za zrakoplove oko 90.000 USD,
- ✓ Fortune 500 lista - prosječan gubitak je oko 96.000 USD po minuti. [61]

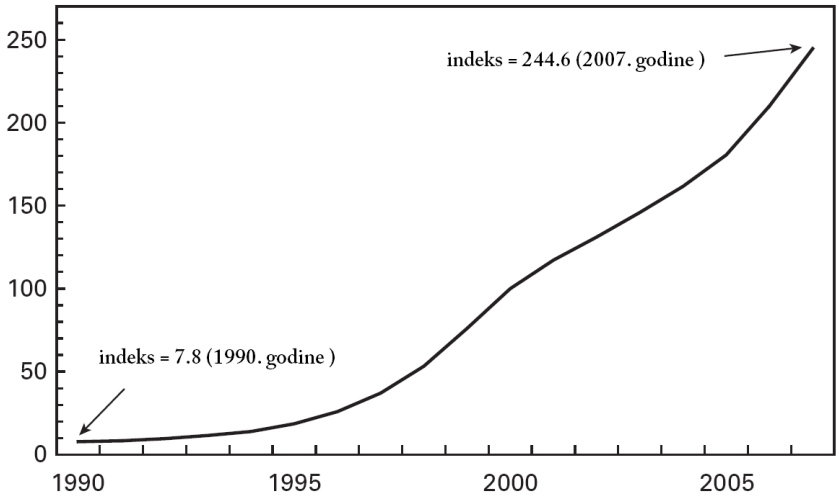
Dakle iz navedenog istraživanja vidljivo je kako organizacije čiji procesi ovise o informacijskim sustavima imaju velike financijske gubitke ukoliko dođe do prekida njihovih izvođenja. Dostupnost informacijskog sustava je bitna ne samo jer su veliki financijski gubitci u slučaju nedostupnosti sustava već uz pomoć njih organizacije ostaju u utrci s konkurencijom. Sljedeća tablica prikazuje kolika je dostupnost pojedinih informacijskih sustava bitna za poslovanje organizacija kako bi se njihovi procesi mogli odvijati neprekidno. [61]

Tablica 2.1. - Dostupnost informacijski sustava [61]

Vrijeme dostupnosti	Maksimalno vrijeme nedostupnosti u jednoj godini
99.9999%	31.5 sekundi
99.999%	5 minuta i 35 sekundi
99.99%	52 minuta i 33 sekunde
99.9%	8 sati i 46 minuta
99.0%	87 sati i 36 minuta
95.0%	18 dana i 8 sati
90.0%	36 dana i 12 sati

Informacijsku imovinu poslovnog sustava predstavlja sve ono što za njega ima vrijednost. Najčešće to uključuje podatke iz baza podataka, podatke, aplikacije, dokumentaciju aplikacija, interne akte i slično. [36] Kako bi ta imovina bila dostupna bitna je sigurnost informacijske imovine, jer analogno sigurnosti fizičke imovine, postoji potreba zaštite informacijske imovine. Organizacije žele biti sigurne da će njihovu informacijsku imovinu koristiti samo oni, i isto tako da će pristup njihovim podacima imati samo oni kojima

se pristup dozvoli. Bitno je spomenuti da je informacijska imovina u poslovnim sustavima u naglom porastu zadnjih deset godina. [12]



Grafikon 2.1. - Porast informacijske imovine u poslovnim sustavima [12]

Broj informacijske imovine koje poslovni sustavi koriste na području Sjedinjenih Američki Država je izražen indeksom sa grafikona. U godini 2000. iznosio je 100. [12]

Uloga suvremenih poslovnih informacijskih sustava se svodi na dvije osnovne funkcije:

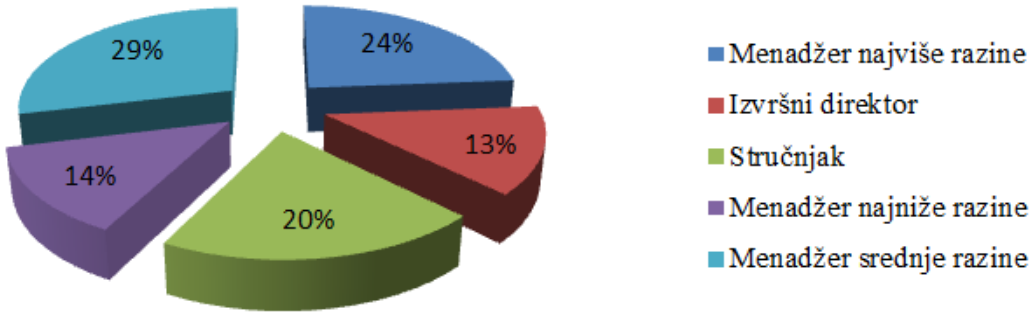
- ✓ pripremu informacijske podloge za donošenje poslovnih odluka,
- ✓ dokumentiranje, odnosno trajno pohranjivanje ranije generiranih informacija. [62, 63]

Da bi se moglo govoriti o suvremenom i sustavnom načinu poslovanja i donošenja poslovnih odluka, jedan od važnih preduvjeta je učestalo korištenje kvalitetne informacijske podloge integriranog poslovno-informacijskog sustava. Prema rezultatima istraživanja koja su provedena u poslovnim sustavima na području Hrvatske, različite razine menadžmenta s različitom učestalosti koriste informacije iz poslovno-informacijskog sustava u poslovnom odlučivanju. [12]

Tablica 2.2. - Korištenje poslovnih informacija pri poslovnom odlučivanju [12]

Učestalost korištenja informacija	**Niži menadžment**	**Srednji menadžment**	**Viši menadžment**
Vrlo rijetko	8,5%	0,0%	5,1%
Rijetko	18,6%	8,5%	10,2%
Povremeno	30,5%	33,9%	28,8%
Često	20,4%	39,0%	18,6%
Vrlo često	22,0%	18,6%	37,3%
Ukupno	**100,0%**	**100,0%**	**100,0%**

Prema rezultatima iz gornje tablice, vidljivo je da se rijetko i vrlo rijetko poslovne informacije iz poslovno-informacijskog sustava pri poslovnom odlučivanju koriste kod nižeg menadžmenta (27,1%), zatim kod višeg menadžmenta (15,3%) i, naposljetku, kod srednjeg menadžmenta (8,5%). Može se zaključiti da poslovne informacije pri poslovnom odlučivanju najčešće koristi srednji, zatim viši, a najrjeđe niži menadžment. Struktura ispitanika prema nazivu radnog mjesta prikazana je na sljedećem grafikonu. [12]



Grafikon 2.2. - Struktura ispitanika prema nazivu radnog mjesta [12]

Rezultati pokazuju praktično prihvatljivu i pozitivno sugestivnu činjenicu da s obzirom na vrstu radnih zadataka pojedine razine menadžmenta u dovoljnoj mjeri koriste poslovne informacije pri poslovnom odlučivanju. Integriranost poslovno informacijskog sustava nameće se sama po sebi kao integrirajući element cjelovite poslovne organizacije, koja računa na buduće kvalitetno i konkurentno poslovanje. Upravo je navedeni razlog glavni pokretač razvoja, poboljšanja i objedinjenosti poslovnih procesa, što utječe i na integriranost poslovnog informacijskog sustava. [12]

PwC[1] je anketirala 436 generalnih menadžera kompanija koji su se jednoglasno složili da je IT važan u njihovom poslovanju. Osamdeset posto ispitanika smatra da su IT u najvećoj mjeri važne ili vrlo važne za njihovo poslovanje. Kompanije koje spadaju u tih 80% ostvarile su 72% veći rast prihoda nego kompanije čiji vrhovni menadžeri smatraju IT (samo) važnim u svom poslovanju. Najvažnije informacijske tehnologije primijenjene od strane kompanija koje su sudjelovale u anketi predstavljaju financijske i upravljačke sustave (implementirani u 57% slučajeva), marketinške sustave (52%) i sustave koji podržavaju prodaju i usluge kupcima (37%). [63]

Osnovni problem uporabe IT u poslovanju predstavlja nedostatak sigurnosti (84%, što predstavlja rast od 7% u odnosu na rezultate prijašnjih anketa) i nestručnost ili nedovoljno obrazovanje osoblja (26%, koje je u prvom anketiranju iznosilo 48%). [63]

Učestalost i intenzitet prijetnji poslovnog sustava se povećava sukladno sa porastom njegove oslonjenosti na informacijsku i komunikacijsku tehnologiju.

[1] **PwC** (**P**rice**w**aterhouse**C**oopers) je globalna profesionalna organizacija sa sjedištem u Londonu, koja se bavi pružanjem usluga financijskog savjetovanja.

[2] **NIST** - ***N**ational **I**nstitute of **S**tandards and **T**echnology, u periodu između 1901. i 1988. poznatiji kao*

3. Sigurnost informacijskih sustava

Kako bi važnost informacije bila što jasnija potrebno je detaljnije definirati određene pojmove. Informacija predstavlja imovinu i kao takvu ju je potrebno dodatno zaštititi, kako bi se poslovanje organizacije moglo normalno izvršavati. Danas bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti prikladno zaštićena. Pod pojmom informacijske sigurnosti podrazumijeva se zaštita informacija od velikog broja prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik te povećao broj poslovnih prilika što u konačnici rezultira i većom dobiti. Kako bi se zaštitile informacije potrebno je primijeniti određene kontrole, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkcije sklopovske i programske opreme. Također je potrebno provesti i sigurnosne mjere koje uključuju mehanizme i procedure koje trebaju biti implementirane u svrhu odvraćanja, prevencije, detektiranja i oporavka od utjecaja incidenata koji djeluju na povjerljivost, cjelovitost i raspoloživost podataka. Prilikom napada na sustav, njegove servise ili resurse, potrebno je napraviti izvještavanje o napadima na sigurnost. Sigurnost informacijskih sustava je dinamičan proces tijekom cijelog životnog ciklusa sustava te se on treba razmatrati od faze njegovog planiranja, razvoja, provedbe, operativnosti, rasta do rashodovanja i uništavanja prema potrebi. To je zapravo proces upravljanja rizikom koji se koristi za procjenu, nadgledanje, ukidanje, izbjegavanje, prijenos ili prihvaćanje rizika. Općenito se može reći da sigurnost informacijskih sustava obuhvaća sve što i informacijska sigurnost u širem smislu, samo primijenjeno u užim tehnološkim okvirima. Danas se organizacije suočavaju s velikim brojem sigurnosnih prijetnji poput računalnih prijevara, špijunaže, sabotaže, vandalizma, ali i onih ekoloških kao što su požar, poplava i sl. Upravo radi velikog broja raznih prijetnji za upravljanje sigurnošću informacijskog sustava potrebno je sudjelovanje svih zaposlenika organizacije, a često je potrebna pomoć vanjskih konzultanata. [45]

3.1. Povijesni razvoj odnosa prema temeljnim principima procjene rizika IS

Razvoj na području unapređenja sigurnosti IS-a upravljanjem sigurnosnim rizicima počinje 70-tih godina nastajanjem prve metodologija upravljanja rizikom FIPS 65 pod pokroviteljstvom Nacionalnog ureda za standardizaciju (*National Bureau of Standards*) Vlade Sjedinjenih Američkih Država. Ta je metodologija potaknula nastanak cijelog niza metoda koje su pokušavale zadovoljiti zahtjeve i propise sigurnosti IS-a koje je određivala Vlada SAD-a. Vlada SAD-a u svojim je institucijama definirala nekoliko kriterija namijenjenih

unapređenju sigurnosti u državnim organizacijama. Među njima se ističu kriteriji koje propisuje Ured za menadžment i proračun (*Office of Management and Budget - OMB*) Ministarstvo obrane (DoD), *Computer Security Act* i mnogi drugi. Posebno su na području sigurnosti IS-a napredovale *National Institution for Standardization* (NIST) i *Government Accounting Office* (GAO) agencije. U SAD-u je u razvoj područja unapređenja sigurnosti IS-a od početaka uključeno i Ministarstvo obrane (*Department of Defense- DoD*) koje potiče nastajanje publikacija serije 5200 koje su temelj kasnijem Army Regulation 380-19. [64]

Najveći doprinos upravljanju sigurnosnim rizicima na području Europe dala je Vlada Velike Britanije i njezino Ministarstvo trgovine i industrije (*UK Department of Trade and Industry – DTI*) koje je predstavilo kriterije sigurnosti IS-a British Standard 7799 (BS 7799). Ti su kriterij temelj metodama CRAMM, COBRA i RuSecure. Nešto se kasnije i *International Standardization Organization* (ISO) pridružila naporima za unapređenje sigurnosti IS-a iz kojih nastaje norma ISO/IEC 17799 kao jedna od najpopularnijih. ISO je nastavio razvoj sigurnosti i na drugim područjima i to nizom drugi projekata kao sto su *Guidelines for the Menagement of IT Security* (GMITS) i *Common Criteria* (CC). Uz te metode treba spomenuti i metodu FMEA koju razvija *DoD,*a koristi je *National Agency of Space Exploration* (NASA), te metode MARION, MEHARI i MELISA koje su nastale na izvornim kriterijima propisuje francuska vojska odnosno industrija IT-a u Francuskoj. Osim njih postoje i nezavisni kriteriji zadržani u publikaciji *Cobit Control Objectives* i pripadnoj metodi koji nastaju na temelju najboljih iskustava drugih kriterija i metoda upravljanja rizikom i sigurnošću. Navedeni pravci razvoja metoda i metodologija za procjenu rizika osim po području nastanka razlikuju se po metodološkim osobinama te učestalosti primjene. [64]

NIST[2] metoda poštuje kriterije zadane u NIST 800-14 *Generally Accepted Principles and Practices for Security Information Technology Systems* publikaciji kojom su izvedeni kriteriji iz vladinih pravilnika (OMB,*Computer Security Act* i dr.) i jasno određuje procjenu rizika kao prvi korak u procesu upravljanja rizikom. U trećem dijelu publikacije SP NIST 800-30 popisuju se postupci i tehnike procjene rizika GAO ured (*General Accounting Office*) SAD-a potaknut zahtjevima vlade SAD-a izrađuje skup tehnički dokumenata za upravljanje rizikom. U seriji njegovi izdanja propisuje se način upravljanja rizikom, a osnovni je dokument *Executive Guide for* Information Security Menagment GAO/AIMD-98-68 koji je

[2] **NIST** - ***N**ational **I**nstitute of **S**tandards and **T**echnology, u periodu između 1901. i 1988. poznatiji kao Nacionalni ured za standarde (NBS).*

1998. nastao. Krajem 1999. objavljen je i dotatak pod nazivom *Information Security Risk Managemend, Practices of Leading Organizations* GAO/AIMD-00-33 u kojem se opisuje sam proces procjene rizika. Načela upravljanja rizikom utvrđena u tim istraživanjima GAO sažima u sljedeće korake :

- ✓ uspostava središnje točke interesa,
- ✓ utvrđivanje potreba i procjena rizika,
- ✓ primjena odgovarajućih politika i kontrola,
- ✓ promidžba svijesti o sigurnosti,
- ✓ praćenje i procjenjivanje politike i učinkovitosti kontrola. [64]

Kriterije metode COBIT (*Control Objectives for Information related Technology*) razvija *IT Governace Institute* (ITGI) koji je osnovao *Information Systems Audit i Control Fundation* (ISACF). COBIT se sastoji od jedinstvenog skupa kontrolnih uputa definiranih *Framework and Control Objectives – Audit Guidelines* dokumentu. To je model koji zadovoljava potrebe cjelovitog upravljanja IT-om. COBIT se sastoji od jedinstvenog skupa kontrolnih uputa i programskog proizvoda koji omogućava implementaciju uputa definiranih u Framework and *Control Objectives – Audit Guidelines*. Upute *COBIT Management Guidelines* razvijene su na rezultatima mnogobrojnih Rasprava i iskustvima 40 stručnjaka iz područja sigurnosti i isto toliko standarda i praksi iz cijelog svijeta. Uključuje standarde kao što su ISO, DTI, OECD, NIST, BS, CC i mnogi druge. [64]

3.2. Koraci izgradnje sustava informacijske sigurnosti

Da bi se izgradnja informacijskog sustava sigurnosti mogla provesti potrebna je potpuna suglasnost uprave poslovnog sustava za njeno provođenje. Uprava mora donijeti odluku o granici razvoja informacijskog sustava sigurnosti kako bi opseg razvoja bio potpuno jasan. Također mora odobriti predviđeni financijski proračun jer se bez novca ne mogu osigurati potrebni resursi za izgradnju informacijskog sustava sigurnosti. Na samom kraju uprava mora donijeti odluku o izgradnji informacijskog sustava sigurnosti i tek nakon toga projekt može krenuti sa svojom realizacijom.

Koraci izgradnje sustava informacijske sigurnosti su:

1. Definiranje i donošenje politike sigurnosti

2. Procjena sigurnosnih rizika

a) Identifikacija informacijske imovine i određivanje njezinog vlasnika

b) Procjena značaja podatkovnog sadržaja

c) Procjena izvora, oblika i intenziteta prijetnji

d) Izračun rizika

3. Odabir mjera za smanjenje rizika

4. Izjava o primjenjivosti

5. Praćenje efikasnosti (funkcionalnosti) postavljenog sustava

6. Dogradnja sustava ISMS (Information Security Management System).[36]

Politiku sigurnosti dužna je donijeti uprava, a ona može biti u obliku krovnog dokumenta, pravilnika ili može biti sadržana u statutu poslovnog sustava. Ključan dio izgradnje informacijskog sustava je procjena sigurnosnih rizika. Ukoliko bi se krivo procijenili sigurnosni rizici ne bi se postigla adekvatna zaštita i poslovni sustav bi zbog toga moglo ostvariti velike gubitke. [36]

Procjena sigurnosti rizika se sastoji od više aktivnosti. Prvo je potrebno identificirati svu informacijsku imovinu poslovnog sustava. Informacijska imovina je važna za poslovni sustav jer bez potrebnih informacija može doći do ne mogućnosti izvođenja procesa i poslovne djelatnosti. Vrlo je važno identificirati svu informacijsku imovinu poslovnog sustava u opsegu izgradnje sustava jer će se svi daljnji koraci provoditi samo na identificiranoj informacijskoj imovini. Ukoliko se ne identificira neka informacijska imovina sustav sigurnosti neće biti u stanju zaštititi tu informacijsku imovinu od mogućih prijetnji te će njihova realizacija moći ugroziti odvijanje poslovnog procesa ili više njih. Potrebno je za svaku identificiranu informacijsku imovinu utvrditi njezinog vlasnika kako bi se znalo tko je točno za nju odgovoran, tko će provoditi određene mjere zaštite za tu imovinu i tko će odgovarati za tu imovinu. Nakon što je identificirana sva informacijska imovina poslovnog sustava potrebno je procijeniti njezin značaj. Od vlasnika svake identificirane informacijske imovine treba prikupiti podatke kako bi se ustanovilo koliki značaj ima pojedina imovina na izvođenje poslovnih procesa. Nakon toga treba izraditi popis prijetnji te navesti izvore prijetnji, oblike i intenzitet prijetnji kako bi se moglo odlučiti kako će se upravljati rizikom i kako bi se mogao izračunati rizik. Izračun rizika ovisi o metodi kojom se provodi procjena sigurnosnih rizika. [36]

Na temelju identificiranih prijetnji odabrat će se mjere za smanjenje rizika. Prije revizije izjavom o primjenjivosti moraju se opravdati sve kontrole koje će se koristiti. Sustav je potrebno stalno nadograđivati jer se stalno pojavljuju novi oblici prijetnji. [36]

4. Metode procjene rizika

Danas postoji veliki broj pristupa procjeni rizika te različite metode i tehnike za njihovu procjenu. Stoga nije jednostavno odrediti primjerenost pojedine metode jer takav odabir ovisi o većem broju čimbenika. Tako da će u nekim slučajevima biti bolje primijeniti neku određenu metodu. To ne znači da bi procjena provedena nekom drugom metodom bila pogrešna nego da bi bila primjerenija za postojeću situaciju. Neki od čimbenika koji utječu na odabir metode mogu biti: složenost sustava koji se izgrađuje, dostupni resursi, određeni zahtjevi i mogućnost predviđanja rizika.

4.1. Upravljanje sigurnosnim rizicima

Općenito, rizik kao pojam predstavlja kombinaciju vjerojatnosti nekog događaja i utjecaja, odnosno (negativne) posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti. Svako ulaganje u informacijsku sigurnost potrebno je promatrati kao investiciju. Od svake investicije, pa tako i od ulaganja u informacijsku sigurnost, očekuje se pozitivni povrat sredstava. U tom kontekstu upravljanje sigurnosti se može promatrati u smislu smanjenja troškova koji mogu nastati uslijed realizacije napada na sigurnost u informacijskom sustavu. U kontekstu upravljanja rizikom potrebno je identificirati osnovne elemente:

- ✓ osjetljivost (ranjivost) sustava,
- ✓ potencijalne prijetnje,
- ✓ posljedice,
- ✓ protumjere [9, 46]

Potencijalne prijetnje ili nedostaci su prisutniji u svim sustavima. Ranjivost sustava proizlazi iz ranjivosti dijelova sustava, odnosno resursa. Potencijalne prijetnje mogu koristiti neku od ranjivosti sustava ili egzistirati neovisno o sigurnosti samog sustava. Izvori prijetnji mogu biti razni:

- ✓ pogreške ili kvarovi na resursima (programske pogreške, kvarovi na sklopovlju itd.),
- ✓ napadi (izvana i iznutra),
- ✓ havarije (požari, elementarne nepogode itd.),
- ✓ ljudske pogreške i drugi. [9, 46]

Posljedice ostvarivanja neke prijetnje mogu varirati te općenito mogu biti materijalne (štete na uređajima i sl.) i nematerijalne (otkrivanje informacija, trajni ili privremeni gubitak informacija itd.). Postojanje neke prijetnje ne implicira nužno da će ta prijetnja biti i ostvarena, odnosno da će doći do materijalne ili nematerijalne štete. Važan dio upravljanja sigurnošću predstavlja upravljanje rizikom, odnosno uspostava relacija između ranjivosti, potencijalnih prijetnji i posljedica, odnosno utjecaja na informacijski sustav. [9, 46]

4.2. Procjena nematerijalne i materijalne imovine IS-a

Imovinu IS-a čini nematerijalna imovina (znanje, informacije, podaci itd.) te materijalna (oprema i druga fizička sredstva). Prema Guide to BS7799 Risk Assessment and Risk management poslovna imovina se dijeli na:

- ✓ *papirnati dokumenti (ugovore, upute, poslovna dokumentacija, poslovni rezultati itd.);*
- ✓ *nematerijalna (baze podataka, sistemska dokumentacija, korisnički priručnici, operativne procedure, planovi itd.);*
- ✓ *software (aplikacijski i sistemski software, razvojni alati i pomoćni alati);*
- ✓ *ljudi (osoblje, potrošači);*
- ✓ *opremu ili fizičku imovinu (računala i komunikacijska oprema, magnetski mediji, ostala tehnička oprema);*
- ✓ *ugled i reputacija tvrtke;*
- ✓ *servisi (računalni i komunikacijski servisi, ostali servisi za podršku rada).* [25, 35]

Tablica 4.1. - Elementi metrike rizika sigurnosti [57]

Element rizika	Značenje
Prijetnja	financijska vrijednost poslovne (materijalne i nematerijalne) imovine
Ranjivost	intenzitet i učestalost prijetnji sigurnosti
Vjerojatnost	osjetljivost i slabost elemenata IS-a prema utjecajima okoline
Predviđeni gubitak	vjerojatnost da će prijetnja iskoristiti ranjivost imovine
Ostvareni gubitak	mogući gubitak nastao djelovanjem prijetnji
Postojeća zaštita	financijski troškovi održavanja, poslovanja i zamjene sigurnosnih kontrola, učinkovitost postojećih mjera

Ovaj popis predstavlja uobičajene elemente IS-a prema većini autora, ali uz njih treba uvrstiti i znanje kao nematerijalnu imovinu koje predstavlja skup uređenih informacija. Znanje je izvor IS-a koji se sve češće spominje kao najvrjedniji dio i pokretač funkcija i procesa IS-a po kojima se uspješna organizacija razlikuje od loših. [25, 35]

Tablica 4.2. - Struktura vrijednosti informacija [57]

Struktura važnosti podatkovnih sadržaja	
Kvalitativna proizlazi iz: ✓ važnosti za poslovne procese i funkcije, ✓ važnosti za pojedinca i njegov rad, ✓ važnosti poslovne ciljeve, ✓ potrebe arhiviranja i dokumentiranja.	Kvantitativna proizlazi iz: ✓ mogućnosti kapitalizacije informacija na tržištu, ✓ mogućnost financijskog gubitka, ✓ troškovi izrade obnove ili nadograđivanja.

Kvalitativne osobine poslovnih informacija stvaraju problem njihovog vrednovanja koji nije u potpunosti razjašnjen. Problem je potaknut zbog potrebe jedinstvenog i razumljivog načina koji bi istovremeno bio primjeren za proces procjene rizika sigurnosti. Poteškoće procjene poslovnih informacija proizlaze iz toga što informaciju ne možemo razumjeti i odrediti kao fizičku pojavu i veličinu. Ona je nematerijalna i nema fizičkih osobina (iako je gledamo kao fizički zapis na nekom od medija). Iako se količina informacijskog sadržaja može relativno izraziti kod procjene njene poslovne vrijednosti nije cilj utvrditi fizičku količinu prenesenog ili pohranjenog sadržaja. Količina nije u sprezi s kvalitetom i značenjem sadržaja [25, 35]

4.2.1. Određivanje razine integriteta informacijske imovine

Razina integriteta informacijske imovine određuje se prema visini moguće štete zbog neovlaštenih radnji i potencijalnih posljedica. One nisu određene zakonom, nego ih se specificira individualno. Način takvog klasificiranja može biti sljedeći:

- **Nužan** - informacijska imovina koja je ključna za rad i nesmetano poslovanje (transakcije, izvršni kod programa itd.)
- **Važan** - informacijska imovina koja je važna (ali ne ključna) za nesmetano poslovanje (radne statistike, izvorni kod programa itd.).
- **Uobičajen** - sva ostala imovina koja nije neposredno neophodna ili se može osigurati iz nekih drugih izvora. [9, 46]

3.2.2. Određivanje razine raspoloživosti informacijske imovine

Raspoloživost informacijske imovine odnosi se na razinu potreba u normalnim ili izvanrednim uvjetima te na veličinu štete ukoliko to nije tako. Kao i razine integriteta, ni razine raspoloživosti nisu određene zakonom, nego ih svaka organizacija definira prema svojim kriterijima. Primjer klasificiranja razina raspoloživosti može izgledati ovako:

- **Kritična** (bez odgode) - privremeni gubitak ili neraspoloživost informacijske imovine ozbiljno bi ugrozio pružanje usluga korisnicima ili bi rezultirao nepovratnom štetom u poslovanju, financijama ili samom ugledu organizacije.
- **Visoka** (do 6 sati) - privremeni gubitak informacijske imovine iznimno bi loše utjecao na korisnike i na poslovanje te bi mogao rezultirati stvaranjem novih troškova.
- **Standardna** (do 24 sata) - privremeni gubitak informacijske imovine ne bi značajnije utjecao na poslovanje organizacije.
- **Umjerena** (do 72 sata) - gubitak informacija doveo bi korisnike u neugodnu situaciju ili bi rezultirao nekim manjim utjecajem na operacije i financije.
- **Niska** (do tjedan dana) - gubitak takvih informacija korisnici bi jedva primijetili, a neznatno bi utjecao na financije ili operacije.
- **Bez utjecaja** (preko tjedan dana) - privremeni gubitak informacijske imovine imao bi zanemariv utjecaj na poslovanje organizacije te ga korisnici ne bi primijetili. [9, 46]

4.3. Važnost upravljanja rizikom

Jedna od glavnih poslovnih potreba predstavlja upravljanje informacijskom sigurnošću. Kako bi pravilno upravljali informacijskim sustavom moramo poznavati razne zakonske propise koji direktno ili indirektno utječu na sam sustav. Upravljanje rizikom je proces kroz koji se potvrđuje poslovna opravdanost odabira sigurnosnih rješenja i kontrola koje će osigurati dovoljnu razinu sigurnosti. Proces upravljanja rizikom omogućuje razvoj strategije i postavljanje ciljeva u području informacijske sigurnosti. Upravljanje rizikom uključuje tri procesa:

- ✓ procjenu rizika (identifikacije resursa),
- ✓ umanjivanje rizika (analize rizika) i
- ✓ evaluaciju rizika (interpretacije rezultata i poduzimanja odgovarajućih protumjera). [9, 46]

Kako bi se stvorila ravnoteža između operativnih i ekonomski troškova potrebno je zaštiti informacijski sustav i podatke. Zbog toga dobro strukturirana metodologija upravljanja rizikom je jedan od ključnih čimbenika pri odabiru prikladnih sigurnosnih kontrola koje osiguravaju kontinuirano odvijanje poslovnih procesa.

4.3.1. Analiza rizika

Danas postoji veliki broj metoda procjene rizika. Prema ISSA[3] istraživanju ima čak više od 70 vrsta metoda iako sve nisu prikladne za procjenu rizika sigurnosti IS-a, a neke od njih ni ne podržavaju cijeli proces procjene. Kad su u pitanju rješenja za procjenu rizika sigurnosti IS-a postoje određene nejasnoće. Istraživanjem dostupnih internetskih i knjižničnih izvora te iskustva velikih poslovnih organizacija u vezi s unapređenjem sigurnosti IS-a utvrđeno je da se za procjenu rizika sigurnosti IS-a koriste raznovrsni pristupi, metode, tehnike i alati. Pristupi se isprepleću, metode se različito tumače, mnogo je pomoćnih metoda i tehnika koje se koriste pri procjeni rizika, a još je više nezavisnih programskih paketa. Može se činiti da se različita rješenja koriste bez pravila te da je izbor potpore procjeni rizika sigurnosti IS-a slučajan i/ili da zavisi o sklonosti poslovne organizacije koja je provodi. Analiza rizika je postupak kojem je cilj ustanoviti ranjivosti sustava, uočiti potencijalne prijetnje, te na odgovarajući način kvantificirati moguće posljedice, da bi se mogao odabrati najefikasniji način zaštite, odnosno procijeniti opravdanost uvođenja dodatnih protumjera. Metodologija procjene rizika je prevladavajući oblik prema kojem se procjenjuju čimbenici rizika. Metodologije mogu biti formalne i neformalne, detaljne ili jednostavne, ali od osamdesetih godina prošlog stoljeća razlikujemo dvije osnovne metodologije procjene rizika:

- ✓ kvantitativna metoda (utemeljena na opisima ili rangiranju) i
- ✓ kvalitativna metoda i (utemeljena na numeričkom izračunavanju). [9, 46]

Danas pored ovih metoda prisutna je i kombinirana metoda u koju spadaju kombinacije prve dvije metode. Pripadnost neke metode pojedinoj metodologiji određuje se na osnovi pretežnog oblika procjene elemenata metrike rizika sigurnosti. Budući da se danas isprepleću različiti pristupi u procjeni, teško je govoriti o potpuno kvalitativnoj ili kvantitativnoj metodologiji.

[3] ***ISSA*** *- **I**nternational **S**ystem **S**ecurity **A**ssociation – neprofitna, profesionalna međunarodna organizacija profesionalaca i stručnjaka za informacisjku sigurnost.*

4.3.2. Kvantitativna metoda

Kvantitativna metoda podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjoj razini. Većina organizacija preferira ovakav načina analize pošto im je na taj način omogućeno planiranje novčanih sredstava, a upravi se omogućava da bez tehničkih pojedinosti može donijeti odgovarajuće odluke. Pri tom valja imati na umu da vrijednost nekih resursa nije uvijek moguće iskazati novčano, a također se kao rezultat mogu pojaviti i brojke koje ne predstavljaju realno stanje. Ova metrika je prvi put predstavljana u FIPS-65[4] pod nazivom ALE[5]. U početku je davala dobre rezultate, ali s vremenom početne prednosti su postale nedovoljne, a metodologija neprikladna za čitav niz problema procjene.

Tablica 4.3. - Oblici kvantitativne metrike rizika sigurnosti [30]

Oblici metrike	Osobine
Financijska vrijednost	✓ omogućava izražavanje odnosa trošak/korist u jasnim varijablama; ✓ može se prenijeti na svu imovinu i mjere zaštite; ✓ podržava matematičke i statističke kalkulacije; ✓ može otežati procjenu;
Postoci (0.0 – 100) vjerojatnosti (Probability)	✓ metriku vjerojatnosti da će se nešto dogoditi u nekom intervalu ili konačnom broju; ✓ mogu se koristiti ljestvice; ✓ podržava matematičke i statističke kalkulacije; ✓ pojmovi su razumljivi; ✓ jasno izražavaju neizvjesnost; ✓ ako se koristi ručno zahtjeva puno znanja i sposobnosti; ✓ ručno korištenje te metrike traži puno vremena i troškova te je zbog toga subjektivna;
Lančana distribucija (Bounded Distribution)	✓ statistički mehanizmi koji određuju vrijednost elemenata rizika utvrđuje uspostavu gornjih i donjih veza; ✓ može se primijeniti na najveći broj elemenata rizika; ✓ podržava matematičke i statističke izračune; ✓ pojmovi su razumljivi; ✓ zahtjeva automatizirani alat za izračune algoritma;

[4] ***FIPS - 65*** *- **F**ederal **I**nformation **P**rocessing **S**tandards predstavljaju javno objavljene standarde od strane federalne vlade Sjedinjenih Država za upotrebu u računalnim sustavima. Mnogi FIPS standardi predstavljaju izmijenjene inačice standarda koji se koriste u široj zajednici (ANSI, IEEE, ISO, itd.).*

[5] ***ALE*** *- **A**nnualized **L**oss **E**xpectancy predstavlja godišnju proizvodnu stopu i jednogodišnji očekivani gubitak.*

Kvantitativna metrika se najviše koristi kod procjene materijalne imovine, vjerojatnosti pojave, ali je učinkovita i u identificiranju moguće opasnosti i pogrešaka u IS-u. Glavni nedostaci ove metode su :

- ✓ zahtjevi za velikom količinom preciznih povijesnih podataka,
- ✓ poboljšanje algoritma brojčanog označavanja i razlike između intenziteta,
- ✓ razvoj automatiziranih alata za podršku procjene,
- ✓ teškoće u utvrđivanju nematerijalne imovine. [9, 46]

4.3.2. Kvalitativna metoda

Kvalitativna metoda za procjenu rizika predstavlja subjektivniji pristup pri kojem se resursi, rizici i protumjere promatraju relativno obzirom na sam sustav. Za provođenje kvalitativne metode nije nužno detaljno poznavanje poslovnih procesa i njihove vrijednosti, već je dovoljan općeniti uvid u sam sustav. Rezultat kvalitativne metode iskazuje samo relativni odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i implementacije protumjera. Pri tome valja imati na umu da je ta procjena subjektivne naravi te da je kao takva podložna pogreškama. Ova metrika nastaje nakon što su uočeni nedostaci izvornog kvantitativnog pristupa. Kvalitativna metrika najčešće primjenu nalazi u rješavanju skupine zadataka za koje je bio neprimjeren kvantitativni pristup.

Tablica 4.4. - Oblici kvalitativne metrike rizika sigurnosti [30]

Oblik metrike	Osobine
Nisko, srednje, visoko; (1, 2, 3)	✓ metrika je jasna, mora biti odgovoren skup pravila za kategorizaciju tj. prepoznavanje intenziteta razina; ✓ može se primijeniti na sve elemente metrike rizika; ✓ ne traži puno vremena; ✓ pojmovi su razumljivi; ✓ kalkulacije su jednostavne; ✓ grupa podjela intenziteta čini je nefleksibilnom, nisu podržane analize troškova/korist.
Jedan, dva, tri, četiri, pet (1, 2, 3, 4, 5); Ključna, kritična, važna, povjerljiva i informativna i sl.	✓ podržava pet razina važnosti; ✓ uspješnost te metrike ovisi o subjektivnoj definiciji kriterija koji određuju pojedinu razinu; ✓ pruža veću fleksibilnost, ne traži puno vremena, kalkulacije su relativno jednostavne; ✓ korisna ako je financijska vrijednost imovine nebitna ili nepoznata; ✓ može se primijeniti samo za procjenu vrijednosti, rezultat je subjektivan; ✓ ne podržava analizu troškova/korist.

Ova metrika je jednostavna za shvaćanje i dostupnija je manjim poslovnim

organizacijama upravo iz razloga što se brže provodi. Glavni nedostatak je taj što zanemaruje financijsku važnost koju je teško izraditi određenim brojem razina sličnosti, izražavanje subjektivnosti i onemogućuje planiranje i analize troškova. Ova metoda se najviše koristi u procjeni nematerijalne komponente IS-a, ali većina poznatih metoda procjene rizika koristi ovu metriku pokušavajući je što više prilagoditi potrebama analize troškova. [9, 46]

4.3.3. Usporedba metoda te njihove prednosti/nedostaci

Većina postojećih metoda procjene pokušava iskoristiti najbolje osobine iz obje metodologije. Zbog težišta procjene na nematerijalnu imovinu IS-a u posljednje je vrijeme izraženije zanimanje za kvalitativne metodologije, ali ni kvantitativnu metodologiju se ne smije zanemariti jer je bitna prilikom procjene nekih skupina čimbenika rizika. [9, 46]

Tablica 4.5. - Usporedba kvalitativne i kvantitativne analize rizika [9, 46]

Svojstvo	**Kvalitativna metoda**	**Kvantitativna metoda**
Financijski prikaz	Ne	Da
Omjer uloženog i dobivenog	Ne	Da
Složenost	Ne	Da
Subjektivnost	Da	Ne
Mogućnost automatizacije	Ne	Da
Potrebno vrijeme	Kratko	Dugo
Potrebna količina informacija	Mala	Velika

Analizom rizika moraju se utvrditi sljedeće činjenice:

- ✓ kritični resursi i njihova vrijednost (relativna ili novčana),
- ✓ popis mogućih prijetnji i vjerojatnost njihove pojave,
- ✓ potencijalni gubici koje uzrokuje ostvarenje prijetnje,
- ✓ preporučene protumjere i zaštita. [9, 46]

Na temelju dobivenih rezultata potrebno je odlučiti kakve protumjere treba poduzeti. Postoje tri mogućnosti djelovanja, koje nisu nužno međusobno isključive:

- ✓ smanjenje rizika,
- ✓ prijenos rizika i
- ✓ prihvaćanje rizika. [9, 46]

Jedini važni parametar pri odabiru načina djelovanja jest isplativost za organizaciju.

Tablica 4.6. - Usporedba primjene kvalitativne i kvantitativne metrike rizika [45]

	Kvantitativna				Kvalitativna		
Procjena rizika	Financijska vrijednost	Postoci	Očekivani godišnji gubitak(Annual Loss Expectancy)	Lančana distribucija (Bounded Distribution)	Nizak, srednji, visok	Rangiranje rednim brojevima	Ključni, kritični, važni
Vrijednost imovine	X			X	X	X	X
Učestalost prijetnji			X	X	X	X	
Izloženost prijetnjama		X		X	X	X	
Učinkovitost mjera zaštite		X		X	X	X	
Trošak zaštite	X			X	X	X	
Neizvjesnost		X		X	X	X	

Vidljivo je da i sama kvalitativna metodologija posjeduje kvantitativnu komponentu. Razlog tome je zato što opisno izraženi intenziteti kvalitativne metodologije moraju pretvoriti u numeričke tj. kvantitativne pokazatelje koji se mogu koristiti kod mjerenja rizika. Primjer tome je kad kažemo "rizik je velik", u tom slučaju teško je reći koliko točno financijskih sredstava treba potrošiti. Kvalitativni se intenziteti pretvaraju u kvantitativne primjenom različitih oblika ljestvica intenziteta koje su specifične za svoje metode. [9, 46]

Tablica 4.7. - Osnovne značajke metodologija procjene rizika sigurnosti [57]

Kvalitativna	Kvantitativna
traži softversku podršku, dugotrajna, složene kalkulacije, često nerazumna, nije standardizirana	subjektivna, razumljiva, jednostavna, relativno kratkotrajna
rezultati su razumljivi menadžeru, razmatra stvarne vrijednosti i trošak, bolja je osnova upravljanja sigurnošću i analizu troškova	nije moguće pratiti performanse sustava, nije temelj za analizu troškova, bolje procjenjivanje nematerijalne imovine

4.4. Integracija upravljanja rizikom u životni ciklus razvoja sustava

Razlog zašto organizacije usvajaju proces upravljanja rizikom pri razvoju IT sustava je taj što im takav proces pruža osnovu za donošenje odluka i pridonosi smanjenju negativnog učinka na organizaciju. Da bi se postigla potpuna efikasnost upravljanja rizikom, proces je potrebno integrirati u životni ciklus razvoja sustava (*engl. System Development Life Cycle - SDLC*). Životni ciklus razvoja IT sustava ima 5 faza:

- ✓ inicijalna faza,
- ✓ faza razvoja ili akvizicije,
- ✓ implementacijska faza,
- ✓ faza operativnosti i održavanja i
- ✓ faza odlaganja. [64]

Upravljanje rizikom je iterativni proces koji se može odvijati tijekom svake faze životnog ciklusa razvoja sustava. Sljedeća tablica (*Tablica 4.8.*) prikazuje i opisuje pojedine faze životnog ciklusa razvoja sustava te načine upravljanja rizikom u svakoj fazi. [64]

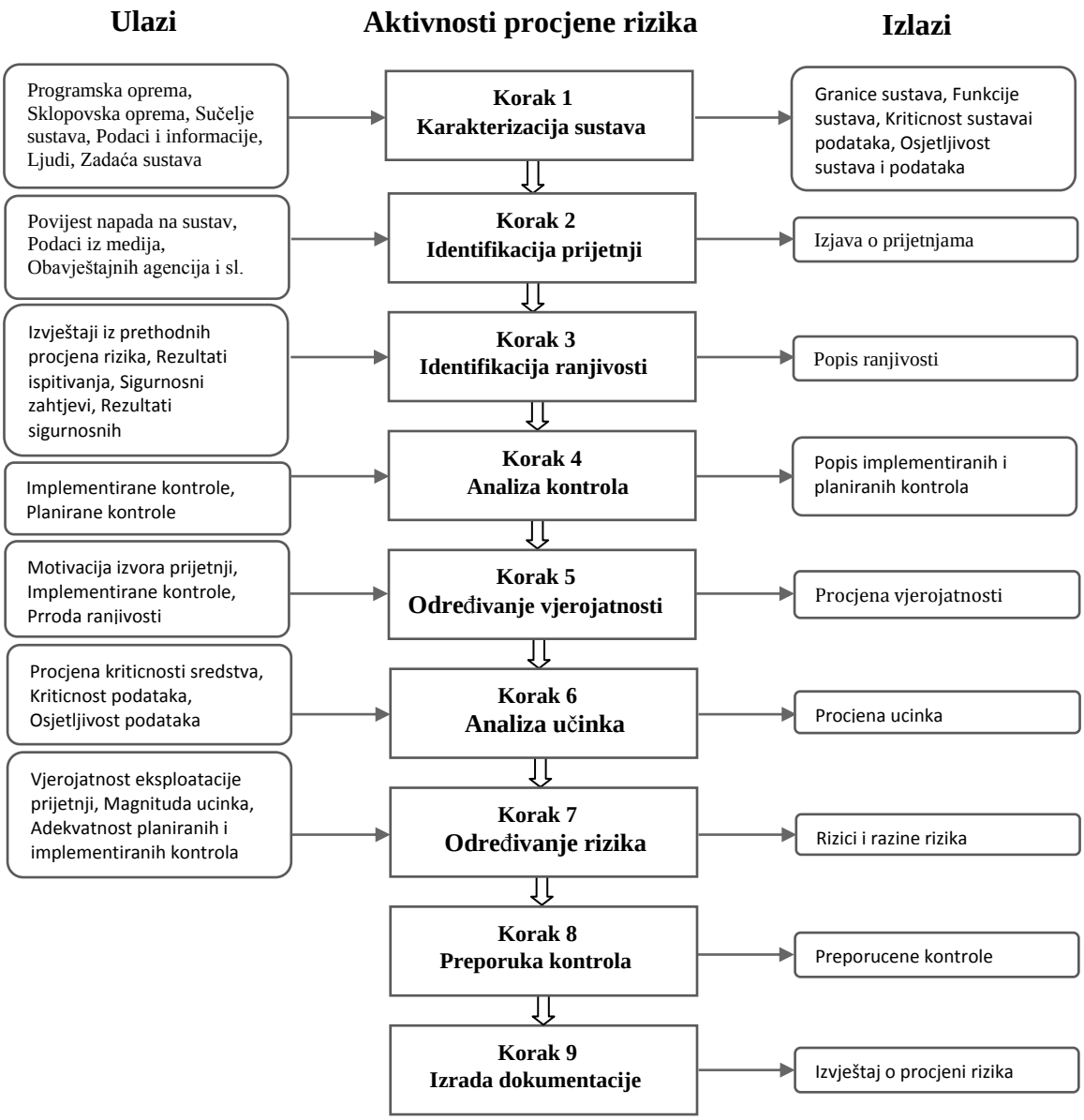
Tablica 4.8. - Integracija upravljanja rizikom u životni ciklus razvoja sustava [64]

SDLC faza	Obilježja	Upravljanje rizikom
Inicijalna faza	Izražava se potreba za IT sustavom, te se dokumentira namjena i opseg sustava.	Identificirani rizici omogućuju izgradnju sigurnosnih zahtjeva i razvoj sigurnosne strategije.
Faza razvoja ili akvizicije	IT sustav se dizajnira, naručuje, programira, razvija ili na neki drugi način izgrađuje.	Rizici identificirani u ovoj fazi omogućuju sigurnosnu analizu IT sustava te balansiranje tijekom razvoja sustava.
Implementacijska faza	Sigurnosni elementi se konfiguriraju, testiraju i verificiraju.	Uspoređuje se implementacija u operativnom okruženju sa sigurnosnim zahtjevima. Odluke o upravljanju rizikom se donose prije operativnosti sustava.
Faza operativnosti i održavanja	Sustav obavlja svoju funkciju. Sustav se modificira u skladu s promjenama organizacijske politike, procedura i procesa ili promjenama u sklopovskoj ili programskoj opremi.	Upravljanje rizikom se odvija u skladu s periodičkom akreditacijom ili autorizacijom sustava ili kad se dogode značajne promjene u IT sustavu ili operativnom okruženju.
Faza odlaganja	U ovoj fazi dolazi do odlaganja informacija, programske ili sklopovske opreme.	Upravljanje rizikom osigurava da se ispravno postupa s podacima ili opremom koja se odlaže.

4.4.1. Procjena rizika prema NIST-ovim preporukama

Procjena rizika je prvi proces u metodologiji upravljanja rizikom. Organizacije na osnovu procjene rizika mogu odrediti opseg potencijalnih prijetnji i rizika koji se pojavljuje u životnom ciklusu razvoja sustava. Rizik je funkcija vjerojatnosti nekog

događaja i utjecaja, odnosno (negativne) posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti. Da bi se odredila vjerojatnost pojave štetnog događaja, potrebno je analizirati prijetnje i potencijalne ranjivosti. Metodologija procjene rizika prema NIST-u rizika obuhvaća devet koraka koji su prikazani na sljedećoj slici (*Slika 4.1.*). [64]



Slika 4.1. - Postupak procjene rizika prema NIST-ovim preporukama [8]

Ostale metodologije imaju ponešto drugačije faze, ali se manje-više svode na isto. Prvi korak je definirati sustav nad kojim će se promatrati rizici. Mnoge metodologije govore o registru informacijske imovine (eng. asset register) koji nije samo registar osobnih računala, poslužitelja i aplikacijskog softvera. Informacijska imovina je sve ono što predstavlja vrijednost za organizaciju, a sadrži ili jest informacija odnosno se koristi u procesima podrške

uslugama koje počivaju na tim informacijama. U registru informacijske imovine će se tako naći poslovni procesi, računalne i komunikacijske usluge, aplikacijski i sistemski softver, računalna i komunikacijska oprema, mediji, izvori napajanja, klima uređaji, vanjski partneri, djelatnici organizacije i sl. NIST-ova metodologija navodi pojam „karakterizacija sustava“ (eng. system characterization) što se čini boljim pojmom za one organizacije koje se po prvi put susreću s procesom upravljanja rizikom. Naime, registar imovine često zna navesti na pogrešan korak sastavljanja neke vrste kataloga sve moguće informacijske i komunikacijske tehnologije, što zna biti dugotrajan posao, a neopipljiva imovina, poput procesa ili usluga se pri tom zaboravlja. Jedan takav registar više je plod upravljanja imovinom (eng. asset management) kao zasebnom disciplinom, iako nije loše objediniti te dvije discipline oko te zajedničke točke. Kada je poznat opseg sustava te informacijska imovina koja se nalazi u tom sustavu, potrebno je identificirati prijetnje koje mogu djelovati na tu imovinu te ranjivosti imovine koju takve prijetnje mogu iskoristiti. Sljedeća slika daje popis dijela prijetnji i ranjivosti na informacijsku imovinu.

Tablica 4.9. - Primjeri prijetnji i ranjivosti [64]

Tip imovine	Ranjivost	Prijetnja
Sklopovska oprema	Neredovito održavanje	Tehnički kvar na sustavu
	Nezaključani ormarići	Krađa medija i dokumenata
	Nekontrolirano odbacivanje medija	Krađa medija i dokumenata
Programska oprema	Nedovoljno testiranje softvera	Greška u aplikaciji
	Poznate ranjivosti u softveru	Iskorištavanje poznatih ranjivosti
	Nedostatak operativnih i sistemskih zapisa	Neovlaštene promjene u sustavu
Mreža	Slabo upravljanje zaporkama	Napadi probijanjem zaporki
	Nekriptirani promet	Prisluškivanje prometa
	Neredundantna oprema	Kvar na mrežnom uređaju
Ljudi	Nedovoljna obučenost djelatnika	Greške pri korištenju
	Manjak obučenog kadra	Otkaz djelatnika
Lokacija	Blizina rijeke	Poplava
	Nedostatak agregata i/ili UPS-ova	Nestanak struje

Procjena rizika započinje s identifikacijom resursa koji su u sklopu opsega ISMS-a[6]. Svaki resurs ima svog vlasnika. Resursi su podijeljeni po kategorijama:

[6] ***ISMS*** *- **I**nformation **S**ecurity **M**anagement **S**ystem je skup pravila koje se bave upravljanjem sigurnošću informacija. Nastao je prvenstveno iz ISO 27001norme.*

- ✓ *sklopovska oprema* - uključuje poslužitelje, vatrozide, osobna računala, prijenosna računala, mrežnu opremu, perifernu računalnu opremu i sl.;
- ✓ *programska oprema* - uključuje aplikacije, operacijske sustave, sustavske pomoćne programe, sigurnosne zakrpe i sl.;
- ✓ *podaci i dokumenti* - uključuje informacije u bilo kojem obliku, npr. pisanom, elektroničkom, u obliku video zapisa i sl.;
- ✓ *ljudski resursi* - uključuje sve zaposlenike koji na bilo koji način sudjeluju u procesu;
- ✓ *komunikacije* - uključuje sve vrste komunikacija, npr. telefonska komunikacija, komunikacija elektroničkom poštom, Internet;
- ✓ *općenito* - u ovu kategoriju spadaju resursi koji se nisu mogli svrstati u neku od prethodnih kategorija, npr. vanjski partneri. [64]

Nakon što su resursi identificirani, potrebno je izvršiti vrednovanje resursa u odnosu na tri sigurnosna zahtjeva:

- ✓ povjerljivost (*engl. confidentiality*, C),
- ✓ integritet (*engl. integrity*, *I*),
- ✓ raspoloživost (*engl. availability*, *A*). [64]

Skala za vrednovanje resursa sadrži četiri vrijednosti:

- ✓ niska (*N*),
- ✓ srednja (*S*),
- ✓ visoka (*V*) i
- ✓ vrlo visoka (*VV*). [64]

Tablica 4.10. - Način izračuna rizika po metodi NIST [64]

Vjerojatnost prijetnje	**Utjecaj**		
	Nizak (10)	Srednji (50)	Visok (100)
Visok (1.0)	Nizak 10 × 1.0 = 10	Srednji 50 × 1.0 = 50	Visok 100 × 1.0 = 100
Srednji (0.5)	Nizak 10 × 0.5 = 5	Srednji 50 × 0.5 = 25	Srednje 100 × 0.5 = 50
Nizak (0.1)	Nizak 10 × 0.1 = 1	Nizak 50 × 0.1 = 5	Nizak 100 × 0.1 = 10

Ljestvica rizika: visok (>50 - 100); srednji (>10 - 50); nizak (1 - 10);

Tablica 4.11. - Vjerojatnost ostvarenja prijetnje prema utjecajima [38]

	Utjecaj			
Vjerojatnost ostvarenja prijetnje	Vrlo veliki (100)	Usmjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)
Usmjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)
Srednja do mala (0,1)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)

Ukupna vrijednost resursa se računa tako da se uzme maksimalna vrijednost resursa u odnosu na tri sigurnosna zahtjeva. U tablici 3.12. nalazi se primjer vrednovanja resursa.

Tablica 4.12. - Primjer identifikacije i vrednovanja resursa [64]

Kategorija	**Naziv resursa**	**Vlasnik**	**C**	**I**	**A**	**Max(C, I, A)**
Software	Sigurnosne zakrpe	Tvrtka X	N	S	S	V
Podaci / Dokumenti	Web forma	Tvrtka X	N	V	V	V
Podaci / Dokumenti	E-mail sa zahtjevom klijenta	Voditelj	S	V	S	V

Nakon identifikacije resursa slijedi identifikacija prijetnji i ranjivosti za svaki pojedini resurs. Pri razmatranju prijetnji potrebno je imati na umu sve tipove prijetnji:

- ✓ maliciozne,
- ✓ nenamjerne ili
- ✓ fizičke.

Nedostatak procedura i politika koje definiraju prihvatljivo postupanje s resursima predstavljaju izvore ranjivosti. Svaki resurs koji ima neku ranjivost posjeduje i barem jednu prijetnju koja može iskoristiti tu ranjivost. U sljedećoj tablici nalazi se primjer ranjivosti na kategoriju resursa koja obuhvaća programsku opremu. Također, u tablici je dana po jedna prijetnja koja može iskoristiti tu ranjivost.

Tablica 4.13. - Primjer ranjivosti i pripadnih prijetnji [64]

Ranjivost	Prijetnja
Nema specifikacije za razvoj aplikacije	Ostavljanje pozadinskih vrata
Aplikacija nije testirana	Degradacija aplikacije
Nema dokumentacije	Otežano korištenje aplikacije
Neprikladna zaštita izvornog koda	Krađa izvornog koda
Neprimjena kontrola pristupa	Maskiranje
Nedostatak zaštite od malicioznog softvera	Ostavljanje pozadinskih vrata

Nakon identificiranja prijetnji i ranjivosti, procjenjuje se vjerojatnost ostvarenja prijetnje (*engl. Threat probability, P(T)*) i posljedice ostvarenja prijetnje (*engl. Threat impact , I(T)*). Skala za vrednovanje vjerojatnosti ostvarenja prijetnje i posljedica ostvarenja prijetnje je ista kao kod određivanja vrijednosti resursa: niska (*N - vrijednost 1*), srednja (*S- vrijednost 2*), visoka (*V- vrijednost 3*) i vrlo visoka (*VV- vrijednost 4*). Konačno, izvodi se procjena rizika. Prema utvrđenoj metodologiji za procjenu rizika , rizik se računa kao umnožak vrijednosti resursa (*engl. Asset value, AV*), vjerojatnosti prijetnje i posljedicama ostvarenja prijetnje. Tj.

$$R = AV \times P(T) \times I(T).$$

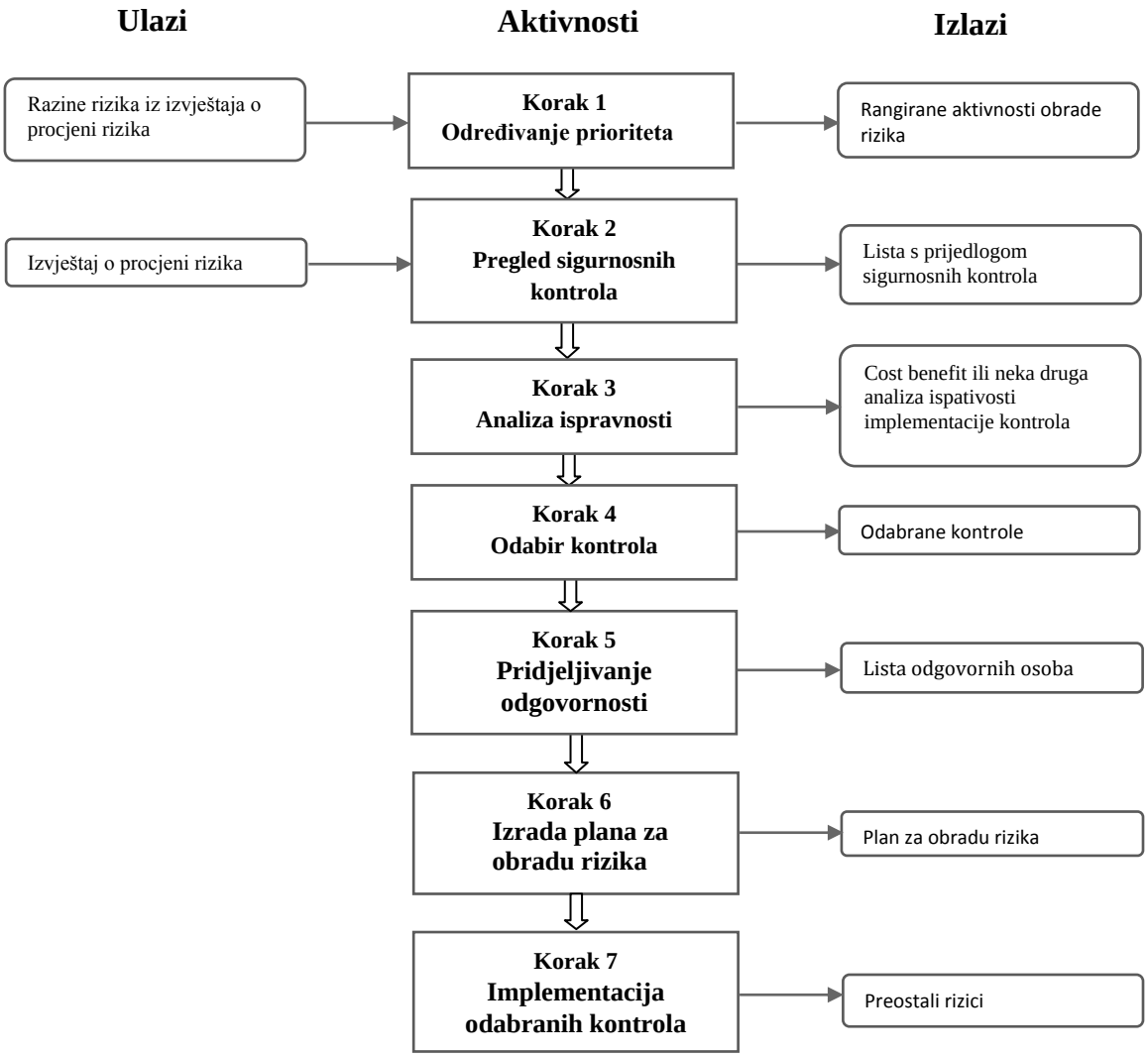
U sljedećoj tablici (*Tablica 4.14.*) nalazi se primjer za procjenu rizika.

Tablica 4.14. - Primjer procjene rizika [64]

Završni izvještaj, AV = VH				
Ranjivost	**Prijetnja - T**	**P(T)**	**I(T)**	**R=AV×P(T)×I(T)**
Podaci nisu validirani	Netočni podaci	V	VV	48
Neprimjerena klasifikacija	Neautorizirano postupanje s resursom	V	VV	48
Nema sigurnosne kopije	Gubitak podataka	S	S	16
Nema "clean desk" politike	Otkrivanje povjerljivih podataka o klijentu	V	VV	48

Prema metodologiji za procjenu rizika kontrole se primjenjuju za one rizike koji su procijenjeni kao visoki i vrlo visok, tj. za sve rizike čija vrijednost je iznad 16. U navedenoj tablici svi rizici zahtijevaju primjenu kontrola za njihovo smanjenje. Nakon što se rangira katalog rizika, za one rizike koji se žele smanjiti, potrebno je predložiti mjere odnosno kontrole kojima će se to i napraviti. Naravno, neke mjere mogu biti tehnološki vrlo

kompleksne i skupe te je stoga potrebno izraditi neku vrstu analize isplativosti. Naime, čemu potrošiti nekoliko milijuna kuna u visoko kvalitetnu sklopovsku opremu ili programsku opremu za pohranu podataka, ako rizici koji djeluju nad pričuvnom pohranom nisu visoko rangirani. Analiza isplativosti se može raditi brojnim metodama, a danas je jedna od najkorištenijih, metoda „očekivanog godišnjeg gubitka“ (eng. ALE – annual loss expectancy). Ovom metodom se procjenjuje koliki je očekivani gubitak jednog ostvarivanja prijetnje (npr. pola sata zastoja u radu aplikacije A zbog „prljavih“ odnosno nevjerodostojnih podataka košta B kuna). To se množi s procijenjenim brojem takvih događaja godišnje te se dobije očekivani godišnji gubitak C. Ukoliko je za implementaciju kontrole koja smanjuje pojavu ovakvog događaja potrebno utrošiti D kuna, lako je izračunati da li se implementacija takve kontrole isplati ili ne.



Slika 4.2. - Koraci obrade rizika prema NIST-u [64]

Analizom isplativosti organizacija dolazi do konačnog broja sigurnosnih kontrola koje je potrebno implementirati te se na osnovu toga stvara plan obrade rizika, koji jasno komunicira potrebne aktivnosti, odgovornosti u njihovom provođenju, datume početka i kraja implementacije, prioritete aktivnosti i sl. Implementacijom sigurnosnih kontrola odabrani rizici se smanjuju, ali najčešće nikad u potpunosti. Ono što je cilj jest doći do preostalih rizika nakon implementacije koji su dovoljno niski da ih organizacija može prihvatiti. [64]

4.4.2. Procjena rizika uz pomoć matrica

Analiza rizika je proces koji se sastoji od nekoliko faza. Prema standardu ISO/IEC 27005 te faze su:

- ✓ identifikacija i vrednovanje (procjena nepovoljnog učinka na poslovanje) resursa,
- ✓ procjena prijetnji,
- ✓ procjena ranjivosti,
- ✓ procjena postojećih i planiranih mjera zaštite,
- ✓ procjena rizika [38]

Resursi koji imaju neku vrijednost i određeni stupanj ranjivosti su podložni riziku kad god postoji prijetnja koja može iskoristiti tu ranjivost. Procjena rizika je kombinacija potencijalnog nepovoljnog učinka na poslovanje ili neželjenog incidenta i procijenjenih prijetnji i ranjivosti. U praksi, rizik je mjera izloženosti prijetnjama sustava ili organizacije. U sljedećim podnaslovima će biti prikazane četiri glavne metode procjene rizika. Postoji nekoliko varijabli za procjenu rizika uz pomoć ove metode, a one su:

- ✓ procjena vrijednosti resursa (eng. *asset value* - AV), odnosno vjerojatnosti njezina ostvarenja koja može naštetiti resursu,
- ✓ ranjivosti resursa (eng. *vulnerability* - V), odnosno mogućnosti njezina iskorištavanja koja može uzrokovati neželjene posljedice, i postojećih ili planiranih mjera zaštite koje mogu umanjiti opasnost ranjivosti, prijetnji i posljedica,
- ✓ prijetnji koje mogu iskoristiti te ranjivosti (eng. *threat* - T), odnosno vjerojatnosti njezina ostvarenja koja može naštetiti resursu,
- ✓ vjerojatnosti ostvarenja prijetnji (eng. *probability* - P) i posljedice (eng. *impact* - I). koje se mogu dogoditi ukoliko se određena prijetnja ostvari [10, 38]

Dakle, matematički rizik predstavlja funkciju navedenih varijabli.

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

Postoji više kombinacija za ove definirane vrijednosti, kao što su:

- Pristup 1. Procjene rizika na osnovi vrijednosti imovine i razina prijetnji i ranjivosti,
- Pristup 2. Procjene rizika na osnovi rangiranja,
- Pristup 3. Procjene rizika na osnovi vjerojatnosti i utjecaja prijetnji,
- Pristup 4. Procjene rizika na osnovi vjerojatnosti i utjecaja realizacije prijetnji, te vrijednosti i ranjivosti imovine,
- Pristup 5. Procjena rizika na osnovi utjecaja prijetnji i vjerojatnosti nastanka. [10, 38]

Također, da bi se rezultati procjene rizika mogli smatrati valjanim, sam proces mora zadovoljiti sljedeće kriterije:

- ✓ jednoznačnost,
- ✓ objektivnost,
- ✓ pouzdanost,
- ✓ ponovljivost [10, 38]

Cilj analize rizika je identificirati i procijeniti rizik kojem su izloženi informacijski sustavi i njihovi resursi kako bi se odabrale prikladne i opravdane mjere zaštite. Pri procjeni rizika potrebno je razmotriti posljedice ostvarenja prijetnje i vjerojatnost ostvarenja prijetnje. Posljedice se mogu procijeniti na nekoliko načina, uključujući uporabu kvantitativne, odnosno novčane mjere ili kvalitativne mjere. Može se koristiti i kombinacija tih dviju mjera. Kod procjene vjerojatnosti ostvarenja prijetnje, potrebno je utemeljiti vremenski okvir u kojem će resurs imati vrijednost i trebati zaštitu. Vjerojatnost ostvarenja prijetnje ovisi o:

- ✓ privlačnosti resursa, ukoliko se radi o namjernim ljudskim prijetnjama,
- ✓ lakoći iskorištavanja resursa u vlastite svrhe, ukoliko se radi o namjernim ljudskim prijetnjama,
- ✓ tehničkim sposobnostima izvršitelja prijetnje, ukoliko se radi o namjernim ljudskim prijetnjama,
- ✓ mogućnosti ostvarenja prijetnje,

- ✓ podložnosti ranjivosti eksploataciji [10, 38]

Mnoge metode za analizu rizika koriste tablice i kombiniraju empirijske pokazatelje i subjektivnu procjenu. Ne postoji točna niti pogrešna metoda. Kod odabira metode važno je odabrati metodu koja će dati ponovljive rezultate, te pronaći odgovarajuću kombinaciju subjektivne procjene i empirijskih pokazatelja. Sljedeće četiri metode su opisane u dodatku standarda ISO/IEC 27005.

Tablica 4.15. - Određivanje razine vjerojatnosti pojavljivanja prijetnje u e-poslovanju [10, 38]

Razina	Definicija
Visoka (3)	Postoji visoka vjerojatnost da će se konkretna prijetnja ostvariti. To se već ranije događalo i o tome imate statistike ili druge spoznaje, ili je izvor prijetnje jako motiviran izvesti takvu radnju kojom će pokušati iskoristiti Vaše postojeće ranjivosti.
Srednja (2)	Postoji mogućnost da će se pojaviti konkretna prijetnja pojaviti. Ranije ste već imali takvih incidenata, ali oni ipak nisu bili tako česti. No, prepoznajete razlog(e) da izvor prijetnje pokuša iskoristiti Vaše postojeće ranjivosti.
Niska (1)	Nije vjerojatno da će se prijetnja pojaviti, nema incidenata, statistika ili motiva koji bi ukazivali na vjerojatnost da će se to dogoditi.

Tablica 4.16. - Određivanje razine ranjivosti informacijske imovine [10, 38]

Razina	Definicija
Visoka (3)	Jednostavno je iskoristiti Vašu ranjivost jer ne postoje sigurnosne kontrole ili one nisu implementirane ili su implementirane u manjoj mjeri.
Srednja (2)	Vaša ranjivost može se iskoristiti, imate implementirane neke sigurnosne kontrole, no one još nisu dovoljne.
Niska (1)	Vaše sigurnosne kontrole su razvijene i primjenjuju se, tako da je razina ranjivosti niska.

Tablica 4.17. - Određivanje razine ranjivosti informacijske imovine [10, 38]

Razina	Definicija
4	Vrlo vrijedan informacijski resurs za odvijanje Vašeg poslovnog procesa, sa stanovišta povjerljivosti, integriteta i raspoloživosti. Jako ga je teško nadomjestiti u slučaju gubitka, to mora biti ostvareno u vrlo kratkom roku i/ili financijski je jako zahtjevno.
3	Vrijedan informacijski resurs za odvijanje poslovnog procesa, sa stanovišta povjerljivosti, integriteta i raspoloživosti. Teško je zamjenljiv u slučaju gubitka i/ili je to financijski zahtjevno.
2	Takav resurs je potreban da bi se poslovni proces odvijao, može se, ako treba, nadomjestiti u prihvatljivom vremenu i sa stanovišta financija to je prihvatljivo.
1	Resurs se koristi u manjoj mjeri za odvijanje Vašeg poslovnog procesa, može se zamijeniti vrlo jednostavno, nije nužno da to bude u kratkom roku i nije financijski zahtjevno.
0	Resurs je zanemariv i poslovni proces će se moći odvijati i bez njega.

Vrijednost imovine može poprimiti sljedeće razine: 0, 1, 2, 3 i 4.

4.4.2.1. Metoda I - Matrica predefiniranih vrijednosti

Ova metoda za procjenu rizika koristi tri parametra: vrijednost resursa, prijetnje i ranjivosti. Svaki od tih parametara promatra se u odnosu na moguće posljedice, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti . Svi parametri se kvantificiraju proizvoljno.

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

Kod metoda ovog tipa vrijednost fizičkog resursa se procjenjuje u odnosu na trošak zamjene ili rekonstrukcije resursa (kvantitativna mjera). Taj trošak se zatim konvertira u kvalitativnu skalu koja se upotrebljava za podatkovne resurse. Vrijednost programske opreme se procjenjuje isto kao vrijednost fizičkih resursa. Dodatno, ako neki aplikacijski program ima unutarnje zahtjeve povjerljivosti, integriteta ili raspoloživosti, njegova vrijednost se procjenjuje kao i vrijednost podatkovnih resursa. Vrijednost podatkovnih resursa se određuje intervjuiranjem vlasnika podataka koji najbolje poznaju vrijednost i osjetljivost podataka. Neke od bitnih pretpostavki kod određivanja vrijednosti podataka su:

- ✓ sadrži li podatak osobne informacije,
- ✓ koje su zakonske i ugovorne obveze vezane za podatak,

- ✓ koji je ekonomski interes od podatka,
- ✓ znači li neraspoloživost podatka prekid neke poslovne aktivnosti,
- ✓ koji je financijski gubitak u slučaju kompromitiranja podatka i sl. [10, 38]

Ova metoda za procjenu rizika koristi tri parametra: vrijednost resursa, prijetnje i ranjivosti. Svaki od tih parametara promatra se u odnosu na moguće posljedice, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti. Varijacija ove metode eksplicitno navedena u dodatku standarda ISO/IEC 13335-3 i ISO 27005 za određivanje vrijednosti resursa koristi numeričke vrijednosti u rasponu od 0 (mala) do 4 (vrlo velika), dok se za kvantifikaciju ranjivosti i prijetnji koristi raspon od 0 (niska razina) do 2 (visoka razina). Razina rizika se određuje sumom vrijednosti parametara, tj. $R = AV + V + T$.

Na sljedećoj tablici (*Tablica 4.18.*) je prikazana matrica za procjenu rizika koja se dobiva kombinacijom gore navedenih varijabli (vjerojatnost pojavljivanja rizika, razina ranjivosti informacijske imovine i vrijednost imovine). [10, 38]

Tablica 4.18. - Matrica predefiniranih vrijednosti [10, 38]

	Prijetnja	Niska			Srednja			Velika		
Vrijednost resursa	Ranjivost	N	S	V	N	S	V	N	S	V
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Minimalna i maksimalna vrijednost procijenjenog rizika iznose:

$$R_{MIN} = AV_{MIN} + V_{MIN} + T_{MIN} = 0\,,$$
$$R_{MAX} = AV_{MAX} + V_{MAX} + T_{MAX} = 8\,.$$

Procijenjeni rizik može poprimiti sve cjelobrojne vrijednosti između R_{MIN} i R_{MAX}, uključujući i njih. Određivanje rizika nekog resursa se na kraju određuje tablicom pred-definiranih vrijednosti (*Tablica 4.19.*) Vrijednost imovine se određuje u odnosu na sva tri atributa tzv. trojka (povjerljivost, integritet, dostupnost – PID (eng. CIA)). Bitno je spomenuti da se i rizik na kraju procesa također klasificira. Naime cilj određivanja rizika je njegovo smanjivanje, prenošenje na „treću osobu“ ili prihvaćanje. Svaki rizik koji je visok

nužno je smanjiti u što kraćem vremenskom razdoblju. Za srednji rizik vrijeme reakcije se povećava ali još uvijek je bitno reagirati brzo ovisno o procjeni imovine. Na kraju za nizak rizik bitno je da se njega ne zanemari u procesu smanjivanja rizika. [10, 38]

Tablica 4.19. - Tumačenje rizika [10, 38]

Vrijednost	Rizik	Vrijeme djelovanja
0 - 2	Nizak	< 6 mjeseci
3 - 5	Srednji	< 2 mjeseca
6 - 8	Visok	< 2 tjedna

Ovakvim pristupom minimalna vrijednost procijenjenog rizika je 0, a maksimalna 8. Ovom metodom dolazi se do jednog ili više rizika za svaku grupu i/ili stavku informacijske imovine, ovisno o razmatranoj kombinaciji prijetnja – ranjivost. Najkritičniji rizici označeni su crvenom (visok: 5–8), a najmanje kritični zelenom (nizak: 0-2). Srednje kritični rizici označeni su žutom bojom (srednji: 3-4). Ako smo na ovaj način neki rizik procijenili kao visok (crvena polja), moramo uvesti (dodatne) sigurnosne kontrole kako bi smo ga snizili. Ako to nije moguće, možemo ga pokušati prenijeti na treću stranu ili ga svakako trebamo izbjeći. Ako smo neki rizik procijenili kao srednji (žuta polja), svjesni smo ga i moramo odlučiti prihvaćamo li ga ili ćemo ipak uvesti dodatne sigurnosne kontrole. Dobar način takve odluke jest *cost-benefit* analiza (analiza troškova i dobiti). [10, 38]

4.4.2.2. Metoda II - Rangiranje prijetnji prema procjeni rizika

Ova metoda za procjenu rizika formalno koristi samo dva parametra: utjecaj na resurs (vrijednost resursa) i vjerojatnost ostvarenja prijetnje. Implicitno se podrazumijeva da je utjecaj na resurs ekvivalentan vrijednosti resursa, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti. Na taj način procijenjeni rizik postaje funkcija više parametara:

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

Varijacija ove metode koristi jednak raspon vrijednosti za utjecaj (vrijednost resursa) i vjerojatnost ostvarenja prijetnje. Moguće vrijednosti su u rasponu od 1 (mala) do 5 (vrlo velika). Razinu rizika određuje produkt tih dvaju parametra.

$$R = I \times P.$$

Na sljedećoj tablici (*Tablica 4.20.*) je prikazana matrica za procjenu rizika.

Tablica 4.20. - Rangiranje prijetnji prema procjeni rizika [10, 38]

	Utjecaj (vrijednost)	Vjerojatnost ostvarenja	Rizik	Rangiranje prijetnje
Prijetnja **A**	5	2	10	2
Prijetnja **B**	2	4	8	3
Prijetnja **C**	3	5	15	1
Prijetnja **D**	1	3	3	5
Prijetnja **E**	4	1	4	4
Prijetnja **F**	2	4	8	3

Minimalna i maksimalna vrijednost procijenjenog rizika iznose:

$$R_{MIN} = I_{MIN} + P_{MIN} = 1 ,$$

$$R_{MAX} = I_{MAX} + P_{MAX} = 25 .$$

Procijenjeni rizik može poprimiti cjelobrojne vrijednosti između R_{MIN} i R_{MAX}, uključujući i njih, te isključujući proste brojeve izvan raspona vrijednosti i njihove višekratnike. [10, 38]

4.4.2.3. Metoda III - Procjena vjerojatnosti ostvarenja i mogućih posljedica

U ovoj metodi postupak procjene rizika je nešto složeniji nego kod prethodne dvije, a provodi se u tri koraka. Koraci su sljedeći :

1. Dodjeljuje se vrijednost svakom resursu. Vrijednost resursa se bazira na potencijalnim posljedicama u slučaju ostvarenja neke prijetnje.
2. Procjenjuje se vjerojatnost ostvarenja prijetnje za neku ranjivost. Ta vjerojatnost predstavlja kombinaciju mogućnosti pojave prijetnje i lakoće iskorištavanja ranjivosti.

$$P = f(V,T)$$

Tablica 4.21. - Tablica procjene vjerojatnosti ostvarenja [10, 38]

Prijetnja	Niska			Srednja			Velika		
Ranjivost	N	S	V	N	S	V	N	S	V
Vjerojatnost ostvarenja	0	1	2	1	2	3	2	3	4

3. Rizik se procjenjuje kao kombinacija vrijednosti resursa i vjerojatnosti ostvarenja.

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

Varijacija ove metode, eksplicitno opisana u standardu ISO/IEC 27005 za određivanje vrijednosti resursa koristi raspon od 0 (mala) do 4 (vrlo velika). Za određivanje ozbiljnosti ranjivosti i prijetnji koristi se raspon od 0 (mala) do 2 (velika). Vjerojatnost ostvarenja (frekvencija) računa se kao suma procijenjenih veličina ranjivosti i prijetnji.

$$P = V + T.$$

Ukupni rizik računa se kao suma vrijednosti resursa i vjerojatnosti ostvarenja.

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

Tablica 3.22. prikazuje matricu za određivanje vjerojatnosti ostvarenja. Uz određenu vjerojatnost ostvarenja i poznatu vrijednost resursa, rizik se procjenjuje kroz definiranu matricu (*Tablica 3.23.*). Minimalne i maksimalne vrijednosti procijenjenog rizika mogu se izračunati, te ponovno mogu poprimiti sve cjelobrojne vrijednosti između R_{MIN} i R_{MAX} uključujući i njih. [10, 38]

Tablica 4.22. - Određivanje vjerojatnosti ostvarenja [10, 38]

Prijetnja	0			1			2		
Ranjivost	**0**	1	2	0	1	2	0	1	2
Vjerojatnost ostvarenja	0	1	2	1	2	3	2	3	4

Tablica 4.23. - Matrica za procjenu rizika [10, 38]

Vrijednost resursa	0	1	2	3	4
Vjerojatnost ostvarenja					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Procjenom vjerojatnosti ostvarenja i moguće štete omogućava se rangiranje rizika prema procijenjenoj vrijednosti, slično kao i kod korištenja matrice preddefiniranih vrijednosti. Formalno gledajući, formule za procjenu rizika koje se koriste kod metode 1 (matrica preddefiniranih vrijednosti) i kod ove metode su potpuno identične, no suštinska razlika kod njih je da se kod metode 1 prilikom procjena ranjivosti i prijetnji implicitno

odražava vjerojatnost ostvarenja, odnosno frekvencija, dok se kod procjene vjerojatnosti ostvarenja i mogućih posljedica radi obrnuti postupak, odnosno na temelju procjene ranjivosti i prijetnji, određuje se pripadajuća vjerojatnost ostvarenja. Kod ove metode također je problematična nezavisna procjena razine prijetnje i ranjivosti. [10, 38]

4.4.2.4. Metoda IV - Odvajanje prihvatljivih i neprihvatljivih rizika

Još jedan način određivanja rizika je razlikovanje prihvatljivog i neprihvatljivog rizika. Na ovaj način određuje se u kojem je slučaju hitno potrebno reagirati na rizik, a kada se tretiranje rizika ne mora obaviti odmah. Prema ovoj metodi rizik se može iskazati binarno i to:

- prihvatljiv (P ili 0) ili
- neprihvatljiv (N ili 1).

Metoda odvajanja prihvatljivih i neprihvatljivih rizika predstavlja ustvari varijaciju treće metode (procjena vjerojatnosti ostvarenja i mogućih posljedica) ili metode 1 (matrica preddefiniranih vrijednosti). Način procjene rizika može biti identičan način kao i u prethodnoj metodi, jedino je matrica procijenjenih vrijednosti rizika binarna (*Tablica 4.24.*), isto kao i raspon vrijednosti koje može poprimiti procijenjeni rizik. [10, 38]

Tablica 4.24. - Matrica prihvatljivih i neprihvatljivih rizika [10, 38]

Vrijednost resursa	0	1	2	3	4
Vjerojatnost ostvarenja					
0	P	P	P	P	N
1	P	P	P	N	N
2	P	P	N	N	N
3	P	N	N	N	N
4	N	N	N	N	N

$R_{MIN} = 0, \quad R_{MAX}=1.$

Metoda odvajanja prihvatljivih i neprihvatljivih rizika predstavlja ustvari varijaciju metode 3 (procjena vjerojatnosti ostvarenja i mogućih posljedica) ili metode 1 (matrica preddefiniranih vrijednosti), te kao takva nasljeđuje prednosti i nedostatke tih metoda. [12, 15]

4.4.3. Izvor metode za provjeru rizika

Danas postoji veliki broj pristupa procjeni rizika te različite metode i tehnike za njihovu procjenu. Stoga nije jednostavno odrediti primjerenost pojedine metode jer takav odabir ovisi o većem broju čimbenika. Tako da će u nekim slučajevima biti bolje primijeniti neku određenu metodu. To ne znači da bi procjena provedena nekom drugom metodom bila pogrešna nego da bi bila primjerenija za postojeću situaciju. [57]

Kako bi se olakšao proces izbora metode za procjenu rizika potrebno je definirati kriterije koji će se uzimati u obzir kod donošenja odluke. Prilikom procjene kriterija potrebno ih je pažljivo razmotriti, da bi se donijela objektivna procjena. Da bi se metode mogle vrednovati moraju se znati mogućnosti pojedine metode ali i definirati vlastite zahtjeve i ograničenja. Prilikom izbora metode za procjenu važni su sljedeći kriteriji:

- ✓ Primjenjivost metode prema potrebama i motivima,
- ✓ Potrebni resursi,
- ✓ Potpora procjeni [57]

Primjenjivost metode prema motivima ovise o zahtjevima korisnika, performansama sigurnosti, usklađenosti sustava sa normama, dokumentiranjem sustava sigurnosti i o optimalizaciji troškova. Ključne potrebe za resursima se mogu podijeliti na vremenske, financijske, ljudske i materijalne resurse. Primjena svih metoda nije jednako vremenski zahtjevna, niti troškovi nisu isti. [57]

Potpora procjeni rizika se odnosi na softversku i metodološku potporu. Nemaju sve metode za procjenu rizika razvijen softver koji bi podržao procjenu rizika pomoću računala. Prilikom razmatranja metodološke potpore potrebno je razmotriti metriku koja se koristi, objektivnost i točnost, jednostavnost, cjelovitost, dobru dokumentiranost i postojanje uputa. Kod ovog razmatranja dobro je uzeti u razmatranje postojeće rezultate i iskustvo ukoliko postoji. [57]

Kada su definirani kriteriji donositelj odluke mora dodijeliti kriterijima određenu važnost. Nakon toga se uspoređuju mogućnosti sa pojedinim kriterijima kako bi se odredila relativna važnost pojedine alternative. Prilikom odabira metode na krajnji odabir će značajno utjecati iskustvo procjenitelja jer davanjem relativne važnosti kriterijima procjenitelj stavlja težište na one metode koje prema procjenitelju zadovoljava potrebe procjene. [57]

5. Alati za procjenu rizika

Danas na tržištu postoje brojni komercijalni alati za procjenu rizika koji imaju mogućnosti prilagodbe specifičnom slučaju za koji se izvodi procjena rizika. Većina njih ne zahtjeva veliko znanje na području informacijske sigurnosti, te time postaje izuzetno jednostavna za korištenje. Gotovo svi komercijalni alati produciraju izvještaje koji su jasni ne samo tehničkom osoblju, nego i poslovodstvu zaduženom za donošenje odluka. Neki od alata sadrže i podršku za ISO/IEC 17799 standard, odnosno omogućuju mjerenje usklađenosti sa standardom i daju preporuke kako se uskladiti. [8]

5.1. COBRA Risk Consultant

COBRA Risk Consultant je alat koji se na tržištu nalazi od devedesetih. To je upitnik baziran na principu ekspertnog sustava i opširne baze znanja. Alat omogućuje:

- ✓ identifikaciju prijetnji, ranjivosti i čimbenika izloženosti,
- ✓ mjerenje rizika za različite dijelove sustava i određivanje potencijalnih posljedica na poslovanje organizacije,
- ✓ predlaganje detaljnih rješenja za redukciju rizika,
- ✓ izradu tehničkog i poslovnog izvještaja [8]

COBRA Risk Consultant nudi dinamičku prilagodbu upitnika, te generira upitnik prilagođen tipu organizacije, operativnom okruženja i sustavu za koji se procjenjuje rizik. Postoji modul koji omogućuje modifikaciju upitnika. *Risk Consultant* nudi opciju "hipotetskog testiranja" (*engl. hypothesis testing*). Ta opcija određuje utjecaj dodatnih sigurnosnih kontrola na razinu rizika, tj. pomaže pri određivanju opravdanosti i isplativosti kontrola. *COBRA Risk Consultant* sadrži četiri baze znanja:

- ✓ bazu informacijske sigurnosti,
- ✓ bazu operativnog rizika,
- ✓ bazu rizika visoke razine,
- ✓ *e-Security* bazu koja obrađuje moderne mrežne sustave [8]

Alat sadrži i *COBRA ISO17799 Consultant* koji omogućuje praćenje usklađenost s ISO/IEC 17799 standardom i predlaže rješenja koja vode potpunoj usklađenosti sa standardom. Ispunjavanjem upitnika moguće je odrediti razinu usklađenosti s normom

ISO/IEC 17799. Metoda COBRA (*Consultative, Objective and Bi-functional Risk Analysis*), proizvod je tvrtke *C&A System Security Ltd.* i u prvom je redu oblikovana za pomoć i podršku poslovnim organizacijama koje uvode kriterije norme BS ISO/IEC 17799. Sastoji se od niza uputa za procjenu rizika sposobnosti IS-a i alata za procjenu koji se isporučuju u obliku programskog paketa. Osnovni su programski moduli metode *COBRA Risk Consultant i ISO Compliance Aanalyst. COBRA Risk Consultant* podržava potporu procesu procjene rizika:

- ✓ identifikacijom sistemskih prijetnja, ranjivosti i izloženost;
- ✓ mjerenjem stupnja rizika i povezivanjem s potencijalom utjecaja na poslovanje;
- ✓ davanjem detaljnih rješenja i preporuka za smanjivanje rizika. [8]

COBRA ISO Compliance Analyst koristi se za utvrđivanje istovjetnosti procjenjivanog sustava za zahtjevima norme BS ISO/IEC 17799, tako što:

- ✓ identificira postojeće stanje,
- ✓ uspoređuje nepodudarnost utvrđenog stanja sa zahtjevima norme sigurnosti,
- ✓ rezultat prikazuje u obliku izvješća i preporuka o potrebnim ispravcima. [8]

Tablica 5.1. - Osobine metode COBRA [57]

Prednosti	Nedostaci
✓ velika baza sigurnosnih prijetnja	✓ vizualno neprivlačno sučelje
✓ baza znanja može se prilagođavati potrebama	✓ slaba softverska podrška
✓ mogućnost djelomičnog procjenjivanja po pojedinim modulima	✓ dugotrajnost procjene
✓ objektivno procjenjuje prijetnje i ranjivost te predlaže rješenja	✓ izvještaji mogu biti jako dugački
✓ priprema za BS ISO/IEC certifikat	✓ slaba strukturiranost
✓ jednostavnost procjene	✓ nepreglednost procesa procjene
✓ cijena	✓ male mogućnosti prilagođavanja izvješća

Za pomoć u procjeni preporučuju se upitnici, ispitni propisi i intervjui. Nakon toga slijedi promatranje svih prikupljenih podataka. Što je više moguće traži se primjena automatiziranih alata za prikupljanje podataka, a za ručno prikupljanje NIST SP 800-26 nudi skup upitnika i ispitnih propisa za procjenu rizika koje se mogu iskoristiti za izračunavanja. Cjelovita programska podrška metodi NIST sadržana je u programskom paketu CORA. CORA (*Cost-of-Risk Analysis*) je sustav podrške upravljanju rizikom koji pomaže pri procjeni

rizika i izboru strategija umanjivanja rizika, mjera obnove i uspostavi optimalne strategije upravljanja rizikom. Koraci CORA metode odgovaraju u potpunosti zahtjevima iz poglavlja 3 do 4 dokumenta NIST SP 800-30. [57]

CORA je metoda koja se sastoji od dva koraka. U prvom koraku CORA organizirano skuplja, pohranjuje i vrednuje čimbenike rizika i utvrđuje izloženost gubicima u organizaciji. Procjena čimbenika rizika je jednostavna zahvaljujući programskom alatu, a sam se proces procjene ponavlja te se tim postiže objektivnost. Za izradu kvantitativnog modela rizika koriste se prikupljeni podaci i algoritmi. Pri tom CORA izračunava pojedinačni gubitak (*Single Occurrence Loss – SOL*) i godišnji očekivan gubitak (*Annualized Loss Expectancy – ALE*) za svaku prijetnju kojoj je izložen objekt procjene. [57]

Tablica 5.2. - Osobine metode CORA [57]

Prednosti	**Nedostaci**
✓ puna kvalitativna procjena	✓ cijena
✓ najbolja metoda za analizu troškova	✓ potrebno je predznanje
✓ privlačan programski alat	✓ slaba procjena nematerijalne imovine
✓ podrška za Web	✓ nije usklađena s ISO kriterijima
✓ simuliranje scenarija	
✓ grafička izvješća	

5.2. CRAMM

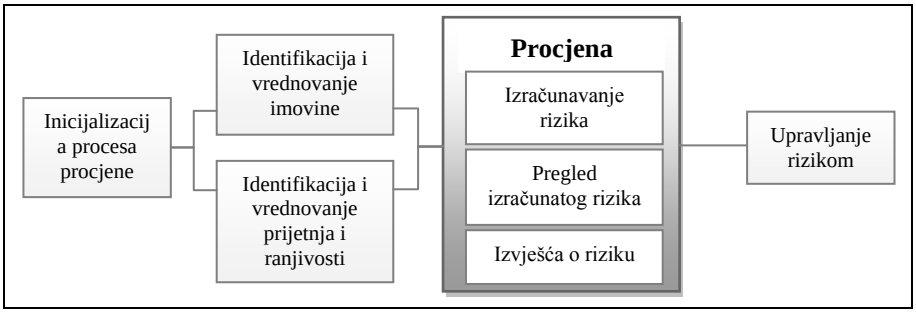
Alat CRAMM oblikovan je u skladu s politikom Vlade Velike Britanije da se strategija izbjegavanja rizika zamijeni strategijom upravljanja rizikom. Početno je aplikacija CRAMM prvenstveno bila napravljena za procjenu rizika državnih sustava, ali je nadopunjena te se danas može upotrjebljavati u različitim tržišnim organizacijama. Alat CRAMM sadrži:

- ✓ alat za procjenu rizika koji je u potpunosti usklađen s ISO/IEC 17799 standardom,
- ✓ niz pomoćnih alata koji daju podršku za planiranje i upravljanje sigurnošću,
- ✓ čarobnjake koji omogućuju kreiranje sigurnosnih politika i ostale dokumentacije,
- ✓ alate koji podržavaju procese za upravljanje kontinuitetom poslovanja,
- ✓ bazu sa više od 3000 sigurnosnih kontrola,
- ✓ alate koji pomažu pri postizanju usklađenosti s ISO/IEC 17799 standardom [8]

CRAMM metoda procjene rizika uključuje tehničke, kao i ne-tehničke (npr. fizička sigurnost) aspekte sigurnosti. Procjena rizika se obavlja u tri faze:

- ✓ identifikacija i vrednovanje resursa,
- ✓ procjena prijetnji i ranjivosti i
- ✓ odabir zaštitnih mjera i preporuka [8]

Metodu CRAMM počeo je razvijati *Central Computer and Telecommunications Agency* 1985. godine pod pokroviteljstvom *UK Government's Cabinet Office*. Prva inačica CRAMM Management Guida je izdana 1996. godine od strane *Goverment's Security Service* koji je tad i preuzeo vlasništvo. Zadnje izdanje je izdano 2003. godine pod nazivom CRAMM 5.0. [8]



Slika 5.1. - Osnovni koraci metode CRAMM [57]

Tablica 5.3. - Osobine CRAMM metode [57]

Prednosti	Nedostaci
✓ CRAMM daje strukturalni pristup procjeni rizika	✓ alat mogu koristiti samo iskusni stručnjaci ili osoblje koje je prošlo usavršavanje
✓ softwerski alat ohrabruje procjenitelje za strogu procjenu sigurnosti IS-a	✓ potpuna revizija traje mjesecima
✓ alat posjeduje hijerarhijsku bazu mjera zaštite	✓ alat proizvodi dugačke sadržaje
✓ alat omogućuje procjeniteljima dovoljno fleksibilnosti u modeliranju sustava	✓ alat ne pruža dovoljno fleksibilnosti pri izboru stila izvještaja
✓ alat nudi pomoć pri planiranju neprekidnog poslovanja	✓ relativno visoka cijena plus dodatni troškovi usavršavanja
✓ može se procijeniti veći ili manji sustav	✓ treba obučiti ljude ili koristiti vanjskog stručnjaka za CRAMM
✓ vizualno privlačni i odličan strukturirani alat	✓ nije primjeren za uspostavu fizičke zaštite i proceduralnih protumjera
✓ podrška pripremi za BS ISO/IEC 17799 certifikat	✓ traži točne podatke koje mu sustav u razvoju ne može pružiti

5.3. OCTAVE

OCTAVE metoda u praksi se uvodi u organizacije tako da se osnivaju radionice u kojima radni timovi uvježbavaju postupke metode OCTAVE i na primjerima i stvarnim situacijama uče uvoditi metodu u svoju okolinu. Postupak se provodi u tri etape :

- ✓ određivanje kritične imovine i prijetnje toj imovini,
- ✓ određivanje organizacijskih i tehnoloških ranjivosti,
- ✓ razvoj strategije zaštite i izbjegavanje rizika za podršku poslovanju [8]

OCTAVE metodologija upotrebljava informacijske kataloge kako bi se analizirale prijetnje, utvrdile prakse koje već postoje unutar organizacije i kako bi se izgradila strategija zaštite. Tri su tipa kataloga:

- ✓ katalog dobrih praksi - zbirka strategija i praksi za upravljanje informacijskom sigurnošću,
- ✓ generički profil prijetnji - kolekcija najčešćih izvora prijetnji,
- ✓ katalog ranjivosti - kolekcija ranjivosti koja ovisi o platformi i aplikaciji koja se promatra [8]

Program OCTAVE (Operationally *Critical Threat, Asset, and Vulnerability Evaluation*) su razvili *Software Engineering Institute* (SEI) i *Carnegie Mellon University* (CMU) na temelju niza zahtjeva i preporuka koje postavlja američko Ministarstvo obrane. Metoda je opće poznata pod nazivom *OCTAVE method*. OCTAVE se neposredno zasniva na kriterijima propisanim u dokumentu *OCTAVE Criteria* (CMU/SEI-2001-TR-016). Provedba i usvajanje metoda OCTAVE objašnjeno je u dokumentima *OCTAVE Method* Implementation Guide i OCTAVE Catalog of Practices (CMU/SEI-2001-TR-020), a izdano je i više drugih dokumenata koji objašnjavaju metodu. [8]

Tablica 5.4. - Osobine OCTAVE metode [57]

Prednosti	Nedostaci
✓ vrlo detaljna i temeljita u uputama	✓ metoda ne sadrži pomoćne metode
✓ potrebni su veliki ljudski i financijski izvori	✓ mjere zaštite mogu biti skupe
✓ preporučuje strategiju zaštite	✓ nema odgovarajućeg softverskog rješenja
✓ fleksibilna, prilagodljiva, kvalitativna	✓ nije usklađena s formalnim nagradama ili podvrgnuta procjeni nezavisnog tijela
✓ cjelovit i univerzalan pristup	✓ primarno je interesira informacijska imovina
✓ vjerojatnost se jednostavno tumači	✓ namijenjena velikim poslovnim organizacijama
✓ gotovo neznatna cijena	✓ nema stručne konzultantske pomoći
✓ ne predstavlja strogi okvir	✓ uvođenje metode je samostalna

5.4. RuSecure

RuSecure metoda tvrtke *GlendaleSystems, Ltd*. Također nastaje kao podrška procjeni rizika po normi BS/ ISO/IEC 177999. Metoda se zasniva na normi BS 7799 i u potpunosti zadovoljava njene kriterije. Metoda se sastoji od uputa u obliku priručnika *Information Security Policies + Glossary and Reference Manual* koji savjetuje procjeniteljima o svima pitanjima vezanim uz procese procjene rizika sigurnosti IS-a. Po svom obliku i mogućnostima metoda ReSecure najviše podsjeća na priručnik *Guide to BS 7799 Risk Assessment and Risk Managment*. [57]

Tablica 5.5. - Osobine metode RuSecure [57]

Prednosti	Nedostaci
✓ preglednost i strukturiranost kriterija	✓ potpuna manualna metoda
✓ jednostavnost	✓ nema podrške programskog alata
✓ nije potrebno posebno predznanje	✓ nemogućnost prilagođavanja potrebama organizacije
✓ brzina provedbe	✓ nepreciznost
✓ podrška BS /ISO/IEC certifikaciji	✓ necjelovitost
✓ cijena	

5.5. NASA - FMEA metoda

NASA stavlja težište na kvantitativnu procjenu za koju posebno koristi grafičke tehnike FTA i ETA, ali najviše primjenjuje metodu FMEA koja je ujedno i prihvaćena kao svoju osnovnu metodu za procjenu rizika. Glavne karakteristike ove metode su:

- ✓ određivanje uzoraka pogrešaka,
- ✓ ocjenjivanje specifikacije za nadzor s obzirom na njihove mogućnosti otkrivanja i prevenciju pogrešaka,
- ✓ sustavno pregledavanje i procjenu svih grešaka i razmatranje njihove posljedice za korisnika,
- ✓ procjene mogućnosti pojave i otkrića pogreške te učinaka na korisnika oblikuju se prioriteti,
- ✓ uspostave odgovarajuće kontrole mjere te odredi odgovornost za njihovo izvršavanje,
- ✓ u skladu s novim procesima isprave identifikacijske i preventivne mjere. [57]

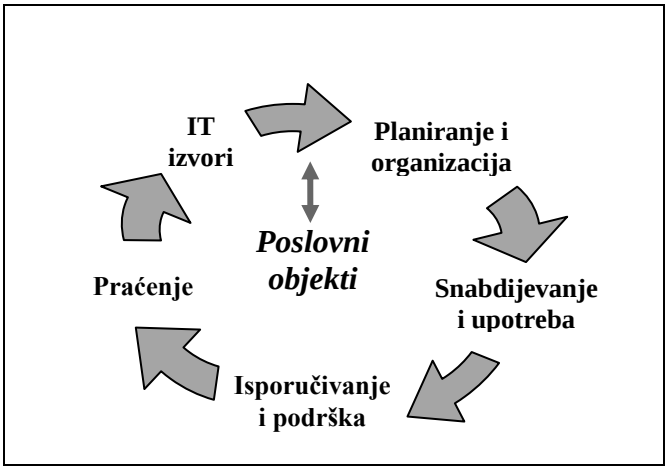
Tablica 5.6. - Osobine metode FMEA [57]

Prednosti	Nedostaci
✓ jednostavnost	✓ neprimjerenost velikim sustavima
✓ jasan i dokumentiran postupak	✓ slaba mogućnost izvještavanja
✓ može se individualno koristiti	✓ ne predlaže protumjere
✓ brzina procjene	✓ nije usklađena s nijednim kriterijem
✓ cijena	✓ nedovoljna dokumentiranost
✓ privlačno programsko sučelje	✓ ne posjeduje bazu prijetnja
✓ primjerena analizi manjeg broja kritičnih izvora	✓ slaba interaktivnost i mogućnost prilagođavanja potrebama organizacije

5.6. COBIT

Upute *COBIT Management Guidelines* su razvijene na rezultatima mnogobrojnih rasprava i iskustava mnogobrojnih stručnjaka iz područja sigurnosti, a temelj metode su svjetski standardi. Metoda COBIT objavljena je u šest dijelova koji zajedno s programskim alatom čine jedinstveni okvir i metodu procjene rizika. Osim osnovne verzije postoji i metoda *COBIT Quick start* namijenjena manjim poslovnim organizacijama gdje IT nije tako kritičan

za poslovanje. U središtu zanimanja osnovne metode COBIT veliki su sustavi s dnevno intenzivnom i raspodijeljenom obradom podataka. [8]



Slika 5.2. - Princip i ideja metode COBIT [57]

Uz pomoć COBIT metode se žele uskladiti poslovni ciljevi i IT tako da ta veza donosi rezultate. Strukturiran je na 34 IT procesa podijeljena u četiri kategorije čijim zadovoljenjem organizacija uspostavlja ravnotežu. [8]

Slika 5.3. - Koraci metode COBIT [57]

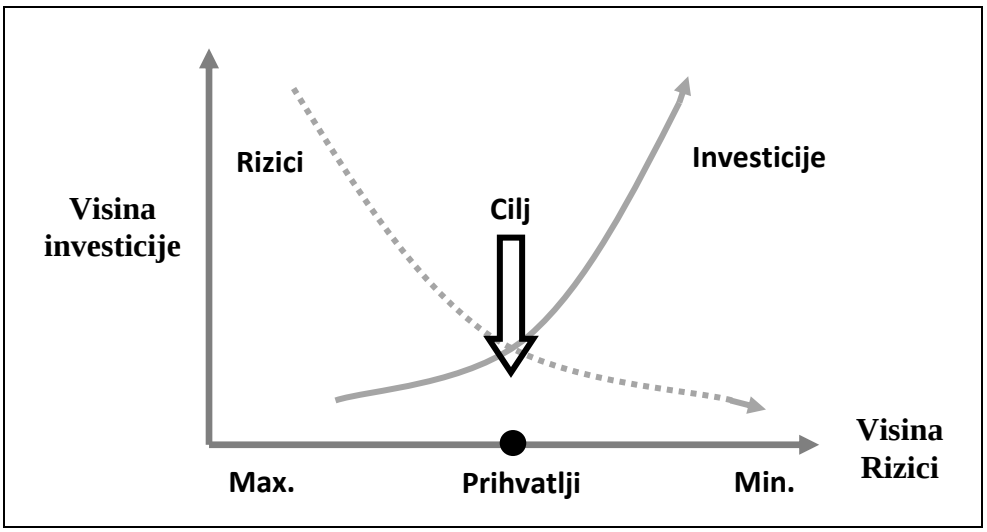
COBIT se ne bavi isključivo procjenom rizika, možda se čak i ne može svrstati među metode procjene rizika, on ipak sadrži kriterije koji se odnose i na procjenu rizika sigurnosti, te opisuje i način na koji se procjena rizika može sprovesti. COBIT se više bavi usklađivanjem IT-a s poslovnim ciljevima. [8]

Tablica 5.7. - Osobine COBIT metode [57]

Prednosti	Nedostaci
✓ jednostavnost	✓ procjena ne donosi bitne rezultate za unapređenje sigurnosti
✓ otvoreni model	✓ služi samo kao preliminarna procjena
✓ povezuje IT izvore s poslovnim ciljevima	✓ slaba razrađenost kriterija
✓ razrađeni programski paket	✓ samo je uvjetno metoda procjene rizika
✓ cijena	

6. Utvrđivanje prihvatljivog rizika

Važnost procjene rizika sigurnosti je u tome što se veličina utvrđenog rizika može izravno upotrijebiti kao pokazatelj potrebnih sigurnosnih rješenja i troškova mjera zaštite. Ulaganja u sigurnost određuju se proporcionalno s mogućim gubicima, tj. utvrđenom riziku jer osiguravanje ne treba biti veće od potrebnog, odnosno optimalno smanjenje rizika nastupa kada daljnje smanjivanje košta više od ostvarenih koristi. [57]



Slika 6.1. - Prikaz odnosa visine investicije i rizika [57]

Kada definiramo rizik u terminima vrijednosti za organizaciju - možemo definirati i cijenu nastupanja rizika u novčanim terminima. Usporedbom te vrijednosti i vrijednosti investicije u zaštitnu mjeru dolazimo do prihvatljive točke. Mora se imati na umu da investicija nije samo izračun uloga u hardware već i troškovi implementacije. Primjena zaštitnih mjera je zadnji dio izgradnje ISMS sustava koji se svojim *Plan-Do-Check-Act* krugom nadopunjuje u krug postavljen implementacijom ISO 9001. [57]

7. Usporedba alata za procjenu rizika

Da bi se metode i tehnike mogle usporediti, utvrditi njihove sličnosti i razlike njihove osobine se mogu vrednovati prema tri intenziteta koja su označena sljedećim simbolima:

● izrazito zadovoljava kriterij tj. označava da je osobina izrazito izražena,

X umjereno zadovoljava kriterij,

- slabo zadovoljava kriterije [57]

Intenziteti su određeni usporedbom svake metode pojedinim kriterijem. Usporedba metoda prema kriterijima vrednovanja prikazana je u tablici 7.1. Ova usporedba je vrlo korisna prilikom odabira metode za procjenu rizika jer se vrlo brzo mogu odrediti alternative prema odabranim kriterijima vrednovanja.[57]

Većina metoda je kompleksna, skupa i nije primjenjiva ako procjenitelj ima malo znanja iz područja sigurnosti. [57]

Tablica 7.1. - Usporedba alata za procjenu rizika [57]

Metode / Kriteriji	BS 7799	RuSecure	NASA	FMEA	NIST	GAO	FIPS 65	CRAMM	COBRA	COBIT	OCTAVE	FRAP	CORA
cijena i ostali troškovi	-	X	-	X	-	-	-	●	X	●	-	-	●
programska podrška	-	●	X	●	X	-	-	●	●	●	X	X	●
preporuka poboljšanja	-	-	●	●	●	●	X	●	●	X	●	X	●
osnova analize troškova	-	-	●	●	●	X	●	●	-	X	X	-	●
primjena u malim sustavima	●	●	X	●	●	X	X	●	●	●	●	●	-
podrška normi sigurnosti	X	●	X	X	X	-	-	●	●	X	-	-	●
točnost i detaljnost	X	X	●	X	●	X	●	●	●	X	X	X	●
mogućnost brze procjene	●	●	-	X	X	-	-	●	-	-	●	X	X
kvantitativnost	X	-	X	-	X		●	-	-	-	X	-	●
kvalitativnost	X	●	X	●	X		-	●	●	●	X	●	X
kombiniranost	●	-	●	-	●	●	-	X	-	-	●	-	X
cjelovitost	-	X	●	X	●	X	X	●	●	●	●	X	●
preporuka alata	X	-	●	-	●	X		-	-	X	●		-
vremenski izvori	-	X	●	X	X		●	●	●	X	●	X	X
ljudski izvori	-	X	X	X	X		●	●	X	●	●	X	X
vjerojatnost	-	X	X	X	●		●	-	-	-	X	-	●
potrebno predznanje	X	-	●	-	●		●	●	X	X	●	X	●
samoprocjena	●	●	X	●	X		X	X	●	●	●	●	X
fleksibilnost	X	X	X	X	X		-	X	X	●	●	X	X
mogućnost prethodne procjene	●	X	-	●	X		-	-	-	●	X	●	-
interaktivnost	-	-	-	●	X	-	-	X	X	X	-	-	X
jednostavnost	●	●	X	●	X		-	-	X	●	X	●	-
dokumentiranost	-	-	X	X	●		X	●	●	X	●	X	X

Kao što je vidljivo iz tablice većina alata su kompleksi, skupi i namijenjeni osobama koje se bave profesionalnom procjenom rizika. Za metodu Octave Allegro nije razvijena programska podrška, ali nema ni formalnih niti zakonskih ograničenja prilikom korištenja. Metoda je orijentirana za procjenu rizika nad srednjim i velikim poslovnim sustavima. Upravo su ovo kriteriji prema kojim je ova metoda odabrana.

Navedeni kriteriji postavljeni su zbog toga jer je jedan od osnovnih ciljeva ovog rada da se korištenje procjene rizika omogući širokom broju korisnika. Putem razvijene web aplikacije osiguran je segment raširenosti i dostupnosti. Provođenjem istraživanja u vezi napada prisutnih u RH, stvaranjem kataloga te njegovom integracijom u aplikaciju osigurana je jednostavnost korištenja metode. Navedeni katalog je ujedno i prvi javni katalog napada na sigurnost u RH. S druge strane ona je besplatna za korištenje pa bi se s time trebao osigurati i veći interes poslovnih sustava da zaštite svoje informacijske sustave. Metode za procjenu rizika su složene te zahtijevaju određeno znanje i iskustvo prilikom njihove primjene, ipak kroz sve navedeno razina potrebnog znanja i iskustva znatno je smanjena.

Kako bi se metoda lakše koristila prevedena je na hrvatski jezik te je detaljno objašnjen način njezinog korištenja.

8. Detaljna obrazloženje metode Octave Allegro

8.1. Uvod u metodu Octave Allegro

Dakle u nastavku ćemo detaljnije obraditi metodu Octave Allegro[7] uz pomoć koje ćemo izvršiti identifikaciju procesa i sistematizaciju opasnosti na konkretnom primjeru. Metoda OCTAVE (The Operationally Critical Threat, Asset and Vulnerability Evaluation) se razvija kroz tri koraka u okviru kojih je potrebno:

- Formulirati profil prijetnji,
- Identificirati ranjivost infrastrukture,
- Razviti sigurnosnu strategiju i planove.

Ti koraci predstavljaju opći pristup u Octave metodi, dok u našem primjeru Octave Allegro ima osam koraka, a oni su:

1. Definiranje kriterija za mjerenje rizika,
2. Kreiranje profila informacijske imovine,
3. Identificirati informacijsku imovinu,
4. Identificirati kritična područja,
5. Prepoznavanje scenarija prijetnji,
6. Identifikacija rizika,
7. Analiza rizika i
8. Odabrati način pristupa.

8.2. Korak 1 – Definiranje kriterija za mjerenje rizika

U prvom koraku je cilj uspostaviti organizacijski pogonski program koji će se koristiti za procjenu učinka rizika za Vašu organizaciju, njenu misiju i poslovne ciljeve. Kako bi se taj program odvijao učinkovito potrebno je definirati određene kriterije za mjerenje rizika. Pravilno definiranje kriterija prilikom procjene rizika predstavlja ključnu ulogu za Vašu informacijsku imovinu. Ukoliko kriteriji nisu definirani onda nije moguće ni definirati mogući rizik koji prijeti organizaciji. Zbog toga organizacija mora jasno definirati koja su joj područja i procesi od velike važnosti kako bi se njeni poslovi mogli izvršavati besprekidno što joj i omogućuje da bude konkurentna. Npr. u nekim organizacijama odnos s kupcima može biti više značajan od utjecaja na njegovu usklađenost s propisima. Prilikom provođenja metode Allegro stvara se niz pravila i kriterija uz pomoć kojih se definira koliki raspon

[7] Orginalna verzija metode je dostupna na: http://www.cert.org/octave/allegro.html

utjecaja rizika za pojedina područja u organizaciji (ovakva rješenja su jedinstvena za svaku organizaciju). Npr., područje učinka može biti zdravlje i sigurnost korisnika i zaposlenika, zakoni i propisi, financije ili ugled organizacije. Uz pomoć predložaka i tablica koje nudi metoda Allegro možemo jasno definirati kriterije za mjerenje rizika te njihovo djelovanje za pojedina područja, nakon toga cilj je dodijeliti prioritete. Važno je definirati konzistentan skup kriterija za mjerenje rizika koji se mogu koristiti prilikom procjene cjelokupne informacijske imovine. Kriteriji trebaju biti usmjereni na organizacijskoj razini tj. više menadžment bi trebao biti upoznat sa svim rizicima koji prijete organizaciji bilo to da su oni vanjski ili unutarnji. Ukoliko su kriteriji i prioriteti jasno definirani onda je i menadžerima lakše donijeti odluka kako pristupiti prema pojedinom riziku (ovo predstavlja zadnju korak metode tj. odabir načina pristupa rizicima).

8.2.1. Pojmovi i definicije

- **Prijetnja** - predstavlja učinak prijetnje na poslovne ciljeve i misiju organizacije.
- **Vrijednost prijetnje** - kvalitativna mjera specifičnih rizika koji utječu na organizaciju (visoka, umjerena ili niska).
- **Kriterij mjerenja rizika** - skup kvalitativna mjera uz pomoć kojih ocjenjujemo rizik koji djeluje na poslovne ciljeve i misiju organizacije. Uz pomoć kriterija mjerenja rizika definiraju se rasponi (visok, srednji, nizak) utjecaja rizika na organizaciju.

8.2.2. Upute i aktivnosti

U prvom koraku postoje dvije aktivnosti:

❑ **Korak 1 Aktivnost 1**

Prvo je potrebno definirati kvalitativni skup mjera (*kriterij mjerenja rizika*) uz pomoć kojeg ćete moći procijeniti utjecaj rizik na Vašu organizaciju, misiju i poslovne ciljeve. Kriterij mjerenja rizika je potrebno dokumentirati u *radnim tabelama*, razmislite o sljedećim područjima utjecaja:

- ✓ Ugled i klijentovo povjerenje (Radna tabela 1, odlomak 2)
- ✓ Financije (Radna tabela 2, odlomak 2)
- ✓ Produktivnost (Radna tabela 3, odlomak 2)
- ✓ Zdravlje i sigurnost (Radna tabela 4, odlomak 2)
- ✓ Pravne i zakonske kazne (Radna tabela 5, odlomak 2)
- ✓ Korisnikova procjena prijetnji (Radna tabela 6, odlomak 2)

Popunite sva prazna područja u radnim tabelama i smatrajte ih važnim za Vašu organizaciju. Također možete promijeniti opis ili dodati novi ako Vam je to potrebno.

Bilješke:

Ukoliko je u Vašoj organizaciji već izvršena ova procjena tj. ako su kriteriji mjerenja rizika već definirani onda se ovaj korak može preskočiti. Međutim, ukoliko su kriteriji stariji ili nepotpuni onda bi ovaj korak svakako trebalo provesti, jer organizacija mora biti upoznata sa trenutnim prijetnjama rizika i njihovom tolerancijom.

Tablica 8.1. - Implementacija: Korak 1, Aktivnost 1

Allegro radna tabela 1	**KRITERIJ MJERA RIZIKA –** Ugled i klijentovo povjerenje		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**
Ugled	*Utječe minimalno na ugled, tj. moguće se oporaviti uz malen ili ikakvih napora i troškove.*	*Ugled je narušen, i potreban je određeni napor i trošak da se oporavi.*	*Ugled je trajno narušen ili oštećen.*
Gubitak klijenata	*Gubitak klijenta manje od 10% zbog smanjenja pouzdanja.*	*10 do 30% zbog smanjenja pouzdanja.*	*Više od 30% zbog smanjenja pouzdanja.*

Navedene su dvije stavke koje predstavljaju primjer kako treba popuniti ovu radnu tabelu

Allegro radna tabela 2	**KRITERIJ MJERA RIZIKA –** Financije		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**
Troškovi poslovanja	*Povećanje godišnji troškova poslovanja manje od 10%.*	*Godišnji troškovi poslovanja povećani od 10 do 20%.*	*Godišnji troškovi poslovanja već od 20%.*
Gubitak prihoda	*Godišnji gubitak prihoda manji od 10%*	*Godišnji gubitak prihoda od 10 do 20%.*	*Godišnji gubitak prihoda veći od 20%.*
Jednokratni financijski gubitci	*Jednokratni financijski gubitci manji od 20 000 KN*	*Jednokratni financijski gubitci od 20 000 KN do 50 000 KN*	*Jednokratni financijski gubitci oveći od 50 000 KN*

Navedene su tri stavke koje predstavljaju primjer kako treba popuniti ovu radnu tabelu

Allegro radna tabela 3	**KRITERIJ MJERA RIZIKA** – Produktivnost		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**
Radni sati zaposlenika	*Radni sati zaposlenika su povećani manje od 10% u 6 radni dana.*	*Radni sati zaposlenika su povećani od 10% do 20% u 6 radni dana.*	*Radni sati zaposlenika su povećani više do 20% u 6 radni dana.*

Navedene stavka predstavlja primjer kako treba popuniti ovu radnu tabelu

Allegro radna tabela 4	**KRITERIJ MJERA RIZIKA –** Zdravlje i sigurnost		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**
Život	*Nema gubitka ili značajnu prijetnju za kupaca ili zaposlenika.*	*Životi kupca ili zaposlenika su ugroženi, ali će se oporaviti nakon pružanja liječničke pomoći.*	*Smrt kupca ili zaposlenika.*
Zdravlje	*Minimalna, i potrebno je odmah liječiti osoblje (kupce i zaposlenike) i da oporavak bude u roku od 4 dana.*	*Privremeno ili oporavak od pogoršanog zdravstvenog stanja osoblja (potrošača i zaposlenika).*	*Trajno pogoršanje zdravlja koje rezultira dugoročni gubitak kupaca ili zaposlenika.*
Sigurnost	*Sigurnost upitna.*	*Sigurnost izložena utjecajima.*	*Sigurnost narušena.*

Navedene su tri stavke koje predstavljaju primjer kako treba popuniti ovu radnu tabelu

Allegro radna tabela 5	**KRITERIJ MJERA RIZIKA –** Pravne i zakonske kazne		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**
Kazna	*Novčana kazna manja od 5 000 KN.*	*Novčana kazna od 5 000 KN do 20 000 KN.*	*Novčana kazna veća 20 000 KN.*
Tužbe	*Ozbiljne tužbe podnesene od strane organizacije koje su manje od 5 000 KN.*	*Ozbiljne tužbe podnesene od strane organizacije koje su od 5 000 KN do 20 000 KN.*	*Ozbiljne tužbe podnesene od strane organizacije koje su veće od 20 000 KN.*
Istrage	*Nema upita od vlade ili drugih istražnih organizacija.*	*Vlada ili druge istražne organizacije traže informacije ili zapise (po zakonskim propisima i obavezama).*	*Vlada ili druge istražne organizacije pokreću intenzivnu istragu u dubinu (detaljnije).*

Navedene su tri stavke koje predstavljaju primjer kako treba popuniti ovu radnu tabelu

Allegro radna tabela 6	**KRITERIJ MJERA RIZIKA –** Korisnikova procjena prijetnji		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

❑ **Korak 1 Aktivnost 2**

U ovom koraku je bitno dodijeliti prioritete od većeg prema manjem za područja koja su pod utjecajem prijetnji (koristeći radnu tabelu 7, odlomak 2). Najvažnija kategorija treba dobiti najveću vrijednost a najmanja važna najmanje.

Bilješke:

Ako imate pet područja utjecaja, području koje je najbitnije dodijelite vrijednost (prioritet) pet, a zatim manje važnom četiri pa tim redom sve do posljednjeg. Sva utjecajna područja koja su identificirana moraju imati svoju dodijeljenu vrijednost. Ova dodjela prioriteta se koristi kasnije u procjeni rizika jer uz pomoć nje organizacija može lakše identificirati pojedini rizik te ga smjestiti u određeno područje.

Tablica 8.2. - Implementacija: Korak 1, Aktivnost 2

Allegro radna tabela 7	**RADNA TABLICA - DOJELA PRIORITETA ZA UTJECAJNA PODRUČJA**
PRIORITET	**PODRUČJE UTJECAJA**
	Ugled i klijentovo povjerenje
	Financije
	Produktivnost
	Zdravlje i sigurnost
	Pravne i zakonske kazne
	Korisnikova procjena prijetnji

8.3. Korak 2 – Kreiranje profila informacijske imovine

8.3.1. Pojmovi i definicije

- **Imovina** – predstavlja sve ono što je važno za poslovni sustav. Korištenjem imovine i sredstva organizacija teži prema ostvarivanju svojih ciljeva, povratu na uložene investicije ali i stvaranju prihoda. Ukupna vrijednost organizacije može se gledati kao vrijednost cjelokupne imovine.
- **Ključna informacijska imovina** – kritična informacije imovina predstavlja najvažnija sredstva za organizaciju. Organizacija će imati negativan učinak ukoliko je:
  - ✓ kritična imovina (informacije) prikazana ili dostupna neovlaštenim osobama,
  - ✓ kritična imovina izmijenjena bez odobrenja,
  - ✓ kritična imovina izgubljena ili uništena,
  - ✓ kritična imovina (informacije) nedostupna tj. prekinut pristup.
- **Informacijska imovina** – informacijsku imovinu predstavljaju sve informacije ili podaci koji imaju vrijednost za organizaciju, uključujući informacije kao što su podaci o kupcima, poslovnim partnerima ili intelektualno vlasništvo (znanje). Ova sredstva mogu postojati u fizičkom obliku (na papiru, CD-u ili na drugim medija) ili elektroničkim obliku (pohranjena na bazama podataka, u datotekama, na osobnim računalima).
- **Profil informacijske imovine** – prikaz informacijske imovine koji opisuje njene jedinstvene značajke, obilježja i vrijednosti.
- **Vlasnici informacijske imovine** – vlasnici informacijske imovine su oni pojedinci čija je primarna odgovornost za održivost, opstanak i fleksibilnost informacijske imovine. Oni trebaju biti upoznati sa sigurnosnom politikom u kojoj su jasno definirani propisi kako osigurati i zaštiti informacijsku imovinu.
- **Skrbnik (*čuvar*) informacijske imovine** – Čuvari informacija imovine su pojedinci u organizaciji koji imaju odgovornost da zaštite informacijsku imovinu koja se pohranjuje, prenosi ili obrađuje. Drugim riječima, čuvari prihvaćaju odgovornost za informacijsku imovinu koju koriste.
- **Ljudi** – U strukturalnoj procjeni rizika, ljudi predstavljaju jednu vrstu "spremnika" informacije imovine. Oni mogu posjedovati specijalizirane ili važne informacije i svakodnevno ih koristiti u svom poslovanju. Informacije koje svakodnevno koriste

predstavljaju intelektualno vlasništvo (znanje). U nekim slučajevima informacije koje ljudi posjeduju, u organizacijama nisu zapisane ni u jednoj formi (tj., ne mogu biti u pisanom obliku).

- **Sigurnosni zahtjevi** – ovim zahtjevima je definirano na koji način će informacijska imovina biti zaštićena. Oni se također često spominju kao "sigurnosni ciljevi".
  - ✓ *Povjerljivost* - osiguranje da samo ovlaštene osobe (ili sustavi) imaju pristup informacijskoj imovini.
  - ✓ *Integritet* - osigurava da stanje informacijske imovine ostane za namjenu i potrebu vlasnika.
  - ✓ *Dostupnost* - osigurava da informacijska imovina bude dostupna ovlaštenim korisnicima.
- **Tehnološka imovina** – pod ovim pojmom podrazumijevamo elektronske spremnike u kojima se informacijska imovina pohranjuje, prenosi i obrađuje. Općenito gledajući ovdje ubrajamo: hardver, softver, aplikacijske sustave, servise i mreže. Ovdje je bitna dostupnost koja osigurava da informacijska imovina bude dostupna ovlaštenim korisnicima.

8.3.2. Opća napomena

Procjenu rizika koju Vi obavljate je usmjerena na informacijsku imovinu organizacije. U ovom koraku možete početi sa procesom definiranja informacijske imovine. Zatim je potrebno identificirati sve "spremnike" informacijske imovine u kojima se pohranjuje, prenosi i obrađuje informacijska imovina. Nakon što popišemo spremnike bitno je identificirati njihovo stanje. To će Vam pomoći da u potpunosti utvrdite sve točke u kojima je informacijska imovina izložena promjenama, gubitku / uništenju ili prekidu (prilikom slanja ili dostupnosti).

Stvaranjem profila za svaku informacijsku imovinu formirana je osnova za identifikaciju prijetnji i rizika u kasnijim koracima. Također, stvaranjem profila informacijske imovine osiguravamo da imovina bude jasno i dosljedno opisana (dokumentirana), da su poznate granice informacijske imovine te da postoje sigurnosni uvjeti koji su adekvatno opisani. Profil informacijske imovine čak može biti nadopunjen pa da uključuje kvantitativnu procjenu imovine, naravno ako to želite.

8.3.3. Upute i aktivnosti

U drugom koraku postoji osam aktivnosti:

❑ **Korak 2 Aktivnost 1**

Prva aktivnost u ovom koraku procjene rizika predstavlja identificiranje i klasifikaciju prikupljenih informacija o imovini. Korisnost procjene je najveća kada je usmjerena na informacijsku imovinu koja je od ključne važnosti za poslovanje poslovnog sustava. Ovisno o razini na kojoj se izvodi procjena rizika, organizaciju je moguće podijeliti na odjele (kadrove) ili bilo koje druge podrazine organizacije.

Da bi to učinili, bitno je da razmotrimo sljedeća pitanja:

- ✓ Koja informacijska imovina ima najveću vrijednosti u Vašoj organizaciji?
- ✓ Koja informacijska imovina se svakodnevno koristi u poslovnim procesima i operacijama?
- ✓ Da li se organizacijski poslovi mogu normalno odvijati ukoliko bi se narušila sigurnost određene informacijske imovine, i da li će onda organizacija biti sposobna da ostvari svoje ciljeve i misiju?
- ✓ Koje su sve druge imovine usko povezane s tom imovinom?

Brainstorm metodom napišite listu informacijske imovine koja je važna za Vašu organizaciju i na kojoj možete obaviti strukturiranu procjenu rizika.

❑ **Korak 2 Aktivnost 2**

"Fokusiranje na nekoliko kritičnih" je bitan princip upravljanja rizicima. Dakle, trebali biste obaviti strukturiranu procjenu rizika samo za onu imovinu koja je najvažnija za postizanje ciljeva i ostvarivanje misije organizacije.

Iz liste koju ste kreirali u prethodnom koraku (*Aktivnost 1*), razmotrite sljedeća pitanja:

- Koja će informacijska imovina sa popisa imati negativan utjecaj na organizacijsko poslovanje ukoliko je ona ugrožena (definirano prilikom određivanja kriterija vrednovanja)? I što ako se desi jedan od sljedećih scenarija:
  - ✓ informacijska imovina je objavljena osobama sa **neovlaštenim pristupom**.
  - ✓ informacijska imovina je **promijenjena** bez odobrenja.
  - ✓ informacijska imovina je **izgubljena** ili **uništena**.
  - ✓ pristup informacijskoj imovini je **prekinut**.

Ukoliko imovini prijeti jedan ili više od ovih kriterija, onda je ta imovina kritična i treba je strukturalnom procjenom rizika zaštiti kako bi se poslovanje organizacije moglo izvršiti sigurno i bezprijekorno.

Sljedeća aktivnost predstavlja proces procjene rizika za Vašu ključnu informacijsku imovinu. Kako bi izvršili procjenu rizika za svu ključnu imovinu, jednostavno ponovite sve korake ispočetka.

❑ **Korak 2 Aktivnost 3**

U sljedećim aktivnostima (3-8) prikupljaju se podaci o informacijskoj imovini koja je potrebna za početak strukturalne procjene rizika. Koristit ćete profil ključne informacijske imovine (radna tabela 8, odlomak 2) za bilježenje tih podataka.

Za početak, zabilježite ime kritične informacijske imovine u radnoj tabeli 8, u stupcu (1).

❑ **Korak 2 Aktivnost 4**

U stupcu (2) od radne tabele 8 dokumentirajte Vaše razloge zašto je određena informacijska imovina važna. Nakon što to učinite, razmislite o sljedećim pitanjima:

- ✓ Zašto je ta informacijska imovina ključna za organizaciju?
- ✓ Da li ta informacijska imovina podliježe zakonskim propisima?

❑ **Korak 2 Aktivnost 5**

Napravite bilješke za opis u radnoj tabeli 8, u stupcu (3). Budite sigurni da ste definirali opseg informacijske imovine i da koristite kao što je dogovoreno, zajedničke definicije.

Prilikom opisa informacijske imovine razmotrite sljedeća pitanja:

- ✓ Koje je zajedničko ime za tu informacijsku imovinu (kako je ljudi unutar organizacije nazivaju)?
- ✓ Da li je ta informacijska imovina elektronska ili fizička (tj. da li je na papiru, ili oboje)?

Bilješke:

Budite sigurni da ste razmotrili i dokumentirali čimbenike koji su bitni ili potrebni za zaštitu informacijske imovine. Na primjer, ako je neka informacijska imovina zaštićena od strane nekog osiguravajućeg društva onda to treba dokumentirati.

Također bi ste trebali popisati koji procesi i servisi (usluge) koriste određenu informacijsku imovinu. Na primjer, uz bazu podataka o klijentima su vezani procesi kao što su kvaliteta proizvoda/usluga, isporuka i prodaja.

❑ **Korak 2 Aktivnost 6**

Identificirati i dokumentirati vlasnike za ključnu informacijsku imovinu. (kako bi lakše utvrdili tko je vlasnik, pogledajte gore navedene definicije.) Bilješke zapišite u radnu tabelu 8, u stupcu (4) .

Prilikom pisanja dokumentacije o vlasnicima informacijske imovine, razmotrite sljedeća pitanja:

- ✓ Tko u organizaciji, ima primarnu odgovornost za tu informacijsku imovinu?
- ✓ Tko je vlasnik poslovnih procesa s kojima je ta informacijsku imovinu u doticaju?
- ✓ Koji su poslovni procesi najbitnijih za tu informacijsku imovinu?
- ✓ Tko će biti odgovoran za vrednovanje informacijske imovine (novčano ili na drugi način)?
- ✓ Na koga će najviše utjecali ako informacijska imovina bude ugrožena?
- ✓ Postoje li različiti vlasnici za različite elemente podataka koje čine informacijsku imovinu?

Bilješke:

U mnogim slučajevima, informacijska imovina je u vlasništvu više od jedne organizacijske jedinice. Ako je to slučaj za Vašu informacijsku imovinu, budite sigurni da definirate dodatne vlasnike prilikom izvođenje procjene rizika. Definiranje profila informacijske imovine može biti nepotpuno ukoliko se ne uzmu u obzir sve organizacijske jedinice koje dijele informacijsku imovinu.

Osim toga, tijekom pisanja dokumentacije bitno je da se popišu stvarna imena vlasnika, pogotovo u organizacijama sa više zaposlenika tako da bude jasno tko je na kojoj poziciji i za što je odgovoran.

❑ **Korak 2 Aktivnost 7**

Dokumentirajte sigurnosne zahtjeve za povjerljivost, integritet i raspoloživost u radnoj tabeli 8, u stupcu (5). Potrebno je redom ispuniti cijelu radnu tabelu. Na desnoj strani radne tabele možete dodati nove zahtjeve ili specificirati postojeće zahtjeve detaljnije. Važno je zapamtiti da tijekom ovog koraka, ukoliko postoji više od jednog vlasnika informacijske imovine, onda je potrebno provesti popis svih vlasnika.

Sigurnosni zahtjevi za informacijsku imovinu su često izvedeni iz zakona i propisa. Zbog tog ukoliko definirate novi sigurnosni zahtjev, potrebno je provjeriti i zakonske propise i regulative koje se odnose na njega.

Bilješke:

Kategoriju pod nazivom "ostali" je predviđena za dodavanje ostalih sigurnosnih zahtjeva koji ne spadaju u prethodno navedene kategorije.

❑ **Korak 2 Aktivnost 8**

Odredite **najvažniji sigurnosni zahtjev** za Vašu informacijsku imovinu tako što ćete ga označiti sa 'X' u okviru pokraj pripadajuće kategorije u radnoj tabeli 8, u stupcu (6). Bitno je da pažljivo odaberete sigurnosni zahtjev, jer ćete ovu odluku koristiti kao zaštitu od potencijalnih rizika.

Tablica 8.3. - Implementacija: Korak 2, Aktivnosti 1 do 8

<table>
<tr><td>Allegro radna tabela 8</td><td colspan="3">PROFIL KLJUČNE INFORMACIJSKE IMOVINE</td></tr>
<tr><td>(1) Ključna imovina
Što je kritična informacijska imovina?</td><td colspan="2">(2) Obrazloženje za izbor
Zašto je ta informacijska imovina važna za organizaciju?</td><td>(3) Opis
Koji je odgovarajući opis za tu informacijsku imovinu?</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">(4) Vlasnik / vlasnici
Tko je vlasnik te informacijske imovine?</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">(5) Sigurnosni zahtjevi
Koji su sigurnosni zahtjevi za ovu informacijsku imovinu?</td></tr>
<tr><td>❑ Povjerljivost</td><td colspan="2">Samo ovlašteno osoblje može vidjeti ovu informacijsku imovinu, a oni su:</td><td></td></tr>
<tr><td>❑ Integritet</td><td colspan="2">Samo ovlašteno osoblje može mijenjati ovu informacijsku imovinu, a oni su:</td><td></td></tr>
<tr><td rowspan="2">❑ Dostupnost</td><td colspan="2">Ova informacijska imovina mora biti na raspolaganju za određeno osoblje kako bi mogli raditi svoj posao, a oni su:</td><td></td></tr>
<tr><td colspan="2">Ova informacijska imovina mora biti na raspolaganju _____ sati, _____ dana / tjedan, _____ tjedana / godišnje.</td><td></td></tr>
<tr><td>❑ Ostalo</td><td colspan="2">Na ovu informacijsku imovinu se\odnose posebni zakonski propisi za zaštitu, a oni su:</td><td></td></tr>
<tr><td colspan="4">(6) Najvažniji sigurnosni zahtjevi
Koji je najvažniji sigurnosni zahtjev za tu informacijsku imovinu?</td></tr>
<tr><td>❑ Povjerljivost</td><td>❑ Integritet</td><td>❑ Dostupnost</td><td>❑ Ostalo</td></tr>
</table>

8.4. Korak 3 - Identificirati informacijsku imovinu

8.4.1. Pojmovi i definicije

- **Spremište informacijske imovine** – predstavlja sredstva na kojima se informacijska imovina pohranjuje, prenosi i obrađuje. Spremište informacijske imovine može biti sklopovska oprema, programi, operacijski sustavi, servisi i mreže (tehnologija). Informacija se na ovim spremištima nalazi u raznim datotekama i datotečnim sustavima. Bitno je spomenuti i ljude koji svojim intelektualnim vlasništvom (znanjem) posjeduju informacijsku imovinu.

8.4.2. Opća napomena

Spremišta informacijske imovine je potrebno zaštititi jer u njima informacije "žive" (tj. pohranjuju, prenose i obrađuju). Upravo radi toga na tim mjestima možemo implementirati razne sigurnosne zaštite i kontrole kako bi osigurali Vašu informacijsku imovinu. Kao što smo spomenuli spremišta mogu biti razna tehnološka sredstva (sklopovska oprema, programi, operacijski sustavi, servisi i mreže) ali mogu također biti i fizička sredstva kao što su komad papira ili osoba koja je važna za organizaciju. Ljudi predstavljaju posebno važna spremišta informacijske imovne s obzirom na njihovo znanje i osjetljivim ili povjerljivim informacijama. Osoba koja dobije tu informaciju, u suštini postaje "spremište", te se ona mora uzeti u obzir prilikom procjene rizika za informacijsku imovinu. U nekim slučajevima kada osoba posjeduje ključne organizacijske informacije (npr., kao što dizajneri proizvoda), njihova nedostupnost može otežavati pripadajuće poslovne procese. Zbog toga je potrebno identificirati ove rizike i, te zatim definirati preventivne mjere.

Postoje tri vrlo važne stavke u procjeni rizika za informacijsku imovinu koje moramo sagledati, a one su:

- ✓ Način na koji je informacijska imovina zaštićena ili osiguran u spremištima. Na primjer, kako bi zaštitili bazu podataka na kojoj se nalaze informacije o klijentima? Jedan od mogući rješenja je zaštita pristupa neovlaštenim osobama, a ovlaštene osobe podijeliti na grupe i dodijeliti im različitu razinu prava.
- ✓ Stupanj sigurnosti informacijske imovine u spremištima je proporcionalan implementiranim kontrolama i mjerama zaštite.
- ✓ Svaka ranjivosti ili prijetnja spremištima informacija predstavlja direktnu prijetnju informacijskoj imovini. To može biti slučaj s ljudima, ako zaposlenik

- ✓ svojom voljom ode ili dobije otkaz, sa njim odlazi i njegovo intelektualno vlasništvo (znanje), zbog toga je potrebno sve dokumentirati.

Prilikom procjene rizika informacijske imovine potrebno je imati popis svih spremišta informacijske imovine ali i detaljniji opis njihove okoline u kojoj se nalaze. Bitno je naglasiti u nekim slučajevima informacijska imovina ne nalazi u spremištima unutar organizacije, tj. organizacije najčešće koriste "outsourcing" tj. njihova ključna imovina se može nalaziti izvan organizacije. Na primjer, mnoge organizacije koriste "outsourcing" kod pružanja nekih IT usluga. Zbog toga ako Vaša organizacija koristi "outsourcing" i usluge druge organizacije onda je potrebno da se sklopi ugovor u kojem će biti jasno definirano da je organizacija koja pruža usluge ujedno i odgovora za zaštitu i sigurnost Vaše informacijske imovine koju koristi.

8.4.3. Upute i aktivnosti

U trećem koraku ima samo jedna aktivnost:

❑ **Korak 3 Aktivnost 1**

Koristeći mapu rizične sredine informacijske imovine (radne tabele 9a, 9b, i 9c, odlomak 2) potrebno je popisati i opisati spremišta informacijske imovine:

- ✓ Koristite radnu tabelu 9a za identifikaciju i opis **tehnički** spremišta informacijske imovine, i to unutarnje (koje kontrolira i nadzire organizacija) ali i vanjske (izvan organizacije).
- ✓ Koristite radnu tabelu 9b za identifikaciju i opis **fizički** lokacija gdje se nalazi informacijska imovina (unutar i izvan organizacije).
- ✓ Uz pomoć radne tabele 9c popišite **ljude** koji znaju ili imaju pristup informacijskoj imovini (unutar i izvan organizacije).

Počnite s radnom tabelom 9a i redom dovršite ostale radne tablice, ako je moguće uz što više detalja. Koristite tablice (uputstvo za spremišta informacijske imovine (1-3)) kako bi što lakše i preciznije definirali spremišta informacijske imovine. Ovaj korak bi trebali raditi u grupi kako bi što detaljnije i preciznije definirali mape rizične sredine informacijske imovine.

Bilješke:

Potrebno je dokumentirati sve vlasnike spremišta informacijske imovine (kad god je to moguće). Prilikom izrade ove aktivnost najbolje bi bilo da budete u kontaktu s vlasnicima informacijske imovine kako bi skupili što preciznije i detaljnije informacije.

Dobro bi bilo popisati i sve vlasnike na svim razinama (dakle "odgovorne odgovornih") i sve njihove radne pozicije. Ovdje ne smijemo zaboraviti važnost vanjskih suradnika i osoblja koje ima kontakt sa našom informacijskom imovinom.

Tabela 1: Uputstvo za spremišta informacijske imovine – Tehnička

Vrsta spremišta	Pitanja koja je potrebno razmotriti
Tehnički **(** *pogledajte radnu tabelu 9a* **)**	***Unutarnji*** ❑ Koji informacijski sustavi ili procesi koriste tu informacijsku imovinu? ***Primjer:*** • ***Baza podataka za dobavljače (informacijska imovina) ima integriran sustav za plaćanje njihovih računa.*** ❑ Koji automatizirani procesi se oslanjanu na tu informacijsku imovinu? ***Primjer:*** • ***Plaćanje računa (proces) zahtijeva podatke o dobavljačima iz baze podataka (informacijska imovina) i za to postoji automatiziran sustav za plaćanje.*** ❑ Na kojoj sklopovskoj opremi se može naći ova informacijska imovina? Razmislite o sljedećim pitanjima: • Ako se informacijska imovina koristi u sustavima, aplikacijama ili procesima, na kojoj sklopovskoj opremi se ona izvršava? ***Primjer:*** • ***Baza podataka o dobavljačima se nalazi na "DIAMOND" serveru.*** ***Vanjski*** ❑ Postoje li vanjski kupci ili partneri koji bi mogli imati pristup i pravo korištenja informacijske imovine? ***Primjer:*** • ***Bazu podataka za plaće (informacijska imovina) koristi sustav za upravljanje plaćama koju vodi dobavljač.*** ❑ Da li postoje automatizirani procesi koji se koriste od strane kupaca ili poslovnih partnera, a da se odnose na informacijsku imovinu? ***Primjer:*** • ***Dobavljača medicinskih instrumenata koristi informacije iz baza podatka (informacijska imovina) prilikom pristupa organizacijskom inventaru kako bi odredio veličinu sljedeće pošiljke.*** ❑ Na kojoj klijentovoj ili partnerovoj sklopovskoj opremi se može naći ova informacijska imovina? Razmislite o sljedećim pitanjima: • Ako se informacijska imovina koristi od strane vanjskih klijentovih ili partnerski sustava, aplikacija ili procesa, na koju se onda sklopovsku opremu ona odnosi? ***Primjer:*** • ***Dobavljačev "OMEGA" server.*** • ***Dobavljačeva "xyz" lokalna mreža.***

Tabela 2: Uputstvo za spremišta informacijske imovine – Fizička

Vrsta spremišta	Pitanja koja je potrebno razmotriti
Fizički **(** *pogledajte radnu tabelu 9b* **)**	***Unutarnji*** ❑ Postoje li druga mjesta osim tehničkih sredstava, gdje ova informacijska imovina prisutna? Razmislite o sljedećim pitanjima: • Da li ljudi često zapisuju ove informacije na papir ili ih čuvaju na svojim radnim stolovima? • Da li postoje papirne kopije informacijske imovine koja je pohranjena? • Da li ljudi koriste papirnati oblik transakcija koje uključuju informacijsku imovinu? • Da li postoje fizičke prostorije za pohranu informacijske imovine u fizičkom obliku? ***Primjer:*** • ***Podaci o pacijentu su pohranjeni datotekama u sobi koja se nalazi na drugom katu.*** • ***Doktori imaju kopirane papirnate zapise svojih pacijenata pohranjene u radnim stolovima.*** ***Vanjski*** ❑ Ima li mjesta izvan organizacije, osim o tehničkim imovine, gdje se ova informacija imovine postoji? Razmislite o sljedećim pitanjima: • Da li partneri često pišu informacije na papiru i da li ih nose sa sobom? • Postoje li papirnate koji je informacijske imovine koja se pohranjuje ili dijeli sa drugim organizacijama? • Da li informacijsku imovinu koriste kupci, partneri ili dobavljači u transakcijama? • Postoje li fizičke prostorije u drugim organizacijama gdje bi se informacijska imovina mogla pohraniti u fizičkom obliku? ***Primjer:*** • ***Dizajn proizvoda je podijeljen sa značajnim klijentima u razvojnom stadiju.*** • ***Papirnati dokumenti su pohranjeni kod vlasnika objekta koji se i brine za njih.*** • ***Računalne backup trake su pohranjene kod "third-party" ugovorne strane koja se i brine o njima.***

Tabela 3: Uputstvo za spremišta informacijske imovine – Ljudi

Vrsta spremišta	Pitanja koja je potrebno razmotriti
Ljudi **(** *pogledajte radnu tabelu 9c* **)**	***Unutarnji*** ❑ Koji ljudi bi mogli imati detaljno znanje o toj informacijskoj imovini? Razmislite o sljedećim pitanjima: • Da li se informacijska imovina smatra intelektualnim vlasništvom ako je neka osoba zna? • Da li je informacijska imovina osjetljiva ili povjerljiva, i da li bi trebala biti poznata određenim pojedincima u organizaciji? • Koji bi ljudi mogli imati pristup informacijskoj imovini, i da li je smiju zadržati ili objaviti, ako su je vidjeli? ***Primjer:*** • ***Pero Perić je razvio novu formulu za boju, za našu novu liniju automobila. Samo on zna formulu i nikada je nije zapisao.*** • ***Ivo Ivić je tajnik u medicinskom odjelu u kojem se nalazi dokumentacija o bolesnicima. Iako mu nikad nije bio dozvoljen direktan pristup podacima o bolesnicima, on često vidi podatke o pacijentima dok kruže po odjelima.*** ***Vanjski*** ❑ Koji ljudi izvan organizacije poznaju tu informacijsku imovinu? Razmislite o sljedećim pitanjima: • Da li se informacijska imovina smatra intelektualnim vlasništvom i da li partneri, davatelji usluga, konzultanti ili klijenti smiju saznati za nju? • Postoji li netko iz vana tko bi mogao imati pristup toj informacijskoj imovini? Da li je mogu zadržati ili objaviti, ako su je vidjeli? ***Primjer:*** • ***Potpredsjednik marketinga često raspravlja o specifikacijama novog proizvoda kojeg nudi najvećim klijentima organizacije.***

Tablica 8.4. - Implementacija: Korak 3, Aktivnost 1

Allegro radna tabela 9a	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (TEHNIČKE)**
UNUTARNJE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	
VANJSKE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	

Allegro radna tabela 9b	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (FIZIČKE)**
UNUTARNJE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	
VANJSKE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	

Allegro radna tabela 9c	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (LJUDI)**
UNUTARNJE OSOBLJE	
IME ILI ULOGA / ODGOVORNOST	**ODJEL ILI JEDINICA**
1.	
2.	
3.	
4.	
VANJSKO OSOBLJE	
DOBAVLJAČ, PRODAVAČ, ITD.	**ORGANIZACIJA**
1.	
2.	
3.	
4.	

8.5. Korak 4 – Identificirati kritična područja

8.5.1. Pojmovi i definicije

- **Interesno područje** – predstavlja opisnu izjavu da su detalji o stanju iz realnog vremena ili situacija koja bi mogle utjecati na informacijsku imovinu u Vašoj organizaciji.

8.5.2. Opća napomena

U četvrtom koraku se početak definiranja profila informacijske imovine. Rizik predstavlja kombinaciju prijetnje i utjecaja prijetnje kao rezultata (posljedica). U četvrtom koraku bi trebali koristiti brainstorming metodu kako bi definirali i popisali moguće uvjete i situacije koje bi mogu ugroziti Vašu informacijsku imovinu. U ovom koraku je potrebno popisati sva interesna područja kako bi u petom koraku mogli u potpunosti definirati rizične profile. Interesna područja ili područja koja su pod utjecajem rizika su najčešće jedinstvena za svaku organizaciju. Svrha ovog koraka nije da se popiše cijela lista mogućih scenarija prijetnje za informacijsku imovinu, već je cilj ukratko popisati scenarije koji Vam prvi "padnu na pamet" te ih dokumentirati.

Prilikom pisanja dokumentacije za ovaj korak, razmislite o različitim sudionicima, motivima ali i posljedicama za pojedina interesna područja. Pokušajte biti što više konkretni prilikom pisanja dokumentacije. Također razmislite o mogućim prijetnjama za sigurnosne zahtjeve Vaše informacijske imovine u stvarnim situacijama.

8.5.3. Upute i aktivnosti

U četvrtom koraku ima samo jedna aktivnost:

❑ **Korak 4 Aktivnost 1**

Kako bi izvršili ovu aktivnost morate koristiti radne tabele (mape rizične sredine informacijske imovine) kao referencu ali i radnu tabelu rizika informacijske imovine (radna tabela10, dodatak A) kako bi mogli definirati interesna područja.

Kako bi uspješno definirali interesna područja, slijedite iduće korake:

1. Koristeći mape rizične sredine informacijske imovine, pregledajte sve spremnike Vaše informacijske imovne i razmislite o mogućim prijetnjama.
2. Dokumentirajte svako interesno područje koje identificirate u radnoj tabeli rizika informacijske imovine. U radnoj tabeli zabilježite ime informacijske imovine i to dokumentirajte područja interesa što je moguće detaljnije. Na radnom listu, napišite naziv informacija imovine i dokument područje interesa u što više detalja. Popunite u radnoj tabeli stupce koji se zovu "Informacijska imovina" i "interesno područje" i ne zaboravite da koristite odvojene radne tabele za svako interesno područje koje identificirate. Proširite svoju dokumentaciju o interesnim područjima kako bi mogli kreirati scenarije prijetnji. Scenarij prijetnji predstavlja detaljniji opis svojstava prijetnji.
3. Kako budete dobili potpuni uvid u interesna područja potrebno je u potpunosti popuniti radnu tabelu deset. Preostala procjena rizika će biti završena u sljedećim koracima.
4. Sagledajte sva spremišta informacijske imovine koja se nalaze u mapama rizične sredine informacijske imovine i nastojite dokumentirati što više interesnih područja. Zapamtite, na jednom spremištu informacijske imovine je moguće identificirati više interesnih područja.

Bilješke:

Kako bi definirali sve rizike Vaše informacijske imovine morate koristiti radnu tabelu (*rizici informacijske imovine*). U svakoj radnoj tabeli će se nalaziti jedinstveni rizik, zbog toga će te morati popuniti više ovih tabela prilikom procjene rizika.

Razmotrite sljedeći primjer za interesna područja:

Interesno područje
Ukoliko prava pristupa na glavnim bazama podataka nisu jasno i korektno definirana, može doći do situacije da osoba slučajno pristupi povjerljivoj medicinskoj dokumentaciji drugog zaposlenika.
Ukoliko baze podataka na kojima se nalaze podaci o plaćama zaposlenika nemaju definiranu kontrolu pristupa, u tom slučaju je moguće da će druga osoba slučajno pogledati visine plaća i načine isplate ostalih zaposlenika.
Ivo Ivić je jedini zaposlenik koji poznaje detaljne specifikacije u proizvodnom odjelu, i te specifikacije nikad nisu dokumentirane. Ivo Ivić je spominjao da će napustiti poduzeće, i ako on to učini cijeli proizvodni odjel će stati sa radom jer glavne specifikacije više nisu dostupne tj. nisu nikad bile dokumentirane.
Medicinska dokumentacija bolesnika koju je medicinska sestra ostavila na radnom stolu biva promijenjena od strane neovlaštene osobe jer nije bilo sigurnosne kontrole i zaštite.

8.6. Korak 5 – Prepoznavanje scenarija prijetnji

8.6.1. Pojmovi i definicije

- **Prijetnja** – predstavlja pokazatelj potencijalnih neželjenih događaja. Prijetnja se odnosi na situaciju (ili scenarij) u kojoj osoba može učiniti nešto nepoželjno (napadač pokreće DoS napad protiv organizacijskog e-mail servera) ili prirodna nepogoda koja može izazvati neželjeni ishod (požar koji može oštetiti sklopovsku opremu na kojoj se nalazi informacijska imovina).
- **Scenarij prijetnji** – scenarij prijetnji predstavlja situaciju u kojoj informacijska imovina može biti ugrožena. Scenarij se sastoji od sudionik, motiva, sredstava (pristupa) i neželjenih ishoda. Scenarij prijetnji predstavlja pojednostavljene načina uz pomoć kojih se može utvrdi da li postoji rizik koji bi mogao utjecati na Vašu informacijsku imovinu.
- **Stablo prijetnji** – koristi se struktura stabla za vizualno predstavljanje raspona scenarija prijetnji. Uz pomoć stabla prijetnji imate bolji uvid u spektar potencijalnih prijetnje, ali i načine kako da se zaštitite i osigurate od njih.

8.6.2. Opća napomena

U četvrtom koraku ste dokumentirati interesna područja za Vašu informacijsku imovinu, a petom koraku ćete interesna područja proširiti sa scenarijima prijetnji koji detaljnije opisuju svojstva rizika. Kako bi proširili interesna područja sa scenarijima prijetnji prvo morate razumjeti osnovne komponente prijetnja. Prijetnja ima sljedeća svojstva:

- ✓ Imovina – predstavlja sve ono što je vrijedno za poslovni sustav.
- ✓ Pristup / sredstva – predstavlja način pristupa i vrstu sredstva prilikom pristupa imovini (tehnička sredstva, fizički pristup). Pristup se odnosi samo na ljudske učesnike.
- ✓ Učesnik – tko ili što može kršiti sigurnosne zahtjeve (povjerljivost, integritet, dostupnost) informacijske imovine.
- ✓ Motiv – učesnikov razlog (npr., namjerno ili slučajno). Motiv se odnosi samo na ljudski učesnike.
- ✓ Ishod – neposredni rezultat (otkrivanje, promjena, uništenja / gubitka, prekid) narušavanja sigurnosnih zahtjeva informacijske imovine.

Raspon scenarija prijetnji može se prikazati vizualno u obliku strukturalnog stabla kako bi opisali svojstva prijetnji. Ovo strukturalno stablo se često naziva i stablo prijetnji. U Allegro

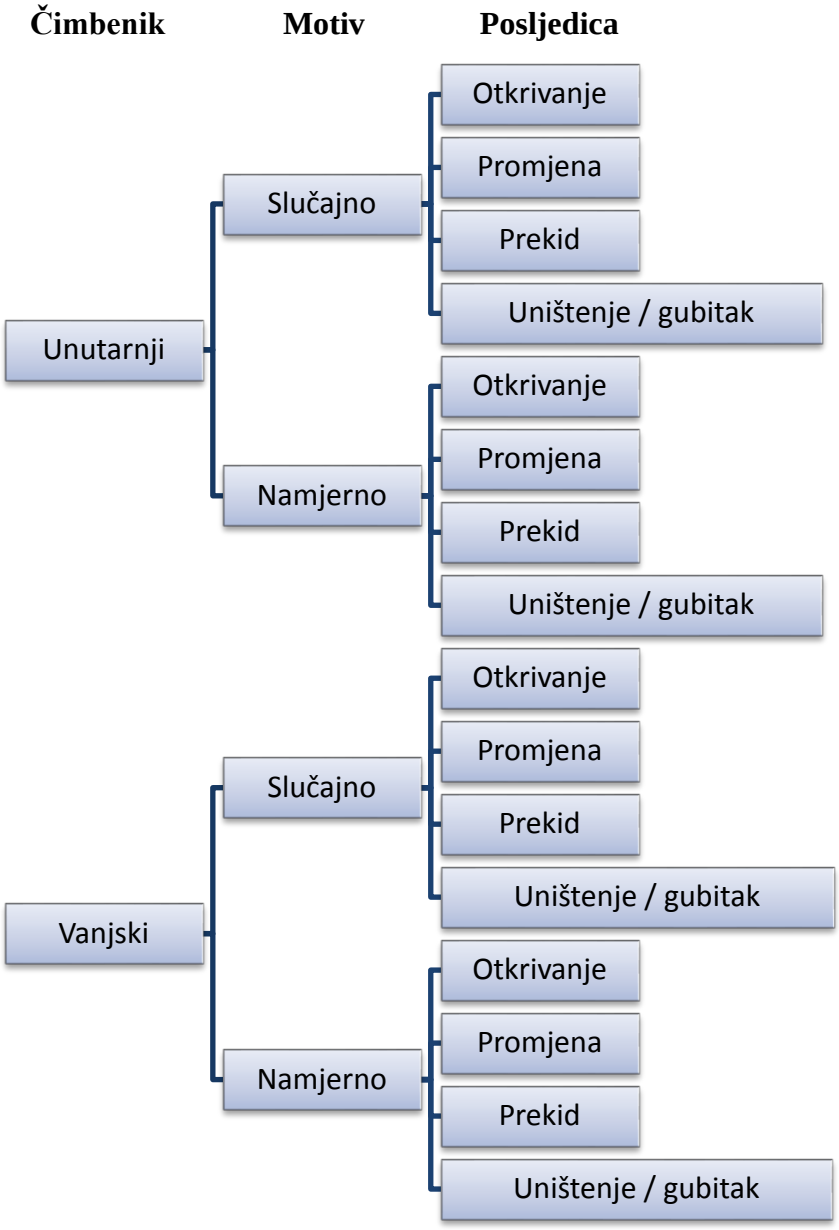
metodi postoje četiri stabla prijetnji koja se moraju uzeti u obzir. Ova stabala su opisana u tabeli 4 i grafički prikazana u tabeli 5.

Tabela 4: Opis stabla prijetnji

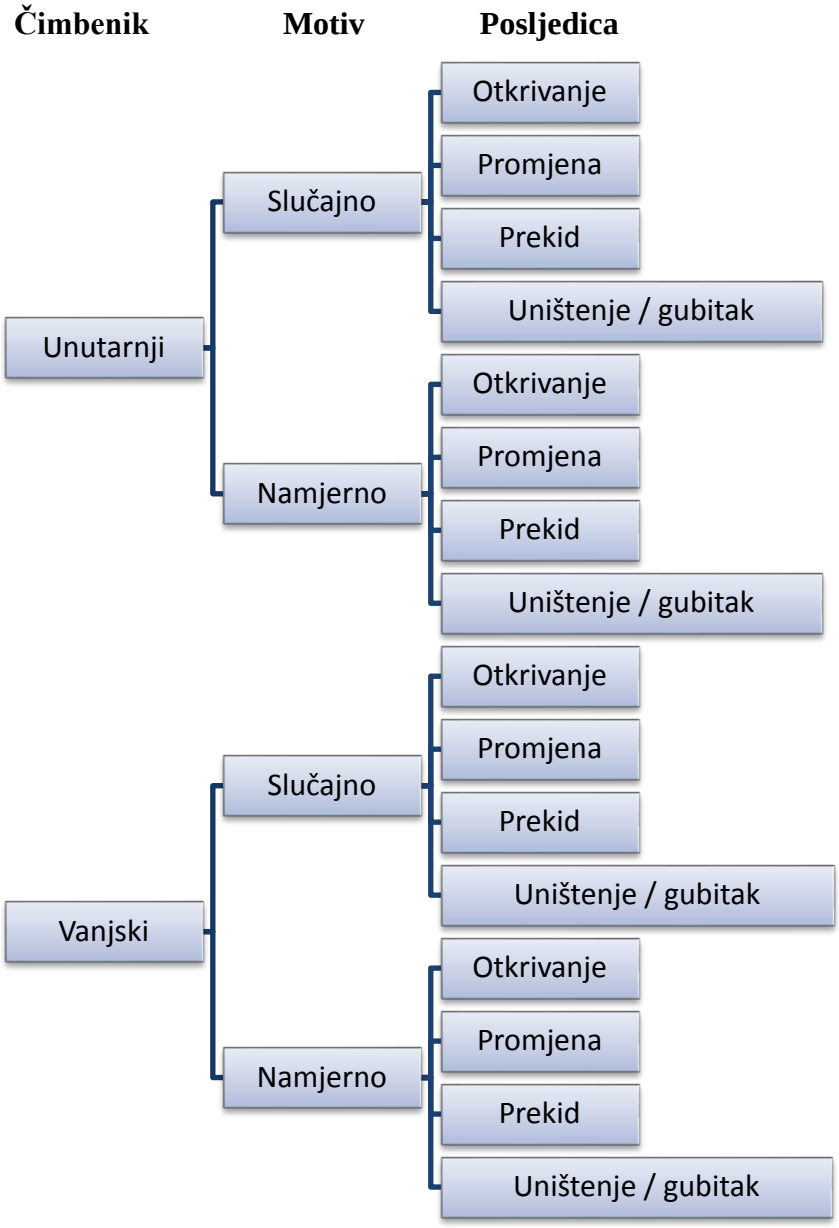
Stablo prijetnji	Definicija
Čovjek koristi tehnička sredstva	Prijetnje iz ove kategorije su nastale putem organizacijske tehničke infrastrukture ili izravnim pristupom spremniku (tehnička sredstva) na kojem je smještena informacijska imovina. To se može desiti slučajno ili namjerno od strane čovjeka.
Čovjek koristi fizička sredstva	Prijetnje iz ove kategorije su najčešće fizički pristupi informacijskoj imovini. Učesnik ih može izazvati na dva načina: slučajno ili namjerno.
Tehnički problemi	Prijetnje u ovoj kategoriji su organizacijski problem s informacijskom tehnologijom i sustavima. Ovdje spadaju greške programske i sklopovske opreme, maliciozni kod (npr. virusi), i drugi međusobno zavisni sustavni problemi.
Ostali problemi	Prijetnje u ovoj kategoriji su problemi ili situacije koje su izvan kontrole organizacije. Ova kategorija prijetnji uključuje prirodne nepogode (npr. poplave, potresi), te međuzavisnosti rizika koja obuhvaća i nedostupnost ključne informacijske imovine (npr. napajanje).

Tabela 5: Grafički prikaz stabala prijetnji

Slika 8.1. - Ljudski čimbenici prilikom korištenja tehnički uređaja

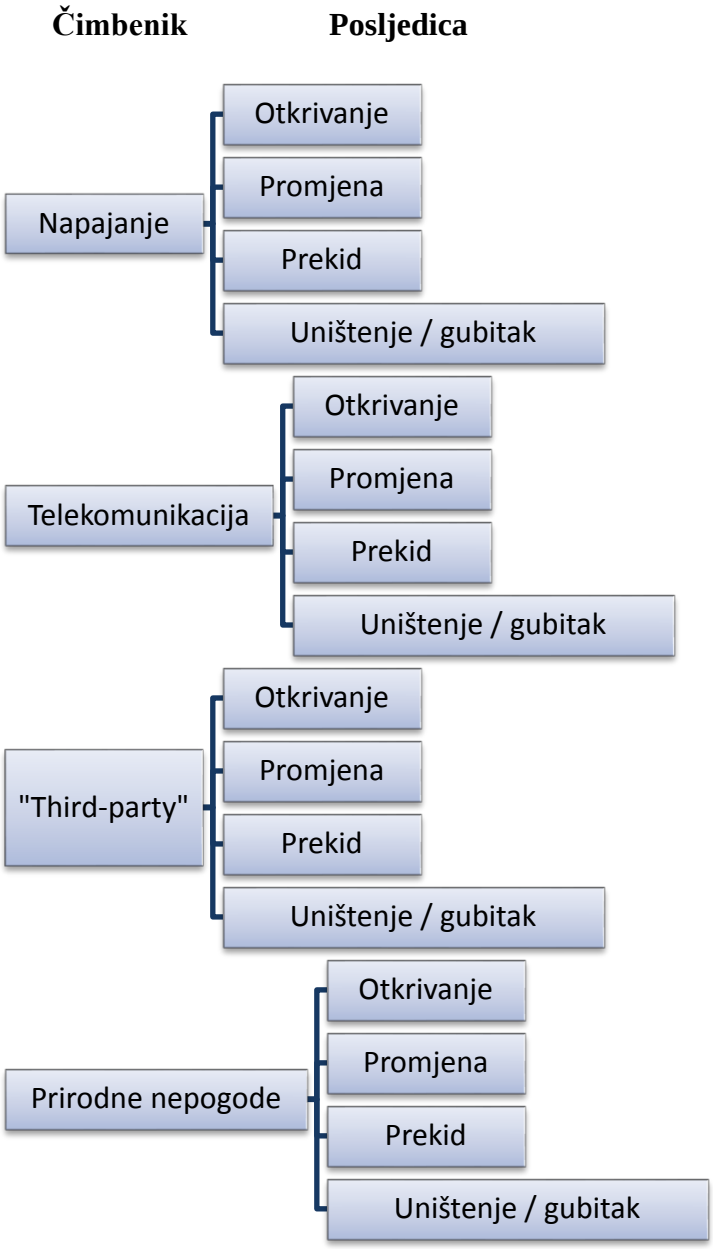


Slika 8.2. - Ljudski čimbenici prilikom korištenja fizički uređaja



Slika 8.3. - Tehnički problemi

Slika 8.4. - Ostali problemi



Scenarij prijetnji proizlaze iz Vaših interesnih područja, što bi trebalo biti vidljivo i na stablima prijetnji (rezultat u obliku puta na stablu). Uz pomoć tablice prijetnji trebate prepoznati sve rizične putove te za njih detaljno definirati kontrole i zaštitu. Obavezno sagledajte sve moguće prijetnje kroz sva stabla prijetnji. U koraku 5 ćete koristiti niz upitnika uz pomoć kojih ćete lakše identificirati scenarije prijetnji.

8.6.3. Upute i aktivnosti

Peti korak ima tri aktivnosti:

❑ **Korak 5 Aktivnost 1**	U ovoj aktivnosti, identificirat ćete dodatne scenarije prijetnji koji nisu bili definirani (prepoznati) u interesnim područjima. Da biste to učinili, morat ćete koristiti upitnike za scenarije prijetnji. Postoji jedan upitnik za svaku vrstu spremnika (tehnički, fizički i ljudi). Svaki upitnik sadrži zbirku scenarija koji su osmišljeni kroz postavljena pitanja kako bi Vam pomogao da identificirate dodatne prijetnje. Kako bi ste završili ovu aktivnost potrebno je koristiti informacije iz mapa rizični sredina informacijske imovine kao vodič, koje ste definirali u koraku 4 (radne tabele 9a, 9b i 9c). **5.** Nastavite sa odgovaranjem na "*Upitnik scenarija prijetnji (1) – Tehnički spremnici*". Ove spremnike informacijske imovine ste već definirali u radnoj tabeli 9a, sada je potrebno da odgovorite na navedena pitanja. **6.** Nastavite sa odgovaranjem na "*Upitnik scenarija prijetnji (2) – Fizički spremnici*", i "*Upitnik scenarija prijetnji (3) – Ljudi*". Ove spremnike informacijske imovine ste već definirali u radnim tabelama 9b i 9c, sada je potrebno da odgovorite na navedena pitanja. **Bilješke:** Imajte na umu da postoji mogućnost više od jednog "Da" odgovora za različite uvjete, u tom slučaju zaokružite više od jednog ako je potrebno.

❑ **Korak 5 Aktivnost 2**	U ovoj aktivnosti je potrebno da popunite radnu table (rizici informacijske imovine) za sve definirane scenarije prijetnji koje ste prepoznali dok ste odgovarali na upitnike. 1. Pregledajte sve svoje odgovore iz upitnika o scenarijima prijetnji. Za sve scenarije prijetnji za koje ste zaokružili “Ne” nije više ništa potrebno poduzeti. 2. Za sve "Da" odgovore, definirajte novu radnu tablicu (rizici informacijske imovine). Odgovorite na dijelove od (1) do (5) na ovoj radnoj tabeli. Ako ustanovite da ste odgovorili "Da" na pitanje, ali se ne možete sjetiti odgovarajućih situacija iz stvarnog života, nastavite dalje. 3. Nastavite sve dok postoji barem jedna radna tabela (rizici informacijske imovine) za svaki “Da” odgovor za bilo koji od upitnika scenarija prijetnji. **Bilješke:** Moguće je da ste imali više od jedne stvarne životne situacije za koju ste odgovorili sa “Da”. Ako je to slučaj, trebate napraviti što je više moguće radnih tabela (rizici informacijske imovine) za svaki “Da” odgovor.

❑ **Korak 5 Aktivnost 3**	Ova aktivnost nije obavezna za profile rizika informacijske imovine. U slučaju da to odlučite napraviti, onda je to potrebno napraviti za sve profile. Također možete dodati i "*vjerojatnost"* prilikom opisa scenarija prijetnji koje ste definirali u radnoj tabeli (*rizici informacijske imovine*). Vjerojatnost Vam pomaže da odredite koji od scenarija su više vjerojatni, što je kasnije bitno za određivanje prioritetnih aktivnosti za smanjenje rizika. Budući da je vrlo teško točno kvantificirati vjerojatnost (posebno s obzirom na sigurnosne propuste i događaje), upravo zbog toga je vjerojatnost u ovoj procjeni izražena kvalitativno (visoko, umjereno, nisko). Drugim riječima, morate odrediti da li postoji jaka (velika) vjerojatnost da će se scenarij dogoditi, srednje vjerojatnost (umjerena) ili mala (niska) vjerojatnost da će se scenarij dogoditi. Ako se odlučite da napravite ovu procjenu, trebali biste provjeriti vjerojatnost u stupcu (6) za sve rizike koje ste definirali. **Bilješke:** Ako se odlučite koristiti "vjerojatnost", onda morate definirati vjerojatnost za svaku prijetnju informacijske imovine.

Upitnik za scenarij prijetnji 1	**Tehnički spremnici**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na tehničkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:
Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više tehničkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:
Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Upitnik za scenarij prijetnji - 1 (nastavak)	**Tehnički spremnici**

Scenarij 3:

U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovine na bilo kojem tehničkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- nenamjerno otkrivanje informacijske imovine
- nenamjerna promjena informacijske imovine
- nenamjerni prekid dostupnosti informacijske imovine
- nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine

Aplikacijski kvar	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Pad sustava iz poznatih ili nepoznatih razloga	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Kvar sklopovske opreme	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Izvršenje malicioznog koda (kao što su virusi, crvi, Trojanski konj ili back door)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prekid napajanja za tehničke spremnike informacijske imovine	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Problemi s telekomunikacijom	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Pojava drugih “third-party” problema.	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**

Upitnik za scenarij prijetnji - 2	**Fizički spremnici**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na fizičkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:

Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više fizičkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:

Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Upitnik za scenarij prijetnji - 2 (nastavak)	**Fizički spremnici**

Scenarij 3:

U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovinu na bilo kojem fizičkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- nenamjerno otkrivanje informacijske imovine
- nenamjerna promjena informacijske imovine
- nenamjerni prekid dostupnosti informacijske imovine
- nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine

Pojava drugih "third-party" problema.	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**

Upitnik za scenarij prijetnji – 3	**Ljudi**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koju znaju ključni ljudi organizacije. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:

Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik ima detaljno znanje o Vašoj informacijskoj imovini (slučajno ili namjerno), što bi moglo rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?[8]	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?[9]	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?[10]	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:

Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

[8] Ovaj slučaj je malo vjerovatan, ali ako je ključna osoba u Vašoj organizaciji imala detaljno znanje o informacijskoj imovini rizik se može pojaviti.

[9] Ovaj slučaj se odnosi na dostupnost informacija. Ako je ključna osoba u Vašoj organizaciji imala detaljno znanje o informacijskoj imovini i ako to znanje ili informacija više nisu dosptuni to bi moglo negativno utjecati na poslovanje organizacije.

[10] Ako je ključna osoba u Vašoj organizaciji imala detaljno znanje o informacijskoj imovini i ako to znanje ili informacija nisu dokumentirani to moglo negativno utjecati na poslovanje organizacije.

8.7. Korak 6 – Identifikacija rizika

8.7.1. Pojmovi i definicije

- **Izjava o utjecaju** – predstavlja opisanu izjavu u kojoj je detaljno opisano koliki je utjecaj (posljedica) nakon što se scenarij prijetnje realizirao. Izjava o utjecaju predstavlja posljedicu izvršenja scenarija prijetnje.
- **Rizik** – predstavlja mogućnost trpljenja štete ili gubitka. Rizik se odnosi na situacije u kojima osoba može učiniti nešto nepoželjno ili prirodna pojava koja može izazvati nepoželjan ishod, što rezultira negativan učinak ili posljedicu. Rizik se sastoji od
  - ✓ događaja,
  - ✓ posljedice i
  - ✓ nesigurnosti.

8.7.2. Opća napomena

Nakon što ste identificirali sve prijetnje i posljedice za organizaciju, sad možete izračunati jednadžbu za rizik. To se može ilustrirati na sljedeći način:

Prijetnja (uvjet) + Utjecaj (posljedica) = Rizik

[Korak 4 i 5] + [Korak 6] = Rizik

8.7.3. Upute i aktivnosti

Šesti korak ima jednu aktivnost:

❑ **Korak 6 Aktivnost 1**

U ovoj aktivnosti, određujete kako će scenariji prijetnji koje ste definirali u radnim tabelama (*rizici informacijske imovine*) utjecati na Vašu organizaciju.

1. Za sve scenarije prijetnji koji ste definirali u radnim tabelama (*rizici informacijske imovine*), trebate odrediti kakva će posljedica biti za Vašu organizaciju ako se scenarij prijetnje dogodi. To je posljedica prijetnji koja upotpunjuje jednadžbu za izračun rizika.
2. Dokumentirajte najmanje jednu od posljedica u odlomku (7) iz radne tabele (*rizici informacijske imovine*). Naknadno možete dokumentirati ostale posljedice ako je potrebno. Budite što više konkretni. Također, obratite pozornost na "ishode", koje ste uzeli u obzir u koraku 5 (aktivnost 5).

U sljedećoj tabeli je navedeno nekoliko primjera.

Scenarij prijetnji	Posljedica
Pogrešno definirana prava pristupa podacima omogućuju da zaposlenici pristupe medicinskoj dokumentaciji ostalih zaposlenika.	Medicinska dokumentacija zaposlenika je javno objavljena, što je rezultiralo tužbu protiv organizacije, a zatim i novčanu kaznu od 200 000 KN.
Ivo Ivić je jedini zaposlenik koji detaljno poznaje specifikacije proizvodnje koje nikad nisu bile dokumentirane. Ivo Ivić je spominjao da bi mogao napustiti poduzeće, ako to učini cijeli proizvodni pogon će stati zbog nedostatka informacija.	Proizvodnja je stala, što je rezultiralo dnevni gubitak od 5 000 000 KN a zatim i gašenje tvrtke.
Medicinski zapisi pacijenata su izmijenjeni od strane neovlaštene osobe zbog slabih sigurnosnih mjera i zaštite.	Pogrešne doze lijekova (ili netočni lijekovi) je rezultiralo smrću pacijenta, što je rezultiralo tužbom (kaznama) i gubitkom ugleda.

8.8. Korak 7 – Analiza rizika

8.8.1. Pojmovi i definicije

- **Vrijednost utjecaja** – kvalitativna vrijednost uz pomoć koje je upisan opseg utjecaja na organizaciju kada se scenarij prijetnje izvrši. Vrijednost utjecaja je izvedena iz kriterija mjerenja rizika.

8.8.2. Opća napomena

U ovom koraku ćete kvalitativno procijeniti prijetnje koje mogu naštetiti Vašoj informacijskoj imovini. Kako bi uvidjeli koje rizike treba ublažiti odmah, potrebno je dodijeliti vrijednosti prijetnjama (izvršiti bodovanje). Nakon toga u osmom koraku definiramo načine pristupa rizicima.

Analiza rizika je složen pothvat i za to je potrebno stručno znanje i detaljno poznavanje organizacije (njene informacijske imovine i poslovnih procesa). U ovoj aktivnosti, izračunat ćete relativni rizik koji predstavlja rezultat posljedica koje utječu na Vašu organizaciju u odnosu na relativnu važnost različitih interesnih područja. Drugim riječima, ako na područje "ugled" (koje je npr., najvažnije za Vašu organizaciju) velika posljedica od rizika, morati ćete poduzeti mjere da se rizik ublaži.

8.8.3. Upute i aktivnosti

U sedmom koraku imaju dvije aktivnosti:
Ove aktivnosti moraju biti izvedena za svaku radnu tabelu (*rizici inforamcijske imovine*). Možete napraviti ove aktivnosti odjednom za svaku radnu tabelu posebno ili da odradite aktivnost 1 za sve radne tabele, pa aktivnost 2, itd.

- **Korak 7 Aktivnost 1**

Započnite pregledom kriterija mjera rizika koje ste definirali u koraku 1, aktivnost 1. Fokusirajte se način kako ste definirali utjecaj na Vašu organizaciju (visoko, umjereno, nisko).

Počevši s prvim rizikom radne tabele, provjerite tvrdnje o posljedicama (ili izjava) koje ste dokumentirali.

Pomoću vodiča za kriterij mjera rizika ocijenite posljedice za svako interesno područje sa vrijednostima "visoko", "umjereno" ili "nisko" u stupcu (8) pod nazivom "Vrijednost". Ako ste napisali više od jedne tvrdnje za posljedicu, budite sigurni da ste ih uzeli sve u obzir prilikom dodjeljivanja vrijednosti. Potrebno je dokumentirati vrijednosti za svako interesno područje.

Razmotrite sljedeći primjer.

Scenarij prijetnji	Posljedice
Pogrešna dodjela prava pristupa rezultiralo je da član osoblja slučajno pristupi u medicinsku dokumentaciju drugom zaposlenika.	Medicinska dokumentacija zaposlenika je javno objavljena, što je rezultiralo tužbom protiv organizacije i novčanom kaznom od 100.000 KN.

Ove posljedice imaju izravan utjecaj na ugled organizacije, potencijalne novčane troškove, tužbe i kazne. Sljedeće vrijednosti su dodijeljene koristeći kriterije za mjerenje organizacijskih rizika.

Rizično područje	Vrijednost prijetnje
Ugled i klijentovo povjerenje	Umjereno
Financije	Nisko
Produktivnost	Nisko
Zdravlje i sigurnost	Nisko
Pravne i zakonske kazne	Visoko

Vrijednost "visoko" je dodijeljeno za pravne i zakonske kazne jer je organizacija postavila prag od 100 000 KN kao gornju granicu. Posljedica ima malen ili nikakav učinak na produktivnost, zbog toga je dodijeljena vrijednost "nisko".

❑ **Korak 7**
Aktivnost 2

U ovom koraku ćete izračunati relativni rizik, uz pomoć kojeg ćete analizirati rizik i definirati odgovarajuće strategije u organizaciji. Ovaj korak ćete napisati u dijelu radne tabele (*rizici informacijske imovine*) koji se naziva "Rezultat" u stupcu (8).

1. Izračunajte rezultat za svako interesno područje utjecaja, tako što ćete pomnožiti vrijednost prioriteta od interesnog područja sa vrijednošću prijetnje (pogledajte listu prioriteta za interesna područja koje ste definirali u koraku 1, aktivnost 2). Zatim zapišite vrijednost u stupcu **"rezultat"**. Vrijednost prijetnji su kvantitativne: Visoko - 3, Umjereno - 2, a Nisko - 1. Budite sigurni da vrijednosti budu konzistentne u svim radnim tabelama.
2. Izračunajte "ukupni rezultat" tako što ćete sabrati sve dobivene rezultate.
3. Razmotrite sljedeći primjer. U sljedećem primjeru je vidljivo da je su financije za organizaciju najvažnije interesno područje, dok je zdravlje i sigurnost najmanje važno. Vrijednost prijetnji su definirane u aktivnosti 1.

Interesno područje	**Prioritet**	**Vrijednost prijetnje**	**Rezultat**
Ugled	4	Umjereno (2)	**8**
Financije	5	Nisko (1)	**5**
Produktivnost	3	Nisko (1)	
Zdravlje i sigurnost	1	Nisko (1)	**1**
Pravo i zakoni		Visoko (3)	**6**
		Ukupni rezultat	**23**

Bilješke:

Rezultati koji su dobiveni u ovoj aktivnosti se koriste kao alat za dodjeljivanje prioriteta. Razlike između rezultata rizika nisu bitne. Drugim riječima, rezultat od 48 znači da je rizik od relativno veće važnosti za organizaciju nego rezultat od 25 (razliku od 13 bodova nije toliko bitna).

8.9. Korak 8 – Odabrati način pristupa

8.9.1. Pojmovi i definicije

- **Pristup ublažavanja** – predstavlja način na koji se organizacija namjerava pristupiti riziku. Organizacija ima sljedeće mogućnosti a one su:

  - ✓ *Prihvaćanje* - odluka koja je nastala tijekom analize rizika. Ovom odlukom organizacija prihvaća posljedice rizika i ništa ne poduzima. Prihvaćeni rizici i njihove posljedice bi trebali imati nizak utjecaj na organizaciju.
  - ✓ *Ublažavanje* - odluka koja je nastala tijekom analize rizika. Ovom odlukom organizacija provodi razne kontrole i postupke za ublažavanje posljedica koje su ostale od prijetnji čije su posljedice najčešće umjerene ili visoke.
  - ✓ *Odgađanje* - situacija u kojoj pristup organizacije nije ni prihvaćanje niti ublažavanje već želja organizacije za prikupljanje dodatnih informacija i obavljanje dodatne analize. Odgođeni rizici se redovito nadziru i ponovno vrednuju u nekom trenutku u budućnosti. Rizici koji su odgođeni najčešće nisu opasni za organizaciju, niti bi trebali značajno utjecati na poslovanje organizacije i u slučaju da se realiziraju.

- **Rezidualni rizik** – predstavlja preostali rizik koji je ostao nakon primjene jedne od vrsta pristupa ublažavanja (*prihvaćanje, ublažavanje, odgađanje*). Rezidualni rizik koji je preostao trebao bi biti prihvatljiv za organizaciju.

U koraku 8, uzmite u obzir rizike koje trebate ublažavati te odaberite način pristupa. Kako bi ovaj korak što točnije napravili morate sagledati prioritet rizika, tj. izabrati one rizike koji imaju najveću posljedicu za Vašu informacijsku imovinu. Odluke kao što su: prihvaćanje, ublažavanje ili odgađanje rizika su veoma važne. Ako bi rizik mogao ozbiljno ili značajno utjecati na organizaciju, ali je mala vjerojatnost da će se desiti, možda ga nećete htjeti ublažavati. Nažalost, ne postoji jasan i odlučan način koje rizike treba ublažiti. Često, tu odluku donose osobe koje dobro poznaju organizaciju i koje su uključene u procjenu rizika. Nakon što donesete odluku o ublažavanju rizika, morate razviti djelotvornu i učinkovitu strategiju ublažavanja. Odlučivanje o tome kako ublažiti rizik je kompleksan poduhvat i može zahtijevati raspravu s drugim kvalificiranim osobljem u Vašoj organizaciji. Činjenica da je vlasnik informacijske imovine jedna osoba, a skrbnik sredstava druga osoba, što znači da

obadvije strane moraju surađivati kako bi se stvorila najbolja strategija za pružanje ukupne zaštite.

Potreba za suradnju između poslovnih stručnjaka i osoblja za informacijske tehnologije ističu scenarij u kojem je vlasnik informacijske imovine drugačiji od skrbnika. Često, pravi vlasnici informacijske imovine su eksperti poslovnog sustava koji povjeravaju IT odjelu svoju tehničku infrastrukturu. Nažalost, ovi vlasnici često nisu svjesni svoje uloge i odriču se odgovornosti čuvanja svojih podataka. Dakle, oni prepuštaju IT odjelu da se u potpunosti brine o njihovoj informacijskoj imovini, i očekuju od njih da primjene svu potrebnu zaštitu i sigurnost.

Kao što se administratori brinu za informacijski sustav i tehničku infrastrukturu, tako IT odjel pruža potporu kako bi se poslovne funkcije u organizaciji izvele besprijekorno. Kako poslovne funkcije ovise o informacijskoj imovini, tako IT odjel igra važnu ulogu u implementaciji definirane strategije zaštite informacijske imovine. Zbog toga je neophodno definirati vlasnike informacijske imovine, i u taj cijeli proces procjene rizika uključiti IT odjel. Također treba biti jako pažljiv prilikom dodjeljivanja informacijske imovine njenim vlasnicima, jer često je slučaj da neku informacijsku imovinu posjeduje više vlasnika. Pored toga treba jasno definirati pravo pristupa i kontrole nad spremištima informacijske imovine. Jer je to mjesto gdje informacijska imovina "živi" tj. provodi najviše vremena i tu je najviše izložena opasnošću. Drugim riječima, sigurnost informacijske imovine je veća što je veća sigurnost i kontrola spremišta informacijske imovine.

Također je bitno zaštititi sredstva uz pomoć kojih se informacijske imovine prenosi između spremnika (tj. server). Bitno je da sigurnosni zahtjevi budu pravilno raspoređeni na sva kritična mjesta (područja). Potrebno je sagledati sva ova pitanja i zahtjeve koji čine dodatnu razinu složenosti zaštite informacijske imovine. Jasno je da nije moguće napraviti idealnu zaštitu za cijelu informacijsku imovinu, te će uvijek preostati neki rizici (*rezidualni rizik*), upravo radi toga je potrebno pravilno izabrati jedan od pristupa ublažavanja rizika.

Kako bi ublažavanje rizika bilo ispravno, morate uzeti u obzir "uravnoteženi" pristup.

- ✓ Možete *izbjeći* rizik primjenom (implementacijom) odgovarajuće kontrole kako bi se spriječili moguće prijetnje i ranjivosti u slučaju da se rizik desi.
- ✓ Možete *ograničiti* rizik primjenom (implementacijom) odgovarajuće strategije koje ograničavaju neželjeni utjecaj na organizaciju ako rizik je desi.

Također je važno uzeti u obzir visinu cijene pri kreiranju strategija za ublažavanje rizika. Troškovi izbjegavanja i ograničavanja rizika moraju biti srazmjerni s vrijednošću imovine koju želite zaštititi od rizika i potencijalnog utjecaja na informacijsku imovinu koja je ugrožena. Osim toga, morate uzeti u obzir da nije moguće eliminirati sve rizike. Nakon primijenjene strategije ublažavanja rizika može ostati rezidualni rizik (*preostali rizik*) koji morate uzeti u obzir (njegovim prihvaćanjem ili nastavkom ublažavanja).

Kako bi strategija ublažavanja bila korektno sprovedena, potrebno je izvršiti temeljitu i čvrstu analizu, zbog toga ove aktivnosti zahtijevaju opsežnu raspravu i planiranje. Važno je imati podršku višeg menadžmenta i suradnju s IT odjelom ali i sa svim interesnim sudionicima (*stakeholders*) kako bi razvili "uravnoteženu" i troškovno isplativu strategiju za ublažavanje rizika.

8.9.2. Upute i aktivnosti

Osmi korak se sastoji od tri aktivnosti:

❑ **Korak 8 Aktivnost 1**

Prva aktivnost u osmom koraku je sortiranje identificiranih rizika prema dodijeljenim (izračunatim) *rezultatima* rizika. Razvrstavanje rizika će omogućiti lakše donošenje odluka o vrsti pristupa ublažavanje rizika koji će biti implementirani.

Postoji mnogo načina na koje organizacija može kategorizirati svoje rizike. Najjednostavniji način bi bilo razvrstavanje rizika od onih koje imaju veći *rezultat* prema manjem. Sljedeći korak je razdvajanje rizika u četiri odjeljka (polja) sa jednakim brojem rizika. Rizici sa najvećim rezultatom bi trebali biti u prvom odjeljku (Polje1), rizici sa sljedećim najvećim rasponom rezultata u drugom odjeljku (Polje 2), sljedeći najveći u treći (Polje 3), a rizici s najmanjim rezultatom u četvrti (Polje 4).

Ako Vaša organizacija koristi *vjerojatnost*, trebali bi razmisliti o kreiranju matrice za kategoriziranje utvrđenih rizika. Matrica koja slijedi predstavlja primjer kako kategorizirati relativni rizik:

MATRICA RELATIVNOG RIZIKA			
VJEROJATNOST	VRIJEDNOST RIZIKA		
	30 DO 45	16 DO 29	0 DO 15
VISOKO	POLJE 1	POLJE 2	POLJE 2
UMJERENO	POLJE 2	POLJE 2	POLJE 3
NISKO	POLJE 3	POLJE 3	POLJE 4

❑ **Korak 8**
Aktivnost 2

Prilikom dodjeljivanja načina pristupa pojedinom riziku, razmislite o korištenju sljedeće tabele kao vodič. Bitno je napomenuti da ta odluka o načinu ublažavanja rizika jako ovisi o operativnim okolnostima i informacijskoj imovini (svaka organizacija ima svoje jedinstveno rješenje).

Polje	**Pristup ublažavanja**
Polje 1	Ublažavanje
Polje 2	Ublažavanje ili odgađanje
Polje 3	Odgađanje ili prihvaćanje
Polje 4	Prihvaćanje

Bilješke:

U nekim slučajevima moguć je prijenos rizika, npr. na osiguravatelja koji u slučaju velikog rizika sam ulaže u izgradnju sigurnosnog sustava kako bi smanjio vlastiti poslovni rizik na drugu stranu. To se može smatrati kao pristup ublažavanja za sve rizike koje razmatrate.

Potrebno je odrediti način pristupa riziku za sve radne tabele (*rizici informacijske imovine*) koje ste definirali, to je potrebno dokumentirati u zadnjoj tabeli u stupcu (9) koji se naziva "*pristupi ublažavanja*". Svaki profil rizika mora imati dokumentiran pristup ublažavanja. Za rizike koje ste odlučili prihvatiti, potrebno je ponovo provjeriti tvrdnje o posljedicama (izjave) i vrijednosti posljedica. Bitno je da ne *prihvaćamo* bilo koji rizik koji bi mogao naškoditi organizaciji i rezultirati ozbiljnim posljedicama.

❑ **Korak 8 Aktivnost 3**

Za sve profile rizika koje ste odlučili ublažiti, morate razviti strategiju ublažavanja. Uzimajući u obzir radnje koje možete poduzeti za ublažavanje rizika, razmotrite strategije ublažavanja za svaki rizik koji ste odabrali, i to na sljedeći način:

1. Morate zabilježiti (označiti) spremnike informacijske imovine na kojima ćete implementirati sigurnosne kontrole i zaštite (ovi spremnici se mogu naći u radnoj tabeli - *rizične sredine informacijske imovine*).
2. Opišite kontrole koje ćete implementirati, te opišite rizik (*rezidualni rizik*) koji će preostati nakon što implementirate kontrole.

Razmotrite sljedeća pitanja prilikom razvoja strategije za ublažavanje rizika:

- ✓ Kako spriječiti učesnika da iskoristi slabost (ranjivost)?
- ✓ Što treba poduzeti da se spriječi način na koji učesnik to čini?
- ✓ Na koji način se motiv (razlog) može spriječiti?
- ✓ Kako bi spriječili mogući ishod?
- ✓ Da li je moguće smanjiti vjerojatnost prijetnje?
- ✓ Što možemo učiniti unaprijed kako bi smanjili utjecaj rizika?
- ✓ Može li organizacija smanjiti ostvareni učinak ili utjecaj rizika?
- ✓ Da li će biti ispunjeni svi sigurnosni zahtjevi primjenom strategije ublažavanja?

Tablica 8.5. - Implementacija: od koraka 4 do koraka 8

Allegro - radna tabela 10	**RADNA TABELA RIZIKA INFORMACIJSKE IMOVINE**			
Rizik informacijske imovine	**Prijetnja**	Informacijska imovina		
		Interesno područje		
		(1) Učesnik *Tko je zadužen za kontrolu određenog interesnog područja ili rizika?*		
		(2) Sredstvo *Kako bi to učesnik napravio? Što bi učesnik napravio?*		
		(3) Motiv *Zbog kojeg razloga je učesnik to uradio?*		
		(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	❑ **Otkrivanje** ❑ **Uništenje** ❑ **Promjena** ❑ **Prekid**	
		(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*		
		(6) Vjerojatnost *Koja je vjerojatnost da se ovaj scenarij prijetnje desi?*	❑ **Visoko**	❑ **Umjereno** ❑ **Nisko**

(7) Posljedice *Koje su posljedice za organizaciju i vlasnika informacijske imovine koje su nastale kršenjem sigurnosnih zahtjeva?*	(8) Ozbiljnost *Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?*		
	Rizično područje	**Vrijednost**	**Rezultat**
	Ugled i klijentovo povjerenje		
	Financije		
	Produktivnost		
	Zdravlje i sigurnost		
	Pravne i zakonske kazne		
	Korisnikova procjena prijetnji		
	Rezultat relativnog rizika		

(9) Pristup ublažavanja

Na temelju ukupnog rezultata rizika, što ćete učiniti?

❑ **Prihvaćanje**	❑ **Odgađanje**	❑ **Ublažavanje**	❑ **Prebacivanje**

Za rizike koje ste odlučili ublažiti, odradite sljedeće:

Na koji spremnik informacijske imovine ćete primijeniti kontrole?	*Koje administrativne, tehničke i fizičke kontrole ćete primijeniti za ovaj spremnik informacijske imovine?Koji rezidualni rizik će biti prihvaćen od strane organizacije?*

9. Analiza provedenog istraživanja i izrada lokaliziranog popisa prijetnji

Katalozi napada na sigurnost koji postoje u svijetu nisu primjenjivi na svim regionalnim područjima već se popis napada na sigurnost treba lokalizirati kako bi se mogao primijeniti u procjeni rizika.

Obrazloženje hipoteze:

Postoje određena odstupanja podataka između različitih baza podataka u kojima se prikupljaju najčešći napadi na sigurnost. Neki napadi na sigurnost su posebno vezani za neke zemlje kao što su napadi iz područja socijalnog inženjeringa koji su posebno zastupljeni u Sjedinjenim Američkim Državama i pojavljuju se u puno različitih oblika. Neki od tih oblika se čak odnose na točno određene organizacije ili društvene skupine u Sjedinjenim Američkim Državama. Takvi oblici napada na sigurnost nisu zabilježeni u popisima najčešćih prijetnji koji se većinom odnose na područje Europe. S druge strane iz dostupnih podataka se može vidjeti kako se neki napadi na sigurnost pojavljuju po cijelom svijetu ali u različitoj učestalosti pojedinih napada.

9.1. Dokaz prve hipoteze: Izrada prvog javnog kataloga napada na sigurnost u RH

9.1.1. Prikupljanje podataka

Podaci o napadima na sigurnost su prikupljani iz različitih izvora kako bi se izgradio što potpuniji katalog. Korišteni izvori se mogu podijeliti u dvije kategorije:

a) Komercijalni izvori

b) Nekomercijalni izvori

Komercijalni izvori su dostupni javnosti. Od komercijalnih izvora podaci su prikupljani iz sljedećih baza podataka: Datalossdb, Common Weakness Enumeration, Common Vulnerabilities and Exposures, Internet crime complaint center i Arbornetworks. Ove baze podataka sadrže veliki broj podataka o napadima od korisnika iz cijelog svijeta. Iz tih podataka su odabrani najčešći napadi koji su zabilježeni do trenutka pisanja rada. Prilikom prikupljanja podataka iz nekomercijalnih izvora korištene su i sljedeće knjige: Uvod u računalnu sigurnost od Miroslava Bače i Common Vulnerability in Network od U.S. Department of Energy.

Nekomercijalni izvori predstavljaju one izvore koji nisu javno dostupni. Od nekomercijalnih izvora korišteni su dobiveni podaci iz CERT-a i iz anonimne ankete koja je provedena u sklopu ovoga rada.

9.1.2. Analiza i obrada prikupljenih podataka

Prilikom procjene rizika potrebno je analizirati podatke koji se mogu prikupiti na temelju vlastitih i tuđih iskustava, dostupne literature, vlastitih mjerenja i dostupnih izvješća. Od prikupljenih podataka kreiran je prvi javni hrvatski katalog napada na sigurnost. Kako bi katalog podataka bio pregledan bilo je potrebno grupirati podatke prema određenim kategorijama. Svrha kataloga je da korisniku koji vrši procjenu rizika osigura brz i jednostavan način prepoznavanja mogućih prijetnji za promatranu organizaciju. Na temelju toga podaci su grupirani prema sljedećim kategorijama i podkategorijama:

Fizičke prijetnje

- *Uništenje ili gubitak podataka*
  - Oštećene baze podataka
  - Oštećenje računala
  - Oštećenje prijenosnih medija
  - Uništenje analogni zapisa
  - Uništenje digitalnih zapisa
- *Promjena podataka*
  - Promjena digitalnih zapisa

Prijetnje izazvane ljudskim djelovanjem

- *Namjerne*
  - Podmetanje požara
  - Provala
  - Umorstvo
  - Zločin iz mržnje
  - Korištenje lažnog imena
  - Uznemirujuća komunikacija
  - Bezobzirno ugrožavanje
  - Ilegalni transport / dostava
  - Krijumčarenje
  - Trovanje alkoholom
  - Dijeljenje korisničkih računa
  - Štrajk
  - Radna stanica bez nadzora
  - Third-party prijetnje
  - Upravljanje tiskanjem

- Kazneni prijestup
- Neautorizirani interni pristup
- Odavanje povjerljivih podataka
- Vandalizam
- Pobune i protesti civila
- Nedisciplina
- Nemar
- Vanjski napadači
- Socijalni inženjering
- Shoulder Surfing
- Strvinarenje
- Oponašanje dostavljača
- Diverzija
- Špijunaža
- Ratno razaranje
- Neautorizirani pristup

o *Nenamjerne*

- Umrorsto
- Uznemirujuća komunikacija
- Nekonfigurirani Firewall
- Nekonfiguriran Backup
- Radna stanica bez nadzora
- Korisnik nije svjestan klasifikacije podataka koje koristi
- Upravljanje tiskanjem
- Nedefiniran plan za oporavak od katastrofa
- Neklasifikacija sadržaja
- Pogrešno objavljivanje povjerljivih podataka
- Odavanje povjerljivih podataka
- Kazneni prijestup
- Nepažnja
- Neznanje
- Neodgovarajući program
- Neodgovarajuća organizacija

o Poteškoće uzrokovane ljudskim djelovanjem

- Onečišćenje zraka
- Zagrijavanje i uvjeti zraka
- Zagađenje
- Nano mašine i mikrobi
- HERF pištolji
- EMP bombe
- Biološke prijetnje
- Eksplozija

o *Unutarnje ljudske prijetnje*

- Nepošteni zaposlenici
- Nezadovoljni zaposlenici
- Sabotaža zaposlenika

- Neposlušnost
- Otkrivanje osjetljivih podataka
- Nenamjerno oštećenje imovine
- Zlouporaba ovlasti
- Ljudska pogreška
- Izvlačenje informacija ili podmićivanje

Programske prijetnje

- *Maliciozni kod*
  - Adware
  - Spyware
  - Crv
  - Trojanski konj
  - Zamka
  - Virus
  - Hoax
  - Stražnja vrata (eng. Backdoor)
  - Botnet
  - Logičke bombe

- *Napadi na aplikacije*
  - Format String napad
  - Buffer Overflow

- *Napadi umetanjem znakova*
  - Cross-Site Request Forgery (CSRF)
  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Nekorektni unos znakova (end. Path Traversal)
  - ASP Injection
  - PHP Injection
  - Shell Injection
  - LDAP Injection
  - SSI Injection
  - XPath Injection
  - XML Injection
  - XQuery Injection
  - Integer Overflow
  - XML poisoning

Mrežne prijetnje

- *Mrežne poteškoće*
  - Oluja razašiljanja (eng. Broadcast storm)
  - ARP prigušenje (eng. ARP throttling)

- *Napadi na mrežnom sloju*
  - Spoofing (IP, login, web, e-mail, DNS)
  - Routing Detour
  - Smurf napad
  - ICMP Flood
  - Otmice sjednica (eng. Session Hijacking)
  - SYN Flood
  - UDP Flood

Neovlašteni pristup

- *Krađa e-maila*
- *Nezakonite transakcije*
- *Neautorizirani vanjski pristup*
- *Neovlašteno prikupljanje podataka*
- *Neovlaštena izmjena podataka*
- *Neovlaštena izmjena programa*
- *Neautorizirani pristup kroz VPN*
- *Uspješno kompromitiranje računala*
- *Nedozvoljene mrežne aktivnosti*
- *Pravo pristupa*
- *Prisluškivanje*
- *Napad lažnim predstavljanjem (eng. Masquerading attack)*
- *Neovlašten pristup podacima ili imovini*
- *Bluetooth prijevare (eng. Blue-jacking)*
- *Preuzimanje HTTP sesije (eng. HTTP session hijacking)*

Internet prijetnje

- *Internet prijevare*
  - Prijevare s kreditnim karticama
  - Aukcijske prijevare
  - WiFi prijevare
  - Napredne prijevare
  - Humanitarne prijevare
  - FBI prijevara
  - Hitman prijevara
  - Nigerijska ili 419 prijevara
  - Iskorištavanje povjerenja
  - URL preusmjeravanje
  - Money mulling

- *Internet krađa*
  - Salama tehnika
  - Krađa identiteta
  - Phishing
  - Krađa identiteta
  - Pharming
  - Nezaštićene online transakcije

- *Internet ucjena*
  - Ucjenjivanje putem email pošte

- *Spam*

Pokušaj neovlaštenog pristupa

- *Fingerprinting*
- *HTTP Response Splitting*
- *Brute Force napad*
- *Pretraživanje (eng. Scanning)*
- *Napadi na Web servere*
- *Višestruka ugroza (eng. Blended threat)*
- *Pristup mrežnoj infrastrukturi*

Prirodne nepogode

- *Meteorološke pojave*
  - Kisele kiše
  - Vlažnost
  - Oborine
  - Sumaglica
  - Kiša
  - Sitna kiša
  - Rosa
  - Snježna vijavica
  - Ledena kiša
  - Bura
  - Grad
  - Mećava
  - Oluja
  - Pješčana oluja
  - Magla
  - Susnježica
  - Munja
  - Grmljavina

- Mraz
- Promrzlina
- Smog
- Snijeg
- Snježna oluja
- Grmljavina
- Kondenzacija

- *Sezonski fenomeni*
  - Monsun
  - Storm surge
  - Tropske oluje
  - Downburst
  - El Nino
  - La Nina
  - Tajfun
  - Uragan
  - Tornado
  - Tsunami
  - Alberta Clipper
  - Virga
- *Osnovni meteorološki elementi*
  - Oblačnost
  - Pritisak
  - Relativna vlažnost
  - Zračne mase
  - Zračni pritisak
  - Temperatura zraka
- *Geofizičke nepogode*
  - Erozija
  - Vulkanska erupcija
  - Poplava
  - Zemljotres
  - Erozije plaže
  - Bujica
  - Vatra
  - Dim
  - Potresi i vibracije
- *Astrofizički fenomeni*
  - Sunčani fenomeni
  - Meteori
  - Kozmička zračenja
- *Biološke prijetnje*
  - Virusi
  - Otrovi

Tehničke poteškoće

- *Vanjski izvori nisu dostupni*
- *Nepotpuno pokrenuti proces*
- *Električni poremećaj*
- *Kvar sklopovske opreme*
- *Curenje tekućine iz instalacija*
- *Prekid telekomunikacije*
- *Ispadi opreme*
- *Prekid komunikacije*
- *Sklopovski čipovi*
- *Gubitak električnog napajanja*
- *Elektromagnetska radijacija*
- *Greške sklopovskih čipova*
- *Tehničke greške (eng. Bugovi)*

Uskraćivanje usluge

- *Fizički napad*
- *Nedostupnost aplikacija*
- *Nedostupnost servera*
- *Nedostupnost baza podataka*
- *Nedostupnost mreže širokog dosega*
- *Nedostupnost lokalne mreže*
- *Nedostupnost Interneta*
- *Prijetnja bombom*
- *Terorističke prijetnje*
- *Uznemiravanje zaposlenika (eng. Cyberstalking)*
- *Uskraćivanje usluge DoS (Denial of Service)*
- *Distributed Denial of Service (DDoS)* [7, 39, 49, 51, 67]

9.1.3. Izrada ankete

Da bi se dokazalo kako različiti oblici prijetnji nisu jednako zastupljeni u svim sredinama provedeno je istraživanje. Istraživanje je provedeno kreiranjem anketnog upitnika.

Cilj ankete je bio odrediti najčešće sigurnosne napade u Hrvatskoj, stoga je u anketu uključen katalog najčešćih napada na sigurnost koji je kreiran iz svih dostupnih izvora. Prilikom ispunjavanja ankete ispitanici su morali označiti one sigurnosne rizike koji su se dogodili u njihovoj organizaciji ili su imali informacija o pojavi tog napada. Prema metodi Octave Allegro sigurnosne napade smo kategorizirali u tri skupine:

- ✓ tehničke,
- ✓ fizičke i
- ✓ ljudi.

Za sve sigurnosne rizike koji su se pojavili u poslovnom sustavu ispitanici su trebali označiti njihov utjecaj na taj sustav tako da su ga rangirali sa **1** (male), **2** (umjerene) ili **3** (velike). Uz to su trebali za svaki identificirani sigurnosni rizik odrediti njegov intenzitet pojavljivanja rangiranjem sa **1** (vrlo mala), **2** (mala), **3** (umjerena), **4** (velika) ili **5** (vrlo velika). Na temelju tako prikupljenih podataka kreiran je katalog najčešćih sigurnosnih rizika u Hrvatskoj.

U anketi su učestvovali hrvatski stručnjacima iz područja informacijske sigurnosti koji rade u različitim djelatnostima. Provedena anketa je bila anonimna pošto je bilo potrebno otkriti unutar ankete povjerljive podatke koji bi se mogli zloupotrijebiti ako bi se podaci povezali sa stvarnim poslovnim sustavima.

Treba napomenuti da obuhvaćeni uzorak ispitanika iz ankete nije reprezentativan jer se nije mogao provesti metodološki korektan uzorak i istraživanje zbog ograničenosti sredstava, vremena i ostalih vanjskih ograničenja. Stoga ovako dobiveni katalog treba prilikom procjene rizika uzeti samo kao naputak i pomoćno sredstvo kako bi se pojednostavio proces procjene.

Na sljedećoj slici prikazana je forma ankete koja je bila dostupna na web stranici u exel formatu.

Izgradnja sustava informacijske sigurnosti – [Anketa]

Autori:
Dino Alagić,
Mario Vagner i
Vedran Branković.

Naziv teme:
Izgradnja sustava informacijske sigurnosti – razvijena aplikacija za procjenu rizika

Opis ankete:
Nakon prikupljenih sigurnosnih napada, izvršena je podjela prema metodi Octave Allegro u tri skupine:
- tehničke,
- fizičke i
- ljudi.

Pojašnjenje stupaca iz anketne tabele:

- Najčešći napadi u svijetu - predstavlja ukupni popis sigurnosnih napada.
- Područje Republike Hrvatske - potrebno je odgovoriti sa: Da ili Ne, a u slučaju da niste dovoljno informisani stavite crticu (-).
- Moguće posljedice - predstavljaja moguće posljedice za pojedine sigurnosne prijetnje. Ovdje je potrebno odgovoriti sa vrijednostima: 1 (male), 2 (umjerene) ili 3 (velike).
- Učestalost prijetnje - predstavljaja učestalost pojedinih sigurnosnih prijetnji. Ovdje je potrebno odgovoriti sa vrijednostima: 1 (vrlo mala), 2 (mala), 3 (umjerena), 4 (velika) ili 5 (vrlo velika).

Tablica 1. - Tehničke vrste napada

Rezultat nije potrebno popunjavati.

	Vrste sigurnosnih napada				
Br.	Najčešći napadi u svijetu	Područje Republike Hrvatske	Moguće posljedice	Učestalost prijetnje	Rezultat
1	Adware				0
2	ARP prigušenje (eng. ARP throttling)				0
3	ASP Injection				0
4	ATM prijevare				0
5	Aukcijske prijevare				0
6	Bluetooth prijevare (eng. Blue-jacking)				0
7	Botnet				0
8	Brute Force napad				0
9	Buffer Overflow				0
10	Cross-Site Request Forgery (CSRF)				0
11	Cross-Site Scripting (XSS)				0
12	Crv				0
13	Curenje tekućine iz instalacija				0
14	Dialeri				0
15	Distributed Denial of Service (DDoS)				0
16	Eksplozija				0
17	Elektromagnetska radijacija				0
18	EMP bombe				0
19	FBI prijevara				0
20	Fingerprinting				0
21	Format String napad				0
22	Greške sklopovskih čipova				0
23	Gubitak električnog napajanja				0
24	HERF pištolji				0
25	Hitman prijevara				0
26	Hoax				0
27	HTTP Response Splitting				0
28	Humanitarne prijevare				0
29	ICMP Flood				0
30	Integer Overflow				0
31	Iskorištavanje povjerenja				0
32	Ispadi opreme				0
33	Krađa e-maila				0
34	Krađa identiteta				0
35	Kvar sklopovske opreme				0
36	LDAP Injection				0
37	Logičke bombe				0

Da
Ne
-

Napomena:
Potrebno je odgovoriti sa: Da ili Ne, a u slučaju da niste dovoljno informirani stavite crticu (-). Ako ste odabrali "Ne" ili "-" onda će se automatski postaviti "-" u iduća dva stupca, jer se podrazumjeva da niste informirani za taj sigurnisni napad.

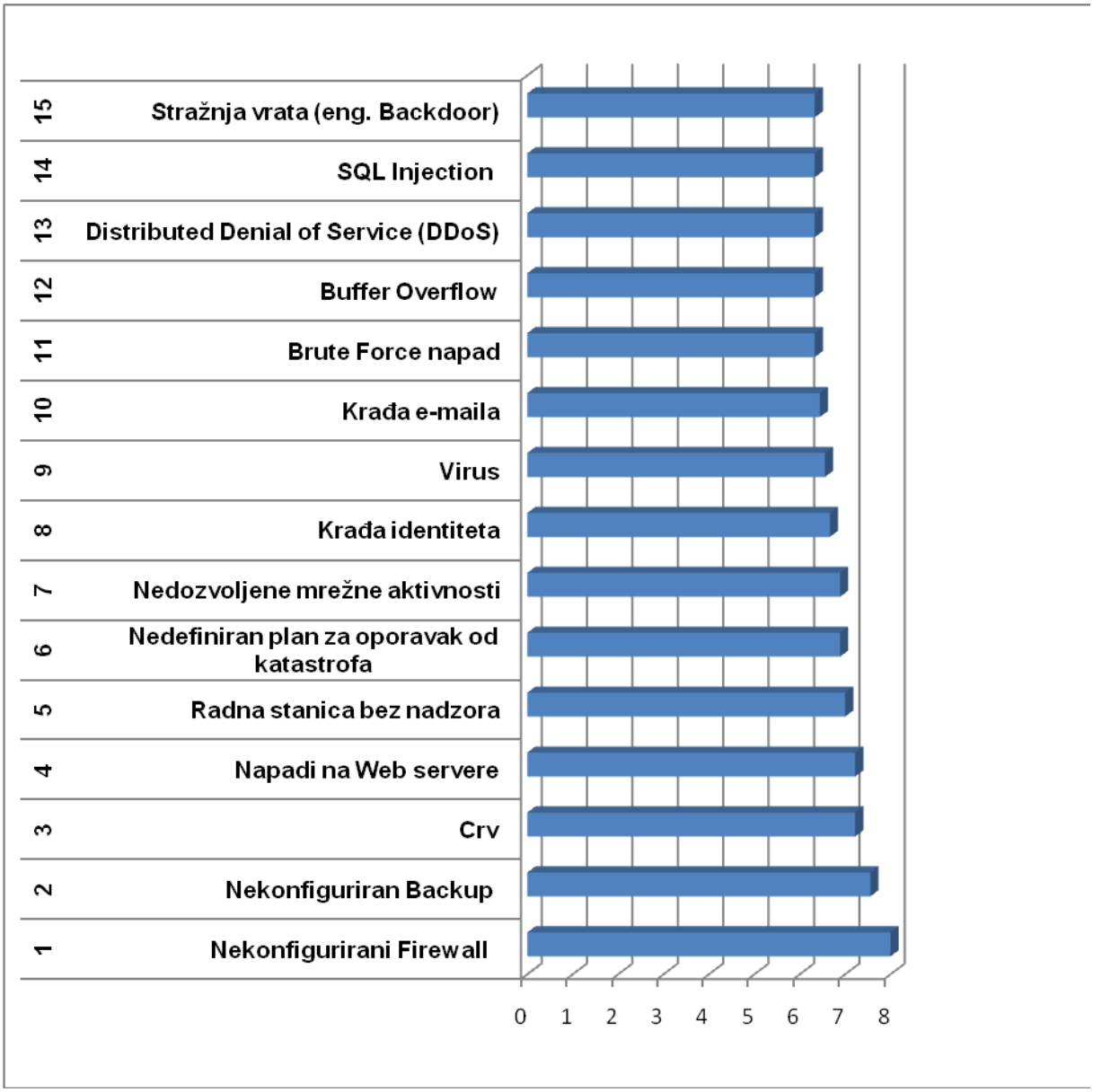
Mogući odgovori po stupcima		
Da	1	1
Ne	2	2
-	3	3
		4
		5

Slika 9.1. - Forma ankete

9.1.4. Rezultati ankete

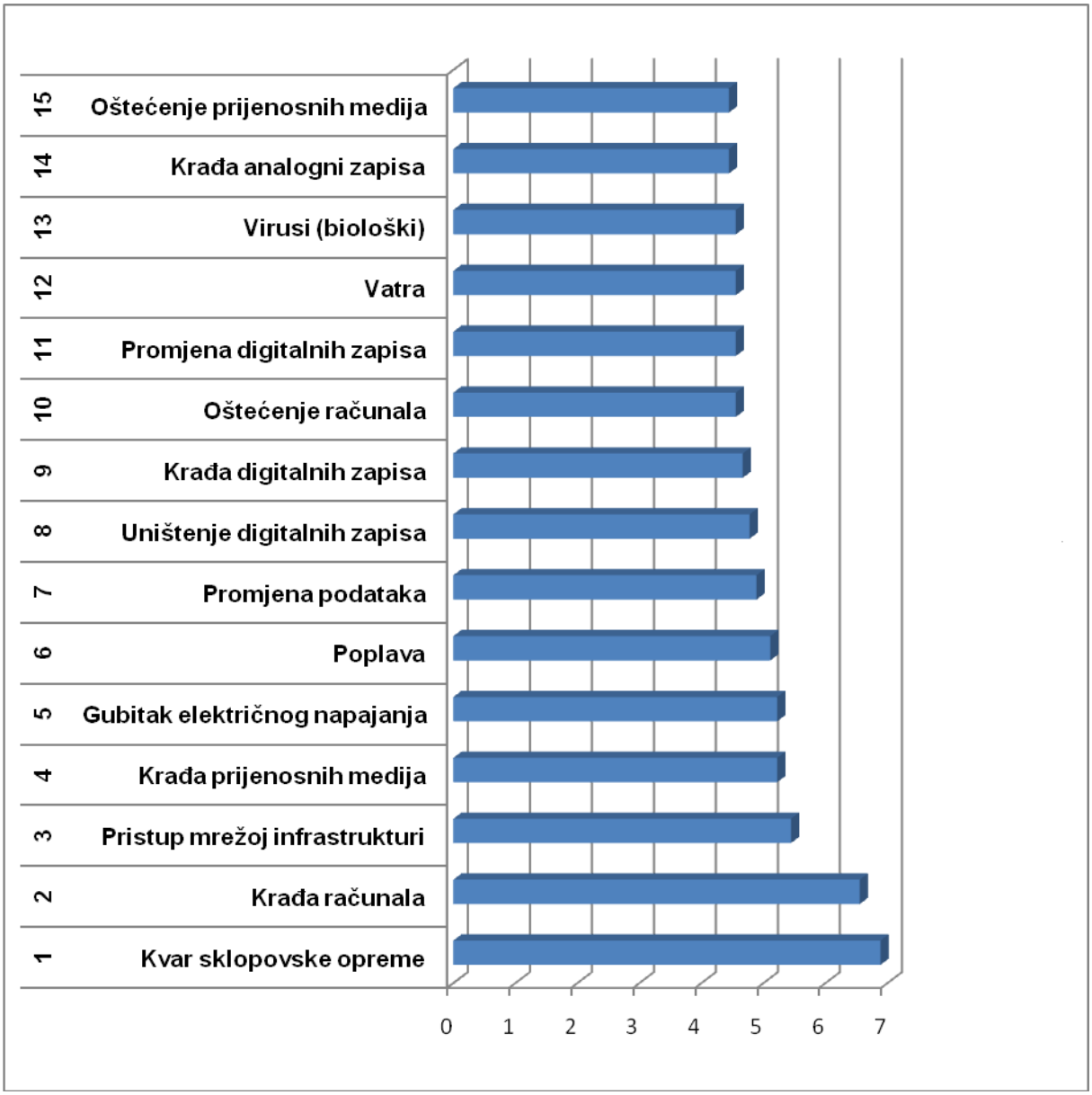
Usporedbom najčešćih napada u svijetu, čiji smo popis prikupili kroz razne izvore s popisom napada prisutnih u RH dobivenog kroz provedeno istraživanje odnosno anketu, došli smo do slijedećih rezultata.

Broj prikupljenih napada na sigurnost u svijetu iznosio je 271, rezultati ankete su pokazali da samo pet napada od ukupnog broja napada nije zabilježeno u RH. Napadi na sigurnost koji nisu zabilježeni u RH su prirodne nepogode koje su specifične za područje Sjedinjenih Američkih država kao što su: Alberta Clipper, Downburst, El Nino i La Nina. Što se tiče tehničkih napada jedina koja nije zabilježena u RH je napad uz pomoć nano mašina i mikroba.



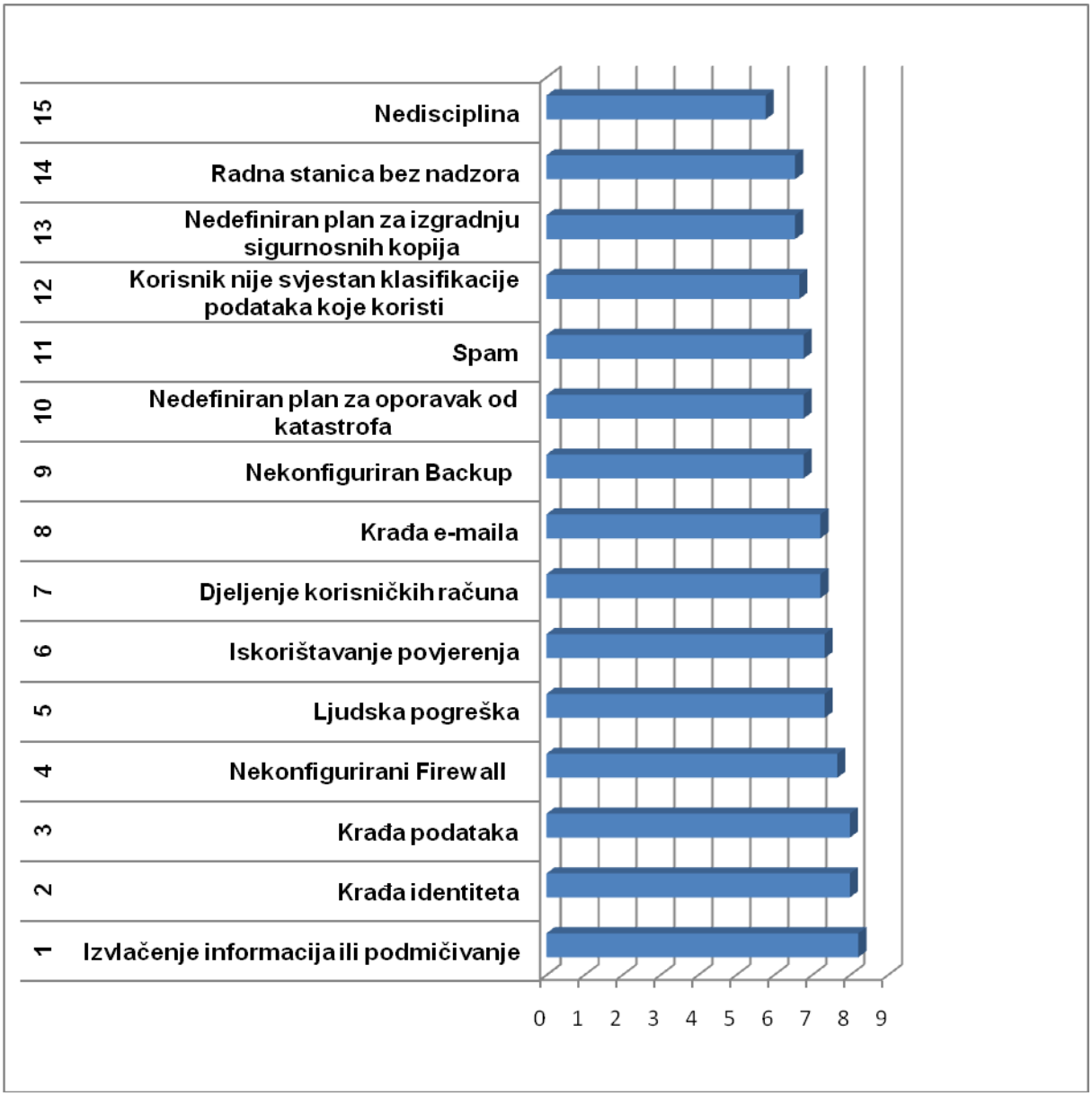
Grafikon 9.1. - Tehničke vrste napada

Na sljedećem grafikonu su prikazani fizički napadi na sigurnost koji je ukupno bilo 76.



Grafikon 9.2. - Fizičke vrste napada

Na posljednjem grafikonu prikazano je 15 najznačajnijih napada na sigurnost prouzrokovanih od strane čovjeka od ukupno 85 identificiranih.



Grafikon 9.3. - Ljudske vrste napada

Zaključak je da nema prevelike razlike između lokaliziranog kataloga i svijetskog kataloga prijetnji, no kako je uzorak bio relativno malen te su ispitanici isključivo ljudi koji se praktično bave područjem sigurnosti anketu su odgovarali što bi se od prijetnji moglo realizirati u RH. Realiziranih prijetnji je manje od prikazanih u istraživanju stoga je potvrđeno da je prva hipoteza dokazana.

10. Način korištenja aplikacije za procjenu rizika po metodi Octave Allegro

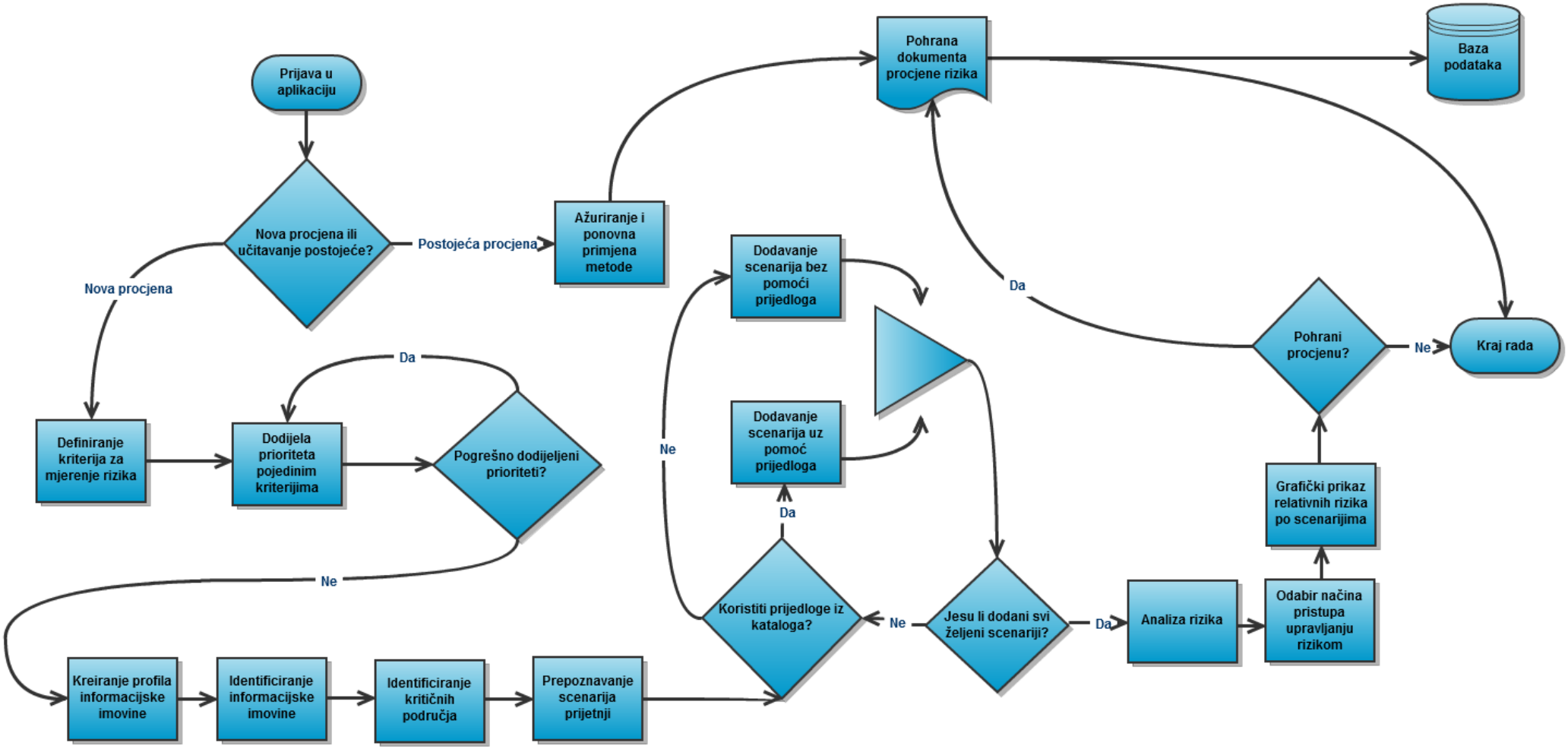
Web aplikacija implementira metodu za procjenu rizika Octave Allegro. Stranica naizgled ne izgleda kompleksno, no kako je metoda jako opširna i kompleksna bio je izazov napraviti stranicu koja će korisniku biti lagana za korištenje. Kroz izradu ove aplikacije upravo se tome težilo. U pozadini postoje implementirana mnoga programska rješenja kako bi se procjena rizika odnosno izlaz iz aplikacije prilagodio za ispis ili pohranu. Ideja je da izlaz iz aplikacije izgleda kao da je napravljen u nekoj od aplikaciji za obradu dokumenata, odnosno da se na nju gleda kao na dokument.

Dizajnirana je tako da korisnik ima na jednom mjestu:

- ✓ *potrebnu dokumentaciju (upute) kako provoditi pojedine korake metode*
- ✓ *sve pripadajuće tablice koje kroz metodu treba ispuniti.*
- ✓ *primjere koje korisniku mogu objasniti moguće nejasna područja metode*

Upute te primjeri implementirani su u aplikaciji na nametljiv način (prema početnim postavkama su skriveni) tako da neće iskusnom korisniku stajati na putu. Pretpostavka je da će upute biti potrebne samo kod procjene rizika za prvih nekoliko stavki imovine dok će kasnije samo smetati korisniku. Kako je stavki obično puno logično je bilo na taj način dizajnirati stranicu. Prilikom izrade stranice posebna pažnja je posvećena jednostavnosti korištenja, preglednom dizajniranu i u sklad sadržaja koji prikazuje.

Korištenje aplikacije prikazano je na sljedećem blok dijagramu.



Slika 10.1. - Blok dijagram koji opisuje provedbu metode kroz aplikaciju

Ovaj blok dijagram prikazuje kako kroz našu aplikaciju provesti procjenu rizika za vlastiti informacijski sustav. Prikazom se nije išlo u detalje, nego se prikazuje globalni proces provođenja metode kako bi se prosječnom korisniku olakšalo razumijevanje korištenja aplikacije.

11. Procjena rizika razvijenom aplikacijom

Razvijenu aplikaciju za procjenu rizika mogu zadovoljavajuće koristiti i slabo sigurnosno educirani korisnici.

Obrazloženje hipoteze:

Postoji jako mali broj poslovnih sustava koja dovoljno brinu o sigurnosti svojih informacijskih sustava. Kao potvrdu ove konstatacije pogledat ćemo broj tvrtki unutar RH koje posjeduju certifikat sigurnosti informacijskog sustava[11]:

Tablica 11.1. - Broj certificiranih poduzeća u RH

Norma po kojoj je poduzeće certificirano	Broj
ISO 27001:2005	13
EAC 33	9
EAC 35,33	2
EAC 28, 34	1
ISO 27001:2005, EAC 35,33	1
Ukupno:	**26**

Kao što možemo vidjeti ova brojka nije obećavajuća. Podaci od zadnjih nekoliko godina ne ukazuju na nikakav značajan trend rasta.

Kroz provedeno istraživanje zaključeno je da je za primjenu u ovom radu najbolji izbor metoda Octave Allegro jer nju smijemo modificirati, može se primjeniti na sve vrste poslovnih sustava, te ne postoji razvijena aplikacija za njeno provođenje.

U nastavku istraživanja podaci dobivene iz ankete iskorišteni su te ugrađeni u aplikaciju u obliku pomoći korisniku na način da mu aplikacija nudi određene napade po kategorijama što uvelike može olakšati postupak procjene rizika. Kao dokaz ove hipoteze u nastavku slijedi primjer korištenja aplikacije od strane prosječnog korisnika, te sigurnosno educiranog korisnika. Prikazane će biti razlike, te zaključci koji podupiru ovu hipotezu.

[11] Dostupno na: http://www.kvaliteta.net/informacije/icertifikati.aspx

11.1. Dokaz druge hipoteze: Korištenje aplikacije od strane različito sigurnosno educiranih korisnika

Kako bi se dokazala druga hipoteza provedena je procjena rizika pomoću razvijene aplikacije u koju je implementiran katalog najznačajnijih napada na sigurnost u Hrvatskoj. Procjenu je prvo proveo stručnjak iz područja informacijske sigurnosti i osoba koja nema kompetentna znanja iz područja informacijske sigurnosti. U oba slučaja procjena rizika se provodila na istom poslovnom sustavu kako bi se dobiveni rezultati testova mogli usporediti. Na sljedećim slikama su prikazani svi koraci procjene rizika koje su ispitanici provodili kroz aplikaciju. Usporedno su prikazani samo oni koraci u procjeni rizika između stručnog i nestručnog procjenitelja koji značajno mogu utjecati na ishod procjene rizika.

11.1.1. Procjena rizika na konkretnom primjeru

Pošto se izneseni podaci u primjeru mogu zloupotrijebiti nije navedeno ime poduzeća već će se daljnje u tekstu ime poduzeća označavati sa „X“. Poduzeće „X“ je osnovano s ciljem pružanja usluga u području servisiranja i prodaje automobila. Glavnu poslovnu aktivnost predstavlja servis u kojem se klijentima pružaju razne usluge od računalne dijagnostike kvarova do popravaka vozila. Također se bavi prodajom auto-dijelova te ugradnjom automobilskih stakala, te spada u mala poduzeća sa svojih deset zaposlenika.

11.1.2. Korak 1 – Definiranje kriterija za mjerenje rizika

Aktivnost 1

Prema metodi Octave Allegro na početku procjene potrebno je definirati nekoliko stvari. Prvo se određuje koja sva područja interesa postoje unutar organizacije. Tako područje interesa mogu biti financije, ugled, produktivnost, zakonska regulativa i slično. Nakon toga treba odrediti važnost pojedinog područja za poslovanje poduzeća nad kojim se provodi procjena rizika kako bi se znalo kasnije rangirat posljedice rizika ukoliko se realizira.

Allegro radna tabela 1 - KRITERIJ MJERA RIZIKA – Ugled i klijentovo povjerenje

prikazi/sakrij primjer

Područje prijetnje	Nisko	Umjereno	Visoko
Ugled poduzeća	Utječe minimalno na ugled, tj. moguće se oporaviti uz malen ili ikakvih napora i troškove.	Ugled je narušen, i potreban je određeni napor i trošak da se oporavi.	Ugled je trajno narušen ili oštećen.
Gubitak klijenata	Gubitak klijenata manje od 10% zbog smanjenja pouzdanja.	10 do 30% zbog smanjenja pouzdanja.	Više od 30% zbog smanjenja pouzdanja.
Ugled dobavljača	Utječe minimalno na ugled, tj. moguće se oporaviti uz malen ili ikakvih napora i troškove.	Ugled je narušen, i potreban je određeni napor i trošak da se oporavi.	Ugled je trajno narušen ili oštećen.
Ugled klijenata	Utječe minimalno na ugled, tj. moguće se oporaviti uz malen ili ikakvih napora i troškove.	Ugled je narušen, i potreban je određeni napor i trošak da se oporavi.	Ugled je trajno narušen ili oštećen.

dodaj stavku

Allegro radna tabela 2 - KRITERIJ MJERA RIZIKA – Financije

prikazi/sakrij primjer

Područje prijetnje	Nisko	Umjereno	Visoko
Troškovi poslovanja	Povećanje godišnji troškova poslovanja manje od 10%.	Godišnji troškovi poslovanja povećani od 10 do 20%.	Godišnji troškovi poslovanja već od 20%.
Gubitak prihoda	Godišnji gubitak prihoda manji od 10%	Godišnji gubitak prihoda od 10 do 20%.	Godišnji gubitak prihoda veći od 20%.
Jednokratni financijski gubitci	Jednokratni financijski gubitci manji od 20 000 KN	Jednokratni financijski gubitci od 20 000 KN do 50 000 KN	Jednokratni financijski gubitci veći od 50 000 KN
Dugoročni financijski gubitci	Dugoročni financijski gubitci manji od 100 000 KN	Dugoročni financijski gubitci od 100 000 KN do 200 000 KN	Dugoročni financijski gubitci veći od 200 000 KN

dodaj stavku

Slika 11.1. - Definiranje kriterija za mjerenje rizika koje su proveli ispitanici

Allegro radna tabela 3 - KRITERIJ MJERA RIZIKA – Produktivnost

prikazi/sakrij primjer

Područje prijetnje	Nisko	Umjereno	Visoko
Radni sati zaposlenika	Radni sati zaposlenika su povećani manje od 10% u 6 radnih dana.	Radni sati zaposlenika su povećani od 10% do 20% u 6 radnih dana.	Radni sati zaposlenika su povećani više od 20% u 6 radnih dana.
Radni sati organizacijske jedinice	Radni sati organizacijske jedinice su povećani manje od 10% u 6 radnih dana.	Radni sati organizacijske jedinice su povećani od 10% do 20% u 6 radnih dana.	Radni sati organizacijske jedinice su povećani više od 20% u 6 radnih dana.
Tehnička oprema	Smanjenje raspoloživost tehničke opreme od 5%	Smanjenje raspoloživost tehničke opreme od 5% do 10%	Smanjenje raspoloživost tehničke opreme veće od 10%

dodaj stavku

Allegro radna tabela 4 - KRITERIJ MJERA RIZIKA – Zdravlje i sigurnost

prikazi/sakrij primjer

Područje prijetnje	Nisko	Umjereno	Visoko
Život	Nema gubitka ili značajnu prijetnju za kupaca ili zaposlenika.	Životi kupca ili zaposlenika su ugroženi, ali će se oporaviti nakon pružanja liječničke pomoći.	Smrt kupca ili zaposlenika.
Zdravlje	Minimalna, i potrebno je odmah lječiti osoblje (kupce i zaposlenike) i da oporavak bude u roku od 4 dana.	Privremeno ili oporavak od pogoršanog zdravstvenog stanja osoblja (potrošača i zaposlenika).	Trajno pogoršanje zdravlja koje rezultira dugoročni gubitak kupaca ili zaposlenika.
Sigurnost	Sigurnost upitna.	Sigurnost izložena utjecajima.	Sigurnost narušena.

dodaj stavku

Slika 11.2. - Definiranje kriterija za mjerenje rizika koje su proveli ispitanici

Allegro radna tabela 5 - KRITERIJ MJERA RIZIKA – Pravne i zakonske kazne

prikazi/sakrij primjer

Područje prijetnje	Nisko	Umjereno	Visoko
Kazna	Novčana kazna manja od 5 000 KN.	Novčana kazna od 5 000 KN do 20 000 KN.	Novčana kazna veća od 20 000 KN.
Tužbe	Ozbiljne tužbe podnesene od strane organizacije koje su manje od 5 000 KN.	Ozbiljne tužbe podnesene od strane organizacije koje su od 5 000 KN do 20 000 KN.	Ozbiljne tužbe podnesene od strane organizacije koje su veće od 20 000 KN.
Istrage	Nema upita od vlade ili drugih istražnih organizacija.	Vlada ili druge istražne organizacije traže informacije ili zapise (po zakonskim propisima i obavezama).	Vlada ili druge istražne organizacije pokreću intenzivnu istragu u dubinu (detaljnije).
Neispunjavanje ugovorenih uvjeta	Neispunjavanje ugovorenih uvjeta u iznosu od 10 000 KN	Neispunjavanje ugovorenih uvjeta u iznosu od 10 000 KN do 20 000 KN	Neispunjavanje ugovorenih uvjeta u iznosu većem od 20 000 KN

dodaj stavku

Allegro radna tabela 6 - KRITERIJ MJERA RIZIKA – Korisnikova procjena prijetnji

Područje prijetnje	Nisko	Umjereno	Visoko
Poslovanje poduzeća	Financijski pokazatelji su jednaki ili bolji od konkurentnih poduzeća	Financijski pokazatelji su nešto lošiji od konkurentnih poduzeća	Financijski pokazatelji su puno lošiji od konkurentnih poduzeća
Kvaliteta usluge	Klijenti vjeruju u kvalitetu usluge	Klijenti sumnljaju u kvalitetu usluge	Klijenti su izgubili povjerenje u kvalitetu usluge

dodaj stavku

Slika 11.3. - Definiranje kriterija za mjerenje rizika koje su proveli ispitanici

Aktivnost 2

U drugoj aktivnosti određuje se važnost pojedinog područja utjecaja za poslovanje poslovnog sustava nad kojim se provodi procjena rizika. To je usko vezano uz način djelovanja poslovnog sustava, stoga se veličine prioriteta mogu razlikovati između poslovnih sustava iz iste djelatnosti. Ova aktivnost je važna jer se određivanjem prioriteta utječe na krajnju pojedinu veličinu relativnog rizika prema područjima interesa.

Allegro radna tabela 7 - RADNA TABLICA - DODJELA PRIORITETA ZA UTJECAJNA PODRUČJA

Prioritet	Područje utjecaja
4	Ugled i klijentovo povjerenje
5	Financije
3	Produktivnost
2	Zdravlje i sigurnost
1	Pravne i zakonske kazne
0	Korisnikova procjena prijetnji

Slika 11.4. - Dodjela prioriteta koju je proveo stručnjak

Allegro radna tabela 7 - RADNA TABLICA - DODJELA PRIORITETA ZA UTJECAJNA PODRUČJA

Prioritet	Područje utjecaja
5	Ugled i klijentovo povjerenje
4	Financije
3	Produktivnost
1	Zdravlje i sigurnost
2	Pravne i zakonske kazne
0	Korisnikova procjena prijetnji

Slika 11.5. - Dodjela prioriteta koju je provela nestručna osoba

11.1.3. Korak 2 – Kreiranje profila informacijske imovine

Cilj ove aktivnosti je kreirati listu na kojoj će se nalaziti informacijska imovina poslovnog sustava koja je od ključne važnosti za njegovo normalno funkcioniranje.

Aktivnost 1

Allegro radna tabela 8 - PROFIL KLJUČNE INFORMACIJSKE IMOVINE

(1) Ključna imovina - *Što je kritična informacijska imovina?*	(2) Obrazloženje za opis - *Zašto je ta informacijska imovina važna za organiaciju?*	(3) Opis - *Koji je odgovarajući opis za tu informacijsku imovinu?*
Baza podataka tehničkih specifikacija	Baza podataka tehničkih specifikacija je važna za pravilno odvijanje procesa u odjelu servisa poduzeća. Ukoliko bi se narušio integritet podataka u toj bazi nastali bi veliki troškovi u poslovanju oduzeća.	U bazi podataka tehničkih specifikacija nalaze se svi podaci koji su neophodni za funkcioniranje dijagnostičkih i nekih radnih alata u servisu.

(4) Vlasnik / vlasnici

-

Tko je vlasnik te informacijske imovine?

Vlasnik ove informacijske imovine je direktor servisa (Dino Mujkić).

(5) Sigurnosni zahtjevi

-

Koji su sigurnosni zahtjevi za ovu informacijsku imovinu?

Povjerljivost	Samo ovlašteno osoblje može vidjeti ovu informacijsku imovinu, a oni su:	Direktor servisa i radnici u servisu.
Integriritet	Samo ovlašteno osoblje može mijenjati ovu informacijsku imovinu, a oni su:	prilikom nadogradnje sustava.
Dostupnost	Ova informacijska imovina mora biti na raspolaganju za određeno osoblje kako bi mogli raditi svoj posao, a oni su:	Direktor servisa i serviseri
	Ova informacijska imovina mora biti na raspolaganju 8 sati, 6 dana / tjedan, 52 tjedana / godišnje.	poslovni procesi neometano obavljali.
Ostalo	Na ovu informacijsku imovinu se\odnose posebni zakonski propisi za zaštitu, a oni su:	-

(6) Najvažniji sigurnosni zahtjevi

-

Koji je najvažniji sigurnosni zahtjev za tu informacijsku imovinu?

Povjerljivost	Integritet	Dostupnost	Ostalo

Slika 11.6. - Kreiranje profila informacijske imovine koju su proveli ispitanici

11.1.4. Korak 3 – Identificiranje informacijske imovine

Potrebno je identificirati ključnu informacijsku imovinu tako da se ustanovi gdje se sve koristi promatrana imovina u poslovanju poslovnog sustava, na kojoj se tehničkoj opremi nalazi te tko je vlasnik te imovine s aspekta upravljanja imovinom. Na temelju ove aktivnosti

će se znati koju informacijsku imovinu treba zaštititi i tko će biti odgovoran za pojedinu informacijsku imovinu.

Aktivnost 1

Allegro radna tabela 9a - MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (TEHNIČKE)

Unutarnje

Opis spremišta	Vlasnik/Vlasnici
1. Baza podataka tehničkih specifikacija se nalazi na računalu za dijagnostiku.	Voditelj servisa
2. Računalo za dijagnostiku sadrži skup aplikacija i baza podataka kako bi omogućio rad dijagnostičkim uređajima u servisu	Voditelj servisa
3. Lokalna mreža poduzeća se koristi za pristupanje i ažuriranje svih podataka koji se nalaze u bazi.	IT odjel poduzeća

dodaj stavku

Vanjske

Opis spremišta	Vlasnik/Vlasnici
4. Internet – putem interneta se obavljaju transakcije između baze podataka artikala i baze podataka koja se nalazi na strani dobavljača.	Nepoznat
5. Baza podataka dobavljača koja se koristi za ažuriranje podataka.	IT odjel dobavljača

dodaj stavku

Allegro radna tabela 9b - MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (FIZIČKE)

Unutarnje

Opis spremišta	Vlasnik/Vlasnici
1. Radionica u kojoj je smješteno računalo za dijagnostiku.	Direktor servisa
2. Ormar koji je smješten u uredu direktora servisa. U ormaru su pohranjene kopije aplikacija i baza podataka koje koriste dijagnostički uređaji.	Direktor servisa

dodaj stavku

Vanjske

Opis spremišta	Vlasnik/Vlasnici
3. Arhiva u kojoj dobavljač čuva sigurnosne kopije baza podataka.	Čuvar
4. Server na kojem se nalaze baze podataka za ažuriranje.	IT odjel poduzeća dobavljača

dodaj stavku

Slika 11.7. - Identificiranje informacijske imovine koju su proveli ispitanici

Allegro radna tabela 9c - MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (LJUDI)

Unutarnje osoblje	
Ime ili uloga / Odgovornost	**Odjel ili Jedinica**
1.Direktor servisa	Servis
2.Serviser	Servis

dodaj stavku

Vanjsko osoblje	
Dobavljač, prodavač, itd.	**Organizacija**
3. Informatičar	Dobavljač
4. Referent osiguranja	Osiguravajuća kuća

dodaj stavku

Slika 11.8. - Identificiranje informacijske imovine koju su proveli ispitanici

11.1.5. Korak 4 – Prepoznavanje scenarija prijetnji

Aktivnost 1

U ovom koraku se određuju interesna područja za prethodno odabranu kritičnu informacijsku imovinu. Kako bi se spriječila redundantnost podataka ovaj korak se ne unosi u aplikaciju, jer se interesna područja navode u šestom koraku metode unutar aplikacije. Pod četvrtim korakom u aplikaciji se objašnjava korisniku što će sve morati napraviti kako bi popunio dio radne tabele u šestom koraku.

11.1.6. Korak 5 – Prepoznavanje scenarija prijetnji

Aktivnost 1

Nakon prethodno određenih interesna područja za svako interesno područje se određuju mogući scenariji napada na sigurnost i prijetnji. Kako bi se došlo do scenarija potrebno je popuniti prethodno pripremljene obrasce. Na temelju popunjenih obrazaca kreira se grafički prikaz scenarija u obliku strukture stabla kako bi prikaz podataka bio pregledan. Ova aktivnost je važna jer će se na temelju nje kasnije odrediti koje će se sve kontrole implementirati kako bi se umanjili sigurnosni rizici u poslovnom sustavu.

Upitnik za scenario prijetnji 1 - Tehnički spremnici

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na tehničkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenario 1: Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više tehničkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:			
Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	Ne	Da (slučajno)	**Da (namjerno)**
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	Ne	Da (slučajno)	**Da (namjerno)**

Scenario 2: Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumjeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:			
Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	Da (slučajno)	Da (namjerno)
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	Ne	Da (slučajno)	**Da (namjerno)**

Slika 11.9. - Prepoznavanje scenarija prijetnji koju su proveli ispitanici

Scenario 3: U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovinue na bilo kojem tehničkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- **nenamjerno otkrivanje informacijske imovine**
- **nenamjerna promjena informacijske imovine**
- **nenamjerni prekid dostupnosti informacijske imovine**
- **nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine**

Aplikacijski kvar	Ne	Da (otkrivanje)	Da (promjena)	**Da (prekid)**	Da (gubitak)
Pad sustava iz poznatih ili nepoznatih razloga	Ne	Da (otkrivanje)	Da (promjena)	**Da (prekid)**	Da (gubitak)
Kvar sklopovske opreme	Ne	Da (otkrivanje)	Da (promjena)	**Da (prekid)**	Da (gubitak)
Izvršenje malicioznog koda (kao što su virusi, crvi, Trojanski konjs ili back door)	Ne	Da (otkrivanje)	**Da (promjena)**	Da (prekid)	Da (gubitak)
Prekid napajanja za tehnikče spremnike inforamcijske imovine	**Ne**	Da (otkrivanje)	Da (promjena)	Da (prekid)	Da (gubitak)
Problemi s telekomunikacijom	**Ne**	Da (otkrivanje)	Da (promjena)	Da (prekid)	Da (gubitak)
Pojava drugih "third-party" problema.	**Ne**	Da (otkrivanje)	Da (promjena)	Da (prekid)	Da (gubitak)
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	Ne	Da (otkrivanje)	Da (promjena)	Da (prekid)	**Da (gubitak)**

Upitnik za scenario prijetnji – 2 Fizički spremnici

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na fizičkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenario 1: Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više fizičkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	Da (slučajno)	Da (namjerno)
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	Da (slučajno)	Da (namjerno)

Slika 11.10. - Prepoznavanje scenarija prijetnji koju su proveli ispitanici

Upitnik za scenario prijetnji – 2 Fizički spremnici

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na fizičkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenario 1: Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više fizičkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	Da (slučajno)	Da (namjerno)
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	Da (slučajno)	Da (namjerno)

Scenario 2: Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumjeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	Da (slučajno)	Da (namjerno)
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	Da (slučajno)	Da (namjerno)

Scenario 3: U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovinue na bilo kojem fizičkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- **nenamjerno otkrivanje informacijske imovine**
- **nenamjerna promjena informacijske imovine**
- **nenamjerni prekid dostupnosti informacijske imovine**
- **nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine**

Pojava drugih "third-party" problema.	**Ne**	Da (otkrivanje)	Da (promjena)	Da (prekid)	Da (gubitak)
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	Ne	Da (otkrivanje)	Da (promjena)	Da (prekid)	**Da (gubitak)**

Slika 11.11. - Prepoznavanje scenarija prijetnji koju su proveli ispitanici

Upitnik za scenario prijetnji 3 - Ljudi

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na tehničkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenario 1: Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik ima detaljno znanje o Vašoj informacijskoj imovini (slučajno ili namjerno), što bi moglo rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	Ne	Da (slučajno)	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	Da (slučajno)	Da (namjerno)
Prekinuti s namjerom da se ne može pistupiti informacijama?	**Ne**	Da (slučajno)	Da (namjerno)
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	Da (slučajno)	Da (namjerno)

Scenario 2: Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumjeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	Ne	**Da (slučajno)**	Da (namjerno)

Slika 11.12. - Prepoznavanje scenarija prijetnji koju su proveli ispitanici

Tabela 5: Grafički prikaz stabala prijetnji

Ljudski čimbenici prilikom korištenja tehničkih uređaja

Ljudski čimbenici prilikom korištenja fizičkih uređaja

Tehnički problemi

Ostali problemi

Slika 11.13. - Grafički prikaz scenarija prijetnji koju su proveli ispitanici

11.1.7. Korak 6 – Identifikacija rizika

Aktivnost 1

Scenarij 1

Koristiti prijedloge? ☐

Informacijska imovina	Baza podataka tehničkih karakteristika
Interesno područje	Nenadzirani pristup neautorizirane osobe podacima iz baze.

Rizik informacijske imovine

Prijetnja

(1) Učesnik *Tko je zadužen za kontrolu određenog interesnog područja ili rizika?*	Voditelj servisa
(2) Sredstvo *Kako bi to učesnik uradio? Što bi učesnik uradio?*	Ukoliko direktor servisa napusti radno mjesto postoji mogućnost da zaposlenici iz servisa pristupe računalu ukoliko ostane nezaštićeno.
(3) Motiv *Zbog kojeg razloga je učesnik to uradio?*	Znatiželja prema novoj tehnologiji
(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	Promjena
(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*	Samo autorizirani zaposlenik može vidjeti podatke iz baze
(6) Vjerovatnost *Koja je vjerovatnost da se ovaj scenario prijetnje desi?*	Umjereno

(7) Posljedice	(8) Ozbiljnost			
Koje su posljedice za organizaciju i vlasnika informacijske imovinene koje su nastale kršenjem sigurnosnih zahtjeva?	*Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?* Rizično područje		Vrijednost	Rezultat
Ukoliko se dogode kvarovi na vozilima zbog krive dijagnoze uzrokovane promjenom parametara dijagnostičkih uređaja oštećeni klijenti mogu tužiti poduzeće.	Ugled i klijentovo povjerenje	Nisko	4	
	Financije	Visoko	15	
Ukoliko klijent dobije parnicu ošteta može biti značajna pošto se može raditi o skupim i specijaliziranim vozilima.	Produktivnost	Visoko	9	
	Zdravlje i sigurnost	Nisko	2	
Ukoliko se poremete parametri na dijagnostičkim uređajima potrebno je uložiti dosta vremena da se uređaji ponovo podese i ispitaju.	Pravne i zakonske kazne	Visoko	3	
	Korisnikova procjena prijetnji	Nisko	0	

Rezultat relativnog rizika 33

Slika 11.14. - Prvi scenarij koji je proveo stručni ispitanik

(9) Pristup Ublažavanje

Na temelju ukupnog rezultata rizika, što ćete učiniti?

Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*

Spremnik	Kontrole i rezidualni rizik
Zaposlenici u servisu	Raspodjela dužnosti kako bi se točno odredilo tko je za što odgovoran unutar odjela servisa.
Baza podataka tehničkih karakteristika	Potrebno je provesti prijavu korisnika na računalo s kojeg se mjenjaju podaci u bazi, tako da se to omogući samo zaposleniku kome je dana ta odgovorrnost. Na taj način će se umanjiti mogućnost podnošenja tužbi protiv poduzeća.

dodaj stavku

Slika 11.15. - Odabir načina postupanja s rizikom za prvi scenarij koji je proveo stručni ispitanik

U ovoj aktivnosti za svaki scenarij prijetnji i svaku odabranu kritičnu informacijsku imovinu koja se prethodno definirala u radnim tabelama treba odrediti kakve će posljedica prouzročiti. Ova aktivnost je važna jer će se shodno na posljedice odlučiti kako će se postupati prema sigurnosnim rizicima koje mogu prouzročit te posljedice. Na slikama 11.13. i 11.14. je prikazan potpuni opis jednog scenarija koji je nastao na temelju svih koraka metode Octave Allegro. U aplikaciji su radne tabele koje opisuju scenarije smještene u šestom koraku, kako bi se do kraja popunila potrebno je pogledati sedmi i osmi korak. Sedmi korak je povezan s prvim, tako da je potrebno odrediti kvalitativne ocjene koje će predstavljati veličinu posljedica koje pojedini rizik može nanijeti pojedinoj kategoriji interesnih područja utvrđenih u prvom koraku. U osmom koraku su objašnjene smjernice kojima se predlaže upravljanje rizikom na temelju prethodno izračunatih relativnih rizika.

Scenarij 2

Koristiti prijedloge? ☐

Informacijska imovina	Baza podataka tehničkih karakteristika
Interesno područje	Denail-of-service napad koji bi onesposobio ažuriranje baze podataka i komunikaciju s ostalim odjelima unutar poduzeća.

Rizik informacijske imovine

Prijetnja

(1) Učesnik *Tko je zadužen za kontrolu određenog interesnog područja ili rizika?*	Haker koji želi nanjeti štetu poduzeću
(2) Sredstvo *Kako bi to učesnik uradio? Što bi učesnik uradio?*	Korištenje dostupnih toolkit-ova
(3) Motiv *Zbog kojeg razloga je učesnik to uradio?*	Zabava
(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	Prekid
(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*	Baza mora biti dostupna za vrijeme radnog vremena kako bi se dijagnostika vozila mogla nesmetano provesti
(6) Vjerovatnost *Koja je vjerovatnost da se ovaj scenario prijetnje desi?*	Nisko

(7) Posljedice	(8) Ozbiljnost		
Koje su posljedice za organizaciju i vlasnika informacijske imovinene koje su nastale kršenjem sigurnosnih zahtjeva?	*Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?* Rizično područje	Vrijednost	Rezultat
Ukoliko se baza vozila pravovremeno ne ažurira može doći do nemogućnosti dijagnostičkih aktivnosti za određeno vozilo.	Ugled i klijentovo povjerenje	Umjereno	8
	Financije	Umjereno	10
Ukoliko klijent dođe na popravak vozila a ne pruži mu se potpuna usluga to će utjecat na buduće povjerenje klijenta.	Produktivnost	Umjereno	6
	Zdravlje i sigurnost	Nisko	2
Ukoliko dijagnostički uređaji ne budu radili past će produktivnost rada.	Pravne i zakonske kazne	Nisko	1
	Korisnikova procjena prijetnji	Nisko	0

Rezultat relativnog rizika 27

Slika 11.16. - Drugi scenarij koji je proveo stručni ispitanik

(9) Pristup Ublažavanje

Na temelju ukupnog rezultata rizika, što ćete učiniti?

Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*

Spremnik	Kontrole i rezidualni rizik
Internet	Potrebno je odabrati pružatelja internetskih usluga koji ima veći broj rješenja za prevenciju DOS napada.
Internet	Potrebno je razmotriti mogućnost direktnog povezivanja sa dobavljačem usluga kroz zaštićene privatne kanale.

dodaj stavku

Slika 11.17. - Odabir načina postupanja s rizikom za drugi scenarij koji je proveo stručni ispitanik

Scenarij 3

Koristiti prijedloge? ☑

Informacijska imovina	Baza podataka tehničkih karakteristika	Fizičke vrste napada
Interesno područje	Pristup mrežoj infrastrukturi	

Kvar sklopovske opreme
Krađa računala
Pristup mrežoj infrastrukturi
Krađa prijenosnih medija
Gubitak električnog napajanja
Poplava
Promjena podataka
Uništenje digitalnih zapisa
Krađa digitalnih zapisa
Oštećenje računala
Promjena digitalnih zapisa
Vatra
Virusi (biološki)
Krađa analogni zapisa
Oštećenje prijenosnih medija

Rizik informacijske imovine — Prijetnja

(1) Učesnik *Tko je zadužen za k… interesnog područja*	
(2) Sredstvo *Kako bi to učesnik u… učesnik uradio?*	…im postupanjem prema opremi za vrijeme čišćenja
(3) Motiv *Zbog kojeg razloga j…*	
(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	Uništenje
(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*	Baza mora biti dostupna za vrijeme radnog vremena kako bi se dijagnostika vozila mogla nesmetano provesti
(6) Vjerovatnost *Koja je vjerovatnost da se ovaj scenario prijetnje desi?*	Umjereno

(7) Posljedice *Koje su posljedice za organizaciju i vlasnika informacijske imovinene koje su nastale kršenjem sigurnosnih zahtjeva?*	(8) Ozbiljnost *Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?* Rizično područje___|_Vrijednost_|_ Rezultat		
Ukoliko klijent dođe na popravak vozila a ne pruži mu se potpuna usluga to će utjecat na buduće povjerenje klijenta.	Ugled i klijentovo povjerenje	Umjereno	8
	Financije	Visoko	15
Ukoliko dođe do oštećenja računala za dijagnostičke uređaje doći će do visokih troškova prilikom zamjene opreme.	Produktivnost	Umjereno	6
	Zdravlje i sigurnost	Nisko	2
Ukoliko dijagnostički uređaji ne budu radili past će produktivnost rada.	Pravne i zakonske kazne	Nisko	1
	Korisnikova procjena prijetnji	Nisko	0

Rezultat relativnog rizika 32

Slika 11.18. - Treći scenarij koji je proveo stručni ispitanik

(9) Pristup Ublažavanje

Na temelju ukupnog rezultata rizika, što ćete učiniti?

Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

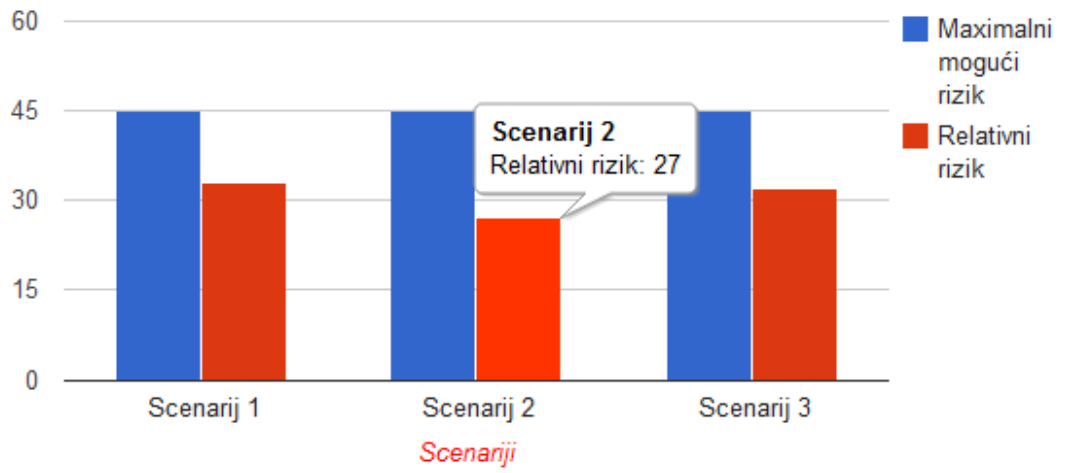
Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*

Spremnik	Kontrole i rezidualni rizik
Dijagnostičko računalo	Potrebno je adekvatno smjestiti centralno računalo u kaveze kako bi se spriječio pristup neautoriziranog osoblja računalu.
Dijagnostičko računalo	Potrebno je uputiti osoblje koje ima pristup centralnom računalu kako se treba ponašati prema toj opremi za vrijeme izvođenja svoga posla.

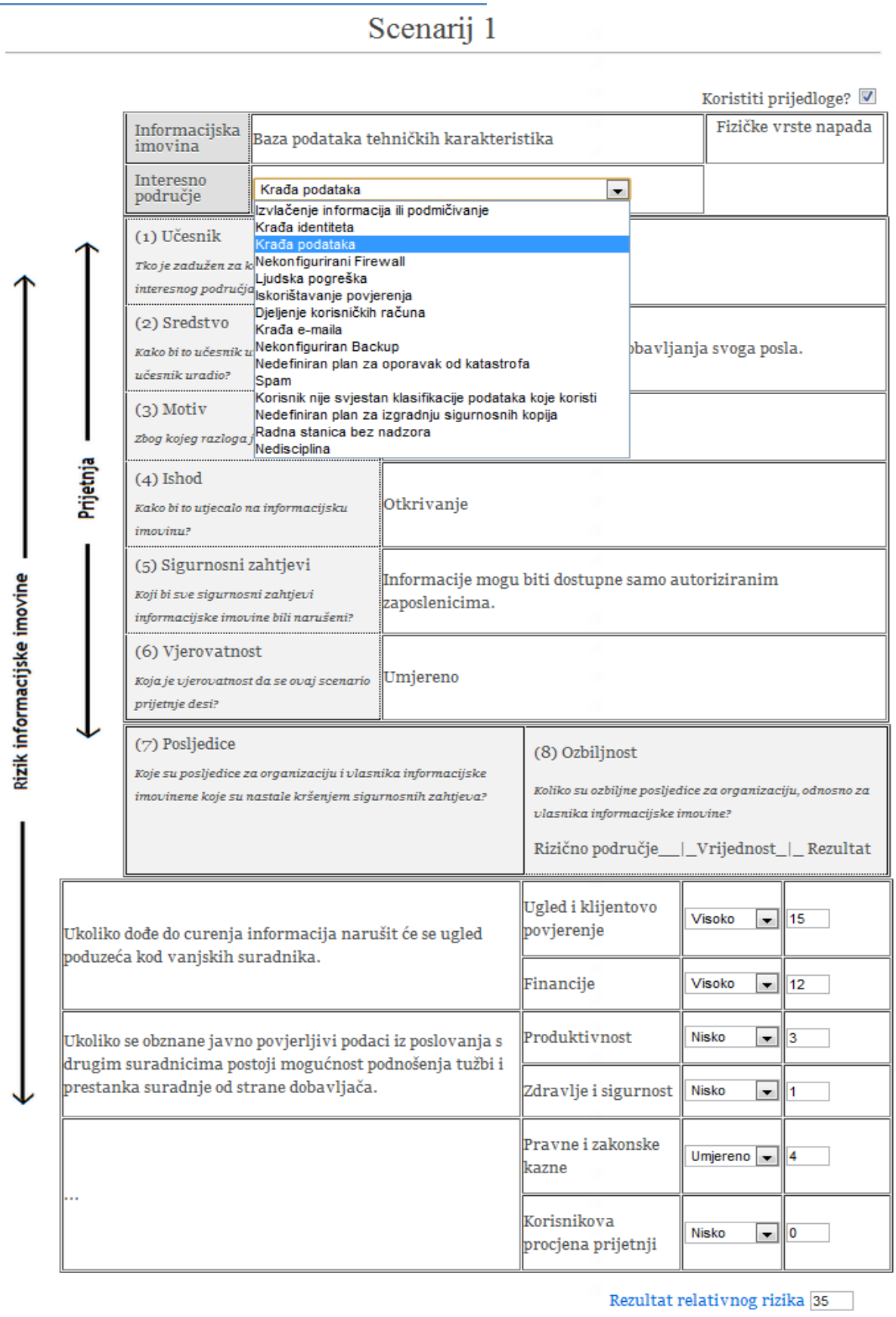
dodaj stavku

Slika 11.19. - Odabir načina postupanja s rizikom za treći scenarij koji je proveo stručni ispitanik



Grafikon 11.1. - Usporedba relativnih veličina rizika za scenarije koje je proveo stručni ispitanik

Relativni rizik predstavlja vrijednost koja je izračunata na osnovu podataka iz prepoznatih scenarija, dok maksimalni mogući rizik predstavlja najveći rizik po pojedinom scenariju.



Slika 11.20. - Prvi scenarij koji je proveo nestručni ispitanik

(9) Pristup Ublažavanje

Na temelju ukupnog rezultata rizika, što ćete učiniti?

Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

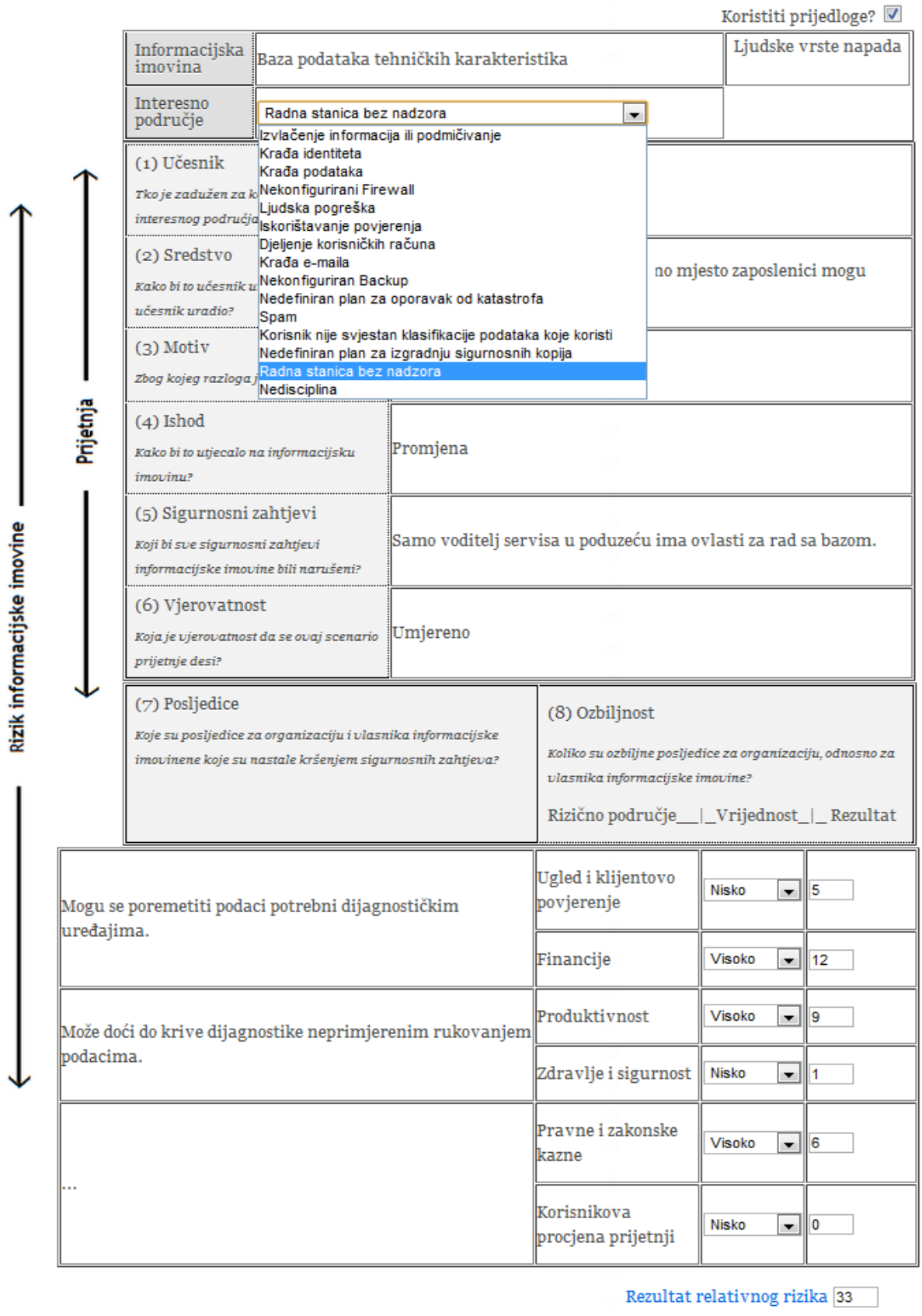
Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*
Spremnik	**Kontrole i rezidualni rizik**
Zaposlenici	Ugovorom obavezati zaposlenike za zabranu prenošenja povjerljivih podataka iz baze ukoliko dođu do njih.

dodaj stavku

Slika 11.21. - Odabir načina postupanja s rizikom za prvi scenarij koji je proveo nestručni ispitanik

Scenarij 2



Slika 11.22. - Drugi scenarij koji je proveo nestručni ispitanik

(9) Pristup ublažavanjem

Na temelju ukupnog rezultata rizika, što ćete učiniti?

Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*

Spremnik	Kontrole i rezidualni rizik
Zaposlenici	Raspodjela dužnosti zaposlenika
Baza podataka tehničkih karakteristika	Autorizacija prilikom korištenja

dodaj stavku

Slika 11.23. - Odabir načina postupanja s rizikom za drugi scenarij koji je proveo nestručni ispitanik

Scenarij 3

Koristiti prijedloge? ☐

Informacijska imovina	Baza podataka tehničkih karakteristika
Interesno područje	Krađa računala

Prijetnja

(1) Učesnik *Tko je zadužen za kontrolu određenog interesnog područja ili rizika?*	Čuvar
(2) Sredstvo *Kako bi to učesnik uradio? Što bi učesnik uradio?*	Neobavljanjem svoga posla.
(3) Motiv *Zbog kojeg razloga je učesnik to uradio?*	Financijska dobit
(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	Prekid
(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*	Otuđenjem opreme
(6) Vjerovatnost *Koja je vjerovatnost da se ovaj scenario prijetnje desi?*	Nisko

Rizik informacijske imovine

(7) Posljedice *Koje su posljedice za organizaciju i vlasnika informacijske imovinene koje su nastale kršenjem sigurnosnih zahtjeva?*	(8) Ozbiljnost *Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?* Rizično područje___|_Vrijednost_|_ Rezultat		
Značajna financijska šteta pošto se radi o skupoj računalnoj opremi.	Ugled i klijentovo povjerenje	Visoko	15
	Financije	Visoko	12
Nemogućnost obavljanja poslova dijagnostike u servisu.	Produktivnost	Visoko	9
	Zdravlje i sigurnost	Nisko	1
Narušen ugled	Pravne i zakonske kazne	Umjereno	4
	Korisnikova procjena prijetnji	Visoko	0

Rezultat relativnog rizika 41

Slika 11.24. -Treći scenarij koji je proveo nestručni ispitanik

(9) Pristup Ublažavanjem

Na temelju ukupnog rezultata rizika, što ćete učiniti?

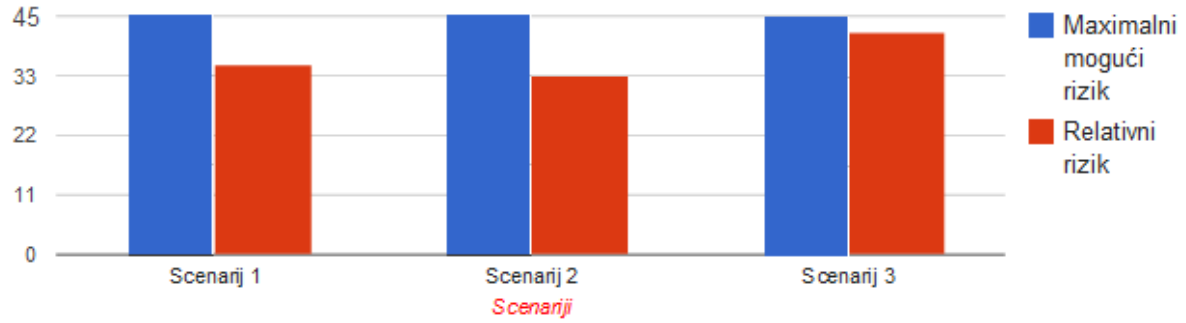
Prihvaćanje	Odgađanje	Ublažavanje	Prebacivanje

Za rizike koje ste odlučili ublažiti **, odradite sljedeće:**

Na koji spremnik informacijske imovine ćete primjeniti kontrole?	*Koje administrativne, tehničke i fizičke kontole ćete primjenitiza ovaj spremnik informacijske imovine? Koji rezidualni rizik će biti prihvaćen od strane organizacije ?*
Spremnik	**Kontrole i rezidualni rizik**
Čuvar	Obavezati čuvara na isplatu štete u slučaju neodgovornog rada.
Baza podataka tehničkih karakteristika	Ograničit fizički pristup bazi podataka.

dodaj stavku

Slika 11.25. - Odabir načina postupanja s rizikom za treći scenarij koji je proveo nestručni ispitanik



Grafikon 11.2. - Usporedba relativnih veličina rizika za scenarije koje je proveo nestručni ispitanik

Na temelju prikupljenih podataka iz provedenih procjena može se vidjeti kako je nestručni korisnik koristio katalog najčešćih napada na sigurnost u 66.66% scenarija dok je stručni korisnik koristio katalog u 33.33% scenarija. Stručni korisnik je procijenio relativni rizik 33 za prvi scenarij, 27 za drugi scenarij i 32 za treći scenarij. Nestručna osoba je procijenila relativni rizik 35 za prvi scenarij, 33 za drugi scenarij i 41 za treći scenarij. Razlika između ukupnog procijenjenog relativnog rizika stručne i nestručne osobe iznosi 17 jedinica. Na temelju prikupljenih podataka može se zaključiti kako uz pomoć razvijene aplikacije i slabo sigurnosno educirani korisnici mogu provesti zadovoljavajuću procjenu rizika.

Nestručna osoba je odmah počela koristiti katalog, čime se osiguralo da u obzir dođu napadi koji su najznačajniji za informacijsku imovinu nad kojoj se provodi procjena. Stručni korisnik je koristio katalog kao pomoćno sredstvo pošto raspolaže određenim iskustvom i znanjem. Ispitanici nisu jednako odabrali scenarije, ali se njihove procjene ne razlikuju značajno.

12. Zaključak

Danas se poslovni procesi u poduzećima sve više oslanjaju na informacijsku potporu kako bi se povećala učinkovitost poslovanja i prilagodilo zahtjevima iz okoline, no kao posljedica toga povećava se i sigurnosni rizik za poduzeće. Upravo se zbog toga u poduzećima moraju provoditi procjene rizika te implementirati mjere za njegovo smanjenje.

Osnovni zahtjevi u funkcioniranju informacijskih sustava su da se sve poslovne aktivnosti neprekidno i pravilno odvijaju. Iz toga proizlazi da prijetnje informacijskim sustavima te procesima predstavljaju i prijetnju kvaliteti poslovne aktivnosti i efikasnosti. Ukoliko poslovne informacije postanu raspoložive konkurentima, postanu tehnički oštećene tijekom prijenosa, netočne ili obrisane, postavlja se pitanje integriteta poslovne aktivnosti što najčešće dovodi i do velikih materijalnih gubitaka što automatski rezultira i ispadanjem iz "utrke" ili stavlja konkurenciju u bolji položaj na tržištu. Sve ovo u konačnici daje i jasno ekonomsko opravdanje investicija u sigurnost, jer one direktno proizlaze iz poslovne strategije i mjerljive su na strateškom nivou.

Kroz rad je objašnjena važnost informacijske tehnologije u poslovanju poduzeća te povezanost sigurnosnog rizika sa primjenom informacijske tehnologije. Zbog toga je neophodno u takvim poduzećima uvesti upravljanje rizikom. Bez procjene rizika nije moguće provesti upravljanje rizikom.

U radu je prikazana prva hipoteza u kojoj se pretpostavilo kako katalozi napada na sigurnost koji postoje u svijetu nisu primjenjivi na svim regionalnim područjima. Hipoteza je dokazana kroz analizu podataka dobivenih iz provedene ankete u kojoj su stručnjaci iz područja informacijske sigurnosti naveli prijetnje za koje je moguće da su prisutne u RH. Kako rezultati pokazuju razlike, te je broj stvarno ostvarenih napada puno manji od onih koji su mogući, prva hipoteza je dokazana. Druga hipoteza u kojoj se pretpostavilo da razvijenu aplikaciju za procjenu rizika mogu zadovoljavajuće koristiti i slabo sigurnosno educirani korisnici, pokazala se kao točna kroz analizu podataka dobivenih iz provedenih ispitivanja u kojem su sigurnosno needucirani korisnik i educirani korisnik koristili aplikaciju za procjenu rizika. Kako su rezultati testa pokazali da nema velike razlike u rezultatima same procjene rizika, dokazana je i druga hipoteza.

Ovim radom se dao doprinos razvoju, pojednostavljenju te povećanju pristupačnosti procjene rizika kroz provedena istraživanja, razradu prethodno postavljenih hipoteza i razvojem aplikacije kroz koju se implementira procjena na način da ju mogu provesti i prosječno informatički pismeni korisnici, a ne samo stručnjaci iz područja informacijske sigurnosti.

13. Literatura

[1]. "419" Scam: Advance Fee / Fake Lottery Scam <dostupno na http://www.419scam.org/ >, [očitano 05.03.2011.]

[2]. Auger, R.: Routing Detour < dostupno na http://projects.webappsec.org/w/page/13246956/Routing-Detour >, [očitano 06.03.2011.]

[3]. Auger, R.: SSI Injection < dostupno na http://projects.webappsec.org/w/page/13246964/SSI-Injection >, [očitano 10.03.2011.]

[4]. Auger, R.: XML Injection < dostupno na http://projects.webappsec.org/w/page/13247004/XML-Injection >, [očitano 7.03.2011.]

[5]. Auger, R.: XPath Injection < dostupno na http://projects.webappsec.org/w/page/13247005/XPath-Injection >, [očitano 7.03.2011.]

[6]. Auger, R.: XQuery Injection < dostupno na http://projects.webappsec.org/w/page/13247006/XQuery-Injection >, [očitano 7.03.2011.]

[7]. Bača, M.: Uvod u računalnu sigurnost, Narodne novine d.d., Zagreb: 2004.

[8]. Bača, M.;The risk assessment of information system security, Fakultet organizacije i informatike, Sveučilište u Zagrebu.< dostupno na http://cuc.carnet.hr/cuc2004/program/radovi/a5_baca/a5_full.pdf >, [očitano 07.10.2010]

[9]. Barbara Guttman,B.; Bagwill, R.; (1997) , Internet Security Policy: A Technical Guide, NIST International Standard ISO/IEC 17799, < dostupno na http://www.rxn.com/services/faq/internet/ISPTG.html >, [očitano 02.10.2010].

[10]. BERR; Department for Business Enterprise & Regulatory Reform . (2008), Technical report: Information Security Breaches Survay. Technical report., < dostupno na http://www.bis.gov.uk/files/file45714.pdf >, [očitano 03.10.2010].

[11]. BJA: Internet Crime Complaint Center < dostupno na http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf >, [očitano 05.03.2011.]

[12]. Brynjolfsson, E.; Saunders, A.; How Information Technology Is Reshaping the Economy < dostupno na http://mitpress.mit.edu/books/chapters/0262013665chap1.pdf >, [očitano 05.02.2011.]

[13]. Butler, S., A.; Security Attribute Evaluation Method., Pittsburgh: School of Computer Science., 2003.

[14]. Carnet: Analiza alata Skipfish < dostupno na http://security.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-08-308.pdf>, [očitano 04.03.2011.]

[15]. Carnet: Brute force napadi < dostupno na http://security.lss.hr/documents/Bruteforcenapadi.html >, [očitano 25.02.2011.]

[16]. Carnet: CSRF napadi < dostupno na http://security.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-04-297.pdf >, [očitano 25.02.2011.]

[17]. Carnet: Metode zaštite dokumenata < dostupno na http://security.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf >, [očitano 08.03.2011.]

[18]. Carnet: Napredne tehnike socijalnog inženjeringa < dostupno na http://security.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-02-292.pdf >, [očitano 09.03.2011.]

[19]. Carnet: Pharming < dostupno na http://security.lss.hr/documents/Pharming.html >, [očitano 06.03.2011.]

[20]. Carnet: Pojmovnik < dostupno na http://www.carnet.hr/tematski/sigurnost/pojmovnik.html >, [očitano 28.02.2011.]

[21]. Carnet: Provjera ranjivosti web aplikacija korištenjem WebScarab alata < dostupno na http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2007-07-199.pdf >, [očitano 1.03.2011.]

[22]. Carnet: Web 2.0 – sigurnosni rizici < dostupno na http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2008-11-245.pdf >, [očitano 24.02.2011.]

[23]. CERT: Software Engineering Institute., Octave Allegro < dostupno na http://www.cert.org/octave/allegro.html >, [očitano 01.11.2010].

[24]. Cisco: Cyber kriminal sve više prelazi s Windowsa na druge operativne sustave i mobilne platform < dostupno na http://www.cisco.com/web/HR/news/2011/2011_news_s02.html >, [očitano 07.03.2011.]

[25]. Chervenak Ann L ., Vivekanand Vellanki and Zachary Kurmas: Protecting File Systems - A Survey of Backup Techniques, Proceedings Joint NASA and IEEE Mass

Storage Conference, 1998., http://www.isi.edu/~annc?papers.html>, [očitano 08.10.2010.]

[26]. Consumer Fraud Reporting: FBI Scams -Ver 3 < dostupno na http://www.consumerfraudreporting.org/fakegovt_FBIv3.php >, [očitano 28.02.2011.]

[27]. Cromwell-intl: Network Monitoring and Packet Sniffing Tools < dostupno na http://cromwell-intl.com/security/monitoring.html >, [očitano 05.03.2011.]

[28]. DeLuccia, J.: Third Party Fraud - Breaking down Trust < dostupno na http://www.itcomplianceandcontrols.com/2009/08/04/third-party-fraud-breaking-down-trust/ >, [očitano 12.03.2011.]

[29]. Dodik, I.: Zaštita ranjivosti mreže od DoS napada < dostupno na http://www.fer.hr/_download/repository/kvalifikacijski-ivica-dodig.pdf >, [očitano 06.03.2011.]

[30]. Ekenberg L., Danielson M.: Handling Imprecise Information in risk Management, < dostupno http://www.dsv.su.se/~mad/what.html>, [očitano 16.01.2003].

[31]. Emery, D.: 'Hit Man' Scam Email <dostupno na http://urbanlegends.about.com/library/bl_hit_man_scam.htm >, [očitano 1.03.2011.]

[32]. ETFOS: Sigurnost u računalnim mrežama < dostupno na http://www.etfos.hr/upload/OBAVIJESTI/obavijesti_preddiplomski/11825sigurnost_2009.pdf>, [očitano 08.03.2011.]

[33]. Fingerprinting Port80 Attacks: A look into web server, and web application attack signatures: Part Two < dostupno na http://www.cgisecurity.com/fingerprinting-port80-attacks-a-look-into-web-server-and-web-application-attack-signatures-part-two.html >, [očitano 1.03.2011.]

[34]. Guberović, J. : Informacijsko ratovanje. Varaždin: 2009. <dostupno na https://export.writer.zoho.com/public/zavrsni.rad1/guberovi%C4%87_informacijsko-ratovanje1/fullpage>, [očitano 28.02.2011.]

[35]. Humphreys E J , Guide to BS 7799 Risk Assessment and Risk Management, British Standards Institution, London, 1998.

[36]. Hutinski, Ž.; Bilješke sa predavanja: Sigurnost informacijskih sustava. Varaždin, FOI, 2010/2011.

[37]. Hutinski, Ž.; Krakar, Z.; Procjena rizika kao dio sustava upravljanja sigurnošću informacija, Zbornik radova - CASE14, Opatija, 2002.

[38]. INFIGO;Information Security. < dostupno na http://www.infigo.hr/hr/dokumenti >, [očitano 05.10.2010].

[39]. Internet Crime Complaint Center (IC3): Internet Crime Repor 2009. < dostupno na http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf >, [očitano 12.02.2010].

[40]. ISSA; Information Systems Security Association., < dostupno na https://www.issa.org/ >, [očitano 03.10.2010].

[41]. Javin network management & security: ICMP Flood < dostupno na http://www.javvin.com/networksecurity/ICMPFlood.html >, [očitano 1.03.2011.]

[42]. Jourdan, G. V.: Command Injections < dostupno na http://www.site.uottawa.ca/~gvj/Courses/CSI4539/lectures/CommandInjections.pdf >, [očitano 12.03.2011.]

[43]. Kabay, M. E.: Salami Fraud < dostupno na http://www.mekabay.com/nwf/116p%20--%20Salami%20Fraud.pdf >, [očitano 07.03.2011.]

[44]. Kalpić, D.: Obrazovni materijali < dostupno na http://www.zpr.fer.hr/zpr/LinkClick.aspx?fileticket=XqesXb40te4%3D&tabid=129&mid=590&language=hr-HR >, [očitano 7.03.2011.]

[45]. Krause, M.; Harold, F. T.; Handbook of Information security management. Auerback Publications., 2002.

[46]. K.rutz, R., L.; Vines, D., V.; The CISSP Prep Guide - Mastering the Ten Domains of Computer Security, Toronto: John Wiley & Sons, Inc., 2001.

[47]. Lider: Prevare na društvenim mrežama sve učestalije < dostupno na http://www.liderpress.hr/Default.aspx?sid=119452 >, [očitano 04.03.2011.]

[48]. Meter, M; SAP: Poslovni informacijski sustavi: značaj, svrha, integriranost (2) < http://www.sapmag.com.hr/show_article.php?id=398 >, [očitano 04.02.2011.]

[49]. MyCERT: Incident Statistics for the year 2010. < dostupno na http://www.mycert.org.my/en/services/statistic/mycert/2010/main/detail/725/index.html >, [očitano 18.02.2011.]

[50]. OWASP: Path Traversal < dostupno na http://www.owasp.org/index.php/Path_Traversal >, [očitano 05.03.2011.]

[51]. Paltier,T. R.: Information Security Risk Analysis, Aurbach: New York, 2001.

[52]. Paltier,T. R.: Information Security Risk Analysis, CRC Press LLC,Boca Raton, Florida, 2000.

[53]. Paralliverse: URL Redirection Attack With Examples < dostupno na http://log0.wordpress.com/2008/06/23/url-redirection-attack-with-examples/ >, [očitano 07.03.2011.]

[54]. Peloquin: SSL protokol < dostupno na http://fly.srk.fer.hr/~peloquin/SSL/ssl.html >, [očitano 09.03.2011.]

[55]. Petrović, K.: Ispitivanje sigurnisti mrežne opreme na uobičajene mrežne napade < dostupno na http://bib.irb.hr/datoteka/449851.Diplomski_-_Kreimir_Petrovi_ISO19005-1-PDFA.pdf >, [očitano 18.02.2011.]

[56]. Reeker Jones: Measuring the Impact of information on Complex Systems, < dostupno na http://www.isd.mel.nist.gov/research_areas/research_engineering/Performance_Metrics/PerMIS_2001_Proceedings/Reeker_Jones.pdf >, [očitano 08.10.2010].

[57]. Sajko, M.; (2004), Usporedba metoda procjene rizika sigurnosti IS-a, Magistarski rad, Fakultet organizacije i informatike, Sveučilište u Zagrebu.

[58]. Saunders H. John: A Risk Management Methodology for Information Security: The Analytic Hierarchy Process, <dostupno na http://www.johnsaunders.com/papers/risk-ahp/risk-ahp.htm >, [očitano 07.10.2010].

[59]. SearchSecurity: Blended threat < dostupno na http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci961251,00.html >, [očitano 12.03.2011.]

[60]. Search software quality: LDAP injection < dostupno na http://searchsoftwarequality.techtarget.com/definition/LDAP-injection>, [očitano 04.03.2011.]

[61]. Spremić, M.: Primjena IT u financijskom izvještavanju Računovodstveni informacijski sustavi. CGEIT: Ekonomski fakultet Zagreb

[62]. Srića, V.: Informatički inženjering i menadžment. Drip: Zagreb, 1990.

[63]. Srića, V.; Spremić, M.: Informacijskom tehnologijom do poslovnog uspjeha. Sinergija: Zagreb, 2000.

[64]. Stoneburner, G.; Goguen, A.; Feringa, A.; Risk Management Guide for Information Technology Systems. Gaithersburg: NIST Special Publication., 2002.

[65]. Suhina, V.: Automatizirano traženje sigurnosnih propusta u web aplikacijama < dostupno na http://www.zemris.fer.hr/~sgros/publications/diploma_thesis/suhina_vanja_diplomski.pdf >, [očitano 18.02.2011.]

[66]. Tomić, I.: Penetracijsko ispitivanje sigurnosti računalnog sustava < dostupno na http://os2.zemris.fer.hr/ns/2008_tomic/skeniranje.html >, [očitano 07.03.2011.]

[67]. The Web Application Security Consortium (WASC) : WWeb Application Security Statistics Project 2007. < dostupno na https://files.pbworks.com/download/f2lIgLtUEl/webappsec/13247068/wasc_wass_2007.pdf >, [očitano 02.02.2010].

[68]. Vose D.: Risk Analysis – A Quantitative Guide 2nd edition, John Wiley & Sons, 2001.

[69]. Zdrnja, B.: Interesting PHP injection < dostupno na http://isc.sans.edu/diary.html?storyid=9478 >, [očitano 06.03.2011.]

[70]. Zelanto, M.: Cross site scripting < dostupno na http://os2.zemris.fer.hr/ns/malware/2007_zelanto/xss.html >, [očitano 25.02.2011.]

[71]. Zelanto, M.: Napad formatiranim nizom znakova <dostupno na http://os2.zemris.fer.hr/ns/malware/2007_zelanto/format.html >, [očitano 1.03.2011.]

[72]. Zelanto, M.: Prekoračenje kapaciteta međuspremnika na stogu <dostupno na http://os2.zemris.fer.hr/ns/malware/2007_zelanto/buffer.html >, [očitano 25.02.2011.]

[73]. Zelanto, M.: SQL injekcija < dostupno na http://os2.zemris.fer.hr/ns/malware/2007_zelanto/sql.html >, [očitano 10.03.2011.]

[74]. ZSIS: Osnovni računalno-sigurnosni rizici < dostupno na http://www.zsis.hr/site/Preporuke/Osnovnira%C4%8Dunalnosigurnosnirizici/tabid/105/Default.aspx >, [očitano 11.03.2011.]

[75]. ZSIS: Virusi, crvi i trojanski konji < dostupno na http://www.zsis.hr/site/Preporuke/Virusicrviitrojanskikonji/tabid/100/Default.aspx>, [očitano 18.01.2011.]

14. Dodatak A

Tehnička dokumentacija web aplikacije

Kako je metoda vrlo kompleksna, a cilj aplikacije je da korisniku provedba procjene rizika po njoj bude jednostavnija, puno se pažnje posvetilo prezentacijskom dijelu aplikacije. Prilagodba prezentacijskog dijela išla je prema tome da izlaz iz aplikacije izgleda kao dokument.

Korištene tehnologije i testiranje:

- Stranica je izrađena u HTML-u, PHP-u, Javascriptu te jQuery-u
- Stranica je izrađena uzimajući u obzir konzistentnost dizajna
- Ispitana je na slijedećim web preglednicima:

1. ***Google Chrome (preporuka developera)***
2. *IE8*
3. *Mozilla Firefox (3.6 i 4)*
4. *Opera 10*

Kao jezik izrade aplikacije odabran je HTML, odnosno aplikacije je napravljena kao web stranica iz razloga što je distribucija tako najlakša, dostupna je na svim platformama, te se može koristiti neovisno o lokaciji. Za napredne mogućnosti aplikacije zadužene su napredne mogućnosti jQuery-a. PHP se koristio kod pohrane i učitavanja podataka u i iz baze podataka. Treba naglasiti da je zbog količine podataka dizajniranje baze podataka bilo vrlo zahtjevno.

Anonimni korisnik ima prava:

- *Pregled početne stranice koja ukratko opisuje metodu i alat*
- *Pregled i korištenje kontakt obrasca*
- *Registracije*

Prijavljeni korisnik ima uz prava anonimnog korisnika i:

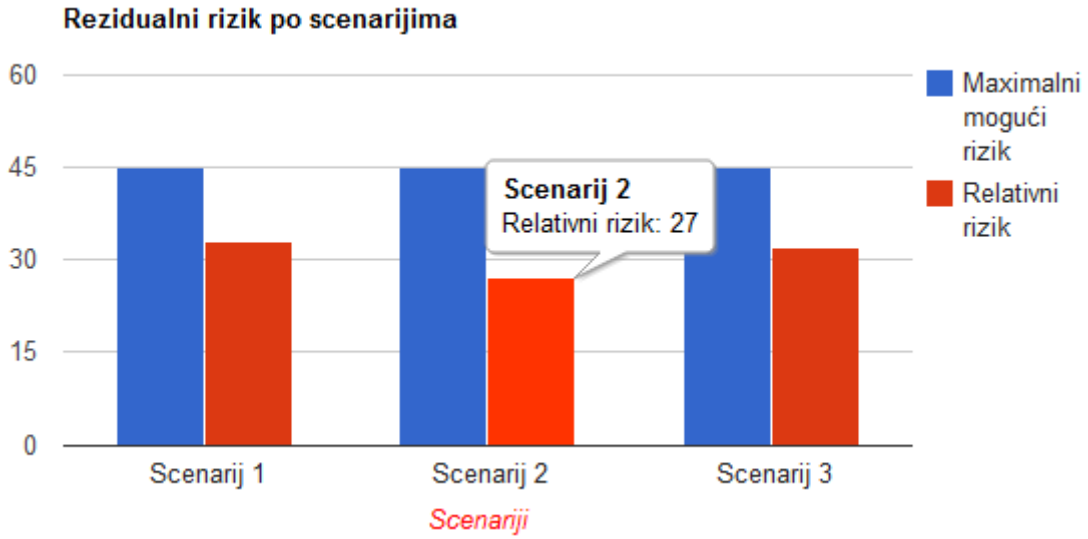
- *Prijave*
- *Kreiranja dokumenta procjene*
- *Pohranu dokumenta procjene*

- *Ažuriranje dokumenta procjene*
- *Učitavanje dokumenta procjene*
- *Brisanje dokumenta procjene*
- *Preuzimanje kompletne izvorne dokumentacije metode Octave Allegro na hrvatskom jeziku*
- *Preuzimanje kompletne izvorne dokumentacije Octave Allegro na engleskom jeziku*
- *Preuzimanje primjera procjene napravljene od OctaveAllegroTeam-a*
- *Preuzimanje praznih Octave Allegro radnih tablica i upitnika za vlastito korištenje*
- *Uvid u rječnik pojmova bitnih za korištenje metode*
- *Uvid u upute za procjenu rizika*

Napredne mogućnosti i korišteni dodaci

Google graph

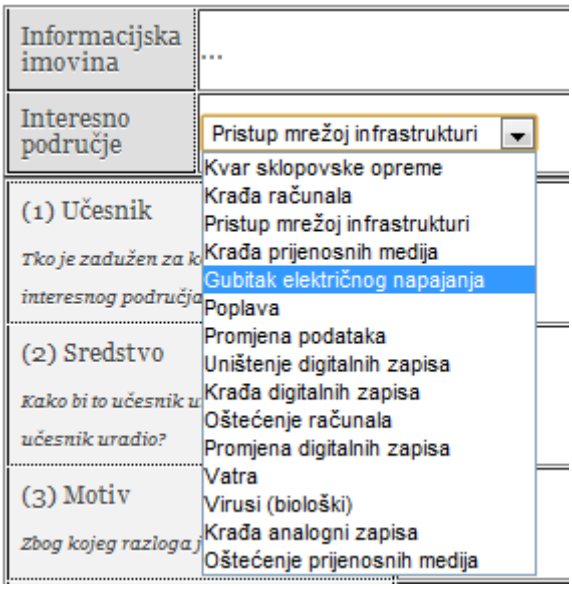
Ovaj dodatak je korišten za iscrtavanje grafikona koji prikazuje relativne rizike u odnosu na maksimalni mogući rizik s obzirom na dodijeljene prioritete. Rađen je u jQuery-u te je jednostavan za implementaciju i razumijevanje, te vizualno atraktivan.



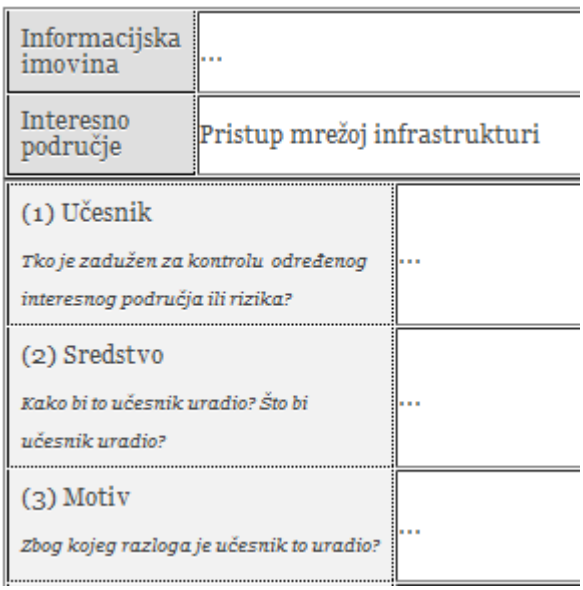
Grafikon 14.1. - Grafikon relativnih rizika

Edit in place

Mogućnost pretvaranja elemenata za unos prilično je bitno kod ove aplikacije radi već prije spomenutog prezentacijskog dijela. Bez ovog elementa dokument procjene bio bi pun elemenata za unos kao što su: polja za unos teksta, padajući izbornici, polja za jednostruki i višestruki odabir...



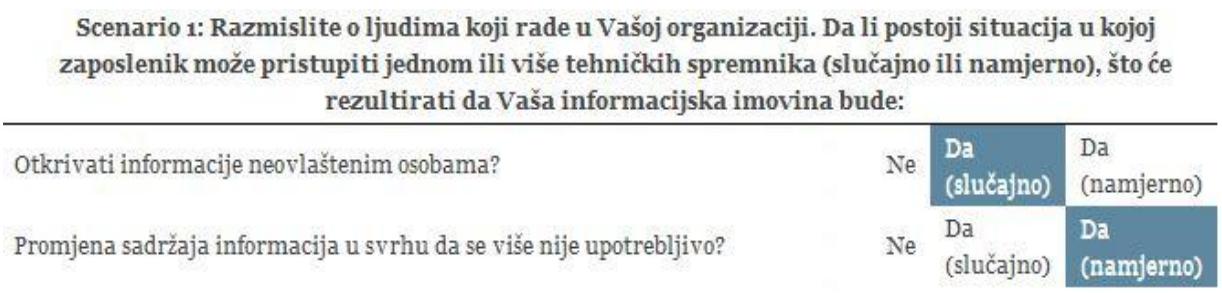
Slika 14.1. - Odabir opcije s padajućeg izbornika



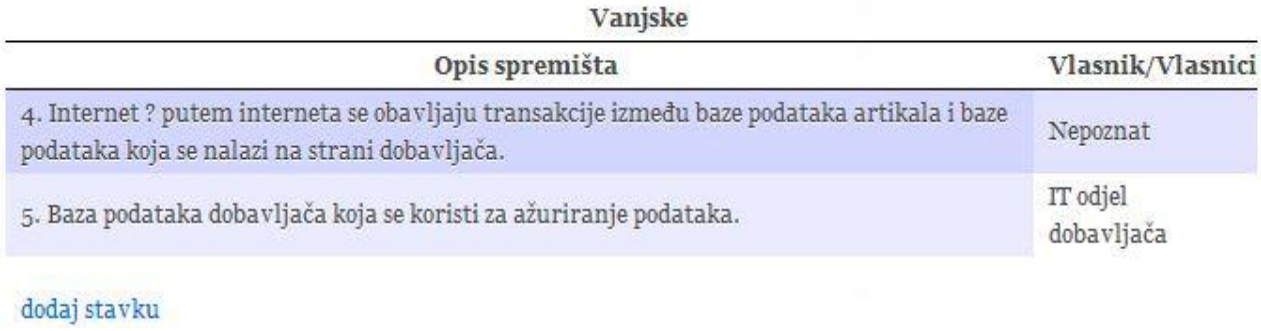
Slika 14.2. - Pretvorba odabira u običan tekst!

Data tables

Ovaj dodatak omogućio je izbjegavanje korištenja radio buttona i checkboxeva kao klasičnih elemenata web stranice, kao i već gotove funkcije za dinamičko dodavanje redova u tablice i sl. Iako je bilo vrlo teško prilagoditi ovaj dodatak da radi na pravilan način odnosno na način kako metoda zahtjeva, opet je uvelike olakšao posao. Pruža vizualnu atraktivnost te je iznimno jednostavan za korištenje. Dinamičko dodavanje redova vrši se jednostavnim pritiskom na „dodaj stavku“ prilikom čega se bez ikakvog osvježavanja stranice dobiva dodan red u tablici. Ovdje je na svaku ćeliju implementiran i ***edit in place*** dodatak kako bi se ona mogla editirati.



Slika 14.3. - Označavanje colona (zamjena za klasične radio buttone)



Slika 14.4. - Dinamičko dodavanje redova

aBuzz

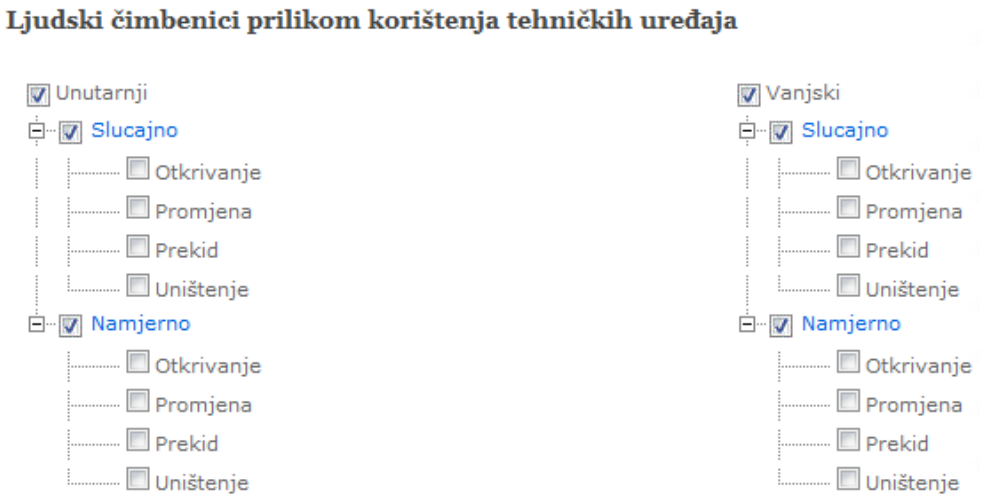
Dodatak korišten za fiksnu navigaciju s lijeve strane. Iznimno koristan dodatan jer je metoda toliko opširna da ukoliko se sve opcije otkriju, te ode 2 koraka niže te se pokuša vratiti na vrh korištenjem miša, za takvu radnju bilo bi potrebno više od minute što je nedopustivo. Korišten je u kombinaciji sa ***jScrolling*** kako bi prijelazi bili glatki.

jScrolling

Scrolling efekt kojeg je nemoguće prikazati slikom ekrana. Zamjenjuje klasičan skok na označeno sidro unutar stranice

dTree

Dodatak korišten za izradu „stabala“ u koraku 5. Jednostavan za korištenje te omogućava korisniku lijep prikaz.



Slika 14.5. - Stabla s prikazom čimbenika po kategorijama

Popis datoteka

PHP datoteke

index.php

- *Glavna datoteka koja sadrži kompletnu implementaciju metode i korisnički prikaz iste*

octaveSave.php

- *Pohranjuje trenutni dokument*

octaveLoad.php

- *Učitava tablicu pohranjenih dokumenata iz za prijavljenog korisnika*

octave.php

- *Učitava odabran dokument iz tablice svih dokumenata trenutno prijavljenog korisnika*

octaveNazivTrenutneDatoteke.php

- *Pribavlja naziv trenutno učitanog dokumenta*

octaveCheckbox.php

- *Pohranjuje 64 checkboxa koja se mogu označiti u 5. koraku metode*

octaveText.php

- *Pohranjuje sve inputTypeText dijelove dokumenta unutar metode*

octaveRegister.php

- *Šalje i provjerava podatke korisnika prilikom njegove registracije*

octaveCheckUsername.php

- *Provjerava zauzeće username-a te vraća je li slobodno ili zauzeto*

octaveActivate.php

- *Služi za provjeru valjanosti korisničkog pokušaja aktivacije te samo njeno provođenje*

octaveLogin.php

- *Provjerava korisničke podatke unesene kod prijave, te ako postoje u bazi pohranjuje korisničke podatke u sesiju*

octaveLogout.php

- *Uništava korisničku sesiju*

octaveScenariji.php

- *Pribavlja podatke o status scenarija: koliko ih je dodano u dokumentu koji se pokušava učitati, koliko je i kojih polja popunjeno itd...*

octaveDelete.php

- *Briše dokument procjene odabran iz tablice svih dokumenata za prijavljenog korisnika*

octaveUpdate.php

- *Pohranjuje novo nastale promjene u trenutno učitanom dokumentu u bazu pod istim imenom*

server_processing_post.php

- *Služi za obradu unosa u ćelije tablica*

Javascript datoteke

main.js

- *Glavna js datoteka koja sadrži sve funkcije obrade događa za elemente stranice*

js_RegistracijaNovogKorisnika.js

- *Provjera ispravnosti korisničkih podataka prilikom registracije*

dataTables.js

- *Omogućuje napredan rad s tablicama: dinamičko dodavanje redova je mogućnost koja je najbitnija u širokom spektru ponuđenih*

scrooling_jquery.easing.1.3.js

- *Omogućuje „smooth scrolling" efekt odnosno glatko kretanje kroz stranicu prilikom korištenja sidra (eng. anchors)*

abuzz_main-ui-resize.js

- *Omogućuje funkcionalnost dijela navigacije s lijeve stranice*

editinplace.js

- *Omogućuje pretvaranje pojedinih elemenata unosa u text:*
  → select box-eva, ćelija tablice...

editinplaceTextarea.js

- *Izdvojena prije navedena funkcionalnost samo za element unosa: Textarea*

jquery.nivo.slider.js

- *Datoteka zadužena za funkcionalnost slidera*

Web stranica je dostupna na sljedećoj adresi: **http://risk.foi.hr/**

15. Dodatak B

Forma Ankete

Tablica 15.1. - Tehničke vrste napada

	Vrste napada na sigurnost				
Br.	Najčešći napadi u svijetu	Područje Republike Hrvatske	Moguće posljedice	Učestalost prijetnje	Rezultat
1	Adware				
2	ARP prigušenje (eng. ARP throttling)				
3	ASP Injection				
4	ATM prijevare				
5	Aukcijske prijevare				
6	Bluetooth prijevare (eng. Blue-jacking)				
7	Botnet				
8	Brute Force napad				
9	Buffer Overflow				
10	Cross-Site Request Forgery (CSRF)				
11	Cross-Site Scripting (XSS)				
12	Crv				
13	Curenje tekućine iz instalacija				
14	Dialeri				
15	Distributed Denial of Service (DDoS)				
16	Eksplozija				
17	Elektromagnetska radijacija				
18	EMP bombe				
19	FBI prijevara				
20	Fingerprinting				
21	Format String napad				
22	Greške sklopovskih čipova				
23	Gubitak električnog napajanja				
24	HERF pištolji				
25	Hitman prijevara				
26	Hoax				
27	HTTP Response Splitting				
28	Humanitarne prijevare				
29	ICMP Flood				
30	Integer Overflow				
31	Iskorištavanje povjerenja				

32	Ispadi opreme				
33	Krađa e-maila				
34	Krađa identiteta				
35	Kvar sklopovske opreme				
36	LDAP Injection				
37	Logičke bombe				
38	Money mulling				
39	Nano mašine i mikrobi				
40	Napad lažnim predstavljanjem (eng. Masquerading attack)				
41	Napadi na Web servere				
42	Napredne prijevare				
43	Neautorizirani interni pristup				
44	Neautorizirani pristup kroz VPN				
45	Neautorizirani vanjski pristup				
46	Nedefiniran plan za izgradnju sigurnosnih kopija				
47	Nedefiniran plan za oporavak od katastrofa				
48	Nedostupnost aplikacija				
49	Nedostupnost baza podataka				
50	Nedostupnost Interneta				
51	Nedostupnost lokalne mreže				
52	Nedostupnost mreže širokog dosega				
53	Nedostupnost servera				
54	Nedozvoljene mrežne aktivnosti				
55	Nekonfiguriran Backup				
56	Nekonfigurirani Firewall				
57	Nekorektni unos znakova (end. Path Traversal)				
58	Neovlaštena izmjena podataka				
59	Neovlaštena izmjena programa				
60	Neovlašteno prikupljanje podataka				
61	Nepotpuno pokrenuti proces				
62	Nezakonite transakcije				
63	Nezaštićene online				

	transakcije				
64	Nigerijska ili 419 prijevara				
65	Oluja razašiljanja (eng. Broadcast storm)				
66	Oštećene baze podataka				
67	Oštećenje računala				
68	Otmice sjednica (eng. Session Hijacking)				
69	Pharming				
70	Phishing				
71	PHP Injection				
72	Pravo pristupa				
73	Prekid komunikacije				
74	Prekid telekomunikacije				
75	Pretraživanje (eng. Scanning)				
76	Preuzimanje HTTP sesije (eng. HTTP session hijacking)				
77	Prijevare s kreditnim karticama				
78	Prisluškivanje				
79	Pristup mrežoj infrastrukturi				
80	Radna stanica bez nadzora				
81	Routing Detour				
82	Salama tehnika				
83	Shell Injection				
84	Smurf napad				
85	Spam				
86	Spoofing (IP, login, web, e-mail, DNS)				
87	Spyware				
88	SQL Injection				
89	SSI Injection				
90	Stražnja vrata (eng. Backdoor)				
91	SYN Flood				
92	Tehničke greške (eng. Bugovi)				
93	Terorističke prijetnje				
94	Trojanski konj				
95	Ucjenjivanje putem email pošte				

96	UDP Flood				
97	Upravljanje tiskanjem (uključujući proizvodnju, distribuciju i uništenje)				
98	URL preusmjeravanje				
99	Uskraćivanje usluge DoS (Denial of Service)				
100	Uspješno kompromitiranje računala				
101	Uznemiravanje zaposlenika (eng. Cyberstalking)				
102	Vanjski izvori nisu dostupni				
103	Virus				
104	Višestruka ugroza (eng. Blended threat)				
105	WiFi prijevare				
106	XML Injection				
107	XML poisoning				
108	XPath Injection				
109	XQuery Injection				
110	Zamka				

Tablica 15.2. - Fizičke vrste napada

	Vrste napada na sigurnost				
Br.	Najčešći napadi u svijetu	Područje Republike Hrvatske	Moguće posljedice	Učestalost prijetnje	Rezultat
1	Alberta Clipper (brzo kretanje niskog tlaka)				
2	Astrofizički fenomeni				
3	Bujica				
4	Bura				
5	Curenje tekućine iz instalacija				
6	Dim				
7	Downburst (jaki vjetar)				
8	El Nino				
9	Električni poremećaj				
10	Elektromagnetska radijacija				
11	Erozija				
12	Erozije plaže				
13	Grad				
14	Grmljavina				
15	Gubitak električnog napajanja				

16	Kisele kiše				
17	Kiša				
18	Kondenzacija				
19	Kozmička zračenja				
20	Krađa analogni zapisa				
21	Krađa digitalnih zapisa				
22	Krađa prijenosnih medija				
23	Krađa računala				
24	Kvar sklopovske opreme				
25	La Nina				
26	Ledena kiša				
27	Magla				
28	Mećava				
29	Meteori				
30	Monsun				
31	Mraz				
32	Munja				
33	Oblačnost				
34	Oborine				
35	Oluja				
36	Oštećenje prijenosnih medija				
37	Oštećenje računala				
38	Otrovi				
39	Pješčana oluja				
40	Poplava				
41	Potresi i vibracije				
42	Prekid telekomunikacije				
43	Prekid telekomunikacije				
44	Pristup mrežnoj infrastrukturi				
45	Pritisak				
46	Promjena digitalnih zapisa				
47	Promjena podataka				
48	Promrzlina				
49	Relativna vlažnost				
50	Rosa				
51	Sezonski fenomeni				
52	Sitna kiša				
53	Smog				
54	Snijeg				
55	Snježna oluja				
56	Snježna vijavica (eng. Drifting snow)				
57	Storm surge (olujni uspor)				
58	Sumaglica				
59	Sunčani fenomeni				

60	Susnježica				
61	Tajfun				
62	Temperatura zraka				
63	Tornado				
64	Tropska oluja				
65	Tsunami				
66	Uništenje analogni zapisa				
67	Uništenje digitalnih zapisa				
68	Uragan				
69	Vatra				
70	Virga (padaline)				
71	Virusi				
72	Vlažnost				
73	Vulkanska erupcija				
74	Zemljotres				
75	Zračne mase				
76	Zračni pritisak				

Tablica 15.3. - Ljudske vrste napada

	Vrste napada na sigurnost				
Br.	Najčešći napadi u svijetu	Područje Republike Hrvatske	Moguće posljedice	Učestalost prijetnje	Rezultat
1	Aukcijske prijevare				
2	Biološke prijetnje				
3	Bluetooth prijevare (eng. Blue-jacking)				
4	Diverzija				
5	Djeljenje korisničkih računa				
6	Eksplozija				
7	FBI prijevara				
8	Fizički napad				
9	Hitman prijevara				
10	Humanitarne prijevare				
11	Ilegalni transport / dostava				
12	Iskorištavanje povjerenja				
13	Izvlačenje informacija ili podmičivanje				
14	Kazneni prijestup				
15	Korisnik nije svjestan klasifikacije podataka koje koristi				
16	Korištenje lažnog imena				
17	Krađa e-maila				
18	Krađa identiteta				

19	Krađa podataka				
20	Krijumčarenje				
21	Ljudska pogreška				
22	Money mulling				
23	Napad lažnim predstavljanjem (eng. Masquerading attack)				
24	Napredne prijevare				
25	Neautorizirani intenri pristup				
26	Neautorizirani pristup				
27	Neautorizirani vanjski pristup				
28	Nedefiniran plan za izgradnju sigurnosnih kopija				
29	Nedefiniran plan za oporavak od katastrofa				
30	Nedisciplina				
31	Neklasifikacija sadržaja				
32	Nekonfiguriran Backup				
33	Nekonfigurirani Firewall				
34	Nemar				
35	Nenamjerno oštećenje imovine				
36	Neodgovarajuća organizacija				
37	Neodgovarajući program				
38	Neovlašten pristup podacima ili imovini				
39	Neovlaštena izmjena podataka				
40	Neovlaštena izmjena programa				
41	Neovlašteno prikupljanje podataka				
42	Nepažnja				
43	Neposlušnost				
44	Nepošteni zaposlenici				
45	Nezadovoljni zaposlenici				
46	Nezakonite transakcije				
47	Neznanje				
48	Nigerijska ili 419 prijevara				
49	Odavanje povjerljivih podataka (objavljivanje)				
50	Onečišćenje zraka				
51	Oponašanje dostavljača				
52	Oštećene baze podataka				

53	Otkrivanje osjetljivih podataka				
54	Phishing				
55	Pobune i protesti civila				
56	Podmetanje požara				
57	Pogrešno objavljivanje povjerljivih podataka				
58	Prijetnja bombom (ekspolzivom)				
59	Prijevare s kreditnim karticama				
60	Prisluškivanje				
61	Provala				
62	Radna stanica bez nadzora				
63	Ratno razaranje				
64	Sabotaža zaposlenika				
65	Shoulder Surfing				
66	Socijalni inženjering				
67	Spam				
68	Strvinarenje				
69	Špijunaža				
70	Štrajk				
71	Terorističke prijetnje				
72	Third-party prijetnje				
73	Trovanje alkoholom				
74	Ucjenjivanje putem email pošte				
75	Umorsto				
76	Upravljanje tiskanjem (uključujući proizvodnju, distribuciju i uništenje)				
77	Uznemiravanje zaposlenika (eng. Cyberstalking)				
78	Uznemirujuća komunikacija				
79	Vandalizam				
80	Vanjski napadači				
81	WiFi prijevare				
82	Zagađenje				
83	Zagrijavanje i uvjeti zraka				
84	Zločin iz mržnje				
85	Zlouporaba ovlasti				

16. Dodatak C

Octave Allegro radne tabele i upitnici

Allegro radna tabela 1	**KRITERIJ MJERA RIZIKA –** Ugled i klijentovo povjerenje		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 2	**KRITERIJ MJERA RIZIKA –** Financije		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 3	**KRITERIJ MJERA RIZIKA –** Produktivnost		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 4	**KRITERIJ MJERA RIZIKA –** Zdravlje i sigurnost		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 5	**KRITERIJ MJERA RIZIKA –** Pravne i zakonske kazne		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 6	**KRITERIJ MJERA RIZIKA –** Korisnikova procjena prijetnji		
Područje prijetnje	**Nisko**	**Umjereno**	**Visoko**

Allegro radna tabela 7	**RADNA TABLICA - DOJELA PRIORITETA ZA UTJECAJNA PODRUČJA**
PRIORITET	**PODRUČJE UTJECAJA**
	Ugled i klijentovo povjerenje
	Financije
	Produktivnost
	Zdravlje i sigurnost
	Pravne i zakonske kazne
	Korisnikova procjena prijetnji

Allegro radna tabela 8	**PROFIL KLJUČNE INFORMACIJSKE IMOVINE**	
(1) Ključna imovina *Što je kritična informacijska imovina?*	**(2) Obrazloženje za izbor** *Zašto je ta informacijska imovina važna za organizaciju?*	**(3) Opis** *Koji je odgovarajući opis za tu informacijsku imovinu?*
(4) Vlasnik / vlasnici *Tko je vlasnik te informacijske imovine?*		
(5) Sigurnosni zahtjevi *Koji su sigurnosni zahtjevi za ovu informacijsku imovinu?*		
❑ **Povjerljivost**	Samo ovlašteno osoblje može vidjeti ovu informacijsku imovinu, a oni su:	
❑ **Integritet**	Samo ovlašteno osoblje može mijenjati ovu informacijsku imovinu, a oni su:	
❑ **Dostupnost**	Ova informacijska imovina mora biti na raspolaganju za određeno osoblje kako bi mogli raditi svoj posao, a oni su:	
	Ova informacijska imovina mora biti na raspolaganju _____ sati, _____ dana / tjedan, _____ tjedana / godišnje.	
❑ **Ostalo**	Na ovu informacijsku imovinu se\odnose posebni zakonski propisi za zaštitu, a oni su:	
(6) Najvažniji sigurnosni zahtjevi *Koji je najvažniji sigurnosni zahtjev za tu informacijsku imovinu?*		
❑ Povjerljivost	❑ Integritet	❑ Dostupnost ❑ Ostalo

Allegro radna tabela 9a	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (TEHNIČKE)**
UNUTARNJE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	
VANJSKE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
5.	
6.	
7.	
8.	

Allegro radna tabela 9b	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (FIZIČKE)**
UNUTARNJE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
1.	
2.	
3.	
4.	
VANJSKE	
OPIS SPREMIŠTA	**VLASNIK / VLASNICI**
5.	
6.	
7.	
8.	

Allegro radna tabela 9c	**MAPA RIZIČNE SREDINE INFORMACIJSKE IMOVINE (LJUDI)**
UNUTARNJE OSOBLJE	
IME ILI ULOGA / ODGOVORNOST	**ODJEL ILI JEDINICA**
1.	
2.	
3.	
4.	
VANJSKO OSOBLJE	
DOBAVLJAČ, PRODAVAČ, ITD.	**ORGANIZACIJA**
5.	
6.	
7.	
8.	

Upitnik za scenarij prijetnji 1	**Tehnički spremnici**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na tehničkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:
Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više tehničkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:
Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Upitnik za scenarij prijetnji – 1 (nastavak)	**Tehnički spremnici**

Scenarij 3:

U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovine na bilo kojem tehničkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- nenamjerno otkrivanje informacijske imovine
- nenamjerna promjena informacijske imovine
- nenamjerni prekid dostupnosti informacijske imovine
- nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine

Aplikacijski kvar	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Pad sustava iz poznatih ili nepoznatih razloga	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Kvar sklopovske opreme	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Izvršenje malicioznog koda (kao što su virusi, crvi, Trojanski konj ili back door)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prekid napajanja za tehničke spremnike informacijske imovine	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Problemi s telekomunikacijom	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Pojava drugih “third-party” problema.	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**

Upitnik za scenarij prijetnji - 2	**Fizički spremnici**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koja se nalazi na fizičkim spremnicima. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:

Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik može pristupiti jednom ili više fizičkih spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:

Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Upitnik za scenarij prijetnji - 2 (nastavak)	**Fizički spremnici**

Scenarij 3:

U ovom scenariju, razmislite o situacijama koje bi mogle utjecati na Vašu informacijsku imovine na bilo kojem fizičkom spremniku koji ste identificirali. Utvrdite da li se desilo jedan od ponuđenih scenarija, ili bi se mogao desiti. U slučaju da se desi potrebno je definirati posljedice sljedećih ishoda:

- nenamjerno otkrivanje informacijske imovine
- nenamjerna promjena informacijske imovine
- nenamjerni prekid dostupnosti informacijske imovine
- nenamjerno trajno uništenje ili privremeni gubitak informacijske imovine

Pojava drugih "third-party" problema.	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**
Prirodne nepogode (poplava, požar, tornado) ili od strane čovjeka (požar, eksplozija)	**Ne**	**Da (otkrivanje)**	**Da (promjena)**	**Da (prekid)**	**Da (gubitak)**

Upitnik za scenarij prijetnji - 3	**Ljudi**

Ova radna tablica će Vam pomoći da razmislite o scenarijima koji bi mogli utjecati na Vašu informacijsku imovinu koju znaju ključni ljudi organizacije. Razmislite o svakom scenariju i zaokružite odgovarajući odgovor. Ako je Vaš odgovor "Da" razmislite da li se scenarij dogodio slučajno ili namjerno, ili oboje.

Scenarij 1:

Razmislite o ljudima koji rade u Vašoj organizaciji. Da li postoji situacija u kojoj zaposlenik ima detaljno znanje o Vašoj informacijskoj imovini (slučajno ili namjerno), što bi moglo rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Promjena sadržaja informacija u svrhu da se više nije upotrebljivo?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Prekinuti s namjerom da se ne može pristupiti informacijama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**
Trajno uništenje ili privremeni gubitak informacija, tako da se ne mogu koristiti za namijenjene svrhe?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Scenarij 2:

Razmislite o ljudima koji su izvan Vaše organizacije. To podrazumijeva ljude koji imaju legitiman poslovni odnos s Vašom organizacije ili ne. Da li postoji situacija gdje "autsajder" može pristupiti jednom ili više tehnički spremnika (slučajno ili namjerno), što će rezultirati da Vaša informacijska imovina bude:

Otkrivati informacije neovlaštenim osobama?	**Ne**	**Da (slučajno)**	**Da (namjerno)**

Allegro - radna tabela 10	**RADNA TABELA RIZIKA INFORMACIJSKE IMOVINE**			
Rizik informacijske imovine	Informacijska imovina			
	Interesno područje			
Prijetnja	(1) Učesnik *Tko je zadužen za kontrolu određenog interesnog područja ili rizika?*			
	(2) Sredstvo *Kako bi to učesnik napravio? Što bi učesnik napravio?*			
	(3) Motiv *Zbog kojeg razloga je učesnik to uradio?*			
	(4) Ishod *Kako bi to utjecalo na informacijsku imovinu?*	❑ **Otkrivanje** ❑ **Uništenje** ❑ **Promjena** ❑ **Prekid**		
	(5) Sigurnosni zahtjevi *Koji bi sve sigurnosni zahtjevi informacijske imovine bili narušeni?*			
	(6) Vjerojatnost *Koja je vjerojatnost da se ovaj scenarij prijetnje desi?*	❑ **Visoko**	❑ **Umjereno**	❑ **Nisko**

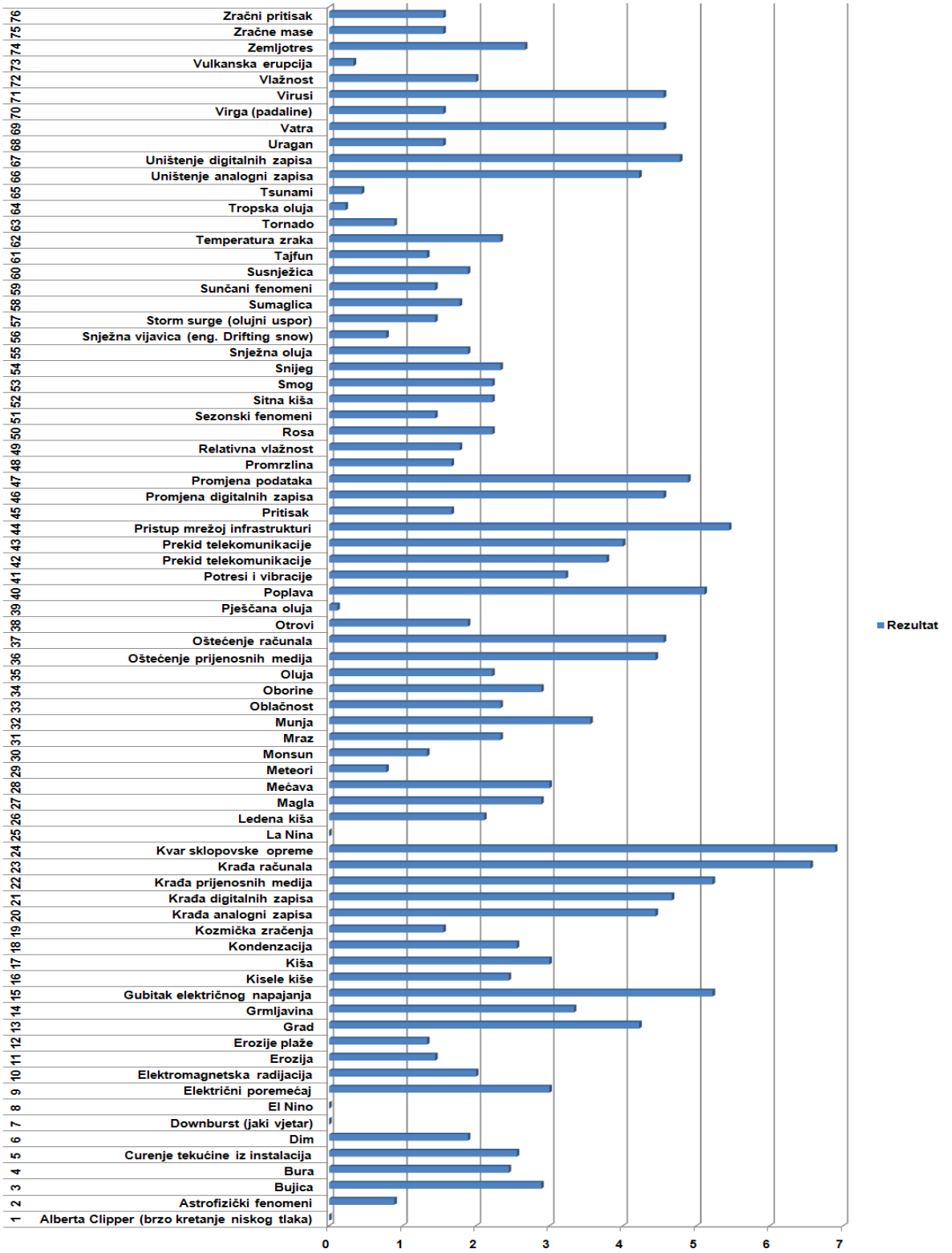
(7) Posljedice *Koje su posljedice za organizaciju i vlasnika informacijske imovine koje su nastale kršenjem sigurnosnih zahtjeva?*	(8) Ozbiljnost *Koliko su ozbiljne posljedice za organizaciju, odnosno za vlasnika informacijske imovine?*		
	Rizično područje	**Vrijednost**	**Rezultat**
	Ugled i klijentovo povjerenje		
	Financije		
	Produktivnost		
	Zdravlje i sigurnost		
	Pravne i zakonske kazne		
	Korisnikova procjena prijetnji		
	Rezultat relativnog rizika		

(9) Pristup ublažavanja *Na temelju ukupnog rezultata rizika, što ćete učiniti?*			
❑ **Prihvaćanje**	❑ **Odgađanje**	❑ **Ublažavanje**	❑ **Prebacivanje**

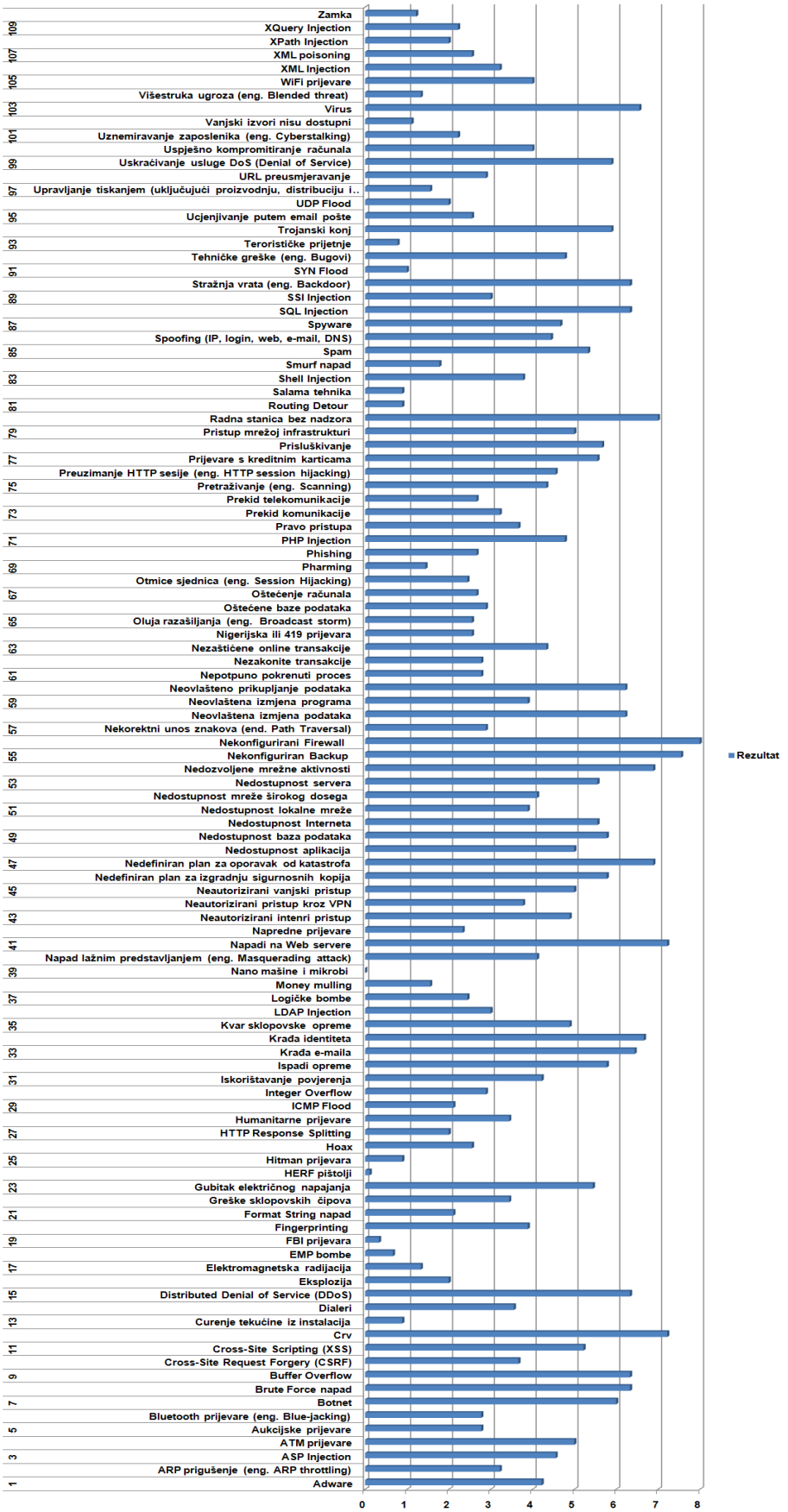
Za rizike koje ste odlučili ublažiti, odradite sljedeće:	
Na koji spremnik informacijske imovine ćete primijeniti kontrole?	*Koje administrativne, tehničke i fizičke kontrole ćete primijeniti za ovaj spremnik informacijske imovine?Koji rezidualni rizik će biti prihvaćen od strane organizacije?*

17. Dodatak D

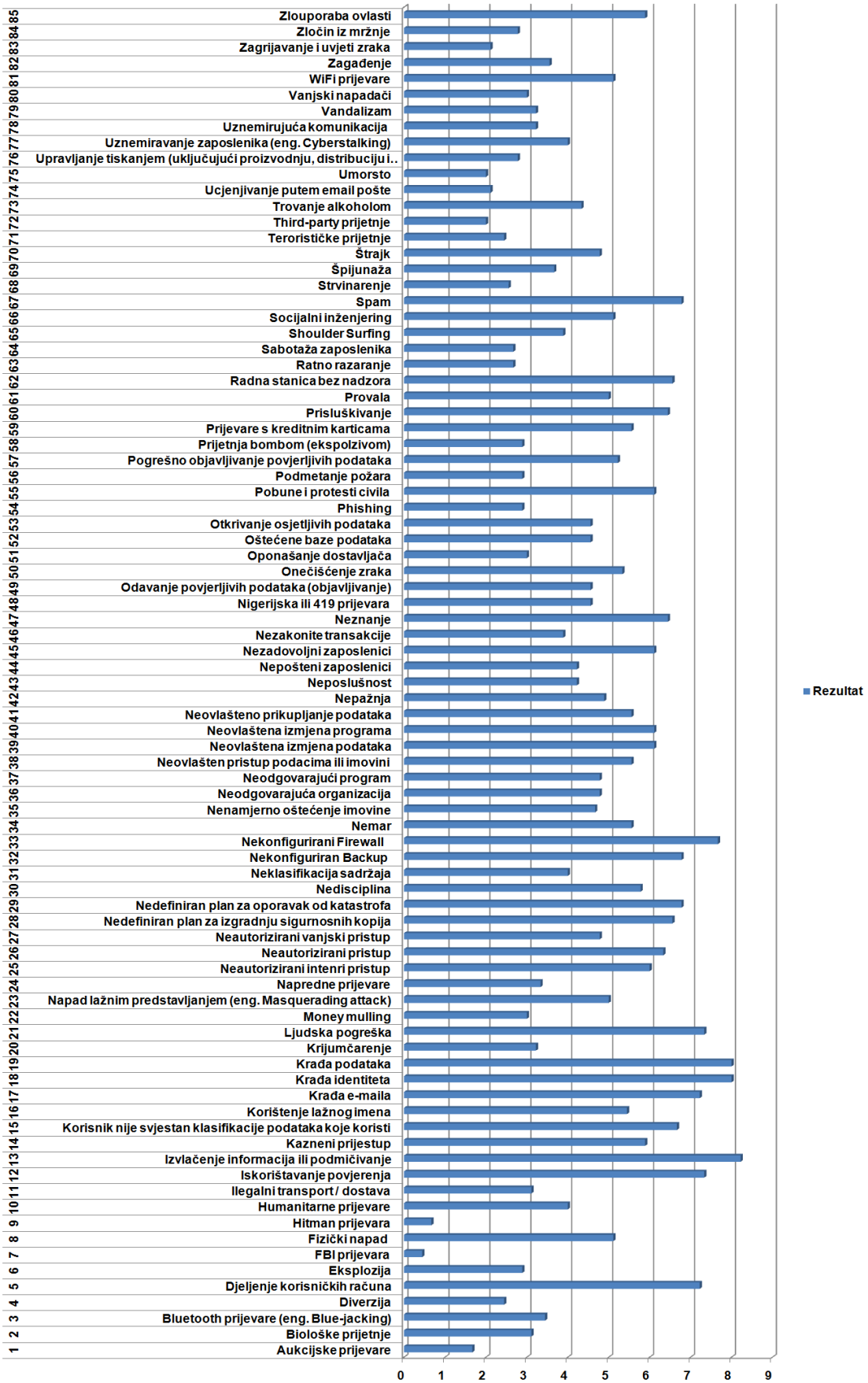
Detaljni rezultati ankete



Grafikon 17.1. - Fizičke vrste napada



Grafikon 17.2. - Tehničke vrste napada



Grafikon 17.3. - Ljudske vrste napada

18. Dodatak E

Riječnik pojmova

Adware (eng. advertising-supported software)

Programi koji automatski prikazuju ili učitavaju oglase ili promidžbene poruke nakon što se instalira na računalo ili za vrijeme korištenja. [75]

ARP prigušenje (eng. ARP throttling)

ARP prigušenje (eng. ARP throttling) je funkcionalnost koju posjeduju sklopovski bazirani CEF usmjerivači. Njegova osnovna zadaća je zaštita glavnog procesora dok god ne završi ARP proces, te se utvrdi odredišna MAC adresa. [55]

ASP Injection

ASP Injection je jedan oblik napada umetanjem koda koji omogućuje umetanje koda u skripte koje se izvršavaju na serveru. [65]

Botnet

Botnet je skupina određenog broja računala kontroliranih od strane zlonamjernog poslužitelja ili gospodara. [22]

Brute Force napad

Koristi se najčešće za otkrivanje zaporki tako da napadač koristi sve moguće kombinacije znakova, ovakav napad ovisi o jačini zaporke i o količini resursa s kojima raspolaže napadač. [72]

Buffer Overflow

Buffer overflow označava prelijevanje bitova tj. dolazi do brisanja vrijednost nekog od registra, što kao rezultat daje to da aplikacija počinje izbacivati greške i više se ne može koristiti. [15]

Cross-Site Request Forgery (CSRF)

CSRF napadi su napadi kojima korisnik nesvjesno izvršava neželjene radnje na prijavljenoj web stranici. [70]

Cross-Site Scripting (XSS)

Metoda kojom se na ranjivu stranicu podmeće zlućudan sadržaj što je omogućeno nedovoljnom provjerom unosa u programskom kodu stranice. [16]

Crv (eng. Worm)

Program ili algoritam koji se sam replicira na zaraženim računalima i pri tome obično čini neku štetu. [75]

Dialeri

Njihova je zadaća u trenutku aktiviranja prekinuti postojeću vezu s Internetom i uz pomoć modema birati broj u nekoj dalekoj zemlji kako bi ostvarili dobit autoru kroz visoke cijene poziva. [20]

Distributed Denial of Service (DDoS)

Vrsta napada kojom se želi onesposobiti korištenje mrežnih i računalnih usluga u ciljanoj mreži, kako bi se prikrili tragovi napada i kako bi se povećao broj napada tijekom napada se koristi više DDoS poslužitelja koji se nalaze na različitim mjestima. [7]

EMP bombe

EMP predstavlja elektromagnetski puls (engl. Electromagnetic Pulse). Izvor može biti nuklearna ili nenuklearna detonacija. Koristi se za onesposobljavanje elektroničkih uređaja. [34]

FBI prijevare

FBI prijevare su prijevare kojima se žrtva obmanjuje tako da svoje podatke jer misli kako joj se obraća FBI. [26]

Fingerprinting

Napadač koristi određene znakove (**" * ", " ~ ", " ' ",...**) koji se kombiniranjem u URL zahtjevu koriste za eksploataciju web aplikacija i web servera. [33]

Format string

Napad ove vrste može prouzročiti rušenje programa ili izvođenje opasnog programskog koda. Problem proizlazi iz korištenja nefiltriranih korisničkih unosa. [71]

HERF pištolji

HREF pištolji su radio prijenosnici koji mogu zračiti koncentrirane radio signale visoke snage kako bi prekinuli rad elektroničkih uređaja ili ih trajno oštetili. [34]

Hit Man prijevara

Pokušaj dobivanja novca ucjenjivanjem žrtve putem email poruka. [31]

Hoax

Hoax prijevara predstavljaju poruke kojima se uz pomoć lažnih informacija nagovara korisnika da oda povjerljive podatke ili bez opravdanog razloga poduzme neku radnju. Najčešće se radi o krađi pristupnih podataka bankovnom računu ili nepostojećim prijetnjama ili ih nagovaraju da poduzmu neku destruktivnu radnju na svom računaru. [20]

HTTP Response Splitting

HTTP Response Splitting je jedan oblik ranjivosti web aplikacija kod koje aplikacija nije u mogućnosti propustiti samo pravilne ulazne vrijednosti, što predstavlja priliku za iskorištenje različitih vrsta napada umetanjem koda. [55]

HTTP session hijacking

HTTP session hijacking predstavlja napad koji se izvršava presretanjem korisnikovog session cookie-ja, te uporabom istog logira na servis kao već autentificirani korisnik, na taj se način vrše krađe identiteta. [21]

ICMP flood

ICMP flood je poznat i kao Ping flood a predstavlja jednu vrstu napada uskraćivanja usluga. U ovom napadu cilj je popuniti TCP/IP stog čime računalo neće moći odgovarati na novopridošle TCP/IP zahtjeve. [41]

Imovina

Predstavlja sve ono što je važno za poslovni sustav. Korištenjem imovine i sredstva organizacija teži prema ostvarivanju svojih ciljeva, povratu na uložene investicije ali i stvaranju prihoda. Ukupna vrijednost organizacije može se gledati kao vrijednost cjelokupne imovine. [23]

Integer Overflow

Integer Overflow predstavlja ranjivost aplikacije zbog koje dolazi do greške u izvođenju programa kada aritmetička operacija da rezultat koji je veći od prethodno namijenjenog prostora za rezultat. [14]

Informacijska imovina

Predstavlja sve informacije ili podatke koji imaju vrijednost za organizaciju, uključujući informacije kao što su podaci o kupcima, poslovnim partnerima ili intelektualno vlasništvo (znanje). Ova sredstva mogu postojati u fizičkom obliku (na papiru, CD-u ili na drugim medija) ili elektroničkim obliku (pohranjena na bazama podataka, u datotekama, na osobnim računalima). [23]

Interesno područje

Predstavlja opisnu izjavu da su detalji o stanju iz realnog vremena ili situacija koja bi mogle utjecati na informacijsku imovinu u Vašoj organizaciji. [23]

Iskorištavanje povjerenja

Bazira se na iskorištavanju ljudskih slabosti i međusobnog povjerenja tako da napadač želi iskoristiti žrtvu na temelju sedam ljudskih slabosti: seksipila, pohlepe, taštine, povjerenja, lijenosti, suosjećanja i hitnosti. [47]

Izjava o utjecaju

Predstavlja opisanu izjavu u kojoj je detaljno opisano koliki je utjecaj (posljedica) nakon što se scenarij prijetnje realizirao. Izjava o utjecaju predstavlja posljedicu izvršenja scenarija prijetnje. [23]

Ključna informacijska imovina

Predstavlja najvažnija sredstva za organizaciju. Organizacija će imati negativan učinak ukoliko je:

- ✓ kritična imovina (informacije) prikazana ili dostupna neovlaštenim osobama,
- ✓ kritična imovina izmijenjena bez odobrenja,
- ✓ kritična imovina izgubljena ili uništena,
- ✓ kritična imovina (informacije) nedostupna tj. prekinut pristup. [23]

Kriterij mjerenja rizika

Predstavlja skup kvalitativna mjera uz pomoć kojih ocjenjujemo rizik koji djeluje na poslovne ciljeve i misiju organizacije. Uz pomoć kriterija mjerenja rizika definiraju se rasponi (visok, srednji, nizak) utjecaja rizika na organizaciju. [23]

LDAP Injection

LDAP Injection je oblik napada umetanja koda koji se koristi za eksploataciju ranjivosti web aplikacija koje koriste Lightweight Directory Access Protocol. Promjenom naredbi u protokolu moguće je ostvariti neovlašteni privilegije u aplikaciji. [60]

Ljudi

U strukturalnoj procjeni rizika, ljudi predstavljaju jednu vrstu "spremnika" informacije imovine. Oni mogu posjedovati specijalizirane ili važne informacije i svakodnevno ih koristiti u svom poslovanju. Informacije koje svakodnevno koriste predstavljaju intelektualno vlasništvo (znanje). U nekim slučajevima informacije koje ljudi posjeduju, u organizacijama nisu zapisane ni u jednoj formi (tj., ne mogu biti u pisanom obliku). [23]

Nano mašine i mikrobi

Nano mašine su sićušni roboti koji se mogu neprimjetno uneseni u informacijski centar i prouzročiti veliku štetu. Mikrobi koji su uzgojeni da jedu silicij mogu uništiti sve integrirane krugove u računalnom sustavu. [7]

Napad lažnim predstavljanjem

Napad lažnim predstavljanjem je metoda koju koristi zlonamjerni korisnik da bi skrio svoj identitet kako bi recimo prikrio svoje tragove prilikom napada uskraćivanjem usluge ili neke druge kriminalne radnje. [55]

Napredne prijevare

Navođenje žrtve na vjerovanje da će ostvariti veliku dobit ali moraju za to uplatiti određen iznos novca. [11]

Nekorektni unos znakova (eng. Path Traversal)

Ova vrsta napada iskorištava ranjivosti u putanji do datoteka ili direktorija te tako napadač u slučaju uspješnog napada može pristupiti onim datotekama i direktorijima kojima inače ne bi smio imati pristup. Takav napad može se iskoristiti u aplikacijama koje traže od korisnika upis neke vrijednosti koja se koristi za dohvat podataka. [50]

Nigerijska ili 419 prijevara

Nigerijska ili 419 prijevara predstavlja jednu vrstu obmane gdje se napadač predstavlja kao stanovnik ili političar iz Nigerije i traži da mu žrtva ustupi svoj račun i pošalje određen iznos novca a žrtvi se lažno obećava provizija, obično se radi o velikoj količini novca tako da se cilja na ljudsku pohlepu. [1]

Njuškanje (eng. Sniffing).

Ova vrsta napada se zasniva na prikupljanju podataka mrežnog prometa u lokalnoj mreži kako bi se prikupile povjerljivi podaci kao što su lozinke i slično. [27]

Oluja razašiljanja (eng. Broadcast storm)

Oluja razašiljanja (eng. broadcast storm) je pojava u mreži, kada poruka koja je poslana svima u mreži, izazove još više odgovora čime dolazi do opterećenja u mreži što može ometati ili potpuno onesposobiti promet paketa u mreži. [55]

Otmice sjednica (eng. Session Hijacking)

Session Hijacking je vrsta napada na računalni sustav gdje napadač fizički pristupa računalu i koristi neprekinute sesije kako bi neautorizirano pristupio sustavu, najčešće se događa kada zaposlenik na kratko napusti radno mjesto a ne odlogira se. [7]

PHP Injection

PHP Injection je jedan oblik napada umetanjem koda koji omogućuje umetanje koda u skripte koje se izvršavaju na serveru. [69]

Pharming

Pharming je oblik udaljenog napada kod kojega se promet usmjeren prema ranjivoj web stranici preusmjerava prema zlonamjerno oblikovanoj web stranici. Ovaj napad moguće je izvesti izmjenama datoteke s informacijama o položaju računala unutar mreže s ciljem prikupljanja korisničkih podataka kao što su zaporke i korisnička imena. [19]

Pranje novca (eng. Money mulling)

Kako se cyber kriminal širi, javlja se i sve veća potreba za „mulama" – ljudima koji otvaraju posebne bankovne račune ili čak koriste vlastite kako bi pomogli kriminalcima podići ili „oprati" novac. [24]

Prijetnja

Predstavlja pokazatelj potencijalnih neželjenih događaja. Prijetnja se odnosi na situaciju (ili scenarij) u kojoj osoba može učiniti nešto nepoželjno (napadač pokreće DoS napad protiv organizacijskog e-mail servera) ili prirodna nepogoda koja može izazvati neželjeni ishod (požar koji može oštetiti sklopovsku opremu na kojoj se nalazi informacijska imovina). [23]

Pristup ublažavanja

Predstavlja način na koji se organizacija namjerava pristupiti riziku. Organizacija ima sljedeće mogućnosti a one su:

- ✓ *Prihvaćanje* - odluka koja je nastala tijekom analize rizika. Ovom odlukom organizacija prihvaća posljedice rizika i ništa ne poduzima. Prihvaćeni rizici i njihove posljedice bi trebali imati nizak utjecaj na organizaciju.
- ✓ *Ublažavanje* - odluka koja je nastala tijekom analize rizika. Ovom odlukom organizacija provodi razne kontrole i postupke za ublažavanje posljedica koje su ostale od prijetnji čije su posljedice najčešće umjerene ili visoke.
- ✓ *Odgađanje* - situacija u kojoj pristup organizacije nije ni prihvaćanje niti ublažavanje već želja organizacije za prikupljanje dodatnih informacija i obavljanje dodatne analize. Odgođeni rizici se redovito nadziru i ponovno vrednuju u nekom trenutku u budućnosti. Rizici koji su odgođeni najčešće nisu opasni za organizaciju, niti bi trebali značajno utjecati na poslovanje organizacije i u slučaju da se realiziraju. [23]

Profil informacijske imovine

Predstavlja prikaz informacijske imovine koji opisuje njene jedinstvene značajke, obilježja i vrijednosti. [23]

Rezidualni rizik

Predstavlja preostali rizik koji je ostao nakon primjene jedne od vrsta pristupa ublažavanja (*prihvaćanje, ublažavanje, odgađanje*). Rezidualni rizik koji je preostao trebao bi biti prihvatljiv za organizaciju. [23]

Rizik

Predstavlja mogućnost trpljenja štete ili gubitka. Rizik se odnosi na situacije u kojima osoba može učiniti nešto nepoželjno ili prirodna pojava koja može izazvati nepoželjan ishod, što rezultira negativan učinak ili posljedicu. Rizik se sastoji od

- ✓ događaja,
- ✓ posljedice i
- ✓ nesigurnosti. [23]

Routing Detour

Routing Detour je vrsta napada u mreži gdje posrednik može promjenom zaglavlja preusmjeravati poruke gdje želi, obično su zaglavlja manje zaštićena od same poruke. [2]

Salama tehnika

Klasična salama tehnika predstavlja jedan oblik internet prijevare gdje se prilikom svake transakcije zaokružuje iznos na određen broj decimala čime se zapravo umanjuje iznos transakcije ali nije lako uočljiv, velikim brojem transakcija može se napraviti velika financijska šteta. [43]

Scanning (Pretraživanje)

Koristi se za otkrivanje određenih informacija o računalnom sustavu analizom otvorenih portova i servisa koji su aktivni, kako bi napadač dobio bolji uvid u sustav i njegove ranjivosti. [66]

Scenarij prijetnji

Predstavlja situaciju u kojoj informacijska imovina može biti ugrožena. Scenarij se sastoji od sudionik, motiva, sredstava (pristupa) i neželjenih ishoda. Scenarij prijetnji predstavlja pojednostavljene načina uz pomoć kojih se može utvrdi da li postoji rizik koji bi mogao utjecati na Vašu informacijsku imovinu. [23]

Shell Injection

Shell Injection je jedan od oblika umetanja koda u aplikacijama koje dozvoljavaju unošenje izvršnih naredbi tako da napadač može zlorabiti takvu mogućnost. [42]

Shoulder Surfing

Shoulder Surfing je jedan oblik socijalnog inženjeringa gdje napadač neposredno dobiva uvid u lozinku dok žrtva unosi lozinku. [17]

Sigurnosni zahtjevi

Ovim zahtjevima je definirano na koji način će informacijska imovina biti zaštićena. Oni se također često spominju kao "sigurnosni ciljevi".

- ✓ *Povjerljivost* - osiguranje da samo ovlaštene osobe (ili sustavi) imaju pristup informacijskoj imovini.
- ✓ *Integritet* - osigurava da stanje informacijske imovine ostane za namjenu i potrebu vlasnika.
- ✓ *Dostupnost* - osigurava da informacijska imovina bude dostupna ovlaštenim korisnicima. [23]

Skrbnik (*čuvar*) informacijske imovine

Čuvari informacija imovine su pojedinci u organizaciji koji imaju odgovornost da zaštite informacijsku imovinu koja se pohranjuje, prenosi ili obrađuje. Drugim riječima, čuvari prihvaćaju odgovornost za informacijsku imovinu koju koriste. [23]

Smurf

Smurf je tehnika koja koristi svojstvo usmjerivača te šalje niz paketa mnoštvu računala. Svaki paket sadržava krivotvorenu izvorišnu adresu žrtve. Računala kojima su poslani ti

krivotvoreni paketi preplavljuju mrežnim prometom računalo žrtve, a mogu u potpunosti onemoguće rad računala ili računalne mreže. [32]

Socijalni inženjering

Napadač koristi ljudske slabosti kako bi uvjerio pojedinca i stekao njegovo povjerenje te na temelju toga došao do željenih informacija ili sredstva. [18]

Splopovski čipovi

Proizvođači mogu lako prilagoditi proizvedene čipove na način da im dodaju neke neočekivane funkcije. Tako mogu biti izgrađeni da zakažu nakon određenog vremena ili da šalju radio signale koji omogućuju točno određivanje lokacije. [7]

Spoofing

Napadač može presresti komunikaciju između dvije strane, promijeniti poruku i poslati je dalje do odredišta. U tom slučaju ni jedna ni druga strana ne zna da su ti podaci promijenjeni i da im druga strana uopće nije poslala ovakve podatke kakvi su stigli na odredište. [54]

Spremište informacijske imovine

Predstavlja sredstva na kojima se informacijska imovina pohranjuje, prenosi i obrađuje. Spremište informacijske imovine može biti sklopovska oprema, programi, operacijski sustavi, servisi i mreže (tehnologija). Informacija se na ovim spremištima nalazi u raznim datotekama i datotečnim sustavima. Bitno je spomenuti i ljude koji svojim intelektualnim vlasništvom (znanjem) posjeduju informacijsku imovinu. [23]

Spyware (eng. Spying software)

Program koji se bez svjesnog pristanka korisnika instalira na računalo i presreće ili čak djelomično preuzima nadzor nad interakcijama korisnika i računala. Tako prikupljene podatke spyware može proslijediti trećoj osobi. [74]

SSI Injection

SSI Injection je serversko orijentirana eksploatacijska tehnika koja omogućuje napadaču slanje koda u web aplikaciju, što kasnije može biti pogubno za rad server. [3]

Stablo prijetnji

Koristi se struktura stabla za vizualno predstavljanje raspona scenarija prijetnji. Uz pomoć stabla prijetnji imate bolji uvid u spektar potencijalnih prijetnje, ali i načine kako da se zaštitite i osigurate od njih. [23]

Stražnja vrata (eng. Backdoor)

Stražnja vrata su mehanizam ugrađen u sustav od strane dizajnera koji ih je kreirao. Funkcija stražnjih vrata je omogućiti dizajneru da se ušulja u sustav, zaobilaženjem uobičajene zaštite sustava. [7]

Strvinarenje

Strvinarenje je jedan od oblika socijalnog inženjeringa gdje se ostavlja mogućnost drugoj osobi da dođe do povjerljivih podataka pregledom neadekvatno odbačenih podataka. [7]

SQL Injection

SQL Injection je tehnika eksploatiranja sigurnosnih ranjivosti sloja baze podataka aplikacije. Najčešće se eksploatiraju web aplikacije koje u svojim SQL upitima koriste podatke koje je isporučio korisnik, ali bez prethodnog ispitivanja da li ti isti korisnički podaci sadrže neke potencijalno štetne znakova poput navodnika, točke-zarez i sl. [73]

SYN Flood

SYN Flood je tehnika kojom se lažira izvorišna adresa računala tako da napadnuto računalo misli kako radi s pouzdanim izvorom. [18]

Tehnološka imovina

Ovaj pojam podrazumijeva elektronske spremnike u kojima se informacijska imovina pohranjuje, prenosi i obrađuje. Općenito gledajući ovdje ubrajamo: hardver, softver, aplikacijske sustave, servise i mreže. Ovdje je bitna dostupnost koja osigurava da informacijska imovina bude dostupna ovlaštenim korisnicima. [23]

Third-party prijetnje

Third-party prijetnje predstavljaju prijetnje od neke treće osobe kuju prenosi neka druga osoba. [28]

Trojanski konj (eng. Trojan horse)

Trojanski konj se predstavlja kao obični, neopasni program a koristi se za lakše upad u računalo. Za razliku od crva, trojanci se ne repliciraju sami. [75]

URL preusmjeravanje

Žrtvi se nude lažni linkovi a zapravo se preusmjerava na druga web mjesta. Ova vrsta napada se može koristiti za instaliranje malicioznog koda na žrtvinom računalu i za preuzimanje kontrole izvršavanja naredbi na računalu. [53]

Uskraćivanje usluga (eng. Denial of Service, DoS).

Napadač sprječava pristup uslugama najčešće web serveru pomoću preopterećivanja računalne mreže slanjem mnogostrukih zahtjeva prema web serveru. Na taj način sprječava se da korisnici pristupaju podacima ili ostalim servisima koji se nalaze na web serveru koji je napadnut. [7]

Virus

Program ili dio koda koji je bez znanja korisnika učitan u računalo korisnika i koji se izvršava bez njegovog znanja, odnosno svjesnog pristanka. [29]

Višestruka ugroza (eng. Blended threat)

Iskorištavanje ranjivosti računala korištenjem kombinacije više vrsta napada kako bi se maksimizirala šteta i kako bi se napravila šteta u što kraćem vremenu. [59]

Vlasnici informacijske imovine

Predstavljaju pojedince čija je primarna odgovornost za održivost, opstanak i fleksibilnost informacijske imovine. Oni trebaju biti upoznati sa sigurnosnom politikom u kojoj su jasno definirani propisi kako osigurati i zaštiti informacijsku imovinu. [23]

Vrijednost prijetnje

Predstavlja kvalitativnu mjeru specifičnih rizika koji utječu na organizaciju (visoka, umjerena ili niska). [23]

Vrijednost utjecaja

Predstavlja kvalitativnu vrijednost uz pomoć koje je upisan opseg utjecaja na organizaciju kada se scenarij prijetnje izvrši. Vrijednost utjecaja je izvedena iz kriterija mjerenja rizika. [23]

Zamka

Zamka predstavlja prekrivenu funkciju krajnjem korisniku koja se može pokrenuti na unaprijed poznat način a koristi se kako bi se običnom korisniku onemogućilo slučajno ili namjerno mijenjanje važnih postavki za rad aplikacije što napadač može to lako iskoristiti za napad na aplikaciju. [7]

Zloćudni kod (eng. Malicious software)

Programski kod koji je načinjen kako bi se, bez svjesnog pristanka korisnika, učitao u korisnikovo računalo i načinio neku štetu. [74]

XML Injection

XML Injection je napadačka tehnika koja se koristi za manipulaciju ili kompromitiranje logike XML aplikacije ili web servisa umetanjem neprimjerenog XML sadržaja unutar XML poruka. [4]

XML poisoning

Ovaj napad je moguće izvesti kada web usluge koriste SOAP protokol za razmjenu XML poruka, ukoliko je to slučaj napadači mogu modificirati SOAP poruke kako bi izložili integritet originalne poruke opasnosti. [44]

XPath Injection

XPath Injection je napadačka tehnika koja se korista za eksploataciju aplikacija koja koristi XPath upite nakon korisničkog unosa. [5]

XQuery Injection

XQuery Injection je varijanta klasičnog SQL napada umetanjem na XML XQuery jezik. XQuery Injection koristi ranjivost nepravilne validacije ulaznih podataka koji se koriste za izvođenje XQuery naredbi. [6]

19. Dodatak F

Odgovornosti autora

Alagić Dino, univ. bacc. inf.

- ✓ sudjelovanje na svim sastancima koji predstavljaju ključne točke projekta, na kojima se utvrđuje da li se sve aktivnosti odvijaju po planu i da li treba nešto dodatno izmijeniti,
- ✓ izrada detaljnog plana izvođenja projekta,
- ✓ koordiniranje rada,
- ✓ prevođenje metode Octave Allegro na hrvatski jezik,
- ✓ analiza metode Octave Allegro,
- ✓ izrada projektne dokumentacije,
- ✓ kontrolu napredovanja tijekom projekta, učinkovitost članova i projekta,
- ✓ dizajniranje aplikacije.
- ✓ testiranje funkcionalnosti aplikacije,
- ✓ analiziranje i izrada ankete.

Branković Vedran, univ. bacc. inf.

- ✓ sudjelovanje na svim sastancima koji predstavljaju ključne točke projekta, na kojima se utvrđuje da li se sve aktivnosti odvijaju po planu i da li treba nešto dodatno izmijeniti,
- ✓ analiza alata za procjenu rizika ,
- ✓ analiza metode Octave Allegro,
- ✓ testiranje aplikacije na konkretnom primjeru poduzeća,
- ✓ prikupljanje napada na sigurnost,
- ✓ analiziranje i izrada ankete,
- ✓ izrada projektne dokumentacije.

Vagner Mario, univ. bacc. inf.

- ✓ sudjelovanje na svim sastancima koji predstavljaju ključne točke projekta, na kojima se utvrđuje da li se sve aktivnosti odvijaju po planu i da li treba nešto dodatno izmijeniti,
- ✓ analiza i izrada baze podataka za aplikaciju,
- ✓ dizajniranje aplikacije,

- ✓ izrada kostura aplikacije i programskog koda,
- ✓ testiranje funkcionalnosti aplikacije,
- ✓ izrada korisničke dokumentacije za aplikaciju,
- ✓ analiziranje i izrada ankete,
- ✓ završno testiranje i optimiziranje aplikacije.