Upravljanje informacijskom sigurnosti u logističkim sustavima

Živković, Nikolina

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:190005

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI U LOGISTIČKIM SUSTAVIMA

INFORMATION RISK MANAGEMENT IN LOGISTICS SYSTEMS

Mentor: doc. dr. sc. Pero Škorput

Student: Nikolina Živković

JMBAG: 0135242655

Zagreb, rujan 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 17. svibnja 2021.

Zavod: **Zavod za inteligentne transportne sustave**
Predmet: **Računalna sigurnost**

DIPLOMSKI ZADATAK br. 6385

Pristupnik: **Nikolina Živković (0135242655)**
Studij: Inteligentni transportni sustavi i logistika
Smjer: Logistika

Zadatak: **Upravljanje informacijskom sigurnosti u logističkim sustavima**

Opis zadatka:

Kibernetički napadi na logističke sustave, nove su vrste ugroza od kojih nisu pošteđene ni logističke usluge. U ovom diplomskom radu potrebno je opisati informacijske sigurnosne rizike i metodološku podlogu za unaprijeđenije informacijske sigurnosti na način da se provedu analize informacijske sigurnosti u području logistike i logističkog poslovanja te analize sličnih metodoloških pristupa za upravljanje rizicima, odnosno upravljanju rizicima u području informacijske sigurnosti. Također, u diplomskom radu potrebno je opisati prijedloge prilagodbe metodologije procjene rizika logističkom problemskom području.

Mentor:

doc. dr. sc. Pero Škorput

Predsjednik povjerenstva za diplomski ispit:

Sažetak

Upravljanje informacijskom sigurnosti u logističkim sustavima u današnje vrijeme nije lako. Uz razne potencijalne rizike za sigurnost informacija i cjelokupnog informacijskog sustava koji proizlaze iz ranjivosti sustava koji u izvor potencijalnih prijetnji i napada na sustav, rukovodstvo logističkog poduzeća ima glavnu ulogu u određivanju kako i na koji način što bolje zaštiti svoj informacijski sustav. Također, postoji i proces procjene rizika koji se može provesti nad informacijskim sustavom kako bi se identificirale sve ranjivosti i prijetnje sustava, te ocijenio koliki rizik predstavljaju za sustav i informacije u sustavu, te se na kraju daju preporučene sigurnosne kontrole čijom primjenom bi se rizik mogao smanjiti na prihvatljivu razinu. Nakon provedbe procesa procjene rizika, rukovodstvo logističkog poduzeća kreće u proces ublažavanja rizika gdje će pomoću analize isplativosti odrediti koje od preporučenih sigurnosnih kontrola su isplative za njihov sustav te će se te sigurnosne kontrole primijeniti i implementirati u njihov informacijski sustav poduzeća kako bi ublažile rizik, a ostale neće.

Ključne riječi: Sigurnost informacijskog sustava, informacijski sustavi, rizik, analiza rizika, aktivnosti upravljanja rizikom, sigurnosne kontrole, ranjivosti informacijskih sustava, prijetnje informacijskim sustavima

Summary

Managing information security in logistics systems nowdays is not easy. In addition to the various potential risks to the security of information and the entire information system arising from the vulnerability of the system to the source of potential threats and attacks on the system, the management of the logistics company has a major role in determining how and in a which way better protect their information system. There is also a risk assessment process that can be performed on the information system to identify all vulnerabilities and threats to the system, and assess how much risk they pose to the system and information in the system, and finally provide recommended security controls whose application could reduce the risk to an acceptable level. After implementing the risk assessment process, the management of the logistics company embarks on a risk mitigation process where they will use cost-benefit analysis to determine which of the recommended security controls are cost-effective for their system and which are not.

Keywords: Information system security, Information systems, Risk, Risk analysis, Risk Management activities, security controls, Vulnerabilities of Information systems, Threats to Information systems

SADRŽAJ

1. UVOD

Upravljanje informacijskom sigurnosti u logističkim sustavima u današnje vrijeme kada su napadi na informacije česti, raznorazne sabotaže ili provođenje napada na sustav iz razonode, nije lako. Najaktualniji su napadi na logističke sustave koji proizlaze kao rezultat ranjivosti i prijetnji informacijskog sustava u logističkom poduzeću. U ovom diplomskom radu opisat će se informacijski sustavi, njihova sigurnost, potencijalni sigurnosni rizici koji se mogu pojaviti u sklopu informacijskog sustava, te će se detaljno opisati na koji način se može provesti postupak procjene rizika za informacijski sustav u logističkom poduzeću.

U drugom poglavlju ovog diplomskog rada definirani su informacijski sustavi, sigurnosti informacijskih sustava i navedeni su izvori problema sigurnosti. Također u sklopu ovog poglavlja su definirane ranjivosti i prijetnje informacijskih sustava u logističkom poduzeću, te koji su sve potrebni sigurnosni procesi kako bi se informacijski sustav zaštitio.

U trećem poglavlju ovog diplomskog rada definiran je rizik. Rizik koji predstavlja opasnost za informacijski sustav logističkog poduzeća, te je definirana koja to materijalna i nematerijalan imovina logističkog poduzeća bi se trebala zaštititi od rizika. Uz to su ukratko objašnjeni proces procjene rizika, na koji način vrednovati rizik i odrediti kolika je njegova razina opasnosti za informacijski sustav logističkog poduzeća.

U četvrtom poglavlju ovog diplomskog rada dan je prijedlog kako provesti postupak procjene rizika za informacijski sustav logističkog poduzeća, detaljno kroz sve korake, a njih je devet. Odnosno definirana je karakterizacija sustava, objašnjena je identifikacija ranjivosti i prijetnji za informacijski sustav, također je objašnjeno kako provesti analizu kontrole sustava, kako odrediti vjerojatnost rizika, te kako analizirati učinak, odnosno kolika će šteta proizaći iskorištenjem rizika. Na kraju je objašnjeno kako se određuje rizik u informacijskom sustavu, te na koji način se izrađuje dokumentacija nakon što se provede postupak procjene rizika za informacijski sustav u logističkom poduzeću.

U petom poglavlju ovog diplomskog rada ukratko je objašnjen postupak ublažavanja rizika u informacijskom sustavu logističkog poduzeća, koji nastupa nakon što se uspješno provede proces procjene rizika. Naime, nakon što se provede proces procjene rizika i definiraju se koji su potencijalni rizici za informacijski sustav, rukovodstvo logističkog poduzeća pristupa procesu ublažavanja rizika gdje pomoću analize isplativosti definiraju i određuju koje od

preporučenih kontrola za ublažavanje rizika su stvarno korisne za njihov informacijski sustav u poduzeću, te s kojim kontrolama će stvarno ublažiti potencijalni rizik na najnižu razinu. Odnosno, rukovodstvo logističkog poduzeća nakon provedenog procesa procjene rizika, a u sklopu procesa ublažavanja rizika odlučuje koje od preporučenih sigurnosnih kontrola za ublažavanje rizika su primjenjive i će primijeniti na svoj informacijski sustav u logističkom poduzeću.

2. INFORMACIJSKI SUSTAVI I SIGURNOST

Svako logističko poduzeće koje danas posluje ima mnogo informacija, povjerljivih i nepovjerljivih, koje treba obraditi, pohraniti, sačuvati i sl. U tu svrhu su razvijeni informacijski sustavi kao pomoć u poslovanju logističkih poduzeća i obradi informacija za što lakši i efikasniji rad uz smanjenje troškova. Prema Hrvatskoj enciklopediji definicija informacijskog sustava glasi: „Informacijski sustav, organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu. Sastavni je dio informacijskog sustava i osoblje obrazovano za rad u sustavu te odgovarajuća oprema. Današnji se informacijski sustavi pretežito ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije. Posebno je značajna uporaba informacijskih sustava unutar poslovnih sustava, gdje služe za njihovo upravljanje i kao potpora izvođenju poslovnih procesa.“ [1]

2.1. Sigurnost informacijskih sustava

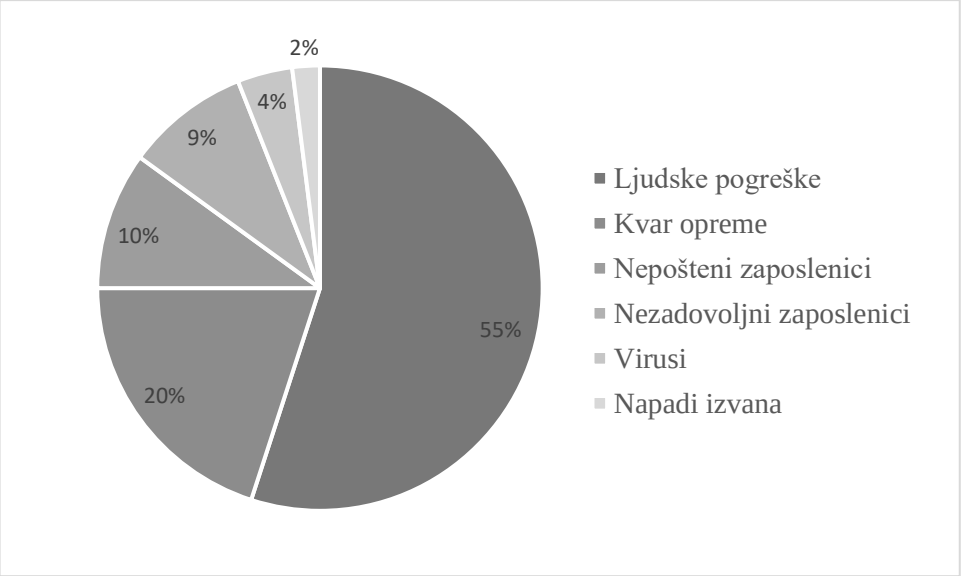
Informacijski sustavi su izloženi određenom riziku, odnosno mogu podlijeći raznim ranjivostima i prijetnjama. Kako bi se to spriječilo potrebno je redovito održavati informacijske sustave i raditi na njihovoj sigurnosti. Prema Zavodu za sigurnost informacijskih sustava, sigurnost informacijskog sustava se definira kao „područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za podatke koji se obrađuju, pohranjuju ili prenose na način da budu upotrebljivi i dostupni ovlaštenim korisnicima, te sigurnost informacijskog sustava obuhvaća zaštitu povjerljivosti, cjelovitosti i raspoloživosti korisničkih podataka“. [2] Sigurnost informacijskog sustava obuhvaća zaštitu informacija u digitalnom obliku i na drugim medijima, te se podjednako odnosi na pisane i govorne podatke.

Zakonom o informacijskoj sigurnosti definirani su pojmovi kao što su informacijska sigurnost i standardi informacijske sigurnosti, a definicija glasi:

- Informacijska sigurnost – „je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“ [3]

- Standardi informacijske sigurnosti – „su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti“. [3]

Kada se radi o sigurnosti informacijskih sustava, istraživanja su pokazala da najčešći uzrok prijetnji sigurnosti nisu napadi izvana, nego ljudske pogreške. Razlog zašto su ljudske pogreške najveći izvor prijetnji sigurnosti informacijskih sustava su nedovoljna pažnja i educiranost zaposlenika. Na grafu 1. su prikazani mogući problemi koji mogu dovesti do prijetnji sigurnosti informacijskih sustava. Da bi se izbjegle sve navedene moguće prijetnje u grafikonu, potrebno je redovito educirati zaposlenike, opremu smještati na sigurnija mjesta te određenim propisima odrediti tko joj smije pristupiti, također bi bilo poželjno uvesti i kontrolu pristupa podacima kako bi se spriječila zlouporaba sustava i sl.



Graf 1. Problemi sigurnosti informacijskih sustava

Izvor: [4]

Učinkovito upravljanje informacijskim sigurnosnim rizikom u logističkom poduzeću zahtijeva sljedeće elemente:

- Dodjela odgovornosti za upravljanje rizicima višim rukovoditeljima
- Prepoznavanje i otkrivanje informacija koje bi značile sigurnosni rizik za poslovanje i imovinu, pojedince, druga poduzeća i osobe koje surađuju s poduzećem i koriste informacijski sustav

- Uspostavljanje organizacijske tolerancije na rizik i priopćavanje o tome cijelom poduzeću, uključujući i smjernice o tome kako tolerancija na rizik utječe na aktivnosti odlučivanja
- Odgovornost viših rukovoditelja za njihove odluke o upravljanju rizicima i provedbe učinkovitih programa za upravljanje rizicima u cijelom poduzeću. [5]

Svi prethodno navedeni elementi mogu se svrstati u jedan proces, a to je proces procjene rizika u logističkim poduzećima, koji je detaljnije po koracima opisan u četvrtom poglavlju ovog diplomskog rada.

2.2. Sigurnosne prijetnje

Prijetnje mogu prouzročiti neželjenu situaciju zbog koje ćemo se morati suočiti sa materijalnom ili nematerijalnom štetom, a izvori tih prijetnji mogu biti razni. Kako bi se informacijski sustav mogao što bolje zaštititi, potrebno je odrediti mjere kojima bi se zaštitio informacijski sustav, a da bi se mogle odrediti adekvatne mjere kojima bi se najbolje zaštitio sustav potrebno je što točnije odrediti vrstu prijetnje, odnosno njezin izvor. Zbog toga vrste prijetnji dijelimo prema njihovom izvoru, a to su:

- Prirodne prijetnje – meteorološke nepogode, geofizičke nepogode, biološke prijetnje, astrofizički fenomeni, sezonski fenomeni itd.
- Namjerne prijetnje ljudi – neautorizirani pristup, prisluškivanje, otkrivanje podataka, sabotaža, zlouporaba ovlasti, namjerno oštećenje opreme, maliciozni programi
- Nenamjerne prijetnje ljudi – nedovoljna educiranost, nepravilno rukovanje, nemar i nepažnja nedisciplina, nenamjerno oštećenje opreme, nenamjerno brisanje podataka
- Oprema – električni kvarovi, ispad opreme, tvorničke greške, prekid komunikacije. [6]

Ako postoji prijetnja sigurnosti informacijskom sustavu, onda postoji i velika mogućnost da će se izvršiti napad na informacijski sustav kojim bi se ugrozila sigurnost informacija u sustavu, ugrozila bi se sigurnost računalnih sustava i sigurnost mreža, odnosno sigurnost cijele računalne infrastrukture. Postoje različite vrste napada koje se mogu podijeliti u razne skupine, a to su:

- Prema načinu djelovanja – krađa, gubitak, prekid usluga, promjena podataka
- Prema mjestu nastanka – unutarnji, vanjski
- Prema mjestu djelovanja – nositelji podataka, ljudski izvori, uređaji, oprema
- Prema karakteru – namjerni, nenamjerni
- Prema izvoru [7]

Međutim, četiri osnovne kategorije napada su:

- Prekid
- Presretanje
- Izmjena
- Proizvodnja [7]

Prekid je metoda napada kod koje se prekidanjem korisniku onemogućuje korištenje usluge, odnosno napadač prekida tok podataka između izvora informacija i njihovog odredišta.

Presretanje je metoda napada kod koje neka treća strana preusmjerava informacije koje se razmjenjuju od izvora informacija do odredišta informacija, na svoje računalo kako bi prikupila što više korisnih informacija i eventualno kontrolirala komunikaciju.

Izmjena je metoda napada kod koje se poslana informacija dohvati prije nego što stigne na odredište, izmjeni u korist napadača, te onda ponovo pošalje k odredištu. Ovakva vrsta napada je štetna jer korisnik može primiti netočne informacije koje bi mogle štetno utjecati na poslovanje.

Proizvodnja je metoda napada kod koje se proizvode, odnosno umeću i izmišljaju netočni i lažni podaci koji su namijenjeni isključivo za krađu i/ili zlonamjerno iskorištavanje povjerljivih informacija poduzeća, a sve s ciljem nanošenja štete.

2.3. Sigurnosni procesi

Kako su informacijski sustavi vrlo važan čimbenik u svakom logističkom poduzeću, važno ih je adekvatno zaštititi od potencijalnih prijetnji i napada koji bi prouzročili veliku štetu za pojedinca ili cijelo poduzeće. Da bi se informacije u sklopu sustava adekvatno zaštitile potrebno je odrediti odgovarajuće sigurnosne politike, procedure i procese kojima će se zaštiti informacijski sustav. Danas se mnoga logistička poduzeća suočavaju sa raznoraznim sigurnosnim prijetnjama poput špijunaže, sabotaže, računalni prijevara i sl., te je zbog toga vrlo važno provođenje upravljanja sigurnosti informacijskog sustava u kojem će sudjelovati svi zaposlenici poduzeća, a možda čak i vanjski suradnici. Da bi se informacije u logističkom poduzeću zaštitile od prijetnji i napada, potrebno je izgraditi sustav informacijske sigurnosti, na način da se:

1. Definiraju i donesu politike sigurnosti
2. Procijeni sigurnosni rizik
    a) Identificira informacijska imovina i odredi njezin vlasnik
    b) Procjeni značaj podatkovnog sadržaja
    c) Procjeni izvor, oblik i intenzitet prijetnji
    d) Izračuna rizik
3. Odaberu mjere za smanjenje rizika
4. Izjave o primjenjivosti
5. Prati efikasnost (funkcionalnost) postavljenog sustava
6. Dogradi sustav ISMS (Information Security Management System). [8]

Najvažniji dio cijelog sigurnosnog procesa je procjena sigurnosnih rizika koja je detaljnije opisana u poglavlju četiri ovog rada. Ako se sigurnosni rizici krivo procijene onda se informacijski sustav neće adekvatno zaštititi i poduzeće može ostvariti velike gubitke. Kod procjene sigurnosnog rizika kao prvo vrlo je važno identificirati svu informacijsku imovinu koju logističko poduzeće posjeduje, jer ako se nešto od imovine ne identificira onda se neće moći provesti adekvatna zaštita od prijetnji nad tim sustavom što bi moglo ugroziti ostatak sustava. Nakon što se sva imovina identificira, slijedeći korak je utvrđivanje vlasnika za svaku pojedinu imovinu kako bi se moglo odrediti tko će točno biti odgovoran za sigurnost kojeg dijela informacijskog sustava, tko će provoditi mjere zaštite, te na samom kraju i odgovarati za tu imovinu. Nakon što smo identificirali svu imovinu i svakoj odredili tko joj je vlasnik i tko je odgovoran za nju, mora se odrediti i njezin značaj u cjelokupnom sustavu poduzeća. Značaj se

određuje tako da se od vlasnika informacijske imovine prikupe podaci o toj imovini, te se na temelju tih podataka određuje koliki značaj pojedina imovina ima na izvođenje određenih poslovnih procesa u cjelokupnom informacijskom sustavu. Značaj imovine se također može odrediti i na temelju tri sigurnosna zahtjeva, a to su:

- Povjerljivost (**C**onfidentiality) – imovina je povjerljiva kada je nerazumljiva svima osim onima koji su ovlašteni za njezino korištenje
- Integritet (**I**ntegrity) – imovina ima integritet tako dugo dok je identična stanju koje je nastalo nakon što je zadnji ovlašteni korisnik završio s njom
- Raspoloživost (**A**vailability) – imovina je raspoloživa kada je dostupna ovlaštenim korisnicima u dogovorenom formatu i razumnom vremenskom roku. [7]

Osim ova tri sigurnosna zahtjeva, imovina se može klasificirati i prema visini moguće štete koja može nastati i/ili potencijalnim posljedicama, a način takvog klasificiranja se dijeli na tri elementa, a to su:

- Nužan – informacijska imovina koja je ključna za rad i nesmetano poslovanje
- Važan – informacijska imovina koja je važna (ali ne i ključna) za nesmetano poslovanje
- Uobičajen – sva ostala informacijska imovina koja nije neposredno neophodna ili se može osigurati iz nekih drugih izvora. [8]

Na samom kraju se izrađuje popis mogućih prijetnji za identificiranu imovinu i njihov izvor, oblik i koliki intenzitet te prijetnje može biti kako bi se mogao izračunati rizik i kako bi se moglo odlučiti kako će se upravljati potencijalnim rizikom.

3. RIZIK

S vremenom su informacijski sustavi, s napretkom i razvitkom novih tehnologija, sve više se razvijali i napredovali, a time se povećavao i potencijalni rizik. Rizik je uvijek prisutan i poslodavci moraju uvijek biti svjesni potencijalnog rizika koji prijeti njihovom poslovanju. Rizik se definira kao „opasnost nastupa neželjena događaja i mogućnost gubitka ili smanjenja imovine, odnosno mogućnost donošenja pogrješne odluke zbog nastupa nepredvidiva događaja i zakazivanja ljudskog faktora, zbog čega nastaje šteta ili opasnost nastupa štetnih posljedica“. [1] Zbog mogućnosti nastupanja rizika i da bi se izbjegle štetne posljedice za poslovanje i logističko poduzeće važno je da se provodi analiza rizika prema koracima kako je objašnjeno u četvrtom poglavlju ovog rada.

Kod analize rizika najvažnije je prvo odrediti što želimo zaštititi i što nam je sve potrebno da to zaštitimo, te koliko bi truda i novca trebali uložiti da bi to mogli adekvatno zaštititi. U logističkim poduzećima imovina koja bi se mogla zaštititi dijeli se na materijalnu i nematerijalnu.

Materijalna imovina koja se može zaštititi je:

- Računalo
- Podaci
- Arhive (Backup)
- Priručnici, knjige, skripte
- Ispisi
- Komercijalni software
- Komunikacijska oprema
- Osobni podaci
- Zapisi o nadzoru. [7]

Nematerijalna imovina koja se može zaštititi je:

- Sigurnost i zdravlje osoblja
- Privatnost korisnika
- Osobne zaporke
- Slika u javnosti i reputacija
- Dobra volja korisnika

- Konfiguracijske informacije
- Dostupnost. [7]

Svaka imovina, bila materijalna ili nematerijalna, ima određenu vrijednost, sklona je ranjivosti i prijetnjama, a ako se one ostvare, logističko poduzeće trpi određene posljedice. Ranjivost se definira kao slabost koja se može slučajno ili namjerno iskoristiti, a posljedica bi bila nanošenje štete informacijskom sustavu i poslovnim ciljevima. Prema Smjernicama za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika Hrvatske narodne banke „ranjivost sama po sebi ne nanosi štetu, nego ranjivost možemo definirati kao stanje ili skup stanja koji može omogućiti nekoj prijetnji da utječe na resurse (primjerice nedostatak mehanizma kontrole pristupa jest ranjivost koja bi mogla omogućiti ostvarenje prijetnje neovlaštenog pristupa, što može dovesti do gubitka ili oštećenja resursa). Ranjivosti koje se povezuju s resursima uključuju, između ostalog, slabosti fizičke sigurnosti, organizacije, internih akata, zaposlenika, upravljačke strukture, hardvera, softvera i informacija." [9] Hrvatska narodna banka u svojim Smjernicama kao zaštitu ranjivosti predlaže analizu ranjivosti s kojom bi se procijenile slabosti koje identificirane prijetnje bi mogle iskoristiti, a tom bi se analizom trebalo uzeti u obzir okruženje, postojeće zaštitne mjere koje postoje i kontrole. Primjer takve analize za logistički sustav dodatno je opisan u poglavlju četiri ovog rada.

Prijetnja, za razliku od ranjivosti je „objekt, osoba ili drugi entitet koji predstavlja stalnu opasnost za imovinu organizacije“. [10] Prijetnja uzrokuje neželjeni incident ili situaciju kojim se izaziva šteta sustavu ili imovini u logističkom poduzeću. Međutim, prijetnja se ne može realizirati bez postojeće ranjivosti, jer ako ne postoji ranjivosti onda nema ni prijetnje, ali ako je sustav ili logističko poduzeće podložno ranjivosti, prijetnja se može realizirati. Ranjivosti mogu biti komunikacijske, ranjivosti osoblja, fizičke, prirodne, strojne i programske i sl., a prijetnje mogu biti izazvane kao namjerno ili slučajno djelovanje čovjeka, kao prirodne pojave, kao tehničke ili organizacijske prijetnje. U tablici 1. su prikazani tipovi imovine te njihove moguće ranjivosti i prijetnje.

Tablica 1. Parovi ranjivost-prijetnja

TIP IMOVINE	RANJIVOST	PRIJETNJA
Hardware	Neredovito održavanje	Tehnički kvar na sustavu
	Nezaključani ormarići	Krađa medija i dokumenata
	Nekontrolirano odbacivanje medija	Krađa medija i dokumenata
Software	Nedovoljno testiranje software-a	Greška u aplikaciji
	Poznate ranjivosti u software-u	Iskorištavanje poznatih ranjivosti
	Nedostatak operativnih sistemskih zapisa	Neovlaštene promjene u sustavu
Mreža	Slabo upravljanje zaporkama	Napadi probijanjem zaporki
	Nekriptirani promet	Prisluškivanje prometa
	Neredundantan 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

Izvor: [7]

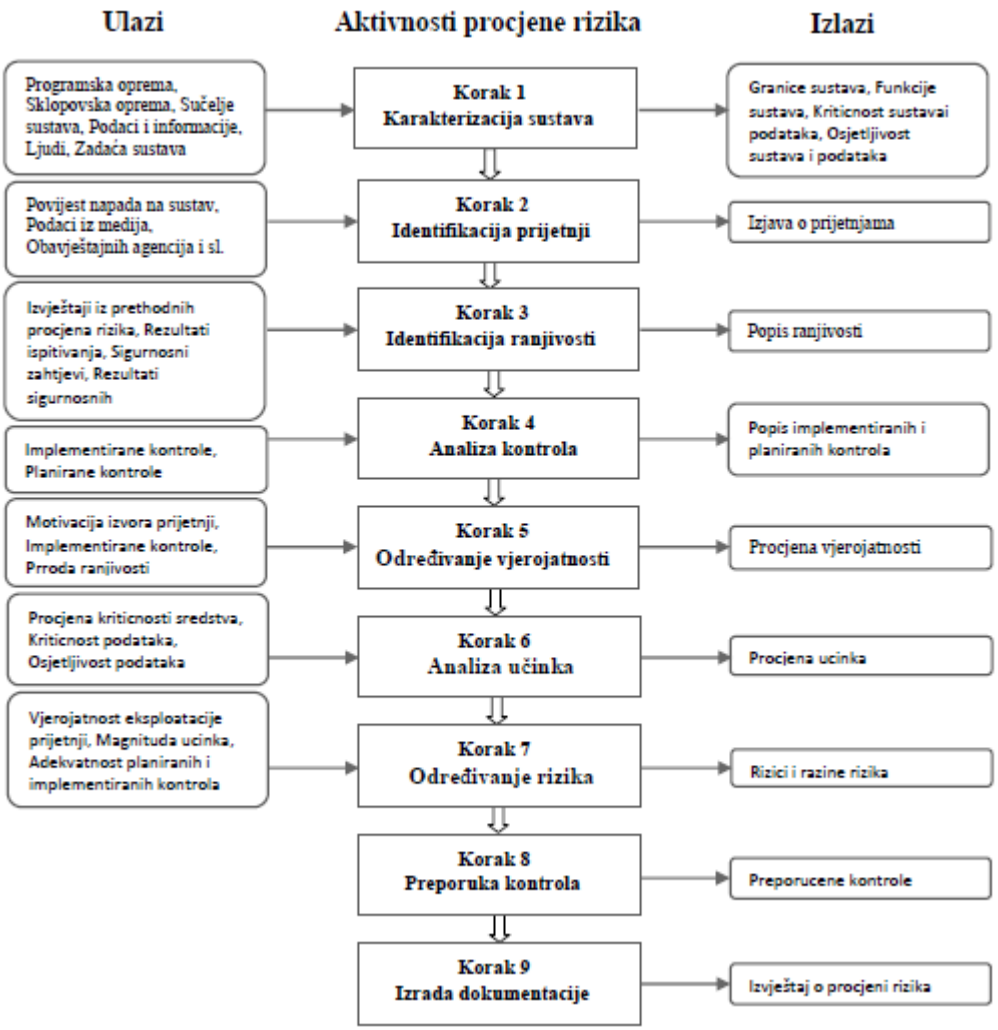
U prethodnoj tablici su navedeni mogući parovi ranjivosti-prijetnja za određeni tip imovine koji se mogu pojaviti ako se kontinuirano ne provode sigurnosne kontrole informacijskih sustava logističkog poduzeća.

3.1. Procjena rizika

Kako bi se spriječio nastanak štetnog događaja ili utvrdila vjerojatnost pojave štetnog događaja, potrebno je izvršiti analizu prijetnje informacijskom sustavu zajedno sa svim njegovim ranjivostima. Analiza prijetnje, također se naziva i procjena rizika te prema NIST metodologiji sastoji se od slijedećih devet koraka koji su i slikovito prikazani na slici 1.:

1. Određivanje obilježja sustava
2. Identifikaciju prijetnji
3. Identifikaciju ranjivosti
4. Analizu sustava kontrola

5. Određivanje vjerojatnosti
6. Analizu učinka
7. Utvrđivanje rizika
8. Predlaganje mjera
9. Dokumentiranje rezultata u obliku formalnog izvješća. [11]



Slika 1. Postupak procjene rizika prema NIST metodologiji

Izvor: [8]

Upravljanje sigurnosti informacijskih sustava, drugim riječima se naziva još i procjena rizika. Procjena rizika predstavlja proces kojim će se identificirati prijetnje, umanjiti rizik te primijeniti mjere i sigurnosna rješenja kako bi se zaštitio informacijski sustav logističkog poduzeća da bi se osigurala dovoljna razina sigurnosti. Proces procjene rizika obuhvaća tri faze, a to su:

- Procjena rizika (identifikacija resursa)
- Umanjivanje rizika (analiza rizika) i
- Evaluaciju rizika (interpretacija rezultata i poduzimanje odgovarajućih protumjera). [8]

Cilj procjene rizika je ustanoviti ranjivosti sustava i potencijalne prijetnje kako bi se mogao odabrati najefikasniji način zaštite informacijskog sustava. Postoje razne metodologije pomoću kojih se može procijeniti rizik, ali dvije osnovne metodologije su:

- Kvantitativna metoda (utemeljena na opisima ili rangiranju) i
- Kvalitativna metoda (utemeljena na numeričkom izračunavanju). [8]

U poglavljima 3.1.1. i 3.1.2. su detaljnije opisane prethodne dvije navedene metode za procjenu rizika.

3.1.1. Kvantitativna metoda

Kvantitativna metoda procjene rizika temelji se na korištenju numeričkih vrijednosti. Parametrima za izračun rizika nastoje se odrediti točne vrijednosti, a vrijednost imovine se prikazuje u novčanim jedinicama. U kvantitativnoj metodi postoji tzv. faktor izloženosti koji označava sve ranjivosti, prijetnje i posljedice, a izražava se u postotku gubitka vrijednosti imovine logističkog poduzeća. Vjerojatnost koja ovisi o ranjivostima i prijetnjama se promatra u zadanom vremenskom periodu pa se u skladu s tim provodi kvantifikacija rizika za taj određeni vremenski period. [12]

Kod procjene rizika informacijske sigurnosti informacijskih sustava ova metoda procjene rizika nije adekvatna. Razlog tome je što se novčana vrijednost imovine određuje na temelju knjigovodstvene vrijednosti, koja ne mora biti ista pravoj vrijednosti imovine. Nadalje, tzv. faktor izloženosti često ga je teško točno odrediti, u nekim slučajevima čak i nemoguće. Glavni nedostaci kvantitativne metode procjene rizika su:

- Zahtjevi za velikom količinom preciznih povijesnih podataka
- Teškoće u utvrđivanju nematerijalne imovine
- Poboljšanje algoritma brojčanog označavanja i razlike između intenziteta
- Razvoj automatiziranih alata za podršku procjene. [8]

Zbog nepouzdanosti svih parametara koji bi se trebali koristiti za izračun kod kvantitativne metode, smatra se da ova metoda procjene rizika u informacijskim sustavima nije prikladna, jer dobiveni rezultati procjene neće biti pouzdani.

3.1.2. Kvalitativna metoda

Za razliku od kvantitativne metode, kvalitativna metoda procjene rizika se temelji na iskustvu, stručnosti i sposobnosti osoba koje provode procjenu rizika što označava subjektivniji pristup. Kod kvalitativne metode procjene rizika rezultati se kvantificiraju zbog lakše interpretacije rezultata i tako dobivene numeričke vrijednosti nisu apsolutne kao kod kvantitativne metode, nego su relativne. Kod kvalitativne metode nije bitno poznavati poslovne procese i njihove vrijednosti, nego je dovoljan općenit uvid u sam sustav. Rezultatom kvalitativne metode procjene rizika se iskazuje relativni odnos vrijednosti štete nastale djelovanjem prijetnji i implementacije protumjera s naglaskom da je rezultat subjektivne naravi te je podložan pogreškama. Kvalitativna metoda procjene rizika se koristi uglavnom kod rješavanja problema za koje se nije mogla koristiti kvantitativna metoda. [8]

3.2. Određivanje rizika

Proces određivanja rizika započinje identifikacijom imovine logističkog poduzeća koja može biti sklopovska oprema, programska oprema, podaci i dokumenti, komunikacije, ljudski resursi i općenito. Kao što je detaljnije objašnjeno u četvrtom poglavlju ovog rada, nakon identifikacije imovine vrši se vrednovanje iste te imovine na temelju tri sigurnosna zahtjeva: povjerljivost, integritet i raspoloživost. Nakon identifikacije imovine i vrednovanja, za određivanje rizika potrebno je razviti ljestvicu/matricu rizika. U tablici 2 je prikazano kako se ukupni rizik može ocijeniti na temelju inputa vjerojatnosti prijetnje i utjecaja prijetnje. Prikazana matrica vjerojatnosti prijetnje je matrica 3x3 koja sadrži tri vrijednosti: visoka, srednja i niska. Ovisno o potrebama logističkog poduzeća i detaljne procjene rizika također se može koristiti i matrica 4x4 ili 5x5, koja će osim uobičajene tri vrijednosti (visoka, srednja i niska) imati i vrijednosti vrlo niska i/ili vrlo visoka vjerojatnost prijetnje ili utjecaj prijetnje kako bi se generirala vrlo niska/vrlo visoka razina rizika. Ako je razina rizika „vrlo visoka“, za

logističko poduzeće bi to moglo rezultirati isključivanje informacijskih sustava ili zaustavljanjem svih postupaka integracije i testiranja informacijskih sustava. [13]

Tablica 2. Matrica izračuna rizika po NIST metodologiji

VJEROJATNOST PRIJETNJE	**UTJECAJ PRIJETNJE**		
	Niska (10)	**Srednja (50)**	**Visoka (100)**
Visoka (1.0)	Niska 10 x 1.0 = 10	Srednja 50 x 1.0 = 50	Visoka 100 x 1.0 = 100
Srednja (0.5)	Niska 10 x 0.5 = 5	Srednja 50 x 0.5 = 25	Srednja 100 x 0.5 = 50
Niska (0.1)	Niska 10 x 0.1 = 1	Niska 50 x 0.1 = 5	Niska 100 x 0.1 = 10

Skala rizika: visok (>50 do 100); srednji (>10 do 50); niski (1 do 10)

Izvor: [13]

Razine rizika koje su prikazane u tablici 2. predstavljaju stupanj, odnosno razinu rizika kojoj bi informacijski sustav, objekt ili postupak mogao biti izložen ako se izvrši određena ranjivost. Skala rizika također predstavlja radnje koje bi viši menadžment ili vlasnici logističkog poduzeća trebali poduzeti za svaku razinu rizika:

- Visoka razina rizika – ako se razina rizika odredi kao visoka, onda su potrebne snažne korektivne mjere. Postojeći informacijski sustav smije nastaviti sa radom, ali je preporučeno da se što prije sastavi plan korektivnih mjera za sustav
- Srednja razina rizika – ako se razina rizika odredi kao srednja, potrebno je izvršiti korektivne radnje u informacijskom sustavu i plan koji će uključivati izvršenje tih radnji u razumnom vremenskom periodu
- Niska razina rizika – ako se razina rizika odredi kao niska, vlasnik poduzeća će utvrditi jesu li potrebne korektivne mjere ili će odlučiti prihvatiti rizik. [13]

Nakon napravljene matrice za izračun rizika, može se odrediti vjerojatnost ostvarenja prijetnje tako da pomnožimo vjerojatnost ostvarivanja prijetnje sa utjecajem na imovinu kao što je prikazano u tablici 3.

Tablica 3. Vjerojatnost ostvarenja prijetnje

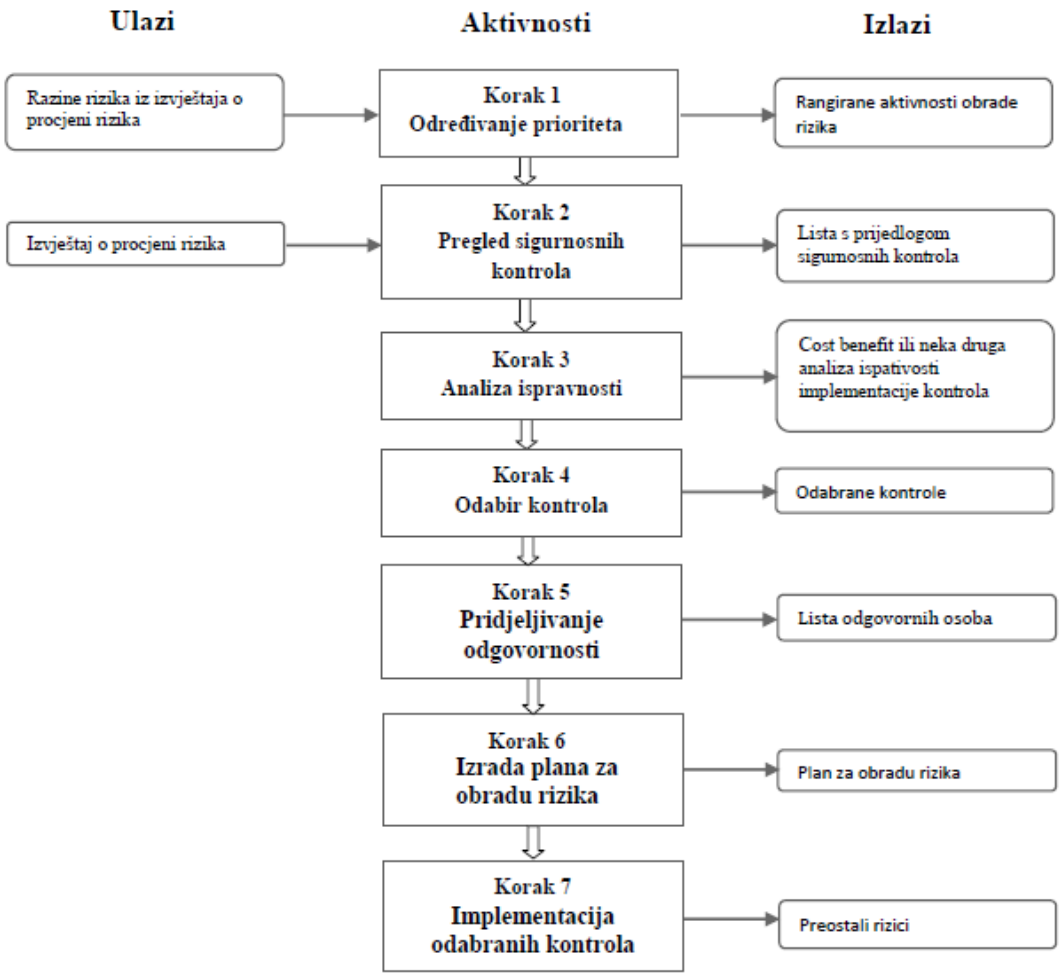
VJEROJATNOST OSTVARENJA PRIJETNJE	**UTJECAJ NA IMOVINU**			
	Vrlo velik (100)	**Umjereno velik (60)**	**Srednji do mali (30)**	**Vrlo mali (10)**
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)
Umjereno velika (0.6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)
Srednja do mala (0.1)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)
Vrlo mala (0.1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)

Izvor: [8]

Nakon izvršene identifikacije imovine mora se izvršiti i identifikacija prijetnji i ranjivosti za svaku pojedinu imovinu. Tipovi prijetnji koji se uzimaju u obzir su: maliciozne prijetnje, nenamjerne prijetnje ili fizičke prijetnje. Nakon identificiranja prijetnji i ranjivosti može se izvesti procjena rizika putem formule:

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

Gdje je rizik jednak umnošku vrijednosti resursa (*Asset value – AV*), vjerojatnosti ostvarenja prijetnje (*Threat probability – P(T))* i posljedicama ostvarenja prijetnje (*Threat impact – I(T))*. Skala za vrednovanje vjerojatnosti ostvarenja prijetnje i njihovih posljedica je ista kao i kod određivanja vrijednosti imovine: vrlo visoka (VV – vrijednost 4), visoka (V – vrijednost 3), srednja (S – vrijednost 2) i niska (N – vrijednost 1).



Slika 2. Postupak ublažavanja rizika prema NIST metodologiji

Izvor: [13]

Prema NIST metodologiji 800-30, preporučeni proces za ublažavanje rizika sastoji se od sedam koraka koji su prikazani na slici 2., a cjelokupan proces za ublažavanje rizika je detaljnije opisan u petom poglavlju ovog diplomskog rada.

4. AKTIVNOSTI PROCJENE RIZIKA U LOGISTIČKIM PODUZEĆIMA

U današnje vrijeme mnoga logistička poduzeća ne shvaćaju koliko je važno provesti procjenu rizika za informacijski sustav koji koriste u poduzeću. S razvojem tehnologije informacija je postala vrlo vrijedna, ali i osjetljiva informacija sklona raznim prijetnjama i napadima, stoga je važno za logističko poduzeće da se provede procjena rizika kroz informacijski sustav kako bi se mogle otkloniti potencijalne prijetnje prije nego prouzroče štetu na informacijskom sustavu.

Procjena rizika je, prema NIST metodologiji 800-30, prvi proces u metodologiji upravljanja rizicima. Mnoge organizacije u svijetu koriste procjenu rizika kako bi utvrdile opseg potencijalne prijetnje i rizika povezane s informacijskim sustavom u svom poduzeću. Ishod procesa procjene rizika pomaže identificirati odgovarajuće kontrole koje će pomoći u smanjenju ili uklanjanju rizika tijekom procesa ublažavanja rizika. NIST metodologija 800-30 rizik definira kao „funkciju vjerojatnosti da određeni izvor prijetnje iskoristi određeni potencijal ranjivosti što će rezultirati štetnim događajem na organizaciju“. [13]

Da bi se utvrdila vjerojatnost budućeg štetnog događaja koji bi ugrozio informacijski sustav, potrebno je analizirati prijetnje informacijskog sustava poduzeća zajedno sa svim potencijalnim ranjivostima. Kao što je ranije navedeno na slici 1 u ovom radu, NIST metodologija 800-30 preporuča devet koraka kojih bi se trebalo pridržavati pri procesu procjene rizika, a to su:

1. korak: Karakterizacija sustava
2. korak: Identifikacija prijetnji
3. korak: Identifikacija ranjivosti
4. korak: Analiza kontrola
5. korak: Određivanje vjerojatnosti
6. korak: Analiza učinka
7. korak: Određivanje rizika
8. korak: Preporuka kontrola
9. korak: Izrada dokumentacije

U narednim poglavljima od 4.1. do 4.9. su detaljnije opisani svaki od devet koraka koji se pojavljuju u provođenju procesa procjene rizika za informacijski sustav logističkog poduzeća.

4.1. Karakterizacija sustava

Prvi korak u procesu procijene rizika je karakterizacija sustava. Karakterizacija sustava znači da se moraju identificirati granice informacijskog sustava poduzeća, zajedno sa svim resursima i informacijama koje čine cjelokupni sustav. Karakteriziranjem informacijskog sustava pokušava se utvrditi opseg procjene rizika, odrediti granice operativnih ovlaštenja koje imaju u informacijskom sustavu i pružaju se informacije o hardware-u, software-u, podršci osoblja i sl. koje su bitne za definiranje rizika. Metodologija za procjenu rizika može se primijeniti za procjene pojedinačnih informacijskih sustava ili za procjene višestrukih, međusobno povezanih informacijskih sustava, ali u svakom slučaju vrlo je važno da domena interesa mora biti dobro definirana prije same primjene metodologije.

Identifikacija rizika za informacijski sustav zahtijeva dobro razumijevanje okoline u kojoj se sustav obrađuje. Osoba ili osobe koje će provesti procjenu rizika nad određenim informacijskim sustavom u logističkom poduzeću, moraju prvo prikupiti sve informacije vezane uz sustav, a koje se klasificiraju na sljedeći način:

- Hardware
- Software
- Sučelje sustava
- Podaci i informacije
- Osobe koje koriste informacijski sustav
- Procesi za koje informacijski sustav služi
- Važnost sustava za poduzeće
- Osjetljivost informacijskog sustava i podataka.

Dodatne informacije za karakterizaciju sustava koje su povezane s radnim okruženjem informacijskog sustava u logističkom poduzeću i njegovim podacima mogu uključivati sljedeće:

- Funkcionalni zahtjevi informacijskog sustava
- Korisnici informacijskog sustava (korisnici koji pružaju tehničku podršku informacijskom sustavu, korisnici aplikacija koji koriste informacijski sustav za obavljanje poslovnih funkcija i sl.)
- Politike sigurnosti sustava koje definiraju upravljanje informacijskim sustavom

- Arhitektura sigurnosti sustava
- Zaštita pohrane informacija u informacijski sustav koja štiti dostupnost, integritet i povjerljivost samih informacija
- Tijek informacija koje se odnose na informacijski sustav (sučelja sustava, unos i sl.)
- Tehničke kontrole koje se koriste za informacijski sustav
- Kontrole upravljanja koje se koriste za informacijski sustav (pravila ponašanja, sigurnosno planiranje i sl.)
- Operativne kontrole koje se koriste za informacijski sustav (sigurnost osoblja, sigurnost kopija, održavanje sustava, postupci uspostavljanja i brisanja korisničkog računa, kontrole segregacije korisničkih funkcija kao što su povlašteni korisnički pristup i sl.)
- Fizičko sigurnosno okruženje informacijskog sustava (sigurnost objekta i sl.)
- Sigurnost okoliša u kojem je implementiran informacijski sustav koji se obrađuje (vlažnost, voda, zagađenje, temperatura, kemikalije i sl.). [13]

Za informacijski sustav koje je u fazi pokretanja ili projektiranja, informacije o njemu mogu se doznati iz projekata ili dokumenata o zahtjevima, a za informacijski sustav koji je u razvoju, potrebno je definirati ključna sigurnosna pravila i atribute koji su planirani za budući informacijski sustav. Dokumenti o projektiranju informacijskog sustava i sigurnosni planovi sustava mogu pružiti vrlo korisne informacije o samoj sigurnosti informacijskog sustava nad kojim se provodi procjena. Vrlo važno je prikupiti sve korisne podatke o sustavu jer se opis sustava može temeljiti na sigurnosti koju pruža temeljna infrastruktura informacijskog sustava ili neki budući planovi za sigurnost informacijskog sustava.

Prikupljanje informacija o informacijskom sustavu može se provoditi tijekom cijelog procesa procjene rizika od 1. koraka – karakterizacije sustava do 9. koraka - dokumentacije rezultata, a za prikupljanje relevantnih informacija o informacijskom sustavu mogu se koristiti različite tehnike prikupljanja informacija, kao što su:

1. **Upitnik** – za prikupljanje relevantnih informacija o sustavu, osoblje koje provodi procjenu rizika može izraditi upitnik o planiranim ili provedenim upravljačkim i operativnim kontrolama za informacijski sustav. Takav upitnik se dostavlja odgovarajućem tehničkom i ne tehničkom osoblju koje projektira ili održava informacijski sustav.

2. **Intervju na licu mjesta** – razgovor s osobljem za podršku informacijskog sustava i menadžmentom može omogućiti osoblju koje obavlja procjenu rizika prikupljanje korisnih informacija o informacijskom sustavu nad kojim se vrši procjena, kao što su informacije o tome kako se sustavom upravlja i sl. Fizički posjet na licu mjesta omogućuje osoblju za procjenu rizika i promatranje i prikupljanje podataka o fizičkim, ekološkim i operativnim sigurnostima informacijskog sustava. Za sustave koji su još u fazi projektiranja tehnika intervjua na licu mjesta bi mogla omogućiti prikupljanje podataka s kojima bi se moglo procijeniti fizičko okruženje u kojem bi taj informacijski sustav funkcionirao. U tablici 4 su prikazani primjeri pitanja koji se koriste tijekom tehnike intervjua na licu mjesta kako bi se postiglo bolje razumijevanje operativnih karakteristika sustava.
3. **Pregled dokumenata** – dokumenti politike (npr. Zakonodavni dokumenti, direktive), sistemska dokumentacija (npr. korisnički vodič, administrativni priručnik, dokument o dizajnu sustava i zahtjevima i sl.) i sigurnosna dokumentacija (npr. prethodno izvješće o reviziji, izvješće o procjeni rizika, rezultati ispitivanja sustava, sigurnosni plan sustava, sigurnosne politike) mogu pružiti korisne informacije o sigurnosnim kontrolama koje su koristili i planirali za informacijski sustav. Analiza učinka misije poduzeća ili procjena kritičnosti imovine pružaju informacije o kritičnosti i osjetljivosti informacija unutar samog sustava.
4. **Korištenje alata za automatsko skeniranje** – mogu se koristiti proaktivne tehničke metode za učinkovito prikupljanje podataka o informacijskom sustavu, kao npr. *Network mapping tool.*

Tablica 4. Primjer pitanja kod tehnike intervjua na licu mjesta

	PITANJA
1.	Tko su ovlašteni korisnici?
2.	Koja je misija poduzeća?
3.	Koja je svrha sustava u odnosu na misiju?
4.	Koliko je sustav važan za misiju poduzeća?
5.	Koji su zahtjevi za dostupnost sustava?
6.	Koje informacije (i dolazne i odlazne) poduzeće zahtijeva?
7.	Koje se informacije generiraju, koriste, obrađuju, pohranjuju i dohvaćaju u sustav?
8.	Koliko su informacije važne za misiju poduzeća?
9.	Koji su putevi protoka informacija?
10.	Koje se vrste informacija obrađuju i pohranjuju u informacijski sustav (npr. financijske, istraživanja i razvoj, kontrola i sl.)?
11.	Koja je razina osjetljivosti tih informacija?
12.	Koje informacije se ne smiju otkriti i kome?
13.	Gdje se konkretno informacije obrađuju i pohranjuju?
14.	Koje su vrste pohrane informacija?
15.	Koliki je potencijalni utjecaj na poduzeće ako se otkrije informacija neovlaštenom osoblju?
16.	Koji su zahtjevi za dostupnost i integritet informacija?
17.	Kakav je učinak na misiju poduzeća ako informacijski sustav ili informacija nisu pouzdani?
18.	Koliko zastoja u sustavu poduzeće može tolerirati? Kojim drugim mogućnostima korištenja sustava korisnik može pristupiti?
19.	Može li sigurnosni kvar sustava ili nedostupnost rezultirati ozljedom ili smrću?

Izvor: [13]

U prethodno navedenoj tablici 4. je dan primjer kakva pitanja se postavljaju i koje korisne informacije se pomoću tih pitanja mogu prikupiti o informacijskom sustavu tijekom provođenja jedne od tehnika za prikupljanje informacija, tzv. tehnike intervju na licu mjesta.

4.2. Identifikacija prijetnji

Kao što je već ranije definirano u ovom radu u poglavlju tri, prijetnja je stalna opasnost koja može izazvati neželjeni incident ili situaciju koja će prouzročiti štetu za informacijski sustav ili cjelokupno logističko poduzeće, a ranjivost sustava je slabost sustava koja može biti slučajno pokrenuta ili pak namjerno iskorištena. Ako postoji izvor prijetnje, ono ne predstavlja rizik za informacijski sustav sve dok ne postoji ranjivost koja bi se mogla iskoristiti protiv njega. Kod identifikacije prijetnje, odnosno određivanja vjerojatnosti prijetnje u obzir se moraju uzeti: izvori prijetnji, potencijalne ranjivosti i postojeće kontrole koje se provode u informacijskom sustavu.

Kada se radi identifikacija izvora prijetnji, važno je identificirati koji je potencijal izvora prijetnji, te sastaviti izjavu o toj prijetnji u kojoj će biti navedeni svi mogući izvori prijetnji koji su primjenjivi na informacijski sustav nad kojim se vrši proces procjene rizika. Izvor prijetnje može biti bilo koja okolnost ili događaj koji ima potencijal da nanese štetu informacijskom sustavu, a uobičajeni izvori prijetnji su:

- Prirodne prijetnje – poplave, tornada, lavine, oluje, klizišta, potresi, itd.
- Prijetnje okolišu – kemikalije, istjecanje tekućine, dugotrajni prekid napajanja, zagađenje i sl.
- Ljudske prijetnje – događaji koji su omogućeni, odnosno prouzrokovani ljudskim djelovanjem, kao što su nenamjeran unos podataka, napadi na mreže, prijenos zlonamjernog software-a, neovlašteni pristup povjerljivim podacima i sl.

Kada se radi procjena izvora prijetnji, vrlo je važno uzeti u obzir sav potencijal izvora prijetnji koji bi mogao prouzročiti štetu za informacijski sustav i njegovo okruženje u logističkom poduzeću. Kao što je već navedeno, ljudske prijetnje su jedne od uobičajenih prijetnji za informacijski sustav, jer ljudi kao izvor prijetnji mogu prouzročiti štetu za sustav kroz namjerne radnje poput namjernih napada od strane zlonamjerne osobe koja bi htjela ugroziti poslovanje logističkog poduzeća samo radi nanošenja štete drugome ili radi svoga profita tzv. sabotaža, nezadovoljni zaposlenici koji također žele nanijeti štetu poduzeću ili nenamjerna djela poput nemara ili pogrešaka. Prema NIST metodologiji smatra se da namjerni napadi na informacijski sustav mogu biti zlonamjerni pokušaji stjecanja neovlaštenog pristupa u informacijski sustav kako bi se ugrozio integritet informacija, dostupnost ili povjerljivost informacija ili mogu biti benigni, ali ipak svrhovit pokušaj zaobilaženja sigurnosti sustava.

Ono što ljude čini potencijalno opasnim izvorom prijetnji je motivacija i resursi za izvođenje napada na informacijski sustav. U tablici 5. su prikazani današnji uobičajeni izvori ljudskih prijetnji, njihove moguće motivacije i metode kojima bi mogli izvršiti sam napad na informacijski sustav, što će biti korisno za logistička poduzeća kako bi mogli bolje promotriti i proučiti radno okruženje i eventualno uočiti neke od ljudskih prijetnji. Također pomoć pri identifikaciji ljudskog izvora prijetnji koji bi mogli naštetiti informacijskom sustavu i njegovim podacima mogu se dobiti iz: pregleda povijesti prekida sustava, prijave kršenja sigurnosti informacijskog sustava, izvješća o incidentnim događajima i sl.

Tablica 5. Primjeri izvora prijetnji, njihove motivacije i metode napada

IZVOR PRIJETNJE	MOTIVACIJA	METODE
Hakeri	• Izazov • Ego • Pobuna	• Hakiranje • Socijalni inženjering • Upad u sustav, provale • Neovlašteni pristup sustavu
Računalni kriminal	• Uništavanje informacija • Nezakonito odavanje informacija • Neovlaštena izmjena podataka	• Računalni kriminal (npr. uhođenje) • Prevara (lažno predstavljanje, presretanje) • Podmićivanje informacija • Upad u sustav
Teroristi	• Ucjena • Uništenje • Iskorištavanje • Osveta	• Bomba/terorizam • Informacijski rat • Sistemski napad (distribuirano uskraćivanje usluge) • Prodor u sustav • Neovlašteno mijenjanje sustava
Industrijska špijunaža (tvrtke, strane vlade, drugi državni interesi)	• Konkurentska prednost • Ekonomska špijunaža	• Ekonomska eksploatacija • Krađa informacija • Ugrožavanje osobne privatnosti • Socijalni inženjering

		• Prodor u sustav • Neovlašteni pristup sustavu (pristup tajnim, vlasničkim i/ili informacijama povezanim s tehnologijom
Zaposlenici (loše obučeni, nezadovoljni, zlonamjerni, nemarni, nepošteni ili otpušteni zaposlenici)	• Znatiželja • Ego • Inteligencija • Osveta • Nehotične pogreške i propusti	• Napad na zaposlenika • Ucjena • Pregledavanje vlasničkih informacija • Zlouporaba računala • Prevara i krađa • Podmićivanje informacija • Unos krivotvorenih ili oštećenih informacija • Presretanje • Zlonamjeran kod (npr. Virus, trojanski konj, logička bomba) • Prodaja osobnih podataka • Sistemske greške • Upad u sustav • Sabotaža sustava • Neovlašteni pristup sustavu

Izvor: [13]

Kako bi se mogla utvrditi vjerojatnost da prijetnja zbilja koristi ranjivost sustava, potrebno je identificirati potencijalni izvor prijetnji te razviti procjenu motivacije, resursa i sposobnosti koje su potrebne da se uspješan napad provede nad informacijskim sustavom u logističkom poduzeću. Sama izjava o prijetnji i/ili popis svih potencijalnih prijetnji za informacijski sustav, trebali bi biti prilagođeni svakom pojedinom logističkom poduzeću i njezinom radnom okruženju, a izjava o prijetnji mora sadržavati popis izvora svih prijetnji koje bi mogle iskoristiti ranjivosti informacijskog sustava u svrhu nanošenja štete. U današnje vrijeme također postoje i mnogobrojni alati za otkrivanje upada u sustave koji postaju sve rasprostranjeniji i dostupniji, a vladine i industrijske organizacije neprestano prikupljaju sve podatke o sigurnosnim događajima čime se radi na poboljšanju sposobnosti realne procjene prijetnji informacijskom sustavu pomoću tih alata.

4.3. Identifikacija ranjivosti

Kao što je već također definirano u ovom radu u poglavlju tri, ranjivosti se smatra svaka slabost informacijskog sustava koja bi se mogla iskoristiti u svrhu nanošenja namjerne ili nenamjerne štete za imovinu logističkog poduzeća. Prema NIST metodologiji 800-30, ranjivosti se smatra svaka greška ili slabost u sigurnosnim postupcima sustava, dizajnu, implementaciji ili unutarnjim kontrolama koje se mogu primijeniti i rezultirati narušavanjem sigurnosti informacijskog sustava. [13] Svaki proces analize prijetnje informacijskog sustava mora uključivati i analizu ranjivosti koje su povezane sa informacijskim sustavom i okolinom u kojoj se on nalazi. Glavni cilj ovog trećeg koraka u procesu procjene rizika je sastaviti popis svih potencijalnih ranjivosti (nedostatke i slabosti) za informacijski sustav koje bi mogle predstavljati potencijalni izvor prijetnji i koje bi mogle biti iskorištene u svrhu nanošenja štete za informacijski sustav u logističkom poduzeću. U tablici 6. su prikazani primjeri mogućih ranjivosti, njihovih prijetnji te koje bi štete mogle biti izazvane preko tih ranjivosti i prijetnji.

Tablica 6. Primjeri ranjivosti, prijetnji i neželjenih incidenata za informacijski sustav

RANJIVOSTI	PRIJETNJE	NEŽELJENI INCIDENT
Sistemski identifikatori otpuštenih zaposlenika (ID zaposlenika) ne uklanjaju se iz informacijskog sustava poduzeća	Otpušteni zaposlenici	Ulaženje u mrežu poduzeća i pristupanje vlasničkim podacima poduzeća
Vatrozid tvrtke dopušta dolazni telnet, te je s ID-em gosta omogućen pristup poznatom serveru poduzeća	Neovlašteni korisnici (hakeri, otpušteni zaposlenici, teroristi, računalni kriminalci)	Korištenje telneta na poznatom serveru poduzeća, te pregledavanje sistemskih datoteka s ID-em gosta
Identificirani su nedostaci u sigurnosnom dizajnu sustava, no nova poboljšanja nisu primijenjena na sustav	Neovlašteni korisnici (hakeri, nezadovoljni zaposlenici, teroristi, računalni kriminalci)	Dobivanje neovlaštenog pristupa osjetljivim informacijama i datotekama u sustavu na temelju poznatih ranjivosti informacijskog sustava
Podatkovni centar koristi raspršivače vode za suzbijanje požara, ali cerade za zaštitu hardware-a i opreme od oštećenja vodom nisu na svome mjestu	Požar, nemarne osobe	Prskalice vode se uključe u podatkovnom centru

Izvor: [13]

Preporučene metode za identificiranje ranjivosti informacijskog sustava su: upotreba izvora ranjivosti, zatim provedba testiranja sigurnosti informacijskog sustava, te na kraju izrada kontrolnog popisa svih sigurnosnih zahtjeva. Ovisno o tome u kojoj se fazi informacijski sustav nalazi i kakve je prirode, vrste ranjivosti mogu varirati, a tako i metodologija koja će biti potrebna za utvrđivanje prisutnosti svih ranjivosti koje postoje u sustavu. Na primjer, ako informacijski sustav još nije dizajniran, onda bi se u procesu identifikacije ranjivosti trebalo usredotočiti na sigurnosne politike sustava, planirane sigurnosne postupke i zahtjeve. Ako je informacijski sustav u procesu implementacije, onda bi se identifikacija ranjivosti trebala proširiti na specifične informacije kao što su planirane sigurnosne značajke opisane u dokumentaciji sigurnosnog projekta, te na rezultate ispitivanja i ocjenjivanja samog informacijskog sustava. A ako je informacijski sustav već u funkciji, odnosno operativan, proces identifikacije ranjivosti bi trebao uključivati analizu svih sigurnosnih značajki i sigurnosnih kontrola informacijskog sustava, te eventualno tehničkih i proceduralnih kontrola koje se koriste za zaštitu sustava.

Tehničke i ne tehničke ranjivosti informacijskog sustava koje su povezane s okruženjem informacijskog sustava, mogu se identificirati pomoću raznih tehnika za prikupljanje informacija. Istraživanjem drugih izvora kao što su web stranice ispitivača koje identificiraju programske greške i nedostatke, mogu biti vrlo korisne kod pripreme intervjua i razvoja upitnika za identifikaciju ranjivosti. Još jedan mogući izvor informacija o poznatim ranjivostima sustava je Internet. Na Internetu se mogu pronaći informacije o poznatim ranjivostima sustava koje su objavili razni ispitivači, gdje su opisani hitni ispravci koji bi se trebali provesti, servisni paketi i druge mogućnosti popravka sustava kako bi se mogle ukloniti ili umanjiti ranjivosti informacijskog sustava. Dokumentirani izvori ranjivosti koji bi se trebali uzeti u obzir pri temeljitoj identifikaciji ranjivosti su:

- Prethodna dokumentacija o procjeni rizika informacijskog sustava
- Izvješća o reviziji informacijskog sustava, izvješće o anomalijama sustava, izvješća o sigurnosnim pregledima, izvješća o testiranjima i ocjenama informacijskog sustava
- Sigurnosni savjeti
- Savjeti ispitivača
- Timovi za komercijalne računalne incidente/hitne slučajeve
- Upozorenja o ranjivosti
- Analize sigurnosti software-a sustava. [13]

Za učinkovito identificiranje ranjivosti informacijskog sustava mogu se koristiti i proaktivne metode za testiranje sustava ovisno o tome koliko je informacijski sustav kritičan i koliki su nam resursi dostupni. Metode identificiranja ranjivosti uključuju: alat za automatsko skeniranje ranjivosti, sigurnosni test i evaluacija (ST&E) i ispitivanje prodora (NIST metodologija 800-42 „*Network Security Testing Overview"* opisuje metodologiju za testiranje mrežnog sustava i korištenje automatiziranih alata). Rezultati bilo koje od prethodne tri navedene metode testiranja sigurnosni informacijskog sustava pomoći će u identificiranju svih ranjivosti informacijskih sustava.

Alati za automatsko skeniranje ranjivosti koriste se za skeniranje grupe hostova ili mreža za poznate ranjive usluge. Međutim, neke od potencijalnih ranjivosti koje je alat za automatsko skeniranje ranjivosti identificirao možda ne predstavljaju stvarnu ranjivost s obzirom na okruženje u kojem se informacijski sustav nalazi. Na primjer, neka potencijalna ranjivost koja je identificirana pomoću alata za automatsko skeniranje ranjivosti, zapravo ne mora predstavljati stvarnu sigurnosnu opasnost za informacijski sustav jer ovakvi alati za prepoznavanje ranjivosti sustava ne uzimaju u obzir okruženje u kojem se informacijski sustav nalazi i zbog toga ovakva metoda identificiranja ranjivosti može dati lažno pozitivne rezultate.

ST&E (Security test and evaluation) je još jedna od metoda identificiranja ranjivosti koja se može koristiti tijekom procesa procjene rizika informacijskih sustava, a može uključivati razvoj i izvršavanje plana ispitivanja kao npr. testna skupina, ispitni postupci i očekivani rezultati ispitivanja. Sama svrha ovakvog ispitivanja sigurnosti informacijskog sustava je provjeriti kolika je učinkovitost sigurnosnih kontrola koje su primijenjene u operativnom okruženju informacijskog sustava, a cilj je da sve sigurnosne kontrole koje su primijenjene na informacijski sustav zadovoljavaju sigurnosne specifikacije za software i hardware i provode sigurnosnu politiku poduzeća, te zadovoljavaju sve industrijske standarde.

Ispitivanje prodora je također jedna od metoda identificiranja ranjivosti, a može se upotrijebiti za nadopunu sigurnosnih kontrola i osiguravanja zaštite različitih aspekata informacijskog sustava. Način rada ove metode identificiranja ranjivosti u sklopu procesa procjene rizika je da se procjenjuje sposobnost informacijskog sustava da izdrži namjerne pokušaje zaobilaženja sigurnosnih mjera informacijskog sustava. Glavni cilj ove metode je testirati informacijski sustav i identificirati potencijalne kvarove u shemama zaštite informacijskog sustava.

Tijekom ovog koraka u procesu procjene rizika, osoblje koje provodi procjenu rizika utvrđuje zadovoljavaju li svi sigurnosni zahtjevi koji su propisani za informacijski sustav sve planirane sigurnosne kontrole. Uglavnom se svi sigurnosni zahtjevi prikazuju u obliku tablice u kojoj se navodi svaki zahtjev, njegovo objašnjenje kako je dizajniran i implementiran u informacijski sustav, te zadovoljava li ili ne zadovoljava sigurnosnu kontrolu. Popis sigurnosnih zahtjeva mora sadržavati osnovne sigurnosne standarde koji bi se trebali koristiti za sustavnu procjenu i identifikaciju ranjivosti informacijskih sustava, kao što su osoblje, hardware-i, software-i, informacije i sl. U tablici 7. su prikazani svi sigurnosni zahtjevi, prema NIST metodologiji 800-30, koji se preporučuju za identifikaciju ranjivosti informacijskog sustava prema sigurnosnim područjima.

Tablica 7. Sigurnosni zahtjevi

PODRUČJE SIGURNOSTI	SIGURNOSNI ZAHTJEVI
Sigurnost upravljanja	• Dodjela odgovornosti • Kontinuitet potpore • Sposobnost odgovora na incident • Povremeni pregled sigurnosnih kontrola • Odobrenje osoblja i pozadinske istrage • Procjena rizika • Sigurnosna i tehnička obuka • Odvajanje dužnosti • Autorizacija sustava i ponovna autorizacija • Sigurnosni plan sustava
Operativna sigurnost	• Kontrola zagađivača iz zraka (dim, prašina, kemikalije) • Kontrole za osiguravanje kvalitetnog napajanja električnom energijom • Pristup i raspolaganje medijskim podacima • Distribucija i označavanje vanjskih podataka • Zaštita objekata (računalne prostorije, podatkovni centar, uredi i sl.) • Kontrola vlažnosti • Kontrola temperature • Radne stanice, prijenosna računala i samostalna osobna računala

Tehnička sigurnost	• Komunikacije (međusobno povezivanje sustava, ruteri i sl.) • Kriptografija • Diskrecijska kontrola pristupa • Identifikacija i provjera autentičnosti • Otkrivanje upada • Ponovna upotreba objekata • Revizija sustava

Izvor: [13]

Ishod identifikacije ranjivosti u procesu procjene rizika je sastaviti kontrolni popis sigurnosnih zahtjeva za informacijski sustav. Također postoji i vodič za samoocjenjivanje sigurnosti za sustave informacijske tehnologije (*Security Self-Assessment Guide for Information Technology Systems*) koje propisuje NIST metodologija 800-26, a pruža opsežan upitnik koji sadrži posebne kontrolne ciljeve prema kojima bi se sigurnost informacijskog sustava mogla testirati i mjeriti.

4.4. Analiza kontrola

Analiza kontrola je četvrti korak u sklopu procesa procjene rizika, a cilj joj je analizirati kontrole koje je logističko poduzeće provelo ili su planirali provesti kako bi se smanjila ili uklonila vjerojatnost prijetnje da iskoristi ranjivost informacijskog sustava. Da bi se mogla odrediti vjerojatnost kojom će potencijalna ranjivost iskoristiti prijetnju u informacijskom sustavu, mora se promotriti provedba trenutnih i/ili planiranih sigurnosnih kontrola sustava. Na primjer, ako se ispostavi da je razina ranjivosti niska ili je vjerojatnost izvora prijetnje niska, onda uz pomoć postojećih sigurnosnih kontrola koje bi trebale ukloniti ili umanjiti štetu, sigurnost informacijskog sustava ne bi trebala biti narušena.

Analiza sigurnosnih kontrola obuhvaća korištenje tehničkih i ne tehničkih metoda. Pod tehničkim metodama se smatraju sve mjere zaštite koje su ugrađene u računalni hardware, software ili firmware, kao što su na primjer mehanizmi za kontrolu pristupa, razno šifriranje informacija, mehanizmi identifikacije i provjere autentičnosti pristupa informacijama, softveri za otkrivanje upada i sl. A pod ne tehničkim metodama sigurnosnih kontrola smatraju se sve sigurnosne politike logističkog poduzeća, operativni postupci i osobna i fizička zaštita okoline informacijskog sustava, odnosno može se reći da u ne tehničke metode upravljačke i operativne sigurnosne kontrole.

Osim kategorizacije analize kontrole na tehničke i ne tehničke metode, one se nadalje mogu klasificirati i na preventivne ili detekcijske kontrole sigurnosti sustava. Svrha preventivnih kontrola sigurnosti informacijskih sustava je sprečavanje svakog pokušaja kršenja sigurnosne politike, a uključuje i provođenje kontrole pristupa, šifriranje informacija i provjere autentičnosti. Svrha detekcijskih kontrola je upozoriti na kršenje ili pokušaje kršenja sigurnosnih politika, a uključuje i metode otkrivanja upada u informacijski sustav i kontrolne sume.

Da bi se sigurnosne kontrole analizirale na sustavan i učinkovit način, od velike pomoći će biti i sastavljanje popisa sigurnosnih zahtjeva ili upotreba dostupnog kontrolnog popisa sigurnosnih zahtjeva informacijskog sustava. Pomoću tog popisa sigurnosnih zahtjeva mogu se provjeriti sve sigurnosne usklađenosti, ali i sigurnosne neusklađenosti u informacijskom sustavu. Stoga je za logističko poduzeće jako važno redovito ažurirati takve kontrolne popise, ako na primjer dođe do promjene sigurnosnih politika, sigurnosnih metoda i sl., kako bi se kontinuirano mogla osigurati valjanost takvog kontrolnog popisa sigurnosnih zahtjeva.

4.5. Određivanje vjerojatnosti

Određivanje vjerojatnosti je peti korak u procesu procjene rizika koji prikazuje vjerojatnost da se potencijalna ranjivost sustava može iskoristiti za provedbu prijetnje, a da bi se ona mogla odrediti moraju se u obzir uzeti sljedeći čimbenici:

- Motivacija i sposobnost izvora prijetnji
- Postojanje i učinkovitost trenutnih sigurnosnih kontrola
- Priroda ranjivosti. [13]

Kao što je već ranije navedeno u poglavlju 3.2. u ovom radu, vjerojatnost da određeni izvor prijetnje iskoristi potencijalnu ranjivost sustava, klasificira se u tri razine, a to su niska, srednja i visoka:

- Niska – izvor prijetnje nema motivaciju ili sposobnosti ili postoje kontrole koje sprječavaju ili eventualno ometaju ranjivost
- Srednja – izvor prijetnje motiviran je i sposoban, ali postoje kontrole koje ometaju uspješno provođenje ranjivosti
- Visoka – izvor prijetnje je visoko motiviran i sposoban, a kontrole koje bi trebale spriječiti ranjivost sustava nisu učinkovite. [13]

Dakle, ishod ovog koraka u procesu procjene rizika je ocjenjena vjerojatnost pomoću tri razine da određeni izvor prijetnje iskoristi potencijalnu ranjivost informacijskog sustava.

4.6. Analiza učinka

Nakon što se napravi analiza kontrole, odredi vjerojatnost prijetnji i ranjivosti, sljedeći korak u procesu procjene rizika je analiza učinka. Analiza učinka određuje koliki je štetan utjecaj koji će proizaći kao rezultat uspješne iskoristivosti ranjivosti informacijskog sustava. Prije početka obavljanja analize učinka potrebno je pribaviti određene informacije, a to su: koja je misija sustava, koje su sve kritičnosti sustava i informacija, te koje su osjetljivosti sustava i informacija.

Sve se navedene informacije mogu pribaviti iz postojećih dokumentacija logističkog poduzeća kao što su izvješća o analizi utjecaja na misiju ili izvješća o procjeni kritičnosti

imovine. Analiza utjecaja na misiju poznata je i kao analiza utjecaja na poslovanje, a prioritet prilikom analize daje razinama utjecaja povezanim s kompromisom informacijske imovine poduzeća na temelju kvantitativne ili kvalitativne procjene imovine. Procjenom kritičnosti imovine identificiraju se osjetljiva i kritična informacijska sredstva u poduzeću, te se kao takvima daje prioritet.

Ako takva dokumentacija u logističkom poduzeću ne postoji, osjetljivost sustava i informacija u informacijskom sustavu logističkog poduzeća može se odrediti na temelju razine zaštite koja je potrebna za održavanje sustava, te za održavanje dostupnosti, integriteta i povjerljivosti informacija. Shodno tome, vlasnici sustava i informacija, odnosno zaposlenici koji su odgovorni za svaki pojedini dio sustava i informacije, odgovorni su za određivanje razine utjecaja na vlastiti sustav i informacije bez obzira koja se metoda koristila za utvrđivanje osjetljivosti informacijskih sustava. Zbog toga se smatra da je kod analize učinka najbolji način za provođenje intervju sa sustavom i vlasnicima informacija. Zato se svaki nepovoljan utjecaj na sigurnost sustava smatra gubitkom ili degradacijom jednog ili kombinacijom nekih od tri sigurnosna cilja, a to su: dostupnost, integritet i povjerljivost. U nastavku su opisani svaki od tri sigurnosna cilja, te njihove posljedice neispunjenja:

1. **Gubitak dostupnosti** – ako informacijski sustav koji je od kritične važnosti za misiju, nije dostupan krajnjim korisnicima, to će onda utjecati na misiju logističkog poduzeća. Gubitak funkcionalnosti sustava i operativne učinkovitosti sustava može rezultirati gubitkom produktivnog vremena, što će rezultirati onemogućenim radom krajnjim korisnicima koji neće moći izvršiti svoju funkciju za koju su zaduženi u procesu rada logističkog poduzeća i izvršenja misije logističkog poduzeća.
2. **Gubitak integriteta** – integritet sustava i informacija se odnosi na zahtjev da se informacije zaštite od nepravilne izmjene. Integritet će se izgubiti ako budu izvršene namjerne ili slučajne radnje neovlaštene izmjene informacija u sustavu ili informacijskog sustava. Ako se gubitak integriteta sustava ili informacija ne ispravi na vrijeme, svaka daljnja uporaba kontaminiranog sustava ili oštećene informacije mogla bi rezultirati netočnošću, prijevarom ili pogrešnim odlukama. Također, kršenje integriteta sustava i informacije može biti prvi korak u uspješnom napadu na dostupnost sustava ili na povjerljivost sustava, zbog toga se smatra da se gubitkom integriteta sustava i informacija umanjuje sigurnost samog informacijskog sustava.

3. **Gubitak povjerljivosti** – povjerljivost sustava i informacija odnosi se na zaštitu informacija od neovlaštenog otkrivanja. Neovlašteno otkrivanje povjerljivih informacija iz sustava može prouzročiti razne štete za logističko poduzeće. Neovlašteno, neočekivano ili nenamjerno objavljivanje povjerljivih informacija mogli bi rezultirati gubitkom povjerenja javnosti, neugodnošću za pojedince ili poduzeće u cijelosti ili sudskim postupcima protiv logističkog poduzeća. [13]

Neki od utjecaja na logističko poduzeće mogu se kvantitativno mjeriti gubitkom prihoda, troškovima popravka sustava, razinom napora koji je potreban da se ispravi problem prouzročen uspješnom akcijom prijetnje, dok se drugi utjecati kao što su štete za interes logističkog poduzeća, gubitak povjerenja javnosti i sl. ne mogu mjeriti u određenim jedinicama, već kvalificiraju u tri razine utjecaja, a to su: niski utjecaj, srednji utjecaj i visoki utjecaj:

- Niski utjecaj – vježba ranjivosti može rezultirati gubitkom neke materijalne imovine ili može značajno utjecati na misiju, ugled i interes poduzeća
- Srednji utjecaj – vježba ranjivosti može rezultirati skupim gubitkom materijalne imovine, može povrijediti ili nanijeti štetu misiji, ugledu i interesu poduzeća, te može dovesti i do ozljeda zaposlenih radnika u poduzeću
- Visoki utjecaj – vježba ranjivosti može rezultirati skupocjenim gubitkom glavne materijalne imovine, može značajno povrijediti ili nanijeti štetu misiji, ugledu i interesu poduzeća, te može rezultirati ljudskom smrću ili nanošenjem teških ozljeda. [13]

Provođenjem analize učinka u obzir bi trebalo uzeti prednosti i nedostatke kvantitativnih u odnosu na kvalitativne metode procjene rizika koje su već ranije opisane u ovom radu. Prednost kvalitativne metode nad kvantitativnom je ta što ona daje prioritet rizicima i identificira područja kod kojih treba provesti trenutno poboljšanje kako bi se umanjila ranjivost sustava. Nedostatak kvalitativne metode je taj što ona ne pruža specifična mjerenja veličine utjecaja na sustav, te je zbog toga analiza isplativosti svih preporučenih kontrola za informacijski sustav otežana, za razliku od kvantitativne metode kojoj je to prednost jer ona omogućuje mjerenje veličine utjecaja na sustav što se može koristiti u analizi isplativosti preporučenih kontrola za informacijski sustav. Nedostatak kvantitativne metode je taj što, ovisno o brojčanim rasponima koji će se koristiti za izražavanje mjera, značenje analize pomoću ove metode može biti pomalo nejasno te se zbog toga rezultat mora interpretirati na kvalitativan način.

4.7. Određivanje rizika

Sedmi korak u procesu procjene rizika je određivanje rizika, a njegova svrha je procijeniti kolika je razina rizika za promatrani informacijski sustav. Određivanje rizika za određeni par prijetnji-ranjivosti može se izraziti kao funkcija vjerojatnosti da određeni izvor prijetnje pokušava iskoristiti zadanu ranjivost ili kao veličina utjecaja kojom bi izvor prijetnje uspješno iskoristio ranjivost sustava ili kao primjerenost planiranih ili postojećih sigurnosnih kontrola za smanjenje ili uklanjanje rizika. [13] Kako bi se rizik mogao izmjeriti potrebno je razviti ljestvicu rizika i matricu rizika kako je već ranije opisano u ovom radu.

Određivanje rizika provodi se tako što se množi ocjena koja je dodijeljena za vjerojatnost prijetnje i utjecaj prijetnje na informacijski sustav. U radu je već prikazano pod tablicom 2 u obliku matrice 3x3 na koji način je moguće odrediti ukupnu ocjenu rizika na temelju vjerojatnosti prijetnje i utjecaja prijetnje. Ovisno o zahtjevima logističkog poduzeća i detaljnoj procijeni rizika može se koristiti i matrica 4x4 ili 5x5. Ako se koriste takve matrice onda one osim klasične podjele vjerojatnosti prijetnje i utjecaja na nisku, srednju i visoku, koriste još i vrlo nisku ili vrlo visoku vjerojatnost prijetnje i vrlo nizak ili vrlo visok utjecaj prijetnje na informacijski sustav kako bi se shodno tome mogla generirati i vrlo niska ili vrlo visoka razina rizika. Ako se procijeni da je razina rizika vrlo visoka, jedino rješenje za sustav je njegovo isključivanje ili zaustavljanje svih pokušaja integracije i testiranja informacijskog sustava u logističko poduzeće.

Razine rizika koje se uglavnom dijele na niska, srednja i visoka, koje su prikazane u tablici 2, također su već opisane u sklopu ovog rada. Ta ljestvica rizika predstavlja stupanj, odnosno razinu rizika kojem će informacijski sustav poduzeća biti izložen ako se ne isprave identificirane ranjivosti sustava. Ljestvica rizika može definirati radnje koje bi više rukovodstvo logističkog poduzeća ili vlasnici logističkog poduzeća trebali ili morali poduzeti za svaku razinu rizika kako bi informacijski sustav logističkog poduzeća bio siguran i kako bi se umanjio rizik prijetnje.

4.8. Preporuka kontrola

Predzadnji korak u procesu procjene rizika je preporuka kontrola za sigurnost informacijskog sustava. Tijekom koraka preporuke kontrola trebali bi se osigurati sve kontrole koje bi mogle umanjiti ili eventualno ukloniti sve identificirane rizike u sustavu. Glavni cilj preporuke kontrola je smanjenje razine rizika informacijskog sustava i njegovih informacija na prihvatljivu razinu. Kod preporuke kontrola i alternativnih rješenja za smanjenje ili uklanjanje identificiranih rizika u obzir treba uzeti neke čimbenike, a to su:

- Organizacijska politika poduzeća
- Zakonodavstvo i propisi
- Učinkovitost preporučenih opcija (kompatibilnost za informacijski sustav)
- Sigurnost i pouzdanost
- Operativni utjecaj.

Preporuke kontrola za informacijski sustav su donijete kao rezultat procesa procjene rizika i omogućuju ulaz u proces ublažavanja rizika tijekom kojeg će se preporučene kontrole (proceduralne i tehničke) ocijeniti, prioritizirati i provesti. Potrebno je napomenuti i da sve kontrole koje su preporučene možda neće biti moguće provesti kako bi se smanjio gubitak, stoga kako bi se moglo odrediti koje su kontrole stvarno potrebne i prikladne i neophodne za informacijski sustav i logističko poduzeće potrebno je provesti analizu troškova i koristi (tzv. *Cost-benefit analysis*) za sve preporučene kontrole kako bi se na taj način pokazalo da će troškovi koji će biti uloženi u provedbu kontrola, biti opravdani smanjenjem razine rizika za poduzeće i informacijski sustav. Osim provođenja analize troškova i koristi nad preporučenim kontrolama za smanjenje rizika, potrebno je i pažljivo procijeniti izvedivost (prihvaćanje korisnika, tehnički zahtjevi i sl.) i operativni utjecaj (učinak na performanse sustava) prilikom provedbe preporučenih kontrola za ublažavanje rizika.

4.9. Izrada dokumentacije

Posljednji korak u procesu procjene rizika je izrada dokumentacije. Nakon što su dovršeni svi koraci u procesu procjene rizika, identificirani su izvori prijetnji i ranjivosti, određene su vjerojatnosti, analiziran je učinak, procijenjen je rizik i preporučene su kontrole, sve te rezultate treba dokumentirati u službenom izvješću.

Dokumentacija koja se sastavlja na kraju procesa procjene rizika naziva se izvješće o procjeni rizika, a ono je upravljačko izvješće koje će pomoći vlasnicima logističkog poduzeća i/ili višem menadžmentu pri donošenju odluka o svim političkim, proceduralnim, proračunskim, operativnim i upravljačkim promjenama u informacijskom sustavu. Izvješće o procjeni rizika smatra se sustavnim i analitičkim pristupom procjeni rizika kako bi više rukovodstvo i vlasnici logističkog poduzeća mogli razumjeti rizike i kako bi uložili određeni dio sredstava za smanjenje i ispravljanje potencijalnih gubitaka.

Tablica 8. Izvješće o procjeni rizika

IZVJEŠĆE O PROCJENI RIZIKA	
I.	**UVOD**
• Svrha • Opseg ove procjene rizika Opišite sve komponente informacijskog sustava, elemente, korisnike i sve ostale pojedinosti o sustavu koje bi trebalo uzeti u obzir pri procjeni rizika.	
II.	**PRISTUP PROCJENI RIZIKA**
Ukratko opišite pristup koji se koristio za provođenje procjene rizika kao na primjer: • Sudionici (članovi tima za procjenu rizika) • Tehnike prikupljanja informacija (koji su alati korišteni za prikupljanje informacija o sustavu, koji su upitnici korišteni i sl.) • Razvoj i opis ljestvice rizika (matrice razine rizika 3x3, 4x4 ili 5x5).	
III.	**KARAKTERIZACIJA SUSTAVA**
Opišite sustav, uključujući hardware (server, ruter i sl.), software (aplikacije, operacijski sustav, protokole i sl.), sučelja sustava (komunikacijska veza), informacije i korisnike. Dostavite dijagram povezivanja ili dijagram toka ulaza i izlaza sustava kako bi se procijenio opseg napora za procjenu rizika za određeni informacijski sustav.	

IV.	**IZJAVA O PRIJETNJI**
Potrebno je sastaviti i navesti sve moguće izvore prijetnji u informacijskom sustavu i sve povezane prijetnje koje se primjenjuju na informacijski sustav koji se procjenjuje.	
V.	**REZULTAT PROCJENE RIZIKA**
Navedite opažanja, koji su parovi ranjivosti-prijetnje. Svako zapažanje mora uključivati: • Broj promatranja i kratak opis promatranja (npr. Opažanje 1.: Zaporke informacijskog sustava mogu se pogoditi ili razbiti) • Raspravu o paru ranjivost-prijetnja • Identifikacija postojećih ublažavajućih sigurnosnih kontrola • Rasprava i procjena vjerojatnosti (velika, srednja ili niska) • Rasprava i evaluacija analize učinka • Ocjena rizika na temelju matrice razine rizika (visoka, srednja ili niska) • Preporučene kontrole ili alternativne mogućnosti za smanjenje rizika.	
VI.	**SAŽETAK**
Ukupan broj opažanja. Opažanja se trebaju sažeti, moraju se povezati razine rizika, definirati preporuke i sve komentare u obliku tablice kako bi se olakšala provedba preporučenih kontrola tijekom procesa ublažavanja rizika za promatrani informacijski sustav.	

Izvor: [13]

Ishod posljednjeg koraka u procesu procjene rizika tzv. izrada dokumentacije je izvješće o procjeni rizika u kojem se opisuju prijetnje i ranjivosti informacijskog sustava, mjeri se rizik i daju se preporuke za provedbu kontrola za umanjenje rizika, a primjer jednog takvog izvješća prikazan je u tablici 8.

5. AKTIVNOSTI UBLAŽAVANJA RIZIKA U LOGISTIČKIM PODUZEĆIMA

Aktivnosti ublažavanja rizika je slijedeći korak koji nastupa nakon završenog procesa procijene rizika, odnosno nakon što se definiraju i odrede koje su ranjivosti, prijetnje i rizici u informacijskom sustavu logističkog poduzeća. Aktivnosti ublažavanja rizika smatraju se drugim procesom upravljanja rizika, a ono uključuje: određivanje prioriteta, ocjenu, te provedbu svih odgovarajućih kontrola koje su potrebne za smanjenje rizika informacijskog sustava logističkog poduzeća, a preporučene su po završetku procesa procjene rizika. Kao što je već ranije spomenuto u ovom radu u poglavlju 4.8., uklanjanje svih postojećih rizika i primjena svih preporučenih kontrola za informacijski sustav neće biti moguća, zbog toga vlasnici logističkog poduzeća ili viši menadžment poduzeća bi trebao odabrati pristup u kojem će biti primijenjene najprikladnije preporučene kontrole za ublažavanje rizika na prihvatljivu razinu.

Kao što je već ranije prikazano u ovom radu na slici 2., aktivnosti procesa ublažavanja rizika u logističkim poduzećima dijele se na sedam koraka, a to su:

1. korak: Određivanje prioriteta
2. korak: Pregled sigurnosnih kontrola
3. korak: Analiza isplativosti
4. korak: Odabir kontrola
5. korak: Dodjeljivanje odgovornosti
6. korak: Izrada plana za obradu rizika
7. korak: Implementacija odabranih kontrola.

Proces ublažavanja rizika vrlo je važan za logističko poduzeće kako bi informacijski sustav i sve informacije poduzeća bile sigurne od prijetnji i narušavanja njihove dostupnosti, integriteta i povjerljivosti. Rizik se, također, može smanjiti i putem opcija za smanjenje rizika, kao na primjer što su preuzimanje rizika, planiranje rizika, istraživanje i priznanje, izbjegavanje rizika, prijenos rizika ili ograničenje rizika. U svakom slučaju, bez obzira koja god opcija za smanjenje rizika bila odabrana od prethodno navedenih, uvijek je potrebno u obzir uzeti ciljeve i misiju logističkog poduzeća. Određivanje koji identificirani rizik ima prioritet u rješavanju se radi tako da se pravo prvenstva daje parovima ranjivost-prijetnja koji bi mogli uzrokovati značajnu štetu na ciljeve i misiju logističkog poduzeća.

Jedno od dva glavna pitanja koja bi si vlasnici logističkih poduzeća i viši menadžment trebali postaviti po dobivanju izvješća o procjeni rizika i prije kretanja u proces ublažavanja rizika su:

- Kada bi trebao primijeniti preporučene kontrole za ublažavanje rizika i zaštititi svoje poduzeće?
- Kada i pod kojim okolnostima bi trebao poduzeti određene mjere?

Prema NIST metodologiji 800-30 postoje smjernice, tzv. strategije o mjerama za ublažavanje rizika kada bi se i što bi se trebalo učiniti:

- Kada postoji ranjivost informacijskog sustava treba provesti određene tehnike kako bi se smanjila vjerojatnost da će se ranjivost iskoristiti.
- Kada se može iskoristiti ranjivost informacijskog sustava potrebno je primijeniti slojevitu zaštitu ili provesti administrativne kontrole kako bi se smanjio rizik ili kako bi se spriječila ova pojava.
- Kada su troškovi napadača manji od potencijalne dobiti onda se nad informacijskim sustavom treba provesti sigurnosna zaštita koja će smanjiti napadačevu motivaciju i povećati mu troškove.
- Kada je gubitak prevelik za poduzeće onda bi se trebala primijeniti tehnička i ne tehnička zaštita informacijskog sustava kako bi se ograničio opseg napada, a time istodobno i smanjila mogućnost gubitka.

Gore navedene strategije se uglavnom koriste za ublažavanje rizika uzrokovanim namjernim ljudskim prijetnjama, ali ako se izuzme treća stavka, navedene strategije se mogu primijeniti i na ublažavanje rizika uzrokovane okolišnim ili ne namjernim ljudskim prijetnjama.

5.1. Pristup za provedbu preporučenih kontrola

Kada se pristupa provođenju preporučenih kontrola za ublažavanje identificiranih rizika, NIST metodologija 800-30 kaže da vrijedi sljedeće pravilo:

„Riješite najveće rizike i težite dovoljnom ublažavanju rizika uz najniže troškove, ali uz minimalan utjecaj na druge sposobnosti misije poduzeća.“

Kao što je već ranije spomenuto u ovom poglavlju, aktivnostima ublažavanja rizika u logističkom poduzeću pristupa se kroz sedam koraka koji određuju kako će se pristupiti provođenju preporučenih kontrola za ublažavanje rizika nakon provedenog procesa procjene rizika nad informacijskim sustavom logističkog poduzeća.

Određivanje prioriteta se radi na način da se prouči izvješće o procjeni rizika i prioritet se da stavkama koje su visoko rizične za logističko poduzeće, odnosno onim stavkama koje imaju neprihvatljivo visoku razinu rizika (ocijenjene su kao vrlo visoka ili visoka razina rizika). Takve stavke, odnosno parovi ranjivost-prijetnja zahtijevaju hitne korektivne mjere kako bi se zaštitio interes i misija logističkog poduzeća.

Pregled sigurnosnih kontrola koje su preporučene po završetku procesa procjene rizika. Jer postoji mogućnost da neke od preporučenih sigurnosnih kontrola nisu najprikladnije za logističko poduzeće ili možda nisu izvedive za određeno logističko poduzeće i njezin informacijski sustav. Zato se tijekom ovog koraka analizira izvedivost sigurnosnih kontrola kao što je prihvaćanje od strane zaposlenika, kompatibilnost s informacijskim sustavom i poduzećem i sl., te učinkovitost sigurnosnih kontrola, odnosno koliko će njihovom primjenom informacijski sustav zapravo biti zaštićen i u kojoj mjeri će rizik biti ublažen. Cilj je pomoću ovog koraka odabrati najprikladniju preporučenu sigurnosnu kontrolu za ublažavanje rizika koja će biti adekvatna za logističko poduzeće i njezin informacijski sustav.

Analiza isplativosti se provodi kako bi se vlasnicima poduzeća i/ili višem menadžmentu pomoglo pri donošenju odluka i identifikaciji koje od preporučenih sigurnosnih kontrola za ublažavanje rizika su isplative za logističko poduzeće. U poglavlju 5.2. će se malo detaljnije opisati provođenje analize isplativosti.

Odabir kontrola se vrši na temelju odrađene analize isplativosti, odnosno vlasnici logističkih poduzeća i/ili viši menadžment će odabrati koje su preporučene sigurnosne kontrole najisplativije za ublažavanje rizika u logističkom poduzeću. Kontrole koje budu odabrane trebale bi kombinirati tehničke, operativne i upravljačke elemente, kako bi se mogla osigurati odgovarajuća sigurnost za informacijski sustav i cijelo logističko poduzeće.

Dodjeljivanje odgovornosti je bitna stavka u procesu ublažavanja rizika, jer je važno identificirati osobe koje imaju odgovarajuću razinu stručnosti, znanja i vještina za provođenje odabranih sigurnosnih kontrola za ublažavanje rizika, te se tim osobama dodjeljuje odgovornost. Na kraju ovog koraka će se izraditi popis odgovornih osoba.

Izrada plana za obradu rizika je korak u procesu ublažavanja rizika u kojem se izrađuje plan za provedbu odabranih sigurnosnih kontrola za ublažavanje rizika, tzv. akcijski plan. Primjer jednog takvog plana prikazan je u tablici 9., a on bi trebao sadržavati neke od sljedećih podataka: rezultate o rizicima iz izvješća o procjeni rizika, odnosno parove ranjivosti-prijetnje, preporučene kontrole, koje su prioritetne radnje (stavke koje su u izvješću označene kao visoki ili vrlo visoki rizik), odabrane planirane kontrole koje su utvrđene na temelju izvedivosti, učinkovitosti i koristi za logističko poduzeće, kolika su potrebna sredstva za provedbu odabranih planiranih kontrola, popis svih odgovornih osoba, datum početka implementacije mjera za ublažavanje rizika, ciljani datum završetka cjelokupnog procesa ublažavanja rizika i koji su zahtjevi za održavanje informacijskog sustava sigurnim. Izradom plana za obradu rizika prikazuju se kontrole koje su prioritetne za provedbu, daju se okvirni početni i završni datumi do kad proces treba biti završen, te se ubrzava izvođenje procesa ublažavanja rizika.

Implementacija odabranih kontrola je zadnji korak u aktivnostima ublažavanja rizika kod kojeg se sve preporučene kontrole koje su određene kao prioritetne implementiraju u informacijski sustav logističkog poduzeća. Implementacijom odabranih sigurnosnih kontrola razina rizika se može ublažiti, ali rizik se ne može ukloniti.

Logistička poduzeća mogu analizirati koliki je opseg smanjenog rizika nakon provedbe i implementacije preporučenih sigurnosnih kontrola u informacijski sustav, a te sigurnosne kontrole mogu umanjiti rizik tako što će ukloniti neke od ranjivosti informacijskog sustava čime će se smanjiti i broj mogućih identificiranih parova ranjivosti-prijetnja, mogu potaći rukovodstvo logističkog poduzeća na dodavanje ciljanih kontrola za sigurnost informacijskog sustava čime će se smanjiti kapacitet i motivacija izvora prijetnje ili će smanjiti veličinu štetnog utjecaja na informacijski sustav.

Tablica 9. Plan za provedbu sigurnosnih kontrola za ublažavanje rizika

(1) **Rizik (par ranjivost-prijetnja)**	Neovlašteni korisnici mogu putem telneta pristupiti poznatom serveru u poduzeću i pregledavati osjetljive informacije pomoću ID-a gosta.
(2) **Razina rizika**	Visoka
(3) **Preporučene kontrole**	• Onemogućiti dolazni telnet • Onemogućiti pristup svima osjetljivim informacijama poduzeća • Onemogućiti ID gosta ili takvom ID-u dodijeliti lozinku koju je teško pogoditi
(4) **Prioritet akcije**	Visoki
(5) **Odabrane planirane kontrole**	• Onemogućiti dolazni telnet • Onemogućiti pristup svima osjetljivim informacijama poduzeća • Onemogućiti ID gosta
(6) **Potrebni resursi**	10 sati za ponovno konfiguriranje i testiranje informacijskog sustava poduzeća
(7) **Odgovorne osobe (tim)**	Pero Perić, administrator sustava logističkog poduzeća Ivo Ivić, administrator zaštitnog zida logističkog poduzeća
(8) **Datum početka/ Datum završetka**	Od 01. 09. 2021. do 02. 09. 2021.
(9) **Uvjeti održavanja/ Komentari**	Izvršavati povremene preglede i testiranja sigurnosti informacijskog sustava kako bi se osigurala odgovarajuća sigurnost za poznati server u logističkom poduzeću

Izvor: [13]

Rizik koji ostane nakon provedbe i implementacije sigurnosnih preporuka za ublažavanje rizika naziva se preostali rizik. U današnjem svijetu niti jedan informacijskih sustav bilo kojeg poduzeća nije bez rizika, rizik uvijek postoji od bilo čega i uvijek je prisutan. Stoga nakon implementiranih sigurnosnih kontrola za ublažavanje rizika uvijek ostaje jedan dio preostalog rizika, jer razina rizika se ne može smanjiti na nulu. Preostali rizik koji ostaje nakon provedbe prioritetnih sigurnosnih kontrola se identificira, te viši menadžment i/ili vlasnici logističkog poduzeća odlučuju trebaju li se ponovno provoditi dodatne kontrole za ublažavanje rizika koji su preostali u informacijskom sustavu logističkog poduzeća.

5.2. Analiza isplativosti

Analiza isplativosti preporučenih sigurnosnih kontrola za ublažavanje rizika informacijskog sustava logističkog poduzeća se provodi kako bi se odredilo koje od preporučenih kontrola su isplative za provođenje u poduzeću. Odnosno, analiza isplativosti se provodi kako bi se pravilo raspodijelili resursi i provele samo one kontrole koje su isplative i primjerene za informacijskog sustava i logističkog poduzeća nad kojima će se provesti.

Analiza isplativosti može biti kvalitativna ili kvantitativna, a njezina svrha je pokazati kako se uloženi troškovi u provedbu sigurnosnih kontrola za ublažavanje rizika mogu opravdati stvarnim smanjenjem rizika za informacijski sustav. Analiza isplativosti koja se provodi nad preporučenim sigurnosnim kontrolama mora obuhvaćati sljedeće elemente:

- Određivanje koliki je učinak ako se preporučene kontrole primjene
- Određivanje koliki će biti utjecaj ako se neke od preporučenih kontrola ne provedu
- Procjenu koliki će biti trošak implementacije preporučenih kontrola, a to može uključivati: kupnju hardware-a i software-a, troškove obuke zaposlenika, troškove održavanja sustava, troškove provedbe dodatnih politika i postupaka, troškovi angažiranja dodatnog osoblja koje će biti potrebno za provedbu preporučenih sigurnosnih kontrola i sl.
- Procjenu troškova i koristi implementacije preporučenih kontrola u odnosu na kritičnost sustava i informacija u kojem se trenutno nalaze

Vlasnici logističkih poduzeća ili viši menadžment će morati procijeniti vrijedi li uložiti u nove preporučene sigurnosne kontrole kako bi se održao prihvatljiv informacijski sustav u poduzeću ili ne, jer kako postoji trošak ulaganja u implementaciju nekih od preporučenih sigurnosnih kontrola za ublažavanje rizika, tako postoji i trošak i za neprovođenje tih kontrola. Rukovodstvo logističkog poduzeća će procijeniti što za njih znači prihvatljiva razina rizika, nakon toga će se procijenit učinak preporučene sigurnosne kontrole, te hoće li se ta kontrola primijeniti ili ne. Također postoje i određena pravila koja vrijede za odlučivanje o poduzimanju preporučenih sigurnosnih kontrola za ublažavanje rizika, a to su:

- Ako preporučena kontrola osigurava dovoljno smanjenje rizika za logističko poduzeće, isplativa je i treba ju primijeniti.

- Ako bi preporučena kontrola smanjila rizik više nego što je potrebno, onda se provjerava postoji li koja jeftinija alternativa.
- Ako preporučena kontrola košta više od predviđenog smanjenja rizika, onda se također provjerava postoji li koja jeftinija alternativa.
- Ako preporučena kontrola ne ublaži rizik na prihvatljivu razinu, primjenjuju se još neke dodatne kontrole ili se traži druga alternativa.

Može se zaključiti kako viši menadžment i/ili vlasnici logističkog poduzeća igraju ključnu ulogu pri donošenju odluka o tome koje bi se preporučene sigurnosne kontrole trebale provesti, a koje ne, jer oni najbolje poznaju misiju poduzeća te sukladno tome znaju kako ju najbolje zaštititi i kolika razina rizika je za njih prihvatljiva.

6. ZAKLJUČAK

U logističkim poduzećima, informacija i informacijski sustav imaju veliku važnost za čitavo poduzeće, jer moraju adekvatno funkcionirati kako bi poduzeće moglo efikasno i kontinuirano poslovati. Jer ako se dogodi zastoj u radu informacijskog sustava zbog na primjer napada na sustav, odnosno zbog nekog iskorištenja ranjivosti u sustavu, moguće je da logističko poduzeće pretrpi veliku štetu i gubitak za poslovanje. Osim funkcionalnosti samog informacijskog sustava, potrebno je da informacije koje dobivaju putem tih sustava budu točne i dostupne u pravo vrijeme. Još jedan razlog zašto je informacijski sustav bitan za logističko poduzeće, jer je on taj koji prikuplja, obrađuje i čuva informacije povjerljive i nepovjerljive podatke o poduzeću i poslovanju.

Kako logističko poduzeće ne bi ostvarilo veliki gubitak za poslovanje, preporuka je redovito održavanje informacijskih sustava i njegove sigurnosti te kontinuirana periodička provedba procjene rizika za cjelokupni informacijski sustav i njegovo okruženje u logističkom poduzeću. Preporuka NIST metodologije 800-39 je da se za razvoj svih operativnih planova logističkog poduzeća moraju procijeniti parovi ranjivosti-prijetnja i njihov utjecaj kako bi se moglo odlučiti gdje bi se trebali uložiti dodatni napori za uklanjanje ili smanjenje prijetnji, te otkloniti ili smanjiti ranjivosti informacijskog sustava logističkog poduzeća.

Cilj i svrha ovog diplomskog rada je bio objasniti važnost same informacije i informacijskih sustava, te važnost očuvanja sigurnosti informacija i informacijskih sustava kako ne bi došlo do narušavanja njihove dostupnosti, integriteta i povjerljivosti. Osim toga, cilj je bio napisati smjernice za provođenje postupka procjene rizika za informacijski sustav koje bi mogle poslužiti kao predložak za upravljanje informacijskim rizicima u logističkim poduzećima.

Može se zaključiti kako je za logističke sustave najbolje da periodično provode procjenu rizika za informacijski sustav i njegovo okruženje pomoću devet koraka koji su navedeni i opisani u ovom diplomskom radu, kako bi bili sigurni da im je informacijski sustav i informacije u njemu, siguran i u optimalnom stanju za kontinuirani rad i funkcionalnost logističkog poduzeća.

7. LITERATURA

[1] »Hrvatska enciklopedija,« Leksikografski zavod Miroslav Krleža, 2021., dostupno na: https://www.enciklopedija.hr/natuknica.aspx?id=27410. [Pristupljeno 23. kolovoz 2021.]

[2] »Zavod za sigurnost informacijskih sustava«, dostupno na: https://www.zsis.hr/default.aspx?id=346. [Pristupljeno: 23. kolovoz 2021.]

[3] »Zakon o informacijskoj sigurnosti«, dostupno na: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti. [Pristupljeno: 23. kolovoz 2021.]

[4] Kovačević D., *Sigurnosna politika,* Zagreb: Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, 2008.

[5] U.S. Department of Commerce, National Institute of Standards and Technology, *NIST Special Publication 800-39,* 2011.

[6] Bukovac T., *Sigurnost informacijskih sustava,* Zagreb: Filozofski fakultet, Sveučilište u Zagrebu, 2016.

[7] Škorput P., *Računalna sigurnost,* Zagreb: Fakultet prometnih znanosti, Aurorizirana predavanja, 2021.

[8] Alagić D., Branković V., Vagner M., *Pojednostavljenje primjene metode procjene rizika uz regionalizaciju prijetnji informacijskom sustavu,* Varaždin: Fakultet organizacije i informatike u Varaždinu, Sveučilište u Zagrebu, 2011.

[9] Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika Hrvatske narodne, dostupno na: https://www.hnb.hr/-/smjernice-za-upravljanje-informacijskim-sustavom-u-cilju-smanjenja-operativnog-rizika. [Pristupljeno 23. kolovoz 2021.]

[10] Vukelić B., »Sigurnost informacijskih sustava - skripta«, dostupno na: https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf. [Pristupljeno 23. kolovoz 2021.]

[11] Božović T., Oreški S., Premužić V., Takač K., »Procjena rizika«, dostupno na: https://security.foi.hr/wiki/index.php/Procjena_rizika.html. [Pristupljeno 25. kolovoz 2021.]

[12] Šegudović H., *Prednosti i nedostaci metoda za kvalitativnu analizu rizika*, Zagreb: Infigo IS, 2006.

[13] Feringa A., Goguen A., Stoneburner G., *Risk Management Guide for Information Technology Systems*, Gaithersburg: NIST Special Publication 800-30, 2002.

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Upravljanje informacijskom sigurnosti u logističkim sustavima** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 6.9.2021 Nikolina Živković

(potpis)