Crna Gora
Agencija za nadzor osiguranja

Adresa: Moskovska 17A M/C1
81000 Podgorica, Crna Gora
tel: +382 20 513 502
fax: +382 20 513 503
www.ano.me

Na osnovu člana 16 stav 1 tačka 2 Statuta Agencije za nadzor osiguranja („Sl. list CG“ br. 30/13), a u vezi sa članom 46 stav 4 i članom 100 Zakona o osiguranju („Sl. list RCG“, br. 078/06, 019/07, „Sl. list CG“, br. 053/09, 073/10, 040/11, 045/12, 006/13, 055/16), Savjet Agencije za nadzor osiguranja na 308. sjednici od 26. 08. 2020. godine donio je

SMJERNICE ZA UPRAVLJANJE IT RIZICIMA U DRUŠTVIMA ZA OSIGURANJE

I. UVODNE ODREDBE

1. Značenje pojmova

Pojedini izrazi upotrijebljeni u ovim smjernicama imaju sljedeća značenja:

Informacioni sistem društva (u daljem tekstu: IS) je sistem međusobno povezanih organizacionih, tehnoloških i ljudskih elemenata u društvu uključenih u proces sakupljanja, snimanja, čuvanja i obrade podataka, potrebnih za ostvarivanje poslovnih ciljeva.

Informacione tehnologije (u daljem tekstu: IT) čine sastavni dio IS, čija je svrha automatizacija i podrška obrade podataka. IT obuhvata:

- hardverske komponente:
  - lap-topovi, računari, serveri i dodatna periferna oprema kao što su ekrani, tastature i slično,
  - pametni mobilni uređaji i drugi „smart“ uređaji,
  - aktivnu i pasivnu mrežnu i telekomunikacionu opremu, video opremu,
  - sve vrste medija za čuvanje i skladištenje podataka,
  - podržavajuću infrastrukturu, kao što su električna napajanja, UPS-ovi, klima uređaji, kablovi i slično.

- Softverske komponente:
  - operativne sisteme,
  - baze podataka,
  - sistemske servere kao što su serveri elektronske pošte i slično,
  - sistemske aplikacije,
  - poslovne aplikacije,

- razvojne alate.

Korisnik informacionog sistema (u daljem tekstu: korisnik IS) je svako fizičko ili pravno lice, koje u svojstvu zaposlenog u društvu za osiguranje, spoljnog saradnika, klijenta, revizije, ili u bilo kojem drugom svojstvu učestvuje u procesima obrade podataka.

Obrada podataka podrazumijeva sve ručne ili automatizovane aktivnosti vezane za podatke tokom njihovog životnog ciklusa, kao što su:

- prikupljanje,
- unos,
- čuvanje,
- prenos,
- uvid,
- prikaz,
- transformacija ili izmjena,
- kombinovanje ili integrisanje,
- povraćaj,
- arhiviranje,
- analiza,
- zaštita,
- obezbjeđivanje pristupa i stavljanje na raspolaganje,
- blokiranje,
- brisanje ili uništavanje.

Resursi informacionog sistema omogućavaju implementaciju procesa obrade podataka, prilagođenih poslovnim potrebama, i uključuju:

- podatke i informacije,
- poslovne korisnike IS,
- zaposlene u društvu za osiguranje ovlašćene za upravljanje IS i IT,
- spoljne saradnike koji učestvuju u upravljanju IS i IT,
- informacione tehnologije,
- stručna znanja, obuke i vještine,
- ugovore i licence,
- interne akte i drugu dokumentaciju,
- finansijska sredstva.

Rizik informacionog sistema podrazumijeva vjerovatnoću da određena prijetnja iskorištavanjem ranjivosti resursa IS ostvari negativan učinak na poslovanje društva za osiguranje ili na bilo koji drugi način nanese štetu.

Upravljanje rizicima informacionog sistema je kontinuirani proces koji obuhvata:

- identifikaciju resursa IS,

- identifikaciju prijetnji resursima IS,
- identifikaciju ranjivosti resursa IS,
- procjenu rizika IS i potencijalnog štetnog uticaja,
- odabir mjera za postupanje u vezi sa procijenjenim rizicima IS,
- praćenje procijenjenih rizika IS i primijenjenih mjera i procedura za njihovo smanjenje ili otklanjanje,
- unaprjeđenje procesa upravljanja rizicima.

Osjetljivi podaci i informacije su oni podaci odnosno informacije kod kojih bi narušavanje svojstva povjerljivosti, cjelovitosti ili dostupnosti izazvalo negativne posljedice na poslovanje društva za osiguranje.

2. Ciljevi, namjena i opseg smjernica

2.1 Ciljevi

Društvo za osiguranje (u daljem tekstu: Društvo) je u svom poslovanju izloženo različitim operativnim rizicima koji obuhvataju i rizike IS. Cilj Smjernica za upravljanje IT rizicima u društvima za osiguranje (u daljem tekstu: Smjernice) su:

- razvoj svijesti Društva o rizicima IS, sa posebnim naglaskom na rizike vezane za upotrebu IT-a kao i
- upoznavanje Društava sa dobrim praksama koje se koriste za ublažavanje rizika IS.

Razumijevanje i primjena mjera i procedura opisanih u Smjernicama doprinosi kvalitetnijem upravljanju rizicima IS Društava, a samim tim i umanjuje:

- izloženost Društva poslovnim rizicima;
- vjerovatnoću neusklađenosti poslovanja Društava sa važećim propisima.

2.2 Namjena Smjernica

Ove Smjernice su namijenjene Društvima, i to naročito:

- članovima odbora Društva,
- odgovornim licima za upravljanje IT-a u Društvu,
- licima odgovornim za sigurnost IS i IT-a,
- licima odgovornim za upravljanje i komunikaciju sa eksternim partnerima i pružaocima usluga,

- licima odgovornim za upravljanje procesima kontinuiteta poslovanja,
- licima koja obavljaju poslove interne kontrole i revizije.

2.3 Opseg Smjernica

Ove Smjernice obuhvataju:

1) Ključne aspekte upravljanja rizicima IS:
    - osnovna načela upravljanja rizicima IS,
    - identifikovanje, procjenu i postupanje po rizicima IS;

2) Mjere i aktivnosti za smanjenje rizika IS:
    - organizaciju i upravljanje IS,
    - razvoj i održavanje IS,
    - upravljanje promjenama u IS,
    - izdvajanje procesa IS,
    - kontinuitet poslovanja i oporavak nakon katastrofe (BCP i DR),
    - fizičku zaštitu,
    - logičke kontrole pristupa,
    - mrežnu sigurnost,
    - sigurnost prenosivih uređaja i medija za čuvanje podataka,
    - upravljanje incidentima,
    - upravljanje operativnim, sistemskim i drugim zapisima,
    - zaštitu od malicioznih kodova.

II. KLJUČNI ASPEKTI UPRAVLJANJA RIZICIMA IS

1. Osnovna načela upravljanja rizicima IS

Procesi upravljanja rizicima su sastavni dio svakodnevnog poslovanja Društva. Društva prepoznaju rizike koji prijete ostvarivanju poslovnih ciljeva i preduzimaju mjere kako bi se ti rizici sveli na prihvatljiv nivo. Sistemski pristup identifikaciji i primjeni mjera i procedura, kroz proces upravljanja rizicima, može donijeti dodatne prednosti, kao što su:

- kvalitetnija zaštita važnih poslovnih procesa i resursa,
- manja vjerovatnoća da će se rizik zanemariti,
- manja vjerovatnoća nepridržavanja važećih propisa,
- donošenje boljih poslovnih odluka,
- manja mogućnost neefikasnog trošenja novca na zaštitne mjere,
- manje utrošenog vremena na upravljanje zaštitnim mjerama i slično.

U ovim Smjernica opisani su osnovni postupci u procesu sistemske identifikacije, procjene i postupanja po rizicima IS.

Fokus procesa upravljanja rizicima IS je na **informaciji**, kao najvažnijem resursu IS.

Vrsta i namjena informacija zavisi od vrste industrije, tržišta, proizvoda i usluga u ponudi, kao i mnogim drugim faktorima. Primjer informacija sa kojima mogu raspolagati Društva u poslovanju su:

- informacije o ponuđenim proizvodima i uslugama,
- informacije o klijentima,
- informacije o novčanim transakcijama i slično.

Raspoloživost tačne i pravovremene informacije može uticati na donošenje ispravnih poslovnih odluka, ali i na poštovanje važećih propisa. Dostupnost osjetljive informacije neovlašćenim licima može dovesti do gubitka prednosti nad konkurencijom, gubitka povjerenja klijenata, kao i do kršenja važećih propisa.

Sa aspekta informacione sigurnosti, informacije imaju tri ključna svojstva, čije narušavanje predstavlja rizik za poslovanje Društva:

1) **Povjerljivost** je svojstvo informacije da je raspoloživa isključivo licima i sistemima koji za to imaju opravdano ovlašćenje. Posljedice narušavanja povjerljivosti informacija mogu biti npr.:
    - gubitak konkurentske prednosti (na primjer, otkrivanjem informacija o osobinama novog proizvoda konkurenciji),
    - gubitak povjerenja klijenata (na primjer, iznošenjem ličnih podataka klijenata u javnost),
    - kršenje važećih propisa (iznošenje ličnih podataka klijenata može predstavljati kršenje regulative u domenu zaštite ličnih podataka)
    - finansijski gubici (iznošenje ličnih podataka može dovesti do pokretanja tužbi klijenata, te rezultirati novčanim kaznama za navedeno kršenje propisa).

2) **Cjelovitost** je svojstvo informacije da postoji čvrsto uvjerenje u njenu ispravnost i tačnost, odnosno da nije neovlašćeno ili nepredviđeno izmijenjena, slučajnim ili namjernim djelovanjem, što podrazumijeva i naknadno dodavanje, izmjenu ili brisanje informacije bez traga o sprovedenim aktivnostima koji se može slijediti. Posljedice narušavanja cjelovitosti informacija mogu biti npr.:
    - donošenje pogrešnih poslovnih odluka (na primjer, zbog pogrešnih informacija predstavljenih u izvještajima prema odboru direktora),
    - gubitak povjerenja klijenata (zbog pogrešno izračunate premije),
    - nepoštovanje važećih propisa (zbog pogrešnih informacija u izvještajima prema regulatoru).

3) **Dostupnost** je svojstvo informacije da po potrebi i u prihvatljivom roku bude dostupna ovlašćenim licima i sistemima. Posljedice narušavanja dostupnosti informacija mogu biti npr.:
    - nemogućnost isporuke proizvoda i usluga klijentima (na primjer, nedostupnost informacija o ugovornim odnosima sa klijentom),
    - nepoštovanje važećih propisa (zbog nedostupnosti informacija potrebnih za sastavljanje izvještaja koji se moraju sačiniti u određenom roku i dostaviti regulatoru),
    - nemogućnost ispunjavanja ugovornih obaveza (zbog nedostupnosti informacija o transakcijama, računima ili nemogućnosti isplate platnih naloga).

Štetni događaji rizika IS utiču na narušavanje navedenih svojstava informacija, a proizilaze iz djelovanja prijetnji, koje štetne efekte ostvaruju iskorišćavanjem **ranjivosti** resursa IS. Zbog toga je bitno identifikovati prijetnje i ranjivosti resursa IS, a samim tim i procijeniti rizike IS i njihove štetne efekte/uticaje, prema kojima bi se postupalo primjenom pravovremenih i odgovarajućih mjera.

2. Identifikovanje, procjena i postupanje po rizicima IS

Osnovni uslov za identifikovanje i procjenu rizika IS je dobro poznavanje poslovnih ciljeva, poslovne strategije i poslovnih procesa u Društvu, kako bi se mogao procijeniti realni uticaj rizika IS na poslovanje.

Stoga je potrebno identifikovati sve resurse IS koji imaju ulogu u ostvarivanju poslovnih ciljeva i strategije ili služe kao podrška poslovnim procesima, a zatim procijeniti njihovu važnost u tim ulogama. Naročito je važno znati da li postoji međusobna povezanost i zavisnost resursa IS. Na primjer, ukoliko je neka informacija bitna za kritični poslovni proces, bitan će biti i server sa bazom podataka na kojem je ta informacija sačuvana, kako operativni sistem tako i sami server, ali i mrežni uređaji i kablovi koji omogućavaju dostupnost informacije putem personalnih računara krajnjem korisniku.

Rizici IS proizilaze iz djelovanja prijetnji. Prijetnje se obično dijele, u zavisnosti na mjesto nastanka, na unutrašnje i spoljnje.

Neke od unutrašnjih prijetnji mogu biti:

- interna prevara (zloupotreba),
- neovlašćeni pristup informacijama iznutra,
- krađa resursa IS,
- greške prilikom unosa podataka u aplikaciju,
- nesvjesno odavanje povjerljivih informacija.

Neke od spoljnih prijetnji mogu bit:

- hakerski napadi,

- maliciozni kod,
- socijalni inženjering,
- epidemije bolesti,
- elementarne nepogode.

Identifikovane prijetnje potrebno je staviti u kontekst ranjivosti resursa IS, odnosno da li pojedine prijetnje mogu iskoristiti ranjivosti na način da izazovu štetni događaj. Neke od ranjivosti mogu biti:

- nepostojanje ili neadekvatna zaštita od malicioznog koda,
- neadekvatna i neodgovarajuća konfiguracija firewall-a,
- neadekvatno uspostavljen sistem korisničkih naloga i prava („rola“) nad poslovnim aplikacijama,
- nedostatak informatičke pismenosti i nivoa svijesti o sigurnosti IS,
- nepostojanje sistema za neprekidno napajanje ključnih sistema (UPS i slično).

Poznavanjem ranjivosti, prijetnji i njihovih štetnih uticaja na poslovanje mogu se procijeniti rizici IS, kroz dva njihova osnovna svojstva:

- vjerovatnoća da će prijetnja iskoristiti ranjivost resursa IS,
- visinu štetnog događaja ukoliko prijetnja uspješno iskoristi ranjivost.

Primjer prepoznavanja ranjivosti kroz navedena svojstva može izgledati ovako:

- Proces prodaje usluga klijentima zavisi od dostupnosti informacija o klijentima, što uključuje podatke kao što su ime, prezime, adresa, vrsta ugovorene usluge i slično;
- Informacije o klijentima čuvaju se na serveru sa bazom podataka. Nestanak električne energije, koji se može dogoditi i više puta godišnje u trajanju od par sati, uzrokovao bi prestanak rada servera baze podataka, obzirom da nije implementiran sistem ili rješenje za neprekidno ili redudantno napajanje;
- Sve dok server sa bazom podataka ne funkcioniše, Društvo nije u stanju pružiti uslugu klijentima i na taj način potencijalno ostaje bez finansijskih prihoda, a velika je i vjerovatnoća narušavanja reputacije i povjerenja klijenata.

Odluka o načinu postupanja sa rizicima IS u pravilu zavisi od samih rizika, kao i važnosti izloženih procesa i resursa.

Postoji više načina upravljanja rizicima a uopšteno mogu se podijeliti na:

- **Izbjegavanje** – podrazumijeva ublažavanje rizika eliminacijom rizičnog procesa odnosno resursa IS. Na primjer, Društvo je zaključilo da je rizik neprihvatljiv, kao i finansijski troškovi neophodni za investiciju nabavke rješenja za neprekidno napajanje, pa je odlučilo da izbaci iz upotrebe server sa tom bazom podataka i sve informacije o klijentima čuva u papirnom obliku. Na taj način eliminiše se ranjivost koju bi mogla iskoristiti prijetnja prekida snadbijevanja električnom energijom.

- **Smanjenje** – podrazumijeva ublažavanje rizika implementacijom mjera kojima se rizik smanjuje. Na primjer, Društvo je zaključilo da je rizik neprihvatljiv. Analizom troškova nabavke i godišnjeg održavanja sistema za neprekidno napajanje, Društvo je zaključilo da su troškovi manji od potencijalnih izgubljenih prihoda ili gubitaka prouzrokovanih narušavanjem reputacije, pa se odlučuje za implementaciju rješenja, čime se umanjuje identifikovani rizik.
- **Prihvatanje** – podrazumijeva prihvatanje potencijalnih posljedica štetnog događaja navedenog rizika. Na primjer, Društvo je svjesno rizika, ali je došlo do zaključka da su troškovi nabavke i godišnjeg održavanja sistema za neprekidno napajanje veći od potencijalnih izgubljenih prihoda ili gubitaka prouzrokovanih narušavanjem reputacije, pa se odlučuje da se prihvati rizik bez implementacije dodatnih mjera.
- **Prenos** – podrazumijeva prenos posljedica štetnog uticaja rizika na druge fizičke ili pravne osobe. Na primjer, kupovinom polise osiguranja od štetnog događaja ili ugovaranjem naknade koju bi pružalac usluga bio dužan platiti za pojedine štetne događaje u slučaju izdvajanja procesa.

Neki rizici se ne mogu ocijeniti prihvatljivima bez obzira na troškove implementacije kontrolnih mjera – na primjer, kod rizika koji za posljedicu imaju ugrožavanje ljudskih života ili pričinjavanje krivičnih djela.

III. MJERE I PROCEDURE ZA SMANJENJE RIZIKA IS

U ovom poglavlju Smjernica opisane su neke mjere i postupci koji spadaju u dobru praksu smanjivanja rizika IS, a naročito one koje se preporučuju bez obzira na svojstva IS Društva.

O načinu sprovođenja preporuka i odabiru tehničkih rješenja koja bi se pri tome eventualno koristila, odlučuje Društvo, na osnovu sopstvene procjene rizika, vodeći se načelom proporcionalnosti kako bi identifikovalo optimalna rješenja za svoj IS.

1. Organizacija i upravljanje IS

1.1 *Organi upravljanja u Društvu*

Funkcionisanje IS Društva u znatnoj mjeri zavisi od podrške organa upravljanja i rukovođenja Društva. Odbor direktora i izvršni direktor odgovorni su za organizaciju, strateško odlučivanje, raspodjelu resursa i donošenje pravila i procedura u kontekstu upravljanja IS, što obuhvata i procese izdavanja određenih poslova spoljnim partnerima i pružaocima usluga. Ukoliko navedeni organi Društva nijesu na primjeren način uključeni u upravljanje IS, Društvo može biti izloženo rizicima kao što su neusklađenost strategije poslovnog razvoja i razvoja IS, što može dovesti do neracionalnog ili neadekvatnog trošenja sredstava za razvoj i održavanje samog IS.

U svrhu umanjenja rizika IS, preporučljivo je da odbor direktora i izvršni direktor Društva primijene najmanje sljedeće mjere i procedure:

- **Uspostavljanje primjerene organizacione strukture** potrebne za funkcionisanje i sigurnost IS, shodno poslovnim potrebama i ciljevima Društva.
- **Osiguravanje resursa** potrebnih za primjerenu funkcionalnost i sigurnost IS, naročito u kontekstu stručnih kadrova, hardvera, softvera i podržavajuće infrastrukture.
- **Imenovanje lica odgovornog za upravljanje IT procesima i operacijama.**
- **Obezbjeđenje kontinuiranog informisanja i upoznavanja odbora direktora i izvršnog direktora sa relevantnim činjenicama** vezanim za funkcionisanje i sigurnost IS, bilo kroz neformalnu komunikaciju sa licima odgovornim za funkcionisanje i sigurnost IS ili kroz formalni način izvještavanja.
- **Usklađivanje strategije razvoja IS i razvoja poslovne strategije Društva**.

Shodno sopstvenoj procjeni rizika, odbor direktora i izvršni direktor Društva mogu dodatno razmotriti primjenu sljedećih mjera i procedura:

- **Formiranje tima za upravljanje IS.** Uobičajena je praksa da u radu tima za upravljanje IS učestvuju odgovorna lica poslovnih organizacionih jedinica i sistema internih kontrola, uz predstavnike navedenih organa Društva i lica odgovorna za sigurnost i funkcionalnost IS. Takođe, uobičajeno je da se rad tima manifestuje kroz zajedničke sjednice ili kolegijume, na kojima se raspravlja o ključnim pitanjima funkcionalnosti i sigurnosti IS. Na taj način se olakšava komunikacija između učesnika, rješavaju problemi u međusobnoj saradnji, a samim tim unaprjeđuje usklađenost djelovanja organizacionih jedinica zaduženih za obezbjeđenje funkcionalnosti i sigurnosti IS i ostalih organizacionih jedinica.
- **Izdvajanje funkcije upravljanja sigurnošću IS od drugih zaduženja vezanih za IS.** Sigurnosni i funkcionalni ciljevi IS mogu biti u suprotnosti u nekim situacijama, stoga je dosadašnja praksa pokazala da je preporučeno razdvajanje tih funkcija na više različitih lica.
- **Razdvajanje međusobno kompatibilnih dužnosti u procesu upravljanja IT,** kao na primjer, sistemskog administratora od programera aplikacija, programera aplikacija od administratora baze podataka, sistemskog administratora od mrežnog administratora i slično. Dodjelom tih funkcija različitim licima omogućava se njihova veća usredsređenost na dužnosti za koje su specijalizovani, pa se istovremeno ograničava potencijalna šteta

koja bi mogla nastati nemarnim štetnim djelovanjem nekog od zaposlenih navedenih u primjeru.

- **Formiranja sistema internih kontrola IS.** Unutrašnje kontrole, u vidu funkcija interne revizije, procjene rizika ili usklađenosti, a koje su nezavisne od ostalih zaduženja vezanih za funkcionalnost ili sigurnost IS, mogu doprinijeti kvalitetnijem upravljanju rizicima IS.
- **Dokumentovanje i usvajanje politika, procedura, pravila, standarda, smjernica, uputstava i radnih procedura u IS.**

1.2 *Ljudski resursi*

Ljudsko djelovanje, namjerno ili nenamjerno, može izložiti IS značajnim rizicima. Primjeri prijetnji nastalih ljudskim djelovanjem su:

- greške u radu sa aplikacijama,
- nesvjesno ili namjerno odavanje povjerljivih podataka,
- greške u razvoju i održavanju IS,
- neadekvatno rukovanje informatičkom opremom i drugo.

Kako bi se umanjile štetne posljedice prijetnji nastale ljudskim djelovanjem, preporučuje se da Društvo obezbijedi da:

- **Zaposleni imaju primjerena znanja i vještine u vezi sa korišćenjem poslovnih aplikacija;**
- **Zaposleni imaju primjerena znanja i vještine u vezi sa upotrebom ostalih resursa IT** koje koriste pri izvršavanju radnih zadataka, kao što su internet, elektronska pošta i slično;
- **Zaposleni odgovorni za upravljanje, razvoj i održavanje IS imaju primjerena znanja i vještine** za dužnosti koje obavljaju;
- **Zaposleni imaju primjereni nivo svijesti o sigurnosti IS**.

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti primjenu sljedećih mjera i postupaka:

- **Uspostavljanje procesa provjere kandidata prilikom zapošljavanja.** Proces može uključiti provjeru tačnosti navoda o radnom iskustvu i obrazovanju, evidenciju osuđivanosti za krivična djela i slično. Takvim i sličnim provjerama smanjuje se mogućnost zapošljavanja lica koje bi mogla da predstavlja sigurnosni rizik po IS.
- **Uspostavljanje procesa kontinuirane edukacije zaposlenih** u cilju podizanja svijesti o sigurnosti IS, što može uključivati planiranje, sprovođenje edukacije i prikupljanje povratnih informacija od učesnika.

2. Razvoj i održavanje IS

2.1 *Održavanje IT*

Hardver, softver i infrastruktura koja služi kao podrška, zahtijeva kontinuirano održavanje kako bi se obezbijedila njihova adekvatna funkcionalnost. Zapostavljena infrastruktura može biti izložena različitim prijetnjama, kao što su:

- greške u funkcionisanju operativnih sistema i aplikacija,
- kvarovi na računarima i mrežnoj opremi,
- kvarovi na infrastrukturi koja služi kao podrška,
- povećana izloženost hakerskim napadima,
- povećana izloženost djelovanju malicioznog koda i slično.

Kako bi se umanjili štetni uticaji nastali zbog neadekvatnog održavanja IT, preporučuje se da Društvo:

- **Obezbijedi adekvatno održavanje hardvera, softvera i infrastrukture koja služi kao podrška**, u vidu nadogradnji i ispravljanja grešaka u softveru, redovnog servisiranja hardvera i ostale infrastrukture, zamjene zastarjelih i dotrajalih komponenti i slično.
- **Ograniči ovlašćenja za izmjene na hardveru, softveru i drugoj infrastrukturi** isključivo na lica koja imaju odgovarajuća stručna znanja i vještine.
- **Adekvatno vrši nadzor ključnih pokazatelja funkcionalnosti IT**, kao što su na primjer raspoloživost prostora za čuvanje podataka na diskovima i ostalim medijima, sistemskih resursa, servera, personalnih računara i slično.

2.2 *Razvoj aplikacija*

Primjerena funkionalnost i sigurnost poslovnih aplikacija veoma je bitna za funkcionalnost i sigurnost IS u cjelini. Stoga je posebno važno posvetiti pažnju razvoju poslovnih, ali i ostalih aplikacija kroz cijeli razvojni ciklus. Propusti u razvoju mogu prouzrokovati izloženost različitim prijetnjama kao što su:

- neusklađenost značajnih aplikacija sa potrebama poslovnih procesa,
- nekompatibilnost aplikacija sa ostalim komponentama IT,
- neovlašćeni pristup osjetljivim podacima,
- greške u funkcionisanju rada aplikacija,
- povećana izloženost hakerskim napadima,
- povećana izloženost djelovanju malicioznog koda i drugo.

Kako bi se umanjilo štetno djelovanje prijetnji nastalih zbog neprimjerenog pristupa razvoju aplikacija, preporučuje se da Društvo:

- **Uključi krajnje korisnike aplikacija u proces izrade specifikacija aplikacije,** kako bi se unaprijed definisale funkcije poput korisničkog interfejsa, ulaznih i izlaznih podataka i slično.

- **Planira sigurnosne kontrole u fazi razvoja**, kao što su identifikacija korisnika i autorizacija pristupa resursima aplikacija, kriptografski mehanizmi, kontrola unosa podataka, kontrola izlaznih podataka i slično.
- **Zaštiti izvorni kod aplikacija od neovlašćenog pristupa.**
- **Testira funkcionalnost i sigurnost novih izmijenjenih aplikacija**, prije njihovog uključenja u normalnu produkciju. Bilo bi poželjno, osim testiranja sistemskih i integrisanih funkcionalnosti, u proces testiranja uključiti i krajnje korisnike i dobiti od njih povratne informacije o prihvatljivosti izvršenih izmjena.

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti primjenu i sljedećih mjera i procedura:

- **Razdvajanje razvojnog i testnog okruženja aplikacija od produkcijskog**, na primjer korišćenjem odvojenih baza podataka ili čak i potpuno odvojenih personalnih i serverskih računara za različita okruženja. Na taj način se znatno umanjuje rizik narušavanja cjelovitosti produkcijskih podataka tokom razvoja ili testiranja.
- **Izbjegavanje korišćenja produkcijskih podataka za potrebe razvoja ili testiranja**. Ukoliko se za potrebe razvoja ili testiranja koriste produkcijski podaci, povećava se rizik pristupa tim podacima od strane neovlašćenih osoba. Stoga nije preporučljivo takve podatke koristiti prilikom razvoja ili testiranja, osim ukoliko se prethodno ne uklone osjetljivi podaci poput ličnih podataka.

Ukoliko se razvoj aplikacija vrši od strane spoljnog partnera ili dobavljača usluga, primjena gore opisanih mjera i procedura može biti znatno otežana. U tom slučaju preporučljivo je da Društvo od samog dobavljača ili pružaoca usluga zatraži informacije o bitnim sigurnosnim aspektima i funkcionalnostima aplikacije kako bi sami procijenili njegovu primjenjivost.

3. Upravljanje promjenama u IS

Promjene u IS neizbježan su dio procesa razvoja i održavanja IS. Međutim, nekontrolisane promjene ujedno mogu proizvesti i negativne efekte, kroz:

- sprovođenje promjena koje mogu narušiti funkcionalnost komponenti IT,
- sprovođenje promjena koje IS mogu izložiti sigurnosnim prijetnjama,
- problemi u radu korisnika koji nisu blagovremeno upoznati sa promjenama, na primjer uvođenje novih funkcionalnosti u aplikacijama i slično.

Kako bi se umanjili štetni uticaji prijetnji nastalih zbog nekontrolisanih promjena, preporučuje se da Društvo obezbijedi da su:

- **Odgovorna lica za upravljanje IT upoznata sa planiranim promjenama i potencijalnim rizicima tih promjena** prije samog izvršenja.

- **Planirane promjene odobrene od strane odgovornog elica za upravljanje IT** prije samog izvršenja.
- **Promjene adekvatno testirane** prije njihove primjene i puštanja u produkciju.
- **Korisnici IS upoznati sa promjenama** ukoliko one utiču na obavljanje svakodnevnih radnih zadataka, na primjer kada se radi o izmjenama funkcionalnosti u poslovnim aplikacijama.

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti primjenu sljedećih mjera i procedura:

- **Vađenje evidencije o promjenama u IS**, što može uključivati i opis svake promjene, ime predlagača, ime lica koje je promjenu odobrilo, procjenu rizika, status odobrenja, status testiranja i status izvršenja. Takva evidencija može se koristiti u svrhu revizije i kontrole, ali i kao baza znanja koja može doprinijeti unapređenju upravljanja promjenama u budućnosti.

4. Izdvajanje procesa u IS

4.1 Izdvajanje ili prenos procesa u IS

Izdvajanje ili prenos procesa ili poslova IS Društva podrazumijeva uključivanje drugog pravnog ili fizičkog lica u obavljanje poslova vezanih za IS kao što su:

- održavanje komponenti i IT infrastrukture,
- razvoj posebno dizajniranih aplikacija, na primjer aplikacija za centralnu podršku poslovnim procesima po narudžbi Društva, izrada internet stranica i slično,
- bilo kakav vid obrade podataka, na primjer administracija naloga, što uključuje kreiranje, izmjene, brisanje korisničkih naloga i prava u operativnim sistemima i mrežnim uređajima, bazama podataka i aplikacija, zatim čuvanje i skladištenje podataka, izrada rezervnih kopija (backup) i slično,
- pružanje usluga korišćenja tehničke i bezbjednosne infrastrukture, iznajmljivanje ili zakup servera u data centrima, zakup prostora (hosting) na serverima kod pružaoca usluga za web servere i slično,
- pružanje konsultantskih usluga poput savjetovanja u vezi sigurnosti IS, vođenja projekta i slično,
- pružanje usluga internih kontrola poput interne revizije IS.

Na primjer, nabavka odnosno kupovina gotovog, već tržišno dostupnog softvera za koji proizvođač izdaje zakrpe i nadogradnje koje Društvo samo primjenjuje u svom sistemu ne smatra se izdvajanjem procesa. Međutim, u slučaju da proizvođač nameće ili vrši ispravke i nadogradnje

u sistemu Društva, što se smatra održavanjem sistema, odnosno ako proizvođač vrši administraciju u vidu upravljanja korisničkim pravima i nalozima umjesto Društva, što se smatra obradom podataka, radi se o izdvajanju procesa.

Naročito je važno naglasiti da izdvajanjem procesa Društva ne mogu ujedno prebaciti i odgovornost za izvršavanje procesa i posljedice nastale prilikom izdvajanja na pružaoca usluge.

S obzirom na zavisnost poslovanja Društva od izdvojenog procesa, može se procijeniti značaj izdvajanja. Na primjer, ukoliko se izdvaja proces funkcionisanja centralnih ili glavnih poslovnih procesa, ili ukoliko se izdvaja proces koji uključuje obradu osjetljivih podataka poput finansijskih ili ličnih, radi se o značajnom izdvajanju odnosno prenosu posla.

Zavisno od značaja izdvajanja, Društvo se može izložiti različitim rizicima, od manjih neugodnosti do znatnih finansijskih gubitaka, narušavanja povjerljivosti, cjelovitosti i dostupnosti osjetljivih podataka, kao i do potencijalnog prekida glavnih poslovnih procesa, izazvanih djelovanjem prijetnji, kao što su:

- nemogućnost eksternog partnera (pružaoca usluga) da obezbijedi dogovoreni nivo usluga,
- potpuni prekid pružanja usluge, usljed stečaja pružaoca usluga, više sile i slično,
- krađu i oštećenje resursa IS od strane pružaoca usluga,
- odavanje povjerljivih podataka od strane pružaoca usluga,
- nemogućnost izvršavanja ugovornih obaveza Društva prema pružaocu.

Kako bi se umanjile štete nastale zbog rizika vezanih za eksterne partnere ili pružaoce usluga, preporučuje se da Društvo:

- **Procijeni rizik izdvajanja procesa.** Potrebno je dokumentovati i izvršiti analizu u cilju dobijanja odgovora na sljedeća pitanja:
    - Na koje poslovne procese i resurse i na koji način na njih utiče izdvajanje procesa?
    - Kako bi prekid pružanja usluga uticao na poslovanje?
    - Kojim rizicima proizašlim usljed izdvajanja bi Društvo bilo izloženo?
    - Na koji način bi Društvo moglo da nadzire i kontroliše kvalitet pružanja usluga i potencijalne rizike?
    - Na koji način se može obezbijediti kontinuitet poslovanja u slučaju prekida pružanja usluge ili neadekvatnog pružanja usluge?
- **Procijeni sposobnost pružaoca usluga.** Potrebno je dokumentovati i izvršiti analizu u cilju dobijanja odgovora na sljedeća pitanja:
    - Da li pružalac usluga ima perspektivu stabilnog poslovanja za vrijeme pružanja usluga?
    - Da li pružalac usluga posjeduje reference, iskustvo, znanje, stručnost, kadrovske i druge resurse i dokaze o istim za adekvatno i kvalitetno pružanje usluga?
    - Da li pružalac usluga obavlja djelatnost u skladu sa važećim zakonima i propisima?

- **Definiše i zaključi ugovor prilagođen potrebama usluge koja se pruža.** Ugovor bi trebalo da sadrži najmanje sljedeće:
    - detaljan opis procesa ili posla koji se izdvaja, odnosno predmet ugovora,
    - obaveze čuvanja povjerljivih podataka,
    - prihvatljiv nivo pružanja usluge (SLA),
    - precizno navedene obaveze i odgovornosti obje strane,
    - finansijski dio ili element ugovora,
    - uslove u slučaju jednostranog raskida ugovora,
    - trajanje ugovora,
    - način rješavanja sporova,
    - izlaznu strategiju.
- **Obezbijedi adekvatan nadzor nad pružaocem usluga.**
- **Obezbijedi pravovremeni pristup informacijama** u vezi pružaoca usluge i same usluge, a koje su relevantne za pružanje usluge.
- **Planira kontinuitet poslovanja** u slučaju prekida ili neadekvatnog pružanja usluge.

4.2 Korišćenje „Cloud" servisa ili usluga u izdvojenim procesima

Claud servisi ili usluge postepeno dobijaju na značaju, a širi se i interesovanje firmi u različitim industrijskim granama za ovakvom vrstom usluga. Prednosti korišćenja Cloud usluga mogu se manifestovati u vidu ušteda kod nabavke informatičke opreme, zapošljavanja stučnih kadrova, troškova održavanja, jednostavnijeg načina rješavanja pitanja plana kontinuiteta poslovanja i oporavka nakon katastrofe i slično.

Cloud u kontekstu izdvajanja procesa, predstavlja obradu podataka korišćenjem računarske infrastrukture pružaoca usluga, dijeljenje sa drugim pravnim ili fizičkim licima kao ravnopravnim korisnicima i smještanje izvan poslovnih prostorija i lokacija Društva, a na kojima se Društvo povezuje koristeći računarske mreže ili druge metode udaljenog pristupa i povezivanja u cilju pristupa i dobijanja svojih podataka.

Upravo iz tih razloga korišćenje Cloud usluga i servisa inherentno nosi sa sobom i neke specifične rizike:

- Kako se **podaci Društva obrađuju izvan njegovih poslovnih prostorija**, postavlja se pitanje koji su tokovi kretanja podataka i ko sve ima pristup istim. Takođe, kako se u većini slučajeva infrastruktura dijeli sa drugim pravnim i fizičkim licima kao korisnicima ravnopravnim Društvu, postavlja se pitanje na koji način je obezbijeđeno kvalitetno razdvajanje i ograničavanje pristupa podacima pojedinih korisnika. Ukoliko navedena pitanja nisu kvalitetno riješena, Društvo se može izložiti povećanom riziku narušavanja povjerljivosti i cjelovitosti svojih podataka od strane neovlašćenih korisnika, a ujedno i mogućem kršenju važećih propisa u kontekstu zaštite ličnih podataka.

- Društvo nema direktnu **kontrolu nad procesima održavanja opreme, infrastrukturom koja služi kao podrška, kontroli fizičkog pristupa i kontroli zaštite životne sredine.** Ukoliko navedene mjere nisu precizno uspostavljene, Društva se izlažu rizicima gubitka povjerljivosti, cjelovitosti i dostupnosti podataka, na primjer usled neovlašćenog pristupa ili elementarnih nepogoda.
- Društva najčešće imaju **ograničenu kontrolu nad kanalima komunikacije preko** kojih pristupaju svojim podacima. Ukoliko ti kanali nisu pouzdani i primjereno zaštičeni, Društva se izlažu rizicima gubitka povjerljivosti, cjelovitosti i dostupnosti podataka, što se može desiti usled prekida veze ili kanala, kao i presretanja komunikacije od strane neovlašćenih osoba.

Kako bi se navedeni rizici umanjili, preporučuje se da se primjenjuju sve mjere i procedure opisane u poglavlju 4.1 Smjernica, ali naročitu pažnju treba obratiti i na sljedeće:

- **Steći uvjerenje da će pružalac usluga izvršavati obaveze u skladu sa zakonom i drugim važećim propisima**, posebno u kontekstu obaveza Društva vezanih za zaštitu podataka, na primjer putem nezavisnih revizorskih izvještaja, direktnim uvidom ili verifikacijom sertifikata i potvrda koje pružalac usluga posjeduje.
- **Steći uvjerenje u adekvatnost tehnološke i podržavajuće infrastrukture, bezbjednosnih i ekoloških kontrola** za šta Društvo takođe može koristiti izvještaje nezavisnog revizora, izvršiti direktan uvid u sertifikate i potvrde koje pružalac posjeduje.

4.3 Izdvajanje ili prenos procesa unutar iste grupe

Česta je poslovna praksa da se izdvajanje procesa ili posla vrši prema pravnim licima koja su dio iste grupe kao i Društvo. S obzirom da se i dalje radi o drugom pravnom subjektu, sprovode se sve mjere i procedure opisane u poglavlju 4.1 Smjernica.

Činjenica da se radi o Društvima povezanim unutar iste grupe može se uzeti u obzir prilikom procjene rizika izdvajanja i analize adekvatnosti pružaoca usluga.

5. Kontinuitet poslovanja i oporavak nakon katastrofe

5.1 *Planiranje kontinuiteta poslovanja*

Vjerovatnoća da će se prijetnje, uprkos adekvatnim zaštitama, mjerama i procedurama, dogoditi i pri tome otežati ili onemogućiti normalno poslovanje uvijek postoji. Zato je potrebno da se takve situacije predvide i isplaniraju kako bi se u tom slučaju nastavilo poslovanje.

Kako bi se umanjili rizici nemogućnosti nastavka poslovanja usljed djelovanja štetnih događaja, preporučuje se da Društvo:

- **Identifikuje ključne poslovne procese i resurse potrebne za njihovo izvršavanje**, što uključuje IT, kadrove, kancelarijsku opremu, ugovore, licence i drugo.
- **Analizira uticaj prekida poslovnih procesa na poslovanje u cjelini** obzirom na različite dužine vremena u kojima su procesi u prekidu, pa na taj način odredi najveće prihvatljive dužine vremena za određeni prekinuti proces.
- **Usvoji i dokumentuje planove kontinuiteta poslovanja u slučaju prekida poslovnih procesa**, zavisno od scenarija, na primjer kroz alternativne načine implementacije procesa, backup podataka sa rezervnih kopija, oporavak kroz aktiviranje rezervne lokacije (DR) i slično.

  Planovi bi trebalo da obuhvataju sve kritične poslovne procese i da sadrže najmanje:
  - odgovornosti i uloge u sprovođenju,
  - kriterijume koji utiču na izvršenje plana, na primjer pojava štetnog scenarija ili prekid kritičnog procesa,
  - mjere i procedure kojima će se osigurati nastavak poslovanja.
- **Obezbijedi da su svi planovi razumljivi i stalno dostupni licima odgovornim za njihovo sprovođenje**. Pri tome je preporučljivo imati i u planu mogućnost pojave štetnih scenarija koji bi mogli ugroziti dostupnost samih planova.
- **Periodično testira efikasnost planova**, kao na primjer kroz testiranje rezervne kopije backupa podataka, „Table Top“ testove i slično.
- **Planove koriguje shodno rezultatima testova i periodično ih prilagođava poslovnim potrebama i ciljevima.**

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti i primjenu sljedećih mjera i procedura:

- **Postavljanje rezervnog data centra** na udaljenoj lokaciji koji svojim kapacitetima može obezbijediti nastavak poslovanja u slučaju nedostupnosti primarnog.
- **Postavljanje alternativne lokacije za oporavak poslovnih procesa (DR)** u slučaju neupotrebljivosti primarne poslovne lokacije.

5.2 *Čuvanje rezervne kopije podataka*

Rezervna kopija podataka omogućava nastavak poslovanja u slučaju gubitka ili narušavanja cjelovitosti poslovnih podataka. Kako bi se ti rizici umanjili preporučeno je da Društvo:

- **Identifikuje ili klasifikuje podatke** koji će biti predmet izrade rezervne kopije, što obično podrazumijeva podatke koji su ocijenjeni kao bitni za poslovanje.
- **Odredi učestalost izrade rezervnih kopija pojedinačnih podataka**. Na primjer, kopije veoma bitnog skupa podataka, podložnog čestim promjenama tokom dana koji se često nalaze u bazama podataka, mogle bi se izrađivati i više puta dnevno, dok kopije manje bitnih, statičkih skupova podataka jednom nedeljno ili mjesečno.
- **Obezbijedi izradu rezervnih kopija podataka** shodno planovima učestalosti.

- **Zaštiti povjerljivost i cjelovitost rezervnih kopija podataka** shodno njihovom značaju. Po pravilu, za rezervne kopije podataka bi trebalo obezbijediti barem jednak nivo zaštite kao i originalnim podacima iz produkcijskih sistema.
- **Periodično testirati mogućnost upotrebe i ispravnosti podataka iz rezervnih kopija.**
- **Dokumentovati aktivnosti izrade i testiranja ispravnosti** rezervnih kopija i njihovog sadržaja putem automatski generisanih zapisa ili ručno.
- **Periodično odlagati rezervne kopije sa podacima na udaljenu lokaciju.** Odgovarajuću udaljenost lokacije bi Društvo trebalo samo odrediti na osnovu sopstvene procjene rizika, ali je ipak preporučeno da se barem radi o izdvojenoj poslovnoj zgradi.

6. Fizička i ekološka sigurnost

6.1 Fizička sigurnost

Fizička sigurnost podrazumijeva primjenu mjera i procedura kako bi se kontrolisao fizički pristup resursima IS. Neuspostavljanjem adekvatnih mjera i procedura fizičke sigurnosti, Društvo se može izložiti rizicima krađe i oštećenja informatičke opreme i time dodatno povećati rizik od neovlašćenog pristupa osjetljivim podacima koji se nalaze na informatičkoj opremi.

Kako bi se umanjili rizici koji proizilaze iz neadekvatno postavljenih kontrola fizičke sigurnosti, preporučuje se da Društvo:

- **Smjesti značajnu informatičku opremu u posebne prostorije**, što na primjer uključuje opremu poput servera, backup uređaja i medija, konfiguracionih terminala, aktivne i pasivne mrežne opreme i slično.
- **Ograniči pravo pristupa prostorijama koje su izdvojene sa bitnom informatičkom opremom** da jedino zaposleni u Društvu koji imaju opravdanu potrebu i pravo za to imaju pristup, na primjer stručno osoblje koje održava tu opremu.
- **Obezbijedi da su osobe koje nemaju pravo pristupa izdvojenim prostorijama sa važnom informatičkom opremom, u slučaju da ipak pristupaju prostorijama, budu pod stalnim nadzorom ovlašćenih osoba.** To se prije svega odnosi na spoljne saradnike i pružaoce usluga koji pristupaju prostorijama zbog održavanja informatičke opreme.
- **Obezbijediti kontrolu pristupa svim važnim uređajima na kojima se vrši čuvanje podataka a koji su bez nadzora**, na primjer, zaključavanjem papirne dokumentacije, CD, DVD, USB, pametnih kartica, drugih eksternih medija i slično, u ormar ili sigurnosni sef.

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti primjenu dodatnih mjera i procedura:

- **Uvođenje evidencije osoba koje pristupaju izdvojenim prostorijama sa važnom informatičkom opremom**, ručnim ili automatizovanim putem.

- **Primjena dodatnih mjera za kontrolu pristupa prostorijama,** kao što su video nadzor, protivprovalna vrata, alarm i slično.

6.2 Ekološka sigurnost

Ekološka sigurnost podrazumijeva primjenu mjera i procedura u cilju zaštite resursa IS od djelovanja prirodnih nepogoda poput vatre, poplave, pojave vlage i slično. Djelovanje prirodnih pojava može biti pogubno po resurse IS i učiniti ih trajno nedostupnima ili neupotrebljivima.

Kako bi se umanjili rizici koji mogu nastati usljed djelovanja prirodnih nepogoda ili pojava, preporučuje se da Društvo:

- **Ograniči izloženost bitne IT opreme prirodnim pojavama.** Pri tome je poželjno:
    - obezbijediti adekvatnu sigurnost prostorije u kojoj je oprema smještena, u smislu da u njoj nisu prisutne sanitarije, da nije izložena spoljnim uticajima poput kiše, vjetra, i sunca, kao i da nije izložena poplavama, na primjer zbog podrumskog položaja ili prisustva vodovodnih cijevi u zidovima.
    - ne skladištiti zapaljivi materijal čije prisustvo nije potrebno za rad ili funkcionisanje opreme u prostoriji, poput raznih papirnih dokumenata i slično.
- **Obezbijedi adekvatnu zaštitu od požara poslovnih prostorija i prostorija sa bitnom IT opremom**, u vidu sistema za detektovanje i gašenje požara na elektro opremi, instalacijama itd. Pri tome naročito je važno da su protivpožarni sistemi redovno održavani i atestirani.
- **Osigura temperaturu prostorije u kojoj se nalazi bitna IT oprema koja je od značaja za funkcionisanje te opreme**, na primjer klima uređaji.

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno obezbijediti i razmotriti dodatno opremanje prostorija poput ugradnje senzora vlage i temperature, sistema za detekciju poplava, ugradnja statičkog poda, protivpožarnih vrata i drugo.

7. Logičke kontrole pristupa

7.1 Logičke kontrole pristupa

Logičke kontrole pristupa pripadaju skupu sigurnosnih mjera implementiranih na softverskom nivou IT opreme, poput operativnih sistema računara i mrežne opreme, baza podataka i aplikacija. Na primjer, mehanizam potvrde identiteta korisnika i autorizacije korisnika u poslovnim aplikacijama spada u mjere logičke sigurnosti. Neadekvatne logičke kontrole pristupa mogu izložiti Društvo različitim prijetnjama putem kojih je moguće ostvariti neovlašćeni pristup IS i time ugroziti sigurnost podataka tipa:

- hakerskih napada,

- malicioznog koda,
- zlonamjernog ili nemarnog djelovanja zaposlenih i drugo.

Kako bi se umanjio rizik koji proizilazi iz neadekvatno uspostavljenih logičkih kontrola pristupa, preporučeno je da Društvo:

- **Obezbijedi postojanje adekvatnih logičkih kontrola pristupa** na operativnim sistemima računara i mrežne opreme, sistemskih, poslovnih aplikacija i servisa, kao i drugim softverskim resursima IS putem kojih je moguće pristupiti osjetljivim podacima i obezbijediti pristup samo ovlašćenim osobama ujedno i resursima za koje te osobe imaju odgovarajuća ovlašćenja pristupa.
- **Obezbijedi logičke kontrole pristupa IT opremi koja je trajno ili privremeno bez nadzora**, na primjer, nametanjem obaveze zaključavanja korisničkog interfejsa ili operativnog sistema na računaru prije napuštanja radnog mjesta od strane korisnika.

7.2 Korisnički nalozi i prava pristupa

Dodjela, izmjena i ukidanje korisničkih naloga i prava pristupa integrisani je dio većine sistema za logičku kontrolu pristupa. Kreiranjem naloga korisniku se omogućava pristup jednom sistemu, na primjer operativnom sistemu računara u sklopu domena ili poslovnoj aplikaciji, dok se dodjelom prava pristupa ovlašćenim korisnicima daje mogućnost pristupa pojedinim resursima unutar toga sistema, recimo određenoj vrsti podataka u sklopu te aplikacije. Neadekvatno upravljanje korisničkim nalozima i pravima pristupa može znatno ugroziti efikasnost mjera logičke kontrole pristupa. Zato je preporučljivo:

- **Dodjelu, izmjenu i ukidanje korisničkih naloga i prava pristupa obavljati na osnovu dokumentovane poslovne potrebe.** Zahtjev za dodjelu, izmjenu ili ukidanje bi trebao biti upućen od strane odgovorne osobe određene organizacione jedinice kojoj korisnik pripada, prema osobama odgovornim za odobravanje i administraciju korisničkih naloga i prava pristupa. Zahtjev bi trebao da bude dokumentovan, na primjer upućen putem elektronske pošte ili za to predviđenog obrasca ukoliko postoji, pa bi samim tim trebalo da sadrži sve bitne informacije za proces dodjele, izmjene ili ukidanja.
- **Dodjelu korisničkih naloga i prava pristupa sprovoditi na način da se daju minimalna potrebna prava za obavljanje posla i radnih zadataka.** Praksa je pokazala da nije dobro dodjeljivati prava pristupa određenim aplikacijama, podacima ili funkcijama ukoliko korisnik svakodnevno ne obavlja posao u vezi sa istim. Ukoliko su prava ipak dodijeljena u svrhu potrebe testiranja ili slično, potrebno je odmah nakon testa ukloniti ta prava.
- **Definisati obavezu periodične usklađenosti dodijeljenih korisničkih naloga i prava pristupa sa stvarnim stanjem i poslovnim potrebama.**
- **Svakom korisniku IS uvijek dodijeliti poseban korisnički nalog** i u najvećoj mogućoj mjeri izbjegavati korišćenje grupnih korisničkih naloga. Nazivi korisničkih naloga u sistemima bi trebalo da se u svakom trenutku mogu naći i lako identifikovati sa stvarnim identitetom korisnika.

7.3 Korisnički nalozi sa privilegovanim pravima pristupa

Korisnički nalozi sa privilegovanim pravima pristupa su oni nalozi čija prava pristupa omogućavaju izmjenu sistemskih podešavanja IT. Prava privilegovanog pristupa bi trebali imati samo oni korisnici čiji radni zadaci odnosno opis posla to opravdava, na primjer stručno osoblje koje održava IT. Zloupotrebom naloga sa ovakvim pravima povećava se rizik od neovlašćenog pristupa i izmjene konfiguracija sistema, na primjer kroz djelovanje malicioznog koda ili zlonamjernih lica. Kako bi se umanjili rizici koji proizilaze iz upotrebe privilegovanih prava pristupa, preporučljivo je sprovoditi mjere i procedure opisane u poglavlju 7.2 Smjernica i za korisničke naloge sa privilegovanim pravima.

7.4 Upravljanje lozinkama

Lozinke u IS predstavljaju mehanizam potvrde korisničkog identiteta i sastavni su dio sistema logičkih kontrola pristupa. Lozinka se najčešće pojavljuje u obliku alfanumeričkog izraza ili identifikacionog broja kojeg korisnik mora unijeti prilikom prijave u sistem kako bi potvrdio svoj identitet. Neadekvatno upravljanje lozinkama može znatno umanjiti nivo sigurnosti i efikasnosti mjera logičke kontrole pristupa. Stoga se preporučuje da Društvo:

- **Identifikuje i primjenjuje minimalne standarde svojstva lozinki za pristup pojedinim resursima IS** shodno sopstvenoj procjeni rizika odnosno važnosti resursa kojima se pristupa. Neka od svojstava lozinki mogu biti:
    - dužina,
    - rok trajanja,
    - složenost odnosno kompleksnost,
    - dopušteni broj unosa lozinke prije zaključavanja naloga, i drugo.
- **Čuva tajnost lozinke**. Lozinku bi trebalo da zna isključivo lice koje njom potvrđuje identitet.
- **Uredi da se lozinke pamte, nikako da se zapisuju na papir ili u elektronskim formatima odnosno datotekama bez zaštite**.
- **Uvijek mijenja „default“ lozinke na resursima IS, odnosno lozinke koje su inicijalno postavljene od strane administratora ili proizvođača.**
- **Obezbijedi da su lozinke u sistemima sačuvane u kriptovanom obliku, odnosno formatu koji se ne može lako očitati.** Kada korisnik ukuca lozinku prilikom prijave u sistem, mehanizam potvrde identiteta vrši upoređivanje unijete lozinke sa onom koja je konfigurisana u sistemu. Takva lozinka bi trebala da bude sačuvana u kriptovanom obliku, kao digitalni potpis i slično.

- **Pri definisanju lozinki izbjegava korišćenje riječi iz naziva naloga, datuma, ličnih podataka ili druge fraze koje se lako mogu pogoditi ili povezati sa korisničkim nalogom.**

8. Mrežna sigurnost

8.1 Mrežna sigurnost

Računarske mreže služe za međusobno povezivanje računara i drugih uređaja i predstavljaju kanal komunikacije za razmjenu podataka elektronskim putem. Računarske mreže koje služe za povezivanje računara i uređaja Društva, a ujedno im je pristup spolja ograničen, zovu se privatne ili lokalne računarske mreže. U većini slučajeva u lokalnim mrežama se vrši najveći dio saobraćaja odnosno prenosa osjetljivih poslovnih podataka, pa je njima potrebno posvetiti najveću pažnju u kontekstu zaštite i sigurnosti. Neadekvatno zaštićena mreža izložena je raznim rizicima od neovlašćenog pristupa i zloupotrebe što može dovesti do narušavanja povjerljivosti, cjelovitosti i dostupnosti važnih poslovnih informmacija.

Kako bi se umanjili rizici koji proizilaze iz neadekvatne zaštite računarskih mreža preporučuje se da Društvo:

- **Ograniči pristup konfiguracionom interfejsu mrežnih uređaja**, poput mrežnih svičeva i rutera, na isključivo za to ovlašćena lica,
- **Adekvatno zaštiti personalne računare i servere u Društvu kojima je omogućen pristup putem javnih mreža**, na primjer, zaštititi web server primjenom firewalla, sistema za detekciju neovlašćenog pristupa i drugih naprednijih sigurnosnih uređaja,
- **Računare i servere kojima je omogućen pristup putem javnih mreža izdvojiti u poseban mrežni segment odvojen od lokalne računarske mreže (**npr. web servere). Serveri toga tipa su izloženi napadima od strane hakera, ili malicioznih kodova putem javnih mreža. U slučaju da dođe do kompromitacije servera u takvim scenarijima, njegovo izdvajanje u poseban mrežni segment otežalo bi dalji pokušaj probijanja unutar lokalne mreže.
- **Adekvatno zaštiti prenos osjetljivih podataka putem javnih mreža,** na primjer upotrebom kriptografske zaštite SSL/TLS protokola.
- **Koristi naprednu zaštitu bežičnih mreža**, poput WPA2 protokola.

8.2 Udaljeni pristup

Udaljeni pristup podrazumijeva pristup lokalnoj mreži i korišćenje IS Društva, računara, servera i slično, sa udaljene lokacije odnosno lokacije izvan njegovih poslovnih prostorija. Za dodjelu prava udaljenog pristupa treba primjenjivati iste preporuke kao što je opisano u poglavlju 7.2 Smjernica. Takođe, u svrhu zaštite mreže pri udaljenom pristupu preporučuje se da Društvo:

- **Adekvatno zaštiti podatke prilikom prenosa između udaljene lokacije i tačke pristupa računarskoj mreži Društva**, na primjer upotrebom protokola SSL ili IPSEC.

- **Obezbijedi postojanje operativnih i sistemskih zapisa (logova) o aktivnostima korisnika udaljenog pristupa.**

9. Sigurnost prenosivih uređaja i medija za čuvanje i prenos podataka

9.1 Sigurnost prenosivih uređaja i medija za čuvanje i prenos podataka

Prenosivi uređaji i mediji za čuvanje i prenos podataka, poput prenosivih računara, „pametnih telefona“ i CD/DVD/USB medija za čuvanje podataka inherentno su izloženi povećanim rizicima od krađe i gubitka zbog svoje prenosivosti, a time i neovlašćenom pristupu osjetljivim podacima ukoliko su isti na njima snimljeni.

- Kako bi se umanjili rizici koji proizilaze iz gubitka ili krađe opreme preporučuje se da Društvo:**Koristi kriptografske tehnike na prenosivim medijima gdje se čuvaju povjerljivi podaci.**
- **Zaštiti pristup interfejsu operativnih sistema prenosivih računara i pametnih telefona metodama potvrde identiteta korisnika**.
- **Omogući udaljeno brisanje podataka snimljenih na pametnim telefonima ili uređajima i medijima koji imaju mogućnost za to** u slučaju njihovog gubitka ili krađe.

9.2 Rashodovanje prenosivih uređaja i medija za čuvanje i prenos podataka

Prilikom rashodovanja prenosivih medija na kojima se čuvaju podaci kao što su hard diskovi u sklopu računara, USB mediji ili magnetne trake, potrebno je voditi računa o podacima koji se na njima nalaze. Prije promjene vlasnika opreme ili odlaganja na otpad potrebno je obezbijediti da su podaci obrisani na siguran način, na primjer upisivanjem novih podataka preko starih ili fizičkim uništavanjem diska i medija, kako bi se obezbijedilo da je neovlašćeni pristup povjerljivim podacima onemogućen.

10. Upravljanje incidentima

Incidenti u kontekstu IS mogu se definisati kao nepredviđeni događaji i situacije koje mogu narušiti funkcionalnost i sigurnost IS. Adekvatna procedura upravljanja incidentima omogućava pravovremenu prijavu, rješavanje i analizu incidenta u svrhu buduće prevencije, kako bi se minimizovao uticaj incidenta na IS.

U cilju adekvatnog upravljanja incidentima, preporučuje se da Društvo:

- **Obezbijediti korisnicima IS pravovremenu prijavu incidenta.**
- **Odredi obaveze i odgovornosti u prijemu i daljem toku rješavanja incidenta.**
- **Rješava uočene incidente i primjenjuje mjere prevencije pojave incidenata u budućnosti.**

Shodno sopstvenoj procjeni rizika, Društva mogu dodatno razmotriti i primjenu nekih od sljedećih mjera:

- **Vođenje evidencije o prijavljenim incidentima**, koja bi sadržala ime osobe koja je prijavila incident, opis incidenta, ime osobe koja je preuzela rješavanje incidenta, način i status rješavanja i slično.
- **Formiranje službe za upravljanje incidentima,** koja bi bila odgovorna za primarni kontakt kod prijave incidenta, evidenciju i analizu, kao i pružanje podrške korisnicima i inicijalno reagovanje na događaj.

11. Upravljanje operativnim i sistemskim zapisima

Operativni i sistemski zapisi komponenti IT, kao što su aplikacije i operativni sistemi radnih stanica, kreiraju se u svrhu bilježenja informacija o aktivnostima i događajima vezanih za njih. Operativni i sistemski zapisi imaju ključnu ulogu u rekonstrukciji događaja vezanih za komponente IT i utvrđivanje individualne odgovornosti korisnika IS koji ih koriste.

U cilju adekvatnog upravljanja operativnim i sistemskim zapisima preporučuje se da Društvo:

- **Obezbijedi kreiranje operativnih i sistemskih zapisa na svim važnim komponentama IT** u mjeri dovoljnoj za rekonstrukciju događaja i utvrđivanje individualne odgovornosti zaposlenog. Korisničko ime osobe koja je izvršila aktivnost, opis aktivnosti, naziv komponente IT i vrijeme događaja je minimalni set podataka potrebnih u većini zapisa.
- **Zaštiti operativne i sistemske zapise važnih komponenti IT od neovlašćenog pristupa.**
- **Redovno vrši backup rezervnih kopija operativnih i sistemskih zapisa svih važnih komponenti IT.**
- **Obezbijedi precizno mjerenje vremena u komponentama IT koje generišu operativne i sistemske zapise** kako bi se obezbijedila tačnost informacija o vremenu nastanka događaja.

12. Zaštita od malicioznog koda

Djelovanje raznih malicioznih kodova (virusa, trojanaca, malvera itd.) može predstavljati značajnu prijetnju za sigurnost i funkcionisanje IS. Maliciozni kod se sve više koristi u svrhu krađe povjerljivih informacija i ostvarivanja finansijske dobiti od strane zlonamjernih osoba ili grupe njih.

U svrhu primjene adekvatne zaštite malicioznog koda preporučuje se da Društvo:

- **Obezbijedi adekvatnu zaštitu i primjenu sistema zaštite komponenti IT od malicioznog koda,** poput antivirusa i drugih naprednijih softvera;
- **Obezbijedi da se sistemi za zaštitu komponenti IT od malicioznih kodova redovno ažuriraju;**
- **Obezbijedi redovnu primjenu i ažuriranje zakrpa na operativnim sistemima i aplikacijama;**
- **Obezbijedi primjerenu upotrebu web browser-a i aplikacija koje koriste zaposleni IS za elektronsku poštu.** Veliki broj napada malicioznih kodova se vrši infiltriranjem u IS usled otvaranja zaraženih priloga elektronske pošte i otvaranja nepouzdanih i neprimjerenih internet stranica.

IV. PRELAZNE I ZAVRŠNE ODREDBE

Ove smjernice stupaju na snagu danom objavljivanja na internet stranici Agencije za nadzor osiguranja.

Broj: 01-701/4-20
Podgorica, 26. 08. 2020. godine

PREDSJEDNIK SAVJETA
Uroš Andrijašević