Na temelju članka 15. točke 7. Zakona o Hrvatskoj agenciji za nadzor financijskih usluga (»Narodne novine« br. 145/05 i 12/12) Upravno vijeće Hrvatske agencije za nadzor financijskih usluga je na sjednici održanoj 21. prosinca 2022. donijelo

SMJERNICE ZA PRIMJERENO UPRAVLJANJE RIZICIMA INFORMACIJSKIH SUSTAVA SUBJEKATA NADZORA

I. UVODNE ODREDBE

1. Značenje pojmova

Subjekti nadzora (u daljnjem tekstu: subjekti) definirani su člankom 2. Zakona o Hrvatskoj agenciji za nadzor financijskih usluga („Narodne novine“ br. 140/05 i 12/12) kao sve pravne ili fizičke osobe koje se bave pružanjem financijskih usluga, savjetovanjem na financijskom tržištu, prodajom, posredovanjem ili upravljanjem imovinom korisnika financijskih usluga.

Informacijski sustav subjekata (u daljnjem tekstu: IS) je sustav međusobno povezanih organizacijskih, tehnoloških i ljudskih elemenata subjekata uključenih u procese obrade podataka, u cilju raspolaganja informacijama potrebnima za ostvarivanje poslovnih ciljeva.

Informacijska tehnologija (u daljnjem u tekstu: IT) je element IS, čija je svrha automatizacija obrade podataka. IT obuhvaća:

- hardverske komponente:
  - osobna, prijenosna i poslužiteljska računala te periferne uređaje kao što su tipkovnice, zasloni i slično,
  - „pametne“ mobilne uređaje,
  - aktivnu i pasivnu mrežnu i telekomunikacijsku opremu,
  - medije za pohranu podataka,
  - podržavajuću infrastrukturu, kao što su električna napajanja, klimatizacijski uređaji, kablovi i slično.
- softverske komponente:
  - operativne sustave,
  - baze podataka,
  - sistemske poslužitelje kao što su poslužitelji elektroničke pošte i slično,
  - sistemske aplikacije,
  - poslovne aplikacije,
  - razvojne alate.

Korisnici informacijskog sustava (u daljnjem u tekstu: korisnici IS) su sve pravne i fizičke osobe koje, kao zaposlenici subjekta, vanjski suradnici, klijenti, regulatorne institucije ili u bilo kojoj drugoj ulozi, sudjeluju u procesima obrade podataka.

Obrada podataka podrazumijeva sve ručne ili automatizirane aktivnosti vezane uz podatke tijekom njihovog cjelokupnog životnog ciklusa, kao što su:

- prikupljanje,
- unos,
- pohrana,
- prijenos,
- uvid,
- prikaz,
- transformacija,
- kombiniranje ili integriranje,
- povrat,
- arhiviranje,
- analiza,
- zaštita,
- omogućavanje pristupa i stavljanje na raspolaganje,
- blokiranje te
- brisanje ili uništavanje.

Resursi informacijskog sustava (u daljnjem u tekstu: resursi IS) omogućavaju provedbu procesa obrade podataka, primjerenih poslovnim potrebama, te obuhvaćaju:

- podatke i informacije,
- poslovne korisnike IS,
- zaposlenike subjekta ovlaštene za upravljanje IS i IT,
- vanjske suradnike koji sudjeluju u upravljanju IS i IT,
- informacijsku tehnologiju,
- stručna znanja,
- ugovore i licence,
- interne akte i drugu dokumentaciju te
- financijska sredstva.

Rizik informacijskog sustava (u daljnjem tekstu: rizik IS) podrazumijeva vjerojatnost da određena prijetnja iskorištavanjem ranjivosti resursa IS ostvari negativan učinak na poslovanje subjekta.

Upravljanje rizicima informacijskog sustava (u daljnjem tekstu: upravljanje rizicima IS) je kontinuirani proces koji obuhvaća:

- identifikaciju resursa IS,
- identifikaciju prijetnji resursima IS,
- identifikaciju ranjivosti resursa IS,
- procjenu rizika IS i njihovog potencijalnog štetnog učinka,
- odabir mjera za postupanje s procijenjenim rizicima IS,
- primjenu mjera za postupanje s procijenjenim rizicima IS
- praćenje procijenjenih rizika IS te primijenjenih mjera za njihovo smanjenje te
- unaprjeđenje procesa upravljanja rizicima.

Osjetljivi podaci odnosno informacije su oni podaci odnosno informacije kod kojih bi narušavanje svojstava povjerljivosti, cjelovitosti ili dostupnosti izazvalo negativne posljedice za poslovanje subjekta.

2. Ciljevi, namjena i opseg

2.1. Ciljevi

Subjekti koji su predmet nadzora Hrvatske agencije za nadzor financijskih usluga (u daljnjem tekstu: Hanfa) u svom poslovanju su izloženi operativnim rizicima koji obuhvaćaju i rizike IS.

Usvajanjem i objavom Smjernica za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora (u daljnjem tekstu: Smjernice) Hanfa želi ostvariti sljedeće ciljeve:

- razvoj svijesti subjekata o rizicima IS, s osobitim naglaskom na rizike vezane uz uporabu IT te
- upoznavanje subjekata nadzora s dobrim praksama ublažavanja rizika IS.

Hanfa očekuje da će razumijevanje i primjena mjera i postupaka opisanih u Smjernicama doprinijeti kvaliteti upravljanja rizicima IS subjekata te na taj način umanjiti izloženost subjekata rizicima poslovanja u cjelini.

2.2. Namjena

Smjernice su namijenjene subjektima, a osobito:

- članovima uprava subjekata,
- odgovornim osobama u organizacijskim jedinicama za upravljanje IT subjekata,
- osobama odgovornima za sigurnost IS odnosno IT subjekata,
- osobama odgovornima za upravljanje odnosima s vanjskim pružateljima usluga IT subjekata,
- osobama odgovornima za upravljanje procesom neprekinutosti poslovanja subjekata te
- osobama koje obavljaju poslove unutarnjih kontrola subjekata.

Hanfa drugim aktima može dodatno propisati kriterije i postupke upravljanja IS i rizicima IS za određene skupine subjekata, koje je potrebno uzeti u obzir prilikom razumijevanja i primjene Smjernica. Također, potrebno je uzeti u obzir i akte propisane od strane Europske Unije, a koji se odnose na upravljanja rizicima vezanim uz uporabu IS.

2.3. Opseg

Smjernicama je obuhvaćeno sljedeće:

1) Ključni aspekti upravljanja rizicima IS:
    - osnovna načela upravljanja rizicima IS,
    - identifikacija, procjena i postupanje s rizicima IS te
    - zaštita od kibernetičkih prijetnji i rizika IS
2) Mjere i postupci za smanjenje rizika IS:
    - organizacija i upravljanje IS,
    - razvoj i održavanje IS,
    - unutarnje kontrole i revizije IS
    - upravljanje promjenama u IS,
    - izdvajanje procesa IS,
    - neprekinutost poslovanja i oporavak nakon katastrofe,
    - fizička i okolišna sigurnost,
    - logičke kontrole pristupa,
    - sigurnost računalnih mreža,
    - sigurnost prijenosnih uređaja i medija za pohranu podataka,
    - podizanje razine svijesti o sigurnosti IS
    - upravljanje incidentima,
    - upravljanje operativnim i sistemskim zapisima te
    - zaštita od malicioznog koda.

II. KLJUČNI ASPEKTI UPRAVLJANJA RIZICIMA INFORMACIJSKIH SUSTAVA

1. Osnovna načela upravljanja rizicima informacijskih sustava

Procesi upravljanja rizicima integralni su dio svakodnevnog poslovanja. Subjekti, u najmanju ruku, iskustveno i intuitivno prepoznaju rizike koji prijete ostvarivanju poslovnih ciljeva i poduzimaju mjere kako bi se ti rizici sveli na prihvatljivu razinu. Sustavni pristup identifikaciji i primjeni mjera i postupaka, kroz proces upravljanja rizicima, može donijeti dodatne prednosti u odnosu na intuitivni odnosno iskustveni, kao što su:

- kvalitetnija zaštita važnih poslovnih procesa i resursa,
- manja vjerojatnost previda rizika kojima je subjekt izložen,
- manja vjerojatnost nepoštivanja mjerodavnih propisa,
- kvalitetnija podrška donošenju poslovnih odluka,
- manja vjerojatnost neučinkovitog trošenja sredstava na zaštitne mjere,
- manji utrošak vremena na upravljanje zaštitnim mjerama i druge.

U nastavku Smjernica opisani su osnovni postupci u procesu sustavne identifikacije, procjene i tretiranja rizika.

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

Vrsta i namjena informacija ovisi o vrsti industrije, tržišta, proizvoda i usluge u ponudi te mnogim druge faktore. Primjeri informacija s kojima subjekti u poslovanju mogu raspolagati su:

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

Raspoloživost točne i pravodobne informacije može utjecati na donošenje ispravnih poslovnih odluka, ali i na poštivanje mjerodavnih propisa. Dostupnost osjetljive informacije neovlaštenim osobama može dovesti do gubitka prednosti nad konkurencijom, gubitka povjerenja klijenata, a također i do nepoštivanja mjerodavnih propisa.

Promatrano sa stajališta informacijske sigurnosti, informacije imaju tri ključna svojstva čije narušavanje predstavlja rizik za poslovanje subjekata:

1) **Povjerljivost** je svojstvo informacije da je raspoloživa isključivo osobama i sustavima koje za to imaju valjano ovlaštenje. Neki primjeri posljedica narušavanja povjerljivosti informacija su:
    - gubitak konkurentske prednosti (na primjer, otkrivanjem informacija o osobinama novog proizvoda konkurenciji),
    - gubitak povjerenja klijenata (na primjer, curenjem osobnih podataka klijenata u javnost),
    - nepoštivanje mjerodavnih propisa (na primjer, curenje osobnih podataka klijenata može predstavljati kršenje regulative u domeni zaštite osobnih podataka),
    - financijske gubitke (na primjer, curenje osobnih podataka može pokrenuti tužbe klijenata i rezultirati isplatom novčanih sredstava u svrhu pokrivanja odštetnih zahtjeva).
2) **Cjelovitost** je svojstvo informacije da postoji razumno uvjerenje u njezinu točnost odnosno da nije neovlašteno ili nepredviđeno izmijenjena, slučajnim ili namjernim djelovanjem, što podrazumijeva i naknadno dodavanje, izmjenu ili brisanje informacija bez traga o provedenim aktivnostima koji se može slijediti. Neki primjeri posljedica narušavanja cjelovitosti informacija su:
    - donošenje pogrešnih poslovnih odluka (na primjer, zbog pogrešnih informacija predstavljenih u važnom izvješću za upravu),
    - gubitak povjerenja klijenata (na primjer, zbog pogrešno izračunate i naplaćene cijene usluge ili proizvoda),
    - nepoštivanje mjerodavnih propisa (na primjer, zbog netočnih informacija u izvješćima namijenjenima regulatoru).
3) **Dostupnost** je svojstvo informacije da po potrebi i u prihvatljivom roku bude dostupna ovlaštenim osobama i sustavima. Neki primjeri posljedica narušavanja dostupnosti informacija su:
    - nemogućnost isporuke proizvoda i usluga klijentima (na primjer, zbog nedostupnosti informacija o ugovornim odnosima s klijentima),
    - nepoštivanje mjerodavnih propisa (na primjer, zbog nedostupnosti informacija potrebnih za sastavljanje izvješća koja se u zadanom roku moraju dostaviti regulatoru),
    - nemogućnost ispunjavanja ugovornih obveza (na primjer, zbog nedostupnosti informacija o transakcijskim računima odnosno nemogućnosti zadavanja platnih naloga).

Štetni učinci rizika IS rezultiraju narušavanjem navedenih svojstava informacija, a proizlaze iz djelovanja **prijetnji**, koje štetne učinke ostvaruju iskorištavanjem **ranjivosti** resursa IS. Upravo zbog toga je bitno identificirati prijetnje i ranjivosti resursa IS te procijeniti rizike IS i njihove štetne učinke, prema kojima bi se postupalo primjenom primjerenih mjera.

2. Identifikacija, procjena i postupanje s rizicima informacijskog sustava

Osnovni preduvjet za identifikaciju i procjenu rizika IS je poznavanje poslovnih ciljeva, poslovne strategije i poslovnih procesa subjekta, kako bi se mogao procijeniti realni utjecaj rizika IS na poslovanje.

Nadalje, potrebno je identificirati sve resurse IS koji imaju ulogu u ostvarivanju poslovnih ciljeva i strategije te podršci poslovnim procesima, a potom i procijeniti njihovu važnost u tim ulogama. Osobito je važno spoznati i međusobne ovisnosti resursa IS. Na primjer, ukoliko je neka informacija bitna za kritični poslovni proces, bitan će biti i poslužitelj baze podataka na kojem je ta informacija pohranjena, kao i operativni sustav i samo poslužiteljsko računalo, ali i mrežna oprema koji omogućuje dostupnost informacije putem osobnog računala krajnjem korisniku.

Rizici IS proizlaze iz djelovanja prijetnji. Prijetnje se obično dijele, s obzirom na mjesto nastanka, na unutrašnje i vanjske.

Neke od unutrašnjih prijetnji mogu biti:

- interna prijevara,
- neovlašteni pristup informacijama iznutra,
- krađa resursa IS,
- greške u unosu podataka u aplikacije,
- nesvjesno odavanje povjerljivih informacija.

Neke od vanjskih prijetnji mogu biti:

- hakerski napadi,
- maliciozni kod,
- socijalni inženjering,
- epidemije,
- elementarne nepogode.

Identificirane prijetnje potrebno je staviti u kontekst ranjivosti resursa IS, koje pojedine prijetnje mogu iskoristiti te na taj način izazvati štetni učinak. Neke od ranjivosti mogu biti:

- nepostojanje zaštite od malicioznog koda,
- neprimjerena konfiguracija vatrozida,
- pristup poslovnim aplikacijama nije kontroliran potvrdom identiteta korisnika,
- zaposlenici imaju nisku razinu svijesti o sigurnosti IS,
- nepostojanje sustava za besprekidnu opskrbu električnom energijom.

U konačnici, poznavanjem ranjivosti, prijetnji i njihovih štetnih učinaka na poslovanje mogu se procijeniti rizici IS, kroz dva njihova temeljna svojstva:

- vjerojatnost da će prijetnja iskoristiti ranjivost resursa IS te
- razina štetnog učinka ukoliko prijetnja uspješno iskoristi ranjivost.

Primjer opisanog procesa može izgledati ovako:

- Proces prodaje usluga klijentima ovisi o dostupnosti informacija o klijentima, što uključuje podatke kao što su ime, prezime, adresa, vrsta ugovorene usluge i slično.
- Informacije o klijentima pohranjene su na poslužitelju baze podataka. Nestanak električne energije, do kojeg prosječno dolazi četiri puta godišnje u trajanju od četiri sata, bi uzrokovao prestanak rada poslužitelja baze podataka, s obzirom da nije implementiran sustav za besprekidno napajanje.
- Sve dok poslužitelj baze podataka ne funkcionira, subjekt nije u stanju pružati uslugu klijentima te na taj način ostaje bez potencijalnih financijskih prihoda, a velika je vjerojatnost i narušavanja reputacije i povjerenja klijenata.

Odluka o načinu postupanja s rizicima IS u pravilu ovisi o samim rizicima te vrijednosti izloženih procesa i resursa.

Načine upravljanja rizicima možemo općenito podijeliti na:

- **Izbjegavanje** - podrazumijeva ublažavanje rizika eliminacijom rizičnog procesa odnosno resursa IS. Nastavno na prethodni primjer, subjekt je zaključio da mu je rizik neprihvatljiv, ali i financijski izdaci investicije nabave sustava za besprekidno napajanje, te je odlučio izbaciti iz uporabe poslužitelj baze podataka i sve informacije o klijentima držati na papirnatim dokumentima. Na taj način eliminirana je ranjivost koju bi mogla iskoristiti prijetnja prekida opskrbe električnom energijom.
- **Smanjenje** - podrazumijeva ublažavanje rizika implementacijom mjera kojima se rizik smanjuje. Nastavno na prethodni primjer, subjekt je zaključio da mu je rizik neprihvatljiv. Analizom troškova nabave i godišnjeg održavanja sustava za besprekidno napajanje, subjekt je zaključio da su troškovi manji od potencijalnih izgubljenih prihoda i gubitaka uzrokovanih narušenom reputacijom te se odlučuje za implementaciju, čime umanjuje identificirani rizik.
- **Prihvaćanje** - podrazumijeva prihvaćanje potencijalnih posljedica štetnog učinka rizika. Nastavno na prethodni primjer, subjekt je svjestan rizika, ali je došao do zaključka da su troškovi nabave i godišnjeg održavanja sustava za besprekidno napajanje veći od potencijalnih izgubljenih prihoda i gubitaka uzrokovanih narušenom reputacijom te se odlučuje za prihvaćanje rizika bez implementacije dodatnih mjera.
- **Prijenos** – podrazumijeva prijenos posljedica štetnog učinka rizika na druge fizičke ili pravne osobe. Na primjer, osiguranjem ključnog resursa kod osiguravajućeg društva od različitih štetnih događaja.

Neki rizici se ne mogu ocijeniti prihvatljivima bez obzira na troškove implementacije kontrolnih mjera – primjerice rizici koji za posljedicu imaju ugrožavanje ljudskih života ili počinjenje kaznenih djela.

III. MJERE I POSTUPCI ZA SMANJENJE RIZIKA INFORMACIJSKOG SUSTAVA

U nastavku Smjernica opisane su neke mjere koje pripadaju u dobre prakse smanjenja rizika IS, a posebno su istaknute one koje je preporučljivo primijeniti bez obzira na svojstva IS subjekta. O načinu provedbe preporuka i odabiru tehničkih rješenja koja bi se pri tome eventualno koristila odlučuju sami subjekti, temeljem vlastite procjene rizika, vodeći se pritom načelom razmjernosti kako bi identificirali optimalna rješenja za svoj IS.

1. Organizacija i upravljanje informacijskim sustavom

1.1. Uprava subjekta

Funkcioniranje IS subjekta u znatnoj mjeri ovisi o podršci uprave subjekta. Uprava je odgovorna za organizaciju, strateško odlučivanje, dodjelu resursa i donošenje pravila i procedura u kontekstu upravljanja IS, što obuhvaća i procese izdvojene vanjskim pružateljima usluga. Ukoliko uprava subjekta nije na primjeren način uključena u upravljanje IS, subjekt se može izložiti rizicima kao što su neusklađenost strategije poslovnog razvoja i razvoja IS te neučinkovito trošenje sredstava za razvoj i održavanje u IS.

U svrhu umanjenja rizika IS, uprava subjekta primjenjuje sljedeće mjere i postupke:

- **Uspostava primjerene organizacijske strukture** potrebne za funkcionalnost i sigurnost IS, sukladno poslovnim ciljevima subjekta.
- **Osiguravanje resursa** potrebnih za primjerenu funkcionalnost i sigurnost IS, poglavito u kontekstu stručnih kadrova, hardvera, softvera i podržavajuće infrastrukture.
- **Imenovanje odgovorne osobe za upravljanje IT procesima i operacijama.**
- **Osiguravanje kontinuirane upoznatosti uprave s relevantnim činjenicama** vezanima uz funkcioniranje i sigurnost IS, bilo kroz neformalnu komunikaciju s osobama odgovornima za funkcioniranje i sigurnost IS ili kroz formalni sustav izvješćivanja.
- **Usklađivanje strategije razvoja IS i razvoja poslovne strategije** subjekta.

Sukladno vlastitoj procjeni rizika, uprava subjekta može dodatno primijeniti sljedeće mjere i postupke:

- **Formiranje odbora za upravljanje IS.** Uobičajena praksa je da u radu odbora za upravljanje IS sudjeluju odgovorne osobe poslovnih organizacijskih jedinica i sustava unutarnjih kontrola, uz članove uprave i osobe odgovorne za sigurnost i funkcionalnost IS. Rad odbora se manifestira kroz zajedničke sjednice, na kojima se raspravlja o ključnim pitanjima funkcionalnosti i sigurnosti IS. Na taj način se olakšava komunikacija između sudionika, rješavaju problemi u međusobnoj suradnji te se unaprjeđuje usklađenost djelovanja organizacijskih jedinica zaduženih za osiguranje funkcionalnosti i sigurnosti IS i ostalih organizacijskih jedinica.
- **Razdvajanje funkcije upravljanja sigurnošću IS od drugih zaduženja vezanih uz IS.** Sigurnosni i funkcionalni ciljevi IS mogu biti u suprotnosti u nekim situacijama, stoga je prisutna praksa razdvajanja tih funkcija dodjelom funkcija različitim osobama.
- **Razdvajanje međusobno nesukladnih 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 drugo. Dodjelom tih funkcija različitim djelatnicima omogućava se njihova veća usredotočenost na dužnosti za koje su specijalizirani, ali se istovremeno ograničava potencijalna šteta koja bi mogla nastati namjernim štetnim djelovanjem nekog od zaposlenika navedenih u primjeru.
- **Formiranje sustava unutarnjih kontrola IS.** Unutarnje kontrole, u vidu funkcija unutarnje revizije, procjene rizika ili usklađenosti, a koje su neovisne od ostalih zaduženja vezanih uz funkcionalnost ili sigurnost IS, mogu doprinijeti kvalitetnijem upravljanju rizicima IS.
- **Dokumentiranje i usvajanje politika, pravila, standarda, smjernica, uputa 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 s aplikacijama,
- nesvjesno ili namjerno odavanje povjerljivih podataka,
- greške u razvoju i održavanju IS,
- neprimjereno rukovanje informatičkom opremom i drugo.

U svrhu smanjenja štetnih učinaka prijetnji nastalih ljudskim djelovanjem, potrebno je osigurati da djelatnici:

- **imaju primjerena znanja i vještine u vezi korištenja poslovnih aplikacija**.
- **imaju primjerena znanja i vještine u vezi uporabe ostalih resursa IT** koje koriste pri izvršavanju radnih zadataka, kao što su Internet, elektronička pošta i slično.
- **djelatnici odgovorni za upravljanje, razvoj i održavanje IS imaju primjerena znanja i vještine** za dužnosti koje obavljaju.
- **djelatnici imaju primjerenu razinu svijesti o sigurnosti IS**.

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Uspostava procesa provjere kandidata za zapošljavanje**. Proces može uključivati provjeru istinitosti navoda o radnom iskustvu i obrazovanju, provjeru o počinjenim kaznenim djelima i slično. Takvim i sličnim provjerama smanjuje se mogućnost zapošljavanja osoba koje bi mogle predstavljati sigurnosni rizik po IS.
- **Uspostava procesa kontinuirane edukacije djelatnika** u cilju podizanja svijesti o sigurnosti IS, što može uključivati planiranje i provedbu edukacije te prikupljanje povratnih informacija od sudionika.

2. Razvoj i održavanje informacijskog sustava

2.1. Održavanje informacijske tehnologije

Hardver, softver i podržavajuća infrastruktura zahtijevaju kontinuirano održavanje kako bi se osigurala njihova primjerena funkcionalnost. Neodržavana infrastruktura može biti izložena različitim prijetnjama, kao što su primjerice:

- greške u funkcioniranju operativnih sustava i aplikacija,
- kvarovi na računalima i mrežnoj opremi,
- kvarovi na podržavajućoj infrastrukturi,
- povećana izloženost raznim oblicima kibernetičkih napada i drugo.

U svrhu smanjenja štetnih učinaka prijetnji nastalih zbog neprimjerenog održavanja IT, potrebno je:

- **Osigurati primjereno održavanje hardvera, softvera i podržavajuće infrastrukture**, u vidu nadogradnji i ispravljanja pogrešaka u softveru, redovnog servisiranja hardvera i podržavajuće infrastrukture, zamjene zastarjelih i dotrajalih komponenti i slično.
- **Ograničiti ovlaštenja za izmjene na hardveru, softveru i podržavajućoj infrastrukturi** isključivo na osobe koje imaju odgovarajuća stručna znanja i vještine.
- **Primjereno nadzirati ključne pokazatelje funkcionalnosti IT,** kao što su primjerice notifikacije o sigurnosti na mrežnim i drugim dijelovima IS, slobodni kapaciteti medija za pohranu podataka, raspoloživost sistemskih resursa poslužiteljskih računala i slično.

2.2. Razvoj aplikacija

Primjerena funkcionalnost i sigurnost poslovnih aplikacija izuzetno je bitna za funkcionalnost i sigurnost IS u cjelini. Stoga je osobito važno posvetiti pozornost razvoju ključnih poslovnih, ali i ostalih aplikacija kroz cijeli razvojni ciklus. Propusti u razvoju mogu rezultirati izloženošću različitim prijetnjama, kao što su na primjer:

- neusklađenost značajki aplikacija s potrebama poslovnih procesa,
- nekompatibilnost aplikacija s ostalim komponentama IT,
- neovlašteni pristup osjetljivim podacima,
- greške u funkcioniranju aplikacija i ostalih komponenti IS,
- povećana izloženost raznim oblicima kibernetičkih prijetnji i drugo.

U svrhu smanjenja štetnih učinaka prijetnji nastalih zbog neprimjerenog pristupa razvoju aplikacija, potrebno je

- **Uključiti krajnje korisnike aplikacija u proces izrade specifikacija aplikacije**, kako bi se unaprijed definirale značajke poput korisničkog sučelja, ulaznih i izlaznih podataka i slično.
- **Planirati sigurnosne kontrole u fazi razvoja**, kao što su identifikacija korisnika i autorizacija pristupa resursima aplikacije, kriptografski mehanizmi, kontrole unosa podataka, kontrole izlaznih podataka i slično.
- **Zaštititi izvorni kod aplikacija od neovlaštenog pristupa**.
- **Testirati funkcionalnost i sigurnost novih i izmijenjenih aplikacija** prije njihovog uključenja u normalnu produkciju. Osim testiranja sistemskih i integracijskih značajki, u proces testiranja funkcionalnosti potrebno je uključiti i krajnje korisnike i dobiti povratne informacije od njih o prihvatljivosti uporabnih svojstava aplikacije.

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Razdvajanje razvojnog i testnog okruženja aplikacija od produkcijskog,** primjerice korištenjem odvojenih baza podataka ili čak i potpuno odvojenih osobnih i poslužiteljskih računala za različita okruženja. Na taj način se znatno umanjuje rizik narušavanja cjelovitosti produkcijskih podataka tijekom razvoja ili testiranja.
- **Izbjegavanje korištenja 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 neovlaštenih osoba. Stoga je preporučljivo takve podatke ne koristiti prilikom razvoja ili testiranja ili pak prethodno iz njih ukloniti osjetljivi sadržaj poput osobnih podataka.

Ukoliko je razvoj aplikacija izdvojen vanjskim pružateljima usluga, primjena gore opisanih mjera i postupaka može biti znatno otežana. U tom slučaju preporučljivo je da subjekti traže informacije od samog pružatelja usluge o sigurnosnim značajkama aplikacije kako bi procijenili njihovu primjerenost.

3. Upravljanje promjenama u informacijskom sustavu

3.1. Upravljanje promjenama

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

- provedbu promjena koje mogu narušiti funkcionalnost komponenti IT,
- provedbu promjena koje IS mogu izložiti sigurnosnim prijetnjama,
- probleme u radu korisnika koji nisu primjereno upoznati s promjenama, na primjer u vidu novih funkcionalnosti u aplikacijama i slično.

U svrhu smanjenja štetnih učinaka prijetnji nastalih zbog nekontroliranih promjena, potrebno je osigurati da su:

- **odgovorne osobe za upravljanje IT upoznate s planiranim promjenama i potencijalnim rizicima tih promjena** prije same provedbe.
- **planirane promjene odobrene od strane odgovorne osobe za upravljanje IT** prije same provedbe.
- **promjene primjereno testirane što uključuje i testiranje od strane poslovnih korisnika** prije njihove primjene u produkcijskim sustavima,
- **korisnici IS upoznati s promjenama** ukoliko one utječu na provedbu korisničkih radnih zadataka, primjerice kad se radi o funkcionalnim promjenama u poslovnim aplikacijama.

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Vođenje evidencije o promjenama u IS,** što može uključivati opis svake promjene, ime predlagatelja, ime odobravatelja, procijenjene rizike, status odobrenja, status testiranja i status provedbe. Takva evidencija može se koristiti u svrhu revizije i kontrole, ali i kao baza znanja koja može doprinijeti efikasnijem upravljanju promjenama u budućnosti.

4. Izdvajanje procesa informacijskog sustava

4.1. Izdvajanje procesa informacijskog sustava

Izdvajanje procesa IS subjekata podrazumijeva uključivanje druge pravne ili fizičke osobe u obavljanje poslova vezanih uz IS, kao što su primjerice:

- održavanje komponenti IT,
- razvoj posebno dizajniranih aplikacija, primjerice izrada aplikacije za podršku središnjim poslovnim procesima po narudžbi subjekta, izrada internetskih stranica i slično,
- bilo kakav vid obrade podataka, primjerice kreiranje, izmjena i brisanje korisničkih računa i prava u operativnim sustavima računala i mrežnih uređaja, bazama podataka te aplikacijama, zatim pohrana podataka, izrada pričuvnih kopija podataka i slično,
- pružanje usluga uporabe tehničke i sigurnosne infrastrukture, primjerice smještaj poslužitelja u podatkovnom centru pružatelja usluga, smještaj internetskih stranica na poslužitelje pružatelja usluga i slično,
- pružanje savjetodavnih usluga poput vođenja sigurnosti IS, vođenja projekata i slično,
- pružanje usluga unutarnjih kontrola poput unutarnje revizije IS.

Za ilustraciju, kupovina gotovog, tržišno dostupnog softvera za koji proizvođač izdaje ispravke i nadogradnje koje subjekt sam primjenjuje u svom sustavu ne smatra se izdvajanjem procesa. Međutim, u slučaju da proizvođač provodi primjenu ispravaka i nadogradnji u sustavu subjekta, što se smatra održavanjem sustava, odnosno da proizvođač provodi administraciju u vidu upravljanja korisničkim pravima i računima umjesto subjekta, što se smatra obradom podataka, govorimo o izdvajanju procesa.

S obzirom na razinu ovisnosti poslovanja subjekta o izdvojenim procesima, može se procijeniti značajnost izdvajanja. Primjerice, ukoliko o nekom izdvajanju ovisi funkcioniranje središnjih poslovnih procesa, ili pak ukoliko se izdvojenim procesom obrađuju osjetljivi podaci poput financijskih ili osobnih, možemo govoriti o značajnom izdvajanju.

Ovisno o značaju izdvajanja, subjekti se, mogu izložiti različitim rizicima, od manjih neugodnosti, do znatnih financijskih gubitaka, narušavanja povjerljivosti, cjelovitosti i dostupnosti osjetljivih podataka te prekida središnjih poslovnih procesa, izazvanih djelovanjem prijetnji kao što su primjerice:

- nemogućnost pružatelja da osigura primjerenu uslugu,
- potpuni prekid pružanja usluge uslijed prekida poslovanja pružatelja, više sile ili slično
- krađa i oštećenje resursa IS od strane pružatelja,
- odavanje povjerljivih podataka od strane pružatelja,
- nemogućnost izvršavanja ugovornih obveza subjekta prema pružatelju.

U svrhu smanjenja štete nastale zbog rizika vezanih uz vanjske pružatelje usluga, potrebno je :

- **Procijeniti rizike izdvajanja procesa.** Potrebno je provesti i dokumentirati analizu u cilju dobivanja odgovora na pitanja:
    - Na koje poslovne procese i resurse te na koji način utječe izdvajanje procesa?
    - Kako bi prekid pružanja usluge utjecao na poslovanje?
    - Kojim rizicima proizašlima uslijed izdvajanja bi subjekt bio izložen?
    - Na koji način će subjekt nadzirati pružanje usluge i povezane rizike?
    - Na koji način se može osigurati neprekinutost poslovanja u slučaju prekida pružanja usluge ili pružanja neprimjerene usluge?
- **Procijeniti primjerenost pružatelja usluga**. Potrebno je provesti i dokumentirati analizu u cilju dobivanja odgovora na pitanja:
    - Da li pružatelj ima perspektivu stabilnog poslovanja za vrijeme pružanja usluge?
    - Da li pružatelj posjeduje reference, iskustvo, znanje, stručnost te kadrove i druge resurse koji daju razumno uvjerenje u primjereno pružanje usluge?
    - Da li pružatelj udovoljava relevantnim regulatornim propisima u kontekstu pružane usluge?
- **Definirati i sklopiti ugovor primjeren usluzi koja se pruža.** Ugovor bi trebao sadržavati barem sljedeće stavke:
    - detaljan opis predmeta ugovora,
    - obveze čuvanja povjerljivih podataka,
    - prihvatljive razine pružane usluge,
    - obveze i odgovornosti pružatelja i subjekta,
    - novčanu vrijednost ugovora,
    - uvjete jednostranog raskida ugovora i izlaznu strategiju
    - trajanje ugovora te
    - način rješavanja sporova.
- **Osigurati primjeren nadzor** nad pružanjem usluge**.**
- **Osigurati pravodoban pristup informacijama** u vezi pružatelja i same usluge, a koje su relevantne za pružanje usluge.
- **Osigurati neprekinutost poslovanja** u slučaju prestanka ili neprimjerenog pružanja usluge.

4.2. Uporaba „Cloud Computing“ usluga u izdvojenim procesima

„Cloud Computing“ usluge postupno dobivaju na značaju i pobuđuju interes tvrtki u različitim industrijskim granama. Prednosti korištenja „Cloud Computing“ usluga mogu se manifestirati u vidu ušteda kod nabavke informatičke opreme, kod zapošljavanja stručnih kadrova, kod troškova održavanja, zatim jednostavnog načina rješavanja pitanja planova oporavka nakon katastrofe i drugih.

„Cloud Computing“, u kontekstu izdvajanja procesa, predstavlja obradu podataka korištenjem računalne infrastrukture pružatelja usluga, dijeljene s drugim pravnim ili fizičkim osobama kao jednakopravnim korisnicima te smještene izvan poslovnih lokacija subjekta, a na koju se subjekt povezuje koristeći računalne mreže ili druge metode udaljenog povezivanja u cilju pristupa svojim podacima.

Upravo zbog tih osobina, uporaba „Cloud Computing“ usluga inherentno nosi sa sobom i neke specifične rizike:

- Kako se **podaci subjekta obrađuju izvan njegovih poslovnih prostorija**, postavlja se pitanje koji su tokovi kretanja podataka i tko ima pristup podacima subjekta. Nadalje, kako se u većini slučajeva infrastruktura dijeli s drugim pravnim i fizičkim osobama kao korisnicima jednakopravnima subjektu, postavlja se pitanje na koji način je osigurano kvalitetno razdvajanje i ograničavanje pristupa podacima pojedinih korisnika. Ukoliko navedena pitanja nisu kvalitetno riješena, subjekt se može izložiti povećanim rizicima narušavanja povjerljivosti i cjelovitosti svojih podataka od strane neovlaštenih korisnika te kršenju regulatornih odredbi u kontekstu zaštite osobnih podataka.
- Subjekt nema izravnu **kontrolu nad procesima održavanja opreme, podržavajućom infrastrukturom, kontrolama fizičkog pristupa te kontrolama zaštite od prijetnji iz okoliša**. Ukoliko navedene mjere nisu primjereno uspostavljene, subjekti se izlažu rizicima gubitka povjerljivosti, cjelovitosti i dostupnosti podataka, primjerice uslijed neovlaštenog pristupa ili elementarnih nepogoda.
- Subjekt najčešće ima **ograničenu kontrolu nad komunikacijskim kanalima** kojima pristupa svojim podacima. Ukoliko komunikacijski kanali nisu pouzdani i primjereno zaštićeni, subjekti se izlažu rizicima gubitka povjerljivosti, cjelovitosti i dostupnosti podataka, primjerice uslijed nedostupnosti kanala ili presretanja komunikacije od strane neovlaštenih osoba.

U svrhu smanjenja navedenih rizika, potrebno je primjenjivati sve mjere i postupke opisane u poglavlju 4.1. Smjernica, ali i posebnu pozornost obratiti na primjenu sljedećeg:

- **Steći uvjerenje da će pružatelj obavljati uslugu u skladu s relevantnom regulativom,** poglavito u kontekstu obveza subjekta vezanih za zaštitu podataka, primjerice putem neovisnih revizijskih izvješća, izravnim uvidom ili verifikacijom certifikata i potvrda koje pružatelj usluga posjeduje.
- **Steći uvjerenje u primjerenost tehnološke i podržavajuće infrastrukture te sigurnosnih i okolišnih kontrola** za što subjekt također može koristiti neovisna revizijska izvješća, izravni uvid ili verifikaciju certifikata i potvrda koje pružatelj usluga posjeduje.

4.3. Izdvajanje unutar iste grupe poduzeća

Česta je poslovna praksa izdvajanje procesa pravnim osobama koje su dio iste grupe poduzeća. Budući da se i dalje radi o drugoj pravnoj osobi, potrebno je provesti sve mjere opisane u poglavlju 4.1. Smjernica.

Činjenica da se radi o poduzećima povezanima unutar iste grupe može se uzeti u obzir prilikom procjene rizika izdvajanja i analize primjerenosti pružatelja usluga.

5. Neprekinutost poslovanja i oporavak nakon katastrofe

5.1. Planiranje neprekinutosti poslovanja

Vjerojatnost da prijetnje, usprkos primijenjenim zaštitnim mjerama, ostvare štetne učinke i pri tome otežaju ili onemoguće normalno poslovanje, uvijek postoji. Stoga je potrebno takve situacije predvidjeti i planirati kako u tom slučaju nastaviti poslovanje.

U svrhu smanjenja rizika nemogućnosti nastavka poslovanja uslijed djelovanja štetnih događaja, potrebno je :

- **Identificirati ključne poslovne procese i resurse potrebne za njihovo izvršavanje**, što uključuje IT resurse, djelatnike, uredsku opremu, ugovore, licence i drugo.
- **Analizirati kako prekid poslovnih procesa utječe na poslovanje u cjelini** s obzirom na različite dužine vremena u kojima su procesi u prekidu te na taj način odrediti najveće prihvatljive dužine vremena prekinutosti procesa.
- **Usvojiti i dokumentirati planove nastavka poslovanja u slučaju prekida poslovnih procesa,** primjerice, ovisno o scenariju, kroz alternativne načine provedbe procesa, povrat podataka iz pričuvne pohrane, oporavak procesa na alternativnoj lokaciji i slično. Planovi bi trebali obuhvatiti sve kritične poslovne procese te sadržavati:
    - odgovornosti i uloge u provedbi,
    - kriterije koji utječu na provedbu plana, primjerice pojava štetnog scenarija ili prekid kritičnog procesa te
    - mjere kojima će se osigurati nastavak poslovanja.
- **Osigurati da su planovi razumljivi i stalno dostupni osobama odgovornima za njihovu provedbu**. Pri tome je potrebno predvidjeti i djelovanje štetnih scenarija koji bi mogli ugroziti dostupnost samih planova.
- **Periodički testirati efikasnost planova,** primjerice kroz testiranje povrata podataka iz pričuvne pohrane, „Table Top“ testove i slično.
- **Planove korigirati sukladno rezultatima testova i periodički prilagođavati poslovnim potrebama i ciljevima.**

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Uspostava pričuvnog računalnog centra** na udaljenoj lokaciji koji svojim kapacitetima može osigurati nastavak poslovanja u slučaju nedostupnosti primarnog.
- **Omogućavanje rada od kuće** u slučaju neupotrebljivosti primarne poslovne lokacije.

5.2. Pričuvna pohrana podataka

Pričuvna pohrana podataka omogućava nastavak poslovanja u slučaju gubitka ili narušavanja cjelovitosti poslovnih podataka. U svrhu smanjenja rizika potrebno je:

- **Identificirati podatke** koji će biti predmet izrade pričuvne pohrane, što obično podrazumijeva podatke koji su ocijenjeni kao bitni za poslovanje.
- **Identificirati učestalost izrade pričuvnih kopija pojedinih podataka**. Primjerice, kopije veoma bitnog skupa podataka, podložnog čestim promjenama u toku dana, mogu se izrađivati i više puta dnevno, a kopije manje bitnih, statičnih skupova podataka jednom tjedno ili mjesečno.
- **Osigurati izradu pričuvnih kopija podataka** sukladno planovima učestalosti.
- **Zaštititi povjerljivost i cjelovitost pričuvnih kopija podataka** sukladno njihovom značaju. U pravilu, pričuvnim kopijama podataka bi trebalo osigurati barem jednaku razinu zaštite kao i izvornicima u produkcijskim sustavima.
- **Periodički testirati mogućnost povrata podataka iz pričuvnih kopija**.
- **Dokumentirati aktivnosti izrade i testiranja povrata** pričuvnih kopija podataka putem automatski generiranih zapisa ili ručno.
- **Periodički odlagati pričuvne kopije podataka na udaljenu lokaciju.** Primjerenu udaljenost lokacije bi subjekti trebali odrediti temeljem vlastite procjene rizika, pri čemu je potrebno da se barem radi o izdvojenoj poslovnoj zgradi.

6. Fizička i okolišna sigurnost

6.1. Fizička sigurnost

Fizička sigurnost podrazumijeva primjenu mjera i postupaka kako bi se kontrolirao fizički pristup resursima IS. Nepostojanjem primjerenih mjera i postupaka fizičke sigurnosti, subjekti se mogu izložiti rizicima otuđenja i oštećenja komponenata IS te dodatno povećati rizike neovlaštenog pristupa osjetljivim podacima pohranjenima na IS.

U svrhu smanjenja rizika koji proizlaze iz nepostojanja primjerenih kontrola fizičke sigurnosti, potrebno je :

- **Smjestiti značajnu informatičku opremu u posebne prostorije,** što primjerice uključuje opremu poput poslužiteljskih računala, medija za pohranu podataka, konfiguracijskih terminala, aktivne mrežne opreme i slično.
- **Ograničiti pravo pristupa prostorijama u kojima je smještena značajna informatička oprema** na zaposlenike subjekta koji imaju za to opravdanu potrebu, primjerice stručno osoblje subjekta koje održava tu opremu.
- **Osigurati da su osobe koje pristupaju prostorijama sa značajnom informatičkom opremom, a koje za to inače nemaju pravo pristupa, pod stalnim nadzorom ovlaštenih osoba.** To se prije svega odnosi na vanjske suradnike koje pristupaju prostorijama zbog održavanja informatičke opreme.
- **Osigurati kontrolu pristupa medijima za pohranu podataka koji su bez nadzora,** primjerice zaključavanjem u ormar ili sigurnosni sef papirnatih dokumenata, raznih podatkovnih medija, pametnih kartica i slično.

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Vođenje evidencije osoba koje pristupaju prostorijama sa značajnom informatičkom opremom,** ručnim ili automatiziranim putem.
- **Primjena dodatnih mjera za kontrolu pristupa prostorijama sa značajnom računalnom opremom,** kao što su primjerice video nadzor, protuprovalni alarm, protuprovalna vrata i slično.

6.2. Okolišna sigurnost

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

U svrhu smanjenja rizika nastalih uslijed djelovanja prirodnih pojava, potrebno je:

- **Ograničiti izloženost značajne informatičke opreme prirodnim pojavama.** Pri tome je potrebno:
    - osigurati primjerenost prostorije u kojoj je smještena, u smislu da nije izložena vanjskim utjecajima poput kiše, vjetra i sunca te da nije izložena prodoru vode, primjerice zbog podrumskog položaja ili prisustva vodovodnih cijevi u zidovima.

    - ne koristiti prostoriju predviđenu za smještaj opreme IS kao priručno skladište, posebice zapaljivih stvari.
- **Osigurati primjerenu zaštitu od požara poslovnih prostora i prostorija sa značajnom informatičkom opremom**, u vidu sustava za detekciju i gašenje požara na elektroničkoj opremi. Pri tome je osobito važno da su protupožarni sustavi redovito održavani i atestirani.
- **Osigurati temperaturu prostorije u kojoj je smještena značajna informatička oprema primjerenu za funkcioniranje te opreme**, primjerice putem uređaja za klimatizaciju.

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedećih mjera:

- **Primjena dodatnih mjera okolišne sigurnosti** poput senzora vlage, sustava za detekciju prodora vode i drugih.

7. Logičke kontrole pristupa

7.1. Logičke kontrole pristupa

Logičke kontrole pristupa pripadaju skupu sigurnosnih mjera implementiranih na softverskoj razini informatičke opreme, poput operativnih sustava računala i mrežne opreme, baza podataka te aplikacija. Primjerice, mehanizam potvrde identiteta i autorizacije korisnika u poslovnim aplikacijama pripada u mjere logičke sigurnosti. Neprimjerene logičke kontrole pristupa mogu izložiti subjekte različitim prijetnjama putem kojih je moguće ostvariti neovlašteni pristup IS, primjerice poput:

- raznih oblika kibernetičkih napada,
- zlonamjernog djelovanja zaposlenika i drugih.

U svrhu smanjenja rizika proizašlih iz neprimjerenih logičkih kontrola pristupa, potrebno je osigurati:

- **postojanje primjerenih logičkih kontrola pristupa** operativnim sustavima računala i mrežne opreme, sistemskih i poslovnih aplikacija i servisa te drugim softverskim resursima IS putem kojih je omogućen pristup osjetljivim podacima te putem njih omogućiti pristup samo ovlaštenim osobama i to samo resursima za koje te osobe imaju odgovarajuća ovlaštenja pristupa sukladno poslovnim potrebama.
- **logičke kontrole pristupa informatičkoj opremi koja je privremeno bez nadzora,** primjerice obvezom zaključavanja korisničkog sučelja operativnog sustava računala prije napuštanja radnog mjesta od strane korisnika.

7.2. Korisnički računi i prava pristupa

Dodjela, izmjena i ukidanje korisničkih računa i prava pristupa integralni je dio većine sustava za logičku kontrolu pristupa. Dodjelom računa korisniku se omogućuje pristup jednom sustavu, primjerice operativnom sustavu računala ili poslovnoj aplikaciji, dok se dodjelom prava pristupa ovlaštenim korisnicima omogućuje pristup pojedinačnim resursima unutar tog sustava, primjerice samo određenom skupu podataka unutar aplikacije. Neprimjereno upravljanje korisničkim računima i pravima pristupa može znatno umanjiti učinkovitost mjera logičke kontrole pristupa. Stoga je potrebno:

- **Dodjelu, izmjenu i ukidanje korisničkih računa i prava pristupa provoditi na temelju dokumentirane poslovne potrebe.** Zahtjev za dodjelu, izmjenu ili ukidanje treba biti upućen od strane odgovorne osobe organizacijskoj jedinici kojoj pripada korisnik prema osobama odgovornima za odobravanje i provedbu operacija vezanih uz korisničke račune i prava pristupa. Zahtjev treba biti dokumentiran, primjerice upućen putem odgovarajuće aplikacije, elektroničke pošte ili za to predviđenog obrasca, te treba sadržavati sve informacije bitne za provedbu operacija dodjele, izmjene ili ukidanja.
- **Dodjelu korisničkih računa i prava pristupa provoditi temeljem minimalnih potrebnih prava za obavljanje radnih zadataka**.
- **Provoditi periodičku provjeru usklađenosti dodijeljenih korisničkih računa i prava pristupa s poslovnim potrebama.**
- **Svakom korisniku IS dodijeliti poseban korisnički račun** te u najvećoj mogućoj mjeri izbjegavati korištenje grupnih korisničkih računa. Nazivi korisničkih računa u sustavima se u svakom trenutku moraju moći identificirati sa stvarnim identitetom korisnika.

7.3. Korisnički računi s pravima povlaštenog pristupa

Korisnički računi s povlaštenim pravima pristupa su oni računi čija prava pristupa omogućavaju izmjenu sistemskih postavki IT. Prava povlaštenog pristupa trebaju imati samo oni korisnici čiji radni zadaci to opravdavaju, primjerice stručno osoblje koje održava IT. Zloupotrebom računa s pravima povlaštenog pristupa povećava se rizik od neovlaštenog pristupa i izmjene konfiguracija sustava, kroz djelovanje nekog oblika kibernetičke prijetnje ili zlonamjernih osoba. U svrhu smanjenja rizika proizašlih iz zlouporabe povlaštenih prava pristupa potrebno je provoditi mjere i postupke opisane u poglavlju 7.2. smjernica i za korisničke račune s pravima povlaštenog pristupa.

7.4. Upravljanje lozinkama

Lozinke u IS predstavljaju mehanizam potvrde korisničkog identiteta te su dio sustava logičkih kontrola pristupa. Lozinka se najčešće pojavljuje u obliku alfanumeričke fraze ili identifikacijskog broja kojeg korisnik mora unijeti prilikom prijave u sustav kako bi potvrdio svoj identitet. Neprimjereno upravljanje lozinkama može znatno umanjiti učinkovitost mjera logičke kontrole pristupa. Stoga je potrebno:

- **Identificirati i primijeniti minimalne standarde svojstava lozinki za pristup pojedinim resursima IS** sukladno vlastitoj procjeni rizika odnosno važnosti resursa kojima se pristupa. Neka svojstva lozinki mogu biti:
    - dužina,
    - rok trajanja,
    - složenost,
    - dopušteni broj unosa lozinke prije zaključavanja korisničkog računa i druga.
- **Čuvati tajnost lozinke.** Lozinku smije znati isključivo osoba koja njome potvrđuje svoj identitet.
- **Lozinke pamtiti, nikad ih zapisivati na papir ili u nezaštićene elektroničke datoteke .**
- **Izmijeniti lozinke na resursima IS koje su inicijalno postavljene od administratora sustava ili proizvođača opreme.**
- **Osigurati da su lozinke u sustavima pohranjene u nečitljivom obliku.** Kad korisnik unese lozinku u sustav, mehanizam potvrde identiteta uspoređuje unesenu lozinku s onom pohranjenom u sustavu. Takva lozinka mora biti pohranjena u nečitljivom obliku, primjerice kao ireverzibilni digitalni sažetak.
- **Pri definiranju lozinki izbjegavati korištenje riječi iz rječnika, osobne podatke ili druge fraze koje se mogu lako pogoditi ili povezati s korisnikom računa.**

8. Sigurnost računalnih mreža

8.1. Sigurnost računalnih mreža

Računalne mreže služe za međusobno povezivanje računala i drugih uređaja te predstavljaju komunikacijski kanal za razmjenu podataka elektroničkim putem. Računalne mreže koje služe za povezivanje računala i uređaja subjekta te im je pristup izvana ograničen nazivaju se privatne ili lokalne računalne mreže. U većini slučajeva lokalnim mrežama se vrši najveći dio prijenosa osjetljivih poslovnih podataka te je njima potrebno pružiti i najveću pozornost u kontekstu zaštite i sigurnosti. Neprimjereno zaštićene računalne mreže izložene su rizicima neovlaštenog pristupa i zlouporabe što može dovesti do narušavanja povjerljivosti, cjelovitosti i dostupnosti važnih poslovnih informacija.

U svrhu smanjenja rizika proizašlih iz neprimjerene zaštite računalnih mreža potrebno je:

- **Ograničiti pristup konfiguracijskim sučeljima mrežnih uređaja**, poput preklopnika i usmjerivača, na isključivo za to ovlaštene osobe,
- **Primjereno zaštititi računala i poslužiteljske servise subjekta kojima je omogućen pristup putem javnih mreža,** primjerice zaštititi poslužitelj internetske stranice primjenom vatrozida i drugih sustava ili sustava za detekciju neovlaštenog pristupa.
- **Računala i poslužiteljske servise kojima je omogućen pristup putem javnih mreža izdvojiti u mrežni segment odvojen od lokalne računalne mreže**. Primjer takvog sustava je poslužitelj internetske stranice. Takav poslužitelj je izložen zlonamjernom djelovanju osoba i malicioznog koda putem javnih mreža. U slučaju i da dođe do kompromitacije poslužitelja u takvim scenarijima, njegovo izdvajanje u poseban segment otežalo bi daljnji neovlašteni pristup lokalnoj mreži.
- **Primjereno zaštititi prijenos osjetljivih podataka putem javnih mreža,** primjerice kriptografskom zaštitom SSL/TLS komunikacijskog protokola.
- **Koristiti naprednu zaštitu bežičnih mreža**.

8.2. Udaljeni pristup

Udaljeni pristup podrazumijeva pristup lokalnoj mreži i korištenje IS subjekta s lokacije smještene izvan njegovih poslovnih prostora. Za dodjelu prava udaljenog pristupa vrijede iste preporuke kao i u poglavlju 7.2. Smjernica. Nadalje, u svrhu primjerene zaštite računalnih mreža pri udaljenom pristupu potrebno je:

- **Primjereno zaštititi podatke u prijenosu između udaljene lokacije i točke pristupa računalnoj mreži subjekta**.
- **Osigurati izradu operativnih i sistemskih zapisa o aktivnostima korisnika udaljenog pristupa.**

9. Sigurnost prijenosnih uređaja i medija za pohranu podataka

9.1. Sigurnost prijenosnih uređaja i medija za pohranu podataka

Prijenosni uređaji i mediji za pohranu podataka, poput prijenosnih računala, „pametnih“ telefona i drugih prijenosnih medija za pohranu podataka inherentno su izloženi povećanim rizicima otuđenja i gubitka zbog svoje prenosivosti.

U svrhu smanjenja rizika gubitka ili otuđenja opreme, a pri tome i mogućeg neovlaštenog pristupa osjetljivim podacima koji bi na njima mogli biti pohranjeni, potrebno je:

- **Koristiti tehnike kriptiranja povjerljivih podataka pohranjenih na prijenosnim uređajima i medijima za pohranu**.
- **Zaštititi pristup sučeljima operativnih sustava prijenosnih računala i „pametnih“ telefona metodama potvrde identiteta korisnika**, primjerice putem lozinke ili skeniranjem otiska prsta.
- **Omogućiti udaljeno brisanje podataka pohranjenih na „pametnim“ telefonima** u slučajevima njihovog gubitka ili otuđenja.

9.2. Otpis medija za pohranu podataka

Prilikom otpisa medija za pohranu podataka, primjerice tvrdih diskova unutar računala, USB medija ili magnetnih traka, potrebno je voditi računa o podacima koji su na njima pohranjeni. Prije promjene vlasnika opreme ili njezinog odlaganja na elektronički otpad potrebno je osigurati da su podaci obrisani na siguran način, primjerice upisivanjem novih podataka preko starih ili fizičkim oštećivanjem medija, kako bi se osiguralo da je neovlašteni pristup povjerljivim podacima onemogućen.

10. Upravljanje incidentima

Incidenti u kontekstu IS mogu se definirati kao nepredviđeni događaji i situacije koje mogu narušiti funkcionalnost i sigurnost IS. Primjereni proces upravljanja incidentima omogućuje pravovremenu prijavu, rješavanje i analizu incidenata u svrhu buduće prevencije, kako bi se minimizirao utjecaj incidenata na IS. U cilju primjerenog upravljanja incidentima, potrebno je:

- **Omogućiti korisnicima IS pravovremenu prijavu uočenih incidenata.**
- **Odrediti obveze i odgovornosti u zaprimanju, daljnjoj eskalaciji i rješavanju incidenata.**
- **Rješavati uočene incidente i primjenjivati mjere u prevenciji pojave incidenata u budućnosti.**

Sukladno vlastitoj procjeni rizika, subjekti mogu dodatno primijeniti sljedeće mjere:

- **Vođenje evidencije o prijavljenim incidentima,** koja bi sadrži ime osobe koja je prijavila incident, opis incidenta, ime osobe koja je preuzela rješavanje incidenta, način i status rješavanja i slično.

11. Upravljanje operativnim i sistemskim zapisima

Operativni i sistemski zapisi komponenti IT, primjerice aplikacija, baza podataka i operativnih sustava računala, generiraju se u svrhu bilježenja informacija o aktivnostima i događajima vezanima uz njih. Operativni i sistemski zapisi imaju ključnu ulogu u rekonstrukciji događaja vezanih uz komponente IT te u utvrđivanju individualne odgovornosti korisnika IS koji ih koriste. U cilju primjerenog upravljanja operativnim i sistemskim zapisima potrebno je:

- **Osigurati generiranje operativnih i sistemskih zapisa u svim važnim komponentama IT** u mjeri dovoljnoj za rekonstrukciju događaja i utvrđivanje individualne odgovornosti korisnika. Korisničko ime osobe koja je provela aktivnost, opis aktivnosti, naziv komponente IT i vrijeme događaja minimalni su podaci koji bi trebaju biti sadržani u većini zapisa.
- **Zaštititi operativne i sistemske zapise važnih komponenti IT od neovlaštenog pristupa.**
- **Izrađivati pričuvne kopije operativnih i sistemskih zapisa važnih komponenti IT.**
- **Osigurati točnost mjerenja vremena u komponentama IT koje generiraju operativne i sistemske zapise** kako bi se osigurala točnost podataka o vremenu nastanka događaja.

12. Zaštita od kibernetičkih prijetnji

Djelovanje kibernetičkih prijetnji može predstavljati značajnu prijetnju sigurnosti i funkcionalnosti IS. Razni oblici kibernetičkih napada se sve više koristi u svrhu otuđenja povjerljivih informacija i prisvajanja protupravne financijske dobiti od strane zlonamjernih osoba i skupina. U svrhu primjerene zaštite od kibernetičkih prijetnji i rizika potrebno je:

- **Osigurati primjerenu primjenu sustava zaštite komponenti IT od kibernetičkih prijetnji**, poput IDS, IPS sustava, antivirusnog i antispam softvera i drugo.
- **Osigurati ažurnost sustava za zaštitu komponenti IT od kibernetičkih prijetnji.**
- **Osigurati redovnu primjenu sigurnosnih ispravaka operativnih sustava i aplikacija.**
- **Osigurati primjerenu uporabu preglednika internetskih stranica i klijenata elektroničke pošte od strane korisnika IS**. Značajan udio kibernetičkih prijetnji npr malicioznog koda infiltrira se u IS uslijed otvaranja zaraženih priloga elektroničke pošte i otvaranja internetskih stranica koje sadrže maliciozni kod.

IV. PRIJELAZNE I ZAVRŠNE ODREDBE

Ove Smjernice se objavljuju na internetskoj stranici Hanfe te stupaju na snagu danom objave.

Stupanjem na snagu ovih Smjernica, prestaju važiti Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora od 24. listopada 2014.

KLASA: 011-01/22-07/02
URBROJ: 326-01-25-22-1
Zagreb, 21. prosinca, 2022.

PREDSJEDNIK UPRAVNOG VIJEĆA

dr. sc. Ante Žigman