SMJERNICE ZA OVLADAVANJE RIZIKOM INFORMACIJSKOG SUSTAVA U KREDITNIM UNIJAMA

STUDENI 2007.

HRVATSKA NARODNA BANKA

SADRŽAJ

1. Uvod

Hrvatska narodna banka uočila je potrebu da kreditne unije upozori na pitanja vezana uz rizik informacijskog sustava odnosno rizik koji proizlazi iz korištenja informacijskim sustavom. S obzirom na to da poslovanje kreditne unije ovisi i o informacijskom sustavu, potrebno je posvetiti pozornost ovladavanju rizikom informacijskog sustava kreditne unije kako bi se osiguralo pouzdano i sigurno poslovanje kreditne unije.

Cilj je *Smjernica za ovladavanje rizikom informacijskog sustava u kreditnim unijama* (u nastavku teksta: *Smjernice*) upoznati kreditne unije sa stavom Hrvatske narodne banke u svezi s postupcima koje bi kreditna unija trebala napraviti kako bi ovladala rizikom informacijskog sustava. *Smjernice* razrađuju područja koja su bitna za ovladavanje rizikom informacijskog sustava kreditne unije te daju prikaz očekivanja u skladu s kojima će Hrvatska narodna banka u izravnim nadzorima informacijskih sustava kreditnih unija obavljati procjenu stanja informacijskih sustava kreditnih unija te rizika informacijskog sustava kojem su kreditne unije izložene.

Pri provođenju izravnih nadzora informacijskih sustava kreditnih unija supervizori Hrvatske narodne banke uzet će u obzir sve objektivne razloge i činjenice koji su mogli utjecati na primjenu *Smjernica*, pri čemu se misli na čimbenike kao što su veličina i kompleksnost informacijskog sustava, veličina kreditne unije te udio na tržištu. Hrvatska narodna banka je pri sastavljanju ovih *Smjernica* uzela u obzir:

- specifičnosti poslovanja kreditnih unija s obzirom na poslove koje kreditna unija može obavljati prema Zakonu o kreditnim unijama ("Narodne novine", br. 141/2006.);
- organizacijska ograničenja kreditnih unija;
- kompleksnost informacijskih sustava kreditnih unija;
- pretpostavku da će informacijski sustavi kreditnih unija imati zadovoljavajuću razinu funkcionalnosti u smislu podrške poslovnim procesima kreditne unije;
- veličinu aktive kreditnih unija u odnosu na ukupnu aktivu bankovnog sustava.

Hrvatska narodna banka izdala je *Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika* (ožujak 2006.) *i Odluku o primjerenom upravljanju informacijskim sustavom* ("Narodne novine", br. 80/2007., kolovoz 2007.), koje se odnose na poslovanje banaka, stambenih štedionica i štednih banaka. Navedeni dokumenti mogu poslužiti kao dodatna pomoć pri ovladavanju rizikom informacijskog sustava (primjerice u *Smjernicama* se ne razrađuju zahtjevi u svezi s uspostavom procesa upravljanja rizikom i upravljanja kontinuitetom poslovanja, nego je naglasak na upravljanju podacima odnosno na tome kako osigurati da se podaci bitni za poslovanje kreditne unije ni u kojem trenutku ne kompromitiraju, izbrišu, izgube ili na drugi način nepovratno unište). Kreditne unije trebale bi poduzeti sve što je potrebno kako bi osigurale povjerljivost, integritet i raspoloživost informacija.

2. Definicije pojmova

U nastavku su navedene definicije nekih pojmova za potrebe *Smjernica*.

Softverske komponente (softverska imovina) uključuju aplikacijski softver, sistemski softver, baze podataka, softverske razvojne alate, uslužne programe te ostali softver.

Hardverske komponente (hardverska imovina) uključuju računala i računalnu opremu (stacionarna i prijenosna osobna računala, poslužitelje, monitore, tipkovnice, pisače i slično), komunikacijsku opremu (usmjernike, preklopnike, vatrozide i slično), medije za pohranu podataka (magnetne diskove, magnetne vrpce, optičke diskove i slično) te ostalu tehničku opremu koja podržava rad informacijskog sustava (uređaje za neprekidno napajanje električnom strujom, klimatizacijske uređaje i slično).

Informacijska imovina uključuje podatke u bazama podataka, datoteke s podacima, programski kôd, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, planove, interne akte i slično.

Informacijska tehnologija omogućuje automatizirano prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijska se tehnologija sastoji od softverskih i hardverskih komponenata.

Informacijski je **sustav** sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijski sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste.

Korisnici informacijskog sustava jesu sve osobe koje se koriste informacijskim sustavom (zaposlenici kreditne unije, zaposlenici pružatelja usluga, zaposlenici pravnih osoba koji se koriste informacijskim sustavom kreditne unije itd.).

Resursi informacijskog sustava uključuju informacijsku imovinu, softverske komponente i hardverske komponente.

Svojstva informacija i procesa:

- **Povjerljivost** je svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima.
- **Integritet** je svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.
- **Raspoloživost** je svojstvo informacija i procesa koje omogućuje pristup i upotrebljivost tih informacija i procesa, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta.

- **Autentičnost** je svojstvo koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest.
- **Neporecivost** je svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka).
- **Dokazivost** je svojstvo koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta.
- **Pouzdanost** je svojstvo dosljednoga, očekivanog ponašanja i rezultata.

Kontrole se dijele na upravljačke, logičke i fizičke:

- **Upravljačke kontrole** uključuju donošenje internih akata vezanih uz informacijski sustav i uspostavljanje odgovarajuće organizacijske strukture te osiguravaju primjenu internih akata vezanih uz informacijski sustav u cilju osiguravanja funkcionalnosti i sigurnosti informacijskog sustava.
- **Logičke kontrole** su kontrole implementirane na softverskim komponentama informacijskog sustava.
- **Fizičke kontrole** su kontrole koje štite resurse informacijskog sustava od neovlaštenoga fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja.

3. Upravljanje informacijskim sustavom

3.1. Uprava kreditne unije

Upravljanje informacijskim sustavom vrlo je važno u procesu donošenja poslovnih odluka. Kako bi kreditna unija primjereno upravljala informacijskim sustavom, uprava bi kreditne unije, između ostalog, trebala:

- biti upoznata s konceptima i aktivnostima vezanim uz informacijski sustav;
- uspostaviti adekvatnu organizacijsku strukturu;
- delegirati ovlasti prema uspostavljenoj organizacijskoj strukturi;
- definirati kriterije, načine i postupke izvješćivanja uprave;
- donijeti interne akte kojima se uređuje upravljanje informacijskim sustavom.

3.2. Interni akti

Donošenje i primjena internih akata vezanih uz informacijski sustav osnova su za uspostavljanje i održavanje upravljačkih kontrola koje bi trebale biti slojevite i hijerarhijski uspostavljene od najviše (strateške) razine prema najnižoj (operativnoj) razini. Kreditna bi unija trebala donijeti, dokumentirati, provoditi i održavati interne akte kako bi djelotvorno upravljala informacijskim sustavom. Internim aktima smatraju se odluke, politike, standardi, smjernice, procedure, upute i ostali dokumenti za čije je donošenje odgovorna uprava kreditne unije. Interne akte potrebno je integrirati u procese informacijskog sustava i svakodnevne aktivnosti zaposlenika. Nadalje, interni bi akti trebali biti usklađeni s propisima, standardima i pravilima struke.

Interni akti na najvišoj konceptualnoj ili hijerarhijskoj razini (primjerice politike) trebali bi obuhvatiti sva područja i aspekte informacijskog sustava kreditne unije, uključujući osobe, sustave i procese. Kreditna bi unija trebala procijeniti i odrediti koja je područja i aspekte informacijskog sustava potrebno razraditi detaljnijim internim aktima niže razine (primjerice uputama i procedurama) te definirati razinu detaljnosti razrade. Razina detaljnosti i obuhvat pojedinog internog akta ovise o njegovoj svrsi, namjeni, vrsti te o kompleksnosti informacijskog sustava.

3.3. Dokumentacija

Sve procese povezane s informacijskim sustavom potrebno je dokumentirati. Dokumentacija je korisna samo ako je točna, potpuna i ažurna, te bi je takvom trebalo i održavati. Pristup povjerljivoj dokumentaciji trebao bi biti ograničen, kako bi svaki zaposlenik mogao pristupiti samo dokumentima za koje je ovlašten. Važnu dokumentaciju trebalo bi pohraniti i na sigurnu udaljenu lokaciju te je periodično

ažurirati. Kreditna bi unija trebala zaposlenicima osigurati pristup dokumentaciji koja je povezana s njihovim poslovnim potrebama.

4. Izobrazba

Izobrazba, odnosno edukacija, kontinuirani je proces koji se mora neprekidno odvijati kako bi se osiguralo da znanja korisnika sustava prate promjene i u informacijskom sustavu i u njegovoj okolini. Spomenute promjene uključuju izmjene postojećih funkcija i sigurnosnih obilježja informacijskog sustava ili dodavanje novih kao i sve promjene izvan informacijskog sustava kreditne unije koje na njega mogu utjecati.

Većina štetnih (neplaniranih i neželjenih) događaja na informacijskim sustavima nastaje kao posljedica ljudskog djelovanja. Od navedenih štetnih događaja zaposlenici poslovnog subjekta uzrokuju kudikamo veći broj nego ostale osobe. Neplanirani i neželjeni događaji najčešće nastaju kao posljedica nenamjernih radnja (pogrešaka ili propusta) ili, rjeđe, kao posljedica namjernih radnja počinjenih s ciljem nanošenja štete informacijskom sustavu kreditne unije. Kako bi se navedeni događaji i njihovo štetno djelovanje sveli na prihvatljivu razinu, potrebno je primjereno educirati sve korisnike informacijskog sustava kreditne unije.

Posljedica primjerene izobrazbe bit će smanjivanje broja pogrešaka i propusta i ograničavanje njihova dosega te uočavanje i sprječavanje pokušaja narušavanja povjerljivosti, integriteta i raspoloživosti informacijskog sustava.

Edukacija bi trebala obuhvatiti sve osobe koje se koriste informacijskim sustavom kreditne unije. Izobrazba korisnika informacijskog sustava trebala bi omogućiti navedenim osobama djelotvorno obavljanje radnih zadataka uz istodobno svođenje neželjenih događaja na prihvatljivu razinu. Preciznije, ciljevi edukacije korisnika informacijskog sustava kreditne unije jesu:

- razviti i održavati znanja i vještine korisnika na primjerenoj razini kako bi oni mogli obavljati radne zadatke na djelotvoran i siguran način;
- upoznati korisnike s internim aktima (politikama, procedurama i ostalim postupcima kojih se navedeni korisnici moraju pridržavati) kako bi se točno ustanovili zadaci, okviri djelovanja i osobna odgovornost svakog korisnika;
- uspostaviti i unapređivati svijest o potrebi zaštite resursa informacijskog sustava;
- razviti i održavati znanja potrebna da bi se funkcionalnost i sigurnost informacijskog sustava zadržale na zadovoljavajućoj razini tijekom cijeloga životnog ciklusa informacijskog sustava.

Kvalitetno planirana i provedena izobrazba povećat će produktivnost i iskorištenost postojećih resursa te omogućiti podizanje razine sigurnosti cjelokupnoga informacijskog sustava kreditne unije.

Izobrazbu je moguće provoditi na različite načine, od najjednostavnijih poput distribucije pisane dokumentacije do kompleksnih i dugotrajnih usavršavanja. Opseg, detaljnost, trajanje i način provođenja edukacije trebaju biti u skladu s obilježjima ciljane grupe odnosno ciljanih korisnika te s opsežnosti i kompleksnosti tematike. Pri

određivanju obilježja ciljanih korisnika potrebno je uzeti u obzir poslovne funkcije koje navedeni korisnici obavljaju, njihovo predznanje o predmetu edukacije te općenito poznavanje funkcioniranja informacijskih sustava. Korisnike je potrebno educirati do razine detaljnosti koju zahtijevaju njihovi poslovni zadaci. Posebno su za kreditnu uniju važne izobrazba korisnika o upotrebi aplikacija kojima se podržavaju poslovni procesi te provedba programa podizanja razine svijesti o sigurnosti informacijskog sustava (engl. *security awareness*).

Program podizanja razine svijesti o sigurnosti informacijskog sustava provodi se radi usmjeravanja korisnika informacijskog sustava na prepoznavanje sigurnosnih pitanja i radi edukacije o primjerenom postupanju u vezi sa sigurnosti odnosno očekivanim pravilima ponašanja. Navedeni program trebao bi se usredotočiti na dobre sigurnosne prakse te bi svim korisnicima trebao dati kratke, jasne i primjenjive preporuke. Primjer teme koju bi trebalo obraditi u sklopu programa podizanja razine svijesti o sigurnosti informacijskog sustava jest zaštita od malicioznoga programskoga kôda. U sklopu te teme korisnicima se primjerice može izložiti i ukratko objasniti sljedeće:

- što je maliciozni programski kôd (npr. što je virus, trojanski konj, crv i slično);
- što se može dogoditi ako se računalo "zarazi" malicioznim programskim kôdom;
- koje je aktivnosti potrebno poduzeti kako bi se zaštitilo od malicioznoga programskoga kôda;
- što treba učiniti ako se uoči prisutnost malicioznoga programskoga kôda na računalu.

Primjeri ostalih tema koje bi trebalo obraditi u sklopu programa podizanja razine svijesti o sigurnosti informacijskog sustava jesu:

- postupanje u skladu s načelima dodjele najmanjih mogućih ovlasti potrebnih za djelotovorno obavljanje poslovnih zadataka te segregacije dužnosti
- zaštita poslovnih podataka koji se pohranjuju, prenose ili obrađuju pomoću informacijske tehnologije
- upravljanje korisničko-identifikacijskim oznakama i zaporkama, uključujući njihovu izradu, učestalost promjene te potrebu za očuvanjem povjerljivosti
- postupanje s neželjenim porukama elektroničke pošte (engl. *spam*)
- postupanje s porukama elektroničke pošte dobivenima od nepoznatog pošiljatelja te s nepoznatim prilozima (engl. *attachment*)
- upotreba interneta, s naglaskom na dopuštene i zabranjene aktivnosti te preporučena pravila upotrebe
- prepoznavanje socijalnog inženjeringa i odgovor na socijalni inženjering (engl. *social engineering*)
- prepoznavanje incidentnih situacija i postupanje u takvim situacijama
- pravodobna primjena programskih ispravaka.

Važno je naglasiti da bi svi korisnici informacijskog sustava unutar organizacije morali biti uključeni u provedbu programa podizanja razine svijesti o sigurnosti informacijskog sustava.

5. Eksternalizacija

Eksternalizacija (odnosno izdvajanje dijela poslovanja) jest korištenje usluga koje čine sastavni dio poslovnih procesa kreditne unije, a koje na temelju ugovora kreditnoj uniji pružaju pružatelji usluga na kontinuiranoj osnovi i kojima se podržavaju poslovi kreditne unije u skladu s člankom 3. Zakona o kreditnim unijama ("Narodne novine", br. 141/2006.).

Eksternalizacija aktivnosti vezanih uz informacijski sustav kreditne unije smatra se eksternalizacijom (dijela) informacijskog sustava.

Postupak nabave robe i ugovor(i) o nabavi robe (primjerice o nabavi informacijske imovine te hardverskih i softverskih komponenata) ne smatraju se eksternalizacijom.

Rizik u poslovanju postoji bez obzira na to hoće li kreditne unije same obavljati aktivnosti vezane uz informacijski sustav ili će se koristiti uslugama pružatelja usluga. Pri razmatranju svrhovitosti eksternalizacije aktivnosti vezanih uz informacijski sustav kreditne unije trebaju:

- biti svjesne rizika vezanog uz eksternalizaciju tih aktivnosti;
- osigurati da odnos između kreditne unije i pružatelja usluga bude prihvatljiv sa stajališta rizika i u skladu s poslovnim ciljevima kreditne unije;
- regulirati sve elemente i postupke koji se odnose na eksternalizaciju aktivnosti vezanih uz informacijski sustav svojim internim aktima.

Predmetom eksternalizacije mogu biti različite aktivnosti vezane uz informacijski sustav, primjerice:

- usluge održavanja hardvera
- usluge obrade podataka
- usluge razvoja poslovnih aplikacija
- usluge održavanja poslovnih aplikacija
- usluge upravljanja operacijskim sustavima i usluge održavanja tih sustava
- usluge upravljanja telekomunikacijskim mrežama i održavanja tih mreža
- usluge upravljanja bazama podataka i održavanja tih baza
- usluge upravljanja sigurnosnom infrastrukturom i održavanja te infrastrukture
- usluge upravljanja internetskim stranicama i održavanja tih stranica.

Upravljanje rizikom eksternalizacije uključuje:

- procjenu rizika vezanog uz eksternalizaciju
- detaljnu analizu pružatelja usluga pri njegovu odabiru
- definiranje sadržaja ugovora s pružateljem usluga
- osiguravanje kontinuiranog nadzora pružanja usluga u skladu s ugovornim obvezama
- osiguravanje neograničenoga i svakodobnog pristupa informacijama povezanim s uslugom koja je predmet eksternalizacije.

5.1. Procjena rizika vezanog uz eksternalizaciju

Prije sklapanja ugovora s pružateljem usluga kreditna bi unija trebala procijeniti rizik eksternalizacije i mogućnosti kontrole tog rizika. Pri toj procjeni potrebno je osobitu pozornost posvetiti procjeni rizika koji bi mogli utjecati na financijske rezultate, financijsku poziciju, kontinuitet poslovanja ili reputaciju kreditne unije. Za svaki slučaj eksternalizacije (dijela) poslovnih procesa kreditna unija treba procijeniti rizik eksternalizacije. Pri procjeni rizika vezanog uz eksternalizaciju aktivnosti vezanih uz informacijski sustav kreditna bi unija trebala procijeniti sljedeće:

- mogućnost pružatelja usluga da osigura pružanje usluga u skladu sa strateškim ciljevima i poslovnim potrebama kreditne unije;
- pouzdanost, ekonomsku održivost i sposobnost pružatelja usluga;
- način na koji će kreditna unija nadzirati pružanje usluga;
- adekvatnost stručnog osoblja u kreditnoj uniji, odnosno je li ono u stanju provoditi kvalitetan nadzor nad pružateljem usluga i na adekvatan način upravljati odnosom s pružateljem usluga;
- važnost, opseg i složenost (dijelova) poslovnih procesa koji su predmet eksternalizacije.

5.2. Analiza pružatelja usluga pri njegovu odabiru

Nakon što je obavljena procjena rizika eksternalizacije kreditna bi unija trebala provesti analizu pružatelja usluga kako bi se utvrdilo može li pružatelj usluga (financijski i operativno) pružiti kreditnoj uniji zahtijevane usluge. Odabir sposobnoga i kvalitetnog pružatelja usluga osobito je važan kako bi se smanjio rizik eksternalizacije. Ovisno o utvrđenim rizicima kreditna bi unija trebala pri analizi pružatelja usluga uzeti u obzir sljedeće:

- iskustvo pružatelja usluga i mogućnosti pružanja potrebnih usluga radi ispunjavanja postojećih i očekivanih potreba kreditne unije;
- reputaciju i tržišni udio pružatelja usluga;
- eventualne podizvođače pružatelja usluga koji će pružati podršku pružatelju usluga u ispunjavanju ugovornih obveza prema kreditnoj uniji;
- eventualnu potrebu za dodatnim sustavima, konverzijama podataka i uslugama;
- sposobnost pružatelja usluga da na odgovarajući način postupi u slučaju privremene nemogućnosti pružanja usluga iz bilo kojeg razloga;
- stručnu osposobljenost odgovornih osoba koje će biti određene za pružanje podrške kreditnoj uniji;
- lokaciju pružanja usluga kako bi se utvrdili uvjeti pod kojima pružatelj usluga djeluje i pruža svoje usluge;
- revizorska i posljednja financijska izvješća pružatelja usluga;

- mogućnost neograničenog i svakodobnog pristupa svojim informacijama;
- poznavanje propisa relevantnih za pružanje usluga koje su predmet eksternalizacije.

5.3. Definiranje sadržaja ugovora s pružateljem usluga

U ugovorima između kreditne unije i pružatelja usluga treba definirati poslovne potrebe kreditne unije te regulirati čimbenike rizika identificirane pri procjeni rizika eksternalizacije i analize pružatelja usluga.

Ugovori trebaju biti u pisanom obliku, jasno sastavljeni i dovoljno detaljni kako bi osigurali ispunjavanje preuzetih obveza koje se odnose na pružanje usluga. Isto tako, ugovori trebaju jasno definirati sve relevantne pojmove, uvjete, prava i obveze te odgovornosti ugovornih strana. Pri definiranju sadržaja ugovora s pružateljima usluga kreditna bi unija trebala uzeti u obzir sljedeće čimbenike:

- detaljan opis usluga koje su predmet ugovora te način ispunjavanja ugovornih obveza;
- odgovornost za štetu u slučaju povrede ugovornih obveza;
- obvezu čuvanja povjerljivih podataka;
- detaljan opis prava i obveza ugovornih strana za slučaj prestanka ugovora, i to na način koji će osigurati dostupnost podataka koji su u vlasništvu kreditne unije, a predmet su eksternalizacije;
- pravo kreditne unije na pristup informacijama i vlasništvo nad informacijama;
- način na koji će kreditna unija obavljati nadzor nad pružateljem usluga;
- osigurati zaposlenicima Hrvatske narodne banke izravni nadzor djelatnosti i poslova u svezi s kojima Hrvatska narodna banka obavlja nadzor;
- osigurati zaposlenicima Hrvatske narodne banke fizički pristup resursima pružatelja usluga koji su neophodni za izvršavanje usluga koje su predmet ugovora;
- odgovornost pružatelja usluga za neobavljene, nepravodobne i neispravne transakcije i ostale ugovorene aktivnosti;
- identifikaciju ključnih kontrola, vremena odgovora na incidente, procedura i stupnjeva eskalacije u slučaju pojave nepredviđenih događaja, pokrivenosti osiguranjem, mogućnosti oporavka te drugih mjera upravljanja rizicima koje bi pružatelj usluga trebao primijeniti;
- osigurati uvid u financijska izvješća, izvješća unutarnje i vanjske revizije, kao i u ostala izvješća vezana uz poslovanje pružatelja usluga, a koja bi mogla biti relevantna za kreditnu uniju.

5.4. Osiguravanje kontinuiranog nadzora pružanja usluga u skladu s ugovornim obvezama

Nakon sklapanja ugovora s pružateljem usluga kreditna bi unija trebala uvesti adekvatan sustav nadzora i kontinuirano ga provoditi kako bi kontrolirala način pružanja usluga i kvalitetu pruženih usluga. Isto tako, kreditna unija treba utvrditi je li pružatelj usluga implementirao i primjenjuje li kontinuirano adekvatne kontrole vezane uz pružanje usluga koje su predmet ugovora. Kontrole trebaju biti barem jednake kontrolama koje bi bile primijenjene kad bi se dotične aktivnosti obavljale u kreditnoj uniji.

Kreditna unija treba osigurati kvalitetan nadzor nad pružateljem usluga i na adekvatan način upravljati odnosom s pružateljem usluga.

Kontinuirani nadzor pružanja usluga u skladu s ugovornim obvezama treba obuhvaćati barem sljedeće:

- praćenje i analiziranje kvalitete obavljanja usluga;
- praćenje svih činjenica i okolnosti koje mogu utjecati na potrebu da se izmijeni ugovor;
- praćenje i analiziranje financijskog stanja te priljeva i odljeva kadrova kod pružatelja usluga kako bi se na vrijeme uočile financijske poteškoće i izbjegli rizici za kreditnu uniju koji proizlaze iz nemogućnosti pružanja ugovorenih usluga (npr. BON-1, BON-2, dostupna financijska izvješća potvrđena od ovlaštenih revizora).

5.5. Osiguravanje neograničenoga i svakodobnog pristupa podacima

Kreditnoj uniji mora biti osiguran neograničen i svakodobni pristup podacima koji su predmet eksternalizacije ili su na bilo koji način povezani s eksternalizacijom (dijela) poslovnih procesa. Isto tako, kreditne bi unije trebale imati adekvatan plan kako bi se osigurao kontinuirani pristup podacima u slučaju neočekivanog prekida ili ograničenja pružanja usluga od strane pružatelja usluga.

6. Upravljanje kontrolama pristupa

Kontrole pristupa omogućuju provođenje radnja nad resursima informacijskog sustava (primjerice korištenje, mijenjanje, pregled) u skladu s dodijeljenim ovlastima. Pristup se može definirati kao svojstvo koje omogućuje obavljanje različitih radnja na informacijskom sustavu. Kontrolama pristupa eksplicitno se omogućava, ograničava ili zabranjuje pristup resursima informacijskog sustava, i to korištenjem pojedine kontrole ili kombinacijom upravljačkih, logičkih i fizičkih kontrola. Proces kontrole pristupa obuhvaća uvođenje niza pojedinačnih kontrola pristupa. Cilj uvođenja kontrola pristupa jest sprječavanje neovlaštenog pristupa resursima informacijskog sustava. Pri implementaciji kontrola pristupa potrebno je uzeti u obzir sigurnosne zahtjeve, zahtjeve poslovnih procesa i jednostavnost korištenja za korisnike.

Kreditna unija trebala bi kontrolirati pristup resursima informacijskog sustava primjenjujući kriterije identiteta i funkcije korisnika informacijskog sustava. Svakog korisnika informacijskog sustava potrebno je identificirati, a identitet korisnika mora biti jedinstven kako bi se mogle utvrditi ovlasti i odgovornosti svakog korisnika. Pristup informacijama mora biti kontroliran na temelju dodijeljenih poslova i dužnosti u skladu s načelima podjele poslova i segregacije dužnosti. Navedeno uključuje određivanje radnja koje se mogu obavljati nad resursima informacijskog sustava (primjerice pravo čitanja, pisanja, izvršavanja i brisanja).

6.1. Upravljanje korisničkim pravima

Cilj upravljanja pravima pristupa jest identificirati i ograničiti pristup pojedinom resursu na minimalnu razinu dovoljnu za djelotvorno obavljanje radnih zadataka. Logička prava pristupa definiraju se pomoću korisničkih računa. Korisnički račun najčešće je povezan s jednom osobom (korisnikom informacijskog sustava) te sadrži informacije o pravima pristupa tog korisnika resursima informacijskog sustava (primjerice prava pristupa datotekama, tablicama s podacima i samim podacima, prava provođenja aktivnosti i slično). Korisničkim računom u smislu ovog dokumenta ne smatra se knjigovodstveni račun ni račun partije.

Upravljanje korisničkim pravima sastoji se od sljedećih procesa:

- **Evidentiranje.** Podrazumijeva dodavanje novih korisnika informacijskog sustava. Ovim procesom utvrđuje se identitet korisnika te određuju informacije i sustavi potrebni za obavljanje radnih zadataka u skladu s opisom radnoga mjesta. Primjeri su procesa evidentiranja otvaranje korisničkog računa u aplikaciji, bazi podataka ili na operacijskom sustavu.
- **Autorizacija.** Podrazumijeva dodjelu prava pristupa korisnika informacijskom sustavu kreditne unije. Navedeno obuhvaća dodavanje, brisanje ili modificiranje dodijeljenih prava pristupa operacijskim sustavima, bazama podataka,

aplikacijama i specifičnim vrstama informacija. Postupak dodjele prava pristupa treba biti formaliziran te sva prava trebaju odobriti ovlaštene osobe. Primjer je procesa autorizacije dodjela prava za rad u aplikaciji određenom korisniku od strane ovlaštene osobe te postavljanje tih prava u aplikaciji od strane administratora aplikacije.

- **Identifikacija i autentifikacija.** Podrazumijeva identifikaciju korisnika i potvrdu njegova identiteta prilikom prijave i tijekom provođenja radnja na informacijskom sustavu. Identifikacija i autentifikacija se provode prilikom prijave korisnika u aplikaciju, na bazu podataka ili na operacijski sustav, pri korištenju magnetske kartice za ulaz u sistemske prostorije i slično.
- **Nadzor.** Obuhvaća praćenje, izmjenu i revidiranje prava pristupa korisnika informacijskog sustava.

Procesi evidentiranja i autorizacije često se provode zajedno.

Kreditna bi unija trebala uspostaviti djelotvoran proces upravljanja korisničkim pravima pristupa. Navedeni proces trebao bi uključiti sljedeće kontrole:

- Dodjeljivanje korisnicima prava pristupa informacijskom sustavu koja su strogo ograničena samo na prava potrebna za obavljanje redovnih poslovnih zadataka. Primjerice:
    - Zaposlenici koji se u skladu sa svojim radnim zadacima samo koriste aplikacijama ne bi trebali imati povlaštena prava pristupa resursima informacijskog sustava, odnosno ne bi smjeli biti administratori baza podataka, operacijskih sustava, mrežne opreme i slično.
    - Zaposlenici čiji radni zadaci primjerice uključuju unos zahtjeva za dodjelu kredita u aplikaciju, ali ne i odobravanje kredita, ne bi smjeli imati prava pristupa aplikaciji koja omogućuje odobravanje kredita.
    - Osobe koje (u skladu s dodijeljenim radnim zadacima) održavaju operacijski sustav ili mrežnu opremu, a ne i bazu podataka, ne bi smjele imati administratorska prava pristupa bazi podataka.
- Ažuriranje prava pristupa. Prava pristupa morala bi uvijek odgovarati dodijeljenim radnim zadacima. Primjerice:
    - Svim zaposlenicima koji napuštaju organizaciju (zbog prekida radnog odnosa, izvanrednog otkaza i sl.) potrebno je pravodobno ukinuti prava pristupa resursima informacijskog sustava, uključujući aplikacije, baze podataka, operacijske sustave, mrežnu opremu itd.
    - Svim zaposlenicima koji mijenjaju radno mjesto ili kojima se mijenja opis radnog mjesta potrebno je pravodobno uskladiti prava pristupa resursima informacijskog sustava s novim radnim zadacima.
    - U slučaju prekida ugovornog odnosa s pružateljem usluga koji je održavao dio informacijskog sustava kreditne unije potrebno je pravodobno ukinuti sva prava pristupa informacijskom sustavu kreditne unije koja su imali zaposlenici pružatelja usluga.
- Periodično pregledavanje korisničkih prava pristupa. Odgovorne bi osobe periodično (primjerice svaka tri mjeseca ili svakih šest mjeseci) trebale

pregledavati prava pristupa svih korisnika informacijskog sustava, usporediti ih s radnim zadacima tih korisnika te, ukoliko je potrebno, prilagoditi ih. Navedeno uključuje pristup aplikacijama, bazama podataka, operacijskim sustavima, mrežnoj opremi i slično.

6.2. Identifikacija i autentifikacija

Identifikacija i autentifikacija ključne su komponente u izgradnji sigurnosti informacijskog sustava jer su osnova za mnoge vrste kontrola pristupa i utvrđivanja odgovornosti korisnika (dokazivost, neporecivost). Utvrđivanje odgovornosti korisnika zahtijeva povezivanje aktivnosti na informacijskom sustavu s točno određenim osobama, procesima ili sustavima te je u tu svrhu potrebno da ih informacijski sustav identificira i autentificira.

Identifikacija je proces kojim korisnik predočava informacijskom sustavu zahtijevani identitet. Identifikacija na informacijskim sustavima najčešće se provodi pomoću jedinstvene korisničko-identifikacijske oznake (engl. *User ID*). Pri upotrebi navedene oznake potrebno je obratiti posebnu pozornost na sljedeće:

- **Jedinstvenu identifikaciju.** Potrebno je osigurati jedinstvenu identifikaciju svakom korisniku informacijskog sustava. Sve grupne korisničke račune koji već postoje na informacijskom sustavu potrebno je onemogućiti ukoliko je to moguće.
- **Upravljanje jedinstvenim korisničko-identifikacijskim oznakama.** Ovlasti za rad na sustavu potrebno je pratiti i ažurirati kako bi pratile promjene u organizaciji (primjerice promjenu radnog mjesta, zapošljavanje, prekid radnog odnosa). Kako bi se omogućilo praćenje povijesnih aktivnosti korisnika, potrebno je procijeniti potrebu za čuvanjem korisničko-identifikacijske oznake i nakon ukidanja korisnikovih ovlasti (primjerice administratori sustava mogu umjesto brisanja određene korisničko-identifikacijske oznake samo onemogućiti prijavu u sustav pomoću te oznake; tako će se i u budućnosti moći pregledati koje je radnje proveo korisnik koji se koristio tom korisničko-identifikacijskom oznakom).
- **Neaktivne jedinstvene korisničko-identifikacijske oznake.** Korisnike koji su u određenom duljem razdoblju neaktivni na pojedinom resursu informacijskog sustava (primjerice 3 mjeseca), treba analizirati i prema procjeni dezaktivirati njihove oznake i ukinuti ovlasti.
- **Uzajamnu povezanost aktivnosti i korisnika.** Informacijski sustav treba osigurati praćenje identiteta svih korisnika i biti sposoban povezati aktivnosti s točno određenim korisnicima. Sve radnje povezane s financijskim podacima (primjerice uplate i isplate, isplate kredita, obračune kamata, korištenje tehnike storna i slično), promjene matičnih podataka (primjerice unos i promjenu podataka o članovima kreditne unije) te ostale važne poslovne aktivnosti (primjerice otvaranje i zatvaranje kredita, depozita i jamstava, odobravanje kredita i slično) kojima je podrška informacijski sustav, trebalo bi biti moguće

jednoznačno povezati s korisnikom informacijskog sustava koji je te aktivnosti proveo.

Autentifikacija je proces kojim se potvrđuje korisnički identitet koji zahtijeva pristup informacijskom sustavu. Postoje tri načina utvrđivanja neospornosti korisničkog identiteta koji se mogu primjenjivati samostalno ili u kombinaciji:

- Nešto što samo korisnik zna (primjerice zaporka, PIN, kriptografski ključ). Mogućnost autentifikacije korisnika ovisi o očuvanju tajnosti autentifikacijskih podataka, odnosno korisnik ni na koji način ne bi smio omogućiti drugim osobama pristup tim podacima.
- Nešto što samo korisnik posjeduje (primjerice "token", magnetska kartica, "pametna kartica"). Mogućnost autentifikacije korisnika ovisi o posjedovanju autentifikacijskog uređaja, odnosno korisnik ne bi smio omogućiti drugim osobama da pristupe tom uređaju.
- Nešto što korisnik jest (primjerice biometrijske metode kao što su otisak prsta, skeniranje rožnice, prepoznavanje glasa).

Dobra pravila o upravljanju korisničkim pravima pristupa uključuju sljedeće:

- **Autentificiranje korisnika.** Informacijski sustav kreditne unije trebao bi biti takav da od korisnika zahtijeva da potvrdi svoj identitet na informacijskom sustavu.
- **Ograničen pristup autentifikacijskim oznakama.** Autentifikacijske oznake trebaju biti adekvatno zaštićene (primjerice primjenom rigoroznih kontrola pristupa tim oznakama i jednosmjernim kriptiranjem) kako bi se spriječilo da neovlašteni korisnici dođu u posjed navedenih oznaka.
- **Siguran prijenos autentifikacijskih oznaka.** Kreditna bi unija trebala adekvatno zaštititi autentifikacijske oznake pri njihovu prijenosu javno dostupnim (primjerice internet) ili privatnim telekomunikacijskim mrežama. Primjer je mehanizma zaštite enkripcija navedenih podataka.
- **Ograničiti broj pokušaja pristupa.** Kreditna bi unija trebala ograničiti broj neuspjelih pokušaja pristupa, odnosno onemogućiti upotrebu korisničko-identifikacijske oznake nakon određenog broja neuspjelih pokušaja pristupa resursima informacijskog sustava.
- **Zaštita autentifikacijskih oznaka pri unošenju.** Kreditna bi unija trebala adekvatno zaštititi autentifikacijske oznake od kompromitiranja pri unosu u informacijski sustav (primjerice skrivanje odnosno neprikazivanje znakova od kojih se sastoji zaporka pri unosu zaporke).
- **Upravljanje autentifikacijskim oznakama.** Kreditna bi unija trebala adekvatno upravljati autentifikacijskim oznakama (primjerice definirati postupke za aktivaciju autentifikacijskih oznaka i dezaktivaciju izgubljenih i ukradenih oznaka).

6.3. Upravljanje zaporkama

Zaporke su najčešće upotrebljavan mehanizam autentifikacije korisnika. Međutim, zbog neprimjerenih navika korisnika informacijskog sustava one su i jedan od najslabijih mehanizama autentifikacije. Neprimjerene navike korisnika informacijskog sustava uključuju odavanje zaporke drugim osobama, neadekvatnu pohranu zaporka (primjerice zapisivanje zaporke pokraj računala) i upotrebu neprimjerenih zaporka (primjerice jednostavne zaporke koju je moguće pogoditi ili kratke zaporke). Primjereno upravljanje zaporkama može uvelike unaprijediti sigurnost informacijskog sustava. Kreditna bi unija trebala postići primjerenu razinu zaštite zaporka implementacijom odgovarajućih upravljačkih, logičkih i fizičkih kontrola.

Pri upravljanju zaporkama kreditna bi unija trebala uzeti u obzir barem sljedeće:

- Sve zaporke moraju biti povjerljive. Korisnici ne bi smjeli odavati zaporke drugim osobama (čak ni korisnicima s povlaštenim pravima pristupa informacijskom sustavu).
- Zaporke ne bi smjele biti predvidljive. Primjeri predvidljivih zaporka jesu:
    - Zaporke koje se sastoje samo od jedne riječi koja ima poznato značenje te ju je moguće pronaći u rječniku.
    - Zaporke koje sadrže informacije koje je moguće jednostavno povezati s vlasnikom korisničkog računa (primjerice datum rođenja, imena djece, supružnika ili prijatelja, marke automobila, imena kućnih ljubimaca).
    - Nizovi znakova na tastaturi kao što su "abcdefgh", "qwertzu", "987654321" i slično.
- Zaporka ili pravilo prema kojem je kreirana trebali bi biti jednostavni za pamćenje kako bi se smanjila vjerojatnost da će korisnik zaboraviti ili zapisati zaporku.
- Zaporke ne smiju biti pohranjene ni prikazane u čitljivom (nekriptiranom) obliku izvan adekvatno osigurane okoline (primjerice sefa). Primjeri loših praksa rukovanja zaporkama jesu zapisivanje zaporke pokraj računala, zapisivanje zaporke u čitljivom obliku u porukama elektroničke pošte i slično.
- Potrebno je definirati razdoblje nakon kojega se zaporka mora izmijeniti (primjerice svakih 30 dana ili svakih 45 dana) te onemogućiti višekratnu upotrebu iste zaporke.
- Zaporke je potrebno izmijeniti ukoliko se pojavi i najmanja sumnja da su njihova povjerljivost ili integritet narušeni.
- Potrebno je propisati načine kreiranja zaporka koji će biti u skladu s dobrim praksama i ograničenjima sustava za autentifikaciju te uključivati propisivanje:
    - Najmanje dopuštene duljine zaporka. Zaporke bi, u skladu s dobrim praksama, trebale imati duljinu od barem 8 znakova. Općenito govoreći, duljina je zaporke jedno od najboljih jamstava očuvanja povjerljivosti odnosno tajnosti te zaporke.
    - Obavezne uporabe što šireg znakovnog skupa. Svaka zaporka trebala bi se sastojati od barem dva tipa znakova (različiti tipovi znakova uključuju slova, brojke i specijalne znakove).

    - Nemogućnosti upotrebe tri ili više uzastopnih identičnih simbola u zaporki.
- Pri prvoj upotrebi potrebno je izmijeniti sve prvobitne (inicijalne) i standardne zaporke, kao i ostale zaporke koje su zadali proizvođači i dobavljači informacijske opreme ili pružatelji usluga, a pomoću kojih se pristupa resursima kreditne unije. Ukoliko inicijalna zaporka ne postoji, odnosno ako je prazna, treba je zadati. Primjeri korisničkih računa čije inicijalne zaporke treba promijeniti jesu:
    - korisnički računi *Administrator* i *Guest* na operacijskom sustavu *Microsoft Windows*;
    - korisnički račun *root* na operacijskim sustavima UNIX i Linux;
    - inicijalne zaporke korisničkih računa *SYS*, *SYSTEM, SCOTT* itd. na bazama podataka Oracle.
- Mogućnost autentifikacije pomoću određene zaporke potrebno je spriječiti ako korisnik više puta uzastopno pogriješi pri unosu te zaporke.

U nastavku su navedene neke preporuke za izradu kvalitetnih zaporka pomoću jednostavnih pravila koja olakšavaju i pamćenje zaporka:

- Jednostavna sintaktička pravila:
    - Kombinacija velikih i malih slova prema nekom jednostavnom pravilu. Primjerice:
        - promjena riječi "eventualno" u "eVeNtUaLnO"
        - promjena riječi "dinosaurus" u "dinOSAurUS".
    - Zamjena nekih slova brojkama ili specijalnim znakovima. Primjerice:
        - promjena riječi "investicija" u "1nvest1c1ja"
        - promjena riječi "omotnica" u "0m0tn&ca".
- Složenije smjernice vezane uz konstrukciju zaporke:
    - Stvaranje proizvoljnih akronima nekih poznatih fraza. Primjerice:
        - promjena izraza "vrijeme nikoga ne čeka" u "vriniknecek".
    - Komponiranje jednostavnih nizova slova i brojaka u jedan kompleksan niz. Primjerice:
        - spajanje niza "123456789" i "smjernice" u "s1m2j3e4r5n6i7c8e9"
        - spajanje niza "88888888" i "osmica" u "8888osm8888ica"
        - kombiniranje znakova "*" i "#" te riječi "ovan" u "o**#v**#a**#n**#".
    - Upotreba logičkih izraza. Primjerice:
        - upotreba matematičkih operacija: "1+2+3+4+5=15" ili "pet+sedam=dvanaest".
    - Povezivanje više riječi odnosno "tajnih rečenica" (engl. *passphrase*). Primjerice:
        - pretvaranje rečenice "ovo je složena rečenica za zaporku" u "ovojeslozenarecenicazazaporku".

Preporučuje se i primjena više pravila istodobno, posebice ako se rabe jednostavna sintaktička pravila.

6.4. Povlašteni pristup

Povlašteni pristup resursima informacijskog sustava (engl. *administrative access* odnosno administratorski pristup) jest onaj pristup resursima informacijskog sustava koji je omogućen korisnicima informacijskog sustava koji imaju velike ovlasti koje im omogućuju zaobilaženje ugrađenih logičkih kontrola. Primjeri korisnika s povlaštenim pravima pristupa informacijskom sustavu jesu administratori aplikacija, administratori baza podataka, administratori operacijskih sustava te administratori mrežne opreme. Ukoliko je moguće, trebalo bi uspostaviti segregaciju dužnosti između korisnika koji imaju povlaštena prava pristupa resursima informacijskog sustava. Primjerice osobe koje provode administraciju baza podataka, ne bi trebale provoditi administraciju operacijskih sustava, mrežne opreme i aplikacija. Posebnu pozornost trebalo bi posvetiti nadzoru aktivnosti zaposlenika pružatelja usluga koji imaju prava povlaštenog pristupa informacijskom sustavu (primjerice ako je kreditna unija eksternalizirala održavanje aplikacija, baza podataka, operacijskih sustava ili mrežne opreme).

Dobre prakse kontrole povlaštenog pristupa uključuju:

- Identificiranje svih osoba, procesa i sustava s povlaštenim pravima pristupa. Kreditna bi unija morala identificirati sve osobe koje imaju prava pristupa bilo kojem resursu informacijskog sustava kreditne unije.
- Uspostavu formalnog sustava dodjele prava povlaštenog pristupa.
- Korištenje povlaštenim pristupom isključivo za radnje koje se ne mogu obaviti pomoću pristupa s manjim pravima (primjerice u slučaju nemogućnosti provođenja segregacije dužnosti neki zaposlenici kreditne unije mogu biti korisnici poslovnih aplikacija, ali i administratori dijela sustava). Te bi osobe u svakodnevnom radu pri služenju poslovnim aplikacijama trebale upotrebljavati korisničke račune bez povlaštenih prava pristupa. Korisničkim računima s povlaštenim pravima pristupa trebalo bi se koristiti samo za administriranje sustava.
- Periodično revidiranje dodijeljenih prava povlaštenog pristupa informacijskom sustavu.
- Evidentiranje i prema potrebi pregledavanje i analizu aktivnosti koje se provode putem povlaštenog pristupa (primjerice pregledom sistemskih i operativnih zapisa).
- Rigoroznu zaštitu identifikacijskih i autentifikacijskih oznaka koje se rabe za povlašteni pristup na informacijskom sustavu. Neprimjerena zaštita ovih oznaka izlaže kreditnu uniju velikom riziku od narušavanja povjerljivosti, integriteta i raspoloživosti informacijskog sustava.
- Definiranje postupaka koji će u izvanrednim situacijama ovlaštenim osobama omogućiti povlašteni pristup informacijskom sustavu (primjerice saznavanje identifikacijskih i autentifikacijskih oznaka korisnika s administratorskim ovlastima pohranjenih u sefu u čitljivom obliku).
- Izbjegavanje dijeljenja istih identifikacijskih i autentifikacijskih oznaka s pravima povlaštenog pristupa između više korisnika (primjerice ukoliko pružatelj usluga

ima povlaštena prava pristupa, zaposlenici pružatelja usluga ne bi smjeli međusobno dijeliti identifikacijske i autentifikacijske oznake, odnosno svaki zaposlenik pružatelja usluga morao bi imati jedinstvene identifikacijske i autentifikacijske oznake).

6.5. Pristup telekomunikacijskim mrežama

Mrežna sigurnost zahtijeva djelotvornu primjenu različitih vrsta kontrola kako bi se adekvatno zaštitio pristup resursima informacijskog sustava. Prema složenosti njezine telekomunikacijske mreže kreditna bi unija trebala ocijeniti i na odgovarajući način primijeniti upravljačke, logičke i fizičke kontrole. Dobre prakse nalažu uvođenje sljedećeg:

- grupiranje mrežnih poslužitelja, aplikacija, korisnika te ostalih resursa informacijskog sustava u sigurnosne zone, primjerice podjelu u zonu nad kojom kreditna unija nema potpunu kontrolu (npr. internet), zonu vanjskih pružatelja usluga i zone različitih grupa internih korisnika;
- uspostavu odgovarajućih pravila pristupa unutar pojedine sigurnosne zone ili između više različitih zona;
- primjenu odgovarajućih upravljačkih, logičkih i fizičkih kontrola kako bi se dosljedno udovoljilo prethodno navedenim pristupnim zahtjevima.

Posebno je za sigurnost informacijskog sustava kreditne unije važna povezanost kreditne unije s internetom. Ako je telekomunikacijska mreža kreditne unije povezana s internetom, kreditna bi unija morala implementirati vatrozid (engl. *firewall*) koji će filtrirati sav promet između telekomunikacijske mreže kreditne unije i interneta. U skladu s dobrim praksama vatrozid bi trebao biti konfiguriran prema principu inicijalne zabrane svih tipova mrežnog prometa (engl. *default-deny*) te naknadnog omogućavanja pojedinih načina komunikacije u skladu s poslovnim potrebama. Konačna konfiguracija vatrozida morala bi biti postavljena u skladu sa sljedećim načelima:

1. načelom zabrane svih aktivnosti (uključujući protokole, portove i slično) koje nisu eksplicitno dopuštene na temelju poslovnih potreba;
2. načelom dodjele najmanjih mogućih prava resursima informacijskog sustava (poslužiteljima, mrežnim uređajima i slično) koja omogućuju djelotvorno obavljanje radnih zadataka.

Bežična mrežna infrastruktura sve se češće upotrebljava za razmjenu podataka unutar organizacije i za pristup internetu. Međutim, upotreba bežičnih komunikacijskih protokola (primjerice obitelji komunikacijskih protokola IEEE 802.11) bez implementacije odgovarajućih mehanizama zaštite može izložiti kreditnu uniju znatnom riziku od narušavanja povjerljivosti i integriteta podataka. Bežične mreže trebalo bi zaštititi primjenom slojevitih logičkih (primjerice enkripcijom prometa i filtriranjem MAC adresa) i fizičkih kontrola. Posebnu bi pozornost trebalo posvetiti enkripciji

prometa te izbjegavati oslanjanje na nedovoljno sigurne enkripcijske algoritme odnosno protokole (primjerice *Wired Equivalent Privacy* –WEP).

6.6. Udaljeni pristup

Udaljeni pristup resursima informacijskog sustava kreditne unije jest pristup tim resursima s udaljene lokacije pomoću telekomunikacijske infrastrukture nad kojom kreditna unija nema potpunu kontrolu ili nadzor. Kreditna unija trebala bi biti svjesna mogućnosti koje pruža udaljeni pristup sustavu i ranjivosti koje iz toga proizlaze, te bi prema tome trebala definirati načine primjene i ograničenja udaljenog pristupa. Svrha je navedenog svođenje na najmanju moguću razinu izloženosti kreditne unije šteti koja može proizići iz neovlaštenog korištenja informacijskih resursa kreditne unije. Primjeri mehanizama udaljenog pristupa informacijskom sustavu (tj. pristupa informacijskom sustavu s udaljene lokacije) jesu povezivanje pomoću modema i telefonske infrastrukture, povezivanje preko interneta i virtualne privatne mreže (engl. *Virtual Private Network – VPN*) i slično. Kreditna bi unija trebala zaštititi pristup svojem informacijskom sustavu s udaljene lokacije uzimajući u obzir sljedeće:

- Internim je aktima potrebno onemogućiti udaljeni pristup osim ako za to postoje opravdane poslovne potrebe.
- Potrebno je strogo kontrolirati pristup pomoću formalnog sustava odobrenja i periodične revizije dodijeljenih prava za udaljeni pristup.
- Potrebno je uvesti rigorozne kontrole nad konfiguracijama resursa informacijskog sustava koji omogućuju udaljeni pristup kako bi se kreditna unija zaštitila od moguće zloupotrebe udaljenog pristupa (primjer je takve kontrole automatski povratni poziv).
- Primjenu evidentiranja i nadzora svih radnja provedenih korištenjem udaljenog pristupa (primjerice praćenjem sistemskih i operativnih zapisa). Navedeno uključuje podatke kao što su datum, vrijeme, korisnik, lokacija korisnika, trajanje i svrha svih udaljenih pristupa.
- U svrhu zaštite komunikacija preporučljiva je primjena "jakih" autentifikacijskih mehanizama (primjerice kombinacija dvaju načina utvrđivanja neospornosti korisničkog identiteta) i enkripcije.

7. Upravljanje operativnim i sistemskim zapisima

Operativni i sistemski zapisi (engl. *log* ili *audit trail*) jesu bilješke o aktivnostima na resursima informacijskog sustava nastale onim slijedom kako su se te aktivnosti ostvarivale (zapisi operacijskih sustava, vatrozida, usmjernika, baza podataka, aplikacijskih sustava, procesa, osoba). U kombinaciji s odgovarajućim internim aktima, procedurama i alatima operativni i sistemski zapisi (u nastavku poglavlja: zapisi) omogućuju postizanje ciljeva povezanih sa sigurnošću i funkcionalnošću, uključujući rekonstrukciju događaja, osobnu odgovornost, otkrivanje neovlaštenog pristupa i radnja te identifikaciju problema. Zapisi se, između ostalog, upotrebljavaju za sljedeće:

- **Rekonstrukciju događaja.** Kreditna unija može upotrebljavati zapise za rekonstrukciju izvršenih radnja (primjerice kao pomoć u naknadnoj istrazi kojom se utvrđuje kako, kada i zašto su redovne operacije prekinute te tko je, kako i kada obavio određenu radnju).
- **Osobna odgovornost.** Zapisi služe za poticanje savjesnog korištenja resursa jer korisnici znaju da se njihove radnje mogu naknadno analizirati i jedinstveno pratiti do izvora.
- **Otkrivanje neovlaštenog pristupa i radnja na sustavu.** Zapisi se mogu rabiti kao pomoć u otkrivanju neovlaštenog pristupa i radnja na sustavu ukoliko je sustav za otkrivanje takvih aktivnosti pravilno konfiguriran, odnosno ako bilježi odgovarajuće informacije. Navedene aktivnosti mogu biti otkrivene u realnom vremenu analizom zapisa u trenutku kreiranja ili naknadno.
- **Identifikacija problema.** Zapisi mogu također pomoći u identificiranju ostalih sigurnosnih i funkcionalnih problema na informacijskom sustavu u realnom vremenu.

Zapisi trebaju sadržavati dovoljnu količinu informacija za utvrđivanje pojave događaja i njihova uzroka. Obuhvat i sadržaj zapisa potrebno je pomno definirati kako bi se uravnotežila potreba za sigurnošću s jedne strane te učinkovitost i troškovi s druge strane. Općenito, zapis o događaju treba pružiti informaciju:

- o vrsti događaja;
- o vremenu kada se događaj dogodio;
- o identifikaciji osoba, sustava ili procesa povezanih s događajem;
- o programu ili naredbi koja je upotrijebljena za pokretanje događaja.

U skladu sa smjernicama iz poglavlja 6.2. sve radnje povezane s financijskim podacima (primjerice uplate i isplate, isplata kredita, obračuni kamata, korištenje tehnike storna), promjene matičnih podataka (primjerice unos i promjena podataka o članovima kreditne unije) te ostale važne poslovne aktivnosti (primjerice otvaranje i zatvaranje kredita, depozita i jamstava, odobravanje kredita) kojima je podrška informacijski sustav mora biti moguće jednoznačno povezati s korisnikom informacijskog sustava koji je te aktivnosti proveo. Sve takve radnje trebalo bi bilježiti u zapise. Te zapise trebalo bi čuvati dok god postoji potreba za postojanjem podataka na koje se zapisi odnose. Nadalje, u zapise bi se morale bilježiti sve uspješne i neuspješne prijave te odjave iz

resursa informacijskog sustava. Svaku radnju zabilježenu u zapis trebalo bi biti moguće povezati s datumom i vremenom provođenja te s korisničkim računom koji je proveo tu radnju.

Radi zaštite integriteta, dokazivosti i neporecivosti informacijskog sustava operativni i sistemski zapisi moraju biti adekvatno zaštićeni od neovlaštenog pristupa, izmjena i brisanja, pri čemu treba imati u vidu barem sljedeće:

- Povjerljivost i integritet zapisa moraju biti primjereno zaštićeni. Zaštitu je moguće ostvariti implementacijom slojevitih kontrola koje mogu uključivati sljedeće:
    - onemogućavanje promjene ili brisanja već nastalih zapisa
    - omogućavanje pristupa zapisima samo korisnicima s povlaštenim pravima pristupa resursima informacijskog sustava
    - pohranjivanje ili kopiranje zapisa nastalih na jednom resursu informacijskog sustava na drugi resurs (primjerice pohranjivanje ili kopiranje zapisa jednog poslužitelja na drugi poslužitelj)
    - periodičnu izradu pričuvnih kopija zapisa.
- Pristup zapisima putem javno dostupnih telekomunikacijskih mreža (primjerice interneta) treba biti strogo kontroliran.

8. Upravljanje promjenama

Brzi napredak informacijske tehnologije kao i česte izmjene poslovnih zahtjeva uzrokuju potrebu za promjenom softverskih i hardverskih komponenata informacijskog sustava. Navedene promjene mogu rezultirati neočekivanim ponašanjem informacijskog sustava (primjerice nekompatibilnošću i nestabilnošću dijelova sustava te programskim pogreškama – engl. *bug*) i negativno utjecati na njegovu sigurnost. Stoga postupke izmjene informacijskih sustava treba formalno propisati te se ponašati oprezno i u skladu s dobrim praksama kako bi se negativni utjecaji sveli na najmanju moguću mjeru. Osnovni je zadatak upravljanja promjenama osigurati da promjene komponenata informacijskog sustava ne naruše (namjerno ili nenamjerno) sigurnost i funkcionalnost informacijskog sustava.

Kreditna bi unija trebala uspostaviti proces upravljanja promjenama softverskih komponenata informacijskog sustava koji bi obuhvatio barem sljedeće postupke:

- Utvrđivanje početnih inačica softverskih komponenata informacijskog sustava.
- Identifikaciju i praćenje svih programskih promjena aplikacijskog softvera koji podržava provođenje poslova kreditne unije (definiranih Zakonom o kreditnim unijama, "Narodne novine", br. 141/2006.).
- Identifikaciju i praćenje svih promjena arhitekture baza podataka koje podržavaju provođenje poslova kreditne unije (definiranih Zakonom o kreditnim unijama, "Narodne novine", br. 141/2006.).
- Identifikaciju i praćenje promjena svih ostalih softverskih komponenata informacijskog sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost informacijskog sustava.

Upravljanje promjenama uključuje i upravljanje novim verzijama softvera i hardverskim komponentama, kao i upravljanje programskim ispravcima ("zakrpa", engl. *patch*). Potrebno je sustavno pratiti objavljivanje programskih ispravaka i izmjena, kao i novih verzija aplikativnih programa i operacijskih sustava te ih, ovisno o procjeni prednosti i nedostataka, implementirati na informacijskom sustavu. Posebnu pozornost treba posvetiti programskim ispravcima i novim verzijama dijelova informacijskog sustava koji ispravljaju sigurnosne propuste.

Proces promjene informacijskih sustava trebao bi biti propisan, standardiziran i obuhvaćati barem sljedeće:

- Definiranje zahtjeva kojim se traži promjena i razloge provođenja te promjene. Primjerice:
    - Prije provođenja promjene poslovne aplikacije ili arhitekture baze podataka trebalo bi definirati razloge provođenja te promjene i specifikaciju promjene.
    - Prije primjene programskog ispravka trebalo bi definirati razloge implementacije tog ispravka (npr. uklanjanje kritičnih sigurnosnih propusta na operacijskom sustavu Microsoft Windows XP).

- Sve je promjene prije postavljanja u produkcijsku okolinu potrebno testirati u testnoj okolini. Testiranje bi se moralo obaviti u obuhvatu koji odgovara opsegu i karakteristikama promjene sustava. Testna okolina morala bi zadovoljavati sljedeće zahtjeve:
    - Testna okolina mora biti odvojena od produkcijske okoline.
    - Problemi i zastoji u radu testne okoline ne smiju moći (negativno) utjecati na rad produkcijske okoline.
    - Testna okolina bi prema svojim karakteristikama trebala biti čim sličnija produkcijskoj okolini, a podaci u testnoj okolini trebali bi biti čim sličniji produkcijskim podacima.
- Odgovorna bi osoba trebala formalno odobriti (na temelju rezultata provedenog testiranja) postavljanje svake promjene informacijskog sustava u produkcijsku okolinu.
- Sve promjene informacijskog sustava morale bi biti evidentirane onim slijedom kako su nastajale zajedno s vremenom nastanka promjene.
- Pri provođenju promjene trebalo bi, ukoliko je potrebno, ažurirati dokumentaciju (primjerice upute o upotrebi aplikacija, procedure izrade pričuvnih kopija, upute o služenju elektroničkom poštom i slično).
- Pril provođenju većih promjena trebalo bi razmotriti potrebu provođenja dodatne edukacije korisnika informacijskog sustava.

Posebno je za održavanje zadovoljavajuće razine sigurnosti informacijskog sustava važna pravodobna primjena sigurnosnih programskih nadogradnja i ispravaka. Proces upravljanja programskim nadogradnjama i ispravcima trebao bi obuhvatiti barem sljedeće:

- Trebao bi postojati sustav praćenja objave novih programskih nadogradnja i ispravaka. Ovaj sustav može biti automatiziran ili osobe odgovorne za praćenje i primjenu programskih nadogradnja i ispravaka mogu periodično provjeravati njihovu dostupnost. Barem jednom mjesečno trebalo bi provjeravati postojanje odnosno dostupnost novih programskih nadogradnja i ispravaka za sve softverske komponente (operacijski sustavi, baze podataka, aplikacije, mrežna oprema) koje podržavaju važne poslovne procese. Posebnu pozornost trebalo bi posvetiti osobito raširenim softverskim komponentama s većim brojem poznatih sigurnosnih propusta.
- Sve programske ispravke i nadogradnje trebalo bi prije integracije u produkcijsku okolinu testirati na primjeren način u testnoj okolini kako bi se osiguralo da primjena pojedinog ispravka ili nadogradnje nema znatan negativan utjecaj na rad sustava.
- Sve programske ispravke i nadogradnje koje uklanjaju sigurnosne propuste (tj. ranjivosti) na informacijskom sustavu kreditne unije, a nemaju znatan negativan utjecaj na rad sustava, trebalo bi integrirati u informacijski sustav. Sve programske ispravke i nadogradnje koje uklanjaju posebno važne (kritične) sigurnosne propuste treba u što kraćem vremenu testirati i integrirati u produkcijsku okolinu.

9. Upravljanje konfiguracijama

Većinu hardverskih i softverskih komponenata informacijskog sustava moguće je pomoću niza postavka prilagoditi specifičnim potrebama kreditne unije. Navedene postavke morale bi biti na zadovoljavajući način konfigurirane, kako bi se funkcionalnost i sigurnost sustava dovele i održale na potrebnoj razini. Postupak upravljanja postavkama sustava nazivamo upravljanjem konfiguracijama sustava. Upravljanje konfiguracijama je proces analize, definiranja, dokumentiranja, testiranja, uvođenja u produkcijski rad, kontrole i praćenja izmjena u postavkama komponenata informacijskog sustava. Upravljanje konfiguracijama trebalo bi obuhvatiti sve osjetljive postavke informacijskog sustava. Osjetljivim postavkama smatraju se sve postavke čija izmjena može znatno utjecati na sigurnost ili funkcionalnost informacijskog sustava.

Izmjene postavka komponenata informacijskog sustava potrebno je provoditi pomoću sustava upravljanja promjenama. Sustav upravljanja konfiguracijama trebao bi omogućiti identifikaciju svih osjetljivih postavka informacijskog sustava (koje su bitne za djelotvorno i sigurno funkcioniranje sustava) u određenom trenutku. Pristup postavkama koje mogu utjecati na sigurnost i mogućnost njihove izmjene moraju biti nadzirani i kontrolirani (primjerice implementacijom odgovarajućih prava pristupa korisnika prema principu dodjele najmanjih ovlasti potrebnih za sigurno i uspješno provođenje radnih zadataka).

Svi resursi bitni za odvijanje poslovnih procesa trebali bi biti "ojačani" (engl. *system hardening*). Ojačavanje sustava uključuje, između ostalog, sljedeće postupke:

- Isključivanje svih funkcija koje nisu potrebne za sigurno i uspješno provođenje radnih zadataka. Većina resursa informacijskog sustava prema inicijalnoj konfiguraciji koja nastaje nakon instalacije ima omogućen veliki broj servisa, usluga te ostalih funkcija. Isključivanje nepotrebnih funkcija znatno smanjuje mogućnost narušavanja sigurnosti tog resursa te posljedično sigurnosti cjelokupnoga informacijskog sustava.
- Upotreba sigurnijih servisa i komunikacijskih protokola (primjerice upotreba komunikacijskih protokola *SSH* i *SCP* umjesto *telnet* i *FTP*).
- Primjenu svih relevantnih sigurnosnih ispravaka i nadogradnja.
- Promjenu svih inicijalnih zaporka (primjerice početnih zaporka korisničkih računa s povlaštenim pravima pristupa) te ostalih inicijalno postavljenih parametara koji bi trebali biti povjerljivi (primjerice inicijalnih komunikacijskih nizova i kriptografskih ključeva).
- Ograničavanje prava pristupa korisnika informacijskog sustava na najmanja potrebna za sigurno i uspješno obavljanje radnih zadataka.
- Uklanjanje informacija o sustavu koje zlonamjernim osobama mogu olakšati neovlašteni pristup sustavu (primjerice informacija o verziji sustava, informacija o aktivnim servisima i slično).

Najčešće se provodi ojačavanje operacijskih sustava, međutim moguće je ojačavati i mrežne uređaje, baze podataka itd. Posebno je važno provoditi ojačavanje raširenih softverskih komponenata koje su česta "meta" pokušaja neovlaštenog pristupa (primjerice operacijskih sustava Linux, Unix i Microsoft Windows, baza podataka Microsoft SQL Server i Oracle, web-preglednika itd.). S obzirom na navedeno, primjerenu pozornost trebalo bi posvetiti ojačavanju osobnih računala.

Proizvođači softverskih komponenata kao i razne neovisne organizacije te državne ustanove objavljuju smjernice za ojačavanje sustava. Implementacija preporuka iz takvih dokumenata može znatno smanjiti rizik od narušavanja sigurnosti informacijskog sustava kreditne unije.

U sklopu procesa upravljanja konfiguracijama posebnu pozornost trebalo bi posvetiti prijenosnim uređajima koji se upotrebljavaju i izvan informacijskog sustava kreditne unije. Korištenje prijenosnim računalima (engl. *laptop*), ali i drugim prijenosnim uređajima i medijima (primjerice dlanovnicima, memorijskim karticama, optičkim medijima i slično) koji sadrže poslovne podatke izlaže kreditnu uniju riziku od narušavanja povjerljivosti tih podataka. Stoga bi svi osjetljivi podaci (primjerice povjerljivi podaci prema Zakonu o kreditnim unijama, "Narodne novine", br. 141/2006.) trebali biti na odgovarajući način zaštićeni (primjerice pomoću enkripcije). Ako se prijenosno računalo upotrebljava za povezivanje i na druge telekomunikacijske mreže osim mreže kreditne unije (primjerice internet, mreže drugih poslovnih partnera) navedeno računalo trebalo bi zaštititi primjenom osobnog vatrozida (engl. *personal firewall*). Osobni vatrozid trebalo bi konfigurirati u skladu s dobrim praksama konfiguracije vatrozida navedenima u poglavlju 6.5.

10. Zaštita od malicioznoga programskoga kôda

Maliciozni programski kôd (engl. *malicious code*) jest svaki oblik programskoga kôda koji djeluje neočekivano i na potencijalno štetan način. Uobičajene su vrste malicioznog programskog kôda virusi, crvi i "trojanski konji", a njihovo djelovanje može imati samostalan učinak ili kombinirani, čime se postiže veća šteta. Maliciozni programski kôd može imati mogućnost replikacije i širenja na druge resurse informacijskog sustava. Nadalje, maliciozni programski kôd može ugroziti povjerljivost, integritet i raspoloživost resursa informacijskog sustava mijenjajući i brišući podatke, šaljući podatke izvan informacijskog sustava, uklanjajući dokaze koji se mogu iskoristiti za potrebe forenzike ili stvarajući skrivene ranjivosti koje mogu olakšati neovlašteni pristup i radnje na informacijskom sustavu.

Zaštitne mjere i kontrole koje se primjenjuju radi smanjenja rizika od narušavanja ili gubitka povjerljivosti, integriteta i raspoloživosti resursa informacijskog sustava zbog utjecaja malicioznoga programskoga kôda podrazumijevaju slojevito oblikovanje sigurnosne infrastrukture, što, između ostalog, uključuje primjenu adekvatne tehnologije, internih akata i edukaciju zaposlenika. Kontrole koje bi kreditna unija trebala primijeniti kako bi smanjila navedene rizike uključuju uz ostalo proizvode i sustave za otkrivanje i uništavanje malicioznoga programskoga kôda (primjerice antivirusne programe) kao i ostale sustave za ograničavanje i otkrivanje neuobičajenih ili neovlaštenih radnja te za nadziranje i upravljanje radnjama koje su dopuštene (primjerice vatrozid). Sve resurse informacijskog sustava koji mogu biti "zaraženi" malicioznim programskim kôdom trebalo bi zaštiti implementacijom sustava za otkrivanje i uništavanje malicioznoga programskoga kôda.

Budući da se svakodnevno pojavljuju novi primjeri malicioznoga programskoga kôda, veliku pozornost potrebno je posvetiti održavanju ažurnosti sustava zaštite od malicioznoga programskoga kôda. Kreditna bi unija trebala provjeravati ažurnost antivirusnih definicija barem jednom tjedno te, ukoliko su nove antivirusne definicije raspoložive, provesti nadogradnju antivirusnog programa novim antivirusnim definicijama na svim računalima na koje je to primjenjivo (primjerice radnim stanicama i poslužiteljima). Nadalje, barem jednom tjedno trebala bi se provesti provjera postojanja malicioznoga programskoga kôda (tzv. "skeniranje") na svim sustavima koji mogu biti "zaraženi".

Kreditna bi unija, zbog potencijalno sve složenijih neovlaštenih radnja i zbog toga što se autori malicioznoga programskoga kôda često koriste metodama socijalnog inženjeringa, trebala implementirati i ostale kontrole koje, između ostalog, uključuju interne akte o upotrebi resursa informacijskog sustava i edukaciju korisnika informacijskog sustava o mogućim prijetnjama.

Kreditna unija trebala bi posvetiti pozornost čimbenicima koji mogu utjecati na pojavu i širenje malicioznoga programskoga kôda kao što su:

- sprječavanje neovlaštene instalacije softvera;
- edukacija zaposlenika kako bi ih se upozorilo na opasnosti čitanja poruka nepoznatog podrijetla, pokretanja izvršnih datoteka, socijalni inženjering i slično;
- rukovanje medijima za pohranu i prijenos podataka;
- dopuštene aktivnosti tijekom pristupa javno dostupnim telekomunikacijskim mrežama kao i tijekom upotrebe tehnologije za komunikaciju (primjerice elektroničke pošte i slično);
- uklanjanje ranjivosti sustava povezanih s poznatim malicioznim programskim kôdovima.

11. Upotreba elektroničke pošte i interneta

Elektronička pošta (engl. *e-mail*) jest način (protokol) razmjene poruka putem računala i sustava koji ta računala međusobno povezuju.

Internet i elektronička pošta u poslovanju kreditne unije trebali bi se, u skladu s dobrim praksama, upotrebljavati samo za poslovne potrebe. Da bi se to osiguralo, kreditna bi unija trebala definirati prihvatljive načine služenja elektroničkom poštom i internetom u svom poslovanju (primjerice donijeti interne akte kojima će se definirati pravila i principi upotrebe elektroničke pošte i interneta za potrebe poslovanja).

Kreditna bi unija trebala posvetiti posebnu pozornost služenju elektroničkom poštom za razmjenu povjerljivih informacija s obzirom na to da upotreba elektroničke pošte bez dodatnih mehanizama zaštite (primjerice enkripcije, digitalnog potpisa, sažetaka podataka – engl. *hash* i slično) ne osigurava povjerljivost, integritet, autentičnost, neporecivost i dokazivost poruka elektroničke pošte niti informacija koje sadrže. Nadalje, korištenje elektroničkom poštom može ugroziti sigurnost informacijskog sustava jer poruke elektroničke pošte mogu sadržavati prikrivene programe unutar priloga (engl. *attachment*). Takvi prikriveni i maliciozni programi mogu provesti mnogobrojne štetne radnje (primjerice "zarazu" računala virusima, krađu povjerljivih podataka, preuzimanje nedopuštenih sadržaja, generiranje velikog broja novih poruka elektroničke pošte koje se šalju na adrese osoba koje se nalaze u adresaru ili drugdje na računalu korisnika).

Kreditna unija trebala bi veliku pozornost posvetiti edukaciji korisnika koji se koriste elektroničkom poštom i internetom u svom svakodnevnom radu (primjerice provođenjem programa podizanja razine svijesti o sigurnosti informacijskog sustava).

Primjeri dobrih praksa i principa povezanih s upotrebom elektroničke pošte jesu sljedeći:

- Ne bi trebalo otvarati prilog poruke elektroničke pošte koji izgleda sumnjivo. Posebnu pozornost trebalo bi obratiti:
  - na datoteke s aktivnim sadržajem (npr. datoteke s ekstenzijama EXE, VBS, JS itd.)
  - na višestruke ekstenzije datoteka u prilogu poruke (npr. *.doc.exe)
  - na datoteke s audiosadržajima i videosadržajima (npr. datoteke s ekstenzijama MP3, MPEG, MID itd.).
- Ne bi trebalo otvarati prilog poruke elektroničke pošte koji primatelj ne očekuje.
- Trebalo bi ograničiti veličine odlaznih i dolaznih poruka elektroničke pošte.
- Trebalo bi zabraniti slanje elektroničke pošte neprihvatljivog sadržaja (primjerice uznemiravajući, seksualno eksplicitan, nepristojan, klevetnički i zakonski nedopušten sadržaj).

- Ne bi trebalo rabiti privatni račun elektroničke pošte kako bi se zaobišla sigurnosna ograničenja implementirana u sustav elektroničke pošte kreditne unije.

Primjeri su dobrih praksa i principa povezanih sa služenjem internetom sljedeći:

- Sav promet prema internetu treba biti filtriran pomoću pravilno konfiguriranog vatrozida.
- Postavke web-preglednika (engl. *web browser*) ne bi smjele smanjiti razinu sigurnosti informacijskog sustava kreditne unije (primjerice primjena odgovarajućih sigurnosnih razina u web-pregledniku).
- Trebalo bi ograničiti nekontrolirano preuzimanje potencijalno štetnih sadržaja (primjerice preuzimanje datoteka s aktivnim sadržajem, audiodatoteka i videodatoteka).
- Trebalo bi zabraniti nezakonito kopiranje i upotrebu softvera koji je zaštićen autorskim pravima.
- Ne bi se trebalo koristiti resursima informacijskog sustava kreditne unije radi pribavljanja osobne financijske koristi.

12. Upravljanje pričuvnom pohranom

Proces upravljanja pričuvnom pohranom obuhvaća postupke izrade, pohrane, testiranja i restauracije podataka s pričuvnih kopija podataka. Pričuvne kopije podataka jesu pričuvne inačice podataka (engl. *backup*). Pričuvne kopije podataka moraju sadržavati sve podatke (poslovne podatke, dokumentaciju, aplikacijski i sistemski softver i slično) koji su potrebni za ponovno uspostavljanje poslovnih procesa koje podržava informacijski sustav kreditne unije te ostale podatke za koje kreditna unija procijeni da ih je potrebno pohraniti kao pričuvu.

Kreditna bi unija trebala osigurati postojanje ažurnih pričuvnih kopija podataka kao i provjerenih i testiranih metoda restauriranja podataka kako bi bio moguć uspješan oporavak u slučajevima gubitka podataka povezanih s događajima kao što su:

- sigurnosni incidenti
- slučajno ili namjerno brisanje podataka
- neočekivani prekidi u radu informacijskog sustava
- havarije
- ostali neželjeni i nepredviđeni događaji.

Kreditna unija trebala bi donijeti interne akte kojima se definiraju kriteriji, načini i postupci upravljanja pričuvnom pohranom kao što su kategorizacija, učestalost izrade, vrsta, rukovanje, pohrana, restauracija i čuvanje pričuvnih kopija podataka. Isto tako, potrebno je definirati i ovlasti i odgovornosti za upravljanje pričuvnom pohranom.

Uobičajene dobre prakse pri uspostavljanju procesa upravljanja pričuvnom pohranom uključuju, između ostalog, sljedeće:

- izradu, održavanje i pregled evidencije o pričuvnim kopijama podataka;
- obilježavanje medija (primjerice CD, DVD, DAT vrpce) na kojima su pohranjeni podaci, što može uključivati informacije poput sadržaja, datuma izrade, vrste kopije, sistemskog okruženja, razine osjetljivosti i slično;
- izradu pričuvnih kopija sistemskih datoteka (primjerice operacijskih sustava, pogonskih programa za hardver i slično);
- adekvatno upravljanje fizičkom sigurnošću pričuvnih kopija podataka;
- verificiranje podataka na pričuvnim kopijama kako bi se omogućila uspješna restauracija podataka;
- periodično restauriranje podataka na testnu okolinu i/ili provjeru pomoću odgovarajućega softverskog alata kako bi se potvrdilo da su pričuvne kopije podataka pohranjene na ispravan način, da nije narušen integritet podataka te da je podatke moguće restaurirati;
- periodično revidiranje procesa izrade i pohrane pričuvnih kopija podataka;
- redovito pohranjivanje pričuvnih kopija podataka na udaljenu sigurnu lokaciju;
- uporabu kriptografskih metoda;
- pravodobno zamjenjivanje i trajno odlaganje (engl. *disposal*) medija na kojima se podaci pohranjuju kao pričuva.

Kako bi osigurala postojanje pričuvnih kopija podataka, kreditna unija trebala bi provesti sljedeće:

- Sve poslovne podatke (primjerice financijske podatke, matične podatke, poruke elektroničke pošte povezane s poslovnim aktivnostima i slično) trebalo bi kao pričuvu pohranjivati barem jednom tjedno.
- Pričuvne kopije podataka trebaju biti ažurne i pohranjene na primjeren način na jednoj ili više lokacija od kojih najmanje jedna mora biti dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci (od kojih su izrađene pričuvne kopije podataka). Kreditna unija trebala bi moći pravodobno i bez ograničenja pristupiti pričuvnim kopijama podataka.
- Barem jednom godišnje trebalo bi revidirati postupke izrade i pohrane pričuvnih kopija podataka. U okviru toga trebalo bi testirati postupke restauracije podataka s pričuvnih kopija podataka kako bi kreditna unija potvrdila mogućnost obnavljanja podataka s pričuvnih kopija podataka. Trebalo bi sastaviti pisano izvješće o rezultatima testiranja.

13. Fizička sigurnost

Fizička sigurnost obuhvaća kontrole koje se provode radi zaštite resursa informacijskog sustava od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja. Kreditna bi unija trebala uzeti u obzir sljedeće čimbenike koji mogu utjecati na fizičku sigurnost:

- **Kontrole fizičkog pristupa resursima informacijskog sustava.** Kontrole fizičkog pristupa resursima informacijskog sustava ograničavaju ulaske i napuštanje prostorija u kojima su smješteni resursi informacijskog sustava (poslužitelji, komunikacijska oprema, sustavi za podršku i slično), kao i unošenje te iznošenje opreme i medija. Primjeri su kontrola fizičkog pristupa:
    - sustav videonadzora ulaska u sistemsku prostoriju i/ili nadzora sistemske prostorije
    - biometrijske kontrole pristupa sistemskoj prostoriji
    - magnetske kartice kojima se omogućava pristup sistemskoj prostoriji
    - protuprovalna vrata na ulasku u sistemsku prostoriju
    - sigurnosne brave na ulasku u sistemsku prostoriju
    - senzori pokreta unutar sistemske prostorije
    - zaštitne prozorske rešetke i senzori loma stakla (ukoliko sistemska prostorija ima prozor).

- **Zaštita od požara.** Požar ima potencijal da djelomično ili potpuno uništi resurse informacijskog sustava. Primjeri su kontrola zaštite od požara:
    - vatrodojavni sustav
    - sustavi za automatsko gašenje požara vodom (sustav suhih cijevi – engl. *dry sprinkler*) ili plinom (primjerice FM-200)
    - aparati za gašenje požara u sistemskoj prostoriji i/ili ispred nje
    - protupožarna vrata na ulasku u sistemsku prostoriju
    - zabrana korištenja zapaljivih materijala u sistemskoj prostoriji (tepih, različita papirnata dokumentacija).

- **Sustavi za podršku funkcioniranju informacijskog sustava.** Zastoji u radu sustava za podršku mogu izazivati prekide u radu informacijskog sustava i njegovo oštećenje. Primjeri su sustava za podršku funkcioniranju informacijskog sustava:
    - sustavi za održavanje stabilnog i neprekinutog napajanja električnom energijom (engl. *Uniterrupted Power Supply – UPS*)
    - agregati za napajanje informacijskog sustava električnom energijom
    - sustavi za grijanje
    - sustavi za klimatizaciju
    - sustavi kontrole svojstava zraka (primjerice temperature, vlažnosti i koncentracije onečišćenosti zraka).

- **Zaštita od utjecaja vode.** Prodor vode može biti razoran za informacijski sustav odnosno dovesti do zastoja funkcioniranja informacijskog sustava te gubitka podataka. Primjeri su kontrola zaštite od utjecaja prodora vode:
    - podizanje resursa informacijskog sustava iznad razine poda u sistemskoj prostoriji
    - detektori razine vode u sistemskoj prostoriji
    - sustav za odvodnjavanje ili pumpe za izbacivanje vode u slučaju poplave
    - "dvostruki pod" u sistemskoj prostoriji
    - uklanjanje aktivnih vodovodnih instalacija koje se nalaze u blizini sistemske prostorije.

14. Završna razmatranja

Adekvatna primjena preporuka navedenih u *Smjernicama* trebala bi omogućiti kreditnoj uniji da ovlada rizikom informacijskog sustava. Time bi se trebala smanjiti mogućnost pojave i učinak neželjenih događaja koji narušavaju povjerljivost, integritet i/ili raspoloživost informacija i procesa koji se odvijaju u kreditnoj uniji.

Primjena preporuka navedenih u *Smjernicama* vjerojatno će dovesti do uspostave novih ili prilagodbe postojećih procesa povezanih s informacijskim sustavom kreditne unije, a implementacija nekih preporuka dovest će i do organizacijskih promjena. Uspostava ili prilagodba nekih procesa zahtijevat će znatan angažman zaposlenika kreditne unije te određena financijska ulaganja. Kreditna bi unija trebala posvetiti posebnu pozornost procesu planiranja da bi se za sve planirane postupke predvidjela dovoljna financijska sredstva, osigurala raspoloživost zaposlenika kreditne unije te raspoloživost vanjskih suradnika kako bi planirani postupci doveli do željenih rezultata u očekivanom vremenu te uz očekivani utrošak resursa. Važno je naglasiti da bi svi procesi povezani s informacijskim sustavom kreditne unije morali biti na primjeren način propisani (internim aktima) i dokumentirani, pri čemu bi dokumentacija morala biti točna, potpuna i ažurna.

Područje je informacijske tehnologije kompleksno i specifično te su za pravilnu uspostavu nekih procesa potrebna visoko specijalizirana tehnička znanja koja se stječu kontinuiranom izobrazbom i stručnim usavršavanjem, pri čemu je važno i iskustvo u uspostavi i provođenju tih procesa. Kreditna unija trebala bi razmotriti mogućnost i potrebu suradnje s pružateljima usluga koji imaju odgovarajuća stručna znanja i iskustvo kako bi se osiguralo da će uspostavljeni procesi rezultirati funkcionalnim i sigurnim informacijskim sustavom. Kreditna bi unija trebala ispitati i mogućnost i potrebu provođenja drugih aktivnosti koje mogu znatno unaprijediti funkcionalnost i sigurnost procesa koji se odvijaju u kreditnoj uniji. Primjeri su takvih aktivnosti:

- pravilna implementacija svjetski priznatih standarda (primjerice ISO/IEC 17799 odnosno ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 9001)
- periodično provođenje revizije informacijskog sustava kreditne unije
- periodično provođenje testiranja pokušaja proboja (engl. *penetration testing*) u informacijski sustav kreditne unije.