REPUBLIKA HRVATSKA
MINISTARSTVO GOSPODARSTVA

Klasa: 080-01/11-01/154
Urbroj: 526-04-01-02-01/2-13-32

NACIONALNI CA ZA REPUBLIKU HRVATSKU (NCARH)

OPĆA PRAVILA SIGURNOSTI

Verzija 1.1

Datum 05. 11. 2013.

AUTORSKA PRAVA

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene Povjerenstvu za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i postupke (dalje u tekstu: PMA HR PKI).

Obavijest o finalnim promjenama

PMA HR PKI odrediti će period za obavijest o finalnim promjenama.

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene
1	**1.1**		**Usklađivanje sa zakonskom regulativom u RH**	**05. 11. 2013.**

OBJAVA

Na temelju odluke o prihvaćanju i objavi dokumenata NCARH-a donijete na sjednici Povjerenstva za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju održanoj dana 14. listopada 2013.godine, Ministarstvo gospodarstva objavljuje navedene dokumente.

U Zagrebu 05. studenog 2013.g.

MINISTAR GOSPODARSTVA

Ivan Vrdoljak

Sadržaj

Sadržaj

1. UVOD

1.1. Svrha dokumenta

Ovaj dokument opisuje način na koji su opća pravila sigurnosti pripremljena, vođena i objavljena. Dokument sadrži dijelove koji se odnose na:

- fizičku sigurnost;
- kontrolu pristupa sustavu;
- operativnu sigurnost;
- izradu pričuvnih kopija i arhiviranje podataka;
- operativno osoblje;
- tajnost informacija;
- detaljne dokumente koji se odnose na opća pravila sigurnosti, uključivo:
  - *plan sigurnosti informatičkog sustava,*
  - *plan fizičke sigurnosti,*
  - *plan oporavka u slučaju incidenta,*
  - *plan izrade pričuvnih kopija softvera i podataka,*
  - *operativni priručnik za NCARH.*

1.2. Politika sigurnosti

Politika sigurnosti je strateški dokument visoke razine i odražava poslovne potrebe Ministarstva gospodarstva i PMA HR PKI za zaštitom NCARH sustava. Politika sigurnosti sadrži sljedeće:

- zahtjeve PMA HR PKI u provedbi zaštite;
- obvezujuće principe poslovanja u HR PKI; i
- smisao i svrhu sigurnosti u HR PKI.

1.2.1. Smisao sigurnosti

Planiranje, implementacija i upravljanje mjerama zaštite i sigurnosti HR PKI sustava provodi se sa ciljem postizanja sigurnog, pouzdanog i kvalitetnog NCARH sustava izdavanja certifikata u HR PKI domeni.

Glavni je cilj sigurnosti u NCARH sljedeći:

- spriječiti svaku neautoriziranu akciju koja se pojavi,
  - *otkriti i bilježiti svaku neautoriziranu akciju koja se pojavi,*
- poduzeti akcije koje su potrebne nakon primitka potrebne informacije.

1.2.2. Upravljanje

Upravljanje se odnosi na kontrole u NCARH koje se odnose na sigurnost sustava i na osobe uključene u održavanje sigurne okoline, njihove zadaće i odgovornost.

1.2.3. Arhitektura i planiranje

Ovo se odnosi na postizanje sigurnosti pri izvedbi NCARH prostora, također se odnosi na fizičke barijere koje ograničavaju kretanje na mjesta gdje se nalazi tehnologija, i kontrole pristupa osjetljivim mrežama i infrastrukturi. Arhitektura i planiranje također prepoznaje različite grupe korisnika u okviru NCARH prostora te kako su ti korisnici odijeljeni.

1.2.4. Primjena tehnologija

Tehnološki se element sigurnosti odnosi na opremu NCARH sustava koja podržava upravljanje sigurnošću.

2. PROCEDURE ZA PROVEDBU SIGURNOSTI

Procedure za provedbu sigurnosti su skup sigurnosnih postupaka, koji opisuje način upravljanja sredstvima/resursima (uređaji, servisi, informacije i osoblje), način njihove zaštite i distribucije.

Krajnji cilj dokumenta **Opća pravila sigurnosti** je izrada okvira kojim se osigurava, postizanje najviše moguće razine sigurnosti NCARH.

Opća se pravila sigurnosti odnose na cijeli sustav na kojem se temelji NCARH, i uvode se procedure po kojima se uspješno obavlja izdavanje certifikata i upravljanje njihovim životnim ciklusom.

Odredbe iz ovog dokumenta u skladu su s priznatim međunarodnim PKI normama.

2.1. Pregled

U namjeri da se postigne visoka razina sigurnosti nužno je primjeniti najviše standarde povjerenja i sigurnosti NCARH usluga. Ti se standardi očituju postizanjem sljedećeg:

- sigurna fizička okolina;
- izrada pravilnika i procedura;
- primjenjena tehnologija;,
- stručno iskustvo;,
- revizija sustava;,
- odabir osoblja;,
- pravna ekspertiza;,
- operacije.

2.1.1. Norme

Sigurnosna se politika temelji na sljedećim normama iz područja informacijske sigurnosti :

- HRN ISO/IEC 27001:2006 HRN ISO/IEC 27001:2006 Informacijska tehnologija -- Sigurnosne tehnike -- Sustavi upravljanja informacijskom

sigurnošću – Zahtjevi; Information technology – Security techniques – Information security management systems – Requirements [14];

- HRN ISO/IEC 27002:2006 Informacijska tehnologija -- Sigurnosne tehnike -- Kodeks postupaka za upravljanje informacijskom sigurnošću;Information technology - Security techniques - Code of practice for information security management [15];

3. NAČELA POSLOVANJA

3.1. Cjelovitost - integritet

Zahtjevi za izdavanje certifikata i informacije u certifikatu u okviru NCARH sustava i X.500 imenika ne mogu se mijenjati, brisati ili dodavati na bilo koji način od strane operativnog osoblja NCARH.

Kontrole pristupa i ograničenje prava pristupa opremi ovlaštenim osobama NCARH sustava opisane su u internim dokumentima NCARH.

Samo ovlašteno NCARH i RA operativno osoblje ima dozvolu za dodavanje novih zahtjeva u NCARH sustav. Takvi registracijski zahtjevi ne mogu biti mijenjani, brisani ili dodavani ni na koji način. Nadgledanje na razini aplikacije i podatkovne osnovice biti će uvedeno da bi se kontrolirao pristup tim informacijama. Podatkovna osnovica je zaštićena imenom korisnika i zaporkom.

3.2. Raspoloživost

U skladu sa NCARH politikom davanja usluga izdavanja certifikata, X.500 imenik je dostupan klijentima 24 sata na dan, 7 dana u tjednu. Nemogućnost da pouzdajuće strane pristupe toj podatkovnoj osnovici znači da se zahtjevi za validaciju certifikata ne mogu procesuirati sve do ponovnog uspostavljanja servisa, odnosno da korisnik neće moći koristiti svoju PKI aplikaciju ili se pouzdati u certifikat. Za NCARH je imperativ održavanje mogućnosti da sudionici mogu neprekidno pristupati tim servisima.

CRL mora biti dostupna u svako vrijeme radi osiguranja da pouzdajuće strane imaju mogućnost provjeriti da certifikat s kojim rade nije bio opozvan.

3.3. Ključevi

3.3.1. NCARH privatni ključevi

Tajnost i povjerljivost NCARH privatnih ključeva osigurana je sljedećim mjerama:

- fizička sigurnost na visokoj razini;

- složene kontrolne sigurnosne mjere koje uključuju detekciju upada, višestruke vatrozidove i sistemsko nadgledanje;
- stroge fizičke kontrole pristupa;
- uvođenje pravila o ograničavanju boravka samo jedne osobe u prostorima u kojima se generiraju i pohranjuju ključevi;,
- odabir osoblja;,
- plan akcija za oporavak u slučaju nezgode.

3.3.2. Zaštita ključeva

Potpisni ključ mora biti zaštićen tako da spriječi svaku mogućnost njegovog kompromitiranja. Plan za oporavak od nezgode, procjena rizika i opasnosti te plan o kontinuitetu poslovanja razvijeni su da bi jamčili sigurnost, raspoloživost i integritet potpisnih ključeva.

Potpisni ključevi koji čine temelj HR PKI sustava povjerenja su:

- NCARH ključevi;
- CA ključevi.

3.4. Sigurnosne zone

3.4.1. Zone u kojima je potrebna nazočnost dva ovlaštena zaposlenika

NCARH ima uvedene zone u kojima je potrebna nazočnost najmanje dva ovlaštena zaposlenika, u okviru posebnih područja u višeslojnim sigurnim zonama. To znači da postoje područja u operativnom centru gdje nije dopušteno da jedna osoba bude sama, te je potrebna nazočnost dviju ovlaštenih osoba kad god se ulazi u ta područja.

Zone u kojima je potrebna nazočnost dva ovlaštena zaposlenika uključuju:

- područja u kojima se čuvaju online kriptografski podaci;
- područja u kojima se čuvaju offline kriptografski podaci,
- prostorija u kojoj se generiraju ključevi,
- prostor u koji je smještena oprema produkcijske mreže.

3.4.2. Kontrole pristupa

Kontrola se pristupa na NCARH računalnu mrežu provodi zaporkom i/ili certifikatom za autentifikaciju. Od cjelokupnog se osoblja zahtijeva da se pridržavaju uputa u odnosu na konstrukciju zaporke, njenu uporabu, vrijeme valjanosti i sigurnost, kao što je opisano u priručniku za zaposlenike.

Redovita se kontrola provodi o uporabi zaporki na sustavu s ciljem da se osigura njihova usklađenost s uputama.

4. PKI ULOGE I ODGOVORNOSTI

4.1. PMA HR PKI

PMA HR PKI je odgovoran za iniciranje promjena i odobravanje Općih pravila sigurnosti, za periodičku reviziju provođenja sigurnosnih procedura te za provjeru usklađenosti rada NCARH, RA i LRA s Općim pravilima sigurnosti, CP-om i CPS-om te drugim internim dokumentima.

4.2. NCARH

4.2.1. Voditelj OA NCARH

Voditelj OA NCARH je odgovoran za:

- operativno vođenje OA NCARH;
- pripremu i izdavanje internih priručnika, uputa i procedura.

4.2.2. Specijalist sigurnosti

Specijalist sigurnosti je odgovoran za svakodnevno administriranje sigurnosnih postupaka:

- razvoj i implementacija procedura fizičke sigurnosti;
- razvoj i implementacija procedura sigurnosti IT sustava;
- administriranje i nadgledanje procesa promjena u NCARH sustavu;
- nadgledanje prikupljanja revizijskih zapisa;
- promidžbu svijesti o sigurnosti u OA NCARH;
- otkrivanje prekršaja i krivotvorina;
- izobrazbu svih korisnika o pravilima sigurnosti;
- izvještavanje o incidentima.

Cjelokupno je operativno osoblje OA NCARH odgovorno za osiguranje obavljanja poslova u skladu s Općim pravilima sigurnosti.

5. ZAPOSLENICI

5.1. PKI povjerljive uloge

Kao dio visokog standarda povjerenja i sigurnosti koje implementira HR PKI, svim zaposlenicima s povjerljivim korisničkim ulogama moraju biti provjereni životopisi, te moraju proći sigurnosne provjere da bi se ustanovila njihova pouzdanost za visoku razinu povjerenja.

OA NCARH provodi odgovarajuću provjeru životopisa osoblja koje radi na povjerljivim korisničkim ulogama (prije zaposlenja, te poslije, s vremena na vrijeme).Provjera osoblja koje radi na povjerljivim korisničkim ulogama uključuje:

- potvrdu o nekažnjavanju;
- provjeru ranijih zaposlenja da bi se dobile informacije o godinama rada, profesionalne kvalifikacije, reference.
-

5.2. Odgovornosti zaposlenika

Sve osobe moraju potpisati ugovor o čuvanju poslovne tajne prije zaposlenja u OA NCARH.

Sve osobe moraju pročitati i potpisati pristanak da su spremne pridržavati se Priručnika za zaposlenike.

Svi su zaposlenici OA NCARH odgovorni za primjereno korištenje računalnih resursa, za svako korištenje svojih prijava na sustav te moraju čuvati i ne otkrivati svoje pristupne podatke da bi zaštitili NCARH računalne resurse.

Osobe koje koriste Internet preko NCARH infrastrukture, moraju poštivati pravila koja su detaljno opisana u Priručniku za zaposlenike.

Zaposlenici neće pokušati pristupiti NCARH resursima za koje nemaju autorizaciju.

Zaposlenici su odgovorni za:

- pridržavanje procedura, primjenu zaštitnih zaporki i izbjegavanje rizika od računalnih virusa;
- izvješćivanje nadređenog zaposlenika o prekršajima i pokušajima prekršaja sigurnosti;
- izvješćivanje nadređenog zaposlenika o inficiranju ili sumnji o inficiranju računalnim virusom;
- provođenje lokalnih procedura vodeći pritom računa o sigurnosti informacija;
- primjerenu zaštitu informacija uključujući i one koje su u ranom stadiju pripreme ili diskusije i ne mogu još formalno biti zabilježene u informacijski sustav;
- siguran prijenos informacija na način koji minimizira rizik slučajne ili namjerne zlouporabe izvan NCARH.

5.3. Privatnost

Za čuvanje privatnosti osobnih informacija odgovornost je na svim zaposlenicima OA NCARH. Važno je za svakog zaposlenika da poštuje privatnost drugih.

Kada pristupna prava i ovlasti dopuštaju pristup osobnim informacijama koje drži NCARH u računalnom formatu, pristup će bit odobren jedino kada je stvarna potreba za tim radi izvršavanja zaposlenikovih zadaća.

.

Zaposlenik ne može pristupiti ili otkriti osobne ili tajne informacije, osim u iznimnim okolnostima. Te okolnosti uključuju, ali nisu limitirane na sljedeće:

- pristanak osobe na koju se informacija odnosi;
- na zahtjev nadležnog suda;
- u skladu s nekim drugim zakonskim obavezama.

U svim će ovim slučajevima davanje informacija nadgledati i odobravati PMA HR PKI.

5.4. Školovanje i obuka

Obuka za područje sigurnosti je bitan element za postizanje znanja i vještina potrebnih za osoblje OA NCARH. Obuku osoblja treba provoditi učestalo da bi osoblje postalo svjesno svojih obaveza i odgovornosti u odnosu na sigurnost.

Na voditelju je OA NCARH da osigura školovanje za područje sigurnosti.

Ova obuka uključuje školovanje svih novih članova osoblja o Općim pravilima sigurnosti te potpuno objašnjenje svih odgovornosti.

Nove sigurnosne procedure ne smiju biti uvedene bez odgovarajućeg programa školovanja koji osigurava upoznavanje osoblja s njihovim novim odgovornostima.

5.5. Računala i softver u privatnom vlasništvu

Opremu u privatnom vlasništvu zabranjeno je priključiti na NCARH računalni sustav. Nema iznimki za ovo pravilo.

Prijenosna računala koje upotrebljavaju osobe pod ugovorom ne smiju se priključiti na produkcijsku mrežu NCARH.

Korištenje privatnih vanjskih medija pri priključivanju na NCARH sustav je zabranjena.

Sva su NCARH računala konfigurirana za standardiziranu operativnu okolinu. Promjenu ove okoline, odnosno dodavanje, brisanje ili promjenu softvera mora dopustiti voditelj OA NCARH-a.

5.6. Autorska prava na softver

Autorska prava ograničavaju načine upotrebe softvera i podataka. Bilo koje narušavanje autorskih prava može izazvati sudski postupak protiv osobe i/ili tvrtke. Cjelokupno osoblje OA NCARH-a mora se pridržavati pravila, da softver zaštićen autorskim pravima i pripadajući materijal, upotrebljavaju u skladu s uvjetima licenci koje se na to odnose. Osoblje smije koristiti samo legalni softver. To znači softver koji je legalno nabavljen ili razvijen i upotrebljava se u skladu s uvjetima nabave.

Sistemski administratori moraju osigurati primjenu i održavanje mehanizama koji provjeravaju je li upotrebljavan samo legalni softver. Bilo koji neautorizirani softver otkriven na mreži odmah treba prijaviti voditelju OA NCARH-a.

Voditelj OA NCARH mora osigurati da svi zaposlenici budu obaviješteni o odredbama politike autorskih prava te propisanim procedurama kojih se mora pridržavati.

5.7. Elektronička pošta

Elektroničku poštu koriste kao pomoć zaposlenici u svakodnevnom izvršavanju svojih zadataka. Ako se elektronička pošta koristi za slanje osobnih poruka, one će biti tretirane kao i poruke koje se odnose na posao.

Osobna upotreba ne smije:

- preklapati se s normalnim radnim aktivnostima;
- biti povezana s nekom vanjskom poslovnom aktivnošću;
- biti za bilo koju aktivnost koja može ugroziti NCARH.

Ako je primljena bilo kakva poruka koja je uvredljiva, anonimna ili se čini da je primljena od nekoga tko nije pravi pošiljatelj, o tome treba obavijestiti voditelja OA NCARH.

Svaka je zlouporaba e-mail sustava neprihvatljiva i to povlači sankcije ili druge disciplinske akcije.

5.8. Sankcije

Ako se otkrije da je autorizirani zaposlenik zlouporabio resurse na koje mu je bio odobren pristup i/ili je izvršio aktivnosti štetne za sigurnost tih resursa, takva aktivnost mora biti dokumentirana i o tome mora biti obaviješten voditelj OA NCARH-a, koji treba o tome obavijestiti PMA HR PKI.

Sankcije će protiv zaposlenika pod ugovorom biti u skladu s odredbama ugovora.

Ovisno o prirodi zaposlenikove akcije, sankcije se mogu kretati od savjetovanja ili suspenzije prava pristupa sustavu do otkaza ugovora o radu i/ili druge pravne akcije.

6. UPRAVLJANJE NCARH SUSTAVOM

6.1. Kontrola upravljanja

Kontrola upravljanja NCARH sustavom je uvedena da bi se osiguralo da promjene konfiguracije ne proizvode samo željeni učinak nego da, također osiguravaju i normalan nastavak dnevnih aktivnosti. Jedan je od takvih zahtjeva sigurnost NCARH sustava. Stoga kontrola izmjene konfiguracije sustava osigurava da predložene promjene na temeljnoj konfiguraciji ne degradiraju sigurnost sustava na bilo koji način. Sve promjene temeljne konfiguracije sustava zahtijevaju ponovnu procjenu rizika i opasnosti.

Kontrola će se izmjene konfiguracije provoditi da bi se nadgledalo sve promjene temeljne konfiguracije na računalima, na svim NCARH mrežama, uključujući:

- hardverske promjene,
- softverske promjene,
- dokumentaciju hardverskih i softverskih promjena.

Potpuno je dokumentirana temeljna konfiguracija uspostavljena za NCARH. Ova se konfiguracija nadopunjuje na istovjetan način za cijeli sustav.

PMA HR PKI će odobravati sve promjene NCARH konfiguracije.

Sve promjene na temeljnoj konfiguraciji bilo da se radi o hardveru, softveru ili dokumentaciji moraju biti zabilježene **mehanizmom kontrole promjena**.

6.2. Povjerenstvo za kontrolu promjena

Povjerenstvo za kontrolu promjena čine:

- predstavnici PMA HR PKI;
- predstavnici OA NCARH:
  - *osoblje zaduženo za sigurnost;*
  - *sistem administratori;*
  - *osoblje zaduženo za operativni rad.*

Ovo povjerenstvo mora razmotriti svaku promjenu u hardveru, softveru ili procedurama i utjecaj svake promjene na sigurnost i raspoloživost mreže. Jednom kad je dopuštenje za promjenu dano, zahtjev za promjenu se prosljeđuje PMA HR PKI za konačnu autorizaciju.

Promjene se ne smiju provesti prije nego što PMA HR PKI izvrši njihovu autorizaciju.

6.2.1. Kontrola softvera

Kontrola softvera uključuje odabir softvera, instalaciju, razvoj i dokumentaciju softvera. Povjerenstvo za kontrolu promjena nadzire sav operativni softver NCARH. Jedina iznimka su programi koji se upotrebljavaju za svrhe razvoja, koji se mogu koristiti samo u razvojnoj okolini, odvojeno od produkcijske mreže.

6.3. Operacije

Transportni mehanizmi za ključeve i certifikate osiguravaju da isključivo pravi vlasnici dobivaju privatne ključeve i njihove certifikate, te da autorizirani korisnici dobivaju javne ključeve.

Uspostavljen je X.500 imenik koji omogućuje pristup statusima certifikata i javnim ključevima.

Dokumentacija za planiranje i održavanje HR PKI sustava osigurava pravilnu operativnost servisa.

Minimalna dokumentacija sadrži:

- koncept operacija;
- procjenu rizika i opasnosti;

- plan sigurnosti informatičkog sustava;
- plan za oporavak u slučaju nezgode;

6.4. Tehnologija

NCARH, CA-ovi i RA-ovi čine HR PKI hijerarhiju.

NCARH će raditi u skladu sa sigurnosnim standardima, što pokriva sljedeća područja:

- pripremu;
- okolinu;
- tehničku sigurnost;
- inspekciju i izvješćivanje o sigurnosti;
- poseban značaj mreže;
- sigurnost malih sustava;
- ostala područja.

Nitko od OA NCARH osoblja ne smije:

- koristiti bilo koji računalni ili mrežni uređaj bez ispravne autorizacije;
- pomagati, ohrabriti bilo koju neautoriziranu upotrebu ili pokušaj neautorizirane upotrebe računalnog ili mrežnog uređaja;
- svjesno dovesti u opasnost sigurnost bilo kojeg računala ili mrežnog uređaja.

7. SIGURNOST INFRASTRUKTURE

7.1. Sigurnost mreže

Norme koje se primjenjuju za sigurnost mreže za NCARH računalni sustav su u skladu s međunarodnim normama. Fizički pristup komunikacijskoj opremi odobrava voditelj OA NCARH.

Da bi se osigurala sigurna mrežna okolina, NCARH produkcijska mreža oblikovana je upotrebom kombinacije vatrozidova, visoko raspoloživog softvera za vatrozid i sustava za otkrivanje pokušaja upada u sustav. S namjenskim sustavom za upravljanje mrežom, nadziranjem u realnom vremenu cijele mrežne infrastrukture, operativnom osoblju NCARH omogućeno je pravodobno upozorenje ako se nešto neregularno događa na mreži.

Također, postoji sustav bilježenja ako se dogodi bilo koji incident na mreži.

7.2. Konfiguracija vatrozida

Konfiguracija vatrozidova (firewall) na NCARH produkcijskoj mreži smatra se sa stanovišta sigurnosti posebno osjetljivom i zato je klasificirana kao "**visoko zaštićena**".

Samo voditelj OA NCARH, glavni CSP i specijalist sigurnosti imaju pristup tim informacijama.

8. SIGURNOST PODATAKA

Vlasnik je informacije odgovoran da se podaci koji se nalaze pod njegovom kontrolom klasificiraju u skladu s njihovom tajnošću, osjetljivošću i kritičnošću.

8.1. Obilježavanje i pohranjivanje osjetljivih medija

Kada se osjetljive informacije zapisuju na disketu, magnetsku vrpcu, smart karticu, optički medij za pohranu ili druge medije, medij mora biti označen s najvišom klasifikacijom pohranjenih informacija. Kada nisu u upotrebi, svi mediji s tom klasifikacijom podataka moraju biti pohranjeni u sigurne kontejnere.

8.2. Sigurnost medija

Izraz IT mediji za pohranjivanje odnosi se na magnetske vrpce, kasete, tvrde diskove, optičke medije za pohranu i drugu opremu za pohranjivanje podataka.

Sistemski administratori su odgovorni da kada IT medij za pohranjivanje bude ponovno korišten ili stavljen izvan upotrebe ne postoji mogućnost narušavanja tajnosti podataka zbog neautoriziranog pristupa podacima na mediju.

Mediji koji su bili upotrebljavani za pohranjivanje visoko zaštićenih informacija ne smiju se ponovo koristiti za pohranjivanje informacija niže sigurnosne klasifikacije. Voditelj je OA NCARH odgovoran za osiguranje IT medija za pohranjivanje, tj. spremanje u sigurne kontejnere.

8.3. Prijenos i pohranjivanje podataka

Bilo koji IT medij za pohranjivanje koji se upotrebljava za prijenos informacija ne smije sadržavati nikakve informacije za pristup kojima primatelj nema autorizaciju. Ako se prisutnost informacija na korištenim medijima ne može odrediti, mora se koristiti novi medij za prijenos podataka. Mediji za pohranjivanje koji su ranije sadržavali visoko klasificirane informacije ili podatke ostaju rangirani u sigurnosnoj klasifikaciji tih podataka.

8.4. Prijenosna računala

Osoba koja je preuzela opremu odgovara za zaštitu NCARH prijenosnih računala i podataka koji se nalaze na njima.

Kada se upotrebljavaju za obradu osjetljivih informacija, prijenosna će računala bit konfigurirana tako da zahtijevaju zaporku prilikom prijave.

Svi osjetljivi podaci koji se čuvaju na tvrdom disku prijenosnog računala, enkriptirani su automatskim procesom enkripcije.

Prijenosna računala trebaju imati ažurne verzije programa za detekciju i zaštitu od virusa.

Prijenosna računala, kad nisu pod nadzorom, moraju uvijek biti čuvana na sigurnom.

8.5. Računalni virusi

Voditelj je OA NCARH odgovoran:

- da je instalirana zaštita od zlonamjernog koda na sve poslužitelje i računala koja rade na svim NCARH mrežama;
- da su nove verzije programa za zaštitu od zlonamjernog koda instalirane na svim računalima i mrežnim poslužiteljima, i to odmah čim su one raspoložive.

Svi vanjski mediji koji ulaze u NCARH prostor moraju prije uporabe biti provjereni na zlonamjerni kod, a provjeru provodi osoba zadužena za sigurnost.

Svi korisnici moraju hitno obavijestiti voditelja OA NCARH sumnjaju li na zlonamjerni kod **ili program koji uništava sadržaj na mediju. Time će se osigurati pravodobno poduzimanje radnji koje će spriječiti daljnje** širenje zlonamjernog koda.

8.6. Arhiva

8.6.1. Tipovi pohranjenih podataka

NCARH arhivira sljedeće tipove podataka, automatski ili ručno:

- događaje koji su predmet revizije;
- certifikate i CRL;
- javne ključeve;
- izvještaje o kompromitiranosti, neusklađenosti i prijepisku.

8.6.2. Period arhiviranja

NCARH arhivira zapise dnevnika sustava na vremenski period od najmanje 10 godina. Certifikati, CRL i javni ključevi se arhiviraju na vremenski period od najmanje 30 godina. NCARH prepiska se arhivira na vremenski period od najmanje 10 godina.

9. FIZIČKA ZAŠTITA

Zgrada u kojoj se nalazi NCARH operativni centar je sigurna zgrada, koja ima višeslojne sigurnosne barijere.

Sigurnosna tehnologija koja se koristi u operativnom centru sastoji se od integriranih rješenja suvremenih tehnologija koje zadovoljavaju zahtjeve visoke razine sigurnosti.

9.1. Vođenje evidencije pristupa NCARH prostoru

Voditelj je OA NCARH odgovoran za vođenje evidencije pristupa te održavanje svih kontrola pristupa u NCARH. Izmjene će se u pristupnoj listi održavati ažurno.

9.2. Evidentiranje imovine

Sva se imovina, uključujući računalnu opremu, namještaj i računalni softver evidentira u "**Registru imovine"**. Ovaj registar održava voditelj OA NCARH i dopunjava se u sljedećim situacijama:

- instaliranje/deinstaliranje/promjena uređaja i softvera;
- postojeća se imovina ne može servisirati zbog:
  - *oštećenja;*
  - *dotrajalosti;*
  - *promjene u tehnologiji.*
- prijenos uređaja na drugu lokaciju tvrtke;
- dogradnja.

Sva je imovina označena s jedinstvenom identifikacijskom oznakom, čiji se detalji bilježe u registru imovine zajedno s punim opisom pojedinog predmeta (komada/dijela).

10. NARUŠAVANJE SIGURNOSTI

10.1. Unutarnje narušavanje sigurnosti

U slučaju unutarnjeg narušavanja IT sigurnosti, od strane zaposlenika, glavni CSP obavještava PMA HR PKI, te se poduzimaju mjere u skladu s internim pravilnicima i zakonom.

U takvim situacijama ima više mogućnosti izbora:

- formalni sastanak sa zaposlenikom i otkaz ugovora o radu ili službena opomena;
- u slučaju industrijske špijunaže, slučaj se može sudski procesuirati.

Svi će relevantni zapisi podataka biti potrebni kao evidencija za dalje sudsko procesiranje. Zato oni moraju biti ispravno označeni i spremljeni na sigurnu lokaciju.

10.2. Vanjsko narušavanje sigurnosti

Dođe li do vanjskog narušavanja sigurnosti NCARH računalne mreže, prioritet je zaustavljanje same te akcije. Ako je osoba pokušala pristupiti mreži, svi napori moraju biti učinjeni za zaustavljanje tog pristupa. Ako je pristup bio uspješan, tada se mora primijeniti plan za odgovor na kritični incident. U tom su slučaju pohranjeni zapisi važni, jer će to pomoći pri izoliranju prvog pristupa ili bilo kojeg višestrukog pristupa.

Sve datoteke zapisa sustava na poslužiteljima moraju biti održavane i pohranjene na sigurnom mjestu.

10.3. Procedure izvještavanja o unutarnjem ili vanjskom narušavanju sigurnosti

U slučaju bilo kakvog unutarnjeg ili vanjskog narušavanja sigurnosti, treba slijediti sljedeće procedure:

- obavijest voditelju OA NCARH;
- detaljni izvještaj PMA HR PKI;
- voditelj OA NCARH i PMA HR PKI donose odluku o daljnjim akcijama ;
- specijalist će sigurnosti pretražiti i zadržati sve relevantne zapise sustava na poslužiteljima. U slučaju da su datoteke bile promijenjene one moraju biti izolirane za analize revizora, a za vrijeme ovog procesa trebaju biti izrađene bilješke o svim poduzetim akcijama
- sustav treba biti vraćen u zadnje radno stanje.

Ako bilo koje narušavanje sigurnosti ima utjecaj na nekog sudionika o tome treba obavijestiti osoblje koje kontaktira s korisnicima.

11. OSIGURANJE KONTINUITETA POSLOVANJA

11.1. Procjena ranjivosti

Da bi osigurao najviši stupanj sigurnosti PMA HR PKI poslovanja formira skupinu za procjenu ranjivosti i saniranje kriznih situacija. Skupina se sastoji od:

- člana PMA HR PKI,
- voditelja OA NCARH i glavnih CSP,
- specijalista sigurnosti.

Skupina provodi reviziju konfiguracije NCARH aplikacijskog i operativnog softvera, kao i periodična testiranja konfiguracije vatrozida, usmjerivača, podatkovne osnovice i javnog imenika.

11.2. Plan oporavka u slučaju incidenta

Voditelj OA NCARH operacija je odgovoran za održavanje ažurnih i važećih planova za oporavak u slučaju incidenta. Takovi će planovi bit testirani i pregledavani redovito po nalogu PMA HR PKI-a.

Specijalist sigurnosti odgovoran je za identificiranje rizika i provedbu ponovne procjene rizika.

Osoblje NCARH će se prema svojim odgovornostima redovito uvježbavati za provođenje primjerenih procedura za slučaj nezgode.

Procedure izrade sigurnosnih kopija sustava trebaju biti odgovarajuće, detaljne i aktualne da bi odgovarale potrebama oporavka sustava.

Nužno je da postoje procedure za vraćanje sustava u normalan rad nakon nezgode.

PMA HR PKI je odgovoran za uspostavu plana za oporavak u slučaju nezgode, što uključuje sljedeće:

- procedure za izradu sigurnosnih kopija sustava koje su dovoljne za obnovu uređaja i kritičnih aplikacija, i njihovo arhiviranje;
- upute za procjenu hitnih situacija i određivanje akcija za njihovo rješavanje,
- određivanje uvjeta za prelazak na drugu lokaciju, izvojenu od sustava certificiranja u uporabi, prelazak na tu lokaciju, te povratak na primarnu lokaciju,
- procedure za izradu sigurnosnih kopija NCARH baza podataka, te povrat podataka i softvera,
- procedure za testiranje.

Cjelokupno NCARH osoblje koje bi radilo u ovakvim situacijama mora biti informirano o svojim odgovornostima i mora biti redovito obučavano za svoje zadaće.

Plan za oporavak u slučaju nezgode i plan za nastavak rada su izrađeni tako da osiguraju pravodoban oporavak za nastavak rada u slučaju velikih nezgoda. Plan osigurava brzi nastavak bitnih operacija.

Plan mora biti redovito testiran da bi se provjerila izvedivost. Scenarij će za provjeru plana bit izrađen te će se naznačiti kako i kada će se pojedini elementi plana provjeriti.

Plan zbog promjena u poslovanju zastarijeva brzo i zbog toga će biti dopunjavan dva puta godišnje da bi se osigurala njegova stalna učinkovitost.

Primjeri izmjena koje mogu nastati su ovi:

- nova oprema;
- dopuna ili promjena operacijskog sustava;
- primjena nove tehnologije za kontrolu pristupa i detekciju ulaska;
- promjene osoblja;
- promjene ugovornih odnosa i isporučitelja;
- promjena telefonskih brojeva i adresa;
- prestanak rada, izmjena ili uvođenje novih poslovnih procesa;
- promjena u postupcima rada na sustavu;
- promjene u zakonskoj regulativi.

11.3. Odaziv na kritične nezgode

PMA HR PKI formira skupinu za odaziv na kritične nezgode, da bi pravodobno odgovorili na kritične nezgode te da bi se primijenio plan za oporavak u slučaju nezgode. Skupina se sastoji od člana PMA HR PKI, voditelja OA NCARH i glavnog korisnika.

Zadatak skupine je:

- odrediti pristupne točke resursima;
- minimalizacija učinka bilo koje nezgode na NCARH poslovnu praksu;
- primjena strategija za minimiziranje štete;
- hitna reakcija na nezgodu;
- prikupljanje podataka za disciplinske postupke;
- izvještavanje PMA HRPKI.

Neke nezgode zahtijevaju taktičke odluke, primjerice, prekid aktivnosti koja je izazvala incident, o čemu će odluku donijeti PMA HR PKI, vodeći računa o sljedećem:

- prioritet je minimiziranje rizika ili opasnosti za NCARH sustav;
- identificiranje slabosti u sustavu;
- identificiranje osoba koje su sudjelovale u nezgodi;
- važnost prikupljenih informacija.

Voditelj OA NCARH vodi evidenciju za sve kritične nezgode. Tu dokumentaciju pregledava PMA HR PKI i ona se čuva za potrebe revizije.