SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI ZADATAK br. 1714

SIGURNOSNA POLITIKA

mentor: doc.dr.sc. Marin Golub
Damir Kovačević

Zagreb, veljača 2008.

Zahvaljujem se svojoj obitelji, prijatelju Zvonimiru i djevojci Ani koji su mi bili velika podrška i motivacija tijekom studija.

Posebno bih se zahvalio svom mentoru, profesoru Marinu Golubu na stručnom vodstvu i pomoći u nastanku ovog rada.

Sažetak

Ovim radom dan je kratak uvid u osnovne pojmove sigurnosti informacijskih sustava, prikazani su problemi sigurnosti informacijskih sustava s naglaskom na glavne probleme današnjice, te je na primjeru pokazan način izrade dokumenta sigurnosne politike prema normi ISO/IEC 17799:2005.

Abstract

This paper presents short introduction of basic terms in the field of information security systems; nformation security systems issues are presented with emphasis on main actual problems. The development process of security policy document, based on ISO/IEC 17799:2005, is shown at an example.

Sadržaj

1. Uvod

Razvojem računala i računalnih tehnologija život je čovjeku uvelike olakšan. Mnoge poslove koje je do tada obavljao čovjek sada obavljaju i kontroliraju računala. Na sve pozitivno što pruža računalna tehnologija sjenu baca njena negativna strana, a to je računalni kriminal. Računalni kriminal danas je jedan od najznačajnijih i najbrže rastućih vrsta kriminala uopće i stoga mu se pridodaje sve veća pažnja.

Shvativši ozbiljnost problema stručnjaci za sigurnost od samog nastanka računalnog kriminala počeli su razmišljati na koji način zaštiti računala i računalne sustave od zlonamjernih korisnika, tzv. hakera. Tražeći adekvatna rješenja razvili su mnoge danas poznate metode zaštite, no zanemarili su jednu činjenicu, a to je ljudski faktor.

Sigurnost informacijskih sustava danas se u tehničkom pogledu za relativno malo novaca (i puno znanja) može dovesti praktički do savršenstva. Usprkos tome u IT svijetu sve je veći problem sigurnost informacijskih sustava. Što je uzrok ove kontradikcije? Godinama su se ogromne količine novca ulagale u poboljšanje tehničke komponente zaštite sustava kao što su sigurnosne stijene (eng. f*irewall*), izrade sigurnosnih kopija podataka, siguran fizički smještaj opreme itd. Svi ti elementi zaštite itekako su bitni, bez njih informacijski sustav zasigurno ne bi mogao biti siguran, no činjenica je da se u edukaciju korisnika ulagalo vrlo malo, ponekad i ništa. Navedeni propust prepoznali su zlonamjerni korisnici te su svoje napade počeli temeljiti na način da od ovlaštenih korisnika prikupljaju informacije koje im uvelike olakšavaju izvršavanje zlonamjernih radnji.

Danas je broj korisnika računala, Interneta i informacijskih sustava vrlo velik. Velik dio njih moglo bi se nazvati needuciranim i nemarnim korisnicima. Budući se ne znaju koristiti računalom (Internetom), rad za računalom svodi im se na unaprijed „naštrebane“ radnje ili čine ono što im netko savjetuje. Navedenu „vrlinu“ prepoznali su zlonamjerni korisnici kao mogućnost jednostavnog pribavljanja podataka o sustavu ili čak zaporke za prijavu na sustav. Iskorištavanjem naivnosti korisnika hakeri elegantno dolaze do podataka do kojih su u prošlosti morali dolaziti mukotrpnim traženjem propusta u operacijskim sustavima, programima i sigurnosnim zaštitama, te je stoga ovaj način napada postao vrlo popularan.

Stručnjaci za sigurnost sve više shvaćaju veličinu ovog problema, koja nije u njegovoj kompleksnosti ili ne postojanju rješenja. Ono što problem čini velikim je enorman broj korisnika koje treba educirati i potaknuti da razmišljaju „svojom glavom“. Relativno jednostavnom edukacijom korisnika i poticanjem na razmišljanje broj sigurnosnih napada izvedenih na ovaj način višestruko bi se smanjio. Dodatnu veličinu ovom problemu zadaju rukovoditelji organizacija. Često su i oni sami u onoj skupini needuciranih korisnika, te im nije jasno zašto je potrebno izdvajati sredstva za educiranje korisnika „da ne pružaju hakerima povjerljive informacije“.

Iako moderni načini ugrožavanja sustava od strane hakera trenutno zadaju najviše problema sigurnosnim stručnjacima, prilikom razmatranja sigurnosti informacijskih sustava nikako se ne smije zaboraviti na ustaljene načine zaštite. Hakeri su osobe koje će pokušati ugroziti naš sustav na svaki mogući način, bilo da se radi o „normalnom“, „modernom“ ili nekom trećem načinu osmišljenom od strane samog hakera.

Bez obzira na djelovanja hakera, cilj osobe odgovorne za sigurnost informacijskog sustava jest poduzeti niz radnji s ciljem smanjenja ranjivosti sustava i povećanju njegove sigurnosti. Informacijski sustav ne može se u potpunosti zaštiti i to je činjenica koje mora biti svjestan svaki korisnik. Radnje odgovornih osoba u cilju povećanja sigurnosti sustava vrlo su individualne zbog individualnosti samih informacijskih sustava i stoga se ne mogu definirati univerzalne radnje prema kojima bi se gradila sigurnost sustava. Individualnost je u planiranju sigurnosti i vrlo preporučljiva, jer se na taj način otežava planiranje i izvršavanje napada od strane zlonamjernih korisnika.

Sigurnost informacijskih sustava vrlo je kompleksna i široka tema u kojoj je jasna jedino činjenica da bez kvalitetnog programa sigurnosti sustav nije moguće u cijelosti zaštiti. Kvalitetan program omogućava uspostavu sigurnosti na svim kritičnim točkama sustava, u bilo kojem segmentu sigurnosti, a jedan od najboljih programa za postizanje navedenog cilja zasigurno je definiranje sigurnosne politike.

2. Sigurnosna politika

2.1 Što je sigurnosna politika

Informacijski sustavi sadrže podatke kojima se služe ovlašteni korisnici i koji služe kako bi korisnicima bilo omogućeno korištenje sustavom (ime identifikacije, lozinka itd.). Budući takvi podaci ne smiju biti javno dostupni (moraju biti tajni), ne smiju biti mijenjani bez odobrenja i ne smiju biti nedostupni korisnicima, važno je provesti određene korake sigurnosti kako bi navedeni uvjeti uvijek bili zadovoljeni.

Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti. Ona govori korisnicima što smiju raditi, što ne smiju raditi, što moraju raditi i koja je njihova odgovornost (određuje sankcije ukoliko se korisnik ne pridržava pravila određenih sigurnosnom politikom). Politikom ne određujemo na koji način zaštiti informacijski sustav već samo što zaštititi. Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sustav. Stoga definiranje općenite sigurnosne politike za informacijske sustave nije moguće i jednom napisana politika mora se redovito pregledavati, mijenjati i nadopunjavati kada se za tim ukaže potreba.

Sigurnosnom politikom definirana su pravila koja se odnose na:

- svu računalnu opremu institucije (hardver i softver),
- osobe odgovorne za administraciju informacijskog sustava,
- sve zaposlenike i korisnike sustava, odnosno osobe koje imaju pravo pristupa,
- vanjske suradnike (npr. ovlaštene djelatnike zadužene za održavanje sustava).

Sigurnosnom politikom obuhvaćaju se široka područja sigurnosnih mjera, ali nisu svi dijelovi politike potrebni pojedinim skupinama korisnika. Na primjer, zaposlenici koji koriste sustav ne trebaju znati dio politike koji se odnosi na sigurnost tehničke opreme ili onaj dio namijenjen vanjskim suradnicima. Stoga je preporučljivo sigurnosnu politiku pisati u više dijelova.

Korisnici, kojima je sigurnosna politika namijenjena, često nemaju strpljenja čitati mnoštvo stranica teksta. Oni uglavnom imaju vrlo mala znanja o tehnologijama koje koriste pri radu i zbog toga je nužno definirati sigurnosnu politiku tako da bude kratka i jasna, napisana na način da ju korisnici mogu razumjeti. Politiku napisanu opširno i stručnim jezikom običan korisnik ne razumije i površno ju ili nikako ne analizira, pa je stoga ne može niti primijeniti.

Nakon definiranja sigurnosne politike važno je osigurati da se pravila koja su definirana sigurnosnom politikom provode i poštuju. Kako bi se to postiglo bitno je svakom korisniku sustava dati na znanje da je sigurnosna politika uvedena i upoznati ga s njegovim dužnostima. Postoji više načina kako korisnike upoznati sa sigurnosnom politikom, npr. dijeljenjem dokumenta politike ili objavljivanjem sigurnosne politike na web stranicama kompanije.

2.2 Uloga sigurnosne politike

Sigurnost informacijskih sustava bazira se na ljudima. Tehnologijom nije moguće u potpunosti osigurati sigurnost sustava i stoga je važno uvesti dodatne mjere, a prvi korak k tome je definiranje sigurnosne politike. Primarna uloga sigurnosne politike je određivanje prihvatljivog i neprihvatljivog načina ponašanja kako bi zaštitili vrijednosti informacijskog sustava, uključujući opremu (*eng. hardware*), programsku podršku (*eng. software*) i podatke.

Na temelju pravila definiranih u dokumentu, njen je zadatak osigurati tri jedinstvena svojstva informacija:

- povjerljivost (tajnost),
- integritet,
- dostupnost.

Povjerljivost (eng. *confidentiality*)

Povjerljivost je zaštita podataka koje sadrži sustav od neovlaštenog pristupa. Iako je opće mišljenje da je ovaj tip zaštite od najveće važnosti za državne institucije i vojsku jer svoje planove i mogućnosti moraju čuvati tajno od mogućih neprijatelja, ono također može biti značajno za kompanije koje imaju potrebu zaštititi poslovne planove i informacijske vrijednosti od konkurencije ili kako bi zaštitili podatke od neovlaštenog pristupa. Problemima privatnosti, koji u zadnjih par godina privlače sve više interesa, posvećuje se sve više pažnje, kako u državnim institucijama tako i u privatnom sektoru. Ključni aspekt povjerljivosti je identifikacija korisnika i provjera autentičnosti.

Identifikacija je proces prijave korisnika na sustav, pri čemu sustav zna da takav korisnik postoji. Na primjer, korisnik A želi se prijaviti na sustav. Sustav provjeri da li je korisnik A prijavljen na sustav i ako je tada slijedi proces provjere autentičnosti. Provjera autentičnosti je proces kojim sustav želi biti siguran da je korisnik koji se prijavljuje pod imenom A upravo osoba A. Postoji više načina provjere autentičnosti. Najraširenija je unos lozinke, ali se i sve više razvija tehnička oprema koja jedinstvene ljudske osobine, poput otiska prsta ili mrežnice oka pretvara u digitalne signale. Na primjer, kako bi sustav provjerio da li je korisnik koji se pokušava prijaviti kao osoba A upravo ta osoba, može pri prijavi tražiti od korisnika A određenu lozinku koju zna samo osoba A. Ako korisnik A pošalje upravo tu lozinku, sustav zna da je korisnik upravo osoba A. U suprotnom, korisnik nije osoba A te mu sustav ne dozvoljava korištenje sustava.

Povjerljivost može biti narušena na nekoliko načina. Navedene su najčešće prijetnje povjerljivosti:

- hakeri,
- lažno predstavljanje,
- neovlaštena aktivnost,
- nezaštićeno preuzimanje podataka,
- trojanski konji itd.

Hakeri. Hakeri su osobe koje koriste sigurnosne slabosti sustava na način da neovlašteno koriste sustav ili ga onesposobe. Mnogi hakeri, osim sigurnosnih slabosti sustava, koriste i metode otkrivanja lozinki ovlaštenih korisnika. Naime, lozinke koje su riječi koje se nalaze u rječniku ili često korištene lozinke, iskusnijim hakerima pomoću programske podrške vrlo lako je otkriti. Otkrivanjem lozinke korisnika haker se prijavljuje na sustav kao ovlašteni korisnik i vrlo jednostavno obavlja kopiranje, brisanje ili mijenjanje podataka, ili ih kopira na lokacije s kojih su dostupni određenom krugu ljudi ili čak svim korisnicima Interneta. Iz tih razloga aktivnost hakera predstavlja veliku opasnost povjerljivosti informacija.

Lažno predstavljanje. Lažno predstavljanje je prijetnja u kojoj korisnik preko lozinke drugog korisnika dobiva mogućnost pristupa sustavu pod drugim imenom, te mu se na taj način „otvaraju vrata“ za obavljanje zlonamjernih radnji. Lažno predstavljanje je čest slučaj u kompanijama koje dozvoljavaju korisnicima da razmjenjuju lozinke.

Neovlaštena aktivnost. Ovaj tip aktivnosti događa se kad ovlašteni korisnik sustava koristi podatke za koje nema ovlasti. Nedovoljna kontrola pristupa i zaštita podataka omogućuju neovlašten pristup, što može ugroziti njihovu povjerljivost.

Kopiranje podataka na nezaštićene lokacije. Kopiranje podataka može ugroziti njihovu povjerljivost ukoliko se podaci kopiraju na sustav s nedovoljnom sigurnosnom zaštitom. Primjer ove vrste prijetnje je kopiranje podataka sustava na lokacije sustava koje nemaju adekvatnu razinu zaštite. Ukoliko do kopiranih podataka pristup imaju ostali ovlašteni korisnici sustava njihova je tajnost ugrožena.

Lokalna mreža. Lokalna mreža predstavlja prijetnju jer podaci koji putuju mrežom mogu biti dohvaćeni u svakom čvoru mreže. Kako bi se izbjegla ova vrsta prijetnje svi tajni podaci koji bi smjeli biti dostupni samo u određenim čvorovima moraju biti kriptirani kako bi njihova povjerljivost ostala neupitna.

Trojanski konji. Trojanski konj je vrsta aplikacije koja može izazvati vrlo velike štete sustavima. Primjer trojanskog konja je aplikacija instalirana na računalo sustava nakon što ga nesvjesno pokrene ovlašteni korisnik, te je tako programirana da kopira podatke na nezaštićene dijelove sustava. Jednom pokrenut, trojanski konj ostaje aktivan na sustavu i konstantno obavlja programirane zadatke.

Integritet (eng. *integrity*)

Integritet predstavlja zaštitu podataka od namjernog ili slučajnog neovlaštenog mijenjanja. Dodatni element integriteta jest zaštita procesa ili programa kako bi se onemogućilo neovlašteno mijenjanje podataka. Glavni zahtjev komercijalnih i državnih institucija jest osigurati integritet podataka kako bi se izbjegle zlouporabe i greške. To je imperativ kako korisnici ne bi mogli mijenjati podatke na način da ih izbrišu, promjene ili učine ključne podatke nesigurnima. Primjeri gdje je integritet podataka od ključne važnosti su sustav za kontrolu leta, sustavi u medicinskim ustanovama, sustavi u financijskim ustanovama itd.

Ključni elementi za postizanje integriteta podataka su identifikacija i provjera autentičnosti korisnika. Budući integritet ovisi o kontroli pristupa, važno je pozitivno i jedinstveno utvrditi identičnost svih korisnika prijavljenih na sustav.

Zaštita integriteta

Kao i povjerljivost, integritet može biti ugrožen od hakera, lažnog predstavljanja, neovlaštenih aktivnosti i nedozvoljenih programa (virusi, trojanski konji) jer sve navedene aktivnosti mogu dovesti do neovlaštenog mijenjanja podataka.

Osnovni principi za kontrolu integriteta:

- dodjeljivanje pristupa na temelju potreba,
- razdvajanje obaveza,
- rotiranje obaveza.

Dodjeljivanje pristupa na temelju potreba. Korisnici bi trebali dobiti pristup samo onim podacima koji su im potrebni kako bi mogli obavljati zadane poslove. Korisnikov pristup ključnim podacima trebao bi biti dodatno ograničen kvalitetno definiranim transakcijama koje osiguravaju da korisnik podatke može mijenjati u strogo kontroliranim uvjetima kako bi se sačuvao integritet podataka. Bitan element kvalitetno definiranih transakcija je bilježenje podataka o mijenjanju podataka (tko, kada i koje podatke) kako bi se moglo utvrditi da li su podaci ispravno mijenjani od

ovlaštene osobe. Kako bi bile djelotvorne, transakcije bi trebale dopuštati izmjenu podataka samo od unaprijed odabranih programa. Odabrani programi moraju biti ispitani kako bi se izbjegla neovlaštena aktivnost.

Kako bi korisnici mogli uspješno koristiti sustav, privilegija pristupa mora biti razumno raspodijeljena kako bi se omogućila potrebna operativna fleksibilnost. Dodjeljivanje pristupa na temelju potreba ima zadaću osigurati maksimalnu kontrolu uz minimalno ograničavanje korisnika.

Razdvajanje obaveza. Kako bi se osiguralo da niti jedan pojedinac nema kontrolu transakcije od početka do kraja, dvoje ili više ljudi moralo bi biti odgovorno za obavljanje njezinog izvršavanja. Jedan od načina razdvajanja obaveza je da se svima koji imaju dozvolu za kreiranje transakcije ukine pravo izvršavanja transakcija. Time se sprječava da se transakcije koriste za obavljanje vlastitih interesa, osim ukoliko se suglase sve odgovorne osobe.

Rotiranje obaveza. Radne obaveze pojedinih zaposlenika trebale bi se periodično mijenjati kako bi kontroliranje transakcija za osobne potrebe bilo još kompliciranije. Ovaj princip je efektivan u kombinaciji s razdvajanjem obaveza. Problem u rotiranju obaveza se obično javlja u organizacijama s ograničenim brojem kvalificiranog kadra.

Dostupnost (eng. *availability*)

Dostupnost je garancija ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku kad za njim imaju potrebu.

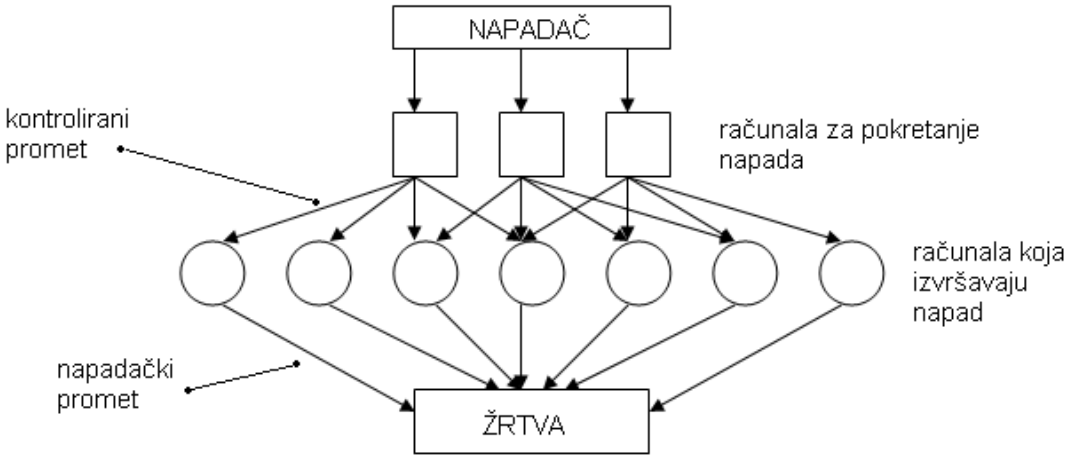
Dva su najčešća uzroka neraspoloživosti sustava:

- odbijanje usluge (*eng. Denial Of Service*) i
- gubitak mogućnosti obrade podataka.

Odbijanje usluge (DoS) svaki je zlonamjeran napad kojem je cilj uskraćivanje legitimnim korisnicima mogućnost pristupa (Internet) uslugama (npr. web poslužitelj). Napad odbijanja usluge možemo podijeliti u dvije kategorije:

1. *Ranjivost poslužitelja na napade odbijanja usluge*: napadi koji iskorištavaju poznate greške (propuste) u operacijskim sustavima i poslužiteljima. Ovi napadi koriste se za „rušenje“ programa. Na taj način uskraćuju se usluge (servisi) koji ti programi pružaju. Primjeri ranjivih operacijskih sustava uključuju sve sustave, kao što su na primjer Windows NT ili Linux, također i različite poslužitelje kao što su DNS ili Microsoft`s IIS Server. Svi ovi programi, koji imaju važnu i korisnu funkciju, posjeduju programske propuste (eng. *bug*) koje hakeri koriste kako bi ih „srušili“ ili *hakirali*. Ovakvi tipovi napada odbijanja usluge obično dolaze s jednog računala koji traže propuste u programima kako bi obavili napad. Ukoliko je propust uočen, počinje napad odbijanja usluge s ciljem uskraćivanja usluge ovlaštenim korisnicima. Za ovakav tip napada nije potreban širokopojasni (brzi) pristup Internetu.
2. *Napad odbijanja usluge poplavom paketa*: napadi koji iskorištavaju slabosti infrastrukture Interneta i njegovih protokola. Poplavom naizgled normalnih paketa iskorištavaju se resursi programa (poslužitelja). Na taj način uskraćuju se usluge legitimnim korisnicima. Za razliku od prve kategorije napada, u ovom slučaju napadač za uspješan napad mora imati širokopojasni pristup Internetu. Bolje od korištenja vlastite infrastrukture za počinjene napada (napad s vlastitog računala; ovakav napad je lakše detektirati), napadači preferiraju izvršavanje napada s računala posrednika (*zombie* računala) koje napadač već kontrolira (na *zombie* računala obavi se napad prije DoS napada). Napadač kontrolira *zombie* računala i u određenom trenutku s njih pokreće napad. Ovakav napad naziva se raspodijeljeni napad odbijanja usluge (eng. *distributed DoS – DdoS*). Ovakvom tipu napada naročito je teško uči u trag i teško se obraniti od ovakvog napada.

Većina *zombie* računala su kućna računala, računala sveučilišta i sličnih ranjivih infrastruktura. Često vlasnici *zombie* računala nisu niti svjesni da njihova računala sudjeluju u takvim napadima. Primjer napada odbijanja usluge poplavom paketa prikazan je slikom 2.1:



Slika 2.1 – Primjer napada odbijanja usluge

Slikom 2.1 prikazan je jedan od načina napada odbijanja usluge, tzv. napad poplavom paketa. Napadač kontrolira računala za pokretanje napada koji kontroliraju računala za izvršavanje napada (*zombie* računala). Sa slike je vidljivo da napadač nije u direktnoj vezi sa žrtvom i stoga mu je puno teže ući u trag. Napad počinje tako da računala koja izvršavaju napad u istom trenutku počnu slati promet prema računalu žrtve. Uglavnom je to vrlo velik broj računala koja generiraju velik broj zahtjeva i žrtva nije u mogućnosti svima odgovoriti. Budući računalo žrtve ne može znati koje računalo izvršava napad a koje je stvarni korisnik, ono odbija sve novopristigle zahtjeve. U trenutku napada svi zahtjevi stvarnih korisnika se odbijaju, tj. sustav postaje nedostupan.

Gubitak mogućnosti obrade podataka može biti rezultat prirodnih katastrofa ili destruktivnog djelovanja ljudi na sustav. Prirodnim katastrofama poput potresa ili požara može doći do oštećenja opreme, pa tako i podataka pohranjenih na sustavu, pri čemu je trenutno onemogućeno funkcioniranje sustava. Čovjek može na informacijski sustav destruktivno djelovati slučajnim ili namjernim destruktivnim radnjama.

Sigurnosne mjere kojima osiguravamo dostupnost dijelimo na:

- fizičke,
- tehničke,
- administrativne.

Fizičke mjere uključuju kontrolu pristupa koja sprječava neovlaštenim osobama pristup sklopovlju informacijskog sustava, protupožarnim sustavima, sustavima za kontrolu temperature prostorija itd.

Tehničke mjere sprječavaju nefunkcioniranje sustava koje uzrokuje kvar opreme raznim mjerama poput zrcaljenja diskova, tj. više diskova sadrži iste informacije – ako se jedan pokvari, njegovu funkciju preuzima drugi. Jedna od mjera je konstantna provjera rada aplikacija – ako aplikacija ne izvršava zadatke ona se automatski ponovno pokreće). Tehničke mjere također sadrže mehanizme oporavka nakon nestanka struje (automatski se pokreće sekundarno napajanje), automatsko kreiranje kopija podataka itd.

Administrativne mjere uključuju kontrolu pristupa, kontrolu izvršavanja procedura i educiranje korisnika. Odgovarajuća osposobljenost programera i sigurnosnih stručnjaka također je bitan faktor dostupnosti sustava. Na primjer, ostane li prilikom kontrole sustava baza podataka zaključana, korisnici se ne mogu koristiti podacima koje ona sadrži, tj. sustav postaje nedostupan.

2.3 Procjena rizika

Procjena rizika bitan je korak pri uspostavi sigurnosti informacijskih sustava. Iako je temeljni dio sustava upravljanja sigurnošću informacija (ISMS), procjena rizika usko je vezana s definiranjem politike sigurnosti.

Proces procjene rizika nije nimalo jednostavan, ali najlakše bi se mogao opisati kao davanje odgovora (za svaku vrijednost koju organizacija posjeduje) na sljedeća četiri pitanja:

- što se može dogoditi? (događaj prijetnje)
- ako se dogodi, kolika šteta može nastati? (učinak prijetnje)
- koliko često se može dogoditi? (frekvencija prijetnje)
- koliko su točni odgovori na prva tri pitanja?

Odgovori na navedena pitanja mogu biti vrlo opsežni, lista onoga što bi se trebalo uraditi vrlo dugačka, stoga je navedena četiri pitanja često potrebno proširiti s još tri:

- što se može učiniti?
- koliko će učinjeno koštati?
- da li je utrošeno isplativo?

Odgovori na ova pitanja uravnotežuju potrebe i mogućnosti organizacija za implementacijom sigurnosnih kontrola. Kako bi se postigla ravnoteža potreba i mogućnosti neke je rizike potrebno prihvatiti. Rizik je na primjer moguće prihvatiti ukoliko je on vrlo malen ili ukoliko su posljedice nezgode prihvatljive za organizaciju.

Važan dio upravljanja sigurnošću predstavlja upravljanje rizikom, odnosno uspostava odnosa između ranjivosti, potencijalnih prijetnji i posljedica, to jest utjecaja na informacijski sustav.

Proces upravljanja rizikom sastoji se od sljedećih koraka:

- identifikacije resursa,
- analize rizika,
- tumačenja rezultata i poduzimanja odgovarajućih protumjera.

Identifikacija resursa

Jedan od uvjeta za uspješno upravljanje sigurnošću informacijskog sustava jest identifikacija resursa koji su dio tog sustava. Bez precizne identifikacije resursa nije moguće provesti njihovu kvalitetnu zaštitu.

Kroz proces identifikacije resursa potrebno je prebrojati sve resurse unutar informacijskog sustava te procijeniti njihovu relativnu vrijednost za organizaciju. Kako bi se mogla odrediti vrijednost resursa za organizaciju, potrebno je poznavanje poslovnih procesa koji se odvijaju u organizaciji. Na temelju toga je kasnije u procesu upravljanja rizikom, odnosno prilikom analize rizika moguće učinkovito ocijeniti potrebnu razinu zaštite za svaki pojedini resurs bitan za funkcioniranje poslovnih procesa unutar organizacije.

Kvalitetnom identifikacijom resursa nužno je postići sljedeće zahtjeve:

- ustanoviti vlasnike poslovnih procesa, odnosno odgovorne osobe,
- identificirati pojedine resurse bitne za funkcioniranje poslovnih procesa,
- procijeniti vrijednost resursa,

- ustanoviti njihovo fizičko ili logičko mjesto u sustavu,
- napraviti odgovarajuću dokumentaciju.

U načelu, vlasnik procesa je taj koji bi morao znati procijeniti vrijednosti resursa bitnih za funkcioniranje poslovnih procesa, no u praksi to često i nije slučaj. To ukazuje na probleme u organizaciji tvrtke i u takvim slučajevima uspostava sustava za upravljanje informacijskom sigurnošću obično je jalov posao.

Podjela resursa

Podjelu resursa moguće je napraviti prema raznim pravilima. U informacijskim sustavima resurse je ugrubo moguće podijeliti u sljedeće kategorije:

- informacije (baze podataka, dokumentacija, autorska djela itd.),
- programska podrška (aplikacije, operacijski sustavi, razvojni alati itd.),
- oprema (računalna oprema, mrežno-komunikacijska oprema, mediji za pohranu podataka i ostala oprema nužna za rad informacijskog sustava),
- servisi (računalni i komunikacijski te općeniti servisi kao što su, primjerice grijanje, osvjetljenje itd.).

Za svaki od identificiranih resursa potrebno je napraviti procjenu njegove relativne vrijednosti unutar sustava bez obzira u koju kategoriju pripada. Često se naglasak prilikom upravljanja sigurnošću informacijskog sustava polaže na same informacije, dok su, na primjer servisi zanemareni. No, gubitak nekog od tih resursa može dovesti do narušavanja rada sustava, pa čak i potpunog zastoja poslovnog procesa.

Klasifikacija informacija

Resurse koji pripadaju različitim kategorijama moguće je klasificirati na razne načine. S obzirom na to da je u informacijskom sustavu ipak najvažnija sama informacija, potrebno je uspostaviti odgovarajući sustav klasifikacije.

Unutar sustava općenito su pohranjene informacije različitih vrijednosti za organizaciju: od potpuno nevažnih do onih ključnih, pa i kritičnih. Cilj klasifikacije informacija je osiguranje njihove odgovarajuće zaštite.

Klasifikacija se obično provodi s obzirom na postavljene kriterije (vrijednost same informacije, utjecaj vremena na njenu vrijednost, povezanost s pojedinim osobama itd.). U većini organizacija općenito je prikladan sljedeći sustav klasifikacije:

- javne,
- osjetljive,
- povjerljive,
- tajne.

Javne informacije mogu se ponekad poistovjetiti i s informacijama koje ne spadaju u sustav klasifikacije, a odnose se na one informacije čije otkrivanje ne predstavlja nikakav potencijalni rizik za organizaciju. Za njih obično nije nužno postaviti sigurnosni nadzor. Osjetljive informacije zahtijevaju veću razinu nadzora jer njihovo otkrivanje ili gubitak integriteta mogu izazvati određene gubitke (koji ne moraju biti izravno materijalne prirode).

Povjerljive informacije su namijenjene samo uporabi unutar organizacije. Njihovo otkrivanje može imati negativan utjecaj na organizaciju ili njene zaposlenike, tako da je nužna implementacija odgovarajućih sigurnosnih mehanizama. Tajne informacije odnose se na najosjetljivije podatke i bilo kakve neovlaštene aktivnosti vezane uz njih mogu dovesti do vrlo ozbiljnih posljedica za organizaciju. Odgovarajuća implementacija sigurnosti za ovakve informacije je od kritične važnosti.

Uz procjenu rizika potrebno je odrediti kako postupati s rizicima. Mogući postupci uključuju:

- ugrađivanje odgovarajućih kontrola koje smanjuju rizik,
- svjesno i objektivno prihvaćanje rizika, udovoljavajući sigurnosnoj politici organizacije i kriterijima prihvatljivog rizika,
- izbjegavanje rizika zabranama, tj. onemogućavanjem akcija koje uzrokuju rizik.

Za rizike čiji postupci uključuju implementiranje odgovarajućih kontrola, te kontrole moraju biti odabrane i implementirane zadovoljavajući zahtjeve definirane procjenom rizika.

Kontrole moraju osiguravati da su rizici reducirani na prihvatljiv nivo uzimajući u obzir:

- ograničenja i zahtjeve definirane nacionalnim i internacionalnim zakonima i propisima,
- ciljeve organizacije,
- operativne potrebe i ograničenja,
- cijenu implementiranja.

Analiza rizika

Analiza rizika je postupak kojem je cilj ustanoviti ranjivosti sustava, uočiti potencijalne prijetnje (rizike) te na odgovarajući način kvantificirati moguće posljedice kako bi se mogao odabrati najučinkovitiji način zaštite, odnosno procijeniti opravdanost uvođenja dodatnih protumjera.

Postoje dva osnovna pristupa analizi rizika:

- Kvantitativna analiza;
- Kvalitativna analiza.

Kvantitativna analiza podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjoj razini, dok rezultat kvalitativne analize iskazuje samo relativan odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i uvođenja protumjera. Pritom valja imati na umu da je ta procjena subjektivne naravi te je stoga podložna pogreškama.

U načelu kombinacija kvantitativne i kvalitativne analize predstavlja pristup prikladan za većinu tvrtki. Čista kvantitativna analiza uglavnom se primjenjuje samo u financijskim institucijama poput banaka i osiguravajućih društava.

Tumačenje rezultata

Analizom rizika moraju se utvrditi sljedeće činjenice:

- kritični resursi i prijetnji i vjerojatnost njihove pojave,
- potencijalni gubici koje uzrokuje ostvarenje prijetnje,
- preporučene protumjere njihova vrijednost (relativna ili novčana),
- popis mogućih (nadzor) i zaštita.

Na temelju dobivenih rezultata potrebno je odlučiti kakve treba poduzeti protumjere. Postoje tri mogućnosti djelovanja koje nužno nisu međusobno isključive:

- smanjenje rizika,
- prijenos rizika,
- prihvaćanje rizika.

Jedini važan parametar pri odabiru načina djelovanja je isplativost za organizaciju.

Smanjenje rizika predstavlja proces u kojem se na temelju provedene analize rizika nastoje provesti odgovarajuće protumjere i uvesti sigurnosni nadzor da bi se zaštitili resursi organizacije. U tom postupku nastoji se smanjiti vjerojatnost prijetnje i(ili) njen utjecaj na organizaciju. Ukoliko se pokaže isplativijim, rizik je moguće prenijeti na treću stranu (primjerice, osiguravajuće društvo). Isto tako moguće je da implementacija protumjera ili prijenos rizika nisu isplativi. U tom slučaju organizacija može odlučiti prihvatiti rizik, odnosno troškove koji iz toga proizlaze.

Jedini pristup koji u upravljanju rizikom nije prihvatljiv je ignoriranje ili zanemarivanje rizika. Treba znati da je upravljanje rizikom stalan proces te da se odnos vrijednosti resursa, ranjivosti i prijetnji s vremenom mijenja.

3. Norme

Sigurnost informacijskih sustava danas je nezaobilazna tema kojoj se posvećuje mnogo pažnje. Zaštita je postala moralna i poslovna obaveza, te neophodan postupak pri osmišljavanju i izgradnji informacijskih sustava. Kako bi se olakšala implementacija sigurnosti u organizacije, na tržištu su se pojavili standardi vezani uz sigurnost informacijskih sustava. Implementacija sigurnosnih kontrola po standardima ne samo da onemogućava previd pojedinih kontrola, već je i dokaz kvalitete uspostavljenih sigurnosnih kontrola.

Danas je na tržištu prisutno mnogo normi, referenci i savjeta za uspostavu sigurnosti u informacijske sustave, no dva najpoznatija standarda zasigurno su ISO/IEC 17799 i ISO/IEC 27001. Standardi ISO/IEC 17799 i 27001 se međusobno ne isključuju. Naprotiv, za uspostavu kvalitetnog sustava upravljanja sigurnošću informacija nužno je koristiti oba standarda.

3.1 ISO/IEC 17799

ISO (eng. *the International Organization for Standardization*) i IEC (eng. *the International Electrotechnical Commission*) dva su tijela koji zajedno čine sustav za međunarodnu standardizaciju. ISO/IEC 17799 je norma formulirana na mnogim postavkama BS 7799 (eng. *British Standards*) norme koja od 1995., kada je donesena, predstavlja najraširenij pokušaj uvođenja međunarodno priznatih normi na području upravljanja informacijskom sigurnošću. Prva verzija ISO/IEC standarda nazvana je 17799:2000. Godine 2005. izdana je nova verzija nazvana ISO/IEC 17799:2005. Poboljšanja koja nova norma posjeduje su između ostalih bolja organizacija sigurnosti prilikom poslovanja s drugim poslovnim subjektima i naglasak na rješavanju sigurnosnih problema koji mogu nastati korištenjem mobilnih tehnologija i bežičnih računalnih mreža.

Jedna od osnovnih namjena primjene ISO/IEC 17799 norme jest pružiti efikasno upravljanje informacijskom sigurnošću. ISO/IEC ističe da 17799 nije prvenstveno namijenjen certificiranju, već širenju svjesnosti o potrebi organizacije sustava zaštite informacija kroz opis najboljih već primijenjenih metoda i principa za uspostavu i održavanje takvih sustava. Budući se primjenom čisto tehničkih sredstava može postići samo ograničen stupanj informacijske sigurnosti, ova norma naglašava važnost uspostavljanja nadzornih procedura i sustava kontrole uz sudjelovanje svih zaposlenih.

Normu ISO/IEC 17799 moguće je implementirati u sve vrste informacijskih sustava bez obzira na njihovu veličinu. Navedena karakteristika utjecala je na popularnost standarda i njegovu sveopću prihvaćenost.

ISO/IEC 17799:2005 sastoji se od 11 domena sigurnosnih kontrola koje zajedno sadrže 39 osnovnih sigurnosnih kategorija i jednu uvodnu domenu koja nas upoznaje s procjenom rizika.

Svaka domena sadrži određeni broj glavnih sigurnosnih kategorija (navedenih u zagradi). Domene su:

1) Sigurnosna politika (1),
2) Organiziranje informacijske sigurnosti (2),
3) Upravljanje imovinom (2),
4) Sigurnost i ljudski resursi (3),
5) Fizička zaštita i zaštita od okoline (2),
6) Upravljanje komunikacijama i operacijama (10),

7) Kontrola pristupa (7),
8) Obogaćivanje, razvoj i održavanje informacijskog sustava (6),
9) Upravljanje incidentima informacijskog sustava (2),
10) Upravljanje poslovnim kontinuitetom (1),
11) Usklađivanje (3).

Svaka glavna sigurnosna kategorija sadrži:
- kontrolni cilj koji je potrebno ostvariti,
- jednu ili više kontrola koje se mogu primijeniti kako bi se ostvario kontrolni cilj.

Opisi kontrola su strukturirani na sljedeći način:
- **Kontrola**: definira određenu kontrolu koja treba zadovoljiti kontrolni cilj,
- **Implementacijske smjernice**: pružaju detaljnije informacije za implementiranje kontrole. Neki od koraka pri implementaciji nisu primjenjivi za neke slučajeve, pa je tada potrebno na neki prikladniji način implementirati kontrolu,
- **Dodatne informacije**: pružaju dodatne informacije koje je potrebno razmotriti pri uvođenju neke kontrole, npr. legalne aspekte kontrole i reference na neke druge standarde.

Dokument ISO 17799:2005 norme organiziran je u petnaestak poglavlja. Dio dokumenta tematizira upoznavanje s problemom upravljanja informacijskom sigurnošću. Uz prijedlog ustroja zaštite informacija obrazlaže se i sustav provjera koji se može primijeniti na gotovo sve poslovne subjekte i javne organizacije. ISO 17799:2005 norma razlikuje provjeru sigurnosne politike, ljudskih resursa, komunikacija i operativnog sustava, nabavu, organizaciju i održavanje IT sustava, odgovor na incidente te općenito pridržavanje uobičajenih poslovnih običaja. Najveći dio dokumenta odnosi se na provjeru sustava komunikacija i ostalih informacijskih tehnologija koje se koriste u poslovnim procesima. Provjera pristupa posebna je cjelina. Kako bi tehnička sredstva koja su danas na raspolaganju polučila najbolje rezultate, smatraju tvorci norme, potrebno je naglasiti važnost donošenja jasnih pravila o tome tko ima pristup kojim resursima.

3.2 ISO/IEC 27001

ISO/IEC 27001:2005 je standard objavljen u listopadu 2005. godine, razvijen je na temeljima BS 7799 standarda, točnije njegovog drugog dijela. Namjena ovog standarda je kvalitetna uspostava sustava upravljanja sigurnošću informacija (ISMS), a sadrži skup zahtjeva koje organizacija mora ispuniti da bi se priznao certifikat za informacijsku sigurnost. Iako standard 27001 obuhvaća izradu sigurnosne politike, njegova prvenstvena uloga je način implementacije sigurnosnih kontrola i samim time nije prikladan kao temelj pisanja sigurnosne politike.

Implementacija standarda ISO/IEC 27001:2005 u organizaciju odvija se kroz dvije faze. Prva faza mogla bi se nazvati *administrativna*, u njoj menadžment donosi stratešku odluku da se ide u taj projekt, odnosno osigurava punu podršku implementaciji.

Druga faza odvija se kroz nekoliko koraka: određivanje opsega i granice ISMS, definiranje politike ISMS, evidencija imovine (za čuvanje, prijenos i obradu informacija), procjena rizika, donošenje dokumenta „Izjava o prihvatljivosti“ (SoA), prihvaćanje i odobrenje uprave, priprema dokumentacije, implementacija ISMS, izrada procedura za upravljanje incidentima, provođenje *monitoringa*, identifikacija i implementacija poboljšanja itd.

Standard 27001:2005 razlikuje dvije vrste zahtjeva za upravljanje informacijskom sigurnošću:
- metodološki zahtjevi (poglavlja 4-8),

- zahtjevi za sigurnosne kontrole (Anex A standarda).

Poglavlja 4-8 standarda sadrže metodološke zahtjeve jer ona kažu „kako“ razviti i upravljati informacijskom sigurnošću i ne spominju se kontrole koje je potrebno implementirati.

Anex A standarda ISO/IEC 27001:2005 sadrži 2 vrste zahtjeva za sigurnosnim kontrolama:

- kontrolni ciljevi (eng. *Control Objectives*),
- sigurnosne kontrole (eng. *Security Control*).

Kontrolni zahtjevi su kopirani iz standarda ISO/IEC 17799:2005, poglavlja 5-15. Na njih se referira kao na sigurnosne kontrolne zahtjeve jer čine polazište za ISMS.

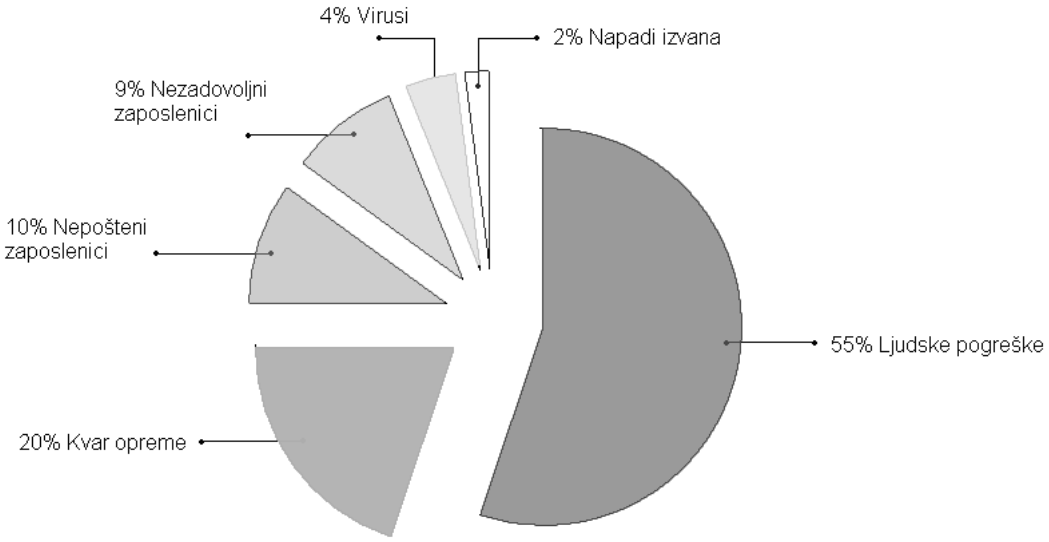
Ključni dokument koji se u cijelom projektu implementacije koristi kao temelj za donošenje odluke uprave o konačnom prihvaćanju strukture ISMS je „Izjava o prihvatljivosti“ (SoA – eng. *Statement of Applicatibility*). Kroz taj dokument točno se definira što sve treba od kontrola primijeniti u organizaciji kako bi se uspostavio željeni ISMS. Ukoliko se kontrola ne primjenjuje tada se mora u dokumentu SoA detaljno navesti razlog zašto se ta kontrola ne koristi u okviru konkretnog ISMS. Osnove za definiranje dokumenta SoA su sigurnosna politika organizacije, definirana na početku, te u skladu s njom izvršena procjena rizika. To drugim riječima znači, da rezultati procjene rizika na imovini određuju sve kriterije za bilo kakve potrebne kontrole i aktivnosti vezane za uspostavu ISMS.

4. Sigurnost informacijskih sustava

Kao što je navedeno u prethodnim poglavljima sigurnost informacijskih sustava može biti ugrožena na više načina. Prijetnje možemo podijeliti prema izvoru:

- ljudi – namjerne prijetnje,
- ljudi – nenamjerne prijetnje,
- oprema,
- prirodne nepogode.

Iako mnogi smatraju da prijetnje sigurnosti sustava najčešće dolaze izvana (napadi hakera), istraživanja koja su obavljena i objavljena u knjizi D. Seger, K., VonStroch, W. «*Computer Crime A Crimefighter's Handbook*», O'Reilly & Associates pokazuju sasvim suprotne činjenice. Statistički podaci koji su prikazani na slici 4.1 pokazuju da najvećim postotkom probleme sigurnosti uzrokuju ljudske greške. One se najčešće dogode zbog nedovoljne pažnje i educiranosti zaposlenika. Drugi najveći uzrok grešaka u sustavima je kvar opreme, slijede zaposlenici koji svoj položaj u instituciji koriste za vlastitu korist i zaposlenici koji na ovakav način izražavaju svoje nezadovoljstvo prema poduzeću ili nadređenoj osobi.



Slika 4.1 – Problemi sigurnosti u velikim kompanijama

Kako bi spriječili mogućnost obavljanja ovakvih neželjenih radnji potrebno je uvesti odgovarajuće mjere. Mjerama poput educiranja zaposlenika smanjuje se vjerojatnost njihove pogreške kojima bi mogli ugroziti integritet i sigurnost sustava. Smještajem opreme na kojima se čuvaju podaci u posebnu prostoriju, propisima kojima se određuje tko joj smije pristupiti, kontroliranjem uvjeta u takvoj prostoriji kao što su temperatura i vlaga, postižemo duži radni vijek opreme a time i pouzdaniji rad sustava. Uvođenjem kontrole pristupa podacima i definiranjem sankcija onima koji se ne pridržavaju propisanih pravila suzbijamo zlouporabu sustava od strane zaposlenika.

Najrjeđi, ali napadi koji najčešće uzrokuju najveće štete su napadi "izvana". Oni sudjeluju u vrlo malom postotku, a cilj im je pribavljanje informacija, njihovo mijenjanje ili uništavanje. Sustav se od takvih napada brani kontrolom prometa s Interneta prema sustavu i obrnuto, sprječavanjem instaliranja programa u operacijski sustav ili kriptiranjem podataka. Uvođenjem ovakvih mjera u informacijskim sustavima podižemo njegov stupanj sigurnosti, a mogućnost obavljanja neželjenih radnji svodimo na minimum.

Kako bi se postigla maksimalna sigurnost sustava potrebno je obratiti pažnju na:

- fizičku sigurnost,
- sigurnosne mjere za osoblje,
- sigurnost komunikacija i
- operacijsku sigurnost.

Fizička sigurnost. Osnova fizičke sigurnosti je zaštita fizičkog dijela informatičke infrastrukture, zgrade u kojoj je ona smještena, medija za pohranu podataka i komunikacijske opreme. Mjere fizičke sigurnosti obuhvaćaju sve obrambene mjere poduzete u svrhu zaštite računalne infrastrukture od prirodnih nepogoda, problema u okolini, nezgoda i namjernih oštećenja.

Fizičku sigurnost sustava mogu ugroziti prirodne nepogode poput požara, poplava, udara groma ili potresa, prijetnje iz okoline poput zagrijavanja, hlađenja ili električne energije, zatim korisnici sustava ili osobe koje sustavu nemaju pravo pristupa. Prirodne nepogode mogu imati veliki utjecaj na sigurnost informacijskih sustava. Računalna oprema jako je osjetljiva na dim, prašinu, vibracije, vlagu itd., pa ako ne postoji dovoljna razina zaštite pri njihovom djelovanju može doći do uništenja sustava i podataka koje oni sadrže. Električna energija je prijetnja koja ugrožava svaki informacijski sustav. Računalna je infrastruktura vrlo osjetljiva na promjene električne energije i njezinu kvalitetu. U slučaju nekvalitetne električne energije može doći do oštećenja sustava ili potpunog gubitka podataka. Elektronička oprema osjetljiva je i na temperaturu pri kojoj radi, stoga je potrebno kontrolirati temperaturu i vlažnost zraka u prostorijama u kojima se takva oprema nalazi. Kako bi se postigla odgovarajuća fizička sigurnost s obzirom na destruktivno djelovanje ljudi, kružni pristup računalima i računalnoj opremi jedna je od polaznih točaka razmatranja. Shematski prikaz kružnog pristupa prikazan je na slici 4.2.

Slika 4.2 - Shematski prikaz kružnog pristupa

Pristup računalnom sustavu koji želimo zaštititi trebao bi se organizirati kroz više kontrolnih točaka. Na primjer, osoba koja želi uči u zgradu gdje se nalazi računalna oprema prvo mora proći čuvara objekta. Potom mora proći sobe koje su zaključane, pod alarmnim sustavom i/ili nekim drugim oblikom zaštite kako bi došao do sobe koja

sadrži računalnu opremu. Definiranjem većeg broja krugova potencijalnom napadaču otežava pristup opremi, a samim time i izvršavanje destruktivnih radnji.

Ispitivanje fizičke sigurnosti informacijskih sustava jedan je od bitnih dijelova definiranja sigurnosti. Najgori događaj u ispitivanju sigurnosti jest onaj koji nastaje djelovanjem počinitelja. Stoga je potrebno nakon definiranja sigurnosnih mjera ispitati njezinu učinkovitost. Postoje najmanje tri tipova testova kojima je moguće ispitati i ocijeniti fizičku sigurnost sustava. Jedan od njih je konstantno ispitivanje fizičke sigurnosti, drugi je provođenje nenajavljenih provjera kako bi se provjerilo da djelatnici ne zaobilaze sigurnosne mjere kada nisu pod nadzorom i treći je da se na posebno osjetljivim mjestima simuliraju napadi.

Provjere sigurnosti provode kvalificirani djelatnici koji su zaposleni u samoj organizaciji ili nekoj drugoj organizaciji koja se bavi fizičkom sigurnosti koristeći unaprijed definirane metode ispitivanja. Unaprijed definirane metode pomažu kako bi se provjerile sve potencijalne opasnosti. Izvještaji koje načine kvalificirane osobe u pravilu su tehnički detaljne i opširne, te se koriste za kratkoročna i dugoročna planiranja zaštite sustava. Ove informacije je vrlo važno čuvati kao vrlo povjerljive, jer potencijalni napadači pomoću njih mogu otkriti ranjive točke sustava te tako zaobići zaštitu i ugroziti sustav.

Sigurnosne mjere za osoblje. Najveće prijetnje informacijskim sustavima su ljudi koji s njim imaju vezu, kroz svakodnevni rad ili kroz povremeno održavanje. Neke osobe nisu dovoljno kvalificirane za određeni posao te se može dogoditi da takva osoba slučajno uništi podatke te ugrozi informacijski sustav. Ugrožavanje sustava je također moguće namjernim radnjama korisnika sustava, bilo radi zadovoljstva, osobne koristi ili nekog drugog razloga.

Ako se promotri statistika prijetnji sigurnosnim sustavima, moguće je zaključiti kako većina prijetnji sustavima dolazi od osoba koje dolaze u doticaj sa sustavom, bez obzira na motiv. Kako računalo omogućuje i upade izvan organizacije, sigurnosne mjere za osoblje moraju obuhvatiti i osobe koje ne rade u organizaciji ali s njom dolaze u kontakt.

Svaka organizacija mora se oslanjati na kvalitetne sigurnosne mjere za osoblje, te je stoga vrlo važno pažljivo odabirati zaposlenike, što znači da se u obzir moraju uzimati i najmanji detalji. Promatranjem zbivanja unutar organizacije i izvan nje, moguće je pravovremeno spriječiti potencijalne opasnosti i unaprijediti sigurnosne mjere. Organizacija koja ima problema sa svojim zaposlenicima može postati metom napada zaposlenika ili osoba izvan organizacije koje se solidariziraju sa zaposlenikom.

Sigurnost komunikacija. Komunikacija između računala doprinosi povećanju snage sustava, brzini obrade podataka, dostupnosti, ali što više računala komunicira sa drugim računalima to je organizacija u kojoj se ona nalaze ranjivija.

Komunikaciju mrežom možemo učiniti sigurnijom kontrolom pristupa, kriptiranjem podataka koji putuju mrežom, zaštitom sigurnosnim stijenama i ostalim mjerama fizičke zaštite. Kontrola pristupa je bitan čimbenik u ostvarivanju računalne sigurnosti u mrežnom okružju. Mnogi računalni sustavi koriste zaporke u smislu osiguravanja kontrole pristupa, svatko tko zna ispravnu zaporku ima dozvoljen pristup računalnom sustavu.

Stoga je bitno da zaporku poznaju samo ovlašteni korisnici. Kako bi kontrola pristupa imala svoj smisao, korisnici se moraju pridržavati osnovnih pravila pri čuvanju zaporke:

- nikada zaporku čuvati u blizini računala ili terminala,
- zaporka ne smije biti ime korisnika ili neki pojam kojeg je lako pogoditi,
- zaporku se ne smije spremati u datoteci na računalu.

Osim ovih pravila, moguće je definirati dodatna pravila koje kontrolira sustav:

- ***Zaporke generirane od sustava*** – zahtjeva od korisnika korištenje slučajno generirane zaporke. Sustav generira zaporku koju je u pravilu nemoguće pogoditi. Budući je tako generirana zaporka i teško pamtljiva, korisnik je primoran zaporku zapisati što je velika mana ovog pravila.
- ***Minimalna duljina zaporke*** – općenito su dulje zaporke bolje od kratkih, ne samo što ih je teže pogoditi već i stoga što je potrebno puno više vremena za njihovo probijanje. Mnogi računalni sustavi nameću minimalnu duljinu zaporke.
- ***Vijek trajanja zaporke*** – kako bi se otežala mogućnost pogađanja, a ujedno i probijanja lozinke mnogi računalni sustavi zahtijevaju periodičko mijenjanje zaporki korisnika. Korisnik je dužan svako određeno vrijeme promijeniti zaporku, a ako to ne učini, zaporka prestaje vrijediti.
- ***Ograničen broj pokušaja*** – mnogi računalni sustavi dopuštaju ograničen broj pokušaja pristupa sustavu. Ako korisnik pokuša više od nekoliko puta (najčešće tri) pristupiti sustavu s krivom zaporkom, sustav ga odbacuje.
- ***Poruka o zadnjem pristupu*** – kada korisnik pristupi informacijskom sustavu, prikazivanjem datuma ili točnog vremena zadnjeg pristupa (ili pokušaja pristupa) može biti vrlo korisno. Naime, ako se korisnik nije duže vrijeme koristio sustavom, a primijeti da je netko pokušao pristupiti, to bi trebalo potaknuti sumnju da je netko pokušao probiti zaporku.
- ***Šifrirani i skriveni zapisi o zaporci*** – mnogi sustavi koriste šifrirane zapise za čuvanje zaporki pojedinih korisnika, te se takvi zapisi čuvaju unutar informacijskih sustava na dobro osiguranim mjestima.
- ***Zaključavanje zaporki*** – administratori informacijskih sustava mogu koristiti zaključavanje zaporki pojedinih korisnika kako bi se ograničio pristup sustavu ako korisnik nije u mogućnosti koristiti sustav određeno vrijeme ili nakon radnog vremena.
- ***Pametne kartice*** – neki sustavi zahtijevaju pristup putem pametnih kartica i upisa osobnog identifikacijskog broja, prije negoli se dozvoli daljnji pristup provjeri zaporke.
- ***Dodatne zaporke*** – neki informacijski sustavi imaju mogućnost postavljanja ove vrste zaporke. Kako bi korisnik pristupio sustavu mora upisati zaporku sustava pa svoju vlastitu zaporku. Također je moguće definirati potrebu unosa zaporke ako se korisnik želi koristiti jedinicama za unos podataka i sl.
- ***Jednokratne zaporke*** – koriste se i vrijede samo jednom. S obzirom da se ne treba pamtiti, vrlo ju je teško ukrasti. Jedan od najpoznatijih sustava koji nudi ovu metodu je *S/Key*.
- ***Vremenski ovisne zaporke*** – neki sustavi koriste ovaj tip zaštite koji je ovisan o vremenu., tj. zaporke se mijenjaju svake minute. Pametna kartica sadrži podatke poput trenutnog vremena i tajnog korisničkog ključa. Kako bi pristupio sustavu, korisnik mora upisati broj baziran na trenutnom vremenu i njegovom ključu.

Kriptografske metode predstavljaju drugi način ograničavanja pristupa podacima. Ona je osobito važna kada se povjerljivi podaci šalju računalnom mrežom. Tehnike enkripcije određuju koliko će proces biti složen.

Kriptografske metode mogu osigurati ili pomoći u ostvarenju:

- *tajnosti izvornog teksta* – sprječava neovlašten uvid u sadržaj izvornog teksta,
- *autentičnosti izvornog teksta* – osiguranje vjerodostojnosti sadržaja poruke,
- *integriteta izvornog teksta* – sprječava neovlašteno mijenjanje sadržaja izvornog teksta, te slučajno ili namjerno oštećenje ili uništenje.

Zaštita informacijskih sustava od neprijateljskih računalnih mreža ili pojedinaca vrlo je važan segment sigurnosti i danas predstavlja najveći izazov osobama koje štite

sustav i osobama koje ga napadaju. Jedan od najboljih današnjih sustava za zaštitu računalnih mreža naziva se sigurnosna stijena. Sigurnosna stijena služi kako bi se korisnicima osigurao pristup Internetu ili općenito bilo kojoj mreži od koje prijeti opasnost. Takav sustav zaštite funkcionira na principu kontrole količine i vrste prometa.

Postoje dvije vrste konfiguriranja sigurnosnih stijena:

- *određena dozvola* – postavlja se skupina uvjeta koja će rezultirati blokiranjem podataka, sav promet koji nije pokriven policom bit će pušten;
- *određena zabrana* – upisuje se određeni protokol koji omogućuje prolaz samo unaprijed definiranoj vrsti prometa.

Svaki od ovih načina ima svoje prednosti i nedostatke. Osnovna prednost određene dozvole je to što je lakša za konfiguriranje: blokiraju se protokoli koji se smatraju opasnima. S druge strane, kod određene zabrane omogućavaju se protokoli koji su traženi od strane korisnika ili rukovoditelja. Svi ostali protokoli neće biti podržani i biti će blokirani.

Operacijska sigurnost. Operacijska sigurnost uključuje dva aspekta sigurnosti informacijskih sustava. Prvi se odnosi na povećanje svijesti među potencijalnim žrtvama, a drugi predstavlja načine na koji se računalni kriminalci mogu spriječiti u počinjenju djela.

Povećanje svijesti postiže se tako da kad god je to moguće zaposlenici budu uključeni u sigurnosni program te ih po potrebi educirati na koji način je sigurnost ugrožena i kako svi dijele rizik i odgovornost. Jednom kada se analiziraju rizici sustava, potrebno je odrediti količinu informacija koja će se podijeliti sa zaposlenicima. Jasno je da povjerljive informacije neće biti dostupne svima, već samo malom broju osoba kojima su one nužne za obavljanje poslova. Općenito gledajući, operacijska sigurnost ne može postojati i biti dostatna sama sebi. Jedini način na koji ona može postojati jest uključivanje operacijske sigurnosti u programe ostalih načina zaštite sustava.

5. Primjer sigurnosne politike

Sigurnost informacijskih sustava danas vrlo bitan element poslovanja mnogih kompanija, važno je unaprijed osmisliti na koji način se sustav planira zaštititi od potencijalnih prijetnji. Temeljitim proučavanjem sustava od strane kvalificiranih i stručnih osoba procjenjuju se rizici i otkrivaju prijetnje sustavu. Nakon procijene sigurnosti sustava treba definirati sigurnosnu politiku u kojoj je potrebno detaljno opisati što sve treba zaštititi kako bi sustav imao željenu razinu sigurnosti.

Sigurnosna politika može se definirati na dva načina. Prvi način je kopiranje već postojeće sigurnosne politike, tj. implementiranje jedne od normi. Ovaj način prikladan je za kompanije koje nemaju dostatna sredstva za detaljnu sigurnosnu politiku niti imaju za njom potrebu. Po potrebi je moguće iz odabrane norme izbaciti pojedine dijelove politike ili kombiniranjem dviju ili više normi osmisliti potrebnu sigurnosnu politiku.

Drugi način definiranja sigurnosne politike je detaljno proučavanje informacijskog sustava, uočavanje njegovih potencijalnih mjesta napada, te odlučivanje o tome kako će se ona zaštiti uz testiranje cjelokupne sigurnosti sustava. Ovako definirana sigurnosna politika pruža puno veću sigurnost, ali zbog toga ima i puno veću cijenu. Pri definiranju sigurnosne politike na ovakav način, svakom informacijskom sustavu pristupa se individualno, angažiranjem velikog broja stručnjaka i ulaganjem velikih sredstava ne samo u njeno definiranje, već i u implementaciju, održavanje i provođenje. Iako početna velika ulaganja mnoge odvraća, ovako definirana sigurnosna politika osigurava kompanijama nesmetano poslovanje i visok stupanj sigurnosti što je dugoročno gledano svakako isplativa investicija.

Primjer sigurnosne politike definiran u ovom diplomskom radu odnositi će se na zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave (u nastavku ZEMRIS). Sigurnosna politika biti će definirana prema normi ISO/IEC 17799:2005 uz konzultacije sa sigurnosnim stručnjacima fakulteta o dodatnim kontrolama.

Trenutno najpoznatiji standard za sigurnost, ISO/IEC 17799, jedan je od mnogih dokumenata na kojemu se može temeljiti razvoj sigurnosne politike.

ISO/IEC 17799:2005 sastoji se od sljedećih 11 domena:

1) Sigurnosna politika
2) Organiziranje informacijske sigurnosti
3) Upravljanje imovinom
4) Sigurnost i ljudski resursi
5) Fizička zaštita i zaštita od okoline
6) Upravljanje komunikacijama i operacijama
7) Kontrola pristupa
8) Obogaćivanje, razvoj i održavanje informacijskog sustava
9) Upravljanje incidentima informacijskog sustava
10) Upravljanje poslovnim kontinuitetom
11) Usklađivanje

Svaka od navedenih domena sadrži popis smjernica, pravila i definicija s naglaskom na to *što* treba napraviti, odnosno zanemaruje način *kako* navedene kontrole implementirati. Upravo iz ovog razloga standard 17799 pogodan je za temelj pisanja sigurnosne politike stoga će u nastavku biti detaljnije obrađen.

5.1 Sigurnosna politika

Sigurnosna politika odražava stav najvišeg poslovodstva o pravcima u pogledu sigurnosti u kojima jasno iskazuju snažnu potporu svim subjektima poslovnog sustava u pogledu sigurnosti.

Najviše poslovodstvo mora definirati politiku te iskazati podršku i predanost sigurnosti informacija kroz izradu, doradu, naglašavanje i podržavanje politike sigurnosti u cijeloj organizaciji.

Dokument sigurnosne politike

Dokument sigurnosne politike treba biti odobren od strane upravitelja, objavljen i poslan svim zaposlenicima i korisnicima kojima je namijenjena.

Politika treba odražavati stavove rukovoditelja i definirati koncept upravljanja sigurnosti informacija. Dokument politike treba sadržavati iskaze koje se odnose na:

- definicije sigurnosti informacija, njezine sveobuhvatne ciljeve i djelokrug, te važnost sigurnosti kao temeljni mehanizam dijeljenja informacija,
- stavove rukovoditelja, podržavajući ciljeve i principe informacijske sigurnosti u skladu s poslovnom strategijom,
- okvire uspostave kontrolnih ciljeva i kontrola, uključujući načela procjene rizika,
- jezgrovito objašnjenje sigurnosne politike, načela i standarda,
- suglasnost sa zakonodavnim, nadzornim i ugovornim zahtjevima,
- zahtjevima o educiranju o sigurnosti,
- posljedicama nepridržavanja pravila sigurnosne politike,
- definicije općih i specifičnih odgovornosti rukovoditelja informacijske sigurnosti, uključujući izvještavanje o sigurnosnim incidentima,
- reference na dokumentaciju koja može podržati politiku.

Sigurnosna politika mora biti pisana u odgovarajućem obliku, dostupna i razumljiva onome kome je namijenjena.

Provjera sigurnosne politike

Svakim danom otkrivaju se nove prijetnje informacijskim sustavima, u informacijske sustave ugrađuje se nova oprema, zapošljavaju se novi kadrovi itd. Ukoliko sve ove promjene ne bi utjecale na sigurnosnu politiku, politika bi nakon nekog vremena zastarjela. Iz tog razloga politika sigurnosti mora biti periodično pregledavana, a ako se dogode značajne promjene unutar sustava i prije. Cilj provjere je zadržati i osigurati prikladnost, kompetentnost i djelotvornost politike.

Politika sigurnosti treba imati vlasnika, tj. odgovornu osobu zaduženu za razvoj, provjeru i valorizaciju sigurnosne politike. Provjera treba sadržavati određivanje mogućnosti poboljšanja sigurnosne politike i predlaganje promjena u okolnostima poslovanja, organizacije, pravnim ili tehničkim aspektima.

Činjenice koje je potrebno razmotriti u procesu provjere sigurnosne politike su sljedeće:

- povratne informacije,
- rezultati neovisnih ispitivanja,
- status preventivnih aktivnosti,
- promjene koje mogu pozitivno utjecati na informacijsku sigurnost,
- trendovi koji se odnose na prijetnje i ranjivosti,
- izvješća o sigurnosnim incidentima,
- preporuke mjerodavnih.

Rezultati provjere mogu sadržavati bilo koje odluke i akcije temeljene na:

- poboljšanju pristupa organizacije u upravljanju informacijskom sigurnosti,
- poboljšanju kontrolnih ciljeva i kontrola,
- poboljšanju u dijeljenju resursa i/ili odgovornosti.

Primjena norme u sigurnosnoj politici

Dokument sigurnosne politike ZEMRIS-a treba jasno definirati stav Zavoda i Fakulteta prema sigurnosti informacijskih sustava.

Što želimo zaštititi:

- **podatke** - zaposlenici i studenti svoja znanja prezentiraju kroz računalo. Većina njihovih projekata, članaka, predavanja i vježbi pohranjenih u elektronskom obliku predstavlja neprocjenjivu vrijednost za fakultet,
- **reputaciju** - fakultet elektrotehnike i računarstva ne smije si dopustiti sigurnosne incidente koji bi degradirali reputaciju građenu desetljećima i generacijama izvrsnih zaposlenika i studenata,
- **ostale korisnike Interneta** - računalni sustav Zavoda može biti velika potencijalna prijetnja drugim korisnicima Interneta ili privatnim mrežama spojenim na mrežu Zavoda ukoliko kontrolu nad sustavom preuzme napadač.

Važnost zaštite informacijskog sustava ZEMRIS-a nedvojbeno je prepoznata od strane rukovodećih ljudi fakulteta i zavoda te je pružena maksimalna podrška u razvoju politike i implementaciji sigurnosnih kontrola.

Provjera sigurnosne politike obavljati će se periodično svakih godinu dana, a po potrebi je nužno provjeru provesti i ranije. Prijevremenu provjeru sigurnosne politike potrebno je napraviti:

- ako se dogode sigurnosni incidenti,
- ako se otkriju potencijalne ranjivosti sustava,
- ako se implementiraju novi servisi, hardver, softver,
- ako se dogode promjene u strukturi zaposlenika itd.

5.2 Organizacija informacijske sigurnosti

Stav rukovoditelja

Rukovoditelji moraju aktivno podupirati provedbu sigurnosne politike svojim čvrstim stavom u pogledu sigurnosti, dajući potporu svim potrebnim zahtjevima za uspostavu sigurnosti te strogo kažnjavajući one koji je se ne pridržavaju.

Odgovornosti rukovoditelja sigurnosti:

- osigurati jasne ciljeve sigurnosti informacija koji podupiru potrebe organizacije i integrirani su u relevantne procese,
- formulirati i provjeravati sigurnosnu politiku,
- provjeravati efikasnost implementirane politike,
- osigurati podršku za sigurnosne inicijative,
- osigurati resurse koje iziskuje informacijska sigurnost,
- odobriti određivanje specifičnih uloga i odgovornosti za informacijsku sigurnost unutar organizacije,
- osigurati implementaciju sigurnosnih kontrola u skladu s organizacijom,
- odrediti postoji li potreba za savjetodavnim stručnjakom informacijske sigurnosti.

Koordinacija informacijske sigurnosti

U velikim organizacijama može se formirati tim za koordinaciju – predstavnici svih relevantnih dijelova organizacije, radi koordiniranja u sustavu sigurnosti informacija.

Takav tim:

- dogovara specifične uloge i odgovornosti za sigurnost informacija cijele organizacije,
- dogovara metode i procese vezane za sigurnost informacija, na primjer za upravljanje rizikom, klasifikaciju informacija,
- koordinira i podržava inicijative vezane uz sigurnost informacija,
- osigurava da je sigurnost dio procesa planiranja i razvoja,
- procjenjuje valjanost sigurnosnih kontrola i koordinira uvođenje kontrola u novim sustavima i servisima,
- pregledava izvješća o sigurnosnim incidentima,
- promovira potporu sustavu sigurnosti informacija kroz cijelu organizaciju.

Dodjela odgovornosti za sigurnost informacija

Cilj – sve odgovornosti informacijske sigurnosti moraju biti jasno određene.

Podjela odgovornosti mora biti učinjena u skladu s politikom sigurnosti. Odgovornosti za zaštitu pojedinih vrijednosti i za izvršavanje pojedinih sigurnosnih procesa trebaju biti jasno definirane i dokumentirane. Politika sigurnosti treba pružiti smjernice za dodjelu sigurnosnih uloga i odgovornosti u organizaciji. Treba jasno definirati lokalne odgovornosti za pojedinačne dijelove fizičke i informacijske imovine, te za sigurnosne procese.

Vlasnici informacijske imovine mogu prenositi svoje sigurnosne odgovornosti na pojedinačne članove. Vlasnik ima konačnu odgovornost za sigurnost imovine, te mora biti u stanju odrediti da li se raspodijeljene odgovornosti pravilno provode.

Važno je jasno definirati područja odgovornosti, a naročito se mora poduzeti sljedeće:

- identificirati i jasno definirati dijelove imovine i sigurnosnih procesa pridruženih svakom pojedinom sustavu,

- dogovoriti tko je odgovoran za pojedini dio imovine ili sigurnosni proces, te dokumentirati pojedinosti dogovora,
- definirati i dokumentirati razine ovlasti.

Proces autorizacije

Cilj – proces autorizacije novih situacija (objekata) mora biti definiran i izvediv.

Sljedeće smjernice potrebno je uzeti u obzir prilikom procesa autorizacije:

- novi organizacijski dijelovi moraju imati odgovarajuće odobrenje, kojim se autorizira njihova namjena i korištenje,
- po potrebi treba provesti pregled hardvera i softvera kako bi se osigurala kompatibilnost sa ostalim komponentama sustava,
- korištenje osobnih sredstava kao što je prijenosno računalo ili ručno računalo treba biti sigurnosno procijenjeno i odobreno.

Ugovor o povjerenju

Potreba za ugovorom o povjerenju odražava stav organizacije prema zaštiti vrijednosti koje posjeduje na način da svaki pristup vrijednostima bilježi i dokumentira. Ugovori o povjerenju imaju svrhu da na temelju zakona zaštite vrijednosti od kopiranja, uništavanja, zamjene i svih ostalih neželjenih radnji do strane zaposlenika, partnera ili treće strane.

Ugovor o povjerenju treba sadržavati:

- što treba zaštititi,
- očekivano trajanje ugovora,
- koje je akcije potrebno poduzeti prilikom raskida ugovora,
- odgovornosti i akcije odgovornih kako bi se spriječilo neovlašteno širenje informacija,
- koja prava imaju ovlašteni pri uporabi informacija,
- prava provjere, kontrole i nadgledanja pri uporabi osjetljivih informacija,
- procese za obavještavanje i prijavu neovlaštenog širenja informacija ili otkrivanje povjerljivih informacija,
- popis informacija koje moraju biti uništene, promijenjene ili vraćena pri prekidu ugovora,
- akcije koje je potrebno poduzeti ukoliko dođe do nepoštivanja ugovora.

Savjeti stručnjaka za informacijsku sigurnost

Stručnjaci za sigurnost imaju zadaću pružanja usluge informiranja i savjetovanja o svim aspektima sigurnosti, koristeći bilo vlastite bilo vanjske savjete. Kvaliteta njihovih procjena prijetnji i savjetovanja o sigurnosnim kontrolama može određivati učinkovitost sigurnosti informacijskog sustava. Stručnjake za sigurnost treba obavijestiti o sigurnosnim incidentima u što kraćem roku.

Suradnja s drugim organizacijama

Potrebno je održavati kontakte s organizacijama koje se bave sigurnošću, zakonodavnim i koordinativnim tijelima, pružateljima informacijskih usluga te razmotriti mogućnost članstva u sigurnosnim grupama i forumima kako bi se osiguralo da se u slučaju incidenta brzo mogu poduzeti prikladne akcije i pribaviti potrebna pomoć.

Suradnja s drugim organizacijama trebala bi:

- unaprijediti znanje o sigurnosti i biti u toku s važnim sigurnosnim informacijama,

- osigurati da je znanje o informacijskoj sigurnosti kompletno,
- omogućiti rano otkrivanje mogućnosti ranjivosti sustava kako bi se implementirale potrebne zakrpe,
- osigurati savjete specijalista za pojedine segmente sigurnosti,
- dijeliti i razmjenjivati informacije o novim tehnologijama, proizvodima, prijetnjama i ranjivostima.

Razmjena sigurnosnih informacija treba biti ograničena kako bi se osiguralo da povjerljive organizacijske informacije nisu proslijeđene neovlaštenim osobama.

Provjera sigurnosti sustava

Dokument sigurnosne politike oblikuje politiku i odgovornosti za sigurnost. Njenu implementaciju treba provjeravati, kako bi se osiguralo da praksa u organizaciji pravilno odražava politiku sigurnosti, te da je ona izvediva i fleksibilna.

Takvu provjeru može obaviti unutarnja nadzorna funkcija, neovisni menadžer ili vanjska organizacija koja je specijalizirana za takve preglede i čiji članovi posjeduju potrebne vještine i iskustva.

Sigurnost pristupa treće strane

Cilj – održati potrebnu razinu sigurnosti organizacijskih jedinica gdje se izvodi obrada podataka kao i organizacijskih vrijednosti do kojih pristup imaju treće strane.

Identifikacija rizika kod pristupa treće strane

Prije dodjele prava pristupa trećoj strani potrebno je provesti identifikaciju rizika, odrediti njegovu veličinu i prema dobivenim rezultatima implementirati sigurnosne kontrole.

Pri identifikaciji rizika kod pristupa treće strane treba:

- odrediti kojim organizacijskim jedinicama treće strane pristupaju,
- odrediti tip pristupa treće strane:
  - *fizički pristup* – pristup uredima, prostorijama s računalnom opremom, ormarima za pohranu,
  - *logički pristup* – pristup bazama podataka organizacije,
  - *pristup mreži organizacije* – umrežavanje organizacije i treće strane.
- odrediti vrijednost i osjetljivost informacijama kojima pristupa treća strana,
- definirati sigurnosne kontrole koje je neophodno implementirati za zaštitu vrijednosti kojima treća strana nema pravo pristupa,
- poimence definirati tko ima i koju razinu prava pristupa, te odluke pismeno dokumentirati,
- odrediti na koji način identificirati osobu i na koji način provesti autorizaciju,
- definirati kako regulirati odnose ukoliko organizacija nije u mogućnosti pružiti pristup informacijama, te koliko takva situacija šteti trećoj strani,
- uzeti u obzir zakonske i ugovorne okvire.

Pravo pristupa trećoj strani ne smije biti dozvoljena dok se ne implementiraju i provjere sve sigurnosne kontrole nužne za sigurnost sustava, te dok se ne dokumentiraju i potpišu ugovori koji obje strane potiču na pridržavanje sigurnosnih mjera.

Zahtjevi sigurnosti u ugovorima s trećom stranom

Dogovori koji uključuju pristup treće strane organizacijskim jedinicama za obradu informacija trebaju se temeljiti na formalnom ugovoru koji sadrži, ili se referencira na sve zahtjeve sigurnosti kako bi se osigurala uskladivost sa politikom sigurnosti i

standardima. Ugovorima treba osigurati da ne dođe do nesporazuma između organizacije i treće strane.

U ugovore bi trebalo uključite sljedeće:

- sigurnosnu politiku,
- zaštitu imovine, uključujući:
  - procedure za zaštitu organizacijske imovine, uključujući informacije i softver,
  - procedure za određivanje da li je neki dio imovine izgubljen ili izmijenjen;
  - kontrole za osiguravanje povrata ili uništavanje informacija i imovine na kraju ugovornog odnosa ili u dogovoreno vrijeme,
  - integritet i dostupnost,
  - ograničenja na kopiranje i otkrivanje informacija.
- opis svakog servisa koji će se učiniti dostupnim,
- ciljana razina usluga i neželjena razina usluga,
- odgovarajuće obveze ugovornih strana,
- odgovornosti usklađene sa pravnim zahtjevima,
- određivanje prava na intelektualno vlasništvo i prava kopiranja, te zaštita zajedničkog rada,
- sporazume o kontroli pristupa, uključujući:
  - dopuštene metode pristupa, te kontrolu i korištenje jedinstvenih identifikatora,
  - proces autorizacije za dodjelu prava pristupa,
  - zahtjev za održavanje popisa ovlaštenih osoba.
- pravo na praćenje korisničkih aktivnosti,
- pravo na nadzor ugovornih odgovornosti,
- odgovornost glede instalacije i održavanja hardvera,
- jasnu strukturu izvješćivanja i oblik izvješćivanja,
- jasan i određen proces upravljanja promjenama,
- izobrazba korisnika i administratora o metodama, procedurama i sigurnosti,
- kontrolne mehanizme za osiguranje zaštite od malicioznog softvera.

Primjena norme u sigurnosnoj politici

Organizacija informacijske sigurnosti dio je standarda namijenjen prvenstveno administratoru sustava. Koordinacija sigurnosti, autorizacija, ugovori o povjerenju sigurnosne su kontrole o kojima moraju brinuti osobe odgovorne za sigurnost sustava.

Pristup informacijskom sustavu ZEMRIS imaju mnogi. Broj korisnika sustava svakodnevno se mijenja i velik je broj korisnika kojima se oduzima pravo pristupa odnosno kojima se pristup sustavu dozvoljava. Zbog toga je vrlo važno kvalitetno organizirati način dodjeljivanja načina pristupa i ukidanja istih prava. Nerijetki je scenarij da korisnici kojima je formalno ukinuto pravo pristupa sustavu zbog sporosti ili propusta u provedbi i dalje mogu koristiti sustav što je „plodno tlo“ za obavljanje zlonamjernih radnji.

Kako bi se spriječili navedeni propusti potrebno je odrediti procedure prilikom dodjeljivanja prava pristupa informacijskom sustavu ZEMRIS.

Prijedlog otvaranja korisničkog računa:
pravo pristupa informacijskom sustavu ZEMRIS dodjeljuje se:

- novom zaposleniku,
- studentu,

- trećoj strani.

Zaposlenicima se korisnički račun otvara na taj način da tajnica zavoda sakupi podatke o novom zaposleniku, te podatke proslijedi administratoru sustava. Studentima se automatski prilikom upisa studija otvara korisnički račun za otvaranje korisničkog računa trećoj strani potrebna je suglasnost odgovorne osobe. Odgovorna osoba je glavna i odgovorna osoba u suradnji s trećom stranom, i kao takva ima prava davanja suglasnosti za otvaranje korisničkih računa prilikom otvaranja korisničkog računa trećoj stranici potrebno je odrediti vremenski period aktivnosti računa, tj. kada postaje nevažeći.

Prijedlog zatvaranja korisničkog računa:

- ukoliko korisnik prestane biti zaposlenik zavoda, tajnica zavoda je dužna obavijestiti administratora da je korisniku potrebno zatvoriti korisnički račun,
- studentima se korisnički račun automatski zatvara prilikom završetka studija,
- trećoj stranici korisnički se računa zatvara nakon definiranog vremenskog perioda prilikom otvaranja računa, ili ukoliko je potrebno prije na zahtjev odgovorne osobe zadužene za suradnju s trećom stranom.

Poželjno je osmisliti komunikacijske protokole kojima će administrator sustava kontaktirati s korisnicima koji predaju zahtjeve za otvaranjem, odnosno zatvaranjem korisničkih računa u sam protokol poželjno je implementirati mogućnost jednostavnog zatvaranja korisničkog računa kako bi zatvaranje bilo odmah izvršeno nakon primitka zahtjeva.

Dodjela prava pristupa:

- administrator sustava glavni je u hijerarhiji kontrole pristupa i dodjeljivanju prava pristupa,
- administrator sustava ima pravo dodijeliti drugim korisnicima prava dodjeljivanja prava pristupa (na primjer, ukoliko je studentu potrebno dodijeliti pravo pristupa, to može učiniti asistent umjesto administratora),
- svaki od korisnika iz grupe zaposlenika ili studenata inicijalno ima ista minimalna prava pristupa potrebna (minimalna prava određuje administrator),
- svakom korisniku moguće je dati dodatna prava pristupa, ukoliko za tim postoji potreba,
- za pravo pristupa osjetljivim i tajnim podacima potrebno je ispuniti obrazac dodjele prava pristupa,
- trećoj strani prava pristupa određuje odgovorna osoba, te uz suglasnost administratora ista im se i dodjeljuju prilikom otvaranja korisničkog računa.

Ugovor o povjerenju jedna je od sigurnosnih kontroli pri zapošljavanju zaposlenika, pri suradnji Zavoda s vanjskim suradnicima ili u nekoj drugoj situaciji gdje postoji potreba za takvim ugovorom.

Ugovor o povjerenju treba uključiti:

- dužnosti Zavoda i dužnosti druge strane,
- odgovornosti Zavoda i odgovornosti druge strane,
- koje ovlasti nad vrijednostima ima Zavod, a koje druga strana,
- ukoliko je potrebno, sa svakim pojedincem potpisati ugovor o povjerenju, za svakog otvoriti korisnički račun i odrediti prava pristupa očekivano trajanje ugovora,
- tko je nadležan za ugovor od strane Zavoda, a tko od druge strane,
- koja prava ima Zavod, koja prava ima druga strana pri čemu je posebno potrebno naglasiti prava provjere, kontrole i nadgledanja,
- prava na intelektualno vlasništvo,
- na koji način reagirati u slučaju incidenta,
- dužnosti, obaveze i odgovornosti u slučaju prijevremenog raskida ugovora,

- koje akcije je potrebno poduzeti prilikom raskida ugovora (npr. uništavanje dokumenata).

Proces autorizacije sigurnosna je kontrola koja sprječava neovlaštenu nadogradnju informacijskog sustava, bilo da se ono odnosi na hardver ili softver.

Osoba odgovorna za sigurnost sustava dužna je:

- procijeniti i po potrebi napraviti ispitivanja da li je novi hardver kompatibilan s postojećim hardverom,
- procijeniti da li bi implementacijom novog hardvera sigurnost sustava bila znatno umanjena,
- procijeniti kvalitetu programske opreme, po potrebi izvršiti ispitivanja i kontaktirati specijalizirane stručnjake,
- procijeniti i odobriti korištenje osobnih sredstava u radu (prijenosno računalo, dlanovnik itd.),
- onemogućiti samovoljnu nadogradnju sustava,
- implementirati kontrole za detekciju nepravilnosti.

5.3 Upravljanje imovinom

Cilj – održati odgovarajuću zaštitu organizacijske imovine.

Popis imovine

Organizacija mora biti u stanju identificirati svoju imovinu i njenu relativnu vrijednost i važnost, na temelju čega se određuje razina zaštite.

Potrebno je sastaviti i održavati popis važnog inventara u svakom informacijskom sustavu. Svaki dio imovine treba biti jasno definiran, sa dogovorenim i dokumentiranim vlasništvom i sigurnosnim klasifikacijama te mora biti definirana njegova lokacija.

Primjeri imovine:

- *informacijska imovina* – baze podataka i datoteke s podacima, sistemska dokumentacija, procedure za podršku, planovi oporavka, sporazumi itd.,
- *softverska imovina* – aplikacijski softver, sistemski softver,
- *fizička imovina* – računalna oprema, komunikacijska oprema, magnetski mediji, ostala tehnička oprema.

Vlasništvo nad imovinom

Cilj – svim vrijednostima organizacije potrebno je odrediti vlasnika. Vlasnik je u ovom slučaju osoba odgovorna za imovinu u smislu sigurnosti (da ne dođe do mijenjanja, otuđivanja imovine itd.), te je dužna poduzeti sve potrebne kontrole kako bi imovina bila sigurna. Vlasnik je također odgovoran za klasifikaciju imovine i dodjeljivanje prava pristupa, uzimajući u obzir i poštujući odrednice politike sigurnosti.

Prihvatljivo korištenje imovine

Cilj – definiranje pravila pravilnog korištenja imovine. Smjernicama politike potrebno je ograničiti prava korištenja imovine u onim slučajevima gdje postoji rizik da se nepažljivim rukovanjem imovina (samim time cijeli informacijski sustav) izloži opasnosti.

Ova pravila najčešće uključuju:

- pravila korištenja elektroničke pošte i Interneta,
- smjernice za uporabu prijenosnih uređaja, posebno njihova uporaba izvan organizacije.

Klasifikacija informacija

Cilj – osigurati da informacijske vrijednosti dobiju odgovarajuću razinu zaštite.

Informacija treba biti klasificirana kako bi se iskazala potreba, prioritet i razina zaštite. Informacije posjeduju različite razine osjetljivosti. Neki predmeti mogu zahtijevati dodatnu zaštitu ili poseban način rukovanja. Sustav klasifikacije treba koristiti kako bi se definirale potrebne razine zaštite i kako bi se iskazala potreba za posebnim mjerama rukovanja.

Smjernice za klasifikaciju

Klasificiranjem informacije zapravo određujemo na koji način koristiti informaciju i kako ju štititi.

Klasifikacija se obavlja na temelju:

- vrijednosti,
- osjetljivosti,

- važnosti za organizaciju i
- zakonodavnih zahtjeva.

Pri klasificiranju potrebno je odrediti broj klasifikacijskih kategorija i koristi koje proizlaze iz njihova korištenja. Previše složene sheme (prevelik broj kategorija) mogu postati „uteg“ pri provedbi sigurnosti, te preteške i neekonomične za korištenje. Vrlo važno je biti oprezan kod interpretacije klasifikacijskih oznaka drugih organizacije, koje mogu imati drugačije definicije za slične ili iste oznake.

Odgovornost za definiciju klasifikacije neke informacije i za povremene preglede klasifikacije leži na vlasniku ili tvorcu informacije.

Označavanje i rukovanje informacijama

Cilj – definirati skup procedura za označavanje i rukovanje informacijama, u skladu sa shemom klasifikacije usvojenom od strane organizacije. Te procedure trebaju obuhvatiti informaciju kao imovinu i u fizičkom i u elektroničkom obliku. Za svaku klasifikaciju treba definirati procedure za rukovanje.

Procedure za rukovanje trebaju obuhvatiti sljedeće tipove aktivnosti obrade informacija:

- kopiranje,
- pohranu,
- prijenos poštom, faksom ili elektroničkom poštom,
- prijenos kroz razgovor, uključujući i mobilne telefone, telefonske sekretarice, glasovnu poštu,
- uništavanje.

Primjena norme u sigurnosnoj politici

Kada govorimo o zaštiti imovine, govorimo o zaštiti vrijednosti koje organizacija posjeduje, bilo da se radi o hardveru, softveru ili nekim drugim vrijednostima. Budući je fakultet institucija kojoj pristup ima mnogo osoba, kako bi sigurnost hardvera i softvera bila na zadovoljavajućoj razini nužno je uspostaviti adekvatne mjere sigurnost. Jedna od takvih mjera je *upravljanje imovinom*. Ova mjera kontrolira imovinu na način da se za svaki njen dio zna tko je vlasnik, kako je imovina klasificirana, vrsta imovine, postoji li sigurnosna kopija (za softver), lokacija imovine itd.

Zašto je to važno? U slučaju gubitka informacijskih vrijednosti, ukoliko nije poznato što je izgubljeno, vrlo je teško vratiti prvobitno stanje. Drugi primjer je napad hakera na informacijski sustav zavoda. Ako ne postoji kontrola imovine, haker može zamijeniti originalni hardver sustava svojim modificiranim hardverom i na taj način otvoriti mogućnost probijanja sigurnosne zaštite. Treći primjer je prekid zaposlenja administratora. Novi administrator više nije u mogućnosti uspostaviti kvalitetnu zaštitu sustava jer je vrijeme adaptacije tada puno duže. Ovi i još mnogi primjeri razlog su važnosti uspostave *upravljanja imovinom*.

Pri popisu imovine u informacijskom sustavu ZEMRIS, potrebno je sakupiti sljedeće podatke:

- **ID** – imovinu je potrebno označiti (ukoliko je riječ o hardveru) jedinstvenom identifikacijskom oznakom koja sadrži specifična obilježja kako ne bi mogla biti krivotvorena,
- **opis** – kratak opis imovine (monitor, telefon i sl.),
- **vrsta imovine** – da li je riječ o softveru, hardveru ili nekoj drugoj imovini,
- **vlasnik** – tko je odgovoran za imovinu, tko ju koristi,

- **klasifikacija** – vrijednost imovine okarakterizirano brojem prema klasifikaciji imovine,
- **lokacija** – gdje se fizički imovina nalazi,
- **sigurnosna kopija** – ako je vrsta imovine softver, gdje se nalazi sigurnosna kopija (ako postoji).

Osim popisa imovine, važno je odrediti prihvatljivo postupanje s imovinom. Prihvatljivo postupanje sprječava da se nestručnim rukovanjem imovinom ugrozi sigurnost informacijskog sustava. Prihvatljivo postupanje uključuje sve postojeće procedure rukovanja softverom, hardverom i ostalom imovinom informacijskog sustava ZEMRIS.

Klasifikacija informacijskih resursa jedna je od sigurnosnih mjera s ciljem označavanja imovine prema vrijednosti, osjetljivosti, važnosti za organizaciju i prema zakonodavnim zahtjevima. Klasifikacija resursa na je iz razloga što informacijski sustav ZEMRIS sadrži velik broj vrlo povjerljivih podataka (podaci o studentima, računima i sl.), te zbog podataka koji zahtijevaju visoke kriterije sigurnosti (ocjene studenata, ispitna pitanja i sl.).

5.4 Sigurnost i ljudski resursi

Cilj – smanjiti rizik od ljudske pogreške, krađa, prijevara i zlouporabe resursa.

Uloge i odgovornosti

Uloga osiguranja i odgovornost zaposlenika, ugovornih djelatnika i treće strane moraju biti definirana i dokumentirana u skladu sa sigurnosnom politikom organizacije.

Uloge i odgovornosti moraju uključiti potrebu za:

- zaštitom resursa od neovlaštenog pristupa, otkrivanja, mijenjanja, uništavanja ili ometanja,
- postupanjem u skladu s politikom sigurnosti,
- potpunim izvršavanjem sigurnosnih postupaka,
- prijavljivanjem prijetnji ili mogućih prijetnji nadležnim tijelima.

Provjera

Provjera (eng. *screening*) u svrhu kontrole potencijalnih zaposlenika, ulagača ili poslovnih partnera jedna je od preventivnih metoda kojima organizacija može djelovati na sigurnost informacijskog sustava.

Proces provjere i ispitivanja mora uzeti u obzir sva prava i zakonske odredbe privatnosti, te ukoliko je dopušteno uključiti sljedeće:

- raspoložive reference karaktera, poslovanja itd.,
- pregled dostupnih CV-a (*curriculum vitae*), kontrola dostavljenih podataka,
- potvrde o školovanju, profesionalnim kvalifikacijama,
- dokazi identiteta (putovnica),
- da li postoji kreditna zaduženost,
- da li je osoba kazneno gonjena itd.

Uvjeti zaposlenja

Prije zaposlenja radnika, sklapanja partnerstva s drugom organizacijom ili uključivanja u posao treće strane neophodno je u ugovor uključiti dio koji sve strane obavezuje na pridržavanje pravila definiranih sigurnosnom politikom.

Ugovor treba sadržavati dodatak s pojašnjenjima i stavovima:

- da svaki zaposlenik, partner ili treća strana, prije dobivanja prava pristupa imovini organizacije, mora potpisati ugovor o povjerenju,
- o zakonskim pravima i odgovornostima svakog zaposlenika,
- korisnika i poslovnog partnera,
- o odgovornostima organizacije o čuvanju i rukovanju informacijama o zaposlenicima,
- o odgovornostima u slučaju obavljanja posla izvan radnog vremena ili izvan prostorija organizacije, npr. kod kuće,
- o akcijama koje je potrebno poduzeti ukoliko se utvrdi nepridržavanje pravila definiranih sigurnosnom politikom.

Odgovornosti rukovoditelja

Rukovoditelji moraju zahtijevati i inzistirati na pridržavanju pravila definiranih sigurnosnom politikom od strane zaposlenika, korisnika, poslovnih partnera i treće strane.

Njihova je zadaća sve zaposlenike, korisnike, partnere i treće strane:

- pravilno i jasno informirati o njihovim ulogama u provedbi sigurnosti, te o njihovim odgovornostima prije dodjeljivanja prava pristupa osjetljivim informacijama,
- pružiti im uvid u obliku smjernica o tome što se očekuje od njih ovisno o njihovim ulogama,
- motivirati da se pridržavaju pravila definiranih sigurnosnom politikom,
- osigurati potrebnu razinu svijesti o potrebi za sigurnošću, ovisno o ulogama.

Edukacija o informacijskoj sigurnosti

Svi zaposlenici organizacije, i ukoliko se ukaže potreba, partneri i osoblje treće strane moraju proći odgovarajuću obuku o svijesti o informacijskoj sigurnosti, te pravovremeno biti upoznati s dopunama ili promjenama u sigurnosnoj politici organizacije.

Osnovni pojmovi o sigurnosti i obuka o svijesti o informacijskoj sigurnosti moraju biti prezentirani zaposlenicima, partnerima i trećoj strani prije dodjeljivanja prava pristupa informacijama. Edukacija korisnika mora biti prikladna s ulogom, sposobnosti i odgovornosti pojedinca.

Raskid ugovora

Postupci i odgovornosti kod prekida radnog odnosa, raskida ugovora ili promjene radnog mjesta moraju biti jasno propisani. Zaposlenik, partner ili treća strana mora vratiti u posjed organizacije sve materijalne vrijednosti koje je dobio na korištenje tijekom radnog odnosa osim ukoliko je ugovorom drugačije dogovoreno. Zaposleniku, partneru ili trećoj strani nakon raskida ugovora moraju biti oduzeta sva prava pristupa informacijama i drugim osjetljivim vrijednostima. Sve odgovornosti nad imovinom koju je dosad imao zaposlenik moraju biti dodijeljene drugoj odgovornoj osobi.

Primjena norme u sigurnosnoj politici

Velik broj vrlo osjetljivih i tajnih podataka koje informacijski sustav ZEMRIS sadrži razlog su potrebe za visokim stupnjem sigurnosti. Jedna od preventivnih metoda kojima možemo utjecati na sigurnost je i kontrola korisnika (zaposlenici, studenti, treće strane..) kojima dodjeljujemo prava pristupa osjetljivim podacima.

Ova vrsta kontrole definirana je u dokumentu *Pravilnik o sklapanju i raskidu ugovora*, a definira na koje je predradnje potrebno poduzeti prilikom sklapanja ugovora, koje sve mjere sigurnosti treba definirati ugovor, te kako osigurati kvalitetan raskid ugovora.

5.5 Fizička zaštita i zaštita od okoline

Cilj – spriječiti neovlašteni pristup, štetu i ometanje poslovnih prostorija i informacija.

Kritične i osjetljive poslovne objekte za obradu informacija treba postaviti u sigurnom području, zaštićene prema klasifikaciji (osjetljivost i i važnosti objekta koji se štiti). Fizička zaštita područja sastoji se od ograđivanja (najčešće zidovima i protuprovalnim-protupožarnim vratima) i kontrolom pristupa (ući mogu samo ovlaštene osobe, snimanje prostorija itd.).

Područje fizičke zaštite

Sigurnosne barijere poput zidova ili karticom kontrolirani ulazi u prostorije trebaju služiti za zaštitu onih dijelova organizacije koji sadrže povjerljive informacije i objekte.

Sljedeće smjernice moraju biti razmotrene i po potrebi implementirane gdje postoji potreba za fizičkom zaštitom:

- sigurnosna područja moraju biti strogo označena; jačina i opseg zaštite ovisi o procjeni rizika, vrijednosti i osjetljivosti imovine koje to područje sadrži,
- kontrolnim mehanizmima potrebno je spriječiti svaki pokušaj neovlaštenog pristupa,
- vrata na ulazima u zaštićena područja moraju biti otporna na požare, poplave, probijanja itd.,
- svi ulazi u zaštićena područja trebaju biti nadgledana i snimana pomoću kamera,
- glavni ulazi u sigurnosna područja moraju imati čuvara koji kontrolira tko ulazi, što se unosi te je po potrebi spreman intervenirati,
- svi kontrolni mehanizmi moraju biti periodički pregledavani kako bi se na vrijeme uočili nedostaci zaštite ili pokušaji neovlaštenog pristupa itd.

Fizička kontrola ulaska

Sigurnosna područja moraju biti zaštićena odgovarajućim kontrolama ulaska kako bi se osiguralo da mogućnost ulaska imaju samo ovlaštene osobe.

Potrebno je proučiti sljedeće smjernice:

- datum i vrijeme ulaska te odlazak osobe mora biti zabilježen,
- sve aktivnosti korisnika moraju biti nadgledane, osim ukoliko posebnim odrednicama nije drugačije definirano,
- pristup sigurnosnim područjima trebaju imati samo ovlaštene osobe čiji rad ovisi o opremi i informacijama iz tog područja,
- pristup područjima treba biti definiran prema područjima, a ne prema „klasifikaciji“ zaposlenika,
- svi zaposlenici, poslovni partneri i treća strana trebaju nositi prepoznatljivu odjeću; ukoliko se pojavi netko bez takve odjeće potrebno je odmah alarmirati odgovorne za sigurnost,
- prava pristupa trebaju biti periodički pregledavana i ažurirana.

Sigurnost opreme

Cilj – spriječiti gubitke, štetu ili kompromitiranje imovine i prekid poslovnih aktivnosti.

Oprema treba biti zaštićena od prijetnji i opasnosti iz okoline. Zaštita opreme je neophodna kako bi se smanjio rizik neovlaštenog pristupa podacima, te kako ne bi došlo do gubljenja i oštećenja imovine.

Smještaj i zaštita opreme

Sljedeće smjernice treba uzeti u obzir pri zaštiti opreme:

- oprema mora biti smještena tako da je nepotrebni pristup opremi minimalan,
- jedinice za obradu podataka moraju biti smještene tako da je smanjena mogućnost promatranja neovlaštenim korisnicima (na primjer, postavljanje monitora pod takvim kutom da samo osoba za računalom vidi sliku),
- kontrole je potrebno implementirati tako da minimaliziraju rizik od potencijalnih prijetnji; primjer: krađa, požar, dim, voda, vibracije, radijacije itd.,
- da li je dopušteno jesti, piti, pušiti u blizini opreme,
- uvjeti okružja (temperatura, vlaga) koji mogu utjecati na rad jedinica za obradu informacija trebaju biti nadzirane.

Sigurnost instalacija

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u opskrbi energijom, vodom, odvodnjom otpadnih voda, grijanjem/hlađenjem itd. Sve navedene instalacije moraju biti pravovremeno pregledane i testirane kako bi se na vrijeme uočile i ispravile greške u radu.

Jedinice za neprestano napajanje (UPS – *eng. uninterruptible power supply*) neophodne su u slučaju nestanka struje. Takve jedinice vremenski vrlo kratko mogu napajati jedinice za obradu podataka, pogotovo ukoliko je sustav velik. Stoga je važno razmotriti ugradnju strujnih generatora čija je mogućnost napajanja daleka veća od običnih jedinica za neprestano napajanje.

Nestanak struje, poplavu, požar ili bilo koju drugu prijetnju bitno je alarmirati zvučnim i svjetlosnim signalima kako bi se pravovremeno poduzele propisane akcije u slučaju nezgode. Opskrba vodom mora biti redovito kontrolirana kako ispravnost uređaja za gašenje požara ne bi bila upitna. Telekomunikacijska oprema mora biti instalirana na način da eventualan prekid veze ne utječe na kompletan prekid komunikacije. Primjer rješenja ovog problema je priključenje komunikacijskih uređaja na više poslužitelja.

Sigurnost kod kabliranja

Kablovi za opskrbu električnom energijom i telekomunikacijski kablovi moraju biti adekvatno zaštićeni od oštećenja, prekida ili priključenja neovlaštenih korisnika na mrežu.

Prije kabliranja mora biti razmotreno sljedeće:

- kabeli za napajanje jedinica za obradu podataka, ukoliko je moguće, moraju biti položeni podzemno; alternativa je adekvatna fizička zaštita,
- isto vrijedi i za telekomunikacijske kabele,
- kabeli za napajanje moraju biti razdvojeni od telekomunikacijskih kako bi se izbjeglo međudjelovanje,
- označavanje kabela posebnim identifikacijskim oznakama spriječiti će greške u spajanju; oznake je potrebno dokumentirati.

Održavanje opreme

Održavanje opreme treba biti redovito i obavljeno od strane stručnjaka kako bi se osigurala ispravnost, tj. neprekidan rad.

Pri održavanju opreme treba se pridržavati sljedećeg:

- održavanje opreme mora biti u skladu s preporukama proizvođača, u određenim vremenskim intervalima i po zadanim specifikacijama,
- samo ovlaštene osobe smiju servisirati opremu,

- prije servisiranja opreme potrebno je implementirati odgovarajuće sigurnosne kontrole ukoliko za tim postoji potreba, te je potrebno obrisati povjerljive informacije (potrebe za ovakvim mjerama nastaju ukoliko servisiranje izvršava vanjski partner ili treća strana).

Primjena norme u sigurnosnoj politici

Zbog velikog broja ljudi koji koriste resurse zavoda i relativno lakog pristupa pojedinca prostorijama zavoda politika fizičke zaštite ovdje je vrlo bitna. Kako bi se spriječile nezakonite radnje zlonamjernih korisnika, ali i slučajne pogreške zaposlenika ili studenata, pristup prostorijama koje sadržavaju osjetljivu opremu (poslužitelji, baze podataka i sl.) mora bit strogo kontroliran. Nužno je omogućiti pristup isključivo ovlaštenim osobama koji za pristupom imaju potrebu zbog prirode obavljanja posla. Svim ostalim korisnicima pristup mora biti strogo zabranjen. Osim prostorija velika pažnja mora se posvetiti sigurnosti kabela. Svi kablovi (napajanje, komunikacijski i sl.) moraju biti fizički zaštićeni i odvojeni od neovlaštenih korisnika. Svu opremu koju fizički nije moguće smjestiti u „sigurne“ prostorije mora biti zaštićena od neovlaštenih korisnika na način da se postavi u sigurnosne ormariće. Posebnu pažnju treba posvetiti održavanju opreme, te kontroliranju da li postoji naznake zlonamjernih radnji – oštećenje, krađa, mijenjanje opreme i sl.

5.6 Upravljanje komunikacijama i operacijama

Procedure rada i odgovornosti

Cilj – osigurati pravilan i siguran rad jedinica za obradu informacija.

Potrebno je definirati odgovornosti i procedure za upravljanje i rad svih jedinica za obradu informacija, uključujući razvoj odgovarajućih operativnih instrukcija i procedura koje se koriste prilikom incidenata. Ukoliko postoji mogućnost, potrebno je implementirati i *dijeljenje dužnosti* kako bi se smanjio rizik od zlouporabe izazvane nemarom ili namjerno.

Dokumentirane procedure rada

Operativne procedure moraju biti dokumentirane, održavane i dostupne svim korisnicima koji ih koriste.

One moraju odrediti upute za detaljno izvođenje svakog posla, uključujući:

- obradu i rukovanje informacijama,
- izradu sigurnosne kopije (eng. backup),
- planiranje potreba, uključujući međuovisnosti s drugim sustavima te najranije vrijeme početka i najkasnije vrijeme završetka posla,
- upute za rukovanje greškama i ostalim iznimnim uvjetima, koji mogu nastati prilikom izvršavanja posla,
- kontakt osobe za podršku prilikom neočekivanih operativnih ili tehničkih poteškoća,
- posebne upute za rukovanjem rezultatima rada, kao što je uporaba posebnog pribora ili upravljanje povjerljivim rezultatima,
- postupke za ponovno pokretanje i oporavak sustava u slučaju kvara.

Nadzor promjena u operativi

Cilj - promjene vezane uz objekte i sustave za obradu informacija moraju biti kontrolirane.

Nedovoljna kontrola promjena u jedinicama i sustavima za obradu informacija najčešći je uzrok sigurnosnih ili sistemskih ispada. Potrebno je uspostaviti formalne odgovornosti i postupke kako bi se osigurala zadovoljavajuća kontrola svih promjena u opremi, softveru ili procedurama.

Sljedeće kontrole treba uzeti u obzir:

- identifikacija i bilježenje značajnih promjena,
- planiranje i testiranje promjena,
- ocjenjivanje potencijalnih utjecaja, na primjer sigurnosnih pri određenim promjenama,
- odobrenja za predložene promjene,
- objavljivanje promjena svim relevantnim osobama,
- procedure u slučaju opasnosti, na primjer procedure i odgovornosti za prekid neočekivanih događaja i obnovu neuspješnih promjena.

Odvajanje dužnosti

Obveze i područja odgovornosti trebaju biti odvojene kako bi se mogućnost obavljanja neovlaštenih i neželjenih radnji svela na minimum.

Odvajanje dužnosti metoda je kojom se reducira rizik od zlouporabe sustava. Zaštita bi trebala biti organizirana na taj način da osoba kao pojedinac nema ovlasti nad imovinom. Drugim riječima, kako bi se obavila radnja mijenjanja, čitanja, ili brisanja

informacije, suglasnost mora dati više ovlaštenih osoba. Na taj način uklanja se mogućnost da ovlaštena osoba svojevoljno izvrši štetnu radnju po imovinu organizacije.

Kontrola *odvajanje dužnosti* u praksi je vrlo komplicirana i primjenjiva je jedino za postupke vezane uz imovinu vrlo visokog rizika i vrijednosti. Kad god je teško razdvojiti dužnosti (npr. zbog veličine organizacije) potrebno je upotrebljavati druge kontrole. Važno je voditi računa o tome da niti jedna osoba ne može neopaženo počiniti prijevaru.

Razdvajanje objekata za razvoj, testiranje i operativni rad

Razdvajanje objekata za razvoj, testiranje i operativni rad važno je kako bi se postiglo odvajanje uključenih uloga. Pravila prelaska softvera iz razvojnog u operativni rad moraju biti definirana i dokumentirana.

Razvojne i testne aktivnosti mogu uzrokovati ozbiljne probleme, na primjer neželjene promjene sistemske okoline ili pad sustava. Mora se uzeti u obzir nivo potrebnog razdvajanja između operativnih, testnih i razvojnih okolina kako bi se spriječili operativni problemi.

Potrebno je održati poznatu i stabilnu okolinu u kojoj je moguće izvoditi značajno testiranje i spriječiti neprimjeren pristup razvojnog osoblja.

Tamo gdje razvojno i testno osoblje ima pristup do operativnih sustava i njihovih podataka, postoji mogućnost da uvedu neovlašteni i neispitani kôd ili izmjene operativne podatke. U nekim sustavima se ta mogućnost može iskoristiti kako bi se počinila prijevara ili za unošenje neispitanog ili malicioznog kôda. Neispitani ili maliciozni kôd može prouzročiti ozbiljne operativne probleme. Razvojno i testno osoblje predstavlja prijetnju i za povjerljivost operativnih informacija.

Aktivnosti testiranja i razvoja mogu prouzročiti neželjene izmjene u softveru i informacijama, ako se izvršavaju u zajedničkom računalnom okruženju. Odvajanje razvoja, testiranja i operative je stoga poželjno radi reduciranja rizika od slučajnih izmjena ili neovlaštenog pristupa operativnom softveru i poslovnim podacima.

Potrebno je uzeti u obzir sljedeće kontrole:

- razvojni i operativni softver treba izvršavati na različitim računalima,
- aktivnosti razvoja i testiranja treba što više razdvojiti,
- za razvojne i operativne sustave potrebno je koristiti različite postupke prijave u sustav. Korisnike treba poticati da koriste različite lozinke za takve sustave, a izbornici trebaju prikazivati kojim sustavom se korisnik koristi.

Planiranje i prihvaćanje sustava

Cilj – smanjiti rizik pada sustava.

Planiranje i pripreme su potrebne kako bi se osigurala dostupnost prikladnih kapaciteta i resursa. Nužno je napraviti projekcije budućih zahtjeva kapaciteta i izvršiti procjene kako bi se smanjio rizik preopterećenja sustava. Operativni zahtjevi novog sustava trebaju se utvrditi, dokumentirati i testirati prije njegovog prihvaćanja i upotrebe.

Planiranje kapaciteta

Potrebno je pratiti zahtjeve za kapacitetima i napraviti projekcije budućih zahtjeva za kapacitetima, kako bi se osigurala odgovarajuća procesna snaga i prostor za pohranu. Projekcije trebaju uzeti u obzir nove poslovne i sistemske zahtjeve, te trenutne i projicirane trendove u obradi informacija u organizaciji.

Serverska računala zahtijevaju posebnu pažnju zbog puno većih troškova i vremena nabave novih kapaciteta. Zbog toga je unaprijed potrebno uzeti u obzir sve relevantne parametre koji utječu i koji bi mogli utjecati na rad sustava kako bi identificirala i izbjegla potencijalna uska grla.

Prihvaćanje sustava

Rukovoditelji su dužni osigurati da su zahtjevi i kriteriji za prihvaćanje novog informacijskog sustava ili nadogradnji jasno definirani, dogovoreni, dokumentirani i testirani.

Potrebno je razmotriti sljedeće kontrolne mehanizme:

- zahtjevi za kapacitetom i performansama računala,
- postupci za oporavak od pogrešaka i za ponovno pokretanje sustava,
- priprema i testiranje rutinskih operativnih postupaka prema definiranim normama,
- postavljanje i pridržavanje dogovorenog skupa kontrolnih mehanizama,
- trening za operativnu uporabu novih sustava.

Zaštita od malicioznog softvera

Cilj – zaštititi integritet softvera i informacija.

Mjere zaštite potrebne su kako bi se spriječila i na vrijeme uočila uporaba malicioznog softvera. Softver i objekti za obradu informacija ranjivi su obzirom na zloćudni softver kao što su računalni virusi, mrežni crvi, logičke bombe itd. Korisnike treba upoznati s opasnostima uporabe neodobrenog ili zloćudnog softvera i rukovoditelji bi trebali, ukoliko postoje mogućnosti, potaknuti implementaciju kontrola koji detektiraju i sprječavaju uporabu takvog softvera.

Kontrole protiv malicioznog softvera

Cilj – implementirati kontrolne mehanizme koji preventivno djeluju na prijetnje malicioznog softvera i razviti procedure koje osiguravaju svjesnost korisnika.

Sljedeće kontrolne mehanizme potrebno je uzeti u obzir:

- formalna politika koja zahtjeva sukladnost sa softverskim licencama i koja zabranjuje uporabu neautoriziranog softvera,
- mora biti uspostavljena formalna politika koja se odnosi na rizike vezane uz nabavu softvera i datoteka s vanjskih mreža ili s nekog drugog medija. U toj politici treba biti naznačeno koje je zaštitne mjere potrebno poduzeti,
- potrebna je instalacija i redovno ažuriranje antivirusnih programa,
- potrebno je redovito provoditi provjeru softvera i podataka koji podržavaju kritične poslovne procese. Postojanje bilo kakvih neodobrenih datoteka mora se formalno istražiti,
- provjera na zloćudni softver svih datoteka na elektroničkim medijima nesigurnog ili neautoriziranog porijekla,
- provjera na zloćudni softver svih datoteka nabavljenih preko nesigurnih mreža,
- provjera na zloćudni softver svih mail privitaka,
- plan oporavka i kontinuiranog poslovanja u slučaju napada malicioznog softvera,
- izrada sigurnosnih kopija svih neophodnih podataka.

Izrada sigurnosnih kopija

Cilj – očuvanje integriteta i dostupnosti podataka redovitom izradom sigurnosnih kopija neophodnih poslovnih informacija.

Pri izradi sigurnosnih kopija treba uzeti u obzir:

- na udaljenoj lokaciji potrebno je spremati minimalni broj sigurnosnih kopija informacija, zajedno s točnim i potpunim zapisima o sigurnosnim kopijama i dokumentiranim procedurama za ponovno osposobljavanje sustava. Lokacija mora biti na dovoljnoj udaljenosti od glavne lokacije kako bi se izbjegla šteta koja može nastati od posljedica katastrofe na glavnoj lokaciji,
- sigurnosnim kopijama mora se osigurati prikladna razina fizičke zaštite i zaštite okoline u skladu s normama koje se primjenjuju na glavnoj lokaciji,
- mediji sigurnosnih kopija, gdje je primjenjivo, moraju se redovno testirati kako bi se osiguralo da se na njih može računati u slučaju potrebe,
- procedure za ponovno uspostavljanje sustava moraju se redovito provjeravati i testirati kako bi se osigurala njihova učinkovitost i mogućnost izvršavanja u predviđenom vremenu,
- vrijeme čuvanja sigurnosnih kopija mora biti točno određeno.

Upravljanje sigurnošću mreže

Cilj – osigurati zaštitu informacija na mreži i zaštitu infrastrukture.

Rukovoditelji sigurnosti mreža dužni su sveobuhvatnim pristupom i pažljivim razmatranjem osigurati sigurnost informacija na svakom dijelu njihovog puta. Također su dužni implementirati dodatne kontrole za zaštitu osjetljivih podataka koji putuju preko javnih ili nezaštićenih mreža.

Za postizanje i održavanje mrežne sigurnosti potrebno je primijeniti niz kontrolnih mehanizama. Posebno je potrebno promotriti sljedeće:

- operativne odgovornosti za mreže trebaju biti odvojene od računalne operative gdje je to moguće,
- potrebno je uspostaviti postupke i odgovornosti za upravljanje udaljenom opremom,
- potrebno je uspostaviti kontrole kako bi se sačuvala povjerljivost i integritet podataka koji prolaze nezaštićenim mrežama.

Rukovanje i sigurnost medija

Cilj – spriječiti štetu na imovini i prekide poslovnih aktivnosti. U svrhu zaštite potrebno je uspostaviti odgovarajuće procedure za zaštitu dokumenata, računalnih medija i sistemske dokumentacije od krađe, neovlaštenog pristupa, povrede integriteta itd.

Upravljanje prijenosnim medijima

Cilj – uspostava postupaka za upravljanje izmjenjivim računalnim medijima (trake, kazete, CD, DVD, štampana izvješća itd.).

Treba uzeti u obzir sljedeće kontrole:

- ako više nisu potrebni, treba obrisati prijašnje sadržaje svakog ponovno iskoristivog medija koji će biti uklonjen iz organizacije,
- potrebno je tražiti ovlaštenje za uklanjanje medija iz organizacije, te se mora voditi zapis o takvim aktivnostima,
- svi mediji moraju biti pohranjeni na sigurnom i zaštićenom mjestu, u skladu sa specifikacijama proizvođača,
- svi postupci i razine ovlaštenja moraju biti jasno određeni i dokumentirani.

Uklanjanje medija

Cilj – ukoliko više nisu potrebni mediji se moraju ukloniti na siguran način, u suprotnom može doći do „curenja“ osjetljivih informacija. Kako bi se rizik „curenja“ sveo na minimum potrebno je uspostaviti formalne smjernice za sigurno uklanjanje medija.

Lista dokumenata koji mogu zahtijevati sigurno uklanjanje:

- papirnati dokumenti,
- snimljeni glas,
- indigo papir,
- traka za printer,
- magnetski mediji,
- optički mediji,
- sistemska dokumentacija itd.

Uklanjanje osjetljivih medija treba biti provjereno i dokumentirano.

Procedure za rukovanje informacijama

Cilj – uspostaviti procedure za rukovanje informacijama kako bi se informacije zaštitile od neovlaštenog otkrivanja i zlouporabe.

Procedure treba razraditi tako da rukovanje informacijama bude sukladno sa njenom klasifikacijom.

Treba uzeti u obzir sljedeće kontrole:

- rukovanje medijima i označavanje identifikacijskom oznakom,
- ograničavanje pristupa,
- održavanje popisa ovlaštenih primaoca podataka,
- pohrana podataka po specifikacijama proizvođača,
- zaštita podataka u skladu s njihovom osjetljivošću,
- minimalna distribucija podataka,
- jasno označavanje svih kopija podataka.

Razmjena informacija

Cilj – osigurati sigurnost pri razmjeni informacija i softvera unutar organizacije ili izvan nje. Kako bi se zaštitila razmjena podataka potrebno je definirati smjernice razmjene, uspostaviti i vršiti kontrolu, te sankcionirati prekršitelje prema važećim zakonima.

Potrebno je uspostaviti sporazume o razmjeni informacija i softvera između organizacija. Oni trebaju uključiti:

- odgovornosti rukovoditelja za kontrolu i obavještavanje o razmjenama,
- procedure za obavještavanje pošiljaoca za slanje i primanje podataka,
- minimalne tehničke norme za pakiranje i prijenos,
- norme za identifikaciju,
- odgovornosti i obveze u slučaju gubitka podataka,
- korištenje dogovorenog sustava označavanja osjetljivih informacija,
- odgovornosti i vlasništvo nad softverom i informacijama radi njihove zaštite, uskladivosti s autorskim pravima i sl.

Nadgledanje

Cilj – pravovremeno uočavanje neovlaštenih aktivnosti.

Informacijski sustav nužno je konstantno nadzirati (eng. *monitoring*) te bilježiti svaku aktivnost. Nadziranje mora biti zadovoljavati sve važeće zakone, korisnike treba obavijestiti o nadgledanju i dati im do znanja da su im prava privatnosti minimalna.

Kako bi bili uočeni eventualni propusti u implementaciji sigurnosnih kontrola potrebno je voditi dnevnik svih aktivnosti i događaja unutar sustava. Provjerom zabilježenih podataka moguće je otkriti nepravilnosti i na vrijeme ih ukloniti.

U bilješkama dnevnika treba biti sadržano:

- korisnička identifikacija (ID),
- datum, vrijeme, detalji akcije (prijava, odjava itd.),
- identifikacija računala,
- mjesto pristupa,
- (ne)uspješan pristup sustavu,
- (ne)uspješan pristup podacima,
- mijenjanje postavki sustava,
- korištenje privilegija,
- korištenja usluga sustava i aplikacija,
- način pristupa podacima,
- mrežna adresa i protokol,
- aktivacija i deaktivacija zaštite sustava,
- uključenje alarma itd.

Primjena norme u sigurnosnoj politici

Informacijski sustav ZEMRIS relativno je mali sustav, s malim brojem odgovornih korisnika. Zbog toga je nepotrebno uvoditi sigurnosne kontrole kao što je odvajanje dužnosti, razdvajanje objekata za razvoj, testiranje, operativni rad, kapaciteti sustava su kontinuirani –nije potrebno provoditi planiranje kapaciteta i sl.

Informacijski sustav ZEMRIS u svrhu kvalitetnijeg upravljanja komunikacijama i operacijama zahtjeva posebnu pažnju na sljedećim elementima sigurnosti:

- zaštita od malicioznog softvera – velik broj korisnika; educiranost korisnika upitna; potrebno je djelovati na sve korisnike i educirati ih o mogućim prijetnjama kako svojim neznanjem ne bi olakšali zlonamjernim korisnicima put ka počinjenju zlonamjernih radnji,
- izrada sigurnosnih kopija – podaci koje je vrlo teško ili nemoguće obnoviti ukoliko ne postoje sigurnosne kopije – nužno redovita izrada sigurnosnih kopija; ne treba za sve podatke jednako često raditi sigurnosnu kopiju – treba uspostaviti više kategorija sigurnosnih kopija (dnevne, tjedne, mjesečne, godišnje) kako se ne bi nepotrebno trošili resursi,
- edukacija korisnika – korisnici svojim neznanjem ili slučajnim radnjama mogu ugroziti informacijski sustav; neophodno je djelovati preventivno, educirati korisnike o sigurnosnim prijetnjama i potaknuti ih da razmišljaju „svojom glavom“,
- nadgledanje – pravovremeno uočavanje neovlaštenih aktivnosti; u slučaju uspješnog napada lakše doći do napadača,
- upravljanje sigurnosti mreže – općenito o sigurnosti sustava; odnosi se na administratora, tj. glavnu odgovornu osobu.

5.7 Kontrola pristupa

Kontrola pristupa u skladu s poslovnim zahtjevima

Pristup informacijama, jedinicama za obradu informacija i poslovnim procesima treba biti kontroliran na temelju zahtjeva poslovanja i sustava sigurnosti.

Politika kontrole pristupa

Prava pristupa svakog pojedinca ili grupe korisnike trebaju biti jasno definirana u politici kontrole pristupa.

Politika kontrole pristupa treba obuhvatiti:

- zahtjeve sigurnosti pojedinačnih poslovnih aplikacija,
- identifikaciju svih informacija vezanih uz poslovne aplikacije,
- politiku za širenje i autorizaciju informacija (klasifikacija),
- konzistentnost kontrole pristupa s politikom klasifikacije informacija u raznim sustavima,
- relevantne zakone i ugovorne obveze koje se odnose na zaštitu pristupa,
- standardizirane profile pristupa za uobičajene kategorije poslova,
- upravljanje pravima pristupa.

Upravljanje pristupom korisnika

Cilj – spriječiti neovlašteni pristup informacijskim sustavima.

Potrebno je uspostaviti procedure za kontrolu dodjele prava pristupa informacijskim sustavima. Te procedure trebaju obuhvatiti sve stadije u životnom ciklusu korisničkog pristupa – od početne registracije novog korisnika do konačnog odjavljivanja korisnika kojem više nije potreban pristup sustavu i uslugama.

Registracija korisnika

Mora postojati formalna registracija i odjava korisnika radi dobivanja prava pristupa višekorisničkim informacijskim sustavima i servisima.

Pristup treba kontrolirati kroz proces registracije korisnika, koji uključuje:

- korištenje jednostavnih korisničkih imena, kako bi se korisnike moglo povezati s njihovim aktivnostima i učiniti odgovornima,
- provjera ovlaštenja korisnika za korištenje informacijskog sustava ili servisa,
- provjera da dozvoljena razina pristupa odgovara poslovnim potrebama i da je u skladu s politikom sigurnosti,
- korisnicima je potrebno dati pismene izjave o pravima pristupa te zahtijevati od njih da potpišu izjavu kao znak primitka i razumijevanja uvjeta pristupa,
- osiguranje da pružatelj usluge ne dozvoli pristup dok nije proveden autorizacijski postupak,
- održavanje popisa svih korisnika registriranih za korištenje servisa,
- trenutačno ukidanje prava korisnika,
- povremene provjere korisničkih imena i računa.

Upravljanje privilegijama

Cilj - dodjela i korištenje privilegija treba biti ograničena i strogo kontrolirano.

Potrebno je razmotriti:

- identificirati privilegije i korisnike kojima ih treba dodijeliti,
- privilegije treba dodjeljivati pojedincima na temelju potreba i situacija,
- razina privilegije mora biti minimalna potrebna za funkcioniranje,

- bilježenje svih dodijeljenih privilegija,
- dodjeljivanje privilegija pod novim korisničkim imenom.

Upravljanje korisničkim lozinkama

Raspodjelu lozinki treba kontrolirati kroz formalni proces upravljanja lozinkama koji uključuje:

- zahtijevati od korisnika da potpišu izjavu u kojoj se obvezuju da će čuvati lozinke povjerljivima,
- zahtijevati da se lozinke proslјeđuju korisnicima na siguran način,
- uporabu elektroničke pošte ili treće strane treba izbjegavati,
- lozinke se ne smiju pohranjivati na računalu u nezaštićenom obliku.

Odgovornost korisnika

Cilj – spriječiti neovlašteni pristup korisnika, potaknuti svijest korisnika o vlastitoj odgovornosti oko korištenja lozinki i sigurnosti opreme koju koriste.

Korisnici se prilikom uporabe lozinki moraju pridržavati sigurnosnih uputa koje su definirane politikom sigurnosti. Oni moraju biti svjesni da se lozinkom potvrđuje njihov identitet, omogućavajući time pravo pristupa do jedinica i servisa za obradu podataka.

Korisnici su dužni:

- čuvati povjerljivost lozinki,
- ne bilježiti lozinke na papir,
- lozinke se ne smiju odavati drugim korisnicima, čak ni administratorima, odgovornim osobama i sl.,
- korisnici ne smiju mijenjati lozinke ukoliko sumnjaju na nepravilnosti u radu servisa (primjer phishing, socijalni inženjering i sl.),
- birati kvalitetne lozinke, duge minimalno 6 znakova, da nisu vezane uz imena, datume, telefonske brojeve i sl.,
- lozinke moraju sadržavati i brojeve i slova, ako je moguće i specijalne znakove,
- izbjegavati ponovnu uporabu starih lozinki,
- izbjegavati lozinke koje već koriste na drugim sustavima,
- redovito mijenjati lozinke itd.

Osim odgovornosti nad uporabom lozinki, korisnici su dužni prikladno zaštititi opremu kada nisu u njezinog blizini. Svi korisnici moraju biti svjesni svojih odgovornosti nad zaštitom neosigurane opreme, koje prvenstveno uključuje:

- korisnici ukoliko se udaljavaju od računala za vrijeme radnog vremena, obavezno moraju osigurati računalo primjerenim sigurnosnim mehanizmima (CTRL + L, screen saveri s lozinkom i sl.),
- prilikom gašenja računala nužno je odjaviti se sa sustava; ne samo ugasiti terminal ili računalo,
- osiguraju računalo i terminale od neovlaštenog korištenja; posebno kada nisu u uporabi.

Kontrola pristupa mreži

Cilj – zaštita mrežnih servisa.

Kontrola pristupa mrežnim servisima (i internim i eksternim) nužna je kako bi se spriječilo kompromitiranje sigurnosti od strane korisnika koji imaju pristup mreži i mrežnim resursima. Sigurnost mrežnih servisa potrebno je provesti kroz:

- osiguranje odgovarajućih sučelja,

- osiguranje mehanizama za provjeru vjerodostojnosti korisnika i opreme,
- kontrolu korisničkog pristupa do informacijskih servisa.

Jedan od koraka uspostave sigurnosti pristupa mreži je u definiranju politike prema kojoj korisnici smiju pristupiti samo onim servisima za koja imaju uređena prava pristupa. Ukoliko korisnik nema definirana prava pristupa, pristup servisu je zabranjen. Kako bi zabrana ili dozvola pristupa bila moguća, potrebno je implementirati kvalitetne kontrole identifikacije i autorizacije, te definirati procedure za zaštitu pristupa mreži mrežnim servisima.

Definiranje propisanog puta od terminala do servisa sigurnosna je kontrola koja sprječava zlonamjernog korisnika da karakteristiku mreže – maksimalno dijeljenje resursa, iskoristi za neautorizirani pristup aplikacijama i uređajima za obradu podataka. Definiranjem propisanog puta korisniku se ne dopušta biranje puta od terminala do servisa, tj. moguće je birati samo propisane. Princip ove kontrole je da se na svakom čvoru unaprijed odrede dopuštene rute.

Primjeri propisanih puta:

- dodjela stalnih linija,
- automatsko spajanje ulaza na određene aplikacije,
- limitiranje opcija u izbornicima za određenu grupu korisnika,
- sve vrste aktivnih kontrola.

Kontrola pristupa operacijskom sustavu

Kako bi spriječili neovlašteni pristup računalnim resursima, potrebno je uspostaviti sigurnosne mehanizmi i unutar samog operativnog sustava.

Time se:

- identificira i provjerava identitet svakog ovlaštenog korisnika,
- provjerava se lokacija terminala,
- bilježe uspješni i neuspješni pristupi sustavu,
- osigurava primjeren način provjere vjerodostojnosti (kvalitetne lozinke i sl.),
- ograničava vrijeme povezivanja korisnika (ako je potrebno).

Za kontrolu pristupa operacijskom sustavu potrebno je uspostaviti:

i. Automatsku identifikaciju terminala

Ova tehnika se koristi i nužna je ukoliko se komunikacija inicira s određene lokacije ili s određenog terminala; kako bi se osigurala sigurnost identifikatora terminala potrebno je terminal fizički zaštititi

ii. Procedure prijave terminala

Pristup do informacijskih resursa treba biti omogućen samo nakon uspješne prijave u sustav; procedura mora biti takva da:

- daje minimalan broj informacije neautoriziranom korisniku ,
- ne smije prikazivati sistemske ili aplikacijske identifikatore sve dok se prijava uspješno ne izvede,
- mora prikazivati obavijesti i upozorenja da računalu smiju pristupiti samo ovlašteni korisnici,
- ne smije prikazivati pomoćne poruke,
- ne smije naznačiti koji dio podataka je netočan,
- mora ograničiti broj neuspješnih prijava,
- treba bilježiti neuspješne prijave,
- treba definirati maksimalno i minimalno vrijeme izvođenja prijave,

- nakon uspješne prijave treba prikazati podatke (datum i vrijeme) zadnje uspješne prijave i detalje o neuspješnim pokušajima prijave od zadnje uspješne.

iii. Identifikacija i provjera vjerodostojnosti korisnika

Svi korisnici moraju imati jedinstven identifikator za svoju osobnu uporabu kako bi se naknadno aktivnosti mogle povezati s pojedinim korisnikom. Iz korisničkog imena ne smije biti moguće otkriti informacije o razini korisnikovih privilegija.

iv. Sustav upravljanja lozinkama

Uporabi lozinki najčešći je oblik načina dokazivanja identiteta, stoga je potrebno osigurati učinkovit, interaktivan način osiguravanja kvalitete lozinki.

Sustav upravljanja lozinki treba:

- nametati korištenje individualnih lozinki radi utvrđivanja odgovornosti (ukoliko je lozinka dodijeljena korisniku, prilikom prve prijave na sustav potrebno je lozinku promijeniti),
- nametati izbor kvalitetnih lozinki,
- nametati promjene lozinki,
- spriječiti korištenje već korištenih lozinki (sustav pamti lozinke),
- ne prikazivati lozinku na ekranu prilikom unosa lozinke,
- pohraniti lozinke u kriptiranom obliku, koristeći algoritme za jednosmjernu enkripciju, odvojene o aplikacijskih podataka.

v. Vrijeme neaktivnosti terminala

Terminale prijavljene na sustav koji nisu korišteni određeno vrijeme, npr. 5min, potrebno je automatski odjaviti. Vrijeme neaktivnosti definira se prema rizičnosti lokacije (mogućnosti pristupa terminalu). Osim odjave potrebno je obrisati ekran terminala, zatvoriti sve aplikacijske i mrežne veze.

Praćenje pristupa i korištenje sustava

Aktivnosti u sustavu treba pratiti i dokumentirati radi pravovremenog uočavanja odstupanja od politike kontrole pristupa i radi pružanja dokaza u slučaju sigurnosnog incidenta.

Bilježenje događaja.

Potrebno je bilježiti aktivnosti nad sustavom te sakupljene informacije čuvati određeni vremenski period kako bi se osigurala podrška u slučaju incidenta i omogućilo praćenje sustava.

Informacije koje je potrebno sakupiti bilježenjem događaja:

- korisnička imena,
- datume vremena prijave u i odjave iz sustava,
- ako je moguće identitet računala (terminala) s kojeg je napravljena prijava,
- zapise o uspješnim i neuspješnim pokušajima pristupa sustavu,
- zapise o uspješnim i neuspješnim pokušajima pristupa podacima i resursima.

Praćenje uporabe sustava.

Kako bi se osiguralo da korisnici izvršavaju samo one aktivnosti za koje su ovlaštenim, nužna je uspostava postupaka za praćenje uporabe jedinica za obradu podataka. Razinu praćenja pojedinih jedinica treba utvrditi kroz procjenu rizika.

Područja o kojima je potrebno voditi računa su:

- ovlašteni pristup (korisnička imena, datum i vrijeme događaja, tipovi događaja, datoteke kojima je pristupano, korišteni programi),
- privilegirane aktivnosti,
- neovlašteni pokušaji pristupa,
- sistemska upozorenja i greške.

Rezultate dobivene praćenjem potrebno je redovito pregledavati i analizirati. Učestalost pregleda ovisi o postojećim rizicima.

Faktore rizika koje treba razmotriti su:
- kritičnost aplikacija,
- vrijednost, osjetljivost i kritičnost informacija,
- iskustva o zlouporabama, neovlaštenim upadima i sl.

Posebnu pažnju treba obratiti na sigurnost dnevnika zapisa o događajima. Prilikom dodjele odgovornosti za pregled dnevnika potrebno je razdvojiti uloge osoba koje obavljaju pregled i onih čije se aktivnosti prate. Također je potrebno omogućiti filtriranje bilježaka, iz razloga što je dnevnici sadrže veliku količinu informacija od koje je većina nebitna za praćenje sigurnosti.

Dnevnike zapisa potrebno je zaštititi od aktivnosti kao što su:
- isključivanje sustava za bilježenje,
- izmjene tipa zabilježenih informacija,
- izmjena ili brisanje podataka,
- spriječiti mogućnost prekida nadziranja zbog nedostatka diskovnog prostora i sl.

Sve nabrojane kontrole ne bi imale očekivani učinak ukoliko nije obavljeno sinkroniziranje računalnih satova. Dnevnici događaja često služe kao dokaz u sudskim ili disciplinskim postupcima, stoga neprecizni podaci mogu ugroziti kredibilitet dokaza. Satove na računalnima ili komunikacijskim uređajima potrebno je podesiti na definirani standard, npr. lokalno standardno vrijeme, te moraju postojati mehanizmi koji će provjeravati i ispravljati varijacije.

Primjena norme u sigurnosnoj politici

Zbog velikog broja korisnika informacijskog sustava ZEMRIS kontrola pristupa izuzetno je važan sigurnosni mehanizam kojem je cilj spriječiti, detektirati i dokumentirati svaki pokušaj neovlaštenog pristupa, bilo da se radi o hardveru ili softveru.

Kako bi kontrola pristupa kao sigurnosni mehanizam bila što kvalitetnije provedena, potrebno je osmisliti prikladne metode identifikacije, autorizacije ali i metode zaštite sustava od nepažljivih korisnika.

Kontrolu pristupa ugrubo možemo podijeliti na:
- kontrola pristupa softveru i
- kontrola pristupa opremi.

Kontrola pristupa softveru temelji se na unaprijed određenim pravilima. Stav struke je da se prava pristupa ne dodjeljuju direktno korisnicima, već da se ona definiraju kroz korisničke grupe.

Na ZEMRIS-u postoje 4 inicijalnih grupa korisnika:
- administrator (voditelj sigurnosti),
- profesori,
- studenti,
- treće strane.

Zbog svakodnevnih potreba za novim grupama nemoguće je unaprijed odrediti ostale grupe. Jedino je važno da se svaka stvorena grupa dokumentira na jedinstvenom mjestu koje odredi odgovorna osoba.

Dokumentacija treba sadržavati:

- naziv grupe,
- prava pristupa,
- identifikacija osobe koja je otvorila grupu,
- datum i vrijeme nastanka grupe,
- rok trajanja.

Prava pristupa pojedinim resursima treba biti sadržana (dokumentirana), a dokumentacija treba sadržavati sljedeće detalje:

- ID – identifikacija prava pristupa,
- pravo pristupa - čitanje, pisanje, izvršavanje,
- identifikacija osobe koja je stvorila zapis,
- vrijeme i datum nastanka zapisa.

Kontrola pristupa ima zadatak zaštiti sustav u maksimalnoj mjeri od nepažljivih korisnika i zlonamjernih osoba. Nepažljivi korisnici smatraju se oni koji na bilo koji način, ne pridržavajući se politike sigurnosti, nesvjesno pomažu hakerima u zlonamjernim radnjama. Neki primjeri su ostavljanje računala prijavljenog na sustav bez nadzora, otkrivanje korisničkih imena i sl. Hakeri ukoliko dođu u posjed prijavljenog računala mogu napraviti veliku štetu ili iskoristiti takvo računalo za prikupljanje informacija potrebnih za obavljanje zlonamjernih radnji. Također odavanje bilo kojih informacija, čak i korisničkog imena, hakerima uvelike olakšava postupak napada na sustav.

Kako bi se zaštitili od nepažljivih korisnika potrebno je implementirati sigurnosne kontrole kao što su:

- automatska odjava sa sustava ukoliko je računalo neaktivno 15min,
- automatska odjava sa sustava ukoliko je terminal neaktivan 3min,
- blokiranje korisničkog računa ukoliko se 3 puta uzastopno unese krivo korisničko ime i lozinka,
- „prisiljavanje“ korisnika na redovito mijenjanje lozinke, svaka 3 mjeseca,
- dopuštanje biranje samo lozinki koje zadovoljavaju pravila sigurnosne politike itd.

Kontrola pristupa hardveru ima identičnu svrhu kao i kontrola pristupa softveru. Važno je osigurati pristup opremi samo onim osobama koje za to imaju potrebu. Pristup opremi pruža se kroz davanje ovlasti pristupa prostorijama u kojima se oprema nalazi.

Pravila pristupa trebaju zadovoljavati sljedeće točke:

- oprema treba biti smještena u odgovarajućim prostorijama, što je oprema osjetljivija, vrjednija, sadrži važnije podatke, to prostorija treba biti pod većim stupnjem zaštite,
- prostorije u kojima se nalazi osjetljiva oprema trebaju biti označene određenom oznakom koja ukazuje na „osjetljivost“ prostorije,
- pristup takvim prostorijama treba biti omogućen putem identifikacijskih kartica kako bi se moglo provoditi nadziranje pristupa; ukoliko iz tehničkih razloga nije moguće koristiti identifikacijske kartice potrebno je koristiti drugi sigurnosni mehanizam (ključ i slično),
- prava pristupa pojedinim prostorijama treba biti dokumentiran.

Nadziranje. Sigurnosne kontrole ne mogu pružiti 100% zaštitu. Hakeri će uvijek tražiti propuste i eventualne „rupe u obrani“ kako bi postigli svoj cilj. Nadziranje je

sigurnosna kontrola čija je svrha bilježiti sve postupke unutar informacijskog sustava. Ova kontrola vrlo je važna kako bi se na vrijeme uočile nepravilnosti unutar sustava (obavljanje nedopuštenih radnji, napadi, pripreme napada i sl.).

Nadziranje informacijskog sustava ZEMRIS treba sakupiti sljedeće informacije:

- korisnička imena,
- datume vremena prijave u i odjave iz sustava,
- ako je moguće identitet računala s kojeg je napravljena prijava,
- zapise o uspješnim i neuspješnim pokušajima pristupa sustavu,
- zapise o uspješnim i neuspješnim pokušajima pristupa podacima i resursima.

Mobilno računarstvo. U današnje vrijeme rad na prijenosnim računalima sve je učestaliji, kako zbog praktičnosti tako i zbog poslovnih potreba. Čest je slučaj da korisnici na sastanke ili na edukaciju donose svoja prijenosna računala pomoću kojih se spajaju na internu mrežu i njima se koriste. Ovakav način poslovanja zasigurno ima svojih prednosti, no zahtjeva dodatne sigurnosne kontrole na području sigurnosti.

Dodatne sigurnosne kontrole trebale bi spriječiti (otežati) sve napade koji mogu biti počinjeni zbog otvaranja prava pristupa s mobilnih računala.

Navedene kontrole prvenstveno trebaju obuhvatiti:

- načini zaštite od malicioznih programa,
- načini i prava pristupa,
- postavke sigurnosne stijene.

Zaštita od malicioznih programa treba osigurati da mobilno računalo ne može ugroziti informacijski sustav zato što se na njemu nalazi maliciozni program.

Osim zaštite od malicioznih programa potrebno je definirati načine pristupa treće strane resursima zavoda. Načini pristupa mogu biti:

- pristup web aplikacijama,
- pristup internet poslužiteljima,
- pristup isključivo određenim direktorijima i sl.

Definiranjem načina pristupa moguće je osigurati potrebnu funkcionalnost bez instaliranja, dogradnje i kontrole mobilnog računala korisnika. Sva kontrola prometa odvija se putem sigurnosne stijene i na strani poslužitelja.

U slučaju kada nije moguće jednostavno odrediti potrebe korisnika (npr. samo pristup web aplikacijama), nužno je provesti kontrole kojima će se osigurati sigurnost sustava. Navedene kontrole prvenstveno uključuju provjeru prilikom spajanja na sustav da li je na računalu instaliran potreban antivirusni softver, te preventivna kontrola koja uključuje kvalitetno dodijeljena prava pristupa.

Glavna odgovorna osoba dužna je osigurati potreban antivirusni softver koji je nužno imati instalirano za spajanje na informacijski sustav, te ažuriranu bazu s podacima o virusima ukoliko se ažuriranje baze ne radi automatski prilikom prijave na sustav.

Osim „tehničkih“ kontrola sigurnosti, korisnike je potrebno upoznati s njihovim dužnostima i odgovornostima, te navedeno dokumentirati potpisivanjem *Ugovora o pridržavanju sigurnosnih pravila*.

5.8 Razvoj i održavanje sustava

Cilj „razvoja i održavanja sustava“ je definirati sve sigurnosne zahtjeve, uključujući procedure u slučaju incidenata. Definirani zahtjevi moraju biti analizirani i dokumentirani.

Sigurnosni zahtjevi uključuju:

- sigurnost kod aplikacija,
- kriptografske metode,
- sigurnost datoteka,
- sigurnost u procesu razvoja i pružanja podrške.

U dizajn aplikacija nužno je implementirati kontrolne mehanizme koji uključuju nadzorne logove, validaciju ulaznih podataka, obrade i izlaznih podataka.

Validacijom ulaznih podataka treba spriječiti slučajno ili namjerno unošenje netočnih podataka. Potrebno je uzeti u obzir sljedeće kontrolne mehanizme:

- nedozvoljene vrijednosti,
- nedopuštene znakove u poljima,
- nepotpuni podaci,
- prekoračenje količine podataka za unos itd.

Kriptografske metode potrebno je definirati kako bi se omogućila zaštita povjerljivosti, autentičnosti i/ili integriteta informacije. Ove metode potrebno je koristiti kod rizičnih, osjetljivih i povjerljivih podataka. Politikom je potrebno odrediti koje tehnike kriptografije (koje kriptografske metode će se koristiti, način čuvanja i raspodijele ključeva, na koji način će se ostvariti digitalni potpis i sl.) će se upotrebljavati u skladu s važećim zakonodavnim restrikcijama i pravima uporabe.

Kontrola operativnog softvera sigurnosni je mehanizam kojem je cilj smanjiti rizik operativnog sustava. Mehanizme koje je potrebno razmotriti:

- nadogradnju operativnih programskih biblioteka smije se izvoditi samo ukoliko to odobri glavna odgovorna osoba,
- u operativnim sustavima smije biti samo izvršni kôd,
- izvršni kôd se smije uvoditi u operativne sustave samo ukoliko zadovolje sigurnosne zahtjeve kod testiranja.

Zaštita testnih podataka. Testni podaci moraju biti zaštićeni i kontrolirani. Testiranje sustava često se odvija na testnim podacima, koji su kopija stvarnih podataka, stoga je potrebno koristiti sljedeće sigurnosne mehanizme:

- procedure za kontrolu pristupa koje su implementirane na operativne aplikacijske sustave, moraju biti primijenjene i na testne aplikacijske sustave,
- za kopiranje operativnih informacija na testni sustav mora postojati posebno pravo pristupa,
- operativne informacije moraju biti obrisane s testnog sustava odmah nakon testiranja,
- rad na testnom sustavu mora biti nadziran kao i operativni, u posebne dnevnike.

Kontrole pristupa bibliotekama izvornog koda moraju biti jasno definiran i dokumentirane. Potrebno je razmotriti sljedeće mehanizme:

- biblioteke izvornog kôda ne smiju biti pohranjene na operativnim sustavima,
- osoblje ne smije imati neograničen pristup bibliotekama, potrebno je odobriti pristup samo ukoliko je pristup neophodan,
- potrebno je jasno označiti operativne biblioteke i one testne, kako ne bi došlo do zamijene.

Primjena norme u sigurnosnoj politici

Ovaj dio standarda puno je važniji za institucije kao što su banke nego za informacijski sustav ZEMRIS. Razlog tome leži u činjenici da ZEMRIS nema tim programera zaduženih za razvoj aplikacija koje se koriste unutar zavoda. Postoje projekti pojedinih profesora, mentora, studenata, ali te programe nikako ne možemo kontrolirati politikom sigurnosti. U institucijama kao što su banke stvar je u potpunosti drukčija. Takve institucije imaju desetine i stotine programera kojima je cilj razvoj aplikacija koje se koriste unutar institucija. Tu postoji mogućnost da jedan od njih svoj položaj unutar organizacije iskoristi za obavljanje zlonamjernih radnji.

Od sigurnosnih kontrola definiranih ovim dijelom standarda važno je ostvariti sljedeće:

- definiranje kriptografskih metoda,
- validaciju ulaznih podataka,
- kontrole pristupa resursima sustava, između ostalog i bibliotekama izvornog kôda.

5.9 Upravljanje incidentima informacijskog sustava

Cilj upravljanja incidentima informacijskog sustava je implementiranje kontrola kako bi se na uočene incidente pravovremeno i kvalitetno reagiralo.

Svi korisnici (zaposlenici, studenti, treće strane..) trebaju biti upoznati s procedurama o obavještavanju različitih tipova potencijalnih sigurnosnih incidenata. Također moraju biti svjesni svoje odgovornosti i dužnosti da prijave svake događaje ili slabosti sustava koji mogu ugroziti sigurnost sustava na bilo koji način.

Prijava sigurnosnih incidenata

Cilj – sigurnosni incidenti moraju biti prijavljen na unaprijed definiran način u što kraćem roku.

Glavna odgovorna osoba dužna je definirati i dokumentirati procedure za prijavu incidenata, definirajući kome se treba obratiti, na koji način i u kojem roku.

Svi korisnici moraju biti upoznati s procedurama o prijavi sigurnosnih incidenata i svojom dužnošću postupanja prema definiranim pravilima.

Primjeri sigurnosnih incidenata:

- gubitak usluge ili opreme,
- oštećenje usluge ili opreme,
- preopterećenje sustava,
- greške ljudi,
- nepridržavanje politike sigurnosti,
- nedopuštene promjene sustava,
- kršenje prava pristupa itd.

Kako bi prijava incidenata bilo što bolje prihvaćena od strane korisnika preporučuje se održavanje „treninga“ tako da se korisnicima primjerima pokaže na koje sve sigurnosne incidente reagirati i na koji način.

Vrlo bitna stvar kod prijave incidenata je slanje povratne obavijesti inicijatoru. U poruci bi trebalo inicijatoru dati do znanja da je napravio „dobro djelo“ i da u budućnosti to svakako opet učini, makar se radilo o „lažnoj uzbuni“.

Prijava slabosti sustava

Budući je uspostava sigurnosti informacijskog sustava vrlo opširan i nedefiniran zadatak, nemoguće je uspostaviti potpunu sigurnost. Čest je slučaj da se prilikom osmišljavanja sigurnosti sustava i implementacije sigurnosnih kontrola dogodi propust te na taj način otvori put počinjenu zlonamjernih radnji.

Kao i kod prijave sigurnosnih incidenata, korisnike treba obvezati i ukazati im da su dužni prijaviti svaku uočenu sigurnosnu slabost sustava. Kako bi prijava slabosti sustava bila izvediva, glavna odgovorna osoba dužna je definirati i dokumentirati na koji način prijaviti primijećene sigurnosne slabosti.

Upravljanje sigurnosnim prijavama

Cilj upravljanja sigurnosnim incidentima je unaprijed definirati i dokumentirati odgovornosti odgovornih osoba, te akcije koje su dužni poduzeti kako bi se osigurali pravovremeni i kvalitetni odgovori na prijavljene incidente.

Odgovornosti i procedure

Sljedeće smjernice trebaju biti proučene kod definiranja procedura za upravljanje incidentima informacijskog sustava:

- procedure trebaju obuhvatiti različite vrste sigurnosnih incidenata, uključujući:
  - prestanak rada sustava,
  - odbijanje usluge,
  - maliciozni kod,
  - kršenje tajnosti ili integriteta,
  - zlouporaba sustava itd.
- u slučaju nepredviđenih događaja, treba definirati sljedeće postupke:
  - plan i implementaciju akcija kako se incident ne bi ponovio,
  - analizu i identifikaciju uzroka incidenta,
  - komunikaciju s „napadnutom“ stranom,
  - izvještavanje nadležnih o incidentu.
- dokumentaciju o incidentu i ostale dokaze treba spremiti i zaštiti s ciljem:
  - interne analize problema,
  - pružanja dokaza u sudskim sporovima.

Primjena norme u sigurnosnoj politici

Informacijski sustav ZEMRIS zbog svoje „otvorenosti“ prema korisnicima (prvenstveno se odnosi na studente) i zbog velikog broja korisnika potencijalno je poželjno odredište za obavljanje zlonamjernih radnji. Stoga je važno da upravljanje sigurnosnim incidentima bude kvalitetno osmišljeno i implementirano.

Kako bi se postigla željena razina kvalitete upravljanja sigurnosnim incidentima, potrebno je implementirati sljedeće sigurnosne mehanizme:

- kontrola dnevnika sa zapisima o nadgledanju,
- definiranje procedura za odgovorne osobe:
  - kako postupiti u slučaju incidenta,
  - kako postupiti u slučaju otkrivanja ranjivosti sustava.
- definiranje smjernica za korisnike:
  - kako postupiti ukoliko uoče događaje koji mogu ugroziti sigurnost sustava (incidente),
  - kako postupiti ukoliko primijete slabosti (ranjivosti sustava).

Kontrola dnevnika sa zapisima o nadgledanju. Izrada bilježaka (tzv. dnevnika događaja) o događajima unutar sustava iznimno je važna ne samo kako bi postojali dokazni materijali u slučaju incidenta, već i kako bi se pravovremeno uočile i spriječile potencijalno opasne radnje kao što su pripreme za napad i sl.

Zbog velike količine podataka koje možemo skupiti nadgledanjem nužno je osmisliti mehanizme kojima ćemo iz sakupljenih podataka izvući (istaknuti) one „važne“ s ciljem otkrivanja potencijalno opasnih radnji. Potencijalno opasne radnje su sve one radnje koje napadači koriste kako bi dobili informacije o sustavu koje mogu pomoći u izvršenju napada, kao što su npr. informacije o postavkama sigurnosne stijene, podaci o korisničkim računima (napadi uzastopnim pokušavanjem (eng. *brute force napad)*) itd.

Mehanizmi koji mogu pomoći u otkrivanju potencijalno opasnih radnji su:

- Softverska rješenja:
  - pozitivno - brza, efikasna u okviru „definicija“,
  - negativno – relativno neinteligentna – ne mogu otkriti potencijalno opasne radnje izvan „definicija“.
- Nadgledanje zapisa od strane ljudi:

- pozitivno – inteligentni, mogu primijetiti potencijalno opasne radnje i izvan „definicija“,
- negativno - spori, mogući propusti u nadgledanju.

Odgovorne osobe – kako postupiti u slučaju incidenta.

Odgovorne osobe osim kontrole dnevnika zapisa moraju pregledavati i prijave korisnika o incidentima i ranjivostima sustava. Kako bi prijava od strane korisnika, odnosno pregled prijava od strane odgovornih osoba bilo što jednostavnije, nužno je uspostaviti prikladne mehanizme.

Mehanizam koji osigurava jednostavno i kvalitetno rješenje je prijava incidenta ili ranjivosti putem web aplikacije. Odgovorne osobe preko web aplikacije mogu pregledavati prijave i ažurirati ih, te na taj način voditi evidenciju zaprimljenih i riješenih prijava.

Za sve prijave pristigle putem web forme treba voditi dnevnik sa podacima:

- kada je napravljena prijava od strane korisnika,
- kada je pregledana prijava od strane odgovorne osobe,
- zapis prijave,
- koje su akcije poduzete u vezi prijave,
- da li je opasnost otklonjena ili ne.

U slučaju incidenta odgovorne osobe moraju reagirati u skladu sa sljedećim točkama:

- spriječiti daljnje počinjenje zlonamjernih radnji,
- pokušati prikupiti dodatne informacije o napadaču, o lokaciji s koje je kazneno djelo izvršeno i sl.,
- pozvati policiju.

Odgovorne osobe - kako postupiti u slučaju otkrivanja ranjivosti sustava.

U slučaju otkrivanja ranjivosti odgovorna osoba treba:

- u što kraćem roku zaustaviti rad komponente koja je uzrok ranjivosti sustava,
- potaknuti pregled i testiranje sigurnosti prijavljene komponente,
- otkriti uzrok ranjivosti,
- ukoliko je za ranjivost odgovorna ljudska radnja (potencijalni napadač) potrebno je napraviti dodatne provjere i po potrebi pozvati policiju,
- uočene ranjivosti otkloniti,
- ponovno napraviti testiranja,
- pustiti komponentu u rad ukoliko zadovoljava sigurnosne norme.

Korisnici – postupanje u slučaju uočavanja incidenta i otkrivanja ranjivosti sustava.

Korisnike treba educirati o potencijalnim opasnostima koje mogu ugroziti sigurnost informacijskog sustava, te im dati do znanja da su svaki uočeni incident dužni i odgovorni prijaviti. Isto moraju postupiti ukoliko primijete bilo koju vrstu sigurnosnog propusta koju zlonamjerni korisnik može iskoristiti za izvršavanje zlonamjernih radnji. Sve uočene nepravilnosti korisnik može prijaviti putem web aplikacije.

5.10 Upravljanje poslovnim kontinuitetom

Proces upravljanja kontinuitetom poslovanja

Ključni elementi upravljanja kontinuitetom poslovanja:

- razumijevanje rizika s kojima je suočena organizacija (svjesnost vjerojatnosti),
- razumijevanje posljedica ukoliko se dogodi incidenta situacija,
- ugovaranje neke od vrsti osiguranja koje bi pokrilo gubitke nastalo incidentnom situacijom,
- definiranje strategije poslovnih procesa,
- izrada planova za kontinuirano poslovanje prema dogovorenoj strategiji,
- redovito testiranje i nadogradnja planova i procesa,
- upravljanje kontinuitetom potrebno je ugraditi u organizacijske strukture i procese.

Kontinuitet poslovanja i analiza učinka

Prvi korak u planiranju kontinuiteta poslovanja jest identificirati događaje koji mogu prekinuti poslovni proces. Takve događaje nazivamo incidentne situacije.

Nakon identificiranja incidentnih situacija potrebno je za svaku od njih provesti analizu kojom se utvrđuje koje posljedice incidenta situacija ima po organizaciju, znači definiranje potencijalne štete i potrebno vrijeme oporavka.

Postupak analize treba obuhvatiti sve poslovne procese, ne samo jedinice za obradu podataka.

Treći korak je definiranje plana za kontinuirano poslovanje. Ono uključuje:
jasnu identifikaciju odgovornosti,

- definiranje procedura za postupanje u hitnim slučajevima kako bi se omogućio oporavak i povrat u minimalnom vremenskom periodu,
- definirane odgovornosti i procedure za oporavak potrebno je dokumentirati,
- eventualne promjene odgovornosti ili promjene u procedurama za oporavak također treba dokumentirati; postojeće procedure odnosno odgovornosti treba označiti kao nevažeće,
- testiranje i nadogradnja planova.

Testiranje i održavanja

Zbog pogrešnih pretpostavki, dijelova koji su se previdjeli ili zbog promjena u osoblju i opremi moguće je da definirane procedure za kontinuirano poslovanje ne podžavaju željenu strategiju i planove. Stoga je redovito potrebno raditi testiranja kako bi se pravovremeno otkrili potencijalni propusti.

Testiranje obuhvaća:

- raspored testiranja – kako i kada testirati svaki pojedini element plana,
- hipotetsko testiranje različitih scenarija – raspravljanje o definiranim procedurama kroz primjere prekida,
- simulacija – s ciljem osposobljavanja osoblja,
- testiranje oporavka s tehničke strane – osiguravanje da informacijski sustavi mogu biti vraćeni u funkciju,
- testiranje usluga treće strane – osiguranje da će ugovoreni servisi s trećom stranom zadovoljiti dogovoreno,
- potpuni pokusi – testiranje da organizacija, osoblje, oprema i procesi mogu podnijeti prekide.

Održavanje:

- održavati planove kroz redovite preglede i nadogradnje,
- dodijeliti odgovornosti za redovito pregledavanje svakog plana za kontinuirano poslovanje – identifikacija promjena,
- situacije koje mogu dovesti do nadopuna planova uključujući nabavu nove opreme, nadogradnju operativnih sustava ili promjene u poslovnom sustavu (osoblje, poslovna strategija, lokacija, resursi, zakonodavstvo, partneri, procesi, rizik...).

Primjena norme u sigurnosnoj politici

Stabilnost i kontinuitet rada željena je karakteristika svakog informacijskog sustava, pa tako i informacijskog sustava ZEMRIS. No cijena kontinuiteta poslovanja ponekad može biti puno veća od one koju je moguće platiti, stoga je potrebno uskladiti želje i mogućnosti.

Kontinuitet poslovanja za neke informacijske sustave (npr. informacijski sustavi banaka) neophodan je element pružanja kvalitetne usluge te se pri implementaciji kontrola za takvo poslovanje ne pita za cijenu. S druge strane postoje sustavi kojima relativno kratak prekid poslovanja ne znači mnogo. Za takve sustave ulaganje u implementaciju kontrola za kontinuirano poslovanje nepotrebna je investicija.

Informacijski sustav ZEMRIS po potrebi za kontinuiranim poslovanjem nalazi se između prethodno opisanih sustava. Prekid u kontinuitetu neće prouzročiti takvu štetu kakvu bi izazvalo u prekidu poslovanja sustava banaka, a s druge strane o sustavu ZEMRIS ovise brojni studenti, zaposlenici i ostali korisnici. Zbog njih je, u slučaju prekida kontinuiteta, sustav potrebno u što kraćem vremenu osposobiti i vratiti u „normalno“ stanje.

Kako bi se zadovoljile osnovne potrebne za kontinuitetom poslovanja, potrebno je učiniti sljedeće:

- identificirati rizik,
- analizirati rizika,
- definirati procedure u slučaju incidentne situacije.

Identifikacija rizika

Kao što definira standard, prvi korak planiranja kontinuiteta poslovanja je identificirati potencijalne prijetnje koje mogu ugroziti kontinuitet. Kontinuitet poslovanja mogu ugroziti:

- korisnici svojim slučajnim ili namjernim postupcima,
- kvar opreme,
- i prirodne katastrofe.

Analiza rizika

Kvar opreme može nastati zbog:

- nepravilnog rukovanja opremom,
- držanje opreme u neadekvatnim uvjetima (uvjetima koji nisu prema preporukama proizvođača); prvenstveno se odnosi na temperaturu i vlagu,
- neodržavanja opreme,
- starosti opreme,
- prenaponskog oštećenja i sl.

Kvar opreme kao uzrok prekida poslovanja poznat je od samog začetka informatizacije, te su se godinama razvijala i smišljala rješenja kako bi se rizik

prestanka poslovanja zbog kvara opreme minimalizirao. Za svaki od uzroka kvara opreme (od rukovanja, održavanja pa sve do oštećenja nastalih „višom silom“) postoje procedure i kontrole koje umanjuju mogućnosti njihova štetnog djelovanja po opremu. Tako npr. kako bi se spriječila oštećenja nastala nepravilnim rukovanjem oprema se smješta u „sigurne prostorije“ kojima pristup imaju isključivo korisnici koji imaju potrebu za pristupom i znaju opremom rukovati. „Sigurne prostorije“, osim što su fizički odvojene od korisnika, imaju mogućnost automatske kontrole i reguliranja temperature i vlage u prostoriji. Na taj način sprječava se kvar opreme nastao držanjem opreme u neprikladnim uvjetima.

Prirodne katastrofe

Prirodne katastrofe (potresi, požari, poplave) potencijalna je prijetnja koju je nemoguće predvidjeti i na koju je nemoguće utjecati. Ono na što se može utjecati je implementacija kontrola za minimiziranje štete nastale ukoliko se neki od oblika katastrofe dogodi.

U svrhu minimiziranja štete nastale prirodnom katastrofom potrebno je:

- ulaze u područje zavoda zaštititi vratima otporna na požar i poplavu,
- osjetljivu opremu smjestiti unutar „sigurnih prostorija“; zaštićene vodonepropusnim i vatrostalnim vratima,
- u prostorije s opremom implementirati kontrole za alarmiranje u slučaju požara ili poplave,
- u prostorije s opremom implementirati uređaje za automatskog gašenja u slučaju požara,
- osjetljivu opremu smjestiti u posebne ormariće, konstruirane tako da izdrže što veći pritisak (u slučaju potresa),
- ukoliko implementirane kontrole zaštite nisu zadovoljavajuće, razmotriti osiguranje opreme kao dodatni mehanizam zaštite.

Korisnici

Korisnici svojim radnjama mogu ugroziti kontinuitet poslovanja te prouzročiti prestanak rada sustava. Kako bi se smanjila mogućnost obavljanja ovakvih radnji, potrebno je osigurati sljedeće:

- korisnici ne smiju imati pristup opremi ukoliko nemaju realnu potrebu za tim,
- pravo pristupa opremi svakog korisnika mora biti jasno dokumentirano,
- korisnici koji imaju pravo pristupa opremi moraju poštivati pravila ponašanja i rukovanja osjetljivom opremom.

Pravila ponašanja i rukovanja osjetljivom opremom:

- u prostorije koje sadrže osjetljivu opremu smiju ulaziti isključivo osobe koje imaju pravo pristupa,
- osobe koje nemaju pravo pristupa ne smiju ulaziti u prostorije s osjetljivom opremom niti uz pratnju osobe koja ima to pravo,
- u prostorije s osjetljivom opremom nije dopušteno unositi hranu i piće,
- unutar prostorija s osjetljivom opremom nije dopušteno pušiti,
- osjetljivom opremom mora se postupati prema pravilima proizvođača.

5.11 Usklađivanje

Identifikacija primjenjivih zakona.

Za svaki informacijski sustav treba eksplicitno definirati i dokumentirati sve relevantne zakonske, običajne i ugovorne zahtjeve.

Intelektualno vlasništvo – autorska prava.

Potrebno je implementirati odgovarajuće procedure za osiguravanje sukladnosti s pravnim ograničenjima za korištenje materijala nad kojima postoji intelektualno vlasništvo, poput prava na kopiranje, prava na dizajn i sl.

Softverski proizvodi isporučuju se s licenčnim ugovorom koji ograničava korištenje proizvoda, te koji može ograničiti kopiranja samo na izradu sigurnosne kopije.

Čuvanje organizacijskih zapisa.

Zapisi trebaju biti zaštićeni od gubitka, uništenja i krivotvorenja. Moraju biti sigurno pohranjeni.

Sprečavanje zlouporabe uređaja za obradu informacija.

Korištenje resursa u neposlovne ili neovlaštene svrhe treba biti dokumentirano kao neprikladno.

Nadgledanje korisnika.

Ukoliko je zakonom propisano, potrebno je pravovremeno obavijestiti korisnike o njihovom eventualnom nadgledanju s ciljem zaštite od zlouporabe sustava.

Prikupljanje dokaza treba zadovoljavati zakonodavne zahtjeve kako bi se u slučaju incidenta prikupljeni dokazi mogli upotrijebiti u sudskom postupku.

Primjena norme u sigurnosnoj politici

Informacijski sustav ZEMRIS zbog velikog broja korisnika i svoje otvorenosti prema njima, potencijalna je meta napada zlonamjernih korisnika ili „odskočna daska“ za obavljanje zlonamjernih radnji nad drugim sustavima.

Zadnja kontrola u cilju zaštite sustava je definiranje i pozivanje na zakonodavne odgovornosti korisnika prema korištenju resursa informacijskog sustava ZEMRIS.

6. Zaključak

Sigurnost u računalnom svijetu često je površno shvaćena. Većina današnjih korisnika računala mogla bi se nazvati needuciranim korisnicima koji ne shvaćaju kompleksnost računalne sigurnosti i to je danas jedan od glavnih problema računalne sigurnosti. Zbog toga je kod uspostave sigurnosti informacijskih sustava posebnu pozornost potrebno usmjeriti na educiranje korisnika o računalnoj sigurnosti (kriminalu), te odgovornostima i dužnostima svakog pojedinca.

Drugi veliki problem sigurnosti je neorganizirano implementiranje sigurnosnih kontrola. Takvim načinom implementacije stvara se prividna sigurnost jer postoji velika vjerojatnost da je neka od kontrola izostavljena. Zbog toga je svaku sigurnosnu kontrolu ugrađenu u sustav potrebno dokumentirati, a sigurnost informacijskih sustava graditi prema unaprijed definiranim pravilima - prema dokumentu sigurnosne politike.

Svi korisnici računala također moraju biti svjesni sljedećih činjenica:
1. sigurnost informacijskih sustava vrlo je široka tema koju je nemoguće jednoznačno definirati,
2. računalna sigurnost je tema koju se ne smije ograničiti i koja zahtjeva neprekidnu pozornost,
3. za uspostavu kvalitetne sigurnosti potrebno je široko znanje različitih područja računarstva, ali i drugih znanosti,
4. računalo/informacijski sustav ne može biti u potpunosti siguran.

Zanemareni informacijski sustav, u smislu ne kontroliranja aktualnih problema sigurnosti, vrlo lako može postati žrtvom napada. Voditelj sigurnosti dužan je periodično kontrolirati sigurnost sustava (testiranje sustava na napade), tražiti načine kako da sustav postane još sigurniji te implementirati dodatne sigurnosne kontrole koje savjetuju sigurnosni stručnjaci.

7. Literatura

[1] Uvod u računalnu sigurnost», Miroslav Bača, Narodne Novine d.d., Zagreb, svibanj 2004.

[2] Crc Press - Information Security Management Handbook, Fifth Edition.

[3] Prijedlog sigurnosne politike informacijskih sustava članica CARNeta, dostupno na Internet adresi:
http://sistemac.carnet.hr/sigurnost/**sigurnosna_politika**_ustanove.pdf

[4] Sigurnosna politika, Aco Dmitrović, SRCE, dostupno na Internet adresi:
http://sistemac.carnet.hr/fileadmin/sem/Politika-ustanove_files/frame.htm

[5] Časopis Mreža, članak: Novi standard zaštite sigurnosti, siječanj – veljača 2006.

[6] Odlomci o sigurnosti informacijskih sustava, dostupni na Internet adresi:
http://www.networkworld.com/newsletters/gwm/

[7] Writing Information Security Policies and Procedures, dostupno na Internet adresi:
www.qaimea.com/pdfs/Writing%20Information%20Security%20Policies%20and%20Procedures.pdf

[8] A Short Primer For Developing Security Policies, Michele D. Guel, 2001., The SANS Institute, dostupno na Internet stranici:
www.sans.org/resources/policies/Policy_Primer.pdf

[9] Sigurnosna politika informacijskih sustava u Gradskoj i Sveučilišnoj knjižnici u Osijeku, dostupno na Internet stranici: http://www.gskos.hr/sigurnostGISKO.doc

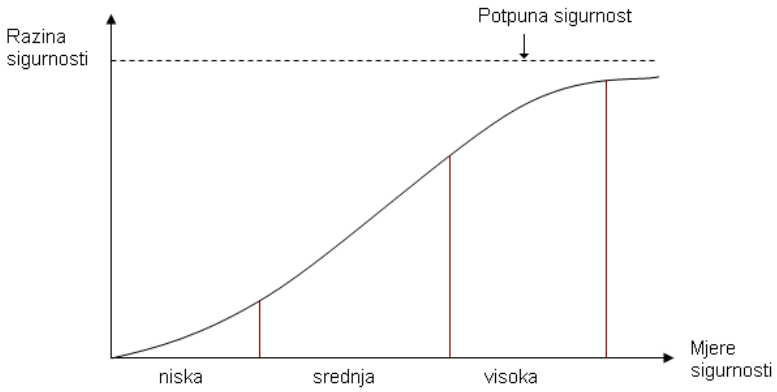
Dodatak A – Osnovni pojmovi

Informacija (eng. *information*) – podatak o nekoj činjenici, izvještaj o čemu;
Informacijski sustav (eng. information system) – organizacijski adekvatno i funkcionalno usmjeren sustav djelovanja sa zadatkom da prikuplja, memorira, obrađuje i distribuira podatke i informacije korisnicima;
Imovina (eng. *asset*) – sve što ima vrijednost za organizaciju;
Prijetnja (eng. *threat*) – ono što može izazvati štetu;
Napad (eng. *attack*) – pokušaj iskorištenja ranjivosti informacijskog sustava;
Ranjivost (eng. *vulnerability*) – slabost sustava koja se može iskoristiti za izazivanje štete;
Nezgoda (eng. *accident*) – neplanirani događaj koji direktno ugrožava ljude i imovinu;
Šteta (eng. *damage*) – mjera gubitka nastalog kao posljedica napada/nezgode;
Žestina opasnosti (eng. *hazard severity*) – procjena moguće štete koja može nastati kao posljedica opasnosti;
Rizik (eng. *risk*) – vjerojatnost da će se dogoditi nezgoda, napad;
Sigurnost (eng. *safety*) – vjerojatno da će sustav raditi ispravno u nekom vremenu;
Zaštita (eng. *security*) – sposobnost sustava da se zaštiti od napada;
Pouzdanost (eng. *reliability*) – vjerojatnost da će sustav u zadanom vremenu i zadanim uvjetima raditi ispravno;
Pogreška (eng. *error*) – ponašanje sustava koje nije u skladu sa specifikacijama i sigurnosti;
Odgovornost (eng. *responsibility*) – savjesno, valjano obavljanje dužnosti u skladu s određenim pravilima;
Spam – internacionalni pojam koji označava neželjenu elektroničku poštu;
Phising - skup aktivnosti kojima neovlašteni korisnici korištenjem lažnih poruka elektroničke pošte i lažnih web stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka kao što su korisnička imena i zaporke, PIN brojevi, brojevi kreditnih kartica i sl. ;
Socijalni inženjering (eng. *social engineering*) – metoda napada u kojem napadač nagovara ili uvjerava korisnika da postupi na određeni način;
Haker (eng. *hacker*) – hakeri su osobe koje posjeduju veliko znanje o računalnim i telekomunikacijskih tehnologijama koje ponekad mogu koristiti u ilegalne svrhe; izraz haker najčešće se spominje u negativnom kontekstu za osobe koje se bave ilegalnim radnjama;
Virus (eng. virus) - zlonamjeran kôd koji se širi dodavanjem svog koda drugim aplikacijama, a ima mogućnost samoumnažanja;
Crv - (engl. worm) zlonamjeran kod koji se, kopiranjem cjelokupnog sadržaja, širi kroz neki medij komunikacije, npr. e-mail ili servis vašeg operativnog sustava, a kojem je namjena učiniti štetu na računalu, koristiti zaraženo računalo za svoje daljnje širenje ili pak preuzeti kontrolu nad računalom;
Trojanski konj – (engl. *trojan horse*) zlonamjerni kôd koji se predstavlja kao bezazlena aplikacija i zahtijeva korisničku akciju za instaliranje;
DDoS – (eng. *Distributed Denial of Service*) oblik napada uskraćivanjem usluga u kojem su izvori zagušujućeg mrežnog prometa distribuirani na više mjesta po Internetu; najčešće se radi o računalima na koja je prethodno provaljeno kako bi ih se iskoristilo za napad na druge mreže ili računala na Internetu;
Ovjera vjerodostojnosti (eng. *authentication*) - utvrđivanje istinitosti deklariranog identiteta odnosno izvornosti; ostvaruje se tehnikama poput digitalnog potpisa
Autorizacija (eng. *authorisation*) – postupak odobravanja pristupa pojedinim informacijama;

Stražnja vrata (eng**.** *backdoor***)** – naziv za zlonamjerne programe koji omogućavaju udaljeni pristup vašem računalu; najčešće rade nezamjetno prikriveni iza ostalih programa primajući vanjske konekcije;
Sigurnosna kopija (eng. *backup*) – sigurnosna kopija datoteka ili programa koja služi za brzu sanaciju i oporavak u slučaju nenadanog gubitka podataka uzrokovanog nestankom struje, kvara računala, napada malicioznih programa itd;
Imovina – sve što je vezi s informacijama a ima vrijednost za organizaciju:

- baze podataka,
- oprema,
- softvere,
- dokumenti (papirnati),
- zaposlenici,
- imidž, reputacija itd.

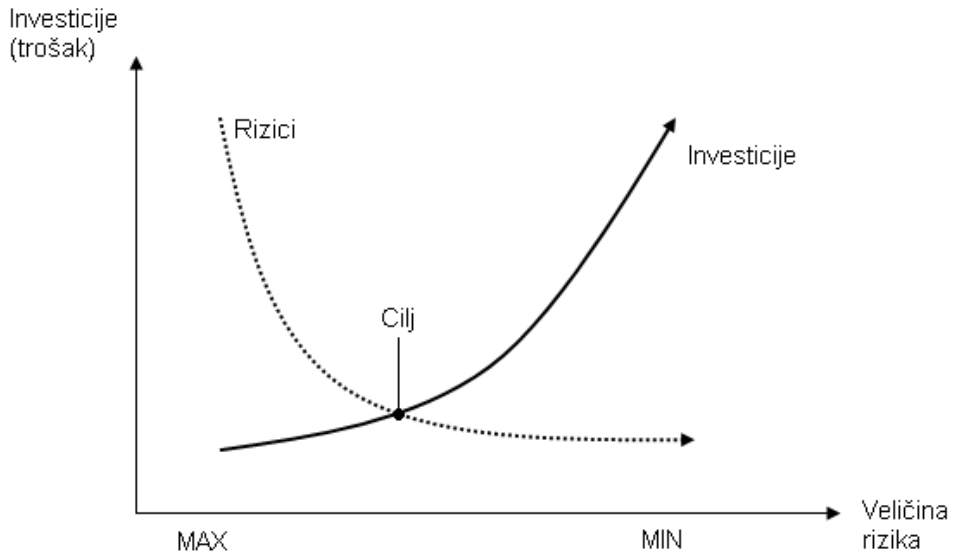
Odnos razine i mjere sigurnosti



Slika A.1 – Grafički prikaz odnosa razine i mjera sigurnosti

Na slici A.1. je grafički prikazan odnos razine sigurnosti i mjera sigurnosti (razina sigurnosti proporcionalna je s mjerama sigurnosti). Ukoliko su mjere sigurnosti male, razina sigurnosti je također mala i samim time je ranjivost velika. Povećanjem mjera sigurnosti raste i razina sigurnosti, a važno je primijetiti da koliko god ulagali sredstava i pažnje u mjere sigurnosti sustav nikada ne može biti potpuno siguran. Činjenica da se ne može postići potpuna sigurnost informacijskih sustava vrlo je važna i bitno ju je naglasiti. Ukoliko su korisnici sustava uvjereni u njegovu potpunu sigurnost uspostavom sigurnosnih mjera briga o sigurnosti prestaje. To uvelike olakšava napade na sustav, a ranjivost sustava se povećava.

Budući je nemoguće postići potpunu sigurnost, veliko je pitanje koliko uložiti u sigurnost sustava i koje sve mjere poduzeti kako bi funkcionalnost bila zadovoljena, troškovi uspostave i održavanja sigurnosti bili prihvatljivi, a sustav bio relativno siguran. Iz tih razloga nužno je odrediti prihvatljiv rizik, a jedna od metoda određivanja prihvatljivog rizika prikazana je slikom A.1. Naravno da ova metoda ne odgovara svim organizacijama, npr. bankama, vojsci ili državnim informacijskim sustavima. Njihova sigurnost zasigurno neće biti uvjetovana novčanim sredstvima, dok će veličina rizika zasigurno biti svedena na minimum.



Slika A.2 - Graf procjene prihvatljivog rizika

Slikom A.2. prikazan je graf procjene prihvatljivog rizika. Krivulja investicije u ovom slučaju predstavlja ulaganje u zaštitu, a rizici rizik informacijskog sustava. Što je ulaganje veće i troškovi organizacije su veći, ali se proporcionalno tome smanjuje rizik. Budući da se teži minimalnim rashodima (troškovi) i maksimalna sigurnost sustava potrebno je odrediti kompromis kako bi oba zahtjeva bila zadovoljena.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Sigurnosna politika

voditelj sigurnosti:

Potrebno dopuniti podacima o voditelju (ime, prezime, mail, broj telefona)

Namijenjeno: svim korisnicima
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Uvod

U današnje vrijeme informacija je jedan od najvažnijih i najskupljih resursa u poslovanju. Njeno pravovremeno posjedovanje, njena ispravnosti i tajnost često su od odlučujuće važnosti u poslovanju bilo koje institucije.

Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave (u nastavku ZEMRIS) dio je ustanove koja svoj rad temelji na informacijama. Za kvalitetan rad potrebno je zaštiti informacije od:

- neovlaštenih izmjena - osigurati **integritet,**
- objavljivanja tajnih informacija - osigurati **tajnost,**
- uskraćivanja dostupnosti informacija ovlaštenim korisnicima - osigurati **dostupnost.**

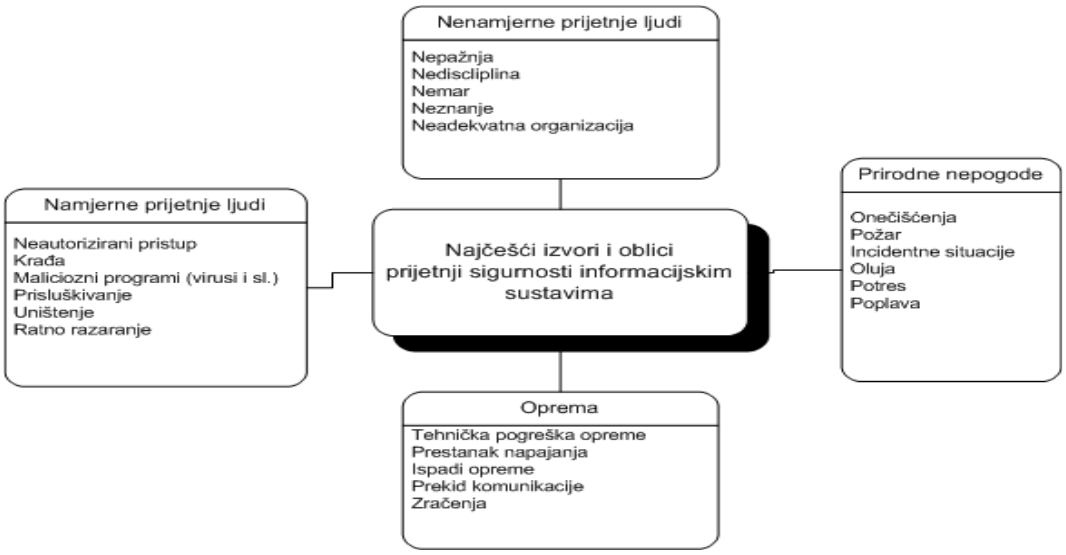
Da bi informacija bila zaštićena nužno je poduzeti velik broj radnji u smislu implementacije kontrola sigurnosti u informacijski sustav i osigurati suradnju i prihvaćanje sigurnosnih pravila od strane korisnika. Sigurnost informacijskih sustava vrlo je kompleksna i široka tema u kojoj je jasna jedino činjenica da bez kvalitetnog programa sigurnosti sustav nije moguće u cijelosti zaštiti. Kvalitetni program omogućava uspostavu sigurnosti na svim kritičnim točkama sustava, u bilo kojem segmentu sigurnosti, a jedan od najboljih programa za postizanje navedenog cilja zasigurno je definiranje sigurnosne politike.

U nastavku dokumenta ukratko je opisan sam pojam sigurnosti, što želimo postići sigurnosnom politikom, te koja je uloga pojedinca u sigurnosti informacijskog sustava ZEMRIS.

2. Sigurnost informacija

Sigurnost informacija termin je kojim opisujemo s kolikom vjerojatnošću se možemo pouzdati da će informacija biti dostupna, ispravna i tajna (ukoliko informaciju definiramo kao tajnu). Budući su informacije dio informacijskog sustava, sigurnost informacijskog sustava možemo povezati sa sigurnošću informacija.

Postoje brojni čimbenici koji mogu ugroziti sigurnost informacija. Na slici B.1. dan je shematski prikaz onih najčešćih.



Slika B.1 – Izvori i oblici prijetnji sigurnosti

Kao što je uočljivo sa slike, prijetnje informacijskim sustavima možemo podijeliti u 4 glavne kategorije. Svaka od kategorija na specifičan način ugrožava sustav te iziskuje specifične mjere zaštite. Sigurnosne kontrole koje smanjuju rizik od prijetnji ispada tehničke opreme, te od prijetnji prirodnih nepogoda vrlo su razvijene i ispravnom implementacijom vrlo je mala mogućnost izazivanja veće štete.

Ono što danas najviše zabrinjava sigurnosne stručnjake je kako zaštiti sustave od ljudi, bilo da se radi o ovlaštenim ili neovlaštenim korisnicima. U oba slučaja, najviše problema u zaštiti informacijskih sustava zadaju needucirani korisnici.

Needucirani korisnici svojim postupcima kao što su slučajno brisanje ili mijenjanje podataka, nepažljivo rukovanje resursima itd., ugrožavaju sigurnost informacija u vrlo velikom postotku od ukupnog broja incidenata. Oni također često nesvjesno pomažu zlonamjernim korisnicima izvršavanje napada pružajući im potrebne podatke. Ova vrsta napada, zvana socijalni inženjering, danas je vrlo aktualna i više o njoj kao i o ostalim načinima ugrožavanja sigurnost možete pročitati u zasebnim dokumentima.

3. Ciljevi politike sigurnosti ZEMRIS-a

Ciljeve sigurnosne politike možemo razmatrati na dva načina. Prvi način sigurnosnu politiku definira kao potrebu zaštite:

- informacijske vrijednosti,
- reputacije fakulteta,
- širenje virusa, napade na druge sustave i sl.

Informacijske vrijednosti su svako intelektualno vlasništvo ZEMRIS-a, u bilo kojem obliku i na bilo kojem mediju. U to su bez ograničenja uključene elektronske i otisnute informacije, mediji i oprema za pohranu, računalni programi i elektronske poruke. Informacije (podaci) predstavljaju najveću vrijednost fakulteta. Znanja i radovi profesora, asistenata, studenata i ostalih suradnika najvećim dijelom pohranjeni su u elektronskom obliku na računalima. Gubitak dijela ili većine podataka predstavljao bi težak udarac fakultetu, onemogućio bi rad zaposlenicima, te bi se negativno odrazio na kvalitetu edukacije studenata.

Reputacija Fakulteta elektrotehnike i računarstva u Zagrebu nedvojbeno ukazuje na visok stupanj kvalitete bilo da se govori o nastavnom kadru, studentima, edukaciji, organizaciji itd. Građena je desetljećima i ponos je svakog profesora i studenta. Sigurnosni incident nastao nemarom zasigurno bi negativno utjecao na reputaciju i stoga smo dužni zbog prethodnih, ali i budućih generacija uložiti maksimalnu pažnju u sigurnost kako bi reputacija fakulteta i dalje ostala na visokoj razini.

Zlonamjerni korisnici često koriste nezaštićena računala kao pomoć pri realizaciji napada. Nemarom oko sigurnosti našeg računala ne samo da olakšavamo zlonamjernim korisnicima napade na drugu računala, već je uvelike otežano otkrivanje napadača ukoliko je napad izveden s našeg računala ili pod našim korisničkim imenom. Iz tog razloga svaki korisnik Interneta ili interne mreže dužan je brinuti o sigurnosti svog računala bez obzira posjeduje li njegovo računalo važne podatke ili ne.

Drugi način definicije sigurnosne politike možemo opisati kao skup sigurnosnih mjera i kontrola nad:

- korisnicima sustava,
- poslužiteljima:
    - mail,
    - web,

    - aplikacijski.
- mrežnom infrastrukturom:
    - mrežni uređaji,
    - kabliranje,
    - IP adrese.
- računalima klijenta (stolna i prijenosna računala i dodatna oprema),
- softverom,
- podacima.

Oba načina definiranja sigurnosne politike su ispravna i jednim se nadopunjuje definicija drugog.

Iako će većina čitatelja ovog dokumente pomisliti da sigurnost informacijskog sustava nema nikakve veze s njima, upravo je ta „pomisao“ glavni uzrok većine sigurnosnih problema prema mišljenju stručnjaka. Naime, „obični“ korisnici svojim postupcima mogu zaštititi sustav u onim točkama gdje je nemoguće implementirati tehničke ili bilo koje druge mjere zaštite. Ova teza vrijedi ukoliko je riječ o educiranom korisniku. Ako je riječ o needuciranom korisniku za iste točke sigurnosti opet vrijedi da je nemoguće implementirati tehničke ili bilo koje druge sigurnosne mjere, no tada neznanje korisnika može ugroziti sigurnost sustava ne samo od strane zlonamjerne osobe već i od samog korisnika.

4. Uloga pojedinca u cjelokupnoj sigurnosti

Jedna od zabluda korisnika informacijskih sustava je da razina sigurnosti sustava ovisi isključivo o administratoru, odnosno osobi odgovornoj za sigurnost. No istina je daleko od toga.

Navedemo li primjere na koje načine pojedinac može ugroziti sigurnost, jasno je da je uloga pojedinca u sigurnosti velika:

- slučajno brisanje podataka,
- slučajno mijenjanje podataka,
- pokretanje malicioznog kôda,
- ostavljanje nezaštićenog računala,
- zapisivanje zaporke na papir,
- bacanje u smeće papira na kojima su zapisani važni podaci,
- odavanje podataka vezano uz socijalni inženjering,
- odavanje podataka vezano uz phising itd.

Navedeni primjeri jasan su pokazatelj da svaki korisnik sustava može ugroziti sustav, odnosno ne čineći nabrojane i slične radnje pridonosi sigurnosti informacijskog sustava.

S ciljem educiranja korisnika o potencijalnim sigurnosnim prijetnjama, odgovornostima i načinu korištenja resursa ZEMRIS-a, svaki korisnik je dužan i odgovoran proučiti sljedeće dokumente i striktno ih se pridržavati:

- *Pravilnik o informatičkoj sigurnosti radnog mjesta*
- *Pravilnik o klasifikaciji informacijskih resursa*

Dopuniti popisom dokumenata koje korisnici trebaju proučiti prije dobivanja prava pristupa sustavu

Voditelj sigurnosti dužan je u ugovor uključiti i druge dokumente koje smatra važnim za zaštitu sigurnosti informacijskog sustava.

5. Popis dokumenata

Dokumenti namijenjeni korisnicima:

- Pravilnik o informatičkoj sigurnosti radnog mjesta;
- Pravilnik o klasifikaciji informacijskih resursa;
- Pravilnik korištenja prijenosnih računala;

Dokumenti namijenjeni voditelju sigurnosti:

- Politika fizičke zaštite;
- Politika kontrole pristupa i bilježenje događaja;
- Politika upravljanja sigurnosnim incidentima;
- Politika upravljanja sigurnosnim zakrpama;
- Pravilnik o korisničkim računima i pravima pristupa;
- Pravilnik o sigurnosnim kopijama;
- Pravilnik o sklapanju i raskidu ugovora;

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik o informatičkoj sigurnosti radnog mjesta

voditelj sigurnosti:

Potrebno dopuniti podacima o voditelju (ime, prezime, mail, broj telefona)

Namijenjeno: svim korisnicima
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Pravilnik o sigurnosti radnog mjesta namijenjen je korisnicima informacijskog sustava ZEMRIS s ciljem pobude svijesti o IT sigurnosti kroz obavljanje svakodnevnih zadataka na računalu, korištenju Interneta, upotrebi elektronske pošte, postupanja s osjetljivim podacima, korištenjem aplikacija. Korisnici također moraju biti svjesni da upravo oni imaju kritičnu ulogu u održavanju uspješne informatičke sigurnosti.

2. Rukovanje zaporkama

Korisnici često smatraju kako ne moraju brinuti o sigurnosti jer njihovo računalo ne sadrži vrijedne informacije. No kompromitiranjem jednog osobnog računala u lokalnoj mreži ili jednog korisničkog računa na poslužitelju napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dešifrirati jednostavne zaporke, dok u isto vrijeme većina ne može pamtiti složene zaporke dugačke osam znakova. Stoga je svaki korisnik dužan pridržavati se pravila korištenja zaporki, te biti svjestan da nepridržavanjem pravila nije moguće uspostaviti kvalitetnu zaštitu cjelokupnog sustava.

Pravila korištenja zaporki

1. Minimalna dužina zaporke

- Kratku zaporku lakše je probiti.
- Minimalna dužina zaporke je 6 znakova.

2. Ne koristiti riječi iz rječnika

- Hakeri posjeduju zbirke suvislih riječi (riječi iz rječnika, imena, prezimena itd.).
- Izborom suvisle riječi haker lako probije zaporku.

3. Izmiješati mala i velika slova s brojevima

- Zaporku je bitno odabrati na taj način da ju lako pamtimo (ne smijemo ju zapisivati) i da je teška za probiti. Primjer – rA4unaL0; na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi računalo. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume...

- Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

- Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Neki korisnici naizmjence koriste dvije standardne zaporke. Iako su dvije zaporke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene lozinki.

6. Tajnost zaporke

- Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.
- Hakeri nastoje izmijeniti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja problema i bez poznavanja korisničkih zaporki.

7. Čuvanje zaporke

- Zaporke se ne smiju ostavljati na papirićima koji su zalijepljeni na ekran, ostavljeni na stolovima ili u ladici. Korisnik je odgovoran za tajnost svoje zaporke te mora naći način da je sakrije.
- Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

3. Antivirusna zaštita

Maliciozni programi (u koje spadaju virusi, crvi, trojanski konji itd.) su svi oni programi kojima je svrha zlonamjeran učinak na računalo (računalni sustav) ili koji obavljaju akcije na računalu bez znanja (pristanka) korisnika.

Na koji način se zaštititi

Da bi računalo bilo zaštićeno od malicioznih programa, korisnik je dužan pridržavati se nekoliko jednostavnih pravila:

- na svakom računalu mora biti instaliran antivirusni program,
- baza podataka s informacijama o novim virusima mora biti redovito ažurirana,
- korisnik mora provoditi provjere na prisutnost virusa kod svih datoteka na elektroničkim medijima nesigurnog ili neautoriziranog porijekla ili datoteka nabavljenih preko neprovjerenih mreže (uključujući Internet),
- činiti provjeru na prisutnost virusa kod svih privitaka elektroničke pošte i preuzetih datoteka,
- korisnik ne smije svojevoljno isključivati antivirusnu zaštitu,
- korisnik ne smije otvarati datoteke sumnjivog sadržaja,
- u programu za pregled pošte treba isključiti mogućnost automatskog otvaranja primljene pošte.

Ukoliko sumnjate u zaraženost vašeg računala malicioznim programom (neobična tromost računala pri radu), svakako učinite sljedeće:

- kontrolom tipki Ctrl+Alt-Del otvoriti Windows Task Manager,
- otvoriti karticu *Processes*,
- kartica *Processes* daje na uvid aktivne procese,
- ukoliko primijetite sumnjivi proces kopirajte njegove ime (s ekstenzijom) u Internet tražilicu Google (www.google.com) ili bilo koju drugu tražilicu te pokrenite pretragu,
- ukoliko je među rezultatima pretrage pronađena stranica s riječju *virus*, *malware*, *trojan* vjerojatno se radi o malicioznom programu i svakako kontaktirajte voditelja sigurnosti.

4. Sigurnost radne okoline

Da bi sigurnost radne okoline bila zadovoljena potrebno je pridržavati se *čistog stola*. Između ostalog korisnik je dužan pridržavati sljedećih pravila:

- važne informacije moraju biti fizički nedostupne svim osobama koje im nemaju pristup,
- kada nije u blizini radnog mjesta korisnik mora onemogućiti pristup sadržaju računala.

5. Uporaba elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne, no njeno korištenje može ozbiljno ugroziti sigurnost informacijskog sustava.

Potencijalne prijetnje i ranjivosti elektroničke pošte:

- **Virusi**
  - Elektronička pošta može biti malicioznog karaktera – u privitku je datoteka koja sadrži virus,
- **Nesigurnost protokola**
  - Poruke putuju kao običan tekst, te ih je lako pročitati ili izmijeniti sadržaj,
  - Lako je krivotvoriti adresu pošiljatelja,
- **Nezgode**
  - Pritiskom na krivu tipku ili odabirom krivog korisnika u adresaru poruka može doći neželjenom korisniku (ili više njih).

Da bi prijetnje informacijskom sustavu izazvane neprimjerenom uporabom elektroničke pošte sveli na minimum, potrebno je pridržavati se sljedećih pravila:

- elektroničku poštu ne smijete koristiti za slanje uvredljivih, omalovažavajućih, seksualno uznemiravajućih i drugih poruka sličnog sadržaja,
- nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi,
- svaka napisana poruka smatra se dokumentom. Nemate pravo poruke koju su poslane Vama osobno proslijediti dalje bez odobrenja autora,
- svaku poruku koja sadrži privitak sumnjivog sadržaja obavezni ste provjeriti antivirusnim programom,
- zavod ima pravo filtriranja poruka s namjerom da zaustavi neželjenu elektroničku poštu (eng. *spam*),
- u slučaju incidenta, Zavod ima pravo pregleda svih podataka (uključujući elektroničku poštu),
- poruke koje su dio poslovnog procesa nužno je arhivirati i čuvati propisani vremenski period,
- korisnik ne smije slati masovne poruke, bez obzira na njihov sadržaj.

6. Socijalni inženjering

Socijalni inženjering vrsta je napada na računalne sustave s ciljem nagovaranja ljudi da ispune zahtjeve napadača. Tu se prvenstveno radi o načinu skupljanja podataka do kojih napadač legalnim putem ne bi mogao doći. Pri tome se ne iskorištavaju propusti implementacija operacijskih sustava, protokola i aplikacija, nego se napad usmjerava na najslabiju kariku cjelokupnog lanca – ljudski faktor.

Najčešće metode prijevare:

- **Lažno predstavljanje** – najčešća metoda napada, postupak u kojem se napadač predstavlja kao neka druga osoba,
- **Uvjeravanje**/**Nagovaranje** – nagovaranje ili uvjeravanje je postupak pri kojem napadač nagovara i uvjerava žrtvu da obavi postupke koje mu nalaže napadač,
- **Stvara odgovarajuće situacije** – napadač stvara „plodno tlo“ za izvršenje napada na način da iskoristi žrtvine slabost; primjer takvog napada je zbližavanje sa žrtvom kako bi došao do informacija, iskorištavanje nespremnost ili nepažnju žrtve kako bi učinila pogrešan potez i sl.,

- **Moralna odgovornost** – žrtva pokuša pomoći napadaču jer osjeća da je to njena moralna obveza; žrtve nisu svjesne da na taj način odaju korisne informacije napadaču,
- **Želja za pomaganjem** – iskorištavanje želje žrtve da pomogne drugima; čest je slučaj da napadač uvjeri žrtvu da će on postupiti isto u situaciji kada žrtvi bude trebala pomoć,
- **Iskorištavanje starih veza i korupcije** – napadač stvara odnos koji je dovoljan za stjecanje povjerenja ili potkupljuje korisnika koji mu odaje željene informacije.

Načini izvršenja napada:

- **Telefonski inženjering** – jedan od najčešćih i najlakših načina izvršavanja socijalnog inženjeringa; napadač naziva npr. jednog od zaposlenika te svojim komunikacijskim vještinama lako stiče njegovo povjerenje,
- **Pretraživanje otpada** – jedan od načina sakupljanja informacija je pretraživanje otpada pri čemu se saznaje mnogo korisnih informacija za izvođenje napada,
- **Korištenjem Interneta** – brojni su načini prikupljanja informacija putem Interneta, a najčešći je slanjem lažnih poruka elektroničkom poštom**.** Na taj načni moguće je doći do vrlo tajnih informacija kao što su zaporke i osobni podaci,
- **Zavirivanje** – tip socijalnog inženjeringa pri kojemu napadači pokušavaju očitati žrtvine pokrete kako bi dobili željene podatke. Primjer ove tehnike je gledanje pokrete ruke prilikom ukucavanja PIN-a na bankomatu ili pri upisivanju zaporke prilikom prijave na sustav,
- **Forenzička analiza** – do korisnih informacija napadač može doći pregledom nepažljivo odbačenih medija (CD, DVD, memorijske kartice, diskovi, USB memorije i sl).

Metode zaštite

Jedini mogući način zaštite od socijalnog inženjeringa je educiranje korisnika uz implementiranje sigurnosnih kontrola pristupa i fizičke sigurnosti. Sve druge tehnike automatske detekcije, bilježenja i suprotstavljanja u ovoj vrsti napada nisu djelotvorne.

Educiranjem korisnika sprječavaju se oni napadi kod kojih žrtve zbog neznanja pružaju napadaču željene informacije. Educiranje korisnika treba sadržavati upute kako prepoznati socijalni inženjering i na koji način pravilno reagirati.

7. Phishing

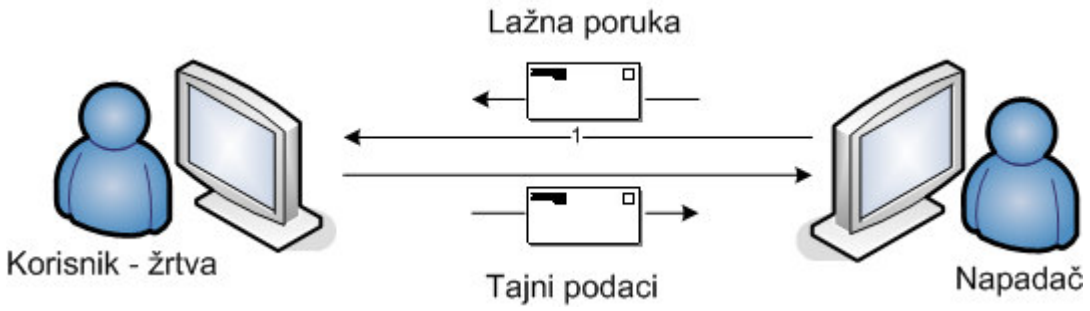
Phishing je vrsta napada u kojem napadač putem elektroničke pošte ili lažnih Internet stranica pokušava doći do povjerljivih informacija u cilju stjecanja financijske koristi. Najčešće je riječ o zaporkama, PIN brojevima, brojevima kreditnih kartica te drugim sličnim povjerljivim informacijama. Ukoliko napadač uspješno obavi napad i prikupi željene informacije, pruža mu se mogućnost pristupa informacijskim sustavima financijskih ustanova ili nekim drugim sustavima preko kojih može steći određenu financijsku korist.

Tijek provođenja phishing napada moguće je podijeliti u tri faze:

- osmišljavanje i pripremanje napada,
- provođenje napada,
- prikupljanje povjerljivih informacija i njihovo iskorištavanje.

Prva faza, osmišljavanje i pripremanje napada najvažniji je dio napada. U toj fazi napadač pokušava skupiti što više informacija o žrtvi, o detaljima žrtvinog operacijskog sustava i informacijskog sustava itd. Što više informacija posjeduje, napadač će s većom vjerojatnošću uspješno obaviti napad i ostati neotkriven.

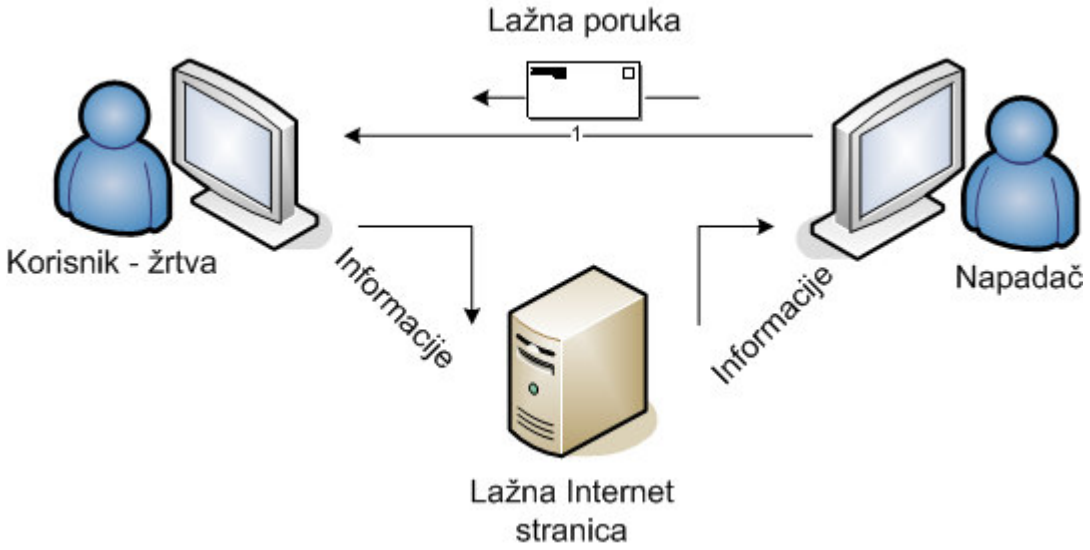
Druga faza je provođenje napada. Način provođenja napada ovisiti će o prikupljenim podacima u prvoj fazi. Slika C.1. shematski prikazuje napad elektroničkom poštom:



Slika C.1. – Primjer phishing napada elektroničkom poštom

Napad elektroničkom poštom realizira se tako da napadač slanjem elektroničke pošte potakne korisnika na odavanje željenih informacija. Jedan od primjera ovog napada prikazan je slikom: napadač šalje korisniku žrtvi lažnu poruku tako da se predstavi kao financijska ustanova. U poruci traži da žrtva hitno pošalje tajne podatke zbog provjere ili gubitka dijela podataka. Ukoliko korisnik ne primijeti prijevaru, šalje napadaču poruku u kojoj su sadržani tajni podaci. Napad je uspješno realiziran i napadač je došao do željenih podataka. Ovaj napad je najjednostavniji, a realizacija ovisi o needuciranosti korisnika žrtve. Ukoliko je žrtva naivna, vjerojatnost uspješnosti napada je relativno velika.

Druga metoda napada elektroničkom poštom je pozivanje korisnika žrtve na lažne Internet stranice. Slika C.2. shematski prikazuje opisani napad.



Slika C.2. – Primjer phishing napada lažnom Internet stranicom

Primjer tijeka napada: korisnik žrtva dobiva lažirani e-mail. U poruci se poziva da zbog određenog razloga posjeti Internet stranice financijske ustanove. Iako žrtva ne sumnja u vjerodostojnost, Internet stranice navedene u poruci su lažirane. Naime, lažne stranice vrlo je teško uočiti. Na primjer, ukoliko je originalna adresa www.financijskaustanova.hr, lažna adresa može biti www.financijska-ustanova.hr. Prosječni korisnik će teško zamijetiti ove razlike stoga treba biti vrlo oprezan. Osim

sličnosti u nazivu, lažirane stranice vizualno su identične originalnim Internet stranicama, stoga korisnici ne sumnjaju u bilo kakav oblik prijevare. Cilj napadača je da se korisnik pokuša prijaviti na sustav na lažnoj Internet stranici. Ukoliko se korisnik pokuša prijaviti, vjerojatno će dobiti poruku o trenutnom nefunkcioniranju sustava. No napadaču to više nije važno. Unosom podataka od strane korisnika napadač je dobio željene podatke za pristup originalnom sustavu banke ili bilo kojeg drugog informacijskog sustava.

Opisani oblici napada su napadi u kojima rezultat napada ovisi o reakciji korisnika. Ostali oblici napada temelje se na sposobnostima napadača da iskoriste propuste u komunikacijskim protokolima, operacijskim sustavima, softveru, sigurnosnim kontrolama itd., te ne ovise o reakcijama korisnika i stoga neće biti detaljnije obrađene.

8. Sigurnost medija

Mediji su resursi zavoda koji služe za pohranu podataka. Kao takvi igraju veliku ulogu u sigurnosti. Dolaskom do medija na kojem su pohranjeni povjerljivi podaci ili podaci za internu uporabu, napadaču mogu biti otvorena vrata za obavljanje zlonamjernih radnji.

Budući korisnici za razmjenu podataka koriste isključivo prijenosne medije (CD, DVD, USB memorije, štampana izvješća itd.), pravilnik o sigurnosti medija definira:

- svi mediji moraju biti pohranjeni na sigurnom i zaštićenom mjestu,
- svi mediji moraju biti čuvani prema specifikacijama proizvođača,
- mediji s povjerljivim podacima ne smiju se davati na korištenje neovlaštenim korisnicima,
- svako dijeljenje medija s povjerljivim podacima mora biti dokumentirano,
- potrebno je tražiti ovlaštenje za uklanjanje medija iz organizacije, te se mora voditi zapis o takvim aktivnostima,
- ako više nisu potrebni, treba obrisati prijašnje sadržaje svakog ponovno iskoristivog medija koji će biti uklonjen iz organizacije.

Uklanjanje medija

Svrha pravilnika o uklanjanju medija je smanjiti rizik od „curenja“ osjetljivih informacija koje može nastati nepravilnim odbacivanjem medija ukoliko medij više nije potreban. Kako bi se rizik „curenja“ sveo na minimum potrebno je uspostaviti formalne smjernice za sigurno uklanjanje medija.

Osim definiranja smjernica, važno je naglasiti da je uklanjanje osjetljivih medija treba biti provjereno i dokumentirano.

Lista dokumenata koji mogu zahtijevati sigurno uklanjanje:

- optički mediji (CD, DVD..),
- USB memorije,
- papirnati dokumenti,
- snimljeni glas,
- indigo papir,
- traka za printer,
- sistemska dokumentacija itd.

Smjernice uklanjanja medija:

- sve medije klasificirane kao osjetljive, koji više nisu za uporabu, potrebno je ukloniti na način da nitko ni na koji način nije u mogućnosti doći do podataka (ili dijela podataka) pohranjenih na mediju,
- papirnate i optičke medije potrebno je ukloniti pomoću aparata za uklanjanje medija,
- USB i ostale memorije potrebno je ukloniti prema pravilima proizvođača ili fizičkim djelovanjem na medij,
- ostale medije potrebno je ukloniti fizičkim djelovanjem, posebnim uređajima ili na treći način prema preporukama stručnjaka.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik o klasifikaciji informacijskih resursa

voditelj sigurnosti:

Potrebno dopuniti podacima o voditelju (ime, prezime, mail, broj telefona)

Namijenjeno: svim korisnicima
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Svrha pravilnika o klasifikaciji informacijskih resursa je uputiti korisnike na koji način rukovati pojedinim resursom. Budući nije moguće za svaki resurs definirati na koji način se prema njemu odnositi u smislu zaštite, nastao je pojam klasifikacije. Cilj klasifikacije je svrstati svaki resurs u pojedinu klasu ovisno o kriterijima klasifikacije. Klasa resursa jednoznačno određuje na koji način je korisnik dužan koristiti resurs, s kolikom pažnjom i odgovornošću.

2. Klasifikacija imovine

Vlasnik resursa dužan je prije njegova puštanja u uporabu klasificirati informaciju. Klasifikacija je postupak procjene informacije prema:

- vrijednosti,
- osjetljivosti,
- dostupnosti,
- tajnosti,
- važnosti za ZEMRIS,
- zakonodavnim zahtjevima.

Ovisno o izvršenoj procjeni svakoj imovini dodjeljuje se klasa. ZEMRIS klasificira imovinu prema 3 postojeće klase:

- Javno dostupno
- Interna uporaba
- Povjerljivo

I. Javno dostupno

Klasa javno dostupno predstavlja podatke:

- čija je uporaba otvorena za sve korisnike,
- koji nisu tajna,
- dijeljenje i objavljivanje ovih podataka ni na koji način ne štete ZEMRIS-u ili Fakultetu,
- ne postoje zakonodavni zahtjevi za „skrivanjem“ podataka.

Primjer *javnih* podataka:

- obavijesti studentima (npr. o početku nastavne godine..),
- radovi studenata (seminarski, diplomski..),
- podaci o fakultetu i sl.

II. Interna uporaba

Interna uporaba označava one podatke prema kojima se zbog zakonodavnih zahtjeva, moralnih obveza, prava privatnosti i sl. mora pažljivo i odgovorno odnositi s ciljem zaštite podataka od neovlaštenog pristupa, modificiranja, kopiranja, prijenosa i ostalih načina zlouporabe. Podaci klasificirani kao *interna uporaba* namijenjeni su isključivo zaposlenicima zavoda koji imaju legitimno pravo pristupa ovakvim podacima.

Primjeri podataka klase *interna uporaba*:

- podaci o zaposlenicima, studentima,
- podaci ugovora s trećom stranom,
- interni telefonski imenik,
- predavanja pojedinih predmeta i sl.

Podaci klase interna uporaba:

- moraju biti zaštićeni od neovlaštenog pristupa,
- podaci moraju biti pohranjeni na sigurnim mjestima u smislu fizičke zaštite,
- ukoliko podaci više nisu potrebni, moraju biti uništeni prema pravilima politike o uklanjanju medija i brisanja informacija.

III. Povjerljivo

Klasa *povjerljivo* označava podatke koji zbog zakonodavnih zahtjeva, propisa fakulteta ili zbog ugovornih obveza moraju biti strogo zaštićeni. Pristup *povjerljivim* podacima imaju samo pojedinci koji ih zbog prirode posla moraju koristiti.

Povjerljivi podaci:

- ukoliko su pohranjeni u elektroničkom formatu, moraju biti zaštićeni jakom lozinkom, pohranjeni na poslužiteljima s jakim sigurnosnim mjerama u svrhu zaštite od gubitka, krađe, neovlaštenog pristupa i razotkrivanja,
- potrebno je redovito raditi sigurnosne kopije podataka,
- sigurnosne kopije *povjerljivih* podataka potrebno je čuvati na mjestima sa strogim sigurnosnim kontrolama,
- ne smiju biti proslijeđene bez eksplicitnog odobrenja odgovornih osoba,
- prava pristupa *povjerljivim* podacima dodjeljuje se isključivo uz odobrenje odgovorne osobe,
- mediji na kojima su povjerljivi podaci pohranjeni moraju se nalaziti u prostorijama do kojih je pristup omogućen samo ovlaštenim osobama,
- ako se podaci šalju putem faksa ili elektroničke pošte mora se koristiti protokol i mehanizmi koji podatke štiti od neovlaštenog pregledavanja ili mijenjanja,
- ukoliko podaci više nisu potrebni, moraju biti uništeni prema pravilima politike o uklanjanju medija i brisanja informacija.

Primjeri *povjerljivih* resursa:

- podaci o studentima (JMBG, brojevi kartica i sl.),
- ocjene studenata,
- ispitna pitanja i sl.

3. Pravila klasifikacije

Svi resursi zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave (ZEMRIS) moraju zadovoljavati sljedeće kriterije:

- vlasnik je dužan provesti klasifikaciju resursa prije njegova puštanja u uporabu,
- svaki resurs (CD, DVD, papirnati dokumenti, web stranice i sl.) mora imati jasno istaknutu oznaku stupnja klasifikacije, osim ukoliko je riječ o javno dostupnim podacima,
- prije usmenog priopćavanja klasificiranih podataka drugim osobama (koje imaju pravo pristupa tim podacima) obavezno se daje prethodno upozorenje o stupnju njihove klasifikacije,
- povjerljivi podaci ne smiju se dijeliti ni na koji način (usmeno, pismeno, elektroničkim putem itd.) osobama koje nemaju pravo pristupa tim podacima,
- svaku uočenu nepravilnost (neovlašteni pristup, mijenjanje, brisanje, dijeljenje informacija i sl.) korisnik je dužan prijaviti odgovornoj osobi,

- klasificirane podatke dobivene od treće strane potrebno je klasificirati prema pravilima klasifikacije ZEMRIS-a; ukoliko ne postoji mogućnost klasifikacije prema internim pravilima, potrebno je proširiti postojeća pravila u skladu s ukazanim potrebama,
- odgovorna osoba dužna je uspostaviti metode vođenja evidencije o pristupu *povjerljivim* podacima.

4. Klasifikacijske oznake

Klasifikacijska oznaka pojedinog informacijskog sustava trebala bi biti jedinstvena zbog toga što u suprotnome može doći do miješanja nejednakih klasifikacijskih oznaka više informacijskih sustava.

Primjer, informacijski sustav A ima klasifikacijsku oznaku 1 za strogo povjerljive podatke. Sustav B s klasifikacijskom oznakom 1 označava javne podatke. Ukoliko medij iz sustava A dopusti korištenje medija (klasificiranim kao 1) korisnicima sustava B, može doći do nesporazuma na način da se strogo povjerljivi podaci koriste kao javni.

Prijedlog klasifikacijskih oznaka ZEMRIS-a:

I. Javno dostupno

II. Interna uporaba

III. Povjerljivo

Klasifikacijske oznake važno je što bolje označiti (npr. različitim bojama, oblicima) i istaknuti ih na uočljivim mjestima kako bi bili sigurni da su ih korisnici uočili (posebno ako je riječ o povjerljivim resursima).

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik korištenja prijenosnih računala

voditelj sigurnosti:

Potrebno dopuniti podacima o voditelju (ime, prezime, mail, broj telefona)

Namijenjeno: svim korisnicima
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Prijenosna računala sve su popularnija. Cjenovno blizu, a praktičnošću puno ispred stolnih računala, postala su česti izbor pri kupnji računala bilo da se radim o poslovnim ili privatnim korisnicima.

No uporaba prijenosnih računala od strane zaposlenika, partnera ili drugih korisnika donosi potrebu za implementacijom dodatnih sigurnosnih kontrola. One moraju spriječiti svaku neovlaštenu radnju koja može ugroziti sigurnost informacijskog sustava.

2. Identifikacija prijetnji

Sigurnost sustava uporabom prijenosnih računala možete biti ugrožena na sljedeće načine:

- slučajni postupci ovlaštenog korisnika prijenosnog računala,
- namjerni postupci ovlaštenog korisnika prijenosnog računala,
- namjerni postupci neovlaštenog (zlonamjernog) korisnika,
- pokretanje malicioznog kôda na prijenosnom računalu,
- krađa, gubitak ili mijenjanje podataka zbog nepravilnog rukovanja prijenosnim računalom, kvara oprema ili nekog drugog razloga.

Kako bi se sigurnosni rizik korištenja prijenosnih računala sveo na minimum, svaki korisnik dužan je pridržavati se pravila definiranih u nastavku.

3. Fizička zaštita prijenosnog računala

Unutar prostorija zavoda.

Unutar prostorija zavoda korisnik je dužan pridržavati se pravila definiranih Pravilnikom o informatičkoj sigurnosti radnog mjesta. To znači da računalo ni u kojem trenutku ne smije ostaviti nezaštićeno bez nadzora. Kod kraćih izbivanja računalo je potrebno zaštititi nekim od jednostavnijih oblika zaštite (kombinacijom tipki ctrl + L; čuvarom ekrana s lozinkom i sl.). Kod dužih izbivanja (godišnji odmor, bolovanje) korisnik je dužan računalo smjestiti u prostor pod fizičkom zaštitom (u zaključani ormar) ili se o zaštiti posavjetovati s voditeljem sigurnosti.

Izvan prostorija zavoda.

Ukoliko prijenosno računalo nosimo izvan prostorija zavoda (na putovanje ili doma), potrebno je pridržavati se sljedećeg:

- vrijeme bez nadzora računala treba biti što kraće,
- računalo ne ostavljati u automobilu na vidljivom mjestu,
- ne ostavljati ga bez nadzora u nezaključanom prostoru;
- ostavljeno prijenosno računalo treba biti isključeno, zaključano u spremištu gdje nije vidljivo.

4. Servis opreme

Servisiranje:

- ukoliko je moguće prije servisiranja potrebno je napraviti sigurnosne kopije svih (važnih) podataka s računala, sigurnosne kopije potrebno je napraviti u skladu s *Pravilnikom o sigurnosnim kopijama*,
- ako servisiranje provodi treća strana, podatke s računala potrebno je zaštititi ovisno o njihovoj klasifikaciji (nekom od kriptografskih metoda), ukoliko postoji potreba podaci s računala moraju biti izbrisani (nakon izrade sigurnosne kopije podataka).

Povratak prijenosnog računala sa servisa:

- sve zaporke moraju biti promijenjene,
- sve funkcionalnosti trebaju biti provjerene,
- sve se mora podvrći antivirusnoj provjeri.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Politika fizičke zaštite

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Svrha politike fizičke zaštite informacijskog sustava je preventivnim metodama osigurati zaštitu sustava ZEMRIS od namjernih ili slučajnih destruktivnih radnji.

Politikom fizičke zaštite želi se:

- spriječiti neovlašteni pristup,
- spriječiti ometanje poslovnih prostorija,
- spriječiti nepotreban pristup korisnika osjetljivoj opremi,
- osigurati zaštita opreme od prirodnih utjecaja,
- osigurati sigurnost instalacija,
- osigurati održavanje opreme.

2. Područje fizičke zaštite

Da bi se osigurala fizička zaštita informacijskog sustava ZEMRIS, odgovorna osoba dužna je implementirati sljedeće točke sigurnosti:

- potrebno je jasno definirati i dokumentirati tko je ovlašten pristupiti pojedinim prostorijama pod fizičkom zaštitom,
- kontrolnim mehanizmima potrebno je spriječiti svaki pokušaj neovlaštenog pristupa; ulazi u prostorije zavoda koje sadrže poslužitelje, medije za pohranu podataka i ostale osjetljive resurse potrebno je zaštititi metodama kontrole ulaska (kartice, ključ i sl.),
- vrata na ulazima u zaštićena područja moraju biti otporna na požare, poplave i probijanja,
- ulazi u prostorije koje sadrže osjetljivu opremu moraju biti jasno označeni,
- svi kontrolni mehanizmi moraju biti periodički pregledavani kako bi se na vrijeme uočili nedostaci zaštite ili pokušaji neovlaštenog pristupa.

3. Sigurnost opreme

Svrha uspostave sigurnosti opreme je spriječiti gubitke, štetu ili kompromitiranje imovine i prekid poslovnih aktivnosti.

Oprema treba biti zaštićena od prijetnji i opasnosti iz okoline. Zaštita opreme je neophodna kako bi se smanjio rizik neovlaštenog pristupa podacima, te kako ne bi došlo do gubljenja i oštećenja imovine.

3.1 Smještaj i zaštita opreme

Sljedeće smjernice treba uzeti u obzir pri fizičkoj zaštiti opreme:

- oprema mora biti smještena tako da je nepotrebni pristup opremi minimalan,
- jedinice za obradu podataka moraju biti smještene tako da je smanjena mogućnost promatranja neovlaštenim korisnicima (primjer: postavljanje monitora pod takvim kutom da samo osoba za računalom vidi sliku),
- kontrole je potrebno implementirati tako da minimaliziraju rizik od potencijalnih prijetnji; primjer: krađa, požar, dim, voda, vibracije, radijacije itd.,
- zabranjeno je jesti, piti, pušiti u blizini opreme,
- uvjeti okružja (temperatura, vlaga) koji mogu utjecati na rad jedinica za obradu informacija trebaju biti definirane od strane odgovorne osobe te strogo nadzirane.

3.2 Sigurnost instalacija

Jedinice za obradu podataka moraju biti zaštićene od grešaka koje mogu nastati u opskrbi energijom, vodom, odvodnjom otpadnih voda, grijanjem/hlađenjem itd. Sve navedene instalacije moraju biti pravovremeno pregledane i testirane kako bi se na vrijeme uočile i ispravile greške u radu.

Nestanak struje, poplavu, požar ili bilo koju drugu prijetnju bitno je alarmirati zvučnim i svjetlosnim signalima kako bi se pravovremeno poduzele propisane akcije u slučaju nezgode. Opskrba vodom mora biti redovito kontrolirana kako ispravnost uređaja za gašenje požara ne bi bila upitna. Telekomunikacijska oprema mora biti instalirana na način da eventualan prekid veze ne utječe na kompletan prekid komunikacije. Primjer rješenja ovog problema je priključenje komunikacijskih uređaja na više poslužitelja.

3.3 Sigurnost kod kabliranja

Kablovi za opskrbu električnom energijom i telekomunikacijski kabeli moraju biti adekvatno zaštićeni od oštećenja, prekida ili priključenja neovlaštenih korisnika na mrežu.

Prije kabliranja mora biti razmotreno sljedeće:

- kabeli za napajanje jedinica za obradu podataka, ukoliko je moguće, moraju biti položeni podzemno; alternativa je adekvatna fizička zaštita,
- isto vrijedi i za telekomunikacijske kabele,
- kabeli za napajanje moraju biti razdvojeni od telekomunikacijskih kako bi se izbjeglo međudjelovanje,
- označavanje kabela posebnim identifikacijskim oznakama spriječiti će greške u spajanju; oznake je potrebno dokumentirati.

4. Održavanje opreme

Održavanje opreme treba biti redovito i obavljeno od strane stručnjaka kako bi se osigurala ispravnost, tj. neprekidan rad.

Pri održavanju opreme treba se pridržavati sljedećeg:

- održavanje opreme mora biti u skladu s preporukama proizvođača, u određenim vremenskim intervalima i po zadanim specifikacijama,
- samo ovlaštene osobe smiju servisirati opremu,
- prije servisiranja opreme potrebno je implementirati odgovarajuće sigurnosne kontrole ukoliko za tim postoji potreba, te je potrebno obrisati povjerljive informacije (potrebe za ovakvim mjerama nastaju ukoliko servisiranje izvršava vanjski partneri ili treća strana),
- pristup opremi od strane vanjskih partnera treba biti strogo kontroliran i dokumentiran,
- pristup opremi od strane vanjskih partnera treba biti ograničen ugovorom.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Politika kontrole pristupa i bilježenje događaja

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Zasigurno jedan od važnijih uzroka problema sigurnosti predstavljaju ovlašteni korisnici. Oni svojim postupcima, bilo slučajnim ili namjernim, ugrožavaju sigurnost sustava u velikoj mjeri.

Neki od uzroka sigurnosnih incidenata od strane ovlaštenih korisnika:

- znatiželja,
- dokazivanje,
- krađa identiteta od strane zlonamjerne osobe,
- slučajni postupci (needuciranost korisnika),
- prikupljanje podataka u zlonamjerne svrhe itd.

Navedene prijetnje sigurnosti informacijskim sustavima razlog su zbog kojih postoji potreba za kontrolom pristupa, tj. zabranom pristupa onim resursima sustava kojima korisnik nema potrebe pristupati.

Osim kontrola pristupa, u svrhu pravovremenog uočavanja odstupanja od politike pristupa i radi pružanja dokaza u slučaju sigurnosnog incidenta, u sustav je potrebno implementirati sigurnosnu kontrolu bilježenje događaja (nadziranje).

2. Kontrola pristupa

i. Prava pristupa u skladu s potrebama

Pristup informacijskim resursima potrebno je odobriti ukoliko zaposlenik, student ili treća strana ima realnu potrebu za pristup traženim resursima. Zahtjev za dodjelu prava pristupa na temelju kojeg je donesena odluka o dodjeli prava pristupa treba biti dokumentiran.

Dokument treba sadržavati:

- identifikator inicijatora zahtjeva,
- identifikator osobe kojoj je potrebno dodijeliti prava pristupa,
- opis zahtjeva,
- datum podnošenja zahtjeva,
- ukratko politiku sigurnosti traženog resursa - klasifikacija resursa, da li postoje zakonske i ugovorne obveze sl.,
- vrijeme trajanja prava pristupa – vremenski period u kojem će dodijeljena prava vrijediti, nakon toga potrebno je ponovno predati zahtjev za dodjelu prava pristupa,
- tko je pregledao i odobrio zahtjev.

ii. Upravljanje pristupom korisnika

S ciljem kvalitetne kontrole pristupa informacijskim sustavima i servisima nužno je uspostaviti odgovarajuće procedure. Te procedure trebaju obuhvatiti sve stadije u životnom ciklusu korisničkog pristupa, od početne registracije novog korisnika do konačnog odjavljivanja korisnika kojem više nije potreban pristup informacijskim resursima. Posebnu pažnju treba posvetiti kontroli dodjele privilegiranih prava pristupa.

Registracija korisnika.
Da bi pojedinom korisniku bila dodijeljena prava pristupa informacijskom sustavu i servisima potrebno je definirati postupke registracije u i odjave iz sustava. Pristup treba kontrolirati kroz proces registracije korisnika koji uključuje:

- korištenje korisničkih imena dodijeljenih od strane administratora sustava ili za to odgovorne osobe,
- korisnička imena trebaju biti jedinstvena kako bi se korisnike moglo povezati s njihovim aktivnostima,
- provjeru autentičnosti korisnika preko lozinke,
- provjeru prava pristupa za korištenje informacijskih resursa prema korisničkom imenu,
- u slučaju planiranog dužeg izostanka s posla, korisnikov račun treba biti zamrznut,
- ukoliko korisnik prestane biti zaposlenik, student ili dođe do raskida ugovara s trećom stranom, trenutačno trebaju biti ukinuta prava dotičnim osobama.

Upravljanje korisničkim lozinkama
Lozinke služe kako bi se putem mreže provjerilo da li je korisnik koji se predstavlja korisničkom lozinkom upravo taj korisnik. Stoga je nužno sigurnosnim mehanizmima osigurati maksimalnu sigurnost lozinki u smislu njihove tajnosti. Osim politike sigurnosti namijenjene korisnicima u kojoj se jasno definira na koji način rukovati lozinkama, osoba odgovorna za sigurnost dužna je držati se sljedećih pravila prilikom raspodjeli lozinka:

- korisnici su dužni prilikom preuzimanja lozinki potpisati izjavu u kojoj se obvezuju rukovati lozinkama prema pravilima definiranim u Pravilniku o informatičkoj sigurnosti radnog mjesta (poglavlje 2. - Rukovanje zaporkama),
- prilikom dodjele lozinke korisniku, prvo im se dodjeljuje privremena lozinka koju u što kraćem roku, pri prvoj prijavi na sustav moraju promijeniti. Sustav treba podesiti na način da ne dozvoljava prijavu privremenom lozinkom,
- lozinke se korisnicima smiju proslijediti isključivo na siguran način, nikako ne elektroničkom poštom, telefonom ili uporabom treće strane,
- lozinke se ne smiju pohranjivati na računalu u nezaštićenom obliku.

iii. Odgovornost korisnika

Uporaba lozinki
Od korisnika je potrebno zahtijevati da pri odabiru i rukovanju lozinkama slijede sigurnosne upute definirane Pravilnikom o informatičkoj sigurnosti radnog mjesta (poglavlje 2. - Rukovanje zaporkama). Korisnike treba savjetovati da:

- čuvaju povjerljivost lozinki,
- ne bilježe lozinke na papire,
- lozinke smiju mijenjati isključivo nakon prijave na sustav,
- biraju kvalitetne lozinke, dugačke minimalno 6 znakova, maksimalno 10,
- lozinke budu lako pamtljive,
- lozinke sadrže brojeve i slova, po potrebi i specijalne znakove,
- lozinke ne predstavljaju imena, prezime, gradove, datume rođenja, nadimke i sl. riječi.
- redovito mijenjaju lozinke,
- ne koriste već upotrebljavane lozinke,
- ne koriste lozinke koje već koriste na drugim sustavima.

Nenadzirana korisnička oprema
Korisnike je potrebno educirati o potrebi zaštite opreme kada nisu u njihovoj blizini. Mnogi korisnici nisu ni svjesni mogućnosti zlouporabe računala, mobitela, ali i drugih komunikacijskih uređaja ukoliko na kratko vrijeme ostanu bez nadzora. Svaki korisnik mora biti svjestan svoje odgovornosti, sigurnosnih zahtjeva i postupaka za zaštitu nenadzirane opreme.

Korisnike treba savjetovati da:

- ukoliko se računalo ostavlja bez nadzora, potrebno se odjaviti sa sustava ili zaštititi računalo posebnim programima (npr. čuvar ekrana),
- nakon završetka posla računalo je potrebno odjaviti sa sustava, nije dovoljno ugasiti terminal ili osobno računalo,
- ukoliko je potrebno, terminale, računala i drugu opremu treba zaključati kada nije u uporabi.

iv. Kontrola pristupa mreži

Svi interni i eksterni mrežni servisi moraju biti kontrolirani u svrhu zaštite resursa od korisnika koji imaju pristup mreži i mrežnim resursima. Kontrola pristupa mreži treba sadržavati sljedeće kontrole:

- korisnici smiju pristupiti samo onim mrežnim servisima za koje imaju definirane eksplicitne ovlasti,
- kontrole upravljanja i procedure za zaštitu pristupa mreži moraju biti jasno definirane,
- u svrhu smanjenja rizika neautoriziranog pristupa, potrebno je odrediti „propisani put“. Cilj „propisanog puta“ je spriječiti korisnike da biraju putove izvan puta od terminala do servisa za koje su oni ovlašteni. Princip rada navedene kontrole je da se u svakom mrežnom čvoru mogućnost usmjeravanja limitira na unaprijed odabrane opcije,
- korisnike koji pristupaju resursima s udaljenih lokacija potrebno je autentificirati posebnim metodama koje osiguravaju odgovarajuću razinu zaštite.

v. Kontrola pristupa operacijskom sustavu

Pristup korisnika operacijskim sustavima potrebno je kontrolirati putem ugrađenih mehanizama, s ciljem sprječavanja neovlaštenog pristupa. Mehanizam kontrole pristupa operacijskom sustavu treba sadržavati:

- prilikom prijave na sustav korisnik treba unjeti svoje korisničko ime i lozinku, na temelju čega se radi provjera identiteta,
- provjeru da li je period valjanosti lozinke istekao; ukoliko jest (svaka 3 mjeseca), obavijestiti korisnika da je potrebno napraviti izmjenu,
- sustav mora bilježiti pristup informacijskom sustavu i pokušaje pristupa (detaljnije u poglavlju 3. – Bilježenje događaja),
- rad korisnika na terminalima treba dodatno kontrolirati na način da se prati vrijeme neaktivnosti; ukoliko je terminal neaktivan duže od 5min, treba napraviti automatsku odjavu sa sustava i obrisati ekran,
- ukoliko je potrebno, kontrolu s koje se lokacije pristupa sustavu,
- broj mogućih prijava na sustav treba ograničiti na 3 prijave.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Politika upravljanja sigurnosnim incidentima

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Bez obzira na sve veća sredstva i napore koji se ulažu u postizanje i održavanje sigurnosti informacijskih sustava, sigurnosni incidenti i dalje su česta pojava. Svaki sigurnosni incident bez obzira na veličinu i trajanje za organizaciju predstavlja gubitak, zbog čega je vrlo važno da se adekvatna pažnja posveti razvoju strategije i planiranju aktivnosti u slučaju pojave sigurnosnih incidenata.

Zbog toga je upravljanje sigurnosnim incidentima važan segment poslovanja svake organizacije. Ukoliko se unaprijed definiraju zaštitne mjere i koraci u slučaju pojave incidenta, znatno se mogu umanjiti gubici i utjecaj incidenta na poslovanje organizacije.

Kako bi upravljanje sigurnosnim incidentima bilo kvalitetno organizirano, potrebno je definirati:

- odgovornosti i uloge,
- potencijalno opasne radnje,
- procedure u slučaju incidenta,
- procedure za pravovremenu detekciju,
- procedure za analizu incidenta i uklanjanje posljedica,
- procedure za vraćanje sustava u inicijalno stanje.

2. Definiranje odgovornosti i uloga

Glavna odgovorna osoba dužna je inicirati provedbu politike upravljanja sigurnosnim incidentima. Odgovornost u organizaciji i provođenju politike može imati jedna osoba, ali i više njih. Važno je da hijerarhija odgovornosti bude jasno definirana i dokumentirana.

Inicijalnu odgovornost nad upravljanjem sigurnosnim incidentima ima glavna odgovorna osoba. Glavna odgovorna osoba odgovornost ili dio odgovornosti može prenesti na drugu osobu/osobe, uz obavezno jasno definiranje i dokumentiranje odgovornosti.

Treba dopuniti smjernicama kako prijaviti sigurnosni incident i potencijalne ranjivosti sustava.

3. Pravovremena detekcija

Kako bi se potencijalne prijetnje i incidenti pravovremeno detektirali, potrebno je osposobiti sljedeće mehanizme:

- softversko praćenje dnevnika zapisa s mogućnošću alarmiranja kod detekcije potencijalno opasnih radnji (DDoS napadi, *brute force* napadi, uporaba resursa informacijskog sustava za slanje neželjene pošte itd.),
- periodički pregled dnevnika zapisa od strane odgovorne osobe s ciljem uočavanja potencijalno opasnih radnji koje softver nije detektirao,
- pregled prijava korisnika o incidentima od strane korisnika,
- pregled prijava korisnika o ranjivostima sustava.

Odgovorne osobe koje pregledavaju prijave korisnika dužne su voditi evidenciju primljenih zahtjeva i akcija koje su poduzete. Dnevnik između ostalog mora sadržavati:

- kada je napravljena prijava od strane korisnika,
- kada je pregledana prijava od strane odgovorne osobe,

- zapis prijave,
- koje su akcije poduzete u vezi prijave,
- da li je opasnost otklonjena ili ne.

5. Kako reagirati u slučaju incidenta

U slučaju incidenta odgovorna osoba mora reagirati na način da zadovolji sljedeće:

- spriječi daljnje počinjenje zlonamjernih radnji,
- pokuša prikupiti dodatne informacije o napadaču (dokazni materijal), o lokaciji s koje je kazneno djelo izvršeno, vrijeme, itd.,
- pozove policiju.

Treba dopuniti definicijama koji su načini sprječavanja daljnjih zlonamjernih radnji.

Treba dopuniti definicijama na koji se način mogu prikupiti dodatni dokazni materijali.

Ukoliko odgovorna osoba primijeti ili dobije prijavu od strane korisnika o potencijalnoj ranjivosti sustava, dužna je učiniti sljedeće:

- napraviti evidenciju zahtjeva na isti način kao kod primitka prijave o incidentu,
- inicirati rješenje problema na način da se obavijesti vlasnika resursa o propustu,
- u evidenciju dodati tko je odgovoran, datum i vrijeme kada je primio obavijest o ranjivosti i kada je ranjivost uklonjena.

6. Analiza incidenata, uklanjanje posljedica

Nakon obavljanja inicijalnih procedura u slučaju incidenta i nakon što je napad (opasnost) prošao, potrebno je napraviti analizu stanja kako bi se utvrdilo što je sve obuhvaćeno incidentom.

Neki od mogućih ciljeva napada:

- iskorištavanje sustava za obavljanje zlonamjernih radnji (slanje neželjene elektroničke pošte, izvršavanje napada odbijanja usluge itd.),
- napadi na sustav odbijanja usluge, *brute force* napadi,
- krađa resursa,
- mijenjanje resursa,
- uništavanje resursa itd.

Analizom je potrebno definirati što je sve bio cilj napada, kolika je šteta i na koji način detektiranu štetu ispraviti, odnosno na koji način sustav dovesti u zadnje “netaknuto” stanje.

U slučaju mijenjanja i uništavanja resursa, ukoliko je riječ o logičkim resursima (informacije, softver), rješenje će vjerojatno biti napraviti obnovu iz sigurnosnih kopija podataka. Ovaj tip incidenta može biti vrlo ozbiljan ukoliko sigurnosne kopije ne postoje (nisu pravovremeno napravljene) jer je ponekad izgubljene podatke nemoguće obnoviti.

Dopuniti definicijama procedura za vraćanje sustava u inicijalno stanje.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Politika upravljanja sigurnosnim zakrpama

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Svrha politike upravljanja sigurnosnim zakrpama je reguliranje procesa otklanjanja skrivenih pogrešaka operacijskih sustava i programskih paketa.

Pravovremeno otklanjanje postojećih pogrešaka operacijskih sustava i programskih paketa sprječava moguću štetu zbog širenja virusa, crva, zlonamjernih kodova i ostalih napada na sigurnost, koji za posljedicu imaju smanjenje operativnosti, integriteta i povjerljivosti informacijskog sustava.

2. Upravljanje sigurnosnim zakrpama

Administrator je odgovoran brinuti osobno ili oformiti grupu zaduženu za upravljanje programskim zakrpama.

Zadatak upravljanja programskim zakrpama je redovna kontrola ažurnosti verzija operacijskih sustava i kritičnih programskih paketa, te dokumentiranje zatečenog stanja. Sukladno provedenoj kontroli, potrebno je poduzeti adekvatne mjere pomoću postojećih mehanizama za primjenu programskih zakrpi i/ili instalaciju novih verzija. Privremeno rješenje može uključivati ukidanje nepotrebnog servisa i/ili promjenu konfiguracijskih parametara.

Preporuka redovitosti kontrola je svakih mjesec dana za Windows okruženje, svaka tri mjeseca za mrežne uređaje i centralna računala; i/ili češće, ovisno o pokazateljima na neispravan rad nekih servisa ili dobivenim/objavljenim upozorenjima od strane proizvođača i odgovarajućih izvora.

Ukoliko postoji mogućnost, poželjno je da se instalacija zakrpa provodi centralizirano – s jednog računala istodobno na sva računala informacijskog sustava. Ako ovakav način instaliranja zakrpa nije moguć, potrebno je osmisliti mehanizme kojima će se osigurati instalacija zakrpa na svako računalo sustava.

Administrator prije odobrenja treba proučiti pripadajuću dokumentaciju i po mogućnosti testirati programsku zakrpu na izdvojenoj testnoj okolini koja je što sličnija produkcijskoj okolini.

Za kritična računala (poslužitelje i računala na kojima su instalirane aplikacije neophodne za normalni tijek poslovnih procesa) prije same instalacije programske zakrpe, potrebno je napraviti sigurnosnu kopiju koja osigurava povratak na staro.

Odgovorne osobe obavezni su voditi ažurnu i jedinstvenu evidenciju primijenjenih programskih zakrpa na računalima. U evidenciju se upisuju i one programske zakrpe koje se nisu mogle primijeniti na računala zbog neadekvatne verzije instaliranog softvera i/ili posebnosti instaliranih aplikacija, čija funkcionalnost, nakon primjene istih, ne bi bila moguća.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik o korisničkim računima i pravima pristupa

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Svrha dokumenta *Pravilnik o korisničkim računima i pravima pristupa* je osigurati kontrolu nad otvaranjem, izmjenom, zamrzavanjem i zatvaranjem korisničkih računa u informacijskom sustavu ZEMRIS, u cilju sprječavanja zastarjelih, redundantnih i korisničkih računa otvorenih na neispravan način. Drugi dio dokumenta odnosi se na dodjelu prava pristupa.

Pravo pristupa vrijednostima informacijskog sustava jedna je od najkritičnijih točaka sigurnosti. Zbog naizgled kompliciranog procesa dodjeljivanja prava pristupa, korisnicima se često dodjeljuju „uobičajena“ prava, koja su najčešće puno veća od potrebnih. Što veća prava pristupa korisnik posjeduje, veće su mogućnosti da slučajnim ili namjernim radnjama ugrozi sigurnost informacijskog sustava. Iz tog razloga potrebno je ograničiti djelovanje korisnika na način da im se dopusti obavljanje samo onih radnji koje su nužne za obavljanje njihova poslova.

2. Evidencija zahtjeva

Pravovremeno zatvaranje korisničkog računa važna je karika u sigurnosti informacijskih sustava. Ukoliko „nevažeći“ korisnički račun nije zatvoren, korisniku je otvoren put obavljanju zlonamjernih radnji. Kako bi proces otvaranja i zatvaranja korisničkih računa bio pravovremeno i kvalitetno obavljen, potrebno je definirati načine komunikacije između podnositelja zahtjeva i administratora sustava, te način evidencije zahtjeva za otvaranjem odnosno zatvaranjem računa.

Prijedlog komunikacije i evidencije zahtjeva:

- komunikacija s osobom odgovornom za upravljanje korisničkim računima obavlja se unaprijed definiranim protokolom, npr. putem web aplikacije,
- kako bi podnositelj zahtjeva pristupio aplikaciji, potrebno je obaviti provjeru autentičnosti i autorizaciju,
- podnositelj zahtjeva na svom računalu otvara aplikaciju i zadaje zahtjev za otvaranjem/zatvaranjem korisničkog računa,
- zahtjev se pohranjuje u bazu podataka,
- administrator ima mogućnost pregleda zahtjeva prema kriteriju,
- administrator je dužan redovito pregledavati zahtjeve,
- zatvaranje zahtjeva ima prednost nad otvaranjem zahtjeva.

Protokol komunikacije između podnositelja zahtjeva i odgovorne osobe, te evidencije samih zahtjeva može biti realiziran i na neki drugi način odobren od strane voditelja sigurnosti.

3. Otvaranje korisničkog računa

Korisnički račun moguće je otvoriti:

- zaposleniku zavoda,
- studentu,
- trećoj strani.

Procedura otvaranja korisničkog računa:

- zaposlenicima:
  - tajnica putem aplikacije podnosi zahtjev za otvaranje korisničkog računa novom zaposleniku,

  - administrator sustava na temelju dobivenih podataka otvara korisnički račun.
- studentima:
  - pri upisu studija studentima se automatski otvara korisnički račun.
- trećoj strani:
  - za otvaranje korisničkog računa trećoj strani potrebna je suglasnost odgovorne osobe,
  - odgovorna osoba je glavna i odgovorna osoba u suradnji s trećom stranom, i kao takva ima prava davanja suglasnosti za otvaranje korisničkih računa,
  - kod otvaranja korisničkog računa za treću stranu potrebno je odrediti vremenski period koliko će račun biti aktivan.

4. Zamrzavanje korisničkog računa

U slučaju duljeg planiranog nekorištenja informacijskog sustava (npr. zbog edukacije u inozemstvu, bolesti, zamrzavanje godine i sl.) korisnički račun potrebno je *zamrznuti*. Zamrzavanjem korisničkog računa izbjegavaju se nepotrebni postupci zatvaranja i otvaranja računa, ali i sprječavaju sigurnosni incidenti koji mogu nastati korištenjem korisničkog računa od strane drugih osoba dok stvarni vlasnik nije prisutan. Zamrzavanje računa odvija se na način da podaci ostanu u bazi podataka o korisniku, ali se u posebno polje naznači da je račun zamrznut.

Zamrznutom korisničkom računu nije potrebno mijenjati lozinku u određenom vremenskom periodu kako je definirano politikom. Također se zaobilaze sve druge sigurnosne kontrole od strane sustava za koje je potrebna interakcija korisnika. Zamrznuti korisnički račun moguće je vratiti u uporabu (*odmrznuti*) na zahtjev korisnika i odgovorne osobe, s time da zahtjev mora biti dokumentiran i odobren kao i kod otvaranja novog zahtjeva.

5. Zatvaranje korisničkog računa

Zatvaranje korisničkog računa iznimno je osjetljiv postupak, a osjetljivost ovisi o organizaciji upravljanja korisničkim računima. Što je upravljanje računima nekvalitetnije izvedeno, to će zatvaranje korisničkih računa biti kompliciranije.

Na primjer, ako se korisnički računi otvaraju bez dokumentiranja i na osnovu trenutnih potreba, nakon npr. godine dana više se ne zna tko ima pravo pristupa nad kojim resursima. Tada je i zatvoriti korisnički račun puno teže. Ukoliko „zatvorenom“ korisniku ostanu neka prava pristupa, put za počinjenje zlonamjernih djela mu je otvoren. Ovo je još jedan primjer zašto je kvalitetna organizacija korisničkih računa nužna.

Zatvaranje korisničkog računa odvija se kroz sljedeće faze:

- pri prekidu radnog odnosa potrebno je predati zahtjev o zatvaranju korisničkog računa zaposlenika,
- za studente je potrebno omogućiti automatsko zatvaranje korisničkog računa prilikom završetka studija,
- trećim osobama korisnički se račun zatvara nakon definiranog vremenskog perioda prilikom otvaranja računa, ili ukoliko je potrebno prije na zahtjev odgovorne osobe zadužene za suradnju s trećom stranom,

- osoba odgovorna za vođenje korisničkih računa dužna je redovito pregledavati zaprimljene zahtjeve za zatvaranjem računa te ih pravovremeno zatvoriti,
- ukoliko postoji potreba, korisniku je moguće prijevremeno zatvoriti korisnički račun bez prethodne obavijesti.

6. Prava pristupa

Dodjela prava pristupa:

- svaki korisnik prilikom otvaranja korisničkog računa, ovisno kojoj grupi korisnika pripada, ima minimalna, tzv. **osnovna** prava,
- svakom korisniku moguće je proširiti osnovna prava ukoliko za tim postoji potreba,
- dodatna prava pristupa može dodijeliti odgovorna osoba (zaposlenik zavoda koji ima pravo dodjele prava pristupa),
- za pravo pristupa osjetljivim i tajnim podacima, korisnik je dužan potpisati izjavu o pridržavanju pravila sigurnosti definiranih Pravilnikom o korištenju i zaštiti informacija i informacijskog sustava,
- pravo pristupa trećoj strani dodjeljuje odgovorna osoba; prije dodjeljivanja prava pristupa treća strana je dužna potpisati izjavu o pridržavanju pravila sigurnosti definiranih Pravilnikom o korištenju i zaštiti informacija i informacijskog sustava,
- ukoliko treća strana zahtjeva pristup osjetljivim ili tajnim podacima, potrebna je suglasnost administratora,
- sva dodijeljena prava pristupa moraju biti jasno dokumentirana,
- potrebno je omogućiti uvid u koja prava pristupa ima pojedini korisnik ili grupa korisnika,
- potrebno je omogućiti uvid tko sve ima prava nad pojedinim resursom, s mogućnošću filtriranja rezultata.

7. Osnovna (minimalna) prava korisnika

Definirati i dokumentirati minimalna prava: zaposlenika studenata treće strane

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik o sigurnosnim kopijama

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha pravilnika

Sigurnosne kopije podataka, smještene na informacijskom sustavu ZEMRIS, rade se u svrhu osiguranja podataka od vitalnog značaja za normalno funkcioniranje zavoda.

Zadatak sigurnosnih kopija je osigurati oporavak sustava na osnovi autentičnih, cjelovitih i raspoloživih prethodno pohranjenih podataka, u slučaju oštećenja nastalih povredom integriteta podataka uslijed vremenskih nepogoda, potresa, ratnih razaranja, požara, poplave ili havarije samih sustava.

2. Upravljanje sigurnosnim kopijama

Pri upravljanju sigurnosnim kopijama potrebno je pridržavati se sljedećih pravila:

- sigurnosne kopije potrebno je čuvati na izdvojenim lokacijama, različitim od lokacije originalnih podataka,
- sigurnosne kopije potrebno je zaštititi strogim sigurnosnim mjerama koje zadovoljavaju politiku fizičke zaštite sustava i prava pristupa,
- mediji sigurnosnih kopija, gdje je primjenjivo, moraju se redovno testirati kako bi se osiguralo da se na njih može računati u slučaju potrebe,
- procedure za ponovno uspostavljanje sustava moraju se redovito provjeravati i testirati kako bi se osigurala njihova učinkovitost i mogućnost izvršavanja u predviđenom vremenu,
- osobni dokumenti pohranjeni na lokalnom računalu korisnika nisu obuhvaćeni ovim pravilnikom; sigurnosne kopije tih podataka dužan je voditi korisnik.

3. Vrste sigurnosnih kopija

Definirane su 3 vrste sigurnosnih kopija:

- **Tjedne:**
  - izrada sigurnosnih kopija svih važnih podataka koje je nemoguće ili vrlo teško obnoviti (npr. ocjene studenata i sl.),
  - podatke za koje je eksplicitno navedeno da je potrebno raditi tjedne kopije.
- **Mjesečne:**
  - sigurnosne kopije radova profesora, studenata i sl. podataka,
  - podatke za koje je eksplicitno navedeno da je potrebno raditi mjesečne kopije.
- **Godišnje:**
  - izrada sigurnosnih kopija svih podataka (npr. podaci o studentima),
  - radi se jednom godišnje,

Periodički je potrebno kontrolirati ispravnost medija na kojima su pohranjene sigurnosne kopije. Ukoliko zbog istrošenosti medija, isteka roka valjanosti medija ili bilo kojeg drugog razloga postoji rizik za gubitkom podataka, odgovorna osoba dužna je kopirati sigurnosne kopije podataka na novi medij te obavljene akcije dokumentirati.

Fakultet elektrotehnike i računarstva u Zagrebu
Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Pravilnik o sklapanju i raskidu ugovora

Namijenjeno: voditelju sigurnosti
Verzija: 1.0
Datum izdavanja: 1.1.2008
Vrijedi do: 1.09.2008

1. Svrha

Svrha pravilnika o sklapanju i raskidu ugovora jest definirati procedure:

- koje je potrebno poduzeti u pogledu sigurnosti kod sklapanja ugovora o zaposlenju ili suradnji,
- koje definiraju koje točke sigurnosti ugovor o zaposlenju ili suradnji mora referencirati,
- koje definiraju na koji način kvalitetno provesti raskid ugovora.

Cilj navedenih procedura je smanjenje rizika od ljudske pogreške, krađa, prijevara i zlouporabe resursa informacijskog sustava ZEMRIS.

2. Procedure sklapanja ugovora

Odgovorne osobe pri sklapanju ugovora o zaposlenju ili suradnji dužne su provesti mjere sigurnosti definirane sljedećim procedurama:

I. Provjera

Provjera (eng. *screening*) u svrhu kontrole potencijalnih zaposlenika, ulagača ili poslovnih partnera jedna je od preventivnih metoda kojima organizacija može djelovati na sigurnost informacijskog sustava. Odgovorna osoba dužna je provesti ili inicirati provjeru i ispitivanje nad potencijalnim zaposlenikom. Proces provjere i ispitivanja mora uzeti u obzir sva prava i zakonske odredbe privatnosti, te ukoliko je dopušteno uključiti sljedeće:

- raspoložive reference karaktera, poslovanja itd.,
- pregled dostupnih CV-a, kontrola dostavljenih podataka,
- potvrde o školovanju i profesionalnim kvalifikacijama,
- dokazi identiteta (putovnica),
- da li je osoba kazneno gonjena itd.

Prikupljene podatke potrebno je dokumentirati kao **povjerljive podatke**, te prema njima napraviti procjenu da li postoji mogućnost zlouporabe informacijskog sustava od strane potencijalnog zaposlenika.

II. Uvjeti zaposlenja i ugovor odgovornosti

Prije zaposlenja radnika, sklapanja partnerstva s drugom organizacijom ili uključivanja u posao treće strane neophodno je u ugovor uključiti dio koji sve strane obavezuje na pridržavanje pravila definiranih sigurnosnom politikom.

Ugovor treba sadržavati dodatak s pojašnjenjima i stavovima:

- da svaki zaposlenik, partner ili treća strana, prije dobivanja prava pristupa imovini organizacije, mora potpisati ugovor o povjerenju,
- o zakonskim pravima i odgovornostima svakog zaposlenika, korisnika i poslovnog partnera,
- o odgovornostima organizacije o čuvanju i rukovanju informacijama o zaposlenicima,
- o odgovornostima u slučaju obavljanja posla izvan radnog vremena ili izvan prostorija organizacije (npr. kod kuće),
- o akcijama koje je potrebno poduzeti ukoliko se utvrdi nepridržavanje pravila definiranih sigurnosnom politikom.

III. Odgovornosti rukovoditelja

Rukovoditelji mora zahtijevati i inzistirati na pridržavanju pravila definiranih sigurnosnom politikom od strane zaposlenika, korisnika, poslovnih partnera i treće strane. Njihova je zadaća sve zaposlenike, korisnike, partnere i treće strane:

- pravilno i jasno informirati o njihovim ulogama u provedbi sigurnosti, te o njihovim odgovornostima prije dodjeljivanja prava pristupa osjetljivim informacijama,
- pružiti im uvid u obliku smjernica o tome što se očekuje od njih ovisno o njihovim ulogama,
- motivirati da se pridržavaju pravila definiranih sigurnosnom politikom,
- osigurati potrebnu razinu svijesti o potrebi za sigurnošću, ovisno o ulogama.

IV. Edukacija o informacijskoj sigurnosti

Svi zaposlenici organizacije, i ukoliko se ukaže potreba, partneri i osoblje treće strane moraju proći odgovarajuću obuku o svijesti o informacijskoj sigurnosti, te pravovremeno biti upoznati s dopunama ili promjenama u sigurnosnoj politici organizacije.

Osnovni pojmovi o sigurnosti i obuka o svijesti o informacijskoj sigurnosti moraju biti prezentirani zaposlenicima, partnerima i trećoj strani prije dodjeljivanja prava pristupa informacijama. Edukacija korisnika mora biti s skladu s ulogom, sposobnošću i odgovornosti pojedinca.

3. Raskid ugovora

Postupak raskida ugovora važno je pravovremeno i kvalitetno obaviti kako se korisniku ne bi pružila mogućnost obavljanja zlonamjernih radnji.

Prilikom raskida ugovora potrebno je zadovoljiti sljedeće sigurnosne kontrole:

- najvažniji dio raskida ugovora – **ukloniti sva prava pristupa** resursima zavoda; ukoliko je moguće potrebno je prava pristupa ukloniti automatski pomoću posebnih programa (pristup programskim resursima),
- svi ključevi, pametne kartice i sl. također moraju biti vraćeni,
- svu imovinu koju je dobio na korištenje korisnik mora vratiti u posjed zavoda,
- vraćena imovina postaje vlasništvom zavoda (za nju postaje odgovorna glavna odgovorna osoba),
- svi postupci vezani uz raskid ugovora (npr. vraćena imovina) moraju biti dokumentirani.

Dodatak M – Dopune

Primjer sigurnosne politike, dan u prethodnim poglavljima, potrebno je dopuniti sljedećim dokumentima:

- Informacijska sigurnost i zakonodavstvo;
- Pravilnik o kriptografskim metodama;
- Kako postupiti u slučaju napada (za korisnike);
- Politika konfiguriranja poslužitelja;
- Politika zaštite sustava kod ugovora s trećom stranom;
- Obrascima i ugovorima o pridržavanju pravila definiranih sigurnosnom politikom ili nekih njenih dijelova;