Sigurnosna politika informacijskih sustava za članice CARNeta

(prijedlog)

Hrvatska akademska i istraživačka mreža – CARNet

prosinac, 2003.

--

Sadržaj

Potreba donošenja sigurnosne politike

Čemu sigurnosna politika?

Informacijske tehnologije svakim danom sve više doprinose efikasnom funkcioniranju akademske i istraživačke zajednice. Korisničke aplikacije, elektronička pošta, web i mreža koja funkcionira ispod toga imaju sve veću važnost u učenju, istraživanju i upravljanju.

Informacijski sustavi, kao i ljudi koji ih koriste i administriraju nisu uvijek pouzdani. Niz uzroka može dovesti do nedostupnosti ili gubitka informacija u elektroničkom obliku: od prirodnih katastrofa, kvara na opremi, grešaka u softveru, do ljudskih postupaka. Ljudski faktor može djelovati izvana ili iznutra, a šteta može biti izazvana slučajno ili namjerno. Radi svega toga treba se organizacijski pripremiti za slučaj incidenata.

Ustanove članice CARNeta na umreženim računalima čuvaju informacije kojima pristup mora biti ograničen, bilo da se radi o knjigovodstvenim podacima, rezultatima istraživanja ili samo o privatnim porukama elektroničke pošte. U svakom slučaju informacijske sustave treba zaštiti kako bi osigurali povjerljivost, integritet i dostupnost podataka.

Čak i ustanove članice koje vjeruju da njihovi sustavi ne sadrže informacije koje bi bile vrijedne brige i dodatnih ulaganja, dužne su brinuti o sigurnosti kako njihova računala ne bi bila odskočna daska za napade na tuđe sustave. Internet je nedjeljiva cjelina, te brigom o sigurnosti ustanove i CARNeta doprinosimo ukupnoj sigurnosti na Internetu.

Internet je postao komunikacijski kanal za obavljanje poslovnih transakcija, a na njega se sve više prenose i političke bitke. Umjesto načela samoregulacije i apeliranja na ponašanje u skladu s netiketom, što je bilo dovoljno u ranoj fazi, sve se više nastoji zakonski regulirati ponašanje na Internetu i omogućiti progon prekršitelja bez obzira na nacionalne granice. Stoga se i naša akademska mreža mora pripremiti za nova vremena, a donošenje sigurnosne politike je svakako jedan od koraka u tom smjeru.

Koje ciljeve treba postići sigurnosna politika?

Sigurnosna politika dio je sustava upravljanja sigurnošću informacijskih sustava. Njezina je svrha da definira prihvatljive i neprihvatljive načine ponašanja, da jasno raspodijeli zadatke i odgovornosti, te da propiše sankcije u slučaju nepridržavanja.

Osnovni dokument, koji postavlja opće principe, prate dokumenti koji definiraju pravila za specifična područja (npr. metode enkripcije, pravila administriranja poslužitelja, pohrane podataka itd.). Ovi dokumenti su radi svoje praktične naravi ovisni o promjenama u tehnologiji i organizaciji, pa će se vjerojatno češće mijenjati i dorađivati.

Sigurnosna politika treba biti primjenjiva, kako ne bi ostala mrtvo slovo na papiru. To znači da mora biti pisana jednostavnim i razumljivim jezikom i prilagođena lokalnoj kulturi, a istovremeno usklađena sa zakonima i propisima koji vrijede u državi. Za njezino provođenje potrebna je podrška uprave, a s njezinim principima treba upoznati sve administratore i korisnike informacijskih sustava. Zato nakon prihvaćanja politike treba uložiti napor u obrazovanje korisnika.

Nove djelatnike treba prilikom zapošljavanja upoznati s pravilima propisanim politikom, a studente pri otvaranju korisničkih računa.

Ustanova je obavezna objaviti na javnim web stranicama Politiku prihvatljivog korištenja, kako bi svi korisnici bili upoznati s njome.

Zaposlenike treba upoznati i s dodatnim dokumentima, na primjer pravilima za korištenje elektroničke pošte, pravilima za korištenje zaporki ili pravilima o čuvanju povjerljivih informacija.

Prateći dokumenti koji se bave razradom konkretnih poslova i mogu sadržavati povjerljive informacije objavljuju se na internom webu ili se dostavljaju samo određenim djelatnicima, koji radi prirode svoga posla moraju biti s njima upoznati.

Kakva treba biti sigurnosna politika u akademskoj sredini?

Sigurnosne politike u poslovnom svijetu iznimno su restriktivne. Pojednostavljeno rečeno, sve je zabranjeno, osim onog što je izričito dozvoljeno. A dozvoljeno je samo ono što je neophodno za obavljanje posla.

Akademska zajednica pripada otvorenoj kulturi, okrenuta je komuniciranju, istraživanju, samorazvoju i učenju. Sveučilište brani svoje slobode i nezavisnost, ne trpi restrikcije. Stoga će i sigurnosna politika biti liberalnija.

Pojedincu se ostavlja mogućnost izbora, ali sloboda se mora uravnotežiti osobnom odgovornošću. Težište provođenja sigurnosne politike treba biti u većoj mjeri na obrazovanju, nego na sužavanju izbora i sankcioniranju.

U pojedinim dijelovima sigurnosna pravila će biti jednaka kao u komercijalnom okruženju. Postupanje s povjerljivim informacijama podliježe jednakim pravilima u banci i na sveučilištu, a akademska sloboda nikoga ne stavlja iznad zakona, morala i pravila pristojnog ponašanja.

Lokalizacija

CARNet donosi ovaj prijedlog sigurnosne politike za ustanove članice, kako bi ih potaknuo da i same donesu svoje vlastite pravilnike.

Ustanove mogu dorađivati i prilagođavati pravila koja su ovdje napisana, kako bi njihova vlastita sigurnosna politika bila primjenjiva u specifičnim uvjetima. Ustanove mogu dodavati nova pravila, u skladu s uslugama koje pružaju korisnicima, ali ne smiju zanemariti osnovne principe sadržane u "Politici prihvatljivog korištenja" koji vrijede za cijeli CARNet.

Ne očekujemo da će ustanove doslovno prepisati ovaj dokument, iako ga mogu usvojiti s minimumom prepravki. Bitno je da se poštuju osnovna načela, a istovremeno politika prilagodi lokalnoj kulturi, napiše na način koji će ljudima biti razumljiv i prihvatljiv.

Na kraju će trebati poraditi na primjeni pravila iz sigurnosne politike, a to će zahtijevati promjene u načinu razmišljanja i rada, što neće uvijek proći bez otpora.

Pri tom treba biti strpljiv i uvjerljiv, umjesto grube sile i sankcija bolje je ulagati vrijeme i sredstva u obrazovanje ljudi, te na konkretnim primjerima pokazivati zašto su sigurnosna pravila važna.

Reference i međunarodni standardi

U svijetu ne postoji standard sigurnosne politike za akademsku zajednicu.

Napravljeni su standardi za komercijalno okruženje, na primjer ISO standard 17799. On je trenutno u fazi intenzivnog preispitivanja, te se uskoro očekuje nova revizija. Konkretno, to znači da se ne može dobiti certifikat o usklađenosti sigurnosne politike sa ISO 17799 standardom.

U SAD je objavljen prijedlog standarda, Draft: Internet Security Policy, A Technical Guide, koji se može pronaći na web stranicama njihova nacionalnog instituta za standarde, na adresi http://www.nist.org

ISO standard može se kupiti u Državnom zavodu za normative i mjeriteljstvo, u Zagrebu. Obrazovne institucije imaju pravo na povlaštenu cijenu.

Ustanove mogu pri donošenju vlastite sigurnosne politike koristiti ova dva standarda i učiti iz njih, iako su njihova pravila previše stroga i primjerenija nekoj banci ili obavještajnoj agenciji. No pojedini dijelovi su primjenjivi, te su iskorišteni i pri izradi ovog dokumenta. Ustanove koje imaju potrebu za strožom i razrađenijom sigurnosnom politikom neka svakako prouče ove standarde.

NISTov standard je fleksibilniji i omogućuje da se razdvoje pravila za pojedine skupine korisnika, prema stupnju rizičnosti i kritičnosti informacija koje treba štititi. Na primjer, pravila za korištenje elektroničke pošte bit će slobodnija ako se odnose na studente, a stroža kada se radi o zaposlenima.

Spomenimo i RFC1855 – Netiquete Guidelines, dokument koji navodi pravila pristojnog ponašanja na Internetu, koji je nastao u vrijeme samoregulacije, kada je bilo dovoljno apeliranje na svijest korisnika Interneta. No njegova je vrijednost neprolazna, tako da ćemo ga prevesti i objaviti na portalu za CARNetove sistem inženjere.

Svjesni činjenice da se radi o velikom i zahtjevnom poslu, koji je nužna stepenica u razvoju akademske mreže, CARNet i SRCE pružiti će ustanovama svu moguću podršku pri donošenju i primjeni sigurnosne politike.

Sigurnosna politika ustanove članice CARNeta (prijedlog)

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu koja se nalazi u prostorima Ustanove.
- Administratore informacijskih sustava
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

Organizacija upravljanja sigurnošću

Ključna stvar pri provođenju sigurnosne politike informacijskog sustava jest da se u svakom trenutku točno zna što je čiji posao i tko za što odgovara. Stoga je potrebno raspodijeliti zaduženja i obrazovati korisnike, te oformiti stručna tijela za upravljanje sigurnošću.

Ljudi koji se u radu koriste računalima dijele se na korisnike i davatelje informacijskih usluga.

Korisnici informatičkih usluga

Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže.

Svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike.
- Izbor kvalitetne zaporke i njezina povremena promjena
- Prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To znači da, na primjer, moraju od davatelja usluga zatražiti da uspostave automatsku pohranu (backup) važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

Glavni korisnik

Ukoliko ustanova koristi aplikacije za obradu podataka, na primjer računovodstvene programe, radi poboljšanja sigurnosti jedna osoba imenuje se glavnim korisnikom. U navedenom primjeru voditelj računovodstva bio bi glavni korisnik.

Dok zaposlenici koji unose podatke odgovaraju za vjerodostojnost tih podataka, glavni je korisnik odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba.

Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.

Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava. Na ustanovama članicama CARNeta to su sistem inženjer i članovi njegova tima. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

Specijalisti za sigurnost

Ustanove mogu za brigu o sigurnosti i pomoć pri rješavanju incidenata koristiti pomoć CARNeta.

Usprkos tome, preporučuje se imenovanje i obrazovanje pojedinaca čija je zadaća briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

Osoba čije je prvenstvena briga sigurnost informacijskih sustava je Voditelj sigurnosti (engl. CSO, Chief Security Officer). Poželjno je da Voditelj sigurnosti bude stručan, ali da istovremeno posjeduje sposobnost za vođenje ljudi i da je komunikativan.

Njegova je briga ukupna sigurnost informacijskih sustava. To uključuje fizičku sigurnost, pri čemu će surađivati s zaposlenicima poput portira, čuvara i slično. Voditelj sigurnosti piše pravilnike, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera, te sudjeluje u razvoju softvera, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

Ako Ustanova zapošljava više stručnjaka za računarstvo, oformiti će Ekipu za hitne intervencije i obučiti je za postupanje u slučaju incidentnih situacija. Ekipu čine specijalisti različitih usmjerenja, na primjer za mrežu, Unix, Microsoft Windowse, baze podataka itd. Ustanova treba u tom slučaju razraditi procedure za postupanje u incidentnim situacijama, te obučiti članove Ekipe za hitne intervencije kako bi mogli izvršiti istragu, te informacijski sustav što prije vratiti u redovno stanje.

Primjer procedura za rješavanje incidenata dan je u pratećem dokumentu pod nazivom "Pravilnik o rješavanju sigurnosnih incidenata".

Ustanova treba izraditi i održavati kontakt listu s imenima, brojevima telefona, e-mail adresama osoba kojima se prijavljuju incidenti, od kvarova opreme, sporosti ili nedostupnosti mrežnih usluga i podataka, do povreda pravila sigurnosne politike ili zakonskih odredbi.

Administriranje računala

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera. Ukoliko napredni korisnici žele sami administrirati svoje osobno računalo, neka potpišu izjavu o tome, nakon čega za njih vrijede sva pravila za administriranje računala.

Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti.

Administratori su dužni prijaviti incidente specijalistu za sigurnost, te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNetovu CERT-u.

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Da bi ih ustanova obavezala na poštivanje tih pravila, neka potpišu Izjavu o čuvanju povjerljivih informacija, čiji je predložak dan među pratećim dokumentima.

Upravljanje mrežom

Ustanove koje posjeduju razgranatu mrežu i svoje vlastite mrežne i komunikacijske uređaje dužne su razraditi pravila koja određuju tko upravlja mrežom, konfigurira mrežne uređaje, dodjeljuje adrese, kreira virtualne LAN-ove itd.

Osim što se odgovornost za rad mreže dodjeljuje određenim ljudima, mogu se propisati i procedure za priključivanje računala u mrežu, odrediti obrasce kojima se izdaje odobrenje za priključenje računala na mrežu i dodjeljuje im se adresa.

Djelatnik zadužen za upravljanjem mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.

Ukoliko je podržan rad na daljinu, na primjer kada se djelatnicima dopušta da sa kućnog računala ažuriraju podatke, potreban je poseban pravilnik s kojim moraju biti upoznati svi koji rade na daljinu. Mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove, s obzirom na mogućnost da ga koriste neautorizirane osobe, članovi obitelji i slično. Povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Ustanova je obavezna razraditi pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Ne smije se dozvoliti da oni po svom nahođenju priključuju računala na mrežu ustanove, radi opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnog prometa, prikupljanja informacija itd. Ustanova može odrediti priključna mjesta, na primjer u predavaonicama, gdje je dozvoljeno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se sa tog segmenta mreže dopre do ostalih računala na ustanovi.

Ukoliko ustanova koristi bežičnu mrežu, mora osigurati da se ne može bilo tko priključiti na privatnu mrežu i snimati promet. To se postiže metodama enkripcije i autentikacije uređaja i korisnika, koji se moraju propisati u zasebnom dokumentu.

Radi zaštite povjerljivih informacije pri prijenosu mrežom, poželjno je da takav promet bude kriptiran. Ustanova će u tom slučaju izdati pravilnik u kojem definira vrstu enkripcije, obvezan softver, procedure za dodjelu i čuvanje kriptografskih ključeva i slično.

Instalacija i licenciranje softvera

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, ustanova zadužuje jednu ili više odgovornih osoba za instaliranje softvera i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom, mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.

Sve korisnike treba obavezati na poštivanje autorskih prava, na primjer potpisivanjem izjave o tome da upoznati s Politikom prihvatljivog korištenja i da je prihvaćaju. Na taj način ustanova odgovornost za eventualno kršenje zakona prebacuje na nesavjesnog korisnika.

Povjerenstvo za sigurnost informacijskih sustava

Kako bi se osiguralo upravljanje sigurnošću, poželjno je oformiti Povjerenstvo za sigurnost sastavljeno od predstavnika uprave i specijalista tehničara (na primjer voditelj sigurnosti, CARNet koordinator, prodekan, glavni korisnik baze podataka koja sadrži povjerljive informacije itd.).

Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njeno poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista. Povjerenstvo daje odobrenje za provođenje istrage u slučaju incidenata.

Povjerenstvo podnosi izvještaj o stanju sigurnosti upravi Ustanove, te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika.

Fizička sigurnost

Prostor na ustanovi dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni, te prostore u koje pristup imaju samo grupe zaposlenih, ovisno o vrsti posla koji obavljaju.

Ustanova je dužna sastaviti popis osoba koje imaju pristup u zaštićena područja, a porta mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Sigurne zone

Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava, ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.

Ustanova je dužna održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone.

U pravilu su to samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme. Stoga je poželjno je administratorima osigurati radni prostor odvojeno od prostorija u kojima je smještena kritična oprema.

Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, što znači da električne instalacije moraju biti izvedene kvalitetno, da se koriste uređaji za neprekidno napajanje, a po potrebi i generatori električne energije.

Treba predvidjeti i druge moguće probleme, poput poplava, požara i slično, te poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Vanjske tvrtke

Povremeno se mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.

Ustanova može u ugovore s vanjskim tvrtkama ugraditi odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.

Ugovorom će se regulirati pristup, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu treba obavezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.

Ustanova može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.

Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video nadzor.

Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Ustanova može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Ustanove radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Ustanovu.

Ustanova zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

Sigurnost opreme

Klasifikacija računalne opreme

Ustanova dijeli svu opremu u grupe prema zadaćama:

- Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.).
- Intranet je privatna mreža Ustanove, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.
- Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).

Poželjno je da Ustanova s vremenom izradi sigurnosnu politiku za svako od navedenih područja, koje će dati konkretne upute administratorima kako zaštiti sustav. Posebno je osjetljivo područje koje nazivamo extranet, jer se tu otvara prolaz u zaštićenu mrežu

korisnicima koji su na putu, kod kuće, ili poslovnim partnerima. Potrebno je izraditi poseban pravilnik za extranet u kojem se reguliraju prava i obaveze, a s vanjske tvrtke kojima se dopušta pristup računalima i podacima u intranetu treba ugovorom obavezati na poštivanje sigurnosnih pravila i čuvanje povjerljivosti informacija.

Podjela opreme prema vlasništvu

U prostorijama Ustanove nalazi se i oprema CARNeta ili Ministarstva znanosti i tehnologije, koja je dana na korištenje Ustanovi.

Ustanova je obavezna održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.

Ustanova brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Manirom dobrog gospodara oprema se čuva od oštećivanja, otuđenja.

Ustanova je dužna osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Ustanovi.

Odgovornost za računalnu opremu

Za fizičku sigurnost opreme odgovoran je rukovoditelj ustanove. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Ustanova je dužna razraditi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme. Na porti treba provjeriti da li oprema koja se iznosi ima potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

Osiguranje neprekidnosti poslovanja

Kako bi se sačuvali podaci u slučaju nezgoda, poput kvarova na sklopovlju, požara, ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporučuje se izrada više kopija, koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Procedure za izradu rezervnih kopija treba razraditi u zasebnom dokumentu. Potrebno je zadužiti konkretne djelatnike za izradu i čuvanje kopija informacija, te ih obavezati na čuvanje povjerljivosti informacija.

Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi, u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Ustanova zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim računalima, te nad načinom korištenja računala.

Nadzor se smije provoditi radi:

- Osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa.

- Provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident.
- Provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je ustanova za to ovlastila.

Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, te se one mogu koristiti u stegovnom ili sudskom postupku.

Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Ustanove i priključena je u mrežu CARNet, na sav instalirani softver, te na sve mrežne servise.

Pravila su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Provođenje

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Isto vrijedi i za aministratore računala i pojedinih servisa, koji su dužni specijalistima za sigurnost pomagati pri istrazi.

Pristup uključuje:

- Pristup na razini korisnika ili sustava svoj računalnoj opremi
- Pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Ustanove, ili oprema Ustanove služi za njezin prijenos.
- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Ustanove

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu uskratiti prava korištenja CARNetove mreže i njezinih servisa.

Prateći dokumenti

S razvojem informatike na ustanovi i porastom ovisnosti o njezinom ispravnom funkcioniranju, javiti će se potreba da se generička sigurnosna politika dopuni pratećim dokumentima, u kojima se definiraju pravila za pojedina područja rada. Dok bi generička politika trebala biti dovoljno općenita kako se ne bi morala često mijenjati, prateći pravilnici pisani su kao upute za rješavanje konkretnih problema i mogu se češće mijenjati.

Primjer je takozvana Backup policy, odnosno Pravila za izradu kopija podataka. Taj će dokument pratiti lokalne potrebe i definirati upute za tehničare prilagođene tehnološkoj osnovi kojom raspolaže ustanova. Kada se nabavi nova oprema za spremanje podataka, bit će potrebno prepraviti dokument, kako bi se uskladio s novim mogućnostima spremanja podataka.

Uz ovaj prijedlog Sigurnosne politike za ustanove prilažemo i nekoliko primjera pratećih pravilnika, kako bismo ustanovama olakšali njihovu izradu.

Prilozi:

Pravilnik o rukovanju zaporkama

Pravilnik o korištenju elektroničke pošte

Pravilnik o antivirusnoj zaštiti

Pravilnik o zaštiti od spama

Pravilnik o rješavanju sigurnosnih incidenata

Pravilnik o rukovanju povjerljivim informacijama

Pravilnik o rukovanju zaporkama (prijedlog)

Svrha

Prosječan korisnik nerijetko smatra kako ne mora brinuti o sigurnosti jer njegovo 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. Lanac puca na najslabijoj karici. Stoga je svaki korisnik dužan izborom zaporke i njezinom povremenom promjenom doprinositi zaštiti ukupnog sustava.

Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dekriptirati jednostavne zaporke, dok u isto vrijeme većina ljudi ne može pamtiti složene zaporke dugačke osam znakova.

Doseg

Svi zaposlenici Ustanove, suradnici i studenti koji u svome radu koriste računala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

   Kratku zaporku lakše je probiti. Stoga neka minimalna dužina zaporke bude šest znakova, ali preporučujemo korištenje još dužih zaporki.

2. Ne koristiti riječi iz rječnika

   Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

   Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. 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 zaporki.

6. Tajnost zaporke

   Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.

   Hakeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja probleme i bez poznavanja korisničkih zaporki.

7. Čuvanje zaporke

   Zaporke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. 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.

8. Administriranje zaporki

   Na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

   Administratori su dužni konfigurirati autentikaciju tako da zaporke zastare nakon 90 dana, te onemogućiti korištenje zaporki koje su već potrošene, ako sustav to dozvoljava.

   Prilikom provjere sustava sigurnosni tim može ispitati da li su korisničke zaporke u skladu s navedenim pravilima.

Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. Ustanova je obavezna odgojno djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.

U slučaju ponovljenog ignoriranja ovih pravila Ustanova može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

Pravilnik o korištenju elektroničke pošte (prijedlog)

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-mailom na Ustanovi zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.

Protokol koji se koristi za prijenos elektroničke pošte, SMTP ili Simple Mail Transport Protocol, nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.

Stoga ćemo se na početku ukratko pozabaviti problemima koji mogu nastati pri korištenju elektroničke pošte.

1. Nesigurnost protokola
    - Poruke putuju kao običan tekst, otvorene kao na razglednici, te ih je lako presresti i pročitati, ili čak izmijeniti sadržaj.
    - Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.
    - Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.
2. Nezgode
    - Uvijek je moguće pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu. Time može nastati nepopravljiva šteta – ne možete zaustaviti poruku koja je već otišla. Ako se umjesto Reply pritisne Reply All, poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
    - Česta je pogreška i kada se pokupi pogrešna adresa iz adresara.
    - Neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.
3. Nesporazumi
    - Ljudi su skloni pisati e-mail poruke na ležerniji, opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.
    - Iza vašeg imena u e-mail adresi nalazi se ime ustanove. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. Otkrivanje informacija

- Poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi
  - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki
  - nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke
  - slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply)
- Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.
- U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Ustanova se obavezuje čuvati povjerljivost takvih poruka, ali to ne može garantirati ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

- Velika količina poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih i zabavnih poruka.
- Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac ("pomozite nesretniku kojem treba operacija", "otvorite račun kako bi svrgnuti diktator mogao izvući novac iz nestabilne afričke države"...). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a "Hoax recognizer"
- Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Ustanova će filtirati spam na poslužitelju elektroničke pošte, ali je obaveza korisnika da sami ne šalju takve poruke.

6. Povreda autorskih prava

- Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora.
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i Ustanovu.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite.

- Pridržavajte se netikete, pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Ustanova zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog djelatnika, rukovodilac zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.

Pri prestanku radnog odnosa, rukovodilac je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa.

Studenti imaju pravo besplatnog korištenja e-maila za vrijeme trajanja studija. Nakon odlaska s fakulteta njihov se korisnički račun zatvara.

Na koga se odnose pravila korištenja e-maila

Pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike, i studente koji imaju otvoren korisnički račun na poslužitelju Ustanove.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila Ustanova može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Pravilnik o antivirusnoj zaštiti (prijedlog)

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.

Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg računala, kako bi hackeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza ustanove, administratora računala i svakog korisnika.

Ustanova propisuje da je zaštita od virusa obavezna i da se provodi na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti sistem inženjera.

Nepridržavanje

Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu, te na taj način izazove štetu, bit će stegovno kažnjen.

Pravilnik o zaštiti od spama (prijedlog)

Svrha

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i tvrtke, jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, ili su prijevara, nastoje pobuditi samilost kako bi se izvukao novac (enlg. hoax). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer.

Pravila za administratore

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi.

Prva mogućnost jest da se definira ulazni filter koji će prilikom primanja poruke konzultirati baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih spamera. Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao spam spremati na određeno vrijeme u karantenu.

Treću razinu zaštite određuju sami korisnici. Poruke dobijaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Informatičar zadužen za sigurnost će obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj.

Upozorenja na viruse su često lažna i šire zablude.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći

računalnu opremu koja pripada ustanovi.

Nepridržavanje

Protiv korisnika koji se oglušuju o pravila prihvatljivog korištenja i šalju masovne neželjene poruke biti će pokrenut stegovni postupak.

Pravilnik o rješavanju sigurnosnih incidenata (prijedlog)

Svrha

Svrha je ovog dokumenta da ustanovi obavezu prijavljivanja sigurnosnih incidenata, te da razradi procedure za provođenje istrage.

Prijava incidenta

Svaki zaposlenik, student ili suradnik Ustanove dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Ustanova treba izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu računala i servisa, te obrazac za prijavu incidenta. Kontakt listu treba podijeliti svim zaposlenima i objaviti je na internim web stranicama Ustanove.

Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.

Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina, kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr

Procedure za rješavanje incidenata

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedozvoljen način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (na pr. dokumenata ili e-mail poruka).

Daljnju istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom ustanove, uz poštivanje slijedećih pravila:

- Istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje
- Najprije se napravi kopija zatečenog stanja (na pr. na traku, CD...), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd).
- Dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.

- O istrazi se napiše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

Ustanova može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Sankcije

Svrha je istrage da se odredi uzrok nastanka problema, te da se iz toga izvuku zaključci o tome kako spriječiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bio ljudski faktor, protiv odgovornih se mogu poduzeti sankcije.

Ustanova može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.

Ukoliko je incident izazvao zaposlenik vanjske tvrke, Ustanova može zatražiti od vanjske tvrtke da ga ukloni sa liste osoba ovlaštenih za obavljanje posla na ustanovi. U slučaju teže povrede pravila sigurnosne politike, Ustanova može raskinuti ugovor s vanjskom tvrtkom.

Pravilnik o upravljanju povjerljivim informacijama (prijedlog)

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01. Uskoro se očekuje i zakon o zaštiti osobnih podataka.

Prema vrsti tajnosti informacije dijele se na vojnu, državnu, službenu, poslovnu i profesionalnu tajnu.

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.

Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Ustanovi ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.)

Profesionalna tajna odnosi na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u referadi, osoba koje unose podatke u baze podataka o studentima ili sistem administratora poslužitelja koji u nekim situacijama može doći u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji izvana dolaze u Ustanovu s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Ustanova proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave (službena, državna ili vojna tajna).

Dokumenti koji se smatraju povjerljivima moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.

Javnima se smatraju sve informacije koje nisu označene kao povjerljive. Izuzetak su osobne informacije, za koje se podrazumijeva da su povjerljive i ne treba ih posebno označavati.

Pravila za čuvanje povjerljivosti odnose se na informacije bez obzira na to u kom su obliku: na papiru, u elektroničkom obliku, zabilježene ili usmeno prenesene, ili su objekti poput maketa, slika itd.

Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je u rukovoditelj Ustanove, koji će izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike Ustanove i vanjske suradnike koji dolaze u doticaj sa osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Čuvanje povjerljivih informacija

Povjerljive informacije, tiskane na papiru ili u elektroničkom obliku, snimljene na neki medij za pohranu podataka, čuvaju se u zaključanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ograničen pristup.

Pristup povjerljivim informacijama regulira se izradom liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

Informacije o zaposlenicima

Socijalni inženjering je metoda koju primjenjuju hackeri kako bi prikupili informacije potrebne za provalu na računala.

Ustanova može informacije o zaposlenima koje se smatraju javnima objaviti na svojim web stranicama. Javnim informacijama smatraju se:

- ime i prezime
- posao koji zaposlenik obavlja
- broj telefona na poslu
- službena e-mail adresa

Na upite o zaposlenicima davati će se samo informacije objavljene na internim web stranicama. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti odobe kojoj podaci pripadaju (na pr. adresa stana, broj privatnog telefona, podaci o primanjima, porezu, osiguranju itd.)

Povjerljive informacije u načelu se ne daju se telefonom jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik Ustanove će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Prenošenje povjerljivih informacija

Informacije koje su klasificirane kao povjerljive zahtijevaju posebne procedure pri slanju i prenošenju.

Povjerljive informacije ne šalju se običnom poštom, već kurirskom. Na odredištu se predaju u ruke osobi kojoj su upućeni, što se potvrđuje potpisom.

Ako se povjerljive informacije šalju elektronički, na primjer kao poruke elektroničke pošte, tada se moraju slati kriptirane.

Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu u Ustanovu ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju Ustanovi smiju se kopirati samo uz dozvolu osobe koja ih je proglasila povjerljivim, odnosno uprave. Kopija se numerira i o njenom izdavanju vodi se evidencija kao i za original s kojeg je proizvedena.

Osoblje koje poslužuje uređaje za kopiranje treba obučiti i obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

Uništavanje povjerljivih informacija

Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (spaljivanjem, usitnjavanjem, prešanjem).

Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno prebriše sadržaj diska.

Nepridržavanje

Zaposlenici i suradnici koji dolaze u dodir s klasificiranim informacijama potpisuju izjavu o čuvanju povjerljivosti informacija.

Protiv zaposlenika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut stegovni postupa, a može ih premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti će se ugovor. Stoga ustanova treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.