Sigurnosna politika informacijskih sustava u Gradskoj i Sveučilišnoj knjižnici u Osijeku

(prijedlog)

Katica Mihelić, rujan, 2005.

Sadržaj

Potreba donošenja mjera sigurnosne politike 2

Sigurnosna politika informacijskih sustava u Gradskoj i sveučilišnoj knjižnici u Osijeku 4

Prilog 1: Pravilnik o rukovanju zaporkama 12

Prilog 2: Pravilnik o korištenju elektroničke pošte 14

Prilog 3: Pravilnik o antivirusnoj zaštiti 17

Prilog 4: Pravilnik o zaštiti od spama 18

Prilog 5: Pravilnik o zaštiti od *špijunskih* i *nametnih* programa 19

Prilog 6: Pravilnik o izradi kopija podataka 20

Prilog 7: Pravilnik o rješavanju sigurnosnih incidenata 21

Prilog 8: Pravilnik o upravljanju povjerljivim informacijama 23

Prilog 9: Pravilnik o korištenju informacijskih sustava Knjižnice za vanjske suradnike i Članove Knjižnice 26

Potreba donošenja mjera 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 sigurni. Niz je uzroka koji mogu dovesti do nedostupnosti ili gubitka informacija u elektroničkom obliku: prirodne katastrofe, kvarovi na opremi, greške u softwareu, ljudski postupci. Čovjek može djelovati izvana ili iznutra, a šteta može biti izazvana slučajno ili namjerno. Radi svega toga treba se organizacijski pripremiti za slučajeve incidenata.

Ustanove članice CARNeta na umreženim računalima čuvaju informacije kojima pristup mora biti ograničen, bilo da se radi o knjigovodstvenim podacima, bazama podataka, 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 ako se vjeruje da sustavi ne sadrže informacije koje bi bile vrijedne brige i dodatnih ulaganja, dužnost je ustanove brinuti o sigurnosti kako njihova računala ne bi bila odskočna daska za napade na tuđe sustave. Internet je nedjeljiva cjelina, pa brigom o sigurnosti informacijskih sustava Gradske i sveučilišne knjižnice u Osijeku doprinosimo ukupnoj sigurnosti na Internetu.

Umjesto načela samoregulacije i apeliranja na ponašanje u skladu s *netiquetom*, 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 mreža mora pripremiti za nova vremena, a donošenje mjera 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 definirati prihvatljive i neprihvatljive načine ponašanja, jasno raspodijeliti zadatke i odgovornosti, te propisati sankcije u slučaju njihova nepridržavanja.

Osnovni dokument o sigurnosti, koji postavlja opće principe, prate drugi dokumenti koji definiraju pravila za specifična područja (npr. pravila o rukovanju zaporkama, o uporabi elektroničke pošte, pohrani podataka i slično). Ta pravila su ovisna o promjenama u tehnologiji i organizaciji, te će se vjerojatno češće mijenjati i dorađivati.

Kako ne bi ostala mrtvo slovo na papiru, sigurnosna politika treba biti primjenjiva. 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 njenog prihvaćanja treba uložiti napor u obrazovanju korisnika.

Prilikom zapošljavanja nove djelatnike treba upoznati s pravilima propisanim sigurnosnom politikom, a nove članove prilikom učlanjenja u Knjižnicu.

Nakon usvajanja, dokument o *Sigurnosnoj politici informacijskih sustava u Gradskoj i sveučilišnoj knjižnici u Osijeku* (u daljnjem tekstu Knjižnica), bit će objavljen na javnim web stranicama Knjižnice.

Sve korisnike treba upoznati i sa svim dodatnim dokumentima koji su u prilogu ovog dokumenta.

Ako prateći dokumenti koji se bave razradom konkretnih poslova sadrže povjerljive informacije, objavljuju se samo na internom webu ili ih se dostavlja određenim djelatnicima, koji zbog prirode svoga posla moraju s njima biti 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 dopušteno. A dopušteno 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 ovdje i sigurnosna politika biti liberalnija. Težište provođenja sigurnosne politike treba biti ponajprije na obrazovanju, a ne na sužavanju izbora i sankcioniranju. Ipak, u pojedinim dijelovima sigurnosna pravila će biti jednako restriktivna, kao i ona 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 je donio prijedlog sigurnosne politike za ustanove članice, kako bi ih potaknuo da i same donesu vlastite pravilnike.

Tako je i Gradska i sveučilišna knjižnica u Osijeku doradila i prilagodila pravila kako bi sigurnosna politika bila primjenjiva i u njezinim, specifičnim uvjetima. U skladu s uslugama koje pružamo korisnicima dopisana su i nova pravila, ali pri tome nisu zanemareni osnovni principi sadržani u *Politici prihvatljivog korištenja* koji vrijede za cijeli CARNet.

Reference i međunarodni standardi

- standardi za komercijalno okruženje (ISO standard 17799),
- prijedlog standarda u SAD, Draft: Internet Security Policy, A Technical Guide, njihova nacionalnog instituta za standarde (*http://www.nist.org*).

Postoji i dokument (*RFC1855 – Netiquete Guidelines)* koji navodi pravila pristojnog ponašanja na Internetu. Dokument je nastao u vrijeme samoregulacije, kada je apeliranje na svijest korisnika Interneta bilo dovoljno. Kako je vrijednost ovog dokumenta neprolazna, bit će objavljen na portalu za CARNetove sistem inženjere (*http://sistemac.carnet.hr*).

CARNet i SRCE pružiti će ustanovama iz akademske mreže, pa tako i Gradskoj i sveučilišnoj knjižnici u Osijeku, svu moguću podršku pri donošenju i primjeni sigurnosne politike.

Sigurnosna politika informacijskih sustava u Gradskoj i sveučilišnoj knjižnici u Osijeku

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu (kao i pripadajuće programe), koja se nalazi u prostorima Knjižnice
- Administratore informacijskih sustava
- Korisnike, u koje spadaju: zaposlenici, vanjski suradnici i članovi Knjižnice
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softwarea

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 informatičkih usluga.

Korisnici informatičkih usluga

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

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

Korisnici su dužni:

- Pridržavati se 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,
- Izabrati kvalitetne zaporke i povremeno ih mijenjati,
- Prijavljivati sigurnosne incidente kako bi problemi što prije nestali,
- Korisnici koji proizvode podatke i dokumente odgovorni su i za njihovo čuvanje. Davatelji usluga osiguravaju automatsku pohranu (backup) važnih informacija, dok za vlastite podatke i dokumente korisnici sami izrađuju sigurnosne kopije.

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

Način korištenja informacijskih sustava Knjižnice za vanjske suradnike i članove Knjižnice bit će reguliran posebnim Pravilnikom.

Glavni korisnik

Knjižnica koristi aplikacije za obradu podataka: računovodstvene programe i programe za obradu knjižnične građe. Radi poboljšanja sigurnosti za svaki od tih programa imenuje se glavni korisnik. Voditelj računovodstva je glavni korisnik za računovodstvene programe, a administrator baze podataka je glavni korisnik programa za obradu knjižne građe.

Zaposlenici koji unose podatke odgovorni su za njihovu vjerodostojnost, dok je glavni korisnik odgovaran za ispravnost podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od neautoriziranih osoba.

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

Ako se ukaže potreba, ravnatelj(ica) Knjižnice može imenovati i zamjenike glavnih korisnika za pojedine aplikacije.

Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu računala i mreže te informacijskih sustava. U Knjižnici to su zaposlenici Odjela za informatičku podršku. Oni su zaduženi za ispravnost i neprekidnost rada informacijskog sustava.

Specijalisti za sigurnost

Knjižnica će pri rješavanju sigurnosnih incidenata koristiti pomoć CARNeta.

Pored toga, Knjižnica će obrazovati i imenovati pojedince čija će zadaća biti briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

Ravnatelj(ica) Knjižnice imenuje voditelja sigurnosti čije je prvenstvena briga sigurnost informacijskih sustava. Poželjno je da voditelj sigurnosti bude stručna osoba, a i da posjeduje sposobnost vođenja ljudi te da je komunikativan.

Njegova je briga ukupna sigurnost informacijskih sustava. To uključuje i fizičku sigurnost sustava, pa će voditelj surađivati i sa ostalim zaposlenicima, poput vratara, 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 softwarea, te sudjeluje u razvoju softwarea, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

Kada Knjižnica bude zapošljavala više stručnjaka za računarstvo, oformiti će se *Ekipa za hitne intervencije,* obučena za postupanje u slučaju incidentnih situacija. Ekipu će činiti specijalisti različitih usmjerenja, na primjer za mrežu, Unix, Microsoft Windowse, baze podataka itd. U tom slučaju Knjižnica treba razraditi procedure za postupanje u incidentnim situacijama, te obučiti članove *Ekipe za hitne intervencije* kako bi mogli izvršiti istragu i što prije vratiti informacijski sustav u redovno stanje.

Postupci za rješavanje incidenata dani su u pratećem dokumentu pod nazivom *Pravilnik o rješavanju sigurnosnih incidenata*.

Knjižnica treba izraditi i održavati kontakt listu s imenima, brojevima telefona, e-mail adresama osoba kojima se prijavljuju incidenti: kvarovi opreme, sporost ili nedostupnost mrežnih usluga i podataka, 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.

Za svako računalo se imenuje administrator, koji odgovara za instalaciju i konfiguraciju softwarea. Ukoliko korisnici žele sami administrirati osobno računalo na kojem rade, 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 dodataka programima po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

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

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Pored toga administratori nadgledaju i rad korisnika, kako bi otkrili i spriječili nedopuštene aktivnosti. U slučajevima kad administrator(i) treba na sustavu obaviti više poslova istovremeno, prioritet određuje samostalno, u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Administratori su dužni prijaviti incidente voditelju sigurnosti, 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 korisnika i povjerljivost informacija s kojima pri obavljanju posla dolaze u dodir. Na poštivanje tih pravila obvezuju se Knjižnici potpisivanjem *Izjave o čuvanju povjerljivih informacija*, čiji je predložak dan među pratećim dokumentima.

Upravljanje mrežom

Ravnatelj(ica) Knjižnice imenuje djelatnika (djelatnike) koji su zaduženi za upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova itd.

Knjižnica treba propisati i postupke za priključivanje računala u mrežu, odrediti obrasce kojima se izdaje odobrenje za priključenje računala na mrežu i dodjelu adrese.

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

Ukoliko se podrži rad na daljinu (npr. kada se djelatnicima dopušta da sa kućnog računala ažuriraju podatke), bit će potreban poseban pravilnik kojeg će se morati poznavati i pridržavati ga se svi koji tako rade. S obzirom na mogućnost da ga koriste neautorizirane osobe (članovi obitelji i slično), morat će se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove. Stoga povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Knjižnica će razraditi pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Zbog opasnosti od širenja virusa ili namjernih nedopuštenih radnji (poput presretanja mrežnog prometa, prikupljanja informacija itd.) ne smije se dozvoliti da oni po svom nahođenju priključuju računala na mrežu Knjižnice. Knjižnica će odrediti mjesta gdje je dopušteno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se sa toga segmenta mreže dopre do ostalih računala u ustanovi.

Dijelovi Knjižnice koji koriste bežičnu mrežu, su osigurani od mogućnosti priključivanja na privatnu mrežu i snimanja prometa. To je postignuto metodama enkripcije i autentifikacije uređaja i korisnika.

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

Instalacija i licenciranje softwarea

Korištenje ilegalnog softwarea predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Knjižnica zadužuje jednu ili više odgovornih osoba za instaliranje softwarea 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, između ostalog i potpisivanjem izjave o tome da su upoznati s ***Politikom prihvatljivog korištenja*** i da će je se pridržavati. Na taj način Knjižnica 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.*** Sačinjavali bi ga predstavnik uprave i specijalisti tehničari (npr. voditelj sigurnosti, CARNet koordinator, glavni korisnik baze podataka koja sadrži povjerljive informacije itd.).

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

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

Fizička sigurnost

Prostor u Knjižnici 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.

Knjižnica je dužna sastaviti popis osoba koje imaju pristup u zaštićene prostore, a vratar mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Sigurne zone

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

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

U pravilu su to 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 administratorima osigurati radni prostor odvojeno od prostorija u kojima je smještena oprema koja sadrži najvažnije informacije.

Ta 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 incidente, poput poplava, požara i slično, te poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak sustava. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Vanjske tvrtke

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

Knjižnica u ugovore s vanjskim tvrtkama ugrađuje odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.

Ugovorom će se regulirati 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.

Knjižnica 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 za to nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je prostor osiguran video nadzorom.

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

Knjižnica zadržava diskreciono pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup u svoje prostorije, ukoliko nisu na popisu ovlaštenih djelatnika dostavljenom Knjižnici.

Sigurnost opreme

Klasifikacija računalne opreme

Knjižnica 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 povezivanje izdvojenih lokacija. U ovu grupu, za sada, se mogu ubrojiti veze lokalnih baza podataka s centralnim poslužiteljima (LDAP, CROLIST-kooperativna katalogizacija), a u budućnosti interni modemski ulazi i sl.

S vremenom će se izraditi sigurnosna politika za svako od navedenih područja, koja će davati 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 će se regulirati prava i obaveze, a vanjske tvrtke kojima će se dopustiti pristup računalima i podacima u intranetu treba ugovorom obavezati na poštivanje sigurnosnih pravila i čuvanje povjerljivosti informacija.

Podjela opreme prema vlasništvu

U prostorijama Knjižnice nalazi se i oprema CARNeta, Ministarstva znanosti obrazovanja i športa Republike Hrvatske, Ministarstva kulture, Iskona koja je dana na korištenje Knjižnici.

Knjižnica je obavezna održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarnim brojevima i slično.

Knjižnica jednako brine o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Oprema se čuva od oštećenja i otuđenja.

Knjižnica je dužna osoblju CARNeta/SRCE-a/Iskona dozvoliti pristup opremi u vlasništvu CARNeta/MZOS-a /Ministarstva kulture/Iskona koja se nalazi u Knjižnici.

Odgovornost za računalnu opremu

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

Knjižnica je dužna razraditi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme. Vratar provjerava je li oprema koja se iznosi ima potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

Osiguranje neprekidnosti poslovanja

Kako bi se u slučaju nezgoda (poput kvarova na sklopovlju, požara, ili ljudskih grešaka) podaci sačuvali, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softwarea. Preporučuje se izraditi više kopija i čuvati ih na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Procedura za izradu rezervnih kopija razrađena je 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. Čuva ih se u pisanom obliku, kako bi se u slučaju nesreće, a kada je došlo do zamjene izvršitelja novozaposlenim djelatnikom, moglo brzo reagirati.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi (koju bi trebalo osigurati zaposlenicima zaduženim za te poslove), u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Knjižnica zadržava pravo nadzora nad instaliranim softwareom 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 Knjižnica za to ovlastila. Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. U slučajevima kada je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, pa se one mogu koristiti u stegovnom ili sudskom postupku.

Doseg

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

Pravila su dužni poštivati i provoditi svi zaposleni, članovi 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 administratore 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 Knjižnice, ili oprema Knjižnice služi za njezin prijenos,

- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.),
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Knjižnice.

Nepridržavanje

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

Praktična primjena sigurnosne politike

Kako bi se sigurnosna politika mogla što uspješnije primijeniti, nužno je:

- Obnoviti postojeći popis računala, pisača i drugih informatičkih uređaja,
- Postojeću skicu mreže provjeriti i ažurirati novim priključcima. Sve mrežne priključke numerirati na razumljiv i jedinstven način u Knjižnici, tako da se svaki priključak može brzo pronaći.

Nakon usvajanja sigurnosne politike, treba napraviti inventuru kompletne računalne opreme, uključujući mrežne i komunikacijske uređaje.
Za svako računalo potrebno je evidentirati koji se operacijski sustav na njemu koristi, te popisati aplikacije koje su na njemu instalirane.
Knjižnica u svakom trenutku treba imati ažurirani popis softwarea koji se koristi u LAN-u, kako bi mogla brinuti o licenciranju.
Zbog svega, gore navedenog potrebno je organizirati stručni tim koji će izvršiti detaljan popis sve informatičke opreme, softwarea, podataka i mrežnih instalacija. U svrhu što efikasnije praktične primjene sigurnosne politike Knjižnica se nada maksimalnoj podršci Ministarstva znanosti, obrazovanja i športa Republike Hrvatske. Zato ubuduće očekujemo odgovarajući broj zaposlenih informatičkih stručnjaka, kao i odgovarajuću informatičku opremu te pripadajući software.

Prateći dokumenti

S nabavom nove informatičke opreme i razvojem informacijskih sustava u Knjižnici, kao i s porastom ovisnosti o njihovom ispravnom funkcioniranju, javlja se potreba da se sigurnosna politika dopuni pratećim dokumentima, u kojima se definiraju pravila za pojedina područja rada. Prateći dokumenti su razni pravilnici. Pisani su kao upute za rješavanje konkretnih problema i mogu se češće mijenjati. Prateći pravilnici su sastavni dio Sigurnosne politike Gradske i sveučilišne knjižnice u Osijeku. To su:
Pravilnik o rukovanju zaporkama
Pravilnik o korištenju elektroničke pošte
Pravilnik o antivirusnoj zaštiti
Pravilnik o zaštiti od spama
Pravilnik o zaštiti od *špijunskih* i *nametnih* programa
Pravilnik o izradi kopija podataka
Pravilnik o rješavanju sigurnosnih incidenata
Pravilnik o rukovanju povjerljivim informacijama
Pravilnik o korištenju informacijskih sustava Knjižnice za vanjske suradnike i članove Knjižnice

Sigurnosna politika informacijskih sustava u Gradskoj i sveučilišnoj knjižnici u Osijeku temelji se na dokumentu *Sigurnosna politika informacijskih sustava za članice CARNeta (prijedlog) (http://sistemac.carnet.hr/sigurnost/sigurnosna_politika_ustanove.pdf).*
Osijek, rujan 2005.

Prijedlog sastavila:

Katica Mihelić, dipl. inž.
Sistem inženjer GISKO-a

Ravnatelj:

Dragutin Katalenac, prof.

Prilog 1

Pravilnik o rukovanju zaporkama

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 korisnici (zaposlenici, suradnici i članovi) Knjižnice 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. Riječi iz rječnika

   Ne koristiti ih, jer 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. Koristiti i specijalne znakove ako su dopušteni u sustavu (npr. $).

4. Imena bliskih osoba, ljubimaca, datumi

   Ne treba koristiti takve zaporke jer se 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

   Potpisom na obrascu za preuzimanje zaporke korisnici preuzimaju odgovornost za svoju zaporku i ni u kom je slučaju ne smiju otkriti. 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

   Ukoliko sustav dopušta 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 dopušta.

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

Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. Knjižnice je obavezna odgojno djelovati i obrazovati korisnike prilikom kreiranja sigurnih zaporki.

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

Prilog 2

Pravilnik o korištenju elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. S obzirom na moguće posljedice treba razmotriti sve aspekte elektroničke komunikacije.

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.

Problemi 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 (Odgovori) pritisne Reply All (Odgovori svima), poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
    - Česta je pogreška i preuzimanje pogrešne adrese 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, npr. 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 (Odgovori svima) umjesto Reply (Odgovori).

- 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. Knjižnica se obavezuje čuvati povjerljivost takvih poruka, ali to neće moći garantirati budu li poruke tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

- Veliki broj 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. Knjižnica će filtrirati spam na poslužitelju elektroničke pošte. Obaveza je 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 Gradsku i sveučilišnu knjižnicu Osijek.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te su korisnici obvezni pridržavati se sljedećih pravila:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa redoviti 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 *netiquete*, pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, za seksualno ili bilo koje drugo uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi a 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.

- Knjižnica zadržava pravo konfiguriranja sustava na način da ne obavještava pošiljatelja i primatelja o otkrivenom virusu u poruci ukoliko se ustanovi da se radi o tzv. virusima koji lažiraju adresu.
- Knjižnica 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, ravnatelj(ica) zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.

Pri prestanku radnog odnosa, ravnatelj(ica) je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa.

Ako zaposlenik nakon odlaska u mirovinu zatraži nastavak korištenja korisničkog računa to mu se, uz suglasnost CARNetove službe za članice, može odobriti.

Na koga se odnose pravila korištenja e-maila

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

Nepridržavanje

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

Prilog 3

Pravilnik o antivirusnoj zaštiti

Virusi i crvi predstavljaju opasnost za informacijske sustave jer ugrožavaju funkcioniranje mreže i povjerljivost podataka.

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

Stoga je zaštita od virusa obaveza Knjižnice, administratora računala i svakog korisnika.

Knjižnica 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 prethodno obavijestiti sistem inženjera.

Nepridržavanje

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

Prilog 4

Pravilnik o zaštiti od spama

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 njihovo radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, nastoje pobuditi samilost kako bi se izvukao novac (eng. 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 je mogućnost 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 mogu određivati sami korisnici. Poruke dobivaju 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 pomagati korisnicima 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 ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke biti će pokrenut stegovni postupak.

Prilog 5

Pravilnik o zaštiti od *špijunskih* i *nametnih* programa

Svrha

Internetom se širi sve više neželjenih, skrivenih, tzv. špijunskih programa koji mogu biti veoma opasni. To su programi koji se često instaliraju na računalo bez znanja korisnika te na računalu čine razne, štetne radnje. Posljedice mogu biti: usporeni rad računala, promijenjena početna web stranica, neprekidna aktivnost na internetu bez obzira što je modem isključen, otvaranje drugog prozora iz čista mira,… Najčešće dolaze *potiho* uz neki besplatan software.

Pravila za administratore

Administratori osobnih računala dužni su na računalo instalirati odgovarajući *antišpijunski* program koji omogućava uklanjanje špijunskih programa s računala. Program je potrebno konfigurirati tako da ga može pokrenuti i tzv. obični korisnik računala.

Pravila za korisnike

Ako instaliraju besplatni software, korisnici su dužni obratiti pozornost da uz njega ne instaliraju i neki od skrivenih programa.

Korisnici su dužni povremeno pokrenuti *antišpijunski* program kako bi uklonili ove maliciozne programe.

Nepridržavanje

Korisnici su dužni obratiti pozornost da na računalo ne instaliraju skriveni programi, a protiv onih koji namjerno instaliraju špijunske programe bit će pokrenut stegovni postupak.

Prilog 6

Pravilnik o izradi kopija podataka

Ravnatelj(ica) Knjižnice određuje tko je od zaposlenika zadužen za izradu kopija pojedine vrste podataka. Veću pozornost treba obratiti na spremanje važnijih podataka (baza podataka, mail, web, dns, …).

Izradu kopija podataka treba prilagoditi postojećoj tehnološkoj osnovi kojom raspolaže Knjižnica.

Osnovna strategija izrade kopija:

- Kopija podataka iz baze podataka knjižnično-informacijskog sustava se izrađuje svakodnevno, na drugoj particiji diska, na traci automatskim noćnim backupom, a jednom tjedno i na traci ručnim backupom, svaka 3 mjeseca se radi potpuni backup.

- Kopija podataka ključnih servisa (mail, web, dns,…), kao i osobnih podataka sa poslužitelja, se izrađuje jednom tjedno,

- Kopije podataka sa osobnih računala se izrađuje prema potrebi.

Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ukoliko im je u tome potrebna pomoć, pomažu im zaposlenici Odjela za informatičku podršku.

Članovi knjižnice, kao i vanjski suradnici, ne mogu koristiti vlastite medije za pohranu podataka (disketa, CD, DVD,…) bez prethodnog odobrenja odgovorne osobe u Knjižnici.

Prilog 7

Pravilnik o rješavanju sigurnosnih incidenata

Svrha

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

Prijava incidenta

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

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

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 (npr. dokumenata ili e-mail poruka).

Provjera sadržaja korisničkih podataka je moguća jedino na zahtjev i uz odobrenje korisnika.

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

- Istragu provodi jedna osoba, ali uz nazočnost 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 (npr. 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.

Dok ne bude formirano *Povjerenstvo za sigurnost*, pri rješavanju sigurnosnih problema, Knjižnica će koristiti pomoć CARNeta.

Knjižnica 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 bila pogreška čovjeka, protiv odgovornih se mogu poduzeti sankcije.

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

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

Prilog 8

Pravilnik o upravljanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01 i zakonom o zaštiti osobnih podataka od 12. lipnja 2003. godine.

Prema vrsti tajnosti, informacije se dijele 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 Knjižnici 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 na Posudbenim odjelima Knjižnice, osoba koje unose podatke u baze podataka o korisnicima ili sistem administratora poslužitelja, koji u nekim situacijama može doći u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji ulaze u Knjižnicu s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Knjižnica 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 ravnatelj(ica) Knjižnice, 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 Knjižnice i vanjske suradnike koji dolaze u doticaj s 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.

Knjižnica 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 osobe kojoj podaci pripadaju (npr. adresa stana, broj privatnog telefona ili mobitela, podaci o primanjima, porezu, osiguranju itd.)

Povjerljive informacije u načelu se ne daju 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 Knjižnice 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 njihovu slanju i prenošenju.

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

Ako se povjerljive informacije šalju elektronički (npr. 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 Knjižnicu ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju Knjižnici 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 njihov 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 briše sadržaj diska.

Nepridržavanje

Zaposlenici i suradnici koji dolaze u dodir s povjerljivim 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 se 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 Knjižnica treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Sastavni dio *Pravilnika o upravljanju povjerljivim informacijama* je i *Izjava o čuvanju povjerljivih informacija*.

Prilog 9

Pravilnik o korištenju informacijskih sustava Knjižnice za vanjske suradnike i članove Knjižnice

Javna računala

Vanjskim suradnicima i članovima ograničeno je korištenje informacijskih sustava Knjižnice.
Korištenje pojedinih vrsta resursa dopušteno im je na za to određenim računalima. Stoga, za vanjske suradnike i članove, u Knjižnici postoji više grupa računala: za pretraživanje lokalne baze podataka, za pretraživanje relevantnih baza podataka te općenito za Internet.
Takva računala su smještena u odjelima, po hodnicima i sličnim prostorima pa ih treba svakako odvojiti u zasebne grupe. U te grupe spadaju ona računala kojima je pristup slobodan i slabije kontroliran.

Mrežu treba segmentirati tako da računala iz ovih grupa, ovisno o namjeni, imaju pristup Internetu, poslužiteljima ustanove u demilitariziranoj zoni, te internim poslužiteljima ustanove ukoliko je to potrebno. Segmentu mreže u kojemu su računala za vanjske korisnike i članove Knjižnice neće se dozvoliti pristup osobnim računalima zaposlenika.

Vanjskim suradnicima ili članovima Knjižnice iznimno se može dopustiti i rad na nekom od računala koje nije javno. Korisnicima koji nisu učlanjeni u Knjižnicu također se može dopustiti korištenje pojedine grupe računala. Ravnatelj(ica) će odrediti odgovorne djelatnike (npr. voditelji odjela) koji će dopustiti rad na tim računalima.

Ispis i kopiranje podataka

Članovi knjižnice i vanjski suradnici ne mogu koristiti vlastite medije za pohranu podataka (disketa, CD, DVD, USB uređaje…) bez prethodnog odobrenja odgovorne osobe u Knjižnici.

Ispis stranica na pisaču te kopiranje podataka na disketu (odnosno CD ili DVD) naplaćuje se prema važećem cjeniku.

Nepridržavanje

U slučajevima kada se članovi Knjižnice (ili vanjski suradnici) ne pridržavaju mjera sigurnosne politike najprije ih se upozori na prekršaj, a kod težih povreda mjera može im se i uskratiti daljnje korištenje građe i svih usluga Knjižnice.