Sigurnosna politika informacijskih sustava Studentskog centra Split

(verzija 1.3)

Split, 24.08. 2011.

Sadržaj

Potreba donošenja mjera sigurnosne politike

Cemu sigurnosna politika?

Informacijske tehnologije svakim danom sve više doprinose efikasnom funkcioniranju akademske i istraživacke zajednice. Korisnicke aplikacije, elektronicka pošta, web i mreža koja funkcionira ispod toga imaju sve vecu važnost u ucenju, 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 elektronickom obliku: prirodne katastrofe, kvarovi na opremi, greške u software-u, ljudski postupci. Covjek može djelovati izvana ili iznutra, a šteta može biti izazvana slucajno ili namjerno. Radi svega toga treba se organizacijski pripremiti za slucajeve incidenata.

Ustanove clanice CARNeta na umreženim racunalima cuvaju informacije kojima pristup mora biti ogranicen, bilo da se radi o knjigovodstvenim podacima, bazama podataka, rezultatima istraživanja ili samo o privatnim porukama elektronicke pošte. U svakom slucaju informacijske sustave treba zaštiti kako bi osigurali povjerljivost, integritet i dostupnost podataka.

Cak 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 racunala ne bi bila odskocna daska za napade na tude sustave. Internet je nedjeljiva cjelina, pa brigom o sigurnosti informacijskih sustava Studentskog Centra u Splitu doprinosimo ukupnoj sigurnosti na Internetu.

Umjesto nacela 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 omoguciti 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 postici sigurnosna politika?

Sigurnosna politika dio je sustava upravljanja sigurnošcu informacijskih sustava. Njezina je svrha definirati prihvatljive i neprihvatljive nacine ponašanja, jasno raspodijeliti zadatke i odgovornosti, te propisati sankcije u slucaju njihova nepridržavanja.

Osnovni dokument o sigurnosti, koji postavlja opce principe, prate drugi dokumenti koji definiraju pravila za specificna podrucja (npr. pravila o rukovanju zaporkama, o uporabi elektronicke pošte, pohrani podataka i slicno). Ta pravila su ovisna o promjenama u tehnologiji i organizaciji, te ce se vjerojatno cešce mijenjati i doradivati.

Kako ne bi ostala mrtvo slovo na papiru, sigurnosna politika treba biti primjenjiva. To znaci da mora biti pisana jednostavnim i razumljivim jezikom i prilagodena lokalnoj kulturi, a istovremeno uskladena sa zakonima i propisima koji vrijede u državi. Za njezino provodenje potrebna je podrška uprave, a s njezinim principima treba upoznati sve administratore i korisnike informacijskih sustava. Zato nakon njenog prihvacanja treba uložiti napor u obrazovanju korisnika.

Prilikom zapošljavanja nove djelatnike treba upoznati s pravilima propisanim sigurnosnom politikom, a nove korisnike prilikom dolaska u Centar.

Nakon usvajanja, dokument o *Sigurnosnoj politici informacijskih sustava u Studentskom Centru u Splitu* (u daljnjem tekstu Centar), bit ce objavljen na javnim web stranicama Centra.

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

Ako prateci dokumenti koji se bave razradom konkretnih poslova sadrže povjerljive informacije, objavljuju se samo na internom webu ili ih se dostavlja odredenim 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 receno, sve je zabranjeno, osim onog što je izricito dopušteno. A dopušteno je samo ono što je neophodno za obavljanje posla.

Akademska zajednica pripada otvorenoj kulturi, okrenuta je komuniciranju, istraživanju, samorazvoju i ucenju. Sveucilište brani svoje slobode i nezavisnost, ne trpi restrikcije. Stoga ce ovdje i sigurnosna politika biti liberalnija. Težište provodenja sigurnosne politike treba biti ponajprije na obrazovanju, a ne na sužavanju izbora i sankcioniranju. Ipak, u pojedinim dijelovima sigurnosna pravila ce biti jednako restriktivna, kao i ona u komercijalnom okruženju.

Postupanje s povjerljivim informacijama podliježe jednakim pravilima u banci i na sveucilištu, a akademska sloboda nikoga ne stavlja iznad zakona, morala i pravila pristojnog ponašanja.

Lokalizacija

CARNet je donio prijedlog sigurnosne politike za ustanove clanice, kako bi ih potaknuo da i same donesu vlastite upute.

Tako je i Studentski centar Split dorado i prilagodio pravila kako bi sigurnosna politika bila primjenjiva i u njegovim, specificnim 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 medunarodni standardi

U svijetu ne postoji standard sigurnosne politike za akademsku zajednicu.

Trenutno postoje dva standarda iz kojih se mogu preuzeti pojedini dijelovi:

- standardi za komercijalno okruženje (ISO standard 27002),
- prijedlog standarda u SAD-u, 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 bila dovoljna. Kako je vrijednost ovog dokumenta neprolazna, bit ce objavljen na portalu za CARNetove sistem inženjere (*http://sistemac.carnet.hr*).

CARNet i SRCE pružiti ce ustanovama iz akademske mreže, pa tako i Centru u Splitu, svu mogucu podršku pri donošenju i primjeni sigurnosne politike.

Sigurnosna politika informacijskih sustava Studentskog centra Split

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- svu racunalnu opremu (kao i pripadajuce programe), koja se nalazi u prostorima Centra,
- administratore informacijskih sustava,
- korisnike, u koje spadaju: zaposlenici, poslovni partneri, vanjski suradnici, studenti i drugi korisnici usluga Centra,
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili software-a.

Organizacija upravljanja sigurnošcu

Kljucna stvar pri provodenju sigurnosne politike informacijskog sustava jest da se u svakom trenutku tocno zna što je ciji posao i tko za što odgovara. Stoga je potrebno raspodijeliti zaduženja i obrazovati korisnike, te oformiti strucna tijela za upravljanje sigurnošcu.

Ljudi koji se u radu koriste racunalima dijele se na korisnike i davatelje informatickih usluga.

Korisnici informatickih usluga

Korisnici su osobe koje se u svom radu ili ucenju služe racunalima, proizvode dokumente ili unose podatke, ali nisu odgovorni za instalaciju i konfiguraciju software-a, niti za ispravan i neprekidan rad racunala 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 znaci da ne smiju koristiti racunala za djelatnosti koje nisu u skladu sa važecim zakonima, etickim 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 cuvanje. Davatelji usluga osiguravaju automatsku pohranu (backup) važnih informacija, dok za vlastite podatke i dokumente korisnici sami izraduju sigurnosne kopije.

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

Nacin korištenja informacijskih sustava Centra za vanjske suradnike i korisnike Centra bit ce reguliran posebnom uputom.

Glavni korisnik

Centar koristi aplikacije za obradu podataka i to racunovodstveno-knjigovodstvene programe kao module centralne aplikacije (blagajna, glavna knjiga i saldo konti, osnovna sredstva, kadrovska evidencija, materijalno knjigovodstvo, sitni inventar, restorani i kantine, skladište, nezavisno fakturiranje, student servis, studentski dom, obracun ugovora o djelu, obracun placa, arhiva) i web aplikacije. Radi poboljšanja sigurnosti za svaki od tih programa imenuje se glavni korisnik. U pravilu je rukovoditelj za financije, knjigovodstvo i kontroling glavni

korisnik za racunovodstveno-knjigovodstvene programe, a web administrator glavni korisnik web aplikacija. 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 sprecavanja izmjene podataka od strane neautoriziranih osoba.

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

Ako se ukaže potreba, ravnatelj Centra može imenovati i zamjenike glavnih korisnika za pojedine aplikacije. U pravilu je zamjenik glavnog korisnika za racunovodstveno-knjigovodstvene programe voditelj knjigovodstva, a zamjenik glavnog korisnika web aplikacija administrator informatickog sustava.

Davatelji informatickih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu racunala i mreže te informacijskih sustava. U Centru je to administrator informatickog sustava i ugovorni vanjski strucni suradnici. Oni su zaduženi za ispravnost i neprekidnost rada informacijskih sustava.

Specijalisti za sigurnost

Centar ce pri rješavanju sigurnosnih incidenata koristiti pomoc CARNeta.

Pored toga, Centar ce obrazovati i imenovati pojedince cija ce zadaca biti briga za organizaciju i provodenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

Ravnatelj Centra imenuje voditelja sigurnosti cije je prvenstvena briga sigurnost informacijskih sustava. Poželjno je da voditelj sigurnosti bude strucna osoba, a i da posjeduje sposobnost vodenja ljudi te da je komunikativan. U pravilu je to koordinator CARNeta za Centar.

Njegova je briga ukupna sigurnost informacijskih sustava. To ukljucuje i fizicku sigurnost sustava, pa ce voditelj suradivati i sa ostalim zaposlenicima, poput vratara, cuvara i slicno. Voditelj sigurnosti piše upute, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi racunala i software-a, te sudjeluje u razvoju software-a, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

Voditelju u radu koristi pomoc vanjskih suradnika, strucnjaka za pojedina podrucja sigurnosti informacijskih sustava kao i pomoc CARNeta.

Postupci za rješavanje incidenata dani su u pratecem dokumentu pod nazivom *Uputa o rješavanju sigurnosnih incidenata*.

Centar 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 racunala

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

Za svako racunalo se imenuje administrator, koji odgovara za instalaciju i konfiguraciju software-a. U pravilu to je administrator informatickog sustava. Samo iznimno, ukoliko se, po procjeni ravnatelja, ukaže potreba da korisnici sami administriraju osobno racunalo na kojem rade, uz posebno dopuštenje-odluku ravnatelja, a uz suglasnost voditelja sigurnosti, potpisuju izjavu o tome, nakon cega za njih vrijede sva pravila za administriranje racunala. Studenti i drugi korisnici usluga Centra koji imaju vlastita racunala i njima se spajaju na mrežu Centra potpisuju prethodnu izjavu-suglasnost u okviru drugih dokumenata vezanih za njihovu prisutnost u Centru (ugovori o smještaju i sl.).

Racunala se moraju konfigurirati na taj nacin da budu zašticena od napada izvana i iznutra, što se osigurava instaliranjem dodataka programima po preporukama proizvodaca, listama pristupa, filtriranjem prometa i drugim sredstvima.

Posebnu pažnju administrator je dužan posvetiti onoj opremi preko koje se obavljaju kljucne funkcije ili koja sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

Administrator racunala svakodnevno prati rad sustava, cita dnevnicke zapise i provjerava rad servisa. Pored toga administrator nadgleda i rad korisnika, kako bi otkrio i sprijecio nedopuštene aktivnosti. U slucajevima kad administrator treba na sustavu obaviti više poslova istovremeno, prioritet odreduje samostalno, u skladu s pravilima struke, brinuci istovremeno o funkcionalnosti i sigurnosti. U dogovoru je sa koordinatorom Centra za CARNet,

Administrator je dužan prijaviti incidente voditelju sigurnosti, te pomoci pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slicne situacije u buducnosti. Ukoliko je incident ozbiljan i ukljucuje 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 Centru potpisivanjem *Izjave o cuvanju povjerljivih informacija*, ciji je predložak dan medu pratecim dokumentima.

Upravljanje mrežom

Ravnatelj Centra imenuje djelatnika koji je zadužen za upravljanje mrežom, konfiguriranje mrežnih uredaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova itd.

Centar treba propisati i postupke za prikljucivanje racunala u mrežu, odrediti obrasce kojima se izdaje odobrenje za prikljucenje racunala na mrežu i dodjelu adrese.

Djelatnik zadužen za upravljanjem mrežom mora u svakom trenutku imati tocan popis svih mrežnih priključaka i umreženih uredaja, ukljucujuci i prijenosna racunala.

Ukoliko se podržava rad na daljinu (npr. kada se djelatnicima dopušta da sa kucnog racunala ažuriraju podatke), bit ce potrebna posebna uputa koja ce se morati poznavati i pridržavati je se svi koji tako rade. S obzirom na mogucnost da ga koriste neautorizirane osobe (clanovi obitelji i slicno), morat ce se osigurati da udaljeno racunalo ne ugrozi sigurnost mreže ustanove. Stoga povjerljivi podaci na udaljenom racunalu moraju biti jednako sigurni kao da se racunalo nalazi u zgradi ustanove.

Centar ce razraditi pravila za spajanje na mrežu gostujucih racunala, koja donose sa sobom vanjski suradnici, predavaci, 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 nahodenju prikljucuju racunala na mrežu Centra. Centar ce odrediti mjesta gdje je dopušteno prikljuciti gostujuca racunala, te konfiguracijom mreže sprijeciti da se sa toga segmenta mreže dopre do ostalih racunala u ustanovi.

Dijelovi Centra koji koriste bežicnu mrežu, su osigurani od mogucnosti prikljucivanja na privatnu mrežu i snimanja prometa. To je postignuto metodama enkripcije i autentifikacije uredaja i korisnika.

Radi zaštite povjerljivih informacija pri prijenosu mrežom, poželjno je da takav promet bude kriptiran. Centar ce u tom slucaju izdati uputa u kojem se definira vrstu enkripcije, obvezan software, procedure za dodjelu i cuvanje kriptografskih kljuceva i slicno.

Instalacija i licenciranje software-a

Korištenje ilegalnog software-a predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Centar zadužuje jednu ili više odgovornih osoba za instaliranje software-a i njegovo licenciranje. U pravilu to su administrator informatickog sustava i web administrator. 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, izmedu ostalog i potpisivanjem izjave o tome da su upoznati s ***Politikom prihvatljivog korištenja*** i da ce je se pridržavati. Na taj nacin Centar odgovornost za eventualno kršenje zakona prebacuje na nesavjesnog korisnika.

Povjerenstvo za sigurnost informacijskih sustava

Kako bi se osiguralo upravljanje sigurnošcu, poželjno je oformiti ***Povjerenstvo za sigurnost.*** Sacinjavali bi ga ravnateljica, lokalni strucnjak za sigurnost, administrator informatickog sustava, voditelj sustava kvalitete, voditelj financija, knjigovodstva i kontrolinga, voditelj knjigovodstva, web administrator i vanjski strucni savjetnik.

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

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

Fizicka sigurnost

Prostor u Centru 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.

Centar je dužan sastaviti popis osoba koje imaju pristup u zašticene prostore, a vratar mora imati popis osoba koje mogu dobiti kljuceve odredenih prostorija.

Sigurne zone

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

Centar je dužan održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone.

U pravilu su to zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje kljucnih 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 zašticena od problema s napajanjem elektricnom energijom, što znaci da elektricne instalacije moraju biti izvedene kvalitetno, da se koriste uredaji za neprekidno napajanje, a po potrebi i generatori elektricne energije.

Treba predvidjeti i druge moguce incidente, poput poplava, požara i slicno, 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, zajednickog poslovanja, konzultacija itd.

Centar u ugovore s vanjskim tvrtkama ugraduje odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.

Ugovorom ce se regulirati pristup prostorijama, pristup opremi ili logicki pristup povjerljivim informacijama. Trecu stranu treba obavezati na cuvanje povjerljivih informacija s kojima dodu u dodir pri obavljanju posla.

Centar može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše *Izjavu o cuvanju 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 zašticenom prostoru samo ako je prostor osiguran video nadzorom.

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

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

Sigurnost opreme

Klasifikacija racunalne opreme

Centar dijeli svu opremu u grupe prema zadacama:

- Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektronicke pošte itd.).
- Intranet je privatna mreža Ustanove, sacinjavaju je poslužitelji internih servisa, osobna racunala zaposlenih, racunalne prostorije te komunikacijska oprema lokalne mreže.
- Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezivanje izdvojenih lokacija.

S vremenom ce se izraditi sigurnosna politika za svako od navedenih podrucja, koja ce davati konkretne upute administratorima kako zaštiti sustav. Posebno je osjetljivo podrucje koje nazivamo extranet, jer se tu otvara prolaz u zašticenu mrežu korisnicima (koji su na putu, kod kuce) ili poslovnim partnerima. Potrebno je izraditi poseban uputa za extranet u kojem ce se regulirati prava i obaveze, a vanjske tvrtke kojima ce se dopustiti pristup racunalima i podacima u intranetu treba ugovorom obavezati na poštivanje sigurnosnih pravila i cuvanje povjerljivosti informacija.

Podjela opreme prema vlasništvu

U prostorijama Centra nalazi se i oprema CARNeta ili Ministarstva znanosti, obrazovanja i športa Republike Hrvatske ili nekog drugog ministarstva koja je dana na korištenje Centru.

Centar je obavezan održavati popis sve racunalne opreme, s opisom ugradenih komponenti, inventarnim brojevima i slicno.

Centar jednako brine o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Oprema se cuva od oštecenja i otudenja.

Centar je dužan osoblju CARNeta/SRCE-a dozvoliti pristup opremi u vlasništvu CARNeta/MZOS-a /ministarstva koja se nalazi u Centru.

Odgovornost za racunalnu opremu

Za fizicku sigurnost opreme odgovoran je rukovoditelj ustanove, ravnatelj. On odgovornost za grupe uredaja ili pojedine uredaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrduju da su preuzeli opremu.

Centar je dužan razraditi procedure kojima se nastoji sprijeciti otudenje i oštecenje racunalne opreme. Osoba zadužena za sigurnost (vratar i sl.) provjerava je li oprema koja se iznosi ima potrebne pratece dokumente, izdatnice, radne naloge za popravak itd.

Osiguranje neprekidnosti poslovanja

Kako bi se u slucaju nezgoda (poput kvarova na sklopovlju, požara, ili ljudskih grešaka) podaci sacuvali, potrebno je redovito izradivati rezervne kopije svih vrijednih informacija, ukljucujuci i konfiguraciju software-a. Preporucuje se izraditi više kopija i cuvati ih na razlicitim mjestima, po mogucnosti u vatrootpornim ormarima.

Procedura za izradu rezervnih kopija razradena je u zasebnom dokumentu. Potrebno je zadužiti konkretne djelatnike za izradu i cuvanje kopija informacija, te ih obavezati na cuvanje povjerljivosti informacija.

Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kriticnih sustava. Cuva ih se u pisanom obliku, kako bi se u slucaju nesrece, 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 racunalima, vec na rezervnoj opremi (koju bi trebalo osigurati zaposlenicima zaduženim za te poslove), u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Centar zadržava pravo nadzora nad instaliranim software-om i podacima koji su pohranjeni na umreženim racunalima, te nad nacinom korištenja racunala.

Nadzor se smije provoditi radi:

- Osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa.
- Provodenja istrage u slucaju 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 Centar za to ovlastio. Pri provodenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. U slucajevima 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 racunalnu opremu koja se nalazi u prostorijama Centra i prikljucena je u mrežu Centra, na sav instalirani software, te na sve mrežne servise.

Pravila su dužni poštivati i provoditi svi zaposleni, vanjski suradnici koji po ugovoru obavljaju odredene poslove, studenti i drugi korisnici usluga Centra.

Provodenje

Svi korisnici su dužni pomoci osobama zaduženim za nadzor informacijskih sustava, na taj nacin što ce im pružiti sve potrebne informacije i omoguciti im pristup prostorijama i opremi radi provodenja nadzora.

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

Pristup ukljucuje:

- pristup na razini korisnika ili sustava svoj racunalnoj opremi,
- pristup svakoj informaciji, u elektronickom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Centra, ili oprema Centra služi za njezin prijenos,
- pristup radnom prostoru (uredu, sigurnoj zoni itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Centra.

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu se mogu uskratiti prava korištenja mreže i njezinih servisa. Ostali korisnici usluga centra koji se ogluše na pravila o nadzoru mogu podlijezati ugovornim sankcijama uz uskracivanje prava korištenja mreže i njezinih servisa.

Prakticna primjena sigurnosne politike

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

- obnoviti postojeci popis racunala, pisaca i drugih informatickih uredaja,
- postojecu skicu mreže provjeriti i ažurirati novim prikljuccima. Sve mrežne prikljucke numerirati na razumljiv i jedinstven nacin u Centru, tako da se svaki prikljucak može brzo pronaci.

Nakon usvajanja sigurnosne politike, treba napraviti inventuru kompletne racunalne opreme, ukljucujuci mrežne i komunikacijske uredaje.
Za svako racunalo potrebno je evidentirati koji se operacijski sustav na njemu koristi, te popisati aplikacije koje su na njemu instalirane.
Centar u svakom trenutku treba imati ažurirani popis software-a koji se koristi u LAN-u, kako bi mogla brinuti o licenciranju.
Zbog svega, gore navedenog potrebno je organizirati tim koji ce izvršiti detaljan popis sve informaticke opreme, software-a, podataka i mrežnih instalacija. U svrhu što efikasnije prakticne primjene sigurnosne politike Centar se nada maksimalnoj podršci Ministarstva znanosti, obrazovanja i športa Republike Hrvatske.

Dokumenti u prilogu

S nabavom nove informaticke opreme i razvojem informacijskih sustava u Centru, kao i s porastom ovisnosti o njihovom ispravnom funkcioniranju, javlja se potreba da se sigurnosna politika dopuni pratecim dokumentima, u kojima se definiraju pravila za pojedina podrucja rada. Prateci dokumenti su razne upute (radne upute). Pisani su kao upute za rješavanje konkretnih problema i mogu se cešce mijenjati. Pratece upute su sastavni dio Sigurnosne politike Studentskog centra Split. To su:
Dokument 1: Uputa o rukovanju zaporkama
Dokument 2: Uputa o korištenju elektronicke pošte
Dokument 3: Uputa o antivirusnoj zaštiti
Dokument 4: Uputa o zaštiti od spama
Dokument 5: Uputa o zaštiti od *špijunskih* i *nametnih* programa
Dokument 6: Uputa o izradi kopija podataka
Dokument 7: Uputa o rješavanju sigurnosnih incidenata
Dokument 8: Uputa o rukovanju povjerljivim informacijama
Dokument 9: Uputa o korištenju informacijskih sustava Centra za vanjske suradnike i korisnike Centra
Dokument 10: Uputa o korištenju prijenosnih racunala Centra
Dokument 11: Uputa o obrazovanju osoba zaduženih za sigurnost racunalnog sustava
Dokument 12: Izjava o cuvanju povjerljivih informacija
Dokument 13: Uputa o pristupu Internetskim stranicama

Sigurnosna politika informacijskih sustava STUDENTSKOG CENTRA Split temelji se na dokumentu *Sigurnosna politika informacijskih sustava za clanice CARNeta (prijedlog)* (*http://sistemac.carnet.hr/sigurnost/sigurnosna_politika_ustanove.pdf*, prosinac 2003.

Pripremio:

Davor Bakotin, dipl. ing.

Ravnateljica:

Gordana Raos, dipl. iur.

Dokument 1

Uputa o rukovanju zaporkama

Svrha

Prosjecan korisnik nerijetko smatra kako ne mora brinuti o sigurnosti jer njegovo racunalo ne sadrži vrijedne informacije. No kompromitiranjem jednog osobnog racunala u lokalnoj mreži ili jednog korisnickog racuna na poslužitelju napadac 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 racunala neprestano raste, ljudske sposobnosti stagniraju. Današnja racunala mogu brzo dekriptirati jednostavne zaporke, dok u isto vrijeme vecina ljudi ne može pamtiti složene zaporke dugacke osam znakova.

Doseg

Svi korisnici (zaposlenici, suradnici i clanovi) Centra koji u svome radu koriste racunala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnicki ugraditi u sve sustave koji to omogucavaju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

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

2. Rijeci iz rjecnika

   Ne koristiti ih, jer hackeri posjeduju zbirke rjecnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

   Na primjer: dje5oJka. Na prvi pogled besmislena i teška za pamcenje, ova je zaporka izvedena iz rijeci djevojka. 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 slucaju ne smiju otkriti. Hakeri nastoje izmamiti zaporke lažno se predstavljajuci kao administratori. Obuceni administratori imaju mogucnost rješavanja probleme i bez poznavanja korisnickih zaporki.

7. Cuvanje zaporke

   Zaporke se ne ostavljaju na papiricima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezakljucanim ladicama itd. Korisnik je odgovoran za tajnost svoje zaporke, te mora naci nacin da je sakrije. Ukoliko korisnik zaboravi zaporku, administrator ce mu omoguciti da unese novu.

8. Administriranje zaporki

Ukoliko sustav dopušta na racunalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj nacin da se korisnicki racun zakljuca nakon tri neuspjela pokušaja prijave. Administratori su dužni konfigurirati autentikaciju tako da zaporke zastare nakon 90 dana, te onemoguciti korištenje zaporki koje su vec potrošene, ako sustav to dopušta.

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

Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. Centar je obavezan obuciti korisnike prilikom kreiranja sigurnih zaporki.

U slucaju ponovljenog ignoriranja ovih pravila Centar može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogucnost ugrožavanja integriteta i sigurnosti sustava i podataka, a u u skladu sa odgovarajucim internim pravilnikom Centra.

Dokument 2

Uputa o korištenju elektronicke pošte

Elektronicka pošta dio je svakodnevne komunikacije, poslovne i privatne. S obzirom na moguce posljedice treba razmotriti sve aspekte elektronicke komunikacije.

Protokol koji se koristi za prijenos elektronicke pošte, SMTP ili Simple Mail Transport Protocol, nije od samog pocetka 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 elektronicke pošte:

1. Nesigurnost protokola
    - Poruke putuju kao obican tekst, te ih je lako presresti i procitati, ili cak izmijeniti sadržaj.
    - Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.
    - Protokoli za citanje elektronicke pošte, POP i IMAP, u svom osnovnom obliku šalju korisnicko ime i zaporku kao obican tekst, pa ih je moguce presresti i procitati. Stoga je potrebno, kad god je to moguce, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.
2. Nezgode
    - Uvijek je moguce pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu. Time može nastati nepopravljiva šteta – ne možete zaustaviti poruku koja je vec otišla. Ako se umjesto Reply (Odgovori) pritisne Reply All (Odgovori svima), poruka ce umjesto jednom primatelju otici na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
    - Cesta 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, slicna onoj koju zapravo želite.
3. Nesporazumi
    - Ljudi su skloni pisati e-mail poruke na opušteniji nacin. To može dovesti do nesporazuma ako druga strana ne shvaca poruku na isti nacin. Stoga službene dopise pišite u službenom tonu.
    - Iza vašeg imena u e-mail adresi nalazi se ime ustanove. Pišuci, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznacite kada je izneseni stav vaše privatno uvjerenje.
4. Otkrivanje informacija
    - Poruke namijenjene jednoj osobi, zacas 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 prosljedivanje poruke,
        - slucajnom omaškom, na primjer nehoticnim klikom mišem na pogrešnu ikonu - Reply All (Odgovori svima) umjesto Reply (Odgovori).
    - Stoga poslovne dopise koji sadrže osjetljive informacije treba oznaciti kao povjerljive, kako bismo primatelja obavezali na diskreciju.

- U slucaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Centar se obavezuje cuvati povjerljivost takvih poruka, ali to nece moci garantirati budu li poruke tretirane kao dokazni materijal u istrazi ili u mogucem sudskom procesu.

5. Radna etika

- Veliki broj poruka koje treba svakodnevno procitati može vam oduzeti znatan dio radnog vremena. Stoga ogranicite broj privatnih poruka.
- Lancane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuce novac (*pomozite nesretniku kojem treba operacija, otvorite racun kako bi svrgnuti diktator mogao izvuci novac iz nestabilne africke države...*). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a *Hoax recognizer*
- Spam, slanje neželjenih komercijalnih poruka, sve više opterecuje promet na Internetu, te oduzima vrijeme, cak i ako brišete takve poruka bez citanja. Centar ce filtrirati spam na poslužitelju elektronicke pošte. Obaveza je korisnika da sami ne šalju takve poruke.

6. Povreda autorskih prava

- Svaka poruka elektronicke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljedivanje tude poruke morate tražiti dozvolu njezina autora.
- Prilozi koji se šalju uz elektronicke poruke mogu sadržavati autorski zašticene informacije, na primjer glazbu, filmove, clanke itd. Primajuci i šaljuci takve sadržaje možete izložiti tužbi ne samo sebe, vec i Studentski centar Split.

Zbog svega nabrojanog korištenje elektronicke pošte smatra se rizicnom djelatnošcu, te su korisnici obvezni pridržavati se sljedecih pravila:

- Zaposlenicima se otvara korisnicki racun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj kolicini, ukoliko to ne ometa redoviti rad. Za privatne potrebe mogu se koristiti za to namijenjene *HR-F domene*.
- Pišuci poruke, budite svjesni da ne predstavljate samo sebe, vec i ustanovu za koju radite.
- Pridržavajte se *netiquete*, pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajucih poruka, za seksualno ili bilo koje drugo uznemiravanje.
- Nije dozvoljeno slanje lancanih poruka kojima se opterecuju mrežni resursi a ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom, te na taj nacin 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 ce automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, nece biti isporucena, a pošiljatelj i primatelj ce biti o tome obaviješteni. Poruka ce provesti odredeno vrijeme u karanteni, odakle ju je moguce na zahtjev primatelja izvuci. Nakon odredenog vremena, obicno mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Centar zadržava pravo konfiguriranja sustava na nacin da ne obavještava pošiljatelja i primatelja o otkrivenom virusu u poruci, a narocito ukoliko se ustanovi da se radi o tzv. virusima koji lažiraju adresu.
- Centar zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slucaju istrage uzrokovane mogucim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke koje su dio poslovnog procesa treba arhivirati i cuvati propisani vremenski period kao i dokumente na papiru.

Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog djelatnika, ravnatelj zatraži od administratora poslužitelja elektronicke pošte otvaranje korisnickog racuna.

Pri prestanku radnog odnosa, ravnatelj je dužan najkasnije u roku od osam dana zatražiti zatvaranje korisnickog racuna.

Ako zaposlenik nakon odlaska u mirovinu zatraži nastavak korištenja korisnickog racuna to mu se, uz suglasnost CARNetove službe za clanice, 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 korisnicki racun na poslužitelju Centra.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila Centra može pokrenuti stegovni postupak, a u skladu sa odgovarajucim internim pravilnikom Centra. U slucaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnicki racun i uskratiti pravo korištenja servisa elektronicke pošte.

Dokument 3

Uputa 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 nazocnost, presrecu unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu poslati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg racunala, kako bi nad njim kontrolu preuzeli hackeri.

Stoga je zaštita od virusa obaveza Centra, administratora racunala i svakog korisnika.

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

- na poslužiteljima elektronicke pošte,
- na internim poslužiteljima, gdje se stavlja centralna instalacija,
- na svakom osobnom racunalu korisnika.

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

Korisnici ne smiju samovoljno iskljuciti antivirusnu zaštitu na svome racunalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti antivirusni program, korisnici prethodno obavijestiti administratora informatickog sustava.

Nepridržavanje

Korisnik koji samovoljno iskljuci antivirusnu zaštitu na svom racunalu, te na taj nacin izazove štetu, može podlijezati odgovarajucim sankcijama u skladu sa odgovarajucim internim pravilnikom Centra.

Dokument 4

Uputa o zaštiti od spama

Svrha

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektronicke pošte najjeftiniji su nacin reklamiranja. Cijenu placaju korisnici i tvrtke, jer citanje i brisanje neželjenih poruka troši njihovo radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvuci primatelja u kriminalne aktivnosti, na primjer otvaranje racuna 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 elektronicke pošte dužni su konfigurirati racunala na taj nacin da se što više neželjenih poruka zaustavi.

Prva je mogucnost da se definira ulazni filter koji ce 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 pronadenih adresa nece se primati.

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

Trecu razinu zaštite mogu odredivati sami korisnici. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguce pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta ukljucivanje bodovanja i konfiguriranje preusmjeravanja oznacenih poruka.

Informaticar zadužen za sigurnost ce 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 cesto lažna i šire zablude.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeci racunalnu opremu koja pripada ustanovi.

Nepridržavanje

Korisnici koji se ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke mogu podlijezati odgovarajucim sankcijama u skladu sa odgovarajucim internim pravilnikom Centra.

Dokument 5

Uputa 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 cesto instaliraju na racunalo bez znanja korisnika te na racunalu cine razne, štetne radnje. Posljedice mogu biti: usporeni rad racunala, promijenjena pocetna web stranica, neprekidna aktivnost na internetu bez obzira što je modem iskljucen, otvaranje drugog prozora iz cista mira,… Najcešce dolaze *potiho* uz neki besplatan software.

Pravila za administratore

Administratori osobnih racunala dužni su na racunalo instalirati odgovarajuci *antišpijunski* program koji omogucava uklanjanje špijunskih programa s racunala. Program je potrebno konfigurirati tako da ga može pokrenuti i tzv. obicni korisnik racunala.

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 racunalo ne instaliraju skriveni program, a oni koji namjerno instaliraju špijunske programe podlijezati ce odgovarajucim sankcijama u skladu sa odgovarajucim internim pravilnikom Centra.

Dokument 6

Uputa o izradi kopija podataka

Ravnatelj centra odreduje tko je od zaposlenika zadužen za izradu kopija pojedine vrste podataka. Vecu pozornost treba obratiti na spremanje važnijih podataka (baza podataka, mail, web, dns, …).

Izradu kopija podataka treba prilagoditi postojecoj tehnološkoj osnovi kojom raspolaže Centar.

Osnovna strategija izrade kopija:

- kopija podataka iz baze podataka informacijskog sustava se izraduje svakodnevno, na drugoj particiji diska, na traci automatskim nocnim backupom, a jednom tjedno i na traci rucnim backupom, svaka 3 mjeseca se radi potpuni backup.

- kopija podataka kljucnih servisa (mail, web, dns,…), kao i osobnih podataka sa poslužitelja, se izraduje jednom tjedno ili najkasnije mjesecno,

- kopije podataka sa osobnih racunala se izraduju prema potrebi.

Podatke s osobnih racunala spremaju korisnici (zaposlenici) pojedinacno. Ukoliko im je u tome potrebna pomoc, pomaže im administrator informatickog sustava.

Zaposlenici centra, kao i vanjski suradnici, ne mogu koristiti vlastite medije za pohranu podataka (USB disk, disketa, CD, DVD,…) bez prethodnog odobrenja odgovorne osobe u Centru (u pravilu ravnatelj ili rukovoditelj odjela).

Dokument 7

Uputa o rješavanju sigurnosnih incidenata

Svrha

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

Prijava incidenta

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

Centar treba izraditi i održavati listu kontakt osoba kojima se prijavljuju problemi u radu racunala i servisa, te obrazac za prijavu incidenta. Listu treba uciniti široko dostupnom na nacin da se podijeli svim zaposlenima i/ili objavitije na oglasnim plocama i/ili 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 cuvaju minimalno 10 godina, kako bi mogli poslužiti za statisticke obrade kojima je cilj ustanoviti najcešce propuste radi njihova sprecavanja, 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 korisnicke procese. Ako sumnjaju da se racunalo koristi na nedozvoljen nacin, mogu izlistati sadržaj korisnickog direktorija, ali ne smiju provjeravati sadržaj korisnickih podatkovnih datoteka (npr. dokumenata ili e-mail poruka).

Provjera sadržaja korisnickih podataka je moguca 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 sljedecih pravila:

- Istragu provodi jedna osoba, ali uz nazocnost svjedoka kako bi se omogucilo svjedocenje o poduzetim radnjama.
- Prvo pravilo forenzicke istrage jest da se informacijski sustav sacuva u zatecenom stanju, odnosno da se ne ucine izmjene koje bi otežale ili onemogucile dijagnosticiranje.
- Najprije se napravi kopija zatecenog stanja (prijenosni medij npr. na traku, CD…), po mogucnosti na takav nacin da se ne izmijene atributi datoteka (npr. Unix naredbom dd).
- Dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- O istrazi se napiše izvještaj, kako bi u slucaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i cuvaju se na taj nacin da im pristup imaju samo ovlaštene osobe.

Dok ne bude formirano *Povjerenstvo za sigurnost*, pri rješavanju sigurnosnih problema, Centar ce koristiti pomoc CARNeta.

Centar može objavljivati statisticke 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 zakljucci o tome kako sprijeciti ponavljanje incidenta, ili se barem bolje pripremiti za slicne situacije. Ako je uzrok sigurnosnom incidentu bila pogreška covjeka, protiv odgovornih se mogu poduzeti sankcije.

Centar može osobama odgovornim za sigurnosni incident zabraniti fizicki pristup prostorijama ili logicki pristup podacima.

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

Dokument 8

Uputa o upravljanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uredeno 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 cije bi otkrivanje moglo nanijeti štetne posljedice Centru ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).

Profesionalna tajna odnosi na zanimanja poput lijecnika, svecenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u posebim odjelima Centra, osoba koje unose podatke u baze podataka o korisnicima ili sistem administratora poslužitelja, koji u nekim situacijama može doci u dodir s podacima koji pripadaju korisnicima racunala.

Dokumenti koji ulaze u Centar s nekom od oznaka povjerljivosti odreduju stupanj povjerljivosti svih dokumenata i informacija koje ce Centar proizvesti kao odgovor. U tom slucaju 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 oznaceni isticanjem vrste i stupnja tajnosti.

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

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

Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je ravnatelj Centra, koji ce izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za cuvanje povjerljivih informacija odnose se na sve zaposlenike Centra i vanjske suradnike koji dolaze u doticaj s osjetljivim podacima. Obaveza cuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Cuvanje povjerljivih informacija

Povjerljive informacije, tiskane na papiru ili u elektronickom obliku, snimljene na neki medij za pohranu podataka, cuvaju se u zakljucanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ogranicen pristup.

Pristup povjerljivim informacijama regulira se izradom liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vracanja 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 racunala.

Centar 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 ce 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 i sl.)

Povjerljive informacije u nacelu 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 Centra ce 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 obicnom vec kurirskom poštom. Na odredištu se predaju u ruke osobi kojoj su upuceni, što se potvrduje potpisom.

Ako se povjerljive informacije šalju elektronicki (npr. kao poruke elektronicke pošte), tada se moraju slati kriptirane.

Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dodu u Centar ne smiju se kopirati bez izricite dozvole pošiljatelja.

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

Osoblje koje poslužuje uredaje za kopiranje/tiskanje/skeniranje treba obuciti i obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

Uništavanje povjerljivih informacija

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

Ukoliko se zastarjela i rashodovana racunalna oprema daje na korištenje trecoj 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 cuvanju povjerljivosti informacija*.

Protiv zaposlenika koji ne poštuju pravila o cuvanju povjerljivih informacija bit ce pokrenut stegovni postupak, u skladu sa odgovarajucim internim pravilnikom Centra.

Centar treba vec u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Sastavni dio *Uputa o upravljanju povjerljivim informacijama* je i *Izjava o cuvanju povjerljivih informacija*.

Dokument 9

Uputa o korištenju informacijskih sustava Centra za vanjske suradnike, studente i korisnike Centra

Informacijski sustav centra

Vanjskim suradnicima i korisnicima ograniceno je korištenje informacijskih sustava Centra.
Korištenje pojedinih vrsta resursa dopušteno im je ograniceno i uz nadzor.

Mrežu treba segmentirati tako da racunala na mreži 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 racunala za vanjske korisnike i korisnike Centra nece se dozvoliti pristup osobnim racunalima zaposlenika.

Vanjskim suradnicima ili korisnicima Centra iznimno se može dopustiti i rad na nekom od racunala kojim se koriste zaposlenici Centra. Ravnatelj ce odrediti odgovorne djelatnike (npr. voditelje odjela) koji ce dopustiti rad na tim racunalima.

Ispis i kopiranje podataka

Kada koriste neko od racunala kojim se koriste zaposlenici Centra, korisnici usluga Centra i vanjski suradnici ne mogu koristiti vlastite medije za pohranu podataka (disketa, CD, DVD, USB uredaje…) bez prethodnog odobrenja odgovorne osobe u Centru.

Nepridržavanje

U slucajevima kada se studenti, korisnici Centra 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 usluga Centra u skladu sa odgovarajucim internim pravilnikom Centra.
Kod vanjskih suradnika mogu se razmatrati i aktivirati ugovorom predvidene i/ili zakonske sankcije.

Dokument 10

Uputa o korištenju prijenosnih racunala Centra

Svrha

Centar je osigurao je odredeni broj prijenosnih racunala za korištenje.

Pravila

1. Ova racunala su prvenstveno namijenjena mobilnim korisnicima, ali mogu se koristiti i u druge svrhe, vezane uz ovaj Centar, uz odobrenje ravnatelja.
Takoder, mogu ih koristiti i vanjski i korisici usluga, ali samo u Centru i uz nadzor i odobrenje administratora informatickog sustava.

2. Ova racunala trebaju se koristiti savjesno i pažljivo, kako bi se osigurala njihova ispravnost, a time i mogucnost korištenja. S obzirom na ogranicena sredstva, Centar nije u mogucnosti svako malo kupovati nova racunala. Zabranjuje se korisnicima da narušavaju fizicki integritet racunala na bilo koji nacin (lupanje, udaranje, trganje, itd.). Takoder, zabranjuje se korisnicima da samovoljno vrše „popravak“ neispravnih racunala. Ukoliko neko racunalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni to prijaviti administratoru informatickog sustava.

3. S obzirom na mogucnost neželjenih problema s racunalima, bilo da se radi o software-skim ili hardware-skim problemima, na mogucnost gubljenja, nestanka, odnosno otudivanja racunala ili pojedinih dijelova, vodit ce se stroga evidencija o korištenju pojedinog racunala. U tu svrhu, bit ce napravljena lista s rasporedom korištenja – tko je koristio koje racunalo, u koje vrijeme, tko je racunalo preuzeo i tko ga je vratio. Racunala ce biti smještena kod administratora informatickog sustava, a preuzeti ih mogu ili vanjski suradnici ili korisici usluga uz odobrenje ravnatelja, a preuzimanje i vracanje osvjedocit ce svojim potpisom na gore spomenutu listu. Ukoliko ce se racunala koristiti izvan radnog vremena administratora informatickog sustava, bit ce ih potrebno preuzeti prije završetka radnog vremena administratora informatickog sustava te ih vratiti u dogovoru sa njim, osim ako se ne zadužuju.

4. U slucaju potrebe instalacije dodatnih aplikacija, potrebno je na vrijeme javiti se administratora informatickog sustava.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, Centar može pokrenuti odgovarajuci postupak u skladu sa odgovarajucim internim pravilnikom Centra. U slucaju ponovljenih težih prekršaja, korisniku se može uskratiti pravo korištenja prijenosnih racunala Centra, kao i naplatiti eventualna ucinjena šteta.

Dokument 11

Uputa o obrazovanju osoba zaduženih

za sigurnost racunalnog sustava

Svrha

Bez kontinuiranog obrazovanja i pracenja najnovijih postignuca u zaštiti racunalnih i informacijskih sustava nema ucinkovite zaštite.

Pravila

Osobe zadužene za sigurnost racunalnog sustava obvezne su pratiti najnovija postignuca u zaštiti racunalnih i informacijskih sustava putem obrazovanja, pracenja literature i informiranja iz raznih izvora. Takoder su obavezne pohadati seminare o sigurnosti racunalnih sustava koji se održavaju u organizaciji CARNet-a.
Isto tako preporucuje se pracenje i ostalih seminara, kojima CARNet usavršava sistem inženjere.
O obukama se obavezno vode odgovarajuci zapisi koji su u skladu sa sustavom kvalitete Centra.

Resursi

Ravnatelj je dužan u okviru mogucnosti centra planirati i osigurati resurse i omoguciti osobama zaduženim za sigurnost racunalnog sustava da prate najnovija postignuca u zaštiti racunalnih i informacijskih sustava.

Dokument 12

STUDENTSKI CENTAR SPLIT	**IZJAVA O CUVANJU POVJERLJIVIH INFORMACIJA**	Stranica: Oznaka:	29 od 30 ZA-12-01
		Izdanje/preradba:	1.00.
		Datum:	01.08.2011..

Ova forma se koristi kao izjava o cuvanju povjerljivih informacija u skladu sa Sigurnosnom politikom Studentskog centra Split.

Postupak

Slijedite navedene korake:

1. Procitajte uputu o upravljanju povjerljivim informacijama Studentskog centra Split.
2. Potpišite se i upišite datum na predvideno mjesto.
3. Vratite potpisani dokument odgovornoj osobi.

Potpis

Svojim potpisom potvrdujem da se slažem sa slijedecim tvrdnjama:

1. Primio(la) sam i procitao(la) uputu o upravljanju povjerljivim informacijama Studentskog centra Split i razumio(la) njen sadržaj.
2. Slažem se da cu povjerljive informacije cuvati te da ih necu kopirati niti proslijedivati nikome izvan Studentskog centra Split, niti cu dozvoliti nikom drugom da kopira i umnožava informacije ili racunalne programe i to sve u skladu sa Uputom o upravljanju povjerljivim informacijama (Dokument 8 Sigurnosne politike Studentskog centra Split).

Split, ___.___._____.god. **Potpis davatelja izjave:**

_____

Potpis odgovorne osobe:

_____

Dokument 13

Uputa o pristupu Internetskim stranicama

Svrha

Pristup Internetu postao je u današnjem dobu nezaobilazan za prakticno bilo kojeg racunalnog korisnika. S druge strane, a kako je to navedeno i u prethodnim dokumentima ove politike, Internetom se širi sve više neželjenih, skrivenih, tzv. špijunskih programa koji mogu biti veoma opasni, virusi i crvi predstavljaju opasnost za informacijske sustave jer ugrožavaju funkcioniranje mreže i povjerljivost podataka, a Internetom putuje i sve više neželjenih komercijalnih poruka.

Pravila

U pravilu se svim zaposlenicima, suradnicima, studentima i ostalim korisnicima usluga Centra koji rade sa racunalnom opremom dozvoljava pristup Internetu i to na kontrolirani nacin. Pravila pristupa u pisanom obliku definira i predlaže povjerenstvo za sigurnost, a ista odobrava ravnatelj. Kod definicije pravila u principu se vodi racuna o sigurnosnim aspektima mreža Centra (izbjeci potencijalne, u „svijetu Interneta“ dobro poznate opasnosti) te o (pre)opterecenju mreže ukupnim prometom. Pravila se postavljaju korištenjem web filtera (monitora i/ili vatrozida). Vode se i odgovarajuce cuvaju i pohranjuju zapisi o pristupu i aktivnosti na Internetu. Administrator informatickog sustava neposredno je zadužen za ovo.

Nepridržavanje

Korisnici su dužni pridržavati se svih pravila iz dokumenata ove sigurnosne politike buduci da su svi oni direktno ili indirektno vezani za pristup Internetu. Nepridržavanje može podlijezati odgovarajucim sankcijama u skladu sa odgovarajucim internim pravilnikom Centra. Ukoliko neki od korisnika ucestalo ili grubo narušava pravila definirana ovom sigurnosnom politikom može mu se, pored ostalog, i ograniciti ili potpuno zabraniti pristup Internetu.