Sveučilište u Rijeci
TEHNIČKI FAKULTET

PRAVILNIK
O SIGURNOSTI INFORMACIJSKIH SUSTAVA TEHNIČKOG FAKULTETA SVEUČILIŠTA U RIJECI

Rijeka, 2005.

Temeljem članka 33. Statuta Tehničkog fakulteta Sveučilišta u Rijeci, a sukladno Prijedlogu sigurnosne politike informacijskih sustava članica CARNet-a, donosim

PRAVILNIK
o sigurnosti informacijskih sustava
Tehničkog fakulteta Sveučilišta u Rijeci

Uvodne odredbe

Članak 1.

Ovim se Pravilnikom uređuje sigurnost upravljanja informacijskim sustavima na Tehničkom fakultetu u Rijeci (dalje: Fakultet), definiraju prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.

Novi zaposlenici dužni su se upoznati s njegovim odredbama prilikom zapošljavanja, a studenti prilikom otvaranja korisničkih računa.

Pravila rada i ponašanja koja su definirana sigurnosnom politikom odnose se na:

- svu računalnu opremu koja se koristi u prostorima Fakulteta,
- administratore informacijskih sustava,
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti,
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

Organizacija upravljanja sigurnošću

Članak 2.

Osobe koji se u radu koriste računalima dijele se na davatelje i korisnike informatičkih usluga.

Davateljima informatičkih usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava.

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

Korisnici informatičkih usluga dužni su:

- pridržavati se pravila prihvatljivog korištenja, to jest ne koristiti računala za radnje koje nisu u skladu sa važećim zakonima, etičkim i moralnim normama, Etičkim kodeksom Sveučilišta u Rijeci i sigurnosnom politikom Fakulteta,
- izabrati kvalitetnu zaporku i povremeno je mijenjati,
- prijaviti svaki sigurnosni incident,
- ukoliko korisnici u svom radu proizvode podatke i dokumente, odgovorni su za vjerodostojnost tih podataka, te za njihovo čuvanje kao i za izradu sigurnosnih kopija podataka.

Članak 3.

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

Članak 4.

Svaka aplikacija koju Fakultet koristi za obradu podataka, a koja je od vitalne važnosti za Fakultet ili njegov dio, mora imati glavnog korisnika.

Glavnog korisnika aplikacije određuje dekan na temelju specifičnosti pojedine aplikacije i odgovornosti zaposlenika.

Glavni korisnik je u pravilu voditelj određene ustrojbene jedinice ili nositelj nekog projekta.

Zaposlenici kojima je glavni korisnik nadređen unose podatke i odgovaraju za vjerodostojnost tih podataka.

Glavni korisnik odgovaran je za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba. Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.

Članak 5.

Osoba čije je prvenstvena briga sigurnost informacijskih sustava je Voditelj sigurnosti. Voditelja sigurnosti imenuje dekan.

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

Članak 6.

Ekipu za hitne intervencije čine djelatnici Računalnog centra (nadalje RC) i CARNet sistem inženjer poslužitelja kojeg je za to ovlastio Voditelj sigurnosti. Ekipu za hitne intervencije imenuje Voditelj sigurnosti.

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

Članak 7.

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

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

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

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

Članak 8.

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

Administratori su dužni prijaviti incidente Votitelju 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 ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla te moraju potpisati Izjavu o čuvanju povjerljivih informacija.

Članak 9.

Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova, te ostale poslove pri upravljanju mrežom vrši RC.

Zahtjev za priključivanje računala na mrežu daje se isključivo RC-u koji provodi daljnje korake za priključivanje računala na mrežu.

RC je dužan voditi Popis mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala. Administratori CARNet-ovih poslužitelja dužni su voditi Popis javnih adresa računala.

Članak 10.

Fakultet je dužan izraditi poseban pravilnik za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Do donošenja ovog pravilnika, spajanje na mrežu navedene opreme dopušteno je samo uz pismeno dopuštenje dekana Fakulteta i uz nadzor djelatnika RC-a.

Gostujuća računala smiju se priključiti na lokalnu mrežu samo na za to predviđenim mjestima u tzv. zelenoj zoni. (informatičke učionice i predavaonice).

Za korištenje bežičnih mrežnih resursa izradit će se poseban dokument kojim će se definirati uvjeti i načini korištenja tih resursa, metode enkripcije i autentifikacije uređaja i korisnika, te ostale sigurnosno važne postavke.

Članak 11.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Dekan zadužuje odgovornu osobu za instaliranje softvera i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom, mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.

Sve korisnike treba obavezati na poštivanje autorskih prava, potpisivanjem izjave o tome da upoznati s Politikom prihvatljivog korištenja i da je prihvaćaju.

Članak 12.

Povjerenstvo za sigurnost imenuje dekan, a sastavljeno je od prodekana, CARNet koordinatora, voditelja sigurnosti, glavnih korisnika, predstavnika studenata i predstavnika oštećenih korisnika ili korisnika osobno.

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

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

U slučaju sigurnosnog incidenta prouzrokovanog od strane osoba koje nisu fakultetski korisnici, Povjerenstvo daje CARNet koordinatoru nalog za prijavu sigurnosnog incidenta CERT-u koji se nalazi u sastavu CARNet-a.

Fizička sigurnost

Članak 13.

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

Voditelj sigurnosti kreira, vodi i održava popis osoba koje imaju pristup u zaštićena područja, a osoblje na portirnici mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Članak 14.

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

Voditelj sigurnosti je dužan održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone. U pravilu su to samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme.

Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, poplava, požara i sl. te treba poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Članak 15.

U navedene prostorije pristup nije dozvoljen osobama koje nisu korisnici usluga ni studentima, a dozvoljen je samo onim osobama koje je ovlastilo dekan Fakulteta izravno ili putem voditelja sigurnosti.

Članak 16.

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

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

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

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

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

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

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

Sigurnost opreme

Članak 17.

Fakultet dijeli svu aktivnu i pasivnu opremu u grupe prema zadaćama:

- zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.), i
- intranet je privatna mreža Fakulteta, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže,
- extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije; u ovu grupu spadaju interni modemski

ulazi (ako ih Fakultet ima), veze lokalnih baza podataka sa središnjim poslužiteljima (LDAP, ISVU, X-ice, baze knjižnice) i sl.

Članak 18.

Fakultet je obavezan održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.

Fakultet je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Fakultetu.

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

Računalna oprema koja pripada Fakultetu daje se korisnicima na raspolaganje radi obavljanja poslova vezanih uz redovno poslovanje fakulteta i nije ju dopušteno koristiti za obavljanje privatnih poslova korisnika.

Fakultet zadržava pravo nadzora nad načinom korištenja računalne opreme.

Privatna računala i računalnu opremu nije dopušteno priključivati na fiksnu računalnu mrežu Fakulteta, osim uz odobrenje dekana.

Računala i računalnu opremu nije dopušteno iznositi izvan prostora Fakulteta bez uredno ovjerene Potvrde o korištenju opreme izvan Fakulteta. Potvrdu izdaje dekan, na obrazloženi zahtjev korisnika. Korisnici koji opremu koriste izvan prostora Fakulteta odgovorni su za tu opremu kao i za sve posljedice koje proizlaze iz korištenja iste.

Osiguranje neprekidnosti poslovanja

Članak 19.

Kako bi se sačuvali podaci u slučaju nezgoda, kvarova na sklopovlju, požara ili ljudskih grešaka, neophodno je redovito izrađivati rezervne kopije svih podataka važnih za održavanje vitalnih funkcija informacijskog sustava i sklopovlja.

Prethodni stavak prvenstveno se odnosi na kopije sustava središnjih poslužitelja, knjižničkog poslužitelja, računovodstvenih podataka i podataka o konfiguraciji softvera neophodnog za funkcioniranje mreže.

Članak 20.

Za izradu rezervnih kopija podataka središnjih poslužitelja zaduženi su CARNet sistem inženjeri koji administriraju te poslužitelje. Za neprekidnost rada središnjeg poslužitelja odgovoran je administrator istog poslužitelja.

Za izradu rezervnih kopija podataka knjižničkog poslužitelja zadužena je tvrtka s kojom Fakultet ima ugovor o održavanju knjižničke programske podrške.

Za izradu rezervnih kopija podataka važnih za održavanje vitalnih mrežnih funkcija i računala važnih za podršku korisnicima, nadležna je osoba iz RC-a koju imenuje voditelj sigurnosti.

Članak 21.

Fakultet je dužan izraditi zaseban dokument u kojem se definiraju procedure za izradu rezervnih kopija, imenuju odgovorne osobe, određuje potrebna oprema, te prostor za čuvanje kopija.

Radi osiguranja neprekinutosti poslovanja, Fakultet je dužan razraditi procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće. Dokumentaciju čuva voditelj sigurnosti.

Osobe zadužene za izradu rezervnih kopija su dužne povremeno provjeravati upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi, u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Članak 22.

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

Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa,
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident,
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Fakultet za to ovlastio.

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

Članak 23.

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 Fakulteta, ili oprema Fakulteta služi za njezin prijenos,
- pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta.

Članak 24.

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

Korištenje računalne opreme Fakulteta

Članak 22.

Nedozvoljenim se smatra svako korištenje računala na način koji bi doveo do povrede važećih zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Fakultet.

Lakšim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- ograničena uporaba nelicenciranog softvera,
- skidanje (download) autorski zaštićenih datoteka bez plaćanja naknade ako su iste javno dostupne,
- skidanje (download) i(ili) distribucija sadržaja koji nije primjeren akademskoj zajednici (pornografija i sl.),
- slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi,
- samovoljna instalacija softvera,
- korištenje neprihvatljivih aplikacija i servisa zbog kojih se narušava sigurnost informacijskih sustava, nepotrebno troše mrežni resursi ili se nanosi bilo kakva materijalna i(ili) nematerijalna šteta Fakultetu,

- korištenje računala Fakulteta i ostalih informatičkih resursa Fakulteta u svrhe koje nisu u skladu s Etičkim kodeksom Sveučilišta u Rijeci.

Težim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.),
- provaljivanje na druga računala,
- traženje ranjivosti i sigurnosnih propusta; korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Fakultetu ili ne,
- napad uskraćivanjem resursa na druga računala,
- vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,
- korištenje mrežnih resursa Fakulteta na način priključivanja vlastitih – privatnih računala na računalnu mrežu Fakulteta.

Članak 23.

Fakultet zadržava pravo procjene prihvatljivog korištenja računalne opreme.

Uprava Fakulteta će sankcionirati neprihvatljive oblike korištenja računalne opreme na Fakultetu sukladno težini neprihvatljivog korištenja, a na temelju procjene/mišljenja Povjerenstva za sigurnost.

Korisnici informatičkih resursa i opreme dužni su upozoriti upravu Fakulteta na svaki oblik neprihvatljivog ponašanja korisnika, a prvenstveno su dužni svojim primjerom pozitivno utjecati na promicanje prihvatljivog ponašanja ostalih korisnika.

Zaporke

Članak 24.

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

Minimalna dužina zaporke mora biti šest znakova. Za zaporku se ne smije koristiti riječi iz rječnika, niti imena bliskih osoba, ljubimaca, datume. U zaporci treba izmiješati mala i velika slova s brojevima

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije.

Članak 25.

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

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

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

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. U slučaju ponovljenog ignoriranja ovih pravila Fakultet može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

Antivirusna zaštita i zaštita od spama

Članak 26.

Zaštita od virusa je obavezna, a provode je davatelji informatičkih usluga nadležni za pojedini dio sustava, i to na:
- poslužiteljima elektroničke pošte – ovlašteni CARNet sistem inženjeri,
- na internim poslužiteljima Fakulteta – djelatnici RC-a ili CARNet sistem inženjeri,
- svakom osobnom računalu korisnika – administratori računala.

Osobe koje provode zaštitu od virusa nisu dužne čuvati elektronske poruke korisnika zaražene virusima.

Članak 27.

Osobe koje provode protuvirusnu zaštitu dužne su instalirati protuvirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u bazi virusa automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju zatražiti dozvolu od nadležnih davatelja informatičkih usluga.

Članak 28.

Administratori poslužitelja elektroničke pošte dužni su postaviti poslužitelje tako da prilikom primanja poruka konzultira 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.

Osobe koje provode zaštitu od spama nisu dužne čuvati spam - poruke poslane korisnicima

Rješavanje sigurnosnih incidenata

Članak 29.

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

Voditelj sigurnosti treba izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu mreže, mrežnih servisa i mrežne opreme, te obrazac za prijavu incidenta. Kontakt listu treba podijeliti svim zaposlenima i objaviti je na internim web stranicama Fakulteta.

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

Članak 30.

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

Članak 31.

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

Daljnju istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost, uz poštivanje slijedećih pravila:

- istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama,
- prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje,
- najprije se napravi kopija zatečenog stanja (na pr. na traku, CD…), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd),
- dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage,
- o istrazi se napiše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima,
- izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

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

Članak 32.

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

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

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

Završne odredbe

Članak 33.

Ovaj Pravilnik stupa na snagu danom objave na oglasnoj ploči i Internet stranici Fakulteta.

Dekan:
v.r.

Prof. dr. sc. Tonči Mikac, dipl. ing.

Rijeka, 10. 06. 2005.
Klasa: 003-05/05-01/03
Ur. br: 2170-57-01-05-01