Sigurnosna politika informacijskih sustava za članice CARNeta

Katolički bogoslovni fakultet u Đakovu

Sveučilište J. J. Strossmayera u Osijeku

verzija 2018-01

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
KATOLIČKI BOGOSLOVNI FAKULTET U ĐAKOVU

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Sadržaj

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
KATOLIČKI BOGOSLOVNI FAKULTET U ĐAKOVU

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Sigurnosna politika Katoličkog bogoslovnog fakulteta u Đakovu

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- svu računalnu opremu i pripadajuće programe koji se nalaze u prostorima KBF-a,
- administratora informacijskih sustava,
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti,
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

Organizacija upravljanja sigurnošću

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

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

Korisnici informatičkih usluga

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

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

Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim i moralnim normama i pravilima lokalne sigurnosne politike.
- Izbor kvalitetne zaporke i njezina povremena promjena.
- Prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi.

• Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To znači da, na primjer, moraju od davatelja usluga zatražiti da uspostave automatsku pohranu (backup) važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije.

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

Glavni korisnik

S obzirom da ustanova koristi aplikacije za obradu podataka, na primjer računovodstvene programe, programe za obradu knjižnične građe, itd., radi poboljšanja sigurnosti jedna osoba imenuje se glavnim korisnikom. U navedenom primjeru voditelj računovodstva bio bi glavni korisnik, odnosno voditelj knjižnice također bi bio glavni korisnik.

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

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

Ako se ukaže potreba, dekan KBF-a može imenovati i zamjenike glavnih korisnika za pojedine aplikacije.

Davatelji informatičkih usluga

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

Specijalisti za sigurnost

KBF će pri rješavanju sigurnosnih incidenata koristiti pomoć CARNeta. Pored toga, KBF će obrazovati i imenovati pojedince čija će zadaća biti briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

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

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

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

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

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

Administriranje računala

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

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

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

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

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti. 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 specijalistu za sigurnost, te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNetovu CERT-u.

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

Upravljanje mrežom

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

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

KBF će razraditi i pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Ne smije se dozvoliti da oni po svom nahođenju priključuju računala na mrežu ustanove, radi opasnosti od širenja virusa ili namjernih agresivnih

radnji, poput presretanja mrežnog prometa, prikupljanja informacija itd. KBF će odrediti priključna mjesta, na primjer u predavaonicama, gdje je dozvoljeno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se sa tog segmenta mreže dopre do ostalih računala na ustanovi.

Ukoliko će KBF koristiti bežičnu mrežu, morat će se osigurati da se ne može bilo tko priključiti na privatnu mrežu i snimati promet. To će se postići metodama enkripcije i autentikacije uređaja i korisnika, te odvajanja lokalnih IP adresa od bežićne mreže na zaseban segment!

Radi zaštite povjerljivih informacije pri prijenosu mrežom, poželjno je da takav promet bude kriptiran. KBF će u tom slučaju izdati pravilnik u kojem definira vrstu enkripcije, obvezan softver, procedure za dodjelu i čuvanje kriptografskih ključeva i slično (uz obavezu upravljanja wi-fi mrežom isključivo od strane CARNet koordinatora).

Instalacija i licenciranje softvera

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

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

Administrator ustanove mora imati osiguran nadzor i pristup svim računalima u bilo koje vrijeme, što omogućuje da se korisnici koji krše pravila odmah isključe s KBF LAN mreže do daljnjega!

Isto povlači i odbijanje instalacije dobivenog licencnog softvera.

Povjerenstvo za sigurnost informacijskih sustava

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

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

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

Fizička sigurnost

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

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

Sigurne zone

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

KBF 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. Stoga je poželjno administratorima osigurati radni prostor odvojeno od prostorija u kojima je smještena kritična oprema.

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

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

Vanjske tvrtke

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

KBF 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.

KBF 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, KBF može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije KBF-a radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti KBF.

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

Sigurnost opreme

Klasifikacija računalne opreme

KBF 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 KBF-a, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.

- Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).

- Wi-fi mreža (kao opcija), otvorena je za djelatnike i studente uz nadzor isključivo administratora i osoba za održavanje opreme na zasebnom segmentu IP adresa van lokalne domene!

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

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

Podjela opreme prema vlasništvu

U prostorijama KBF-a nalazi se i oprema CARNeta i Ministarstva znanosti, obrazovanja i športa Republike Hrvatske i nadbiskupije Đakovačko-osječke, koja je dana na korištenje KBF-u.

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

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

KBF je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na KBF-u.

Odgovornost za računalnu opremu

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

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

Osiguranje neprekidnosti poslovanja

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

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

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

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

Nadzor nad informacijskim sustavima

KBF 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 KBF za to ovlastio (administrator).

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

Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama KBF-a, posebno na onu koja je priključena u mrežu CARNet, na sav instalirani softver, te na sve mrežne servise.

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

Provođenje

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

Isto vrijedi i za 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 KBF-a, ili oprema KBF-a služi za njezin prijenos,
- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni, itd.),
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži KBF-a.

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu uskratiti prava korištenja CARNetove 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,

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

• postojeću skicu mreže provjeriti i ažurirati novim priključcima; sve mrežne priključke numerirati na razumljiv i jedinstven način, 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. KBF u svakom trenutku treba imati ažurirani popis softwarea koji se koristi u LAN-u, kako bi se mogao 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, KBF se nada maksimalnoj podršci Ministarstva znanosti, obrazovanja i športa Republike Hrvatske, te se ubuduće očekuje odgovarajući broj zaposlenih informatičkih stručnjaka, kao i odgovarajuća informatička opremu te pripadajući software.

Prateći dokumenti

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

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Uz ovu *Sigurnosnu politiku* za KBF prilažu se i prateći pravilnici.

Prilozi:

1. Pravilnik o rukovanju zaporkama
2. Pravilnik o korištenju elektroničke pošte
3. Pravilnik o antivirusnoj zaštiti
4. Pravilnik o zaštiti od spama
5. Pravilnik o zaštiti od spywarea
6. Pravilnik o izradi kopija podataka
7. Pravilnik o rješavanju sigurnosnih incidenata
8. Pravilnik o rukovanju povjerljivim informacijama
9. Pravilnik o korištenju javnih računala
10. Pravilnik o korištenju fakultetskih prijenosnih računala
11. Pravilnik o dodjeljivanju AAI@Edu.hr elektroničkih identiteta

Dokument sastavio:

Marin Ivanišić, prof. matematike i informatike

sistem inženjer

_____

Dokument odobrio:

Izv. prof. dr. sc. Vladimir Dugalić
dekan

_____

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

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

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

2. Ne koristiti riječi iz rječnika

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

3. Izmiješati mala i velika slova s brojevima

   Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

   Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Preporuka je mijenjati zaporku barem jednom godišnje.

6. Tajnost zaporke

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

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

7. Čuvanje zaporke

Zaporke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama, itd. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije.

Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

8. Administriranje zaporki

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

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

Nepridržavanje

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

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 2: Pravilnik o korištenju elektroničke pošte

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

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

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 pritisne Reply All, poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.

• Česta je pogreška i kada se pokupi pogrešna adresa iz adresara.

• Neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.

3. Nesporazumi

• Ljudi su skloni pisati e-mail poruke na ležerniji, opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.

• Iza vašeg imena u e-mail adresi nalazi se ime ustanove. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. Otkrivanje informacija

• Poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi:

- (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki
- nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke
- slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply)

• Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.

• U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Ustanova se obavezuje čuvati povjerljivost takvih poruka, ali to ne može garantirati ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

• Velika količina poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih i zabavnih poruka.

• Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac *("pomozite nesretniku kojem treba operacija", "otvorite račun kako bi svrgnuti diktator mogao izvući novac iz nestabilne afričke države"...*). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a "Hoax recognizer"

• Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Ustanova će filtrirati spam na poslužitelju elektroničke pošte, ali je obaveza korisnika da sami ne šalju takve poruke.

6. Povreda autorskih prava

• Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora.

• Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke, itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i KBF.

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

• Zaposlenicima se otvara korisnički račun radi obavljanja posla.

• Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.

• Pridržavajte se pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.

• Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme (osim službenih mail lista).

• 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.

• KBF zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.

• U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.

• Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

Procedura za dodjelu e-mail adrese

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

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

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

Na koga se odnose pravila korištenja e-maila

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

Nepridržavanje

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 3: Pravilnik o antivirusnoj zaštiti

Svrha

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

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

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

Pravila

KBF 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 (samo licencirani AV programi)

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

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

Nepridržavanje

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

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 radno vrijeme i umanjuje produktivnost.

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

Pravila za administratore

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

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

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

Pravila za korisnike

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj (osim obavijesti).

Upozorenja na viruse su često lažna i šire zablude.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

Nepridržavanje

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 5: Pravilnik o zaštiti od spywarea

Svrha

Internetom se širi sve više neželjenih, skrivenih, tzv. špijunskih programa (spyware) 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, otvaranje drugog prozora iz čista mira, itd. Najčešće dolaze potiho uz neki besplatan software.

Pravila za administratore

Administratori osobnih računala dužni su na računalo instalirati odgovarajući antispyware 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 antispyware 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.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 6: Pravilnik o izradi kopija podataka

Dekan, u dogovoru sa sistem inženjerom, 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, itd.).

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

Osnovna strategija izrade kopija:

- Kopija podataka iz baze podataka glavnog servera se izrađuje svakodnevno, na drugoj particiji diska, te u određenim vremenskim intervalima i na traci ručnim backupom. Također, tri ili četiri puta godišnje radi se potpuni backup. Za navedeno je zadužen sistem inženjer ili osoba kojoj on povjeri obavljanje toga zadatka.

- Kopija podataka ključnih servisa (mail, web, dns, itd.), kao i osobnih podataka s poslužitelja, se izrađuje nekoliko puta mjesečno, najčešće jednom tjedno ili dvotjedno.

- Kopije podataka s osobnih računala se izrađuju prema potrebi.

Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ukoliko im je u tome potrebna pomoć, obraćaju se sistem inženjeru.

Zaposlenici i vanjski suradnici za izradu sigurnosnih kopija i pohranu podataka mogu koristiti ili medije dobivene od strane KBF-a ili vlastite medije. U bilo kojem slučaju, svaki pojedinac je sam odgovoran za sigurnost dotičnih.

Svaki korisnik javnih računala (info kabinet, knjižnica) sam je zadužen i odgovoran za sigurnost i pohranu osobnih podataka na javna računala. KBF, odnosno osobe zadužene za brigu o javnim računalima na KBF-u, ne izrađuju sigurnosne kopije privatnih podataka korisnika javnih računala te nisu odgovorni za njihov eventualni gubitak.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 7: Pravilnik o rješavanju sigurnosnih incidenata

Svrha

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

Prijava incidenta

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

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

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.

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

- Istragu provodi jedna osoba, ali uz prisutnost 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 CD, DVD, flash medij, itd.), 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 mogao poslužiti kao dokaz u eventualnim stegovnim ili sudskim procesima.

• Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

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

Sankcije

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

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

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

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

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 KBF-u ili njegovim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).

Profesionalna tajna odnosi se na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u tajništvu, referadi, pravnoj službi, 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 na KBF s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će KBF 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 dekan, 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 KBF-a 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.

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

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

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

Povjerljive informacije u načelu se ne daju putem telefona 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 KBF-a će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Prenošenje povjerljivih informacija

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

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

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

Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu na KBF ne smiju se kopirati bez izričite dozvole pošiljatelja.

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

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

Uništavanje povjerljivih informacija

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

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

Nepridržavanje

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

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

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti

će se ugovor. Stoga ustanova treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 9: Pravilnik o korištenju javnih računala (u Informatičkom klubu i Knjižnici)

Svrha

Katolički bogoslovni fakultet, u suradnji s MZOŠ i CARNetom, osigurao je studentima određeni broj javnih računala na kojima se može pristupiti na Internet, raditi seminarske i druge radove te poslužiti se u neku drugu obrazovnu ili akademsku svrhu. Računala se nalaze u Informatičkom klubu i Središnjoj nadbiskupijskoj i fakultetskoj knjižnici. Za njihovo korištenje donose se sljedeća pravila:

Pravila

1. Pravo korištenja javnih računala imaju djelatnici i studenti KBF-a (u daljnjem tekstu: korisnici).

2. Javna računala trebaju se koristiti savjesno i pažljivo, kako bi se osigurala njihova ispravnost, a time i mogućnost korištenja. S obzirom na ograničena sredstva, KBF nije u mogućnosti svako malo kupovati nova računala. Zabranjuje se korisnicima da narušavaju fizički integritet računala na bilo koji način (lupanje, udaranje, trganje kablova, itd.). Također, zabranjuje se korisnicima da samovoljno premještaju pojedine periferne uređaje (tipkovnice, miševe, monitore, itd.) ili da samovoljno vrše „popravak“ neispravnih računala. Ukoliko neko računalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni to prijaviti sistem inženjeru.

3. *Računala za pretraživanje u Središnjoj nadbiskupijskoj i fakultetskoj knjižnici* – određeni broj računala u Središnjoj nadbiskupijskoj i fakultetskoj knjižnici predviđen je samo za korištenje u svrhu pretraživanja baza podataka, članaka, tekstova i drugih materijala potrebnih u akademske i znanstvene svrhe. Navedena računala nisu predviđena za pisanje seminarskih, diplomskih i drugih znanstvenih radova, kao ni za korištenje Interneta u neke druge svrhe osim gore navedenih i stoga se u te svrhe ne smiju koristiti – za korištenje u te svrhe predviđena su i osigurana druga računala.

4. Korisnici su dužni pridržavati se etičkih i moralnih pravila prilikom korištenja javnih računala, kao i važećih zakona. Zabranjuje se pristup pornografskim, pedofilskim i sličnim sadržajima na Internetu; zabranjuje se korištenje i širenje takvih materijala na javnim računalima. Zabranjuje se nelegalno preuzimanje (download), korištenje i širenje zakonom zaštićenih materijala – softwarea, glazbe, e-knjiga, e-časopisa, dokumenata, filmova, itd. Zabranjuje se postavljanje, pokretanje i širenje malicioznih programa, kodova, virusa, trojanaca, spywarea, malwarea, spama, itd.

5. Zbog velikog negativnog utjecaja na *throughput*, brzinu i performanse pristupa Internetu, te zbog nekoliko slučajeva zlouporabe, do daljnjega se ograničava korištenje bittorent protokola.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, KBF može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja, korisniku se može uskratiti pravo korištenja javnih računala na KBF-u, kao i naplatiti eventualna učinjena šteta.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 10: Pravilnik o korištenju fakultetskih prijenosnih računala

Svrha

Katolički bogoslovni fakultet osigurao je određeni broj prijenosnih računala za korištenje u nastavi. Računala su opremljena svim potrebnim za izvođenje nastavnog programa Katoličkog bogoslovnog fakulteta.

Pravila

1. Ova računala su prvenstveno namijenjena profesorima za korištenje u nastavi, ali mogu se koristiti i u druge svrhe, vezane uz ovaj fakultet, uz odobrenje dekana. Također, mogu ih koristiti i studenti, ali samo u nastavi i uz nadzor i odobrenje profesora.

2. Ova računala trebaju se koristiti savjesno i pažljivo, kako bi se osigurala njihova ispravnost, a time i mogućnost korištenja. S obzirom na ograničena sredstva, KBF nije u mogućnosti svako malo kupovati nova računala. Zabranjuje se korisnicima da narušavaju fizički integritet računala na bilo koji način (lupanje, udaranje, trganje, itd.). Također, zabranjuje se korisnicima da samovoljno vrše „popravak“ neispravnih računala. Ukoliko neko računalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni to prijaviti sistem inženjeru.

3. S obzirom na mogućnost neželjenih problema s računalima, bilo da se radi o softwareskim ili hardwareskim problemima, na mogućnost gubljenja, nestanka, odnosno otuđivanja računala ili pojedinih dijelova, vodit će se stroga evidencija o korištenju pojedinog računala. U tu svrhu, bit će napravljena lista s rasporedom korištenja – tko je koristio koje računalo, u koje vrijeme, tko je računalo preuzeo i tko ga je vratio. Računala će biti smještena kod sistem inženjera, a preuzeti ih mogu ili profesori ili bideli, a preuzimanje i vraćanje osvjedočit će svojim potpisom na gore spomenutu listu. Ukoliko će se računala koristiti izvan radnog vremena sistem inženjera, bit će ih potrebno preuzeti prije završetka radnog vremena sistem inženjera te ih vratiti u dogovoru sa sistem inženjerom.

4. U slučaju potrebe instalacije dodatnih aplikacija, potrebno je na vrijeme javiti se sistem inženjeru.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, KBF može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja, korisniku se može uskratiti pravo korištenja fakultetskih prijenosnih računala, kao i naplatiti eventualna učinjena šteta.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 11: Pravilnik o dodjeljivanju AAI@Edu.hr elektroničkih identiteta

Što je elektronički identitet?

Elektronički identitet je skup podataka o pojedincu, koji se koristi za potrebe autentikacije (provjere identiteta) i autorizacije (provjere prava pristupa) nekom resursu (npr. web stranici, aplikaciji, računalnoj mreži, sustavu, itd.).

Elektronički identitet je skup podataka o pojedincu čije su sastavnice (atributi):

- ime i prezime
- brojčani identifikator osobe (JMBG, OIB)
- korisnička oznaka
- identifikator korisnika u ustanovi
- zaporka
- elektronička adresa
- poštanska adresa
- naziv i oznaka matične ustanove
- itd.

AAI@Edu.hr

AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Sustav AAI@EduHr tehnički je realiziran uporabom distribuiranih LDAP imenika. Svaka matična ustanova iz sustava MZOŠ ima vlastiti LDAP imenik u kojemu su pohranjeni elektronički identiteti korisnika iz te ustanove.

Sustav AAI@EduHR korisnicima (pojedincima) nudi jednostavno, sigurno i pouzdano korištenje svih resursa u sustavu AAI@EduHr uz pomoć jedinstvenog elektroničkog identiteta dobivenog na matičnoj ustanovi.

AAI@Edu.hr e-identitet

Elektronički identitet u sustavu AAI@EduHr je virtualni identitet na CARNet mreži kojega dobivaju pojedinačni korisnici iz ustanova članica CARNeta (učenici, nastavnici, studenti, profesori) i koji im

omogućuje korištenje CARNetovih usluga. Elektronički identitet služi pri autentikaciji i autorizaciji za razne CARNetove usluge, te je nužan za ostvarivanje prava na CARNetove usluge

Oblik: ***korisnik@ustanova.hr***

(npr. horvat@djkbf.hr, pperic@etfos.hr)

Dodjeljivanje e-identiteta

Elektronički identitet otvaraju nadležne matične ustanove i to ovisno o statusu osobe koja traži otvaranje elektroničkog identiteta.

Sve škole članice CARNeta imaju svog administratora imenika zaduženog za otvaranje elektroničkih identiteta u HUSO (Hosting usluga za srednje i osnovne škole) sustavu svim učenicima i nastavnicima.

Elektronički identitet u sustavu AAI@EduHr mogu dobiti pripadnici akademske i istraživačke zajednice u RH i to isključivo u nadležnoj matičnoj ustanovi. Pojedinci čija matična ustanova nije u sustavu AAI@EduHr mogu dobiti elektronički identitet na Javnom poslužitelju CARNeta (public.carnet.hr) slanjem pristupnice u CARNet.

Dodjeljivanje AAI@Edu.hr e-identiteta na KBF-u u Đakovu

Dodjeljivanje AAI@Edu.hr e-identiteta vrši sistem-inženjer.

Studentima se e-indetiteti dodjeljuju prilikom upisa na studij i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom ili prekidom studija. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, krajem listopada, a također i vanredno u određenim prilikama.

Profesorima, nastavnicima i asistentima se e-indetiteti dodjeljuju prilikom zapošljavanja i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom radnog odnosa ili nekim drugim razlogom. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, krajem listopada, a također i vanredno u određenim prilikama.

Ostalim djelatnicima ustanove se e-identiteti dodjeljuju ili na osobni zahtjev ili ukoliko je za vršenje službe nužno posjedovanje e-identiteta, i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom radnog odnosa ili nekim drugim razlogom. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, krajem listopada, a također i vanredno u određenim prilikama.

Uručivanje AAI@Edu.hr e-identiteta na KBF-u u Đakovu

Uručivanje podataka o e-identitetu vrši sistem-inženjer uručujući ih osobno svakom studentu, profesoru, djelatniku. U izvanrednim situacijama, moguće je i slanje podataka poštom. Također, uručivanje podataka profesorima u određenim situacijama može vršiti i tajništvo fakulteta.

Pomoć i podrška

Za sva pitanja oko AAI@Edu.hr e-identiteta, eventualne probleme, kao i za otvaranje AAI@edu.hr e-identiteta, ukoliko on već nije otvoren, može se javiti u ured sistem-inženjera (kabinet br. 5) svakim radnim danom od 08:00 do 15:00 sati.

Petra Preradovića 17, p. p. 54, HR – 31400 Đakovo
web: www.djkbf.hr/hr/sigurnosna-politika

Prilog 12: Obrada osobnih podataka koju provodi ustanova u sustavu AAI@EduHr

Zašto prikupljamo i obrađujemo vaše osobne podatke?

Katolički bogoslovni fakultet u Đakovu je matična ustanova - davatelj elektroničkih identiteta u sustavu AAI@EduHr. Vaši osobni podaci pohranjeni u našem LDAP imeniku služe tome da Vam omoguće korištenje usluga dostupnih kroz sustave AAI@EduHr, eduGAIN i eduroam osiguravajući pri tom pouzdanu, sigurnu i unificiranu prijavu za korištenje tih usluga.

Koje osobne podatke prikupljamo i obrađujemo?

Podaci koji mogu biti pohranjeni u našem LDAP imeniku popisani su na adresi:

https://www.aaiedu.hr/o-sustavu/imenicke-sheme/shema

Sve podatke koji su o vama pohranjeni u LDAP imeniku možete vidjeti (nakon prijave svojom korisničkom oznakom i zaporkom) kroz sučelje za održavanje imenika na adresi:

https://www.djkbf.hr/ldap/

Osim navedenih, prikupljamo i podatke o korištenju vašeg elektroničkog identiteta na način da bilježimo vrijeme i podatke o uređaju i sustavu preko kojeg je stigao zahtjev.

S kim dijelimo vaše osobne podatke?

Da bismo vam omogućili pristup uslugama, potrebnu razinu sigurnosti i kvalitete usluga unutar sustava, u trenutku pristupa nekoj usluzi u sustavu AAI@EduHr usluzi možemo proslijediti neke vaše osobne podatke. Točan popis podataka koje prosljeđujemo pojedinoj usluzi možete za svaku pojedinu uslugu pronaći na adresi:

https://www.aaiedu.hr/statistika-i-stanje-sustava/web-aplikacije

Koliko čuvamo vaše podatke?

Podatke o korištenju vašeg elektroničkog identiteta čuvamo 24 mjeseca (kako bismo mogli osigurati razinu sigurnosti i kvalitete usluge te zadovoljiti zakonske obaveze).

Po gubitku prava na e-identitet vaše osobne podatke brišemo iz LDAP imenika nakon najviše 90 dana.

Koja su vaša prava?

Vaša su prava, sukladno uvjetima iz Opće uredbe o zaštiti podataka, pravo na pristup osobnim podacima koje prikupljamo, pravo na brisanje (zaborav), pravo na ograničenje obrade, pravo na prenosivost podataka te pravo na ispravak osobnih podataka ukoliko su oni neispravni ili su izmijenjeni.