INSTITUT ZA HRVATSKI JEZIK I JEZIKOSLOVLJE
Institute of Croatian Language and Linguistics
Ulica Republike Austrije 16, HR-10000 Zagreb, tel.: ++385 1 3783 833, faks: ++385 1 3783 803,
e-pošta: ured@ihjj.hr, www.ihjj.hr, IBAN: HR6923900011100012967, OIB: 12268324202

Sigurnosna politika informacijskih sustava Instituta za hrvatski jezik i jezikoslovlje

1. Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- svu računalnu opremu koja se nalazi u prostorima Instituta
- administratore informacijskih sustava te pripadajuću tehničku službu
- korisnike, među koje spadaju zaposlenici, vanjski suradnici, volonteri i studenti
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

2. Organizacija upravljanja sigurnošću

Ključna stvar pri provođenju sigurnosne politike informacijskoga sustava jest da se u svakome trenutku točno zna tko je zadužen za obavljanje određenoga zadatka te tko odgovara za određeni segment opreme, odnosno računalnoga programa. Potrebno je, stoga, raspodijeliti zaduženja, obrazovati korisnike te oformiti stručna tijela za upravljanje sigurnošću.

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

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

Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To podrazumijeva da, ako ne postoji automatski sustav stvaranja sigurnosnih kopija, sami moraju 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.

4. Glavni korisnik

Kada postoji više korisnika koji rabe određenu aplikaciju za obradu podataka, primjerice računovodstveni program, radi poboljšanja sigurnosti jedna osoba imenuje se glavnim korisnikom. U navedenome primjeru voditelj računovodstva bio bi glavni korisnik.

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

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

5. Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji se brinu o radu računala, mreže i informacijskih sustava. Ugovoreni davatelj informacijskih usluga za Institut za hrvatski jezik i jezikoslovlje je CS Computer Systems d.o.o. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

6. Specijalisti za sigurnost

U Institutu za hrvatski jezik i jezikoslovlje ne postoji imenovani specijalist za sigurnost, već su članovi Službe za izdavaštvo i računalnu podršku odgovorni za koordinaciju korisnika s davateljem informatičkih usluga.

7. Administriranje računala

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

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

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

Posebnu pozornost administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štititi od neovlaštena pristupa.

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

Administratori su dužni prijaviti incidente tehničkoj službi te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ako 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. Kako bi ih Institut obvezao na poštivanje tih pravila, davatelji usluga potpisuju Izjavu o čuvanju povjerljivih informacija, čiji je predložak dan među pratećim dokumentima.

8. Upravljanje mrežom

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

Ako je podržan rad na daljinu, kada se primjerice djelatnicima dopušta da s kućnoga računala ažuriraju podatke, 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 podatci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Spajanje gostujućih računala na mrežu, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri podrazumijeva poštivanje institutskih pravila koja se odnose na sigurnost i zaštitu podataka. Ne dopušta se da oni po svom nahođenju priključuju računala na mrežu ustanove zbog opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnoga prometa, prikupljanja informacija itd. Institut može odrediti priključna

mjesta, primjerice u određenim uredima, gdje je dopušteno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se s tog segmenta mreže dopre do ostalih računala u ustanovi.
Institutska bežična mreža zaštićena je na način da se ne može bilo tko priključiti i služiti se njome te snimati promet. To se postiže metodama enkripcije i autentifikacije uređaja i korisnika.

9. Instalacija i licenciranje softvera

Korištenje ilegalnoga softvera predstavlja povredu autorskoag prava i intelektualnoga vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Institut zadužuje administratore 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.

10. Fizička sigurnost

Prostor u ustanovi dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni te prostor u koji pristup imaju samo skupine zaposlenih, ovisno o vrsti posla koji obavljaju.
Računalna oprema koja obavlja kritične funkcije, nužne za funkcioniranje informacijskoga sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dopušten samo ovlaštenim osobama.

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

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

11. Vanjske tvrtke

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

Institut 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 videonadzor.

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

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

12. Klasifikacija računalne opreme

Institut 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 Instituta, a čine 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).

13. Podjela opreme prema vlasništvu

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

Institut održava popis sve računalne opreme, s opisom ugrađenih komponenata, inventarnim brojevima itd.

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

Institut je dužna osoblju CARNeta dopustiti pristup opremi u vlasništvu CARNeta koja se nalazi u Institutu.

14. Odgovornost za računalnu opremu

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

Sva oprema koja se iznosi izvan prostorija Instituta podložna je provjeri kako bi se utvrdilo ima li oprema koja se iznosi potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

15. Osiguranje neprekidnosti poslovanja

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

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 nezgoda.

Povremeno se provjerava upotrebljivost pričuvnih kopija podataka te se izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na pričuvnoj opremi.

16. Nadzor nad informacijskim sustavima

Institut zadržava pravo nadzora nad instaliranim softverom i podatcima 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 jesu li informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Institut 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.

17. Doseg

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

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

18. Provođenje

Korisnici su dužni pomoći osobama zaduženima za nadzor informacijskih sustava tako 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 Instituta, ili oprema Instituta služi za njezin prijenos
- pristup radnom prostoru
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Instituta

19. Nepridržavanje

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

20. Prateći dokumenti

Uz pravila nadvedena u Općoj sigurnosnoj politici po potrebi i u posebnim slučajevima primjenjuju se posebna pravila definirana pratećim dokumentima. Prateći protokoli pisani su kao upute za rješavanje konkretnih problema i mogu se mijenjati prema potrebi.

INSTITUT ZA HRVATSKI JEZIK I JEZIKOSLOVLJE
Institute of Croatian Language and Linguistics
Ulica Republike Austrije 16, HR-10000 Zagreb, tel.: ++385 1 3783 833, faks: ++385 1 3783 803,
e-pošta: ured@ihjj.hr, www.ihjj.hr, IBAN: HR6923900011100012967, OIB: 12268324202

20.1. Protokol o rukovanju zaporkama

Svrha

Prosječan korisnik nerijetko smatra kako se ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. No, kompromitiranjem jednoga osobnog računala u lokalnoj mreži ili jednoga korisničkog računa na poslužitelju napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Stoga je svaki korisnik dužan izborom zaporke i njezinom povremenom promjenom doprinositi zaštiti cijeloga 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 od osam i više znakova.

Doseg

Svi zaposlenici Instituta za hrvatski jezik i jezikoslovlje, suradnici i studenti koji se u svome radu služe računalima dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućuju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

Kratku zaporku lakše je probiti. Stoga je minimalna dužina zaporke šest znakova, ali se preporučuje korištenje još dužih zaporki i zaporki koje uključuju barem jedno veliko slovo i jednu brojku, odnosno jedan poseban znak.

2. Ne služiti se riječima iz rječnika

Ne preporučuje se služenje riječima iz standardnojezičnih rječnika. Hakeri 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 po nekom algoritmu provodimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Neki korisnici naizmjence koriste dvije standardne zaporke. Iako su dvije zaporke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene zaporki.

6. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.
Hakeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori (phishing). Pravi administratori imaju mogućnost rješavanja problema 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.
Ako korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

8. Administriranje zaporki

Na računalima koja spadaju u zonu visokoga rizika administratori su dužni konfigurirati sustav na način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.
Administratori su dužni konfigurirati autentifikaciju tako da zaporke zastare nakon 90 dana te onemogućiti korištenje zaporki koje su već potrošene, ako sustav to dopušta.
Prilikom provjere sustava sigurnosni tim može ispitati jesu li korisničke zaporke u skladu s navedenim pravilima.

9. Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskoga sustava. Institut je obavezan djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.
U slučaju ponovljenoga ignoriranja ovih pravila Institut može stegovno djelovati.

20.2. Protokol o korištenju elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-poštom u Institutu za hrvatski jezik i jezikoslovlje zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.

INSTITUT ZA HRVATSKI JEZIK I JEZIKOSLOVLJE
Institute of Croatian Language and Linguistics
Ulica Republike Austrije 16, HR-10000 Zagreb, tel.: ++385 1 3783 833, faks: ++385 1 3783 803,
e-pošta: ured@ihjj.hr, www.ihjj.hr, IBAN: HR6923900011100012967, OIB: 12268324202

Stoga ćemo se početku ukratko navesti problemi koji mogu nastati pri korištenju elektroničke pošte.

1. Nesigurnost protokola

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

- Poruke putuju kao običan tekst te ih je lako presresti i pročitati ili čak izmijeniti njihov 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 poruke e-pošte 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 adresi e-pošte nalazi se ime ustanove. Pišući, zaposlenici moraju svjesni da netko privatnu prepisku može shvatiti kao službeni dopis, a privatno mišljenje kao službeni stav Instituta. Stoga u raspravi uvijek treba jasno naznačiti kada je izneseni stav privatno uvjerenje.

4. Otkrivanje informacija

Poruke namijenjene jednoj osobi lako 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 dopuštenje 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 bi se primatelja obvezalo na diskreciju.

U slučaju sigurnosnoga incidenta istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Institut se obvezuje čuvati povjerljivost takvih poruka, ali to ne može jamčiti 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 oduzeti znatan dio radnog vremena. Stoga se treba ograničiti broj privatnih poruka.

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

Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na internetu te oduzima vrijeme, čak i ako se takve poruka brišu bez čitanja. Institut će filtrirati spam na poslužitelju elektroničke pošte, ali je obveza 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 mora se tražiti dopuštenje 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 se može izložiti tužbi ne samo sebe, već i Institut.

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

- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite. Pridržavajte se netikete, pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.
- Nije dopušteno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom te na taj način podliježe propisima o autorskome pravu i intelektualnome vlasništvu. Nitko nema pravo poruke koju su poslane njemu osobno proslijediti dalje bez dopuštenja autora, odnosno pošiljatelja.
- Sve poruke pregledat će automatska aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Ustanova zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.
- Poruke koje su dio poslovnoga procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

7. Procedura za dodjelu e-mail adrese

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

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

8. Na koga se odnose pravila korištenja e-maila

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

9. Nepridržavanje

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

INSTITUT ZA HRVATSKI JEZIK I JEZIKOSLOVLJE
Institute of Croatian Language and Linguistics
Ulica Republike Austrije 16, HR-10000 Zagreb, tel.: ++385 1 3783 833, faks: ++385 1 3783 803,
e-pošta: ured@ihjj.hr, www.ihjj.hr, IBAN: HR6923900011100012967, OIB: 12268324202

20.3. Protokol o antivirusnoj zaštiti

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.
Nove generacije virusa izuzetno su složene i opasne, sposobne da prikriju svoju nazočnost, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na internet te otvoriti kriptiran kanal do čijeg računala kako bi hakeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa više nije stvar osobnog izbora, već obveza Instituta, administratora računala i svakog korisnika.

Institut za hrvatski jezik i jezikoslovlje propisuje da je zaštita od virusa obvezna i da se provodi na nekoliko razina:

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

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

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

Nepridržavanje

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

INSTITUT ZA HRVATSKI JEZIK I JEZIKOSLOVLJE
Institute of Croatian Language and Linguistics
Ulica Republike Austrije 16, HR-10000 Zagreb, tel.: ++385 1 3783 833, faks: ++385 1 3783 803,
e-pošta: ured@ihjj.hr, www.ihjj.hr, IBAN: HR6923900011100012967, OIB: 12268324202

20.4. Protokol o rješavanju sigurnosnih incidenata

1. Svrha

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

2. Prijava incidenta

Svaki zaposlenik ili suradnik Instituta za hrvatski jezik i jezikoslovlje dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Incident se prijavljuje administratoru ili korisničkoj službi Instituta.

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.

3. Procedure za rješavanje incidenata

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedopušten način, mogu izlistati sadržaj korisničke mape, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (npr. dokumenata ili poruka e-pošte).

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

- Istragu provodi jedna osoba, ali uz nazočnost svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne načine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije se načini kopija zatečenog stanja (npr. na vanjsku memoriju, 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.
- U 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 tako da im pristup imaju samo ovlaštene osobe.
- Institut može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

4. 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 čimbenik, protiv odgovornih se mogu poduzeti sankcije.

Institut može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili pristup podatcima.

Ako je incident izazvao zaposlenik vanjske tvrtke, Institut može zatražiti od vanjske tvrtke da ga ukloni s popisa osoba ovlaštenih za obavljanje posla na Institutu. U slučaju teže povrede pravila sigurnosne politike Institut može raskinuti ugovor s vanjskom tvrtkom.