Sigurnosna politika informacijskog sustava

Pravila, preporuke i smjernice za pravilno rukovanje računalnom mrežom i svim resursima u prostorima škole

Osnovna škola Budrovci
lipanj 2015.

Politiku sigurnosti kreirao:
Dominik Tomislav Vladić, prof.

Uvodne informacije o sigurnosnoj politici

Sigurnosna politika je dokument odnosno skup pravila koji propisuju mjere koje se odnose na informacijski sustav Osnovne škole Budrovci. To su mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sustavom koji se koristi za rad osnovne škole.

Sigurnosna politika je jedan od važnijih dijelova sustava koji upravljanja sigurnošću informacijskih sustava. Sigurnosna politika je važna za uobičajeno, redovito i kvalitetno funkcioniranje sustava. Njezina je svrha:

1. definirati prihvatljive načine ponašanja,
2. definirati neprihvatljive načine ponašanja,
3. jasno raspodijeliti zadatke,
4. jasno raspodijeliti odgovornosti,
5. propisati smjernice i pravila ponašanja tijekom korištenja informacijskog sustava,
6. propisati sankcije u slučaju nepridržavanja smjernica sigurnosne politike.

Sigurnosna politika Osnovne škole Budrovci se odnosi na sve njezine zaposlenike, učenike i osobe koje su tu prisutne po drugim dužnostima, obvezama i razlozima.

Svi zaposlenici, učenici i druge osobe, mogu koristiti informacijski sustav škole pod uvjetima i pravilima koji su propisani za određeni dio informacijskog sustava ili tehničke opreme. Pravila vrijede za sve jednako i moraju se provoditi na način kako je propisano.

Sigurnost informacijskih sustava bazira se na ljudima koji se koriste informacijskim sustavom. Tehnologijom koju imamo nije moguće u potpunosti osigurati sigurnost sustava kao i njegovu funkcionalnost. Stoga je važno uvesti sve potrebne mjere za očuvanje sigurnosti. Prije svega, to je moguće kroz definiranje sigurnosne politike, krovnog dokumenta za održavanje sigurnosti informacijskog sustava. Uloga sigurnosne politike je određivanje prihvatljivog i neprihvatljivog načina ponašanja, što joj je i primarna uloga, a cilj je zaštititi vrijednosti informacijskog sustava, opremu, programsku podršku i podatke.

Glavni zadatak sigurnosne politike je osigurati tri jedinstvena svojstva informacija:

- povjerljivost (tajnost),
- integritet,
- dostupnost.

1. Prihvatljivo ponašanje

Računalna mreža Osnovne škole Budrovci i njezine usluge na raspolaganju su korisnicima radi:

- obavljanja posla,
- učenja, podučavanja, istraživanja,
- usavršavanja u struci,
- drugih razloga koje vodstvo škole daje suglasnost, pismeno ili usmeno

Sva prava korisnici su dužni ostvarivati poštujući potrebe i prava ostalih korisnika informacijskog sustava. Svako korištenje informacijskog sustava je prihvatljivo korištenje, ako se ne krše smjernice i pravila, te ako nisu narušena tuđa prava.

2. Neprihvatljivo ponašanje

Neprihvatljivo ponašanje je svako ponašanje koje nije dopušteno ovim smjernicama ili pravilnikom. Neprihvatljivo je stvaranje ili prijenos datoteka, osim eventualno u okviru znanstvenog istraživanja:

- materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove,
- uvredljivog i ponižavajućeg materijala,
- distribuiranje autorski zaštićenih djela bez dozvole vlasnika prava,
- korištenje računalne mreže Osnovne škole Budrovci na takav način da ometa korištenje drugim korisnicima,
- širenje, virusa, trojanaca, crva i ostalog zloćudnog softvera,
- slanje neželjenih masovnih poruka,
- preuzimanje tuđeg identiteta,
- provaljivanje na računala koristeći sigurnosne propuste u softveru,
- traženje sigurnosnih propusta na umreženim računalima bez dozvole vlasnika opreme,
- izvršavanje napada uskraćivanjem resursa (Denial of Service),
- korumpiranje ili uništavanje podataka drugih korisnika,
- povreda privatnosti drugih korisnika,
- uništavanje tuđih podataka,
- neovlašteno korištenje tuđih radova,
- kopiranje ili instaliranje softvera za koje ne postoji licenca,
- drugih načina kršenja koji nisu u skladu s općeprihvaćenim normama i standardima,

3. Raspodjela zadataka

Zadaci tijekom nadzora pridržavanja smjernica i pravila sigurnosti u Osnovnoj školi Budrovci raspodijeljene su na sljedeći način:

- Odgovorna osoba: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sustava, redovito održava dijelove informacijskog sustava
- Nastavnik informatike: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sustava, redovito održava dijelove informacijskog sustava
- Nastavnici: prijavljuju incidente na propisan način, definiraju pravila ponašanja i korištenja računalne opreme, u skladu s propisanim pravilnicima i politikom sigurnosti, koja su javno objavljena na webu škole i u razredu na panou.
- Ostali zaposlenici: prijavljuju incidente na propisan način
- Učenici: prijavljuju incidente na propisan način, sudjeluju u izradi pravila ponašanja za svoje nastavne predmete s predmetnim učiteljem.
- Druge osobe u školi: prijavljuju incidente na propisan način

Odgovorna osoba, rukovodstvo škole, nastavnici, ostali zaposlenici škole mogu koristiti računalnu opremu za čiju upotrebu imaju dodijeljenu ovlast koristiti je. Učenici mogu koristiti računalnu opremu i mrežu uz dozvolu i prema uputama nastavnika i pod nadzorom nastavnika.

4. Raspodjela odgovornosti

Škola ima odgovornu osobu (administrator resursa) koji brine o sigurnosti i provođenju smjernica i pravila sigurnosti u školi. Odgovorna osoba preuzima prijave o incidentima ili eventualnom kršenju pojedinih smjernica ili pravila ponašanja tijekom korištenja informacijskog sustava.

Škola ima zaposlenog nastavnika informatike. Nastavnik informatike nadzire korištenje sustava na nastavnim satima. Može umjesto odgovorne osobe preuzimati prijave o incidentima ili eventualnom kršenju pojedinih smjernica ili pravila ponašanja tijekom korištenja informacijskog sustava.

Škola ima druge zaposlenika koji mogu koristiti računalnu mrežu. Svi zaposlenici su dužni pridržavati se smjernica i pravila ponašanja tijekom korištenja informacijskog sustava. Sve nepravilnosti su dužno prijavljivati.

Neprijavljivanjem incidenta svaki zaposlenik, učenik ili osoba prisutna u školi koja je to propustila učiniti namjerno, podliježe propisanim sankcijama.

5. Smjernice i pravila ponašanja tijekom korištenja informacijskog sustava

Korištenje informacijskog sustava u kabinetima rukovodstva škole:

- Korištenje informacijskog sustava nije dozvoljeno. Dozvoljeno je samo uz suglasnost ili izričitu dozvolu vlasnika tog dijela informacijskog sustava.

Korištenje informacijskog sustava u zbornici:

- Korištenje je dopušteno svim zaposlenicima škole u skladu s propisanim smjernicama i pravilima.
- Zauzeće resursa dozvoljeno je u skladu s potrebama.
- Nakon korištenja određenog dijela informacijskog sustava, opremu je potrebno vratiti u stanje u kojemu je zatečena prije korištenja.
- Nakon radnog vremena računalnu opremu je potrebno isključiti.

Korištenje informacijskog sustava u učionicama:

- Korištenje je dopušteno svim zaposlenicima škole u skladu s propisanim smjernicama i pravilima.
- Korištenje je dopušteno učenicima škole uz dozvolu nastavnika.
- Učenik resurse koristi samo za one zadatke koje mu je zadao nastavnik.
- Učenik može koristiti računala samo u prisutnosti nastavnika.
- Sve nepravilnosti i kršenja smjernica i pravila, nastavnik prijavljuje na propisan način.
- Zauzeće resursa dozvoljeno je u skladu s potrebama.
- Nakon korištenja određenog dijela informacijskog sustava, opremu je potrebno vratiti u stanje u kojemu je zatečena prije korištenja.
- Nakon radnog vremena računalnu opremu je potrebno isključiti.

Čuvanje osobnih korisnički podataka:

- Korisnički podaci su tajni.
- Svatko je vlasnik svojih korisničkih podataka i dužan ih je čuvati.
- Zabranjeno je ustupanje osobnih korisničkih podataka bilo kojoj drugoj osobi bez obzira na razlog.

Zabranjeno je korištenje tuđeg korisničkog računa.

6. Sankcije u slučaju nepridržavanja smjernica sigurnosne politike

Osoba koja namjerno ili na neki drugi način uzrokuje kvar računalne mreže, računala ili bilo kojeg dijela informacijskog sustava, snosi troškove popravka istoga. Drugačije je moguće postupati u slučaju kada je to tako dokazano i moguće.

PRILOZI

Prilozi su CARNet-ovi dokumenti koji su izrađeni kao smjernica sigurnosne politike za škole. Pravilnici CARNet-a su preuzeti uz minimalne prilagodbe.

Pravilnik o rukovanju zaporkama
Pravilnik o korištenju elektroničke pošte
Pravilnik o antivirusnoj zaštiti
Pravilnik o zaštiti od spama
Pravilnik o rješavanju sigurnosnih incidenata
Pravilnik o rukovanju povjerljivim informacijama

Izvori:
http://www.cert.hr/carnet_sigurnosna_politika
http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf

Prilozi – dokumenti za samovrednovanje:
Samovrednovanje – Stvaranje sigurne lozinke
Samovrednovanje – Čuvanje lozinke
Samovrednovanje – Sigurnosna provjera lozinke
Samovrednovanje – Čuvanje podataka elektroničke pošte
Samovrednovanje – Čuvanje medija za pohranu podataka
Samovrednovanje – Korištenje antivirusne zaštite
Samovrednovanje – Rješavanje sigurnosnih incidenata

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 škole, suradnici i učenici koji u svome radu koriste računala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Pravila za korištenje zaporki

1. **Minimalna dužina zaporke**

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

2. **Ne koristiti riječi iz rječnika**

Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki.

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. 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. 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 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.

Nepridržavanje

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

U slučaju ponovljenog ignoriranja ovih pravila škola može stegovno djelovati ili upoznati zaposlenika o mogućim lošim posljedicama neodgovornog ponašanja.

Pravilnik o korištenju elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-mailom na Ustanovi 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.
Stoga ćemo se na početku ukratko pozabaviti problemima 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 školu.

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.
- 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 dozvoljeno 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 autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- 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 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. Pri prestanku radnog odnosa, rukovodilac je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa. Učenici imaju pravo besplatnog korištenja e-maila za vrijeme trajanja obrazovanja.

Na koga se odnose pravila korištenja e-maila

Pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike, i učenike koji imaju otvoren korisnički račun na poslužitelju škole ili ustanove koja omogućuje korištenje mail adresa.

Nepridržavanje

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

Pravilnik o antivirusnoj zaštiti

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 škole, administratora računala i svakog korisnika.

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

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

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

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti administratora ili odgovornu osobu.

Nepridržavanje

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

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 (eng. hoax). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer.

Pravila za administratore

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

Prva 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.

Treću razinu zaštite određuju sami korisnici. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Informatičar zadužen za sigurnost će obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj. Upozorenja na viruse su često lažna i šire zablude. Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada školi.

Nepridržavanje

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

Pravilnik o rješavanju sigurnosnih incidenata

Svrha

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

Prijava incidenta

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

Škola 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 internim web stranicama škole.

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 (na pr. dokumenata ili e-mail poruka).

Moguće je osnivanje Povjerenstva za sigurnost. Daljnju istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom škole, 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.

Škola 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.

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

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

Pravilnik o upravljanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01. Uskoro se očekuje i zakon o zaštiti osobnih podataka.

Prema vrsti tajnosti informacije dijele se 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 školi ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.)

Profesionalna tajna odnosi na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u referadi, osoba koje unose podatke u baze podataka o studentima ili sistem administratora poslužitelja koji u nekim situacijama može doći u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji izvana dolaze u školu s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će škola 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 u rukovoditelj škole, 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 škole i vanjske suradnike koji dolaze u doticaj sa 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.

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

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

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

Povjerljive informacije u načelu se ne daju se telefonom jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik škole 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 u školu ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju školi 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 postupa, a može ih 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.