Crna Gora
UPRAVA ZA KADROVE

SIGURNOST INFORMACIONO KOMUNIKACIONIH TEHNOLOGIJA UPRAVE ZA KADROVE

Podgorica, mart 2018. godine

1.Uvod

Sigurnosna politika je jedan od segmenata sistema upravljanja sigurnošću informacionih sistema. U tom kontekstu se radi o potrebi za zaštitom svih podataka koji sadrže poslovni, službeni ili drugi oblik tajnosti, kao i o zaštiti IT tehnologije putem definisanja prihvatljivih, ali na drugoj strani i neprihvatljivih načina djelovanja. Za to je potrebna odgovarajuća alokacija zadataka i odgovornosti u okviru sistema.

Informacione tehnologije doprinose efikasnom funkcionisanju državne uprave. Korisničke aplikacije, elektronska pošta, web i mreže koje djeluju ispod toga nivoa, imaju ulogu za efikasno djelovanje moderne državne uprave. Uprava za kadrove svakodnevno dobija, stvara i obrađuje ogroman broj podatka u veoma različitim oblicima. Uništavanje (namjerno ili nenamjerno), krađa i zloupotreba takvih podataka može prouzrokovati veliku štetu. Čitav niz događaja može uzrokovati nepristupačnost informacijama ili čak gubitak informacija u elektronskom obliku: prirodne katastrofe, kvarovi na opremi, greške u softveru, kao i ljudskih grešaka odnosno neodgovarajućih postupaka. Zbog toga je potrebno da Uprava za kadrove ovim aktom definiše jasna pravila i da se organizaciono pripremi za slučaj ovakvih nepredviđenih, odnosno vanrednih događaja.

2. Sprovođenje sigurnosne politike u Upravi za kadrove

U državnom organu (u daljem tekstu Uprava za kadrove) je svaki pojedinac odgovoran za sprovođenje sigurnosti informaciono komunikacionih tehnologija (SIKT). Pravila rada, odnosno djelovanja, definisana sigurnosnom politikom, obavezuju sve zaposlene i odnose se na svu računarsku opremu koja se nalazi u prostorijama uprave.

Što se tiče njihove uloge u sistemu sigurnosti, zaposlena lica možemo podijeliti u dvije grupe:

- Prvu grupu predstavljaju *korisnici Informaciono Komunikacionih Tehnologija (u daljem tekstu IKT)* koji se u svom radu služe kompjuterima i računarskom opremom, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računara i mreža. Svaki korisnik IKT mora znati koja je njegova uloga u okviru sigurnosti ukupnog sistema.

  Dužnosti korisnika su:

  - pridržavanje pravila prihvatljive upotrebe, što znači da kompjutere i računarsku opremu ne smiju koristiti za djelatnosti koje nijesu u skladu sa zakonima, etičkim normama i pravilima lokalne politike sigurnosti sistema;
  - izbor kvalitetnih lozinki i njihova povremena promjena u skladu sa sigurnosnom politikom;
  - prijavljivanje sigurnosnih incidenata kako bi se što brže rješavali nastali problemi.

- Drugu grupu predstavljaju *administratori sistema*, koji su zaduženi za upravljanje (administraciju) kompjutera i mrežne opreme u skladu s pravilima struke. Ova lica se istovremeno brinu o funkcionalnosti i sigurnosti sistema. Svaki kompjuter mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera.
    - Kompjutere treba konfigurirsati tako da budu zaštićeni od napada spolja i iznutra. Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije i/i sadrži vrijedne i povjerljive informacije koje treba štititi od neovlašćenog pristupa.
    - Administratori svakodnevno prate rad sistema i provjeravaju rad servisa. Zadatak administratora je i nadgledanje rada korisnika, kako bi se otkrile zabranjene aktivnosti.

3. Sigurnosni problemi i ljudski resursi

Glavni nosioc ugrožavanja sigurnosti sistema je ljudski faktor. Zbog toga mora biti cilj svake organizacije i rukovodstva da smanje na minimim mogućnost pojavljivanja sigurnosnih problema.

U prošlosti su ovi problemi bili mnogo manji, a to se prije svega odnosi na razdoblje kada su ciljevi i aktivnosti unutar organizacije državne uprave bili relativno stabilni i definisani za duži vremenski period. Danas, u vrijeme naglih promjena i mjenjanja filozofije funkcionisanja državne uprave, i rizik, odnosno povećan stepen pojavljivanja problema sigurnosti sistema, postaje sve veći. Za uspješno rješavanje sigurnosnih problema potrebno je stalno dopunjivati politiku osiguranja odnosno zaštite sistema. Proces razvoja sigurnosti informaciono komunikacionih tehnologija (SIKT) u državnim organima u smislu ljudskih resursa počinje kod planiranja rada, procesa i unutrašnje organizacije. U tom smislu, važni su sledeći aspekti:

- sva zaposlena lica moraju poštovati SIKT; nepoštovanje istih povlači odgovornost;
- svako novo zaposleno lice mora biti informisano o SIKT;
- potrebno je izvoditi redovne programe usavršavanja i osposobljavanja zaposlenih u ovoj oblasti;
- potrebno je stalno obavještavanje o promjenama ISP; zaposlena lica treba redovno upoznavati sa mogućnostima upotrebe različitih komunikacionih oblika i mehanizama (E-mail, sastanci…), a nužno ih je redovno obavještavati i o svim za njih važnim promjenama i novostima u oblasti SIKT;
- ako dužnost čuvanja povjerenih podataka i postupci rukovanja sa njima nijesu dovoljno jasno i precizno definisani postojećim propisima, potrebno je usvojiti interni akt koji precizira ovu materiju; zaposlena lica koja imaju pristup podacima, moraju da potpišu i Izjavu o zaštiti podataka, koja važi za čitav period radnog odnosa (a i nakon toga).

Preporuka: **Zaštita sredstava za pristup sistemu i zabrana pozajmljivanja fizičkih i elektronskih sredstava za pristup**.

Zaposlena lica moraju da čuvaju fizička i elektronska sredstva za pristup sistemu (korisničko ime, lozinka…) i ne pozajmljuju drugim licima. Podaci za pristup sistemu uvijek se tretiraju kao povjerljivi i u skladu sa tom činjenicom treba i rukovati ovim podacima.

Rizik:

Neovlašćena lica mogu upotrebom tuđih (pozajmljenih) sredstava za pristup sistemu doći do podataka i informacija za koje nijesu ovlašćena.

Aktivnost:

- svi zaposleni moraju odmah prijaviti ukradeno ili izgubljeno zaštitno sredstvo za pristup;
- zabranjeno je pozajmljivanje sredstava za pristup sistemu (ovo se odnosi i na ovlašćena lica koja ne smiju pozajmljivati svoja sredstva drugim licima).

Preporuka: **Zabrana zaposlenim licima da upotrebljavaju internet za pristup ili prenos sadržaja odnosno podataka, koji su neprikladni, uvredljivi, nezakoniti ili opasni.**

Korišćenje interneta za lične potrebe dozvoljeno je samo u manjem obimu, koji ne remeti normalan radni proces i ne opterećuje sistem.

Rizik:

Pretjerana odnosno neodgovarajuća upotreba interneta u lične svrhe uzrokuje neprikladno korišćenje resursa i opterećenje sistema. Najčešće aktivnosti u praksi:

- pretraživanje i prenos pornografskih materijala;
- igranje internetnskih igara i korišćenje »prostorija za ćaskanje« (engl. »chat-rooms«) u privatne svrhe;
- upisivanje na različite forume i rasprava na tim forumima uz korišćenje službene e-mail adrese;
- primanje i dalje slanje (distribucija) šaljivih poruka u velikom obimu putem E-maila.

Aktivnost:

- svi zaposleni trebaju se upoznati sa pravilima upotrebe interneta;
- lica, odgovorna za IT infrastrukturu, moraju (čak i putem upotrebe dodatnih softvera i hardvera) obezbijediti ograničenje pristupa sistemu;
- svaka zlouptreba pravila upotrebe sredstava odnosno sistema povlači za sobom odgovornost.

Preporuka: **Upotreba informacione tehnologije i komunikacija za lične namjene.**

Upotreba IKT za lične namjene ne smije uzrokovati nikakve dodatne troškove i ne smije predstavljati nikakve smetnje u funkcionisanju sistema za ostale korisnike.

Rizik:

Nepostojeća ili loše definisana pravila o upotrebi informacione tehnologije za ličnu namjenu može predstavljati dodatan sigurnosni rizik, a može prouzrokovati i zloupotrebu odnosno preopterećenje mreže i kompletnog informacionog sistema.

Aktivnost:

- ovakvo korišćenje informacione tehnologije može biti dozvoljeno samo u obimu koji ne predstavlja dodatni bezbjednosni rizik, ne utiče na službenu upotrebu sistema, odnosno ne preopterećuje sistem.

4. Sigurnosna politika i obezbjeđivanje sigurnog okruženja

Preduslov bilo kakvog efikasnog rada jeste fizička sigurnost i zaposlenih lica i prostorija, opreme i dokumenata. Obezbjeđivanje sigurnog okruženja znači brigu svakog zaposlenog lica za ostvarivanje prikladnog nivoa zaštite podataka i dokumenata sa kojim raspolaže. U tom okviru se sve veća pažnja poklanja kontroli pristupa. Obavezan postupak djelovanja zaposlenih lica kada nijesu na svojim radnim mjestima i u slučajevima kada dođe do uvida neovlašćenog lica u sadržaj informacionog sistema (baze podataka i sl.) podrazumijeva sledeće:

- obavezu zaštite podataka od uništenja u skladu sa zaključkom Vlade Crne Gore o implementaciji servisa na Disaster recovery lokaciji;
- obavezu obezbjeđivanja sigurnog sistemskog okruženja; kod instaliranja informaciono komunikacione opreme treba imati u vidu odgovarajuće mjere sigurnosti i zaštite od uticaja okoline (promjene u temperaturi, vlagi…);
- treba voditi računa o selidbi opreme; svaku selidbu opreme odnosno informacionog sistema potrebno je planirati unaprijed, o njoj treba obavjestiti sva nadležna lica, kontrolisati i dokumentovati proces preseljenja;
- treba voditi računa o preuzimanju opreme i vođenju dokumentacije; dokumentacija o opremi mora biti ažurna i uvijek dostupna zaposlenim licima koja su odgovorna za tu opremu; posebnu pažnju treba posvetiti čuvanju sistemske dokumentacije;
- treba voditi računa o promjeni režima korišćenja i o otpisu opreme; kod promjene režima upotrebe opreme treba uništiti podatke na toj opremi, a sve potrebne aktivnosti mora sprovoditi za to ovlašćeno lice;
- treba voditi računa o postupcima iznošenja opreme iz službenih kancelarija; iz kancelarije se može iznositi samo određena oprema i to mogu raditi samo ovlašćena lica, koja su odgovorna za opremu i za informacioni sistem;
- treba voditi računa o održavanju opreme; za informacionu opremu koja je u redovnoj ili povremenoj upotrebi, mora biti obezbijeđeno održavanje; održavanje opreme treba da vrše ovlašćena stručna lica; kada servis vrše vanjski stručnjaci, potrebno je obezbijediti striktnu zaštitu podataka;
- treba voditi računa o čišćenju hardverske opreme; za čišćenje hardverske opreme upotrebljavaju se samo specijalna sredstva i materijali; sve oblike čišćenja, osim vanjskog čišćenja te čišćenja monitora i tastature, vrše ovlašćena lica.

Preporuka: **Politika urednog stola**

Zaposlena lica ne smiju ostavljati bilo kakve povjerljive podatke bez nadzora, odnosno, mora biti onemogućen neovlašćen uvid ili bilo kakva druga upotreba podataka neovlašćenim licima. Izvan radnog vremena sva oprema mora biti na propisan način fizički i programski zaštićena (radi se o opremi koja se koristi za pristup podacima i za čuvanje podataka).

Rizik:

Dokumente (u klasičnom papirnom ili elektronskom obliku) moguće je uzeti sa radnog stola, štampati, fotokopirati ili jednostavno ukrasti (odnijeti).

Aktivnost:

- dokumenti i pristup kompjuterima (IT) ne smiju se ostavljati bez nadzora;
- kada se napušta radno mjesto na duže vrijeme, obavezno treba spriječiti neovlašćen pristup podacima (zaključavanjem kancelarija i upotrebom lozinki na računaru).

Preporuka: **Politika praznog monitora i obezbjeđivanje privremeno nezauzetog radnog mjesta**

Bez obzira da li je zaposleno lice prisutno na radnom mjestu ili ne, mora biti onemogućen neovlašćen pristup i uvid u računar, a i uopšte, mora biti onemogućena upotreba informaciono-telekomunikacione opreme neovlašćenim licima.

U otvorenim kancelarijama postoji velika mogućnost pristupa neovlašćenih lica, koja mogu u slučaju neodgovarajuće sigurnosne politike doći do različitih podataka. Ako je korisnik i njegova računarska oprema logovana u sistem bez nadzora, neovlašćena lica imaju nesmetan pristup svim podacima.

Rizik:

- neovlašćeno lice može čitati i čak promjeniti podatke koristeći aktivnu aplikaciju;
- neovlašćeno lice može da se loguje u sistem koristeći važeće korisničko ime i lozinku, ako to nije obezbijeđeno na odgovarajući način;
- neodgovarajuće uređenje nivoa pristupa sistemu može uzrokovati mogućnost pristupa zabranjenim oblastima informacionog sistema;
- neovlašćen pristup može da uzrokuje otkrivanje zaštićenih podataka;
- neovlašćena prijava putem nekontrolisanog računara može da dovede do štetnih posledica ili do zloupotrebe unosa (promjenu podataka, zlonamjernu upotrebu E-maila i sl.).

Aktivnosti:

- svaki korisnik sistema mora imati dodijeljena prava za pristup u skladu sa pravima i dužnostima zaposlenog lica na radnom mjestu;
- u slučaju dužeg odsustva zaposleno lice se mora odjaviti iz sistema i isključiti računar;
- u slučaju kraćeg odsustva sa radnog mjesta obavezna je odjava iz sistema ili zaključavanje računara;
- obavezno je podesiti aplikacije i računare, tako da poslije određenog vremena neaktivnosti računar se odjavi i zaključa.

5. Sigurnosna politika i zaštita od zlonamjernog programskog koda, hakerskih napada i neodgovarajuće upotrebe informacionih sistema

Danas se virusi šire mnogo brže nego što je moguće dorađivati programe za antivirusnu zaštitu. Zbog toga je potrebno sprovoditi tehničke i organizacione mjere za odgovarajuće informisanje korisnika. Zaštita od zlonamjernih programskih napada treba da se zasniva na sljedećim aktivnostima:

- potrebna je dobra informisanost korisnika o dobrim metodima zaštite od napada;
- potrebna je adekvatna kontrola obrade podataka u informacionom sistemu;
- nužno je odgovarajuće uvažavanje preporuka za zaštitu informacionog sistema.

Rizici ove vrste konstantno rastu i predstavljaju veliki problem u smislu realizacije sigurnosne politike. Uključivanje u kompjutrske sisteme bez dozvole administratora sistema korišćenjem logina i lozinki drugih korisnika nije dozvoljeno, kao što nije dozvoljeno ni upradanje u kompjutrske sisteme putem zaobilaženja sigurnosnih kontrola. Cilj ovakvih napada su krađe podataka (intelektualnog vlasništva), uništavanje podataka (brisanje, promjene), kao i svi oblici blokada informacionog sistema.

Opšte preporuke:

- nužna je odgovorna i racionalna upotreba informacione tehnologije; prekomjerna i neodgovorna upotreba interneta, e-maila i ostalih tehnologija za lične svrhe može da uzrokuje preopterećenost sistema ili čak probleme u smislu smanjenja sigurnosti sistema;
- potrebno je praćenje kvaliteta funkcionisanja sistema i registrovanje svih sigurnosnih događaja; svaki sumnjiv ili neuobičajen događaj mora se registrovati i saopštiti odgovornom licu.

Preporuka: **Zaštita mrežnih podataka od virusa i ostalih oblika zlonamjernog koda**

Rizik:

Virusi i crvi predstavljaju opasnost za informacione sisteme – ugrožavaju funkcionisanje mreža i povjerljivosti podataka.

Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tastaturi. Informacije poput lozinke ili povjerljivih dokumenata virusi mogu slati svome kreatoru na njegovu IP adresu preko interneta. Osim toga virusi mogu otvoriti i kriptovan kanal do određenog kompjutera, a na taj način hackeri mogu preuzeti kontrolu nad kompjuterom.

Stoga zaštita od virusa ne smije više biti stvar ličnog izbora, već obaveza organa, administratora kompjutera i svakog korisnika.

Aktivnost:

- administratori su dužni instalirati antivirusne programe na sve korisničke kompjutere i konfigurisati ih tako da se izmjene u bazi virusa i u konfiguraciji

automatski šalju sa centralne instalacije na korisničke kompjutere u lokalnoj mreži, bez aktivnog učeća korisnika;
- korisnici ne smiju svojevoljno isključiti protivirusnu zaštitu na svome kompjuteru; ukoliko iz bilo kog razloga moraju privremeno zaustaviti antivirusni program, korisnici o tome moraju odmah obavijestiti administratora;
- ako korisnik primjeti da njegov kompjuter nije zaštićen ili da program za antivirusnu zaštitu već duže vrijeme nije bio ažuriran, mora o tome odmah obavjestiti odgovorno lice u organu.

Preporuka: **Svaku neispravnost na informaciono-komunikacionoj opremi korisnik mora javiti odgovornom licu**

Rizik:

Kvar na opremi može da uzrokuje nepravilan rad, zaustavljanje sistema ili gubljenje podataka.

Aktivnost:

- ovlašćeno lice je dužno da se pobrine za redovno održavanje oprema u skladu sa uputstvima proizvođača opreme;
- u slučaju kvara odgovorno lice je dužno odmah popraviti ili zamjeniti neispravnu opremu;
- u slučaju kvara je nužno odmah ukloniti i bezbjedno skladištiti sve povjerljive podatke;
- o kvaru treba odmah obavijestiti odgovorno lice.

6. Sigurnosna politika i upotreba interneta

Pristup internetu i ostalim korisničkim servisima predstavlja bitno povećanje rizika za sigurnost svakog informacionog sistema.

Pristup internetu

S obzirom da je računarska mreže Uprave za kadrove dio računarske mreže državnih organa, time je definisan pristup internetu. Za sigurnosnu politiku ove oblasti zaduženo je nadležno ministarstvo.

Preporuka: **Upotreba programske opreme za korišćenje internet servisa**

Programska oprema za pristup internet servisima mora biti pravilno konfigurisana i treba je upotrebljavati na način da se spriječi neovlašćen pristup informacionom sistemu.

Rizik:

- 'Web-browser' i 'e-mail client' predstavljaju novu mogućnost neovlašćenog ulaska u informacioni sistem; najproblematičniji su 'Cookies', 'Java Applets', 'JavaScripts', 'ActiveX controls' i virusi;
- povjerljive informacije mogu se upisivai i čitati pomoću 'cooki-a' sa web-sajta na kom se korisnik trenutno nalazi – bez saglasnosti korisnika;
- virusi, Trojan aplikacije i zlonamjerni kodovi mogu da se probiju kroz sistem zaštite i putem aktiviranja web browserom uzrokuju ozbiljnu štetu informacionom sistemu.

Aktivnost:

- treba uvažavati preporučene konfiguracije programske opreme i upotrebu ugrađenih sigurnosnih mehanizama;
- ovlašćena i osposobljena lica treba da definišu standardne konfiguracije programske opreme za pristup internet servisima; korisnici ne smiju mijenjati parametre postavljene konfiguracije;
- upotrebu 'cooki-a' treba omogućiti samo u posebnim situacijama.

Preporuka: **Prenos programa, datoteka i informacija sa interneta**

Velika pažnja treba biti posvećena postupku prenosa informacija i datoteka sa interneta zbog zaštite od zlonamjernih kodova i neprikladnog materijala.

Najčešču korisničku aktivnost na internetu predstavlja presnimavanje programa, igara, muzike i video snimaka. Kod prijenosa bilo kakvih datoteka (programa, skripta, grafičkih fajlova) postoji velik sigurnosni rizik.

Rizik:

- kod prenosa aplikacija (programa) sa interneta na kompjuter postoji velika mogućnost da se zajedno sa traženom aplikacijom prenese i virus ili neki drugi zlonamjerni kod koji može imati uticaj na informacioni sistem; to može imati veoma ozbiljne posledice;
- prenos programske opreme često zahtijeva registraciju i licenciranje te opreme; u slučaju nepoštovanja autorskih prava može biti pokrenut postupak protiv prekršioca;
- informacije na internetu mogu biti netačne, neažurne ili takve da namjerno iskrivljuju činjenice, i bilo kakva odluka koja se bazira na tim informacijama treba biti pažljivo provjerena;
- pogrešna upotreba internet konekcije može preopteretiti sistem i uzrokovati nestabilnost mreže.

Aktivnost:

- programsku opremu može podešavati samo ovlašćeno lice (administrator);
- neophodna je upotreba zaštitne programske opreme (anti-virusna zaštita, firewall, programska oprema za detekciju zlonamjernog koda…);
- prije upotrebe informacija pronađenih na internetu u poslovne svrhe, potrebno je provjeriti izvor podataka i procjeniti pouzdanost informacija.

Preporuka: **Upotreba interneta u poslovne svrhe.**

Upotreba Interneta je veoma raširena i obuhvata važan segment resursa koji zaposlena lica potroše na svom radnom mjestu.

Rizik:

- neautorizovana i nezaštićena upotreba Interneta može omogućiti hakerima da dođu do informacija iz informacionog sistema kao i do samog sistema;
- dolazak na određenu web stranicu često znači i bilježenje pojedinih podataka sa te stranice na korisnikovom kompjuteru; međutim, ovakvo registrovanje i čuvanje informacija dešava se (veoma često) bez korisnikove dozvole;
- neprikladan pristup i prenos programa i drugih datoteka može se tretirati kao

zloupotreba resursa i, u nekim slučajevima, može biti protivzakonito;
- neautorizovan pristup Internetu znači gubljenje vremena i resursa.

Aktivnost:

- administratori sistema moraju redovno vršiti kontrolu opterećenosti sistema i na osnovu takve kontrole pripremiti odgovarajuće mjere.

Preporuka: **Nabavka i plaćanje putem interneta**

Lica koja vrše nabavke i plaćanja usluga ili materijala internetom moraju upotrebljavati odgovarajuće postupke za sigurno sprovođenje tih operacija.

Rizik:

- za vrijeme transakcije može da dođe do krađe ličnih podataka ili drugih tajnih podataka (kreditna kartica: broj, podaci o vlastniku, fajlovi iz računara...), i time do zloupotrebe;
- identitet prodavca je rizičan, pošto nije sigurno da iza nekog naziva firme sa interneta stvarno stoji ta firma.

Aktivnost:

- transakcija odnosno prenos podataka mora da bude dobro zaštićen upotrebom metode kripto zaštite; komunikacija sa serverom se često vrši upotrebom SSL ('Secure Socket Layer') protokola;
- pri slanju tajnih podataka putem interneta uvjek treba upotrebljavati web stranice koje podržavaju sigurno povezivanja korisnika i servera (https);
- lične podatke uvjek treba slati samo provjerenim licima ili organizacijama.

Preporuka: **Upotreba informacija, koje se dobijaju preko interneta**

Informacije dobijene preko interneta treba uvijek provjeriti prije korišćenja za poslovne svrhe.

Rizik:

- informacija, koja se dobije putem interneta može biti netačna ili čak potpuno pogrešna;
- korišćenjem ovako dobijenih podataka može se ugroziti poslovni proces.

Aktivnost:

- upotrijebiti samo informacije dobijene iz pouzdanih izvora;
- provjeriti sve važne informacije, dobijene internetom, prije upotrebe u poslovne svrhe;
- treba biti svjestan da na internetu postoji velika količina izmišljenih i netačnih informacija.

Preporuka: **Potrebno je upotrebljavati softverske filtere i druge tehnike za ograničenje pristupa neprikladnim materijalima na internetu**

Rizik:

Na internetu se pojavljuje sve više neprikladnog sadržaja; pristupanje takvim web stranicama ne znači samo neodgovarajuće korištenje resursa, to predstavlja i prijetnju sigurnosti informacionog sistema.

Aktivnost:

Korisnici interneta mogu slučajnim ili namjernim dostupom i prenosom neprikladnog materijala sa interneta uzrokovati probleme u informacionom sistemu.

Neprikladne ili nelegalne informacije mogu biti dostupne i mogu se prenositi ako sistemi filtriranja nisu odgovarajući.

7. Sigurnosna politika i upotreba elektronske pošte (E-mail)

E-mail je dio svakodnevne komunikacije, poslovne i privatne; komunikacije E-mailom zahtijevaju da se razmotre svi aspekti elektronske komunikacije obzirom na moguće posljedice.

Protokol koji se koristi za prenos elektronske pošte, SMTP ili 'Simple Mail Transport Protocol', nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu svjesni zamki koje se pojavljuju u korišćenju elektronske pošte.

Opšte preporuke:

- svi korisnici elektronske pošte moraju biti na odgovarajući način osposobljeni za upotrebu elektronske pošte i trebaju biti informisani o mogućim problemima u vezi sa sigurnošću sistema; prije svega, korisnici moraju biti svjesni, da osim obezbjeđivanja svih sigurnosnih mjera postoji i mogućnost prisluškivanja, slanja, štampanja i presretanja e-pošte; upravo tako, korisnik mora biti svjestan da je pošta dostupna u sistemu i uprkos brisanju iz poštanskog sanduka (inbox);
- za bezbjednu i nesmetanu upotrebu elektronske pošte brinu se sistemski administratori u organima uprave i centralni administratori u nadležnom ministarstvu.

Rizici:

- nesigurnost protokola
    - poruke putuju kao običan tekst, otvorene kao na razglednici, zato ih je lako presresti i pročitati, ili čak izmijeniti sadržaj;
    - lako se može krivotvoriti adresa lica koje šalje poruku, zato nikada nije sasvim siguran odgovor na pitanje, ko je zaista poslao poruku;
    - protokoli za čitanje e-pošte, POP i IMAP, u svojoj osnovnoj formi šalju korisničko ime i lozinku 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;

- greške

    - uvijek se može desiti da se pritisne pogrešna tipka ili klikne mišem na susjednu ikonu; time može nastati određena šteta – ne može se zaustaviti poruka koja je već poslana; ako se umjesto 'Reply' pritisne 'Reply to All', poruka će umjesto jednom licu otići na više adresa, a povjerljive informacije dospjeti do neželjenih lica;
    - česta je greška da se preuzme pogrešna adresa iz adresara;
    - određeni mail klijenti sami dovršavaju e-mail adresu koju upisuje korisnik; u žurbi se može uključiti pogrešna adresa, slična onoj na koju korisnik želi poslati e-mail.

- nesporazumi

    - ljudi su skloni pisati e-mail poruke na ležerniji, opušteniji način; to može dovesti do nesporazuma ako drugo lice ne shvata poruku na isti način; stoga službene dopise treba pisati u formalnom odnosno službenom jeziku i tonu;
    - iza korisnikovog imena u e-mail adresi nalazi se ime institucije (organa); zato se može desiti sa drugo lice shvati privatnu prepisku kao službeni dopis, određeno privatno mišljenje kao službeni stav organa i sl.; stoga u tekstu treba uvijek jasno naznačiti ako je izneseni stav privatno uvjerenje.

- otkrivanje informacija

    Poruke namijenjene određenom licu mogu se proslijediti drugima, npr. na mailing listu; to se može desiti:

    - (zlo)namjerno, s ciljem da se nanese šteta drugom licu;
    - namjerom lica, koje ne traži dozvolu za prosljeđivanje poruke;
    - slučajnom greškom, npr. nehotičnim klikom mišem na pogrešnu ikonu ('Reply to All' umjesto 'Reply');
    - stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bi slučajnog primaoca obavezali na diskretnost.

- Radna etika

    - velika količina poruka koje treba svakodnevno pročitati može oduzeti znatan dio radnog vremena; stoga treba ograničiti broj privatnih i zabavnih poruka;
    - lančane poruke koje se 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"...);
    - spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako se bez čitanja brišu takve poruka.

- Povreda autorskih prava

    - svaka poruka e-pošte može se smatrati autorskim djelom, stoga ona pripada licu koje ju je poslalo; stoga za prosljeđivanje tuđe poruke treba tražiti dozvolu njezina autora;
    - prilozi koji se šalju uz e-poruke mogu sadržavati autorski zaštićene informacije, na primjer muziku, filmove, članke itd.; primajući i šaljući takve sadržaje lice se može izložiti tužbi (ličnoj, ali tužbi protiv državnog organa).

Aktivnosti:

Zbog svega nabrojanog upotreba elektronske pošte smatra se rizičnom aktivnošću, zbog čega korisnici moraju da se pridržavaju određenih pravila:

- korisnicima se otvara korisnički nalog radi obavljanja posla;
- privatne poruke dozvoljene su u umjerenom obimu, ukoliko to ne ometa rad organa;
- pri pisanju poruke lice treba biti svjesno da ne predstavlja samo sebe, već i organ za koji radi;
- treba se pridržavati pravila pristojnog ponašanja na Internetu, službena e-mail adresa se ne smije 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; niko nema pravo poruke koje su poslane nekome lično, proslijediti dalje bez dozvole autora, odnosno onoga koji je poslao svoju poruku;
- sve poruke pregleda automatska aplikacija koja otkriva viruse; ako poruka sadrži virus, neće biti isporučena, a lice koje poruku šalje i lice koje poruku prima će biti o tome obaviješteni;
- administrator sistema zadržava pravo filtriranja poruka s namjerom da se zaustavi spam;
- poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisanom vremenskom periodu kao i dokumente na papiru.

Preporuka: **Primanje neželjenih poruka (spam)**

Uprava za kadrove mora obezbjediti sve što je potrebno da se spriječi upotreba službene elektronske pošte za slanje neprikladnih materiala (spam, junk-mail, reklame…).

Rizik:

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektronske pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i kompanije, jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost.

Aktivnost:

- Administratorski nivo:
    - administratori servera e-pošte dužni su konfigurisati kompjutere tako da se što više neželjenih poruka zaustavi;
    - informatičar zadužen za sigurnost treba obučiti korisnike i pomoći im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

- Korisnički nivo

    - korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj; upozorenja na viruse su često lažna i šire zablude;

- korisnici ne smiju radi sticanja dobiti slati propagandne poruke koristeći kompjutersku opremu koja pripada državnom organu.

8. Sigurnosna politika, sigurnosni incidenti i kvarovi na opremi

Preporuka: **Prijava sigurnosnih incidenata**

Svaki korisnik sistema dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlašćene razmjene podataka, pojave virusa itd.

Administrator sistema treba pripremiti i ažurirati kontakt listu lica kojima se prijavljuju problemi u radu kompjutera i servisa.

Svaki incident se evidentira; uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac sa opisom incidenta i preduzetih mjera pri rješavanju problema.

Rizik:

- ako nije jasan postupak prijavljivanja sigurnosnih incidenata, korisnici neće javljati takve događaje, što može da uzrokuje eskalaciju nepoželjnih događaja i ozbilnju opasnost po sistem;
- zbog nedefinisanih postupaka prijavljivanja incidenata može doći do smetnji u komunikaciji korisnik – administrator, čime se troši se više vremena za reaktivaciju sistema.

Aktivnost:

- reakcija na sigurnosni incident mora da bude jasno definisana i brza, jer time smanjujemo mogućnost pojavljivanja eskalacije problema;
- sigurnosni incidenat može da se u prvoj fazi javi putem telefona ili elektronske pošte, a poslije obavezno treba evidentirati događaj zbog analize i preduzimanja odgovarajućih mjera;
- incidente treba rangirati prema obzbiljnosti prijetnje.

Preporuka: **Utvrđivanje izvora i posledica sigurnosnog incidenta**

Sigurnosne incidente potrebno je na odgovarajući način analizirati i utvrditi razloge pojavljivanja i uticaj na sistem.

Rizik:

Neprikladno rješavanje pojedinog sigurnosnog incidenta može uzrokovati gubitak ili zloupotrebu podataka.

Aktivnost:

Svaki sigurnosni incidenat mora da bude precizno analiziran, a uz to treba evidentirati slučaj i preduzeti sve potrebne mjere za otklanjanje problema.

Preporuka: **Prijava kvarova ili oštećenja opreme**

Svi korisnici opreme dužni su da prijave svaki kvar, namjerno ili nenamjerno oštećenje informaciono-komunikacione opreme; ovo se obavezno javlja administratoru sistema koji preduzima sve odgovarajuće mjere. Svaki kvar mora da se registruje u evidenciji kvarova opreme.

Rizik:

- postupci prijave i evidencije kvarova nisu definisani;
- nepotpuni podaci mogu da uzrokuju pogrešnu dijagnozu ili problem u smislu smanjenja sigurnosti sistema;

Aktivnost:

- javiti svaki kvar (on line) na opremi administratoru sistema, koji je odgovoran da kvar evidentira i preduzme odgovarajuće mjere;
- treba uvesti poseban sistem registracije
    - opreme, konfiguracije i šeme sistema
    - kvarova i oštećenja opreme
- treba se pobrinuti za jedinstven sistem identifikacije opreme;
- treba se pobrinuti za blagovremeno i redovno servisiranje ili zamjenu opreme.

9. Sigurnosna politika i nadzor pristupa

Jedan od veoma važnih segmenata zaštite podataka jeste nadzor nad pristupom. Nadzor proizilazi iz zahtjeva poslovanja organa i istovremeno precizno definiše odgovornost korisnika za vrijeme dostupa do sistema, podataka i njihove upotrebe.

Svrha upravljanja nadzora pristupa je spjrečavanje neovlašćenog pristupa do informacionog sistema. Za kontrolu dodjele prava pristupa do servisa informacionog sistema moraju postojati formalni postupci koji pokrivaju sve faze korisničkog pristupa – od inicijalnog reiranja novog korisničkog naloga do njegovog brisanja istog.

Preporuka: **Kreiranje novog korisničkog naloga**

Mora biti definisan formalan postupak za upisivanje i brisanje pristupa za svaki servis sistema.

Rizik:

U slučaju da nisu definisane formalne procedure za upisivanje i brisanje pristupa postoji mogućnost neovlašćenog pristupa.

Aktivnost:

- provjera, da li korisnik ima dozvolu vlasnika sistema za upotrebu servisa;
- provjera, da li je dodijeljeni nivo pristupa odgovara funkciji i zaduženjima korisnika.

Preporuka: **Dodjeljivanje lozinki**

Lozinke su najvažniji i često jedini način za proveru identiteta korisnika. Zbog toga, potrebno je definisati formalni postupak dodjeljivanja lozinki.

Rizik:

Lozinka može biti otkrivena neovlašćenom licu.

Aktivnost:

- ovlašćeno lice koje vodi proceduru dodjeljivanja lozinki, mora tretirati lozinku kao tajni podatak i ne smije da je razotkrije neovlašćenom licu;
- korisnici treba da inicijalne lozinke prime na siguran način; početne lozinke moraju biti privremene i treba ih promijeniti odmah poslije prve upotrebe.

Preporuka: **Upotreba lozinki**

Prosječan korisnik često smatra kako ne mora brinuti o sigurnosti jer njegov kompjuter ne sadrži vrijedne informacije. Međutim, nezaštićen kompjuter može poslužiti samo kao ulaz u sistem i dostup do vrijednih informacija.

Svi korisnici sistema dužni su da se pridržavaju pravila korišćenja lozinki, dok su ih administratori dužni tehnički ugraditi u sve sisteme koji to omogućavaju.

Rizik:

Kompromitovanje jednog kompjutera u lokalnoj mreži ili jednog korisničkog računa omogućava napadaču da probije sigurnosni sistem i otvori prolaz za napade na važnije sisteme i informacije. Lanac puca na najslabijoj karici. Zbog toga je svaki korisnik dužan izborom lozinke i njenim povremenim promjenama doprinositi zaštiti ukupnog sistema.

Aktivnost:

- minimalna dužina lozinke
  Kratku lozinku lakše je probiti; stoga neka minimalna dužina lozinke bude šest znakova, ali preporučuje se korišćenje još dužih lozinki.

- ne koristiti riječi iz rječnika
  Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih lozinki (tzv. dictionary attack).

- izmiješati mala i velika slova sa brojevima
  Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je lozinka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

- Ne koristiti imena bliskih lica, kućnih ljubimaca, datume
  Takve se riječi lako otkriju socijalnim inžinjeringom

- Trajanje lozinke
  Promjena lozinke smanjuje vjerovatnost njenog otkrivanja. Neki korisnici naizmjenično koriste dvije standardne lozinke. Iako su dvije lozinke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene lozinke.

- tajnost lozinke

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

Hakeri nastoje izmamiti lozinke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja problema i bez poznavanja korisničkih lozinki.

- Čuvanje lozinke
  Lozinke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, itd. Korisnik je odgovoran za tajnost svoje lozinke, te mora naći način da je sakrije.

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

- Upravljanje lozinki
  Na kompjuterima koji spadaju u zonu visokog rizika administratori su dužni konfigurisati sistem na način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

  Administratori su dužni konfigurisati identifikaciju tako da lozinke zastari nakon 90 dana, te onemogućiti korišćenje lozinki koje su već potrošene, ako sistem to dozvoljava.

Broj: 04-051/18-5929/1

Podgorica, 26.03.2018

Црна Гора Управа за кадрове 1 Подгорица

DIREKTORICA
Svetlana Vuković