

Postojeća regulativa o elektroničkoj pošti i pravnoj zaštiti privatnosti

Pitanje pravne zaštite on-line privatnosti u Republici Hrvatskoj uređeno je kroz veći broj zakona. Dakle, ne postoji jedan zakon, odnosno, kodeks u kojem se mogu naći sve odredbe koje reguliraju to područje.

- Temeljni akt Republike Hrvatske – Ustav, štiti pravnu zaštitu osobnog i obiteljskog života, slobodu i tajnost dopisivanja te sigurnost i tajnost osobnih podataka.
- Kazneni zakon RH inkriminira povredu on-line privatnosti u nekoliko kaznenih djela, a to su: povreda tajnosti pisama i drugih pošiljaka; nedozvoljena uporaba osobnih podataka; povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava; računalno krivotvorenje i računalna prijevara.
- Zakon o odgovornosti pravnih osoba za kaznena djela uvodi kaznenu odgovornost pravnih osoba vezano uz kaznenu odgovornost fizičke osobe koja vodi poslove pravne osobe ili joj je povjereno obavljanje poslova iz područja djelovanja pravne osobe. Dakle, prema ovom Zakonu dolazi u obzir odgovornost trgovačkih društava i drugih pravnih osoba kao poslodavaca za povredu privatnosti poruka elektroničke pošte.
- Zakon o zaštiti osobnih podataka također uređuje zaštitu osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u RH.
- Zakon o radu propisuje zaštitu privatnosti radnika, pa se osobni podaci radnika smiju prikupljati, obrađivati, koristiti i dostavljati trećim osobama samo ako je to određeno ovim ili drugim zakonom ili ako je to potrebno radi ostvarivanja prava i obveza iz radnog odnosa odnosno u svezi s radnim odnosom.
- Zakon o telekomunikacijama te Zakon o elektroničkoj trgovini uvode ograničenja na tzv. spam poruke, odnosno, nezatražena komercijalna i telekomunikacijska priopćenja.

Sve veće hrvatske kompanije pri zapošljavanju zahtijevaju od zaposlenika potpisivanje pravila kojih se moraju pridržavati dok rade na tvrtkinim računalima.

Informacijski sustavi i tehnologije u službi prodaje

U današnjem dinamičnom tržišnom okruženju primjena naprednih informacijskih i komunikacijskih tehnologija uvelike doprinosi uspješnosti poslovanja kompanije. Informacijski sustavi i podaci koje oni sadrže su vrlo bitni za poslovanje tvrtke koje ih koriste. Povećanjem uporabe elektroničkih informacija u poslovanju povećava se i zabrinutost oko sigurnosti sustava i podataka koji su u njemu pohranjeni. Da bi se podaci i informacijski sustavi kvalitetno zaštitili važno je osmisliti i provesti politiku sigurnosti koja ponekad iziskuje velika ulaganja.

PRIPREMIO: *Željko Popović*
FOTO: *Dejan Čikeš*

Sigurnost podataka u poslovanju više nije luksuz već jedan od primarnih ciljeva u razvoju poslovanja. Stoga jača naglasak na sigurnost informacijskoga prostora pojedine tvrtke. Kako Internet omogućuje slobodan pristup informacijama, korisnici računala ne moraju poznavati način rada ili prirodu prijenosa podataka, ali moraju poznavati definirana pravila ponašanja donesena u tvrtki u kojoj rade.

Pravila za ponašanje na Internetu nastala su na temelju RFC-ova (Request for Comments) dokumenta 1855 koji opisuje standarde na kojima se temelji Internet. Prvi dokument napisan je daleke 1969. godine, a danas ih postoji čak 4.402. U dokumentu 1855 navodi se minimalni skup pravila ponašanja koji služi kao predložak različitim tvrtkama, organizacijama i pružateljima usluga za stvaranje vlastitoga kodeksa ponašanja korisnika i administratora. Stoga tvrtke, odnosno organizacije koje pružaju uslugu pristupa i korištenja Interneta izrađuju dokument u

kojem navode opća pravila ponašanja na mreži i smjernice za komuniciranje prilikom korištenja Interneta. Sadržaj pravilnika podijeljen je na nedopuštene aktivnosti i predložene smjernice za komuniciranje preko e-maila, useneta i mailing lista.

Pravila ponašanja na Internetu mogu se podijeliti u dvije skupine: ona koja se odnose na privatnu komunikaciju dviju osoba (e-mail) i ona koja definiraju komunikaciju grupe ljudi, što se odnosi na informacijske grupe, distribucijske liste, foruma i sl.

Svaki zaposlenik koji ima pristup računalu trebao bi imati vlastiti korisnički račun (ime, lozinku) i za sve aktivnosti pod tim računom odgovoran je samo vlasnik korisničkog računa. Stoga je zabranjeno upotrebljavanje tuđeg računa ili posuđivanje vlastitoga drugim osobama. Zabranjeno je i lažno predstavljanje pri korištenju mrežnih usluga i servisa te uporaba podataka

koji nisu javno dostupni, već su namijenjeni privatnoj upotrebi drugih osoba. Nisu dopušteni neautorizirani pokušaji dobivanja pristupa tuđem korisničkom računu i resursima ni mijenjanje ili uništavanje tuđih informacija te ometanje korisnika preko elektroničke pošte u bilo kojem obliku.

Osim stavljanja informacija u javnu upotrebu bez suglasnosti njihova vlasnika, nije dopušteno ni distribuiranje informacija koje su suprotne općeprihvaćenim načelima ponašanja na mreži i moralnim normama te narušavaju ugled pojedinca i tvrtke.

Korisnike pri komuniciranju e-mailom treba upozoriti na to da se gotovo svakodnevno pojavljuju novi virusi koji mogu nanijeti izravnu i neizravnu štetu. Neotkriveni napadi mogu uništiti cijele baze podataka, smanjiti produktivnost i naštetiti ugledu poduzeća ako se preko njegova sustava zaraze i sustavi njegovih poslovnih partnera i klijenata.

Sigurnost kompanijinog informacijskog prostora u kontekstu prodajnih aktivnosti

Tržišna utakmica odvija se sve bržim tempom, zahtjevi krajnjih korisnika sve su složeniji te je uspjeh u prodaji i marketingu informacijsko-komunikacijskih rješenja sve teže postići. Pri tomu je izuzetno značajno korištenje raznih naprednih komunikacijskih tehnologija, što omogućuje razne vidove rada s udaljene lokacije, od kuće, u pokretu odnosno od bilo kuda i u bilo koje vrijeme. U Ericssonu Nikoli Tesli, koji djeluje i kao važan korporativni prodajni i marketinški kanal prema više od deset tržišta Srednje i Istočne Europe te Srednjega istoka velika je pažnja posvećena izgradnji sigurnosnog sustava.

Ericsson ima razrađen vlastiti sustav zaštite te dobro uspostavljene i opisane procese. Zaštita se provodi na nekoliko razina kao što su fizička zaštita, nadzor pristupa, osiguranje podataka i mrežnih komunikacija, osiguranje pouzdanosti i raspoloživosti i slično. Pristup kompanijskom informacijskom prostoru imaju samo autorizirani korisnici koji se jednoznačno identificiraju svojim korisničkim identifikacijskim imenom i potvrđuju lozinkom.

Korisnici imaju pristup samo onim podacima i onim IT resursima kojima zbog prirode svoga posla moraju imati pristup. ETK pristupa Internetu putem 15Mbps MetroEthernet T-Com usluge. Pristup izvana i izlazak iz ETK mreže nadzire se i u skladu je s korporacijskom sigurnosnom politikom, a ostvaruje se

pomoću nekoliko vatrozida, antivirusnih uređaja, filtera sadržaja te zastupnika raznih usluga (HTTP, FTP proxy). Ericsson ima normiranu IT okolinu tako da svi klijenti (Windows platforma) rabe uobičajeni i certificirani niz hardvera i softvera.

Antivirusna zaštita je riješena na korporativnoj razini. Svi klijenti i serveri rabe isti antivirusni softver. Instalacija i nadogradnja softvera na klijentima izvodi se sa središnjih poslužitelja. Ažuriranje virusnih definicija odvija se trenutačno i bez utjecaja korisnika.

Za zaštitu osjetljivih podataka se koristi enkripcija, i to i u pohrani i u komunikaciji putem pošte. Sva Ericssonova prijenosna računala imaju obvezu instaliranja softvera za enkripciju. Zaposlenici naše tvrtke imaju mogućnost pristupa mrežnim resursima od kuće, iz hotela s Internet kioska u zračnim lukama, „cyber caffee“ i slično za što se rabi nekoliko načina uspostave komunikacije preko Interneta SSL/VPN tunelom (GPRS, ISDN, xDSL, UMTS, Edge, Wireless Hot Spots...) ili izravnom modemskim pristupom. U svim slučajevima se koristi dvostruka autentifikacija i to „Radius“ serverom, koristeći

jednokratnu lozinku te putem „Active Directory“ usluge.

Velika pažnja se posvećuje osiguranju pouzdanosti i raspoloživosti IT resursa i stoga su uspostavljene procedure rekonstrukcije podataka u slučajevima pada sustava (disaster recovery and backup/restore procedures), kao i upravljanje promjenama (change management). Svi mrežni resursi se centralno nadgledaju, a zapisi se čuvaju i obrađuju da bi se u slučaju povrede sigurnosti moglo odmah intervenirati.

