



INFORMACIJSKA VARNOST V PODJETJU

Podatki predstavljajo kapital podjetja in prav zaradi tega dejstva je potrebno z njimi tako tudi ravnati. Za učinkovito ravnanje s podatki je potrebno zagotoviti, da so hranjeni varno in so vedno dostopni. V nadaljevanju vam predstavljamo nekaj nasvetov, kako lahko izboljšate informacijsko varnost v vašem podjetju:

1. ZAŠČITITE RAČUNALNIK

Namestite požarni zid in protivirusni program, vse potrebne popravke vašega operacijskega sistema in najnovejšo različico spletnega brskalnika.

2. PAZITE NA GESLA

Izberite geslo, ki ga ni lahko uganiti (daljše od 8 znakov, vsebuje naj male in velike črke, številke in ločila), in ne uporabljajte enakega gesla za vse uporabniške račune. S kvalitetnimi gesli boste goljuhofom otežili dostop do vaših podatkov.

Posebno pozornost je potrebno nameniti tudi pri elektronskem poslovanju z bankami, saj vse več goljufov z različnimi elektronskimi sporočili poskuša pridobiti gesla. Zavedati se moramo, da nas banka ne bi nikoli pozvala, da naj dostavimo osebne podatke in gesla preko elektronskih sporočil.

3. ARHIVIRAJTE, ZAKODIRAJTE ZAUPNE PODATKE IN INFORMACIJE

Pomembno je, da arhivirate ključne oz. občutljive podatke in redno preverjate ali je vse arhivirano tako kot mora biti.

Zaupne informacije zakodirajte tako, da si tehnologijo za kodiranje naložite na vse računalnike, pametne mobilne telefone, tablične računalnike, prenosnike in prenosne medije, kot so USB ključki. Na tak način boste zavarovali zaupne informacije pred vdorom oz. neavtoriziranim vstopom.

4. ZAŠČITITE SVOJE PAMETNE TELEFONE IN TABLIČNE RAČUNALNIKE

Uporaba pametnih telefonov in tabličnih računalnikov narašča z veliko hitrostjo, tako v svetu kot pri nas. te naprave omogočajo vrsto zabave in prav tako vrsto pisarniških opravil. Prav zato je potrebno imeti zanesljivo zaščito, katera ščiti napade preko interneta, pred raznimi škodljivimi programi. Potrebno je zaščititi tudi pomembne podatke, ki so shranjeni v vašem pametnem telefonu ali tabličnem računalniku, v primeru če pride do izgube ali odtujitve naprave. Priporočljivo je, da namestite antivirusni program in ga redno posodabljate; ustvarite zaščito z vklopljenim »požarnim zidom«; posodabljate svoj operacijski sistem; namestite filter za neželeno pošto, proti vohunski program in filter za neprimerne vsebine.

5. VARNO UPORABLJAJTE ELEKTRONSKO POŠTO

Uporaba elektronske pošte je na spletu povsem običajno pravilo, ki je poceni, preprosto in učinkovito sredstvo za komuniciranje. Vendar je vse več prevar z elektronsko pošto, ki se jim lahko izognemo na naslednje načine: ne odpirajte e – pošte od neznancev; neželena sporočila pobrišite takoj; izogibajte se vsem sporočilom, ki vam obljublajo hiter zaslužek; svojih osebnih informacij ne razkrivajte na sumljivih spletnih straneh; redno posodabljate svoj operacijski sistem; izogibajte se brezplačni programski opremi; uporabljajte protivohunski program.

6. ZAŠČITITE SVOJO SPLETNO STRAN

Pri optimizaciji svoje spletne strani bodite posebej pozorni na izbiro partnerjev. Poceni optimizacija ne prinaša vedno pozitivnih učinkov, še posebej ne na dolgi rok. Začetni investiciji optimizacije raje namenite nekoliko višjo vrednost in si na tak način zagotovite strokovnega partnerja, ki bo vaši spletni strani poleg višjega položaja na iskalnikih, zagotovil tudi varnost.

7. IZOBRAZITE ZAPOSLENE

Ne glede na to, kako dobro se zavedate problema varnosti na spletu, vam to nič ne pomaga, če vaši zaposleni nimajo tega znanja. Redno informirajte in izobražujete vaše zaposlene o varnosti na spletu in novih nevarnostih, ki pretijo.

8. BODITE AŽURNI

Ni pomembno, kako dober sistem za varnost ste vgradili, v kolikor je minilo že nekaj mesecev ali let, morda ta sistem sploh ni več primeren za vas. Vse varnostne sisteme morate redno nadgrajevati, saj se vsakodnevno pojavljajo novi virusi, novi črvi in novi načini delovanja spletnega kriminala.


Direktorica: Miroslava ROMIH univ. dipl. ekon.

P.S.: S sodobno in kakovostno varnostno politiko boste sebi in drugim prihranili marsikatere skrbi. Pa varno brskanje po spletnih straneh in internetu vam želimo tudi v letu 2013!

