

Mi az információbiztonság? 2. RÉSZ

Cikkünk második részében az internet, a dokumentumkezelés és a legegyszerűbb kapcsolattartási eszköz, a telefon használatának információbiztonsági kockázataira térnénk ki.

Internet - közösségi oldalak

Napjainkra az internet a mindennapi életünk része lett. Azok is, akik otthon nem rendelkeznek internet-eléréssel, sokszor a munkahelyükön hozzáférhetnek. Az internethasználatnak – kétségtelen előnyei mellett – bizony sok kockázata és veszélye is van. Jelen fejezetben nem foglalkozunk az informatikai, technológiai fenyegetettségekkel, hanem elsősorban az információk interneten való kezelésének módját, veszélyeit tárgyaljuk. Az egyik legfontosabb dolog, hogy személyes adatainkat csak nagyon körültekintő módon adjuk meg, és azt is lehetőleg csak olyan honlapokon, amelyek biztonságosnak tekinthetők. Tipikusan ilyenek (megbízhatóak) a bankok honlapjai, illetve egyéb ismert internetes vásárlói oldalak. Azonban mindenképpen

felhívni a figyelmet az úgynevezett adathalász¹ támadásokra, amelyek során a gyanútlan felhasználóktól kicsalják személyes adataikat, és azokkal különböző csalásokat követnek el. Információbiztonsági szempontból rendkívül veszélyesek az úgynevezett közösségi oldalak, amennyiben a felhasználó nem a megfelelő módon és nem a megfelelő gondossággal használja azokat, hiszen a közösségi oldalak célja, hogy barátokat, ismerősöket hozzon össze az interneten keresztül. Ezek az oldalak mód van arra, hogy minden felhasználó, aki regisztrálta magát, különböző személyes információkat adjon meg magáról, az e-mail címektől kezdve, lakcímet, telefonszámokat, fényképeket, munkahelyeket, hobbit stb. Szeretnénk felhívni a figyelmet, hogy nem csak tisztességes szándékú felhasználók



regisztrálhatnak ezekre a közösségi oldalakra, a közösségi oldalon önként közzétett információkkal könnyen vissza lehet élni.

Dokumentumok kezelése

A kezünkbe kerülő dokumentumokkal is rendkívül körültekintően kell bánnunk. Az esetek túlnyomó részében a napi munkavégzés során bizalmas dokumentumokkal dolgozunk, ezért ügyelni kell arra, hogy a bizalmas üzleti dokumentumok ne kerülhessenek illetéktelen kezekbe. Érdemes odafigyelni arra, hogy a dokumentumok ne szanaszét heverjenek az íróasztalon, hanem rendezetten, iratgyűjtőben, dossziében. Abban az esetben, ha valamilyen okból rövidebb időre el kell hagyni az irodát, célszerű a dokumentumokat vagy lefelé fordítva, vagy egymásra helyezve egy „kupacban” az asztalon hagyni. Amennyiben hosszabb időre kell elhagyni az irodát (legalább félnapos távollét), illetve munkaidő végén, a bizalmas jellegű üzleti dokumentációkat minden esetben célszerű elzárni. Ne feledjük, hogy a takarító személyzetre sem tartoz-

nak a cég belső ügyei! Nagyobb vállalatoknál létezik úgynevezett „Tiszta asztal szabályzat” (Clean Desk Policy), amely többek között szabályozza és egyben segítséget is nyújt (gyakorlati tanácsokkal) abban, hogy az adott munkahelyen hogyan kell a napi munkavégzés során a dokumentumokat kezelni².

Telefonos kapcsolattartás

A telefon akár hagyományos vonalas telefonról, akár mobiltelefonról beszélünk, mára a hétköznapi élet szerves része lett. Gyakorlatilag a tizenéves gyerekektől kezdve a nyugdíjasokig, szinte mindenkinek van valamilyen telefonkészüléke. Az üzleti életben a mindennapi munka elengedhetetlen kelléke, nélküle szinte megállna az élet. Ugyanakkor sokan hajlamosak információbiztonsági szempontból lebecsülni a telefont, mint kockázati tényezőt. Miben rejlik a telefonálás kockázata? A legnagyobb kockázat, hogy igazából nem tudjuk azonosítani a hívó vagy hívott felet. Biztonsággal csak akkor tudunk bárkit azonosítani a vonal másik végén, ha személye-



¹ Akit bővebben érdekel a téma, az keresen rá az interneten az „adathalászat” vagy „phishing” kifejezésekre

² Az iratkezelési vagy dokumentumkezelési szabályzat sokkal generálisabb szabályokat, eljárásokat tartalmaz



sen ismerjük, és természetesen felismerjük a hangját. Az üzleti életben azonban nem ismerhetünk mindenkit személyesen. Ezért fontos hangsúlyozni, hogy a munkatársak legyenek tisztában azzal, hogy telefonon keresztül kinek, milyen információt szabad kiadni. Képesnek kell lenni arra, hogy az esetlegesen tolatkodó vagy akár zaklató jellegű hívásokat megfelelő határozottsággal és kellő diplomáciai érzékkel kezeljük. Ki kell dolgozni azokat a megoldásokat, amelyek segítségével nagy biztonsággal megtudjuk határozni a hívó személyét.

Social Engineering

A fenti kifejezést nehéz megfelelően magyarrá fordítani. A Social Engineering egy elkövetési mód, ahol a tisztességtelen szándékú személy, különböző fortélyokkal, ravasz trükkökkel próbál meg számára fontos információkat megszerezni az áldozatától. Amennyiben pontosabban szeretnénk meghatározni, hogy mit is jelent a kifejezés, akkor azt mondhatjuk, hogy a Social Engineering: emberi hiszékenységen és jóindulaton ala-

puló emberi kapcsolatokat felhasználó csalási forma. Az elkövetők hatalmas eszköztárral rendelkeznek egy-egy információ megszerzésére. Nagyon gyakori eset – telefonos információszerzés esetén –, hogy a hívó fél valamilyen befolyásos barátra, ismerősre vagy – már korábban megszerzett információ alapján – a hívott közvetlen főnökére való hivatkozással kér bizonyos információkat. Szintén itt említanék meg azt az esetet, amikor a hívó a vállalat informatikusának adja ki magát, és különböző dolgokra hivatkozva kéri a felhasználót (hívott fél), hogy adja meg a felhasználói jelszavát vagy esetleg magyarázza el, hogy egy speciális alkalmazást (könyvelőrendszert, készletnyilvántartó rendszert stb.) hogyan is kell használni.

Nem célunk, hogy bárkire fölöslegesen rájesszünk, elsősorban az információbiztonság széleskörűségére szeretnénk rávilágítani. Ahhoz, hogy egy gazdálkodó szervezet üzleti titkait, belső, bizalmas információt megvédhessük, minden apró jelre, tényezőre oda kell figyelni.