Információbiztonság a hétköznapokban

Jelen cikkemben az információbiztonság fontosságát próbálom bemutatni mindennapi tevékenységünk során. Számos olyan szakmai cikk született a témában, amely különböző szakmai szempontok alapján boncolgatta ezt a kérdést, mint például a banki szféra információbiztonsága vagy az internet információbiztonsága.

szerző: KISS PÉTER
Információbiztonsági szakértő, tanácsadó. Rendszeresen tart szervezett képzéseket nagyvállalati környezetben, információbiztonsági témában. Független szakértőként nemzetközi és hazai nagyvállalatoknál segíti az információbiztonsági rendszerek kialakítását, felülvizsgálatát. Közel tíz éves szakmai tapasztalattal rendelkezik az ISO27001-es szabvány bevezetésében, működtetésében, rendelkezik információbiztonsági auditori

Olyan témákra fókuszálok, és olyan példákat próbálok felvillantani, amelyek mindenkinek ismerősek lehetnek a hétköznapi tevékenységei, illetve egyéb, például céges ügyek intézése során.

A BANKI ÜGYINTÉZÉS „CSAPDÁI”

Az egyik klasszikus terület a banki szolgáltatások igénybevétele. Ma már mindenki tudja, hogy a PIN kódot a bankkártyától külön kell tárolni, hogy a pénzkiadó automaták használatakor vagy kártyával történő fizetés esetén, a PIN kódot lehetőleg úgy kell beütni, hogy a mögöttünk álló ne lássa. Ugyanakkor itt hívnám fel a figyelmet, hogy a kamerás megfigyelő rendszerek terjedésével párhuzamosan találkoztam már olyan kamerával (irodaházban), amelyik fölülről pont rálátott a terminál billentyűzetére. Ebben az esetben hiába takarjuk el a testünkkel a billentyűzetet, attól még a kamera rögzíti azt.

Érdekes banki tapasztalat a különböző önindigós nyomtatványok (tipikusan a készpénz be- és kifizetési nyomtatvány) kihelyezése és használata. Sok bankban, ahol ezek a nyomtatványok ki vannak téve, pont akkora a hely, hogy a nyomtatványok ugyan elférnek rajta, de az ügyfeleknek nemigen marad helye azokat kitölteni. Ezért sokan – értelemszerűen – az egymásra helyezett nyomtatványok közül a legfelsőt kezdik el kitölteni, figyelmen kívül hagyva az alatta lévő többi nyomtatványt.

Ebben az esetben a veszély egyértelmű. Miközben az ügyfél kitölti a saját nyomtatványát, e közben – az írása erősségétől függően – a közvetlenül alatta lévőn, egyes esetekben még az alatta lévő harmadik nyomtatványon is láthatóak az adatai. Mivel önindigós nyomtatványokról van szó, ezért a többi nyomtatvány első példányán nem lesznek láthatóak az adatok (nem vesszük észre), viszont a másodpéldányokon igen, mivel az erőteljes kézírás azokon is „átnyomódik”. Jómagam, amikor ilyen szituációban nyomtatványt töltök ki, három esetből egyszer biztosan találok ilyen, nem szándékos „többlet” példányt egy-egy előttem ott járt ügyféltől. Sajnos beidegződés, hogy mielőtt nekiállok kitölteni a saját nyomtatványomat, mindig megnézem, hogy a másodpéldányon láthatóak-e az előző ügyfél adatai. Ezekből többek között kiderül, hogy az előttem ott járt ügyfél mennyi pénzt vett fel, milyen cég

nevében, milyen bankszámlaszámról, ki volt a befizető, milyen okmánnyal igazolta magát, az adott okmány száma, végül, de nem utolsósorban az illető aláírása. Ezek után – gondolom – nem szükséges részleteznem, hogy ezen adatok birtokában milyen visszaéléseket lehet elkövetni pusztán azért, mert az adott személy nem kellő körültekintéssel töltött ki egy önindigós nyomtatványt!

Apró érdekesség az új Széchenyi kártya használatával kapcsolatos. Nem tudom, ki figyelte meg, de a Széchenyi kártyával történő fizetés esetén a visszakapott kártyabizonylat tartalmazza a kártyán maradó összeget is. Ezért nem célszerű ezt a bizonylatot „csak úgy” eldobni, tépjük szét, ha csak nem akarjuk egy esetleges megtaláló tudomására hozni az aktuális egyenlegünket.

OKMÁNYAINK BIZTONSÁGA

Másik, szintén érdekes terület a hétköznapokból a közüzemi szolgáltatóknál (például ELMŰ, Főgáz, E. ON) történő ügyintézés. Nem tudom, hogy az olvasók közül hányan vannak tisztában vele, de minden szolgáltatónál következmények nélkül meg lehet tagadni, hogy a személyazonosító okmányainkról fénymásolatot készítsenek. Hasonlóan érzékeny adat lehet egy adás-vétel kapcsán az adás-vétel összege. Mivel a közüzemi szolgáltatóknál a különböző mérőórák átírásakor elkérik az eredeti szerződéseket, mód van arra, hogy az ügyfél kérje, hogy az adás-vétel összegét kitakarják a fénymásolaton. Ez az információ nem feltétlenül tartozik a szolgáltatókra, illetve az ügyintézőkre.

OKOSTELEFONOK ÉS ALKALMAZÁSAIK

Végül, de nem utolsósorban szeretnék néhány gondolatot megosztani az okostelefonok és az azokon futó alkalmazások biztonságával kapcsolatban. Mindenki ismeri a Facebook-ot, és vélhetően sokan ismerik a FourSquare nevű alkalmazást. Alapvetően mindkettő az ismertségi hálózatok (social networks) körébe tartozik. Míg a Facebook-on gyakorlatilag mindent meg tud osztani magáról a felhasználó, addig a FourSquare alapvetően a felhasználók mozgását, tartózkodási helyét hivatott megosztani. Mindkettő esetében érdemes odafigyelni, hogy a felhasználó, amikor nem használja az alkalmazásokat, minden alakalommal lépjen ki belőlük. Az okostelefonok nyújtotta kényelem miatt a legtöbb felhasználó egyszer beírja az e-mail címét és jelszavát, majd soha többet nem lép ki az alkalmazásokból, szemben a számítógépeken történő használat után. Ez azt a veszélyt hordozza magában, hogy bárki, aki hozzáfér – akár pár percre is – az adott okostelefonhoz, könnyedén hozzáférhet ezekhez az alkalmazásokhoz is. Ugyanez igaz az okostelefonokon futatott (szinkronizált) levelezésekre (e-mail) is. Ezért érdemes beállítani az okostelefonokon, hogy automatikusan zárolják magukat – lehetőleg minél hamarabb – amint nem használjuk őket. Ezen túl célszerű az ilyen alkalmazásokból külön-külön is kilépni.

Szintén érdemes elgondolkozni azon, hogy milyen információkat osztunk meg magunkról. Különösen a FourSquare esetében nem biztos, hogy érdemes minden egyes helyről bejelentkeznünk, ahol járunk, főleg ha esetleg ezt munkaidőben tesszük, nem a munkánkkal összefüggésben, és a főnökünk – mint bejelölt barát – esetleg láthatja, követheti a mozgásunkat. Vélhetően kellemetlen percektől kímélhetjük meg magunkat némi odafigyeléssel a megosztott információk tekintetében. Szintén nem érdemes a saját lakásunk címét létrehozni, és minden alkalommal megadni, bejelentkezni onnan, ha éppen otthon tartózkodunk, mivel így nagy pontossággal követhetővé válik, hogy mikor tartózkodunk otthon. Ezzel kapcsolatban szeretném megemlíteni – nem elrettentésképpen –, hogy követtek már el több betörést is a felhasználó távollétében, mivel – saját közlékenysége okán – a betörő pontosan tudta, hogy az adott időben távol van otthonától. Nem sokat kockáztatott…

Remélem, jelen cikkemmel sikerült egy picit szélesebb, a mindennapokhoz kapcsolódó példákon keresztül bemutatnom az információbiztonság fontosságát, illetve azt, hogy némi odafigyeléssel sok kellemetlenségtől kímélheti meg magát a Tisztelt Olvasó.