

TARTALOMJEGYZÉK

1	Bevezetés.....	2
1.1	Miért fontos az információbiztonsággal foglalkozni?.....	2
1.2	Mit jelent az információbiztonság?.....	2
2	Információbiztonság és a titkárői feladatok.....	4
2.1	Kritikus helyzetek avagy mikor sérülhet az információbiztonság?.....	5
3	Zárszó.....	12

1 Bevezetés

Jelen cikkünkben egy olyan témával szeretnék foglalkozni, amelyet mindenki ismer, munkája során folyamatosan nap, mint nap találkozik vele, de igazából nem vagy csak nehezen tudja egy szóval kifejezni, hogy miről is van szó. Ez a szó pedig az információbiztonság. Jelen van a napi munkavégzés során, hiszen a vállalat cég információit, adatait meg kell tudni védeni a jogosulatlan és/vagy illetéktelen megismeréstől. Tetten érhető a magánéletünkben, hiszen nem kürtöljük világgá, hogy a kosztpénzt hol tartjuk a lakásban, hogy milyen riasztórendszert használunk lakásban vagy, hogy a páncélszekrény pontosan hol is található.

Az információbiztonság azt jelenti, hogy minden információ esetén, függetlenül az információ megjelenési formájától biztosítani kell az információk sértetlenségét, bizalmosságát és rendelkezésre állását.

1.1 Miért fontos az információbiztonsággal foglalkozni?

A mai információs társadalomban az információ az egyik legnagyobb, ha talán nem a legnagyobb érték. Gondoljunk csak bele, aki megfelelő információval rendelkezik pl. egy nagy ingatlan beruházás előtt, az a beruházás tervezett helyén kellő időben megvásárolt földterület segítségével nagyon rövid idő alatt nagyon sok pénzt tud keresni. Szintén ilyen kategória, ha idő előtt kiderül, hogy az egyik cég a jövőben fel kívánja vásárolni a versenytársát, akkor a megvásárolni kívánt cég részvény árfolyamai emelkedni fognak és itt is (a bennfentes kereskedelem felhasználásával, amelyet egyébként a törvény büntet) az illegálisan megszerzett és felhasznált információ segítségével óriási profitra lehet szert tenni. De nem menjünk ilyen messzire a kisebb cégek esetében (Bt.-k, Kft-k) sokkal hangsúlyosabb szerepet kap az üzleti titkaik, belsőinformációk megvédése, mivel ezek a cégek a kis méretüknél fogva (mind pénzügyileg, mind személyi állományt tekintve) sokkal nehezebb képesek túl élni egy-egy bizalmas információ kiszivárgást.

Napjainkban – sajnálatos módon –folyamatosan találkozni olyan híradásokkal, amelyek arról szólnak, hogy hány ezer bankkártya adatot loptak el, hogy törtek fel informatikai rendszerek, a gyanútlan jóhiszemű embereket, hogyan csapták be.

1.2 Mit jelent az információbiztonság?

Nézzük, hogy mit értünk az információk megjelenési formája alatt értjük:

- Dokumentumokat, Az írásos információkat (szerződések, ajánlatok, tervek, szakvélemények, stb.)
- A szóban közölt információkat (beszélgetés a folyosón, büfében, étteremben, stb.)
- Az elektronikusan kezelt, továbbított, tárolt információkat (pl. telefonok, faxok, mobiltelefonok, különböző adathordozók, memória kártyák, SIM kártyák, pendrive-ok, stb.)
- Az informatikai (IT) rendszerekben kezelt, tárolt és feldolgozott információkat (például: e-mail-ek, táblázatok, dokumentumok, adatbázisok)

A fenti – nem teljes körű – felsorolásból is kellőképpen látszik (érezhető), hogy mennyire széleskörű az információk köre és, hogy a mai információs társadalomban mennyire körülveszi az embereket az információ.

Nézzük meg pontosabban, hogy a hármas feltétel rendszert – sértetlenség, bizalmasság és rendelkezésre állás – amelyet az információk biztonsága érdekében biztosítani kell, mit is jelentenek.

Sértetlenség azt jelenti, hogy az információ a folyamatosan megfelel keletkezésekor vagy létrehozásakor állapotának. Bővebben, hogy az eredeti információt nem torzították, nem tettek hozzá és nem vettek el belőle.

Példa

Erre az egyik legjobb példa a monda. A mondákról mindenki tudja, hogy van valóság alapja (tehát van az alap információ), de mire eljut a harmadik, negyedik, sokadik emberhez addigra az alap információ torzul. Lehet, hogy az alap információ szerint valaki meghalt végelgyengülésben a házában, de a monda szerint megölték és nem a házában, hanem egy mezőn.

Bizalmasság azt jelenti, hogy az információkhoz csak és kizárólag azok személyek férhessenek hozzá, akik erre jogosultak.

Példa

Itt a példa kedvéért had említsem meg a bérfizetési papírok esetét. Mindenkinek magánügye, hogy mennyit keres. Ezért az adott vállalatnál a bérszámfejtést végző kollégának rendkívül nagy a felelőssége abban, hogy a bérszámfejtés során, amíg dolgozik a kinyomtatott bérszámfejtési dokumentumokhoz egyik illetéktelen kolléga se férhessen hozzá. Csak és kizárólag zárt borítékban kerüljenek ki az irodából a bérszámfejtési dokumentumok.

Rendelkezésre állás azt jelenti, hogy az információk ott és akkor álljanak rendelkezésre amikor és ahol szükség van rájuk. A példa kedvéért, ha valaki a tőzsdén végez pénzügyi befektetéseket akkor bizonyos üzleti információkra akkor van szüksége mielőtt meghoz bizonyos pénzügyi döntéseket, de ez igaz minden döntés hozatali fázisra, hogy megalapozott döntést csak és kizárólag abban az esetben lehet meghozni ha az összes szükséges releváns információ rendelkezésre áll. Amennyiben az információk rendelkezésre állása nem biztosított, nem lehet megfelelő döntéseket hozni.

Példa

Például, ha valaki elmegy a boltba, hogy szeretne venni 3 üveg üdítőt, és nem tudja előre, hogy mennyi az üdítő ára akkor nem fog tudni elég pénzt magával vinni, hogy megvegye a szükséges mennyiségű üdítőt. A boltban, amikor látja az árcímkét, már nem sokat ér az információval, hiszen a pénze otthon van

Fontosnak tartom kiemelni, hogy az információbiztonság nem azonos az informatikai biztonsággal (IT biztonság, IT security).

Míg az információbiztonság, ahogy a fentiekben már láttuk az információk teljes körű biztonságával foglalkozik (lásd. a definíciót), addig az informatikai biztonság csak és kizárólag az informatikai rendszerek, eszközök biztonságával foglalkozó szakterület. Sajnálatos módon még mindig nagyon sokan összekeverik a két fogalmat és nem csak laikusok, hanem sok szakember is.

Azt, hogy napjainkban mennyire időszerű és kiemelt terület az információbiztonság, az is mutatja, hogy van olyan idehaza is elfogadott nemzetközi szabvány (MSZ ISO 27001:2006 szabvány) amely abban segít a gazdálkodó szervezeteknek, hogy a szabványt bevezetve elfogadott, nemzetközi alapelveken nyugvó információbiztonsági eljárásokat vezethessenek be és alkalmazhassanak.

2 Információbiztonság és a titkárnői feladatok

Miért van kiemelt szerepe az információbiztonságnak a titkárnők, asszisztensek napi munkavégzése során?

A legtöbb gazdasági társaságnál, szerveztél a titkárnők, asszisztensek azok a személyek, akik a lehető legtöbb információt képesek összegyűjteni, összefogni és ráadásul a náluk megjelenő információ legnagyobb része igen értékes információnak tekinthető, mivel – munkakörükből adódóan – valamely vezető mellett dolgoznak, támogatva a vezető napi munkavégzését. A különböző szektorban tevékenykedő gazdasági társaságoknál az asszisztense munkája jelentősen eltérhet. Szintén fontos különbség a titkárnői, asszisztensi munka során az adott vállalat mérete, vállalati kultúrája. Egy-egy kisebb cégnél jellemzős, hogy a titkárnő vagy asszisztens kvázi a „mindenes” funkcióját tölti be. Gyakran ő intézi a különböző beszerzéseket kezdve a kávétól, a nyomtató papíron át a mobiltelefonokig. Sokszor szintén rá bízák, hogy a főnök mobiltelefonját vigye szervizbe, ha az meghibásodik, vagy ha jön a fénymásoló szerelő akkor is ő van jelen, illetve sok egyéb hasonló kisebb nagyobb dolgot felügyel. Éppen ezért fontos, hogy az asszisztens tisztában legyen a munkájára vonatkozó információbiztonsági elvárásokkal.

Szintén meg kell említeni azokat a személyi asszisztenseket, titkárnőket akik valamely közéleti szereplő, politikus vagy ismert ember mellett dolgoznak. Itt is kiemelt szerepe van az információbiztonságnak, vagy is a legtöbb esetben a személyes adatok védelmének. Elég egy apró figyelmetlenség vagy indiszkréción és esetleg máris a bulvársajtóban lehet olvasni az adott személy magánügyeiről.

Általánosságban minden asszisztensről és titkárnőről elmondható, hogy kezeli a főnök naptárát, esetleg az e-maileket, bejárása van a főnök irodájába, gyakran kap(hat) magánügyek elintézésére irányuló feladatot. Ugyanakkor abban is nagy szerepe van az asszisztenseknek, hogy milyen információkat továbbítanak a főnökük felé, hiszen egy elfoglalt vezető vagy egy elfoglalt személyiségnek gyakran nincs ideje arra, hogy saját maga nézze át a bejövő e-maileket, leveleket illetve a megbeszélésekre jelentkezők névsorát. Gyakorlatilag az asszisztensek sokszor szűrőként (is) funkcionálnak a főnökük és a külvilág között. Ezért roppant nagy a felelősségük abban, hogy hogyan és milyen információkat kezelnek, és az adott információkkal milyen gondosan bánnak.

Példa

Példaként hagy említsük meg a mobiltelefonok szervizbe adását. Fontos, hogy ha a cég valamely kulcspozícióban lévő munkatársnak a telefonját szervizbe viszi, megfelelően gondoskodjon a készüléken található információk megfelelő védelméről. Tudni kell, hogy legtöbb mai mobiltelefon sokkal több funkciót képe ellátni, mint az alapvető telefonálási képesség. A legtöbb készüléken van fényképezőgép, hangfelvevő, naptár és internet vagy e-mail funkció. Éppen a bővített funkciók miatt az adott készülék rengeteg olyan információt tartalmazhat, amely információk illetéktelen kézbe való kerülés súlyos üzleti vagy presztízs veszteséget okozhat az adott cégnek. Ezért fontos, hogy mielőtt szervizbe viszik a készüléket, minden esetben távolítsák el róla az összes információt (le lehet menteni) és kizárólag üres memóriával, adatok és információk nélküli készüléket adjunk át szervizelésre. A SIM kártyát se hagyjuk a készülékben, hisz ahhoz, hogy pl., kicseréljék a kijelzőt nem szükséges a SIM kártya, a szerviznek különben is van szerviz kártyája.

2.1 Kritikus helyzetek avagy mikor sérülhet az információbiztonság?

Fecsegés

Rengeteg olyan élethelyzet van a napi munkavégzés során, amikor is birtokunkban levő bizalmas üzleti információk sérülhetnek. Az egyik kockázati tényező maga az ember. Sok emberre jellemző, hogy szeret fecsegni, szeret jól értesültnek látszani, ezért adott helyzetben olyan dolgokról is beszél amelyekről nem lenne szabad.

Példa

Az óvatlan fecsegésre az egyik legjobb példa a vállalati büfé vagy étkezdé, de gyakorlatilag bármelyik étterem is megfelelő példa lehetne. Biztosan Ön is kedves olvasó találkozott már olyan helyzettel, hogy ült az asztalánál éppen az ebédjét fogyasztotta és megütötte a fülét, hogy a másik asztalnál ülő kollégák (a példa kedvéért a bérszámfejtésről) éppen a arról beszélgettek, hogy a különböző vállalatnál a következő évben a különböző területnél miképp fog változni a fizetés. Vagy beszélgethettek arról, hogy az egyik vezető beadta már a felmondását, de még hivatalosan nem jelentette be...

Másik tipikus helyzet a lift illetve az előtér ahol a munkatársak a liftre várakoznak. Nagyobb vállalatok esetén, ahol több száz fő dolgozik, természetes, hogy nem ismer mindenki mindenkit. Óhatatlanul előfordulhat, hogy két kolléga egymással beszélgetve egy harmadik kollégáról olyasmit mond ami kellemetlen lehet. Főleg akkor, ha a szóban forgó kolléga is épp a liftre várakozik, netán épp a liftben utazik... És ebben a példában nem is üzleti információkról beszélünk, pusztán személyes vélemény cseréről.

Informatikai eszközök

Érdekes kérdés információbiztonsági szempontból az informatikai eszközök, rendszerek használata. Az informatikai alkalmazásokkal kapcsolatban rengeteg biztonsági szabályra kell oda figyelni, a teljesség igénye nélkül egy párat azért mi ki szeretnénk emelni.

Jelszavak

Lehetőleg mindig egyedi jelszavakat használjunk illetve ha egy új beállítás miatt a rendszergazda ad a felhasználó számára egy jelszót, azt a felhasználónak haladéktalanul meg kell változtatnia. Ügyeljünk arra, hogy legalább 8 karakter hosszú jelszavakat használjunk, amelyek tartalmaznak kisbetűt, nagybetűt, számot és legalább egy speciális karaktert, mint pl. &; @; +; -; !; \$, stb. Szintén a jelszavak biztonságát növeli, ha

rendszeres időközönként (30 – 60 -90 naponta) megváltoztatjuk az addigi jelszavunkat. Természetesen minél gyakrabban változtatunk jelszót annál biztonságosabbnak tekinthető az aktuális jelszavunk. Ma már nagyon sok vállalatnál kötelezően be állításra került az informatikai rendszerben a jelszavak időnkénti rendszeres cseréje. NAGYON fontos, hogy a jelszavunkat soha senkinek ne áruljuk el, ne írjuk fel, hanem mindig tartsuk fejben. Soha ne adjuk meg senkinek a jelszavainkat, akkor se ha szabadságra megyünk és szeretnénk, hogy az e-mail-einkhez hozzáférjenek a munkatársaink. A mai informatikai rendszerek estén a rendszergazdák kb. 8 perces munkával (néhol a felhasználók maguk) be tudják állítani úgy a felhasználói postafiókot, hogy a felhasználó szabadsága alatt a kijelölt munkatárs anélkül is megkaphassa a szabadságon lévő e-mailjeit, hogy tudnia kellene annak jelszavát. Amikor a felhasználó visszatér a szabadságról akkor pedig megszüntetik a levelek átirányítását és folytatódik a munka a megszokott módon. Szintén nagyon fontos, hogy telefonon keresztül soha senkinek ne adjuk meg a felhasználó jelszavainkat. Amennyiben valaki azzal hív, hogy ő az informatikai terület munkatársa és kéri a felhasználó jelszavunkat valamelyik rendszerhez ne adjuk meg. Egyrészt nem lehetünk biztosak abban, hogy az illető valóban az, mint akinek kiadja magát¹. Másrészt pedig – főleg nagyobb rendszerek estén – az informatikusnak sincs szüksége az egyes felhasználók jelszavára, hiszen mint az adott alkalmazás rendszergazdája minden olyan jogosultsággal rendelkezik, amely ahhoz szükséges, hogy a munkáját maradéktalanul el tudja végezni.

Miért fontos a jelszavainkat biztonságban tartani?

Sokan hajlamosak azt hinni, hogy a jelszavaknak semmi jelentősége sincs, vagy, hogy egy fölösleges rossz vagy, hogy csak azért használjuk őket, mert „szokás” vagy „illik”. De nem így van. Ugyanis a felhasználói jelszavakhoz jogosultság és felelősség is társul. Pont az a jelszavak lényege, hogy egy – egy adott rendszerhez, amely jelszót kér (vagy egyéb azonosító módszert használ²) csak és kizárólag az a felhasználó férhessen hozzá, aki birtokában van az adott jelszónak. Ennek az a célja, hogy lehetőség szerint megakadályozza illetéktelen személyek jogosulatlan hozzáférést egy-egy informatikai rendszerhez. Tudni kell, hogy napjainkban a legtöbb informatikai rendszer képes naplózni, azaz nyomon követni, hogy az adott felhasználó milyen tevékenységet hajtott végre adott alkalmazásban (pl. adatot törölt, adatot módosított, új vevőt vett fel, számlát állított ki, XY-nak bérszámfejtett, stb.). Ez azért van így, hogy bármilyen probléma vagy visszaélés esetén meg lehessen találni a felelőst, hogy melyik felhasználó mit is tett pontosan.

Ugyanakkor az egyszerű jelszavas megoldás – amelyről jelen esetben beszélünk – ahol is a felhasználónak egy bármilyen bonyolult jelszót kell megjegyeznie messze nem nyújt tökéletes védelmet. A legtöbb esetben a felhasználók – szemben a bekezdés elején javasolt módszerrel - egyszerű, gyenge jelszavakat használnak, mert félnek attól, hogy a kicsit bonyolultabbakat nem jegyzi meg. Több statisztika készült, amelyből kiderült, hogy a leggyakoribb jelszavak vagy valamely közeli rokon, ismerős, kedvenc állat, kedvenc sport, csapat neve vagy szintén valamilyen évszám. Ezek a jelszavak nagyon rövidek könnyű a kitalálni vagy feltörni őket. A másik probléma, hogy a felhasználók egy része gondatlan és gyakorlatilag bárkinek megadja a jelszavát. És itt kezdődik a probléma. Ugyanis ha felhasználónak valamilyen módon megszerzik a jelszavát (ellopják, feltörik, jóhiszeműen megmondja, stb.) és a megszerzett felhasználó névvel és jelszóval belépnek egy alkalmazásba, a rendszer szempontjából olyan mintha a valódi és jogosult felhasználó lépett volna be. Az egyszerű jelszavak esetén a rendszer a személyt – aki a jelszót

¹ Lásd a Social Engineering fejezetet lejjebb

² Pl. Biometrikus azonosítás

használja - magát nem tudja azonosítani, erre csak a biometrikus azonosításon alapuló rendszerek alkalmasak.

Példa

A legtöbb felhasználónak például van jelszava az e-mail-jeit kezelő alkalmazáshoz. Miért? Azért mert az e-mailek csak és kizárólag a címzettnek szólnak (gyakorlatilag levéltitoknak minősül a magán e-mailek tartalma) és az a cél, hogy illetéktelenek ne tudják elolvasni. Ez egyaránt igaz akár céges e-mailekről akár magán e-mailekről beszélünk. Nyilván való, hogy a vezérigazgató üzleti levelezése senki másra nem tartozik csak és kizárólag őrá, illetve azokra, akikkel saját akaratából megosztja egy-egy levelének a tartalmát. És itt van az a pont ahol megjelenik az asszisztensek felelőssége (amennyiben a vezérigazgató asszisztense hozzáfér főnöke levelezéséhez) például abban, hogy senkinek ne adja meg saját jelszavát. Nyilván való, hogy amennyiben valaki megszerzi az adott vezető asszisztensének jelszavát, máris módja lesz a vezető e-mailjeit is elolvasni. Ugyanakkor az is az asszisztens felelőssége, hogy ha elhagyja a szobát, akkor a jelszavas képernyővédő segítségével zárolja a számítógépét többek között azért, hogy az ő számítógépén keresztül ne lehessen hozzáférni a főnök adataihoz (e-mail, naptár, to do, stb.)³.

Másik példa egy bérszámfejtő rendszer használata. Azoknak a munkatársaknak, akik bérszámfejtéssel foglalkoznak külön – külön jelszavuk van (ideális esetben) ahhoz, hogy be tudjanak lépni a bérszámfejtő programba. Egyrészt azért, hogy utólag meg lehessen állapítani, hogy pontosan ki mit is csinált a rendszerben, a másik szempont, hogy a különböző felhasználóknak különböző jogosultságai lehetnek. Lehet olyan felhasználó, aki a vállalat összes munkatársának a bérszámfejtését el tudja végezni, törzsadatokat vehet fel, módosíthat, törölhet és lehet olyan felhasználó, aki semmi másra nem jogosult, mint, hogy megnézze az adatokat és esetleg bérjegyzéket nyomtasson. Abban az esetben, ha valaki megszerzi a maximális joggal rendelkező felhasználó jelszavát és a megszerzett jelszóval visszaél (magyarul: belép a bérszámfejtő programba és megváltoztat egy-két törzs adatot, esetleg töröl adatot illegálisan) a rendszer azt fogja naplózni, hogy melyik felhasználó névvel követték el az adatok módosítását. Természetesen ki fog derülni, hogy ki volt az, aki módosított az adatokat és felelősségre fogják vonni. A gyanútlan felhasználó természetesen nem fogja érteni, hogy mi történt és csak egy hosszabb vizsgálat során derül majd ki, hogy pl. valakinek jóhiszeműen elárulta a jelszavát és az visszaélt a megszerzett információval⁴.

Képernyővédő használata

A másik kritikus terület a képernyővédő használata jelszóval védve vagy más néven a számítógép zárolása. Ezt a biztonsági eljárást akkor alkalmazzuk, ha valamilyen oknál fogva elhagyjuk a helyiséget (pl. ebéd, megbeszélés, dohányzás, wc, stb.) és a számítógépünket őrizetlenül hagyjuk. Akkor is őrizetlen a számítógép ha a szobában lévő másik kolléga bent marad, ugyanis nem tudhatjuk, hogy ő nem fogja-e elhagyni a helyiséget időközben. Amennyiben a rendszer magától is elindítja a képernyővédőt (pl. 2 perc nem használat után), akkor se várjuk ezt meg, hanem mielőtt elhagyjuk a helyiséget, mi magunk kézzel aktiváljuk a képernyővédőt. Ez azért fontos, mert egyrészt az alatt a két perc alatt bárki odaülhet a felhasználó számítógépe elé és hozzá férhet az össze információhoz, amire a gép felhasználója jogosult, a másik, hogy ha a 2 percen belül bárki meglöki az egeret vagy megnyom egy billentyűt, újra kezdődik a 2 perc újabb lehetőséget teremtve a jogosulatlan adathozzáféréshez.

³ Lásd a Képernyővédő használat című fejezetet

⁴ Lásd a Social Engineering fejezetet

Példa

A felhasználó elhagyja a szobát és nem zárja le a számítógépét. Bárki, aki odaül a gépe elé el fogja tudni olvasni a felhasználó üzleti levelezését nem beszélve az estelegesen ott lévő személyes tartalmú levelekről. Ezen túlmenően a főnök leveleihez is hozzáférhet a főnök naptárához is (ez természetesen akkor lehetséges, ha a felhasználónak, asszisztensnek joga van a főnök levelezéséhez, naptárához hozzáférni).

Amennyiben a felhasználó a bérszámfejtésen dolgozik, bárki aki odaül az őrizetlen, lezáratlan számítógéphez képes lehet a cég bérszámfejtő rendszeréhez hozzáférni és abból jogosulatlanul adatokat megszerezni.

Internet – közösségi oldalak

Napjainkra az internet a mindennapi életünk része lett. Azok is akik otthon esetleg nem rendelkeznek internet eléréssel sokszor a munkahelyükön hozzáférhetnek. Rengeteg médiumban elmondták már és folyamatosan elmondják, hogy amellet, hogy milyen előnyei vannak, lehetnek az internet használatának, 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 tekinthetőek. Tipikusan ilyenek (megbízhatóak) a bankok honlapjai illetve egyéb ismert internetes vásárlói oldalak. Azonban mindenképen felhívni a figyelmet az ún. adathalász⁵ támadásokra, amelyek során a gyanútlan felhasználóktól kicsalják a személyes adataikat és azokkal különböző csalásokat követnek el.

Információbiztonsági szempontból rendkívül veszélyesek az ún. közösségi oldalak, amennyiben a felhasználó nem a megfelelő módon és nem a megfelelő gondossággal használja azokat. Miről is van szó? A közösségi oldalak célja, hogy barátokat, ismerősöket hozzon össze az interneten keresztül. Ezek az oldalakon mód van arra, hogy minden felhasználó aki regisztrálta magát, különböző személyes információkat adjon meg magáról, az e-mail címetől kezdve, lakcímet, telefonszámokat, fényképeket, munkahelyeket, hobbit, stb. És pontosan ebben rejlik ezeknek az oldalaknak az információbiztonsági kockázata. Megfigyelhető, hogy sok felhasználó egy részt túl sok személyes információt oszt meg másokkal, másrészt pedig olyan információkat is megad, amelyeket nem kellene. Ilyen adat pl. a munkahelyi e-mail cím, vagy az, hogy valakinek mi a pontos beosztása egy adott munkahelyen, vagy, hogy pontosan mivel is foglalkozik. Szeretnénk felhívni a figyelmet, hogy nem csak tisztességes szándékú felhasználók regisztrálhatnak ezekre a közösségi oldalakra, a közösségi oldalon önként közzé tett információkkal könnyen vissza lehet élni.

Példa

Amennyiben valaki állást keres és elküldi valahova az önéletrajzát, legyen tisztában vele, hogy a HR osztály munkatársa nagy valószínűséggel meg fogja nézni a jelentkezőt egy vagy több közösségi oldalon, hogy valóban az-e, mint akinek leírja magát az önéletrajzban. Amennyiben megtalálja a jelentkezőt és véletlenül még közös ismerőst is talál, a pályázó

⁵ Akit bővebben érdekel a téma, az keressen rá az interneten az „adathalászat” vagy „phising” kifejezésekre

biztos lehet benne, hogy a HR-es munkatárs a közös ismerőstől megpróbál majd érdeklődni a pályázó iránt.

Másik esetben a felhasználó valamilyen szempontból (gazdasági, pénzügyi, döntéshozatali, stb.) kulcspozícióban van egy vállalatnál és a közösségi oldalon fel is tünteti a munkaadója nevét illetve a vállalatnál betöltött pozícióját, már is lehetőséget teremt arra, hogy tisztességtelen szándékú személyek az információkkal visszaéljenek. Akinek például munkaköréből eredően hiteket kell elbírálnia, kerülhet olyan helyzetbe, hogy az új barátai nem véletlenül ismerkedtem meg vele, hanem azzal a céllal, hogy a jövőben könnyebben tudjanak hitelügyleteket intézni.

Dokumentumok kezelése

Az asszisztenseknek, titkárnőknek a kezükbe kerülő dokumentumokkal is rendkívül körültekintően kell bánniuk. Az esetek túlnyomó részében napi munkavégzés során bizalmas dokumentumokkal dolgoznak, ezért ügyelni kell arra, hogy a bizalmas üzleti dokumentumok ne kerülhessenek illetéktelen kezekbe. Alapvetően érdemes oda figyelni arra, hogy a dokumentumok ne szanaszét heverjenek az íróasztalon, hanem rendezette 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 (pl. legalább fél napos távollét) illetve munkaidő végén, a bizalmas jellegű üzleti dokumentációkat minden esetben célszerű elzárni. Ne feledjük, hogy a takarító személyzetre sem tartoznak a cég belső ügyei! Nagyobb vállalatoknál létezik ún. Tiszta asztal szabályzat (Clean Desk Policy), amely többek között szabályozza és egyben segítséget is nyújt (gyakorlati tanácsokkal) abban, hogy az adott munkahelyen hogyan és mi módon kell a napi munkavégzés során a dokumentumokat kezelni⁶.

Példa

Figyelni kell arra, hogy soha ne hagyjanak elől az asztalon olyan dokumentumokat, amelyek illetéktelen pillantásoknak lehetnek kitéve. Ilyen helyzet, amikor a vezetőhöz megbeszélésre érkező munkatársak az asszisztens szobájában várakoznak. Előfordulhat, hogy az asszisztensnek el kell hagynia a szobát és a várakozó munkatárs egyedül marad. Nem lenne célszerű, ha az asszisztens asztalán – még az előtt, hogy a munkahelyi vezetővel beszélt volna – meglátná a felmondó levelét, pusztán” az asszisztens hanyagsága miatt.

Telefon, 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 lebecsülni információbiztonsági szempontból 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 személyesen ismerjük és természetesen felismerjük a hangját. Ugyanakkor könnyebb belátható, hogy az üzleti életben nem ismerhetünk mindenkit személyesen. Ezért fontos hangsúlyozni, hogy a munkatársak legyenek tisztában azzal, hogy telefonon keresztül kinek, milyen információt szabad kiadni. Egy

⁶ Az iratkezelési vagy dokumentumkezelési szabályzat sokkal generálisabb szabályokat, eljárásokat tartalmaz

asszisztensnek vagy titkárnőnek nagyon gyakran az is a munkaköri kötelességei közé tartozik, hogy főnökéhez érkező hívásokat fogadja, kezelje és megszűrje. Ugyanakkor folyamatosan több szempontot kell szem előtt tartania, elsősorban a főnöke utasítását másrészt az üzleti érdekeket. Képesnek kell lenni arra, hogy az esetlegesen toladó vagy akár zaklató jellegű hívásokat megfelelő határozottsággal és kellő diplomáciai érzéssel kezelje. Ki kell dolgozni azokat a megoldásokat, amelyek segítségével nagy biztonsággal megtudja határozni a hívó személyét. Erre különböző módszerek léteznek. Mindenképpen legyen gyanús ha valamilyen oknál fogva nem tudjuk a hívó fél kérdését azonnal megválaszolni és felajánljuk, hogy visszahívjuk de ettől mereven elzárkózik és nem hajlandó megadni az elérhetőségét. Szintén kezeljük fenntartással azokat a telefonálókat, akik nem mutatkoznak be. Egyrészt udvariatlanság, másrészt viszont, lehet, hogy szándékosan nem mutatkozik be az illető, mivel nem szeretné felfedni saját magát valamilyen tisztességtelen oknál fogva. Szintén óvatosan kell bánni a telefonon keresztül „közvélemény kutatásokkal”, mert igazából soha nem lehetünk biztosak abban, hogy ki van a vonal másik végén. Hiába mondja azt, hogy X, Y, cég megbízásából telefonál, ezt mi nem tudjuk hitelt érdemlően ellenőrizni. Ugyanakkor sokszor olyan információkat kér az adott (hívott) cégtől, amelyek akár üzleti titoknak is minősülhetnek. Itt szeretném megjegyezni, hogy nagyon figyeljünk oda, hogy milyen információt adunk ki telefonon keresztül a főnökünkről, a cégről vagy más munkatársunkról. Tipikusan a mobiltelefonszám az amit nagyon gyakran kiadnak az elővigyázatlan munkatársak telefonon keresztül. Gondoljunk csak bele, senki nem szeretné ha mobiltelefonján (akár magán akár céges) folyamatosan zaklatnák különböző felmérésekkel, reklámokkal, közvélemény kutatásokkal. Mindenkinek joga van eldönteni, hogy mikor és kinek adja meg saját telefonszámát (és természetesen egyéb személyes adatát). Szintén ilyen gyakori, amikor a hívó téves kapcsolást imitál a telefonba és erre való hivatkozással próbálja megszerezni valamelyik kolléga nevét és elérhetőségét, valahogy így:

Hívó: Jó napot kívánok!
Kovács urat keresem a stratégiai beszerzésről...

Hívott: Jó napot kívánok!
Azt hiszem ez téves, mi a marketing osztály vagyunk...

Hívó: Esetleg meg tudná adni Kovács úr elérhetőségét a stratégiai beszerzésen?

Hívott: Pillanat!
Nincs Kovács, esetleg Kardos?

Hívó: Iiigen, lehet...

Hívott: Megadná akkor Kardos úr elérhetőségét?

Hívott: Természetesen, mondhatom?

belső munkatárs adatainak megszerzése

Érdeemes megfigyelni, hogy a hívó nem mutatkozott be, vélhetően tudta, hogy rossz számot tárcsázott és a Hívott félnek egy pillanatig sem volt semmilyen kétsége afelől, hogy a hívó jogosan próbál meg információt szerezni. Pedig lehet, hogy a hívott felet átejttették...

A fenti példából is látszik, hogy mennyire egyszerűen meglehet szerezni információkat, pusztán a határozott fellépés és az emberi jóhiszeműség kihasználásával.⁷

Social Engineering

A fenti kifejezést nehéz megfelelően magyarra fordítani. A Social Engineering egy elkövetési mód, ahol a tisztességtelen szándékú személy, különböző fortélyokkal, ravasz trükkökkel próbál meg számára fontos információkat megszerezni az áldozatától.

⁷ Bővebben a Social Engineering fejezetben

Amennyiben pontosabban szeretnénk meghatározni, hogy mit is jelent a kifejezés, akkor azt mondhatjuk, hogy a Social Engineering: emberi hiszékenységen és jóindulaton alapuló emberi kapcsolatokat felhasználó csalási forma.

Gyakorlatilag nagyon széles a paletta és az az eszköztár amit az elkövetők bevetnek egy-egy információ megszerzésének érdekében. Az előző fejezetben (Telefon, telefonos kapcsolattartás) leírt módszerek a leggyakoribb Social Engineering módszernek tekinthetők. Itt – lévén szó telefonról – a támadó igazából nem kerül személyes kapcsolatba az áldozattal és még ha nem is éri el a célját, később újra próbálkozhat minimális kockázattal egy újabb kollégánál, hiszen a támadó személyét ne lehet azonosítani, mert senki sem látta. Hang alapján pedig nagyon kevés ember képes idegeneket megkülönböztetni, ráadásul olyat, akinek csak egyszer hallotta a hangját.

Nagyon gyakori eset – telefonos információszerzés esetén -, hogy a hívó fél valamilyen befolyásos barátira, ismerősre vagy - már korábban megszerzett információ alapján – a hívott közvetlen főnökére való hivatkozással kér bizonyos információkat. Szintén itt említenénk meg azt az esetet, amikor a hívó a vállalat informatikusának adja ki magát és különböző okokra hivatkozva kéri a felhasználót (hívott fél), hogy adja meg a felhasználói jelszavát vagy esetleg magyarázza el, hogy egy speciális alkalmazást (pl. könyvelő rendszert, készlet nyilvántartó rendszert stb.) hogyan is kell használni. Szeretném felhívni a figyelmet, hogy szigorúan tilos bárkinek kiadni, elmondani a különböző informatikai rendszerekhez kapott vagy általunk létre hozott jelszavakat akár szóban, akár telefonon kéri! Ebbe bele tartozik a munkahelyi vezető is, neki sem szabad elmondani, valószínűleg fordítva nem is működne a dolog, egyik munkahelyi vezető sem osztaná meg a jelszavát a beosztottjaival.

Social Engineering körébe tartozik az általunk csak „ajtó trükk”-nek nevezett dolog. Napjainkban szintén jellemző, hogy a legtöbb szervezetnél, vállalatnál valamilyen beléptető rendszert alkalmaznak ezzel próbálván megakadályozni illetéktelenek bejutását, illetve ilyen rendszerekkel szabályozzák a munkavállalók mozgását is épületen, gyártelepen belül. Általában valamilyen azonosításra is szolgáló (lehet rajta fénykép, a cég neve, színkódok, számkódok, stb.) műanyag kártya (proxy) kerül alkalmazásra. Gyakorlatilag úgy működik, hogy az ember a leolvasó elé tartja a kártyát és amennyiben jogosult az adott területre bejutni, akkor az elektromos zár kinyitja az ajtót, és az illető beléphet a területre. Igen ám, de nagyon sok helyen a munkavállalók egy-egy belépés esetén megtartják az ajtót azért, hogy a többi kollégának ne kelljen a kártyával „bajlódni”. Ezzel lehetővé teszik, hogy gyakorlatilag bárki ellenőrzés nélkül beléphessen. Vannak olyan nagyvállalatok ahol a munkatársak nem is ismerik egymást, hisz olyan sokan vannak. Szintén az ellenőrzés kijátszására alkalmas az „ajtó trükk”. Ezzel a helyzettel is mindenki találkozott más, sőt valószínűleg részese is volt. Két irányból lehet megközelíteni. Az egyik leggyakoribb, mikor valaki kifelé jön a védett területről és látja, hogy valaki beszeretne jutni. Ilyenkor egyszerűen az történik, hogy a kifelé igyekvő munkatárs kinyitja az ajtót és kilép, és az aki be szeretne jutni – anélkül, hogy a kártyáját használná – becsukódás előtt egyszerűen megfogja az ajtót és belép a védett területre. Ilyen egyszerű! A tapasztalat azt mutatja, hogy senki nem fogja megkérdezni az illetőt, hogy kit keres, hova is akar menni. Ennek az ajtó trükknek a másik változata, amikor a kártyával rendelkező munkavállaló a kártya használatával belép a védett területre és mi előtt becsukódna az ajtó a csaló elkapja az ajtót és kártya nélkül az munkatárs után szintén belép a területre. Amennyiben valamelyik munkatárs rákérdez egy ilyen esetben az illetőre, hogy ki is ő és mit keres, az adott területen akkor a csaló kellően határozott fellépéssel elhitheti a munkavállalókkal, hogy jogosan tartózkodik a területen, például azzal, hogy új munkatárs

csak még nem kapta meg a kártyáját, vagy, hogy másik területen dolgozik és az irodájában hagyta. A legtöbben elfogadják a választ és mennek a dolgukra, pedig tudhatnák, hogy az adott szervezetnél minden munkatársnak kell rendelkeznie azonosító kártyával, mert anélkül sehova nem tudna belépni és/vagy kilépni az épületben.

Példa

Csaló: Szia, Karesz vagyok az informatikáról!
Felhasználó: Szia, Adél vagyok!
Valami gond van a rendszerrel?
Csaló: Igazából nem, csak a biztonság kedvéért hívlak. Te milyen op. rendszert használasz?
Felhasználó: Mit?! Nekem nincs op. rendszerem, csak szövegszerkesztőm, prezentációs programom, egy táblázatkezelőm meg a levelezés.
Csaló: Neked is van op. rendszered. Operációs rendszer, ez indul el amikor bekapcsolod a számítógépet és ezen fut a többi programod, érted?
Felhasználó: Tényleg?! Na, most már ezt is tudom. De miben segíthetek?
Csaló: Amikor bekapcsolod a géped, akkor az op. rendszered elindul anélkül, hogy bármit be kellene gépelned?
Felhasználó: Igen.
Illetve, nem bocsí, felugrik egy kis ablak és oda be kell írnom, hogy PÉNZUGY15.
Csaló: Hmm. Tényleg? Azt, hogy PÉNZUGY15?
Felhasználó: Aha. Ez valami baj?
Csaló: Nem, nem asszem, ez ok. Mi is a vezetékneved?
Felhasználó: Naiv.
Csaló: Értem. Tehát Naiv Adél és azt kell beírnod, hogy PÉNZUGY15.
Felhasználó: Igen. Minden rendben van, tudok dolgozni?
Csaló: Igen, ellenőriztem, minden ok, köszi a segítséget!
És ne feledd, neked is van op. rendszered!
Felhasználó: Kösz! Szia!

felhasználói jelszó kicsalása

3 Zárszó

Ezzel az írással nem az volt a célunk, hogy bárkire ráijesszünk és nem szeretnénk senkit fölöslegesen ijesztgetni. Elsősorban azt szeretttük volna elérni, hogy rávilágítsunk az információbiztonság széleskörűségére, arra, hogy mennyire összetett dolog egy gazdálkodó szervezet üzleti titkait, belső, bizalmas információt megvédeni. Szerettük volna érzékeltetni, hogy az információbiztonság során, mennyi apró dologra kell odafigyelni. Reméljük, hogy a példákkal, amelyeket leírtunk sikerült bemutatni egy-két olyan élethelyzetet, amelyet időben sikerül felismerni és kivédeni, ha Önök közül bárki hasonló szituációba keveredne. Napjainkban annyira kifinomultak az információszerzési technikák, hogy megfelelő védelmet komplex megoldásokkal lehet elérni azzal, hogy a vállalat minden munkatársa tudatában van a lehetséges veszélyeknek és minden tőle telhető erőfeszítést megtesz a szervezet információs vagyonának megőrzéséért.