Mi az információbiztonság? 1. RÉSZ

Jelen cikkünkben egy olyan témával foglakozunk, amelyet mindenki ismer, munkája során nap, mint nap találkozik vele, de nehezen tudja egy szóval kifejezni. Ez a szó pedig az információbiztonság.

Kiss Péter

Információbiztonsági szakértő, tanácsadó. Rendszeresen tart szervezett képzéseket nagyvállalati környezetben, információbiztonsági témában. Független szakértőként nemzetközi és hazai nagyvállalatoknál segít az információbiztonsági rendszerek kialakításában, felülvizsgálatában. Több mint öt éves gyakorlati szakmai tapasztalattal rendelkezik az ISO27001-es szabvány bevezetésére való felkészítésben, rendelkezik információbiztonsági auditori képesítéssel, ISACA tag. Szakmai tapasztalatát többek között az Állami Nyomda Nyrt.-nél, banki, biztonsági szektorban szerezte. Folyamatosan részt vesz nemzetközi projektekben.

Jelen van a napi munkavégzés során, hiszen egy cég információit, adatait meg kell tudni védeni a jogosulatlan és/vagy illetéktelen megismeréstől. Tetten érhető a magánéletünkben is, hiszen nem kürtöljük világgá, hogy a kosztpénzt hol tartjuk a lakásban, hogy milyen riasztórendszert használunk, vagy, hogy a páncélszekrény pontosan hol is található. Az információbiztonságnak eleget kell tennie a sértetlenség, a bizalmasság és a rendelkezésre állás hármas feltételrendszerének.

Miért fontos?

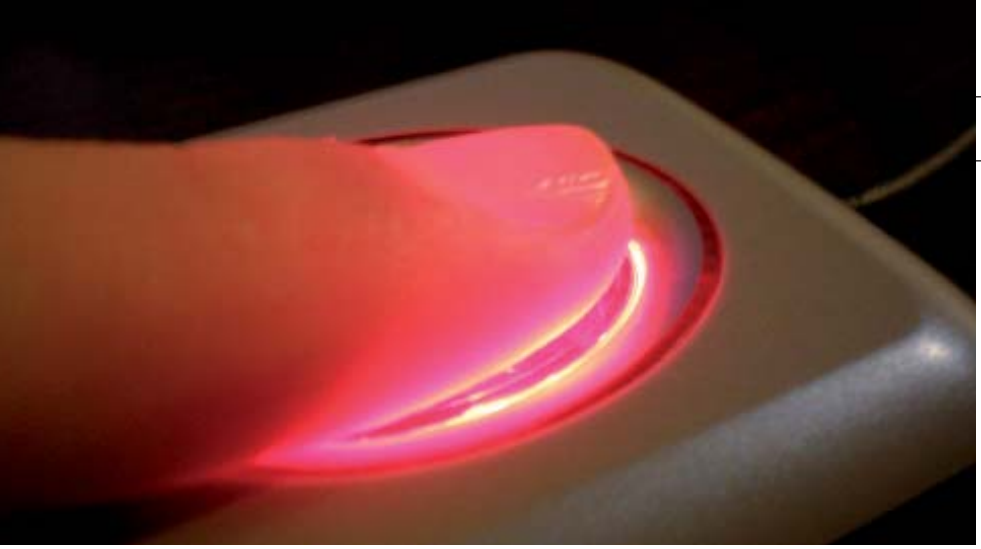
A mai információs társadalomban az információ az egyik legnagyobb érték. Gondoljunk csak bele, aki megfelelő információval rendelkezik például egy nagy ingatlanberuházás előtt, az a beruházás tervezett helyén kellő időben megvásárolt földterület segítségével nagyon rövid idő alatt nagyon sok pénzt tud keresni. Szintén ilyen kategória, ha idő előtt kiderül, hogy az egyik cég a jövőben fel kívánja vásárolni a versenytársát, akkor a megvásárolni kívánt cég részvényárfolyamai emelkedni fognak, és itt úgyszintén (a bennfentes kereskedelem felhasználásával, amelyet egyébként a törvény büntet) az illegálisan megszerzett és felhasznált információ segítségével óriási profitra lehet szert tenni. De ne menjünk ilyen messzire, a kisebb cégek esetében sokkal hangsúlyosabb szerepet kap az üzleti titkaik, belső információik megvédése, mivel ezek a kis méretnél fogva (mind pénzügyileg, mind személyi állományt tekintve) sokkal nehezebben képesek túlélni egy-egy bizalmas információ kiszivárgását.

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

Az információk megjelenési formája

- Dokumentumok, írásos információk (szerződések, ajánlatok, tervek, szakvélemények stb.).
- A szóban közölt információk (beszélgetés a folyosón, büfében, étteremben stb.).
- Az elektronikusan kezelt, továbbított, tárolt információk (telefonok, faxok, mobiltelefonok, különböző adathordozók, memóriakártyák, SIM kártyák, pendrive-ok stb.).
- Az informatikai (IT) rendszerekben kezelt, tárolt és feldolgozott információk (például e-mailek, táblázatok, dokumentumok, adatbázisok).

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, 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.



Az információbiztonság gyenge láncszemei

„Fecsegés”

Rengeteg olyan élethelyzet van a napi munkavégzés során, amikor birtokunkban lévő 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.

Informatikai eszközök

Érdekes kérdés információbiztonsági szempontból az informatikai eszközök, rendszerek használata. Az informatikai alkalmazásokkal kapcsolatban rengeteg biztonsági szabályra kell odafigyelni, a teljesség igénye nélkül az alábbiakban néhányat megemlítünk:

- Jelszavak

  Sokan hajlamosak azt hinni, hogy a jelszavaknak semmi jelentősége nincs. Ez nem így van, ugyanis a felhasználói jelszavakhoz jogosultság és felelősség is társul. A jelszavak lényege pontosan az, hogy egy-egy adott rendszerhez, amely jelszót kér (vagy egyéb azonosító módszert használ, például biometrikus azonosítót) 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. Mindig egyedi jelszavakat használjunk, illetve ha egy új beállítás miatt a rendszergazda ad a felhasználó számára jelszót, azt a felhasználónak haladéktalanul meg kell változtatnia. Ügyeljünk arra, hogy a jelszó legalább nyolc karakter hosszú legyen, amely tartalmaz kisbetűt, nagybetűt, számot és legalább egy speciális karaktert, például &; @; +; -; !; $. Szintén a jelszavak biztonságát növeli, ha rendszeres időközönként (30–60–90 naponta) megváltoztatjuk. Természetesen minél gyakrabban tesszük ezt, annál biztonságosabbnak tekinthető az aktuális jelszavunk. Ma már nagyon sok vállalatnál kötelezően beállításra került az informatikai rendszerben a jelszavak időnkénti rendszeres cseréje. Nagyon fontos, hogy a jelszavunkat soha senkinek ne áruljuk el, ne írjuk fel, mindig tartsuk fejben. Soha ne adjuk meg senkinek a jelszavainkat, akkor se, ha szabadságra megyünk, és szeretnénk, hogy az e-mailjeinkhez hozzáférjenek a munkatársaink.

- Képernyővédő használata

  A másik kritikus terület a képernyővédő használata jelszóval védve, más néven a számítógép zárolása. Ezt a biztonsági eljárást akkor alkalmazzuk, ha valamilyen oknál fogva elhagyjuk a helyiséget (ebéd, megbeszélés, dohányzás, mosdó 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 (például két perc nem használat után), akkor se várjuk ezt meg, hanem mi magunk aktiváljuk, hogy ne adjunk lehetőséget a jogosulatlan adathozzáféréshez.