Az információbiztonság nemcsak informatikai biztonság

Az információvédelem és a BS7799

Az információbiztonság területén napjainkban egy szervezet számos kihívással szembesül. Az információtechnológia töretlen fejlődésével párhuzamosan az információkat, az adatvagyont fenyegető veszélyforrások köre is egyre bővül. Ha egy szervezet sikerrel akar megfelelni ezeknek a kihívásoknak – márpedig ez alapvető érdeke –, akkor tudatos tervezésre és átgondolt működésre van szüksége. Annak érdekében pedig, hogy az információk védelme biztosítható legyen, számos tényező vizsgálata és kezelése szükséges, amelyek azonosítása nem egyszerű feladat. Hogyan lehet mégis kiutat találni ebből a labirintusból? Melyek a hatékony, korszerű információvédelmi rendszer kialakításának sarokkövei, és milyen módon támogatja a rendszer kialakítását a BS7799 szabvány? Cikkünkben ezekre a kérdésekre próbálunk választ adni.

HORVÁTH LÁSZLÓ, AZ AAM VEZETŐ TANÁCSADÓJA

Az információ szerepe a szervezetek életében

Az információ a szervezetek számára a legfőbb erőforrások egyike, a megfelelő és megbízható működés alapja. Kiemelt erőforrásként még nagyobb hangsúlyt kap a gazdálkodó szervezetek életében, ezért minden esetben gondoskodni kell megbízhatóságáról és biztonságáról, hiszen ez alapvetően befolyásolhatja egy szervezet működését, szolgáltatásainak, termékeinek minőségét.

A szervezetek információbiztonsága számos fenyegetésnek van kitéve, elég, ha csak a számítógépes csalásokra, vírustámadásokra, természeti csapásokra, az információfeldolgozó rendszer meghibásodásaira, a hackertámadásokra vagy akár a belső visszaélésekre gondolunk. Annak érdekében, hogy az információk megfelelően védettek legyenek, az alábbiakat kell biztosítani:

1. bizalmasság – vagyis az információ csak az arra felhatalmazottak számára legyen elérhető;

2. sértetlenség – az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése;

3. rendelkezésre állás – annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek az információkhoz, amikor szükséges.

Fontos kiemelni, hogy a fentiek biztosítása nemcsak az informatikai rendszerekben tárolt információk esetében szükséges, hanem az információ összes – az adott szervezet esetében értelmezett – megjelenési formájánál, így például a kinyomtatott dokumentumok, a kézi jegyzetek, a mikrofilmek, a video- és hanganyagok esetében is.

Az információvédelem megvalósítása

Hogyan védekezhetünk az információinkat, adatvagyonunkat fenyegető veszélyforrások ellen? A válasz egyszerűen hangzik: információvédelmi irányítási rendszer kialakításával.

Természetesen felmerül a kérdés, hogy ha egy szervezet

A szerző az AAM Vezetői Informatikai Tanácsadó Rt. vezető tanácsadója, aki amellett, hogy az elmúlt 7 évben részt vett számos, az AAM közreműködésével végzett, informatikai biztonságot érintő projekt munkájában (információbiztonsági szakértőként és/vagy projektvezetőként), egyben az AAM kockázatkezelési üzletágának vezetője. Aktív részese volt a vállalatnál nemrégiben lezajlott BS7799 információvédelmi rendszer kialakításának, valamint a cég információbiztonsági felelőseként részt vesz annak jelenlegi működtetésében is.

rendelkezik a legújabb szoftverekkel, tűzfalakkal, vírusirtókkal és az informatikai infrastruktúrát megfelelően működtető szakembergárdával, akkor ez miért nem elegendő. Nos, mert ez a megoldás önmagában számos gyenge ponttal rendelkezik. Nem védhető ki például a nyomtatott dokumentumokkal történő visszaélés vagy a felelőtlen felhasználói magatartás (pl. jelszavak megosztása, monitorra ragasztott cetliken való tárolása). Gondos tervezés és kiválasztás nélkül semmi garancia sincs arra, hogy a legújabb és legdrágább technológia valóban képes lesz megfelelni az adott szervezet igényeinek. Mindezek tükrében megállapíthatjuk, hogy az információ megfelelő védelmét biztosító megoldás csak a technológiai síktól elvonatkoztatott, komplexebb szemléletmóddal alakítható ki.

A tapasztalatok szerint ma az információs rendszerek (informatikai eszközökkel megvalósított rendszerek, amelyek információkat tárolnak és/vagy kezelnek) jelentős része biztonsági szempontból nincs megfelelően megtervezve. Mivel a biztonság megteremtése technikai eszközökkel csak korlátozott módon valósítható meg, a technológiai háttér tudatos kialakítása nem az egyetlen feladat. Emellett meg kell alkotni az irányítási funkciókat, szabályzatokat és a kapcsolódó eljárásokat, valamint gondoskodni kell a rendszer működtetéséről és felülvizsgálatáról is.

Az információvédelmi rendszer kialakítása gondos és részletekre is kiterjedő tervezést igényel. A leggyengébb láncszem elvét (minden lánc olyan erős, mint a leggyengébb láncszeme) figyelembe véve a rendszert úgy kell kialakítani, hogy minden területen egyenszilárdságú védelmet biztosítson. Például hiába a jól kialakított jogosultsági rendszer, ha egy felügyelet nélküli nyomtatónál bárki hozzáférhet a kinyomtatott bizalmas dokumentumokhoz. A kialakított rendszernek ugyanakkor vonatkoznia kell a szervezet minden alkalmazottjára, de lehetőség szerint a szállítókra, alvállalkozókra és egyes esetekben még a vevőkre is.

A gondos tervezés amellett, hogy biztosítja a rendszer teljességét, lehetővé teszi a költséghatékonysági szempontok érvényesítését is. Ha ugyanis a védelmi intézkedések még a követelménymeghatározás és a tervezés fázisában integrálódnak a rendszerbe, és nem a már működő környezetbe kell azokat beépíteni, akkor a költségek lényegesen alacsonyabbak lehetnek.

Az információvédelmi rendszer kialakításának fő lépései mindezek alapján a következők:

1. védelmi követelmények meghatározása;

2. biztonsági kockázatok felmérése, elemzése;

3. információbiztonsági kiindulási helyzet (azonosított kockázatok és lehetőségek) értékelése, rögzítése;

4. célok kitűzése;

5. megvalósítási eszközök, felelősségek, feladatok meghatározása, szabályozás kialakítása;

6. folyamatos működtetés, monitoring, továbbfejlesztés.

A teljes körű információvédelmi irányítási rendszer kialakításához kiváló alapot teremt a BS7799-es szabvány. Az általa lefedett területeket áttekintve megállapítható, hogy egy adott szervezetnél nem minden esetben értelmezhetők a megfogalmazott követelmények. Ugyanakkor egy szervezetnél lehetnek a szabványban nem rögzített, de a megfelelő védelemhez szükséges szabályozandó területek is. A BS7799-et ennek megfelelően kell kezelni, és a rendszer tényleges elemeit az adott felhasználás, az adott szervezet követelményeinek és céljainak kell meghatározniuk.

Miben segít a BS7799?

Az elmúlt 100 évben a British Standards Institute (BSI) és az International Organization for Standardization (ISO) adta ki

az általános értékelést a működési, gyártási és teljesítményszabványokhoz. Az információ biztonságára vonatkozó szabvány azonban hosszú ideig nem volt fellelhető egyik szervezet palettáján sem. Végül 1995-ben a BSI megjelentette első biztonsági szabványát, a BS7799-et, amely elsősorban az elektronikus kereskedelem területén felmerülő, biztonsággal kapcsolatos kérdésekre volt hivatott választ adni. Sajnálatos módon a BS7799 első változatáról a gyakorlatban kiderült, hogy túl

merev, ráadásul a biztonsági kérdések nem sokakat izgattak akkoriban, így 1999 májusában a BSI kiadta a BS7799 második, alaposan átdolgozott változatát. A számos javítást és fejlesztést tartalmazó második kiadás, valamint az időközben nagyban megváltozott befogadó környezet (mindinkább előtérbe kerültek a biztonsági kérdések) következtében megkezdődött a BS7799 szerint kialakított információvédelmi irányítási rendszerek elterjedése, és ez a tendencia azóta is folytatódik. Ennek eredményeképpen a BS7799 meghatározó tényezővé vált az információvédelmi irányítási rendszerek területén (az amerikai Gartner elemzőcég kutatásai alapján a BS7799 várhatóan 2007-re de facto szabvánnyá válik az informatikai biztonság területén).

Mindjárt adódik a kérdés, hogy mely szervezetek számára lehet különösen fontos a BS7799 szerint tanúsított információvédelmi irányítási rendszer bevezetése. Azoknak, amelyek:

1. létét és szolgáltatásainak minőségét az üzleti információk pontossága határozza meg;

2. elektronikus (kereskedelmi, kommunikációs stb.) csatornákat használnak, illetve ilyen módon tartanak fenn kapcsolatot partnereikkel, vevőikkel;

3. más cégek vagy szervezetek adatainak feldolgozásával foglalkoznak (pl. bankok és vezetési tanácsadó cégek);

4. az információ továbbításának vagy feldolgozásának lehetőségét teremtik meg (pl. távközlési vagy az informatikai háttér kiépítésével foglalkozó vállalatok);

5. meg akarják őrizni a saját vagy az általuk tárolt információk titkosságát;

6. személyi információkkal dolgoznak;

7. az információbiztonsági kérdéseket szeretnék megnyugtatóan és ellenőrzötten kezelni.

Napjainkban elmondható, hogy szinte minden cég, szervezet rendelkezik valamilyen információvédelmi megoldással, de ezek meglehetősen vegyes képet mutatnak (az egyszerű vírusirtó alkalmazás használatától a komplex információvédelmi irányítási rendszer működtetéséig). A BS7799 szerinti tanúsítás megszerzéséhez ezek a megoldások kiváló alapot nyújthatnak, hiszen a szabvány az egyes követelmények teljesítése terén kellő rugalmasságot enged, így egy BS7799 szerint működő információvédelmi rendszerbe többnyire beilleszthetők. Ennek köszönhetően lehetőség van a korábbi működésmód megtartására vagy adott esetben akár a továbbfejlesztésére is.

Ahhoz, hogy az információvédelmi irányítási rendszer kialakítása sikeres legyen, általában a következő tényezők együttes teljesülése szükséges:

1. a vezetés elkötelezettsége és támogatása, ami biztosítja a megfelelő erőforrások rendelkezésre állását, illetve a változások szervezettel történő elfogadtatását;

2. az irányítási célok egyértelmű meghatározása – fontos, hogy a biztonságpolitika, a célok és a tevékenységek az üzleti és működési célokon alapuljanak;

3. a szervezeti kultúra megtartása, hiszen egy működő szervezet nehezen fogad be olyan megoldásokat, illetve változásokat, amelyek jelentősen eltérnek az eddigi működés során megszokottól;

4. a védeni kívánt erőforrások pontos azonosítása, az azokat fenyegető veszélyforrások és hatásaik meghatározása, valamint kockázatarányos védelmi megoldások kialakítása;

5. minden vezető és alkalmazott bevonása, hiszen a rendszer akkor működik jól, ha a szervezet minden pontján minden érintett ismeri és felelősen ellátja az irányítási rendszerben meghatározott feladatait;

6. a kialakítás során az érintettek folyamatos és részletes tájékoztatása;

7. tudatos bevezetés, az érintettek számára megfelelő képzés és oktatás szervezése, akár számonkéréssel egybekötve, valamint folyamatos frissítő oktatások, tájékoztató anyagok a rendszer működése során bekövetkező változásokról;

8. a rendszer tudatos, menedzselt és dokumentált működtetése, működésének folyamatos kontrollja (tesztelés, audit, visszacsatolás), a tapasztalatok alapján a továbbfejlesztési, módosítási lépések végrehajtása.

Az információvédelem irányítási rendszerének fő célja, hogy biztosítsa az üzleti és/vagy szolgáltatásbeli folytonosságot, valamint megelőzéssel vagy a kockázatok elfogadható szintre való mérséklésével csökkentse a biztonsági eseményekből és azok járulékos hatásaiból származó károkat.

Nagyon fontos hangsúlyozni, hogy a BS7799 az információ minden formájára vonatkozik, függetlenül attól, hogy az hol található, milyen formában kezelik, tárolják és továbbítják. Segítséget nyújt a cégeknek, szervezeteknek és ezeken belül az egyéneknek az információval összefüggő kockázatok szervezett rendszerben való kezelésére. Ugyancsak segíti az eseményekből való tanulást, hiszen a bekövetkezett események elemzésével azok jövőbeni bekövetkezési valószínűsége, illetve hatása csökkenthető. A rendszeres ellenőrzések, auditok fenntartják az éberséget, és növelik az érintettek biztonsági tudatosságának szintjét is.

Tanúsított (szabványos) információvédelem

A BS7799 szabvány alapján kialakított információvédelmi irányítási rendszer kellő védelmet nyújthat a szervezet számára. A nemzetközileg elismert szabvány követelményeinek való megfelelőséget igazolva az akkreditált tanúsító testület tanúsítványt ad ki, amely bizonyítja, hogy a szervezet információvédelmi irányítási rendszere megfelel a BS7799 szabvány követelményeinek.

A tanúsítás a következő konkrét előnyökkel jár a szervezet számára:

1. a BS7799 szerinti tanúsítással a szervezet – önmaga, a vezetése, jelenlegi és leendő partnerei, ügyfelei felé – bizonyítani tudja, hogy olyan, nemzetközileg elismert alapokon nyugvó rendszert vezetett be, amely hatékonyan véd az információvesztés, illetve annak következményei ellen;

2. javul a szervezet megítélése, elismertsége, növekszik irányában a bizalom mind partnerei, mind szállítói és megrendelői részéről;

3. a szervezet lépéselőnyhöz jut a BS7799 tanúsítvánnyal nem rendelkező versenytársaival szemben, ugyanis várható, hogy mind gyakrabban lesz pályázati, illetve szerződéskötési feltétel az információvédelmi irányítási rendszer megléte.

A tapasztalatok azt mutatják, hogy a megelőzés mindig kevesebbe kerül, mint a bekövetkezett kár következményeinek megszüntetése. A rendszer elterjedése így nemcsak a versenyhelyzetben tevékenykedő gazdasági szervezetek, hanem a közigazgatásban, az egészségügyben működők és sok más szervezet számára is kívánatos, hiszen számos haszonnal kecsegtet.

Saját tapasztalatok

A végére nem marad más, mint saját tapasztalataim megosztása. Abban a szerencsés helyzetben voltam, hogy részese lehettem az AAM Vezetői Informatikai Tanácsadó Rt. BS7799 szerinti információvédelmi irányítási rendszerének kialakításában, és a mai napig részt veszek a rendszer működtetésében. Mivel az AAM – mint a hazai piac egyik meghatározó tanácsadócége – elsősorban ügyfelei bizalmas anyagait, dokumentumait kezeli, a működés első percétől kezdve kiemelten fontos volt számunkra, hogy ezeket az adatokat, információkat bizalmasan kezeljük. Ennek érdekében az AAM megszerezte az ISO 9001, majd az ISO 9001:2000 tanúsítást, és 2004-ben döntött a BS7799 szerinti működésmód kialakításáról. A kialakítás során alapvetően az ISO-folyamatok kiegészítését kellett elvégeznünk, és a korábban íratlan szabályainkat dokumentálnunk. A folyamat végén az AAM sikeres tanúsító auditon esett át, így elmondhatjuk, hogy teljesítettük a feladatot.

A rendszer működtetése során azt tapasztaltuk, hogy a BS7799 követelményeinek érvényesítésével folyamataink jobban követhetők, amelyek korábban formálisan működtek, most szabályozottan, olajozottan és az érintettek dokumentált tájékoztatása mellett zajlanak. Könnyebbé vált az egyes információbiztonsági események kezelése és a tapasztalatok feldolgozása is. A tapasztalatokhoz hozzátartozik az is, hogy nem szabad elfelejteni: az információvédelmi megoldások alapvetően nem hatékonyságnövelő hatásúak, mivel gyakran rónak pluszterhet a munkatársakra, hogy megfeleljenek a rendszer által támasztott követelményeknek. Ugyanakkor ha szembeállítjuk ezt egy esetlegesen bekövetkező káreseménynyel, látni fogjuk, hogy még így is ez az ésszerű alternatíva.

Összességében elmondható, hogy bár az információbiztonság mindig is hangsúlyos terület volt az AAM életében (ezt igazolja, hogy ebből az okból jelentős kárt, információvesztést vagy sérülést soha nem szenvedtünk el), ez a terület csak a BS7799 segítségével teljesedhetett ki igazán.