



Veszélyben a céges információk

Egy nemzetközi kutatás feltárta a különböző országokra és kultúrákra jellemző viselkedési kockázatokat – a létesítményekbe, illetve hálózatokba történő jogosulatlan behatolástól a vállalati információk szándékos kiszivárogtatásáig.

A Cisco megbízásából készült nemzetközi kutatása feltárja a szervezetek számára egyik legkritikusabb biztonsági probléma, az adatvesztés gyökereit. A 10 ország több mint 2000 alkalmazottja és IT-szakembere körében végzett felmérés rámutat azokra a dolgozók által elkövetett leggyakoribb hibákra, amelyek adatszivárgáshoz vezetnek. Az amerikai InsightExpress piackutató cég által készített kutatás (www.cisco.com/go/dlp) arra is rávilágít, hogy az egyes viselkedési kockázatok országonként, illetve kultúránként eltérők. Ez lehetőséget teremt a vállalatok számára, hogy testre szabott kockázatkezelési tervet állítsanak össze, így a globális jelenségek figyelembevétele mellett helyi szinten készülhetnek a megelőzésre.

A felmérés célja az volt, hogy az adatvesztési és biztonsági problémákat a dinamikusan változó üzleti és társadalmi környezetben tárja fel. A munka, illetve a magánélet határai mindinkább összemosódnak, a vállalati működés és az alkalmazottak életstílusának változása nagyrészt az olyan együttműködő eszközök és alkalmazások elterjedésének tudható be, amelyeket egyaránt használnak a munkához, illetve személyes célokra. Ide tartoznak például a mobiltelefonok, laptopok, web 2.0-s alkalmazások, a videók és a közösségi média. Ez a folyton fejlődő vállalati környezet szolgált a felmérés háttéréül, amelyben 1000-1000, különböző iparágakban és eltérő méretű vállalatoknál dolgozó alkalmazottat, illetve IT-szakembert kérdeztek meg.

A felmérést 10 országban, az Egyesült Államokban, az Egyesült Királyságban, Fran-

ciaországban, Németországban, Olaszországban, Japánban, Kínában, Indiában, Ausztráliában és Brazíliában folytatták le. Ezek az országok azért kerültek be a felmérésbe, mert igen különböző társadalmi és üzleti kultúrát képviselnek, eltérően, illetve stabil gazdasággal rendelkeznek, továbbá az internetes kultúra más-más szintjén állnak.

A viselkedési kockázatokkal kapcsolatos eredmények közül íme a 10 legfigyelemre méltóbb megállapítás:

1. A biztonsági beállítások megváltoztatása a számítógépeken. Minden ötödik alkalmazott módosította munkaeszközein a biztonsági beállításokat, hogy az IT-előírások megkerülésével nem engedélyezett weboldalakhoz férhessen hozzá. Ez a jelenség olyan országokban volt gyakoribb, mint Kína és India. A megkérdezettek 52 százaléka válaszolta azt, hogy egyszerűen csak meg akarta nézni az adott webhelyet, a harmaduk szerint pedig csakis rájuk tartozik, hogy milyen oldalakat nézegetnek.

2. Nem engedélyezett alkalmazások használata. Tízből hét IT-szakember állította, hogy a vállalatnál bekövetkezett adatvesztéses problémák mintegy fele származott abból, hogy az alkalmazottak jogosulatlanul használtak valamilyen alkalmazást, vagy nem engedélyezett webhelyhez fértek hozzá. Példaként említették a közösségi médiát, a zeneletöltő szoftveket és az internetes vásárlóhelyeket. Ez a megállapítás főként az Egyesült Államokban (74%), valamint Indiában (79%) volt érvényes.

3. Jogosulatlan hálózati hozzáférés/behatolás létesítménybe. Az elmúlt évben ötből két IT-szakember szembesült olyan esettel, amikor alkalmazottak jogosulatlanul jutottak a hálózat vagy a létesítmény valamely részébe. Az ilyen esetek többnyire

re Kínában fordultak elő, ahol háromból két válaszadó számolt be hasonló problémáról. Azon válaszadók kétharmada, akik bármely országban ilyen problémával találkoztak, az esetek gyakoriságának a megnövekedését tapasztalta, 14 százalékuk pedig havonta felvetődő kérdésként értékelte.

4. Érzékeny vállalati információk megosztása. Minden negyedik alkalmazott ismerte el, hogy időnként érzékeny információkat oszt meg szóban cégen kívüli személyekkel, például barátokkal, családtagokkal vagy akár idegenekkel is. Ez jól mutatja, hogy a vállalati titkok sokszor nem is olyan titkosak. Magyaratzatként a legjellemzőbb válaszok közé az alábbi kijelentések tartoztak: „Muszáj volt valakinek eldicsekednem az ötlettel”, „Meg kellett osztanom valakivel a gondolataim” vagy „Nem éreztem benne semmi rosszat”.

5. Vállalati eszközök megosztása. A felmérés résztvevőinek közel a fele (44%) osztja meg felügyelet nélkül munkaeszközeit másokkal, akár cégen kívüli személyekkel. Ebből látszik, hogy az adatok gyakran kerülhetnek illetéktelen kezekbe.

6. A személyes és munkaeszközök, illetve a kommunikáció nem megfelelő szétválasztása. Az alkalmazottak majdnem kétharmada vallotta, hogy naponta használja munkahelyi számítógépét személyes célokra. Ilyen tevékenységnek számít többek között a zeneletöltés, az internetes vásárlás és banki ügyintézés, blogolás, chatelés és sok minden más. Az alkalmazottak fele személyes e-mail címéről levelezik az ügyfelekkel és munkatársakkal, holott csak 40 százalékuk rendelkezik az IT-részleg jóváhagyásával.

7. Felügyelet nélküli eszközök. Legalább az alkalmazottak kétharmada hagyja bejelelve, illetve védelem nélkül a számítógépeket.

tógépét akkor is, amikor távol van az íróasztalától. Ezek az alkalmazottak továbbá hajlamosak arra is, hogy laptopjukat éjjelre is az asztalukon hagyják anélkül, hogy kijelentkezzenek, ami alkalmat ad az esetleges tolvajlásokhoz és a vállalati vagy személyes adatok eltulajdonításához.

8. A bejelentkezési adatok és jelszavak tárolása. Minden ötödik alkalmazott a számítógépén tárolja a rendszerjelszavát, valamint a bejelentkezési adatait, vagy le is írják, majd a papírt az asztalukon, nyitott fiókokban, sőt akár a számítógépükre ragasztva hagyják. Néhány országban, például Kínában (28%), az alkalmazottak egy része a céges információk személyes pénzügyi adataival együtt tárolja a jelszót és a bejelentkezési adatokat a munkahelyi gépén, így nemcsak az azonosító adatait, de a pénzügyeit is kockáztatja. Az eszközök felügyelet nélkül hagyása pedig tovább növeli a kockázatot.

9. A hordozható eszközök elvesztése. Majdnem minden negyedik alkalmazott (22%) tárol vállalati adatokat hordozható készülékeken az irodán kívül is. Ez Kínában különösen gyakori, mintegy 41%, és az eszközök elvesztése vagy eltulajdonítása esetén jelentős kockázatot képvisel.

10. „Követés” és felügyelet nélküli jelenlét. A német alkalmazottak több mint egyötöde hagyja, hogy cégen kívüli személyek felügyelet nélkül közlekedjenek az irodákban. A jelenség átlagosan 13 százalékban fordul elő a tanulmány szerint. Továbbá 18 százalékuk hagyta, hogy ismeretlen személyek a nyomukban bejussanak a vállalati létesítménybe.

„A modern kori biztonsági technológiák, előírások, valamint tudatosság és képzés nélkül az információ igen sérülékeny – fejtegette ki John N. Stewart, a Cisco adatbiztonságért felelős vezetője. – Ma már az adatok mindenhol jelen vannak, állandó mozgásban, folyamatos használatban, programok között, mindenféle eszközökön tárolva, de a hagyományos üzleti környezetben túl akár otthon, útközben, kávézókban, repülőgépeken vagy vonatokon is. A hatékony adatvédelemhez elsőként az adott üzletmenet sajátos kockázatait kell felismerni. Csak erre lehet alapozni a megfelelő technológiákat, előírásokat, valamint a képzési és oktatási terveket.”

Stewart szerint a cégek a viselkedési min-

ták révén regionális szinten alakíthatják ki az alkalmazottak képzési programjait, valamint a vállalat globális kockázatkezelési terveit. A biztonsági vezető felsorolta az adatvesztés megelőzésének hatásos eljárásait is:

- ▶ Ismerje az adatait, és kezelje azokat megfelelően: Legyen tisztában azzal, hogy hol és hogyan vannak tárolva az adatai, miként lehet ezekhez hozzáférni és hogyan használhatók.
- ▶ A sajátjaként vigyázzon az adatokra – óvja úgy, mint a személyes pénzügyeit, képezze az alkalmazottakat, vonjon párhuzamot a pénz megkeresése és elvesztése, valamint az adatvédelem között.
- ▶ Vezessen be intézményesített normákat a biztonsági eljárások terén: Határo-

zon meg átfogó célkitűzéseket, és állítson össze az adott ország kultúrájához és sajátos kockázataihoz szabott képzési programot.

- ▶ Alakítson ki bizalmon alapuló kultúrát. Az alkalmazottaknak biztonságban kell érezniük magukat az esetleges problémák jelentéséhez, ami által az IT-szakemberek gyorsabban tudnak intézkedni!
- ▶ A biztonsági kockázatokat tudatosítani kell, az alkalmazottak képzése és oktatása alapvető: Gondolkozzon globálisan, de cselekedjen lokálisan. A képzéseket az adott kultúra, illetve biztonsági környezet sajátosságaihoz mérten kell megvalósítani.

Sajtó alá rendezte: Szalay Dániel