HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

IT BIZTONSÁGI KOCKÁZATOK ÉS KOCKÁZATKEZELÉS

IT SECURITY RISKS AND RISK MANAGEMENT

JAKUS Attila; TICK Andrea

(ORCID ID); (ORCID ID)

attila.jakus.92@gmail.com – Tick.Andrea@uni-bge.hu

Absztrakt

Az IT biztonság területe napjainkban egyre fontosabbá válik a vállalatok és a magánszemélyek életében is. Az informatikai vagyon, kiemelten az adatvagyon, a vállalatok számára meghatározó jelentőségű. Az informatika elválaszthatatlan a vállalati működéstől, a vállalat üzleti folyamataitól. Különösen igaz ez a pénzügyi és biztosítási területre, ahol a visszaélések jelentős károkat tudnak okozni. Az IT biztonsági kockázatok menedzsmentje kulcsszerepet tölt be ezen a területen, hiszen a biztosítókban dolgozó szakemberek, ügyintézők nem informatikusok, mégis sokféle IT biztonsági kockázattal találkozhatnak a munkájuk során. Kezelik az ügyfelek személyes és pénzügyi adatait, mindezt sokszor távoli eléréssel, mobiltelefon vagy saját notebook használatával. Ezért is kulcskérdés az informatikai vagyon védelmében az alkalmazottak biztonságtudatossága. A cikk megvizsgálja és elemzi, hogy milyen IT biztonsági kockázatok azonosíthatók a biztosítási területen, milyen eljárással lehet és érdemes értékelni ezeket a kockázatokat, milyen tipikus kockázatkezelési módszerek állnak rendelkezésre és adódik-e lehetőség a social engineering előfordulására, illetve csökkentésére.

Kulcsszavak: *IT biztonság, IT kockázat, adatvagyon, biztosítási piac*

Abstract

Nowadays for enterprises as well as for individuals IT security is concerned to be a more and more important field in the IT profession. The IT asset, especially the data asset is of dominant importance for the enterprises. Information Technology is inseparable from corporate operation, from the business processes of an enterprise. It is particularly true in the finance and insurance sectors, where IT abuses can cause serious damage to the IT asset even to the business. IT risk management has a key role in this field, since employees, assistants working for these enterprises are not IT experts, even so they might face several types IT security risks during their everyday work. They handle the clientele, their private and financial data, often in remote access using cellular phones or own notebooks. Therefore, it is cruial to increase employees' IT consciousness and awareness in favor of protecting the corporate IT asset. This paper examines and analyses what types of IT security risks can be identified in the field of insurance, how these risks can be evaluated and are worth of evaluating, what typical risk management methods are available and whether there is a chance of the emergence or rolling back of social engineering.

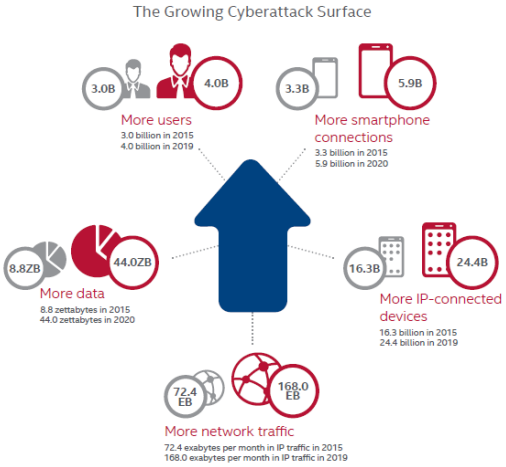
Keywords: *big data, social engineering, IT security, IT risks, IT asset, data asset, insurance market*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.20.

BEVEZETÉS

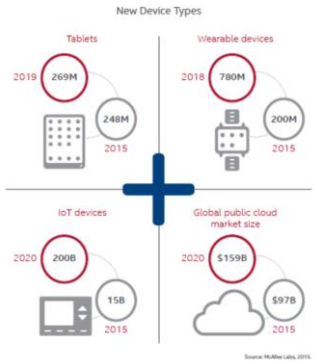
Az IT területén még az egyre nagyobb hangsúlyt élvező biztonságtudatosság fényében is, időről-időre történnek visszaélések. Az elektronikus támadási felület napról napra bővül (1. ábra), egyre több a felhasználó, és a felhasználók egyre többször és többféle módon veszik használatba az internet adta lehetőségeket. A több felhasználó, nagyobb mennyiségű adatot is jelent, növelve így a lehetséges visszaélések számát. A McAfee becslései szerint az adatmennyiség 2020-ra eléri a 44 zettabyte-ot (1. ábra), ami a jelenlegi elérhető adatmennyiségnek közel ötszöröse [1].

A McAfee felmérései alapján a felhasználók száma 2019-re eléri a négy milliárd főt, ami egy milliárdos növekedést jelent 2015-höz képest. Az előrejelzés szerint az IP alapú eszközök száma 2019-re 24,4 milliárd (a 2015-ös érték másfélszerese), míg a mobiltelefonok száma 2020-ra 5,9 milliárd (a 2015-ös értéknek majdnem kétszerese). A hálózati forgalom is jelentősen, több mint kétszeresére nő, 168 exabyte lesz 2019-ben [1].



1. ábra Növekvő kibertámadási lehetőségek [1]

A becslésben nem szabad azt a tényt figyelmen kívül hagyni, hogy egyre több embernek nem csak egy eszköze csatlakozik a hálózathoz, hanem általában legalább kettő, de előfordul három, négy esetleg még több is (2. ábra).



2. ábra A felhasználók és „okos” eszközeik [1]

A mai mobiltelefonok mindegyikéről elmondható, hogy „okosak” tehát támadási oldalról van, illetve lehet rajtuk értékes információ. Az otthoni számítógép, laptop mellett a tabletek is megjelennek ebben a felsorolásban. Ezen kívül használunk okosórákat, okos televíziókat, okos gépjárműveket, vagy például olyan okos segédeszközöket, mint a google szemüveg. Ezek az eszközök gyakran lehetőséget nyújtanak arra, hogy hálózaton keresztül

összehangoljuk őket, egyikről lássuk a másikat és fordítva. Ez a lehetőség, viszont nem csak nekünk jelenthet könnyebbséget, hanem azoknak is, akik valamilyen visszaélést szeretnének végrehajtani. Mivel minden eszköz másfajta védelemmel van felszerelve, és nincs két egyforma felhasználó, aki ugyanazokat az eszközöket ugyanolyan módon használja, rendkívül nagy kihívást jelent naprakésznek maradni az elkövetkező időszakban az IT biztonság területén. Az elektronikus világban, bármit teszünk, annak nyoma marad, a digitális lábnyomunkat otthagyjuk magunk után.

TÁMADÁSOK, FENYEGETETTSÉGEK

Az IT területén még az egyre nagyobb hangsúlyt élvező biztonságtudatosság fényében is, időről-időre történnek visszaélések. 2015 decemberében a MacKeeper (egy segédprogramokat öszegyűjtő program) belső szerveréről 13 millió felhasználói adatot töltöttek le, köztük e-maileket, jelszavakat, telefonszámokat, személyes adatokat. A Facebook (Központ, Kormányzati Eseménykezelő, 2013) hasonló hibát jelentett be, ők az információszivárgást a Facebook Download Your Information Tool-t használó felhasználók között észlelték. Ezzel az eszközzel a felhasználói fiók teljes tartalmát lehet letölteni. A hiba kijavításáig körülbelül hatmillió regisztrációhoz tartozó e-mail címet és telefonszámot lehetett megszerezni.

Az autókban megjelenő új fejlesztések a hozzáférés fenyegetettségének külön csoportját jelentik, amelyre érdemes nagy hangsúlyt fektetni a jövőben. Az elmúlt évben a Chrysler, General Motors, Toyota és a Ford is jelentett különböző mértékű sérülékenységeket. A Nissan elektromos autók feltörését egy mobilalkalmazáson keresztül tudták véghezvinni, tehát a biztonsággal kapcsolatos visszaélések kérdése nem kizárólag az online szolgáltatások terén fontos, hanem hétköznapjaink kulcseleme [1]. Az applikációban lévő rést megtalálva lehetőség nyílt arra, hogy az illetéktelenek különböző adatokat tulajdonítsanak el, például alvázszám, töltöttségi állapot, gps naplók; vagy éppen hozzáférjenek a gépjármű belső rendszeréhez, irányítva a klímaberendezést, elérhetetlenné téve különböző létfontosságú rendszereket. A probléma a Nissan Leaf és eNV200 típusú elektromos autó tulajdonosait érintette, közel kétszázezer embert.

A biztonsági visszaélésekkel kapcsolatos kockázatok felmérésére és ésszerű kezelésére érdemes időt fordítani, hiszen a károk mértékét néhány esetben még felbecsülni is nehéz lenne. Ezt végig gondolva jutott arra a döntésre a svéd adatvédelmi hatóság, hogy az ottani közszférából kitiltja a Google felhő alapú szolgáltatásait [2]. Szerintük a szolgáltatás túl sok lehetőséget ad a Google kezébe az adatok kezelésének kérdésében, ami aggályokat vetett fel több szempontból is, a vállalati adatok kezelésének területén. Ameddig a felhasználói szerződések ilyen szempontból hiányosak, addig a svéd állami szervek a Google naptár, e-mail és adatfeldolgozási funkciók nélkül dolgoznak.

A biztonságtudatosság növelése érdekében Berlinben a közelmúltban tesztelték a köztisztségviselőket. A berlini rendőrség dolgozói kaptak egy próba adathalász linket, amelyet a 466 alany közül 252, azaz az alkalmazottak több mint fele meg is nyitott. A teszt 35 résztvevője még az utasításokat is követte, megadva saját használatú jelszavukat, s így megnyílt az adathalász link [3].

A támadások, fenyegetettségek típusai

Az IT területén végrehajtható támadásoknak rengeteg típusa van, a határ kizárólag a csalók kreativitásán múlik. A számítógépes bűnözésben a támadás forrása és célpontja szerint négy típust különböztethetünk meg (1. táblázat) [4].

Számítógépes bűnözés		
Támadás forrása	**Támadás célpontja**	**Példa**
A bűncselekmény célja a számítógép támadása. Az elkövető egy másik gépet használ a támadás indítására.	Egy konkrét beazonosított számítógép.	DoS támadás (Denial of service) Hacker tevékenység
Az elkövető egy számítógépet használ arra, hogy visszaélést kövessen el egy másik számítógép ellen.	A célpont nem feltétlenül definiált. A támadás pontos cél nélküli.	Kiterjesztett DoS támadás Vírus
A visszaélés eszköze a számítógép. A gép a bűncselekmény végrehajtására használt, de a cél nem egy másik számítógép.	A főbb célpontok az adatok, vagy a számítógépen tárolt információk.	Csalás Jogtalan hozzáférés Phishing Keylogger telepítése
A számítógép a visszaélés szimbóluma. Az elkövető a gép használóját csapja be és használja bizalmas információk megszerzésére.	A célpont a számítógép használója.	Social engineering különböző típusai (Phishing, hamis weboldalak, csaló emailek, spam mailek, hamis önéletrajzok)

1. táblázat A számítógépes bűnözés kategóriái

A biztonsági megoldások leggyengébb láncszeme az ember, sok visszaélés épít erre. A személyes ráhatás (*social engineering*) olyan gépfüggetlen eljárás, melynek lényege, hogy a támadó a rendszerrel dolgozó emberektől megszerzett adatok segítségével tör be a rendszerbe. Részben ilyen jellegű visszaélés a személyazonosság lopás (*identity theft*), ami akkor következik be, amikor az eltulajdonított személyes adatokkal a csaló visszaél. Az ilyen jellegű visszaélések esetében kiemelt szerepe van a biztonságtudatosság erősítésének.

A támadások többféleképpen csoportosíthatók, megkülönböztetnek *aktív* és *passzív* támadásokat [5]. A passzív támadás azt jelenti, hogy a támadó hozzáfér különböző bizalmas információkhoz, de a kommunikációt megváltoztatni nem tudja, tehát hamis információk küldésére nincs lehetősége. Célja az észrevétlen információszerzés. Ezzel szemben egy aktív támadás esetében a támadó behatol a rendszerbe, képes adatokat megváltoztatni, és az információcserét befolyásolni, ki tudja adni magát a küldőnek vagy a címzettnek.

Az előzőekben felsorolt tipikus visszaélések aktív, illetve passzív kategóriáit mutatja a 2. táblázat.

Passzív támadások	**Aktív támadások**
adat remanencia	átejtés
célzott adatbányászat	DoS támadás
kémkedés	hátsókapu
kisugárzás	HTTP beágyazás (HTTP tunneling)
kukabúvárkodás	jelszótörés
lehallgatás	kártékony kód
shoulder surfing	közbeékelődéses támadás (man-in-the-middle attack)
sniffing	social engineering
	személyazonosság lopás
	vírus
	féreg

2. táblázat Aktív és passzív támadások

IT KOCKÁZAT, KOCKÁZATMENEDZSMENT

A vállalatok működésében a kockázatnak kritikus szerepe van. Az üzleti döntések során figyelembe kell venni a döntéssel együtt járó kockázatokat és a lehetséges hasznokat is. Az informatikai kockázatokat gyakran hagyják figyelmen kívül, ami a későbbiekben számos esetben okoz problémákat. Az informatikai kockázatnak több meghatározása ismert.

A RiskIT megközelítése szerint informatikai kockázat alatt az IT használatával kapcsolatos üzleti kockázatot értjük [6]. A Computer and Information Security Handbook meghatározása szerint a kockázat = fenyegetettség x sebezhetőség x az informatikai vagyon értéke (Risk = Threat × Vulnerability × Asset Value) [7]. A COBIT 4.1 magyar változata szerint a kockázat az üzleti életben annak a lehetősége, hogy egy adott fenyegetés ki fogja aknázni egy eszköz, illetve eszközcsoport sebezhetőségeit annak érdekében, hogy az eszközökben veszteséget

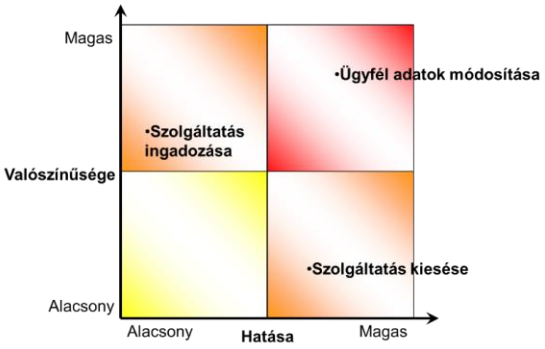
és/vagy kárt okozzon. Mérése általában a bekövetkezés hatásának és valószínűségének kombinációjával történik [8]. Az ISO/IEC 27005:2011 szerinti definícióban IT kockázat alatt értik annak a lehetőségét, hogy egy fenyegetettség kihasználja az informatikai vagyon sebezhetőségét és így kárt okoz a szervezetnek.

Az IT kockázatok sokfélesége a mindennapi működésbeli hibáktól a ritkábban előforduló nagyobb horderejű támadásokig is előfordulhatnak. Az elmúlt időszakban az üzleti rendszerek kritikus fontosságúvá váltak, a tőlük való nagymértékű függőség eredménye, hogy a kockázatokat kötelező felmérni és kezelni. Az informatikai veszélyek egyre nagyobb hányadát teszik ki a vállalatra vonatkozó teljes kockázati halmaznak. Az IT rendszereket veszélyeztető tényezők a szervezetre gyakorolt hatás szerint négy alapvető csoportra oszthatók, ezek a *biztonság*, *rendelkezésre állás*, *teljesítmény*, *megfelelőség* (3. ábra).

3. ábra Az IT rendszereket veszélyeztető tényezők [9]

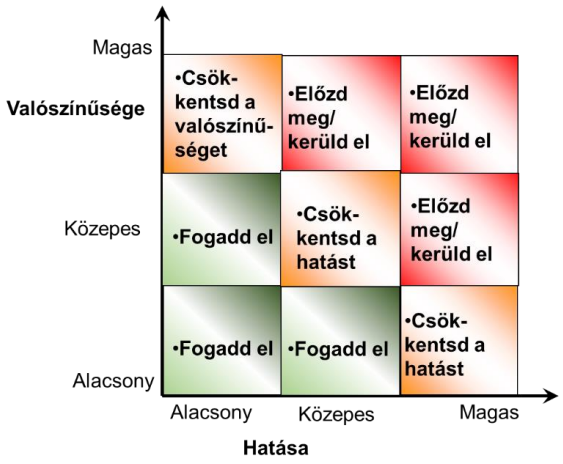
A kockázatmenedzsment két nagyobb területe a kockázatok értékelése és kezelése. A kockázatmenedzsment során az első lépést a lehetséges veszélyek feltárása, a kockázatok azonosítása jelenti. Egy kockázatot célszerű pontos leírással, lehetséges hatásaival, előfordulásának gyakoriságával, kiváltó okaival együtt feljegyezni, hiszen egy összetett vizsgálat, összehasonlítás sokkal pontosabb képet ad majd róla és használható a kockázatok elemzésére és értékelésére. Mivel az előzetesen becsült kockázatok 20%-a okozza a bekövetkezett teljes kockázati hatás 80%-át a kockázatmenedzsmentben is használt Pareto-elv alapján, ezért a kritikus kockázatokra való odafigyelés meghatározó a fenyegetettségek kezelése során.

A kockázatok elemzése és értékelése történhet kvalitatív és kvantitatív módon is, lényege egy rangsor felállítása, amely a lehetséges veszély nagysága alapján állít fel egy sorrendet a kockázatokra vonatkozóan. Kvantitatív értékelés esetén pontosan meg tudjuk mondani, hogy egy adott kockázat bekövetkezése milyen hatást eredményez (kihatás mértéke), pl. 1 napos szolgáltatásleállás forintban kifejezve mekkora kárt okoz a vállalatnak. Kvalitatív módszer esetében gyakran alkalmazott eszköz a szakértői becslés vagy kategóriák definiálása. Ilyen az értékelésben gyakran alkalmazott módszer a kockázati mátrix, amely a kockázatokat az előfordulásuk valószínűsége és a kockázati hatás nagysága alapján osztja be (4. ábra).



4. ábra Lehetséges IT kockázati mátrix

A kockázatok értékeléséhez úgy járul hozzá, hogy a jobb felső részben levő kockázatok a kritikus fontosságúak, a középső területen levők fontosak, míg a bal alsó területen elhelyezkedők kevésbé fontosak. Ennek alapján már kialakíthatók a kockázatkezelési alternatívák (5. ábra).

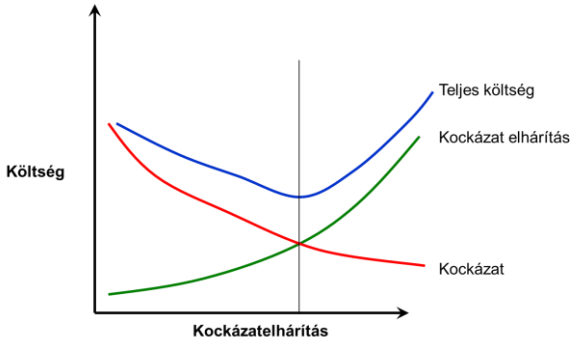


5. ábra Kockázatkezelési alternatívák

A kockázatkezelés gyakran alkalmazott alternatívái, a kockázat megelőzése, elkerülése, a kockázat előfordulási valószínűségének és/vagy hatásának csökkentése, a kockázat áthárítása illetve a kockázat elfogadása, amikor nem teszünk semmit.

Amennyiben a választ megadtuk, a vizsgálat nem érhet véget, hiszen újból ellenőrizni kell, hogy megéri-e, nem hoz-e magával új kockázatokat a változtatás, vagy éppen lehetséges-e meglépni. A megelőzés mellett a hatás csökkentése is opció, ilyenkor elfogadjuk a tényt, hogy előfordulhat a baj, de legjobb tudásunk szerint felkészülünk rá, pl. biztosítást kötünk. A kockázat áthárítása szintén egy lehetséges megoldás, például egy külső szállítót bízhatunk meg a feladattal.

A kockázatkezelési alternatíváknak költsége és erőforrásigénye van, figyelni kell arra, hogy ne legyen drágább a kockázat kezelés, mint az esetlegesen bekövetkező károkozás során fellépő költség (6. ábra).



6. ábra Kockázatelhárítás és költsége [10]

A kockázatmenedzsment ciklikus tevékenység, mivel a kockázatkezelési eljárások végrehajtása után időről időre felül kell vizsgálni a kockázatokat (mivel újabbak jelenhetnek meg) és ennek megfelelően változik a kiértékelés is.

Az informatikai irányítás és a kockázatok kezelése

Az informatikai irányítás (IT Governance) ma már önálló tudományterület a vezetés és szervezés tudományon belül, és a vállalkozás irányításának kihagyhatatlan részét alkotja. Noha az informatikai feladatok ellátásáért az informatikai részleg vezetője a felelős, azonban

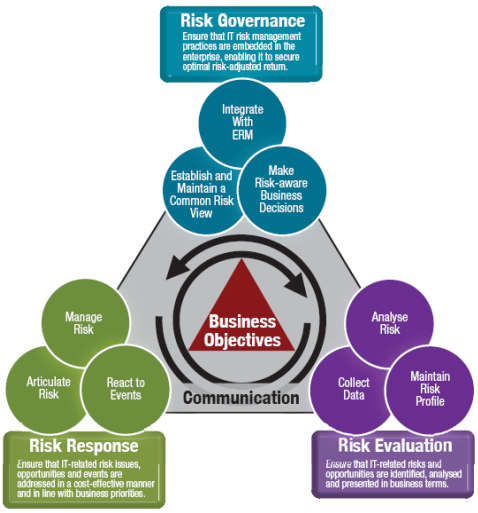
az informatika fejlesztési és stratégiai irányvonalának meghatározásáért a felelősséget az igazgatótanácsnak és az ügyvezető igazgatóknak kell viselniük. Az informatikai irányítás elemei, a vezetői képességek, szervezeti felépítés, a folyamatok együttesen biztosítják azt, hogy a szervezet stratégiájának és célkitűzéseinek megvalósítását a szervezet informatikája folyamatosan tudja segíteni és ki tudja teljesíttetni.

Az informatikai irányítás a vállalatirányítási és ellenőrzési kapcsolatok és eljárások olyan struktúrája, amely új érték hozzáadásával, ugyanakkor a kockázatok és az informatika által kínált előnyök együttes mérlegelésével kívánja megvalósítani a vállalkozás célkitűzéseit.

Az informatikai irányítás fókuszterületei [4] az üzleti és informatikai stratégiai illesztése, az értékelőállítás, az erőforrás gazdálkodás, a kockázatkezelés, és a teljesítménymérés.

A RiskIT keretrendszer

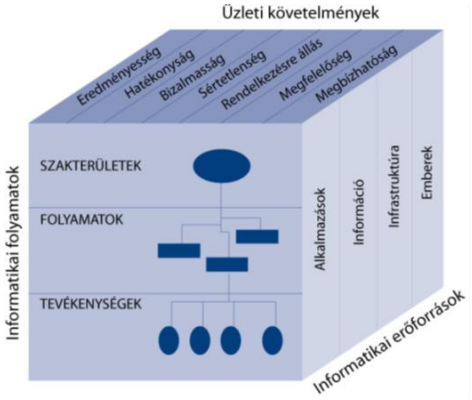
Az ISACA (Information Systems Audit and Control Association - Informatikai Auditorok Nemzetközi Egyesülete) megközelítésében az informatikai irányítás kockázatkezelési területe a RiskIT keretrendszerre épül, amely end-to-end, átfogó megközelítésben tárgyalja az IT használatával kapcsolatos kockázatokat, a kockázatmenedzsment kérdéseit, valamennyi szervezeti szint igényeit és a vállalati kultúra szempontjait is figyelembe véve. Három fő területe a kockázatmenedzsmenttel kapcsolatos irányítási feladatok (risk governance), a kockázatok értékelése (risk evaluation) és a kockázatok kezelése (risk response) (7. ábra). A RiskIT keretrendszer folyamatmodellje bemutatja az egyes területekhez kapcsolódó részfolyamatokat, a folyamatok input és output folyamatait (kapcsolatait), a menedzsment eljárásokat; szerepköröket, felelősségi köröket [RACI – Responsible, Accountable, Consulted, Informed mátrix)], a folyamat célokat és metrikákat és a terület érettségi modelljét.



7. ábra A RiskIT keretrendszer elemei [6]

A COBIT 4.1 keretrendszer

Az ISACA által kidolgozott COBIT (Contol Objectives for IT and Related Technology) olyan keretrendszer, amely általánosan alkalmazható és elfogadott az informatikai biztonsági ellenőrzés és szabályozás területén. Célja „egy irányadó, naprakész, nemzetközileg elfogadott informatikai irányítási kontroll keretrendszer kutatása, kidolgozása, közzététele és népszerűsítése” [8]. A COBIT kocka (8. ábra) bemutatja a COBIT főbb összetevőit és alapelvét, vagyis, hogy az üzleti követelményeknek megfelelő informatikai célok elérése érdekében az informatikai folyamatok menedzselik az informatikai erőforrásokat.



8. ábra A COBIT kocka [8]

A COBIT kocka egyik dimenziója az informatika területét négy szakterületre osztja. Ezek a szakterületek a 4.1 verzióban a „Tervezés és Szervezés” (Plan and Organise), a „Beszerzés és Megvalósítás” (Acquire and Implement), a „Szolgáltatás és Támogatás” (Deliver and Support), valamint a „Figyelemmel kísérés és Értékelés” (Monitor and Evaluate). A szakterületek megfeleltethetők az informatika főbb felelősségi területeinek, a tervezés, fejlesztés, kivitelezés, működtetés és figyelemmel kísérés területeinek. A területeket folyamatokra, azokat pedig tevékenységekre bontja a COBIT. Valamennyi folyamathoz kontroll célkitűzések tartoznak. A COBIT jelenleg használt változata a COBIT 5. Kialakításának egyik legfontosabb célja volt, hogy az üzleti és az informatikai oldalt közelebb hozzák egymáshoz, annak érdekében, hogy az együttműködés hatékonyabbá válhasson. A COBIT 5 támogatja a vállalatokat az IT optimális értékének előállításában a hasznok realizálásán, a kockázatok kézbentartásán és az erőforrások megfelelő használatán keresztül. A COBIT 5 integrált keretrendszert ad, épít a legújabb szabványokra, keretrendszerekre és legjobb gyakorlatokra a vállalati és az informatikai területekről mint például a COS ERM válllati keretrendszerre vagy az ISO/IEC 27000 IT szabványcsaládjára.

Az ISO/IEC 27000-szabványcsalád

Az ISO/IEC 27000-es szabványcsalád az információbiztonsági irányítási rendszerekkel kapcsolatos szabványokat tartalmazza. Az információbiztonsági irányítási rendszerek célja, hogy kockázatkezelési folyamat alkalmazásával és a kockázatok megfelelő kezelésével megfelelően támogassák az információk biztonságát.

A szabványcsalád legfontosabb ajánlása az ISO/IEC 27001 szabvány, amelyben az információbiztonság irányítási rendszer követelményeit tartalmazza. A szabvány legújabb változatában 35 információbiztonsági szabályozási célt határoz meg és 114 kontrollt azonosít az információbiztonsági politika, az informatikai biztonsági irányítási rendszer szervezése, a humán erőforrások biztonsága, eszközkezelés, hozzáférések ellenőrzése, titkosítás, fizikai biztonság és a környezet biztonsága, működésbiztonság, kommunikáció biztonsága, rendszerek beszerzése, fejlesztése és fenntartása, beszállítói kapcsolatok, információbiztonsági incidensek kezelése, üzletmenet-folytonosság valamint a megfelelőség ellenőrzési területeken [11].

A szabvány lehetőséget teremt a szervezetek számára, hogy saját információbiztonságukra vonatkozóan kockázatelemzést végezzenek, majd a kockázatelemzést követően képesek lesznek meghatározni az alkalmazandó kontrollokat. Speciális esetben ez jelentheti az eredeti listában szereplő 114 kontroll kiegészítését is. A kockázatértékelés is nagyobb hangsúlyt kapott, bár annak módszertana nem került meghatározásra.

Az ISO/IEC 27002-es szabvány - az információbiztonság menedzsmentjének gyakorlati kódexe - segítséget nyújt az ISO/IEC 27001 szabványban definiált szabályozási célok és intézkedések értelmezéséhez. Gyakorlati útmutatást ad a szervezet információbiztonságának felmérésére, illetve az alkalmazott kontrollok hatékonyságának meghatározására.

IT BIZTONSÁGI KOCKÁZATOK ÉS KEZELÉSÜK BIZTOSÍTÁSI TERÜLETEN

Az elmúlt időszakban lezajlott botrányok, csődök a biztosítási területen rávilágítottak az informatika kulcsszerepére, az IT biztonsági kockázatok menedzsmentjének fontosságára. A biztosítókban dolgozó szakemberek nem informatikusok, de nagyon sokféle IT biztonsági kockázattal találkoznak rendszeresen. Ügyfelek személyes és pénzügyi adatait kezelik, sokszor a saját notebookon, mobiltelefon segítségével, miközben az ügyfelek és a vállalat sem tudja, milyen IT biztonsági ismeretekkel rendelkeznek, tisztában vannak-e a tipikus IT biztonsági kockázatokkal és a lehetséges védekezési módokkal. Az adatok megfelelő védelme nélkül nem lehet ellenőrizni az adatok kiszivárgását. Az átgondolatlan, ellenőrizetlen módosítások adatvesztést okozhatnak és a nyomnélküli adatvesztés esetén kicsi a helyreállíthatóság esélye. Ennek egy következménye lehet, hogy az adatok nem érhetőek el, amikor szükség van rájuk. Egy vállalat nem tud biztonságosan működni, ha azok az emberek, akik az IT rendszereket használják és működtetik, nem ismerik szerepüket és felelősségüket a rendszerben, nem értik meg a szervezet IT biztonsági szabályzatát, gyakorlatát és eljárásait, nincs legalább alapvető képük a különböző menedzsment, üzemeltetési és technikai eljárásokról.

Biztonsági kockázatok értékelése egy vizsgált biztosítási cégnél

A vizsgált biztosítónál nincs külön IT biztonsági főosztály, szervezeti egység (bár egy hazai vezető biztosítási területen működő cégről van szó), de van 3-4 olyan szakértő, akik munkaidejük egy jelentős részében IT biztonsági feladatokkal foglalkoznak. A vállalat legfontosabb informatikai vagyona az ügyféladatbázis és az alapszolgáltatást nyújtó alkalmazások, pl. partnerkiszolgáló rendszerek. A kérdés, hogy milyen kockázatok merülnek fel és arra milyen védekezési lehetőségekkel tud válaszolni a cég.

IT biztonsági elemek a vizsgált cégnél

A vizsgált cég esetén az IT biztonság kérdése egyre fontosabb, egyre több biztonsági terméket használnak, legfőképpen Symantec-es termékeket. Végpont védelemmel kezdték a védelem kialakítását, majd a standard biztonsági elemek következtek, mint a proxy és a tűzfal, a határvédelem kiépítése. Jelenleg több mint tíz terméket használnak.

Napjaink egyik kihívása a nulla napos sérülékenység és a malware. A nulla napos sérülékenységek ellen még nem adtak ki védelmi eljárást a cégnél, így a védekezés is nehezebb, mint egyéb esetekben. Azonban malware fertőzés, vagy zombi gép gyanúja esetén a kifelé irányuló kommunikációt blokkolják, de a leggyakrabban követett eljárás a kliens gép újratelepítése, amennyiben egy ilyen eset előfordul (zombi számítógép lesz valakinek a gépe, vagy botnetet telepítenek rá). Az ilyen helyzeteknek a kezelésére is vannak kidolgozott eljárások.

A vállalat esetében három főbb terület emelhető ki a tipikus visszaélések közül, a belső támadások közül az adatszivárgás és a személyes ráhatás (social engineering), a külső támadások közül példaként a locky-t, a ransomware (olyan malware, amely valamilyen fenyegetéssel, pl. makro vírus egy ártalmatlannak tűnő emailben, próbál pénzt kicsikarni a felhasználóból) vírusok. Különösen nagy problémát jelenthet, ha egy kulcsfontosságú alkalmazott anyagaival történik mindez.

A locky vírus továbbra is terjed, a biztonsági szakértők szerint a jelenlegi legfontosabb vírusnak számít [12]. A locky vírussal kapcsolatos kockázat csökkentését támogató intézkedés lehet a backup megoldás és a mentés.

Egy másik visszaélés típus elsődlegesen a belső alkalmazottakhoz kapcsolódik, az adatszivárgás. Mivel a cég legfontosabb vagyona az adat, az ügyféladatbázis, kiemelt szerepe van az adatszivárgás megelőzésének, ami ellen használnak adatszivárgást megelőző szoftvert a védelemben. Fokozott figyelmet kell fordítani adatszivárgási szempontból az

adminisztrátori jogkörrel rendelkezőkre, hiszen nekik van joguk ügyféladatok lekérdezéséhez, exportálásához, amivel akár vissza is lehet élni. Ezen a területen is előfordultak incidensek, amelyek elsősorban biztonságtudatosságbeli problémákhoz voltak köthetők. Ilyen eset amikor a felhasználó más cégnek küld ügyféladatot, pl. ha valaki az ügyfélrekord három attribútumára lekérdezést végez (pl. vezéknév, keresztnév, szerződésszám) az ügyféladatbázisból és azt tovább küldi, vagy titkosítás nélkül küld olyan excel táblát, amiben van ügyféladat, akkor az egy biztonsági incidens lesz, amit kezelni kell. Ebben az esetben értesíteni kell az IT biztonsági felelőst (security officer) aki dönt a helyzet kezeléséről. A cégnél végeznek előszűrést, és a gyanús eseteket továbbítják IT biztonsági felelősnek. Ebben a helyzetben az a legfontosabb, hogy az ügyfél ne lehessen beazonosítható, ne lehessen az adataival visszaélni. A cég az adatszivárgások ellen viszonylag jó hatásfokkal tud védekezni.

A harmadik visszaélés fajta a személyes ráhatás (social engineering), ami gépfüggetlen eljárás, így ez ellen a visszaélés ellen talán a legnehezebb a védekezés. Lehet előzetesen megvizsgálni a jelentkező hátterét (pl. pszichológiai tesztekkel), titoktartási nyilatkozatot aláíratni, de ettől függetlenül is elfordulhatnak ilyen esetek, pl. a jelszóelkérés, az ember marad a leggyengébb láncszem a védelemben.

A vizsgált cégnél 2009-ben volt egy conficker virusos eset. A vírus folyamatosan kizárta (kilockolta) az összes felhasználót a rendszerből, és nem csak a felhasználókat hanem az adminisztrátorokat is. A conficker, egy a Microsoft Windows operációs rendszert támadó féreg (worm), 2008 novemberében észlelték először. Kihasználta a Microsoft patch sérülékenységét így hozzáfért fájl megosztásokhoz, felhasználó azonosítókhoz.

A lehetséges védelmi intézkedések közé tartozik a vírusirtó naprakész adatbázissal, valamint az új felhasználóra vonatkozó megfelelő beléptetési feltételek. Ez utóbbinak része az új alkalmazott számítógépének előkészítése, többek között a tűrt, támogatott, tiltott programok meghatározása.

A cég meghatározó informatikai vagyona az ügyféladatbázis és az alapszolgáltatást nyújtó alkalmazások, pl. partnerkiszolgáló rendszerek. A kapcsolódó kockázatok lehetnek az adatvesztés, adatmódosítás, jogosulatlan szolgáltatás igénybevétel, vírusok. Ezekre a vizsgált cégnél is a hálózattal, architektúrával kapcsolatos szokásos védelmi eljárásokat alkalmazzák, mint tűzfal, DMZ, a felhasználók megfelelő autentikációja, vírusirtó szoftver.

A felhasználók általában webes szolgáltatásként veszik igénybe a cég szolgáltatásait (biztosítások kötése, követése), ahol kiemelt figyelmet kap az ügyfél autentikáció és a tranzakció védelme.

Nem csak végponti védelmet alkalmaznak (pl., tűzfal, proxy szerverek, vírusirtók), hanem hardeningelési technikákat is. A hardeningelésre alkalmas szoftverekkel vizsgálják a kiszolgáló szerverek sérülékenységét. A legfontosabb vizsgálandó vagyonelemek az ügyfél adatokat tartalmazó, vagy éles rendszerek (production server). Ezeknek az alkalmazásoknak gyakran vannak publikus IP címeik, ezért ezeket évente legalább kétszer egy blackbox vagy penetration teszttel elemzik sebezhetőségi szempontból. A „blackbox” teszt a funkcionalitás tesztje, amit a specifikációval való összehasonlítással lehet ellenőrizni. A „penetration” teszt során kifejezetten a sebezhetőségeket térképezik fel. A tesztek, elemzések eredményeinek alapján a rendszerfejlesztésnek vagy üzemeltetésnek kötelessége a javításokat elvégezni.

A vállalatnál van formális kockázatértékelés, van kockázatkezelési osztály is. Ha új partner kiszolgáló rendszert fejlesztettek, ami nagy mennyiségű adatot kezel, vagy nagyszámú felhasználó tartozik hozzá, akkor a kockázata is nagy. Kockázatot jelenthet, ha a rendszer nincs megfelelően dokumentálva, implementálva, patchelve, karbantartva, nincs BCP (üzletmenet folytonossági terv), vagy nincs DRP (katasztrófa elhárítási terv). A kockázatértékelés alapján döntik el, hogy egy rendszer elindítható-e vagy sem.

A vizsgált cégnél használnak szabványokat a kockázatok kiértékelésére, ezek a COBIT 5, az ISO 27000, 27001:2005. Alkalmaznak az architektúra menedzselésére TOGAF-ot is,

amely olyan nemzetközileg elfogadott módszertan, mely nagyvállalati architektúrák (Enterprise Architecture) menedzselésére szolgál [13].

A vizsgált cégnél van biztonsági szabályzat, amely sok részterületre kiterjed. Külön szabályzat van az alábbi területekre: személyazonosság-menedzsment (identity management), domain beléptetés, incidenskezelés, változáskezelés, üzletmenetfolytonosság, kockázatmenedzsment. Több tucat biztonsághoz köthető szabályzat és eljárás van, így külön eljárás szabályozza az alábbi területeket: vírusvédelem, sürgős, vagy ad-hoc változtatás, incidenskezelésre, patchelési folyamat (milyen gyakran, mit patchelünk, milyen tesztalakalmazások vannak). A biztonságtudatosság növelésére a cég kihasználja az elektronikus kommunikáció lehetőségeit. A szabályzatok, eljárások publikus része a vállalati intraneten keresztül érhető el, illetve emailen történik a tájékoztatás.

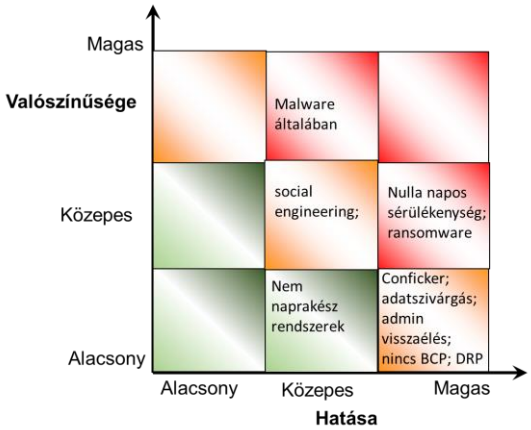
A kockázatok értékelése

A vállalatnál feltárt kockázatok értékelés a nem adhat teljeskörű képet a kockázatokról, mégis a legfontosabb vállalati kockázatokat szemlélteti. A valószínűség és a hatás is három értéket kaphat: alacsony, közepes és magas. A kockázati érték magas, ha a valószínűség vagy hatás közül az egyik legalább közepes, a másik pedig magas. A kockázati érték közepes, ha a valószínűség vagy hatás közül az egyik magas és a másik alacsony, vagy mindkettő közepes. Egyéb esetben a kockázati érték alacsony (3. táblázat).

kockázat neve	valószínűsége	hatása	kockázat értékelése	intézkedés
nulla napos sérülékenység	közepes	magas	magas	FireEye
malware általában (vírus, féreg, kémprogram, agresszív reklámprogram)	magas	közepes	magas	antivirus szoftver, kliens újratelepítés, kifele irányuló kommunikáció blokkolása
malware: ransomware	közepes	magas	magas	backup
malware: conficker vírus	alacsony	magas	közepes	vírusirtó naprakész adatbázissal
adatszivárgás	alacsony	magas	közepes	adatszivárgás elleni szoftver
visszaélés admin jogkörrel	alacsony	magas	közepes	naplózás, nyomonkövetés
social engineering	közepes	közepes	közepes	oktatás
nem naprakész rendszerek (oka: fejlesztés: nincs dokumentáció)	alacsony	közepes	alacsony	rendszerfejlesztési szabványok használata
nem naprakész rendszerek (oka: karbantartás hiány, patch nem naprakész)	alacsony	közepes	alacsony	karbantartási policy-k használata
nincs BCP, DRP	alacsony	magas	közepes	naprakész BCP, DRP

3. táblázat Kockázatok és értékelésük

A kapcsolódó kockázati mátrix látható a 9. ábrán.



9. ábra Kockázati mátrix az interjú alapján

A biztonságtudatosság

Az IT biztonsági kockázatok, kiemelten a biztonságtudatosság vizsgálatának elemzése szintén nem ad teljes képet, mivel a minta nem reprezentatív, de jól szemlélteti egy kis vagy közepes vállakozásnál (biztosítási tanácsadással foglakozó cég alkalmazottai és egy biztosítási bróker kft tanácsadói és ügyintézői) felmerülő kritikus kockázatokat és a lehetséges válaszadási eljárásokat, mivel a kitöltők szakterülete, háttere azonos. A résztvevők 56,3%-a teljes munkaidős, míg 20,8%-a részmunkaidős alkalmazott. IT biztonsági szempontból ennek azért van jelentősége, mert ismert, hogy a visszaélések nagy részét a belső alkalmazottak követik el, hiszen ők ismerik a környezetet, van hozzáférésük a rendszerekhez és az alkalmazott védelmi eljárásokat is tudhatják. A vállalkozók, partnerek (fejlesztők, tanácsadók, egyéb külső közreműködők) szintén jelenthetnek biztonsági kockázatot, pl. az informatikai területen dolgozó vállalkozók hozzáférhetnek bizalmas anyagokhoz. A kérdőíves felmérés alapján három csoport megléte feltételezhető, melyek

- a biztonságtudatos csoport, ahol a cég is figyelmet fordít az IT biztonsági kockázatok elkerülésére, a munkavállalók képzésére,
- a kevésbé biztonságtudatos csoport,
- és a kockázatot jelentő csoport, melynek egyik oka, hogy a cég nincs felkészülve a munkavállalók képzésére, így az emberi tényező okozza a legnagyobb biztonsági kockázatot.

Ezek a munkavállalók kockázatot jelentenek a cég számára, hiszen nem biztonságtudatosak, legyenek teljes munkaidős vagy részmunkaidős alkalmazottak.

A csoportképzés alapját adta, hogy két különböző klaszterezési eljárás során 9 kérdés mindkét eljárásban szignifikánsnak bizonyult, így ezekkel a változókkal készült el a csoportképzés. A következő kérdések szerepeltek a felmérésben (10. ábra).

A felmérés kérdései
Létezik-e az IT biztonságért felelős csapat a vállalatnál?
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?
Észleltél-e már a munkahelyen trójai, vagy egyéb vírusos támadást a gépeden?
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?
Adtál-e már meg bármilyen munkahelyi jelszót másnak?
Ha formázod a merevlemezt, és kitörlöd a fájlokat akkor az összes adat végleg elveszik.
Milyen biztonságosnak tartod a saját számítógéped?
Engedélyezve van-e a tűzfal a számítógépeden?
Automatikus frissítésre van állítva a számítógéped?
Mennyire vagy elővigyázatos, amikor egy csatolt fájlt nyitsz meg e-mailben?
Tudod mi a "phishing"?
Van-e antivírus telepítve, frissítve és engedélyezve a számítógépeden?
Az én számítógépem értéktelen a hackerek számára.
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?
Vannak-e rendelkezések arról, hogy hogyan, mire és mire nem használhatod az e-mailezést munka közben?
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?
Töltöttél-e, és telepítettél-e már le programot a munkahelyeden?
Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?
Ugyanazokat a jelszavakat használod a munkahelyen, mint a privát felhasználói fiókjaidban?(gmail,facebook...)
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?
Amennyiben kitörölsz egy fájlt a számítógépről vagy hordozható eszközről, a rajta lévő információ már nem kinyerhető.
Részt vettél-e IT biztonsági képzésen?

10. ábra A felmérés kérdései

A két eljárásban (hierarchikus klaszterelemzés Ward módszerrel, illetve K-közép módszerrel) a csoportban körülbelül azonos számú egyed került, a válaszadások eltérőek, így a három csoport megléte valószínűsíthető [14].

Két csoport esetén az elemzés során két azonos létszámú csoport jött létre, illetve négy csoport esetén 2 csoport nagyon hasonlónak bizonyult. A három csoport esetén a következő csoportnagyságok születtek a kalszterezési eljárás során minden kérdés felhasználásával (4. ábra).

		K-közép eljárás 3 csoport			
		1	2	3	Összesen
		fő	fő	fő	fő
Ward Method 3 csoport	1	11	0	5	16
	2	0	11	10	21
	3	9	0	2	11
	Összesen	20	11	17	48

4. táblázat Csoportlétszámok Ward és K-közép eljárás során

Mivel 9 kérdés bizonyult szignifikánsnak, ezért ezekkel a változókkal K-közép eljárással újra megnéztük, hogy milyen csoportok jöttek létre, és ezen csoportokat a többi változóval együtt jellemeztük.

A kilenc szignifikáns kérdés látható a 11. ábrán.

A felmérés szignifikáns kérdései
Létezik-e az IT biztonságért felelős csapat a vállalatnál?
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?
Tudod mi a "phishing"?
Az én számítógépem értéktelen a hackerek számára.
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?
Részt vettél-e IT biztonsági képzésen?

11. ábra A felmérés szignfikáns kérdései

Érdekes módon olyan kérdések mint a jelszóhasználat, jelszóátadás bárkinek pl. főnöknek, amely a social engineering egyik kritikus eleme, vagy az emailekben érkező csatolmányok automatikus megnyitására szolgáló szabályok, illetve programletöltések nem bizonyultak szignifikánsnak.

Feltételezéseink szerint az emberi tényező nagy százalékban okoz IT kockázatot, amelyet a felmérés is alátámasztott. Ennek egyik formája a social engineering, mely jelenti például a jelszómegosztást. A biztonságtudatosságot erősíti, hogy a felhasználók jelszóhasználati szokásai a munkahelyi és a privát jelszavak esetében biztatók, jelentős részük, 81,3%-uk más jelszavakat alkalmaz a munkahelyi rendszerekben, mint a privát rendszerekben. Azonban még így is jelentős azoknak az aránya, akik azonos jelszavakat használnak a különböző rendszerekben. Ha ez a jelszó illetéktelen kezekbe kerül, akkor a felhasználó által használt rendszerekhez jogosulatlan hozzáférés valósulhat meg és így különböző visszaélésekre lesz lehetőség. Az így feltört rendszerek között lehetnek fontos vállalati adatokat tartalmazó rendszerek, de a felhasználó olyan privát rendszerei is, mint a home banking rendszer.

A válaszadók közel 23 százaléka tudatosan adta meg másnak is munkahelyi jelszavát, ezzel lehetőséget adva mások számára, hogy az ő nevében használják a rendszert, illetve azokhoz a rendszerelemekhez szerezzenek hozzáférést, amelyhez nem feltétlenül fértek volna hozzá. Az a kérdés is felmerül, hogy a nemet klikkelőkből, hányan adták meg tudtukon kívül

ezen adataikat, vagy hányszor és hogyan adtak erre lehetőséget. Az emberek többsége jóindulatú és konfliktuskerülő, és szívesen segít másnak, ezért meg sem fordul a fejükben, hogy megkérdőjelezzék a belépési adatok elkérésének okát, vagy szükségességét. Egy vállalatnál a jogosultságok kiterjedésének meghatározása fontos IT biztonsági kérdés. A jelszóátadás elkerülésére az oktatás, továbbképzés jelenthet megoldást, hiszen az emberi tényező a leggyengébb láncszem a védekezésben.

A jelszómegosztás, mint a jelszómegadás része további biztonsági kockázatokat rejthet magában. A felhasználók egy része úgy gondolhatja, hogy ha egy munkahelyi vezető, vagy a rendszergazda kéri el a jelszavát akkor azt oda is kell adni. Ez nem igaz, és egyben biztonsági kockázatot is jelent. A jelszómegosztás szintén lehetőséget ad illetéktelen hozzáférésre, visszaélések végrehajtására. Védekezni a felhasználók képzésével lehet.

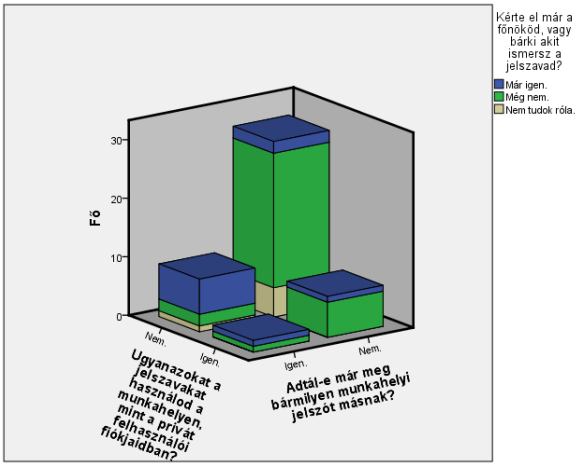
A vizsgálat biztonságtudatosságot erősíti, hiszen tudatosan csak az esetek 15%-ban adták meg az alkalmazottak a jelszavakat (6. táblázat). A 60%-os nem/nem arányt azonban szükséges növelni a tudatosság növelésével. A válaszadók több mint 20%-a már megadta a jelszavát a főnökének, amely arányt tovább kell csökkenteni. Itt közepesen erős, létező összefüggés van, mely a social engineering faktor meglétét támasztja alá (V=0,577, CHI^2=16, p=0.000).

Adtál-e már meg bármilyen munkahelyi jelszót másnak? * Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?

		Kérte el már a főnököd, vagy bárki akit ismersz a jelszavad?			
		Már igen.	Még nem.	Nem tudok róla.	Total
Adtál-e már meg bármilyen munkahelyi jelszót másnak?	Igen.	14,6%	6,3%	2,1%	22,9%
	Nem.	6,3%	60,4%	10,4%	77,1%
Total		20,8%	66,7%	12,5%	100,0%

5. táblázat Jelszómegosztás

A 12. ábrán látható, hogy vannak olyan munkavállalók, akik ugyanazokat a jelszavakat használják a munkahelyen, mint a privát felhasználói fiókokban, már meg adták a jelszavaikat másnak, és a főnökük is elkérte tőlük. Ők a legkockázatosabb csoportba tartoznak biztonságtudatosság szerint, hiszen azzal, hogy megadják jelszavukat, szinte minden fiókjukhoz illetéktelenek hozzáférhetnek.



12. ábra Jelszóhasználati, jelszómegadási eredmények

A vírusok egy jelentős része emailben csatolt fájlként érkezik. Fontos, hogy ezt tudják a felhasználók, amikor leveleznek.

A csatolt fájlok automatikus megnyitása jelentős károkozással járhat, rosszindulatú programok, pl. zsarolóprogramok telepítése történhet meg. A felmérés résztvevőinek 8,3%-a nincs tudatában ennek a problémának, ők jelentik a legnagyobb kockázatot ebben az esetben.

A felhasználók 33%-a megnyitja a csatolt fájlt, ha a feladó ismert, pedig más nevében is lehet emailt küldeni és így visszaélést végrehajtani. Ilyen szempontból a felhasználók egy jelentős része nem kellően tájékozott ezen a területen, áldozata lehet egy ilyen típusú visszaélésnek.

Bár kapcsolat nem mutatható ki a csatolt fájlok megnyitásának gyakorlata és a munkahelyi email használat korlátozása között (mire lehet és mire nem lehet a munkahelyi emailt használni), mégis az rajzolódik ki, hogy a szektorban dolgozók többsége, jelen esetben háromból kettő ember bárkivel, bárhogyan, bármiről levelezhet, tehát semmiféle módon nincsen szabályozva ez a terület. Ennél a kérdésnél is vannak olyan válaszadók (12,5 %), akik tudják, hogy vannak korlátozások, de nem ismerik őket, így nem is tudnak ezeknek megfelelni. Ez szintán kockázatot jelenthet a vállalkozás számásra.

A klaszterezés esetén ezek a kérdések nem kerültek be a klaszterképzés változói közé, de a klaszterek jellemzésébe igen. A kilenc kérdéssel elvégzett elemzés hasonló létszámú csoportokat hozott létre, mint az összes változóval elkészített klaszterek (6. táblázat).

Klaszthereknagyságok eltérése					
		Kilenc változóval készített klaszterek nagysága			
		1	2	3	Összesen
		fő	fő	fő	fő
Klaszter létszámok minden változó felhasználásával	1	15	5	0	20
	2	0	11	0	11
	3	0	5	12	17
	Összesen	15	21	12	48

6. táblázat K-közép eljárással készült klaszternagyságok eltérése

A három klaszter tulajdonságait vizsgálva az első csoport esetében létezik IT részleg, míg a második csoport többsége nem tudja, a harmadik esetében pedig többen állították, hogy nem létezik, mint azt, hogy létezik. Valószínű, hogy a harmadik csoportba tartozók kisebb cégeknél dolgoznak (pl. biztosítási bróker kft-k) ahol az IT biztonsági területhez nem tartozik külön szervezeti egység a cég mérete miatt. Az, hogy a második klaszterben lévők nem tudják, hogy van-e ilyen szervezeti egység nagy biztonsági kockázatot jelenthet, hiszen ezek a válaszadók nincsenek tisztában az IT biztonság vállalati szerepével.

A munkatársak az első klaszterben mind részt vettek IT képzésen, míg a második és a harmadik klaszterben szinte soha senki nem vett részt IT képzésen. Az első csoportban mindenki tisztában van azzal, hogy kit kell értesíteniük vírusfertőzés esetén, tudják, hogy hogyan kell ellenőrizni, hogy vírusos-e a gépük, míg a második csoport fele nem tudja kit értesítsen, és 1/3-uk nem tudja, hogyan ellenőrizze a vírusosságot. A harmadik csoport ugyan tudja kit értesítsen, de a csoport nem tudja hogyan ellenőrizze a gépét, így biztonsági kockázatot jelent a vállalat számára, hiszen nem tudja mikor értesítse az IT munkatársat.

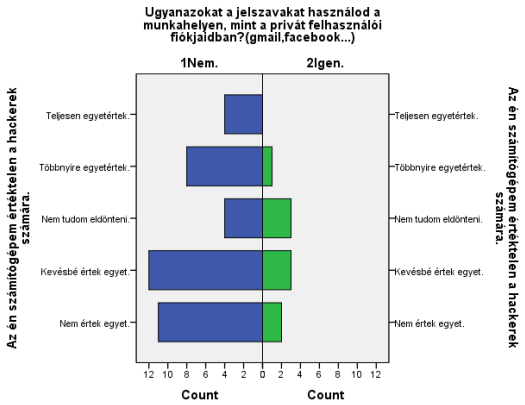
Az első klaszterbe tartozók - nevezhetjük őket most már biztonságtudatos csoportnak, ahol a vállalat számára is fontos az IT szervezeti összefogása, a munkavállalók biztonságtudatossá tétele - 87%-a ismeri az egyik gyakran előforduló visszaélést, a phishing-et (adathalászatot). Azonban a második klaszterbe tartozók - őket nevezhetjük kockázatos csoportnak, ahol megvannak a biztonságtudatosság elemei, de mivel nincs IT szervezeti egység vagy a munkatársak nem tudnak róla, és nem kapnak a munkatársak megfelelő képzést, még nem biztonságtudatos felhasználók - nem tudják mi a phishing, így könnyen megtéveszthetők. Védekezésként a felhasználók tájékoztatása javasolt pl. levélben. A harmadik csoport - az óvatlan csoport – fele nem tudja mi a phising, de itt tréninggel növelhető a biztonságtudatosság. Mindez azt jelentheti, hogy az átlag dolgozó, például egy üzletkötő sok esetben nem kapja meg a megfelelő IT biztonsági képzéseket. Ez felveti azt a problémát, hogy egy átlag felhasználónak vagy saját ismereteire, tapasztalataira kell támaszkodnia a

munkavégzése során, ha biztonságról van szó, vagy valamely másodlagos csatornából érkező információból tudja a kellő lépéseket megtenni, legyen az például egy körbeküldött email. Ennek a tudatában viszont kevésbé hibáztatható egy alkalmazott bármilyen esemény előfordulása esetén, hiszen nagyrészüknek soha nem lett ismertetve az IT biztonsági szempontból szükséges cselekvések köre. Mivel egy-egy ember is kellően nagy károkat tud okozni az informatikai vagyonban, mindenféleképpen szükséges a számítógéppel, illetve internet eléréssel dolgozók teljeskörű tájékoztatását az informatikai biztonság szempontjából.

A vállalat IT szabályozása, illetve annak ismertetése a munkatársakkal csökkenti az IT kockázatokat. Ebben a kérdésben is nagy eltérések mutathatók ki a három csoport között. A biztonságtudatos csoport esetében szabályozva van a bizalmas adatok tárolása, a különböző weboldalak használata, az email használata, illetve a programok letöltése a számítógépekre. A kockázatos csoport esetében a válaszadók 95 és 90%-a szerint sem a weboldalakra sem az emailezésre vonatkozó korlátozások nincsenek a vállalatnál, azaz kockázatos weboldalakat is megnyithatnak. A weboldalak nagy része cookie-kat használ, ami újabb kockázatot jelenthet (pl. adatokat gyűjthet a felhasználó viselkedéséről). A weboldalak látogatásának engedélyezése növeli egy lehetséges támadás esélyét. Az óvatlan csoport 25%-a említette, hogy vannak korlátozások, de nem ismeri őket, így nem is tud ezeknek megfelelni. Az email használati szabályozás még a biztonságtudatos csoportnál is kockázatot jelenthet, hiszen ugyanannyian válaszolták, hogy nincs korlátozás, mint ahányan igennel válaszoltak. A kockázatos csoport esetén semmiféle korlátozás nincs a válaszadók szerint, magában rejtve a lehetséges bejövő vírusok, fertőzött csatolmányok kockázatát.

A vállalat bizalmas adatainak kérdésében az első csoport tisztában van a szabályozással, bár 40%-ban itt is engedélyezve van a bizalmas adatok saját eszközön való tárolása, mely kockázati szempontból azt jelenti, hogy a munkahelyen használt informatikai környezet mellett az otthoni, kevésbé védett környezetben fellépő kockázatokkal is számolni kell. Az otthon használatos eszközök, különösen a portábilis eszközök, mint a mobil telefon, a laptop, tablet általában kevésbé védettek. A felhasználók elveszíthetik őket, ezeket az eszközöket könnyebb ellopni, mint a céges eszközöket, így az adatok illetéktelen kezekbe kerülhetnek. A kockázatos csoport 1/3-a nem tudja, hogy engedélyezve van-e a bizalmas adatok saját eszközön való tárolása, így a csoportban lévő másik 1/3-dal már nagy IT kockázatot jelentenek a vállalat számára. Az óvatlan csoport 15%-a nem tud szabályozásról, ezzel kisebb kockázati tényezőt jelentenek.

Alapvetően kijelenthető, hogy egyetlen hálózatra csatlakozott gép sem értéktelen a hackerek számára, hiszen sokféle támadás létezik, rengeteg, különféle céllal. Itt nem feltétlen adatlopásra kell gondolni, hiszen különböző trójai szoftverekkel, vírusokkal akár a számítógépünk felett más is átveheti az irányítást, innen végezve a támadásokat. Összességében a válaszadók nagyobb része gondolja az állítást kevésbé, vagy nem igaznak. Lényegében ebben a szektorban dolgozók, vállalati adatokat, pénzügyi adatokat és tranzakciókat, valamint személyes adatokat is kezelnek, vagy azokhoz hozzáférnek. A három csoport három különböző módon jellemezhető. A biztonságtudatos csoport mindegy egyes tagja tisztában van azzal, hogy minden gép értékes a hackerek számára, bár még itt is vannak, akik ugyanazokat a jelszavakat használják, ezzel kockáztatva az IT biztonságot (13. ábra). A kockázatos csoport 62%-a vagy nem tudja eldönteni, hogy értékes-e a gépe, vagy úgy gondolja, hogy a gépe valószínűleg értéktelen a hackerek számára, míg az óvatlan csoportban vannak a legtöbben akik teljesen egyetértenek abban, hogy gépük értéktelen a hackerek számára. Mindkét csoportban a biztonságtudatosság növelése a cél.



13. ábra Tudatos jelszóhasználat és a számítógép értéke a biztonságtudatos csoportban

A klaszterezéssel létrehozott csoportokat diszkriminancia elemzéssel visszaellenőriztük, azaz megnéztük, hogy a szignifikáns változók milyen mértékben különítik el a csoportokat, mennyivel jobb-vagy éppen rosszabb a csoportosítás az empírikus csoportosításnál. A változók közötti linearitás létezik (R=0,682), a korreláció nem mutatott kiugróan magas értékeket ($|r|<0,4$), azaz az esetek inkább függetlenek egymástól, illetve a többváltozós normál eloszlás feltételét is ellenőriztük a Mahalanobis távolság kiszámolásával. A csoportok nagyjából azonos elemszámokat tartalmaznak, és a független változók száma kisebb, mint a legkisebb csoportnagyság. A kovarianciamátrixok homogenitása éppenhogy teljesül (Box's M=125,831, sig=0,001) nagyon pici szignifikancia szint mellett. A diszkriminancia elemzés 2 erős és szignifikáns elválasztó függvény meglétét mutatja, 3 jól elkülönülő csoporttal (7. és 8. táblázat).

Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	3,410[a]	67,8	67,8	,879
2	1,623[a]	32,2	100,0	,787

a. First 2 canonical discriminant functions were used in the analysis.

7. táblázat A két elválasztó függvény erőssége az összes változó beszámításával

Wilks' Lambda

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 2	,086	100,376	18	,000
2	,381	39,539	8	,000

8. táblázat A két elválasztó függvény szignifikanciája az összes változó beszámításával

A változók közül a legnagyobb hatással az IT képzésen való részvétel van a csoportokra (Wilks' Lambda=0,437), míg a „Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?", a „Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?" illetve „Az én számítógépem értéktelen a hackerek számára" kérdések közel azonos jelentőségűek (Wilks' Lambda=0,5).

A struktúra mátrix alapján az első dimenziót a szervezeti szabályozással, a vállalati IT felelősségvállalással azonosíthatjuk, míg a második dimenziót a munkavállalói biztonságtudatossággal (9. táblázat).

Structure Matrix

	Function	
	1	2
Részt vettél-e IT biztonsági képzésen?	,551*	-,394
Vannak-e rendelkezések arról, hogy milyen weboldalakat látogathatsz?	,466*	,174
Tudod mi a "phishing"?	,379*	-,187
Tudod-e kit értesíts ha munkahelyeden használt gépedet vírusos, vagy egyéb támadás érte?	,354*	,149
Létezik-e az IT biztonságért felelős csapat a vállalatnál?	,346*	,088
Engedélyezve van-e a vállalat bizalmas adatainak (személyes adatok, pénzügyi adatok) tárolása a saját eszközeiden?	,197*	,005
Milyen gyakran viszel haza adatokat a munkából, hogy otthon folytathasd amit elkezdtél?	,309	,613*
Az én számítógépem értéktelen a hackerek számára.	,354	-,455*
Tudod-e hogyan kell ellenőrizni, hogy vírusos a számítógéped?	,114	-,138*

Pooled within-groups correlations between discriminating variables and standardized canonical discriminant functions
Variables ordered by absolute size of correlation within function.
*. Largest absolute correlation between each variable and any discriminant function

9. táblázat A dimenziókat meghatározó kérdések

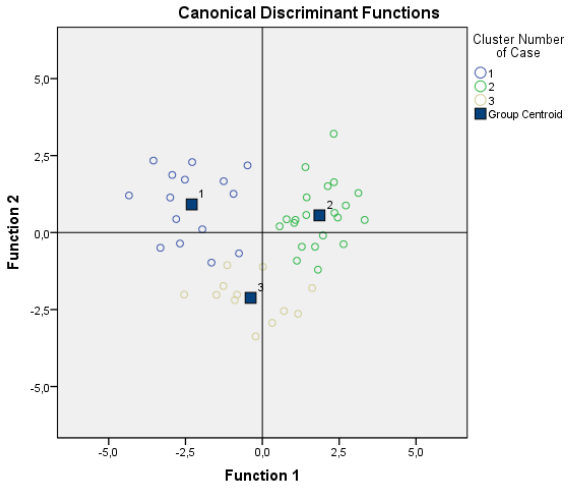
Ezek alapján az első csoport a második dimenzióban rendelkezik magasabb értékkel, a második csoport az első dimenzióban míg a harmadik csoport mindkét dimenzióban alacsony értékekkel rendelkezik (10. táblázat). Így az első csoport a biztonságtudatos, ahol a képzés teszi tudatossá a munkavállalót. A második csoport ténylegesen a kockázatos csoport, hiszen van részleges szabályozottság, de a munkavállalók sok esetben nem tudnak a szabályozásokról, nem kapnak tréninget. A három csoport inkább a szervezeti szabályozottságban különbözik, mint a biztonságtudatosságban (14. ábra).

Functions at Group Centroids

Cluster Number of Case	Function	
	1	2
Biztonságtudatos	-2,297	,914
Kockázatos	1,858	,559
Óvatlan	-,381	-2,120

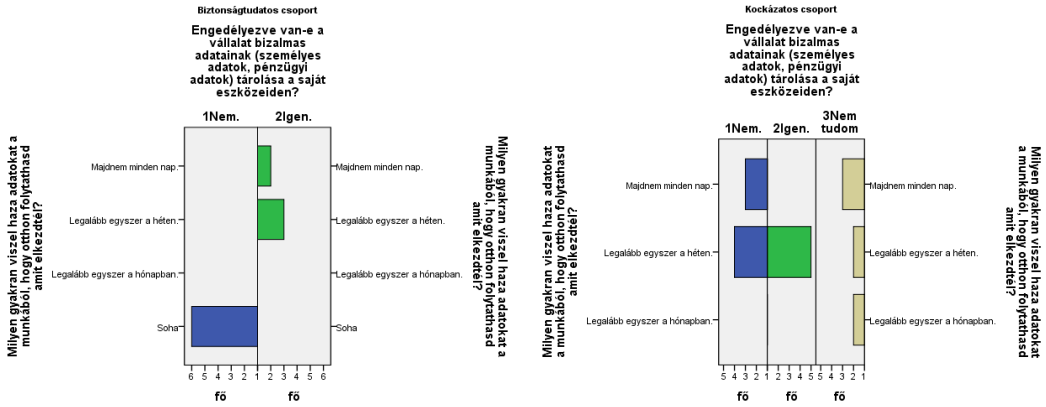
Unstandardized canonical discriminant functions evaluated at group means

10. táblázat A csoportközéppontok 2 elválasztó függvény esetén



14. ábra A három csoport elhelyezkedése kilenc változó figyelembevételénél

A biztonságtudatos csoport esetén inkább nem visznek haza adatokat otthoni munkavégzésre, azonban a kockázatos csoport vagy minden nap vagy legalább egyszer egy héten (85,7%), míg az óvatlan itt a legmegbízhatóbb, hiszen csak egy fő visz haza adatokat, s Ő is csak egyszer egy hónapban. A biztonságtudatos csoportban csak azok visznek haza adatokat, ahol a szabályzat ezt megengedi (15. ábra), míg a kockázatos csoportban annak ellenére hazaviszik az adatokat, hogy nem tudják engedélyezve van-e. Ez a sebezhetőség szempontjából különösen fontos, hiszen a saját otthonukban egy másik hálózatra csatlakozva más biztonsági feltételek mellett végzik a felhasználók ugyanazt a tevékenységet. Az is elég valószínű, hogy az otthoni informatikai környezet kevésbé biztonságos, mint egy nagyvállalatnál lévő, tehát könnyebb támadási felületnek mondható.



15. ábra Bizalmas adatok kezelése és adatok hazavitele

A klasszifikációs táblában kapott eredmények alapján a 2. és a 3. csoport találati aránya 100%, így ezek nagymértékben elkülönülnek egymástól. Mivel az 1. csoport találati aránya 86,7%, így a biztonságtudatosságot még növelni kell a munkavállalókban. A keresztvalidáció találati értéke kisebb, mint az eredeti, de a 81,3%-os teljesítménye jónak mondható, így megbízhatónak tarthatjuk a csoportosítást.

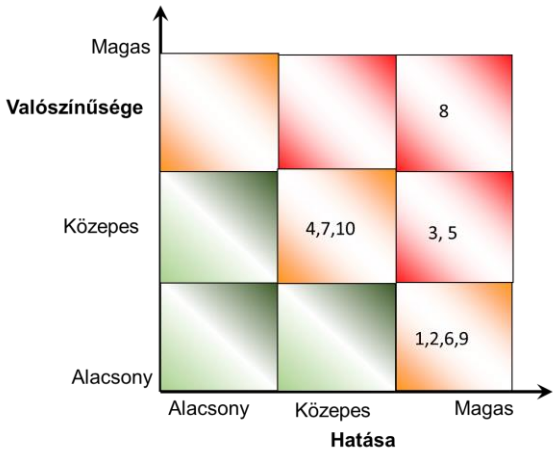
KÖVETKEZTETÉSEK

A vizsgálatok alapján kiemelhető, hogy az emberi tényező, a biztonságtudatosság, valamint a vállalati IT felelősségvállalás játszanak fő szerepet az IT kockázatok esetében. A kockázatértékelés nem ad teljes körű képet, mégis sikerült egzakt vizsgálattal alátámasztani azt az empirikus tapasztalatot, hogy a képzések, tréningek, figyelemfelhívó tájékoztatások érdemben növelhetik a munkavállalói biztonságtudatot, így a kockázatos csoporttagok illetve az óvatlan csoportba tartozók idővel a biztonságtudatos csoportba fognak tartozni. Felhasználva a cikk elején megadott kockázati mátrixot, a következő kép alakul ki (11. táblázat)

a kérdés témaköre	kockázat	valószínűsége	hatása	kockázat értékelése	intézkedés
vírusfertőzés (trójai, stb.)	1.vírusfertőzés (trójai, stb.)	alacsony	magas	közepes	antivírus program
jelszómegosztás, jelszóhasználat	2.illetéktelen hozzáférés	alacsony	magas	közepes	oktatás
adathalászat	3.adatokkal való visszaélés (adathalászat)	közepes	magas	magas	oktatás
email sebezhetőség	4.vírusfertőzés (email), adatvesztés	közepes	közepes	közepes	antivírus program
adattárolás saját eszközön	5.adatokkal való visszaélés (adattárolás)	közepes	magas	magas	oktatás, titkosítás, jogosultsági rendszer, szabályozás
számítógép védelmének hiányosságai (antivírus, tűzfal, frissítés)	6.vírusfertőzés, hackertámadás, adatszivárgás	alacsony	magas	közepes	frissítések telepítése, antivírus program, tűzfal telepítés
internet használati sebezhetőség	7.vírusfertőzés (internet), adatvesztés	közepes	közepes	közepes	szabályozás, oktatás
képzés hiánya	8. vétlen károkozás	magas	magas	magas	oktatás
nincs IT biztonsági csapat	9. nincs incidenskezelés	alacsony	magas	közepes	felelősségi körök meghatározása
programtelepítés lehetősége	10. vírusfertőzés (program-telepítés)	közepes	közepes	közepes	antivírus

11. táblázat Kockázatértékelési táblázat

A kapcsolódó kockázati mátrix látható a 16. ábrán (a számok az egyes kockázatokat jelentik).



16. ábra Kockázatértékelési mátrix

A kockázatelemzési mátrix is azt támasztja alá, hogy az emberi tényező, a képzés hiánya, a vétlen károkozás adja a legmagasabb kockázati kategóriákat, valamint a biztonságtudatossági szint nem megfelelő a vállalatnál, növelésének kiemelt szerepe van az IT biztonság területén. A válaszadók közel 70%-a soha nem vett részt IT biztonsági képzésen, így nem várható el a biztonságtudatos munkavégzés. Valamilyen formában akár a belépéskor szokásos képzés részeként meg kell jelenjen az IT biztonsági képzés. Az adathalászatot (phishing) a felmérés szerint a kitöltők 56%-a nem ismeri, pedig ez a visszaélés jelentős károkat okozhat. A bizalmas adatok saját eszközökön való kezelése, tárolása a felmérés szerint a válaszadók 35,4 százalékának engedélyezett, további 19%-a pedig nem is ismeri a szabályozást. A saját eszközök védelme általában elmarad a vállalati eszközökétől, a cégnek meg kell fontolnia a bizalmas anyagok tárolásának tiltását saját eszközökön. Közepes kategóriába kerültek a felmérés alapján a vírusfertőzés, a jelszómegosztás, az email sebezhetőség, a számítógép védelmi hiányosságok, az internet használattal összefüggő sebezhetőség, a programtelepítési lehetőség és az IT biztonsági csapat hiánya.

Javasolt a legkevesebb jogosultság alkalmazása, vagyis mindenki csak azzal a jogosultsággal rendelkezzen, amire a munkájához szükség van. Fontos az IT biztonsági kockázatok rendszeres felmérése, értékelése és ennek alapján az intézkedések aktualizálása.

Mivel a védelem leggyengébb láncszeme a felhasználó, így a biztonságtudatossággal kapcsolatos képzés az egyik legfontosabb eszköz az IT kockázatkezelésben.

FELHASZNÁLT IRODALOM

[1] Intel Security, (2015) McAfee Labs, 2016 Threats Predictions. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf, 2016. 02 23

[2] DAVIES, S. (2015) Nem használhatja a svéd közszféra a Google felhő alapú szolgáltatásait. http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/ 2016. 02 25

[3] SCHIRMACHER, D. (2013) Phishing-Test bei der Berliner Polizei. http://www.heise.de/security/meldung/Phishing-Test-bei-der-Berliner-Polizei-3028064.html 2016. 02 12

[4] ISACA, (2015) CISA Review Manual 2015. Rolling Meadows, IL 60008 USA: ISACA.

[5] VASVÁRI, G. (1997). Biztonsági rendszerek szervezése. Budapest: Pro-Sec kft.

[6] ISACA. (2009). The RiskIT Farmework. Rolling Meadows, IL 60008 USA: ISACA

[7] CABALLERO, A. (2009). Chapter 14. In J. Vacca, Computer and Information Security Handbook. Morgan Kaufmann Publications, Elsevier Inc.

[8] ISACA Budapest Chapter. (2011). CobiT 4.1 (magyar kiadás). http://www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf, 2014. 02 15

[9] PÓSERNÉ, V. O. (2007). IT kockázatok, elemzésük, kezelésük. Hadmérnök. http://www.zmne.hu/hadmernok/archivum/2007/3/2007_3_poserne.html, 2015. 12. 11

[10] FEHÉR, P. (2012). Működési kockázatok kezelése. http://www.slideshare.net/pethich/mkdsi-kockzatok-kezelse, 2016. 03. 10

[11] IsecT Ltd. . (2016). Information security standards. http://www.iso27001security.com/index.html, 2016. 08. 22

[12] GOMBASZÖGI, A. (2016). Megint terjed a Locky "zsaroló" vírus és mutánsai . http://www.excom.hu/hir-ujdonsag-forum/hirek/64-megint-terjed-a-locky-zsarolo-virus-es-mutansai.html, 2016. 03. 23

[13] Open Group. (2011). TOGAF. http://pubs.opengroup.org/architecture/togaf9-doc/arch/, 2016. 03. 22

[14] SAJTOS, L., MITEV, A. (2007) SPSS Kutatási és adatelemzési kézikönyv, Alinea Kiadó