# Az informatikai biztonság pszichológiája



*Izgalmas pszichológiai háttér húzódik meg a gyakran szürkének látszó informatikai biztonság iparága mögött. Ha megvizsgáljuk a technológiai megoldások és a hozzájuk kapcsolódó érzelmek viszonyát, illetve a vezetői képességek fejlődését, egészen érdekes látleletet kapunk.*

Annak ellenére, hogy a legtöbb gazdasági szervezet esetében jelentős pénzügyi erőforrásokat fordítanak az informatikai biztonság technikai aspektusára, egyelőre viszonylag kevésbé foglalkoznak az információbiztonság humán jellegű kihívásaival. Pedig egy vállalkozás életét nemcsak az informatikai rendszerekben keringő adatok és információk biztonsága határozza meg, hanem a munkatársak információbiztonsági tudatossága is, ami a cég életében kiemelkedően fontosnak tekinthető, fogalmazott *Tarján Gábor,* a MagiCom ügyvezető partnere, aki egy tudományos kutatás keretében méri fel a gazdálkodó szervezetek információbiztonsági tudatosságának érettségi szintjét. Mint mondja, a mai digitális világban kitolódtak a vezetői félelem határai, hiszen azzal is szembesülniük kellett, hogy már nemcsak a cégen belül, hanem az otthoni munkavégzésre és az utazás idejére is különböző biztonsági szabályokat kell kialakítaniuk és azok betartását kell megkövetelniük kollégáiktól és persze saját maguktól is.

**Kinézünk a vállunk felett**

„Különböző felmérések igazolják, hogy például utazás közben a legsérülékenyebb az ember, s nemcsak a csábítóan szabadon hozzáférhető wifi-hálózat miatt, hanem az üzleti dokumentumok láthatósága miatt is” – mondja a szakember. A zsúfolt helyeken vagy hosszú repülőút során az úgynevezett „shoulder surfing”, azaz a vállunk feletti kifigyelés útján súlyos veszélynek vannak kitéve az üzleti tartalmak és személyes adatok.

„Éppen ezért a biztonsági tudatossághoz az is hozzátartozik, hogy tudomásul vesszük, felelősséggel tartozunk az általunk kezelt információkért, amire a sokat szidott GDPR is felhívja a figyelmet. 2012-ben publikálták azt a módszertant, amely leginkább passzol az én filozófiámhoz és szervezeti szinten vizsgálja, milyen érettségi szinten áll egy vállalat” – magyarázza Tarján Gábor.

Képzeljünk el egy ötfokú skálát, amelyen a szervezetek tudatosságának érettségi szintjét sorolják be a nem-létezőtől (1. szint) a robusztus mérőszámrendszerrel megtámogatottig (5. szint). Valószínűleg az első kategóriába is sok cég kerül bele.

„Kíváncsi vagyok, hogy a szervezetek mennyire értékelik alul vagy felül magukat, de a kutatásom összességében arra irányul, hogy képet kapjunk a magyar vállalatok érettségi szint szerinti megoszlásáról az öt kategóriában, és hogy a kutatás kérdőívét kitöltőktől kapunk-e olyan ötleteket, legjobb gyakorlatokat, amelyek mintaként szolgálhatnak más magyar gazdálkodó szervezeteknek” – teszi hozzá a szakember.

**Zsarolóvírusok pszichológiája**

A számítástechnika hőskorában a programoknál elég volt a hibátlan működés. Pár év múlva azonban egyre több vírus, károkozó jelent meg. A hardverek is gyorsan fejlődtek, ez a támadások mértékét, és gyakoriságát is felerősítette.

A kiberveszélyek elleni védekezés magánembertől a multi cégig mindenkit érint, fejti ki *Csizmazia-Darab István,* az ESET–Sicontact IT-biztonsági szakértője. Mára mindenki megtanulhatta, nem létezik száz százalékos védelem, és nincs sebezhetetlen rendszer sem – a Macintosh és a Linux sem az. A 2003-as SQL Slammer pedig azt is bebizonyította, hogy naprakész hibajavító frissítések nélkül sebezhetőek maradnak a rendszereink.

A zsarolóvírusok öt éve tarolnak, és sikerült a felhasználókat érzékeny ponton támadni: az elkódolt dokumentumok elvesztése ijesztő, a „semmiért” váltságdíjat fizetni nyomasztó, a hiányos mentések miatt pedig garantált a lelkiismeret-furdalás. A bűnözők sokszor szokatlan célpontokat választottak: kórházakat, iskolákat, állami hivatalokat, közműveket. Az amerikai kórházak például dollár ezreket fizettek ki a támadóknak.

A ransomware kártevők (például CryptoLocker, TeslaCrypt, Petya, Locky) gonosz módon okosak, az erős titkosítás mellett a pszichológiai nyomásgyakorlást is alkalmazták: a sürgetés, a szűk határidő, másodperc alapú visszaszámláló, újraindításkor tömeges fájltörlés – mindez azért, hogy az áldozatok gyorsabban fizessék ki a virtuális valutában követelt váltságdíjat. Néhány példa: a Jigsaw fertőzésnél minden órával exponenciálisan nőtt a véglegesen törölt fájlok száma. A Popcorn Time nevű zsarolóvírus azt ígérte, ha az áldozat megfertőzi két ismerősét, akkor ő ingyen kaphatja majd meg a saját helyreállító

kulcsát. A Chimera, pedig kifejezetten vállalati áldozatokra szabva jelent meg: az állományokat nem csakzárolta, hanem váltságdíj követelése mellett azzal is fenyegetett, hogy nem fizetés esetén feltölti azokat egy nyilvános weboldalra.

Bár volt néhány hibás zsarolóvírus is – például szimpla statikus kulcsot használt –, a kiberbűnözők folyamatosan továbbfejlesztették programjaikat. Egy idő után például a kártevők elkezdték célzottan törölni a helyi mentéseket, és csak ezután kezdték el az állományok titkosítását. A váltságdíj fizetése egyébként sem jelent automatikusan megoldást, hiszen bűnözőkkel üzletelünk, így gyakran a pénzutalás ellenére sem érkezik meg a feloldó kulcs. De a váltságdíj-fizetési hajlandóság is sajnos erősíti ezt a fajta „üzletágat". A félelem légköre azonban hatott a szervezetekre, amelyek igyekeztek hatékonyabban védekezni.

Szemléletváltás és a GDPR hatása

A zsarolóvírusok mellett ugyancsak nagy lökést adott az IT-szemlélet fejlődéséhez az európai adatvédelmi rendelet, a GDPR hatályba lépése. Bár ebben ez esetben egyes eszközszállítók megpróbálták kihasználni a GDPR farvizét és egy-két eszköz, illetve dobozos szoftver megvételével azt állították, az ügyfelek letudták a rendeletet, a megfelelés ennél sokkal komplexebb. Több kérdéskörrel kell foglalkozni egyszerre: a jogi, az IT-biztonsági és a folyamatkezelési területekkel is. Mindezek elég hangsúlyosak, de maga a törvény is nagy segítséget jelentett, hiszen az informatikai és az információbiztonság, azon belül az adatbiztonság reflektorfénybe került.

Meglátjuk, hogy ez a lelkesedés meddig fog kitartani, mert az igazsághoz az is hozzátartozik, hogy amíg itthon nincsenek elmarasztaló ítéletek vagy komolyabb bírságok, amiről a sajtó beszámol, addig a május 25. után alábbhagyott élénkülés nem fog új lendületet kapni.

Mindenesetre már az is kedvező fordulat, hogy egyáltalán ilyen aktívan foglalkoznak az informatikai és információvédelemmel a vállalatok, hiszen a GDPR előírja a tudatosítást, és így ha még nem is tették meg, akkor hamarosan elkezdődik a cselekvési tervek összeállítása, és elindulnak a várva várt belső képzések a szervezeteken belül, foglalja össze Hirsch Gábor.

**Vállalatbiztonsági kompetenciaközpont a mérnökhiány kezelésére**

Nemcsak az informatikai biztonsági trendek vagy a fenyegetések, hanem például a humán erőforrás hiánya is jelentősen alakítja a szervezetek életét és formálja a vezetők gondolkodását. A megváltozott piaci környezetnek köszönhetően újszerű kompetenciafejlesztési módszerek kerülnek felszínre, hogy a hiányzó mérnöki munkaerőre megoldást kínáljanak.

„A mérnökhiány a Novell esetében is komoly szervezeti változtatásokat és szolgáltatásfejlesztési modelleket igényelt, ezért mi vállalatbiztonsági kompetenciaközpontot hoztunk létre" – mondja *Hargitai Zsolt,* a Micro Focus cégcsoportot hazánkban képviselő Novell Magyarország üzletfejlesztési igazgatója. Mint mondja, a jelenség több problémát is felvet, például: hogyan találják meg a megfelelő embereket és hogyan tartsák meg őket; melyek azok a szolgáltatások, amelyek a legmagasabb értékkel bírnak; illetve hogyan lehet a magasabb óradíjak miatt rövidebb idő alatt kiszolgálni az ügyfeleket.

„A munkatársak elkötelezésére az elmúlt egy-két évben viszonylag újszerű szakember-megtartási és tehetséggondozási programokat alakítottunk ki, illetve komoly

erőfeszítéseket tettünk abba az irányba, hogy az egyetemekről becsatornázzuk a fiatalokat” – magyarázza Hargitai Zsolt. Náluk a cégcsoportnál dolgozó munkatársak mintegy 15 százaléka egyetemi programokon keresztül került a céghez. „A bevezetett új kezdeményezések segítenek abban, hogy a mérnökhiány problémáját vállalati szinten kezeljük” – teszi hozzá az üzletfejlesztési igazgató.

Szolgáltatási oldalról az üzleti folyamatokat automatizáló, új termékkel foglalkoznak kiemelten. „Olyan szoftvermegoldásról van szó, amelyben kódolás és fejlesztői kapacitás nélkül lehet összerakni munka- és üzleti folyamatok, illetve szolgáltatások támogatására szolgáló megoldásokat. A kompetenciaközpont esetében is arra törekedtünk, hogy olyan iránymutató megoldásokat kínáljunk, amelyek használatával kevesebb humán erőforrásra van szükség az üzemeltetés során. Számunkra mindenképpen nagy változást jelent, hogy a piaci igények a szervezeti kérdéseket is átformálják, de ez a változás felpezsdíti a szervezeti kultúrát, megújulásra kényszeríti a menedzsmentet, és a szolgáltatáskínálatunknak is jót tesz, ha követjük a megváltozott ügyféligényeket” – részletezi Hargitai Zsolt.

**Ment és frissít, ment és frissít**

*Hirsch Gábor* független IT-biztonsági szakértő szerint az elmúlt tíz évben alapvetően pozitív irányba változott az informatikai és az információbiztonsági vezetők szemlélete. Mint mondja, ha a magyar nagyvállalatokat vizsgáljuk meg, akkor felfedezhető, hogy esetükben már közép- és hosszú távú stratégiai jelentőséggel tekintenek a kérdéskörre, míg a kkv-k és a mikro cégekre leginkább az ad hoc problémakezelés a jellemző. Utóbbi csoport esetében megfigyelhető az is, hogy döntő többségben csupán akkor kezdenek bizonyos problémakörrel foglalkozni, amikor valamilyen nem kívánt esemény következett be.

Az elmúlt időszakban a zsarolóvírusok irányították rá a figyelmet például a szervezeten belüli mentés fontosságára, vagy a WannaCry zsarolóvírus esetében a frissítések jelentőségére. Általánosságban elmondható, hogy a zsarolóvírusok nagy hatást gyakoroltak a vállalatok információbiztonsági tudatosságára, mivel ezen támadások hatására a felső vezetők megtapasztalhatták, mi történik, ha megfertőződik az egész szervezet – ebben az esetben akár a vezető számítógépe –, és elvesznek a féltve őrzött személyes és céges adatok. Innentől kezdve jobban odafigyeltek a saját szervezetük biztonsági kérdéseire is.