ZALA MIHÁLY, EY MAGYARORSZÁG

FOTÓ: TESZÁR ÁKOS, ITB

LEGYEN A BIZTONSÁG
ALAPÉRTELMEZETT KOMPONENS!

A SIKER KULCSA A TUDATOS VÉDEKEZÉS

Sokat segítene a magyar vállalatok információbiztonsági érettségén, ha több lenne a hazai IT-biztonsági szolgáltató, és jobban bíznának bennük a potenciális ügyfelek. A személyeket tekintve pedig az lenne a fontos, hogy a CIO és a CISO ne a vetélytársat lássa a másikban, hanem tanuljanak meg közös célokért dolgozni.

Az idei már a 21. alkalom, amikor megjelent az EY Global Information Security Survey (a GISS). Az adatgyűjtés még tavaly ősszel, mintegy 1300 felső (többnyire informatikai és információbiztonsági) vezető megkérdezésével történt. A legújabb felmérésben egyebek mellett nagy figyelmet szenteltek annak, hogy milyen visszatérő kommunikációs hibákat követnek el a biztonsági szakemberek, milyen a viszony az információbiztonsági csapat és a vállalat többi területe között, illetve hogy mi lehet a CISO szerepe a digitális átalakulás folyamataiban.

Mire megy el a pénz?

A felmérésben szereplő öt nagyobb kérdéskör közül az első az információbiztonsági költségvetésre vonatkozott – mondta a GISS-t ismertető podcastban *Zala Mihály,* az EY Magyarország IT és technológiai tanácsadásért felelős vezetője. A globális válaszadók közel kétharmada az éves árbevétel kevesebb mint 5 százalékát költi IT-biztonságra, közülük 38 százalék 1 százaléknál is kevesebbet. Ez annak fényében mindenképpen meglepő, hogy számos más felmérésből az derül ki, hogy a vállalatvezetők a kiberbiztonsági kockázatokat teszik az üzletmenet-folytonosságot veszélyeztető tényezők közül az első helyre. Rendkívül beszédes adat az is, hogy a globális válaszadók 16 százalékának fogalma sincs arról, mennyit költenek védekezésre – így pedig azt is lehetetlen megbecsülni, hogy a kockázatokkal arányos-e a ráfordítás.
Jellemző a ráfordítások megoszlása is. A relatív többség (28 százalék) kiberbiztonsági központra (Security Operation Center, SOC) költi a legtöbb pénzt, amit az adatvédelem követ. Utóbbinak is nagy a jelentősége, hiszen a sikeres támadásokhoz sokszor az ellopott személyes adatokon keresztül vezet az út. A szokásostól eltérő kiadásokat az esetek közel felében az új fenyegetésekre adandó válaszlépések teszik szükségessé, amit a változó külső és belső megfelelési (compliance) követelményekhez való alkalmazkodás követ; az új üzleti követelmények megvalósulását lehetővé tévő beruházásokat csak a válaszadók 9 százaléka említette. Hasonlóképpen a compliance és a kockázatcsökkentés az a két terület, amelyre a válaszadók többsége nagyobb figyelmet (és IT-biztonsági költségvetést) biztosít, de a harmadik helyen már a felhőre való felkészülés áll.

Bevonni a vezetést

Az információbiztonságra irányuló egyre nagyobb figyelem egyértelmű jele, hogy a vállalatok vezetése is kiemelten foglalkozik vele. Globálisan a vállalatvezetők 42 százalékát teljesen, további 50 százalékát pedig kismértékben bevonják az IT-biztonság tervezésébe. A podcast hallgatósága is szavazhatott erre a kérdésre, és nagyon hasonló arányok jöttek ki (teljes mértékben: 50 százalék, valamilyen mértékben: 45 százalék), ami mindenképpen örvendetes hír.
Már csak az egyre erősebb bevonódás miatt is fontos kérdés, hogy a vezetés mennyire van birtokában azoknak a kompetenciáknak, amelyekkel meg tudja ítélni az információbiztonsági kockázatokat. Közel felük igen, és majdnem ugyanennyien nem, de ők is erősen igyekeznek elmélyíteni a tudásukat. Zala Mihály ezzel kapcsolatban felhívta a figyelmet arra, hogy az oktatás, a biztonságtudatosság erősítése nemcsak a dolgozók esetében fontos. A menedzsment tagjai (beleértve a legfelső döntéshozót) számára is kellene legalább 1-2 órás workshopokat szervezni, hogy erősödjön affinitásuk a biztonsági kérdések és szempontok iránt. Ha ezt történik, akkor talán egy kicsit csökken a különbség a globális és a magyar helyzet között abban a tekintetben, hogy lát-e jelentős kockázatot a felsővezetés a kiberfenyegetésekben. Nemzetközi téren ugyanis 72 százalék szerint jelentős a kockázat, míg itthon (a podcast hallgatóinak szavazása alapján) csak 56 százalék gondolja ugyanígy.

CIO és CISO – együtt erősebbek

Erősen befolyásolja az információbiztonság vállalaton belüli megítélését, hogy a CISO tagja-e a felső menedzsmentnek, és ha igen, ki alá van rendelve. Globálisan a felmérés szerint 36 százalékban tagja a cégvezetésnek az IT-biztonsági vezető, és legnagyobb arányban (44 százalék) az informatikai vezetőnek (CIO) jelentenek; második helyen a vezérigazgató szerepelt, 18 százalékkal. Erről nem készült hazai kutatás, de a tapasztalatok szerint itthon kisebb arányban kerül a csúcs közelébe a CISO, és a szavazáson az is kiderült, hogy a magyar többség a CIO-nak jelent. Ez utóbbi viszont problémákat szülhet, hiszen az informatikai és az információbiztonsági vezető érdekei nem mindig esnek egybe – egy CISO-nak alapértelmezés szerint a CIO-t is ellenőriznie kellene, amit nehezen tud megtenni, ha alája van rendelve. A legjobb megoldás, ha mindketten vezető pozícióban vannak, és kölcsönösen gyümölcsöző együttműködést tudnak kialakítani: új megoldásokat hívnak életre, csökkentik a költségeket, például felhőmegoldások bevezetésével. „Egy CISO nem azzal éri el a legnagyobb eredményt, ha felnagyítja a meglévő veszélyeket, hanem ha olyan új, kiberbiztonsági szempontból is fejlett platformok, struktúrák bevezetését tudja támogatni, amelyek hosszabb időre is védettséget nyújtanak a vállalatnak", mondja Zala Mihály.

Célkeresztben a személyes adatok

Rákérdeztek a felmérésben, hogy a vállalatok melyik biztonsági keretrendszert használják, és melyiket tartják a legalkalmasabbnak. Nem meglepő módon a két kérdésre adott válaszok nagyon hasonlóak: az első helyen az ISO, a második az amerikai szabványügyi hivatal keretrendszere, a NIST végzett, ez utóbbi alapjaira épül az IBTV (2013. L tv) illetve a kapcsolódó 41/2015-ös BM rendelet is. A tanúsítványok és certifikációk jelentőségét nem szabad alábecsülni, hangsúlyozza Zala Mihály. Ezek követése, betartása bizalmat ébreszt a vállalat iránt a partnerekben, ügyfelekben. Ugyanez egyébként igaz az információbiztonsági szolgáltatókra is. Általánosságban nem bíznak bennük a potenciális ügyfelek – a megkérdezettek 69 százaléka szerint a bizalom attól függ, ki is az adott szolgáltató. A referenciák, a tanúsítványok sokat számítanak, úgy a cég, mint az ott dolgozó szakértők szintjén. Ugyancsak fontos lehet, hogy a gyártónak, szolgáltatónak van-e felelősségbiztosítása – Magyarországon ez utóbbi még nem jellemző.
A céges rendszerek biztonsága szempontjából nagyon nem mindegy az sem, mikor vonják be a kiberbiztonsági csapatot egy új termék vagy szolgáltatás fejlesztésébe. Ebben a kérdésben a magyar cégek hasonlóképpen járnak el, mint külföldi társaik. Bő egyharmaduk már a követelményspecifikáció során megteszi ezt, egynegyedük pedig a rendszertervezésnél számít a biztonsági

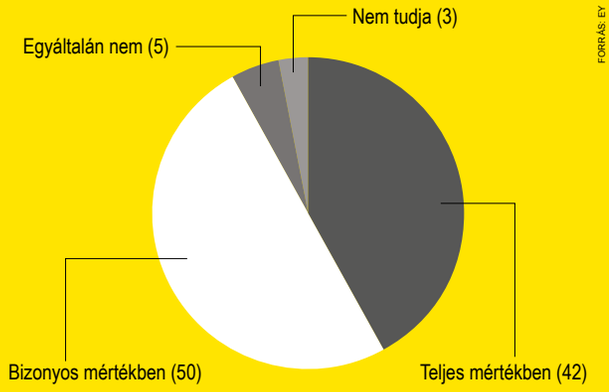
FOTÓ: TESZÁR ÁKOS, ITB

Milyen új üzleti és technológiai területekre fordítanak kiemelt figyelmet és magasabb kiberbiztonsági költségvetést?

(a GISS válaszolóinak százalékában)

Milyen mértékben vonják be a vállalat vezetését az információbiztonság tervezésébe?

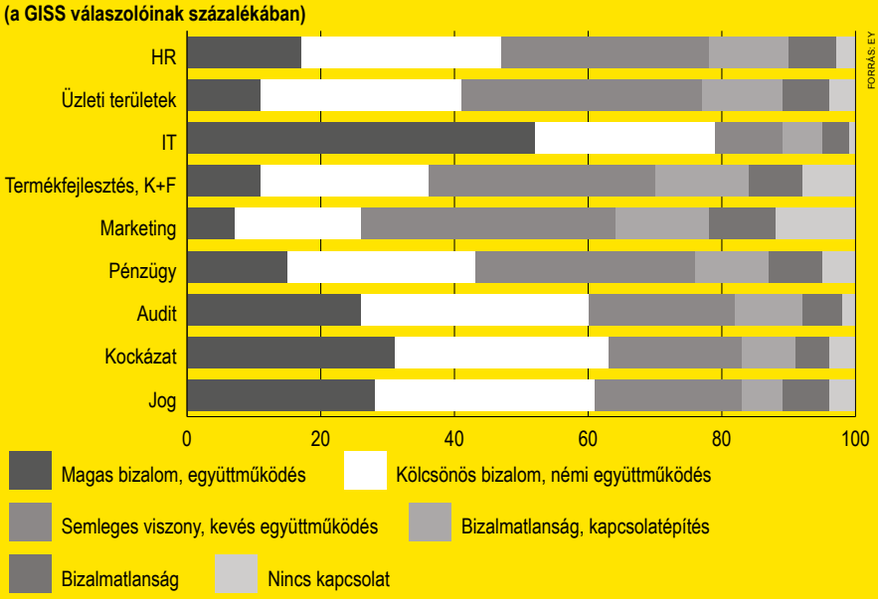
(a GISS válaszolóinak százalékában)



FOTÓ: TESZÁR ÁKOS, ITB

Hogyan értékelné a biztonsági csoport és az egyéb üzleti funkciók kapcsolatát?

(a GISS válaszolóinak százalékában)



FORRÁS: EY

szakemberekre. Aggodalomra egyedül az adhat okot, hogy 9 százalékuk csak a kódolás során teszi meg ezt, 7 százalékuk pedig soha. „Ezzel együtt sajnos a hazai tapasztalat azt mutatja, hogy ha a szándék meg is van arra, hogy az információbiztonsági alapelveket az üzleti igény felmerülésének időpontjától figyelembe vegyék, a gyakorlatban ez nem valósul meg. A tesztelések során olyan alapproblémák kerülnek elő, amelyek egyértelműen mutatják, a szervezetek nem tudtak megbirkózni azzal, hogy a biztonság alapértelmezett komponenssé váljon. Ezért támogatjuk a hazai cégeket abban, hogy elmagyarázzuk nekik és szállítóiknak, hogy kinek milyen felelőssége és feladata van abban, hogy a biztonsági megfontolások a projekt teljes ciklusa alatt határozottan megjelenjenek”, mondja Zala Mihály.

Ami a támadások célpontjait illeti, globálisan és Magyarországon is az ügyfél- és a pénzügyi adatok állnak az első helyen. Itthon nagyjából egyenlő arányban választották ezt a kettőt a válaszadók, míg nemzetközi szinten az ügyféladatok „nyertek”

45-15 százalékarányban – ez azzal is összefüggésben lehet, hogy a GISS-ben erős volt a pénzügyi szektor jelenléte. A támadások mögött a legtöbben a szervezett bűnözői csoportokat gyanítják, de emögött alig lemaradva következnek a hacktivisták és a munkavállalói hibák.
Az eredményeket értelmezve Zala Mihály elmondta, hogy az ismeretlen eredetű támadásokat hajlamosak a cégek a kiberbűnözők nyakába varrni, miközben nem egy esetben azok valamely piaci vetélytárs megrendelését hajtják végre – emiatt is lehet, hogy a partnerek és szállítók csak 6 százalékos arányt képviseltek ebben a válaszban. Az is érdekes, hogy ha összeadjuk dolgozói hibákat és a szándékos belső károkozást, máris a támadások 28 százalékánál járunk – amivel viszont a dolgozók már egyértelműen a legnagyobb veszélyforrássá lépnek elő.

Kellenek a SOC-ok

„Az adatokból kirajzolódik, hogy bár még mindig erős a reaktív hozzáállás az IT-biztonság terén, egyre több olyan vállalkozást találunk, amelyek aktívan próbálnak elébe menni a fenyegetettségeknek. Globálisan és Magyarországon is sokat haladtunk előre, de közben a fenyegetettségek is nőttek, így emiatt még többet kellene tenni", összegezte kérdésünkre tanulságokat Zala Mihály a podcast után. Ugyanakkor még mindig jelentős a különbség az anyagi lehetőségek szempontjából Magyarország és a fejlettebb régiók között.
Külföldön nem kérdés, hogy felállítsanak-e egy SOC-ot, létrehozzanak-e nagy csapatokat, amelyekkel megelőzhető lenne a baj. Itthon – minden tagadhatatlan fejlődés dacára – még most sem könnyű rávenni a vállalatokat, hogy adatszivárgás elleni megoldást vásároljanak vagy megbízható, referenciákkal rendelkező IT-biztonsági szolgáltatót vegyenek igénybe. Különösen erős a lemaradás a SOC-okat tekintve. Magyarországon alig néhány ilyen van, de még azokat is kevesen veszik igénybe, amelyek szolgáltatásként is elérhetőek.
„Egészen nagyméretű cégek nem tartanak fenn biztonsági központot, vagy gondolják azt, hogy egy logelemző rendszer már megfelel a SOC-nak", tárta fel Zala Mihály.
Általánosságban is elmondható, hogy nagyobb a bizalmatlanság az IT-biztonsági szolgáltatók iránt, ezért is óriási kár, hogy nincsenek nagy hazai felhőszolgáltatók. A külföldiekből sokan nem kérnek, pedig számos biztonsági szolgáltatás érhető el náluk, és magasabb szintű védelmet tudnak kínálni, mint a vállalatok döntő többsége. Különösen a kisebb vállalkozások számára lehetne előnyös, ha kis beruházással magasra tudnák emelni védelmi szintjüket", említ egy kimaradt lehetőséget Zala Mihály.
Itthon még az is kevéssé jellemző, hogy nagyvállalatok megköveteljék beszállítóiktól, partnereiktől a biztonsági rendszerek, tanúsítványok meglétét. Ez a gyakorlat inkább csak a nemzetközi cégekre jellemző, amelyek vagy kötelező információbiztonsági bevizsgálást írnak elő beszállítóiknak, vagy évente szúrópróba-szerűen ellenőrzik néhányukat, hogy betartják-e a szerződésben vállaltakat. Ez már csak azért is rendkívül fontos, mert a statisztikák szerint a támadások mintegy 90 százaléka partnereken, beszállítókon keresztül éri el a vállalatokat, attól függetlenül, hogy hacktivisták, vagy épp kiberbűnözők hajtják végre a támadást adott esetben munkavállalói figyelmetlenség kihasználásával.

IT-biztonság a COVID-19 után

Érezhető a magyar vállalatok IT-biztonsági hozzáállásában a vírusjárvány hatása, mondta el kérdésünkre Zala Mihály. Egyrészt megnőtt az érdeklődés az olyan eszközök iránt, amelyek segítségével a munkafolyamatok a távolból is követhetők, ellenőrizhetők – a menedzserek legalább ilyen módon ellenőrizni akarják, mit és mennyit dolgoznak a kollégák.
Másrészt, és ez hosszabb távon is pozitív hatást fog kifejteni, számos vállalatnál felértékelődött a távoli hozzáférésű szolgáltatások és alkalmazások védelme. Gyakorlatilag már eddig is volt minden cégnél olyan szolgáltatás, amelyet akár a dolgozók, akár az ügyfelek elérhettek a weben keresztül. Ezeket az alkalmazásokat viszonylag ritkán vizsgáltatták be biztonsági szempontból, ami viszont megnövelte egy esetleges külső támadás sikerének esélyeit.
Az általánossá vált távmunka hatására a belső rendszerek távoli elérése hirtelen reflektorfénybe került. Emiatt egyre többen veszik fontolóra, hogy a cég összes, a távolból publikusan elérhető szolgáltatásait leteszteltetik, és ha kell, befoltozzák a talált sérülékenységeket.

A lényeg a tudatos védekezés

Ami a cégvezetés és az információbiztonsági vezető és csapat viszonyát illeti, ezen a téren is jó irányba mozdulnak a dolgok Magyarországon. Már abszolút nem jellemző, hogy az IT-biztonságra felesleges pénzkidobásként tekintenek. Ugyanakkor, mondja Zala Mihály, bár a vezetés sokszor érzékeli a veszélyt, még mindig azt hiszik, hogy az incidensek a zsarolóvírusokkal egyenlők (nem függetlenül attól, hogy a tömegmédiában ezek az esetek kapnak nagyobb nyilvánosságot). Gyakori, hogy a látványos kockázatokra fókuszálnak, attól félnek jobban, pedig a nagyobb veszélyt inkább a láthatatlan és észrevehetetlen adatlopások jelentik. Sokan lebecsülik azt a kockázatot is, amelyet a mindenre elszánt konkurencia jelent.
A legfontosabb az lenne, hogy a vállalatok tudatosan közelítsenek az információbiztonság témaköréhez – mondta végül Zala Mihály. Ebbe beletartozik, hogy felmérik az IT-biztonságra fordított összegeket, és azt összehasonlítják az esetleges sikeres támadások okozta károk nagyságával. Innentől kezdve már sokkal biztosabb alapokra építkezve lehet szembeszállni a fenyegetettségekkel. Fontos összetevő az is, hogy tudatában legyenek a külső és belső sérülékenységeikkel, hogy tudják, hol várhatóak a támadók, ezért ajánlott legalább évente (pénzügyi szektorban gyakrabban) átfogó vizsgálatok elvégzése. Ezekkel együtt sokszor nagy beruházásokra sincs szükség: a biztonság szintje már akkor is nagymértékben növelhető, ha a dolgozók rendszeres és hatékony oktatásban részesülnek, és nem kattintanak gyanús linkekre, nem nyitnak meg mindenféle dokumentumot. Az oktatásból viszont nem szabad kihagyni az üzleti vezetőket sem, mert az ő szemléletük alapjaiban tudja befolyásolni a vállalat információbiztonsági hozzáállását.

Schopp Attila