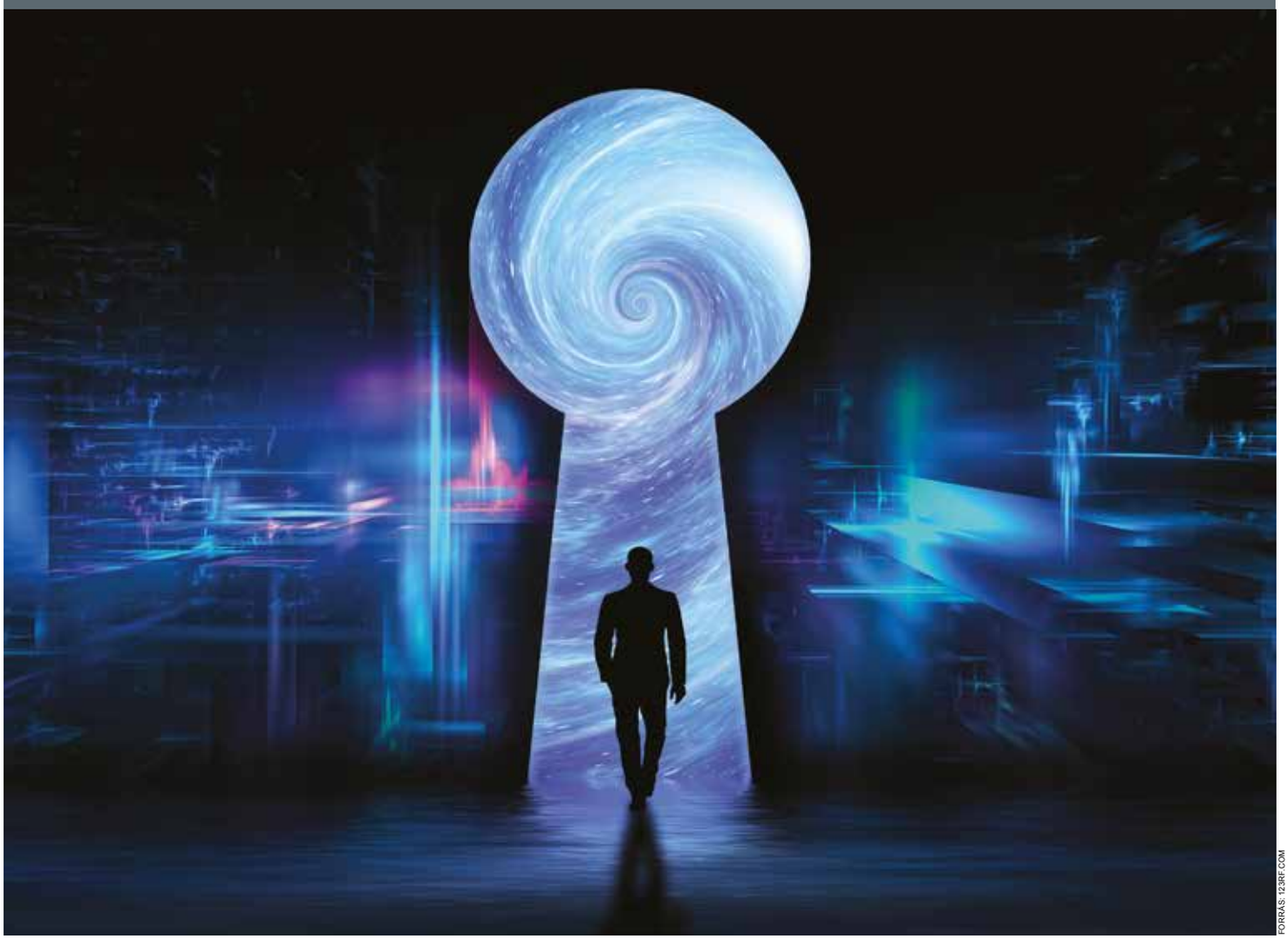
„A TÁMADÓK IS ÉRZIK A VÁLSÁGOT, NEKIK IS TÖBB BEVÉTELRE KELL SZERT TENNIÜK”

A biztonság új bonyodalmai



FORRÁS: 123RF.COM

A CISO-k helyzete dinamikusan változik. Egyes megfigyelők szerint a pandémia, majd az orosz–ukrán háború kellemetlen kiberbiztonsági mellékhatásai növelték a CIO-k és a CISO-k egymásrautaltságát, ami csekély pozitívum azokkal a kihívásokkal összevetve, amelyek napjainkban teszik próbára őket. Aktuális kihívásokról, a jövő fenyegetéseiről és saját CISO-identitásáról kérdeztünk két IT-biztonsági szakembert.

A mostanság legtöbbet feltett kérdésnek mi sem tudtunk ellenállni, így a két sokat tapasztalt IT-biztonsági vezetőt is megkérdeztük a jelen mindennapos kihívásairól, amelyek a sokszorozódó fenyegetésektől a vállalati költségcsökkentésen át felölelik a munkaerőhiányt és az emberi hibák elfordulását is: kihívás-e, hogy nemcsak a fenyegetések, de az emberi természet is változik.

„A szakembereket, különösen a nagyon jó szakembereket nehéz felvenni és megtartani, ráadásul kevesen is vannak. További problémát jelent mindenhol a folyamatos költségcsökkentés. Pedig ezt se lehet végtelen ideig folytatni. Amikor elértük az optimális szintet, akkor meg kell állni. Csakhogy a változó energiaárak, a kiszámíthatatlanság nem teszi könnyűvé ezt sem. Ráadásul a munkaterhelés is nő, és a túlterhelt emberek többet és sűrűbben tudnak

hibázni. Ami pedig az incidensek számát illeti, a pandémia óta egyre több és egyre szofisztikáltabb támadási kísérlet történik”, mondta *Szeiler Andrea,* a Transcom Worldwide AB Global CISO-ja, a WITSEC (Women in IT Security) elnöke.
Tóth Zsolt, a delaware CISO-ja szerint elsősorban nemcsak a fenyegetések sokszorozódnak, „de mindinkább a technológia és a környezet változik, amit az emberek viselkedése nem feltétlen követ. Mindez hatással van az információbiztonsági stratégiára is. Az egyének, csapatok és szervezetek viselkedések megértése, valamint a motivációk, attitűdök, a meglévő tudás feltérképezése jelenti a kihívást. Ha egy szervezet vezetői képesek megfigyelni és megérteni a fentieket, akkor a megfelelő üzenetekkel, oktatásokkal, rendszerekkel és személyes példákkal képesek elindítani egy pozitív irányú változást”, fejtette ki.
Nem lehet elégszer hangsúlyozni, hogy a kiberbiztonságra a szervezetek vezetői ne költségként, hanem befektetésként, esetleg egyfajta biztosításként tekintsenek. Erre erősít rá a Gartner előrejelzése is, amely az információbiztonsági kiadások 11 százalékos növekedését jósolja, csak 2023-ban, ami jól jelzi a területben lévő potenciált.

Újfajta fenyegetettségek a láthatáron

A kötelező „aktuális kihívások” kérdéskörön túl a jövőt feszegető felvetéseket is nagy népszerűség övezi mostanában, így adódik a kihagyhatatlan témakör: mit tartogat a jövő?
„Ha látnám, mi jön, nem itt lennék, hanem a Szilícium-völgyben. Természetesen az irányok, trendek, kirajzolódnak, és azzal is érdemes tisztában lenni, hogy iparáganként, régiónként, szervezetenként változhatnak. Mégis, ha fel kellene sorolnom néhány fenyegetést, amelyekre általában érdemes lesz odafigyelni, a következőket mondanám: social engineering, identity managementhez, valamint felhőhöz kapcsolódó fenyegetettségek, ransomware, távmunkához kapcsolódó fenyegetettségek, digitális beszállítói kockázatok, azaz kultúra, emberek, eszközök, szoftverek, folyamatok”, mondta Tóth Zsolt.
Szeiler Andrea máshonnan indít. „Nemcsak az elszálló árak, hanem az egyre sűrűbb és hosszabb ellátási problémák, áramkiesések azok, amelyekkel foglalkozni kell. A támadók is érzik a válságot, nekik is több bevételre kell szert tenni, tehát egyre több támadást hajtanak majd végre, és a magánszemélyek is készülhetnek, mert a támadóknak mindegy, kitől jön a bevétel, és sajnos ők sokkal védtelenebbek”, figyelmeztetett.
Meglátása szerint a munkaerőhiány sokkal rosszabb lesz, mert a fizetések – a nemzetközi munkaerőpiac eredményeképpen – emelkedni fognak azokban az országokban, ahol jelenleg még azt gondoljuk, olcsó. „De ha az IT-s szakember tud nyugat-európai vagy ahhoz közeli bérért dolgozni, nem fog habozni. A mostani generáció és az utánuk érkezők egyre nyitottabbak lesznek arra, hogy országok között mozogjanak, sokkal inkább, mint a mi generációnk. Ráadásul az érkező generációk teljesen máshogy szeretnének dolgozni. Szabadabban, kevesebb időt töltve egy zárt irodában, korlátozás nélkül használva az informatikai eszközöket. Kevesebb időt töltenek egy szervezetnél, kihívásokat követve szárnyalnak majd. Ehhez nekünk, CISO-knak is alkalmazkodnunk kell, ennek mentén kell biztosítanunk a szervezet és az adatok védelmét. Kihívásban nincs hiány!”, zárta Szeiler Andrea.

Kiss Franciska

FORRÁS: WITSEC

SZEILER ANDREA,
TRANSCOM WORLDWIDE AB

FORRÁS: DELAWARE

TÓTH ZSOLT,
DELAWARE

A biztonsági vezető mibenléte

A „CISO” kifejezést az informatikát csak a partvonalról kísérők is ismerik, de legalábbis van némi elképzelésük arról, hogy mi is csinálnak a szóban forgó pozícióban ülők. Arról azonban már kevesebb szó esik, hogy a CISO-ságnak vannak típusai is: technikai információbiztonsági vezető (technical security officer), üzleti információbiztonsági vezető (business security officer) és stratégiai információbiztonsági vezető (strategic security officer). Ennek mentén arra voltunk kíváncsiak, hogy az elméletben jól körülhatárolt fogalmak miként öltenek testet a valóságban. Szeiler Andrea így fogalmazta meg: „ez egy nagyon érdekes és lényeges kérdés, hiszen nem vagyunk egyformák. Noha első diplomám az informatika területéről származik, a második már közgazdasági, míg a harmadik vezetői. Ehhez tegyük hozzá az életút során szerzett tapasztalatokat is. Ezek alapján én saját magamat a technika területéről érkező, de már a technikától eltávolodott információbiztonsági vezetőnek érzem. A területem a kockázatkezelés, üzleti folyamatok, megfelelőség, magyarul governance. Támogatom az információbiztonsági operációt is, és foglalkozom technológiával is, de nem ez a fő terület. Így azt gondolom én business vagy strategic security officer vagyok”
Hasonló véleményt fogalmazott meg magáról *Tóth Zsolt*. Mint kifejtette, elsősorban stratégiai információbiztonsági vezetőnek tartja magát, „ha a stratégiát hosszabb távú, egy irányba mutató tevékenységek összességének tekintjük bizonyos célok elérése érdekében. Felelősségi köreim közé tartozik a delaware csoport információbiztonsági stratégiájának kialakítása, célok meghatározása, a hosszútávú tervezés, a roadmap, valamint a szükséges erőforrások biztosítása.”