ITEXEC 2022 – IT-BIZTONSÁG

Egyedül nem megy

Az automatizálás és a felhőszolgáltatások igénybevétele ma már elengedhetetlen az IT-biztonságban – derült ki azokból az előadásokból és kerekasztal-beszélgetésekből, amelyek ezt az örök témát vesézték ki konferenciánkon.

A világban az akut Covid-veszély elmúltával (és még inkább az orosz-ukrán háború kitörésével) a kiberbiztonság ismét a vállalati vezetők első számú prioritása lett – idézte az Allianz globális felmérését a konferencia egyik legtöbbet emlegetett előadásában *Zala Mihály*, az EY technológiai tanácsadási és kiberbiztonsági részlegének vezetője. Ehhez képest Magyarországon még régiós összehasonlításban is kevesen alkalmazzák a már jól bevált, de az alapszintű védekezésen túlmutató megoldásokat. Így például miközben a régió többi országában akár több tucat CERT (Computer Emergency Response Team) működik, addig Magyarországon kettő. *(Erről részletesebben is olvashatnak a 48. oldalon.)* A magányos harcosok korszaka véget ért a kiberbiztonságban – figyelmeztetett Zala Mihály, értve ez alatt, hogy külső segítség és szolgáltatások nélkül gyakorlatilag egyetlen szervezet sem képes megvédeni magát.

Kívülről jövő veszélyek

A későbbi előadásokban és beszélgetésekben több más fontos szempont is előkerült. *Urzica Olivér*, a Prianto regionális vezetője is arra hívta fel a figyelmet, hogy ideje lenne szemléletet váltani. Mindeddig a szervezetek önmagukba fordulva, a belső biztonságra fókuszálva próbálták megvédeni magukat, és nem igazán figyeltek arra, ami a külső környezetben, a nagyvilágban történik. A jövőben viszont a korábbinál sokkal nagyobb figyelmet kell szentelni a külső fenyegetettségekre, a szervezet informatikai rendszereinek kitettségére. Ehhez egyrészt kellenek az eszközök, amelyek a rendszerek folyamatos monitorozásával észlelik az incidenseket („nem árt, ha látunk, amikor valamit meg akarunk keresni", fogalmazta ezt meg *Bódis Péter*, a Magyar Államkincstár CISO-ja), vagy akár bepillantást nyerni a támadók zárt világába. Ha kiismerjük motivációikat, módszereiket, akkor védekezni is hatékonyabban tudunk ellenük, fogalmazott.

Horváth Tamás, a Brightdea Solutions ügyvezetője is kritikus területnek értékelte a kívülről elérhető felületek, a kitettség fokozottabb figyelését. Erre is, de számos más feladatra is alkalmasak lehetnek a felhő alapú biztonsági szolgáltatások; egyetértés volt abban, hogy ezek egyre hangsúlyosabbak lesznek, mert belső erőforrásokat mind nehezebb találni.

Az erőforráshiány egy másik megoldási iránya az automatizálás, tette hozzá *Csinos Tamás*, a CLICO country managere; ez egyelőre azért megy nehezen, mert a szükséges kódolási ismeretek nem feltétlenül vannak meg a biztonsági csapatokban.

FORRÁS: ITB

CSINOS TAMÁS, CLICO

Felhasználók, felhasználók, felhasználók

„Az új védelmi határvonal már maga a felhasználó", idézte fel a panelbeszélgetésen az egyik előadást *Rakoncza Zsolt*, a Dell Magyarország ügyvezető igazgatója. Így aztán a felhasználót kell felvértezni minél erősebben; a Dell ezt azzal segíti, hogy számítógépeibe már hardverszinten építik be a védelmi funkciókat. Ennek egyik érdekes példája az „intelligent privacy". Lényege, hogy a laptopok kamerája biztonsági funkciót is kap: figyeli a hátteret is, és ha azt észleli, hogy valaki nézi a monitort, akkor automatikusan elhomályosítja a képét, hogy az illető ne tudja leolvasni az esetlegesen bizalmas információt.

Különösen fontos lehet a felhasználók védelme a hazai kkv-szegmensben, említett egy újabb szempontot *Schneck Zsolt*, a Shield ügyvezetője. A kisvállalkozások zöme nem költ dolgozói biztonságtudatosságának fokozására, az alkalmazott technológiákban is elmaradnak, így 90 százalékukat biztosan fel lehet törni. Ez pedig a beszállítói láncokban jelenthet komoly problémát, hiszen rajtuk keresztül támadhatóvá válnak a nagyobb vállalatok rendszerei is.

Schopp Attila

FORRÁS: ITB

URZICA OLIVÉR, PRIANTO

FORRÁS: ITB

SCHNECK ZSOLT, SHIELD