Sajtóközlemény
Budapest, 2026. szeptember 17.

A VÁLLALATOK HAMIS BIZTONSÁGÉRZETE JELENTHETI A LEGNAGYOBB IT-BIZTONSÁGI KOCKÁZATOT

A közép- és nagyvállalatok kiberbiztonsági felkészültségét vizsgálta a One Solutions és az IVSZ – Digitális Vállalkozások Szövetsége közös kutatása.

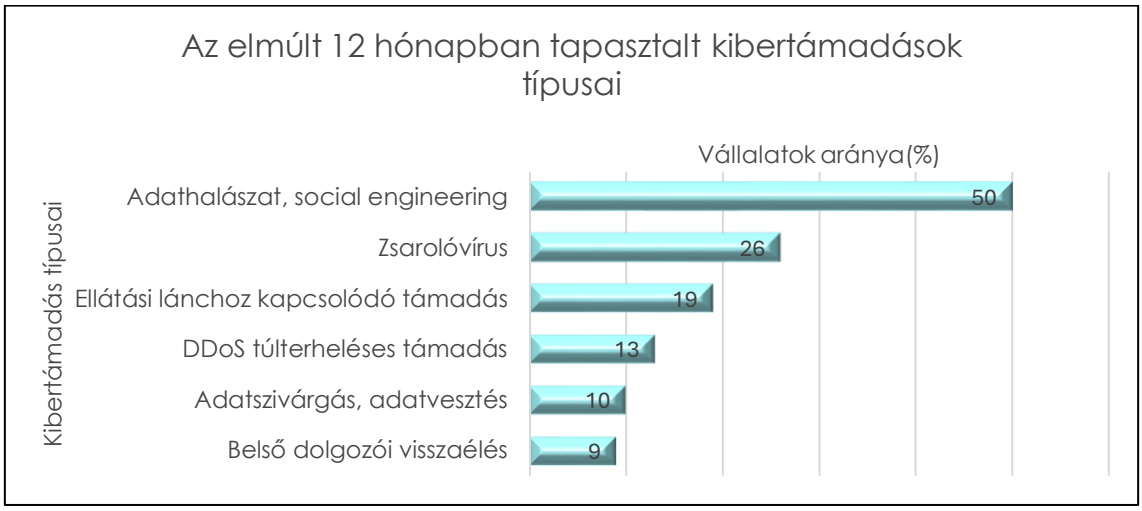
- **A 2026 első felében készített reprezentatív felmérés eredményei szerint a megkérdezett vállalatok több mint a fele (58%) szembesült valamilyen kiberbiztonsági incidenssel az elmúlt egy évben, a nagyvállalatoknál pedig ez az arány elérte a 91 százalékot.**
- **A leggyakoribb támadási formák az adathalászat és más, emberi megtévesztésre épülő social engineering módszerek: ilyen próbálkozásokkal minden második szervezet találkozott (50%). Ezeket követik a zsarolóvírushoz kapcsolódó események (26%) és az ellátási láncot érintő támadások (19%).**
- **Az emberi tényezőt a válaszadók 51 százaléka jelentős vagy kritikus kockázatnak tartja, a nagyvállalatoknál pedig ez az arány meghaladja a 80 százalékot.**
- **A vállalatok 60 százaléka felkészültnek érzi magát, ugyanakkor mindössze 16 százalékuk rendelkezik rendszeresen begyakorolt incidenskezelési folyamattal. Ez jól mutatja, hogy a vállalatok biztonságérzete sokszor előrébb jár, mint a szervezeti és incidenskezelési felkészültségük.**

A hazai közép- és nagyvállalatok kiberbiztonsági felkészültségét vizsgálta az a reprezentatív kutatás, amelyet a One Magyarország Zrt. vállalati üzletága, a One Solutions és az IVSZ – Digitális Vállalkozások Szövetsége megbízásából a BellResearch végzett 2026 márciusában. A felmérésben több mint kétszáz, legalább 50 főt foglalkoztató vállalat vett részt. Az eredmények szerint a felmérést megelőző 12 hónapban a vállalatok 58 százaléka szembesült valamilyen kiberbiztonsági incidenssel. Tízből kilenc (91%) nagyvállalat számolt be legalább egy kiberbiztonsági esetről, és minden második (52%) középvállalat találkozott hasonló eseménnyel a vizsgált időszakban. A megkérdezettek 57 százaléka úgy véli, hogy a következő egy évben tovább erősödnek a kiberfenyegetések, a nagyvállalati válaszadóknak pedig már közel 90 százaléka számít erre. A One Solutions szakértői szerint a legnagyobb IT-biztonsági kockázatot ugyanakkor a vállalatok hamis biztonságérzete jelentheti.

A támadók leggyakrabban az embert veszik célba

A megkérdezett szervezetek fele (50%) találkozott adathalászattal vagy más, emberi megtévesztésre épülő social engineering módszerrel a vizsgált időszakban. A támadók hitelesnek vagy sürgetőnek tűnő üzenetekkel próbálják rávenni a munkatársakat arra, hogy érzékeny információkat adjanak át, rosszindulatú hivatkozásokat nyissanak meg vagy jogosulatlan műveleteket hajtsanak végre.

Zsarolóvírushoz kapcsolódó eseményről a válaszadók 26 százaléka, ellátási láncot érintő támadásról pedig 19 százalékuk számolt be. A vállalatoknak ezért többféle, akár párhuzamosan jelentkező fenyegetésre kell felkészülniük, amelyek a technológiai hiányosságok mellett a működési folyamatok gyenge pontjait és az emberi tévedés lehetőségét is kihasználhatják.

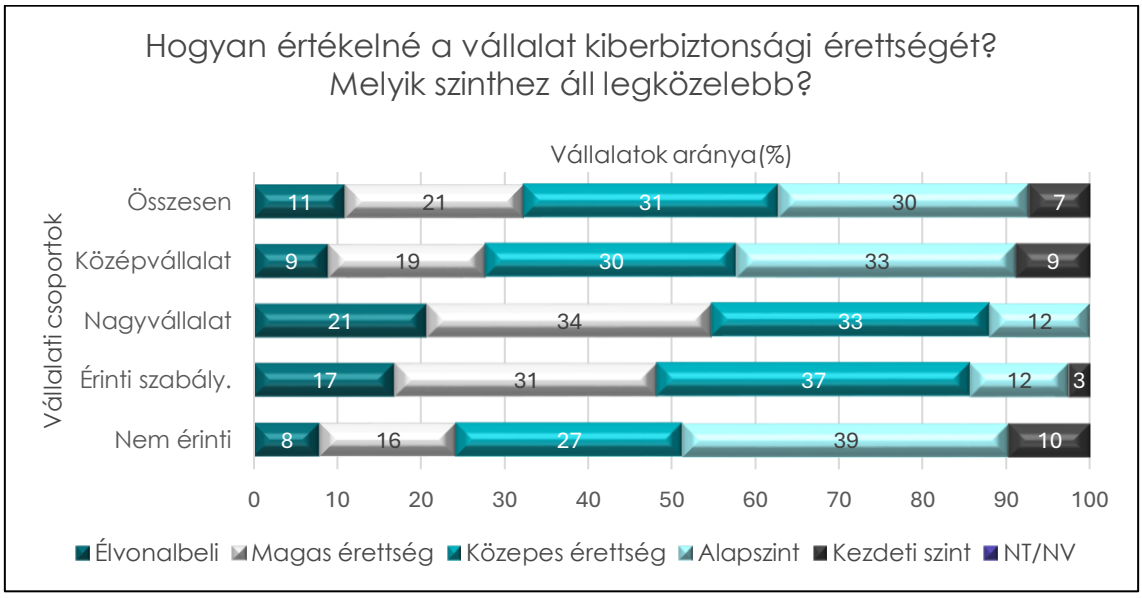


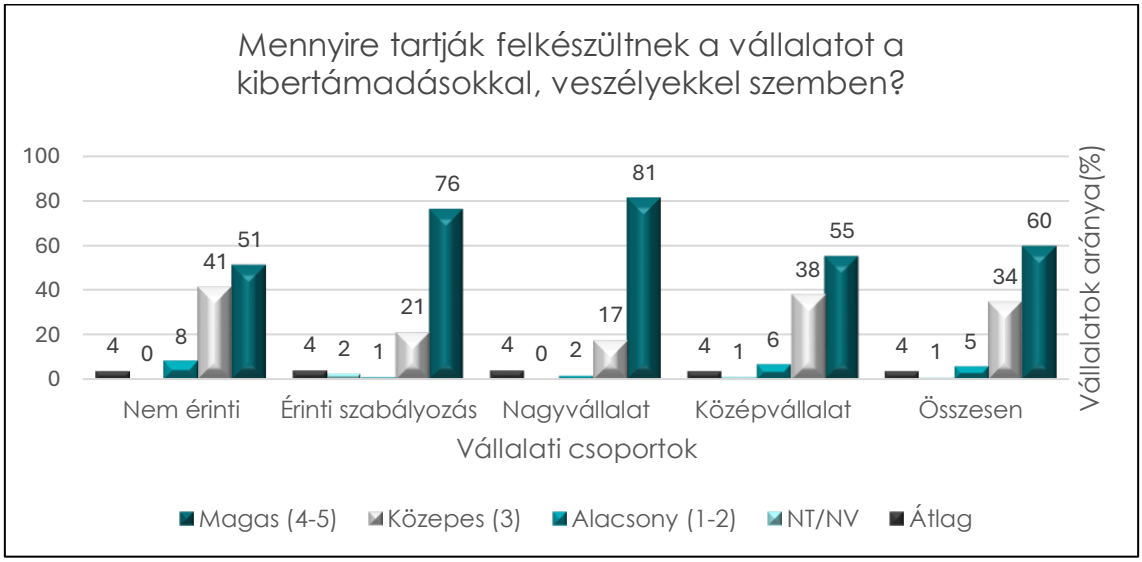
A technológiai felkészültség önmagában nem elég

A közép- és nagyvállalatok háromnegyede (75%) használ összetettebb kiberbiztonsági megoldásokat, például fejlett tűzfalat, végpontvédelmi rendszert vagy adatvesztés-megelőzési technológiát. A nagyvállalatokat tekintve pedig közel száz százalék (97%) alkalmaz legalább egy, ilyen IT-biztonsági megoldást.

Az incidenskezelési gyakorlat azonban jóval kevésbé egységes. A válaszadók közel fele (49%) eseti reakciókra vagy nem rendszeresen alkalmazott alapeljárásokra támaszkodik, további 35 százalékuk pedig dokumentált és időszakosan tesztelt folyamatokkal rendelkezik. Kiforrott, rendszeresen begyakorolt és vezetői szinten megfelelően kezelt eljárásrendről mindössze 16 százalékuk számolt be. A nagyvállalatok körében is csupán 21 százalék ez az arány.

Mindeközben a válaszadók 60 százaléka felkészültnek tartja szervezetét. Az önértékelés és az incidenskezelési érettség közötti eltérés arra utal, hogy a vállalatok sok esetben kedvezőbben ítélik meg felkészültségüket, mint amit tényleges reagálási képességük indokol. Ez hamis biztonságérzetet kelthet, és hátráltathatja a szükséges fejlesztések felismerését.





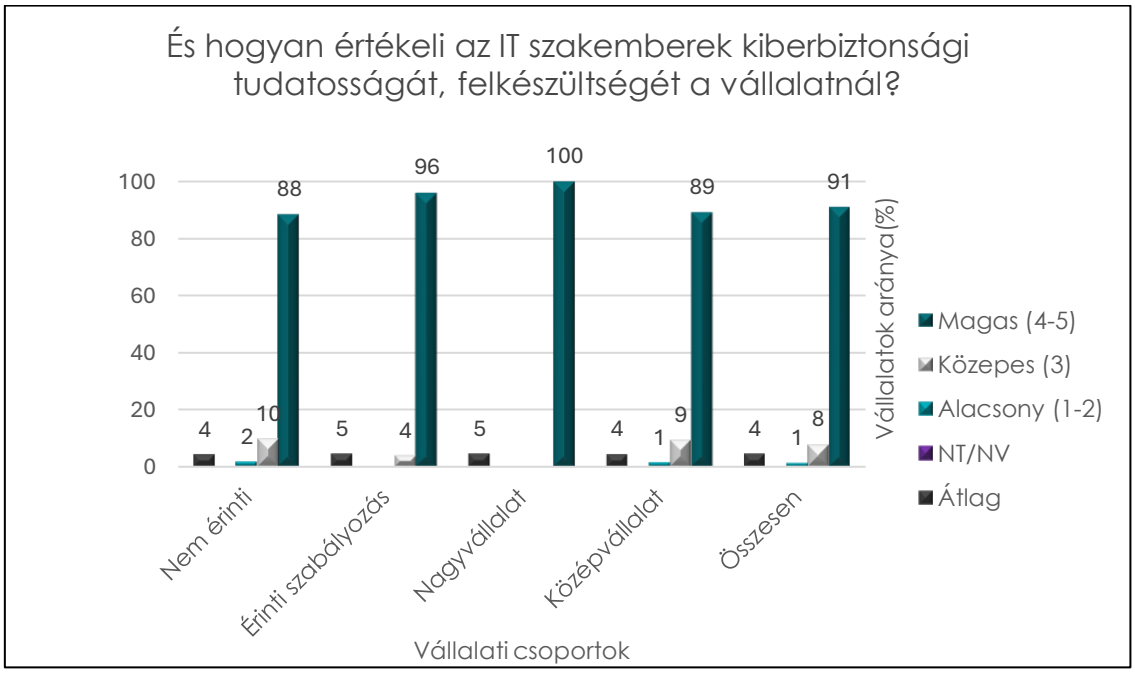
„A korszerű technológia alapvető feltétele a hatékony védekezésnek, önmagában azonban nem készít fel egy szervezetet a támadásokra. A biztonság illúziója akkor alakulhat ki, ha a vezetők az alkalmazott védelmi megoldásokból vagy a szakértői csapat tudásából teljes körű felkészültségre következtetnek, miközben a folyamatok és a döntési rend hiányosságai háttérben maradnak. A mesterséges intelligencia a védekezés lehetőségeit is bővíti, a támadók számára ugyanakkor hitelesebb és személyre szabottabb megtévesztési kísérletek létrehozását teszi lehetővé. A kiberbiztonsági megoldások akkor támogatják hatékonyan a megelőzést és a gyors reagálást, ha begyakorolt eljárások, felkészült és kritikusan gondolkodó munkatársak, valamint egyértelmű vezetői felelősségi körök kapcsolódnak hozzájuk” – mondta Marton László, a One Magyarország Zrt. vezérigazgató-helyettese, a One Solutions vállalati üzletág vezetője.

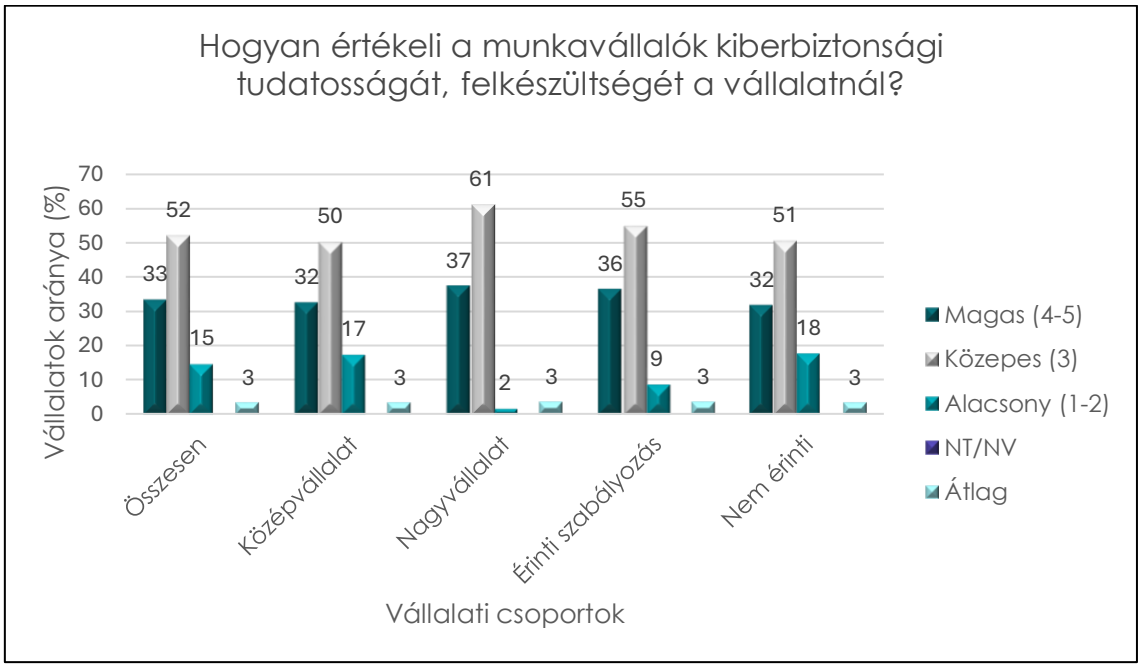
A szakértőkbe vetett bizalom nem helyettesíti a tudatos felkészülést

Az emberi tényezőt a válaszadók 51 százaléka jelentős vagy kritikus kockázatként értékeli, a nagyvállalatok körében pedig ez az arány meghaladja a 80 százalékot. Szembetűnő különbség mutatkozik ugyanakkor az informatikai szakemberek felkészültségének és a teljes munkavállalói kör biztonságtudatosságának megítélése között. Az IT-szakértők felkészültségét a vállalatok 91 százaléka értékeli magasnak, munkatársaik általános biztonságtudatosságáról azonban mindössze 33 százalékuk vélekedik hasonlóan kedvezően.

A megkérdezett szervezetek közel 90 százalékánál működik valamilyen formalizált kiberbiztonsági oktatás. A mélyinterjúk alapján ugyanakkor sok vállalatnál elsősorban a képzések elvégzését követik nyomon, és kevésbé vizsgálják, hogy ennek hatására miként változik a munkavállalók viselkedése és biztonságtudatossága.

„Az oktatás megléte még nem feltétlenül jelenti azt, hogy a munkatársak valós támadási helyzetben is felismerik a megtévesztési kísérleteket, kritikusan értékelik a kapott információkat, és megfelelően reagálnak. A képzések eredményességét ezért a teljesítés mellett a gyakorlatban mutatott reakciók alapján is érdemes mérni. A munkakörökhöz igazított tartalom, a rendszeres tudásellenőrzés és az életszerű gyakorlatok segítenek abban, hogy a munkatársak megszerzett ismereteiket a gyakorlatban is alkalmazni tudják” – tette hozzá Marton László.





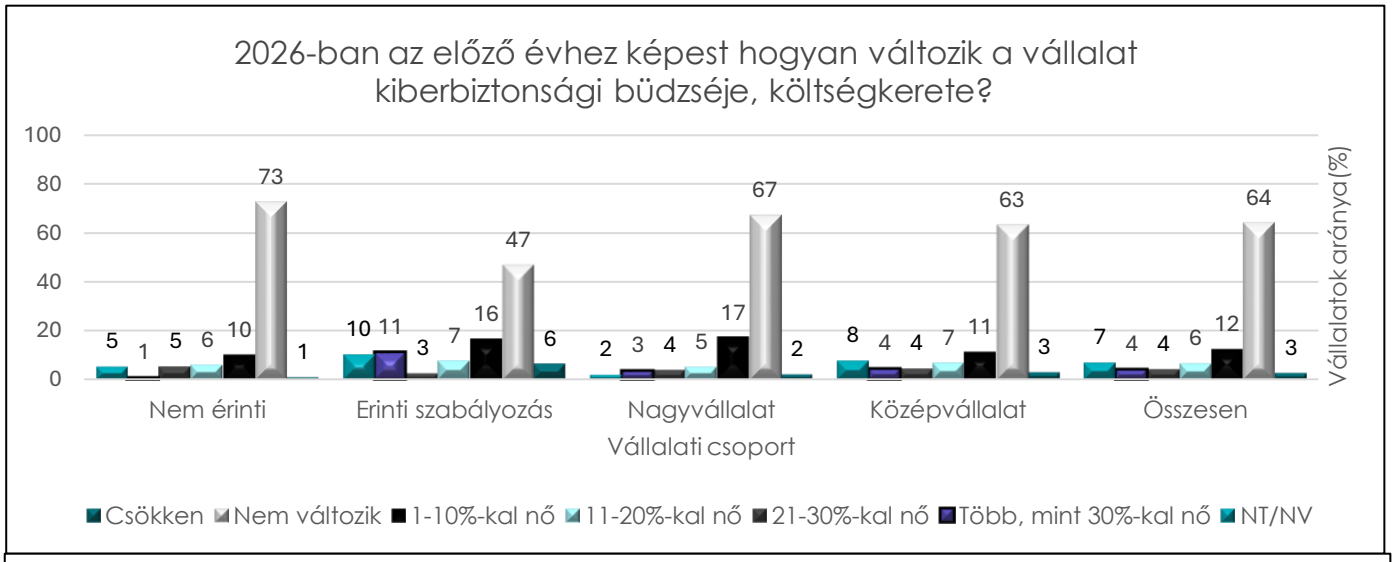
IT-biztonság mint stratégiai prioritás

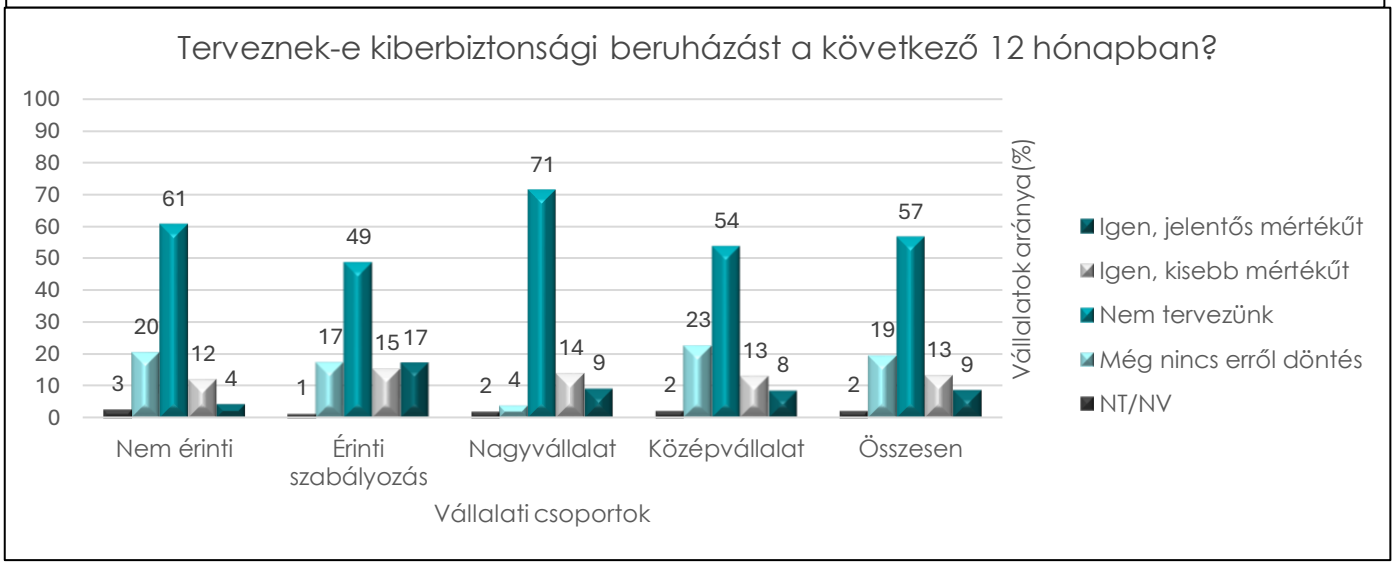
A kiberbiztonság stratégiai jelentőségét a vállalatok többsége felismerte: 68 százalékuk prioritásként tekint a területre. A szabályozás hatálya alá tartozó szervezetek körében ez az arány eléri a 85 százalékot, míg a szabályozás által nem érintett vállalatok esetében 60 százalék. A különbség arra utal, hogy a szabályozói elvárások hozzájárulhatnak a kiberbiztonság vállalati szerepének erősödéséhez és a kapcsolódó fejlesztések előmozdításához. A mélyinterjúk alapján az operatív felelősség jellemzően továbbra is az informatikai szervezetnél marad, miközben a felső vezetés sok vállalatnál nem tekinti át rendszeresen a szervezet kiberbiztonsági felkészültségét és a szükséges fejlesztéseket. A téma sok esetben egy jelentősebb beruházás, szabályozói felkészülés vagy korábbi támadás nyomán kerül a vezetés napirendjére.

„A mesterséges intelligencia terjedésével és az egyre nagyobb, üzletileg értékes adatállományok használatával párhuzamosan a vállalatok kitettsége is nő. Minél értékesebbek az adatok, annál nagyobb az érdek a megszerzésükre, és az AI a támadók eszköztárát is bővíti. Ezért a kiberbiztonságot és a munkatársak biztonságtudatosságát folyamatosan napirenden kell tartani vállalati és vezetői szinten is. Az IVSZ azért tartja fontosnak az ilyen kutatásokban való részvételt, hogy tagvállalataink és a teljes IKT-szektor pontosabb képet kapjon arról, hol tartanak ma a hazai közép- és nagyvállalatok a kiberbiztonsági felkészültség terén. Az eredmények azt mutatják, hogy még a legnagyobb, jelentős technológiai háttérrel rendelkező cégeknek is van teendőjük, különösen a tudatosság, a felkészülés és a rendszeresen gyakorolt incidenskezelés területén” – mondta Tajthy Krisztina, az IVSZ - Digitális Vállalkozások Szövetsége főtitkára.

A következő évben a vállalatok 27 százaléka számít kiberbiztonsági költségvetésének növekedésére, 64 százalékuk pedig változatlan kiadási szinttel számol. Külön beruházást ugyanakkor csak a válaszadók 22 százaléka tervez a következő 12 hónapban. A kiberbiztonság

súlya a teljes informatikai költségvetésen belül vállalatonként jelentősen eltér, ezért a kutatás alapján nem határozható meg egységes, reprezentatív arány.





A kutatás eredményei alapján a vállalatoknak a technológiai védelem mellett munkatársaik tudatosságát, incidenskezelési folyamataikat és vezetői döntési rendjüket is reálisan kell értékelniük. Ezt rendszeres állapotfelmérések, a gyakorlatban is mérhető oktatási programok és életszerű incidensgyakorlatok támogathatják. Külső szakértő bevonásakor a vállalatok számára különösen fontos a megfelelő szakmai kompetencia, a gyors rendelkezésre állás, valamint a szervezet működéséhez és kockázataihoz igazodó támogatás.

A kutatásról

A kutatást a One Magyarország Zrt. és az IVSZ – Digitális Vállalkozások Szövetsége megbízásából a BellResearch végezte 2026 márciusában. A kérdőíves adatfelvételben 202 hazai vállalat vett részt, köztük 150, 50–249 főt foglalkoztató középvállalat és 52, legalább 250 munkavállalóval rendelkező nagyvállalat. A minta alkalmazotti létszám, ágazat és régió szerint reprezentálja a

mintegy 6300 vállalkozást magában foglaló célcsoportot. A teljes minta maximális hibahatára ±6,8 százalékpont. A kvantitatív kutatást nyolc közép- és nagyvállalati döntéshozóval készített mélyinterjú egészítette ki.

One Magyarország

A One Magyarország hazánk egyik vezető telekommunikációs szolgáltatója, amely lakossági és üzleti ügyfelei számára mobil- és vezetékes távközlési, valamint informatikai szolgáltatások széles körét kínálja. Közép- és nagyvállalati üzletága, a One Solutions integrált távközlési és informatikai megoldásokkal támogatja a hazai szervezetek digitális működését. A One Magyarország több évtizedes szakmai tapasztalatot egyesít. Tevékenysége a Vodafone Magyarország és a DIGI mobil- és vezetékes adat- és hangszolgáltatásaira, az Antenna Hungária műsorgyártási és telekommunikációs hagyományára, valamint az Invitech adatközponti, felhőalapú és vezetékes távközlési megoldásaira épül. Célunk, hogy ügyfeleink mindennapjait gazdagabbá tegyük azáltal, hogy korszerű technológiai megoldásokkal támogatjuk kapcsolataik kialakítását és fenntartását. Hiszünk abban, hogy minden kapcsolatteremtési pillanat egyformán fontos, ezért szolgáltatásainkkal ezeket a pillanatokat tesszük teljesebbé. Alapértékeink közé tartozik az innovációra való törekvés és a megújulásra való képesség, valamint a megközelíthetőség és az elérhetőség, hogy ügyfeleink rendelkezésére álljunk a számukra legkényelmesebb módon és csatornán. Kiemelten fontosnak tartjuk továbbá, hogy regionális és helyi szinten is támogassuk a helyi kezdeményezéseket.

A One Magyarország a 4iG Csoport tagja.

www.one.hu

IVSZ

Az IVSZ – Digitális Vállalkozások Szövetsége a legbefolyásosabb hazai szervezet a digitális gazdaság ügyének képviseletére, az informatikai, telekommunikációs és egyéb ágazatok digitalizálódó vállalkozásainak közös érdekei alapján. Közel 300 tagvállalatunknak és számos együttműködő szakmai szervezetnek biztosítunk platformot és nyújtunk szakértő támogatást üzleti környezetük, lehetőségeik és eredményességük növelése, a teljes magyar gazdaság versenyképességének előmozdítása céljából.

www.ivsz.hu

További információ

Elkán Péter
4iG Csoport Vállalati Kapcsolatok és Kommunikációs igazgató
sajto@4ig.hu