A BIZTONSÁG ILLÚZIÓJA

Mennyire felkészült vállalata a kibertámadásokra?

Kutatás a vállalatok kiberbiztonsági tudatosságáról és felkészültségéről, 2026

ONE SOLUTIONS

IVSZ DIGITÁLIS VÁLLALKOZÁSOK SZÖVETSÉGE

BEVEZETŐ

Mit jelent valójában felkészültnek lenni?

A kiberbiztonság egyre hangsúlyosabb szerepet kap a vállalatok működésében. Technológiai védelmi megoldások, szabályozói követelmények, incidenskezelési folyamatok és munkavállalói képzések egyaránt azt szolgálják, hogy a szervezetek felkészültebben nézzenek szembe a digitális működés kockázataival.

De mit jelent valójában a felkészültség? Elegendő-e a fejlett technológiai védelem? Mennyit számítanak az előre kialakított és begyakorolt folyamatok? Milyen szerepet játszanak a munkavállalók, és hogyan jelenik meg a kiberbiztonság a vezetői döntésekben?

A One Solutions és az IVSZ közös kutatása több oldalról vizsgálta a hazai közép- és nagyvállalatok kiberbiztonsági helyzetét. A technológiai védelem mellett feltérképezte az incidensekkel kapcsolatos tapasztalatokat, az incidenskezelési gyakorlatokat, a munkavállalói biztonságtudatosságot, a vezetői prioritásokat, a költségvetési várakozásokat, valamint a belső és külső kompetenciák szerepét.

Az eredményekből összetett kép rajzolódik ki. A felkészültség egyes területei eltérő érettséget mutatnak, ezért egy szervezet kiberbiztonsági helyzete nehezen ítélhető meg egyetlen technológia, folyamat vagy mutató alapján.

A következő oldalakon azt mutatjuk be, hol tartanak a hazai közép- és nagyvállalatok, és milyen összefüggések figyelhetők meg a felkészültség különböző dimenziói között.

KITETTSÉG ÉS INCIDENSEK

A kiberbiztonsági incidensek széles körben érintik a vállalatokat

A kutatás egyik legmarkánsabb eredménye a kiberbiztonsági incidensek magas előfordulási aránya. A vizsgált közép- és nagyvállalatok 58 százaléka számolt be arról, hogy a felmérést megelőző egy évben valamilyen kiberbiztonsági incidens érte. A középvállalatok 52 százalékával szemben a nagyvállalatok 91 százaléka találkozott legalább egy ilyen eseménnyel.

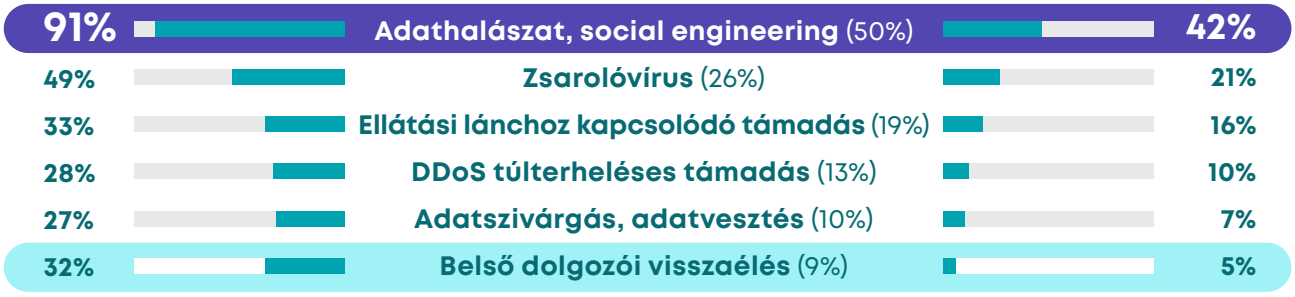
A nagyvállalatok magasabb érintettsége valamennyi vizsgált incidenstípusnál megfigyelhető. Ebben szerepet játszhat a szervezetek nagyobb mérete, összetettebb informatikai környezete és kiterjedtebb digitális kapcsolatrendszere, ugyanakkor a kutatás az eltérés okait nem vizsgálta. A nagyvállalatokat tehát gyakrabban érintik kiberbiztonsági események, de a középvállalatok 52 százalékos érintettsége is számottevő kiberbiztonsági kitettséget jelez.

Az emberi megtévesztés a leggyakoribb

A vizsgált incidensek között az adathalászat és más social engineering módszerek fordultak elő a leggyakrabban: a vállalatok fele találkozott ilyen támadási kísérlettel. A social engineering a technikai sérülékenységek mellett az emberi döntések, a bizalom és a megszokott működési rutinok kihasználására épít. A megtévesztő üzenetek célja jellemzően érzékeny információk megszerzése, rosszindulatú hivatkozások megnyitása vagy jogosulatlan műveletek végrehajtatása.

A második leggyakrabban említett kategória a zsarolóvírus kapcsolódó esemény, amellyel a vállalatok 26 százaléka találkozott. Ellátási lánchoz köthető támadásról 19 százalék, DDoS túlterheléses támadásról 13 százalék, adatszivárgásról vagy adatvesztésről 10 százalék, belső dolgozói visszaélésről pedig 9 százalék számolt be.

A vizsgált incidensek előfordulása



(Teljes mintavételből)

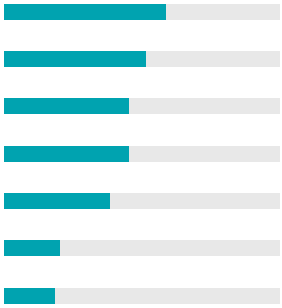
A nagyvállalatok mindegyik vizsgált incidenstípussal nagyobb arányban találkoztak. A legnagyobb eltérés a belső dolgozói visszaéléseknél mutatkozik: a nagyvállalatoknál 32, a középvállalatoknál 5 százalék az arány.

A TECHNOLÓGIAI FELKÉSZÜLTSÉG ALAPJAI

A technológiai alapok széles körben jelen vannak

A vállalati kiberbiztonság technológiai alapjai a kutatás szerint széles körben jelen vannak. A közép- és nagyvállalatok háromnegyede használ összetettebb kiberbiztonsági megoldásokat, például fejlett tűzfalat, végpontvédelmi rendszert vagy adatvesztés-megelőzési technológiát. A nagyvállalatoknál 97 százalék alkalmaz legalább egy ilyen megoldást.

Alkalmazott összetettebb kiberbiztonsági technológiák



- **59% – NGFW, fejlett tűzfal forgalomelemzéssel**
- **52% – EDR, végpontészlelési és reagálási rendszer**
- **46% – DLP, adatvesztés-megelőzés**
- **46% – Zero Trust hozzáférés-ellenőrzés**
- **39% – SIEM, biztonsági eseménykezelés**
- **20% – CTI, kiberfenyegetettségi információgyűjtés és -elemzés**
- **17% – SOC-szolgáltatás**

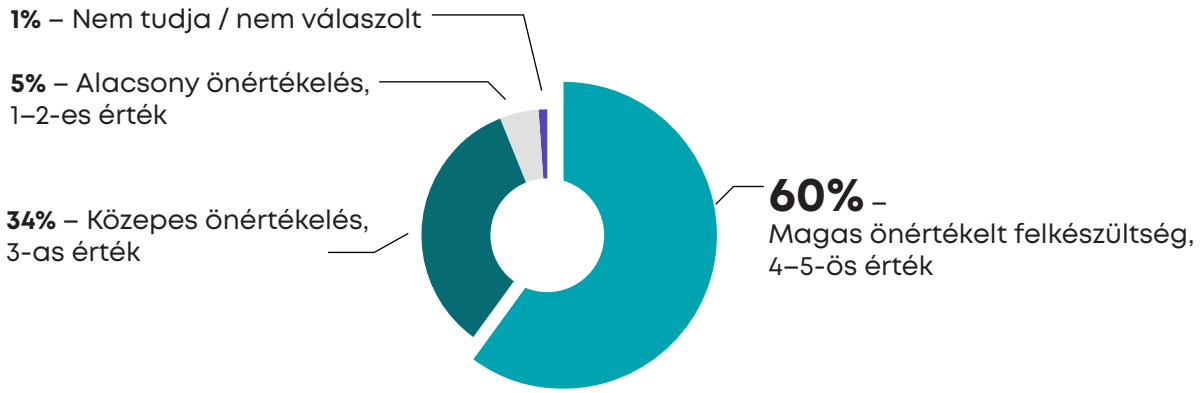
A technológiai védelem elterjedtsége fontos alap, de önmagában nem mutatja meg, hogyan reagálna a szervezet egy tényleges incidensre.

ÖNÉRTÉKELÉS ÉS KIBERBIZTONSÁGI ÉRETTSÉG

Hogyan sorolják be általános kiberbiztonsági érettségüket a vállalatok?

A vállalatok saját felkészültségüket jellemzően kedvezően ítélik meg: 60 százalékuk az ötfokú skála két felső értékének valamelyikét választotta. További 34 százalék közepesnek, 5 százalék pedig alacsonynak értékelte szervezete felkészültségét; 1 százalék nem tudott vagy nem kívánt válaszolni.

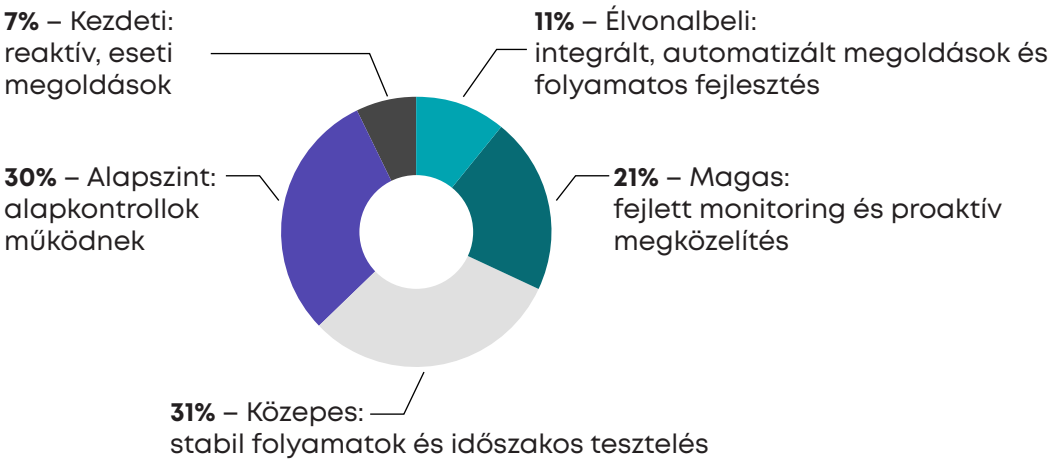
Önbesorolás az általános kiberbiztonsági érettségi szintek szerint



Az általános kiberbiztonsági érettség megítélése

A kutatás külön kérdésben vizsgálta, hogy a vállalatok melyik kiberbiztonsági érettségi szinthez érzik magukat a legközelebb. A válaszadók 11 százaléka élvonalbeli, 21 százaléka magas, 31 százaléka közepes, 30 százaléka alapszintű, 7 százaléka pedig kezdeti érettséget jelölt meg.

Általános kiberbiztonsági érettség



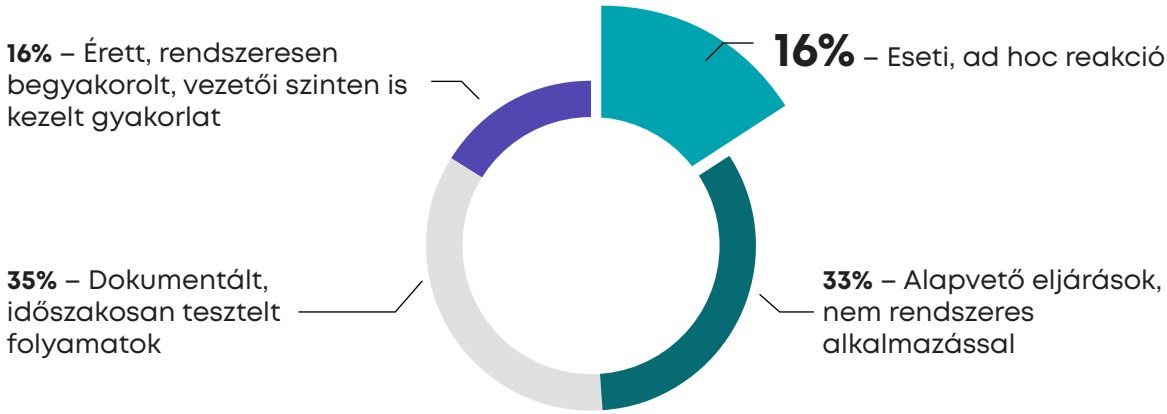
Az önértékelés a felkészültség egyik nézőpontját mutatja meg. A tényleges reagálási képesség megítéléséhez azt is vizsgálni kell, hogy a szervezet rendelkezik-e dokumentált felelősségi körökkel, rendszeresen tesztelt folyamatokkal és begyakorolt incidenskezelési eljárásokkal. A következő oldalon ezért az incidenskezelési gyakorlat érettségét mutatjuk be.

INCIDENSKEZELÉS

A reagálási gyakorlat eltérő képet mutat

A vállalatok 16 százalékánál az incidenskezelés eseti, ad hoc reakciókra épül, további 33 százaléknál pedig léteznek alapvető eljárások, de alkalmazásuk nem rendszeres. A válaszadók 35 százaléka rendelkezik dokumentált, időszakosan tesztelt folyamatokkal. Érett, rendszeresen begyakorolt és vezetői szinten is megfelelően kezelt incidenskezelési gyakorlatról 16 százalék számolt be.

Az incidenskezelési gyakorlat érettsége



A vállalatméret ezen a területen is különbséget mutat. A nagyvállalatok 61 százaléka dokumentált és időszakosan tesztelt incidenskezelési folyamatokról számolt be, az incidenskezelési skála legmagasabb szintjét pedig 21 százalékuk érte el. A középvállalatok körében az eseti és az alapszintű incidenskezelés gyakoribb.

60% ↔ 16%

Felkészültnek tartja szervezetét

Rendelkezik érett, rendszeresen begyakorolt és vezetői szinten is megfelelően kezelt incidenskezelési gyakorlattal

Az önértékelés és az incidenskezelési gyakorlat eltérő képe arra utal, hogy a felkészültség egyes dimenziói nem feltétlenül azonos szinten állnak. Ezért az általános biztonságérzetet érdemes a folyamatok és a tényleges reagálási képesség gyakorlati vizsgálatával is kiegészíteni.

A biztonság illúziója akkor alakulhat ki, ha egy szervezet a korszerű technológiákból vagy valamely területen elért fejlettségéből teljes körű felkészültségre következtet, miközben a folyamatok, a felelősségi körök vagy a döntési rend hiányosságai háttérben maradnak. Ez késleltetheti a szükséges fejlesztések felismerését.

A két adat eltérő kérdésekre adott válaszokból származik, ezért nem mutatja meg közvetlenül, hogy pontosan hány vállalat értékeli túl saját felkészültségét. Együttes vizsgálatuk ugyanakkor segít azonosítani azokat a területeket, ahol az önértékelést további állapotfelméréssel és gyakorlati teszteléssel érdemes kiegészíteni.

AZ INCIDENS ÉSZLELÉSE

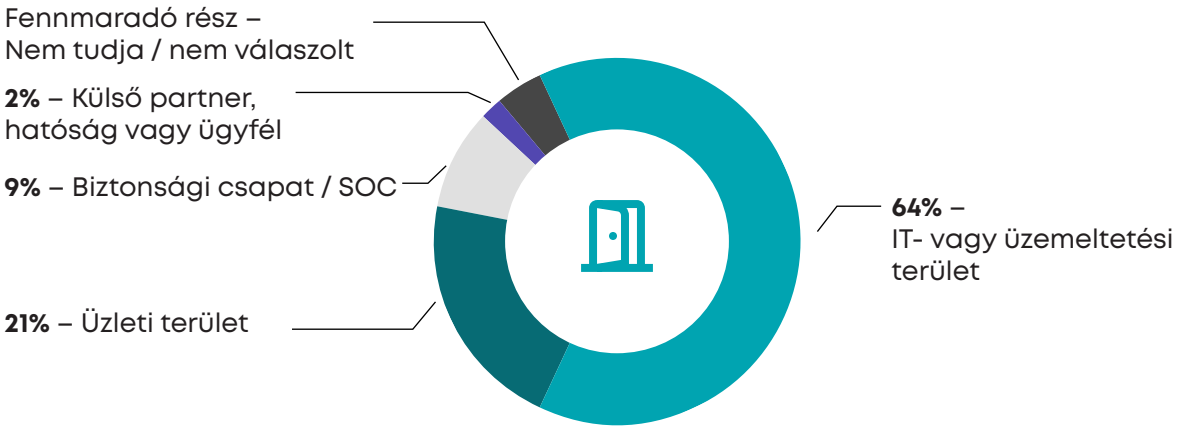
Amikor a felkészültségnek működésbe kell lépnie

Egy kiberbiztonsági incidens során a technológiai védelem mellett az is meghatározó, hogy a szervezet milyen gyorsan ismeri fel a problémát, hol válik láthatóvá az esemény, és hogyan jut el az információ azokhoz, akiknek reagálniuk kell rá. Az incidenskezelés ezért egyszerre technológiai és szervezeti képesség.

Hol válik láthatóvá egy incidens?

A kutatás arra is rákérdezett, hogy egy kiberbiztonsági esemény esetén várhatóan hol derülne ki elsőként a probléma. A válaszadók 64 százaléka az IT- vagy üzemeltetési területet jelölte meg. 21 százalék az üzleti területet nevezte meg, 9 százalék szerint pedig a biztonsági csapat vagy a SOC észlelné elsőként az eseményt.

Hol észlelnék elsőként a kiberbiztonsági eseményt?



A nagyvállalatoknál még hangsúlyosabb az informatikai terület szerepe: 85 százalékuk szerint az IT vagy az üzemeltetés észlelné elsőként az incidenst. A középvállalatoknál nagyobb szerepet kapnak az üzleti területek.

Az észlelés szervezeti kérdés is

Az eredmények arra mutatnak rá, hogy egy incidens első jelei nem kizárólag a belső biztonsági csapatnál vagy a SOC-nál jelenhetnek meg. Egy technikai rendellenességet az üzemeltetés érzékelhet, miközben egy kompromittált üzleti folyamat, gyanús tranzakció vagy szokatlan működés először valamely üzleti területen válhat láthatóvá.

Ez az incidenskezelés szempontjából különösen fontossá teszi a szervezeten belüli információáramlást. Az észlelés önmagában még csak az első lépés: az eseményt azonosítani, megfelelő szinten értékelni és szükség esetén eszkalálni is kell. Ehhez előre meghatározott felelősségi körökre és olyan folyamatokra van szükség, amelyek valós helyzetben is működőképesek.

A kiberbiztonsági felkészültség akkor válik valódi szervezeti képességgé, amikor a technológiai védelemhez egyértelmű felelősségi körök, működő információáramlás és begyakorolt incidenskezelési folyamatok kapcsolódnak.

EMBERI TÉNYEZŐ

A munkavállalói biztonságtudatosság szerepe

A kutatás alapján az emberi tényező a vállalati kiberbiztonság egyik meghatározó kockázati területe. A válaszadók 51 százaléka jelentős vagy kritikus kockázatként értékeli, a nagyvállalatok körében pedig ez az arány meghaladja a 80 százalékot. Az eredmény különösen figyelemre méltó annak fényében, hogy az adathalászat és más social engineering módszerek bizonyultak a leggyakoribb támadási formának.

A vállalatok ugyanakkor jelentős bizalommal tekintenek saját informatikai szakembereikre. 91 százalékuk magasnak értékeli az IT-szakértők felkészültségét. A teljes munkavállalói kör biztonságtudatosságának megítélése lényegesen visszafogottabb: mindössze 33 százalék értékeli magasnak.

91% ↔ 33%

Magasnak értékeli az IT-szakértők felkészültségét

Magasnak értékeli a teljes munkavállalói kör biztonságtudatosságát

A kiberbiztonsági kockázatok kezelése a szervezet jóval szélesebb körét érinti az informatikai szakembereknél. A hozzáférések kezelése, az e-mailek és üzenetek megítélése, az adatok kezelése vagy egy gyanús esemény megfelelő jelzése számos munkakör mindennapi működésének része.

A nyilvánosan megosztott információk kockázata

A One Solutions szakértői szerint a mesterséges intelligencia új dimenziót ad az emberi megtévesztésre épülő támadásoknak. A munkatársak által magánszemélyként megosztott, nyilvánosan hozzáférhető információk felhasználhatók hitelesebb és személyre szabottabb üzenetek létrehozásához. Egy támadó így a vállalati szerepkörre, szakmai kapcsolatokra vagy akár egy magánéleti eseményre hivatkozva is meggyőzőbb megkeresést készíthet. A biztonságtudatosság ezért a vállalati csatornák használatán túl a nyilvánosan megosztott információk tudatos kezelésére is kiterjed.

Az IT-szakértőkbe vetett erős bizalom nem helyettesíti a teljes munkavállalói kör biztonságtudatosságát.

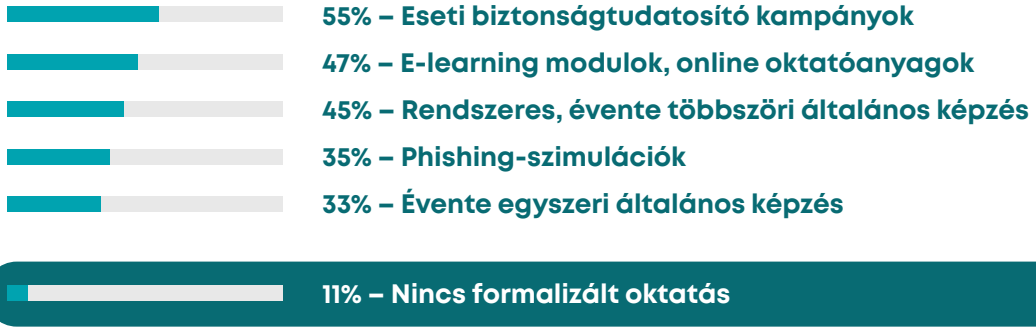
OKTATÁS ÉS GYAKORLATI FELKÉSZÍTÉS

Az oktatás széles körben jelen van

A megkérdezett szervezetek közel 90 százaléka alkalmaz valamilyen formalizált kiberbiztonsági oktatást vagy tudatosító programot. Ez arra utal, hogy a munkavállalói tudatosság fejlesztése széles körben beépült a vállalati biztonsági gyakorlatba.

90%
alkalmaz valamilyen formalizált kiberbiztonsági oktatást vagy tudatosító programot

Alkalmazott oktatási és tudatosító formák



Megjegyzés: Több válasz is megjelölhető volt.

A teljesítésen túl a gyakorlati reakció is számít

A kvantitatív eredményeket kiegészítő mélyinterjúk további összefüggésre világítottak rá. Sok szervezet elsősorban azt követi nyomon, hogy a munkatársak elvégezték-e az előírt képzést, miközben a viselkedés és a biztonságtudatosság tényleges változásának mérése kevésbé hangsúlyos. Az oktatás megléte ezért 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 a teljesítés mellett a gyakorlatban mutatott reakciók alapján is érdemes mérni. A munkakörökhöz igazított tartalom, a rendszeres tudásellenőrzés, a phishing-szimulációk és az életszerű gyakorlatok segítenek abban, hogy a munkatársak megszerzett ismereteiket a mindennapi működésben is alkalmazni tudják. A folyamatos felkészítés különösen fontos, mert a támadási módszerek és a megtévesztéshez használt technológiák is gyorsan változnak.

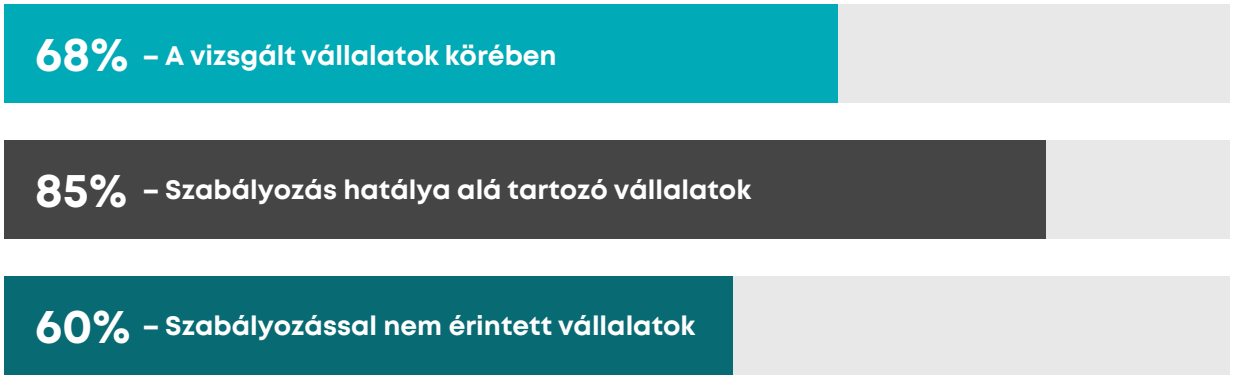
Az oktatás eredményességét a részvétel mellett az mutatja meg, hogyan reagálnak a munkatársak egy életszerű támadási helyzetben.

STRATÉGIAI ÉS VEZETŐI SZEREP

A kiberbiztonság helye a vállalati stratégiában

A megkérdezett vállalatok 68 százaléka stratégiai prioritásként tekint a kiberbiztonságra. A szabályozás hatálya alá tartozó szervezetek körében ez az arány 85 százalék, míg a szabályozással nem érintett vállalatoknál 60 százalék.

A kiberbiztonságot stratégiai prioritásként kezelő vállalatok aránya



A különbség arra utal, hogy a szabályozói elvárások hozzájárulhatnak a kiberbiztonság vállalati szerepének erősödéséhez és a kapcsolódó fejlesztések előmozdításához.

A kvalitatív kutatás árnyalja a stratégiai prioritás jelentését. A mélyinterjúkban részt vevő vállalatoknál a kiberbiztonság jellemzően az informatikai területhez kapcsolódik, miközben az üzletmenet-folytonosság fontos összetevőjeként tekintenek rá. Az operatív felelősség is többnyire az informatikai területhez kötődik, a kiberbiztonsági felkészültség rendszeres felsővezetői értékelése pedig még nem általános gyakorlat. A téma sok esetben egy jelentősebb beruházás, szabályozói felkészülés vagy korábbi támadás nyomán kerül hangsúlyosabban a vezetés napirendjére.

A kvantitatív és kvalitatív eredmények együtt arra utalnak, hogy különbség lehet a kiberbiztonság stratégiai jelentőségének felismerése és annak szervezeti megjelenése között. A terület magas prioritása önmagában nem határozza meg, hogy milyen gyakorisággal, milyen döntési szinten és milyen szervezeti struktúrában foglalkoznak vele.

A stratégiai prioritás a vezetői gyakorlatban akkor válik láthatóvá, ha a felsővezetés rendszeresen áttekinti a felkészültséget, a kockázatokat és a szükséges fejlesztéseket.

FENYEGETETTSÉGI VÁRAKOZÁSOK ÉS KÖLTSÉGVETÉS

Erősödő fenyegetések, visszafogott költségvetési tervek

A vállalatok többsége nem számít a kiberbiztonsági kockázatok enyhülésére. A válaszadók 57 százaléka úgy véli, hogy a következő egy évben tovább erősödnek a kiberfenyegetések, a nagyvállalati válaszadóknál pedig ez az arány megközelíti a 90 százalékot.

A költségvetési várakozások ennél kiegyensúlyozottabb képet mutatnak. A vállalatok 27 százaléka számít kiberbiztonsági költségvetésének növekedésére, 64 százalék változatlan költségkerettel tervez. A nagyvállalatok 29, a középvállalatok 26 százaléka vár növekedést.

Külön kiberbiztonsági beruházást a válaszadók 22 százaléka tervez a következő 12 hónapban. A kiberbiztonsági ráfordítások teljes informatikai költségvetésen belüli súlya vállalatonként jelentősen eltér, ezért egységes, reprezentatív arány nem határozható meg.

57% – A fenyegetések erősödésére számít

27% – Növekvő kiberbiztonsági költségvetéssel tervez

64% – Változatlan költségkerettel számol

22% – Külön kiberbiztonsági beruházást tervez

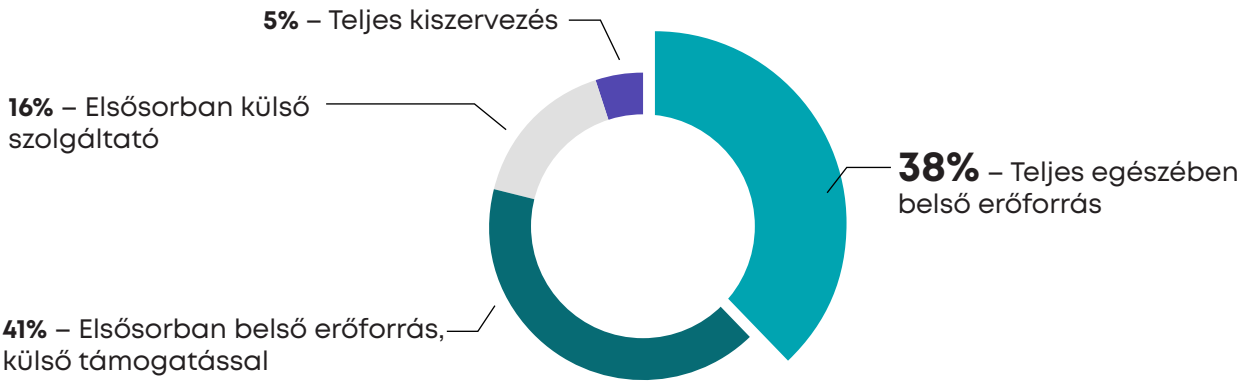
Az adatok közötti különbség figyelemre méltó, ugyanakkor önmagában nem értelmezhető finanszírozási hiányként. A fenyegetettség megítélése, az éves költségvetés változása és az egyedi beruházási tervek eltérő kérdéseket mérnek, a ráfordítások kiinduló szintje pedig vállalatonként jelentősen különbözhet.

A kvalitatív interjúk is ezt az eltérést mutatják: a kiberbiztonsági költéseket a szabályozói megfelelés, a vállalat üzleti helyzete, a meglévő technológiai környezet és az aktuális informatikai fejlesztések egyaránt alakítják.

BELSŐ ÉS KÜLSŐ KOMPETENCIÁK

A vállalatok többsége külső szakértelemre is támaszkodik

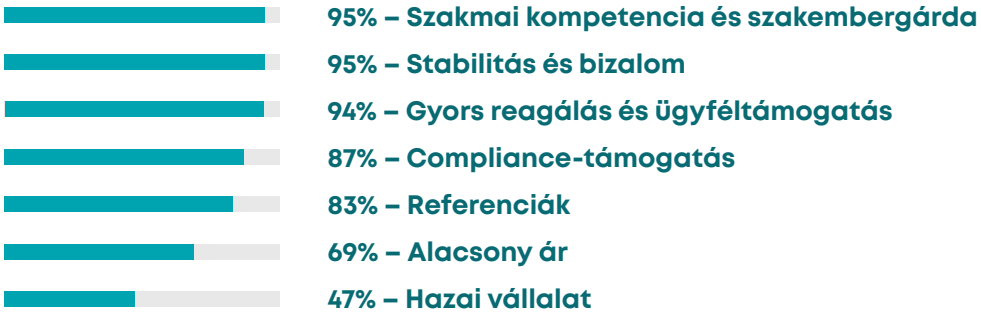
A vállalati kiberbiztonság jellemzően belső és külső kompetenciák kombinációjára épül. A vállalatok 38 százaléka teljes egészében belső erőforrással dolgozik. 41 százalék elsősorban belső szakembereire támaszkodik, külső támogatás mellett; 16 százalék elsősorban külső szolgáltatót vesz igénybe, 5 százalék pedig teljesen kiszervezi a feladatokat.



62% – Részben vagy teljes egészében külső szolgáltatóra is támaszkodik.

A középvállalatok 64 százaléka vesz igénybe külső szolgáltatót, míg a nagyvállalatoknál 50 százalék ez az arány. A nagyvállalatok fele teljes mértékben belső erőforrással kezeli a kiberbiztonsági feladatokat.

Mit várnak el a vállalatok egy kiberbiztonsági szolgáltatótól?



Megjegyzés: Az egyes szempontokat fontosnak tartók aránya; több szempont is megjelölhető volt.

A szolgáltatóválasztásban a szakmai kompetencia, a stabilitás és a bizalom, valamint a gyors reagálás és ügyféltámogatás lényegesen fontosabb szempontnak bizonyul, mint az alacsony ár. A kvalitatív interjúkban szintén a kompetencia, a megbízhatóság, a gyorsaság, a rendelkezésre állás és a felelősségvállalás jelentősége került előtérbe.

ÖSSZEGZÉS ÉS MÓDSZERTAN

Mit rajzolnak ki együtt az eredmények?

A kiberbiztonsági felkészültség nem írható le egyetlen mutatóval. A technológiai védelem fejlettsége, az incidenskezelési folyamatok érettsége, a munkavállalók biztonságtudatossága és a vezetői szerepvállalás különböző oldalról mutatják meg, hogyan képes egy szervezet reagálni a kiberbiztonsági kockázatokra.

Ezek a területek nem feltétlenül azonos ütemben fejlődnek. A fejlett technológiai védelemhez nem minden esetben társul ugyanolyan kiforrott incidenskezelési gyakorlat, a rendszeres oktatás pedig önmagában nem határozza meg a teljes munkavállalói kör biztonságtudatosságát. Hasonló különbség figyelhető meg a kiberbiztonság stratégiai jelentőségének felismerése és annak szervezeti megjelenése között.

A biztonság illúziója akkor alakulhat ki, ha a szervezet egy-egy erős területből következtet általános felkészültségére, miközben más képességek érettsége eltérő szinten áll.

A vállalati felkészültség négy meghatározó területe:

- **TECHNOLÓGIAI VÉDELEM:** a védelmi képességek technológiai alapjai.
- **INCIDENSKEZELÉS:** az észlelés, a reagálás és az eszkaláció működő folyamatai.
- **MUNKAVÁLLALÓI FELKÉSZÜLTSÉG:** a kockázatok felismeréséhez szükséges tudás és tudatosság.
- **VEZETŐI SZEREPVÁLLALÁS:** a kiberbiztonság beépülése a döntésekbe és a szervezeti működésbe.

A kutatásról

A kiberbiztonsági tudatosságot és felkészültséget vizsgáló kutatást a One Magyarország Zrt. és az IVSZ – Digitális Vállalkozások Szövetsége megbízásából a BellResearch végezte 2026 márciusában.

A kvantitatív kutatásban 202 legalább 50 főt foglalkoztató hazai vállalat vett részt: 150 középvállalat és 52 nagyvállalat. A minta alkalmazotti létszám, ágazat és régió szerint reprezentálja a mintegy 6300 vállalkozást magában foglaló célcsoportot. A teljes minta maximális mintavételi hibahatára ±6,8 százalékpont.

A kvantitatív adatfelvételt nyolc közép- és nagyvállalati döntéshozóval készített kvalitatív mélyinterjú egészítette ki. Ennek célja a vállalati döntési folyamatok, kiberbiztonsági gyakorlatok és vezetői szempontok részletesebb megértése volt.

Forrás: One Solutions – IVSZ kiberbiztonsági tudatosság és felkészültség kutatás, 2026

KEZDJÜK EL A BESZÉLGETÉST

A kutatás eredményei több olyan kérdést vetnek fel, amelyekre minden szervezetnek a saját működése, kockázatai és felkészültsége alapján kell választ adnia. Ha szeretné szakértőinkkel áttekinteni, mit jelentenek ezek az eredmények vállalata számára, szakértői konzultáció keretében közösen is megvizsgálhatjuk a legfontosabb kérdéseket.

VEGYE FEL A KAPCSOLATOT KIBERBIZTONSÁGI SZAKÉRTŐNKKEL!

Egy körben a megoldás.

ONE SOLUTIONS

Kutatási partner:
BellResearch

IVSZ DIGITÁLIS VÁLLALKOZÁSOK SZÖVETSÉGE