CSO

Microsoft Security

SZPONZORÁLT TARTALOM

Zero Trust Security: **Tanulságok az első felhasználóktól**

CSO Microsoft Security

Tartalom

- Bevezetés
- A Zero Trust beváltja a hozzá fűzött ígéretet
- A Zero Trust bevezetését ösztönző tényezők
- Számtalan fenyegetés
- A Zero Trust bevezetésének akadályai
- A bevezetéssel kapcsolatos kihívások
- Bevált gyakorlatok a Zero Trust bevezetéséhez
- Ön hol jár a Zero Trust felé vezető úton?

CSO Microsoft Security

Bevezetés

Az elmúlt két év viszontagságai alaposan felrázták a hagyományos IT- és biztonsági modellek világát. A Zero Trust Security így érdekes elképzelésből gyorsan a modern vállalati biztonság egyik fontos alappillérévé fejlődött.

A Foundry új kutatásából kiderül, hogy a vállalatok 52%-a már bevezette (vagy jelenleg teszteli) a Zero Trust architektúrát, további 15% pedig a Zero Trust modellek vizsgálatán dolgozik. Ezek a cégek számos előnyről számolnak be a bevezetés óta: az ügyféladatok hatékonyabb védelmet élveznek, csökkent a komplexitás, és a dolgozók megbízható, biztonságos hozzáférést élveznek a vállalati erőforrásokhoz.

Ebben az e-könyvben megismerkedünk a Foundry kutatásának eredményeivel, amelyek aláhúzzák, milyen sokat segíthet a Zero Trust stratégia az IT-biztonsági vezetőknek, akiknek számtalan támadási vektorral és kockázattal szemben kell megvédeniük vállalatukat. A könyv emellett útmutatást nyújt a Zero Trust bevezetéséhez azoknak, akik még az út elején járnak.

A felmérésről

A Foundry egyesült államokbeli cégeket kérdezett meg 2022. február és március között a Zero Trust modell bevezetésének állapotáról. Legalább 500 főt foglalkoztató vállalatok olyan IT-menedzsereivel beszéltek, akiknek szerepük van a kiberbiztonsági termékek és szolgáltatások beszerzésében.

A 23 kérdésből álló kérdőívre összesen 250-en adtak választ.

CSO Microsoft Security

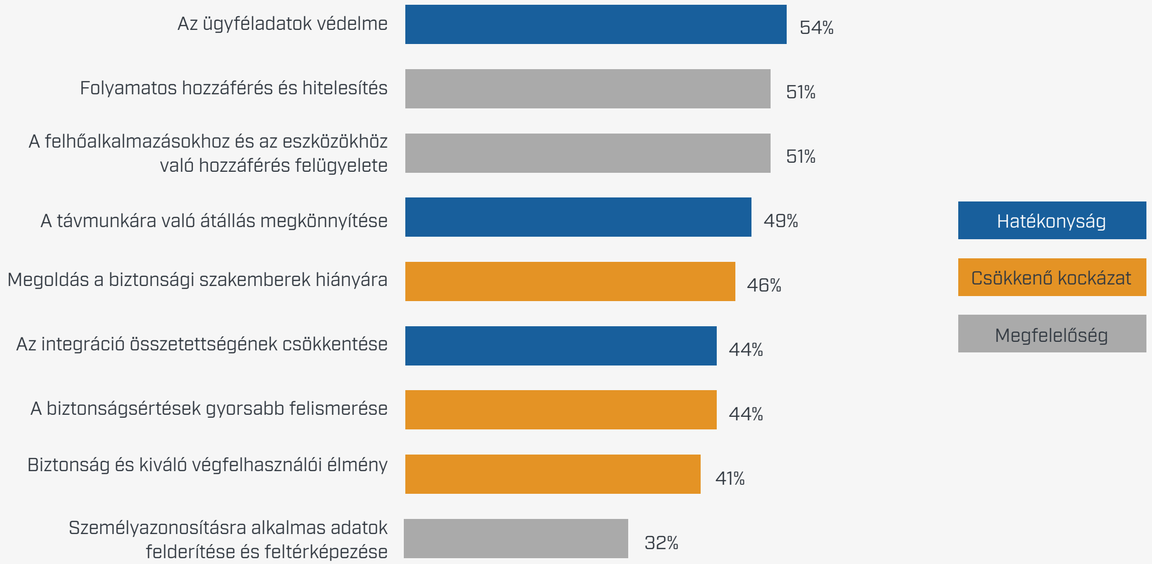
A Zero Trust beváltja a hozzá fűzött ígéretet

A felmérésből és az IT- és biztonsági vezetőkkel folytatott mélyinterjúkból egyértelműen kiderül, hogy a legtöbb vállalatot foglalkoztatják a Zero Trustban rejlő lehetőségek. Azok pedig, akik már bevezették a Zero Trust különböző elemeit, már élvezik is ennek előnyeit.

A Zero Trust modellt bevezető válaszadók nagy többsége (87%) úgy véli, hogy az architektúra teljesíti, sőt meg is haladja az implementáció, a bevezetés és az integráció terén eredetileg kitűzött célokat.

„A Zero Trust nálunk bevett működési móddá vált. Nem hiszem, hogy valaha is visszatérünk a régi módszerekhez” – magyarázza egy globális kiskereskedelmi cég IT-igazgatója. (A válaszadók nevét nem közöljük, hogy szabadon beszélhessenek cégük biztonsági terveiről.)

A Zero Trust bevezetése óta elért előnyök



12% a válaszadók közül az *összes* fenti előnyt élvezi

Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 250

CSO Microsoft Security

A válaszadók 44%-a emellett arról is beszámolt, hogy a Zero Trust segítségével csökkent az integrált biztonsági architektúra bevezetésével általában együtt járó komplexitás. „Mivel rendelkezésre áll egy kész keretrendszer, sokkal egyszerűbb dolgunk van” – mutat rá egy 3500 főt foglalkoztató ügyfélszolgálati cég IT-biztonsági vezetője.

Egy 17 000 fős pénzügyi szolgáltató cég alelnöke és IT-biztonsági vezetője arról számol be, hogy a Zero Trust keretében bevezetett többfaktoros hitelesítés rendkívül népszerű a munkatársak körében. „Sokat hozzátett a dolgozói elégedettséghez, mivel ennek a megoldásnak köszönhetően már nem kell a céges gépet, sem VPN-klienst használni: bárhonnan elérik a szükséges erőforrásokat” – magyarázza.

A legkisebb jogosultság elvének alkalmazása is hasznosnak bizonyult a biztonsági vezető szerint. „A rendszergazdák kevesebb katasztrofális hibát vétenek, mióta bevezettük a jogosultságok korlátozására épülő rendszert – mondja. – Csak konkrét feladatokhoz és időtartamokra osztjuk ki az engedélyeket, így kisebb a hibák kockázata.”

Az adathalászat és más kibertámadások terjedésének időszakában a kiskereskedelmi cég IT-igazgatója így foglalja össze a Zero Trust előnyeit: „Ha nem férnénk hozzá ezekhez az eszközökhöz, valószínűleg nehéz helyzetben lennénk, és akár már most is zsarolóknak kellene fizetnünk bitcoinban”.

CSO Microsoft Security

A Zero Trust bevezetését ösztönző tényezők

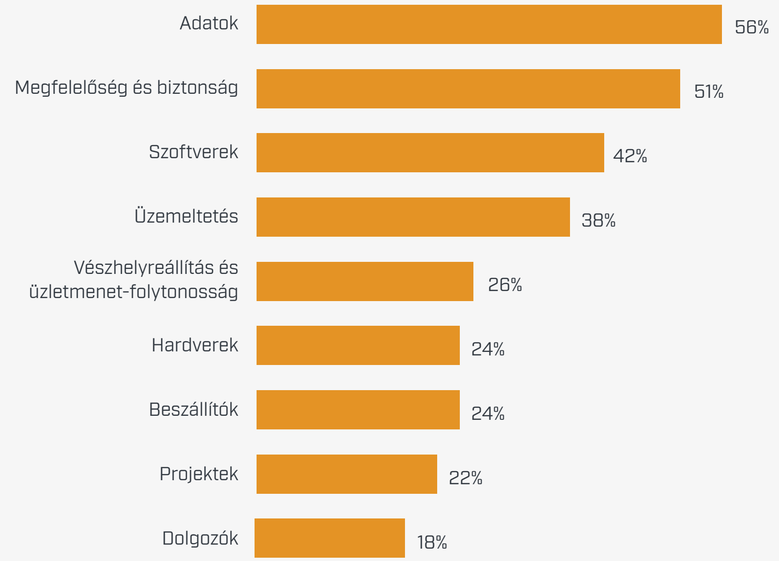
Számos körülmény együttállása ösztönzi arra a vállalatokat, hogy legalábbis megfontolják a Zero Trust architektúra bevezetését. A lista első helyén az áll, hogy a cégeknek rengeteg erőforrásra irányuló számos különböző fenyegetés jelentette kockázatokat kell kezelniük. A válaszadók számos különböző okra vezették vissza az előző évi biztonsági incidenseket, amelyek között a cégen kívüli személyek és szervezetek által okozott biztonsági sérülékenységek álltak az első helyen. Néhány további ok, amelyet megemlítettek:

- Váratlan üzleti kockázatok
- Szolgáltatások vagy rendszerek helytelen konfigurálása
- Rosszindulatú belső személyek támadásai
- Nem szándékos felhasználói hibák, például adathalászok áldozatává vált dolgozók
- Jogosulatlan kézbe került identitások
- Szoftveres javítások telepítésének elmulasztása
- Ellopott hitelesítő adatok

Ezek az incidensek számos különböző kockázattal járnak, különösen az adatok terén.

A világjárvány hatására számos cégnek gyorsan át kellett állnia a távmunkára, ami tovább sürgette a Zero Trust bevezetését, hiszen a hagyományos, hálózatperemen alapuló biztonsági modellek elavulttá váltak. Sok vállalat már korábban is ebbe az irányba haladt, hiszen egyre több alkalmazást és IT-infrastruktúrát költöztetett a felhőbe. A világjárvány azonban lendületet adott a folyamatnak.

A kiberfenyegetéseknek leginkább kitett területek



Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 250

CSO Microsoft Security

Egy 1700 dolgozót foglalkoztató egészségügyi technológiai vállalat IT-biztonsági igazgatója úgy fogalmaz, hogy a felhőmigráció és a világjárvány nagyban befolyásolták a Zero Trust bevezetését, amely bármilyen jövőbeni munkahelyi modellhez biztonságos alapot teremt.

„Az üzleti hajtóerő az volt, hogy felhőalapú vállalat lévén képesnek kell lennünk a környezetünk védelmére – mutat rá. – Emellett a világjárvány során lehetővé kellett tennünk a hatékony távmunkát. A Zero Trust segítségével jelentősen csökkentettük irodaterületünket, és valószínűleg a jövőben is legalább 60%-ban virtuálisan, távmunkában dolgozó cég leszünk.”

CSO Microsoft Security

Számtalan fenyegetés

A megfelelőségi igények is ösztönzést nyújtottak az átfogóbb biztonsági modellek kialakításához. „A szabályozók rajtunk tartják a szemüket, és elvárják, hogy egyre fejlettebb biztonsági keretrendszert alakítsunk ki” – magyarázza egy 290 000 dolgozóval rendelkező pénzügyi szolgáltató vállalat senior globális információbiztonsági alelnöke.

Egyes vállalatok proaktív lépéseket tettek a Zero Trust bevezetése érdekében, hogy elkerüljék a súlyos incidenseket, amelyek általában komoly negatív hírverést generálnak. „Számunkra az volt a fontos, hogy megelőzzük a bajt, és ne kerüljünk be a hírekbe – magyarázza egy 3500 főt foglalkoztató felsőoktatási intézmény IT-vezetője. – Sok rémisztő történetet hallottunk hozzánk hasonló méretű helyi intézményekről, amelyeknek hosszú időre leálltak a rendszerei.”

Mások már megtapasztalták, milyen hatása van a súlyos kiberbiztonsági incidenseknek, és ennek hatására elhatározták, hogy gyorsan átalakítják biztonsági stratégiájukat. Miután egy 6000 dolgozóval rendelkező biztosítótársaság zsarolótámadás áldozatává vált, amely két hétre leállította a vállalat hálózatát, a vezérigazgató döntésére azonnal megkezdődött a Zero Trust bevezetése. „A lehető leggyorsabban dolgoztunk az implementáción – magyarázza a cég IT-fejlesztésért felelős alelnöke. – Kezdetben a bevált gyakorlatokra koncentráltunk, de a zsarolótámadást követően minden folyamat felgyorsult.”

Felhőalapú hajtóerő

Egy jelentős pénzügyi szolgáltató vállalat alelnöke és IT-biztonsági vezetője úgy fogalmaz, hogy csapata már évekkel ezelőtt felismerte, hogy a felhőalapú erőforrások bevezetése és az egyre mobilisabb felhasználói kör miatt új biztonsági architektúrára van szükség.

„Beláttuk, hogy az erőforrások elhatárolását célzó hagyományos módszerek a jövőben nem fognak kellő védelmet nyújtani a támadókkal szemben” – emlékszik vissza.

Ez a feltevés 2020 elején bizonyítást is nyert, amikor a vállalat felfedezte, hogy az előző év során egy támadó átjutott a védővonalakon, és azóta is észrevétlenül mozgott a rendszerekben. „Új architektúrára volt szükségünk, amellyel megvédhetjük az erőforrásokat és hitelesíthetjük a használatukat, legyenek bárhol. A Zero Trust pontosan erre szolgál.”

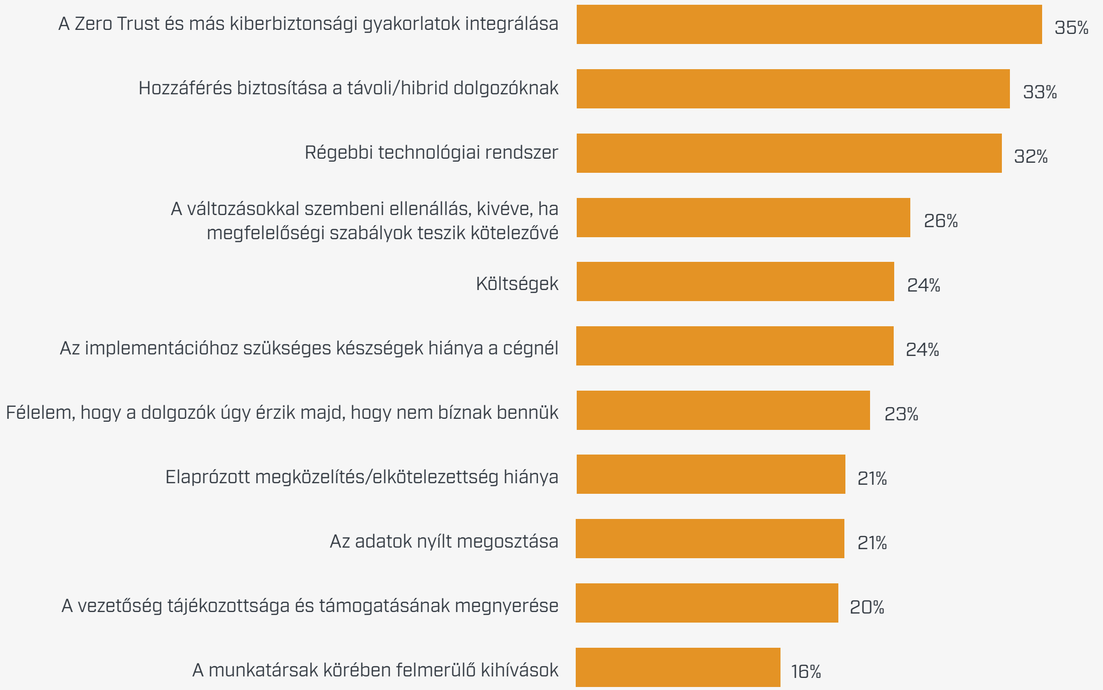
CSO Microsoft Security

A Zero Trust bevezetésének akadályai

A Zero Trust számos cég számára alapvető változást jelent a biztonsági struktúra, folyamatok és megközelítés terén – ez magyarázatot ad arra, hogy milyen akadályokat kell sokaknak leküzdeni a bevezetéséhez.

„Számtalan, egymástól elszigetelt rendszer nehezítette a dolgunkat – mutat rá az ügyfélszolgálati cég IT-igazgatója: a szerverekkel, a hálózattal és az adatbázisokkal foglalkozó csapatok mind saját webszervereket és eszközöket használtak. – Ez lelassította a folyamatot, mivel mindenkinek más elképzelése volt a célokról és azok elérésének módjáról.”

Milyen tényezők nehezítik a Zero Trust bevezetését?



Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 250

CSO Microsoft Security

A Zero Trust bevezetésének egyik pozitív mellékhatása lehet, hogy napvilágra hozza az ilyen problémákat – véli Anthony Mocny, a Microsoft Zero Trustért felelős senior marketingmenedzsere. „A Zero Trust architektúra célja, hogy megszüntesse a cég különböző technológiai pilléreiért felelős biztonsági csapatok elszigeteltségét, és így erősítse a kohéziót – magyarázza. -Ez egyben kulturális változást, a csapatok együttműködési módszereinek átalakítását is jelentheti."

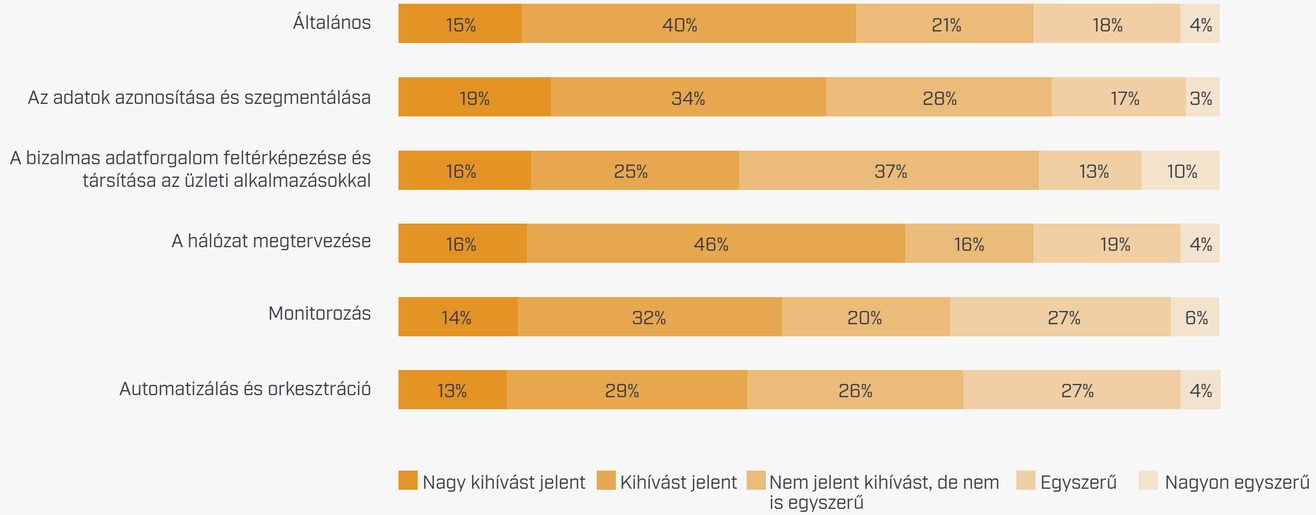
A pénzügyi szolgáltató cég alelnöke/IT-biztonsági igazgatója számára a régebbi alkalmazások jelentették a legnagyobb akadályt a Zero Trust felé vezető úton. „Modern hitelesítési technológiát kellett beépítenünk ezekbe a megoldásokba – mondja. – A régebbi alkalmazások esetében ez közel sem volt egyszerű feladat.”

CSO Microsoft Security

A bevezetéssel kapcsolatos kihívások

Amikor a vállalatok belefogtak a Zero Trust bevezetésébe, számos kihívással találták szembe magukat. A válaszadók több mint fele (56%) kihívásként vagy komoly kihívásként élte meg a Zero Trust implementációját. Különösen a következőket:

Mekkora kihívást jelent a Zero Trust bevezetése?



Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 168

CSO Microsoft Security

A részletes beszélgetések során gyakran felmerültek a szegmentálással és a mikroszegmentálással kapcsolatos kihívások.

„Egészen az egyes hosztok szintjéig szegmentálni kell a hálózatot – magyarázza a pénzügyi szolgáltató cég alelnöke/IT-igazgatója. – Mintha a belső hálózaton minden egyes hoszt közé kisebb tűzfalakat húznánk fel, hogy megfigyelhessük és akár az egyes gépeken is szabályozhassuk a forgalmat. Ez komoly biztonsági előnyökkel jár, de rendkívül nehéz megvalósítani, mivel gyakorlatilag több tízezer tűzfalat kell menedzselni.”

A forgalom áramlásának feltérképezése is többhónapos művelet lehet. Egy 5000 főt foglalkoztató kiadó- és médiavállalat technológiai igazgatója beszámolt róla, hogy a legfontosabb védendő adatok, alkalmazások és hálózati szolgáltatások meghatározása után „feltérképeztük a hálózatban folyó tranzakciókat, és megpróbáltuk információcsoportként értelmezni őket. Ezt követően szegmentáltuk az információk bizonyos részeit, és megvizsgáltuk, hogyan haladnak végig a hálózaton, egészen az önálló csomagok szintjéig.” A vállalat ekkor Zero Trust-szabályzatokat alkalmazott a különböző típusú forgalomáramlásokra. „Emellett új funkciókat építettünk ki a hálózat monitorozásához és karbantartásához.”

A kihívások ellenére számos válaszadó úgy véli, hogy a Zero Trust valójában egyszerűbbé tette a mindennapi működést. A hagyományos technológiákkal „több napba telik, mire elvégezzük a módosításokat, hiszen az összes hardver- és szoftverkomponensre le kell küldeni őket, és ez rengeteg erőforrást igényel – magyarázta a pénzügyi szolgáltató cég globális információbiztonsági alelnöke. – A Zero Trust ezzel szemben hosszú távon minimalizálja az architektúra összetettségét, így kevesebb munkatárs is el tudja végezni ugyanazt a munkát.”

Bevált gyakorlatok a Zero Trust bevezetéséhez

Egyre több vállalat vezet be Zero Trust architektúrát, és sok közülük útvonalterveket és bevált gyakorlatokat is kidolgoz, amelyeket mások is követhetnek. A bevezetés megtervezése során érdemes figyelembe venni az alábbi öt tényezőt:

Ne vállaljon elsőre túl sokat!

A Zero Trust stratégia kidolgozása túl nagy falatnak tűnhet, ha csak arra gondolunk, hogy minden hálózat, adat, alkalmazás, identitás, végpont és infrastruktúra kapcsán át kell dolgozni a szabályzatokat és a védelmi intézkedéseket. „Kezdetben mindez megoldhatatlanul nagy feladatnak tűnt, és felmerült bennünk, hogy nem fogjuk tudni teljesíteni – emlékszik vissza a felsőoktatási IT-igazgató. – Ezért fontos, hogy lépésről lépésre haladjunk.”

Az IT-igazgató és csapata végül a „kövesd a pénzt” elvet követte: elsőként a pénzügyi és bérszámfejtési alkalmazásokat szegmentálták egy különálló hálózaton.

Mocny szerint érdemes a legfontosabb védeni kívánt erőforrások azonosításával kezdeni. „Nem szabad elfelejteni, hogy miért döntöttünk a Zero Trust bevezetése mellett” – mutat rá.

Ha nem biztos a dolgában, kezdje a többfaktoros hitelesítéssel!

A biztonsági képességek rangsorolásakor számos IT-biztonsági szakember és szolgáltató javasolja, hogy kezdetben fókuszáljunk a hitelesítésre és a többi identitásalapú védelmi mechanizmusra. „Ha nem tudják biztosan, hogy mivel kezdjenek, a többfaktoros hitelesítéssel nem hibázhatnak túl nagyot” – véli Mocny.

A Microsoft becslései szerint a többfaktoros hitelesítéssel az identitásalapú támadások több mint 90%-a megelőzhető.

A pénzügyi szolgáltató cég alelnöke/IT-biztonsági igazgatója is egyetért. „A hitelesítés a Zero Trust architektúra megvalósításának egyik alapeleme. Ha nincs megoldva a végfelhasználók identitásának ellenőrzése, a többi komponens sem fog működni, ezért érdemes ezzel kezdeni.”

A pénzügyi szolgáltató cég alelnöke/IT-igazgatója ezt követően a hálózati komponenst vette célba, amely azonnali előnyöket nyújtott a távmunkások támogatása terén. A csapat későbbre hagyta a mikroszegmentálást, mivel ennek nincs olyan látványos hatása a vállalat egészében. „Ez a művelet nagyban fokozza a biztonságot, de ezt általában nem sokan veszik észre” – magyarázza.

CSO Microsoft Security

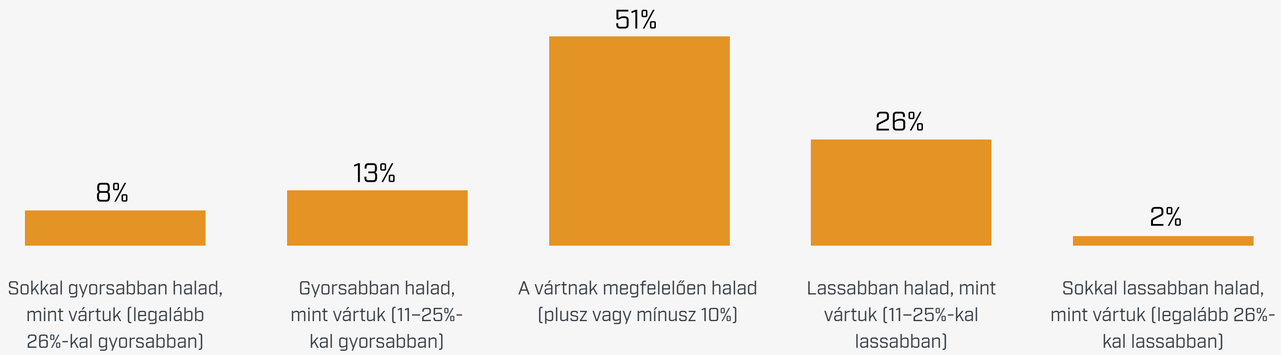
Tűzzön ki realisztikus határidőket!

Fontos, hogy az IT-biztonsági vezetők megvalósítható elvárásokat tűzzenek ki a Zero Trust bevezetése kapcsán. „A Zero Trust architektúra bevezetése inkább program, mint projekt – véli a pénzügyi szolgáltató cég alelnöke/IT-igazgatója. – Ez hatalmas változást jelentett számunkra. A helyes megvalósításhoz sok projektre lesz szükség, és a folyamat valószínűleg éveken át tart majd. A Zero Trust architektúra bevezetésének nincs gyors és egyszerű módja."

A pénzügyi cég senior alelnöke is így gondolja. „Tulajdonképpen soha nem leszünk készen, hiszen mindig újabb technológiák jelennek meg, újabb rosszindulatú szoftverek, fenyegetések tűnnek fel" – véli.

A válaszadók többsége (72%) úgy fogalmaz, hogy a bevezetés a tervek szerint vagy a vártnál gyorsabban halad, a többieknél azonban az implementáció lassabb a vártnál.

Az előzetes ütemtervnek megfelelően halad a Zero Trust bevezetése?



Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 168

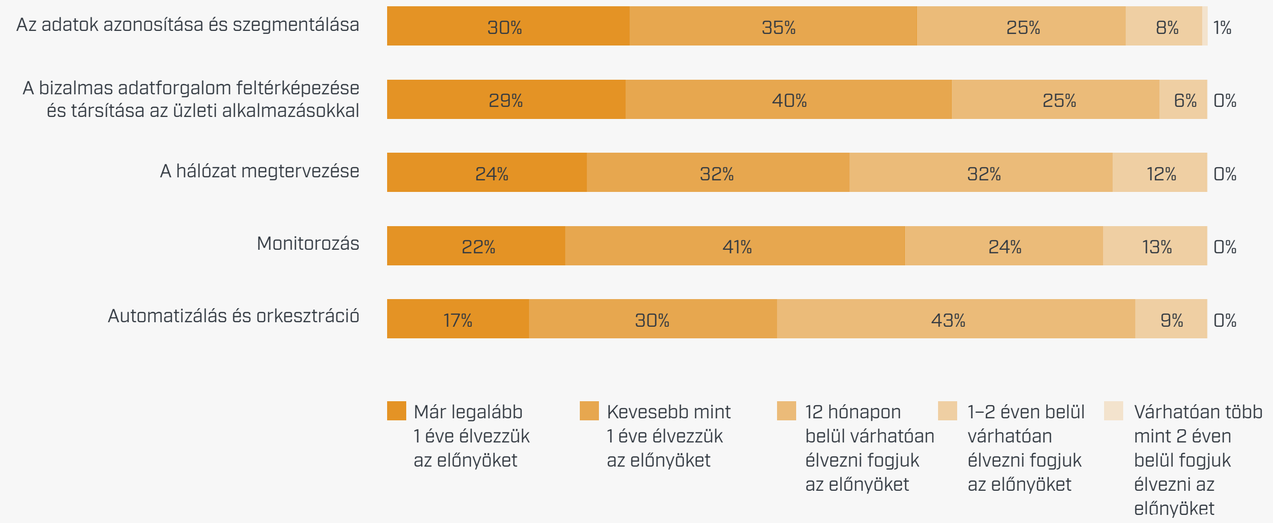
CSO Microsoft Security

Fontosak a folyamatos mérések

A Zero Trust bevezetése ugyan hosszú távú folyamat, de fontos, hogy az IT-biztonsági vezetők mérföldköveket határozzanak meg az előrehaladás méréséhez. Jó jel, hogy a válaszadók körülbelül kétharmada úgy fogalmazott, hogy a projekt legtöbb területén kevesebb mint egy év alatt sikerült elérni bizonyos előnyöket, és további egynegyedük szerint ez 12 hónapon belül várható. Ebbe beletartoznak az olyan fontos tevékenységek, mint az adatok azonosítása és szegmentálása, a forgalom feltérképezése és a hálózat megtervezése.

„A Zero Trust bevezetése leginkább egy utazáshoz hasonló, de út közben folyamatosan fel kell mérnünk, hogy hol tartunk, hogy megfelelően védekezhessünk a változó támadásokkal szemben” – fogalmaz Mocny. „Mindig keresnünk kell a fejlődés lehetőségét.”

A Zero Trust előnyeinek eléréséhez szükséges idő



Forrás: Zero Trust Adoption Survey, 2022. március, Foundry. Megkérdezettek száma: 103

CSO Microsoft Security

Foglalkozzon az emberekkel, ne csak a technológiával!

A Zero Trust Security modell átfogó jellege miatt minden dolgozóra hatással lesz, beleértve a megvalósításával megbízott IT- és biztonsági csapatokat is. Ezért mint minden nagy léptékű technológiai projektnél, itt is fontos, hogy a bevezetést megfelelő új folyamatok és változáskezelési gyakorlatok kísérjék, mivel ezek feltétlenül szükségesek a zökkenőmentes és sikeres megvalósításhoz.

„Ez nem csupán technológiai, hanem kulturális változás is egyben – mutat rá Mocny. – Ha több csapat is foglalkozik a biztonsággal (például hálózati architectek és identitáskezelési szakértők), akkor a közöttük fennálló együttműködést is át kell alakítani. Le kell bontani a korlátokat, hogy minden technológia hatékonyan működhessen.”

Az elszigetelt rendszerek felszámolásához minden szakembert be kell vonni a próbaprojektekbe és a koncepció igazolásába. Egy körülbelül 2000 fős telekommunikációs vállalat IT-rendszerekért felelős igazgatója akkor látta ezt be, amikor a bevezetés során számos területen kritikus meghibásodási pontokat fedeztek fel: egyes szolgáltatásoknál nem működött a hitelesítés, ezért hirtelen „megbízhatatlanná” és – más rendszerekkel együtt – elérhetetlenné váltak.

„A szolgáltatások bevezetése dominóhatást válthat ki, és elronthatja mások működését” – magyarázza. A jövőben „sokkal óvatosabban fogunk eljárni: a bevezetés előtt több időt fordítunk majd a koncepcióigazolásra, több értékelést és architektúra-ellenőrzést fogunk végezni különféle témaszakértők részvételével”.

A Zero Trust megtérülése

A Forrester Consulting 2021-es **megbízásából készült Forrester Consulting Total Economic Impact™ tanulmánya** számszerűsítette a Microsoft Zero Trust megoldásaival elérhető költségmegtakarításokat és üzleti előnyöket. A Forrester által megkérdezett öt nagyvállalat alapján kidolgozott kompozit szervezet három év alatt 92%-os megtérülést ért el a Microsoft Zero Trust architektúra bevezetésével.

Ez a kompozit cég emellett átlagosan 20 USD-t takarított meg havonta és dolgozónként a Zero Trustnak köszönhetően redundánssá váló biztonsági eszközök, például a végpontok felügyelete, a vírusvédelmi és kártevőírtó megoldások kivezetésével.

CSO Microsoft Security

Ön hol jár a Zero Trust felé vezető úton?

A felmérés alapján a Zero Trust Security modell előnyei egyértelműen megérik az IT-biztonsági vezetők és csapataik által a bevezetés során tapasztalt kihívások leküzdését. Ha a vállalat alaposan kidolgozott tervekkel vág neki e kihívások leküzdésének, rövid idő alatt továbbfejlesztheti a biztonságát, csökkentheti a kockázatokat, és minden területen értéket teremthet.

Ha szeretné felmérni vállalata Zero Trusttal kapcsolatos fejlettségi szintjét, és kíváncsi a bevezetést segítő gyakorlati forrásainkra, végezze el a Microsoft által kidolgozott **Zero Trust fejlettségi modell felmérését**!