CTI Jelentés

Végpontvédelem és annak megvalósítása II.

Szervezeti stratégia, oktatás és jövőálló biztonság

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

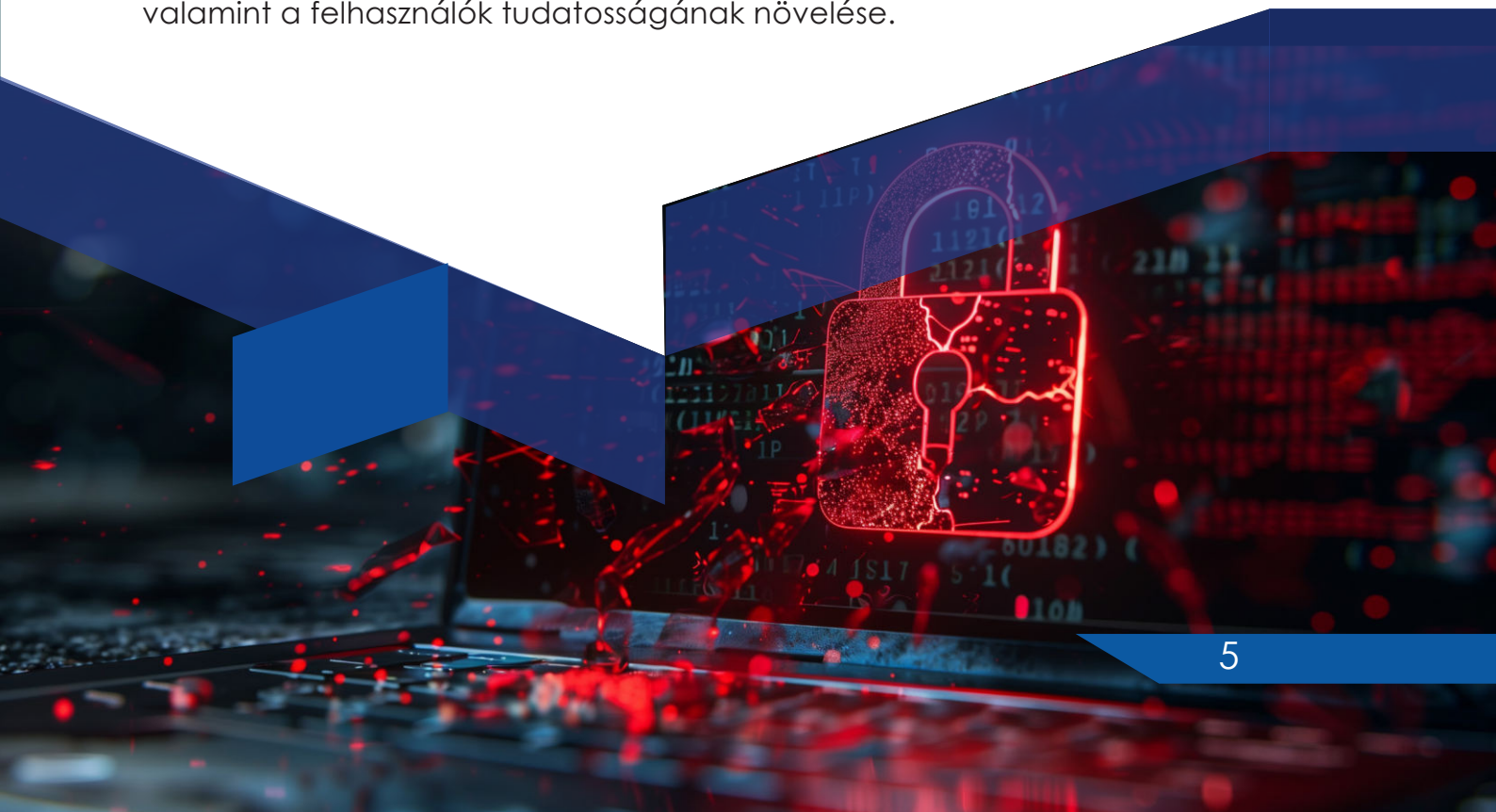
Tartalomjegyzék

Ez a dokumentum a korábban megjelent „Végpontvédelem és annak megvalósítása I. - Technológiai alapok és veszélyforrások” című kiberbiztonsági elemzés folytatása, amelyben a végpontvédelem során előforduló fenyegetettségeket és az ezek ellen felhasználható védelmi eszközöket mutattuk be. A jelenlegi írásunk célja, hogy a végpontvédelem témakörét most a stratégiák és a tervezés szempontjából vizsgáljuk, annak érdekében, hogy az olvasó tovább mélyíthesse ismereteit.

Kockázati tényezők, azonosított belső és külső kockázatok

A végpontvédelem területén a kockázatok két fő csoportra oszthatók: belső és külső fenyegetésekre. A belső kockázatok közé tartoznak a felhasználói hibák, a nem megfelelő jogosultságkezelés, a nem frissített vagy hibásan konfigurált szoftverek, valamint a belső rosszindulatú tevékenységek és adatvesztések. Ezzel szemben a külső fenyegetések – mint a kártékony kódok (malware, ransomware), a célozott adathalász támadások (phishing), illetve más automatizált vagy célzott behatolási kísérletek – általában a hálózaton kívülről érkeznek, és gyakran a nem megfelelően védett végpontokat veszik célba.

E kockázatok együttes jelenléte jelentősen növeli a szervezet sérülékenységét és támadási felületét, ezért elengedhetetlen a folyamatos rendszerfelügyelet, a biztonsági frissítések rendszeres alkalmazása, valamint a felhasználók tudatosságának növelése.



Kockázati felmérés - Az egyes kockázatok valószínűsége és hatása

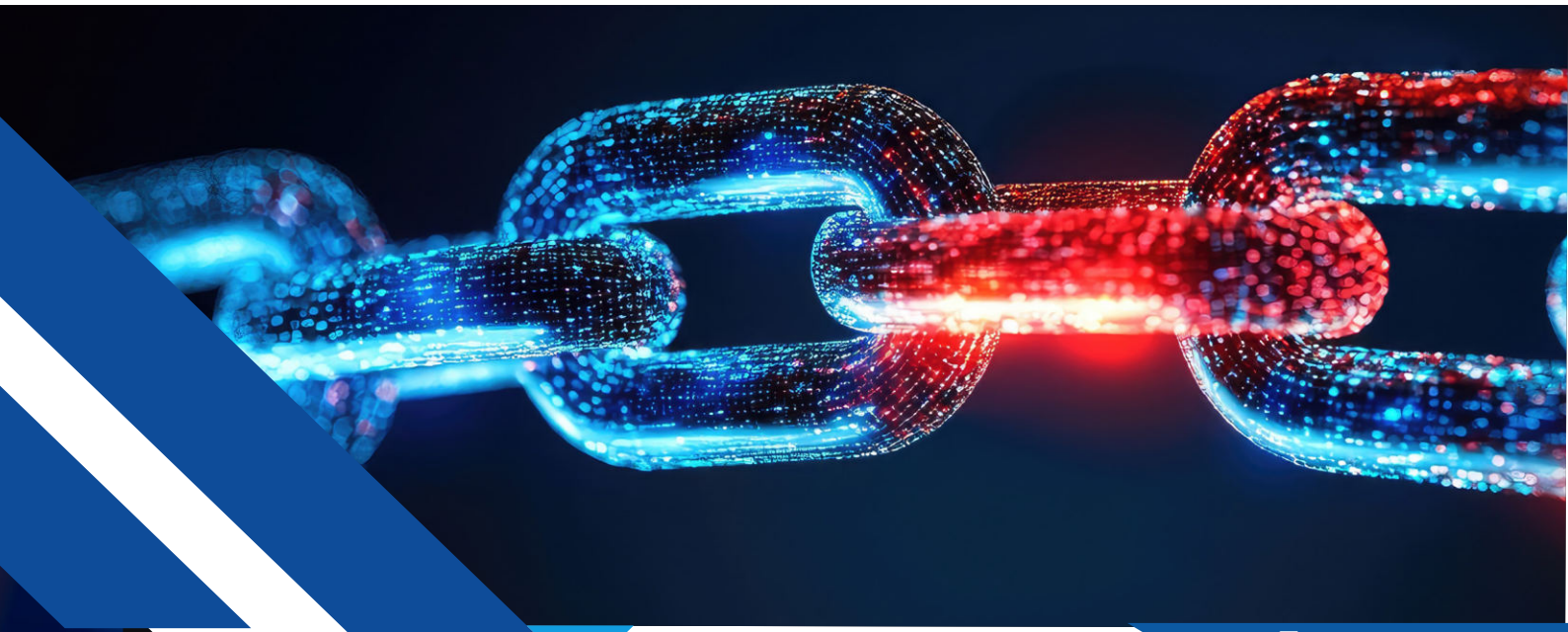
A kockázati felmérés célja, hogy objektív módszerekkel értékelje a különböző fenyegetések bekövetkezési valószínűségét és potenciális hatását a vállalat rendszereire. A folyamat során kvantitatív (számszerűsített) és kvalitatív (leíró) elemzési módszerek segítségével mérik fel, hogy például elavult szoftverek, hibás konfigurációk vagy emberi mulasztások milyen gyakorisággal fordulnak elő, és milyen szintű üzemzavart, adatvesztést vagy anyagi kárt okozhatnak.

Az eredmények alapján lehetőség nyílik a kockázatok priorizálására, vagyis a legsúlyosabb veszélyforrásokra történő célzott válaszintézkedések kidolgozására. Ezzel nemcsak a megelőzés válik hatékonyabbá, hanem a védekezési képesség is jelentősen javulhat, még a kifinomult támadásokkal szemben is.

Sebezhetőségek - A jelenlegi védelmi rendszerek gyenge pontjai

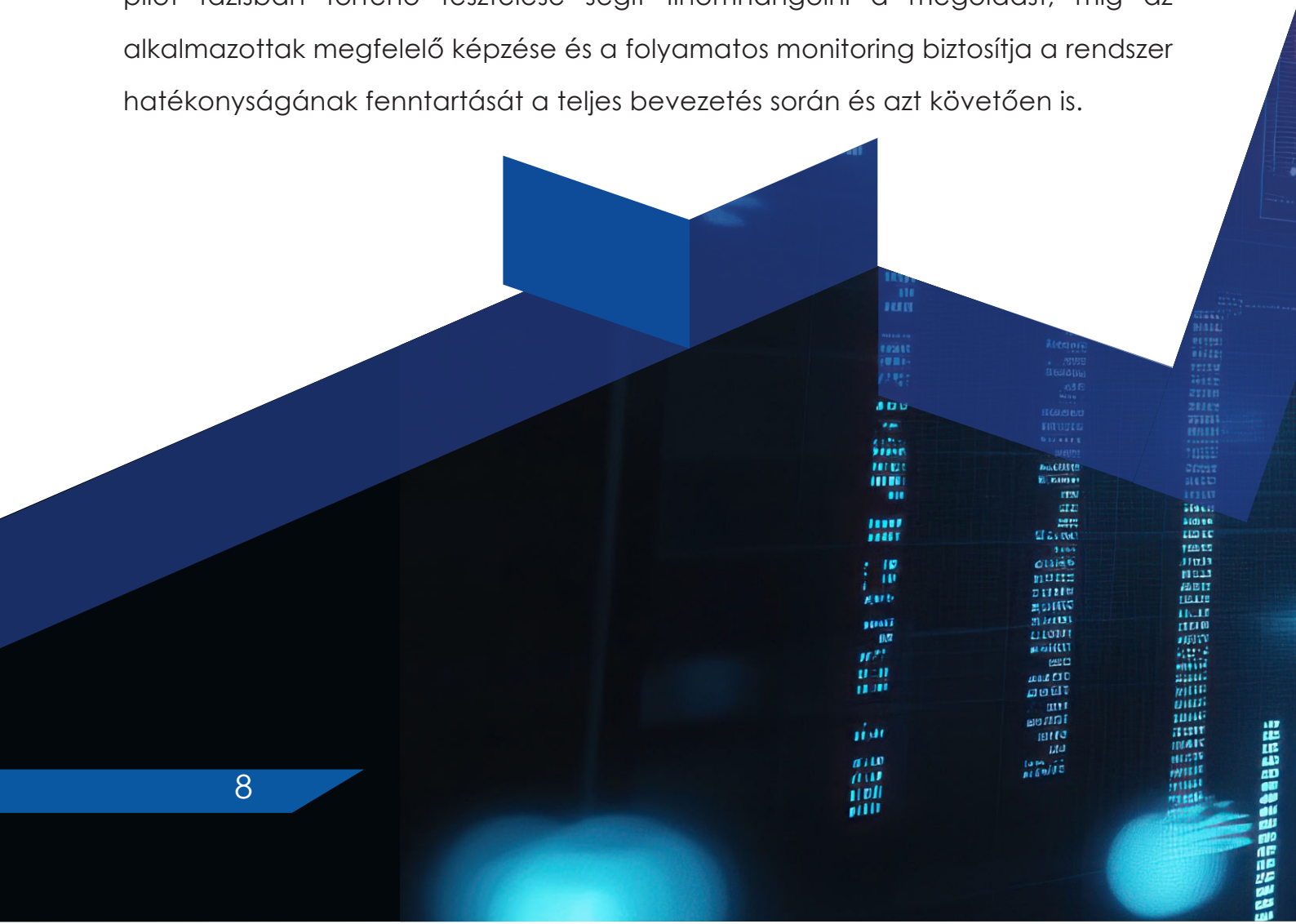
A legtöbb szervezet végpontvédelmi rendszere a folyamatosan fejlődő kiberfenyegetésekkel szemben időnként elégtelennek bizonyul. Gyakori probléma az elavult szoftververziók használata, a nem megfelelő patch management, valamint az olyan sérülékenységek, amelyeket a támadók zero-day exploitok vagy más ismert hibák kihasználásával képesek támadni.

A technológiák közötti integráció hiánya, a nem egységes jogosultságkezelés, valamint a felhasználói tudatosság alacsony szintje tovább növeli a támadók mozgásterét. Ezek a gyenge pontok jelentősen megnehezítik a valós idejű fenyegetésészlelést, és lassítják az automatizált válaszadási folyamatokat, ami lehetővé teszi a támadások mélyebb behatolását és nagyobb kártételét.



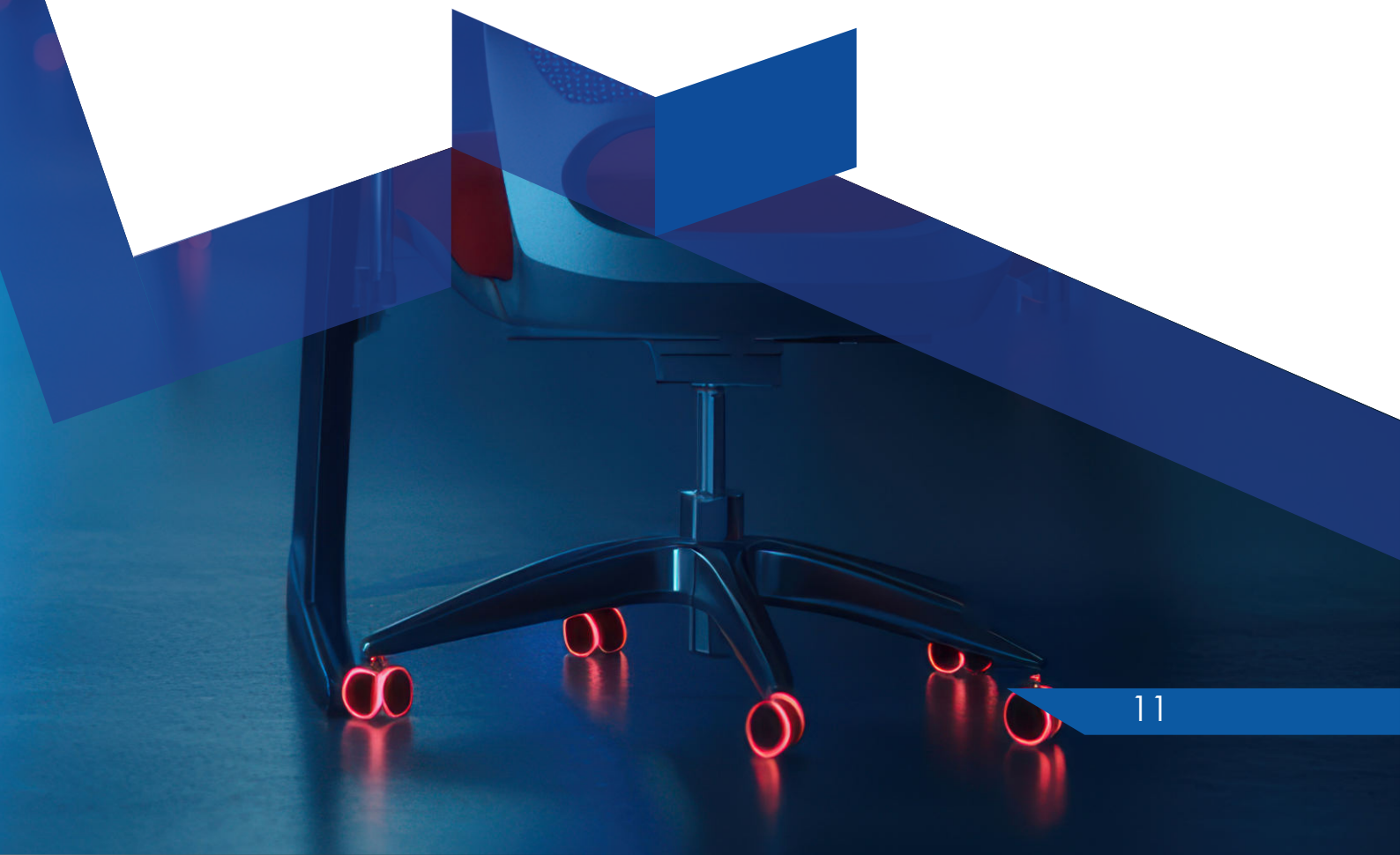
Megfelelő eszközök azonosítása és bevezetése

A megfelelő végpontvédelmi eszközök azonosítása és bevezetése egy strukturált, több lépésből álló folyamat, amely a vállalat egyedi igényeinek és kockázati profiljának alapos felmérésével kezdődik. Először szükséges a kockázatelemzés elvégzése, amely feltárja a rendszerek sebezhetőségeit és a potenciális fenyegetéseket, így meghatározható, hogy mely biztonsági rétegek hiányosak. Ezt követően azonosítani kell a piacon elérhető technológiákat és össze kell hasonlítani azokat a már meglévő IT infrastruktúrával való kompatibilitás, a skálázhatóság, a szabályozási megfelelés és a menedzselhetőség szempontjából. A kiválasztott eszközök pilot fázisban történő tesztelése segít finomhangolni a megoldást, míg az alkalmazottak megfelelő képzése és a folyamatos monitoring biztosítja a rendszer hatékonyságának fenntartását a teljes bevezetés során és azt követően is.



Képzés és tudatosság, képzési programok

A végpontvédelem hatékonyságának egyik alapköve a folyamatos képzés és tudatosság növelése a szervezeten belül. A dolgozók rendszeres oktatása – például interaktív tréningek, adathalász szimulációk, e-learning modulok és workshopok segítségével – lehetővé teszi, hogy megismerjék a legújabb kiberfenyegetéseket, felismerjék a gyanús tevékenységeket, és pontosan tudják, hogyan kell reagálni egy esetleges biztonsági incidensre. Ezek a képzési programok nem csupán elméleti tudást adnak át, hanem gyakorlati megoldásokat is kínálnak, így jelentősen csökkentve az emberi hibából eredő kockázatokat és elősegítve a vállalat végpontvédelmi eszközeinek hatékony használatát. Emellett a tudatossági programok hozzájárulnak a vállalati biztonsági kultúra kialakításához, ami hosszú távon növeli a szervezet ellenállóképességét a modern kiberfenyegetésekkel szemben.



Javaslatok a dolgozók végpontvédelmi ismereteinek bővítésére

A dolgozók kiberbiztonsági tudatossága kulcsszerepet játszik a végpontok védelmében. Az alábbi javaslatokkal erősíthető a szervezeten belüli felkészültség és a biztonságtudatos viselkedés.

- **Rendszeres kiberbiztonsági tréningek:** Szervezzünk interaktív e-learning modulokat, workshopokat és szemináriumokat, amelyek az aktuális fenyegetéseket, a sebezhetőségek felismerését és a helyes válaszintézkedéseket ismertetik. A képzések során külön figyelmet kell fordítani az adathalászat, a zsarolóvírusok és más gyakori kiberfenyegetések elleni védekezésre.

- **Gyakorlati szimulációk és phishing tesztek:** Rendszeres, valósághű adathalász kampányok és más biztonsági szimulációk segítségével a munkavállalók gyakorlatban is megtanulhatják felismerni a gyanús e-maileket, linkeket és mellékleteket. Az eredmények alapján célzott utóképzésekkel fejleszthetők az egyéni és csoportszintű hiányosságok.

- **Folyamatos tudatosságnövelő kampányok:** Hozzunk létre belső hírleveleket, infografikákat és esettanulmányokat, amelyek a legfrissebb kiberbiztonsági trendeket, támadástípusokat és megelőzési módszereket mutatják be. Játékos elemekkel – például kvízekkel, versenyekkel, díjazásokkal – ösztönözhető a munkatársak folyamatos érdeklődése és részvétele.

- **Szerepkör-alapú oktatás (role-based training):** Minden szervezeti egység más típusú fenyegetésekkel néz szembe – ezért célszerű személyre

szabott tananyagokat biztosítani külön a pénzügyi, HR, IT és egyéb részlegeknek. Így mindenki a számára leginkább releváns kockázatokat és védelmi stratégiákat ismeri meg.

- **„Just-in-time" oktatási emlékeztetők:** Használjunk valós idejű figyelmeztetéseket, például felugró ablakokat, ha egy felhasználó gyanús e-mailt nyit meg, nem biztonságos weboldalt látogat, vagy USB-eszközt csatlakoztat. Ezek a helyzethez illeszkedő mini-üzenetek hatékonyan erősítik a biztonságtudatos viselkedést.

- **Oktatási tartalom integrálása a végpontvédelmi rendszerekbe:** A vírusirtó, tűzfal vagy egyéb biztonsági eszközök eseményeihez rövid magyarázó anyagokat, videókat kapcsolhatunk. Így a dolgozók jobban megértik, miért történt egy blokkolás vagy figyelmeztetés – és mit tehetnek a jövőben ennek elkerülésére.

- **Belépéskori és napi szintű figyelemfelhívások:** Forgó képernyővédők, belépéskori üzenetek vagy asztali háttérképek formájában rendszeresen jelenjenek meg emlékeztetők: például „Ne add meg a jelszavad e-mailben!", „Mindig zárold a géped, ha elhagyod az asztalt!".

- **Elismerés és pozitív megerősítés:** Hozzunk létre egy belső elismerési rendszert, amely jutalmazza a példás kiberbiztonsági viselkedést – például a valós támadások észlelését, kiváló phishing-teszt eredményeket vagy aktív részvételt a képzéseken.

- **Tanulás valós vagy szimulált incidensekből:** Egy-egy (akár szimulált) biztonsági incidens után érdemes anonim módon bemutatni a történteket: mi történt, hogyan lehetett volna megelőzni, és mit tanulhatunk belőle. Ezek a konkrét példák hosszú távon jobban rögzülnek, mint az elméleti anyagok.

Jövőbeli trendek és fejlesztések, jövőbeli fejlesztési irányok

A végpontvédelem jövője számos technológiai és stratégiai fejlesztést vetít előre, amelyek célja, hogy rugalmasabb és proaktívabb védelmet nyújtsanak a folyamatosan változó kiberfenyegetésekkel szemben. A fejlesztési irányok egyik legmeghatározóbb eleme a mesterséges intelligencia (AI) és a gépi tanulás egyre szélesebb körű alkalmazása. Ezek a technológiák lehetővé teszik a viselkedésalapú fenyegetésészlelést, amely valós időben azonosítja a szokatlan mintázatokat és automatikusan reagál a gyanús tevékenységekre – még akkor is, ha azok korábban ismeretlen támadási formák.

A Zero Trust biztonsági modell további térnyerése szintén meghatározó, mivel segít a minimális jogosultság elvének érvényesítésében, a hozzáférések folyamatos ellenőrzésében, és a hálózaton belüli mozgás szigorú korlátozásában. Ennek kiegészítéseként a mikroszegmentáció és a dinamikus hozzáférés-kezelés egyre inkább beépül a szervezetek biztonsági architektúrájába.

Az XDR (Extended Detection and Response) rendszerek fejlesztése szintén kulcsszerepet kap, mivel ezek képesek összehangolt védelmet nyújtani a végpontok, hálózatok, felhőkörnyezetek és más infrastruktúraelemek között, megszüntetve a „siloszerű" működésből fakadó hiányosságokat.

A növekvő mértékű távmunkavégzés, a felhőalapú szolgáltatások térnyerése és az IoT-eszközök számának robbanásszerű növekedése miatt a felhőalapú és hibrid végpontvédelmi megoldások egyre inkább alapkövetelménnyé válnak. Ezek a rendszerek kiemelten fontosak a mobil munkaerő és a decentralizált vállalati környezetek biztonságának fenntartásában.

A jövőben különös figyelmet kap a rendszerek közötti interoperabilitás, vagyis a különféle védelmi megoldások zökkenőmentes együttműködése, valamint a folyamatos és automatizált frissítés, amely biztosítja, hogy a végpontvédelmi eszközök mindig naprakészek legyenek a legújabb fenyegetések kezelésében.

Hosszú távú stratégiai javaslatok a vállalatok végpontvédelmi rendszereinek továbbfejlesztésére

A vállalati végpontvédelem hatékonyságának növelése érdekében elengedhetetlen egy hosszú távú, komplex biztonsági stratégia kialakítása, amely nemcsak a technológiai eszközökre, hanem a szervezeti működés egészére kiterjed.

Az egyik legfontosabb fejlesztési irány a többrétegű, integrált biztonsági architektúra kialakítása, amely a Zero Trust modell alapelveire épül. Ez magában foglalja a felhasználók, eszközök és alkalmazások folyamatos hitelesítését, a mikroszegmentáció alkalmazását a hálózaton belüli mozgás korlátozására, valamint az EDR-rendszerek és a kockázatalapú sérülékenységmenedzsment integrálását. A patch management eszközökkel kiegészítve egy egységes, proaktív védelmi platform alakítható ki, amely hatékonyan kezeli a különféle fenyegetéseket.

Szintén kulcsszerepet kap a mesterséges intelligencia (AI) és az automatizáció egyre szélesebb körű alkalmazása. A gépitanulás-alapú viselkedéselemzés segíti az ismeretlen fenyegetések korai felismerését, míg az automatizált válaszintézkedések csökkentik az emberi beavatkozáshoz szükséges időt. Az XDR-rendszerek központosított adatelemzése lehetővé teszi a gyors és hatékony reagálást a különböző támadási mintázatokra.

A felhőalapú és hibrid védelmi architektúrák alkalmazása elengedhetetlenné vált a távoli munkavégzés, a mobil eszközhasználat és a decentralizált hálózatok elterjedésével. A felhőmegoldások skálázhatósága és globális lefedettsége nemcsak a működési költségeket csökkenti, hanem a nemzetközi fenyegetésekkel szemben is rugalmas és hatékony védelmet nyújt.

A technológiai megoldások mellett fontos szerepet kap a folyamatos kockázatértékelés és a rendszeres auditálás, amelyek feltárják a biztonsági rések meglétét, és segítik a szervezetet abban, hogy időben beavatkozhasson. Az állandó monitorozás, valamint a sebezhetőségvizsgálatok lehetővé teszik a rendszerek naprakészen tartását, és hozzájárulnak a védelmi szint folyamatos optimalizálásához.

Végül, de nem utolsósorban, a felhasználók biztonságtudatossága kulcsfontosságú tényező. Az emberi tényező továbbra is az egyik legnagyobb kockázati forrás, ezért javasolt rendszeres képzések, phishing szimulációk, valamint interaktív tudatosságnövelő programok bevezetése. Ezek hosszú távon nemcsak csökkentik a felhasználói hibák számát, hanem hozzájárulnak egy biztonságtudatos vállalati kultúra kialakításához is.

Védelmi stratégiák

A végpontvédelem hatékonysága azon múlik, hogy a szervezet milyen átfogó és integrált stratégiát alkalmaz a modern kiberfenyegetésekkel szemben. Az eredményes védekezés három fő pilléren nyugszik: megelőzésen, észlelésen és reagáláson, valamint a válaszintézkedések és helyreállítás képességén.

Az első pillér a megelőző intézkedések rendszere. Ide tartozik a kockázatértékelés és a sebezhetőségek rendszeres felmérése, amely lehetővé teszi a kritikus gyenge pontok azonosítását. Ezen az alapon történik a patch management, az eszközök és alkalmazások biztonságos konfigurálása, valamint a szoftverek és firmware-ek folyamatos frissítése. Kiemelten fontos az identitás- és hozzáféréskezelés korszerűsítése, különösen a Zero Trust modell alkalmazásával, amely megakadályozza a belső jogosulatlan mozgást. A hálózati mikroszegmentáció tovább csökkenti a támadók mozgásterét, ha egy végpont kompromittálódik.

A második pillért a felderítő és reagáló mechanizmusok jelentik. Ebben kulcsszerepet kapnak a modern EDR-rendszerek, amelyek valós időben figyelik a végpontokon zajló eseményeket, és képesek észlelni az anomáliákat és gyanús viselkedési mintázatokat. Az ilyen rendszerek gyakran kapcsolódnak threat intelligence forrásokhoz és kockázatmenedzsment eszközökhöz, így a fenyegetések korai felismerése és az automatizált válaszlépések gyors végrehajtása válik lehetővé.

A harmadik pillér a válaszintézkedések és helyreállítás folyamata. Egy jól működő stratégia részét kell képezze egy részletes incidenskezelési terv, amely lefedi az észleléstől a riasztáson, izoláláson és karanténozáson át a helyreállításig tartó teljes folyamatot. Fontos, hogy az eseményeket dokumentálják, és az esetekből tanulságokat vonjanak le, amit rendszeres auditálás és folyamatos fejlesztés követ. Emellett elengedhetetlen a dolgozók biztonságtudatosságának erősítése képzésekkel, szimulációkkal és oktatási kampányokkal, mivel a gyors és hatékony reagálás alapja gyakran az emberi tényezőn múlik.

Cselekvési terv

A cselekvési terv a végpontvédelem keretében egy részletes, előre kidolgozott dokumentum, amely meghatározza, hogyan reagáljon az adott vállalat egy biztonsági incidens vagy sebezhetőség felfedezése esetén. Ez a terv tartalmazza az incidenskezelési lépéseket, az érintett felelősök szerepét, a kommunikációs csatornákat, valamint a határidőket és prioritásokat, hogy a támadás vagy hiba bekövetkezése után a lehető leggyorsabban és leghatékonyabban lehessen visszaállítani a normál működést. Emellett a cselekvési terv segít azonosítani a szükséges erőforrásokat és intézkedéseket, amelyek révén csökkenthető a károk mértéke, és biztosítható, hogy a jövőben előforduló hasonló események elkerülhetőek legyenek.

Lépésenkénti intézkedési javaslatok: Konkrét tevékenységek és felelősök kijelölése

Ezen pont célja, hogy a cselekvési terv végrehajtását egyértelműen strukturálja, meghatározva, hogy mely konkrét lépések szükségesek a biztonsági incidensek megelőzésére, elhárítására és a rendszer helyreállítására, valamint ki felel ezekért a feladatokért.

Ajánlott a következő megközelítést alkalmazni:

- **Lépésről lépésre felosztott intézkedések:** Minden egyes lépést részletesen meg kell határozni, kezdve az incidens korai felismerésétől a fertőzött eszközök elkülönítésén, a források azonosításán és a helyreállítási folyamat elindításán át egészen az utólagos auditálásig. Az egyes lépésekhez időkereteket és mérföldköveket kell rendelni, hogy az intézkedések hatékonyságát és időben történő végrehajtását folyamatosan ellenőrizni lehessen.

- **Konkrét tevékenységek meghatározása:** Az intézkedési javaslatok tartalmazzák azokat a konkrét műveleteket, mint például a fertőzött eszközök azonnali elkülönítése, a hálózati forgalom blokkolása, a patch management és javítások végrehajtása, valamint a részletes incidens analízis elvégzése. Fontos, hogy minden tevékenység egyértelműen definiált legyen, és tartalmazza a szükséges eszközöket, módszereket, valamint a kapcsolódó dokumentációs követelményeket.

- **Felelősök kijelölése:** Minden egyes lépéshez rendelni kell egy konkrét felelőst vagy csapatot, akiknek szerepeik és feladataik világosan rögzítve vannak a cselekvési terv dokumentumában. A felelősök közötti koordináció érdekében érdemes rendszeres státuszjelentéseket és visszajelző mechanizmusokat bevezetni, amelyek segítik a folyamatok átláthatóságát és a gyors beavatkozást, ha valamilyen lépés elmarad vagy módosításra szorul.

Időzítés: Javasolt ütemterv az ajánlások megvalósítására

A cselekvési tervben javasolt meghatározni a rövid, közép- és hosszú távú intézkedések ütemezését, figyelembe véve a vállalat aktuális kockázati profilját, erőforrásait és prioritásait. Például rövid távon (0–3 hónap) a sürgős sebezhetőségek javítása, a kritikus patch-ek telepítése, valamint az incidensfigyelő és riasztórendszerek finomhangolása szükséges; középtávon (3–12 hónap) a rendszeres kockázatértékelés, fejlettebb technológiák bevezetése, valamint a dolgozói kiberbiztonsági tudatosság növelésére irányuló tréningprogramok elindítása javasolt; hosszú távon (1 év felett) pedig a végpontvédelmi rendszer integrációjának és folyamatos fejlesztésének fenntartása, a rendszeres auditok és visszajelzési mechanizmusok kialakítása, valamint a technológiai innovációk adaptálása szükséges. Az ütemterv rugalmasan kezelje a dinamikus fenyegetési környezet változásait, és rendszeres felülvizsgálatokkal biztosítsa, hogy a megvalósítás folyamatosan összhangban marad a vállalat biztonsági stratégiájával.

Erőforrás-szükséglet: Az ajánlások megvalósításához szükséges humán és anyagi erőforrások becslése

Az ajánlások megvalósításához szükséges erőforrások becslésében a következő pontokat érdemes figyelembe venni.

- **Humán erőforrások:** Az ajánlások implementálásához elengedhetetlen a megfelelő szakértelemmel rendelkező kiberbiztonsági szakemberek, IT rendszergazdák és végpontvédelmi szakértők bevonása. Fontos meghatározni, hogy hány főre van szükség az incidensfigyelés, sebezhetőségvizsgálat, rendszerintegráció, valamint az alkalmazottak oktatásának lebonyolításához. Ezen felül érdemes számításba venni a projekt menedzsmentjére, a belső auditokra és a külső tanácsadók, illetve auditcégek szolgáltatásainak igénybevételét.

- **Anyagi erőforrások:** Az anyagi erőforrások közé tartozik a szükséges szoftverlicencek, hardverek, valamint a felhőalapú szolgáltatások és biztonsági eszközök beszerzéséhez szükséges költségvetés. Ezen túlmenően a képzési programok, workshopok és egyéb tudatosságnövelő kezdeményezések szervezése is jelentős anyagi ráfordítást igényel. A költségvetésnek tükröznie kell a rendszeres frissítések, karbantartás, valamint a pilot projektek során szerzett tapasztalatok alapján szükséges módosításokat.

- **Ütemezés és rugalmas tervezés:** Mivel a vállalat mérete, az aktuális IT infrastruktúra állapota és a cselekvési terv prioritásai egyénenként változnak, fontos, hogy az erőforrás-szükséglet becslése rugalmas legyen. Javasolt pilot projektek indítása az új megoldások tesztelésére, amelyek alapján pontosítható a humán és anyagi erőforrások elosztása a hosszú távú fejlesztési ciklus során.

Források

SentinelOne (2025) Top 10 Endpoint Security Risks in 2025. SentinelOne Cybersecurity 101. https://www.sentinelone.com/cybersecurity-101/endpoint-security/endpoint-security-risks/ (Letöltve: 2025.04.29.)

Enterprise Strategy Group (2020) Reimagining Endpoint Security (ESG White Paper). Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/esg-reimagining-endpoint-security-white-paper.pdf (Letöltve: 2025.05.12.)

Rotate Blog (2025) The Future of Endpoint Security: Trends and Predictions. WithRotate. https://www.blog.withrotate.com/post/the-future-of-endpoint-security-trends-and-predictions (Letöltve: 2025.06.03.)

TechRadar (2025) 8 signs your company needs to upgrade its cybersecurity. TechRadar Pro. https://www.techradar.com/pro/software-services/8-signs-your-company-needs-to-upgrade-its-cybersecurity (Letöltve: 2025.06.06.)

Khan, N., Bhati, H., Vishwakarma, N. & Yadav, A. (2025) The Future of Endpoint Security: Trends, Challenges and Innovations. International Journal of Innovative Research in Technology (IJIRT), Vol. 11 Issue 11. https://ijirt.org/publishedpaper/IJIRT174661_PAPER.pdf (Letöltve: 2025.05.20.)

Adelusi, J. B. (2024) Endpoint Security Strategies for Safeguarding Digital Infrastructure. University of Abuja – ResearchGate. https://www.researchgate.net/publication/387225060_Endpoint_Security_Strategies_for_Safeguarding_Digital_Infrastructure (Letöltve: 2025.05.22.)

Qawasmeh, S. A. D., AlQahtani, A. A. S. & Khan, M. K. (2024) Navigating Cybersecurity Training: A Comprehensive Review. ArXiv https://arxiv.org/abs/2401.11326 (Letöltve: 2025.05.21.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025