CTI Jelentés

Végpontvédelem és annak megvalósítása I.

Technológiai alapok és veszélyforrások

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Mi az a végpontvédelem?

A végpontvédelem egy olyan biztonsági intézkedés, amely a hálózati végpontokat, például számítógépeket, laptopokat, okostelefonokat, táblagépeket és más IT-eszközöket – például hálózati nyomtatókat vagy munkavégzésre használt okoseszközöket – véd a kiberfenyegetésekkel szemben. Amennyiben vállalati környezetben is használunk ilyen eszközöket, akkor különösen fontos, hogy védettek legyenek a rosszindulatú támadások, vírusok, kártevők, zsarolóprogramok vagy adathalászati kísérletek ellen. A végpontvédelem egy komplex megoldást jelent, amely különböző biztonsági funkciókat ötvöz. Optimális esetben központilag kezelhetők, így a rendszergazdák folyamatosan nyomon követhetik a hálózathoz csatlakozó eszközök állapotát, és gyorsan reagálhatnak egy esetleges biztonsági incidensre.

A végpontok típusai

Munkaállomások

A munkaállomások kiemelten fontos szerepet töltenek be a végpontvédelemben, hiszen ezek az eszközök jelentik a mindennapi munkavégzés elsődleges felületét. Ide tartoznak elsősorban az asztali számítógépek és a hordozható laptopok, amelyekkel a dolgozók közvetlenül férnek hozzá a vállalat rendszereihez, üzleti adataihoz és belső hálózatához.

Mivel ezeken az eszközökön rendszerint adatbevitel, dokumentumkezelés, e-mailezés és internetelérés történik, különösen ki vannak téve a kibertámadásoknak – legyen szó adathalász kísérletekről, kártevőkről vagy nem biztonságos weboldalakról. Ezért a munkaállomások védelme nem csupán technikai feladat, hanem az egész szervezet információbiztonságának alapvető eleme. Ide tartozik a megfelelő vírusvédelem, a rendszeres frissítések biztosítása, a hozzáférési jogosultságok szabályozása, valamint a biztonságtudatos felhasználói magatartás kialakítása és ösztönzése.

Mobil eszközök

A mobil eszközök – elsősorban az okostelefonok és táblagépek – a munkahelyi környezetben és a mindennapi életben is nélkülözhetetlen szerepet töltenek be. A megfelelően beállított készülékek lehetővé teszik üzleti e-mailek küldését és fogadását, belső rendszerekhez való hozzáférést, valamint egyedi vállalati alkalmazások használatát – akár irodán kívül is.

Biztonsági szempontból ezek az eszközök többféle kihívást is rejtenek. Mivel szinte folyamatosan hálózatra csatlakoznak – gyakran nyilvános vagy kevésbé megbízható Wi-Fi hálózatokra –, és használatuk jellemzően helyfüggetlen, fokozott kockázatot jelentenek az adatszivárgás és illetéktelen hozzáférés szempontjából. Ráadásul az elvesztés vagy eltulajdonítás esélye is jóval magasabb, mint például egy asztali számítógép esetében.

Éppen ezért a mobil eszközök védelme kulcsfontosságú: ide tartozik az eszközök titkosítása, a jelszavas vagy biometrikus védelem alkalmazása, a távoli zárolás vagy törlés lehetősége, valamint a mobil eszközkezelő (MDM) rendszerek bevezetése. Ezek együttesen járulnak hozzá ahhoz, hogy egy elvesztett vagy feltört mobiltelefon ne jelentsen azonnali adatvédelmi kockázatot a szervezet számára.

Szerverek

A szerverek biztonsága alapvető fontosságú minden vállalati IT-infrastruktúrában, hiszen ezek az eszközök tárolják és kiszolgálják a legkritikusabb üzleti adatokat, alkalmazásokat és szolgáltatásokat. A szerverek a hálózati rendszer központi elemeinek számítanak, ezért, ha támadás éri őket, az akár az egész vállalat működését is megbéníthatja.

Ezek az eszközök jellemzően folyamatos kapcsolatban állnak különféle hálózati kliensekkel és más végpontokkal, miközben többféle szolgáltatást – például weboldalakat, adatbázisokat vagy távoli hozzáférést – tesznek elérhetővé. Ezekhez a funkciókhoz különböző nyitott portokon keresztül lehet kapcsolódni. Ha ezek a kapcsolódási pontok nincsenek megfelelően védve, frissítve vagy konfigurálva, akkor komoly támadási felületet jelentenek a kibertámadók számára.

A szervervédelem tehát komplex feladat, amely magában foglalja a rendszeres biztonsági frissítések alkalmazását, a hozzáférések szigorú szabályozását, a naplózás és monitorozás bevezetését, valamint a tűzfalak, IDS/IPS rendszerek, a hálózati szegmentáció és a minimális jogosultság elvének alkalmazását is.

IoT eszközök

Az IoT (Internet of Things) eszközök végpontvédelme egyre nagyobb kihívást jelent, mivel ezek az eszközök rohamosan terjednek az ipari, lakossági és vállalati környezetekben is. Az IoT eszközök olyan hálózatra kapcsolódó eszközök, amelyek adatokat gyűjtenek, elemeznek és továbbítanak. Ilyenek lehetnek például az intelligens otthoni eszközök vagy ipari érzékelők. Ezek az eszközök sokszor kritikus szerepet töltenek be a mindennapi működésben, de gyakran alacsony szintű biztonsági védelemmel rendelkeznek. Az IoT végpontvédelem biztosításához átfogó megoldásokra van szükség, amelyek magukban foglalják a hálózati szegmentációt, a titkosítást, a hozzáférések kezelését és az eszközök folyamatos monitorozását. Ezenkívül a gyártói szabványok követése és a rendszeres biztonsági auditok elengedhetetlenek ahhoz, hogy az IoT eszközök megfelelő védelmet nyújtsanak a modern fenyegetésekkel szemben.

2017-ben az Amerikai Élelmiszer- és Gyógyszerügyi Hatóság (FDA) mintegy 465 ezer implantálható pacemaker visszahívását rendelte el, miután kiderült, hogy az eszközök sebezhetőek távoli, illetéktelen hozzáféréssel végrehajtható kibertámadásokkal szemben. A pacemakerek beépített vezeték nélküli kommunikációs funkciói lehetővé tették, hogy egy rosszindulatú támadó módosítsa az eszköz beállításait – például a szívritmust szabályozó parancsokat –, amely súlyos esetben az akkumulátor idő előtti lemerüléséhez vagy az életmentő működés leállásához vezethetett volna. A kockázatok mérséklése érdekében a gyártó biztonsági célú firmware-frissítést adott ki, amely kizárólag egészségügyi szakemberek közreműködésével volt telepíthető klinikai környezetben.

2015-ben Charlie Miller és Chris Valasek biztonsági kutatók egy nagy visszhangot kiváltó demonstráció során távolról átvették az irányítást egy Jeep Cherokee felett, a jármű Uconnect infotainment rendszerének sérülékenységeit kihasználva. A támadók képesek voltak beavatkozni a jármű kormányzásába, a fékrendszerbe és a motorvezérlésbe is, miközben az autó valós forgalmi környezetben közlekedett. Ez a demonstráció erőteljesen rámutatott arra, hogy az internetre kapcsolt járművek – különösen az integrált vezérlőrendszerek és távoli hozzáférési felületek révén – súlyos, akár életveszélyes kiberbiztonsági kockázatokat hordozhatnak. Az eset iparági szinten is fordulópontot jelentett, mivel jelentős szigorításokat eredményezett az autóipari szoftverbiztonság, távoli frissítések és kockázatkezelési protokollok területén.

Nyomtatók és szkennerek

A nyomtatók és szkennerek a végpontvédelem szempontjából gyakran figyelmen kívül hagyott eszközök, pedig ezek is hálózati végpontok, amelyek hozzáférnek és kezelhetik a vállalati hálózat érzékeny adatait. Mivel a modern nyomtatók és szkennerek hálózati kapcsolattal rendelkeznek, távoli hozzáférést biztosítanak, adatokat tárolhatnak, és akár felhőalapú szolgáltatásokhoz is kapcsolódhatnak, emiatt komoly biztonsági kockázatokat hordozhatnak. Ebben az esetben is érdemes kiemelni a hálózati szegmentációt, a jogosultságok megfelelő kezelését, valamint a rendszeres frissítéseket és a naplózás fontosságát.

2017-ben egy Stackoverflowin álnéven ismertté vált támadó automatizált szkripttel célzottan keresett fel internetre közvetlenül csatlakozó nyomtatókat, és több mint 150 000 eszközön nyomtatott figyelmeztető üzeneteket. A támadás során olyan gyakran nyitva hagyott szolgáltatásokat használt ki, mint az IPP (Internet Printing Protocol), az LPD (Line Printer Daemon) és a 9100-as TCP port. Az eset jelentős médiavisszhangot váltott ki, és jól példázta, milyen könnyen kihasználhatók a nem megfelelően védett, nyilvánosan elérhető hálózati eszközök.

Virtuális végpontok

A virtuális végpontok – például a virtuális gépek (VM-ek), a konténerek, valamint a különféle felhőalapú szolgáltatások által biztosított környezetek – egyre nagyobb szerepet kapnak a modern vállalati IT-infrastruktúrákban. Ezek a rendszerek a hagyományos fizikai eszközökhöz hasonlóan képesek alkalmazások futtatására, adatok tárolására és hálózati kommunikációra, ugyanakkor sajátos működésük miatt speciális biztonsági megközelítést igényelnek.

A virtuális környezetek dinamikusak és gyorsan változóak: új példányok akár percek alatt létrejöhetnek vagy megszűnhetnek, ami megnehezíti a hagyományos végpontvédelmi eszközök alkalmazását. Emiatt különösen fontos a hálózati szegmentáció, a folyamatos naplózás és monitorozás, valamint a sérülékenységek rendszeres felmérése és javítása. Mivel ezek a rendszerek gyakran több virtuális gépet vagy konténert futtatnak ugyanazon fizikai infrastruktúrán, a hypervisor védelme kulcsszerepet játszik: ennek kompromittálása az összes kapcsolódó virtuális végpontot veszélybe sodorhatja.

A felhőalapú szolgáltatások esetében további kihívás a megosztott felelősség modellje – vagyis a biztonság egy része a szolgáltató, más része viszont az ügyfél felelőssége. Ezért elengedhetetlen a biztonsági beállítások alapos átvizsgálása, az erős hitelesítés, az identitáskezelés, valamint a megfelelő hozzáférési szabályok kialakítása is.

Fenyegetettségek és kockázatok – avagy mi ellen védekezzünk?

Malware

A malware, vagyis a rosszindulatú szoftverek az egyik legelterjedtebb és legsúlyosabb fenyegetést jelentik a végpontvédelem szempontjából. Céljuk, hogy károsítsák, manipulálják vagy illetéktelen módon kihasználják a hálózatra kapcsolódó eszközöket, adatokat és erőforrásokat. Egyes kártevők akár hosszú időn keresztül is képesek észrevétlenül megbújni a rendszerben, például háttérfolyamatként futva vagy legitim alkalmazásokba ágyazva.

A malware-ek különböző formákban fordulhatnak elő, például klasszikus vírusként, rejtett trójai programként, adatokat titkosító zsarolóvírusként, információkat gyűjtő kémprogramként, gyorsan terjedő féregként vagy a rendszer mélyebb rétegeit elérő rootkitként. Egyes esetekben backdoor-okat is létrehoznak, amelyeken keresztül a támadók később újra hozzáférhetnek az érintett eszközhöz.

Mivel a támadások egyre kifinomultabbak, a védekezés nem alapulhat csupán hagyományos vírusirtókon. Szükség van viselkedéselemző technológiákra, valós idejű fenyegetésészlelésre, valamint olyan megoldásokra, mint a sandboxing vagy a kiterjesztett észlelés és válaszadás (XDR). A védekezési módszerek folyamatos fejlesztése és naprakészen tartása kulcsfontosságú ahhoz, hogy a szervezetek időben felismerjék és megállítsák a legújabb malware-típusokat is.

Adathalászat

Az adathalászat egy nagyon gyakran előforduló támadási módszer. Az adathalászat során a támadók megtévesztő e-maileket, weboldalakat vagy üzeneteket használnak annak érdekében, hogy érzékeny információkat, például jelszavakat, bankkártyaadatokat vagy egyéb személyes adatokat szerezzenek meg. Végpontvédelmi szempontból az adathalászat különösen veszélyes, hiszen közvetlenül a felhasználói viselkedésre, reakcióra épít, és kihasználja a felhasználók esetleges figyelmetlenségét, kapkodását vagy ismerethiányát. A hatékony védelemhez többrétegű megközelítés szükséges, amely magában foglalja a felhasználók oktatását, a levelező rendszer biztonsági funkcióit, az MFA-t és a folyamatos hálózati monitorozást.

Sérülékenységek

A sérülékenységek kiemelt kockázatot jelentenek, mivel a támadók ezeket felhasználva hozzáférhetnek vállalati rendszerekhez, adatbázisokhoz és érzékeny információkhoz is. A sérülékenységek jellemzően olyan hibák vagy hiányosságok a végpontokon futó szoftverekben, operációs rendszerekben, hálózati beállításokban vagy hardverekben, amelyek lehetőséget adnak a rosszindulatú szereplőknek, hogy kárt tegyenek a védett rendszerben. A végpontvédelem egyik célja, hogy az ilyen sérülékenységeket időben felismerje, javítsa, vagy minimálisra csökkentse azok hatását. Ezt a folyamatos frissítésekkel, valamint megfelelő jogosultságkezelő és monitorozási rendszerek kiépítésével és használatával lehetséges elérni.

Adatszivárgás, adatlopás

Az adatszivárgás és az adatlopás olyan **súlyos biztonsági incidensek**, amelyek közvetlenül érintik a szervezetek egyik legértékesebb erőforrását: az adatvagyont. Ilyen események során érzékeny üzleti, pénzügyi, vagy akár személyes információk kerülhetnek illetéktelen kezekbe, ami jelentős anyagi, jogi és reputációs károkat okozhat a szervezet számára.

Az adatszivárgás jellemzően olyan helyzetet jelent, amikor az adatok akaratlanul – például figyelmetlenségből, hibás beállításból vagy technikai mulasztásból – kerülnek ki a szervezet ellenőrzése alól. Ezzel szemben az adatlopás kifejezetten szándékos, rosszindulatú tevékenység, amely során támadók célzottan próbálnak hozzáférni védett információkhoz, akár külső behatolás, akár belső visszaélés révén.

A végpontvédelem egyik **kulcsfeladata az ilyen jellegű események megelőzése**, illetve bekövetkezésük esetén a **károk minimalizálása**. E célból fontos a titkosítás alkalmazása, a hozzáférések szigorú szabályozása, a felhasználói tudatosság erősítése, valamint a modern adatvesztés-megelőző (Data Loss Prevention - DLP) megoldások használata. Mindezek együttesen biztosítják, hogy az érzékeny adatok kizárólag azok számára legyenek elérhetők, akik valóban jogosultak rájuk, és kizárják a kiszivárgás vagy illetéktelen hozzáférés lehetőségét.

2023 októberében a British Library súlyos zsarolóvírus-támadás áldozatává vált, amelyet a Rhysida nevű, hírhedt ransomware-csoport hajtott végre. A támadók kompromittálták a könyvtár informatikai rendszereit, és mintegy 600 GB-nyi adatot – több mint 500 000 fájlt – tulajdonítottak el, köztük alkalmazottak és felhasználók érzékeny személyes adataival együtt. A támadók megközelítőleg 20 bitcoin értékű váltságdíjat követeltek (akkori árfolyamon mintegy 600 000 angol font), ám az intézmény – a nemzetközi kiberbiztonsági ajánlásoknak megfelelően – nem tett eleget a követelésnek. Ennek következményeként az elrabolt adatokat a dark weben közzétették, a rendszerek egy részét titkosították, illetve megsemmisítették, ami több hónapig tartó szolgáltatás-kiesést és működési zavarokat okozott. Az incidens jól példázza, milyen súlyos következményei lehetnek a kritikus rendszerek elavultságának, valamint az alapvető védelmi intézkedések – például a többfaktoros hitelesítés – hiányának.

Fizikai hozzáférés

A fizikai hozzáférésből eredő kockázatok a végpontvédelem szempontjából gyakran háttérbe szorulnak, pedig jelentős fenyegetést jelenthetnek, különösen abban az esetben, ha illetéktelen személyek közvetlen hozzáférést szereznek eszközökhöz, szerverekhez, adatközpontokhoz vagy hálózati infrastruktúrához. Noha a végpontvédelmi megoldások jellemzően kiberfenyegetések elhárítására koncentrálnak, a fizikai hozzáférés lehetősége olyan megkerülési pontot jelent, amely révén a támadók kijátszhatják a szoftveres védelmi rétegeket.

A hatékony védelemhez elengedhetetlen a fizikai biztonság integrálása a végpontvédelmi stratégiába. Ez magában foglalja az eszközök titkosítását, a hozzáférési jogosultságok szigorú szabályozását, a zárt szerverszobák és zónák kialakítását, valamint a mobil és hordozható eszközök védelmét. A biztonsági zárak, beléptető rendszerek, kamerás megfigyelés, valamint a fizikai auditálási folyamatok együttes alkalmazása nagymértékben csökkentheti annak esélyét, hogy egy kompromittált végpont fizikai manipuláció révén veszélyeztesse az egész vállalati hálózatot.

Nem megfelelő konfiguráció és menedzsment

A nem megfelelő konfiguráció és menedzsment az egyik leggyakoribb kockázati tényező a végpontvédelemben, amely jellemzően emberi hibákra, hiányos biztonsági szabályozásokra, illetve a rendszerek összetettségéből fakadó félreértésekre vezethető vissza. Az helytelenül konfigurált végpontok és szerverek súlyos sebezhetőségeket eredményezhetnek, amelyeket a támadók – legyenek akár külső, akár belső szereplők – könnyedén kihasználhatnak.

A hatékony végpontvédelem érdekében elengedhetetlen a megfelelő kezdeti konfiguráció, valamint a folyamatos, tudatos rendszerüzemeltetés. Mindez magában foglalja a konzisztens jogosultságkezelést, a rendszeres auditokat, valamint a konfigurációs állapotok automatizált ellenőrzését is. A biztonsági frissítések és patch-ek naprakészen tartása szintén kulcsszerepet játszik a támadási felület minimalizálásában, amelyért elsősorban az üzemeltetési és IT-biztonsági csapat felelős. A megfelelő eszközök és folyamatok alkalmazása segíti a hibalehetőségek csökkentését és a védelmi stratégia megbízható működtetését.

Felhasználói hibák

A felhasználói hibák az egyik leggyakoribb és legkönnyebben kihasználható gyenge pontot jelentik a kiberbiztonságban. Az emberi tényező sok esetben a legsebezhetőbb láncszem: a támadók gyakran építenek a tájékozatlanságra, a figyelmetlenségre, vagy a rossz biztonságtudatos szokásokra, hogy jogosulatlan hozzáférést szerezzenek, adatokat lopjanak, vagy működési zavart okozzanak.

Tipikus felhasználói hibák közé tartozik például a gyenge jelszavak használata, a kéretlen e-mailek megnyitása, a nem biztonságos weboldalak látogatása, vagy a szoftverfrissítések elmulasztása. Sok esetben ezek a hibák nem szándékosak, mégis komoly biztonsági rést nyithatnak a támadók számára.

A végpontvédelem egyik kulcseleme, hogy ne csak technikai eszközökkel – például jogosultságkezeléssel, hozzáférés-korlátozással vagy automatikus fenyegetésészleléssel – csökkentse a kockázatokat, hanem aktívan elősegítse a felhasználói tudatosság növelését is. Rendszeres képzések, szimulációs gyakorlatok és belső kommunikációs kampányok segítségével csökkenthető a hibázás esélye, és a felhasználók a szervezet biztonságának tudatos részeseivé válhatnak.

Social engineering

A social engineering napjaink egyik legeredményesebb és legnehezebben kivédhető támadási módszere, amely nem technikai sebezhetőségeket, hanem az emberi tényezőt célozza meg. A támadók pszichológiai manipuláció révén próbálják megtéveszteni a felhasználót, és rávenni, hogy érzékeny információkat adjon ki, vagy olyan műveleteket hajtson végre (például fájlok megnyitása, linkekre kattintás, jelszavak megadása), amelyek hozzáférést biztosítanak a vállalati rendszerekhez.

Mivel ezek a támadások nem feltétlenül hagynak technikai nyomot, a hagyományos végpontvédelmi megoldások gyakran nem képesek időben detektálni vagy megakadályozni őket. Ennek következtében kiemelten fontos a felhasználói tudatosság fejlesztése, a rendszeres biztonságtudatossági képzések és szimulációk alkalmazása, amelyek során a munkavállalók megtanulhatják felismerni és elkerülni az ilyen jellegű fenyegetéseket.

A védekezés technikai oldalról is erősíthető: a többlépcsős hitelesítés (MFA) alkalmazása, az adathalászat-ellenes szűrők, valamint a valós idejű forgalomfigyelés és riasztások hozzájárulnak a social engineering támadások felismeréséhez és korlátozásához. A technológiai és oktatási elemek kombinálása képezi a leghatékonyabb védelmi stratégiát ezzel az egyre gyakoribb fenyegetéstípussal szemben.

A végpontvédelemben használt technológiák és eszközök

A végpontvédelemben használt eszközök közé tartoznak többek között az antivírus- és antimalware-programok, tűzfalak, behatolás-megelőző rendszerek (IPS), adatvesztés-megelőzés (DLP), valamint fejlett viselkedéselemző algoritmusok, amelyek képesek azonosítani és blokkolni a gyanús tevékenységeket. Az ilyen rendszerek központi menedzsmentet biztosítanak, lehetővé téve a biztonsági szakemberek számára, hogy hatékonyan kezeljék és monitorozzák a hálózat végpontjainak védelmét. A következőkben a jelenleg használt ismertebb eszközök és technológiák kerülnek bemutatásra.

Antivírus szoftverek

Az antivírus szoftverek a végpontvédelem egyik legalapvetőbb technológiai pillérét jelentik. Feladatuk, hogy megvédjék a végfelhasználói eszközöket a különféle rosszindulatú programokkal – például vírusokkal, férgekkel, trójai programokkal, zsarolóvírusokkal és más kártékony kódokkal – szemben.

A legtöbb antivírus megoldás biztosít valós idejű védelmet, vagyis folyamatosan figyeli a rendszer működését, és automatikusan blokkolja a gyanús vagy káros tevékenységeket. Emellett lehetőséget nyújt rendszeres vagy manuális víruskeresésre, amelynek során átvizsgálja az eszközön található fájlokat, folyamatokat, és eltávolítja az esetleges fertőzéseket.

A felismerés egyik alapját a gyártók által folyamatosan frissített fenyegetésadatbázis jelenti, amely a már ismert kártevők jellemzőit tartalmazza. Az újabb megoldások azonban nem kizárólag erre támaszkodnak: a viselkedéselemzés a futó folyamatok szokatlan mintáit figyeli, míg a heurisztikus elemzés lehetővé teszi a korábban nem ismert vagy mutálódott kártevők felismerését. A gyanús fájlokat az antivírus rendszer általában karanténba helyezi, így azok nem tudnak további kárt okozni a rendszerben.

A modern antivírus technológiák egyre gyakrabban alkalmaznak felhőalapú megoldásokat, amelyek a fenyegetések kiértékelését a felhőben végzik, így gyorsabb és kevésbé erőforrás-igényes működést tesznek lehetővé. Emellett egyre több gyártó épít be mesterséges intelligencián (AI) és gépi tanuláson (machine learning) alapuló modulokat is, amelyek képesek a korábban ismeretlen, nulladik napi fenyegetések felismerésére.

Fontos szempont az antivírus rendszerek összehangolása más végpontvédelmi technológiákkal, különösen az EDR (Endpoint Detection and Response) megoldásokkal. Az integráció révén lehetőség nyílik a fenyegetések átfogóbb vizsgálatára, az események láncolatainak feltérképezésére, valamint a gyors és célzott válaszintézkedések meghozatalára is – ezt a következő szakaszban részletesebben is tárgyaljuk.

Tűzfalak

A tűzfalak a végpontvédelem alapvető elemei közé tartoznak. Fő feladatuk, hogy meggátolják a jogosulatlan hozzáférést a hálózatokhoz és az egyes eszközökhöz, miközben biztosítják a rendszer külső és belső fenyegetésekkel szembeni védelmét. Működésük során szabályrendszereket és forgalomszűrési eljárásokat alkalmaznak, amelyek segítségével ellenőrzik és szűrik a bejövő és kimenő adatforgalmat.

Típusukat tekintve a tűzfalak leggyakrabban hálózati és végponti tűzfalakra oszthatók. A hálózati tűzfalak jellemzően a teljes hálózatra kiterjedő védelmet biztosítanak, és leggyakrabban hardveres vagy virtuális formában jelennek meg – ezek tipikusan vállalati környezetekben fordulnak elő. A végponti tűzfalak ezzel szemben egyes eszközök – például laptopok, okostelefonok vagy szerverek – védelmét látják el, és főként a felhasználói eszközök szintjén működnek.

A korszerű végponti tűzfalak már nem csupán statikus szabályokon alapulnak: egyre gyakrabban alkalmaznak gépi tanuláson alapuló algoritmusokat és viselkedéselemzést, hogy képesek legyenek felismerni az új, eddig ismeretlen fenyegetéseket is. Ezeket a megoldásokat gyakran integrálják más védelmi eszközökkel, például antivírus szoftverekkel vagy EDR-rendszerekkel, így komplexebb védelmi környezetet hozva létre.

A tűzfalak képesek hozzáférés-szabályozásra és adatforgalom-szűrésre, amely során a megadott szabályok alapján engedélyezik vagy blokkolják az egyes kapcsolódási kísérleteket. Szerepük fontos a DDoS-támadások elleni védelemben is, ahol a túlterhelési próbálkozásokat azonosítani és szűrni tudják. Emellett lehetőséget biztosítanak alkalmazás- és tartalomszűrésre, vagyis korlátozhatják bizonyos alkalmazások vagy nemkívánatos weboldalak elérését. Sok modern tűzfal támogatja a VPN-kapcsolatok biztonságos kezelését, így titkosított, védett hozzáférést nyújt a vállalati hálózathoz távolról dolgozók számára is. Végül, de nem utolsósorban, a tűzfalak naplózzák a hálózati eseményeket, lehetővé téve az események utólagos elemzését és a gyors reagálást az esetleges fenyegetésekre.

Endpoint Detection and Response (EDR)

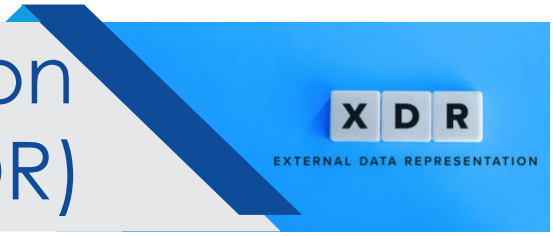
Az EDR-technológia (Endpoint Detection and Response) a végpontvédelem egyik leggyorsabban fejlődő területe, amely kulcsszerepet tölt be a kibertámadások korai észlelésében és az azokra adott gyors válaszlépések biztosításában. Az ilyen rendszerek képesek valós időben monitorozni a végpontokon zajló eseményeket, például a folyamatokat, hálózati kommunikációt vagy fájlhozzáféréseket, és gyanús viselkedési minták alapján azonosítani a zero-day támadásokat vagy más, korábban ismeretlen fenyegetéseket is.

Az EDR rendszerek egyik legnagyobb előnye, hogy lehetőséget adnak a támadások részletes elemzésére és visszakövetésére. A rendszer részletes információkat gyűjt a támadás módjáról, idővonaláról, a használt technikákról és az érintett fájlokról, ezzel támogatva az informatikai biztonsági csapatokat a teljes támadási lánc megértésében. Ezen túlmenően az EDR rendszerek képesek automatikus válaszlépésekre is, például leállítják a veszélyes folyamatokat, karanténba helyezik a fertőzött fájlokat, vagy szükség esetén elszigetelik a kompromittált végpontot a hálózattól.

Fontos jellemzőjük, hogy az eseményadatokat hosszabb távon tárolják, ami lehetővé teszi a retrospektív elemzést, a visszatérő minták felismerését és a védekezési szabályok folyamatos finomhangolását. Az EDR megoldások emellett könnyen integrálhatók más biztonsági rendszerekkel, például SIEM (Security Information and Event Management) vagy hálózati biztonsági megoldásokkal, így egy átfogóbb, egymásra épülő védelmi architektúra részévé válhatnak.

Napjainkban az EDR egyre gyakrabban jelenik meg összehangolt védelmi rendszerek, például az XDR (Extended Detection and Response) részeként, amelyek a végponti védelmet kiterjesztik a hálózati, felhőalapú és egyéb biztonsági rétegekre is. Ez a szemlélet jelentősen javítja a fenyegetések észlelésének pontosságát és a válaszlépések gyorsaságát, miközben csökkenti az izoláltan működő rendszerekből fakadó vakfoltokat.

Extended Detection and Response (XDR)



Az XDR (Extended Detection and Response) egy korszerű, integrált kibervédelmi megoldás, amely a hagyományos biztonsági rendszerekhez képest átfogóbb és hatékonyabb fenyegetésészlelést és -kezelést kínál. Lényege, hogy különböző védelmi rétegek – például a végpontok, hálózat, e-mail, felhő és alkalmazások – biztonsági eseményeit egységes rendszerbe kapcsolja, és ezek alapján komplex elemzéseket végez.

Az XDR célja, hogy átlátható és összehangolt védelmet biztosítson az egész informatikai infrastruktúra számára, ne csupán az egyes komponensek szintjén. Ehhez fejlett analitikai eszközöket, viselkedéselemzést, valamint gépi tanulási algoritmusokat alkalmaz, amelyek nemcsak a már ismert támadások felismerésére képesek, hanem a szokatlan mintázatok, anomáliák és gyanús viselkedések alapján akár új, korábban nem látott fenyegetéseket is észlelhetnek.

Az XDR rendszerek nem csupán figyelmeztetéseket küldenek, hanem automatizált válaszintézkedéseket is képesek végrehajtani. Ilyen lehet például egy fertőzött végpont elszigetelése a hálózattól, egy gyanús fájl karanténba helyezése vagy törlése, vagy a támadásban érintett rendszerfolyamatok azonnali leállítása. Ezek a válaszlépések jelentősen csökkentik a reagálási időt és a potenciális károk mértékét.

Az XDR egyik legnagyobb előnye a teljes körű kontextus biztosítása: nemcsak egy-egy eseményt mutat be, hanem képes azokat összekapcsolni, ok-okozati láncolatba rendezni, így segítve a biztonsági szakértőket abban, hogy átlássák a támadás teljes folyamatát, és proaktív lépéseket tegyenek a hasonló fenyegetések megelőzésére.

Intrusion Detection System (IDS) - Intrusion Prevention System (IPS)

Az IDS (Intrusion Detection System) és az IPS (Intrusion Prevention System) rendszerek kulcsszerepet töltenek be a modern végpontvédelmi és hálózatbiztonsági architektúrákban. Közös céljuk a fenyegetések korai észlelése és az incidensek gyors kezelése, ám működésük és felhasználási módjuk eltérő.

Az IDS rendszerek elsősorban passzív védelmet nyújtanak. Folyamatosan figyelik a hálózati forgalmat és a végpontok aktivitását, és riasztást generálnak, ha gyanús viselkedést, ismert támadási mintákat vagy anomáliákat észlelnek. Mivel az IDS nem avatkozik be közvetlenül a forgalomba, az észlelt események kezelése emberi beavatkozást igényel. Az IDS aláírás-alapú és anomália-alapú észlelési módszereket használ, hasonlóan az antivírus rendszerekhez.

Ezzel szemben az IPS rendszerek aktív védelmi funkciót látnak el: nemcsak észlelik a támadásokat, hanem azonnali válaszlépéseket is végrehajtanak. Képesek például blokkolni a káros hálózati forgalmat, elszigetelni fertőzött eszközöket, vagy megszakítani gyanús kapcsolatokat. Az IPS működése valós időben történik, így hatékonyan előzheti meg a támadások kibontakozását.

Az észlelési technológiák itt is aláírás- és anomáliaalapú megközelítést követnek, de gyakran kiegészülnek viselkedéselemzéssel és automatizált szabályérvényesítéssel.

A két rendszer együtt alkalmazva nyújtja a legnagyobb biztonságot. A modern végpontvédelmi megoldások gyakran integrált IDS/IPS képességekkel rendelkeznek, így egy platformon biztosítják mind a riasztásalapú észlelést, mind az automatikus válaszadást. Az IDS által generált riasztások alapján az IPS képes célzottan és gyorsan beavatkozni, ami csökkenti a reakcióidőt és az emberi beavatkozás szükségességét.

Az IDS tehát főként a láthatóságot és korai figyelmeztetést, az IPS pedig az aktív védekezést és a fenyegetések megelőzését szolgálja – együttes alkalmazásuk pedig lehetővé teszi a proaktív, mélységi védekezést az összetettebb támadásokkal szemben.

Mobile Device Management (MDM) és Mobile Application Management (MAM)

A Mobile Device Management (MDM) és a Mobile Application Management (MAM) rendszerek kulcsszerepet játszanak a vállalati mobil eszközök és az azokon futó alkalmazások biztonságos kezelésében. A modern munkakörnyezetben – ahol a dolgozók gyakran használnak saját tulajdonú eszközöket (BYOD – Bring Your Own Device) is – ezek a technológiák elengedhetetlenek az adatbiztonság fenntartásához és az informatikai szabályok betartatásához.

Az MDM rendszerek lehetővé teszik az informatikai részlegek számára, hogy központilag felügyeljék és konfigurálják a vállalati vagy személyes használatú mobil eszközöket – például okostelefonokat, táblagépeket vagy más hordozható készülékeket. Távolról beállíthatók rajtuk a szükséges biztonsági szabályok, például jelszókövetelmények, titkosítási protokollok, vagy rendszerfrissítési kötelezettségek. Emellett lehetőség van az eszköz távoli zárolására vagy adattartalmának törlésére is arra az esetre, ha az elveszne vagy illetéktelen kezekbe kerülne.

A MAM rendszerek ezzel szemben alkalmazásközpontú védelmet nyújtanak: nem magát az eszközt, hanem az azon futó vállalati alkalmazásokat és adatokat kezelik.

Lehetővé teszik az alkalmazások központi telepítését, frissítését és eltávolítását, így a vállalat biztosítani tudja, hogy csak a jóváhagyott és biztonságos szoftverek kerüljenek használatba. A konténerizációs technológiák révén a MAM rendszerek képesek elkülöníteni a vállalati adatokat a személyes adatoktól, ezáltal jelentősen csökkentve az adatszivárgás kockázatát.

Az ilyen megoldások előnye, hogy miközben megerősítik az informatikai kontrollt, nem korlátozzák feleslegesen a felhasználói élményt. A MAM rendszerek lehetővé teszik, hogy a munkavállalók kényelmesen és gyorsan hozzáférjenek a munkához szükséges alkalmazásokhoz anélkül, hogy az érzékeny vállalati információk veszélybe kerülnének.

Security Information and Event Management (SIEM)

A SIEM rendszerek (Security Information and Event Management) olyan központi biztonsági megoldások, amelyek célja a különböző informatikai rendszerekből származó naplóadatok és események valós idejű gyűjtése, elemzése és korrelálása. E technológia kulcsszerepet játszik a fenyegetések azonosításában, a gyors riasztásokban és az incidenskezelés támogatásában.

A SIEM működésének alapja a **széles körű adatgyűjtés**: képes eseményeket fogadni többféle forrásból, például végpontokról, szerverekről, hálózati eszközökről, tűzfalakról, valamint IDS/IPS rendszerekből. Az így beérkező adatokat a rendszer **egységesített formátumra** (normalizált struktúrára) alakítja, hogy összehasonlíthatók és elemezhetők legyenek.

Az adatok korrelálása során a SIEM összekapcsolja az egymástól függetlennek tűnő eseményeket, és képes felismerni azokat a mintázatokat, amelyek összetett támadásokra vagy rendszerszintű fenyegetésekre utalnak. Olyan tevékenységekre is fényt deríthet, amelyek egyedileg nem tűnnek veszélyesnek, de együttes előfordulásuk már súlyos biztonsági incidenst jelezhet.

A SIEM **folyamatosan monitorozza** a rendszereket, és az előre meghatározott szabályok, viselkedési profilok alapján valós idejű riasztásokat generál, ha rendellenes vagy kockázatos tevékenységet észlel. Így **jelentősen csökkenthető a támadások észlelésének ideje**, és lehetővé válik a gyors beavatkozás.

Emellett a SIEM rendszerek hatékony eszközt biztosítanak az incidenskezeléshez és a forenzikus vizsgálatokhoz is. A korábban rögzített események alapján visszamenőleg is rekonstruálható egy támadás teljes lefolyása, amely nemcsak a kárfelmérést segíti, hanem hozzájárul a jövőbeni védekezési stratégiák kialakításához is. A SIEM tehát nem csupán eszköz a riasztásokhoz, hanem a biztonsági döntéshozatal egyik legfontosabb támogató rendszere.

A SIEM rendszerek működéséről egy részletesebb kiberbiztonsági elemzés is készült, amely elolvasható az NKI weboldalán.

Data Loss Prevention (DLP)

A Data Loss Prevention (DLP) rendszerek célja, hogy megelőzzék a vállalati adatok véletlen vagy szándékos kiszivárgását, különös tekintettel az érzékeny és bizalmas információkra. Ezek a megoldások központi szerepet töltenek be abban, hogy az adatok ne hagyhassák el engedély nélkül a vállalati környezetet, legyen szó végponti eszközökről, hálózati forgalomról vagy felhőszolgáltatásokról.

A DLP rendszerek első lépésben felismerik és osztályozzák az adatokat, vagyis képesek meghatározni, hogy mely fájlok, dokumentumok vagy adatmezők minősülnek például személyes, pénzügyi vagy üzleti szempontból kritikus információnak. Az így kategorizált adatok ezután kiemelt védelmet kapnak.

A rendszer ezután folyamatosan monitorozza az adatáramlást: figyelemmel kíséri az e-maileket, a hálózati fájlmozgásokat, a felhőalapú tárolásokat és az USB-eszközökre történő másolásokat is. Ha az adatok használatában rendellenes mintázatot vagy gyanús tevékenységet észlel – például egy érzékeny dokumentumot próbálnak nem titkosított formában e-mailben továbbítani –, a rendszer riasztást generál vagy beavatkozik.

A beépített szabályrendszer lehetővé teszi, hogy a vállalat előre meghatározott biztonsági előírásokat alkalmazzon, például automatikusan megakadályozza bizonyos fájlok megosztását, kötelező titkosítást írjon elő, vagy akár blokkolja az adott műveletet.

A DLP rendszerek képesek reaktív válaszintézkedéseket is végrehajtani, például zárolhatják az eszközt, megszakíthatják a kapcsolatot vagy figyelmeztetést küldenek a biztonsági csapatnak.

Ezek a rendszerek emellett kulcsfontosságúak a jogi megfelelés és a szabályozói auditálás szempontjából is. A DLP naplózza az összes eseményt és műveletet, így támogatja a GDPR, HIPAA, PCI-DSS és más adatvédelmi előírások betartását, valamint segíti az események visszakövethetőségét és az incidens utáni vizsgálatokat.

Vulnerability Management

A Vulnerability Management (sebezhetőségkezelési) rendszerek célja, hogy a vállalatok időben felismerjék, értékeljék és kezeljék az informatikai környezetükben előforduló biztonsági réseket. Ezek a megoldások közvetlenül hozzájárulnak a végpontvédelem hatékonyságához, mivel lehetővé teszik a proaktív kockázatkezelést és a támadási felületek csökkentését.

A rendszer folyamatosan szkenneli a hálózatot és a végpontokat, hogy azonosítsa a szoftverekben, operációs rendszerekben vagy konfigurációkban található ismert sebezhetőségeket. Ezt követően kockázati szintek szerint sorolja be az egyes problémákat, figyelembe véve azok súlyosságát, az érintett eszköz értékét és a támadási lehetőségek valószínűségét. Ez a priorizálás segíti az informatikai csapatokat abban, hogy a legkritikusabb problémák megoldására koncentráljanak elsőként.

A Vulnerability Management rendszerek gyakran szoros integrációban működnek a patch management megoldásokkal, így lehetőség van az automatizált javításokra, frissítések alkalmazására vagy konfigurációs változtatások végrehajtására. Emellett részletes riportokat és trendelemzéseket is készítenek, amelyek segítik a biztonsági döntéshozatalt, és támogatják a szabályozói megfelelőség elérését is.

E technológia nemcsak a meglévő gyenge pontokat tárja fel, hanem hozzájárul a hosszú távú védekezési stratégia kialakításához is – lehetővé téve, hogy a szervezet előre gondolkodjon, és ne csupán reagáljon a már bekövetkezett incidensekre.

Patch Management

A Patch Management (javításkezelési) rendszerek feladata, hogy a vállalati informatikai környezetben használt operációs rendszerek, alkalmazások és egyéb szoftverek mindig naprakészek legyenek a biztonsági javítások és frissítések szempontjából. Ezek a megoldások jelentősen hozzájárulnak a sebezhetőségek minimalizálásához, hiszen sok kiberincidens alapja az, hogy a támadók kihasználják az elavult vagy hibás szoftververziókban rejlő gyenge pontokat.

A modern patch management rendszerek automatizált módon ellenőrzik az eszközökön futó szoftverek verzióit, majd letöltik és telepítik a szükséges frissítéseket. Ez nemcsak időt takarít meg a rendszergazdák számára, hanem csökkenti az emberi hibák esélyét is, amelyek kézi frissítés esetén gyakran előfordulhatnak.

A rendszer célja, hogy az ismert biztonsági réseket mielőbb bezárja, így védelmet nyújtson a legújabb fenyegetésekkel szemben, és egyúttal biztosítsa a rendszerstabilitást és a működés folyamatosságát. Emellett a patch management megoldások részletes naplózási és riportkészítési funkciókat is kínálnak: a rendszergazdák nyomon követhetik, hogy mely javítások kerültek telepítésre, mikor történtek frissítések, illetve azonosíthatják azokat az eszközöket, amelyek valamilyen okból kimaradtak a folyamatból.

A patching nem csupán technikai feladat, hanem a végpontvédelem egyik alappillére, amely nélkül a legjobb biztonsági eszközök is könnyen megkerülhetők.

Sandboxing

A sandboxing technológia célja, hogy biztonságos, izolált környezetet biztosítson a gyanús vagy ismeretlen fájlok, programok futtatására, elemzésére. Ez a megközelítés lehetővé teszi, hogy a potenciálisan rosszindulatú kódokat a valódi rendszer károsítása nélkül teszteljék, így időben felismerhetők a fenyegetések.

A sandbox egy virtuális futtatókörnyezet, amely teljesen elkülönül a tényleges rendszertől, tehát a benne zajló tevékenységek semmilyen módon nem tudják elérni vagy befolyásolni a működő infrastruktúra többi részét. Ezáltal a fertőzések, adatvesztések vagy hálózati terjedés kockázata minimálisra csökkenthető, még akkor is, ha valóban rosszindulatú programot futtatnak benne.

A sandboxban végzett futtatás során a rendszer folyamatosan figyeli a kód viselkedését – például az operációs rendszerhez való hozzáférési kísérleteket, fájlmódosításokat, hálózati kapcsolatokat vagy gyanús rendszerhívásokat. Az automatikus viselkedéselemzés lehetővé teszi, hogy a rendszer valós időben riasztást adjon ki, ha olyan aktivitást észlel, amelyre jellemző egy ismert malware működése.

A sandboxing gyakran integrált része a fejlettebb végpontvédelmi architektúráknak, és együttműködik más biztonsági technológiákkal, például antivírus, EDR, SIEM, vagy tűzfalmegoldásokkal. Az így kialakított többrétegű védelem lehetővé teszi, hogy a szervezetek a nulladik napi (zero-day) fenyegetésekkel szemben is hatékonyabban lépjenek fel, még akkor is, ha azok még nem szerepelnek a fenyegetés-adatbázisokban.

Secure Web Gateways (SWG)

A Secure Web Gateway (SWG) rendszerek olyan hálózatbiztonsági megoldások, amelyek a felhasználók és az internet közötti webes adatforgalmat vizsgálják és szűrik, mielőtt az elérhetné a vállalati hálózatot. Szerepük különösen fontos a modern, felhőalapú és távmunka-környezetekben, ahol a munkavállalók gyakran nem a belső hálózatról érik el az internetes erőforrásokat.

Az SWG megoldások átfogó forgalomellenőrzést biztosítanak: képesek átvizsgálni a teljes bejövő és kimenő webforgalmat, beleértve a HTTPS titkosított kapcsolatokat is. A webtartalom-szűrés, az URL kategorizálás, a káros kódok felismerése és a webalapú alkalmazások korlátozása mind hozzájárulnak ahhoz, hogy a felhasználók csak biztonságos és jóváhagyott tartalmakhoz férjenek hozzá.

A SWG rendszerek egyre gyakrabban tartalmaznak integrált adatvesztés-megelőző (DLP) funkciókat is, amelyek segítenek megakadályozni, hogy a bizalmas vállalati adatok – akár tudatosan, akár véletlenül – kiszivárogjanak az internet irányába. Ezzel nemcsak a kibertámadások elleni védekezést támogatják, hanem a jogi és megfelelőségi követelmények teljesítését is.

A rendszer képes a vállalati biztonsági szabályzatok automatikus érvényesítésére (policy enforcement), és alkalmazásszintű vezérlést is biztosít. Ennek köszönhetően csak azok a webes tartalmak és szolgáltatások lesznek elérhetők a dolgozók számára, amelyek megfelelnek az adott szervezeti irányelveknek, ezzel is csökkentve a kockázatokat és a nem kívánt felhasználói viselkedésből fakadó problémákat.

Virtual Private Network (VPN)

A Virtual Private Network, röviden VPN, egy olyan technológia, amely titkosított, biztonságos kapcsolatot hoz létre a felhasználók és a vállalati hálózat között, még akkor is, ha az adatátvitel nyilvános Wi-Fi hálózaton keresztül történik. A VPN célja, hogy a hálózati kommunikációt védett csatornán keresztül bonyolítsa, ezzel megelőzze az adatok lehallgatását, módosítását vagy illetéktelen hozzáférését.

A VPN-ek a titkosított adatátvitel révén biztosítják, hogy a hálózaton keresztül továbbított információk – legyenek azok üzleti dokumentumok, hitelesítési adatok vagy érzékeny személyes információk – ne kerülhessenek illetéktelen kezekbe. A titkosítási protokollok (pl. IPSec, SSL/TLS) gondoskodnak arról, hogy az adatok olvashatatlanná váljanak az átviteli útvonalon.

A VPN használata különösen fontos a távmunkában dolgozók esetében, akik így biztonságosan csatlakozhatnak a vállalati hálózathoz a világ bármely pontjáról, anélkül, hogy kompromittálnák annak integritását. A VPN segítségével biztonságosan elérhetők a belső rendszerek, például fájlmegosztók, levelezőszerverek vagy intranet portálok.

Emellett a VPN technológia az IP-címek elfedésével növeli a felhasználók anonimitását, megnehezítve ezzel a rosszindulatú támadók dolgát a célpontok azonosításában. Ez különösen hasznos lehet például geolokáció-alapú tiltások kikerülésénél vagy adatvédelem szempontjából érzékeny környezetekben.

A korszerű VPN-megoldások gyakran integrálódnak más végpontvédelmi technológiákkal, például EDR, SWG vagy DLP rendszerekkel, hogy egy összetett, többrétegű védelmi vonalat alkossanak a hálózat, a végpont és a felhasználó adatainak biztonsága érdekében.

A VPN működéséről és alkalmazásáról egy részletesebb kiberbiztonsági elemzés is készült, amely elolvasható az NKI weboldalán.

Zero Trust modellek

A Zero Trust modell egy korszerű kiberbiztonsági megközelítés, amely azt az elvet követi, hogy semmilyen felhasználóban vagy eszközben nem lehet automatikusan megbízni – függetlenül attól, hogy az a szervezeten belül vagy kívül helyezkedik el. A modell lényege, hogy minden hozzáférési kísérletet alapos hitelesítési és engedélyezési eljárások előznek meg, és az engedély csak akkor adható meg, ha az adott kérés megfelel az előre definiált biztonsági feltételeknek.

A Zero Trust megközelítés célja, hogy a legkisebb szükséges jogosultság elvét érvényesítve, folyamatos ellenőrzés mellett biztosítsa a hozzáféréseket, és minimalizálja a biztonsági kockázatokat – akár belső, akár külső fenyegetésekről van szó.

A modell központi eleme a többlépcsős hitelesítés (például többfaktoros azonosítás), az identitásalapú hozzáférés-vezérlés, valamint a folyamatos viselkedéselemzés, amely képes felismerni a megszokottól eltérő, potenciálisan gyanús tevékenységeket. Ha például egy felhasználó szokatlan időpontban vagy ismeretlen földrajzi helyről próbál elérni bizalmas erőforrásokat, a rendszer automatikusan további hitelesítést kérhet, vagy akár blokkolhatja a hozzáférést.

A hálózati mikroszegmentáció szintén fontos eleme a Zero Trust stratégiának: ennek révén a belső hálózat kisebb, egymástól elhatárolt szegmensekre bontható, így egy sikeres behatolás esetén csak az adott szegmens érintett, nem az egész vállalati infrastruktúra.

Emellett a modell az adatbiztonságra is kiemelt figyelmet fordít, beleértve a titkosítást, az adatvesztés-megelőző (DLP) technológiák alkalmazását, valamint a részletes naplózást és auditálást.

A Zero Trust környezetekben elengedhetetlen az automatizált válaszintézkedések megléte: ezek lehetővé teszik, hogy egy gyanús viselkedés észlelésekor a rendszer emberi beavatkozás nélkül reagáljon – például lezárja a kapcsolatot, karanténba helyezzen egy végpontot, vagy értesítést küldjön a biztonsági csapatnak.

Fontos hangsúlyozni, hogy a Zero Trust nem egyetlen termék vagy szoftver, hanem egy átfogó, hosszú távú biztonsági stratégia, amelyet lépésről lépésre lehet bevezetni. A gyakorlatban ez kezdődhet például a hozzáférések felülvizsgálatával, a jogosultságok korlátozásával, a hálózat szegmentálásával, vagy éppen a végpontok és felhasználók viselkedésének mélyebb elemzésével.

A Zero Trust modell különösen jól alkalmazható olyan környezetekben, ahol a munkavállalók különféle eszközökről dolgoznak (például céges laptopról, otthoni számítógépről vagy mobiltelefonról), és az adatok több helyen – például helyi szervereken, felhőalapú rendszerekben vagy végpontokon – oszlanak meg. Az ilyen sokrétű infrastruktúrák védelme érdekében a Zero Trust megközelítés ma már egyre inkább alapelvként jelenik meg a szervezetek információbiztonsági stratégiáiban.

Források

Fortinet (n.d.) What Is a Firewall? Fortinet. https://www.fortinet.com/resources/cyberglossary/firewall (Letöltve: 2024.11.14.)

Palo Alto Networks (n.d.) What is EDR vs. XDR? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr (Letöltve: 2024.11.20.)

Palo Alto Networks (n.d.) IPS vs. IDS vs. Firewall: What Are the Differences? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips (Letöltve: 2025.04.15.)

Olsen, G. & Kosht, M. (2021) MDM vs. MAM: Comparing enterprise mobile security management options. TechTarget. https://www.techtarget.com/searchsecurity/feature/MDM-vs-MAM-Comparing-enterprise-mobile-security-management-options (Letöltve: 2024.11.29.)

Fortinet (n.d.) What is DLP (Data Loss Prevention)? Fortinet. https://www.fortinet.com/resources/cyberglossary/dlp (Letöltve: 2024.12.04.)

Shein, E. (2024) Patch management vs. vulnerability management: Key differences. TechTarget. https://www.techtarget.com/searchenterprisedesktop/tip/Patch-management-vs-vulnerability-management-Key-differences (Letöltve: 2025.01.14.)

Fortinet (n.d.) What Is Sandboxing? Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing (Letöltve: 2025.01.29.)

Palo Alto Networks (n.d.) What Is a Secure Web Gateway (SWG)? Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-secure-web-gateway (Letöltve: 2025.04.15.)

Cimpanu, C. (2017) A Hacker Just Pwned Over 150,000 Printers Left Exposed Online. BleepingComputer. https://www.bleepingcomputer.com/news/security/a-hacker-just-pwned-over-150-000-printers-left-exposed-online/ (Letöltve: 2025.04.15.)

Hern, A. (2017) Hacking risk: recall of pacemakers raises patient death fears. The Guardian. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update (Letöltve: 2025.04.15.)

Greenberg, A. (2015) Hackers Remotely Kill a Jeep on the Highway. Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Letöltve: 2025.04.15.)

Hern, A. (2024) Ransomware groups warned there is no money in attacking British state. The Guardian. https://www.theguardian.com/technology/2024/mar/12/ransomware-groups-warned-there-is-no-money-in-attacking-british-state (Letöltve: 2025.04.15.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025