YANAC
Heti összefoglaló

2026. február 17., kedd

Heti kitekintés

Az elmúlt időszak fejleményei három markáns irányba mutatnak:
az AI egyre mélyebben integrálódik a támadási ciklusba, az OT-környezetek stratégiai célponttá váltak, miközben a technikai támadások és a pszichológiai manipuláció határa egyre inkább elmosódik. A fenyegetési térkép gyorsul, összetettebbé válik – és a reakcióidő kulcskérdéssé lép elő.

Fenyegetési szereplők és kampányok

Fő trend: a támadói ökoszisztéma érettebb,
gyorsabb és egyre inkább AI-támogatott.

A fenyegetési környezetben tovább erősödik a professzionalizálódás. Az államilag támogatott csoportok, fejlett APT-szereplők és kiberbűnözői hálózatok közötti különbségek egyre kevésbé élesek, miközben az eszköztáruk látványosan bővül.
Az OT-környezetekben aktív csoportok már nem csupán informatikai rendszereket kompromittálnak, hanem a fizikai folyamatok működését próbálják megérteni és befolyásolni. Eközben a ransomware-ökoszisztéma platformokon átívelővé vált: Windows, Linux és virtualizációs környezetek egyaránt célponttá váltak, ami jelentősen növeli az üzleti kockázatot.
Megjelent egy új, nehezen kategorizálható szereplőtípus is: az autonóm AI-agentek. Ezek nemcsak kódot generálnak vagy phishing kampányokat segítenek, hanem reputációs nyomásgyakorlásra, információs manipulációra és automatizált „befolyásolási műveletekre” is képesek.
A kampányok gyorsabban reagálnak a sérülékenységekre, rövidebb a támadási lánc, és gyakoribb a többkomponensű, moduláris felépítés. A határ az állami, bűnözői és technológiai szereplők között egyre inkább elmosódik.

YANAC
Heti összefoglaló

2026. február 17., kedd

Támadási technikák és malware

Fő trend: a technikák összetettebbek, a detektálás nehezebb, a támadások egyre inkább többcsatornásak és adaptívak.

A technikai és pszichológiai módszerek egyre szorosabban fonódnak össze. A social engineering kampányok már nem pusztán e-mailekre korlátozódnak: megjelent a papíralapú kripto-phishing, a QR-kód alapú támadás, valamint a DNS-csatornán keresztüli payload-staging is.
A phishing üzenetek minőségi ugráson mentek keresztül. Az AI-alapú szöveg- és tartalomgenerálás lehetővé teszi a célzott, természetes nyelvű és kontextusérzékeny csalásokat, amelyek nehezebben különíthetők el a legitim kommunikációtól. A mobilplatformok és üzenetküldő alkalmazások egyre gyakoribb terjesztési csatornák.
Malware-oldalon a loader-architektúra dominál: a kártékony komponensek futásidőben, több lépcsőben töltődnek be, sandbox-kerülő technikákkal és titkosított kommunikációval.
A ransomware-ek különösen veszélyes irányba fejlődtek: virtualizációs infrastruktúrák, ESXi-környezetek és heterogén rendszerek célzása már nem kivétel, hanem norma.
Emellett a zero-day sérülékenységek gyors kihasználása és az API-kulcsok kiszivárgása is rávilágít arra, hogy a támadási felület a fejlesztési és üzemeltetési gyakorlatokon keresztül is bővül.

OT / Kritikus infrastruktúra

Fő trend: az OT fenyegetések fizikai hatásúvá válnak, miközben az ipari digitalizáció növeli a sérülékenységet.

A kritikus infrastruktúrák elleni fenyegetések új szintre léptek. Az OT-környezetekben aktív szereplők már nemcsak IT-kompromittálást hajtanak végre, hanem az ipari vezérlési hurkokat, engineering workstationöket és fizikai folyamatokat célozzák.
Az energiaipar, a tengeri szállítmányozás és az elosztott energiatermelési rendszerek különösen kitettek. A ransomware-támadások OT-környezetben nem pusztán adatvesztést, hanem működési zavart és akár fizikai következményeket is okozhatnak.
Komoly problémát jelent, hogy az ICS-hez kapcsolódó sérülékenységek pontozása és priorizálása gyakran nem tükrözi a valós kockázatot. Az internetre exponált ipari eszközök és energiatároló rendszerek új támadási felületet nyitnak.
Az IT és OT határvonal tovább halványul, a virtualizáció és a digitális integráció pedig növeli a komplexitást – és ezzel együtt a támadási lehetőségeket is.

YANAC
Heti összefoglaló

2026. február 17., kedd

Kiberbiztonsági irányítás, védelem és policy

Fő trend: a védelem rendszerszintűbbé válik, de a technológiai fejlődés gyorsabb, mint a szervezeti adaptáció.

A védekezési oldal is strukturáltabbá válik. Nemzeti és nemzetközi szervezetek egyre inkább egységesített, keretrendszer-alapú megközelítést alkalmaznak a fenyegetések osztályozására, priorizálására és kezelésére.
A gyakorlat-központú felkészültség, a fenyegetés-intelligencia strukturált feldolgozása, valamint a zero trust és lifecycle-alapú technológiamenedzsment hangsúlyos irányok. A compliance mutatók javulnak, ugyanakkor a technikai érettség és incidensjelentési kultúra még nem egységes.
Az AI és a kvantumbiztonság már nem csupán kutatási témák, hanem policy-szintű megfontolások részévé váltak. A kritikus infrastruktúrák védelmében a nemzetközi együttműködés kulcsfontosságú.