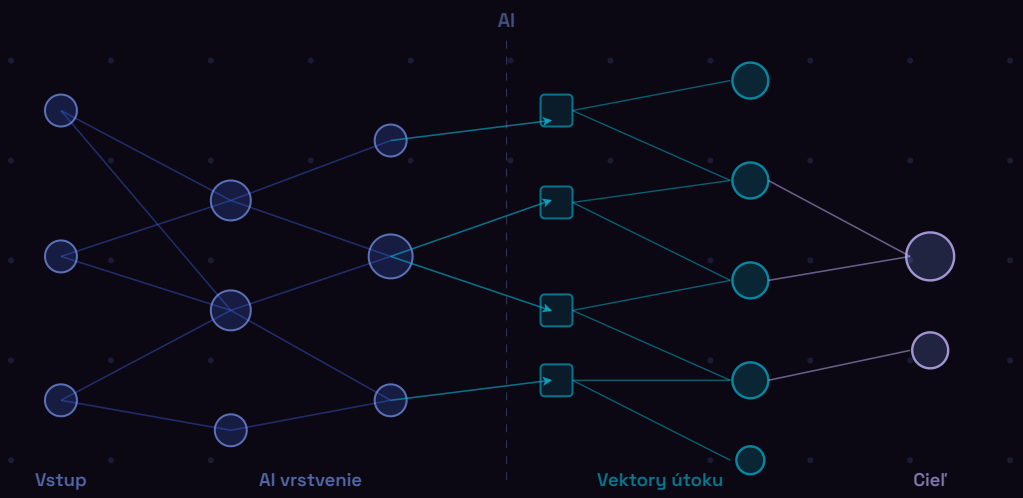


HROZBY · 2026

AI mení kybernetické útoky

Päť fáz útoku, ktoré umelá inteligencia zrýchlila alebo zlacnila, a čo z toho vyplýva pre obranu.

ÚVOD

Čo fungovalo vlani, dnes nestačí

Ešte pred dvoma rokmi vyžadoval sofistikovaný kybernetický útok technické znalosti, čas a zdroje. Dnes tieto bariéry prakticky neexistujú.

AI nástroje automatizujú to, čo predtým trvalo hodiny, a sprístupňujú pokročilé techniky útoku komukoľvek s internetovým pripojením. Nemení sa pritom len to, čo útočník dokáže. Mení sa aj to, koľko ľudí to dokáže.

Dôsledkom je vyšší počet útokov, vyššia rýchlosť a vyššia miera personalizácie. Nasledujúcich päť kapitol prechádza oblasti, kde je tá zmena najviditeľnejšia, a pri každej sa pýta to isté: čo to znamená pre firmu, ktorá sa bráni.

ČAS NA PRIESKUM

dni

→ minúty

Skenovanie a analýza, ktoré útočníkovi trvali dni, zvládne AI za minúty.

OKNO NA REAKCIU

týždne

→ hodiny

Medzi zverejnením zraniteľnosti a jej aktívnym zneužitím.

OBSAH BROŽÚRY

KAPITOLA 01

Automatické objavovanie zraniteľností

Tradičný útočník musel manuálne skenovať systémy, analyzovať výsledky a identifikovať využiteľné slabiny. Celý proces trval dni.

AI to zvláda za minúty. Nástroje postavené na veľkých jazykových modeloch dokážu automaticky prechádzať exponovanú infraštruktúru, identifikovať zastaraný softvér, odhaliť nesprávne konfigurácie a navrhnúť spôsob exploitácie, a to v škále, ktorú ľudský útočník nikdy nedosiahne.

Graf 1: Zrýchlenie fáz útoku: bez AI vs. s AI. Okno na reakciu obrancov sa skrátilo z dní na hodiny.

KRITICKÝ DÔSLEDOK

Pre organizácie to znamená, že okno medzi **zverejnením zraniteľnosti a jej aktívnym zneužitím** sa skrátilo z týždňov na hodiny. Patch management musí byť automatizovaný a riadený rizikom, nie manuálny harmonogram.

ČO TO MENÍ PRE VAŠE PROCESY

Tradičný patch cyklus (raz týždenne, manuálna prioritizácia) je dnes nedostatočný. Útočník sleduje zverejnené zraniteľnosti a začne ich zneužívať v priebehu hodín, teda dávno pred tým, než väčšina organizácií stihne nasadiť záplatu.

RÝCHLOSŤ

minúty

AI prechádza exponovanú infraštruktúru, kde ľudský útočník potrebuje dni.

OKNO REAKCIE

týždne → hodiny

Medzi zverejnením CVE a aktívnym zneužitím.

ŠKÁLOVANIE

Nejde len o rýchlosť. Jeden operátor dnes pokryje stovky cieľov súčasne.

KAPITOLA 02

Deepfake podvody pri social engineeringu

Phishingový e-mail s gramatickými chybami je minulosť. Dnes útočníci generujú hlasové správy, ktoré znejú ako váš CEO, videohovory s tvárou dôveryhodného kolegu a personalizované správy bez jedinej chyby.

Na vytvorenie presvedčivého hlasového klonu dnes stačia **tri sekundy zvuku**, či už z konferenčného hovoru, LinkedIn videa alebo firemnej prezentácie. Tieto techniky sa dnes aktívne využívajú pri podvodoch typu Business Email Compromise, kde útočník vydávajúci sa za manažéra žiada o urgentný bankový prevod.

„Tri sekundy zvuku stačia na hlasový klon. Váš CEO môže požiadať o prevod, aj keď práve sedí na stretnutí.“

Ako funguje deepfake útok krok za krokom

- Útočník zbiera verejné záznamy hlasu cieľovej osoby (LinkedIn, YouTube, podcasty).
- AI model trénuje hlasový klon za sekundy až minúty.
- Generuje sa audio správa alebo hovor napodobňujúci hlas manažéra.
- Obeť dostáva inštrukciu na urgentný prevod alebo zdieľanie prístupu.
- Podvod sa realizuje skôr, než ktokoľvek stihne overiť autenticitu hovoru.

KONTEXTOVÝ VEKTOR ÚTOKU

Business Email Compromise (BEC)

Deepfake audio dáva podvodu to, čo mu dovtedy chýbalo: dôveryhodnosť v priamom kontakte. Obeť nedokáže rozoznať falzifikát od originálu bez technického overenia, a na to pri urgentnom hovore nemá čas ani dôvod.

VSTUP

3 sek.

Zvukový záznam potrebný na vytvorenie presvedčivého hlasového klonu.

ZDROJE HLASU

LinkedIn video
YouTube prezentácia
Konferenčný hovor
Firemný podcast

TYP ÚTOKU

Business Email Compromise (BEC): urgentné platobné inštrukcie od „manažéra“.

KAPITOLA 03

AI agenti schopní samostatného pohybu sieťou

Toto je možno najzásadnejšia zmena. Nová generácia útočných nástrojov nie sú len skripty, ktoré vykonávajú vopred definované kroky. Sú to agenti, ktorí sa rozhodujú sami.

Po počiatočnom prieniku do systému dokáže AI agent samostatne mapovať sieť, identifikovať hodnotné ciele, prispôsobovať taktiku podľa prostredia a vyhýbať sa detekcii bez toho, aby útočník musel byť aktívne prítomný. Lateral movement, ktorý predtým vyžadoval skúseného operátora, sa stáva automatizovaným procesom.

Schéma 3: AI agent postupuje autonómne: žiadny ľudský operátor nepotrebuje byť aktívne prítomný po počiatočnom prieniku.

ČO TO ZNAMENÁ PRE DETEKCIU

Lateral movement riadený AI agentom nevyzerá ako tradičný útok. Mení taktiku podľa prostredia a vyhýba sa pravidlám napísaným pre statické skripty. Detekcia musí sledovať správanie, nie len podpisy.

TYP HROZBY

Autonómni útočné AI agenti

Rozhodujú sa sami, bez aktívnej prítomnosti útočníka.

KĽÚČOVÉ SCHOPNOSTI

Mapovanie siete
Identifikácia cieľov
Prispôsobenie taktiky
Vyhýbanie sa detekcii

ZÁSADNÁ ZMENA

Lateral movement, predtým vyžadujúci skúseného operátora, je teraz automatizovaný.

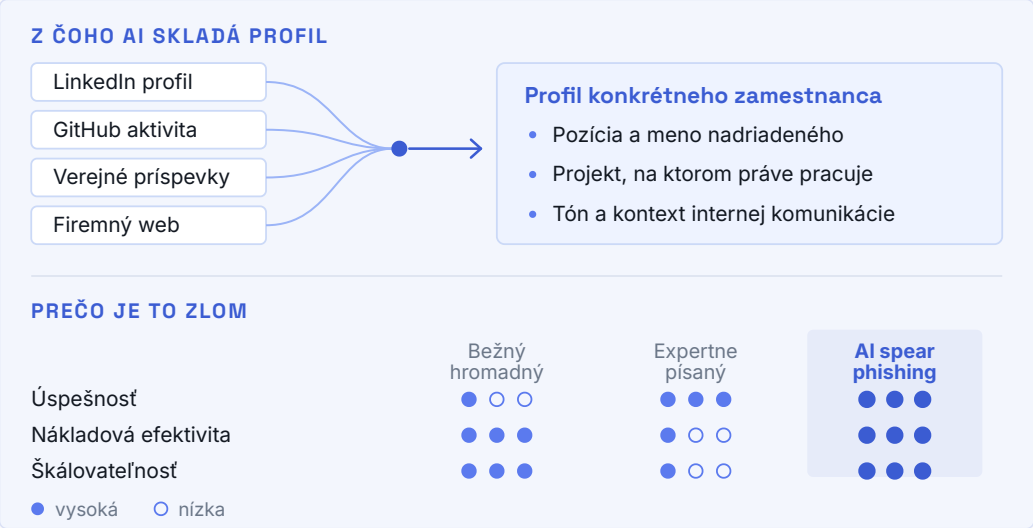
KAPITOLA 04

Hyper-personalizovaný phishing

Klasický phishing bol hromadný: rovnaká správa, tisíce príjemcov, nízka úspešnosť. AI to zmenila. Dnes každá správa vyzerá, akoby bola napísaná osobne pre vás.

Útočníci zbierajú OSINT o každom zamestnancovi, teda LinkedIn profil, GitHub aktivitu, verejné príspevky aj pracovnú pozíciu, a generujú správy šité na mieru konkrétnej osobe. Správa obsahuje meno nadriadeného, odkaz na reálny projekt a kontext, ktorý obeť pozná. Niet dôvod na podozrenie.

AI-generovaný spear phishing dosahuje rovnakú mieru úspešnosti ako phishing písaný expertom, pri zlomku nákladov a v násobku objemu.



Graf 4: Expert dosiahne vysokú úspešnosť, ale draho a v malom počte. Hromadný phishing je lacný a škálovateľný, ale neúčinný. AI spája oboje.

PREČO TU PRAVOPIS PRESTAL POMÁHAŤ

Rada „dávajte pozor na gramatické chyby" fungovala, kým phishing písal niekto, kto jazyk neovládal. Dnes je správa bezchybná, obsahuje meno nadriadeného a odkazuje na projekt, ktorý naozaj beží. Zamestnanec nemá podľa čoho pochybovať. Ťažisko obrany sa preto presúva z obsahu správy na jej kontext: kto ju posiela, odkiaľ a či odkaz smeruje tam, kam tvrdí.

PRÍSTUP K DÁTAM

OSINT

+ AI profiling

LinkedIn, GitHub, verejné príspevky. Každý zamestnanec má digitálnu stopu.

NÁKLADOVÁ EFEKTIVITA

zlomok

Náklady AI phishingu oproti expertne písanému, pri rovnakej úspešnosti.

OCHRANA

Technické filtre nestačia. Nutná behaviorálna analýza e-mailov a školenie zamestnancov na AI hrozby.

KAPITOLA 05

Automatická analýza ukradnutých dát

Útočník, ktorý prenikne do siete a exfiltruje terabajtové úložisko, čelil pred érou AI problému: ako rýchlo nájsť to cenné?

Dnes AI automaticky triedi ukradnuté súbory, identifikuje heslá, kľúče API, zmluvy a osobné údaje a zostavuje zoznam najhodnotnejších cieľov pre ďalší útok alebo predaj. Čas medzi exfiltráciou a zneužitím dát sa dramaticky skrátil.

Predtým: exfiltrované dáta čakali na manuálne spracovanie.
Dnes: AI zostaví zoznam najhodnotnejších cieľov v minútach.

Čo AI klasifikuje v ukradnutých dátach

- **Heslá a prístupové tokeny**: okamžité zneužitie na ďalší prienik alebo predaj na dark webe.
- **Kľúče API a certifikáty**: prístup do cloudových prostredí a tretích strán.
- **Zmluvy a obchodné tajomstvá**: priemyselná špionáž a vydieranie.
- **Osobné údaje (PII)**: predaj, identitné podvody, GDPR expozícia.
- **Interné plány a komunikácia**: príprava cieleného útoku na vedenie firmy.

DOPAD NA INCIDENT RESPONSE

Kratší čas od exfiltrácie k zneužitiu znamená, že **zálohovanie samo o sebe nestačí**. Organizácie musia detekovať a zastaviť exfiltráciu skôr, než k nej dôjde, nie len obnovovať dáta po útoku.

SPOJITOSŤ S MITRE ATT&CK

Táto fáza zodpovedá taktikám **Collection (TA0009)** a **Exfiltration (TA0010)** v MITRE ATT&CK frameworku. AI automatizuje celú kill chain od zberu po analýzu bez ľudskej intervencie.

DÁTA V RIZIKU

Heslá · API kľúče
Zmluvy · PII
Interná komunikácia

RÝCHLOSŤ KLASIFIKÁCIE

minúty

AI zostaví zoznam najhodnotnejších cieľov z TB dát za minúty.

MITRE ATT&CK

TA0009 Collection
TA0010 Exfiltration
AI automatizuje obe taktiky.

AI KILL CHAIN · CELKOVÝ POHĽAD

Päť fáz AI-riadeného útoku

Útočníci nasadzujú AI na každú fázu útoku, od prvého skenovania až po analýzu ukradnutých dát. Každá fáza je dnes rýchlejšia, lacnejšia a presnejšia než kedykoľvek predtým.

01 **Automatický prieskum** — minúty
Skenovanie infraštruktúry, zverejnených zraniteľností a konfigurácií

02 **Deepfake a social engineering** — 3 sek. zvuku
Hlasový klon manažéra, podvod typu BEC, personalizované správy

03 **Pohyb agenta sieťou** — bez operátora
Autonómne mapovanie siete a eskalácia oprávnení

04 **Hyper-personalizovaný phishing** — zlomok nákladov
Profilovanie z verejných zdrojov, správy šité na mieru, hromadný objem

05 **Analýza ukradnutých dát** — minúty
Triedenie terabajtov: heslá, API kľúče, zmluvy, osobné údaje

AI zasahuje do každej fázy reťazca. Útočník nemusí byť prítomný pri každom kroku.

KDE DO REŤAZCA VIDÍTE

Pri každej z piatich fáz existuje signál, ktorý sa dá zachytiť: skenovanie z neznámych adries, neobvyklý hovor tesne pred platbou, pohyb medzi zariadeniami mimo bežného vzoru, nárast podobných správ do schránok, odchádzajúci objem dát. Otázka nie je, či stopa existuje. Otázka je, či ju niekto číta.

ČO SA NEZMENILO

AI útok zrýchľuje a zlacňuje, ale nemení jeho vstupné body. Stále ide o používateľa, heslo alebo službu dostupnú z internetu. Základná hygiena preto neprestáva platiť. Prestáva len stačiť sama o sebe.

ZÁSADNÁ ZMENA

AI nenasadzujú útočníci len na jednu fázu. Každý krok útočného reťazca je dnes automatizovaný.

DÔSLEDOK PRE SOC

Manuálne procesy a statické pravidlá nestačia. Nutná AI-asistovaná detekcia v reálnom čase.

ODPOVEĎ

Nie nahradiť analytikov strojmi, ale dať im nástroje na tempo útočníka.

ODPOVEĎ

Čo to znamená pre váš SOC?

Ak útočníci nasadzujú AI na každú fázu útoku, od reconnaissance cez prienik až po exfiltráciu, obrana postavená na manuálnych procesoch a statických pravidlách nestačí.

Odpoveďou nie je nahradiť analytikov strojmi. Je to **dať analytikom nástroje, ktoré im umožnia pracovať rovnakou rýchlosťou, akou pracuje útočník.**

V exe:SOC integrujeme AI analytiku priamo do detekčných procesov. Nie ako marketingový buzzword, ale ako reálny nástroj, ktorý skracuje čas detekcie, redukuje false positives a pomáha analytikom sústrediť sa na to, čo skutočne vyžaduje ľudský úsudok.

Tri piliere obrany v AI ére

- **Behaviorálna analýza**: sledovanie anomálií v správaní, nie len zhody s podpismi. AI agent nevyzerá ako tradičný útok.
- **Automatizovaný patch management**: okno medzi CVE a exploitom sa skrátilo na hodiny. Manuálny cyklus nestačí.
- **Detekcia exfiltrácie v reálnom čase**: zálohovanie nezachráni dáta, ktoré útočník už skopíroval. Dôležité je zachytiť prenos ešte pred jeho dokončením.

Útočník pracuje s AI, 24/7, bez prestávok. Váš SOC musí mať nástroje, ktoré držia krok.

EXE:SOC PRÍSTUP

AI analytika v detekčnom procese

Integrujeme AI nástroje do Microsoft Sentinel a detekčných pracovných tokov. Výsledok: kratší MTTD (Mean Time to Detect), menej falošných poplachov, analytici sa sústredia na skutočné incidenty.

TRI PILIERE

1. Behaviorálna analýza

2. Auto patch mgmt

3. Detekcia exfiltrácie

METRIKA

MTTD

Mean Time to Detect. Čím rýchlejšie útočí protistrana, tým viac o obrane rozhoduje práve táto hodnota.

PLATFORMA

Microsoft Sentinel + AI analytika + tím exe:SOC analytikov.

AKČNÝ CHECKLIST

Päť otázok pre váš bezpečnostný tím

Otázky na preverenie pripravenosti vašej organizácie voči AI-posilneným hrozbám. Každá záporná odpoveď je signál na riešenie.

- [ ] **Zvládate patch management v hodinách, nie v dňoch?**
  Okno medzi zverejnením CVE a exploitom sa skrátilo z týždňov na hodiny. Manuálny týždenný cyklus vás robí zraniteľnými.

- [ ] **Máte zavedený overovací protokol pre nezvyčajné platobné požiadavky?**
  Deepfake hlasové klony sú presvedčivé. Druhý kanál overenia, napríklad osobný hovor, je nevyhnutný aj pre „urgentné“ situácie.

- [ ] **Detekujete abnormálny lateral movement v sieti v reálnom čase?**
  AI agent sa pohybuje inak ako tradičný skript. Pravidlá napísané pre staré techniky ho nevychytia. Nutná behaviorálna analýza.

- [ ] **Sú vaši zamestnanci školení na AI-generovaný phishing?**
  AI spear phishing neobsahuje gramatické chyby ani podozrivé znaky. Klasické školenie o phishingu nestačí, treba nové scenáre.

- [ ] **Monitorujete exfiltráciu dát proaktívne, nie len zálohy?**
  Zálohy zachránia dáta pre obnovu, ale nie pre dôvernosť. Ak útočník dáta skopíroval, záloha situáciu nerieši.

SKÓRE

5/5 Áno
Dobrá východisková pozícia

3–4/5 Áno
Prioritizujte záporné

0–2/5 Áno
Konzultujte so SOC

KONZULTÁCIA

exe:SOC vám prejde jednotlivé body a navrhne prioritizáciu. 30 minút, zdarma.

KONTAKT

exesoc.sk/contact
exesoc@exe.sk

EXE:SOC · CHECKLIST PRIPRAVENOSTI

ZÁVER

Stíhate tempo, akým sa dnes útočí?

AI zmenila útočné reťazce zo synchrónnych, ľudsky riadených operácií na asynchrónne, autonómne procesy. Päť hrozieb popísaných v tejto brožúre nie sú budúcnosť. Sú to metódy, ktoré sa dnes aktívne používajú.

Odpoveď na AI hrozby nie je strojom nahradiť analytikov. Je to dať im nástroje, ktoré im umožnia pracovať rovnakou rýchlosťou ako útočník.

Prejdeme s vami, kde vám manuálne procesy berú čas a kde vie AI reálne pomôcť detekcii. Konzultácia je zdarma a trvá 30 minút.

Bezplatná konzultácia s exe:SOC

Zistíme spoločne, kde sú vaše najväčšie expozície voči AI-posilneným hrozbám a ako ich riešiť prakticky.

Web
exesoc.sk/contact

E-mail
exesoc@exe.sk

Telefón
+421 2 3211 0010

exesoc.sk/contact

MANAGED SOC

exe:SOC: monitoring počas pracovných hodín s on-call rotáciou pre kritické incidenty, AI-asistovaná detekcia, tím analytikov.

PLATFORMA

Microsoft Sentinel · MITRE ATT&CK · podpora pre NIS2

EXE A.S.

Managed Security Operations Center, súčasť skupiny exe a.s., Slovensko.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Funded by the European Union

Realizované s podporou Európskej únie v zmysle grantovej zmluvy k projektu EXE-SOC č. 101128063. Názory vyjadrené v tomto dokumente sú výlučne názormi autora(-ov) a nemusia odrážať stanoviská Európskej únie.