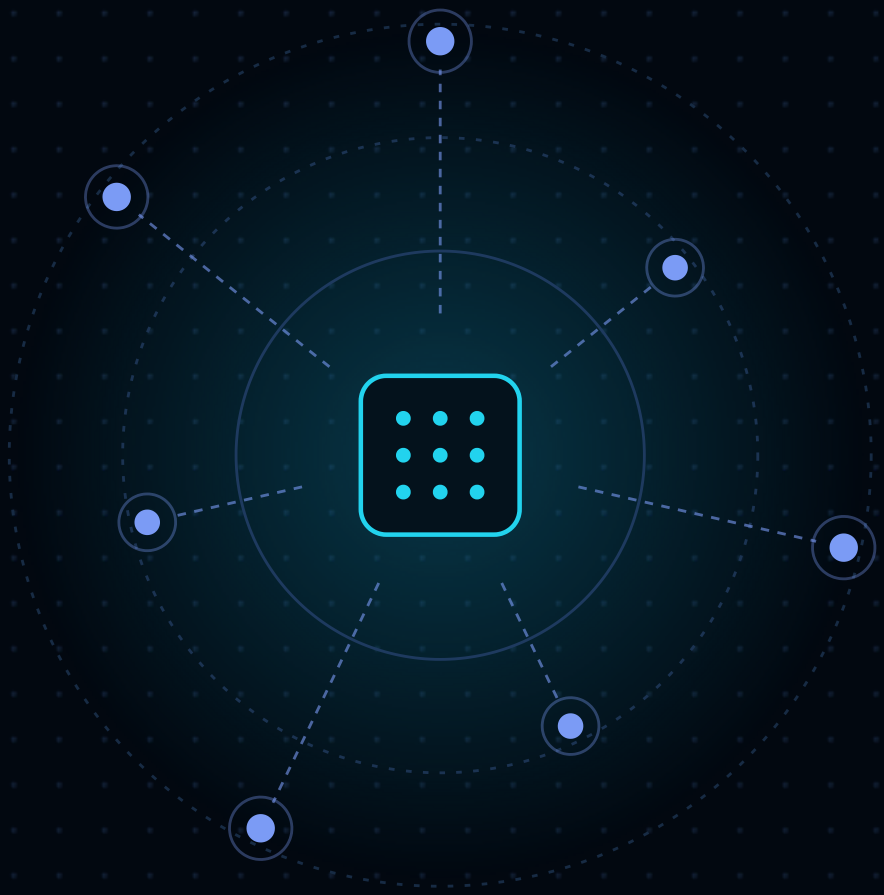


DRUHY ÚTOKOV

Sedem útokov a ako im odolať

Ako útok vyzerá zvnútra, podľa čoho ho spoznáte a čo proti nemu vo firme skutočne funguje.

ÚVOD

Väčšina útokov nezačína technicky komplikovane

Firewall a antivírus nie sú zárukou bezpečnosti. Znižujú riziko, ale nezastavia každý útok. Útočníci najčastejšie nevyužívajú zložitú techniku. Využívajú dôveru, nepozornosť alebo jednu obyčajnú chybu.

Táto brožúra prechádza sedem útokov, s ktorými sa firmy stretávajú najčastejšie. Pri každom nájdete rovnakú štruktúru: ako útok reálne prebieha, čo z neho má útočník, podľa akých signálov ho vie zachytiť bezpečnostný dohľad a čo proti nemu funguje na vašej strane.

Nie je to zoznam nástrojov na nákup. Je to mapa toho, ako útok vyzerá zvnútra, aby ste ho spoznali skôr, než sa prejaví na faktúre, na prevádzke alebo na povesti firmy.

- **Strana útočníka**
  Čo robí, prečo to robí a čo tým získa.
- **Strana obrany**
  Čo vidí SOC a čo viete nastaviť vy.

OBSAH

VÝCHODISKO

Prečo samotné nástroje nestačia

Nástroje znižujú riziko. Význam alertom ale dávajú až ľudia a procesy.

JEDEN ÚTOK, TRI ODDELENÉ STOPY

Firewall vidí sieť, EDR zariadenie, identita prihlásenia. Každý z nich má pravdu a žiadny z nich nevidí útok celý.

ČO TO ZNAMENÁ V PRAXI

Alert je len začiatok

Niekto ho musí vyhodnotiť a rozhodnúť o ďalšom postupe. Bez procesu sa dôležitý signál stratí a v záplave hluku môže uniknúť prebiehajúci útok.

ČO POMÁHA

Spoločný pohľad naprieč

Až keď sa udalosti z identity, e-mailu, endpointov a siete vyhodnocujú spoločne, dá sa určiť závažnosť a koordinovať reakcia.

Podstatné: firewall a antivírus nie sú zárukou bezpečnosti. Znižujú riziko, ale nezastavia každý útok. Bez kontextu zostávajú len „hlásičmi požiaru“: povedia, že niečo horí, ale nie čo, kde a či na to treba reagovať práve teraz.

AKO TO FUNGUJE

SOC = ľudia + procesy + technológie

Tri piliere musia fungovať spoločne. Ak vypadne ktorýkoľvek z nich, oslabia sa aj zvyšné dva.

PILIER 01

Ľudia

Rozhodnutie a koordináciu robia analytici, nie nástroj.

- L1 analytik prijíma a triedi alerty
- L2 preveruje súvislosti a hľadá príčinu
- Incident responder koordinuje izoláciu účtu alebo zariadenia
- Threat hunter hľadá skryté hrozby
- SOC manažér riadi priority aj komunikáciu

PILIER 02

Procesy

Určujú, čo sa stane po tom, čo alert vznikne.

- Triage určí dôveryhodnosť a urgenciu
- Klasifikácia stanoví typ a dopad
- Eskalácia určí, kto má konať
- Komunikácia dá zákazníkovi jasný stav
- Lessons learned menia skúsenosť na lepšiu ochranu

PILIER 03

Technológie

Dodávajú dáta a kontext, z ktorého sa skladá obraz.

- SIEM koreluje udalosti naprieč zdrojmi
- EDR/XDR sleduje zariadenia
- Identity systémy ukazujú rizikové prihlásenia
- Firewally a IDS/IPS dopĺňajú sieťový kontext
- Threat intelligence pridáva známe hrozby

Podstatné: SIEM bez analytikov, kontaktov, pravidiel eskalácie a oprávnení na zásah incident nevyrieši. Technológia poskytuje dáta, rozhodnutie a koordináciu robia ľudia.

01

ÚTOK 01 / 07

FALOŠNÉ MICROSOFT PRIHLÁSENIE

Najbežnejší vstup do firmy. Nepotrebuje zraniteľnosť, stačí jeden unáhlený klik.

01 **Správa o vypršaní hesla**

02 **Kópia prihlasovacej stránky**

03 **Prevzatie schránky**

04 **Útok zvnútra firmy**

AKO ÚTOK PREBIEHA

Zamestnancovi príde správa, že mu vyprší heslo alebo že je účet zablokovaný. Odkaz vedie na prihlasovaciu stránku, ktorá je kópiou tej pravej. Rozdiel býva len v doméne. Heslo, ktoré tam používateľ zadá, má útočník k dispozícii v priebehu sekúnd.

CIEĽ ÚTOČNÍKA

Nie je ním samotné heslo, ale to, čo je za ním. Z prevzatej schránky sa dá čítať korešpondencia, sťahovať dokumenty a písať kolegom aj dodávateľom z adresy, ktorej dôverujú.

AKO TO ZACHYTÍ SOC

Samotné prihlásenie nemusí vyzerať podozrivo. Podozrivé je až to, čo nasleduje: prístup z inej krajiny, nová registrácia MFA, pravidlo presúvajúce prichádzajúcu poštu do archívu alebo náhly nárast odoslaných správ.

AKO SA BRÁNIŤ

Viacfaktorové overenie a podmienený prístup. Ak k incidentu už došlo, nestačí zmeniť heslo. Treba ukončiť všetky aktívne relácie, inak útočník zostáva prihlásený.

VAROVNÉ SIGNÁLY

- Prihlásenie z novej krajiny
- Nová registrácia MFA
- Pravidlo na presun pošty
- Nárast odoslaných správ
- Neznáme zariadenie

Prečo to funguje: správa neobsahuje nič škodlivé, čo by dokázala zachytiť e-mailová ochrana. Jediné, čo od obete žiada, je aby sa prihlásila, teda presne to, čo robí každý deň.

02

ÚTOK 02 / 07

RANSOMWARE A ŠIFROVANIE DÁT

Šifrovanie nie je prvý krok útoku. Je posledný.

01 **Nenápadný vstup do siete**

02 **Zbieranie oprávnení**

03 **Kópia dát von**

04 **Šifrovanie a výkupné**

AKO ÚTOK PREBIEHA

Vstup býva nenápadný: príloha, ukradnuté heslo alebo neaktualizovaná služba dostupná z internetu. Nasleduje obdobie, keď útočník mapuje sieť, hľadá zálohy a zbiera oprávnenia. Šifrovanie spustí až vtedy, keď má istotu, že obnova nebude jednoduchá.

CIEĽ ÚTOČNÍKA

Zastaviť prevádzku a vynútiť platbu. Dáta sa spravidla najprv skopírujú von, takže aj firma s funkčnými zálohami čelí hrozbe ich zverejnenia.

AKO TO ZACHYTÍ SOC

Prípravná fáza je hlučnejšia než samotné šifrovanie. Vidno v nej pokusy vypnúť ochranu, spúšťanie administrátorských nástrojov na staniciach, kde nemajú čo robiť, a prístup k súborom v objeme, aký bežný používateľ nevygeneruje.

AKO SA BRÁNIŤ

EDR dokáže podozrivý proces zastaviť a zariadenie odpojiť od siete. Segmentácia rozhoduje o tom, či incident zostane na jednom oddelení. Zálohy majú zmysel len oddelené od domény a pravidelne skúšobne obnovené.

VAROVNÉ SIGNÁLY

- Vypnutá ochrana na stanici
- Admin nástroje mimo IT
- Masové zmeny súborov
- Pohyb medzi zariadeniami
- Odchádzajúci objem dát

Kde sa to láme: medzi prvým prienikom a šifrovaním uplynú spravidla dni až týždne. To je celý priestor, ktorý firma na zásah má, a bez monitoringu prejde nepovšimnutý.

03

ÚTOK 03 / 07

PODVODNÁ FAKTÚRA OD „RIADITEĽA“

Útok bez malvéru. Terčom nie je systém, ale schvaľovací proces.

01 **Správa v mene konateľa**

02 **Zmena bankového spojenia**

03 **Tlak na rýchlosť a mlčanie**

04 **Odoslaná platba**

AKO ÚTOK PREBIEHA

Správa prichádza v mene konateľa alebo dlhoročného dodávateľa, spravidla v čase, keď je adresát pod tlakom. Žiada úhradu mimo poradia alebo oznamuje zmenu bankového spojenia. Býva doplnená prosbou nekomunikovať o veci ďalej.

CIEĽ ÚTOČNÍKA

Jediná platba na jeho účet. Nič sa nešifruje, nič nevypadne. Firma sa o strate dozvie až vtedy, keď sa ozve skutočný dodávateľ s otázkou, prečo faktúra nie je uhradená.

AKO TO ZACHYTÍ SOC

Ak útoku predchádzalo prevzatie schránky, stopy tam sú: prihlásenie z neznámeho zariadenia, pravidlo na preposielanie, zmazané odoslané správy. Pri podvrhnutej doméne pomáha kontrola pravosti odosielateľa.

AKO SA BRÁNIŤ

Zmena bankového účtu sa overuje telefonicky na číslo z existujúcej zmluvy, nie na číslo z e-mailu. Nad dohodnutú sumu dvojité schválenie. Na vlastnej doméne nastavené SPF, DKIM a DMARC.

VAROVNÉ SIGNÁLY

- Doména na jeden znak iná
- Žiadosť o zmenu účtu
- Nová adresa pre odpoveď
- Pravidlo na preposielanie
- Tlak na mlčanlivosť

Čo to stojí: tento útok nemá technickú stopu, na ktorú by sa dalo upozorniť. Zastaví ho len proces, ktorý platí rovnako pre konateľa aj pre účtovníčku a ktorý sa nedá obísť naliehavou správou.

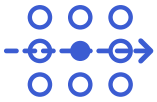
Ďalšie hrozby, ktoré treba poznať

Krátke situácie pre používateľov aj IT tím.

04

Deepfake a hlasové podvody

Hlas konateľa sa dá naklonovať z krátkej nahrávky. Stačí videovizitka, podcast alebo záznam z konferencie. Telefonát potom znie vierohodne vrátane intonácie a pauz. Overenie preto nemôže stáť na tom, koho na linke počujeme.



05

Password spraying a brute force

Password spraying skúša jedno rozšírené heslo naprieč všetkými známymi účtami, takže nespustí uzamknutie konkrétneho konta. Brute force ide opačne: jedno konto, tisíce pokusov. V logoch po oboch zostane séria neúspešných prihlásení a jedno úspešné, ktoré medzi nimi ľahko zapadne.

06

MFA fatigue

Heslo už útočník má a spolieha sa na to, že používateľ výzvu odklikne. Notifikácie chodia v sérii, najčastejšie večer alebo cez víkend. Platí jednoduché pravidlo: výzvu, ktorú som nevyvolal, zamietam a hlásim. Number matching tento útok prakticky odstráni.

07

Zraniteľné verejné služby

Testovací server, na ktorý sa zabudlo. VPN bez poslednej záplaty. Úložisko omylom otvorené do internetu. Útočník tieto veci nehľadá cielene u vás. Skenuje celé rozsahy a vyberie si, čo je otvorené. Základ obrany je zoznam všetkého dostupného zvonku a menovitý vlastník pri každej položke.

Spoločný menovateľ: žiadny z týchto štyroch útokov nelomí šifrovanie ani nehľadá zero-day. Stačí im naliehavosť, zvyk alebo služba, na ktorú sa zabudlo. Všetky štyri pritom zanechávajú stopu v logoch, ktoré firma už má.

ZHRNUTIE

Štyri vety, ktoré sa oplatí zapamätať

01 **Väčšina útokov nezačína technicky komplikovane.**

Často využívajú dôveru, nepozornosť alebo jednoduchú chybu.

02 **Najčastejším vstupom je používateľ, heslo alebo služba.**

Phishing, slabé identity a internetová expozícia otvárajú dvere.

03 **Prevencia je dôležitá, ale bez detekcie firma nevie, čo sa deje.**

Monitoring ukazuje, či niekto ochranné vrstvy práve obchádza.

04 **SOC pomáha odhaliť útok počas jeho priebehu.**

Spája signály, určuje prioritu a podporuje reakciu.

Prevencia rieši prvé dve fázy. Všetko za nimi je otázka toho, či sa niekto na dáta pozerá, a ako rýchlo.

ČO Z TOHO VYPLÝVA

Útok nie je moment

Je to postupnosť krokov, ktorá trvá dni až mesiace. Každý z nich zanecháva stopu. Otázka je len, či ju niekto číta.

KDE JE PÁKA

Skrátiť čas, nie vylúčiť útok

Cieľom nie je nulový počet pokusov. Cieľom je zachytiť útok skôr, než sa dostane k fáze s reálnym dopadom.

Čo SOC nie je

Realistické očakávania pomáhajú nastaviť spoluprácu, ktorá naozaj funguje.

Nie je zárukou, že útok nenastane.

Žiadna ochrana nie je stopercentná. SOC skracuje čas od odhalenia po reakciu, ale nevie garantovať zastavenie každého pokusu ešte pred prvým dopadom.

Nie je iba nástroj alebo softvér.

SIEM bez analytikov, kontaktov, pravidiel eskalácie a oprávnení na zásah incident nevyrieši. Technológia poskytuje dáta, rozhodnutie a koordináciu robia ľudia.

Nenahrádza bezpečnostnú hygienu.

Patchovanie, MFA, minimálne oprávnenia, segmentácia a testované zálohy zostávajú základom. SOC tieto opatrenia dopĺňa monitoringom a reakciou.

Nevidí dáta, ktoré sa nezbierajú.

Ak systém neposiela udalosti alebo má príliš krátku retenciu, SOC nevie spätne poskladať celý priebeh incidentu. Chýbajúce logy vytvárajú slepé miesta.

Bez zákazníka nepozná obchodný dopad.

SOC potrebuje vedieť, ktoré služby a dáta sú kritické, kto je ich vlastník, koho kontaktovať a aké zásahy môže bezpečne vykonať bez ďalšieho schválenia.

Čo SOC naopak je: vrstva, ktorá z roztrúsených udalostí poskladá obraz, určí prioritu a odovzdá ju tomu, kto môže konať. Jeho hodnota rastie s tým, koľko systémov doň zapojíte a ako presne máte vopred dohodnuté, čo smie urobiť.

PRVÝ PRAKTICKÝ KROK

Čo si spísať ešte tento týždeň

Začnite tým, čo máte, čo z toho vidíte a kto môže konať. Tri otázky, na ktoré stačí hodina s vaším IT.

1 Zdroje

Spíšte používateľské a administrátorské identity, počítače, servery, firewally, cloudové služby a kritické aplikácie. Pri každom zdroji určte vlastníka, význam pre prevádzku, dostupnosť z internetu a prioritu ochrany.

2 Udalosti

Zistite, aké bezpečnostné logy jednotlivé systémy poskytujú, či sa skutočne zbierajú, ako dlho sa uchovávajú a kto ich kontroluje. Označte kritické zdroje bez logovania alebo s nedostatočnou retenciou.

3 Reakcia

Určte primárne a záložné kontaktné osoby, priority incidentov a komunikačný kanál. Vopred dohodnite povolené zásahy, napríklad vypnutie účtu, ukončenie relácií, blokovanie adresy alebo izolovanie zariadenia.

Ak pri niektorej z troch otázok zaváhate, našli ste miesto, kde začať. Nie je to dôvod kupovať ďalší nástroj. Je to dôvod získať viditeľnosť do toho, čo už máte.

exe : SOC

ĎALŠÍ KROK

Ktorý z tých siedmich by ste dnes zachytili?

Konzultácia zdarma, 30 minút

Prejdeme s vami sedem útokov z tejto brožúry a pri každom si povieme, či a odkiaľ by ste ho dnes videli. Bez záväzkov a bez prípravy na vašej strane.

exesoc.sk/contact

exesoc@exe.sk
+421 2 3211 0010

Naskenujte telefónom

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union

Tento projekt je spolufinancovaný Európskou úniou v zmysle grantovej zmluvy k projektu EXE-SOC č. 101128063. Názory a stanoviská vyjadrené v tomto dokumente sú výlučne názormi autorov a nemusia nevyhnutne odrážať názory Európskej únie. Európska únia za ne nenesie zodpovednosť.