exe SOC

DIGITÁLNA BROŽÚRA

DETEKCIA HROZIEB

Útočník je už vnútri

Prečo o prieniku do siete neviete celé mesiace, čo za ten čas útočník stihne a ako ten čas skrátiť.

ÚVOD

Otázka nie je či, ale kedy to zistíte

Väčšina firiem si kybernetický útok predstavuje ako hlasnú udalosť. Zašifrované disky, výpadok systémov, výzva na zaplatenie výkupného. V skutočnosti sa to podstatné deje potichu a dávno predtým.

Útočník, ktorý sa dostane do siete, nemá dôvod na seba upozorňovať. Jeho cieľom je zostať čo najdlhšie nepovšimnutý, zmapovať prostredie a nájsť to, čo má pre neho hodnotu. Škoda nevzniká v momente vstupu. Vzniká počas celého obdobia, keď sa útočník v prostredí voľne pohybuje.

Táto brožúra vedie jedným príbehom v troch kapitolách: ako sa útočník dovnútra dostane, ako dlho tam vydrží a čo o vašej firme vie ešte predtým, než čokoľvek spustí. Na konci nájdete päť otázok pre váš tím.

POZNÁMKA K ČÍSLAM

Údaje uvedené v brožúre vychádzajú z verejne dostupných priemyselných štatistík a bezpečnostných správ. Konkrétne hodnoty sa medzi jednotlivými správami a rokmi líšia. Zmyslom čísel tu nie je presná metrika, ale rád veličiny: ide o mesiace, nie o hodiny.

OBSAH

01 **Dostane sa dnu**
Prieniky do systémov sú dnes najčastejšou kategóriou incidentov. Prečo preventívne nástroje na hranici siete nestačia.

02 **A zostane tam mesiace**
Čo je dwell time, prečo detekcia trvá tak dlho a čo každý ďalší deň v prostredí útočníka reálne stojí.

03 **Vie o vás viac, než si myslíte**
Päť informácií, ktoré útočník o vašej firme pozná z verejných zdrojov ešte pred prvým pokusom o prienik.

KAPITOLA 01

Dostane sa dnu

Prienik do systémov nie je okrajový scenár. Je to najčastejšia podoba dnešného incidentu.

60 % **bezpečnostných incidentov**
tvoria prieniky do systémov. Táto kategória predbehla všetky ostatné.

Čo prienik v praxi znamená

Prienik do systémov neznamená, že útočník zaútočil a vy ste útok zaznamenali. Znamená, že sa dostal dovnútra, pohyboval sa laterálne cez vašu sieť, hľadal hodnotné dáta a systémy, a väčšina organizácií to zistila až po dlhom čase.

- Útočníci sa dostali do vnútra a pohybovali sa laterálne naprieč prostredím.
- Priemerný čas do odhalenia narušenia sa podľa dlhodobých priemyselných metrík pohybuje v stovkách dní.
- Škody nenastávajú pri vstupe, ale počas pobytu útočníka v systéme.

Toto je kľúčový posun v chápaní hrozieb. Útočník nespôsobí škodu vo chvíli, keď prekoná perimeter. Spôsobuje ju počas mesiacov, keď sa v systéme pohybuje nepovšimnutý a postupne si rozširuje prístup.

„Otázka nie je, či nás napadnú. Otázka je, ako dlho tam budú, kým ich objavíme.“

Formulácia, ktorá mení spôsob, akým sa meria úspech bezpečnostného tímu

Prečo reaktívna detekcia nestačí

Väčšina bezpečnostných tímov je nastavená reaktívne. Čaká na alert a potom rieši. Lenže útočník, ktorý sa pohybuje laterálne po sieti, nemusí spustiť žiadny alarm, ak na jeho techniky nie sú napísané detekčné pravidlá.

Laterálny pohyb, perzistencia a príprava na exfiltráciu sú fázy útoku, ktoré prebiehajú potichu. Práve preto je podstatné mať detekciu, ktorá tieto signály aktívne hľadá, aj keď samy osebe nevyzerajú ako incident.

KAPITOLA 02

A zostane tam mesiace

Čas medzi prienikom a odhalením je najdrahšia veličina v celom incidente.

277

dní, teda takmer deväť mesiacov

trvá podľa viacerých bezpečnostných štúdií organizáciám, kým incident identifikujú a zastavia.

Predstavte si, že sa útočník dostane do vašej siete dnes. Nezačne okamžite šifrovať dáta ani vypínať systémy. Namiesto toho zostane nenápadný. Sleduje, zbiera informácie, hľadá prístupové údaje, mapuje infraštruktúru a čaká na správny moment.

ČO JE DWELL TIME

Čas, ktorý útočník strávi vo vnútri nepovšimnutý

Počíta sa od prvého úspešného prieniku po odhalenie a zastavenie útoku. Nie je to len štatistika. Je to presne ten čas, ktorý útočník využíva na prieskum siete, získavanie oprávnení a prípravu finálnej fázy útoku.

Prečo trvá detekcia tak dlho

Mnohé organizácie investovali do firewallov, antivírusov aj riešení EDR. Problém spravidla nie je nedostatok nástrojov. Problém je, že nikto aktívne nesleduje, čo sa deje. Každý deň vznikajú tisíce udalostí a logov, medzi ktorými sa strácajú prvé indikátory kompromitácie:

- podozrivé prihlásenia
- neobvyklé pohyby používateľských účtov
- komunikácia s podozrivými servermi
- pokusy o eskaláciu oprávnení
- laterálny pohyb útočníka v sieti

Jednotlivo môžu tieto udalosti vyzerať neškodne. Až keď sa spoja do jedného príbehu, začne byť zrejmé, že ide o útok. Práve v tomto bode veľa organizácií zlyháva: dáta majú, ale nikto ich nespája dohromady.

POZOR NA ZÁMENU POJMOV

Zbierať logy neznamená mať detekciu

Logy uložené v archíve pomôžu pri forenznej analýze po incidente. Detekcia znamená, že sa na tie dáta niekto alebo niečo pozerá priebežne a vie rozpoznať vzorec útoku. Bez toho zostáva ukladanie logov len nákladom na úložisko.

Cena neskorej detekcie

Každý deň, počas ktorého útočník zostáva v prostredí, zvyšuje potenciálne škody. Dôjsť môže k úniku citlivých údajov, prerušeniu prevádzky, finančným stratám, poškodeniu reputácie aj k porušeniu legislatívnych požiadaviek.

Mnohé organizácie pritom zistia, že boli kompromitované, až v momente, keď ich kontaktuje zákazník, obchodný partner alebo regulačný orgán. Vtedy už býva neskoro na čokoľvek iné než na zmierňovanie následkov.

„Ak by sa dnes útočník dostal do vašej siete, ako dlho by trvalo, kým by si to niekto všimol? Hodiny? Týždne? Alebo práve tých 277 dní?“

Čo čas do odhalenia reálne skracuje

Neexistuje jeden nástroj, ktorý by problém vyriešil. Funguje kombinácia troch vecí, z ktorých každá je bez tých ostatných výrazne slabšia:

- **Centralizovaný zber logov** zo všetkých kľúčových systémov, nie len z tých, ktoré sa nastavili ako prvé.
- **Korelácia udalostí** naprieč prostredím, ktorá z jednotlivých neškodne vyzerajúcich udalostí poskladá vzorec útoku.
- **Tím, ktorý výstupy skutočne vyhodnocuje.** Samotné nasadenie technológie bez ľudí, ktorí ju sledujú, čas do odhalenia neskráti.

KDE ZAČAŤ, AK NEVIETE, KDE STOJÍTE

Východiskom je bezpečnostné posúdenie prostredia. Čo všetko logujete, ktoré systémy zostávajú bez dohľadu a či viete spätne zrekonštruovať aktivitu za posledné mesiace. Ak na tieto otázky neviete odpovedať, prvým krokom nie je nákup ďalšieho nástroja, ale získanie viditeľnosti.

KAPITOLA 03

Vie o vás viac, než si myslíte

Útok sa často začína informáciami, ktoré sú voľne dostupné. Bez toho, aby útočník čokoľvek prelomil.

Mnoho informácií, ktoré útočníci potrebujú na prípravu útoku, je verejne dostupných. Nemusia sa nikam nabúravať ani obchádzať bezpečnostné mechanizmy. Stačí vedieť, kde hľadať.

Preto je jednou z najdôležitejších otázok modernej kybernetickej bezpečnosti: viete, čo všetko o vašej organizácii vidí internet? Nasleduje päť informácií, ktoré útočníci často poznajú ešte predtým, ako spustia prvý útok.

1 Ktoré porty a služby máte otvorené do internetu

Každé zariadenie pripojené k internetu zanecháva stopu. Pomocou verejných databáz a skenovacích nástrojov útočník rýchlo zistí, ktoré servery prevádzkujete, aké služby sú dostupné zvonku, ktoré porty sú otvorené a aké technológie používate. Pre vás ide o bežnú prevádzku. Pre útočníka je to mapa vstupných bodov.

2 Aký softvér používate

Webové stránky, riešenia VPN, e-mailové systémy či vzdialené prístupy často prezrádzajú, na akých technológiách fungujú. Ak útočník zistí konkrétny produkt alebo verziu, okamžite si overí známe zraniteľnosti, verejne dostupné exploity aj odporúčané techniky útoku.

Preto sa často stáva, že útok nie je cielený na konkrétnu firmu. Útočník vyhľadáva organizácie používajúce zraniteľnú technológiu a potom si vyberá najľahší cieľ.

3 E-mailové adresy vašich zamestnancov

Firemné weby, sociálne siete, pracovné portály, tlačové správy aj verejné registre bežne obsahujú adresy zamestnancov, kontakty na vedenie, údaje o IT oddelení aj organizačnú štruktúru. Vďaka nim vie útočník pripraviť presvedčivý phishingový útok alebo sa vydávať za interného zamestnanca. Čím viac informácií má, tým dôveryhodnejšie útok pôsobí.

4 Či unikli vaše prihlasovacie údaje

Každý rok dochádza k únikom miliónov používateľských účtov. Zamestnanci si často neuvedomujú, že ich firemná adresa alebo heslo sa mohli objaviť v niektorom z historických únikov. Útočníci tieto databázy aktívne monitorujú a pri náleze sa pokúsia o:

- útoky typu credential stuffing
- prevzatie účtov
- prístup do firemných systémov
- kompromitáciu cloudových služieb

Často stačí jediný účet, aby sa otvorili dvere do celej organizácie.

5 Kde máte slepé miesta v monitoringu

Toto je informácia, ktorú si firmy uvedomujú najmenej. Útočníci počas prieskumu testujú nielen technológie, ale aj schopnosť organizácie reagovať. Sledujú, ktoré aktivity vyvolajú reakciu, ktoré systémy sú monitorované, ako rýchlo organizácia reaguje a ktoré časti infraštruktúry zostávajú bez dohľadu.

Ak objavia miesto, kde monitoring nefunguje alebo chýba úplne, získavajú priestor na pohyb bez povšimnutia. Práve tieto slepé miesta často rozhodujú o úspechu útoku.

PRAKTICKÉ OPATRENIE

Jedno heslo navyše nestačí

Kontrola domény voči databázam únikov má zmysel len vtedy, ak po náleze nasleduje akcia: vynútená zmena hesla, overenie, či sa účet nepoužil inde, a zapnutá viacfaktorová autentifikácia. Bez nej zostáva uniknuté heslo použiteľné.

„Moderná bezpečnosť nie je len o ochrane infraštruktúry. Je aj o pochopení toho, čo všetko o vás dokáže zistiť niekto zvonku.“

ČO S TÝM

Päť otázok pre váš tím

Nemusíte kupovať nič nové, aby ste zistili, ako na tom ste. Prejdite týchto päť otázok s človekom, ktorý u vás zodpovedá za IT. Ak pri niektorej zaváhate, našli ste miesto, kde začať.

- [ ] **Viete, ktoré vaše služby sú dostupné z internetu?**
  Existuje aktuálny zoznam verejne dostupných systémov, portov a technológií? Kedy ste ho naposledy overili zvonku, nie z internej dokumentácie?

- [ ] **Zbierate logy zo všetkých kľúčových systémov?**
  Alebo len z tých, ktoré sa nastavili ako prvé a odvtedy sa k nim nikto nevrátil? Systém bez logov je systém bez dohľadu.

- [ ] **Pozerá sa niekto na tie dáta priebežne?**
  Archív logov pomôže až pri forenznej analýze po incidente. Detekcia vzniká až vtedy, keď udalosti niekto priebežne vyhodnocuje a spája do súvislostí.

- [ ] **Viete spätne zrekonštruovať aktivitu za posledné mesiace?**
  Ak by sa dnes ukázalo, že útočník je vo vašom prostredí od jari, dokázali by ste dohľadať, kadiaľ sa pohyboval a k čomu sa dostal?

- [ ] **Kontrolujete doménu voči databázam únikov a konáte po náleze?**
  Samotné zistenie, že heslo uniklo, nič nerieši. Rozhodujúce je, čo po náleze nasleduje: zmena hesla, overenie ďalšieho použitia a zapnutá viacfaktorová autentifikácia.

AKO TO ROBÍME MY

V exe:SOC staviame detekciu na centralizovanom zbere logov, korelácii udalostí naprieč prostredím a analytikoch, ktorí výstupy skutočne vyhodnocujú. Monitorujeme počas pracovných hodín, s on-call rotáciou pre kritické incidenty. Rozsah pokrytia vždy závisí od toho, aké systémy do monitoringu zapojíte.

exe : SOC

ĎALŠÍ KROK

Viete, čo sa vo vašej sieti deje práve teraz?

Konzultácia zdarma, 30 minút

Prejdeme s vami, ktoré fázy útoku dnes viete detegovať a kde máte slepé miesta. 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.