

PŘEHLED ŘEŠENÍ

Prevence narušení

Zastavte útok dřív, než napáchá škody.

Detekce je důležitá, ale nejlevnější incident je ten, který se vůbec nestane. Prevence narušení aktivně blokuje známé útoky, zneužití zranitelností i škodlivý provoz – na hranici sítě, uvnitř ní i na koncových zařízeních.

Co nasazujeme a nastavujeme

- systémy prevence průniku (IPS) a firewally nové generace
- segmentaci sítě, která omezí šíření útoku
- ochranu koncových stanic a serverů (EDR)
- zabezpečení vzdáleného přístupu
- bezpečné nastavení (hardening) klíčových systémů

Jak postupujeme

- 1 Vyhodnotíme, odkud vám hrozí největší riziko.
- 2 Navrhujeme vrstvenou ochranu odpovídající vašemu prostředí.
- 3 Ochranu nasazujeme postupně, nejprve v režimu sledování, abychom neomezili provoz.
- 4 Pravidla průběžně ladíme a aktualizujeme.

Co získáte

- automatické blokování známých útoků a škodlivého provozu
- menší prostor pro útočníka, i kdyby se dostal dovnitř
- ochranu nastavenou tak, aby nebrzdila běžný provoz

AI

AI v praxi: Moderní ochranné nástroje využívají AI k rozpoznání nových, dosud neznámých útoků.

Pro koho: pro organizace, které chtějí útokům aktivně bránit, ne je jen zaznamenávat.

Probereme, jak posílit vaši ochranu

info@anomalis.cz · +420 603 106 456 (v naléhavých případech nonstop) · www.anomalis.cz

Anomalis IT s.r.o. · Korunní 2569/108, 101 00 Praha 10 · IČO 09717404 · DIČ CZ09717404