

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **159** ze dne **13.10.2026**

Kybernetické hrozby se v éře AI mění každou hodinou

Generativní AI a pokročilá automatizace kompletně změnily tempo i charakter kybernetických útoků. Zatímco dříve útočníci připravovali průniky do firemních sítí celé týdny, dnes vytvářejí škodlivé skripty a cílené phishingové kampaně během několika minut. Bezpečnostní týmy se dostávají pod obrovský tlak. Útočníci totiž využívají stejné nástroje jako vývojáři a jejich reakční doba se smršťuje. Tradiční bezpečnostní nástroje s pasivním monitoringem a statickými pravidly soubor s časem prohrávají, ale s přístupem Managed Detection and Response (MDR) se tento souboj dá vyhrát.

Rychlost útoků versus reakční schopnost

Dynamika kybernetických hrozeb se za posledních zhruba pět let změnila naprosto radikálně. Podle bezpečnostní zprávy Mandiant M-Trends dosahuje medián doby do odhalení průniku 14 dní. Dva týdny dají útočníkovi neomezený prostor k prozkoumání sítě, krádeži citlivých dat a přípravě likvidačního ransomwaru. Stejně varovný zůstává fakt, že vývojářům trvá podle reportu Verizon Data Breach Investigations v průměru 43 dní, než plně nasadí opravu kritické zranitelnosti. Co to znamená: že mezi objevením díry v systému a jejím záplatováním vznikne obrovské časové okno, v němž útočník využije příležitosti.

Nemálo firemních manažerů přitom stále žije v hlubokém přesvědčení, že kvalitní antivirus a firewall poskytují dostatečnou ochranu. Jenomže antivirus řeší především známý malware a podezřelé soubory. "Moderní" útočníci na to ale jdou daleko důmyslněji. Už neztrácejí čas instalováním známých virů, ale zneužívají zcela legitimní nástroje operačního systému, takzvané techniky living-off-the-land, případně vzdálený přístup přes ukradené přihlašovací údaje.

Když potom získají přístupové údaje zaměstnance, běžný bezpečnostní software ho vidí jako oprávněného uživatele. Současná infrastruktura navíc propojuje servery v kanceláři, desítky cloudových aplikací, vzdálené notebooky a hybridní prostředí. Bezpečnostní specialisté proto musí sledovat jak samotná zařízení, a také hlavně chování uživatelů a tok dat v reálném čase. Také jim už dnes v práci pomáhá AI. Rychlý rozvoj AI dává do rukou nevídanou sílu útočníkům, ale zároveň stejná technologie pomáhá obráncům odhalovat i ty nejjemnější odchylky v chování systémů. Pokud ji ovšem umí efektivně využít.

Řízená detekce a reakce je cestou k obraně v reálném čase

Zmíněné faktory vedou v podnikovém prostředí k prosazení přístupu Managed Detection and Response, tedy takzvané řízené detekce a reakce (MDR). Tento přístup sází na okamžitý aktivní zásah. Systém hrozbu neprodleně zastaví a napadené zařízení izoluje dřív, než se útok rozšíří do zbytku infrastruktury.

Klíč spočívá v kombinaci pokročilé automatizace a lidského úsudku. Moderní dohledové systémy celosvětově vyhodnocují přes 500 milionů bezpečnostních událostí denně. Procházet takový objem dat ručně nedává smysl a vlastně ani není v lidských silách. Přesně tady nastupuje umělá inteligence, která události v reálném čase filtruje, porovnává a hledá skryté anomálie.

Jakmile systém odhalí podezřelé chování, expertní dohledový tým okamžitě zasahuje. My jsme si to změřili. A tak víme, že doba reakce a izolace napadeného zařízení se zkracuje pod 30 minut. Včasná

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **159** ze dne **13.10.2026**

izolace jednoho notebooku ušetří firmu od zablokování celé sítě a ztráty kritických dat.

Když snahy o vlastní obranu narazí na trh práce a regulaci

Proč si tedy nebudovat vlastní bezpečnostní dohledové centrum (Security Operations Center, zkráceně SOC) a raději si na to najímat externího partnera? Realita trhu práce je neúprosná. Bezpečnostních expertů je zoufale málo a jejich cena se počítá v milionech korun ročně. Zajištění provozu v režimu 24/7 navíc vyžaduje minimálně pět až šest plně kvalifikovaných analytiků.

Do hry vstupuje i regulatorní tlak. Jak ukazuje současný vývoj kolem evropské směrnice NIS2 a nového kybernetického zákona, povinnost hlídat infrastrukturu dopadá na stále širší okruh firem. Díky službě podnik získává špičkový dohledový tým i potřebnou technologii bez nutnosti rozšiřovat vlastní stav zaměstnanců.

AV centrum ČR