

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **106** ze dne **6.5.2025**

Kyberútočníci exfiltrují data firem již za tři dny

Sophos zveřejnil studii Sophos Active Adversary Report 2025, která podrobně popisuje chování a techniky útočníků ve více než 400 případech zásahů služby řízené detekce a reakce (Managed Detection and Response, MDR) a reakce na incidenty (Incident Response, IR) v roce 2024. Studie zjistila, že hlavním způsobem, jak útočníci získali prvotní přístup do sítí (56 % všech případů reakce MDR a IR), bylo zneužití externích vzdálených služeb, což zahrnuje zařízení na okrajích sítě, jako jsou firewally a VPN, s využitím platných uživatelských účtů.

Kombinace externích vzdálených služeb a legitimních účtů odpovídá i hlavním příčinám útoků. Již druhý rok po sobě byla hlavní příčinou útoků právě kompromitace přihlašovacích údajů (41 % případů). Následovalo zneužití zranitelností (21,79 %) a útoky hrubou silou (21,07 %).

Změny v rychlosti útoků

Při analýze vyšetřování zásahů MDR a IR se tým Sophos X-Ops zaměřil zejména na případy ransomwaru, exfiltrace dat a vydírání na základě odcizených dat, aby zjistil, jak rychle útočníci postupují jednotlivými fázemi útoku na organizace. V těchto třech typech případů činil medián doby mezi začátkem útoku a exfiltrací dat pouze 72,98 hodiny (3,04 dne). Navíc od exfiltrace do odhalení útoku uplynulo podle mediánu hodnot pouze 2,7 hodiny.

"Pasivní zabezpečení již nestačí. Přestože je základem prevence, kriticky důležitá je především rychlá reakce. Organizace musí aktivně monitorovat síť a rychle reagovat na zjištěné skutečnosti. Koordinované útoky motivovaných protivníků vyžadují i koordinovanou obranu. Pro mnoho organizací to znamená kombinaci znalostí specifických pro daný podnik s odborně vedenou detekcí a reakcí. Naše studie potvrzuje, že organizace s proaktivním monitorováním odhalují útoky rychleji a dosahují lepších výsledků," řekl John Shier, Field CISO společnosti Sophos.

Útočníci mohou převzít kontrolu nad systémem za pouhých 11 hodin

Medián doby mezi první akcí útočníků a jejich prvním (často úspěšným) pokusem o napadení služby Active Directory (AD) – pravděpodobně jednoho z nejdůležitějších prostředků v síti Windows – byl pouhých 11 hodin. V případě úspěchu mohou útočníci mnohem snadněji převzít kontrolu nad organizací.

Hlavní ransomwarové skupiny v případech zkoumaných experty společnosti Sophos

V roce 2024 byla do útoků nejčastěji zapojena ransomwarová skupina Akira, následovaná skupinami Fog a LockBit - navzdory tomu, že bezpečnostní složky měly počátkem roku LockBit zlikvidovat.

Doba setrvání v síti se snížila na pouhé dva dny – hlavně díky MDR

Celkově se doba setrvání útočníků v síti oběti, tedy doba od začátku útoku do jeho odhalení, se v roce 2024 snížila ze čtyř dnů na pouhé dva dny. A to zejména díky tomu, že do souboru zkoumaných útoků přibýly případy využívající MDR.

Doba setrvání v síti v případech se zásahem služby reakce na incidenty

Délka od napadení do odhalení zůstala stabilní na čtyřech dnech u ransomwarových útoků a 11,5 dne u případů nezahrnujících ransomware.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **106** ze dne **6.5.2025**

Doba setrvání v síti v případech se zásahem služby MDR

Při vyšetřování případů, u kterých došlo k zásahu MDR, byla doba od průniku do odhalení pouze tři dny u ransomwarových případů a pouze den u případů nezahrnujících ransomware. To naznačuje, že jsou týmy MDR schopny útoky odhalit rychleji a také na ně úspěšně reagovat.

Ransomwarové skupiny operují přes noc

V roce 2024 bylo 84 % binárních souborů ransomwaru spuštěno mimo místní pracovní dobu obětí útoků.

Protokol vzdálené plochy nadále dominuje

RDP (Remote Desktop Protocol) byl zapojen do 84 % případů s reakcí MDR/IR, což z něj činí nejčastěji zneužívaný nástroj od Microsoftu.

Zdroj: AVcentrum ČR