# Obsah



*Vážené čtenářky, vážení čtenáři,*

velice zajímavý a svým způsobem alarmující průzkum nedávno uveřejnila renomovaná organizace SANS Institute ve spolupráci s bezpečnostní firmou Bishop Fox – podle jejich zjištění většina hackerů potřebuje k proniknutí do podnikového prostředí maximálně pět hodin.

Tento závěr vychází z odpovědí 300 dotázaných etických hackerů pracujících v různých rolích uvnitř organizací s různou úrovní zkušeností v různých oblastech ochrany dat, přičemž 90 % z nich bylo držitelem certifikace pro bezpečnost informací a mezi jejich hlavní specializace patřila především síťová bezpečnost, interní penetrační testování, bezpečnost aplikací, red-teaming či cloudová bezpečnost.

Přibližně 40 % těchto hackerů uvedlo, že se dokážou nabourat do většiny prostředí, která testují, ne-li do všech. A téměř 60 % pak prohlásilo, že potřebují pět hodin nebo méně, aby pronikli do podnikového prostředí, jakmile zjistí nějakou jeho slabinu. V průměru by hackeři podle svých tvrzení potřebovali pět hodin na každý krok řetězce útoků: průzkum, zneužití, eskalaci oprávnění a exfiltraci dat, přičemž úplný útok by podle všeho trval méně než 24 hodin.

Na otázku, kolik času obvykle potřebují k identifikaci slabiny ve vyhlédnutém prostředí, 57 % dotázaných etických hackerů uvedlo méně než deset hodin: každý šestý odpověděl šest až deset hodin, každý čtvrtý tři až pět hodin, každý desátý jednu až dvě hodiny a konečně každý dvacátý méně než hodinu.

Za zmínku také stojí, že 28 % hackerů odpovědělo, že neví, což ale může být z různých důvodů (třeba kvůli tomu, že takový čas nesledují, protože to není pro ně důležité) a nikoliv nutně proto, že by jim to trvalo déle než deset hodin. Více než třetina respondentů pak uvedla, že mohou zvýšit svá oprávnění a pohybovat se příčně prostředím v čase do tří až pěti hodin po počátečním narušení, a pětina to dokáže dokonce za dvě nebo méně hodin.

Nejrizikovější pro organizace jsou podle hackerů připojení třetích stran, příliš rychlé tempo vývoje a nasazení aplikací, nesprávné přijetí cloudové infrastruktury, špatně nakonfigurovaná vzdálená práce či zfušované procesy při fúzích a akvizicích.

Pokud jde o typy ohrožení, které etičtí hackeři nejčastěji využívali, byly na prvním místě nesprávné konfigurace následované zranitelným softwarem, veřejně vystavenými webovými službami, expozicemi citlivých informací či problémy s ověřováním nebo řízením přístupu.

Pozitivní zprávou ale je, že pokud jsou odhalení a zablokovaní, jen málokterý hacker se hned dokáže úspěšně přeorientovat na jinou metodu ataku – jinými slovy, pokud útok zachytí nějaký typ firemní ochrany, hacker, který většinou volí cestu „nejmenšího odporu", operaci vzdává a přechází na jiný, jednodušší cíl.

Zajímavé také je, že etičtí hackeři se z velké míry spoléhají na nástroje open source či jiné veřejné zdroje, zatímco s exploity či vlastními řešeními pracuje jen minimum z nich.

A co z toho celého vyplývá? SANS Institute radí, aby organizace především zlepšily svůj průměrný čas na odhalení a zadržení útoku vícevrstvou ochranou a také zaměřením na obranu proti veřejným nástrojům a exploitům, které se k útokům nejčastěji používají.

S přáním příjemně stráveného závěru letošního roku a vykročení tou správnou nohou v roce příštím

Pavel Louda,
vedoucí projektu