SYXSENSE

Koncové body jako cíl

Zjednodušeně řečeno se IT infrastruktura každé organizace skládá ze dvou složek. Ty tvoří sítě a koncové body. Obě složky jsou potřebné a obě musí být chráněny před zneužitím, ale v konečném důsledku se útočníci z těchto dvou zaměřují na získání nezjištěného privilegovaného přístupu ke koncovým bodům.

Koncové body, ať už se jedná o servery, virtuální počítače, pracovní stanice, desktopy, notebooky, tablety nebo mobilní zařízení, jsou místem, kde se pracuje. Na nich jsou provozovány různé aplikace, které vytvářejí, ukládají a manipulují s daty. Navíc se připojují ke zdrojům dat a dalším zařízením.

Dnešní mobilní pracovní prostředí znamená, že koncové body mohou být kdekoli a pohybovat se všude. Infiltrátoři si uvědomují, že aby nakonec uspěli, musí žít na koncovém bodě, což vysvětluje, proč kyberzločinci chtějí vždy ovládnout koncové body.

Kompromitace koncového bodu poskytuje útočníkům výchozí bod pro hlubší infiltraci do podnikové sítě nebo v některých případech přímo k průniku do sítě s přístupem k cenným datům. Život na koncovém bodě nebo na více koncových bodech, umožňuje útočníkovi působit zdánlivě autenticky.

Síť je cestou útoku,
ale koncové body
jsou cílem útoku.

Narušitelé zpravidla využívají své nové pozice ke shromažďování informací o provozu společnosti a chování systému což posiluje jejich legitimitu.

Koncový bod se stává bezpečným útočištěm, ze kterého mohou dále získat další pověření, přesunout se v rámci sítě podnikového prostředí, udržovat perzistenci a nakonec exfiltrovat data. Jakmile se jednou usadí, může být obtížné je zlikvidovat, protože je obtížné zajistit, aby byly odstraněny všechny stopy narušitelů. Často totiž existuje určitá neochota zasahovat do některých zařízení ze strachu, aby se nezasahovalo do jejich chodu, což může snadno způsobit negativní dopady na podnikové operace.

Vědomí, že koncové body jsou ceněnými cíli, nezabrání tomu, aby byly kompromitovány. Jedním z důvodů je, že koncové body jsou neustále používány, a proto je obtížné je uzamknout. Rostoucí počet a typy zařízení, která se neustále připojují a odpojují k síti, vytváří samy o sobě větší prostor pro útoky všeobecně známý jako plocha útoku (Attack Surface).

Attack Surface Management (ASM)

ASM zahrnuje kombinaci lidí, procesů, technologií a služeb určených k průběžnému zjišťování, inventarizaci a správě aktiv organizace. Tato aktiva mohou být interní i externí povahy a představují digitální rizika. Tento přehled může pomoci snížit riziko, které by mohli zneužít aktéři škodlivých hrozeb.

Gartner, 2022

Útočníci mají také k dispozici obrovský soubor útočných technik – konkrétní kroky nebo chování, které se kaskádovitě skládají do řetězce činností potřebných k instalaci malwaru a získání operační kontroly nad koncovými body. Komplexní seznam technik útoku je obsažen v dokumentu MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge).

Q1 2022
Incident Response Insights

57%

všech incidentů bylo způsobeno zneužitím externích zranitelností.

Zdroj: Tetra Defense

Od července 2022 evidujeme již 191 hlavních technik a 385 dílčích technik, jak mohou útočníci proniknout do podnikové sítě. Přibližně 200 z nich popisuje útočné metody specificky zaměřené na kompromitaci koncových bodů. Konkrétní metody, které útočníci používají, jsou důležité, ale potenciálně větší význam má to, že útočníkům pomáhá stav cílových zařízení.

Mnoho metod útoku funguje pouze proti systémům zranitelným vůči konkrétnímu útoku. V konečném důsledku mají úspěšné útoky za následek zneužití zranitelností.

Vzhledem k tomu, že ve Spojených státech bylo podle Národní databáze zranitelností (NVD) Common Vulnerabilities and Exposures (CVE) identifikováno více než 176 000 zranitelností a jejich počet roste o více než 20 000 ročně, není překvapivé, že záplatování zranitelností je v současné době obtížné.

Cesty útoku na koncová zařízení se neomezují pouze na softwarové zranitelnosti ale umožňují je také chybné konfigurace (misconfigurations). Analytická společnost ESG uvedla, že chybné konfigurace koncových bodů – zahrnující takové položky, jako jsou například nesprávně použitá oprávnění, nastavení prohlížeče, otevřené porty a aktivní nepotřebné služby – jsou vstupním bodem ve čtvrtině všech kompromitovaných koncových zařízení.

Podstatné je, že zabezpečení podniku proti útokům, zejména těm, které jsou zaměřeny na koncové body, je obtížné. Profesionálové zabývající se problematikou kybernetické bezpečnosti pracují na ochraně prostředí a to vyžaduje holistický bezpečnostní rámec zaměřený na uzavření všech cest útoku.

FREEDIVISION S.R.O.
Rektorská 50/52, 108 00 Praha 10 – Malešice, Česká republika

FREEDIVISION for safety reasons
www.freedivision.com
assistant@freedivision.com
+420 220 972 426