

Nástroje pro správu zranitelností – co dělat a co nikoliv

Vyhněte se běžným chybám správy zabezpečení a získejte ze svých nástrojů maximum

NEIL ROITER

Nepodceňujte nutnost nápravy. Organizace překvapivě provádějí skeny zabezpečení nebo si najdou někoho k provedení skenu, dostanou report a poté nepostupují podle výsledků. Vyberou si jednu nebo dvě kritické položky a zbytek zanedbají. Výsledkem je, že organizace vydaly čas a peníze a moc toho pro své zabezpečení neudělají.

„Některé organizace se zastaví na detekci,“ uvádí Chenxi Wang, hlavní analytik společnosti Forrester. „To vám popíše vaši situaci, ale s rizikem to neudělá vůbec nic.“

Správa zranitelností a konfigurací musí být napravena pomocí dobře definovaného procesu řízení změn za podpory nástroje správy zranitelností a provázána s vašimi kontrolními mechanismy, jako jsou tiketové systémy.

Nástroj by měl podporovat proces nejen prostřednictvím detekce zranitelností a chyb, ale také prostřednictvím vyhodnocení rizik podle závažnosti hrozby a hodnoty zranitelného systému. Proces není kompletní a případ (tiket) nelze uzavřít, dokud není zopakováno skenování za účelem ověřit, že oprava byla účinná, tj. že se jí podařilo nainstalovat úspěšně nebo že chyba konfigurace byla opravena.

„Některé organizace jsou velmi proaktivní, některé jsou reaktivní,“ prohlašuje bezpečnostní konzultant Shaheen Abdul Jabbar. „Viděl jsem bezpečnostní personál provádět skenování, oznámit výsledky oddělení IT, ale bez následné kontroly, zda byly problémy vyřešeny, a to až do dalšího auditu.“

Používejte skenovací služby. Pokud jste subjekt podřízený směrnicím, které vyžadují pravidelné nezávislé skenování, stejně nemáte na výběr. V takovém případě se však neomezujte na splnění minimálních požadavků směrnic. Projděte také procesem nápravy – dobří auditoři na tom budou trvat.

Nezávisle na regulačních povinnostech jsou služby SaaS (software jako služba) a po-

skytování řízených služeb životaschopné varianty pro správu zranitelností. Několik hlavních dodavatelů se významně nebo dokonce výhradně zaměřilo na služby a umožňují jejich použití jako alternativy či doplňky k vlastnímu skenování.

Nabídky SaaS jsou podle své podstaty zaměřeny na systémy komunikující s veřejností. Pro komplexnější skenování používají poskytovatelé služeb vlastní zařízení umístěné do sítě zákazníka, které zjistí a ohlásí výsledky.

Některé firmy jsou nedůvěřivé a nechtějí povolit sdílení vně organizace u všech dat nashromážděných skenováním. Zajistěte si ochranu dat pomocí silného šifrování se solidní správou klíčů a to, aby přístup k takovým datům měl pouze váš autorizovaný personál, a nikoli zaměstnanci dodavatele.

Také zajistěte, aby pověření pro autentizované skenování bylo dostatečně zabezpečeno, ať už pomocí vlastní technologie dodavatele nebo pomocí dobrého produktu ve formě digitálního trezoru a správy privilegovaných identit.

Správa zranitelností v podobě služby dokáže ušetřit peníze v oblasti investičních výdajů, náročnosti správy a počtu personálu.

Zvažte navíc využívání služeb konzultantů a poskytovatelů služeb, minimálně periodicky jako formu doplnění vašeho interního skenování. Využití nezainteresovaného poskytovatele je ochranou reportů před interní předpojatostí či zakrýváním vlastních chyb.

Trvejte na použitelných reportech. To se týká mnoha úrovní. Na nejvyšší úrovni samozřejmě chcete report pro management, který by obsahoval trendy a celkový stav. Na úrovni zabezpečení by měl nástroj správy zranitelností poskytnout informace o bezpečnostních tržlinách na základě standardů, jako je například seznam CVE (Common Vulnerabilities and Exposure) nebo CVSS (Common Vulnerability Scoring System), zároveň s přidělením váhy podle hodnoty, kterou vaše organizace přiřkládá danému vybavení.

Report by měl sdělit, co je zranitelné, jak je to zranitelné a jak vysoké riziko existuje. Provozní reporty pro personál zodpovědný za opravu by měly být přímočaré a orientované na činnosti.

Instalace oprav a změny konfigurací jsou

Skenování zranitelností s využitím agentů, nebo bez nich

„Náboženské války“ mezi dodavateli a koncovými uživateli se točí kolem skenování s agenty a bez nich.

Výhody použití agentů:

- Jsou vždy připraveni, umožňují získávat informace bez spuštění skenování.
- Poskytují velmi podrobné údaje o konfiguraci, operačním systému, službách a aplikacích, snižují četnost falešných poplachů.
- Nejsou rušivé.
- Nepodléhají občasným chybám aktivního skenování (interference s firewally, zahozené pakety atd.).

Nevýhody použití agentů:

- Je nutné je spravovat, což vyžaduje po organizacích zvýšení režie při udržování dalšího agenta v zařízeních.
- Možnost vzniku konfliktů podle toho, co dalšího je ještě spuštěno.
- Může to být zakázáno na některých zařízeních směrnicemi či zásadami.
- Nelze je použít v zařízeních, která nemají rozhraní pro jejich podporu, včetně síťových zařízení, jako jsou směrovače a přepínače.
- Lze je umístit pouze na známá spravovaná zařízení, takže je stále potřebné skenování minimálně za účelem zjištění vybavení.

„Technologie vyhodnocení zranitelností potřebuje nasadit agenty, kdekoli je to možné, a podporovat funkci bez agentů všude tam, kde to možné není,“ vysvětluje Chenxi Wang, hlavní analytik společnosti Forrester Research. „Agenti poskytují mnohem hlubší pohled na konfiguraci zařízení a služeb, které na nich běží. Množství zjistitelných informací je nesrovnatelné.“

Přechodný přístup využívá dočasné agenty, kteří jsou umístěni v cílovém zařízení pro sběr informací při absenci skenování a poté jsou smazáni, když je práce dokončena.



obvykle prováděny personálem síťového provozu a systémovými správci. Nejsou to profesionálové v oblasti zabezpečení, takže reporty a instrukce by měly být popsány z hlediska instalace oprav, změn konfigurací, a nikoli zranitelností.

Reporty auditu by měly jasně demonstrovat, že byla detekována zranitelnost či chyba konfigurace, bylo vyhodnoceno riziko a otevřen tiket. Samozřejmě také později, že byl tiket uzavřen po vyřešení problému a zejména že bylo vyřešení ověřeno finální kontrolou.

Nakonec by měly být reporty schopny použít stejná data pro různé účely – reporty pro různé části organizace a různé typy cílových osob, reporty pro různé sady směrnic atd.

„V dřívějších dobách bylo nutné spouštět sken pro každý report,“ vzpomíná Gary Davis, senior manažer skupiny pro rizika a dodržování směrnic ve společnosti McAfee, „ale ve skutečnosti potřebujete model jednoho skenování s mnoha reporty, který odělí skenování od reportování samotného.“

Integrujte správu zranitelností s dalšími nástroji zabezpečení. Prvním na seznamu je systém SIEM (správa událostí a bezpečnostních informací). Správa zranitelností je kritickým zdrojem informací pro SIEM jako



součástí celkového programu správy rizik.

Jakmile je zjištěna zranitelnost či problém s konfigurací, měla by být tato informace předána do nástroje SIEM, aby ji bylo možno uvést do souvislosti s informacemi z dalších zdrojů, jako jsou firewally a systémy IPS.

Správa zranitelností se také dobře integruje se systémy IPS, jež mohou využívat in-

ventář vybavení a informace o zranitelnostech ke zjištění, které útoky představují skutečné ohrožení a které lze bezpečně ignorovat.

Pokud nástroj správy zranitelností obsahuje skenování aplikací, mohou být výsledky použity k vytváření či modifikaci pravidel ochrany pro firewally webových aplikací.

KOMERČNÍ PREZENTACE

Český webfiltr v českém prostředí – jednoduché a účinné řešení...

Produkt Kernun Clear Web společnosti TNS, a.s.

Kernun Clear Web je webový filtr orientovaný primárně na prostředí českého internetu. Cílem je maximální úspěšnost kategorizace navštěvovaných webových odkazů z interní sítě zákazníka. Nasazením produktu lze aplikovat bezpečnostní politiky pro omezení nežádoucí činnosti zaměstnanců, která může vést ke vzniku bezpečnostních incidentů.

Pro dosažení vysoké přesnosti databáze kategorií je proces kategorizace prováděn částečně automaticky, hlavně ale týmem kategorizátorů. Lidský faktor a znalost prostředí českého internetu je to, co přispívá k jedinečnosti a vysoké úspěšnosti Kernun Clear Webu.

Případová studie

Po nasazení u zákazníka došlo k meziročnímu snížení počtu nákaz koncových stanic o 47%. Filtr způsobil i změnu chování uživatelů – došlo ke snížení používání anonymních úložišť nebo freemailů. Nasazením Kernun Clear Webu vzrostla efektivita využívání pracovní doby – přístup na služby typu e-shop nebo homebanking, které nejsou zakázány, ale jen detailně monitorovány, meziročně poklesl o 63%.

Webfiltr jako bezpečnostní opatření

Analýza bezpečnostních incidentů ukazuje, že nejčastěji je škodlivý kód zanesen do interní sítě prostřednictvím webové stránky. K tomu

útočníci často využívají metod sociálního inženýrství – nakažené stránky jsou umístěny na serverech, které lákají pozornost uživatelů, ať jde o nakupování, hobby servery nebo pornografii.

Detailní záznam aktivity na internetu

Bezpečnostní politika zákazníka vymezuje, které z 61 kategorií filtru jsou pro plnění úkolů zaměstnanců nezbytné a které naopak nevhodné. Kernun Clear Web podporuje uživatelské skupiny, whitelisty a blacklisty, což umožňuje jemné nastavení filtrování obsahu pro jednotlivé pozice zaměstnanců. Kategorie, které mají být přístupné pouze „občas“ (např. weby leteckých společností

při plánování služebních cest), jsou zpřístupněny po potvrzení tzv. Bypassu. Tato funkce webový obsah dočasně zpřístupní a aktivitu zaznamená. Nasazením tohoto opatření se mimo jiné snížil počet přístupů na služby internet bankingu o 63%.

Integrace do stávající sítě a přínos pro zákazníka

Kernun Clear Web může zákazník před zakoupením otestovat nebo dokonce zapůjčit na omezenou dobu přímo do cílového prostředí. V síti zmíněného zákazníka je Kernun Clear Web nasazen jako modul stávajícího firewallu Kernun. Statistiky chování uživatelů jsou samozřejmě k dispozici vedení. Nasazení Kernun Clear Webu, díky detailnímu přehledu o využívání webových serverů jednotlivými zaměstnanci, často vede k výraznému snížení počtu přístupů na volnočasové webové stránky.

