Kyberprevence

Správa záplat: Závod s kyberzločinci

Digital Security
Progress. Protected.

Podle posledních zpráv z oblasti kyberbezpečnosti se **řada společností stává obětí útoků přes známé i dříve opravené zranitelnosti.** Nedávno došlo u jedné z nich k úniku dat, který postihl více než 30 milionů zákazníků. Únik souvisel se zranitelností softwaru, jež byla opravena pouhý týden před útokem.

Ačkoli je nedbalost v oblasti kybernetické bezpečnosti odsouzeníhodná, nebudeme tady bičovat společnosti za pozdní záplatování nebo za to, že neberou zabezpečení dostatečně vážně. Pravdou je, že aplikace záplat ve velkých podnicích, a dokonce i v menších organizacích, není jen o kliknutí na jediné tlačítko, kterým se vše aktualizuje. Celý proces je mnohem náročnější.

A rozsah tohoto problému je obrovský. Podle nejnovější zprávy Verizon Data Breach Investigations Report je zneužití zranitelností třetím nejpoužívanějším způsobem přístupu do organizace.

Dobrou zprávou je, že existují profesionální nástroje, které posílí preventivní mechanismy v bezpečnostní strategii. Konkrétně ESET Vulnerability & Patch Management (V&PM), řešení v rámci naší rozmanité platformy ESET PROTECT, využívá automatizovaný nástroj, který detekuje zranitelnosti a aplikuje nejnovější záplaty pro aplikace a operační systémy na všech koncových bodech.

Souboj s Goliášem

Obecně platí, že společnosti na celém světě potřebují na opravu zranitelností v průměru 82 až 208 dní. Pokud jde o kritické zranitelnosti, situace není o mnoho lepší – zranitelnosti s vysokou mírou závažnosti se stále opravují v průměru za 146 dní.

A situace se zhoršuje. Podle průzkumu britského ministerstva pro vědu, inovace a technologie klesl ve Spojeném království počet podniků, které mají aktualizace bezpečnostního softwaru pro správu záplat (aplikace zásad) provedené do 14 dnů od zpřístupnění záplat, ze 43 % v roce 2021 na 31 % v roce 2023.

Co může způsobit opožděná instalace záplat:

- **Útok ransomwarem, který zašifruje firemní data, za která útočníci požadují výkupné.**
- **Úniky dat, které odhalí citlivé informace o klientech, zaměstnancích nebo obchodních partnerech.**
- **Dlouhodobý trvalý přístup k informacím o cílových podnikových systémech a činnostech.**
- **Závažné kyberincidenty, které mohou vést ke ztrátě důvěry zákazníků a partnerů.**
- **Rizika spojená s dodržováním předpisů a problémy s pojištěním.**

Jedním z hlavních důvodů, proč manažeři nechávají svoje systémy zranitelné vůči kybernetickým útokům, kterým lze předejít, je to, že **procesy správy záplat jsou stále složitější a časově náročnější**.

Ponemon Institute report z roku 2022 o stavu správy zranitelností v DevSecOps uvádí, že 47 % vedoucích pracovníků v oblasti bezpečnosti nezajistili aplikace, které byly identifikovány jako zranitelné. Je to jako David stojící proti Goliášovi. Více než polovina manažerů bezpečnosti uvádí, že takové aplikace obsahují více než 100 000 zranitelností, a **tvrdí, že se jim podařilo opravit méně než 50 % z nich.**

A Goliáš se jen zvětšuje. V dubnu 2023 překročil seznam běžných zranitelností a chyb v zabezpečení (CVE – Common Vulnerabilities and Exposures) společnosti MITRE ATT&CK hranici 200 000 záznamů a do konce února 2024 vzrostl jejich počet na více než 225 000.

Záplatování není hračka

Příval zranitelností není to jediné, s čím se podniky musí vypořádat. Samotná složitost IT služeb a aplikací vytváří další výzvy, které jsou umocněny rostoucím počtem zaměstnanců vykonávajících svou práci na dálku.

Rozmanitost systémů a aplikací se neustále rozšiřuje. **Podniky nyní fungují na více operačních systémech a aplikacích třetích stran různých dodavatelů**. To ztěžuje hledání bezpečnostních mezer a aplikace záplat.

Přibývá zaměstnanců pracujících v hybridním modelu. Jejich počet výrazně vzrostl v době vypuknutí pandemie COVID-19. Například v USA před pandemií pracovalo alespoň jednou týdně z domova 4,7 % zaměstnanců. V roce 2023 to bylo 28,2 %. Pro firmy to také znamená více zaměstnanců, kteří pracují na vlastním zařízení (BYOD).

Aplikace záplat je náročná. Před aplikací záplat musí firmy otestovat, zda nedochází k chybám nebo vedlejším účinkům, a naplánovat nasazení tak, aby nedošlo k narušení interních pracovních činností. Po aplikaci záplat práce ještě není hotová. **IT správci musí sledovat účinnost záplat,** kontrolovat, zda jsou aktualizována všechna relevantní zařízení, a případně řešit problémy po nasazení.

Záplatování musí být určena důležitost. Vzhledem k obrovskému počtu zveřejněných CVE, vydaných záplat a aktualizací musí společnosti vyhodnotit rizika a stanovit priority záplatování.

Nedostatek IT zdrojů s rostoucím počtem kybernetických útoků, CVE, cloud computingem, a prací na dálku představuje pro IT týmy vyšší zátěž než kdy dříve.
Podle studie z roku 2022 více než třetině IT týmů chybí účinné nástroje (43 %) a zdroje (38 %).

Snížení zátěže pomocí automatizace

Pozitivní je, že s rostoucí komplexitou IT se rozšiřují i řešení, **která pomáhají snižovat zátěž pracovníků kyberbezpečnosti.** Nemohou vyřešit všechno, ale mohou podnikům poskytnout tolik potřebnou podporu v závodě o to, kdo dřív opraví nebo zneužije zranitelnost.

Jaké jsou výhody automatizované správy zranitelností a záplat?

- **Automatizované záplatování všech koncových bodů.**
- **Automatizované skenování softwaru koncových bodů a aplikací třetích stran + okamžité hlášení a přehled o zranitelnostech.**
- **Zprávy o zranitelnostech nejzranitelnějšího softwaru a zařízení.**
- **Možnosti konfigurace automatického záplatování, nastavení strategie záplatování a definování časových intervalů, kdy má záplatování probíhat.**

ESET Vulnerability & Patch Management poskytuje všechny tyto funkce. A co víc, firmy mohou spravovat své záplaty prostřednictvím platformy ESET PROTECT, který centralizuje a automatizuje více úkolů v oblasti IT bezpečnosti a správy, čímž snižuje složitost IT procesů, zejména řešení nevyřešených zranitelností.

My jsme ESET

Proaktivní ochrana.

Eliminujeme způsoby, kterými útočníci mohou proniknout do vaší organizace.

Buďte o krok napřed před známými i nově vznikajícími kybernetickými hrozbami a zaměřte se na prevenci. Bezpečnostní řešení od ESETu efektivně **kombinují umělou inteligenci a odborné znalosti našich expertů.**

Zažijte nejlepší ochranu ve své třídě díky **zpravodajství o hrozbách**, které je již více než 30 let hnacím motorem naší rozsáhlé sítě výzkumných a vývojových poboček vedených **uznávanými specialisty v oboru**. ESET chrání vaši firmu, aby mohla naplno využít potenciál technologií.

ZJISTIT VÍCE

ESET®

Digital Security
Progress. Protected.