Význam **release a patch** managementu

Petr Javora

Tento článek si bere za cíl upozornit na klíčovou, i když často upozaděnou oblast, kterou je release a patch management. Systém bez příslušných aktualizací je a vždy bude zranitelný. Často nepomůže ani jinak bezchybné nasazení ostatních bezpečnostních technologií a produktů. Využití zranitelností se drží dlouhodobě na předním místě v metodách útoků. Nejedná se ale o útoky jen na samotný operační systém, či aplikace, ale i na hardwarové prvky, např. routery, tiskárny, atd.

ZeroDay zranitelnost

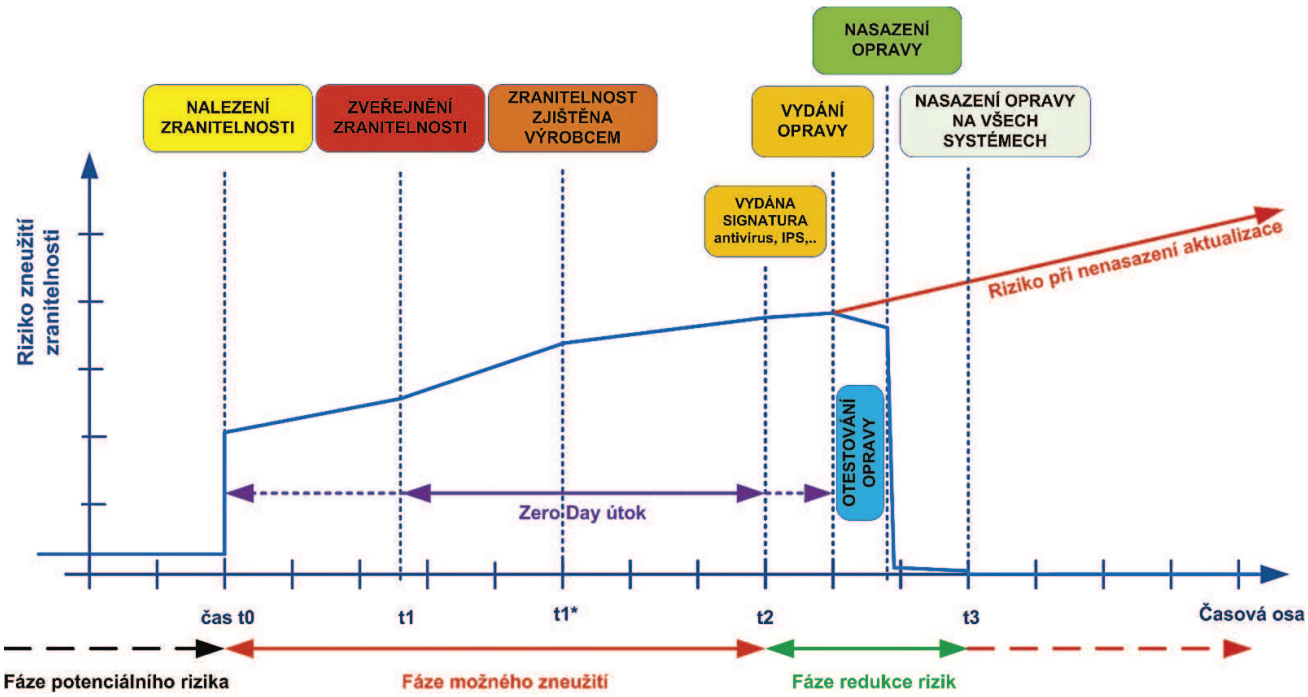
Zranitelnosti typu ZeroDay představují významný problém z pohledu bezpečnosti. Jedná se v podstatě o všechny chyby v aplikacích použitelné k útoku, které nenašel a neodstranil výrobce. Z pohledu zabezpečení firemního prostředí je klíčové „ZeroDay“ období mezi časy nalezení zranitelnosti (t0) a vydáním signatur pro bezpečnostní produkty (t2). Viz graf životního cyklu zranitelnosti na obrázku 1. V tomto čase není možné efektivně reagovat na vzniklou bezpečnostní situaci jinak než systém/aplikaci prostě vypnout či smazat! A toto období nemusí být vůbec krátké. Jsou známé případy zranitelností, které byly neopravené i řadu let! Následný interval mezi vydáním signatur (t2) a plošným nasazením oprav (t3) je možné výrazně zkrátit. Slouží k tomu nejrůznější bezpečnostní nástroje pro vyhledání zranitelností, testování systémů a následné nasazení oprav. Důležité je si uvědomit, že riziko není nulové, dokud existuje v organizaci byť jen jediný systém s touto slabinou. Často se jedná například o snapshot virtuálního systému, který po spuštění není chráněn. Stejná situace nastává i u dlouhodobě vypnutého uživatelského počítače.

Časová osa zranitelností

Před t0 – existuje zranitelnost, ale neví se o ní
t0 – zranitelnost nalezena, další postup záleží na motivech objevitele
t1 – zveřejněna informace o zranitelnosti
t1* – výrobce se dozví o zranitelnosti ve svém produktu a předpokládá se vydání bezpečnostní opravy. To platí pouze za předpokladu, že:

- Výrobce stále existuje.
- Zranitelný produkt je podporovaný.
- Výrobce vyhodnotí hrozbu jako dostatečnou, aby se vyplatilo opravu vydat.
- Výrobce má kapacity na vývoj a následné testování oprav. Jinak hrozí situace, kdy

Obr 1: Životní cyklus zranitelnosti



oprava přinese naopak další potenciální problémy.
- Výrobce vydá opravu v rozumném časovém rámci.

t2 – dostupné signatury sloužící k ochraně systému pomocí bezpečnostních produktů (IPS, Antivirus, Application Control,...)
t3 – oprava je nainstalována všude
Aktualizace pro koncové stanice/zařízení by měly být nasazeny bezodkladně, co se týká serverů, tak dle nastaveného plánu a priority (rizika) aktualizovat buď:
- Při dalším technologickém oknu – s rizikem prodlení. Technologická okna pro provedení aktualizací společně s dalšími naplánovanými úkoly (backup, restart, apod.) přináší značné riziko v tom, že bývají v intervalu týdnů až měsíců. Celý tento čas není systém náležitě zabezpečený.
- Okamžitě s omezením dostupnosti systému.

Patchování má probíhat automaticky na všech systémech, i momentálně vypnutých, jen tak lze zajistit dostatečnou úroveň bezpečnosti!

Release vs. patch

Obvykle se rozlišuje základní verze produktu (majoritní) a dále oprava/vylepšení (minoritní) verze. Existuje velké množství kombinací verzí a bezpečnostních oprav produktu. Dle statistik je situace ve většině společností taková, že souběžně existují v prostředí obvykle 2 majoritní verze každé aplikace a ke každé existuje několik oprav. Přičemž každá tato varianta čelí jiným hrozbám, což klade na správu prostředí značné nároky. Obecným doporučením je tak mít prostředí s minimem rozdílných konfigurací.

Jak provádět kontrolu?

Dalším problémem je, jak aktualizace nejen instalovat, ale i následně kontrolovat, že instalace proběhla korektně. Statistiky z WSUS představují dobré vodítko, ale doporučený postup je využít VMS (Vulnerability Management System) pro vyhledání nejen chybných konfigurací, ale i verzí produktů.

Aktualizace také nemusí být nainstalované na počítačích vyskytujících se často mimo firemní síť, např. home office. To z důvodu pomalého připojení, zapnutí jen nárazově, nebo například vlivem dlouhodobého uspávání bez provedení restartu. V oblasti bezpečnosti jsou klíčové 3 přístupy, které by měli zodpovědní pracovníci vykovávat:
- **Vědět** – sledovat aktuální dění v oblasti bezpečnosti. Když o nějakém riziku nevíte, těžko na něj budete adekvátně reagovat.
- **Konat** – operativně reagovat na vzniklou situaci, ať už zásahem administrátora, nebo nasazením produktu, který proces automatizuje. Klíčové je vypracování metodiky a pověření zodpovědných osob.
- **Ověřovat** – kontrolovat, jestli jsou rizika správně ošetřena na všech systémech. Zde se hlavně uplatní automatické dohledové nástroje, ale stále je někdo musí konfigurovat a vyhodnocovat stav.

Opatření	Váha z pohledu bezpečnosti
Používat legální SW	3/5
Používat aktuální SW	4/5
Nasazovat aktualizace všude	5/5
Kontrolovat aktualizace	4/5
Správná konfigurace	4/5
IPS/IDS/NGFW	3/5
Web/E-mail Security	4/5
SIEM	4/5

Co patchovat?

V případě instalace aktualizací se nejedná ani zdaleka jen o samotný operační systém, ale o všechny aplikace použitelné k získání přístupu k datům / systému / vzdálené správě. Často představuje významnou slabinu i neaktuálnost systémových ovladačů. Na co je vhodné se zaměřit? Dle statistik zranitelností: OS, Office, IE, Chrome, Firefox, Java, Flash Player, atd., ale situace je individuální, podle regionu a zaměření společnosti.

Patch je řešením i potenciálním problémem

Otázkou zůstává, jestli dostupný patch okamžitě nasadit, nebo provést alespoň zrychlené testování. Situaci je vhodné rozdělit podle velikosti organizace na malé – střední a velké. U malých a středních je obvyklé nasazovat opravy i s případným rizikem potenciálních problémů. U velkých společností je potřeba počítat s procesem testování aplikací/aktualizací před jejich nasazením do produkčního prostředí. Tímto způsobem se předchází potenciálním problémům s kompatibilitou a následnou nutností tyto problémy řešit. Přesto je obecné doporučení nasazovat opravy v co nejkratší době od zveřejnění, i přes případná rizika do budoucna.

Riziko v čase

Zajímavá situace nastává v dlouhodobém horizontu, kdy se riziko zneužití konkrétní zranitelnosti začne v čase snižovat. Nakonec s vymizením konkrétní platformy/aplikace/verze z prostředí prostě riziko kompletně vymizí. Neznamená to ale, že budete v dnešní době v bezpečí, když budete provozovat například Microsoft Windows 98, přestože pro něj prakticky nevznikají nové hrozby.

Co dělat, když patch není?

V situaci, kdy je společnost nucena využívat neaktuální/nepodporované verze aplikací, je prakticky jedinou cestou mít nasazeno zabezpečení na ostatních vrstvách (web/e-mail security, firewall, IPS, application control, account management,...), nebo zranitelné systémy izolovat nejen od internetu, ale i od firemní sítě.

Pokud nemáte nástroj pro správu aplikací a vyhledávání zranitelností, zaměřte se nejen na využívané aplikace, ale hlavně na ty nevyužívané. Není neobvyklé, že se vyskytují na počítačích 6–8 roků staré aplikace, prostě proto, že už se nepoužívají, ale nikdo je neodstranil. To představuje problém nejen z pohledu bezpečnosti, ale i při nasazení nových produktů, které kontrolují digitální podpisy všech aplikací a knihoven (např. upgrade na Windows 10).

Aktualizujte!

Release a patch management představuje neustálý souboj, vedete si v něm dostatečně dobře? Pokud se oblasti nasazení oprav nevěnujete dostatečně, využijte externí dodavatele s patřičnými zkušenostmi pro vypracování koncepce, či přímo pomoc s procesem a podporou. Nezapomínejte ale ani na výběr produktů od společností poskytujících nadstandardní podporu. Že základem je mít produkt zakoupený legálně a k němu příslušnou podporu, není předpokládám potřeba zdůrazňovat. ■

Ing. Petr Javora
Autor článku je konzultantem ve společnosti AEC, a. s.