UMĚNÍ NEPODLEHNOUT

Řízení zranitelností aneb vulnerability management v praxi

Jistě ve své firmě používáte firewall, antimalware, IPS, proxy… tedy nástroje, které chrání před nezneužitím zranitelností hardwarových zařízení či softwarových aplikací. Co ale jít ještě hlouběji a odstranit samotné zranitelnosti?

Lidské tělo odolá díky své přirozené imunitě většině virových nákaz. Sem tam se však objeví v obranném systému slabé místo, které je třeba dodatečně zahojit, ať již pouhým podáním vitamínových přípravků, či v závažnějším případě preventivním očkováním, viz nedávná vlna očkování proti prasečí chřipce.

Podobná situace panuje i u softwarového a hardwarové vybavení. Jeho tvůrci při programovaní sice dbají na ochranu před zneužitím, přesto žádný IT produkt nakonec není tak dokonalý, aby nepotřeboval v průběhu svého životního cyklu updaty, ať už co do funkčnosti, či bezpečnosti.

Zranitelnosti ICT

Co vůbec znamená zranitelnost systému? Z pohledu norem jde o slabé místo, které může být zneužito vnější hrozbou tak, že zapříčiní negativní dopad.

U ICT produktů jde zejména o chyby v programovém kódu, vzniklé během vývoje produktů nebo při jejich aktualizacích a opravách. Najdeme je prakticky u veškerých technických prostředků informačních systémů, tedy ve firmwaru serverů, PC a notebooků, aktivních síťových prvků, telekomunikačních zařízeních, osobních diářů, PDA, GPS a mobilních telefonů. Ještě častěji než ve firmwarech se technické zranitelnosti vyskytují u operačních systémů a aplikačního programového vybavení, tedy u aplikací, které se na technické prostředky IS instalují, jako jsou serverové a uživatelské aplikace, včetně na první pohled nevinně se tvářících programů pro kreslení anebo přehrávání hudby a videa.

Vedle výše uvedených zranitelností programového kódu představují druhou významnou skupinu zranitelností ICT chyby v instalaci a konfiguraci jak technických prostředků, tak instalovaného programového vybavení.

Je libo zevnitř či zvenku?

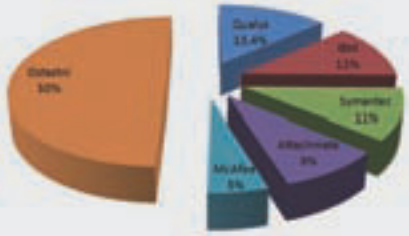
Zranitelnosti ICT produktů a systémů lze dělit podle způsobu zneužití vnější hrozbou na: „network-based“ a „host-based“. První skupina zranitelností je dostupná po síti libovolnému anonymnímu útočníkovi, a to bez potřeby bližší znalosti zranitelného systému. Stačí zde pouhá síťová konektivita na otevřené TCP nebo UDP porty, na nichž poslouchají síťové služby obsahující neošetřenou zranitelnost. Tyto „network-based“ zranitelnosti bývají útočníkům vstupní branou pro další stupňování útoku na daném systému a uvnitř infrastruktury IS. Leckdy i postačují k úplné kompromitaci systému, získání příkazového řádku, nebo k odepření funkčnosti služeb či vypnutí celého systému – to v lepším případě, protože nefunkční systém je snadno detekovatelným incidentem s rychlou dobou odezvy.

V horším případě poskytne zneužitá „network-based“ zranitelnost dveře k odhalení řady čekajících „host-based“ typů zranitelností, které lze objevit a zneužít až po získání vzdáleného přístupu na zranitelný systém. Získání vyšších privilegií, výpisů adresářových struktur či výpisů přístupových práv citlivých adresářů jsou příklady těch lehčích kalibrů „host-based“ zranitelností. Mezi těžší typy lze zařadit zavlečení a spuštění vzdáleného kódu, získání seznamu uživatelských účtů, jejich hesel, obsahů souborů, modifikace log souborů a další nepřeberné množství „vychytávek“, které šikovnému hackerovi pomohou získat potřebné informace a ještě za sebou uklidit stopy tak důkladně, že forenznímu auditu zbudou pouze oči pro pláč.

Komu se nelení…

Dlouhodobým statistickým sledováním nových typů zranitelností ICT, aplikovatelných hrozeb a útoků šířících se internetem i sledováním opakovaných výskytů určitých typů zranitelností v IS organizací byly, na žádost amerického kongresu k tématu boje proti kyberterorismu v roce 2005, sestaveny firmou Qualys zákonitosti chování zranitelností ICT produktů v IS. Z analýzy těchto nálezů lze odvodit, že zranitelnosti

Celosvětový prodej zařízení pro hodnocení zranitelností za rok 2008



Celkové tržby: 376,4 milionů dolarů
Zdroj: IDC

AUTOR

Zbyněk Marx
Konzultant společnosti Risk Analysis Consultants.

Marek Skalický
Technický obchodní manažer pro východní Evropu společnosti Qualys.

ICT produktů představují pro jejich uživatele a správce vážný problém a že systematickým přístupem k jejich eliminaci lze významně snížit riziko úspěšného napadení IS. Jeden příklad za všechny: pokud analyzujeme danou infrastrukturu IS a identifikujeme 10 % nejkritičtějších zranitelností z celého rozsahu výsledků a odstraníme je do 15 dnů, snížíme tak o 90 % pravděpodobnost úspěšného útoku na náš systém. Takové významné zvýšení bezpečnosti provozu IS už stojí za povšimnutí a za systematický přístup k řešení této problematiky.

Pokud odstraníte 10 % nejkritičtějších zranitelností do 15 dnů od jejich zveřejnění, snížíte pravděpodobnost úspěšného útoku na váš systém o 90 %

Proces řízení zranitelností ICT není nijak komplikovaný a při respektování požadavků opatření 12.6.1 normy ISO 27002:2005 jej lze sumarizovat do šesti základních kroků, které se periodicky opakují, viz box Šest kroků pro řízení zranitelností. Hlavním principem tohoto procesu je nastavení sledovaného a řízeného stavu, kdy víme, kolik jak závažných zranitelností se kde nachází, a jejich postupné eliminace, v závislosti na kapacitách a nastavených prioritách organizace. Je zřejmé, že prioritně je potřeba řešit nejzávažnější zranitelnosti, s největším negativním dopadem na nejkritičtějších systémech a poté se věnovat těm méně závažným.

Šest kroků pro řízení zranitelností

- Identifikace a zjištění přesného stavu aktivních a neaktivních systémů v IS.
- Rozlišení důležitosti jednotlivých systémů pro organizaci a následné nastavení priorit pro eliminaci zranitelností.
- Hledání zranitelností metodou network-based a nebo host-based.
- Rozhodnutí o pořadí odstraňování zjištěných zranitelností.
- Kontrola, že proces eliminace probíhá v souladu se stanovanými prioritami.
- Definování bezpečnostní politiky. akceptovatelných a neakceptovatelných zranitelností a kontrola stanovených cílů.

Dvě cesty, jeden cíl

V informačním systému středně velké organizace (několik set až tisíc zaměstnanců) máme desítky až stovky důležitých ICT prvků a systémů, které je třeba testovat a záplatovat. Ty standardně obsahují v souhrnu tisíce zranitelností, od nejnižší po nejvyšší hodnotu negativního dopadu. Aby byl proces řízení zranitelností v takovém rozsahu funkční, je naprosto nezbytné jej co nejvíce automatizovat. Z uvedeného seznamu šesti kroků je zřejmé, že automatizovat se dá až 90 % činností, při použití správné kombinace nástrojů na asset management, vulnerability management a patch management.

Automatizovat lze 1. a 2. fázi vyhledávání nových prvků v IS a jejich prioritizaci na základě předem dané škály hodnot. Naprosto nezbytné je automatizovat 3. fázi (hledání zranitelností), pro kterou na trhu existuje největší počet nástrojů, s různě obsáhlou databází zranitelností, s různě velkou podporou platforem a metod testování zranitelností (viz host-based a network-based). Existují dva způsoby, jak k hledání zranitelností přistoupit. První, pracnější, kdy na svůj hardware nasadíte nástroj pro hledání zranitelností. Druhý, elegantnější, kdy si skenování zranitelností pořídíte jako službu. Do datové sítě zapojíte pouze zařízení pro skenování a o nic víc už se nestaráte. Jen čekáte na hotové reporty. Rozdíly mezi oběma variantami najdete v tabulce Porovnání řešení SaaS a In House.

Pro automatizaci následující 4. fáze je velmi důležité, jak podrobné a přesné návody na eliminaci zranitelností testovací nástroj obsahuje. Nelze totiž předpokládat, že snadno nasadíme nástroj pro automatickou distribuci patchů pro celou infrastrukturu IS. Existuje totiž velké množství zranitelností, které nelze eliminovat instalací záplat, ale pouze ruční modifikací konfigurace. Ve výsledku tedy vždy zbyde v tomto kroku manuální práce pro administrátory systémů, kteří budou potřebovat kvalitní podklady pro řešení problémů. Ty dnes dokáže většina nástrojů pro testování zranitelností vygenerovat, byť v různé kvalitě a míře detailu. Automatizovat lze v tomto kroku také samotnou prioritizaci (nastavení pořadí) nápravných kroků, které je třeba zrealizovat. Tento seznam úkolů s přiřazenými odpovědnými administrátory a lhůtami pro řešení lze exportovat do nástrojů typu HelpDesk do jednotného prostředí, ve kterém administrátoři přijímají pokyny k řešení. Pokud nástroj pro vulnerability management umožňuje definovat politiky pro různé platformy a skupiny systémů, dokáže jistě také pravidelně reportovat o dosažené míře shody.

Pracujte chytře

Ačkoli se může zdát, že řízení zranitelností je komplikovaný proces, ve skutečnosti tomu tak vůbec nemusí být. Stačí si pořídit chytré nástroje, které udělají drtivou většinu rutinní práce za vás. Během pár hodin tak můžete proměnit váš děravý IS v neprůstřelnou tvrz a stávající adhoc přístup ke sledování zranitelností v transparentní, automatizovaný a měřitelný proces. Nejen štěstí přeje připraveným. ❑

Vulnerability management - Porovnání řešení SaaS a In House

	SaaS (Software jako služba – Software as a Service)	In House
Licence	Vždy zpoplatněna nezanedbatelnou částkou dle rozsahu sledovaných systémů	Kromě placených verzí programů existují i freewarové open-source nástroje
Náklady na hardware	Žádné, vše se nachází u dodavatele služby	Je nutno vyhradit hardwarové prostředky pro nasazení softwaru VM
Náklady na ostatní software	Žádné, vše se nachází u dodavatele služby	Operační, databázový a reportovací systém aj.
Náklady na zaměstnance	Jednotky člověkohodin (nasazení služby)	Desíky i stovky člověkohodin (nasazení, konfigurace, údržba, aktulizace. provádění testů, tvorba reportů aj.)
Přesnost a stabilita	Celkové odladění, stabilita a mizivé procento false-positive nálezů dané centrální správou systému výrobcem.	Jde-li o open-source řešení, nutno počítat s větším procentem (5 % - 10 %) false-positive rate
Škálovatelnost	Stačí zakoupit větší počet testovaných IP adres	Nutno počítat s případným navýšením kapacit HW, SW, zaměstnanců
Podpora	Mnohdy 24×7×365 jako součást služby	Jde-li o open-source řešení, jste závislí na ochotě a seriózności anonymní komunity
Reportování	Centrální uložiště dat, agregace a normalizace dat z různých testů dává jednotné reporty kdykoliv, přes celý IS a v libovolné míře detailu.	Problematická práce s porovnáváním více různých výsledků testování v čase. Zvýšené nároky na manuální a poloautomatické skripty pro reportování napříč IS.
Bezpečnost dat	Data jsou uložena u výrobce/poskytovatele služby, což lze považovat za riziko. Na druhou stranu nutno podotknout, že výrobce služby zpravidla používá velmi vysoké profi-zabezpečení, kterým zákazník většinou nedisponuje.	Data jsou uložena ve firmě, bezpečnost dat se rovná bezpečnosti samotné organizace a je na interních postupech a technologiích, jak data ochránit.
Přizpůsobivost	Závislost na nastavení od dodavatele	Software lze uzpůsobit dle svých požadavků
Legenda	*Plusy*	*Minusy*