

Zákony zranitelností z let 2008–2009

Jaké jsou trendy v chování zranitelností? Dokážeme se poučit z vlastních nebo cizích chyb? Mnohé napoví zkoumání zákonitostí zranitelností prováděné společností Qualys.

Tento článek navazuje na [1] a přináší stručné shrnutí nálezů statistického výzkumu, který provedla firma Qualys v roce 2009 nad výsledky testování svých zákazníků v roce 2008. Výsledky tohoto výzkumu byly poprvé prezentovány na konferenci Black Hat v Las Vegas v červnu 2009 ve formě prezentace a zprávy s názvem Zákony zranitelností ICT verze 2.0 [3]. Definice těchto zákonů je obsažena v tabulce 1.

Úvod – popis zdroje dat

Čtenáře jistě zajímá, na jak velkém reprezentativním vzorku dat bylo statistické chování zranitelností analyzováno a dle jakých závěrů byly Zákony zranitelností definovány. Zdrojem dat pro tento výzkum byly anonymizované výsledky testování zranitelností 80 mil. různých IP adres zhruba 3 500 zákazníků firmy Qualys Inc. Tito zákazníci

v roce 2008 provedli službou QualysGuard celkem 104 mil. testů zranitelností, z nichž 82 mil. bylo zaměřeno na interní IP adresy a 22 mil. testů na externí (internetové) IP adresy. Celkem bylo nalezeno 680 mil. zranitelností, z nichž 72 mil. bylo kritických, tj. stupeň 4–5 z pěti možných.

Výklad použité metodiky a techniky testování, klasifikace zranitelností a míra přesnosti zjištěných nálezů by vydaly na samostatný článek, což je mimo možný rozsah tohoto textu. Zvídavé čtenáře je nutno odkázat na zdroje firmy Qualys nebo na autora tohoto článku. V tomto statisticky významném zkoumaném vzorku jsou proporcionalně zastoupeny všechny hlavní oblasti podnikání a státní správy, z nichž žádná nezabírá více než 15% celkového rozsahu. Z hlediska velikosti zkoumaných organizací ani jedna nepředsta-

vuje více než 5% celkového rozsahu. Vzhledem k architektuře služby QualysGuard založené na SaaS (Software as a Service), silné kryptografii a restriktivní správě klíčů jsou z výsledků testování dostupná pouze sumární data s počty a identifikátory nalezených zranitelností a informace o tom, zda byly detekovány vnitřním testem IP adres nebo vnějším (internetovým) testem. V žádném případě nejsou firmě Qualys dostupné informace o IP adresách, otevřených TCP/UDP portech, verzích instalovaného softwaru ani dalších nastaveních systémů zákazníků.

Rozborem získaných statistických dat byly definovány čtyři klíčové charakteristiky životního cyklu zranitelností od jejich první detekce na zákaznických systémech až do doby, než jsou odstraněny instalací záplaty (Patch, Hotfix) nebo nahrazeny jiným software

Původní název	Volný překlad	Interpretace
Half-life	Poločas rozpadu	Doba, po kterou organizacím trvá snížit počet neošetřených kritických zranitelností na polovinu, nadále setrvává na průměrné lhůtě 30 dnů. Tato lhůta nyní více odráží zranitelnosti nalezené na vnitřních systémech IS. Jejich poločas rozpadu byl v letech 2002–2005 48 dnů, což značí pozitivní trend.
Prevalence	Přetrvávání	Procentuální míra přetrvávání kritických zranitelností v seznamu Qualys TOP20 nejčastěji se vyskytujících klesla z původních 50 na 40 %. To znamená, že pouhých 8 kritických zranitelností zůstalo v seznamu po celý rok. To je pozitivní trend.
Persistence	Trvanlivost	Délka životnosti kritických zranitelností v informačních systémech a sítích organizací zůstává teoreticky nekonečná. Zvýšilo se však procento míry trvale přítomných zranitelností z původních 4 na 7 % což je negativní trend odpovídající více realitě interních systémů.
Exploitation	Využitelnost	Doba, za jak dlouho je sestaven a publikován exploit od prvního zveřejnění zranitelnosti, se v průměru zkrátala z původních 60 na 10 dnů. Zároveň se výrazně zkracuje doba k úspěšně zrealizovanému útoku z původních 15 dní na několik jednotek dní, což je negativní trend.

Tabulka 1: Aktualizované Zákony zranitelností ICT v.2.0.

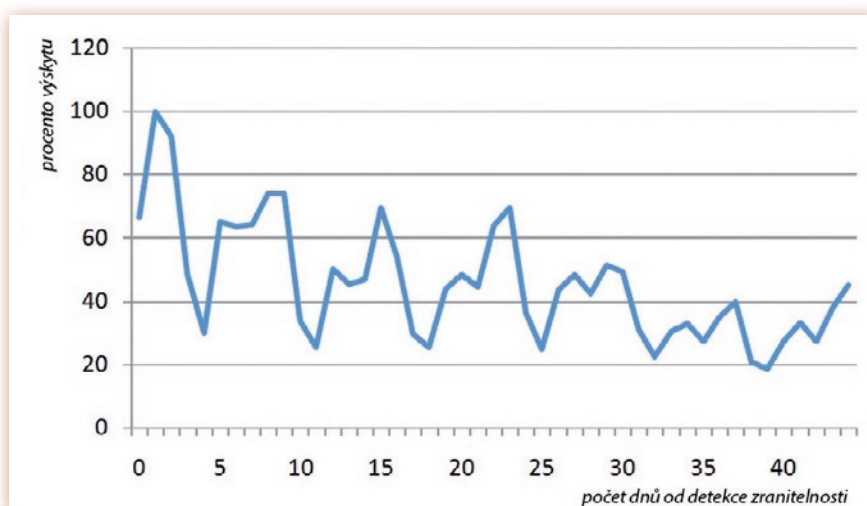
produktem. Následující čtyři kapitoly stručně popisují zjištěné kvality jednotlivých charakteristik a závěry z nich vyplývající.

Zákon 1 – Half-life / Poločas rozpadu

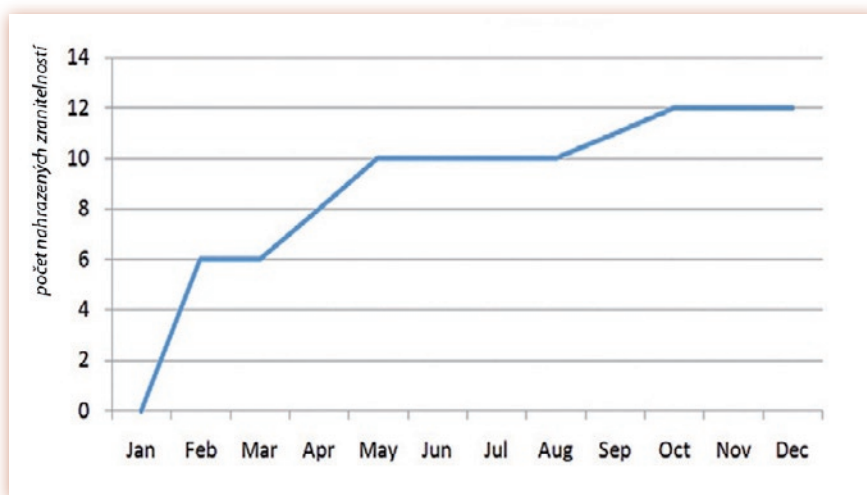
Poločas rozpadu zranitelností ICT znamená dobu měřenou ve dnech, za jak dlouho se podaří organizaci snížit výskyt určité zranitelnosti na 50% maximálního zjištěného rozsahu. Tato charakteristika ukazuje, jak rychle se daří administrátorům odstraňovat zranitelnosti na nejdůležitějších systémech organizace za předpokladu, že tyto jsou aktualizovány nejdříve a zbylých 50% nálezů se nachází na méně kritické infrastruktuře.

Při vyhodnocování této charakteristiky byly vzaty v úvahu pouze nálezy 72 mil. kritických zranitelností (s hodnocením závažnosti 4–5 z pěti možných), protože systematické úsilí při odstraňování zranitelností by mělo být zaměřeno primárně na nejkritičtější zranitelnosti představující největší rizika pro organizace. Obr. 1 ukazuje křivku závislosti výskytu kritických zranitelností na počtu dní, kolik organizace potřebují ke snížení procenta jejich výskytu na polovinu. Nápadně opakující se vzor křivky odpovídá průměrné periodicitě distribuce bezpečnostních aktualizací (záplat), tj. zhruba 1–2x týdně.

Z uvedených dat lze vyslovit první závěr, že průměrná doba potřebná ke snížení počtu kritických zranitelností na systémech organizace na polovinu trvá 29,5 dne. To představuje oproti zjištění z let 2002–2005 pouze mírné zlepšení, neboť tehdy trvalo jejich odstranění průměrně 33,5 dne, přesněji 19 dní u externích systémů a 48 dní u interních systémů. K tomu je nutno uvést, že v letech 2002–2004 převažoval poměr mezi externími a interními testy ve prospěch externích a od druhé poloviny 2004 začal převažovat počet interních



Obr. 1: Poločas rozpadu pro kritické zranitelnosti ICT.



Obr. 2: Přetrvávání nejčastějších kritických zranitelností seznamu TOP20 v roce 2008.

testů nad externími. Od té doby se každým rokem zvyšuje tento poměr ve výrazný prospěch interních takovým tempem, že na konci roku 2008 bylo 80% všech realizovaných testů provedeno na vnitřních LAN zákazníků. Na základě tohoto upřesnění lze vyslovit druhý závěr, že dochází k pozitivnímu trendu zkracování doby odstraňování zranitelností na interních systémech z hodnoty 48 dní na 30 dní.

Zákon 2 – Prevalence / Přetrvávání

Druhý zákon přinesl autorovi tohoto článku největší trápení s překladem a interpretací. V původní zprávě firmy Qualys je tato charakteristika definována jako

míra obměny zranitelností v seznamu Qualys TOP20 [4] nejčastěji se vyskytujících zranitelností v průběhu roku. Qualys tento seznam sestavuje každý týden na základě statistického vyhodnocení 10 nejčastěji se vyskytujících kritických zranitelností ve výsledcích vnitřního testování sítě a 10 nejčastějších kritických zranitelností ve výsledcích externích testů. Opět se tedy jedná o analýzu 72 mil. zranitelností s mírou kritičnosti 4–5 z pěti možných.

Obr. 2 ukazuje, kolik zranitelností ze seznamu Qualys TOP20 bylo v průběhu roku 2008 nahrazeno jinými. Pokud se na graf podíváme obráceně, můžeme si představit, kolik nejčastěji se objevujících kritických zranitelností přetrvává

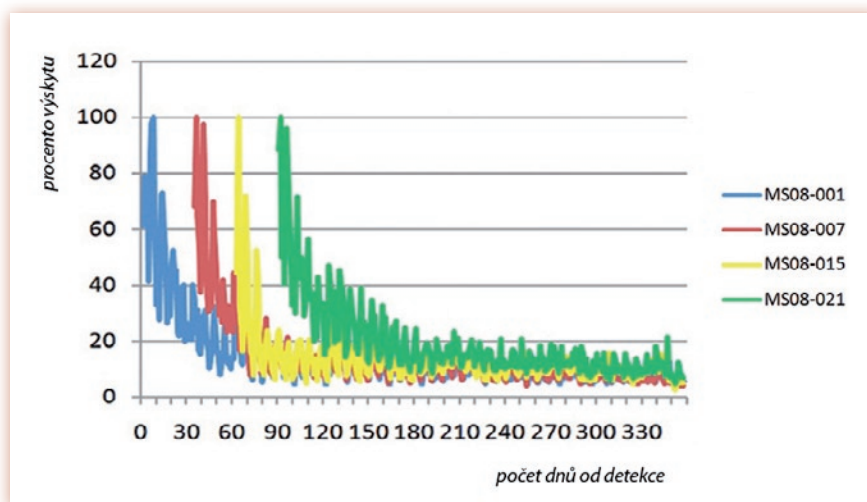
v průběhu roku v seznamu TOP20 beze změny a náhrady.

Na základě analýzy uvedených dat lze vyslovit třetí závěr, že na konci roku 2008 bylo celkem 12 nejčastěji se objevujících zranitelností postupně nahrazeno jinými. To znamená, že 8 zranitelností (40%) se udrželo v seznamu TOP20 po celý rok. Tyto zranitelnosti představují pro útočníky největší sázku na jistotu úspěšného útoku namířenému vůči většině organizací. O které konkrétní zranitelnosti se jedná, zpráva neuvádí.

Z obdobných statistických výzkumů, které provedli další výrobci software [5], [6] v letech 2008 a 2009, vyplývá, že největší počet opomenutých, tj. neodstraněných kritických zranitelností v počítačových sítích se týká desktop aplikací Microsoft Office, Acrobat Reader, QuickTime a Real Player a také to, že na tyto zranitelnosti směřuje stále více cílených útoků. Tímto lze vyslovit čtvrtý závěr, že je třeba zaměřit úsilí administrátorů na záplatování kritických zranitelností uvedených desktop aplikací a vyvarovat se instalace a spouštění těchto aplikací na serverech.

Zákon 3 – Persistence / Trvanlivost

Trvanlivost je charakteristika, která představuje životnost existence vybraných kritických zranitelností (míra 4–5 z pěti možných) v informačních systémech a sítích organizací. Původní předpoklad založený na prvním zákonu napovídal, že by procento výskytu stejných typů zranitelností v organizacích mělo klesnout pod 1% po 7 měsících od jejich nalezení, ale analýza výsledků testování tuto domněnku nepotvrdila. Ukázalo se, že téměř všechny kritické zranitelnosti se bez ohledu na typ a platformu po zhruba půl roce od prvního nálezu ustálí na v průměru 7% trvalé existence, čili nikdy nejsou zcela vymý-



Obr. 3: Míra trvanlivosti vybraných kritických Microsoft zranitelností.

ceny z informačního systému organizace. To je zhoršení oproti výzkumu z let 2002–2005, kde charakteristika trvalé přítomnosti kritických zranitelností v IS byla pouhá 4%.

Toto zjištění vedlo k formulaci zákona trvanlivosti. Lze tak vyslovit pátý závěr, že teoretická trvanlivost (životnost) zranitelností v informačním systému je nekonečná, jak ukazují příklady grafů čtyř Microsoft zranitelností na obr. 3. Jedná se o zranitelnosti Core OS, WebDAV, Outlook a Graphic Libraries, které byly publikovány v lednu, únoru, březnu a dubnu 2008 a které se vždy po cca šesti měsících ustálily na zhruba 7% rozsahu výskytu.

Jako vysvětlení tohoto jevu se nabízí domněnka, že administrátoři postupují při odstraňování zranitelností dle priorit s ohledem na hodnotu zranitelného systému. Vždy se tak najde v organizaci několik zapomenutých pomocných nebo testovacích systémů, k jejichž aktualizaci nikdy nedojde anebo jsou umístěny mimo dosah nástrojů pro distribuci aktualizací. Přesto jsou alespoň jednou v roce zahrnuty do testu zranitelností, které tyto zranitelnosti znovu objeví.

Šestý závěr říká, že do procesů Řízení zranitelností ICT a distribuce bez-

pečnostních aktualizací by měly být zahrnuty všechny aktivní informační systémy organizace, neboť opomenutí méně důležitých systémů může přinést riziko úspěšného průniku do interní IS organizace a následné kompromitace klíčových a kritických systémů zevnitř IS.

Zákon 4 – Exploitation / Využitelnost

Poslední zákon se zabývá dobou, za jakou je sestaven a publikován exploit od prvního zveřejnění zranitelnosti a za jak dlouho dojde k úspěšně zrealizovanému útoku od okamžiku jeho zveřejnění. Exploitem se v informační bezpečnosti rozumí programový kód navržený za účelem kompromitace cílového systému pomocí jedné nebo více konkrétních zranitelností. Výzkum této charakteristiky v letech 2002–2005 ukázal, že pro 80% kritických zranitelností byl sestaven exploit do 60 dnů od jejich zveřejnění a že 90% úspěšně realizovaných útoků bylo provedeno ve lhůtě do 15 dnů od uvolnění exploitů, např. Blaster, Code Red, Nachi, Sasser, Slapper nebo Zobot.

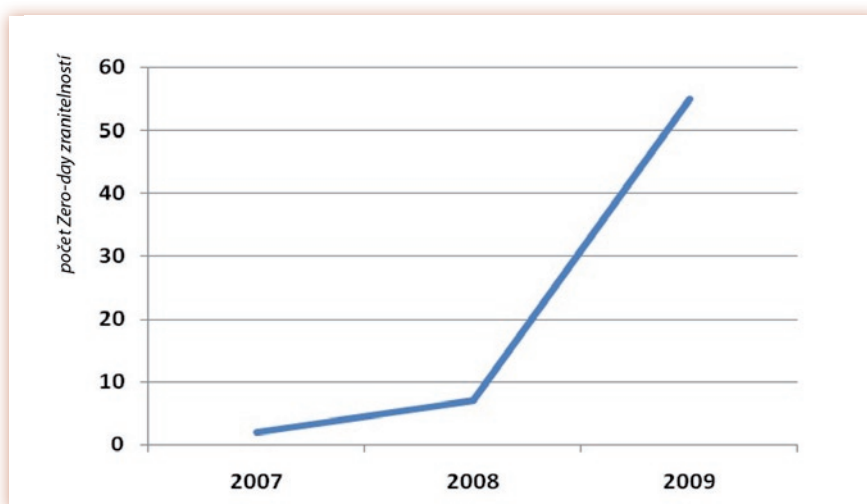
Aktualizovaný výzkum založený na datech z let 2008–2009 ukázal, jak dramatickému zkrácení doby využitelnosti nově publikovaných zranitelností

došlo. Pro mnoho kritických zranitelností jsou k dispozici exploity ve lhůtách kratších než 10 dnů, ideálem je jejich zveřejnění do 24 hodin (Zero-day Vulnerability). Bohužel v mnoha případech je třeba čekat dny, týdny a někdy i měsíce, než výrobce daného software uvolní příslušnou bezpečnostní aktualizaci.

Takové zranitelnosti dávají odpovědným pracovníkům minimální prostor na účinnou reakci a vyvíjejí tlak na výrobce testovacích nástrojů a sond pro detekci síťových útoků na nepřetržitou aktualizaci svých databází signatur (vzorků detekujících a popisujících danou zranitelnost). Důležité je také zodpovědné nakládání s informacemi o nově objevených zranitelnostech. Prospěšné aktivity v tomto směru a cenné informační zdroje poskytuje např. firma VeriSign se svojí „iDefense Initiative“ [7] nebo firma TippingPoint se svojí „Zero-Day Initiative“ [8], které zastřešují bezpečnou komunikaci mezi nezávislými vývojáři/testery a komerčními výrobci software ohledně nově nalezených a dosud nepublikovaných zranitelností. Obr. 4 ukazuje nárůst Zero-day zranitelností v letech 2007–2009.

Předposlední závěr lze definovat tak, že kdo chce proaktivně bránit své systémy před zneužitím kritických zranitelností, měl by systémy testovat v periodě minimálně 1x týdně a ve lhůtě kratší než 10 dnů distribuovat bezpečnostní aktualizace.

Poslední závěr říká, že s ohledem na kritičnost systémů a požadavky na jejich dostupnost nelze všechny systémy v IS aktualizovat stejně často a bez dů-




Obr. 4: Trend Zero-day zranitelností v letech 2007–2009.

kladného prověření dopadu na dostupnost systému. Jako řešení se tudíž nabízí rozdělit systémy na skupinu rychlé distribuce bezpečnostních aktualizací (s menšími požadavky na dostupnost) a skupinu pomalé distribuce aktualizací (s většími požadavky na dostupnost a stabilitu), u které bude třeba zvážit implementaci doplňkových opatření na technické a procedurální úrovni.

Shrnutí

Analýza uvedených charakteristik zranitelností vyústila k sestavení čtyř hlavních Zákonů zranitelností ICT, jejichž stručné definice jsou obsaženy v tabulce 1 v úvodní kapitole. Oproti předchozímu znění Zákonů zranitelností ICT z roku 2006 [2] byly zredukovány z 6 na 4.

Z výsledků statistického výzkumu je patrné určité zlepšení v systematickosti boje organizací s odstraňováním zranitelností. U středních a velkých informačních systémů je dnes aplikace

automatizovaných nástrojů pro rychlou detekci zranitelností na síťové a aplikační vrstvě a nástrojů pro rychlou distribuci aktualizací naprostou nutností. Současné dynamice hrozby zneužití kritických zranitelností již ad-hoc manuální testování nestačí. Riziko rychlé a úspěšné kompromitace informačních systémů je stále aktuální v oblasti zranitelností operačních systémů (viz Conficker) i ve stále rostoucí oblasti zranitelností na aplikační rovině – zejména u desktop a webových aplikací. 

Marek Skalický
mskalicky@qualys.com

Marek Skalický



Regional Account Manager společnosti Qualys pro země střední a východní Evropy. Dříve pracoval jako Senior Consultant ve společnosti RAC.

POUŽITÁ LITERATURA

- [1] SKALICKÝ, M. *Úvod do řízení zranitelností ICT*. DSM č. 3/2007, s. 28–31.
- [2] ESCHELBECK, G. *The Laws of Vulnerabilities: Six Axioms for Understanding Risk*. Qualys Inc. 2006. <http://www.qualys.com/docs/Laws-Report.pdf>.
- [3] KANDEK, W. *The Laws of Vulnerabilities 2.0: Black Hat 2009 Edition*. Qualys Inc. 2009. http://www.qualys.com/docs/Laws_2.0.pdf.
- [4] *Qualys TOP20 Vulnerabilities*. Qualys Inc. <http://www.qualys.com/research/rnd/top10/>.
- [5] *Microsoft Security Intelligence Report, Vol.6 / 2008*. <http://www.microsoft.com/security/about/sir.aspx>.
- [6] *PDF file format vulnerabilities*. F-Secure Inc. 2009. <http://www.f-secure.com/weblog/archives/00001676.html>.
- [7] *iDefense Labs*. VeriSign Inc. <http://labs.iddefense.com/>.
- [8] *Zero-Day Initiative*. TippingPoint Inc. <http://www.zerodayinitiative.com/>.