

Úvod do řízení zranitelností ICT

Co jsou technické zranitelnosti ICT produktů si dnes každý dokáže představit sám, většinou na základě své vlastní bořké zkušenosti. Že lze něco takového řídit a hlavně proč a jak napoví úvodní článek do této problematiky.

S technickými zranitelnostmi nejrůznějších ICT produktů se sice setkáváme dnes a denně, ale většina z nás o tom nemá tušení. Vlastníme a využíváme informační a komunikační technologie, které obsahují zpravidla desítky neošetřených zranitelností. Řídíme provoz či jsme odpovědní za bezpečnost informačních systémů, které obsahují v souhrnu stovky až tisíce zranitelností aniž bychom tušili jejich kvantitu a závažnost. Pro někoho sladká nevědomost, pro jiné noční můra.

CO JSOU ZRANITELNOSTI ICT A CO VŠECHNO JE ZRANITELNÉ?

Z bezpečnostních příruček a norem víme, že zranitelnost systému nebo jeho prvku je slabé místo, které může být využito vnější hrozbou tak, že dokáže způsobit negativní dopad [1]. Stejně jako bezpečnost informací řešíme v rovině fyzické, technologické, personální a administrativní, rozeznáváme také zranitelnosti dle uvedených oblastí [2]. Na zranitelnosti technického a programového vybavení a komunikačních prostředků v technologické rovině bezpečnosti je zaměřen tento článek.

Technické zranitelnosti ICT produktů vycházejí z jejich povahy a jsou to nejčastěji chyby v programovém kódu, vzniklé během vývoje produktů nebo při jejich aktualizacích a opravách. První skupinu tvoří chyby v kódu technických prostředků informačních systémů, tedy ve firmware obsaženém v nejrůznějších zařízeních a jejich komponentách. Druhou a nejpočetnější skupinou jsou technické zranitelnosti v kódu operačních systémů a aplikačního programového vybavení, které se na technické prostředky IS instalují. Třetí významnou

skupinu zranitelností ICT představují chyby v instalaci a konfiguraci jak technických prostředků, tak instalovaného programového vybavení. Chybně nastavený parametr operačního systému či firewallu stejně jako ponechané výchozí heslo u aktivního síťového prvku již mnohokrát poskytly velkou radost hackerům a lammerům nebo emoci prostou vstupní bránu třeba pro vniknutí červa dovnitř infrastruktury IS. Konečně také chyby v návrhu bezpečnostní architektury IS, jaké představuje například nevhodně zvolený typ aktivního prvku, představují poslední skupinu technických zranitelností, které v IS čekají na úspěšné zneužití správně nasměrovanou hrozbou.

ZÁKONITOSTI CHOVÁNÍ ZRANITELNOSTÍ V IS

Zranitelnosti ICT produktů a systémů lze dělit podle způsobu jejich dostupnosti, tedy způsobu zneužití, na: „network-based“ a „host-based“. První skupina zranitelností je využitelná po síti libovolným i anonymním útočníkem zpravidla pomocí protokolu TCP/IP bez potřeby bližší znalosti cílového systému. Tyto zranitelnosti bývají vstupní branou pro další eskalaci útoku uvnitř infrastruktury IS nebo mohou daný systém zcela kompromitovat. Příklady mohou být získání příkazového řádku v kontextu systémové služby, 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 umožní zneužitá „network-based“ zranitelnost vzdálený přístup a otevře dveře k odhalení plejády čekajících „host-based“ typů zranitel-

ností. Získání vyšších privilegií, výpisy adresářových struktur či výpisy přístupových práv citlivých adresářů jsou příklady těch lehčích kalibrů „host-based“ zranitelností. Dalším typem může být možnost zavlčení a spuštění vzdáleného kódu, získání seznamů uživatelských účtů a jejich hesel, získání obsahu souborů, modifikace log souborů; zkrátka pestrá paleta nástrojů, které šikovnému hackerovi pomohou získat potřebné informace a ještě za sebou uklidit stopy – ať se za pár měsíců forenzní audit vyřadí. Většinu správců IS možná napadne, že hrozby průmyslové špiónáže v českých zemích nejsou aktuálním problémem, ale stačí se podívat kolem sebe. Například v sousedním Německu v automobilovém průmyslu toto představuje již mnoho let reálnou hrozbu a neoprávněná manipulace se stavem bankovního účtu (pochopitelně cizího) cestou elektronického bankovníctví pronikla již i do České republiky.

Na základě dlouhodobého statistického sledování vývoje nových typů zranitelností ICT a hrozeb šířících se Internetem a sledováním chování zranitelností a příčin útoků v IS organizací byl sestaven dokument, popisující zákonitosti chování technických zranitelností ICT [5]. Dokument vytvořil technický ředitel firmy Qualys Inc. na žádost amerického kongresu k tématu boje proti cyberterorismu v roce 2005 a shrnuje výsledky výzkumu této společnosti od roku 2002. Stručné shrnutí této zprávy obsahuje tabulka 1. Z analýzy lze odvodit, že zranitelnosti ICT produktů představují pro jejich uživatele a správce závažný problém a systematickým přístupem k jejich eliminaci lze významně snížit riziko úspěšného napadení IS. Jeden příklad



za všechny: pokud nalezneme 10 nejkritičtějších zranitelností a odstraníme je do 15 dnů od jejich zveřejnění, snížíme tím o 90 % pravděpodobnost úspěšného útoku na náš systém, tj. na pouhých 10 %. Takové zvýšení bezpečnosti provozu IS už stojí za pozornost. Kde se vzal Vulnerability Management? Pokud považujeme za bernou minci pro návrh a řízení bezpečnosti lety provedené a renomované ISO normy, vzniklé převážně na základě původních britských standardů řady BS 7799, tak v normě ISO 17799 [3] ve vydání z roku 2000 ještě není systematickému zvládnutí zranitelností ICT věnována dostatečná pozornost. Změna nastává až s aktualizací této normy v roce 2005, který můžeme bez nadsázky nazvat rokem vzniku problematiky v originále nazvané „Vulnerability Management“. Český překlad zní „Řízení zranitelností“ a není to pouze v souvislosti se sestavením zmiňovaných zákonitostí chování zranitelností ICT.

V roce 2005 je přidána do nového (a dosud platného) vydání normy ISO 17799 [3] kapitola druhé úrovně 12.6 „Technical Vulnerability Management“, před-

stavující samostatnou kategorii bezpečnosti, se specifikovaným cílem „Snížit rizika vyplývající ze zneužití veřejně publikovaných technických zranitelností“ a s nově doporučeným opatřením číslo 12.6.1 „Řízení, správa a kontrola technických zranitelností“. Zároveň v tomto roce vychází výrazně přepracovaný standard amerického normalizačního institutu NIST pod označením Special Publication 800-40 v.2.0 [6], který se touto problematikou podrobně zabývá na 75 stranách.

Konečně také v roce 2005 došlo k převzetí britského standardu BS 7799-2:2002 do soustavy norem ISO řady 27001:2005 [4] a tím byla otevřena cesta k certifikačním systémům řízení bezpečnosti informací dle uvedeného mezinárodního standardu. Tento standard klade důraz na systematický a dlouhodobý přístup k analýze a zvládnutí rizik IS obecně, kam bezpochyby zranitelnosti ICT produktů náleží. Zajímavostí je, že nové opatření 12.6.1 normy ISO 17799 [3] bylo hned v úvodní kapitole této normy zařazeno do výčtu několika vybraných opatření, která jsou považována za základ nejlepších praktik a měla by být

aplikována ve všech organizacích bez rozdílu velikosti a zaměření. Bude zajímavé sledovat, jak se tímto doporučením budou řídit nejenom bezpečnostní manažeři, ale také auditorské firmy právě při certifikacích organizací na systém řízení bezpečnosti informací dle normy ISO 27001.

Jak proces řízení zranitelností funguje? Samotný proces řízení zranitelností ICT není z hlediska architektury nijak komplikovaný a při respektování požadavků opatření 12.6.1 normy ISO 17799 [3] jej lze sumarizovat do šesti základních kroků, které, jak ukazuje obr. 1, se periodicky opakují. Hlavním účelem tohoto procesu je posunout organizace z výchozího adhoc řešení této problematiky do sledovaného a řízeného stavu, ve kterém je známo kolik, kde a jak závažných zranitelností se v IS nachází a jejich postupné eliminace v závislosti na kapacitách a nastavených prioritách organizace. Je zřejmé, že prioritně je potřeba řešit nejzávažnější zranitelnosti, s potenciálně největším negativním dopadem na nejkritičtější systémy, a poté se věnovat těm méně závažným. Má to své opodstatnění i z hlediska zjištěných

zákonitostí chování zranitelností [5]. Pokud z celkového objemu prací potřebných na eliminaci všech zjištěných zranitelností vynaložíme pouhých 10 % přesně a cíleně, snížíme míru rizika úspěšného zneužití zranitelností na pouhých 10 %.

Abychom dosáhli kýženého cíle, je nutně třeba mít přesný výčet aktivních a neaktivních systémů v IS. To je úkolem 1. fáze procesu. Neznámý aktivní prvek v systému představuje riziko neznámé velikosti a o tom, že každý obsahuje zra-

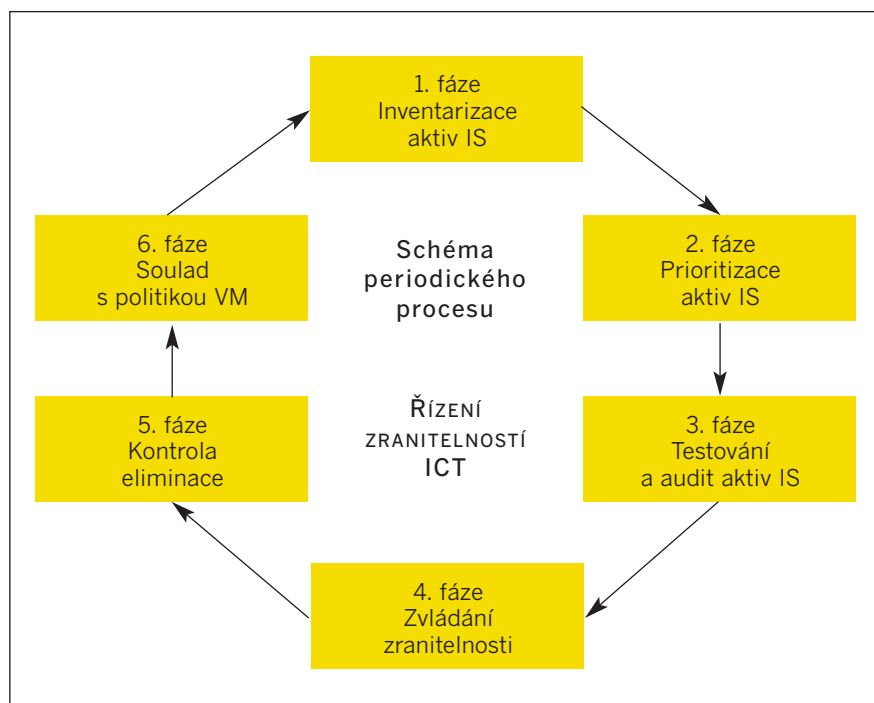
produktů a jejich zranitelností včetně jejich ohodnocení a podrobného výkladu a návodu na odstranění.

Poté, co máme otestovanou infrastrukturu IS, je třeba přistoupit ke klíčovému okamžiku procesu a tím je rozhodnutí o pořadí eliminace zjištěných zranitelností. Toto je prvním krokem 4. fáze procesu, ve kterém by mělo dojít k porovnání hodnot zranitelností s hodnotou systému, na kterém byla detekována, a dle těchto hodnot stanovit kritičnost

platformy a skupiny prvků IS různé bezpečnostní politiky akceptovatelných a neakceptovatelných zranitelností a kontrolovat, zda se daří tyto cíle naplňovat. Velmi účinné bývá zohlednit splnění těchto cílů v prémiových ukazatelích odpovědných administrátorů; to už ale nepatří do řízení zranitelností, ale do řízení lidských zdrojů.

JAK PROCES ŘÍZENÍ ZRANITELNOSTÍ ZEFEKTIVNIT?

Je zřejmé, že 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 i tisíce zranitelností, od málo významných až po nejkritičtější. Aby byl proces řízení zranitelností v takovém rozsahu funkční, je naprosto nezbytné jej co nejvíce automatizovat. Z výše uvedeného popisu jeho funkcí a kroků je zřejmé, že automatizovat se dá převážná část činností (podle mého odhadu až 90 %), a to při použití správné kombinace nástrojů na asset management, vulnerability management a patch management. Na trhu existuje několik málo produktů, které pokrývají více těchto funkcí, ovšem každá integrace funkcí znamená zpravidla nižší podporu platform a produktů, na které lze řešení aplikovat. Výběr správné kombinace nástrojů záleží na mnoha faktorech a není již předmětem tohoto článku.



OBR. 1: SCHÉMA PERIODICKÉHO PROCESU ŘÍZENÍ ZRANITELNOSTI ICT.

nitelnosti, není pochyb. Pokud evidujeme všechny systémy v IS, musíme nutně rozlišit jejich důležitost pro organizaci a dle ní nastavit priority při eliminaci zranitelností. To je úkolem 2. fáze procesu. Nutnou podmínkou pro tento krok musí být alespoň rámcově provedená analýza dopadů (BIA – Business Impact Analysis), aby bylo možné jednotlivým prvkům v IS přiřadit hodnoty. Zjišťování existujících zranitelností metodou network-based a nebo host-based je úkolem 3. fáze procesu. K tomu je nezbytné použít některý z automatizovaných nástrojů pro testování zranitelností IS. Na trhu jich je celá řada, od jednoduchých open-source až po složité profesionální nástroje s velmi přesnými testovacími mechanismy a obsáhlými databázemi ICT

zranitelnosti a její prioritu pro organizaci. Měla by také existovat bezpečnostní politika nebo směrnice pro řízení zranitelností, která definuje časové okno pro eliminaci zjištěných zranitelností právě na základě míry jejich kritičnosti pro organizaci. Čím je kritičnost vyšší, tím kratší je časový úsek a vyšší priorita k jejich odstranění. Kontrolou, že proces eliminace probíhá v souladu se stanovenými prioritami, se zabývá 5. fáze procesu. Zdroje organizace jsou omezené, čas administrátorů IS drahý a tak je třeba se při odstraňování zranitelností důsledně řídit bezpečnostními prioritami a potřebami, jinak proces řízení zranitelností neplní svou funkci. Poslední, 6. krok procesu, nám umožňuje definovat pro určité

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, pro kterou na trhu existuje největší počet nástrojů, s různě obsáhlou databází zranitelností, s různě velkou podporou platform a metod testování zranitelností (viz host-based a network-based). Pro automatizaci následující 4. fáze je velmi důležité, jak podrobné a přesné návody na eliminaci zranitelností testovací nástroj obsahuje. Nelze totiž předpokládat, že snadno a plošně nasadíme nástroj pro automatickou distribuci patchů pro infrastrukturu IS v heterogenním prostředí. Také existuje velké množství zranitelností, které

ZÁKON	PŮVODNÍ NÁZEV	VOLNÝ PŘEKLAD	INTERPRETACE
1	Half-life	Poločas rozpadu	Doba, po kterou organizacím trvá snížit počet neošetřených nejkritičtějších zranitelností na polovinu, je u externích systémů zpravidla 19 dnů, u interních 48 dnů.
2	Prevalence	Periodicita	50 % nejrozšířenějších a nejkritičtějších zranitelností (SANS TOP20 list) se každoročně vrací do oběhu, někdy mírně modifikované (např. CVE-2005-0560).
3	Persistence	Trvanlivost	4 % nejkritičtějších zranitelností zůstává v IS trvale aktivními a neošetřenými. Vrací se s novými instalacemi nebo jsou opomenuty v rámci patch managementu.
4	Focus	Ohnisko útoků	90 % všech úspěšných útoků na ICT infrastrukturu bylo provedeno s využitím pouze 10 nejkritičtějších zranitelností. Jejich rozpoznáním a prioritní eliminací lze dosáhnout výrazného snížení rizika úspěšného průniku do IS.
5	Exposure	Okno k útoku	Pro 80 % zranitelností se objeví „exploit“ dříve, než uplyne poločas jejich rozpadu (snížení jejich počtu v IS pod 50 %). Je nutná průběžná detekce a rychlá reakce v řádu dní.
6	Exploitation	Využití útoku	Téměř 90 % všech úspěšných útoků na ICT bylo provedeno v časovém okně do 15 dnů od zveřejnění zranitelnosti, která byla útokem využita. Perioda testování a záplatování ICT produktů musí být proto výrazně kratší než 14 dnů.

TABULKA 1: ZÁKONITOSTI CHOVÁNÍ ZRANITELNOSTÍ ICT.

nelze eliminovat instalací záplaty, ale pouze ruční modifikací konfigurace, takže v tomto kroku vždy zbude manuální práce pro administrátory systémů a ti budou potřebovat kvalitní podklady pro řešení problémů. Automatizovat lze v tomto kroku 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, ve kterém administrátoři přijímají pokyny k řešení. Pokud nástroj pro řízení zranitelností umožňuje definovat politiky pro různé platformy a skupiny systémů, dokáže i stále také pravidelně podávat zprávy o dosažené míře shody.

ZÁVĚR

Předcházející kapitoly naznačily, že problematika řízení zranitelností ICT přesahuje do dalších souvisejících procesů v řízení provozu a bezpečnosti IS jako je řízení HelpDesku, Patch Management,

Asset Management nebo Risk Management. Jedná se tedy o komplexní problematiku, kterou je třeba implementovat na míru, dle prostředí a preferencí každé organizace, a snažit se maximálně napojit na stávající postupy a již implementované nástroje pro jejich automatizaci.

Problematika řízení zranitelností ICT je primárně doménou bezpečnostního správce IS a bezpečnostních manažerů v organizacích, protože ti jsou odpovědní za identifikaci rizik a návrh odpovídajících, přijatelných a účinných opatření. Smysluplně nasazený proces s kvalitním nástrojem pro řízení zranitelností však významně pomůže zefektivnit práci také IT managerům a administrátorům IS, kteří jsou odpovědní nejen za provoz IS, ale také za implementaci bezpečnostních opatření. Proces spolu s vhodným nástrojem včas upozorní na nejdůležitější problémy, přiřadí jim optimální prioritu a poskytne detailní návod na jejich odstranění.

Řada realizovaných projektů implementace procesu řízení zranitelností IS, spolu s nasazením nástrojů pro jejich automatizaci v praxi ukázala, že střízlivě navržená politika řízení zranitelností spolu se směrnicí definující základní kroky, priority a odpovědnosti v řízení a eliminaci zranitelností v organizaci přispívá ke zlepšení spolupráce mezi odděleními bezpečnosti a správy IS.

MAREK SKALICKÝ
skalicky@rac.cz



MAREK SKALICKÝ

Nastoupil do společnosti Risk Analysis Consultant v roce 2003, kde se jako Senior Consultant věnuje projektům v oblasti řízení bezpečnosti informací v organizacích a jako QualysGuard Solution Manager také oblasti řízení zranitelností ICT s využitím produktů firmy Qualys.

LITERATURA:

- [1] ISO/IEC 13335-1:2004 IT - Security techniques - Concepts and models for information and communications technology security management
- [2] BS 7799-3:2006 ISMS - Guidelines for information security risk management
- [3] ISO/IEC 17799:2005 IT - Security techniques - Code of practice for information security management
- [4] ISO/IEC 27001:2005 IT - Security techniques - Information security management systems – Requirements
- [5] Qualys Inc, Gerhard Eschelbeck - The Laws of Vulnerabilities: Six Axioms for Understanding Risk; <http://www.qualys.com/docs/Laws-Report.pdf>
- [6] NIST SP 800-40 Version 2.0 – Creating a Patch and Vulnerability Management Program; <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

MANAGEMENT SUMMARY

Donedávna byla problematika testování zranitelností ICT a jejich odstraňování chápána jako umění hackerů ve službách konzultačních firem a nárazové obtěžování administrátorů IS formou penetračního testování. Kam ale ve skutečnosti patří, jak zvládnutí zranitelností IS plošně a efektivně provádět a koho se v organizacích týká? Článek popisuje proces řízení zranitelností ICT ve světle požadavků norem ISO a v kontextu řízení rizik a bezpečnosti v organizacích.