Ing. Miroslav Čermák
Policejní akademie České republiky v Praze
student doktorského studia

Úskalí řízení technických zranitelností

Řízení technických zranitelností, v anglosaské literatuře označované jako vulnerability management je jedna z mnoha činností manažera kybernetické bezpečnosti,[1] které by se měl manažer intenzivně věnovat, neboť do značné míry rozhoduje o tom, zda útok na organizaci, pro kterou pracuje, bude úspěšný či nikoliv. Je tomu tak proto, že drtivá většina útoků z kyberprostoru na informační systémy zneužívá technických zranitelností v systémech a nejsou to primárně jen tzv. zranitelnosti nultého dne, jejichž podstata je blíže vysvětlena dále v této práci, nýbrž zranitelnosti, které jsou veřejně známé po poměrně dlouhou dobu a existují pro ně i odpovídající záplaty.

Manažer kybernetické bezpečnosti by měl proto tyto zranitelnosti v provozovaných systémech identifikovat a řídit, tzn., že by měl vždy posoudit závažnost dané zranitelnosti ve vztahu k provozovanému systému a cílům organizace. Za tímto účelem by měl provádět pravidelné skeny zranitelností a odebírat bezpečnostní zpravodaje týkající se systémů, které organizace, jež ho najala, provozuje. Je třeba si však uvědomit, že organizace se může stát jak předmětem cíleného, tak i plošného útoku a včasné odhalení bezpečnostních zranitelností a jejich odstranění anebo nasazení záplaty nebo workaroundu (náhradní řešení) podstatně snižuje dopady vyplývající z daného kybernetického útoku.

Zpravidla se za tímto účelem používají automatické skenery, které prohledávají určitý IP adresní rozsah a vyhodnocují, zda na komponentě, které je daná IP adresa přidělena, neběží nějaký produkt, který by trpěl určitou zranitelností. Problém je, že dost často se pak počet zranitelností bere jako jedna z klíčových metrik při posuzování úrovně kybernetické bezpečnosti v organizaci a jejich rostoucí nebo klesající počet je pak mylně interpretován jak zhoršení nebo naopak zlepšení stavu kybernetické bezpečnosti v organizaci.

Tento příspěvek si proto klade za cíl popsat, co je to zranitelnost, jak je třeba její závažnost hodnotit, jaký je její životní cyklus a konečně proč nemůže být nějaký trend v počtu zranitelností brán jako klíčový faktor v hodnocení úrovně kybernetické bezpečnosti v organizaci, aniž by byly vzaty v úvahu skutečnosti uvedené dále.

Zranitelnosti

Nejprve je třeba vysvětlit, co je to zranitelnost neboli slabina, a že zranitelnosti jsou nedílnou součástí informačních systémů a ten jich může obsahovat i více. Zranitelnost může být do systému zanesena úmyslně anebo neúmyslně už v okamžiku jeho návrhu (design flaw), při kódování (coding error) nebo implementaci (implementation error) v konkrétním prostředí a nacházet se může i v jakékoliv

[1] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

komponentě tvořící informační systém, avšak o její přítomnosti nemusí mít nikdo po poměrně dlouhou dobu vůbec tušení.

Na této skutečnosti nic nemění ani fakt, zda se jedná o otevřený nebo uzavřený systém a zda jsou k dispozici zdrojové kódy (open source) či nikoliv (closed source), protože zranitelnosti se běžně nacházejí v obou případech.

V okamžiku, kdy je zranitelnost odhalena bezpečnostním výzkumníkem (security researcher), a není k dispozici žádné řešení odstraňující danou zranitelnost, tak hovoříme o **zranitelnosti nultého dne** (zero day vulnerability) a to až do té doby, dokud nejsou zveřejněny informace ohledně této zranitelnosti.

Pojem zero day v sobě nese odkaz na fenomén 90 let, kdy docházelo ke krádežím oblíbených komerčních aplikací díky průnikům do firemních počítačů jednotlivých vývojářských studií a následnému zpřístupnění těchto aplikací na tzv. warez fórech, přičemž počet dnů vyjadřoval kolik dní od oficiálního prodeje se na warez fóru aplikace objevila. A v okamžiku, kdy dříve než v obchodě, tak se hovořilo o Zero Day.

Životní cyklus zranitelnosti

V okamžiku objevení zranitelnosti se otevírá tzv. **okno zranitelnosti** (Window of Vulnerability, zkr. WoV) někdy též nazývané jako okno příležitosti (Window of Opportunity nebo také Window of Exposure). WoV zůstává otevřené do té doby, než uživatel nasadí **záplatu** (patch) odstraňující danou zranitelnost anebo novou verzi, která ji už neobsahuje a teprve pak se WoV uzavírá.

Ovšem ne každá organizace může záplatu, odstraňují nějakou zranitelnost, ihned nasadit, obzvlášť pokud provozuje kritický systém. Nemůže totiž akceptovat ne zcela zanedbatelné riziko, že by záplata mohla způsobit významnou degradaci výkonu,[1] pád daného systému, anebo by také nemusel nastartovat vůbec,[2] takže ji musí za tímto účelem nejprve otestovat. Otestování takového systému pak může trvat i několik týdnů, a proto může být taková organizaci i několik týdnu po uvolnění záplaty stále zranitelná. Zkušenosti z několika organizací ze státního i soukromého sektoru, které byly sledovány po dobu několika let, ukazují, že tato doba se i v případě vysoké automatizace, virtualizace a použití cloudů pohybuje v řádu jednotek dnů až týdnů, což může být problém.

Pro úplnost je nutné dodat, že v okamžiku, kdy se záplata na danou zranitelnost neobjeví vůbec, což není zase až tak výjimečný případ, jak by se mohlo zdát, tak se pak dokonce s jistou nadsázkou dá hovořit o věčné zranitelnosti (forever day vulnerability).

Přítomnost zranitelnosti ještě neznamená, že jí bude automaticky zneužito, k tomu může dojít až v okamžiku, kdy někdo napíše funkční **exploit**, což je kód, který dokáže dané zranitelnosti zneužít, a který pak zpravidla v sobě nese i nějaký payload,

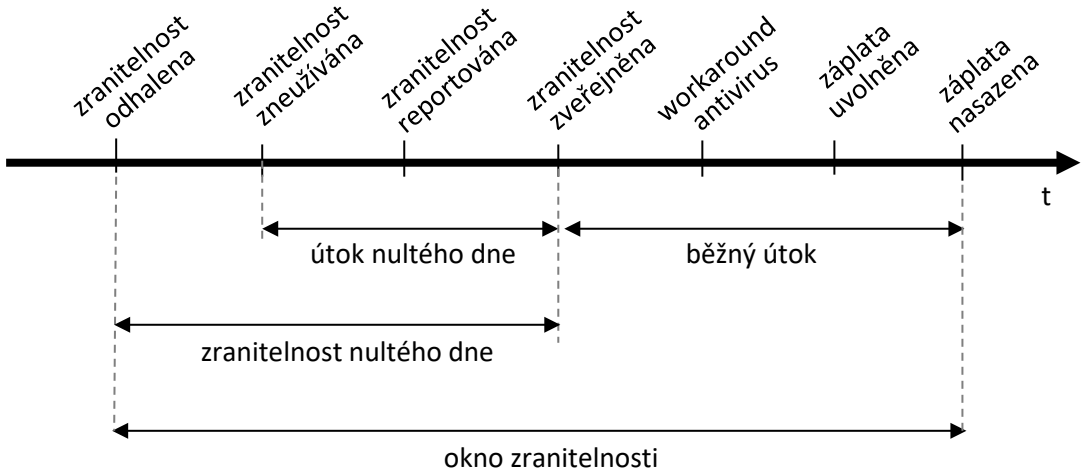
[1] MAURO, Andrea. Performance impact of CPU bug fixes - vInfrastructure Blog [online]. 25. srpen 2018 [vid. 17. únor 2019]. Získáno z: https://vinfrastructure.it/2018/08/performance-impact-of-cpu-bug-fixes/

[2] VENKAT0745. A patch is preventing the system from starting [online]. 20. únor 2014 [vid. 17. únor 2019]. Získáno z: https://answers.microsoft.com/en-us/windows/forum/all/a-patch-is-preventing-the-system-from-starting/590fab3b-6efc-46f1-beb0-9bb1d1dc7b29

který provádí vlastní škodlivou činnost. A pokud k tomu dojde, tak hovoříme o **útoku nultého dne** (zero day attack).

Tato skutečnost je mainstreamovými médii nejčastěji znázorňována na jedné časové ose, tak jak je uvedeno na *Obrázek 1 – životní cyklus zranitelnosti*.

Obrázek 1 – životní cyklus zranitelnosti



Zdroj: vlastní zpracování

Na *Obrázek 1 – životní cyklus zranitelnosti* si lze také všimnout, že antivirus, zkr. AV, je nasazen až poté, co je zveřejněna daná zranitelnost, ovšem může být nasazen i dříve, např. v okamžiku, kdy je detekován exploit, a ten může být detekován i dříve, než je zranitelnost reportována vývojáři a zveřejněna.

U zranitelnosti (vulnerability), exploitu a záplaty (patch) lze v zásadě identifikovat 4 různé stavy, ty jsou zachyceny v *Tabulka 1 – zranitelnost-exploit-záplata*. Z důvodu neexistence odpovídajícího českého výrazu je použit původní termín exploit. Jednotlivé stavy u zranitelnosti, exploitu a záplaty jsou uvedeny v pořadí, v jakém po sobě zpravidla následují, ale ne vždy tomu tak musí být.

Tabulka 1 – zranitelnost-exploit-záplata

zranitelnost (vulnerability)	přítomna (present)	odhalena (disclosed)	nahlášena (reported)	zveřejněna (published)
Exploit	neexistuje (not exists)	vyvinut (developed)	prodán (sold)	zneužit (misused)
Záplata (patch)	neexistuje (not exists)	vytvořena (created)	uvolněna (released)	nasazena (deployed)

Zdroj: vlastní zpracování

Zranitelnost může být:

- přítomna v produktu od začátku, jen ještě nebyla odhalena, a také odhalena být nikdy nemusí, na některé zranitelnosti se přišlo až po několika desítkách let;
- odhalena bezpečnostním výzkumníkem, který zranitelnosti cíleně vyhledává, vývojářem daného produktu, ale stejně tak může být odhalena i zcela náhodou uživatelem;
- nahlášena vývojáři, a ten by měl zranitelnost v produktu odstranit;
- zveřejněna a uvedena např. v nějaké oficiální veřejně dostupné databázi zranitelností.

Exploit

- neexistuje minimálně do té doby, dokud někdo neodhalí konkrétní zranitelnost;
- vyvinut přímo výzkumníkem, který danou zranitelnost našel nebo někým jiným;
- prodán poskytnut vývojáři zranitelného produktu, bezpečnostní komunitě anebo prodán tomu, kdo nejvíce zaplatí;
- zneužit přímo výzkumníkem, ale ten jej zpravidla prodá, a exploit se pak stane součástí nějakého exploit kitu a je zneužíván k (Advance Persistent Threat, zkr. APT) útokům.

Záplata

- neexistuje do té doby, dokud zranitelnost není nahlášena nebo zveřejněna;
- vytvořena v okamžiku, kdy se autor daného produktu o zranitelnosti dozví, může na záplatě začít pracovat a připravit ji;
- uvolněna v okamžiku, kdy je záplata uvolněna, tak kdokoliv, kdo používá produkt trpící danou zranitelností, ji může nasadit;
- nasazena a rychlost nasazení záplaty závisí na tom, zda se uživatel daného produkt vůbec o tom, že jeho produkt nějakou zranitelnost obsahuje, dozví a nasadí ji, anebo zda se produkt sám aktualizuje.

Vzhledem k tomu, že životní cyklus zranitelnosti, exploitu a záplaty jsou na sobě relativně nezávislé, jediným předpokladem je, že exploit může vzniknout až po odhalení zranitelnosti a záplata zase až poté, co je daná zranitelnost nahlášena, tak přechod mezi ostatními stavy je relativně volný. *Obrázek 2 – exploit-zranitelnost-záplata* zachycuje jen jeden z několika možných případů.

Obrázek 2 – exploit-zranitelnost-záplata

Zdroj: vlastní zpracování

V reálném světě můžeme zaznamenat hned několik situací, ke kterým může s větší či menší pravděpodobností dojít, a které jsou zachyceny v *Tabulka* 2 – exploit-zranitelnost-záplata a možné stavy. Další příklad je uveden v *Příloha E – Životní cyklus zranitelnosti*. V zásadě může nastat 6 různých stavů, neboť se jedná o permutaci 3 prvkové množiny, kterou tvoří stav zranitelnost, exploit a záplata, a kterou lze zapsat jako 3!

Tabulka 2 – exploit-zranitelnost-záplata a možné stavy

Stav	Fáze 1	Fáze 2	Fáze 3
1.	zranitelnost zveřejněna	exploit zneužíván	záplata nasazena
2.	zranitelnost zveřejněna	záplata nasazena	exploit zneužíván
3.	exploit zneužíván	zranitelnost zveřejněna	záplata nasazena
4.	exploit zneužíván	záplata nasazena	zranitelnost zveřejněna
5.	záplata nasazena	zranitelnost zveřejněna	exploit zneužíván
6.	záplata nasazena	exploit zneužíván	zranitelnost zveřejněna

Zdroj: vlastní zpracování

Jednotlivé situace uvedené v *Tabulka 2 – exploit-zranitelnost-záplata* a možné stavy lze popsat takto:

1. Bezpečnostní výzkumník objevil zranitelnost a ta byla zveřejněna včetně podstatných detailů, která umožnila vytvoření exploitu zneužívající tuto zranitelnost. Obvykle k této situaci dochází v okamžiku, kdy vývojář nespolupracuje na jejím odstranění. Záplata pak zpravidla přichází až v okamžiku, kdy je zranitelnost aktivně zneužívána.
2. Je zveřejněna základní informace o zranitelnosti, zpravidla obsahující jen nezbytně nutné informace, a v rychlém časovém sledu pak je uvolněna i záplata. Teprve poté se objevuje exploit, takže v ohrožení jsou jen ti, co záplatu nenasadili. Tento stav by se dal označit jako ideální.
3. Po objevení zranitelnosti bezpečnostním výzkumníkem dochází i k vytvoření exploitu a k aktivnímu zneužívání dané zranitelnosti, což nakonec vede ke zveřejnění zranitelnosti a následnému uvolnění záplaty. Tento stav provází většinu zero day útoků.
4. Po objevení zranitelnosti dochází k její exploitaci, je uvolněna záplata a zveřejněna zranitelnost. Spíš teoretický stav, ale nelze vyloučit.
5. Je nasazena záplata na blíže neurčenou zranitelnost, která je později zveřejněna a objeví se i exploit. Spíš teoretický stav, ale nelze vyloučit.

6. Je nasazena záplata a na blíže neurčenou zranitelnost, a později se objeví exploit a je zveřejněna zranitelnost.

Obvyklý, resp. bezpečnostní komunitou očekávaný a žádoucí stav je, že v okamžiku, kdy bezpečnostní výzkumník najde zranitelnost, tak ji nahlásí vývojáři daného produktu a ten uvolní odpovídající záplatu. Současně s tím zveřejní i základní informace o dané zranitelnosti.

Ne každý bezpečnostní výzkumník je však čestný a tak se může stát, že příslušnou zranitelnost včetně exploitu prodá firmě jako je např. Revuln[1] nebo Zerodium,[2] specializující se na jejich nákup a platící za ně až několik miliónů USD, vizte *Příloha A – odměna za zranitelnosti na desktopech, serverech a mobilech*.

Je nasnadě, že tyto zranitelnosti jsou dále zneužívány k cíleným APT útokům a odprodávány ve formě nástrojů pro sledování[3] dalším společnostem jako je např. HackingTeam,[4] který pak svůj nástroj RCS prodával dál, např. i PČR, jak rovněž uvádí Malý, který tento nástroj i analyzoval.

Kromě toho může nastat situace, kdy autor produktu, který danou zranitelností trpí, nemá zájem ji odstranit, vůbec nereaguje anebo z pohledu výzkumníka reaguje příliš pomalu a ten se rozhodne informace o dané zranitelnosti zveřejnit.

Zde existuje v rámci bezpečnostní komunity spor ohledně toho, zda by se měly informace o zranitelnostech zveřejňovat či nikoliv, přičemž oba tábory jsou přibližně stejně početné. To ostatně vyplývá i z ankety realizované mezi bezpečnostními profesionály v ČR.[5]

Existuje zde ne nepodstatné riziko, že informace týkající se dané zranitelnosti povedou spíš ke vzniku exploitu a jejího aktivního zneužívání, či dokonce jeho enormního nárůstu,[6] než aby přispěly k rychlejšímu uvolnění záplaty nebo virové signatury a ochraně uživatelů daného produktu, který zranitelností trpí.

Je tomu tak především proto, že drtivá většina uživatelů jakéhokoliv produktu informace o zranitelnostech nesleduje, a i kdyby ano, tak jej kvůli zranitelnosti nepřestane používat a nedokáže ani přijmout vhodná bezpečnostní opatření, která by

---

[1] REVULN. REVULN - Hong Kong, 2019 May 15-16 [online]. [vid. 18. únor 2019]. Získáno z: https://revuln.com

[2] ZERODIUM - The Leading Exploit Acquisition Platform [online]. [vid. 17. únor 2019]. Získáno z: http://zerodium.com/

[3] MALÝ, Robert. Kauza Hacking Team, aneb jak funguje Remote Control System - CleverAndSmart [online]. 22. červenec 2015 [vid. 18. únor 2019]. Získáno z: https://www.cleverandsmart.cz/kauza-hacking-team-aneb-jak-funguje-remote-control-system/

[4] HackingTeam [online]. [vid. 18. únor 2019]. Získáno z: http://www.hackingteam.it/

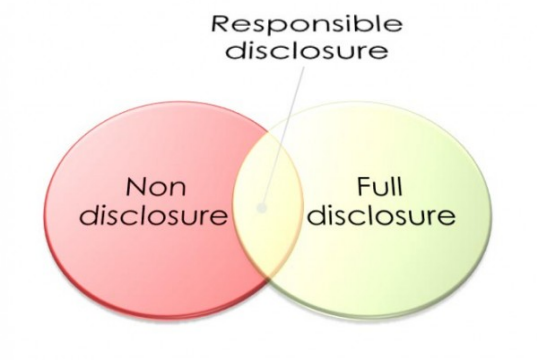
[5] ČERMÁK, Miroslav. Měly by se informace o zranitelnostech zveřejňovat? *CleverAndSmart* [online]. 21. květen 2013 [vid. 18. únor 2019]. Získáno z: https://www.cleverandsmart.cz/mely-by-se-informace-o-zranitelnostech-zverejnovat/

[6] BILGE, Leyla a Tudor DUMITRAS. Before we knew it: an empirical study of zero-day attacks in the real world. In: *the 2012 ACM conference*: *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* [online]. Raleigh, North Carolina, USA: ACM Press, 2012, s. 833 [vid. 18. únor 2019]. ISBN 978-1-4503-1651-4. Získáno z: doi:10.1145/2382196.2382284

zabránila případnému útočníkovi ve zneužití dané zranitelnosti. Jednoduše proto, že nedisponuje takovými znalostmi a dovednostmi, aby toho byla schopna.

Řešením je tzv. odpovědné zveřejňování (responsible disclosure) informací o zranitelnostech, *Obrázek 3 – Non-Full-Responsible disclosure*, kdy je zranitelnosti přiděleno CVE-ID, uvedeno CWE ID je zaevidována v NVD, kde je následně doplněn stručný popis a hodnocení dle CVSSv3. Tak mohou provozovatelé systému na zranitelnost reagovat a útočník nezískává informace potřebné ke snadnému vytvoření exploitu.

Obrázek 3 – Non-Full-Responsible disclosure



Zdroj: vlastní zpracování

Pokud je zranitelnost zveřejněna, tak je jí zpravidla přiděleno nějaké ID, zpravidla dle Common Vulnerabilities and Exposures, zkr. CVE[1] ve tvaru CVE-YYYY-NNNN, kde YYYY je rok a NNNN je pořadové číslo zranitelnosti v daném roce.

Detailní popis této zranitelnosti pak lze dohledat v National Vulnerability Database, zkr. NVD, kde se pak zpravidla nachází i odkaz na hodnocení této zranitelnosti dle všeobecně nejuznávanější metodiky pro hodnocení zranitelností CVSS organizace First, která se v době psaní této práce nachází ve verzi 3 a míru zranitelnosti hodnotí na základě několika faktorů a dále pak související slabina dle metodiky CWE.

Hodnocení zranitelností

V současné době se pro hodnocení zranitelností paralelně s CVSSv3 ve stále mnoha bezpečnostních řešeních a reportech používá i hodnocení zranitelností dle CVSSv2, a vzhledem k tomu, že tyto verze generují při hodnocení stejné zranitelnosti rozdílné výsledky, je vždy nanejvýš žádoucí uvést, jaká verze byla pro hodnocení použita.

Cílem organizace First bylo představit veřejnosti takovou metodiku hodnocení, která by zabránila nafukování jednotlivých zranitelností do obrovských rozměrů a dělání z komára velblouda, v originále “make mountains out of mole hills”. Většina bezpečnostních řešení, pokud uvádí závažnost zranitelnosti, tak zpravidla tzv. base score.

[1] CVE - CVE ID Syntax Change (Archived) [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/cve/identifiers/syntaxchange.html

Base Score

CVSSv2 používá ke stanovení úrovně zranitelnosti tzv. základního skóre (Base Score, zkr. BS) následujících 6 faktorů (první 3 fakory představuji tzv. Exploitability Metrics a další 3 pak Impact Metrics):

- **Access Vector (AV) -** zde se ptáme, odkud může být veden útok. A možnosti jsou: z internetu (network, zkr. N), ze sítě, kde se nachází systém trpící danou zranitelností (adjacent network, zkr. A) nebo útočník musí mít fyzický přístup k danému systému (local, zkr, L).
- **Access Complexity (AC)** - ke zneužití dané zranitelnosti již nemusí být splněny žádné podmínky, není potřeba žádná součinnost (low, zkr. L), je nutné mít určité informace o systému, je potřeba minimální součinnost ze strany oběti, jako je třeba kliknutí na odkaz (medium, zkr. M), útok je možné realizovat jen za určitých podmínek, na určité konfiguraci a je nutné, aby oběť provedla několik kroků (high, zkr. H).
- **Authentication** (Au) - Ke zneužití zranitelnosti není nutný účet v systému (none, zkr. N), je nutné se přihlásit (single, zkr. S), je nutné se přihlásit do systému i do aplikace (multiple, zkr. M).
- **Confidentiality impact (C)** - zde se ptáme, zda zneužitím zranitelnosti dojde k získání citlivých informací, a to všech dat, která se nacházejí v paměti nebo na disku (complete, zkr. C), nebo jen části z nich (partial, zkr. P) anebo vůbec žádných (none, zkr. N).
- **Integrity impact** (I) - zde se ptáme, zda zneužitím zranitelnosti dojde ke znehodnocení všech dat, která se nacházejí v paměti nebo na disku (complete, zkr. C), nebo jen části z nich (partial, zkr. P) anebo vůbec žádných (none, zkr. N).
- **Availability impact (A)** - zde se ptáme, zda zneužitím zranitelnosti dojde k znepřístupnění dat nebo služby (complete, zkr. C), anebo jen k částečnému omezení funkčnosti a dostupnosti dat (partial, zkr. P) anebo to nemá vůbec žádných dopad (none, zkr. N).

CVSSv3 používá ke stanovení úrovně zranitelnosti tzv. základního skóre (Base Score, zkr. BS) následujících 8 otázek (prvních 5 faktorů představuje tzv. Exploitability Metrics a další 3 pak Impact Metrics):

- **Attack Vector** (AV) rozlišuje, zda je možné útok realizovat z internetu (Network, zkr. N), z místní sítě ze stejného subnetu (Adjacent, zkr. A), lokálně (Local, zkr. L), anebo zda je nutné mít i fyzický přístup k danému zařízení (Physical, zkr. P). V okamžiku, kdy je možné vést útok přes internet, tak je zde větší množství útočníků, větší anonymita a nižší šance na odhalení útočníka a tudíž se zneužití dané zranitelnosti stává mnohem pravděpodobnější, než když je nutné k danému zařízení získat fyzický přístup.
- **Attack Complexity** (AC) může nabývat jen dvou hodnot a to (Low, zkr. L), kdy k realizaci útoku nemusí být splněny žádné podmínky nebo (High, zkr. H), kdy naopak musí být splněny určité podmínky. Je zřejmé, že v okamžiku, kdy je možno útok realizovat prakticky kdykoliv a není k tomu nutné splnit žádné podmínky,

tak je pravděpodobnost zneužití takové zranitelností mnohem vyšší, než když je ji možno zneužít jen při splnění určitých podmínek.

- **User Interaction** (UI) může nabývat dvou hodnot, a to (None, zkr. N), kdy žádná interakce ze strany oběti není k realizaci útoku nutná anebo (Required, zkr. R), kdy jak již sama hodnota napovídá, je nějak interakce ze strany oběti vyžadována. Závažnost zranitelnosti je vyšší v okamžiku, kdy žádná interakce ze strany uživatele není nutná a zneužití dané zranitelnosti je tak zcela nezávislé na vůli uživatele a jeho bezpečnostním povědomí.
- **Privileges Required** (PR) může nabývat třech hodnot. (None, zkr. N), kdy útočník nemusí disponovat žádným účtem v systému, (Low, zkr. L), kdy má útočník v systému nějaký účet s omezenými právy a (High, zkr. H), kdy má v systému účet se silnými právy. Závažnost zranitelnosti je vyšší v okamžiku, kdy útočník žádnými privilegii v systému disponovat nemusí, v takovém případě je značně ztížena identifikace uživatele a pravděpodobnost zneužitá dané zranitelnosti roste.
- **Scope** (S) bere v úvahu tu skutečnost, že byť se zranitelnost může nacházet v jedné komponentě, tak úspěšný útok může mít dopad na zcela jinou komponentu. Scope tak může nabývat dvou hodnot, nezměněn (Unchanged, zkr. U) zranitelnost i dopad se týká stejné komponenty a změněn (Changed, zkr. C), kdy zneužití zranitelnosti má dopad na jinou komponentu.
- **Impact Metrics** se zabývá hodnocením toho, k jakému narušení bezpečnosti došlo, zda se týká důvěrnosti (Confidentiality, zkr. C), integrity (Integrity, zkr. I) a dostupnosti (Availability, zkr. A) a jakého rozsahu dané narušení je, zda žádné (none, zkr. N) nízké, (low, zkr. L) nebo vysoké (high, zkr. H). Je zřejmé, že závažnost dané zranitelnosti bude tím vyšší, čím vyšší bude onen dopad z jejího zneužití.
- **Confidentiality impact (C)** - zde se ptáme, zda zneužití zranitelnosti může vést k získání citlivých informací, a zda útočník má kontrolu nad tím, jaké informace může získat (High, zkr. H) anebo ne (Low, zkr. L), anebo nemá možnost přistoupit k žádným datům (none, zkr. N)
- **Integrity impact** (I) - zde se ptáme, zda zneužití zranitelnosti může vést ke změně dat, a zda mám nad onou modifikací útočník plnou kontrolu (High, zkr. H) či nikoliv (Low, zkr. L) anebo nemůže provést žádnou neautorizovanou modifikaci (none, zkr. N).
- **Availability impact (A)** - zde se ptáme, zda zneužití zranitelnosti může vést částečné (Low, zkr. L) anebo úplné nedostupnosti (High, zkr. H) systému anebo nemůže vůbec ohrozit dostupnost daného systému (none, zkr. N).

Ze srovnání CVSSv2 a CVSSv3 vyplývají následující podstatné skutečnosti:

- **Access vector** byl přejmenován na Attack vector, avšak nadále platí, že z čím větší vzdálenosti je možné vést útok, tím závažnější je daná zranitelnost. Nově se rozlišuje, zda je možné útok realizovat jen díky možnosti se přihlásit lokálně do daného systému (Local), anebo zda je nutné mít i fyzický přístup k danému zařízení (Physical).
- **Access complexity** faktor byl de facto rozdělen na faktory dva a to Attack Complexity a User Interaction.

- **User Interaction** je zcela nový faktor, ale de facto se jedná o jeho vyčlenění z Access Complexity.
- **Privileges Required** je též zcela nový faktor, ale v zásadě vznikl přejmenováním Authentication, nicméně částečně došlo i k posunu významu.
- **Scope** je zcela nový faktorem, který bere v úvahu tu skutečnost, že byť se zranitelnost může nacházet v jedné komponentě, tak úspěšný útok může mít dopad na zcela jinou komponentu.
- **Impact Metrics** prošly rovněž změnou, neboť došlo v podstatě k rozšíření možností a to ze dvou na tři, kdy u důvěrnosti, integrity a dostupnosti byly možnosti Partial a Full nahrazeny Low, Medium a High.

Tyto změny vedly ve výsledku k tomu, že stejná zranitelnost hodnocená stejným způsobem dosahuje v CVSSv2 a CVSSv3 rozdílného skóre. Ověřit to lze poměrně snadno pomocí on-line kalkulátoru CVSSv2[1] a CVSSv3.[2]

Nejvíce se pak liší Exploitability Subscore (zneužitelnost) a Impact Subscore (dopad) vstupující do výpočtu Base Score (základní skóre), tedy toho, které je u každé zranitelnosti běžně uváděno.

Exploitable Subscore může ve CVSSv2 nabývat hodnot 1,2 až 10 a v CVSSv3 pak 0,1 až 3,9. Impact Subscore může ve verzi CVSSv2 nabývat hodnot 0 až 10 a v CVSSv3 pak 0 až 6. Exploitable Subscore a Impact Subscore v CVSSv2 a CVSSv3 jsou tak vzájemně neporovnatelné. Na první pohled dává hodnocení v CVSSv2 větší smysl. Nicméně vzhledem k tomu, že s Exploitable Subscore a Impact Subscore téměř nikdo nepracuje, tak to není až zásadní nedostatek.

Dále je třeba se věnovat rozdílnému hodnocení AV (vektor útoku), který v CVSSv3 používá oproti CVSSv2 čtyři stupně hodnocení namísto třech, kdy vektor útoku Local (místní), tak jak ho vnímá CVSSv3, není totéž co v CVSSv2, neboť Local ve CVSSv2 odpovídá Physical (fyzický) v CVSSv3, kdy je skutečně nutné disponovat fyzickým přístupem k zařízení.

Temporal Score

Vzhledem k tomu, že závažnost zranitelnosti ještě ovlivňuje faktor času, tak je možné její hodnotu ještě upravit na základě další sady otázek určující tzv. Temporal Score, zkr TS, tedy dočasné, a to proto, že se skutečně v čase mění. Vzhledem k jeho nestálosti se nikde neviduje a má smysl se jím zabývat snad jen v okamžiku hodnocení dané zranitelnosti. CVSSv2 i CVSSv3 hodnotí při stanovení temporal skóre následující faktory:

- **Exploitability** (E) – pokud je k dispozici malware, který se již šíří (high, zkr. H), existuje jen exploit (functional, zkr. F), bylo zmíněno, že se někomu podařilo zranitelnosti zneužít (proof-of-concept, zkr. POC), nebo byla zranitelnost popsána

[1] NVD - CVSS v2 Calculator [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
[2] NVD - CVSS v3 Calculator [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

jen v teoretické rovině (unproven, zkr. U). Nedefinováno (Not Defined, zkr. ND) znamená, že tento faktor nebude vstupovat do výpočtu.

- **Remediation Level** (RL) - Momentálně neexistuje žádné řešení pro snížení zranitelnosti (unavailable), je k dispozici neoficiální řešení (workaround), je k dispozici oficiální dočasný fix, workaround od vendora (Temporary fix), je k dispozici kompletní řešení, patch od vendora (official fix). Pokud zvolíte Not Defined, tak nebude tento faktor vstupovat do výpočtu.
- **Report Confidence** (RC) - Zranitelnost byla oficiálně potvrzena vendorem (confirmed), zranitelnost byla potvrzena ostatnímu firmami (uncorroborated), o zranitelnosti informuje jen jeden zdroj, podsvětí a objevují se různé spekulace a protichůdné názory (uncomfirmed). Pokud zvolíte Not Defined, tak nebude tento faktor vstupovat do výpočtu.

Environmental Score

Kromě faktoru času vstupuje do hodnocení závažnosti zranitelnosti i prostředí, ve kterém je daný systém provozován, komu a k čemu slouží, a jaký by mohl vzniknout následek z narušení bezpečnosti. K zohlednění této skutečnosti slouží sada otázek tzv. Environmental Score, zkr. ES, které se rovněž nikde neobjevuje, a neeviduje, protože slouží čistě jen manažerovi kybernetické bezpečnosti k přehodnocení dané zranitelnosti a stanovení priority řešení v případě, že by více zranitelností dosáhlo stejného base score a temporal score, kdy je možné AV, AC, PR, UI, S, C, I, A, CR, IR a AR předefinovat a tím zjistit, jak závažná je daná zranitelnost za aktuálních podmínek pro danou organizaci.

Závažnost zranitelnosti může nabývat hodnot z intervalu <0,10>, přičemž pro jejich zvládání v CVSSv2 pracuje se těmito 3 stupni zatímco CVSSv3 pak s 5 resp. 4 stupni. Tuto skutečnost lze přehledně zachytit v *Tabulka 3 – srovnání hodnocení CVSSv2 a* CVSSv3.

Tabulka 3 – srovnání hodnocení CVSSv2 a CVSSv3

CVSSv2		**CVSSv3**	
interval	popis	interval	popis
0,0 – 3,9	nízká (low)	0,0 – 3,9	nízká (low)
4,0 – 6,9	střední (medium)	4,0 – 6,9	střední (medium)
7,0 – 10,0	vysoká (high)	7,0 – 8,9	vysoká (high)
-	-	9,0 – 10,0	kritická (critical)

Zdroj: vlastní zpracování

Z *Tabulka 3 – srovnání hodnocení CVSSv2 a CVSSv3* vyplývá, že došlo k rozdělení intervalu <7,10>, tedy zranitelností v CVSSv2 označených jako vysoké na vysoké <7,9) a kritické <9,10> v CVSSv3, což umožňuje lepší prioritizaci zranitelností.

Co z výše uvedeného vyplývá? Že jen identifikovat a počítat zranitelnosti nestačí, ale že je nutné exaktně hodnotit i jejich závažnost v konkrétním prostředí a tedy, že zranitelnost, která je pro jednu organizaci naprosto kritická, tak pro druhou organizaci být kritická vůbec nemusí, a proto je na místě řízení zranitelností.

Řízení zranitelností

Řízení zranitelností je opakující se činnost skládající se z několika fází, zpravidla identifikace, vyhodnocení, mitigace a kontroly.[1] Manažer kybernetické bezpečnosti může pro identifikaci zranitelností použít automatické skenery,[2] ty však neprovádějí nějakou sofistikovanou heuristickou analýzu, ani nepracují na principu umělé inteligence, nýbrž jen jednoduše využívají databáze zranitelností, jakými je dnes asi nejznámější a veřejně dostupná Common Vulnerabilities and Exposures databáze, zkr. CVE[3] a s ní pak synchronizovaná National Vulnerability Database, zkr. NVD[4] a rovněž pak i komerční databáze VulnDB,[5] ve kterých se nacházejí všechny doposud objevené resp. zveřejněné zranitelnosti.

A v okamžiku, kdy tyto skenery provádějící sken sítě,[6] nějaký SW, který danou zranitelností trpí, ve své databázi najdou, tak i uvedou, jaká je závažnost dané zranitelnosti dle Common Vulnerability Scoring System, zkr. CVSS[7] a případně jakého typu daná zranitelnost je, resp. o jakou se jedná slabinu dle Common Weaknesses Enumeration, zkr. CWE.[8] Některá řešení pak navíc nabídnou i odkaz na záplatu nebo workaround, který danou zranitelnost řeší.

Celé řízení technických zranitelností je pak v zásadě postaveno jen na včasné detekci veřejně známé zranitelnosti v konkrétním produktu a nasazení patche anebo workaroundu. A to může být mnohdy zásadní problém, nehledě na to, že zde jsou i další úskalí, o kterých se běžně v mainstreamových médiích nemluví a ani odborné literatura se tomuto problému dostatečně nevěnuje.

V některých organizacích jsou pak navíc na počtu zranitelností v jednotlivých provozovaných systémech a době potřebné k jejich odstranění postavené i nejrůznější metriky sledující celkový počet zranitelností o určité výši a daného typu a sledování trendů, tedy jestli se jejich počet zvyšuje, klesá, je stabilní, a jak dlouho trvá, než jsou odstraněny, ale tím už se zabývá patch management, který s vulnerability

[1] FOREMAN, Park. *Vulnerability management* [online]. Boca Raton, Fla.: Auerbach Publications, 2010 [vid. 19. únor 2019]. ISBN 978-1-4398-0151-2. Získáno z: http://www.crcnetbase.com/isbn/9781439801505

[2] QUALYS. *Vulnerability management for dummies*. Chichester: John Wiley & Sons, 2011. ISBN 978-0-470-69457-2.

[3] CVE - Common Vulnerabilities and Exposures (CVE) [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/index.html

[4] NVD - Home [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/

[5] VulnDB [online]. [vid. 18. únor 2019]. Získáno z: https://vulndb.cyberriskanalytics.com/

[6] MANZUIK, Steve, André GOLD a Chris GATFORD. *Network security assessment from vulnerability to patch*. 2007. ISBN 978-1-4294-5379-0.

[7] Common Vulnerability Scoring System SIG. *FIRST — Forum of Incident Response and Security Teams* [online]. [vid. 18. únor 2019]. Získáno z: https://www.first.org/cvss

[8] CWE - Common Weakness Enumeration [online]. [vid. 18. únor 2019]. Získáno z: https://cwe.mitre.org/

managementem velice úzce souvisí, ale ve větších organizacích ho vykonává zcela jiný tým, než který se věnuje identifikaci zranitelností a jejich analýze.[1]

Problém je, že v okamžiku, kdy se objeví větší počet zranitelností, tak někdo musí stanovit, kterým zranitelnostem je třeba se věnovat jako prvním, protože zdroje organizace jsou zpravidla omezené a nelze tak nasadit všechny záplaty najednou, nehledě na to, že záplaty je třeba nejprve důkladně otestovat, neboť zde vždy volíme mezi dvěma riziky.

Rizikem, že do té doby, než se záplata nasadí a otestuje v neprodukčním prostředí, tak že dané zranitelnosti někdo zneužije, anebo že když se záplata bez nějakého důkladného testování nasadí ihned, tak že to povede k úplnému nebo částečnému omezení dostupnosti daného systému. Zranitelnosti je nutné vždy posuzovat v kontextu cílů organizace.[2]

Na tomto místě je třeba uvést, že aby se daná zranitelnost dostala do databáze zranitelností, tak ji musí nejprve někdo najít a v případě CVE/NVD i nahlásit prostřednictvím CVE Numbering Authority, zkr. CNA a teprve ta ji může, ale také nemusí do DB přidat.[3] Možná i proto se objevují názory, že CVE/NVD neobsahuje všechny zranitelnosti, a že komerční VulnDB je lepší.

Zde je však nutné uvést, že VulnDB je postavena na Open Source Vulnerability Database, zkr. OSVDB. Ta vznikla v roce 2002, veřejnosti byla poprvé představena Jakem Kouhnsem v roce 2004, aby skončila po více jak deseti letech provozu v roce 2016, kdy bylo jako důvod ukončení činnosti uvedeno, že je to především proto, že byť měla sloužit jen pro nekomerční využití, a určitá skupina firem informace z ní vytěžovala a poskytovala dál za úplatu, tak se zároveň nenašel nikdo, kdo by měl zájem tuto aktivitu finančně dál podporovat.[4]

Je zajímavé, že navzdory těmto skutečnostem byla již v roce 2011 založena společnost Risk Based Security týmž Jakem Kouhnsem, která později začala, nabízet přístup k databázi nazvané VulnDB za úplatu. Je nasnadě, že následně došlo ke ztrátě podpory ze strany bezpečnostní komunity, která do OSVDB do té doby přispívala nezištně a v dobré víře, že budou moci recipročně a bezúplatně využívat informace o zranitelnostech do této DB vložené i ostatními členy komunity. Je otázka, zdali již od počátku nebylo plánováno zpoplatnění této DB a její zpřístupnění veřejnosti nemělo sloužit jen k jejímu vybudování a získání odběratelů těchto informací.

V odborných kruzích se vedou diskuse, zda je pravda, že VulnDB obsahuje více zranitelností než CVE. A Risk Based Security se v tomto směru nebojí jít ani do u nás v ČR zakázané srovnávací reklamy, kdy porovnává počet zranitelností v jejich VulnDB

---

[1] GIUFFRIDA, Cristiano, Sébastien BARDIN a Gregory BLANC. *Detection of intrusions and Malware, and vulnerability assessment*. New York, NY: Springer Berlin Heidelberg, 2018. ISBN 978-3-319-93410-5.

[2] PELTIER, THOMAS R. *Managing a network vulnerability assessment.* Place of publication not identified: CRC Press, 2017. ISBN 978-1-138-43688-6.

[3] CVE - Request CVE IDs [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/cve/request_id.html

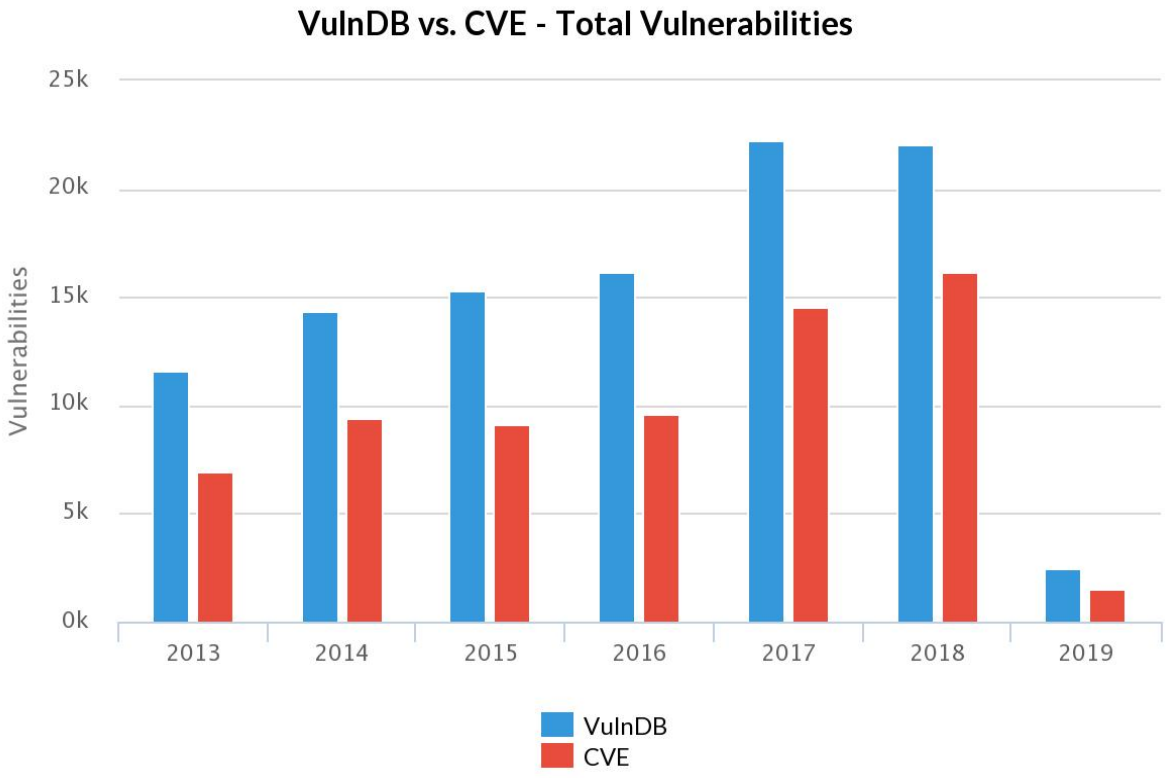
[4] OSVDB: FIN | OSVDB [online]. [vid. 18. únor 2019]. Získáno z: https://blog.osvdb.org/2016/04/05/osvdb-fin/

databázi s počtem zranitelností uvedených ve veřejně dostupné CVE/NVD databázi.[1] Risk Based Security mapuje zranitelnosti v jejich VulnDB na zranitelnosti uvedené v CVE a tvrdí, že z tohoto mapování vyplývá, že v jejich VulnDB databázi je až o několik desítek tisíc zranitelností více.

Je však nutné si uvědomit, že tento počet je kumulativní, tj. že se jedná o zranitelnosti odhalené od roku 2013 do současnosti a tudíž, že mnohé z nich již byly dávno odstraněny a prakticky jich není možné zneužít. To však nic nemění na skutečnosti, že VulnDB eviduje až o několik tisíc zranitelností více než CVE/NVD databáze. Není však zřejmé, o jaké zranitelnosti se jedná, tedy v jakých produktech se nachází a jaká je jejich závažnost.

Dalo by se předpokládat, že pokud v CVE/NVD jsou uvedeny zranitelnosti v nejpoužívanějších produktech, tak není moc pravděpodobné, že by se ve VulnDB našly zranitelnosti, které se těchto produktů týkají, daleko pravděpodobnější je, že se v ní nachází zranitelnosti ve spíše méně používaných produktech, anebo ty, kterým z nějakého důvodu nebylo přiděleno CVE-ID. Tomu by odpovídal i podobný průběh křivky na *Obrázek 4 - VulnDB vs. CVE*, naznačující, že zde zcela jistě bude určitá korelace mezi počtem zranitelnosti v CVE/NVD a VulnDB.

Obrázek 4 - VulnDB vs. CVE



Zdroj: https://vulndb.cyberriskanalytics.com/

[1] VulnDB [online]. [vid. 18. únor 2019]. Získáno z: https://vulndb.cyberriskanalytics.com/

Risk Based Security však ve svém reportu[1] uvádí, že např. v roce 2017 publikovali 6295 zranitelností, které nebyly uvedeny v CVE/NVD databázi. A že cca 44 % z nich dosáhlo skóre mezi 7,0 až 10 a téměř 20 % pak 9 až 10, což představuje kritickou zranitelnost. Pokud jde o samotné produkty, tak uvádí, že se jednalo např. i o zranitelnosti v prohlížeči Chrome, ke kterým byl k dispozici i exploit a téměř 70 % zranitelností spočívalo v nedostatečné validaci vstupu.

Risk Based Security rozporuje přístup CVE/NVD k počítání zranitelností a upozorňuje na 10.000 CVE, které jsou rezervovány[2] již několik let, a dále pak na nafukování počtu zranitelností ze strany některých organizací (neuvádějí kterých, ale nejspíš narážejí na CVE/NVD) spravujících databáze zranitelností, a které započítávají některé zranitelností vícekrát s tím, že oni sami počítají zranitelnost např. v OpenSSL knihovně využívané v mnoha produktech, jen jednou. A konečně na dlouhou prodlevu mezi oznámením zranitelnosti a jejím začleněním do CVE/NVD v některých případech až po více jak 30 dnech.

Ověření všech tvrzení a kvality VulnDB databáze by vyžadovalo další hlubší analýzu a k té by bylo nutné získat přístup k samotné DB, který je zpoplatněn. Dále proto bude v rámci této práce využíváno informací o zranitelnostech, které jsou uvedeny v bezplatné CVE/NVD databázi.

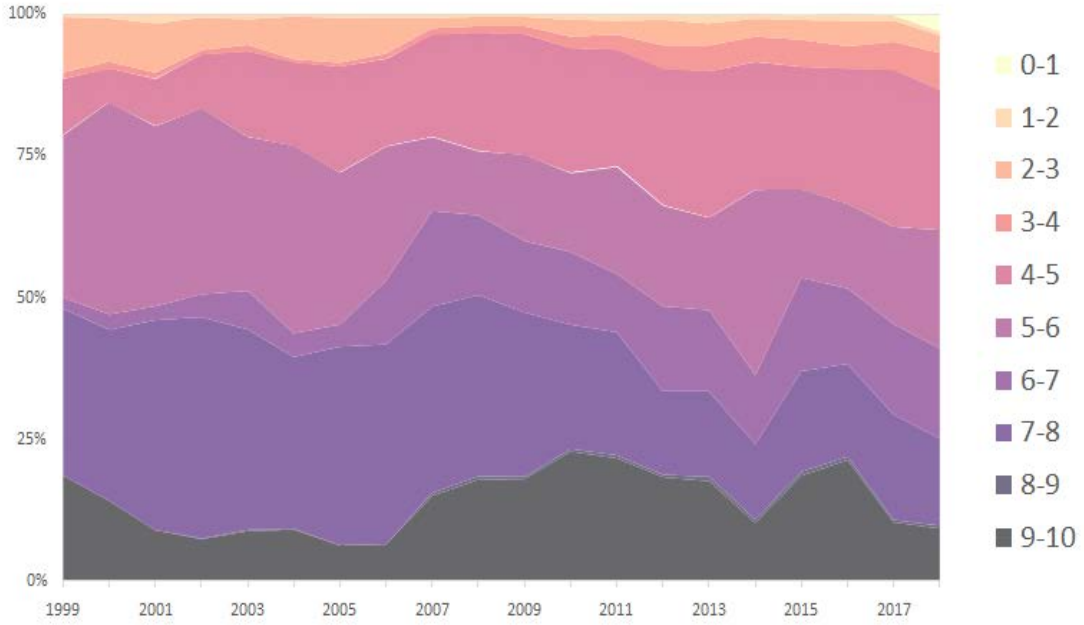
Vzhledem k tomu, že přítomnost zranitelnosti v systému je pro hodnocení možnosti jeho kompromitace klíčová, je nutné provést analýzu jednotlivých zranitelností. Jako zdrojová data byla použita databáze zranitelností CVE/NVD, kde jsou všechny hlášené zranitelnosti evidovány.

Vzhledem k tomu, že databáze zranitelností čítá více jako 100.000 záznamů a počet těchto záznamů roste, je v tomto článku uvedena jen matice zachycující počet CVE se stejným CVSS skóre v jednotlivých letech. Tato data pak lze vizualizovat např. tak, jak je uvedeno na *Obrázek 5 - relativní četnost CVE v letech*, z kterého vyplývá, že přestože v posledních dvou dekádách nedošlo k nějakým dramatickým změnám, a že zastoupení jednotlivých zranitelností hodnocených stejným stupněm závažnosti je více či méně rovnoměrné, tak je z grafu nicméně patrné, že četnost výskytu zranitelností o stejné závažnosti z počátku až tak rovnoměrná nebyla, ale v čase lze tento trend pozorovat.

[1] SECURITY, Risk Based. Request the latest Vulnerability Quick View Report from Risk Based Security [online]. [vid. 18. únor 2019]. Získáno z: https://pages.riskbasedsecurity.com/2017-q3-vulnerability-quickview-report

[2] V CVE se skutečně nacházejí zranitelnosti označené jako **RESERVED**, v NVD však již uváděny nejsou.

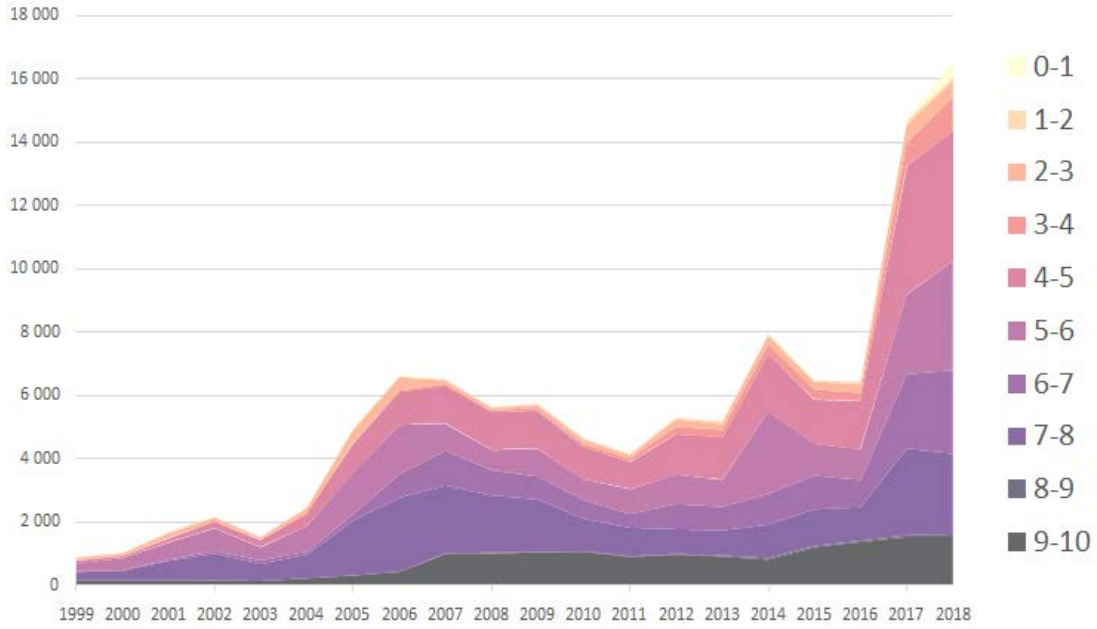
Obrázek 5 - relativní četnost CVE v letech



Zdroj: vlastní zpracování

Mnohem zajímavější přehled o vývoji zranitelností v posledních dvou dekádách však přináší *Obrázek 6 - absolutní četnost CVE v letech*. Zde je na první pohled vidět, že zatímco v prvních letech rostl počet zranitelností pozvolna, a svého lokálního maxima dosáhl v roce 2006, a v dalších deseti letech se počet nově objevených zranitelností pohyboval mezi 4 až 7 tisíci zranitelností ročně, tak v roce 2017 došlo k náhlému prudkému nárůstu zranitelností a to o více jak 100 %.

Obrázek 6 - absolutní četnost CVE v letech



Zdroj: vlastní zpracování

Na základě výše uvedené analýzy lze vyslovit jednoznačný závěr, že počet zranitelností nepochybně nadále poroste. Rovněž platí, že kromě zranitelností, kterým bylo přiděleno CVE-ID, existuje ještě velké množství zranitelností, které nebyly nahlášeny anebo byly nahlášeny, a přesto jim nebylo přiděleno CVE-ID.

Dle VulnDB se jedná až o několik desítek tisíc takových zranitelností.[1] Je samozřejmě otázka, zda uvedené číslo není nadhodnocené, ovšem z rozhovoru s namátkou oslovenými penetračními testery vyplynulo, že mnohé jimi identifikované zranitelnosti v CVE/NVD databázi nejsou uvedeny.

Výše uvedené grafy však nepřináší odpověď na otázku, které systémy nebo produkty obsahují nejvíce zranitelností a zda zde existuje nějaký trend, na základě kterého by se dalo usuzovat, jak se bude trh se zranitelnostmi dále vyvíjet a jakých zranitelností a v jakých produktech bude dále zneužíváno.

Když se podíváme např. na seznam 50 produktů s největším počtem zranitelností,[2] tak jsou zde v zásadě uvedeny všechny nejpoužívanější OS, prohlížeče a další aplikace. Lze předpokládat, že nejvíce zranitelností bude nadále hledáno a nacházeno v nejpoužívanějších OS, aplikacích, webových službách a zařízeních, neb tam bude vždy dostatečný počet potenciálních obětí, a nic nenaznačuje, že by se na tomto trendu mělo v nejbližších letech něco podstatného změnit.

A pokud zde budou navíc ještě firmy obchodující s exploity, jako že budou, tak potom musíme počítat s tím, že určité zero-day zranitelnosti budou zneužívány i po dobu několika týdnů, měsíců až let k cíleným útokům na konkrétní subjekty.

A pokud snad dojde ke zveřejnění určité zranitelnosti, tak se kód zneužívající této zranitelnosti poměrně rychle stane součástí běžných exploit kitů, což dosavadní zkušenosti rovněž potvrzují.

Z výše uvedeného lze odvodit, že **od počtu zranitelností v provozovaných systémech nelze odvodit úroveň bezpečnosti v dané organizaci, a že by hodnocení mělo být založeno na zvládnutí procesu řízení technických zranitelností**. Jaká je úroveň tohoto procesu v organizacích by mělo být předmětem dalšího výzkumu.

[1] VulnDB [online]. [vid. 18. únor 2019]. Získáno z: https://vulndb.cyberriskanalytics.com/#statistics

[2] CVSS Score Distribution For Top 50 Products By Total Number Of Distinct Vulnerabilities [online]. [vid. 18. únor 2019]. Získáno z: https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

Závěr

Při řízení zranitelností je nutné se seznámit s tím, jak životní cyklus zranitelností funguje a při hodnocení zranitelnosti se zaměřit na zjištění skutečné závažnosti dané zranitelnosti v konkrétním prostředí, neboť ta se může od zveřejněné značně lišit. Stejně tak je nutné si uvědomit, že od počtu zranitelnosti v daném produktu není možné odvíjet úroveň bezpečnosti daného produktu, protože zvýšený počet nově objevných zranitelností může být dán jen zvýšeným zájmem o daný produkt ze strany bezpečnostních výzkumníků. Vzhledem k tomu, že dosavadní trend nasvědčuje, že počet zranitelností nadále poroste, mělo by se řízení zranitelností stát nedílnou součástí řízení IT bezpečnosti a zranitelnosti by měly být včas odstraňovány, aby nemohly být zneužity. V dalším výzkumu by bylo vhodné se zaměřit na detailnější srovnání i těch databází zranitelností, ke kterým je možné se dostat jen za úplatu.

Literatura

BILGE, Leyla a Tudor DUMITRAS. Before we knew it: an empirical study of zero-day attacks in the real world. In: *the 2012 ACM conference*: *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* [online]. Raleigh, North Carolina, USA: ACM Press, 2012, s. 833 [vid. 18. únor 2019]. ISBN 978-1-4503-1651-4. Získáno z: doi:10.1145/2382196.2382284

Common Vulnerability Scoring System SIG. *FIRST — Forum of Incident Response and Security Teams* [online]. [vid. 18. únor 2019]. Získáno z: https://www.first.org/cvss

CVE - Common Vulnerabilities and Exposures (CVE) [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/index.html

CVE - CVE ID Syntax Change (Archived) [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/cve/identifiers/syntaxchange.html

CVE - Request CVE IDs [online]. [vid. 18. únor 2019]. Získáno z: https://cve.mitre.org/cve/request_id.html

CVSS Score Distribution For Top 50 Products By Total Number Of Distinct Vulnerabilities [online]. [vid. 18. únor 2019]. Získáno z: https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

CWE - Common Weakness Enumeration [online]. [vid. 18. únor 2019]. Získáno z: https://cwe.mitre.org/

ČERMÁK, Miroslav. Měly by se informace o zranitelnostech zveřejňovat? *CleverAndSmart* [online]. 21. květen 2013 [vid. 18. únor 2019]. Získáno z: https://www.cleverandsmart.cz/mely-by-se-informace-o-zranitelnostech-zverejnovat/

FOREMAN, Park. *Vulnerability management* [online]. Boca Raton, Fla.: Auerbach Publications, 2010 [vid. 19. únor 2019]. ISBN 978-1-4398-0151-2. Získáno z: http://www.crcnetbase.com/isbn/9781439801505

GIUFFRIDA, Cristiano; BARDIN, Sébastien a Gregory BLANC. *Detection of intrusions and Malware, and vulnerability assessment*. New York, NY: Springer Berlin Heidelberg, 2018. ISBN 978-3-319-93410-5.

HackingTeam [online]. [vid. 18. únor 2019]. Získáno z: http://www.hackingteam.it/

MALÝ, Robert. Kauza Hacking Team, aneb jak funguje Remote Control System - CleverAndSmart [online]. 22. červenec 2015 [vid. 18. únor 2019]. Získáno z: https://www.cleverandsmart.cz/kauza-hacking-team-aneb-jak-funguje-remote-control-system/

MANZUIK, Steve, André GOLD a Chris GATFORD. *Network security assessment from vulnerability to patch*. 2007. ISBN 978-1-4294-5379-0.

MAURO, Andrea. Performance impact of CPU bug fixes - vInfrastructure Blog [online]. 25. srpen 2018 [vid. 17. únor 2019]. Získáno z: https://vinfrastructure.it/2018/08/performance-impact-of-cpu-bug-fixes/

NVD - CVSS v2 Calculator [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

NVD - CVSS v3 Calculator [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

NVD - Home [online]. [vid. 18. únor 2019]. Získáno z: https://nvd.nist.gov/

OSVDB: FIN | OSVDB [online]. [vid. 18. únor 2019]. Získáno z: https://blog.osvdb.org/2016/04/05/osvdb-fin/

PELTIER, THOMAS R. *Managing a network vulnerability assessment.* Place of publication not identified: CRC Press, 2017. ISBN 978-1-138-43688-6.

POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

QUALYS. *Vulnerability management for dummies*. Chichester: John Wiley & Sons, 2011. ISBN 978-0-470-69457-2.

REVULN. REVULN - Hong Kong, 2019 May 15-16 [online]. [vid. 18. únor 2019]. Získáno z: https://revuln.com

SECURITY, Risk Based. Request the latest Vulnerability Quick View Report from Risk Based Security [online]. [vid. 18. únor 2019]. Získáno z: https://pages.riskbasedsecurity.com/2017-q3-vulnerability-quickview-report

VENKAT0745. A patch is preventing the system from starting [online]. 20. únor 2014 [vid. 17. únor 2019]. Získáno z: https://answers.microsoft.com/en-us/windows/forum/all/a-patch-is-preventing-the-system-from-starting/590fab3b-6efc-46f1-beb0-9bb1d1dc7b29

VulnDB [online]. [vid. 18. únor 2019]. Získáno z: https://vulndb.cyberriskanalytics.com/

VulnDB [online]. [vid. 18. únor 2019]. Získáno z: https://vulndb.cyberriskanalytics.com/#statistics

ZERODIUM - The Leading Exploit Acquisition Platform [online]. [vid. 17. únor 2019]. Získáno z: http://zerodium.com/

R E S U M É

Článek popisuje, co je to zranitelnost, jaký je životní cyklus zranitelnosti, jak zranitelnost vzniká, jaký vztah mezi zranitelností, exploitem a patchem a charakterizuje 6 možných stavů. Dále uvádí, proč je možné při hodnocení závažnosti zranitelnosti dle metodiky CVSSv2 a CVSSv3 dospět k velmi rozdílným výsledkům, a jak počet zranitelností prudce vzrostl, zatímco závažnost samotné zranitelnosti dlouhodobě směřuje k jistému rovnoměrnému rozložení. V neposlední řadě je pak uvedeno, že v rámci řízení zranitelností je nutné přistoupit k počtu zranitelností uváděných v databázích zranitelností CVE/NVD a VulnDB se značnou rezervou, neboť uvedené počty zranitelností jsou značně zavádějící.

Klíčová slova: zranitelnost, exploit, životní cyklus zranitelnosti, databáze zranitelností, řízení technických zranitelností.

S U M M A R Y

ČERMÁK, Miroslav: DIFFICULTIES OF TECHNICAL VULNERABILITY MANAGEMENT

The article describes what vulnerability is, what the life cycle of vulnerability is, how vulnerability arises, what the relationship between vulnerability, an exploit and a patch is and characterizes 6 possible states. It also presents why it is possible to achieve very different results when assessing the severity of vulnerabilities according to the CVSSv2 and CVSSv3 methodologies, and how the number of vulnerabilities has increased sharply, while the severity of vulnerability itself tends to be evenly distributed in the long run. Last but not least, it is stated that in the context of vulnerability management, it is necessary to approach the number of vulnerabilities listed in the CVE / NVD and VulnDB vulnerability databases with a considerable margin, as these numbers of vulnerabilities are substantially misleading.

Keywords: vulnerability, exploit, life cycle of vulnerability, vulnerability database, technical vulnerability management.