Hodnocení zranitelností

část I.

Nedostatky současných metod

Většina databází zranitelností dnes pracuje s hodnocením zranitelností založených na Common Vulnerability Scoring Systému (CVSS). Výrobci technologií typu Vulnerability Management k doplnění hodnocení používají proprietární metody, u kterých však není zveřejněn detailní princip jejich fungování. V článku budou detailněji rozebrány dvě nejznámější metody CVSS a OWASP Risk Rating, princip, na kterém fungují, jejich výhody a nevýhody. Druhá část bude zaměřena na návrh nové metodiky pro hodnocení zranitelností, která bude minimalizovat identifikované nedostatky.

zranitelnost hodnocení CVSS OWASP

Úvod

Ročně je objeveno obrovské množství zranitelností a sledovat můžeme i meziroční nárůst. Dle společnosti Imperva bylo v roce 2017 objeveno 14 086 zranitelností, rok 2018 zaznamenal nárůst na 17 308 a v loňském roce jsme se dostali až na číslo 20 362 nově objevených zranitelností. Celkem byl tedy zaznamenán nárůst o 44,5 % od roku 2017. [1] Když se podrobněji podíváme na rok 2018 a přes 17 tisíc objevených zranitelností, podstatná část z nich je hodnocena jako kritická nebo alespoň vysoká. Téměř 59 % z nich má dle Common Vulnerability Scoring Systému (dále jen „CVSS“) hodnocení více než 7 bodů a 15 % má hodnocení více než 9 bodů z 10bodové stupnice. [2]

Vzhledem k tomu, že v současné době je více než desetina veškerých nově objevených zranitelností hodnocena jako kritická, je na místě se zamyslet, zda je rozsáhle užívaná metodika hodnocení CVSS stále vhodná a zda její funkce prioritizace dostačuje rapidně přibývajícímu počtu nových zranitelností. Již několikrát bylo zmiňováno, že je tato metodika zastaralá a její algoritmus hodnocení závažnosti zranitelností nereflektuje některé důležité parametry. [3] Z uvedeného důvodu vznikla novější verze standardu – CVSS verze 3, která pro hodnocení zranitelností používá další parametry oproti předchozí verzi. I přes uvedení třetí verze CVSS používají hlavní výrobci nástrojů pro skenování různé další metodiky. Např. společnost Tenable v roce 2018 představila funkci Predictive Prioritization, společnost Qualys hodnotí zranitelnosti nejen na základě CVSS, ale také pomocí své vlastní metody Qualys Severity Score, společnost BeyondTrust používá mimo jiné vlastní metriku pro hodnocení kvality dostupného exploitu. Společně tyto společnosti ukazují na jeden fakt – CVSS hodnocení nedostačuje a nezohledňuje některé důležité parametry! [2], [4], [5]

Common Vulnerability Scoring System

Metodika CVSS hodnotí zranitelnosti na bodové stupnici od 0 (nejméně závažná) do 10 (nejzávažnější). Kromě samotného číselného hodnocení by se u každé zranitelnosti měl objevit také tzv. CVSS vektor, který odráží hodnoty jednotlivých metrik použitých pro výpočet konečného hodnocení. Metodika CVSS je založena na třech oblastech hodnocení závažnosti zranitelností:

- základní skóre (Base Score),
- dočasné skóre (Temporal Score),
- skóre prostředí (Environmental Score).

Každá z těchto oblastí je dále hodnocena na základě souboru metrik, které se liší v závislosti na použité verzi CVSS.

Oblasti hodnocení závažnosti zranitelností

Základní skóre

Základní skóre se dá stanovit ihned po objevení zranitelnosti. Vyjadřuje závažnost zranitelnosti samotné a nepočítá s žádnými vnějšími vlivy a okolnostmi, které běžně ovlivňují závažnost dané zranitelnosti. Obecně lze konstatovat, že závisí na dopadu na důvěrnost, dostupnost a integritu zranitelného systému, na náročnosti zneužití zranitelnosti a na vektoru útoku. Základní skóre je v průběhu času neměnné a je stejné pro všechny výskyty dané zranitelnosti nezávisle na prostředí a čase. K určení jeho hodnoty je nutné nejdříve stanovit příslušné parametry (vektor a komplexita útoku, vyžadovaná oprávnění, interakce uživatele, dopad na důvěrnost, dostupnost a integritu) a následně je možné stanovit skóre dle dále uvedených rovnic (viz Tab. 1).

Parametr základního skóre	Možné hodnoty	Číselné ohodnocení	Poznámka
Vektor útoku	Vnější síťový	0,85	-
	Vnitřní síťový	0,62	-
	Lokální	0,55	-
	Fyzický	0,20	-
Komplexita útoku	Nízká	0,77	-
	Vysoká	0,44	-
Vyžadované oprávnění	Žádné	0,85	-
	Nízké	0,62	Použije se hodnota 0,68, pokud má parametr Rozsah hodnotu Změněný
	Vysoké	0,27	Použije se hodnota 0,5, pokud má parametr Rozsah hodnotu Změněný
Interakce uživatele	Žádná	0,85	-
	Vyžadovaná	0,62	-
Dopad na důvěrnost/ dostupnost/integritu	Vysoký	0,56	-
	Nízký	0,22	-
	Žádný	0	-

Tab. 1: Číselné hodnocení parametrů základního skóre dle CVSS

Číselné ohodnocení, rovněž i hodnota parametru Rozsah jsou konstantní číselné hodnoty definované přímo metodikou CVSS.

Základní skóre je vypočteno na základě uvedené soustavy rovnic, které vyjadřují dopad a možnost exploitace. Nejprve je nezbytné stanovit hodnotu dopadu. ❶

Následující rovnice vychází z hodnoty parametru Rozsah. Pokud je Nezměněný, použije se rovnice. ❷

Je-li hodnota parametru Rozsah = Změněný, použije se rovnice. ❸

Následně je vypočtena hodnota exploitovatelnosti. ❹

Poslední rovnice pro výpočet základního skóre je opět volena ze dvou hodnot parametru Rozsah. A je vypočtena za použití funkce Roundup, která vrací nejmenší číslo s přesností na jedno desetinné místo, jež je stejně velké nebo vyšší než číslo na vstupu. ❺

❶ $Dopad = 1 - [(1 - DopadNaDůvěrnost) * (1 - DopadNaDostupnost) * (1 - DopadNaIntegritu)]$

❷ $Dopad_{RosahNezměněný} = 6{,}52 * Dopad$

❸ $Dopad_{RosahZměněný} = 7{,}52 * (Dopad - 0{,}029) - 3{,}25 * (Dopad - 0{,}02)^{15}$

❹ $Exploitovatelnost = 8{,}22 * VektorÚtoku * KomplexitaÚtoku * VyžadovanáOprávnění * InterakceUživatele$

❺ $ZákladníSkóre_{RozsahNezměněný} = Roundup\ (Minimum[(Dopad_{RozsahNezměněný} + Exploitovatelnost),\ 10]$
$ZákladníSkóre_{RozsahZměněný} = Roundup\ (Minimum[1{,}08 * (Dopad_{RozsahZměněný} + Exploitovatelnost),\ 10]$

Dočasné skóre

Na rozdíl od základního skóre se v čase mění a odráží závažnost zranitelnosti v dané době na základě kvality a dostupnosti exploitu, možnosti odstranění zranitelnosti a množství informací, které lze o zranitelnosti v dané době zjistit. Tato část skóre se nevztahuje na zranitelnost jako takovou, ale počítá s vnějšími vlivy, které mohou skóre snížit, nebo naopak zvýšit. Dočasné skóre je stejné pro všechny výskyty dané zranitelnosti. Pro výpočet dočasného skóre je nutné stanovit aktuální hodnoty parametrů: kvalita exploitu, úro-

veň nápravy a dostupné informace, které mohou nabývat tabulkou prezentovaných hodnot (viz Tab. 2).

Dočasné skóre se vypočítá z parametrů hodnocených v tomto skóre a z hodnoty základního skóre. ❻

Skóre prostředí

Skóre prostředí se skládá z parametrů, které jsou stejné jako v základním skóre, ale mají přídomek – modifikovaný, protože se vztahují na konkrétní prostředí, takže mohou nabývat jiných hodnot než u základního skóre. Číselné ohodnocení parametrů ze základního skóre a modifikovaných parametrů je však pro jednotlivé hodnoty stejné. Mimo tyto stejné parametry jsou u skóre prostředí přidány další tři, pro které jsou možné hodnoty a jejich číselné ohodnocení uvedeny v Tab. 3.

Pro výpočet skóre prostředí je nejprve vypočítán modifikovaný dopad, který vyjadřuje závislost dopadu na důvěrnost, dostupnost a integritu a požadavku na tyto tři hodnoty. ❼

Další rovnice vychází z hodnoty parametru Modifikovaný rozsah. Pokud je hodnota Nezměněný, použije se rovnice. ❽

Pokud je hodnota Změněný, použije se rovnice. ❾

Následně je vypočtena hodnota modifikované exploitovatelnosti. ❿

V posledním kroku výpočtu se opět volí ze dvou hodnot parametru Modifikovaný rozsah. Pro Hodnotu Nezměněný se zvolí následující rovnice. ⓫

Pro hodnotu Změněný se zvolí následující rovnice. ⓬

Parametr dočasného skóre	Možné hodnoty	Číselné ohodnocení
Kvalita exploitu	Není definováno	1
	Bez důkazů	0,91
	Proof-of-Concept	0,94
	Funkční	0,97
	Vysoká kvalita	1
Úroveň nápravy	Není definováno	1
	Oficiální záplata	0,95
	Dočasná záplata	0,96
	Workaround	0,97
	Nedostupná záplata	1
Dostupné informace	Není definováno	1
	Nízké	0,92
	Střední	0,96
	Detailní	1

Tab. 2: Číselné hodnocení parametrů dočasného skóre dle CVSS

Parametr dočasného skóre	Možné hodnoty	Číselné ohodnocení
Požadavek důvěrnosti/ dostupnosti/integrity	Není definováno	1
	Nízký	0,5
	Střední	1
	Vysoký	1,5

Tab. 3: Číselné hodnocení parametrů dočasného skóre dle CVSS

❻ $DočasnéSkóre = Roundup(ZákladníSkóre * KvalitaExploitu * ÚroveňNápravy * DostupnéInformace)$

❼ $$ModifikovanýDopad = Minimun\ (1 - [(1 - PožadavekDůvěrnosti * ModifikovanýDopadNaDůvěrnost) * (1 - PožadavekDostupnosti * ModifikovanýDopadNaDostupnost) * (1 - PožadavekIntegrity * ModifikovanýDopadNaIntegritu), 0,915]$$

❽ $ModifikovanýDopad_{ModifikovanýRozsahNezměněný} = 6,42 * ModifikovanýDopad$

❾ $$ModifikovanýDopad_{ModifikovanýRozsahZměněný} = 7,52 * (ModifikovanýDopad - 0,029) - 3,25 * (ModifikovanýDopad * 0,9731 - 0,02^{13})$$

❿ $$ModifikovanáExploitovatelnost = 8,22 * ModifikovanýVektorÚtoku * ModifikovanáKomplexitaÚtoku * ModifikovanáVyžadovanáOprávnění * ModifikovanáInterakceUživatele$$

⓫ $$SkóreProstředí_{ModifikovanýRozsahNezměněný} = Roundup\ (Roundup(Minimum[(ModifikovanýDopad_{ModifikovanýRozsahNezměněný} + ModifikovanáExploitovatelnost), 10] * KvalitaExploitu * ÚroveňNápravy * DostupnéInformace)$$

⓬ $$SkóreProstředí_{ModifikovanýRozsahZměněný} = Roundup\ (Roundup(Minimum[1,08 * (ModifikovanýDopad_{ModifikovanýRozsahZměněný} + ModifikovanáExploitovatelnost), 10] * KvalitaExploitu * ÚroveňNápravy * DostupnéInformace)$$

Výhody a nevýhody CVSS

Hlavní výhodou CVSS metodiky je její komplexnost, což je zároveň i její hlavní nevýhodou. [6], [7] Pokud je pro stanovení priority zranitelnosti použito poslední Environmental Score, výsledná hodnota bude velmi přesně odrážet závažnost pro dané prostředí. Bohužel je pro stanovení takového skóre nezbytné obrovské množství informací, které ve většině případů nelze zpracovat automatizovaně. Podíváme-li se na dočasné skóre, je velmi dobře navrženo. Bohužel je jeho reálné využití v současné době téměř nulové. Žádný z nástrojů pro detekci zranitelností ani sami „nálezci" zranitelností dočasné skóre příliš nepoužívají.

Nevýhodou CVSS je, že většina nástrojů pro detekci zranitelností a pro stanovení rizik počítá pouze s metrikou základního skóre. Důvodem je skutečnost, že je téměř nemožné automatizovaně, bez poskytnutí množství informací stanovit skóre prostředí. Prioritizace zranitelností je tedy ponechána na uživatelově nástroji. Pro přesné určení priority je však nutné přesně vědět, o jaký systém se jedná. Základní skóre CVSS nebere vůbec v potaz důležitost zranitelného systému, např. zda se jedná o produkční server umístěný v demilitarizované zóně, nebo o server v uzavřeném testovacím prostředí, který neobsahuje produkční data. Když se podíváme na výpočet dočasného skóre, můžeme si všimnout, že hodnota kvality exploitu se násobí základním skóre.

Kvalita exploitu ale více souvisí s dopadem na důvěrnost, dostupnost nebo integritu. [6] Pokud nejsou data, která by mohla být odcizena, může být exploit sebelepší, ale pro útočníka je daleko důležitější užitek v podobě zisku z útoku než jeho jednoduchost. A je-li narušena pouze jedna položka z důvěrnosti, dostupnosti nebo integrity, základní skóre se rapidně sníží, ačkoli pro útočníka může být stále velmi lákavé zneužít danou zranitelnost, provést útok a mít možnost např. pozměnit soubory. Stejně tak z business pohledu na systém může mít zmíněné fatální následky.

OWASP Risk Rating Methodology

Tato metodika je primárně zaměřena na zranitelnosti, které se nacházejí ve webových aplikacích. Nicméně je možné tuto metodiku použít i na hodnocení jakýchkoli dalších bezpečnostních zranitelností systémů. OWASP metodika není zdaleka tak rozšířená jako CVSS, která víceméně představuje standard v oblasti hodnocení závažnosti zranitelností. Základní myšlenkou této metodiky je vztah mezi rizikem, pravděpodobností zneužití a dopadem při zneužití zranitelnosti. Celá metodika je založena na tom, že riziko je přímo úměrné pravděpodobnosti zneužití a dopadu. Jak tedy vyplývá z uvedeného, základními oblastmi pro hodnocení závažnosti zranitelnosti dle OWASP Risk Rating Methodology jsou pravděpodobnost zneužití a dopad na systém při zneužití zranitelnosti.

Oblasti hodnocení

Stanovení pravděpodobnosti zneužití

První oblastí pro stanovení finálního rizika je pravděpodobnost zneužití dané zranitelnosti. Hodnotí se osm různých faktorů rozdělených do dvou skupin – faktory nositelů hrozby (Threat Agent Factors) a faktory zranitelnosti samotné (Vulnerability Factors). Pravděpodobnost zneužití je stanovena jako průměr hodnot jednotlivých faktorů. Faktory obou skupin jsou uvedeny v Tab. 4.

Číselným ohodnocením jednotlivých faktorů jsou konstantní číselné hodnoty, které jsou definovány přímo metodikou OWASP Risk Rating.

Skupina faktorů	Faktor	Možné hodnoty	Číselné ohodnocení
Faktory nositelů hrozby	Úroveň schopností	Žádné technické schopnosti	1
		Nízké technické schopnosti	3
		Pokročilý uživatel	5
		Síťové znalosti a programovací schopnosti	6
		Penetrační tester	9
	Motivace	Nízká nebo žádná	1
		Střední	4
		Vysoká	9
	Obtížnost zneužití zranitelnosti	Velmi vysoká	0
		Vysoká	4
		Nízká	7
		Velmi nízká	9
	Skupina nositelů hrozby	Vývojáři	2
		Systémoví administrátoři	2
		Uživatelé interní sítě	4
		Partneři	5
		Autentizovaní uživatelé	6
		Anonymní uživatelé internetu	9
Faktory zranitelnosti	Objevení zranitelnosti	Velmi obtížné	1
		Obtížné	3
		Jednoduché	7
		Pomocí automatizovaných nástrojů	9
	Exploitace	Teoretická	1
		Obtížná	3
		Jednoduchá	5
		Pomocí automatizovaných nástrojů	9
	Informace o zranitelnosti	Neznámé	1
		Tajné	4
		Známé	6
		Veřejně známé	9
	Detekce průniku	Aktivní detekce v aplikaci	1
		Logováno a kontrolováno	3
		Logováno bez kontroly	8
		Bez logování	9

Tab. 4: Číselné hodnocení OWASP faktorů pro stanovení pravděpodobnosti zneužití

Stanovení dopadu zneužití

Rovněž jako v předchozí oblasti je zde hodnoceno osm různých faktorů, které jsou rozděleny do dvou skupin – faktory technického dopadu (Technical Impact Factors) a faktory business dopadu (Business Impact Factors). [9] Zde se nepočítá s průměrem hodnot, ale pro hodnocení jsou brány buď technické, nebo business faktory, pokud jsou k dispozici. Ne vždy je možné ohodnotit dopad na business v případě zneužití zranitelnosti, proto je druhou možností použití hodnoty faktoru technického dopadu. Jednotlivé faktory z obou skupin jsou uvedeny v Tab. 5.

Stanovení celkového rizika

Pro finální stanovení hodnoty rizika je nejdříve nutné slovní ohodnocení jednotlivých číselných hodnot dle převodní Tab. 6.

Pravděpodobnost zneužití je stanovena jako průměr všech hodnot faktorů nositelů hrozby a faktorů zranitelnosti. Dopad při zneužití je stanoven jako průměr hodnot faktorů business dopadu, a pokud tyto faktory nelze ohodnotit, tak jako průměr hodnot faktorů technického dopadu. Pro určení výsledné míry rizika se vychází z následující Tab. 7.

Výhody a nevýhody OWASP Risk Rating Methodology

Výhodou této metodiky je jednoznačně její jednoduchost, která je zajištěna díky menšímu množství faktorů (parametrů), než je tomu u CVSS, a také jednoduchým principem vyhodnocení celkové míry rizika. Díky tomu je snadno použitelná různými nástroji. [10] Vzhledem k masivnímu rozšíření CVSS je však tato metodika vídána zřídka. Druhou velkou

Skupina faktorů	Faktor	Možné hodnoty	Číselné ohodnocení
Faktory technického dopadu	Ztráta důvěrnosti	Minimální množství odcizených necitlivých dat	2
		Minimální množství odcizených kritických dat	6
		Rozsáhlé množství odcizených necitlivých dat	6
		Rozsáhlé množství odcizených kritických dat	7
		Odcizení všech dat	9
	Ztráta integrity	Minimální množství lehce poškozených dat	1
		Minimální množství vážně poškozených dat	3
		Rozsáhlé množství lehce poškozených dat	5
		Rozsáhlé množství vážně poškozených dat	7
		Úplné poškození všech dat	9
	Ztráta dostupnosti	Minimální nedostupnost sekundární služby	1
		Minimální nedostupnost primární služby	5
		Rozsáhlá nedostupnost sekundární služby	5
		Rozsáhlá nedostupnost primární služby	7
		Úplná nedostupnost všech služeb	9
	Odhalení útočníka	Úplné vysledování	1
		Možné vysledování	7
		Nemožné vysledování	9
Faktory business dopadu	Finanční poškození	Menší než náklady na opravu zranitelnosti	1
		Malý vliv na roční zisk	3
		Významný vliv na roční zisk	7
		Bankrot	9
	Poškození reputace	Nízké poškození	1
		Ztráta významných zákazníků	4
		Ztráta dobrého jména	5
		Úplné poškození značky	9
	Nedodržení požadavků	Málo závažné porušení požadavků	2
		Významné porušení požadavků	5
		Velmi závažné porušení požadavků	7
	Porušení soukromí	Konkrétního jedince	3
		Stovek lidí	5
		Tisíců lidí	7
		Miliónů lidí	9

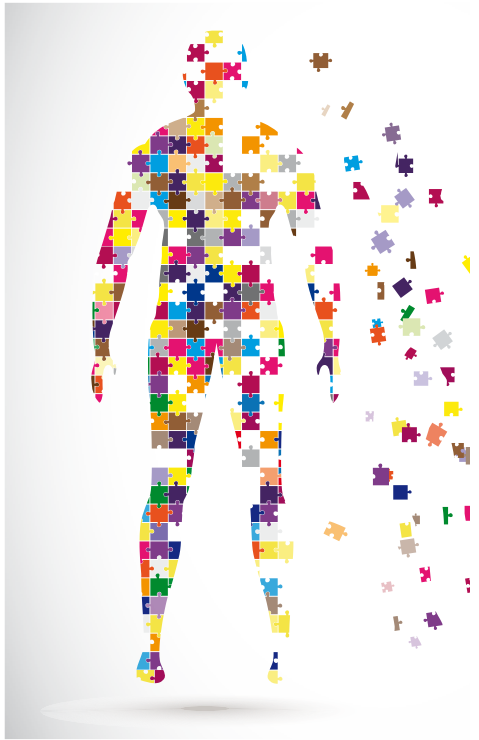
Tab. 5: Číselné hodnocení OWASP faktorů pro stanovení dopadu zneužití

Číselné ohodnocení	Slovní hodnocení
0 až 3	Nízké
3 až 6	Střední
6 až 9	Vysoké

Tab. 6: Převodní tabulka číselného ohodnocení na slovní hodnocení

		Míra rizika		
Dopad	Vysoký	Střední	Vysoká	Kritická
	Střední	Nízká	Střední	Vysoká
	Nízký	Žádná	Nízká	Střední
		Nízká	Střední	Vysoká
		Pravděpodobnost		

Tab. 7: Míra rizika dle OWASP Risk Rating



výhodou je preference business faktorů před těmi technickými. Pro každý systém v různých organizacích může ta samá zranitelnost představovat jiné riziko, je tedy vhodné ji i jinak ohodnotit. Díky tomu, že metodika OWASP preferuje business faktory před technickými, je prioritizace přesnější než např. u základního skóre CVSS. [11] Dále metodika OWASP reflektuje parametry, které CVSS buď vůbec nemá, nebo je zohledňuje v jiném než základním skóre. Jedná se např. o faktory exploitace nebo informace o zranitelnosti, které jsou obsaženy až v dočasném CVSS skóre. Dále metodika OWASP vychází z faktorů motivace útočníka a možnosti jeho odhalení. Zejména první z těchto faktorů je velmi důležitý pro prioritizaci zranitelnosti. [12]

Nevýhodou této metodiky je právě ona jednoduchost. To, co je v CVSS skóre hodnoceno pomocí čtyř parametrů (vektor útoku, komplexita útoku, úroveň oprávnění, interakce uživatele), je zde hodnoceno pouze faktory obtížnost zneužití zranitelnosti a skupina nositelů hrozby. Není zde tedy možné specifikovat do takové hloubky detailu všechny parametry pro hodnocení zranitelností, které např. CVSS metodika ve všech svých hodnoceních obsahuje.

Závěr

Každá z popsaných metodik pro stanovení závažnosti zranitelností vychází z určitého základního principu. Na základě uvedených informací je možné konstatovat, že metodika CVSS je v tomto ohledu složitější než metodika OWASP. U obou metodik je však možné shledat velkou míru nepřesnosti výsledných hodnot zranitelností. Tento fakt může mít fatální dopad na samotnou hodnotu zranitelnosti i na hodnocený systém v případě, že tato zranitelnost nebude prioritně řešena a dojde k jejímu zneužití, a to i přes aktuálnost problematiky.

Aktuálnost řešení problematiky hodnocení zranitelností je jasně podpořena jejich každoročním nárůstem v řádech tisíců. Hodnocení nově objevených zranitelností dle uvedených metodik vykazuje velkou míru nepřesnosti, tyto zranitelnosti jsou na stupnici závažnosti nadhodnocovány. Pro vlastníky aktiv je pak obtížné až přímo nemožné prioritizovat zranitelnosti vlastními silami a v akceptovatelné době zranitelnosti na systémech odstraňovat. I přes nedostatky popsaných metodik a přes aktuálnost této problematiky není hodnocení zranitelností věnována dostatečná pozornost. Na základě uvedených nedostatků bude v druhém dílu tohoto článku prezentována nová metodika pro hodnocení zranitelností, která je bude minimalizovat.

Lubomír Almer
lubomir.almer@aec.cz
David Pecl
david.pecl@aec.cz

Lubomír Almer

Bezpečnostní specialista ve společnosti AEC a.s. se zaměřením na analýzy, návrhy a implementace technologických řešení. Specializuje se především na oblast bezpečnostního monitoringu a řízení identit.

David Pecl

Bezpečnostní specialista se zaměřením na ochranu koncových stanic a na řízení zranitelností ve společnosti AEC a.s. V rámci těchto oblastí zastává také roli produktového manažera.

POUŽITÉ ZDROJE

[1] https://www.imperva.com/blog/the-state-of-vulnerabilities-in-2019/, Imperva. [online].
[2] Vulnerability Intelligence Report. Tenable [online]. Columbia, 2018, 11/18 [cit. 2019-12-08]. Dostupné z: https://static.tenable.com/translations/en/Vulnerability_Intelligence_Report-ENG.pdf.
[3] Predictive Prioritization: Data Science Lets You Focus On The 3% Of Vulnerabilities Likely To Be Exploited. Tenable [online]. Columbia, 2019, 04. 12. 2019 [cit. 2019-12-08]. Dostupné z: https://lookbook.tenable.com/predictive-prioritization/technical-whit.
[4] WALKER, Martin. Qualys Severity Score vs CVSS Scoring. Qualys. Community [online]. 2019, 11. 8. 2016 [cit. 2019-12-08]. Dostupné z: https://discussions.qualys.com/docs/DOC-5767-qualys-severity-score-vs-cvss-scoring.
[5] HABER, Morey J. Why Exploitability Matters. BeyondTrust Corporation [online]. 2019, 19. 7. 2011 [cit. 2019-12-08]. Dostupné z: https://www.beyondtrust.com/blog/entry/why-exploitability-matters.
[6] Don't Substitute CVSS for Risk: Scoring System Inflates Importance of CVE-2017-3735. McAfee [online]. United States / English, 2019, 24. 11. 2017 [cit. 2019-12-08]. Dostupné z: https://securingtomorrow.mcafee.com/mcafee-labs/dont-substitute-cvss-for-risk-.
[7] CVSS – Is 3 The Magic Number? Risk Based Security [online]. 2019, 5. 6. 2017 [cit. 2019-12-08]. Dostupné z: https://www.riskbasedsecurity.com/2017/06/05/cvss-is-3-the-magic-number/.
[8] 2007, RFC 4949. Internet Security Glossary. Version 2.
[9] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, OWASP Risk Rating Methodology. OWASP [online]. 27. 6. 2019 [cit. 2019-12-08].
[10] RAMADLAN, M. Febri. Introduction and implementation OWASP Risk Rating Management [online]. [cit. 2019-12-08]. Dostupné z: https://www.owasp.org/images/9/9c/Riskratingmanagement-170615172835.pdf.
[11] ASTAFYEU, Aliaksandr. Information Security Risk Assessment Methodologies in Vulnerability Assessment of Information Systems. 2015. Master thesis. Technical University of Denmark.
[12] IMPE, Koen Van. Simplifying Risk Management. Security Intelligence Logo [online]. 2019, 28. 3. 2017 [cit. 2019-12-08]. Dostupné z: https://securityintelligence.com/simplifying-risk-management/.
[13] Imperva. [online] https://www.imperva.com/blog/the-state-of-vulnerabilities-in-2019/.