Hodnocení zranitelností

část II.

Nedostatky současných metod

Návrh nové metody pro hodnocení zranitelností, který eliminuje nedostatky Common Vulnerability Scoring Systému a OWASP Risk Rating. Využívá jednotlivé silné stránky těchto nejpoužívanějších metod a zároveň minimalizuje jejich slabé stránky. Utváří tak komplexní metodu pro efektivní a přesné hodnocení zranitelností, které je vztažené přímo na hodnocené prostředí.

zranitelnost hodnocení CVSS OWASP

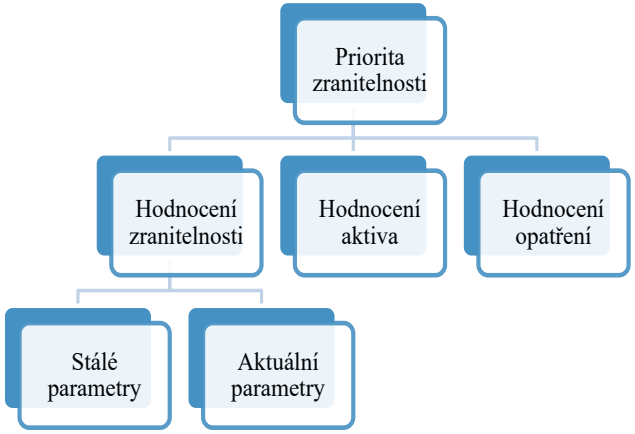
Princip metody

Metoda pro prioritizaci zranitelností vychází z principu, kdy není hodnocena pouze samotná zranitelnost, ale pro výslednou hodnotu jsou použity i informace o zranitelném systému, které mohou ve výsledku snížit nebo naopak zvýšit prioritu zranitelnosti. Dále jsou hodnoceny informace o implementovaných opatřeních, tedy ochranách, které pomáhají zajišťovat důvěrnost, dostupnost a integritu systému (CIA triáda) a ve výsledku mohou prioritu zranitelnosti snížit. Základem metody jsou tři části – hodnocení zranitelnosti, hodnocení aktiva, tj. priority systému, a implementovaná opatření. Schematicky je navržená metoda znázorněna na Obr. 1.

Hodnocení zranitelnosti

Parametry v této oblasti jsou dále rozděleny do dvou skupin, a to na stálé a aktuální parametry. Stálé parametry jsou z hlediska prioritizace v čase neměnné, oproti tomu aktuální parametry se v čase mohou měnit a znatelně ovlivňovat prioritu zranitelnosti.

Mezi stálé parametry patří dopad na CIA triádu a obtížnost zneužití, mezi aktuální patří dostupnost informací, možnosti exploitace a informace o aktivním zneužívání zranitelnosti. Hlavními parametry pro stanovení závažnosti zranitelnosti jsou bezpochyby dopady na CIA triádu. Samotná informace o dopadu na jednu z těchto tří položek však nestačí.



Obr. 1: Schéma navržené metody

Z hlediska prioritizace je nezbytné pracovat také s požadavkem na tyto tři položky. Pokud hodnocený systém nemá požadavek důvěrnosti, tj. data na něm jsou veřejná, zranitelnost s dopadem na důvěrnost pro tento systém není vůbec prioritní. Z uvedeného důvodu je nezbytné při stanovení priority počítat nejen s ohrožením CIA triády, ale také s tím, jestli existují požadavky na tuto triádu a jaké jsou. Dále mezi stále parametry patří obtížnost zneužití zranitelnosti, vyžadovaná interakce uživatele a případné oprávnění, které je k úspěšnému zneužití potřebné. Do parametru obtížnost zneužití se promítá technická náročnost exploitace dané zranitelnosti, zda je nezbytné využít řetězec zranitelností, nebo je možné rovnou zneužít hodnocenou zranitelnost, jakým způsobem zneužití probíhá a další parametry vztahující se k obtížnosti zneužití.

Mezi aktuální parametry patří dostupnost informací, tj. zda jsou dostupné technické informace o zranitelnosti, zda je popsán způsob, jak zranitelnost funguje, jakým způsobem je možné ji zneužít a další informace. Pro tento parametr je důležité, i pokud žádné informace zveřejněny nejsou a technické informace o zranitelnosti jsou utajené. [1] Druhým parametrem je exploitace, resp. možnosti její automatizace, a kvalita exploitu. Stejně jako popsaný parametr dostupnost informací je parametr exploitace převzat z metody OWASP Risk Rating. Posledním parametrem je informace o aktivním zneužívání zranitelnosti z tzv. Threat Intelligence. Společnost Gartner pojem definuje jako „databázi znalostí o existující nebo vznikající hrozbě, které jsou založeny na důkazech, včetně kontextu, mechanismu fungování hrozby, indikátorů, důsledků, a díky kterým je možné se informovaně rozhodnout o případné reakci na tuto hrozbu“. [2]

Hodnocení stálých parametrů

Dopad na důvěrnost

Vyjadřuje, jak velké množství dat může být odcizeno a jak citlivá tato data jsou. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Minimální množství odcizených necitlivých dat	0,22
Minimální množství odcizených kritických dat	0,67
Rozsáhlé množství odcizených necitlivých dat	0,67
Rozsáhlé množství odcizených kritických dat	0,78
Odcizení veškerých dat	1,00

Tab. 1: Možné hodnoty dopadu na důvěrnost

Dopad na dostupnost

Vyjadřuje, jak velké množství služeb může být vyřazeno z provozu a jak důležité tyto služby jsou. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Minimální nedostupnost sekundární služby	0,11
Minimální nedostupnost primární služby	0,56
Rozsáhlá nedostupnost sekundární služby	0,56
Rozsáhlá nedostupnost primární služby	0,78
Úplná nedostupnost všech služeb	1,00

Tab. 2: Možné hodnoty dopadu na dostupnost

Dopad na integritu

Vyjadřuje, jak velké množství dat může být poškozeno a jak rozsáhlé dané poškození může být. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Minimální množství lehce poškozených dat	0,11
Minimální množství vážně poškozených dat	0,33
Rozsáhlé množství lehce poškozených dat	0,56
Rozsáhlé množství vážně poškozených dat	0,78
Úplné poškození veškerých dat	1,00

Tab. 3: Možné hodnoty dopadu na integritu

Obtížnost zneužití

Vyjadřuje, jaké zdroje jsou nezbytné ke zneužití zranitelnosti, zda je potřebné před zneužitím dané zranitelnosti zneužít i jiné zranitelnosti (řetězec zranitelností), o jak komplexní zneužití se jedná (řetězec aktivit, které musejí být úspěšně provedeny, aby se útočník mohl pokusit o zneužití dané zranitelnosti) a další. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Velmi vysoká	0,00
Vysoká	0,44
Nízká	0,78
Velmi nízká	1,00

Tab. 4: Možné hodnoty obtížnosti zneužití

Požadovaná oprávnění

Vyjadřuje úroveň oprávnění, které musí útočník mít, než zneužije hodnocenou zranitelnost. Vychází z CVSS metody. [4]

Slovní hodnocení	Číselné ohodnocení
Žádná	1,00
Nízká	0,80
Vysoká	0,40

Tab. 5: Možné hodnoty požadovaných oprávnění

Interakce uživatele

Vyjadřuje nutnost uživatelské aktivity před nebo při zneužití. Vychází z CVSS metody. [4]

Slovní hodnocení	Číselné ohodnocení
Žádná	1,00
Vyžadována	0,40

Tab. 6: Možné hodnoty interakce uživatele

Hodnocení aktuálních parametrů

Dostupnost informací

Vyjadřuje, jaké množství informací o zranitelnosti je zveřejněno. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Není definováno	0,50
Neznámé	0,11
Tajné	0,44
Známé	0,67
Veřejně známé	1,00

Tab. 7: Možné hodnoty dostupnosti informací

Exploitace

Vyjadřuje možnost zneužití zranitelnosti pomocí automatizovaných nástrojů a kvalitu dostupných exploitů. Vychází z OWASP Risk Rating metody. [3]

Slovní hodnocení	Číselné ohodnocení
Není definováno	0,50
Teoretická	0,11
Proof-of-Concept	0,33
Jednoduchá	0,56
Pomocí automatizovaných nástrojů	1,00

Tab. 8: Možné hodnoty exploitace

Threat Intelligence

Zohledňuje aktuální zneužívání zranitelnosti zachycené monitorovacími službami Threat Intelligence.

Slovní hodnocení	Číselné ohodnocení
Není definováno	0,50
Žádná	0,00
Nízká	0,25
Střední	0,50
Vysoká	0,75
Velmi vysoká	1,00

Tab. 9: Možné hodnoty Threat Intelligence

Otázka	Slovní hodnocení	Číselné hodnocení
Jakého typu data jsou	Osobní data	0,8
	Osobní citlivá data	1
	Jiná data	0,5
Ke komu se data vztahují	Zaměstnancům společnosti	0,9
	Zákazníkům společnosti	1
	Jiným fyzickým nebo právnickým osobám	0,8
Je daný systém produkčního typu	Ano	1
	Ne	0
Je systém dostupný z internetu	Ano	1
	Ne	0

Tab. 10: Hodnotící otázky okruhu Obecné informace

Hodnocení aktiva

Pro správnou prioritizaci zranitelnosti je nezbytné vědět, o jaký zranitelný systém se jedná. Způsobů pro hodnocení důležitosti aktiva je mnoho. Každý z těchto způsobů vyžaduje značné množství informací o hodnoceném aktivu. Tyto informace je nezbytné získat od vlastníků dotčených aktiv, a to z důvodu, že tito vlastníci mají nejpřesnější informaci o tom, jaká data jsou na systémech uchovávána, k čemu systém slouží, kdo k němu má přístup a další důležité informace pro stanovení priority aktiva. Pro hodnocení aktiva byla vybrána forma dotazníkového šetření, díky kterému je možné pomocí klíčových dotazů určit důležitost dat uložených na hodnoceném systému.

Hodnoticí otázky

Uvedené otázky jsou rozděleny do dvou okruhů – obecné informace a požadavky důvěrnosti, dostupnosti a integrity (viz Tab. 10 a Tab. 11).

Hodnocení opatření

Uvedená opatření, stejně jako v předchozím případě při hodnocení aktiva, jsou hodnocena za použití dotazníku. V rámci dotazníku se zvolí, zda je dané opatření implementováno a dle zvolené odpovědi je následně určeno číselné hodnocení. Seznam opatření je možné dále rozšířit. Není hodnocena implementace a její rozsah jako takový. Z uvedeného důvodu se jedná o pouze základní hodnocení opatření, které může být dále rozšířeno či modifikováno dle potřeb hodnoceného subjektu.

Ochrana důvěrnosti

V rámci ochrany důvěrnosti je hodnoceno pět základních opatření z pohledu, zda jsou či nejsou implementována (viz Tab. 12).

Ochrana dostupnosti

Do této skupiny jsou zařazena tři opatření: mechanismus vysoké dostupnosti, zálohování a ochrana proti nedostupnosti služeb (viz Tab. 13).

Ochrana integrity

V této skupině je hodnoceno pět různých opatření, která mají vliv na zajištění integrity nebo na její ochranu (viz. Tab. 14).

Výpočet priority zranitelnosti

Parametry popisující dopad na CIA triádu zranitelného systému je pro stanovení priority žádoucí kombinovat s požadavky na tuto triádu. Pro tento účel je samotný výpočet priority zranitelnosti složen ze tří návazných fází: stanovení parametrů zranitelnosti, stanovení požadavků na CIA triádu a výpočet hodnoty zranitelnosti.

Stanovení parametrů zranitelnosti

V první fázi se stanoví hodnota veškerých parametrů popisujících zranitelnost definovaných v kapitole Hodnocení zranitelnosti, kde každému slovnímu ohodnocení odpovídá číselné. Výsledné číselné hodnoty všech parametrů, kromě dopadu na CIA triádu, zapíšeme do množiny, kterou budeme označovat jako *D*. Tato množina má přesně 6 prvků (jednotlivé parametry).

$$D = \{d_1, d_2, \ldots, d_6\}$$

Každý parametr má danou váhu pro stanovení jeho důležitosti. Váha je definována na množině reálných čísel z intervalu ⟨0,1⟩.

Otázka	Slovní hodnocení	Číselné hodnocení
Dojde k porušení legislativy při narušení důvěrnosti/dostupnosti/integrity dat	Ano	1
	Ne	0
Dojde k porušení interních předpisů při narušení důvěrnosti/dostupnosti/integrity dat	Ano	1
	Ne	0
Dojde k porušení jiných nařízení při narušení důvěrnosti/dostupnosti/integrity dat	Ano	1
	Ne	0
Je vaše společnost smluvně vázána k zajištění důvěrnosti/dostupnosti/integrity dat	Ano	1
	Ne	0
Jaký dopad na finanční stránku vaší společnosti může mít narušení důvěrnosti/dostupnosti/integrity dat	Žádný	0
	Minimální	0,25
	Menší vliv na roční zisk	0,50
	Významný vliv na roční zisk	0,75
	Bankrot	1
Může mít narušení důvěrnosti/dostupnosti/integrity dat dopad na finanční stránku společnosti, které data patří	Ano	1
	Ne	0
Může mít narušení důvěrnosti/dostupnosti/integrity dat dopad na finanční stránku jiné společnosti	Ano	1
	Ne	0
Jaký dopad na pověst vaší společnosti může mít narušení důvěrnosti/dostupnosti/integrity dat	Žádný	0
	Minimální	0,25
	Ztráta klíčových zákazníků	0,50
	Poškození dobrého jména společnosti	0,74
	Poškození celé značky	1
Může mít narušení důvěrnosti/dostupnosti/integrity dat dopad na pověst společnosti, které data patří	Ano	1
	Ne	0
Může mít narušení důvěrnosti/dostupnosti/integrity dat dopad na pověst jiné společnost	Ano	1
	Ne	0
Může mít narušení důvěrnosti/dostupnosti/integrity dat vliv na zaměstnance vaší firmy	Ano	1
	Ne	0
Jaké typy procesů ve vaší firmě by byly v případě narušení důvěrnosti/dostupnosti/integrity dat ovlivněny	Žádné	0
	Nevýznamné procesy	0,25
	Významné procesy týkající se obchodních aktivit	0,50
	Významné procesy týkající se jiných aktivit	0,75
	Kritické procesy	1
Jaké subjekty kromě vaší firmy by ovlivnilo narušení důvěrnosti/dostupnosti/integrity dat	Žádné	0
	Zákazníky	0,8
	Širokou veřejnost	1
Kolik subjektů by bylo ovlivněno v případě narušení důvěrnosti/dostupnosti/integrity dat	Žádný	0
	Jeden	0,10
	Desítky	0,30
	Stovky	0,70
	Tisíce	0,90
	Statisíce	0,95
	Milióny	1
Jak byste ohodnotili požadavek důvěrnosti/dostupnosti/integrity dat	Žádné požadavky	0
	Nízké požadavky	0,25
	Střední požadavky	0,50
	Vysoké požadavky	0,75
	Kritické požadavky	1

Tab. 11: Hodnotící otázky okruhu Požadavky důvěrnosti, dostupnosti a integrity

Jednotlivé váhy jsou uvedeny v následující tabulce.

Slovní hodnocení	Číselné ohodnocení
Není definováno	0,50
Žádná	0,00
Nízká	0,25
Střední	0,50
Vysoká	0,75
Velmi vysoká	1,00

Tab. 15: Váha jednotlivých parametrů popisujících zranitelnost

Množinu váhových hodnot odpovídajících prvkům množiny parametrů *D* budeme označovat jako množinu D_w. Tato množina má stejně jako množina *D* přesně 6 prvků.

$$D_w = \{d_{w1}, d_{w2}, \ldots, d_{w6}\}$$

Kromě uvedených parametrů je nezbytné stanovit dopad na důvěrnost, dostupnost a integritu zranitelného systému. Možné hodnoty jsou rovněž jako u ostatních parametrů předem dané.

Stanovení požadavků na CIA triádu

Po stanovení parametrů popisujících zranitelnost je nezbytné definovat požadavky na důvěrnost, dostupnost a integritu. Tyto požadavky vycházejí z odpovědí z uvedeného dotazníku. Každá otázka má dvě nebo více možných slovních odpovědí, kterým odpovídá předem stanovené číselné hodnocení. To se pohybuje na intervalu ⟨0,1⟩ nad množinou reálných čísel. Výsledné skóre okruhu se spočítá jako součet číselných hodnocení jednotlivých odpovědí z příslušného okruhu.

$$SkoreOkruhu = \sum CiselneHodnoceniOdpovedi$$

Hodnocení uvedených tří požadavků je vypočteno jako podíl součtu skóre příslušného okruhu a skóre z obecných otázek a maximálního počtu bodů.

Opatření	Popis	Číselné hodnocení
Šifrování	Šifrování je implementováno	0,8
	Šifrování není implementováno	1
Řízení přístupu	Pro přístup k systému/datům je nutná autentizace a autorizace přistupujícího	0,8
	Autentizace ani autorizace není vyžadována	1
Firewall	Systém je od nedůvěryhodných částí sítě oddělen firewallem	0,9
	Firewallová ochrana pro tento systém není implementována nebo neposkytuje dostatečné zabezpečení	1
Mikrosegmentace	Je zavedena mikrosegmentace, která zajišťuje minimální přístup k systému	0,9
	Mikrosegmentace sítě není implementována	1
Antivirový systém	Na systému běží antivirový program, který mimo jiné blokuje nežádoucí přístup k chráněným datům	0,9
	Antivirový program není nainstalován nebo neobsahuje modul pro blokování nežádoucího přístupu k chráněným datům	1

Tab. 12: Opatření vztahující se k ochraně důvěrnosti

Opatření	Popis	Číselné hodnocení
Vysoká dostupnost	Systém běží v režimu vysoké dostupnosti	0,8
	Režim vysoké dostupnosti není implementován	1
Zálohování	Systém/data jsou pravidelně zálohována na externí systém/úložiště	0,8
	Není implementován proces zálohování	1
DoS ochrana	Je implementována ochrana proti DoS útokům	0,9
	DoS ochrana není implementována	1

Tab. 13: Opatření vztahující se k ochraně dostupnosti

Opatření	Popis	Číselné hodnocení
Nástroje pro kontrolu integrity	Jsou implementovány nástroje pro kontrolu integrity a v pravidelných intervalech kontrolují integritu dat	0,8
	Nástroje pro kontrolu integrity nejsou implementovány	1
Řízení přístupu	Pro přístup k systému/datům je nutná autentizace a autorizace přistupujícího	0,8
	Autentizace ani autorizace není vyžadována	1
Správa oprávnění	Běžný uživatel má oprávnění pouze pro čtení dat	0,9
	Běžný uživatel má plná oprávnění pro práci s daty	1
Logování	Veškeré operace s daty jsou logovány, dá se tedy zjistit, jaké změny byly provedeny a jakým uživatelem	0,9
	Operace s daty nejsou logovány	1
Zálohování	Systém/data jsou pravidelně zálohována na externí systém/úložiště	0,9
	Není implementován proces zálohování	1

Tab. 14: Opatření vztahující se k ochraně integrity

$$(Duvernost)\ C_R = \frac{SkoreOtazekDuvernosti + SkoreObecnychOtazek}{19}$$

$$(Dostupnost)\ A_R = \frac{SkoreOtazekDostupnosti + SkoreObecnychOtazek}{19}$$

$$(Integrita)\ I_R = \frac{SkoreOtazekIntegrity + SkoreObecnychOtazek}{19}$$

V případě, že je skóre otázek daného okruhu rovno nule, je i celý požadavek roven nule.

Stanovení ohodnocení opatření

Toto ohodnocení se promítá do CIA triády, resp. do modifikované verze dopadu na CIA triádu, která zohledňuje i požadavek na zajištění všech tří parametrů. Díky tomu je opatření provázáno jak se samotnou zranitelností, tak s aktivem, na kterém je zranitelnost přítomna. Ohodnocení ochrany je vypočteno jako součin všech číselných hodnot jednotlivých položek v dané skupině. Jednotlivé hodnoty jsou vypočteny za použití následujících rovnic.

Pro výpočet ochrany důvěrnosti C_P je použita následující rovnice.

$$C_P = P_{c1} * P_{c2} * P_{c3} * P_{c4} * P_{c5}$$

Pro výpočet ochrany dostupnosti A_P je použita následující rovnice.

$$A_P = P_{a1} * P_{a2} * P_{a3}$$

Pro výpočet ochrany integrity I_P je použita následující rovnice

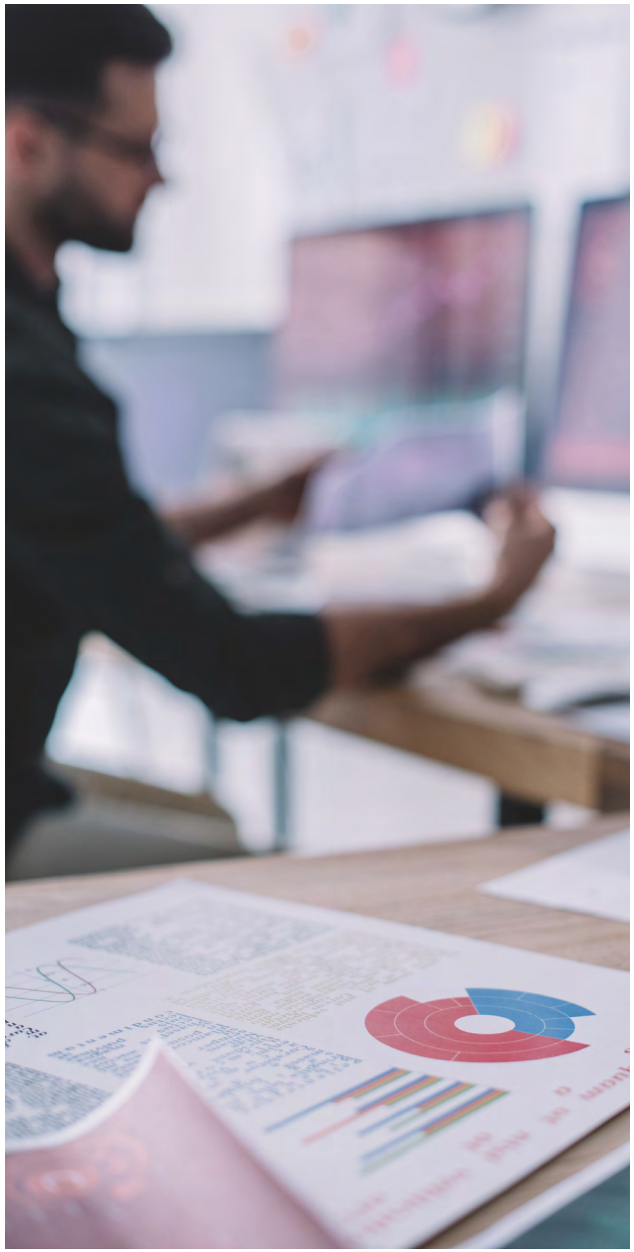
$$I_P = P_{i1} * P_{i2} * P_{i3} * P_{i4} * P_{i5}$$

Výpočet priority zranitelnosti

Nejdříve je vypočteno skóre zranitelnosti, do kterého není započítán dopad na CIA triádu. Toto skóre je vypočteno jako suma všech parametrů násobených jejich váhou. Skóre zranitelnosti S je číselné vyjádření parametrů zranitelnosti, které ovlivňuje její prioritu. Je definováno jako součin prvků množiny D a k nim odpovídajících vah z množiny D_w.

$$S = \sum_{i=1}^{6} D_i D_{wi}$$

Následně je nezbytné stanovit modifikovaný dopad na jednotlivé parametry CIA triády. To znamená provázat hodnotu požadavků důvěrnosti, dostupnosti a integrity s dopadem určeným při hodnocení zranitelnosti a s ochranou těchto parametrů, kterou poskytují implementovaná opatření. Modifikovaný dopad je kalkulován jako součin dopadu, požadavku na daný parametr a míry ochrany.



Pro výpočet modifikovaného dopadu na důvěrnost C_M je použita následující rovnice.

$$C_M = C * C_R * C_P$$

Pro výpočet modifikovaného dopadu na dostupnost A_M je použita následující rovnice.

$$A_M = A * A_R * A_P$$

Pro výpočet modifikovaného dopadu na integritu I_M je použita následující rovnice.

$$I_M = I * I_R * I_P$$

Modifikované skóre zranitelnosti S_M je následně definováno jako součin skóre zranitelnosti a součtu všech modifikovaných parametrů CIA triády.

$$S_M = S * (C_M + A_M + I_M)$$

Následně je již možné stanovit prioritu zranitelnosti *P*. Tato priorita je definována intervalem ⟨0,1000⟩ nad množinou celých čísel, kde vyšší číselné ohodnocení znamená vyšší prioritu a je vypočítáno jako poměr modifikovaného skóre zranitelnosti vůči maximálnímu možnému skóre. Maximální skóre v této metodice je 12,3. Výsledná hodnota je následně multiplikována hodnotou 1000 pro lepší prioritizaci bez desetinných čísel a je zaokrouhlena na celé číslo.

$$P = \frac{SM}{12,3} * 1000$$

Závěr

Navržená metoda pro prioritizaci zranitelností hodnotí zranitelnost pomocí devíti parametrů, které jsou rozděleny do dvou skupin. Toto hodnocení je dále doplněno o ohodnocení aktiva, na kterém se zranitelnost nachází, tuto číselnou hodnotu provazuje s dopadem na CIA triádu a výslednou hodnotu započítává do celkového skóre priority zranitelnosti. Do metody vstupuje i hodnocení implementovaných opatření, které je stejně jako priorita aktiva provázáno s dopadem na CIA triádu. Opatření snižují riziko zneužití zranitelnosti a z tohoto důvodu jsou do metody zahrnuta. Formální výpočet priority je postaven na základních matematických operacích tak, aby byla metoda co nejjednodušší, ale zároveň aby její výsledky byly přínosné.

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] Predictive Prioritization: Data Science Lets You Focus On The 3% Of Vulnerabilities Likely To Be Exploited. Tenable [online]. Columbia, 2019, 4. 12. 2019 [cit. 2019-12-08]. Dostupné z: https://lookbook.tenable.com/predictive-prioritization/technical-whitepaper-predictive-prioritization

[2] Definition: Threat Intelligence. Gartner [online]. 2019, 16. 5. 2013 [cit. 2019-12-08]. Dostupné z: https://www.gartner.com/en/documents/2487216

[3] OWASP Risk Rating Methodology. OWASP [online]. 27. 6. 2019 [cit. 2019-12-08]. Dostupné z: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[4] Common Vulnerability Scoring System version 3.1: Specification Document: CVSS Version 3.1 Release. First Improving Security Together [online]. 2019 [cit. 2019-12-08]. Dostupné z: https://www.first.org/cvss/specification-document