VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH METODY PRO HODNOCENÍ BEZPEČNOSTNÍCH ZRANITELNOSTÍ SYSTÉMŮ
DESIGN OF METHODOLOGY FOR VULNERABILITY ASSESMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. David Pecl

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Tomáš Gerlich

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. David Pecl ***ID:*** 185940

Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Návrh metody pro hodnocení bezpečnostních zranitelností systémů

POKYNY PRO VYPRACOVÁNÍ:

Diplomová práce bude zaměřena na návrh a implementaci nového metody hodnocení zranitelností. Student v rámci teoretické části nejprve analyzuje současně používané metody pro hodnocení závažnosti zranitelností a parametry, které jsou v jednotlivých metodách použity. Vycházejte především z rozšířeného hodnocení CVSS (Common Vulnerability Scoring System) a dostupných skenerů zranitelností. V praktické části práce student navrhne a implementuje vlastní metodu pro hodnocení zranitelností, jejímž cílem je lépe prioritizovat zranitelnosti. Funkčnost implementace bude ověřena na experimentálním pracovišti obsahujícím několik zranitelných systémů. Dosažené výsledky budou porovnány s výsledky dostupných skenerů.

DOPORUČENÁ LITERATURA:

[1] SCARFONE, Karen a Peter MELL. An analysis of CVSS version 2 vulnerability scoring. 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE, 2009, 2009, , 516-525. DOI: 10.1109/ESEM.2009.5314220. ISBN 978-1-4244-4842-5. Dostupné také z: http://ieeexplore.ieee.org/document/5314220/

[2] FRUHWIRTH, Christian a Tomi MANNISTO. Improving CVSS-based vulnerability prioritization and response with context information. 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE, 2009, 2009, , 535-544. DOI: 10.1109/ESEM.2009.5314230. ISBN 978-1-4244-4842-5. Dostupné také z: http://ieeexplore.ieee.org/document/5314230/

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Tomáš Gerlich

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

Abstrakt

Práce se zabývá problematikou hodnocení bezpečnostních zranitelností. Cílem práce je vytvořit novou metodu hodnocení zranitelností, která bude lépe prioritizovat kritické zranitelnosti a reflektovat parametry, které v aktuálně využívaných metodách nejsou použity.

Nejdříve popisuje současné metody, které se pro hodnocení zranitelností používají, a parametry, které jsou v jednotlivých metodách použity. První popsanou metodou je Common Vulnerability Scoring System, u které jsou popsané i všechny tři typy skóre, které tato metoda používá. Druhou analyzovanou metodou je OWASP Risk Rating Methodology.

Druhá část je věnována návrhu vlastní metody, která má za cíl hodnotit zranitelnosti tak, aby bylo snadnější určit ty s vysokou prioritou. Metoda vychází ze třech skupin parametrů. První skupina popisuje technické hodnocení zranitelnosti, druhá vychází z požadavků na zajištění důvěrnosti, integrity a dostupnosti aktiva a třetí skupina parametrů hodnotí implementovaná protiopatření. Všechny tyto tři skupiny parametrů jsou pro prioritizaci důležité. Parametry popisující zranitelnost jsou rozděleny na stálé a aktuální, kdy mezi aktuální patří především informace ze služeb Threat Intelligence a náročnost exploitace.

Parametry dopadu na důvěrnost, integritu a dostupnost jsou provázány s požadavky na zajištění těchto parametrů, neboli s prioritou aktiva, a dále s hodnocením protiopatření, která naopak zvyšují ochranu důvěrnosti, integrity a dostupnosti. Priorita aktiva a kvalita protiopatření se hodnotí na základě dotazníků, které jsou předloženy vlastníkům zkoumaných aktiv v rámci hodnocení zranitelností.

V třetí části práce je navržená metoda srovnána s v současnosti velmi používanou metodou Common Vulnerability Scoring System. Na několika příkladech jsou ukázány silné stránky navržené metody, kdy je vidět efektivita prioritizace při zohlednění požadavků na zajištění důvěrnosti, integrity a dostupnosti a zvýšená ochrana těchto parametrů díky implementovaným protiopatřením.

Metoda byla prakticky testována v laboratorním prostředí, kde byly na několika různých aktivech nasimulovány zranitelnosti. Tyto zranitelnosti byly ohodnoceny navrženou metodou, byla zohledněna priorita aktiva a kvalita protiopatření a vše bylo zahrnuto do výsledné priority zranitelností. V rámci tohoto testování bylo potvrzeno, že navržená metoda efektivněji prioritizuje zranitelnosti, které jsou jednoduše exploitovatelné, v poslední době často zneužívané a jsou přítomny na aktivech s minimální ochranou a vyšší prioritou.

Klíčová slova

Aktivum, bezpečnost, CVSS, dostupnost, důvěrnost, hodnocení zranitelnosti, integrita, OWASP, priorita, bezpečnostní protiopatření, zranitelnost

Abstract

The thesis deals with the assessment of security vulnerabilities. The aim of this work is to create a new method of vulnerability assessment, which will better prioritize critical vulnerabilities and reflect parameters that are not used in currently used methods.

Firstly, it describes the common methods used to assess vulnerabilities and the parameters used in each method. The first described method is the Common Vulnerability Scoring System for which are described all three types of scores. The second analysed method is OWASP Risk Rating Methodology.

The second part is devoted to the design of the own method, which aims to assess vulnerabilities that it is easier to identify those with high priority. The method is based on three groups of parameters. The first group describes the technical assessment of the vulnerability, the second is based on the requirements to ensure the confidentiality, integrity and availability of the asset and the third group of parameters evaluates the implemented security measures. All three groups of parameters are important for prioritization. Parameters describing the vulnerability are divided into permanent and up-to-date, where the most important up-to-date parameter are Threat Intelligence and easy of exploitation.

The parameters of the impact on confidentiality, integrity and availability are linked to the priority of the asset, and to the evaluation of security measures, which increase the protection of confidentiality, integrity and availability. The priority of the asset and the quality of the countermeasures are assessed based on questionnaires, which are submitted to the owners of the examined assets as part of the vulnerability assessment.

In the third part of the thesis, the method is compared with the currently widely used the Common Vulnerability Scoring System. The strengths of the proposed method are shown in several examples. The effectiveness of prioritization is based primarily on the priority of the asset and the security measures in place.

The method was practically tested in a laboratory environment, where vulnerabilities were made on several different assets. These vulnerabilities were assessed using the proposed method, the priority of the asset and the quality of the measures were considered, and everything was included in the priority of vulnerability. This testing confirmed that the method more effectively prioritizes vulnerabilities that are easily exploitable, recently exploited by an attacker, and found on assets with minimal protection and higher priority.

Keywords

Asset, security, CVSS, availability, confidentiality, vulnerability assessment, integrity, OWASP, priority, security measure, vulnerability

Bibliografická citace:

PECL, David. *Návrh metody pro hodnocení bezpečnostních zranitelností systémů.* Brno, 2020. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/125988. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Tomáš Gerlich.

Prohlášení

„Prohlašuji, že svou závěrečnou práci na téma Návrh metody pro hodnocení bezpečnostních zranitelností systémů jsem vypracoval samostatně pod vedením vedoucího diplomové práce a konzultanta diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.“

V Brně dne 30. května 2020 ……

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce, Ing. Tomáši Gerlichovi, za cennou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce. Dále bych chtěl poděkovat firmě AEC, a. s., která mi poskytla možnost zpracovávat diplomovou práci v jejich prostředí pod dohledem zkušených bezpečnostních konzultantů, kteří mi poskytli mnoho odborných rad. Také bych chtěl poděkovat konzultantovi diplomové práce, Ing. Mateji Kačicovi, Ph.D. a kolegovi Ing. Lubomíru Almerovi, Ph.D., kteří mi poskytovali jak odborné, tak pedagogické rady.

V Brně dne 30. května 2020 ……

podpis autora

Obsah

Úvod **12**

1 Zranitelnost a její životní cyklus **14**

1.1 Definice zranitelnosti 14
1.2 Životní cyklus zranitelnosti 14

2 Současné metody hodnocení zranitelností **16**

2.1 Common Vulnerability Scoring System 16
2.1.1 Princip CVSS 16
2.1.2 Verze CVSS 17
2.1.3 CVSS verze 3.1 18
2.1.4 Výhody a nevýhody CVSS v3.1 25
2.2 OWASP Risk Rating Methodology 26
2.2.1 Stanovení pravděpodobnosti zneužití 26
2.2.2 Stanovení dopadu zneužití 27
2.2.3 Stanovení celkového rizika 29
2.2.4 Výhody a nevýhody OWASP Risk Rating Methodology 29

3 Návrh vlastní metody pro hodnocení zranitelností **31**

3.1 Princip metody 31
3.2 Hodnocení zranitelnosti 32
3.2.1 Parametry popisující zranitelnost 33
3.3 Hodnocení aktiva 37
3.3.1 Stanovení požadavků na CIA triádu 37
3.3.2 Hodnotící otázky 38
3.4 Hodnocení protiopatření 40
3.4.1 Protiopatření použitá v metodice 41

4 Výpočet priority zranitelnosti **45**

4.1 Stanovení parametrů zranitelnosti 45
4.2 Stanovení požadavků na CIA triádu 46
4.3 Stanovení ohodnocení protiopatření 48
4.4 Výpočet priority zranitelnosti 49
4.5 Příklad výpočtu – CVE-2019-0708 51

5 Teoretické porovnání navržené metody a CVSSv3 55

5.1 Srovnání hodnocení zranitelností navržené metody a CVSSv3 55
5.2 Srovnání hodnocení zranitelností na systémech s různou prioritou 56
5.3 Srovnání hodnocení zranitelností s různými implementovanými protiopatřeními 58

6 Výsledky testování navržené metody 61

6.1 Testované systémy 61
6.1.1 Webový server IIS 61
6.1.2 Databázový server 62
6.1.3 Webový server Apache 62
6.1.4 Uživatelský systém 62
6.2 Průběh testování 63
6.3 Výsledky testování 63

7 Závěr 68

Seznam použitých zdrojů 70

Seznam příloh 74

Seznam obrázků

Obrázek 3.1: Schéma navržené metody.....31
Obrázek 5.1: Srovnání hodnocení zranitelností dle CVSS metody a dle navržené metody.....56
Obrázek 5.2: Porovnání zranitelností na systémech s různými požadavky na zajištění CIA triády.....58
Obrázek 5.3: Porovnání zranitelností na systémech s různými implementovanými protiopatřeními.....60
Obrázek 6.1: Srovnání CVSSv3 a navržené metody na webovém serveru IIS.....64
Obrázek 6.2: Srovnání CVSSv3 a navržené metody na databázovém serveru.....65
Obrázek 6.3: Srovnání CVSSv3 a navržené metody na webovém serveru Apache.....65
Obrázek 6.4: Srovnání CVSSv3 a navržené metody na uživatelském systému.....66

Seznam tabulek

Tabulka 2.1: Parametry základního skóre metodiky CVSS [11] 19
Tabulka 2.2: Parametry dočasného skóre metodiky CVSS [11] 20
Tabulka 2.3: Parametry skóre prostředí metodiky CVSS [11] 21
Tabulka 2.4: Číselné hodnocení základního skóre 22
Tabulka 2.5: Číselné hodnocení dočasného skóre 23
Tabulka 2.6: Číselné hodnocení skóre prostředí 24
Tabulka 2.7: Hodnocení pravděpodobnosti zneužití dle metodiky OWASP 26
Tabulka 2.8: Hodnoceni dopadu zneužití dle metodiky OWASP 28
Tabulka 2.9: Vztah mezi číselným a slovním hodnocením celkového rizika dle metodiky OWASP 29
Tabulka 2.10: Určení finální míry rizika dle metodiky OWASP [17] 29
Tabulka 3.1: Možné hodnoty dopadu na důvěrnost 33
Tabulka 3.2: Možné hodnoty dopadu na integritu 33
Tabulka 3.3: Možné hodnoty dopadu na dostupnost 34
Tabulka 3.4: Možné hodnoty obtížnosti zneužití 34
Tabulka 3.5: Možné hodnoty požadovaných oprávnění 35
Tabulka 3.6: Možné hodnoty interakce uživatele 35
Tabulka 3.7: Možné hodnoty dostupnosti informací 35
Tabulka 3.8: Možné hodnoty exploitace 36
Tabulka 3.9: Možné hodnoty Threat Intelligence 36
Tabulka 3.10: Hodnotící otázky okruhu Obecné informace 38
Tabulka 3.11: Hodnotící otázky okruhu Požadavky důvěrnosti 39
Tabulka 3.12: Protiopatření vztahující se k ochraně důvěrnosti 42
Tabulka 3.13: Protiopatření vztahující se k ochraně integrity 43
Tabulka 3.14: Protiopatření vztahující se k ochraně dostupnosti 43
Tabulka 4.1: Váha jednotlivých parametrů popisujících zranitelnost 45
Tabulka 4.2: Hodnocení parametrů popisujících zranitelnost CVE-2019-0708 51
Tabulka 5.1: Zkoumaná aktiva a jejich požadavky na zajištění CIA triády 57
Tabulka 5.2: Hodnocené zranitelnosti při srovnání metody 57
Tabulka 5.3: Vliv různých protiopatření na míru ochrany prvků CIA triády 59
Tabulka 6.1: Priorita aktiv v laboratorním prostředí 63
Tabulka 6.2: Implementovaná protiopatření na systémech v laboratorním prostředí 64
Tabulka 6.3: Srovnání hodnocení konkrétních zranitelností dle CVSSv3 a navržené metody 67

Úvod

Bezpečnost sítě a koncových zařízení je téma, kterým se v dnešní době zabývá většina jednotlivců i společností. Pro zajištění bezpečnosti systému se používají různé nástroje jako firewally, antivirové programy, systémy pro prevenci odcizení dat a další. Nesmí se však zapomínat ani na bezpečnost samotného operačního systému a aplikací, které na něm běží. Každý software má své nedostatky a ty bezpečnostní jsou zvlášť důležité. Zranitelnosti operačních systémů a aplikací jsou něco, s čím se potýkáme dnes a denně.

Ročně je objeveno obrovské množství zranitelností, v roce 2018 jich bylo nově objeveno přes 16 tisíc [1]. Z tohoto velkého čísla je podstatná část zranitelností hodnocena jako kritická nebo alespoň vysoká, téměř 59 % má dle Common Vulnerability Scoring System (CVSS) hodnocení více než 7 a 15 % má hodnocení více než 9 bodů [2].

Vzhledem k tomu, že více než desetina všech nově objevených zranitelností je hodnocena jako kritická, je na místě se zamyslet, zda v současnosti velmi rozsáhle užívaná metodika hodnocení zranitelností Common Vulnerability Scoring System je stále vhodná a zda její funkce prioritizace dostačuje rapidně přibývajícímu počtu nových zranitelností.

Již několikrát bylo zmiňováno, že metodika CVSS je zastaralá a její algoritmus hodnocení závažnosti zranitelností nereflektuje některé důležité parametry [3]. Vznikla proto novější verze tohoto standardu – CVSS verze 3, která počítá při hodnocení zranitelnosti s dalšími parametry oproti svému předchůdci.

I přes uvedení třetí verze CVSS používají hlavní výrobci nástrojů pro skenování různé další metodiky pro hodnocení a prioritizaci zranitelností. Namátkově se můžeme podívat na společnost Tenable, která v roce 2018 představila funkci Predictive Prioritization, Qualys hodnotí zranitelnosti nejen na základě CVSS, ale také pomocí své vlastní metody Qualys Severity Score, BeyondTrust používá mimo jiné vlastní metriku pro hodnocení kvality dostupného exploitu. Všechny tyto příklady ukazují na jednu věc – CVSS hodnocení v dnešní době nedostačuje a nezohledňuje některé důležité parametry [1, 4, 5].

Tato práce si dává za cíl analyzovat některé ze stávajících metod, které se pro hodnocení zranitelností používají. Důraz bude kladen na v současnosti nejpoužívanější metodu CVSS verze 2 i verze 3 a obě srovnáme. Zaměříme se také na další metodiku, která je pro tento účel používána, a to OWASP Risk Rating Methodology.

Hlavním cílem této práce však je porovnat jednotlivé metodiky a najít parametry, které jsou důležité pro hodnocení závažnosti zranitelností. Na základě této analýzy bude vytvořen návrh nové metody, která bude lépe prioritizovat nalezené zranitelnosti jak z hlediska technické úrovně zranitelnosti, tak z hlediska důležitosti zranitelného systému a dat na něm uložených. Mimo výše uvedené bude metoda zohledňovat i protiopatření, která mohou zajistit vyšší ochranu důvěrnosti, integrity a dostupnosti dat a systému.

Na závěr práce je provedeno teoretické srovnání CVSSv3 a navržené metody, které by mělo ukázat silné stránky navržené metody a vyšší efektivitu prioritizace při jejím využití. Na teoretické srovnání navazuje testování v laboratorním prostředí, kdy cílem je odzkoušet metodu na prostředí s nasimulovanými zranitelnostmi.

První kapitola této práce se zaměřuje na definici pojmu zranitelnost a popis jejího životního cyklu od detekce, přes analýzu a prioritizaci až po její odstranění. Pochopení tohoto cyklu je důležité, aby čtenář lépe porozuměl důvodům, proč je nutné prioritizaci zranitelností řešit a jakým způsobem je k hodnocení zranitelnosti přistupováno dnes.

V druhé kapitole je uveden teoretický rozbor dvou velmi používaných metod – CVSS a OWASP. Rozebereme, jaké parametry jsou pro hodnocení zranitelností používány v obou metodách, jaké jsou možné hodnoty u jednotlivých parametrů a jakým způsobem je stanoveno výsledné skóre zranitelnosti. U metody CVSS je blíže popsána aktuální verze CVSS 3.1.

Kapitola třetí již detailně popisuje navrženou metodu pro hodnocení zranitelností. Jsou zde popsány parametry, které jsou v této metodě použité, a jejich možné hodnoty a číselné ohodnocení. Dále je zde uvedeno, proč je důležité při prioritizaci zranitelností posuzovat i systém, na kterém se zranitelnost nachází, a jakým způsobem s prioritou aktiva pracuje tato nová metoda. Kromě technického posouzení zranitelnosti a priority aktiva pracuje metoda i s implementovanými protiopatřeními, které mohou zajistit vyšší ochranu důvěrnosti, integrity a dostupnosti. Práce se zabývá například protiopatřeními poskytované šifrováním, firewally, řízením přístupů a oprávnění, vysokou dostupností systémů nebo zálohováním.

Čtvrtá kapitola je zaměřena na matematické stanovení výsledné priority zranitelnosti. Podíváme se na použité parametry z matematického hlediska, uvedeme výpočty použité při stanovení priority a zaměříme se také na popis vztahu mezi aktivem, implementovaným protiopatřením a zranitelností. Na závěr je uveden příklad hodnocení zranitelnosti podle této nové metody.

Pátá kapitola obsahuje teoretické srovnání navržené metody a metody CVSS verze 3, kdy se zabývá jak samotným hodnocením zranitelnosti bez ohledu na požadavky aktiva na zajištění důvěrnosti, integrity a dostupnosti, tak hodnocením stejných zranitelností na různých systémech s různými požadavky na CIA triádu. Dále jsou zde srovnány zranitelnosti na systémech s různými implementovanými protiopatřeními

Obsahem poslední kapitoly je testování navržené metody v laboratorním prostředí. V rámci testování byly připraveny čtyři systémy, které jsou v této kapitole popsány, a na nich uměle vytvořeny zranitelnosti, které jsou navrženou metodou ohodnoceny. Jsou zde shrnuty výsledky jednak priority zranitelností na daných systémech, a dále na konkrétních příkladech z testování představeny silné stránky navržené metody.

1 Zranitelnost a její životní cyklus

Na úvod této kapitoly je vhodné si pro upřesnění definovat pojem zranitelnost. Termín zranitelnost popisuje spousta publikací a standardů, níže jsou uvedeny dvě základní definice dle standardu ISO 27005 a dle RFC 4949. První standard ISO 27005 patří do rodiny mezinárodních standardů ISO 27000, které se zaměřují na řízení informační bezpečnosti v organizacích. Druhý standard RFC 4949 je součástí řady dokumentů popisujících fungování počítačových sítí, protokolů a dalších, tento s názvem Internet Security Glossary je zaměřen na výklad termínů z oblasti informační bezpečnosti.

1.1 Definice zranitelnosti

Zranitelnost dle standardu ISO 27005 je definována jako „*A weakness of an asset or group of assets that can be exploited by one or more threats*“ [6]. V překladu tak můžeme říct, že se jedná o slabinu systému, která může být zneužita nositelem hrozby.

Zranitelnost dle standardu RFC 4949 je definována jako „*A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy*“ [7]. Tato definice popisuje zranitelnost jako slabinu v návrhu, implementaci, provozování nebo správě systému, při jejímž zneužití může dojít k narušení bezpečnosti tohoto systému.

Pro potřebu této práce je tedy zranitelnost slabinou systému, kterou může útočník zneužít a získat tak možnost přístupu k datům, jejich změny nebo dočasného či trvalého znedostupnění.

1.2 Životní cyklus zranitelnosti

Žádný systém není stoprocentně bezpečný, neboli každý systém má zranitelnosti [8]. To říká dokumentace vývojářů z Mozilly. Budeme-li se bavit o životním cyklu zranitelnosti, ten začíná ve chvíli, kdy je zranitelnost systému poprvé objevena.

Objevení zranitelnosti provází spousta dalších aktivit, nejprve je nutné potvrdit, zda se vůbec jedná o zranitelnost a pokud ano, jak závažná je. K tomu se používají různé metody pro hodnocení závažnosti zranitelností, některé z nich jsou blíže popsány v kapitole 2.

Pokud se ale na tento cyklus podíváme z pohledu správce systému nebo vlastníka aktiva, funguje poněkud odlišně. Objevení zranitelnosti není to „první“, kdy se sestavuje popis zranitelnosti a hodnocení její závažnosti. Objevení z pohledu správce[1], administrátora nebo bezpečnostního technika společnosti nastane teprve tehdy, když zjistí, že je daná zranitelnost přítomna na některém ze systému, které má pod svojí kontrolou.

V tomto případě už neprobíhá proces stanovení závažnosti zranitelnosti, závažnost už je dána některou z dostupných metodik. Naopak nastává proces prioritizace, protože takových zranitelností bývá v síti daleko více než jedna, jak bylo popsáno v úvodu. A právě prioritizace je jedna z věcí, kterou se tato práce zabývá.

V rámci analýzy zranitelností objevených v síti je nutné vybrat ty, které představují největší riziko, a sestavit plán odstraňování zranitelností v pořadí od těch nejrizikovějších po ty nejméně rizikové. Je nutné vzít také v potaz, na jakém systému se zranitelnost nachází, zda se jedná o produkční systém dostupný z internetu nebo o testovací server za několika firewally v části sítě, která nemá do internetu vůbec přístup. Také je vhodné zvážit další parametry, jako například dostupnost informací nebo aktuální zneužívání zranitelnosti ve světě [9].

Na konci tohoto cyklu dochází k odstranění zranitelnosti dvěma způsoby. Prvním, a tím nejlepším, je její „opravdové“ odstranění. Může se jednat o instalaci záplaty, úpravu konfigurace nebo aktualizaci zranitelného programu. Pokud odstranění zranitelnosti není možné (typicky se může jednat o nemožnost aktualizovat operační systém, protože na něm běží software, který není na novější verzi OS podporován), je třeba přistoupit k akceptaci zranitelnosti [9]. Akceptace zranitelnosti je druhým možným způsobem „odstranění“ zranitelnosti.

[1] V angličtině se používají dvě různá slovesa pro odlišení, zda byla dosud neznámá zranitelnost poprvé odhalena výzkumníkem (používá se slovo „discover“ nebo „find“), nebo zda byla detekována již známá zranitelnost administrátorem na některém zařízení v síti (tento význam se častěji spojuje se slovesem „detect“).

2 Současné metody hodnocení zranitelností

Většina databází zranitelností dnes pracuje s hodnocením zranitelností CVSS [10]. Existují však další metody, které slouží ke stejnému účelu. Může se jednat i o proprietární metody, které nejčastěji používají výrobci nástrojů pro skenování zranitelností (rozuměj detekci), u těchto metod však často není zveřejněn detailní princip fungování.

V následujících kapitolách se podíváme na dvě asi nejznámější – zmiňovanou metodu CVSS a OWASP.

2.1 Common Vulnerability Scoring System

Jednou z doposud nejpoužívanějších metodik pro hodnocení zranitelností je systém zvaný Common Vulnerability Scoring System, zkráceně CVSS, který je určený pro stanovení závažnosti zranitelností [11]. Je využíván jednak výrobci softwaru pro stanovení závažnosti nově objevené zranitelnosti (mimo jiné velká část z nich používá ještě vlastní hodnocení) a také ho využívají výrobci nástrojů pro skenování a řízení zranitelností. Ti díky němu mohou efektivně stanovit závažnost nalezených zranitelností.

Jak bude popsáno dále, CVSS není jedinou metodikou pro hodnocení závažnosti zranitelností. Existuje spousta dalších, ať už komerčních nebo nekomerčních. Velkou výhodou CVSS je fakt, že se jedná o volně dostupný framework, který není licenčně nijak omezen. Proto je hojně využíván právě v různých nástrojích pro skenování zranitelností[2].

Metodika CVSS hodnotí zranitelnosti na stupnici od 0 (nejméně závažná) do 10 bodů (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. Tento vektor dokáže daleko více zpřesnit, proč je daná zranitelnost hodnocena daným číselným skórem (například útočník nepotřebuje interakci uživatele) a představuje přehled o možnostech zneužití zranitelnosti a dopadu na systém při samotném incidentu.

2.1.1 Princip CVSS

Metodika CVSS je založena na třech oblastech hodnocení závažnosti zranitelností – základní skóre (tzv. Base Score), dočasné skóre (tzv. Temporal Score) a skóre prostředí (tzv. Environmental Score). Každá z těchto oblastí je dále hodnocena na základě více metrik, které se liší v závislosti na použité verzi CVSS [11].

[2] Seznam společností, které využívají CVSS metodiku ve svých produktech, je uveden na webu společnosti First: https://www.first.org/cvss/v2/adopters. Aktuálně se jedná o více než třicet společností.

Základní skóre vyjadřuje závažnost zranitelnosti samotné a nepočítá s žádnými vnějšími vlivy a okolnostmi, které běžně ovlivňují závažnost dané zranitelnosti. Samotné metriky se liší dle verze CVSS, obecně se ale dá říct, že závisí na dopadu na integritu, dostupnost a důvěrnost zranitelného systému, na náročnosti zneužití takové zranitelnosti (potřeba interakce uživatele nebo vyššího oprávnění) a na vektoru útoku. Základní skóre je v průběhu času neměnné a je stejné pro všechny výskyty dané zranitelnosti nezávisle na prostředí a čase.

Dočasné skóre na rozdíl od základního 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 již nevztahuje na zranitelnost samotnou, ale počítá s vnějšími vlivy, které mohou skóre zranitelnosti snížit (například v případě, že není dostupný exploit), nebo naopak zvýšit (například pokud je dostupný kvalitní exploit nebo neexistuje záplata na danou zranitelnost). Dočasné skóre je stejné pro všechny výskyty dané zranitelnosti, ať už se jedná o zranitelnost produkčního systému v malé firmě nebo o testovací systém ve velkém korporátu.

Skóre prostředí je stejně jako dočasné skóre velmi důležité pro konečnou prioritizaci dané zranitelnosti. Odráží totiž vliv prostředí, ve kterém se daná zranitelnost nachází – typ zranitelného systému, jeho umístění v síti, bezpečnostní opatření, která ovlivňují tento systém atd. Toto skóre se z principu liší pro jednotlivé výskyty dané zranitelnosti „v čase i v prostoru“, neboť každý systém může mít jinou důležitost, jsou na něm uložena různě důležitá data, používají se různé bezpečnostní opatření. Z tohoto důvodu je nutné, aby skóre prostředí stanovil vždy někdo se znalostí dané zranitelnosti, systému a dat na něm uložených, prostředí a všech bezpečnostních opatření, která jsou implementována. Toto skóre se tedy mění v průběhu času a je specifické pro jednotlivé výskyty zranitelností.

2.1.2 Verze CVSS

Aktuálně používaná metodika CVSS je ve verzi 3.1. Nová verze CVSS vychází vždy ze zpětné vazby uživatelů i výrobců, kteří tuto metodiku používají ve svých produktech. Nejčastější změny se týkají váhy jednotlivých metrik a jejich hodnot. Samotný princip tří oblastí hodnocení zůstal zachován od vzniku CVSS metodiky.

Ve verzi 3.0 došlo oproti verzi 2.0 k několika změnám [12, 13]. Ty nejdůležitější týkající se základního skóre jsou uvedeny v přehledu níže:

- rozšíření možných hodnot v metrice *Attack Vector (ze tří na čtyři)*;
- odstranění hodnoty *Medium* v metrice *Attack Complexity* (zůstává tedy jen *High* a *Low*);
- nahrazení metriky *Authentication* metrikou *Privileges Required*[3];

[3] Původní metrika reflektovala počet nutných autentizací před tím, než bude možné zranitelnost zneužít, ale nepočítala s úrovní autentizace (běžný uživatel nebo administrátor). Nová metrika *Privileges Required* spíše než počet nutných autentizací počítá s úrovní nutného oprávnění.

- přidání metriky *User Interaction*, která hodnotí nutnost interakce ze strany uživatele;
- přidání metriky *Scope*, která hodnotí možnost útoku na další systémy, které již neobsahují danou zranitelnost;
- změna váhy jednotlivých metrik a číselného hodnocení jednotlivých hodnot v metrikách.

2.1.3 CVSS verze 3.1

Verze 3.1 [11] má nově vysvětlené některé metodiky a je lépe pochopitelné, jaká hodnota daných metrik má být při hodnocení zranitelnosti použita. Samotné metriky a hodnoty nebyly změněny.

Níže v tabulkách 2.1, 2.2 a 2.3 jsou uvedeny jednotlivé parametry pro všechny tři typy skóre, popis parametrů a jednotlivých hodnot.

Tabulka 2.1: Parametry základního skóre metodiky CVSS [11]

Název metriky	**Popis metriky**	**Možné hodnoty**	**Popis hodnot**
Vektor útoku	Odráží typ hrozby	Vnější síťový	Útok z venkovní sítě (WAN, GSM)
		Vnitřní síťový	Útok z lokální sítě (LAN, Bluetooth, Wi-Fi)
		Lokální	Lokální útok ze zařízení (pomocí číst, zapisovat, spouštět)
		Fyzický	Útočník potřebuje fyzický přístup k zařízení
Komplexita útoku	Jaké podmínky musí být splněny, aby byla hrozba relevantní (nastavení zařízení, získané informace apod.)	Nízká	Úspěšnost útoku závisí pouze na útočníkovi a není potřeba splnění jiných podmínek, nebo jen minimálních
		Vysoká	Úspěšnost útoku nezávisí pouze na útočníkovi, ale na splnění podmínek, které nejsou útočníkem ovlivnitelné
Vyžadovaná oprávnění	Jaké oprávnění musí útočník mít, aby byla hrozba relevantní	Žádná	Útok je nezávislý na oprávnění útočníka k zařízení
		Nízká	Útok nevyžaduje žádné vyšší oprávnění k zařízení
		Vysoká	Útok vyžaduje vyšší oprávnění k zařízení
Interakce uživatele	Zda je vyžadována interakce uživatele (např. spuštění aplikace)	Žádná	Útok nevyžaduje interakci uživatele
		Vyžadována	Útok vyžaduje interakci uživatele
Rozsah	Odráží možnost, jestli se útok může rozšířit z jednoho zařízení na druhé	Nezměněný	Hrozba je reálná pouze pro napadené zařízení
		Změněný	Útočník může využít různých mechanizmů k tomu, aby napadl další zařízení
Dopad na důvěrnost	Hodnotí dopad na důvěrnost uložených nebo přenášených dat	Žádný	Žádný dopad na důvěrnost dat
		Nízký	Nízký dopad na důvěrnost dat
		Vysoký	Vysoký dopad na důvěrnost dat
Dopad na integritu	Hodnotí dopad na integritu uložených nebo přenášených dat	Žádný	Žádný dopad na integritu dat
		Nízký	Nízký dopad na integritu dat
		Vysoký	Vysoký dopad na integritu dat
Dopad na dostupnost	Hodnotí dopad na dostupnost uložených nebo přenášených dat	Žádný	Žádný dopad na dostupnost dat
		Nízký	Nízký dopad na dostupnost dat
		Vysoký	Vysoký dopad na dostupnost dat

Tabulka 2.2: Parametry dočasného skóre metodiky CVSS [11]

Název metriky	**Popis metriky**	**Možné hodnoty**	**Popis hodnot**
Kvalita exploitu	Hodnotí dostupnost a kvalitu případného exploitu	Není definováno	Nedostatek informací pro stanovení hodnoty
		Bez důkazů	Není znám žádný exploit
		Proof-of-Concept	Exploitace zranitelnosti byla demonstrována na konkrétním systému za přesně daných podmínek a je nepravděpodobné široké využití takového exploitu
		Funkční	Exploit funguje na většině zranitelných systémů
		Vysoká kvalita	Exploit funguje na všech zranitelných systémech a může být proveden i pomocí automatizovaného systému jako je např. malware
Úroveň nápravy	Hodnotí dostupnost nápravy ze strany výrobce a kvalitu této nápravy	Není definováno	Nedostatek informací pro stanovení hodnoty
		Oficiální záplata	Výrobce zranitelného systému vydal oficiální záplatu
		Dočasná záplata	Výrobce zranitelného systému vydal dočasnou záplatu, která bude později nahrazena oficiální
		Workaround	Neoficiální náprava zranitelnosti, která typicky nepochází od výrobce zranitelného systému[4]
		Nedostupná záplata	Žádná náprava není dostupná
Dostupnost informací	Kolik a jak kvalitních informací je o dané zranitelnosti dostupných, zda jsou tyto informace veřejně dostupné	Není definováno	Nedostatek informací pro stanovení hodnoty
		Nízké	Byly zveřejněny informace o existenci zranitelnosti bez technických detailů
		Střední	Byly zveřejněny technické detaily o dané zranitelnosti
		Detailní	Byly zveřejněny technické detaily o dané zranitelnosti a zdrojový kód je dostupný, tudíž lze jednoduše dohledat informace o provázanosti zranitelnosti s dalšími částmi systému

[4] Tento typ nápravy je specifický pro daný systém, prostředí a konfiguraci.

Tabulka 2.3: Parametry skóre prostředí metodiky CVSS [11]

Název metriky	**Popis metriky**	**Možné hodnoty**	**Popis hodnot**
Požadavek důvěrnosti	Jak vysoké jsou požadavky na zajištění důvěrnosti dat a samotného systému, na kterém je přítomna daná zranitelnost	Není definováno	Nedostatek informací pro stanovení hodnoty
		Nízký	Narušení důvěrnosti bude mít pravděpodobně nízký dopad na zaměstnance, zákazníky nebo celou organizaci
		Střední	Tato hodnota neovlivňuje výsledné skóre
		Vysoký	Narušení důvěrnosti bude mít pravděpodobně velmi vysoký dopad na zaměstnance, zákazníky nebo celou organizaci
Požadavek integrity	Jak vysoké jsou požadavky na zajištění integrity dat a samotného systému, na kterém je přítomna daná zranitelnost	Není definováno	Nedostatek informací pro stanovení hodnoty
		Nízký	Narušení integrity bude mít pravděpodobně nízký dopad na zaměstnance, zákazníky nebo celou organizaci
		Střední	Tato hodnota neovlivňuje výsledné skóre
		Vysoký	Narušení integrity bude mít pravděpodobně velmi vysoký dopad na zaměstnance, zákazníky nebo celou organizaci
Požadavek dostupnosti	Jak vysoké jsou požadavky na zajištění dostupnosti dat a samotného systému, na kterém je přítomna daná zranitelnost	Není definováno	Nedostatek informací pro stanovení hodnoty
		Nízký	Narušení dostupnosti bude mít pravděpodobně nízký dopad na zaměstnance, zákazníky nebo celou organizaci
		Střední	Tato hodnota neovlivňuje výsledné skóre
		Vysoký	Narušení dostupnosti bude mít pravděpodobně velmi vysoký dopad na zaměstnance, zákazníky nebo celou organizaci

Výpočet základního skóre

Jak již bylo zmíněno, základní skóre je tím nejpoužívanějším a tím, které se dá stanovit ihned po objevení zranitelnosti. K určení jeho hodnoty je nutné nejdříve stanovit příslušné parametry uvedené v tabulce 2.4. Teprve poté je možné stanovit skóre dle níže uvedených výpočtů [11].

Tabulka 2.4: Číselné hodnocení základního skóre

Parametr základního skóre	**Možné hodnoty**	**Číselné ohodnocení**
Vektor útoku	Vnější síťový	0,85
	Vnitřní síťový	0,62
	Lokální	0,55
	Fyzický	0,2
Komplexita útoku	Nízká	0,77
	Vysoká	0,44
Vyžadovaná oprávnění	Žádná	0,85
	Nízká	0,62[5]
	Vysoká	0,27[6]
Interakce uživatele	Žádná	0,85
	Vyžadována	0,62
Dopad na důvěrnost/integritu/dostupnost	Vysoký	0,56
	Nízký	0,22
	Žádný	0

Základní skóre se počítá pomocí několika rovnic, které vyjadřují dopad a možnost exploitace.

$$Dopad = 1 - [(1 - DopadNaDuvernost) \cdot (1 - DopadNaIntegritu) \cdot (1 - DopadNaDostupnost)] \quad (2.1)$$

Další rovnice vychází z hodnoty parametru Rozsah. Pokud je hodnota Nezměněný, použije se následující rovnice.

$$Dopad_{RozsahNezmeneny} = 6{,}42 \cdot Dopad \quad (2.2)$$

Pokud je hodnota Změněný, použije se následující rovnice.

$$Dopad_{RozsahZmeneny} = 7{,}52 \cdot (Dopad - 0{,}029) - 3{,}25 \cdot (Dopad - 0{,}02)^{15} \quad (2.3)$$

[5] nebo 0,68 pokud má parametr *Rozsah* hodnotu *Změněný*

[6] nebo 0,5 pokud má parametr *Rozsah* hodnotu *Změněný*

V další rovnici se počítá hodnota exploitovatelnosti.

$$Exploitovatelnost = 8{,}22 \times VektorUtoku \cdot KomplexitaUtoku \cdot VyzadovanaOpravneni \cdot InterakceUzivatele \quad (2.4)$$

Poslední rovnice se opět zvolí ze dvou dle hodnoty parametru Rozsah.

$$ZakladniSkore_{RozsahNezmeneny} = \text{Roundup}^{7}(\text{Minimum}[(Dopad_{RozsahNezmeneny} + Exploitovatelnost), 10]) \quad (2.5)$$

$$ZakladniSkore_{RozsahZmeneny} = \text{Roundup}(\text{Minimum}[1{,}08 \cdot (Dopad_{RozsahZmeneny} + Exploitovatelnost), 10]) \quad (2.6)$$

Výpočet dočasného skóre

Pro hodnocení dočasného skóre je nutné stanovit aktuální hodnoty parametrů uvedených v tabulce 2.5.

Tabulka 2.5: Číselné hodnocení dočasného skóre

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

[7] Funkce Roundup vrací nejmenší číslo s přesností na jedno desetinné místo, které je stejně velké nebo vyšší než číslo na vstupu. Pro vstup například 4,325 vrátí číslo 4,4, pro vstup 4,00 vrátí číslo 4,0.

Dočasné skóre se vypočítá z parametrů hodnocených v tomto skóre a ze základního skóre [11].

$$DocasneSkore = \text{Roundup}(ZakladniSkore \cdot KvalitaExploitu \cdot UrovenNapravy \cdot DostupneInformace) \tag{2.7}$$

Výpočet skóre prostředí

Skóre prostředí se skládá ze stejných parametrů jako základní skóre. Parametry, které jsou stejné jako v základním skóre, mají přídomek „modifikovaný“, protože se vztahují na dané prostředí, takže mohou mít jinou hodnotu než u základního skóre. Číselné ohodnocení parametrů ze základního skóre a modifikovaných parametrů je však pro jednotlivé hodnoty stejné.

Dále má skóre prostředí tři další parametry, pro které jsou možné hodnoty a jejich číselné ohodnocení uvedeny níže v tabulce 2.6.

Tabulka 2.6: Číselné hodnocení skóre prostředí

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

Pro výpočet skóre prostředí se nejdříve vypočítá modifikovaný dopad, který vyjadřuje závislost dopadu na důvěrnost/integritu/dostupnost a požadavku na tyto tři hodnoty [11].

$$\begin{aligned} ModifikovanyDopad = \text{Minimum}(&1 \\ &- [(1 - PozadavekDuvernosti \\ &\cdot ModifikovanyDopadNaDuvernost) \\ &\cdot (1 - PozadavekIntegrity \\ &\cdot ModifikovanyDopadNaIntegritu) \\ &\cdot (1 - PozadavekDostupnosti \\ &\cdot ModifikovanyDopadNaDostupnost)], 0{,}915) \end{aligned} \tag{2.8}$$

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

$$ModifikovanyDopad_{ModifikovanyRozsahNezmeneny} = 6{,}42 \cdot ModifikvaonyDopad \tag{2.9}$$

Pokud je hodnota *Změněný*, použije se následující rovnice.

$$\begin{aligned} ModifikovanyDopad_{ModifikovanyRozsahZmeneny} &= 7{,}52 \cdot (ModifikovanyDopad - 0{,}029) - 3{,}25 \\ &\cdot (ModifikovanyDopad \times 0{,}9731 - 0{,}02)^{13} \end{aligned} \tag{2.10}$$

V další rovnici se počítá hodnota modifikované exploitovatelnosti.

$$
\begin{aligned}
&ModifikovanaExploitovatelnost \\
&\quad = 8{,}22 \cdot ModifikovanyVektorUtoku \\
&\quad \cdot ModifikovanaKomplexitaUtoku \\
&\quad \cdot ModifikovanaVyzadovanaOpravneni \\
&\quad \cdot ModifikovanaInterakceUzivatele
\end{aligned}
\tag{2.11}
$$

Poslední rovnice se opět zvolí ze dvou dle hodnoty parametru *Modifikovaný rozsah*. Pro hodnotu *Nezměněný* se zvolí následující rovnice.

$$
\begin{aligned}
&SkoreProstedi_{ModifikovanyRozsahNezmeneny} \\
&= \mathrm{Roundup}\big(\mathrm{Roundup}\big(Minimum\big[\big(ModifikovanyDopad_{ModifikovanyRozsahNezmeneny} \\
&+ ModifikovanaExploitovatelnost\big), 10\big]\big) \cdot KvalitaExploitu \cdot UrovenNapravy \\
&\cdot DostupneInformace\big)
\end{aligned}
\tag{2.12}
$$

Pro hodnotu *Změněný* se zvolí následující rovnice.

$$
\begin{aligned}
&SkoreProstedi_{ModifikovanyRozsahZmeneny} \\
&\quad = \mathrm{Roundup}\big(\mathrm{Roundup}\big(Minimum\big[1{,}08 \\
&\quad \cdot \big(ModifikovanyDopad_{ModifikovanyRozsahNezmeneny} \\
&\quad + ModifikovanaExploitovatelnost\big), 10\big]\big) \\
&\quad \cdot KvalitaExploitu \cdot UrovenNapravy \\
&\quad \cdot DostupneInformace\big)
\end{aligned}
\tag{2.13}
$$

2.1.4 Výhody a nevýhody CVSS v3.1

Hlavní výhodou CVSS metodiky je její komplexnost, což je však i její hlavní nevýhodou [14, 15]. Pokud pro stanovení závažnosti zranitelnosti použijete až poslední skóre prostředí, výsledná hodnota závažnosti bude velmi přesně odrážet závažnost pro dané prostředí. Bohužel pro stanovení takového skóre je potřebné obrovské množství informací, které ve většině případů nejde zpracovat automatizovaně. Navíc samotná metodika je velmi komplikovaná, váha jednotlivých parametrů a jejich číselné ohodnocení je založeno na předchozích zkušenostech, ale pro každé prostředí může být vhodné nastavit váhu parametrů a číselné ohodnocení jinak [16].

Další nevýhodou CVSS je, že většina nástrojů pro detekci zranitelností a pro stanovení rizik počítá se základní variantou skóre. Je to právě z toho důvodu, že je téměř nemožné automatizovaně bez poskytnutí množství informací spočítat skóre prostředí. Prioritizace je tedy ponechána na uživateli nástroje.

Když se podíváme na výpočet dočasného skóre, můžeme si všimnout, že hodnota kvality exploitu se násobí základním skórem. Kvalita exploitu ale více souvisí s dopadem na důvěrnost, dostupnost nebo integritu [14]. Pokud nejsou data, která by mohla být odcizena, může být exploit sebelepší, ale pro útočníka je daleko více důležitý užitek z útoku než jeho jednoduchost. Stejně tak, pokud je narušena pouze jedna položka z triády důvěrnost, dostupnost, integrita,

základní skóre se rapidně sníží, ačkoliv pro útočníka může být stále velmi lákavé zneužít danou zranitelnost, provést útok a mít tak možnost například pozměnit soubory (v případě vysokého dopadu na integritu). Stejně tak z business pohledu na systém to může mít fatální následky.

2.2 OWASP Risk Rating Methodology

Další metodikou, která se používá pro hodnocení závažnosti zranitelností, je OWASP Risk Rating Methodology [17], která je primárně zaměřena na zranitelnosti ve webových aplikacích. Stejně tak se dá ale použít na hodnocení jakýchkoliv jiných bezpečnostních zranitelností systémů.

Tato metodika není zdaleka tak rozšířená jako CVSS skóre, které víceméně představuje standard v oblasti hodnocení závažnosti zranitelností, ale vzhledem k její jednoduchosti určitě stojí za zmínku. Základní myšlenkou tohoto hodnocení 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.

$$Riziko = Pravděpodobnost \cdot Dopad \tag{2.14}$$

Jak tedy vyplývá z výše uvedené rovnice, základními dvěma oblastmi pro hodnocení závažnosti zranitelnosti jsou pravděpodobnost zneužití a dopad na systém, při zneužití takové zranitelnosti.

2.2.1 Stanovení pravděpodobnosti zneužití

První oblastí pro stanovení finálního rizika je pravděpodobnost zneužití dané zranitelnosti. V této oblasti se hodnotí osm různých faktorů [17] rozdělených do dvou skupin – faktory nositelů hrozby (tzv. Threat Agent Factors) a faktory zranitelnosti samotné (tzv. Vulnerability Factors). Stanovení pravděpodobnosti zneužití pak proběhne jako průměr hodnot jednotlivých faktorů. Faktory z obou skupin jsou uvedeny níže v tabulce 2.7.

Tabulka 2.7: Hodnocení pravděpodobnosti zneužití dle metodiky OWASP

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

2.2.2 Stanovení dopadu zneužití

Druhou oblastí pro stanovení finálního rizika je dopad při zneužití dané zranitelnosti. Stejně jako v předchozí oblasti se hodnotí osm různých [17] faktorů rozdělených do dvou skupin – faktory technického dopadu (tzv. Technical Impact Factors) a faktory business dopadu (tzv. Business Impact Factors). Zde se už ale nedělá průměr hodnot, ale pro hodnocení se vezmou buď jen technické faktory, nebo lépe business faktory, pokud jsou k dispozici. Ne vždy se totiž dá ohodnotit dopad na business v případě zneužití zranitelnosti, proto je druhou možností počítat s technickými faktory, které lze ohodnotit vždy. Jednotlivé faktory z obou skupin jsou uvedeny níže v tabulce 2.8.

Tabulka 2.8: Hodnoceni dopadu zneužití dle metodiky OWASP

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
		Stovky lidí	5
		Tisíců lidí	7
		Miliónů lidí	9

2.2.3 Stanovení celkového rizika

Pro finální stanovení rizika je nejdříve nutné slovní ohodnocení jednotlivých číselných hodnot. To zobrazuje tabulka 2.9.

Tabulka 2.9: Vztah mezi číselným a slovním hodnocením celkového rizika dle metodiky OWASP

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

Jak již bylo řečeno, pravděpodobnost zneužití se vypočítá jako průměr všech hodnot faktorů nositelů hrozby a faktorů zranitelnosti, dopad při zneužití se spočítá jako průměr hodnot faktorů business dopadu, nebo pokud tyto faktory nelze ohodnotit, tak jako průměr hodnot faktorů technického dopadu. Pro určení finální míry rizika se vychází z tabulky 2.10.

Tabulka 2.10: Určení finální míry rizika dle metodiky OWASP [17]

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

2.2.4 Výhody a nevýhody OWASP Risk Rating Methodology

Výhodou této metodiky je jednoznačně jednoduchost, která je zajištěna díky menšímu množství faktorů (parametrů) než je tomu u CVSS a také jednoduchým principem vyhodnocení celkové míry rizika. Díky tomu se snadno implementuje do různých nástrojů [18], vzhledem ale k masivnímu rozšíření CVSS skóre tuto metodiku vídáme jen zřídka. Stejně tak je jednoznačná přímá úměra mezi pravděpodobností zneužití a dopadem při zneužití zranitelnosti. Druhou velkou výhodou je preference business faktorů před těmi technickými. Pro každý systém v různých organizacích může ta samá zranitelnost představovat jinou míru rizika, je tedy vhodné ji i jinak ohodnotit. Díky tomu, že metodika OWASP preferuje business faktory před těmi technickými, je prioritizace přesnější než například u základního skóre CVSS [19].

Dále metodika OWASP reflektuje parametry, které CVSS buď vůbec nemá, nebo je zohledňuje v jiném než základním skóre. Jedná se například o faktory exploitace nebo informace o zranitelnosti, které jsou obsaženy až v dočasném CVSS skóre. Dále metodika OWASP vychází také z faktorů motivace útočníka a možnosti odhalení útočníka. Hlavně první zmíněný faktor je velmi důležitý pro prioritizaci zranitelností. Útočníkova motivace mimo jiné závisí i na „odměně“, kterou může za zneužití zranitelnosti získat, což přímo souvisí s dopadem na důvěrnost, dostupnost a integritu [20]. Právě tento parametr je jeden z nevýhod CVSS metodiky.

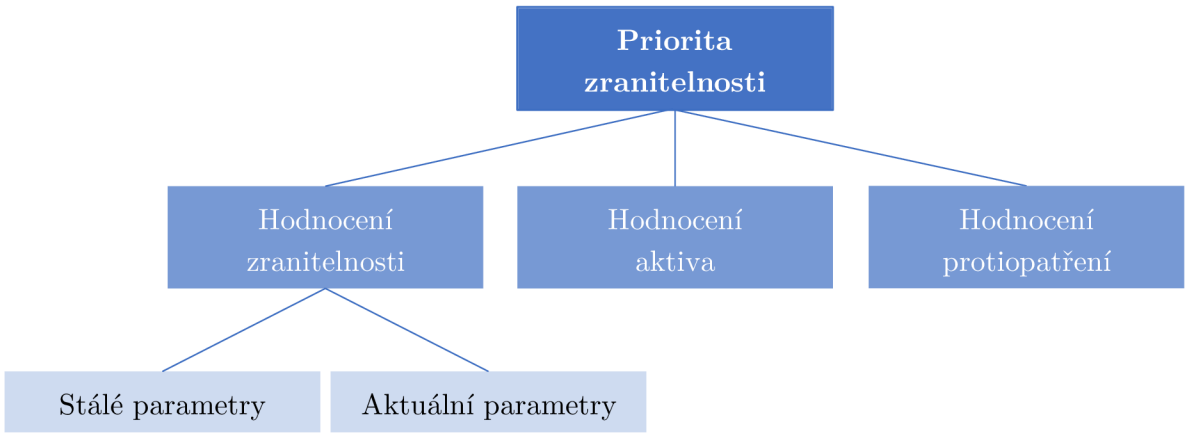
Nevýhodou této metodiky je právě ona jednoduchost. To, co je v CVSS skóre hodnoceno pomocí čtyř parametrů (vektor útoku, komplexita útoku, úroveň oprávnění, interakce uživatele), je zde hodnoceno pouze faktory obtížnost zneužití zranitelnosti a skupina nositelů hrozby. Není zde tedy možné specifikovat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

3 Návrh vlastní metody pro hodnocení zranitelností

Každá metoda pro stanovení závažnosti zranitelností vychází z určitého základního principu. Některé metodiky mají princip složitější, jako například výše uvedené hodnocení CVSS, naopak jiné koncepty pracují s jednoduchým principem, aby samotná metoda byla lehká na pochopení a snadná na implementaci, takovým příkladem může být zmíněná metoda OWASP.

3.1 Princip metody

Vlastní metoda pro prioritizaci zranitelností vychází z principu, kdy není hodnocena pouze samotná zranitelnost, ale pro výsledné číslo určující prioritu se používají i informace o zranitelném systému, které můžou ve výsledku snížit nebo naopak zvýšit prioritu zranitelnosti, a informace o implementovaných protiopatřeních, tedy ochranách, které pomáhají zajišťovat důvěrnost, integritu a dostupnost systému a ve výsledku mohou snížit prioritu zranitelnosti. Základem jsou tedy tři části – hodnocení zranitelnosti, zranitelného systému a protiopatření. Schéma hodnocení priority zranitelnosti je zobrazeno na obrázku 3.1.



Obrázek 3.1: Schéma navržené metody

Hodnocení zranitelnosti se skládá z devíti různých parametrů, které jsou popsány dále a které mají hodnoty od 0 do 1. Každý parametr má od dvou do šesti různých slovních popisů, které jsou dále převedeny na číslo v intervalu 0 až 1. Slovní popis je určen pro stanovení hodnoty parametru, protože pro člověka je téměř nemožné stanovit například obtížnost zneužití od 0 do 1, ale pomocí slovního popisu a uvedených příkladů u jednotlivých hodnot zvládne tohle stanovení daleko přesněji.

Hodnocení aktiva (zranitelného systému) je stanoveno na základě tří parametrů – požadavku na důvěrnost, integritu a dostupnost systému nebo dat na něm. Stanovení hodnoty je založeno na základě dotazníku, který pomáhá a zjednodušuje tento proces.

Požadavek na jeden ze tří parametrů CIA triády (důvěrnost, integrita a dostupnost z anglického *confidentiality, integrity, availability*) je pak použit při prioritizaci zranitelnosti a výsledná priorita zranitelnosti je posuzována jak z hlediska tohoto požadavku, tak z hlediska dopadu při zneužití zranitelnosti.

Hodnocení protiopatření je opět stanoveno na základě dotazníku, ve kterém se hodnotí, zda jsou implementovány mechanizmy pro zajištění důvěrnosti, integrity a dostupnosti. Tohle hodnocení je provázáno jak se samotnou zranitelností, tak se zranitelným systémem – ovlivňují se tedy všechny tři typy hodnocení vzájemně.

3.2 Hodnocení zranitelnosti

První oblastí při stanovení priority je hodnocení zranitelnosti. Parametry v této oblasti jsou dále rozděleny do dvou skupin – stálé parametry a aktuální parametry. Stálé parametry jsou z hlediska prioritizace v čase neměnné, naopak aktuální parametry se v čase mohou měnit a znatelně tak ovlivňovat prioritu zranitelnosti. Mezi ty stálé 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 dopad na CIA triádu, tedy dopad na důvěrnost, integritu a dostupnost. Tyto hodnoty vyjadřují, jak moc může zneužití zranitelnosti ohrozit zranitelný systém nebo data na něm uložená. Samotná informace o dopadu na jednu z těchto tří položek ale nestačí. Pro správnou prioritizaci je nutné pracovat také s požadavkem na tyto tři položky. Pokud daný systém nemá požadavek důvěrnosti, tj. data na něm jsou veřejná, zranitelnost s dopadem na důvěrnost pro tento daný systém není vůbec prioritní. Z tohoto důvodu je nutné při stanovení priority počítat nejen s ohrožením základní CIA triády, ale také s tím, jestli existují požadavky na důvěrnost, integritu a dostupnost a jak vysoké jsou. V dalších kapitolách bude vztah mezi dopadem na CIA triádu a požadavky na tyto parametry vysvětlen.

Mezi stálé parametry patří ještě obtížnost zneužití zranitelnosti, vyžadovaná interakce uživatele a případné oprávnění, které je k úspěšnému zneužití potřebné. Interakce uživatele a požadovaná oprávnění jsou víceméně stejné jako u metody hodnocení CVSS. Do parametru obtížnost zneužití se promítá technická náročnost exploitace dané zranitelnosti, zda je potřeba využít řetězec zranitelností nebo je možné rovnou zneužít hodnocenou zranitelnost, jakým způsobem zneužití vůbec probíhá (přetečení zásobníku a další metody) a další parametry vztahující se k obtížnosti zneužití.

Kromě výše popsaných stálých parametrů pracuje tato metoda ještě s aktuálními parametry, tedy těmi, které se v čase mění a jejich změna ovlivňuje také prioritu zranitelnosti. Prvním z těchto parametrů je dostupnost informací, čili zda jsou dostupné technické informace o zranitelnosti, zda je popsaný způsob, jak zranitelnost funguje, jakým způsobem je možné ji zneužít

a další. Pro tento parametr je také důležité, pokud žádné informace zveřejněny nejsou a technické informace o zranitelnosti jsou utajené [3]. Druhým parametrem je exploitace, respektive její možnosti automatizace, a kvalita exploitu. Stejně jako výše popsaný parametr dostupnost informací je parametr exploitace převzat z metody OWASP.

Posledním parametrem je informace o aktivním zneužívání zranitelnosti tedy informace z tzv. Threat Intelligence. Společnost Gartner definuje pojem Threat Intelligence jako „*databázi znalostí o existující nebo vznikající hrozbě, které jsou založeny na důkazech, včetně kontextu, mechanizmu fungování hrozby, indikátorů, důsledků a díky kterým je možné se informovaně rozhodnout o případné reakci na tuto hrozbu*“ [21].

Jedná se o služby, které se zabývají monitorováním útoků a technických bezpečnostních hrozeb na celém světě. Data z těchto služeb z hlediska prioritizace tedy vyjadřují, jak moc je daná zranitelnost v poslední době zneužívaná. Služby Threat Intelligence se používají například v antivirových programech nebo v mnoha jiných bezpečnostních nástrojích [22].

3.2.1 Parametry popisující zranitelnost

Dopad na důvěrnost

Dopad na důvěrnost vyjadřuje, jak velké množství dat může být odcizeno a jak citlivá tato data jsou. Vychází z OWASP metodologie [17].

Typ: stálý parametr

Tabulka 3.1: Možné hodnoty dopadu na důvěrnost

Slovní hodnocení	**Číselné hodnocení**
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 všech dat	1,00

Dopad na integritu

Dopad na integritu vyjadřuje, jak velké množství dat může být poškozeno a jak rozsáhlé tohle poškození může být. Vychází z OWASP metodologie [17].

Typ: stálý parametr

Tabulka 3.2: Možné hodnoty dopadu na integritu

Slovní hodnocení	**Číselné hodnocení**
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 všech dat	1,00

Dopad na dostupnost

Dopad na dostupnost vyjadřuje, jak velké množství služeb může být vyřazeno z provozu a jak důležité tyto služby jsou. Vychází z OWASP metodologie [17].

Typ: stálý parametr

Tabulka 3.3: Možné hodnoty dopadu na dostupnost

Slovní hodnocení	**Číselné hodnocení**
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

Obtížnost zneužití

Obtížnost zneužití vyjadřuje, jaké zdroje potřebuje útočník ke zneužití zranitelnosti, zda je potřebné před zneužitím dané zranitelnosti zneužít i jiné zranitelnosti (řetězec zneužití zranitelností), o jak komplexní útok se jedná (řetězec aktivit, které musí být úspěšně provedeny, aby se útočník mohl pokusit o zneužití dané zranitelnosti) atd. Vychází z OWASP metodologie [17].

Typ: stálý parametr

Tabulka 3.4: Možné hodnoty obtížnosti zneužití

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

Požadovaná oprávnění

Parametr požadovaná oprávnění vyjadřuje úroveň oprávnění, které musí útočník mít, než zneužije danou zranitelnost. Pokud není potřeba žádné oprávnění, je parametr hodnocen nejvyšším číslem. Slovní hodnocení nízká vyjadřuje například oprávnění běžného uživatele, slovní hodnocení vysoká například administrátorské oprávnění. Vychází z CVSS metodologie [11].

Typ: stálý parametr

Tabulka 3.5: Možné hodnoty požadovaných oprávnění

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

Interakce uživatele

Interakce uživatele vyjadřuje nutnost uživatelské aktivity před nebo při zneužití zranitelnosti. Může se jednat například o spuštění programu, vložení USB disku do počítače, přístup na webovou stránku a další. Pokud není zneužití zranitelnosti vázáno na interakci uživatele, je parametr ohodnocen číslem 1. Vychází z CVSS metodologie [11].

Typ: stálý parametr

Tabulka 3.6: Možné hodnoty interakce uživatele

Slovní hodnocení	Číselné hodnocení
Žádná	1
Vyžadována	0,40

Dostupnost informací

Tento parametr vyjadřuje, jaké množství informací o zranitelnosti je zveřejněno. Některé nově objevené zranitelnosti zůstávají v tajnosti až do doby, než je k dispozici oficiální záplata výrobce. Naopak se může stát, že informace o zranitelnosti jsou publikovány v studijní nebo vědecké zprávě, kde jsou popsány i veškeré technické informace o tom, jak zranitelnost funguje a jak je možné ji zneužít. Vychází z OWASP metodologie [17].

Typ: aktuální parametr

Tabulka 3.7: Možné hodnoty dostupnosti informací

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

Exploitace

Exploitace vyjadřuje možnost zneužití zranitelnosti pomocí automatizovaných nástrojů a kvalitu dostupných exploitů. Pokud je možné zranitelnost zneužit pomocí automatizovaných nástrojů jako je metasploit a další, je číselné hodnocení nejvyšší, naopak pokud neexistuje žádný známý exploit, je číselné hodnocení minimální. Vychází z OWASP metodologie [17].

Typ: aktuální parametr

Tabulka 3.8: Možné hodnoty exploitace

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

Threat Intelligence

Parametr Threat Intelligence zohledňuje aktuální zneužívání zranitelnosti zachycené monitorovacími službami Threat Intelligence. Pokud nejsou k dispozici žádné informace z těchto služeb, je použita hodnota Není definováno. Pokud jsou však tyto služby dostupné, ale nemají žádné informace o zneužívání zranitelnosti, použije se hodnota „*žádná*“ s číselným hodnocením 0. Naopak ve chvíli, kdy tyto služby zachytí několik desítek pokusů o zneužití za den, je zvolena nejvyšší hodnota „*velmi vysoká*“ s hodnocením 1,00.

Typ: aktuální parametr

Tabulka 3.9: Možné hodnoty Threat Intelligence

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

3.3 Hodnocení aktiva

Pro správnou prioritizaci zranitelnosti je nutné vědět, o jaký zranitelný systém se jedná. Základní skóre CVSS nebere v potaz důležitost zranitelného systému, zda se jedná o produkční server v DMZ[8] zóně nebo o server v uzavřeném testovacím prostředí. Tyto a další informace o aktivu je nutné zhodnotit při stanovení priority zranitelnosti [23].

Způsobů, jak ohodnotit důležitost aktiva, je velmi mnoho. Každá z metod však vyžaduje značné množství informací o daném aktivu. Tyto informace je nutné získat od vlastníků dotčených aktiv, protože oni jediní ví, jaká data jsou na systému uchovávána, k čemu systém slouží, kdo na něj má přístup a další důležité parametry pro stanovení priority aktiva.

Pro náš způsob hodnocení aktiva byla vybrána forma dotazníku, díky kterému pomocí několika otázek je možné určit důležitost dat uložených na daném systému z hlediska CIA triády. Určení těchto požadavků na důvěru, integritu a dostupnost může snížit nebo zvýšit výslednou prioritu zranitelnosti v závislosti na parametrech dopadu na jeden z těchto parametrů (při případném zneužití zranitelnosti).

3.3.1 Stanovení požadavků na CIA triádu

Výše zmíněný dotazník, který je uveden jako příloha A, se skládá z 52 otázek rozdělených do čtyř okruhů:

- obecné informace,
- požadavky důvěrnosti,
- požadavky integrity,
- požadavky dostupnosti.

Otázky v posledních třech hodnotících kategoriích jsou unifikovány, tj. stejná otázka je kladena při stanovení důvěrnosti, integrity i dostupnosti. Výhodou toho je jednodušší a rychlejší vyplnění pro vlastníka aktiva.

Každý z výše uvedených okruhů má dále otázky rozdělené do několika oblastí. První skupina s názvem *Obecné informace* má tři oblasti otázek:

- charakter dat,
- vztah vaší firmy k datům,
- charakter aktiva.

[8] Tzv. demilitarizovaná zóna. Jedná se o speciální část sítě, která je určena pro komunikaci s internetem. Obvykle se v ní nachází webové a další servery, u kterých je potřeba zajistit přístup z internetu. Tato část sítě obvykle nemůže komunikovat do interní sítě.

Další tři okruhy zaměřené na požadavky CIA triády mají otázky sjednocené, jak již bylo uvedeno, a jsou rozděleny do následujících oblastí:

- legislativní, smluvní a jiné nařízení CIA,
- finanční dopad při narušení CIA,
- dopad na pověst při narušení CIA,
- vliv na vaši firmu při narušení CIA,
- vliv na jiné firmy při narušení CIA,
- množství dat,
- odhad požadavku CIA.

Každá odpověď v tomto dotazníku je hodnocena 0 až 1 bodem (včetně možných desetinných čísel). Následně se sečte počet bodů za všechny otázky z jednotlivých okruhů a výsledkem je hodnota požadavku na danou oblast CIA triády. Podrobněji je celý formální proces hodnocení popsán v kapitole 4.2. Toto hodnocení se následně použije pro stanovení priority zranitelnosti.

3.3.2 Hodnotící otázky

Všechny otázky pro hodnocení požadavku důvěrnosti, integrity a dostupnosti mají přesně dané možnosti odpovědi, kdy každá odpověď je ještě speciálně číselně ohodnocena. Většina otázek se zaměřuje přímo na samotná data, která jsou na daném systému uložena nebo v nějaké formě zpracovávána.

Otázky z prvního okruhu *Obecné informace* jsou určeny pro základní stanovení priority aktiva a jsou uvedeny v tabulce 3.10.

Tabulka 3.10: Hodnotící otázky okruhu Obecné informace

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
Patří data vaší společnosti?[9]	Ano	-

[9] Tato otázka se již nezapočítává do výsledného skóre požadavku důvěrnosti, integrity nebo dostupnosti, ale je uvedena jen pro případné upřesnění informací o aktivu.

	Ne	-
Je vaše firma zpracovatelem těchto dat?[9]	Ano	-
	Ne	-
Je vaše firma uchovatelem těchto dat ve významu dlouhodobého uložení dat (déle než je potřeba na běžné zpracování)?[9]	Ano	-
	Ne	-

Další okruh *Požadavky důvěrnosti* obsahuje otázky zaměřující se na hodnocení důležitosti parametru důvěrnosti pro daný systém a data na něm uložená nebo zpracovávaná. Stejně tak pro ostatní okruhy *Požadavky integrity* a *Požadavky dostupnosti* jsou otázky víceméně podobné, proto jsou uvedeny pouze otázky z prvního okruhu, a to v tabulce 3.11.

Tabulka 3.11: Hodnotící otázky okruhu Požadavky důvěrnosti

Otázka	**Slovní hodnocení**	**Číselné hodnocení**
Dojde k porušení legislativy při narušení důvěrnosti dat?	Ano	1
	Ne	0
Dojde k porušení interních předpisů při narušení důvěrnosti dat?	Ano	1
	Ne	0
Dojde k porušení jiných nařízení při narušení důvěrnosti dat?	Ano	1
	Ne	0
Je vaše společnost smluvně vázána k zajištění důvěrnosti dat?	Ano	1
	Ne	0
Jaký dopad na finanční stránku vaší společnosti může mít narušení důvěrnosti 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 dat dopad na finanční stránku společnosti, které data patří?	Ano	1
	Ne	0
Může mít narušení důvěrnosti dat dopad na finanční stránku jiné společnosti?	Ano	1
	Ne	0
Jaký dopad na pověst vaší společnosti může mít narušení důvěrnosti dat?	Žádný	0
	Minimální	0,25
	Ztráta klíčových zákazníků	0,50
	Poškození dobrého jména společnosti	0,75
	Poškození celé značky	1
Může mít narušení důvěrnosti dat dopad na pověst společnosti, které data patří?	Ano	1
	Ne	0
	Ano	1

Může mít narušení důvěrnosti dat dopad na pověst jiné společnosti?	Ne	0
Může mít narušení důvěrnosti dat vliv na zaměstnance vaší firmy?	Ano	1
	Ne	0
Jaké typy procesů ve vaší firmě by byly v případě narušení důvěrnosti 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 dat?	Žádné	0
	Zákazníky	0,8
	Širokou veřejnost	1
Kolik subjektů by bylo ovlivněno v případě narušení důvěrnosti?	Žádný	0
	Jeden	0,10
	Desítky	0,30
	Stovky	0,70
	Tisíce	0,90
	Statisíce	0,95
	Miliony	1
Jak byste ohodnotili požadavek důvěrnosti dat?	Žádné požadavky	0
	Nízké požadavky	0,25
	Střední požadavky	0,50
	Vysoké požadavky	0,75
	Kritické požadavky	1

3.4 Hodnocení protiopatření

Abychom správně ohodnotili dopad na CIA triádu, je vhodné počítat také s protiopatřeními, která mohou mít vliv na tyto hodnoty. Pro představu je možné uvést příklad se zranitelností, která má vysoký dopad na dostupnost systému. Pokud máme systém v módu vysoké dostupnosti[10] a máme prováděné pravidelné zálohy, dopad na dostupnost nebude tak vysoký, než kdyby se jednalo o běžný server, který by nebyl zálohován a neměl svoji redundantní kopii v provozu. Stejný princip můžeme aplikovat i u ostatních hodnot dopadu na integritu a do-

[10] Vysoká dostupnost (v angličtině označováno jako „High Availability“) je režim, ve kterém je daný systém provozován v několika stejných instancích. V případě výpadku jedné instance je provoz přesměrován automaticky na druhou instanci. Může se jednat o jednu instanci v provozu a ostatní v pohotovostním módu (tzv. stand-by), nebo o režim, ve kterém jsou všechny instance provozovány zároveň a kromě vysoké dostupnosti je zajištěno také úměrné rozložení zátěže provozu (tzv. load-balancing).

stupnost systému. Jako protiopatření můžeme brát firewall umístěný před serverem nebo mikrosegmentaci (ochrana důvěrnosti) nebo třeba nástroje pro kontrolu integrity nebo řízení přístupu (v případě ochrany integrity).

Tato protiopatření, stejně jako v předchozím případě při hodnocení aktiva, jsou hodnocena na základě dotazníku, který je obsahem přílohy A. Vlastník aktiva případně správce infrastruktury dokáže určit, jaké protiopatření jsou v případě konkrétního systému použita. V rámci dotazníku zvolí, zda je dané protiopatření implementováno a dle zvolené odpovědi se určí číselné hodnocení. To se následně promítne do výsledné priority zranitelnosti.

3.4.1 Protiopatření použitá v metodice

Protiopatření, která jsou v rámci navržené metodiky hodnocena, jsou uvedena v tabulkách 3.12, 3.13 a 3.14. Konkrétní protiopatření se může vztahovat k více než jednomu prvku CIA triády a dle toho jsou také rozdělena do tří skupin.

V následujícím textu jsou popsány protiopatření, se kterými tato metodika pracuje, společně s jejich schopností zajistit ochranu důvěrnosti, integrity a dostupnosti.

Šifrování je mechanizmus zajišťující v případě této metodiky pouze ochranu důvěrnosti dat. Metodika nemá za cíl hodnotit kvalitu zvoleného šifrovacího algoritmu, délky klíčů ani kvalitu implementace, hodnotí se pouze, zda šifrování je implementováno nebo není.

Řízení přístupu se vztahuje nejen k zajištění důvěrnosti, ale i integrity dat. Pokud je přístup na daný systém regulován (je nutná autentizace a autorizace, teprve poté získá uživatel přístup k datům), snižuje se možnost neoprávněného čtení nebo modifikace dat.

Dalším nástrojem, který v rámci této metodiky pomáhá zajistit důvěrnost dat, je **firewall**. Metodika pracuje s předpokladem jeho nasazení před zkoumaným systémem a nastavení takové politiky, která povoluje jen předem definovanou komunikaci. Stejně jako v případě šifrování a dalších mechanizmů není hodnocena kvalita firewallové politiky a schopnosti detekce, ale pouze fakt, zda firewall je implementován, nebo ne.

Mikrosegmentace je dalším mechanizmem, který může pomoci zajistit důvěrnost systému. Společně s firewallem tvoří pomyslnou síťovou bezpečnost a předpokládá se, že komunikace se zranitelným systémem je povolena pouze v rámci daného mikrosegmentu s případným povolením konkrétních typů komunikace.

K ochranně důvěrnosti může dále přispět **antivirový systém**. Samotný antivir dokáže pomoci v mnoha dalších ohledech, zde se ale bavíme o konkrétním modulu pro blokování nežádoucího přístupu k chráněným datům. Většina výrobců antivirových programů tento modul zahrnula do svého produktu, proto i v případě této metodiky je s ním počítáno.

Pro ochranu integrity mohou sloužit specializované nástroje, které v pravidelných intervalech kontrolují, zda nedošlo ke změně souborů. Tyto **nástroje pro kontrolu integrity** jsou součástí také této metodiky. Jejich významnou funkcí je ohlášení každé změny v souborech,

tudíž je včas ohlášeno, že došlo k modifikaci souboru. Díky tomu může být finální dopad na integritu dat značně snížený.

Správa oprávnění je dalších mechanizmem, který pomáhá zajistit integritu systému. Pokud uživatelům udělíme pouze práva ke čtení souborů, jsou tím značně omezeny jejich schopnosti modifikovat chráněná data.

Důležitým mechanizmem pro zajištění integrity je také **logování**, které samo o sobě nedokáže ochránit data před jejich neoprávněnou modifikací, ale takovou událost zaznamená a při zpětném vyšetřování je jednodušší zjistit, jaká data byla modifikována. Kromě toho může být o neoprávněné modifikaci včas upozorněn vlastník daného aktiva.

Zálohování přispívá jak k zajištění integrity, tak dostupnosti dat. Opět jako v předchozím případě ne přímo, ale právě pomocí jednoduchého obnovení původních souborů. Jak bylo zmíněno už u předchozích mechanizmů, není hodnocena kvalita a pravidelnost zálohování, ale pouze jestli je zálohování implementováno, nebo není.

Pro zajištění dostupnosti slouží také funkce **vysoké dostupnosti**. Díky té mohou být servery provozovány ve více než jedné instanci a při výpadku jednoho serveru je provoz přesměrován na druhý (záložní) server.

Posledním mechanizmem, se kterým metodika pracuje, je **ochrana vůči DoS**[11]. Jedná se většinou o specializovaná zařízení, která jsou schopna filtrovat provoz a ponechat ten legitimní.

Ochrana důvěrnosti

V rámci ochrany důvěrnosti je v metodice hodnoceno pět protiopatření způsobem „je implementováno“ nebo „není implementováno“. Dle úrovně možného zajištění důvěrnosti je slovní hodnocení „je implementováno“ hodnoceno číslem 0,8 případně 0,9.

Tabulka 3.12: Protiopatření vztahující se k ochraně důvěrnosti

Protiopatření	**Popis**	**Číselné hodnocení**
Šifrování	Šifrování dat je implementováno.	0,8
	Šifrování dat není implementováno.	1
Řízení přístupu	Pro přístup k systému / datům je nutná autentizace a autorizace uživatele.	0,8
	Autentizace a autorizace uživatele 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

[11] Útok odepřením služby (z anglického „Denial of Service“).

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

Ochrana integrity

Protiopatření vztahující se k zajištění integrity nebo k ochraně integrity jsou hodnocena stejně jako v předchozím případě. V této skupině je hodnoceno opět pět různých protiopatření, která mají vliv na zajištění integrity nebo na její ochranu.

Tabulka 3.13: Protiopatření vztahující se k ochraně integrity

Protiopatření	**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 uživatele.	0,8
	Autentizace a autorizace uživatele 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	Všechny operace s daty jsou logovány a 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.	0,9
	Není implementován proces zálohování.	1

Ochrana dostupnosti

Poslední skupinou jsou protiopatření, která mají vliv na dostupnost systému. Do této skupiny se řadí tři protiopatření – mechanizmus vysoké dostupnosti, zálohování a DoS ochrana.

Tabulka 3.14: Protiopatření vztahující se k ochraně dostupnosti

Protiopatření	**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.	0,8
	Není implementován proces zálohování.	1
DoS ochrana	Je implementována ochrana proti DoS útokům.	0,9
	DoS ochrana není implementována.	1

4 Výpočet priority zranitelnosti

Parametry popisující dopad na CIA triádu zranitelného systému je pro stanovení priority nutné kombinovat s požadavky na tuto triádu. Pro tento účel je výpočet priority zranitelnosti rozdělen na tři fáze:

- stanovení parametrů zranitelnosti,
- stanovení požadavků na CIA triádu,
- výpočet priority zranitelnosti.

4.1 Stanovení parametrů zranitelnosti

Během první fáze se stanoví hodnota všech parametrů popisujících zranitelnost, které byly uvedeny v kapitole 3.2.1. Každému slovnímu ohodnocení odpovídá číselné ohodnocení. Výsledné číselné hodnoty všech parametrů, kromě dopadů na CIA triádu, zapíšeme do množiny.

Definice 4.1 Množinu všech parametrů, které popisují zranitelnost, budeme označovat jako D. Tato množina má přesně 6 prvků[12], protože počet parametrů je přesně daný.

$$D = \{d_1, d_2, \dots, d_6\} \tag{4.1}$$

Každý parametr má stanovenou svoji váhu, aby mohla být zohledněna jejich důležitost. Ta je definována na množině reálných čísel z intervalu $\langle 0, 1 \rangle$. Váha jednotlivých prvků je uvedena v tabulce 4.1.

Tabulka 4.1: Váha jednotlivých parametrů popisujících zranitelnost

Parametr	**Váha**
Threat Intelligence	1
Exploitace	0,8
Dostupnost informací	0,4
Interakce uživatele	0,7
Požadované oprávnění	0,7
Obtížnost zneužití	0,5

Definice 4.2 Množinu váhových hodnot odpovídajícím prvkům množiny parametrů D budeme označovat jako množinu D_W. Tato množina má stejně jako množina D přesně 6 prvků.

$$D_W = \{d_{W_1}, d_{W_2}, \dots, d_{W_6}\} \tag{4.2}$$

[12] Jedná se o parametry *Threat Intelligence*, *Exploitace*, *Dostupnost informací*, *Interakce uživatele*, *Požadované oprávnění* a *Obtížnost zneužití*.

Při hodnocení parametrů popisujících zranitelnost je pro snadnější stanovení hodnoty umožněn výběr pouze z předdefinovaných možností. Každý parametr má přesně uvedené možnosti slovního hodnocení a k nim přiřazenou číselnou hodnotu na intervalu od 0 do 1. Tato hodnota je stejně jako slovní hodnocení přesně daná a neměnná. Možné hodnoty u jednotlivých parametrů jsou sepsány v kapitole 3.2.1.

Kromě výše uvedených parametrů je nutné stanovit také dopad na důvěrnost, integritu a dostupnost zranitelného systému. Možné hodnoty jsou stejně jako u ostatních parametrů předem dané pro jednodušší výběr, protože zde se vychází z popisu zranitelnosti a tyto parametry stanovuje člověk a nikoliv algoritmus. Pro další výpočty je vhodné si tyto tři důležité parametry definovat.

Definice 4.3 Dopad na důvěrnost C je číselné vyjádření možného dopadu na důvěrnost zranitelného systému v případě zneužití zranitelnosti. Je definován prvkem z množiny hodnot $\{0{,}22;\ 0{,}67;\ 0{,}78;\ 1\}$. Vyšší číselné ohodnocení znamená vyšší dopad na důvěrnost.

$$C \in \{0{,}22;\ 0{,}67;\ 0{,}78;\ 1\} \tag{4.3}$$

Definice 4.4 Dopad na integritu I je číselné vyjádření možného dopadu na integritu zranitelného systému v případě zneužití zranitelnosti. Je definován prvkem z množiny hodnot $\{0{,}11;\ 0{,}33;\ 0{,}56;\ 0{,}78;\ 1\}$. Vyšší číselné ohodnocení znamená vyšší dopad na integritu.

$$I \in \{0{,}11;\ 0{,}33;\ 0{,}56;\ 0{,}78;\ 1\} \tag{4.4}$$

Definice 4.5 Dopad na dostupnost A je číselné vyjádření možného dopadu na dostupnost zranitelného systému v případě zneužití zranitelnosti. Je definován prvkem z množiny hodnot $\{0{,}11;\ 0{,}56;\ 0{,}78;\ 1\}$. Vyšší číselné ohodnocení znamená vyšší dopad na dostupnost.

$$A \in \{0{,}11;\ 0{,}56;\ 0{,}78;\ 1\} \tag{4.5}$$

4.2 Stanovení požadavků na CIA triádu

Jakmile máme stanoveny parametry popisující zranitelnost, přichází na řadu definování požadavků na důvěrnost, integritu a dostupnost. Tyto požadavky vycházejí z odpovědí z dotazníku, který je blíže popsán v kapitole 3.3. Pro další výpočty je vhodné si tyto požadavky definovat.

Definice 4.6 Požadavek důvěrnosti C_R je číselné vyjádření požadavku na zajištění důvěrnosti zkoumaného aktiva. Je definován intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší požadavek důvěrnosti.

$$C_R = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.6}$$

Definice 4.7 Požadavek integrity I_R je číselné vyjádření požadavku na zajištění integrity zkoumaného aktiva. Je definován intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší požadavek integrity.

$$I_R = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.7}$$

Definice 4.8 Požadavek dostupnosti A_R je číselné vyjádření požadavku na zajištění dostupnosti zkoumaného aktiva. Je definován intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší požadavek dostupnosti.

$$A_R = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.8}$$

Jak již bylo uvedeno v předešlé kapitole, dotazník je rozdělen do čtyř okruhů. Okruhy zabývající se důvěrností, integritou a dostupností mají maximální počet bodů z dotazníku 15. Okruh obecných otázek má maximální počet bodů roven 4.

Každá otázka má dvě nebo více možných slovních odpovědí, kterým odpovídá předem stanovené číselné hodnocení. To se pohybuje opět na intervalu $\langle 0, 1 \rangle$ nad množinou reálných čísel. Výsledné skóre okruhu se spočítá jako součet číselných hodnocení jednotlivých odpovědí z příslušného okruhu.

$$SkoreOkruhu = \sum CiselneHodnoceniOdpovedi \tag{4.9}$$

Hodnocení všech tří požadavků se spočítá jako podíl součtu skóre z příslušného okruhu a skóre z obecných otázek a maximálního počtu bodů, tedy čísla 19.

$$\begin{aligned} C_R &= \frac{SkoreOtazekDuvernosti + SkoreObecnychOtazek}{19} \\ I_R &= \frac{SkoreOtazekIntegrity + SkoreObecnychOtazek}{19} \\ A_R &= \frac{SkoreOtazekDostupnosti + SkoreObecnychOtazek}{19} \end{aligned} \tag{4.10}$$

Zde však nastává jedna výjimka, a to v případě, že je skóre otázek daného okruhu rovno nule. V tom případě bude i požadavek roven nule.

$$\begin{aligned} &\text{if } (SkoreOtazekDuvernosti == 0) \text{ then } C_R = 0 \\ &\text{if } (SkoreOtazekIntegrity == 0) \text{ then } I_R = 0 \\ &\text{if } (SkoreOtazekDostupnosti == 0) \text{ then } A_R = 0 \end{aligned} \tag{4.11}$$

4.3 Stanovení ohodnocení protiopatření

Poslední částí před konečným výpočtem priority zranitelnosti je stanovení číselného ohodnocení protiopatření. To se promítá do CIA triády, respektive do modifikované verze dopadu na CIA triádu, která zohledňuje i požadavek na zajištění všech tří parametrů. Díky tomu je protiopatření provázáno jak se samotnou zranitelností, tak s aktivem, na kterém je zranitelnost přítomna. Nejdříve si musíme definovat tři hodnoty, se kterými budeme dále pracovat.

Definice 4.9 Ochrana důvěrnosti C_P je číselné vyjádření ochrany důvěrnosti daného aktiva za využití definovaných protiopatření. Tato hodnota je definována intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená menší vliv na míru ochrany důvěrnosti, tedy ve výsledku vyšší prioritu zranitelnosti.

$$C_P = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.12}$$

Definice 4.10 Ochrana integrity I_P je číselné vyjádření ochrany integrity daného aktiva za využití definovaných protiopatření. Tato hodnota je definována intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená menší vliv na míru ochrany integrity, tedy ve výsledku vyšší prioritu zranitelnosti.

$$I_P = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.13}$$

Definice 4.11 Ochrana dostupnosti A_P je číselné vyjádření ochrany dostupnosti daného aktiva za využití definovaných protiopatření. Tato hodnota je definována intervalem $\langle 0, 1 \rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená menší vliv na míru ochrany dostupnosti, tedy ve výsledku vyšší prioritu zranitelnosti.

$$A_P = \langle 0, 1 \rangle \subset \mathbb{R} \tag{4.14}$$

Dotazník pro ohodnocení protiopatření (blíže popsaný v kapitole 3.4) je tvořen 13 položkami rozdělenými do skupin dle parametru CIA triády, jehož ochranu pomáhají zajišťovat.

Ohodnocení ochrany důvěrnosti, integrity a dostupnosti se spočítá jako součin všech číselných hodnot jednotlivých položek v dané skupině.

Jako příklad uveďme hodnocení ochrany důvěrnosti. Do této skupiny spadá pět položek – šifrování, řízení přístupu, firewall, mikrosegmentace a antivirový systém. Z číselných ohodnocení se vytvoří součin a výsledek je míra ochrany důvěrnosti pro dané aktivum.

Pokud číselnou hodnotu protiopatření ze skupiny *důvěrnost* označíme P_{C_i}, kde i je iterátor napříč všemi položkami ve skupině, analogicky hodnotu protiopatření ze skupiny *integrita* označíme P_{I_i} a hodnotu protiopatření ze skupiny *dostupnost* označíme P_{A_i}, pak můžeme vztah pro výpočet ochrany jednotlivých prvků CIA triády spočítat dle následujících vztahů.

$$\begin{aligned} C_P &= P_{C_1} \cdot P_{C_2} \cdot P_{C_3} \cdot P_{C_4} \cdot P_{C_5} \\ I_P &= P_{I_1} \cdot P_{I_2} \cdot P_{I_3} \cdot P_{I_4} \cdot P_{I_5} \\ A_P &= P_{A_1} \cdot P_{A_2} \cdot P_{A_3} \end{aligned} \tag{4.15}$$

4.4 Výpočet priority zranitelnosti

Jakmile máme stanovené hodnoty parametrů popisujících zranitelnost i požadavky na zajištění CIA triády zranitelného systému, můžeme přistoupit k finálnímu výpočtu priority. Nejdříve se spočítá skóre zranitelnosti, do kterého v tuto chvíli ještě není započítaný dopad na CIA triádu. To se počítá jako součet všech parametrů násobených jejich váhou.

Definice 4.12 Skóre zranitelnosti S je číselné vyjádření parametrů zranitelnosti, které ovlivňují její prioritu. Je definováno jako součin prvků množiny D a k nim odpovídající váhy z množiny D_W viz definice 4.1 a 4.2.

$$S = \sum_{i=1}^{6} D_i D_{W_i} \tag{4.16}$$

Jakmile máme vypočítané skóre zranitelnosti, musíme spočítat modifikovaný dopad na jednotlivé parametry CIA triády. To znamená provázat hodnotu požadavků důvěrnosti, integrity a dostupnosti s dopadem určeným při hodnocení zranitelnosti a s ochranou těchto parametrů, kterou poskytují implementovaná opatření. Tento modifikovaný dopad se spočítá jako součin dopadu, požadavku na daný parametr a míry ochrany.

Definice 4.13 Modifikovaný dopad na důvěrnost C_M je číselné vyjádření možného dopadu na důvěrnost zranitelného systému v případě zneužití zranitelnosti, do kterého už je

započítán i požadavek důvěrnosti C_R a ochrana důvěrnosti C_P. Je definován intervalem $\langle 0, 1\rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší dopad na důvěrnost.

$$\begin{aligned} C_M &= \langle 0, 1\rangle \subset \mathbb{R} \\ C_M &= C \cdot C_R \cdot C_P \end{aligned} \tag{4.17}$$

Definice 4.14 Modifikovaný dopad na integritu I_M je číselné vyjádření možného dopadu na integritu zranitelného systému v případě zneužití zranitelnosti, do kterého už je započítán i požadavek integrity I_R a ochrana integrity I_P. Je definován intervalem $\langle 0, 1\rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší dopad na integritu.

$$\begin{aligned} I_M &= \langle 0, 1\rangle \subset \mathbb{R} \\ I_M &= I \cdot I_R \cdot I_P \end{aligned} \tag{4.18}$$

Definice 4.15 Modifikovaný dopad na dostupnost A_M je číselné vyjádření možného dopadu na dostupnost zranitelného systému v případě zneužití zranitelnosti, do kterého už je započítán i požadavek dostupnost A_R a ochrana dostupnosti A_P. Je definován intervalem $\langle 0, 1\rangle$ nad množinou reálných čísel. Vyšší číselné ohodnocení znamená vyšší dopad na dostupnost.

$$\begin{aligned} A_M &= \langle 0, 1\rangle \subset \mathbb{R} \\ A_M &= A \cdot A_R \cdot A_P \end{aligned} \tag{4.19}$$

Následně můžeme spočítat modifikované skóre zranitelnosti, které už zohledňuje i modifikované dopady na prvky CIA triády.

Definice 4.16 Modifikované skóre zranitelnosti S_M je číselné vyjádření parametrů zranitelnosti, které ovlivňují její prioritu. Místo parametrů důvěrnosti, integrity a dostupnosti je zde počítáno s jejich modifikovanými verzemi, které zohledňují také požadavek na tyto parametry z hlediska priority aktiva a míru ochrany zajišťovanou implementovanými protiopatřeními. Modifikované skóre je definováno jako součin skóre zranitelnosti a součtu všech modifikovaných parametrů CIA triády.

$$S_M = S \cdot (C_M + I_M + A_M) \tag{4.20}$$

Nyní už můžeme definovat a následně stanovit výslednou prioritu zranitelnosti.

Definice 4.17 Priorita zranitelnosti P je číselné vyjádření závažnosti zranitelnosti z hlediska nutnosti jejího odstranění. Je definovaná intervalem $\langle 0, 1000\rangle$ nad množinou celých čísel. Vyšší číselné ohodnocení znamená vyšší prioritu.

$$P = \langle 0, 1000 \rangle \subset \mathbb{R} \tag{4.21}$$

Priorita zranitelnosti se vypočítá jako poměr modifikovaného skóre zranitelnosti se vůči maximálnímu možnému skóre. Maximální skóre v této metodice je hodnota 12,3. Výsledek se ještě vynásobí tisíci pro lepší prioritizaci bez desetinných čísel a je zaokrouhlen na celé číslo.

$$P = \frac{S_M}{12{,}3} \cdot 1000 \tag{4.22}$$

Pro lepší orientaci ve výpočtu finální priority zranitelností je níže v rovnici 4.23 uveden kompletní vzorec pro výpočet priority.

$$P = \frac{\sum_{i=1}^{6} D_i D_{W_i} \cdot (C \cdot C_R \cdot C_P + I \cdot I_R \cdot I_P + A \cdot A_R \cdot A_P)}{12{,}3} \cdot 1000 \tag{4.23}$$

4.5 Příklad výpočtu – CVE-2019-0708

V této kapitole si ukážeme příklad výpočtu na konkrétní zranitelnosti označené jako CVE-2019-0708[13]. Jedná se o zranitelnost ve službě Remote Desktop Service, která umožňuje útočníkovi bez nutnosti autentizace spustit vlastní kód tak, že se připojí k cíli pomocí RDP (Remote Desktop Protocol)[14] a pošle speciálně upravené požadavky na připojení [25]. Kód, který si útočník spustí, pak bude spuštěn s plnými právy.

Stanovení skóre zranitelnosti je možné na základě dokumentace Microsoftu, výzkumných zpráv a databáze zranitelností NVD (National Vulnerability Database[15]) [26]. Skóre zranitelnosti je vidět v tabulce 4.2.

Tabulka 4.2: Hodnocení parametrů popisujících zranitelnost CVE-2019-0708

Parametr	**Hodnota**	**Číselné hodnocení**
Threat Intelligence	Není definováno	0,5
Exploitace	Pomocí automatizovaných nástrojů	1
Dostupnost informací	Veřejně známé	1
Interakce uživatele	Žádná	1
Požadované oprávnění	Žádná	1
Obtížnost zneužití	Nízká	0,78

[13] Označení CVE (Common Vulnerabilities and Exposures) se používá jako jednoznačný identifikátor zranitelnosti v téměř všech databázích zranitelností včetně National Vulnerability Database. Tento systém identifikátorů spravuje společnost MITRE Corporation.

[14] Remote Desktop Protocol je název protokolu pro připojení ke vzdálené ploše. Nejčastěji je využíván v operačních systémech Microsoft Windows.

[15] National Vulnerability Database je databáze zranitelností provozována americkou vládou.

Dopad na důvěrnost	Odcizení všech dat	1
Dopad na integritu	Úplné poškození všech dat	1
Dopad na dostupnost	Úplná nedostupnost všech služeb	1

1. Stanovíme si nejdříve množinu parametrů popisujících zranitelnost (kromě dopadu na CIA triádu) a následně množinu váhových hodnot k těmto parametrům.

$$\begin{aligned} D &= \{0{,}5; 1; 1; 1; 1; 0{,}78\} \\ D_W &= \{1; 0{,}8; 0{,}4; 0{,}7; 0{,}7; 0{,}5\} \end{aligned} \tag{4.24}$$

2. Následně určíme dopad na důvěrnost, integritu a dostupnost.

$$\begin{aligned} C_R &= 1 \\ I_R &= 1 \\ A_R &= 1 \end{aligned} \tag{4.25}$$

3. Stanovíme požadavky na CIA triádu.

   Pro stanovení požadavků na CIA triádu musíme znát systém, na kterém je zranitelnost přítomna. V tomto případě budeme předpokládat, že zranitelnost se nachází na systému v interní síti, na kterém se nachází účetní software. Zaměstnanci z finančního oddělení na něj přistupují každý den pro vystavení faktur právě pomocí RDP protokolu. Jelikož se nejedná o velkou firmu, mají pouze jeden server s účetním systémem, u kterého není zajištěna vysoká dostupnost, ačkoliv může být požadována. Uložená data se pravidelně na konci měsíce zálohují na zálohovací servery. Dále předpokládejme, že společnost má do stovky zaměstnanců a její zákazníci jsou výrobní společnosti po celém světě. Z výše uvedeného popisu jsme schopni vyplnit dotazník týkající se priority aktiva. Vyplněný dotazník je uveden v příloze B.

   Na základě dotazníku jsme byli schopni stanovit prioritu aktiva, respektive požadavky na důvěrnost, integritu a dostupnost následovně.

   Důvěrnost

$$\begin{aligned} C_R &= \frac{12{,}5 + 2{,}8}{19} \\ C_R &= 0{,}81 \end{aligned} \tag{4.26}$$

   Integrita

$$\begin{aligned} I_R &= \frac{13 + 2{,}8}{19} \\ I_R &= 0{,}83 \end{aligned} \tag{4.27}$$

Dostupnost

$$A_R = \frac{6{,}5 + 2{,}8}{19}$$
$$A_R = 0{,}49 \tag{4.28}$$

4. Dále ohodnotíme implementovaná protiopatření.

   Pro číselné ohodnocení ochrany důvěrnosti, integrity a dostupnosti můžeme opět využít dotazník hodnotící implementovaná protiopatření. Předpokládejme stejný systém jako v předchozím kroku, protože se nachází v interní síti, je oddělený firewallem a kromě základních firewallových prostupů je povolen ještě protokol RDP. Data uložená na serveru jsou šifrována pomocí technologie File Level Encryption[16]. Pro uživatele přistupující přes RDP je nastaveno základní řízení přístupu dle skupiny v Active Directory, ve které se nachází. Jak bylo uvedeno už v bodě výše, data na serveru jsou pravidelně zálohována. Z popisu aktiva a protiopatření jsme schopni vyplnit dotazník, díky kterému můžeme stanovit míru ochrany CIA triády. Vyplněný dotazník je uveden v příloze B.

   Na základě dotazníku jsme schopni stanovit hodnoty ochrany důvěrnosti, integrity a dostupnosti.

   Důvěrnost

$$C_P = 0{,}8 \cdot 0{,}8 \cdot 0{,}9 \cdot 1 \cdot 1$$
$$C_P = 0{,}58 \tag{4.29}$$

   Integrita

$$I_P = 1 \cdot 0{,}8 \cdot 1 \cdot 1 \cdot 0{,}9$$
$$I_P = 0{,}72 \tag{4.30}$$

   Dostupnost

$$A_P = 1 \cdot 0{,}8 \cdot 1$$
$$A_P = 0{,}80 \tag{4.31}$$

5. Dalším krokem je výpočet skóre zranitelnosti.

$$S = 0{,}75 \cdot 1 + 1 \cdot 0{,}8 + 1 \cdot 0{,}4 + 1 \cdot 0{,}7 + 1 \cdot 0{,}7 + 0{,}78 \cdot 0{,}5$$
$$S \doteq 3{,}489 \tag{4.32}$$

[16] Tato technologie šifrování umožňuje šifrovat pouze konkrétní soubory a složky. Nejedná se tedy o šifrování celého disku (jak pracuje například technologie BitLocker), ale zašifruje předem vybrané soubory a adresáře.

6. Nyní určíme modifikované dopady na CIA triádu pomocí hodnoty dopadu na parametr CIA triády, požadavku systému na tento parametr a míry ochrany.

Důvěrnost

$$\begin{aligned} C_M &= 1 \cdot 0{,}81 \cdot 0{,}58 \\ C_M &= 0{,}47 \end{aligned} \tag{4.33}$$

Integrita

$$\begin{aligned} I_M &= 1 \cdot 0{,}83 \cdot 0{,}72 \\ I_M &= 0{,}60 \end{aligned} \tag{4.34}$$

Dostupnost

$$\begin{aligned} A_M &= 1 \cdot 0{,}49 \cdot 0{,}80 \\ A_M &= 0{,}39 \end{aligned} \tag{4.35}$$

7. V tomto okamžiku už můžeme určit modifikované skóre zranitelnosti.

$$\begin{aligned} S_M &= 3{,}489 \cdot (0{,}47 + 0{,}60 + 0{,}39) \\ S_M &\doteq 7{,}077 \end{aligned} \tag{4.36}$$

8. Posledním krokem je určení výsledné priority zranitelnosti.

$$\begin{aligned} P &= \frac{7{,}077}{12{,}3} \cdot 1000 \\ \underline{P &\doteq 575} \end{aligned} \tag{4.37}$$

Oproti skóre CVSSv3, které zranitelnost hodnotí 9,8 body z 10, se může zdát, že zde navržená metoda nedostačuje. Naopak však lépe prioritizuje, protože zranitelností, které mají dle CVSS kritickou závažnost, je obrovské množství (viz úvodní kapitola). V navržené metodě je navíc zohledněn i požadavek na zajištění důvěrnosti, integrity a dostupnosti a dále implementovaná protiopatření.

5 Teoretické porovnání navržené metody a CVSSv3

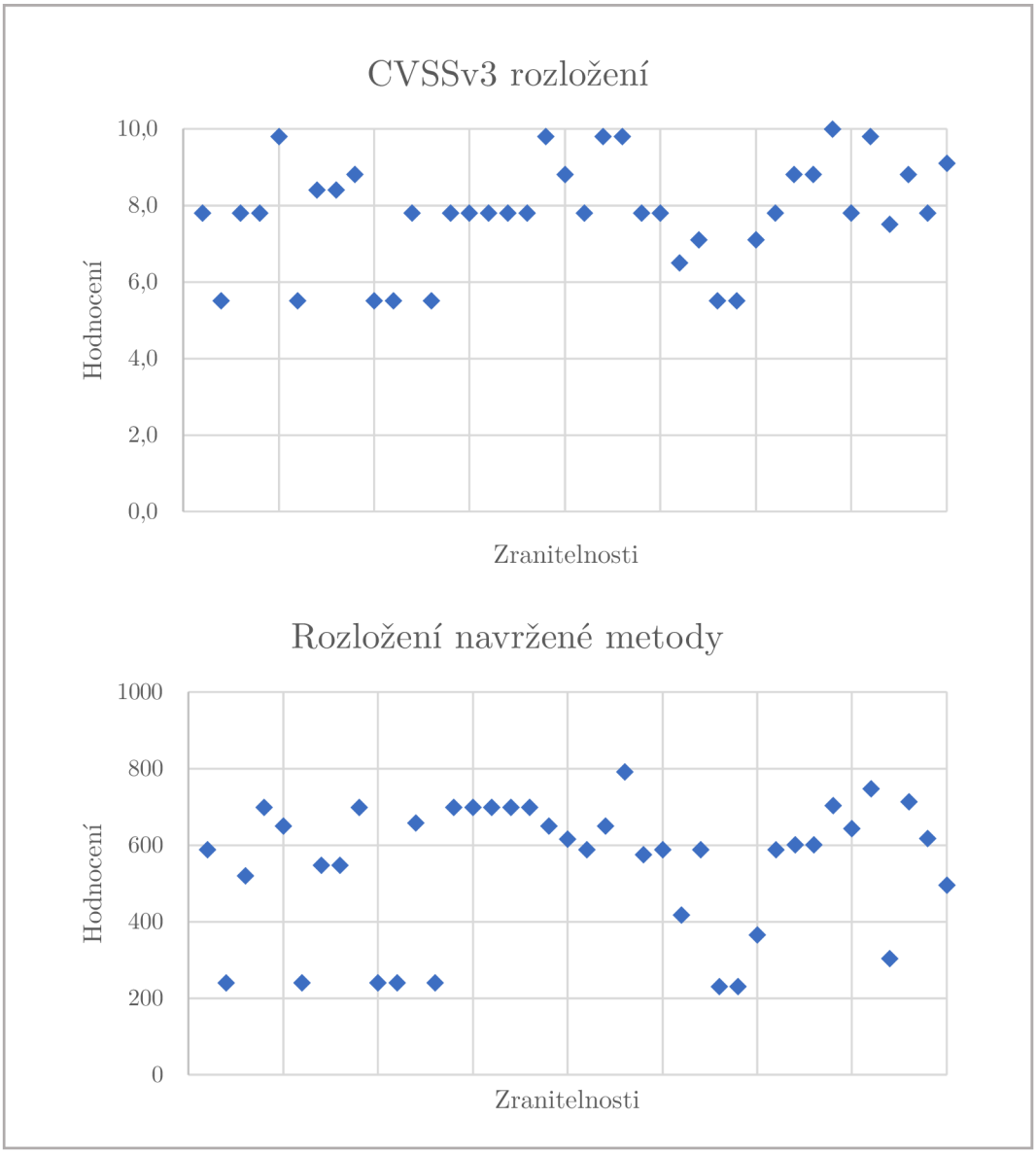
V této kapitole se podíváme na teoretické porovnání dnes běžně používané metody hodnocení zranitelností CVSS verze 3 a navržené metody. Dále v kapitole jsou uvedena dvě srovnání. První se zabývá srovnáním samotného hodnocení zranitelností bez zaměření na prioritizaci aktiva, tedy nebere ohled na požadavky na zajištění důvěrnosti, integrity a dostupnosti. Druhé srovnání už hodnotí efektivitu metody samotné, tedy srovnání hodnocení stejných zranitelností na několika systémech, které všechny mají různé požadavky na zajištění CIA triády.

5.1 Srovnání hodnocení zranitelností navržené metody a CVSSv3

První srovnání se zabývá hodnocením dle navržené metody a dle CVSS verze 3. Je hodnoceno 40 různých zranitelností nově objevených v roce 2019, jejich výběr byl postupný tak, jak byly publikovány od 1. ledna 2019 v databázi zranitelností NVD. Předpokládáme přítomnost všech zranitelností na systému s maximálními požadavky na zajištění důvěrnosti, integrity a dostupnosti, tedy číslem 1,00 u všech třech parametrů. Stejně tak předpokládáme, že není implementováno žádné protiopatření, tedy i hodnoty ochrany důvěrnosti, integrity a dostupnosti bez vlivu na výslednou prioritu.

Hodnocení zranitelností jak dle CVSS tak dle navržené metody, konkrétní číselné ohodnocení a výslednou prioritu lze najít v příloze C. Při číselném ohodnocení zranitelností pro účely tohoto srovnání se vycházelo z veřejně dostupných informací o zranitelnostech, konkrétně se jednalo o databázi NVD, ExploitDB pro určení možnosti exploitace a databáze zranitelností společnosti Tenable, která obsahuje odkazy na zprávy a reporty zabývající se těmito zranitelnostmi. Hodnota parametru Threat Intelligence byla u všech zranitelností ponechána jako „není definováno“ a počítalo se tedy s číslem 0,5.

Na níže uvedených grafech na obrázku 5.1 je možné najít korelaci mezi hodnocením dle navržené metody a dle CVSS. Účelem těchto grafů je ale poukázat na to, že u navržené metody je stále možné zvýšit prioritu zranitelností (například pomocí vynechaného parametru Threat Intelligence) a stejně tak ji snížit v případě nižších požadavků na zajištění důvěrnosti, integrity a dostupnosti nebo v případě implementace některého z možných protiopatření.



Obrázek 5.1: Srovnání hodnocení zranitelností dle CVSS metody a dle navržené metody

5.2 Srovnání hodnocení zranitelností na systémech s různou prioritou

Druhým srovnáním je priorita čtyř různých zranitelností na čtyřech různých systémech s různými požadavky na zajištění CIA triády. První zkoumaný systém má maximální požadavky na zajištění všech parametrů CIA triády, nebyla tedy uvedena žádná prioritizace aktiva. Druhý systém je účetní server, který byl uveden již v kapitole 4.4 a má určité požadavky na všechny tři parametry. Třetím aktivem je webový server, který má požadavky pouze na dostupnost, a posledním systémem je zálohovací server s požadavky na důvěrnost a integritu. Požadavky na jednotlivé parametry jsou uvedeny v tabulce 5.1. Vyplněné dotazníky, na základě kterých bylo hodnocení aktiva stanoveno, jsou uvedeny v příloze D.

Tabulka 5.1: Zkoumaná aktiva a jejich požadavky na zajištění CIA triády

Aktivum	**Požadavek na důvěrnost**	**Požadavek na integritu**	**Požadavek na dostupnost**
Bez prioritizace	1,00	1,00	1,00
Účetní server	0,81	0,83	0,49
Webový server	0,00	0,00	0,34
Zálohovací server	0,67	0,48	0,00

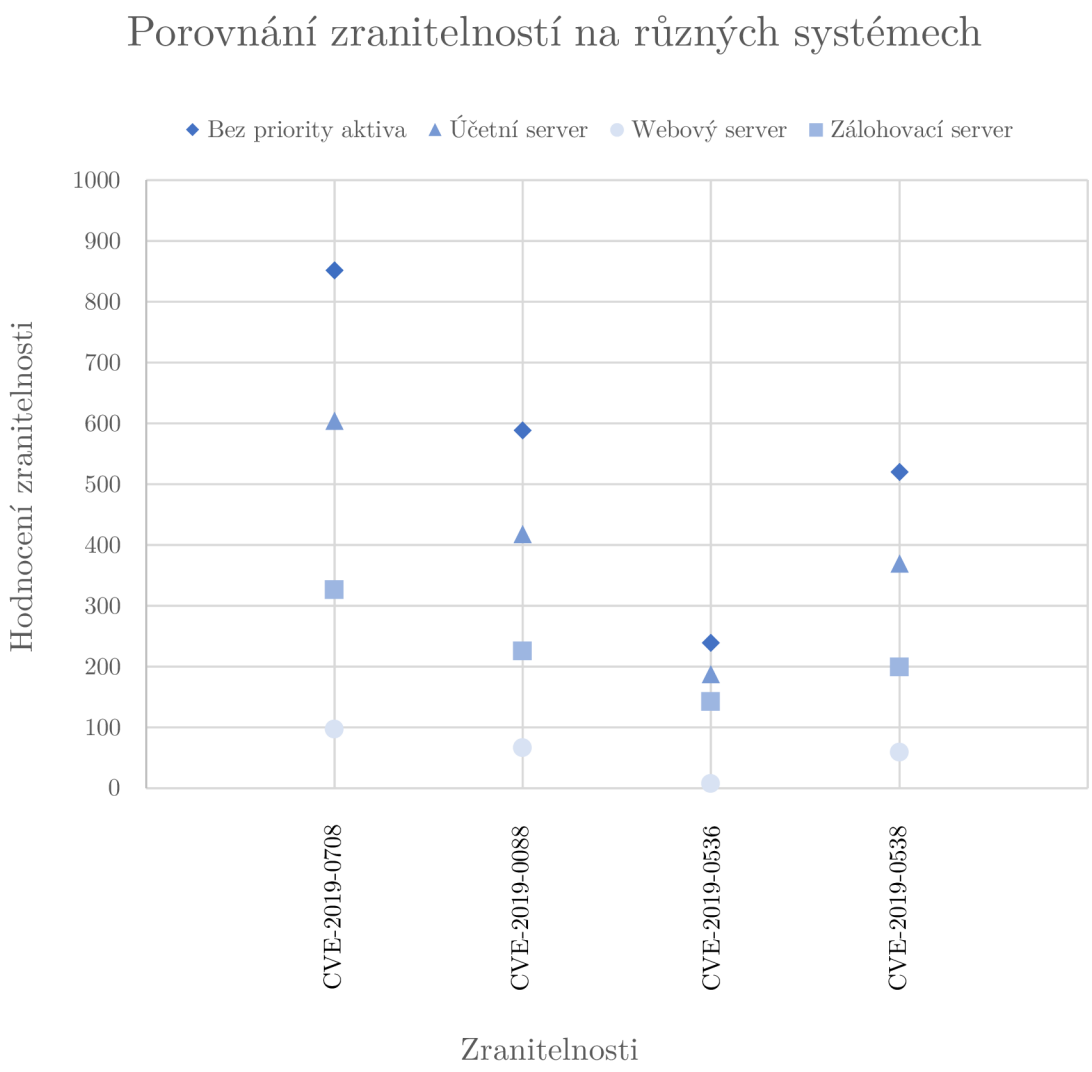
Zranitelnosti použité pro toto porovnání jsou čtyři náhodně vybrané. Jejich číselné ohodnocení použité v metodice je uvedeno v tabulce 5.2.

Tabulka 5.2: Hodnocené zranitelnosti při srovnání metody

Zranitelnost	**Threat Intelligence**	**Exploitace**	**Dostupnost informací**	**Interakce uživatele**	**Požadovaná oprávnění**
CVE-2019-0708	0,50	1,00	1,00	1,00	1,00
CVE-2019-0088	0,50	0,11	0,44	1,00	0,80
CVE-2019-0536	0,50	0,11	0,44	1,00	0,80
CVE-2019-0538	0,50	0,11	0,44	0,40	1,00

Zranitelnost	**Obtížnost zneužití**	**Dopad na důvěrnost**	**Dopad na integritu**	**Dopad na dostupnost**
CVE-2019-0708	0,78	1,00	1,00	1,00
CVE-2019-0088	0,78	1,00	1,00	1,00
CVE-2019-0536	0,78	1,00	0,11	0,11
CVE-2019-0538	0,78	1,00	1,00	1,00

Na obrázku 5.1 je uveden graf, který znázorňuje výše popsané srovnání a z nějž vyplývá, že prioritizace aktiva, respektive ohodnocení požadavku na zajištění důvěrnosti, integrity a dostupnosti, je důležitou a nedílnou součástí prioritizace zranitelnosti. Díky tomuto může dojít ke snížení priority vzhledem k tomu, že její dopad nemusí souviset s účelem aktiva.



Obrázek 5.2: Porovnání zranitelností na systémech s různými požadavky na zajištění CIA triády

5.3 Srovnání hodnocení zranitelností s různými implementovanými protiopatřeními

Třetí teoretické srovnání hodnotí efektivitu při zohledňování implementovaných protiopatření. Porovnává stejné zranitelnosti na stejných systémech, ale tentokrát s různým počtem a typem mechanizmů a nástrojů, které mají vliv na ochranu CIA triády.

Stejně jako v předchozím případě jsou hodnoceny čtyři různé zranitelnosti ve čtyřech různých případech, kdy jsou implementována různá protiopatření. V prvním případě není implementováno žádné protiopatření pro zajištění CIA triády. V druhém máme implementováno šifrování a zálohování dat, tedy běžné dva způsoby ochrany. Ve třetím případě nám k těmto dvěma mechanizmům přibude ještě firewall, řízení přístupu a správa oprávnění. V posledním

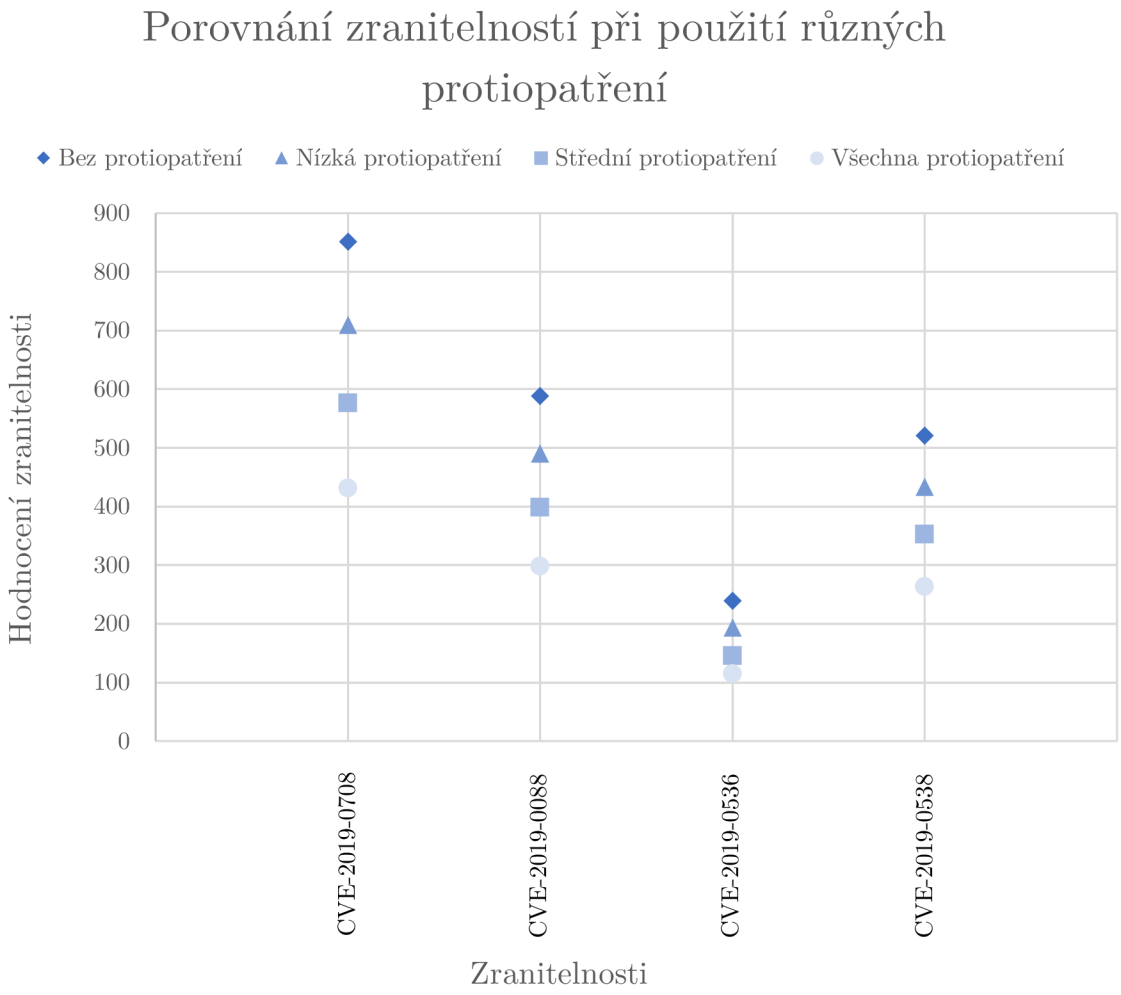
případě jsou implementována všechna protiopatření, která jsou popsána v kapitole 3.4. Hodnoty zajištění ochrany jednotlivých prvků CIA triády je možné vidět v tabulce 5.2, kde nižší hodnota znamená efektivnější protiopatření.

Tabulka 5.3: Vliv různých protiopatření na míru ochrany prvků CIA triády

Protiopatření	**Priorita po započítání ochrany důvěrnosti**	**Priorita po započítání ochrany integrity**	**Priorita po započítání ochrany dostupnosti**
Bez protiopatření	1,00	1,00	1,00
Šifrování a zálohování	0,80	0,90	0,80
Šifrování, zálohování, firewall, řízení přístupu a správa oprávnění	0,58	0,65	0,80
Všechna protiopatření	0,47	0,47	0,58

Pro porovnání jsou opět zvoleny zranitelnosti jako v předchozí kapitole, viz tabulka 5.2. V teoretickém srovnání je možné vidět, že implementovaná protiopatření značně snižují výslednou prioritu zranitelnosti. Vzhledem k tomu, že jsou protiopatření provázána jak s požadavkem na zajištění CIA triády, tak s dopadem na CIA triádu, u všech zranitelností ovlivňují protiopatření výslednou prioritu jiným způsobem a tím pádem se projevují i jinou číselnou hodnotou. Na níže uvedeném grafu 5.3 jsou srovnány čtyři různé zranitelnosti a jejich výsledná priorita dle implementovaných protiopatření. V reálné síti tak budou zvýhodněny ty zranitelnosti (budou mít vyšší prioritu), které budou na systémech bez ochrany, kde nejsou data šifrována, neprobíhají zálohy a další.

Základní předpoklad pro lepší prioritizaci, tedy hodnocení priority aktiva (respektive požadavku na zajištění důvěrnosti, integrity a dostupnosti) je v metodě obsažen. Stejně tak druhá hlavní část, hodnocení protiopatření, ovlivňuje výslednou prioritu zranitelnosti. Všechny tři výše uvedená teoretická srovnání ukazují, že metoda nejen že z technického hlediska hodnotí zranitelnosti podobně jako například CVSSv3 (protože je založena na stejných faktorech) a v tomto ohledu ji můžeme použít pro hodnocení zranitelností, ale dále ještě lépe prioritizuje díky vztahu mezi zranitelností, zranitelným systémem a implementovaným protiopatřením.



Obrázek 5.3: Porovnání zranitelností na systémech s různými implementovanými protiopatřeními

6 Výsledky testování navržené metody

Teoretické srovnání v předchozí kapitole ukázalo silné stránky metody, které se by měly projevit i používání v praxi. Z toho důvodu bude v této kapitole ukázáno ověření metody na reálném prostředí. Metoda byla implementována do prostředí středně velké firmy, jejíž základní infrastrukturu tvoří zhruba 30 serverů a dalších 200 koncových stanic. Výsledky tohoto ověření byly v souladu s očekáváním. Možnost prioritizace na základě implementovaných protiopatření a kritičnosti aktiva z hlediska požadavků na zajištění CIA triády značně ovlivnila výsledné skóre detekovaných zranitelností.

Protože není možné výsledky z této reálné sítě publikovat, navržená metoda byla otestována na malém laboratorním prostředí, které obsahovalo velmi zjednodušenou podobnou infrastrukturu jako při pilotním testování v reálném prostředí. Laboratorní prostředí se skládá ze čtyř různých systémů, které jsou dále popsány níže. Všechny tyto systémy obsahovaly stejné zranitelnosti, které byly detekovány i v reálném prostředí.

6.1 Testované systémy

Laboratorní prostředí tvořily čtyři různé systémy – tři servery a jeden desktopový systém. Serverové systémy s operačními systémy Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2 a CentOS 7 představují základní infrastrukturu. Jedná se o servery zajišťující interní portál firmy běžící na Microsoft IIS, databázový server Microsoft SQL obsahující data o zaměstnancích, zákaznících a běžících projektech a poslední server s operačním systémem CentOS 7 s webovým serverem Apache, který zajišťuje běh webových stránek firmy. Čtvrtým systémem je desktopový operační systém Windows 10, který reprezentuje vzorek koncových stanic a notebooků běžných uživatelů.

6.1.1 Webový server IIS

Webový server IIS běžící na Windows Server 2016 zajišťuje provoz intranetového portálu, přes který zaměstnanci firmy přistupují ke všem firemním datům. Tento portál má několik částí, z čehož ty nejdůležitější jsou HR část (z anglického *human resources* neboli oddělení lidských zdrojů), projektová část a obchodní část. Pro HR oddělení je přístupná HR část, která umožňuje přístup k informacím o zaměstnancích jako jsou osobní údaje (jméno, datum narození, informace potřebné pro vedení zaměstnaneckého poměru, výše platu...), pozice zaměstnance ve firmě, zápisy z pravidelných pohovorů s nadřízeným a podobně. Projektová část portálu zpřístupňuje informace o aktuálních i minulých projektech a jsou skrze ni dostupné smlouvy k projektům a další důležité údaje. Nabídky, finanční zprávy, ekonomika firmy a další jsou dostupné obchodnímu oddělení a managementu firmy přes obchodní část portálu.

Tento systém leží v interní síti firmy za perimetrovým firewallem a od ostatních částí sítě je také oddělený interním firewallem. Samozřejmostí je řízení přístupu a nastavení oprávnění pro přistupující uživatele, veškerá aktivita na systému je logována. Z hlediska běžné ochrany není na serveru provozován žádný antivirový program.

Samotný systém není úložištěm výše uvedených dat. Tato data jsou uložena na databázovém serveru, který zároveň funguje jako souborový server a je popsaný v další části.

6.1.2 Databázový server

Všechna data přístupná přes interní portál firmy jsou uložena na databázovém serveru s operačním systémem Windows Server 2012 R2 a databázovým systémem Microsoft SQL Server. Tento systém zároveň funguje jako sdílené úložiště. K databázi ani k uloženým souborům nepřistupují uživatelé napřímo, ale právě za využití výše popsaného webového serveru s intranetovým portálem.

Stejně jako webový server IIS leží i tento server v oddělené části sítě za interním firewallem. Opět je zde řízení přístupu a správa oprávnění napřímo přistupujících účtů, veškeré aktivity jsou logovány. Databáze i adresáře sdíleného úložiště jsou v pravidelných intervalech zálohovány na zálohovací server, který je dále na měsíční bázi zálohován na offline úložiště.

6.1.3 Webový server Apache

Server s operačním systémem CentOS 7 a webovým serverem Apache zajišťuje provoz webových stránek firmy. Web je určen pouze pro prezentaci firmy, nejsou na něm uložena žádná důležitá ani citlivá data. Z tohoto důvodu tak není požadována žádná důvěrnost uložených dat. Co se týká integrity a dostupnosti systému, zajištění těchto položek CIA triády je důležité pouze pro marketingové účely firmy. I z tohoto důvodu z hlediska požadavků na zajištění CIA triády je aktivum hodnoceno jako nekritické.

Systém leží ve firewallem oddělené DMZ zóně bez přístupu do interní sítě. Správa webových stránek probíhá přímo na daném serveru přes rozhraní samotného operačního systému, neboť webové stránky se mění jen jednou ročně. Jediná protiopatření, která jsou na tomto systému implementována, jsou řízení přístupu a logování aktivity.

6.1.4 Uživatelský systém

Vzorek koncových stanic a notebooků uživatelů v našem testování reprezentuje desktopový systém Windows 10. Většinou se jedná o notebooky uživatelů, kteří často cestují a jsou tedy mimo interní síť. Běžnou náplní práce uživatelů je zpracování zákaznicích dat. Uživatelům není bráněno v instalaci jakéhokoliv softwaru, na svých noteboocích mají práva lokálního administrátora. Z tohoto důvodu je z hlediska jednotného softwaru značná roztříštěnost napříč firmou, což zvyšuje celkový počet zranitelností a ztěžuje patchování systémů, které provádějí sami uživatelé.

Kvůli citlivým datům, která jsou dočasně na uživatelských systémech uchovávána, je nařízeno šifrovat zákaznická data pomocí nástroje na šifrování souborů a složek. Dále je na všech zařízeních instalován antivirový program, samozřejmostí je také řízení přístupu a logování aktivity.

6.2 Průběh testování

Před samotným ohodnocením detekovaných zranitelností bylo nutné vyplnit formuláře, ze kterých vyplynula priorita aktiva, respektive požadavky na zajištění CIA triády a úroveň protiopatření. Tyto hodnoty poté budou ovlivňovat technické ohodnocení zranitelností.

Zranitelnosti na celém laboratorním prostředí byly skenovány pomocí nástroje Nessus Professional, respektive s nástavbou Tenable.sc, která dále umožňuje zjistit detailnější informace o detekovaných zranitelnostech. Parametry Threat Intelligence a Dostupnost informací, které jsou v metodě používány, vycházejí právě z dostupných dat nástroje Tenable.sc, který tyto informace sbírá ze služeb Threat Intelligence třetích stran. Při reálném použití v praxi se může jako zdroj informací pro tyto dva parametry zvolit libovolná služba Threat Intelligence.

6.3 Výsledky testování

V tabulkách 6.1 a 6.2 níže jsou uvedeny číselné hodnoty požadavků na zajištění CIA triády pro všechny čtyři typy systémů a také číselné hodnoty reflektující implementovaná protiopatření. Kompletní vyplněné dotazníky hodnocení aktiva a hodnocení protiopatření jsou uvedené v příloze E.

Tabulka 6.1: Priorita aktiv v laboratorním prostředí

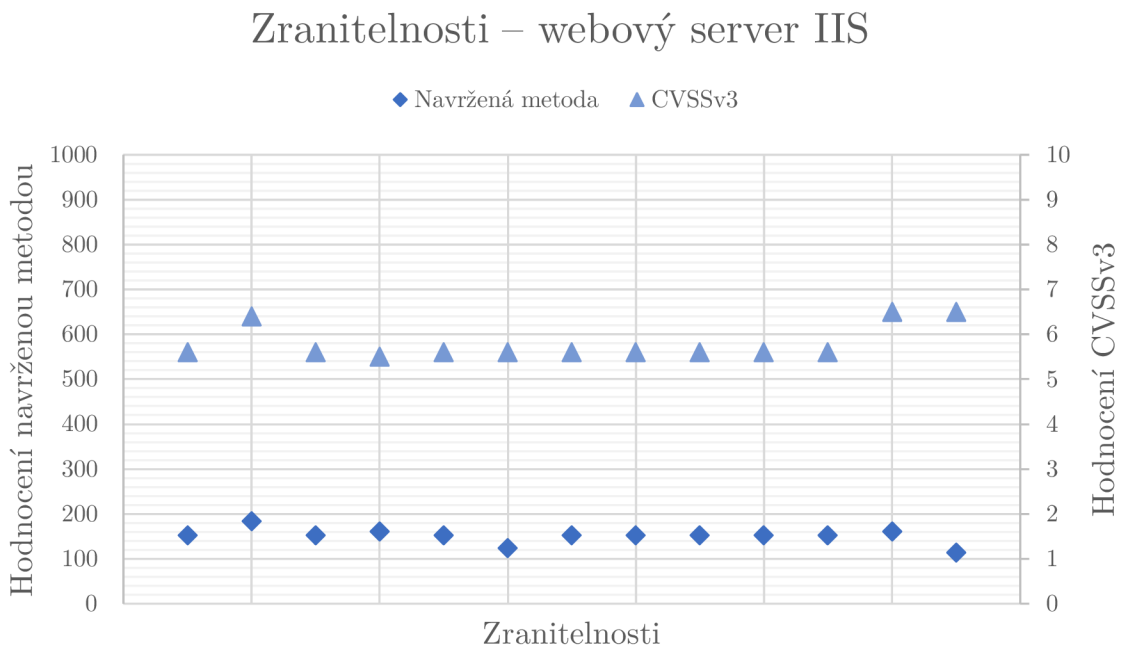
Aktivum	**Požadavek na důvěrnost**	**Požadavek na integritu**	**Požadavek na dostupnost**
Webový server IIS	0,75	0,45	0,51
Databázový server	0,75	0,45	0,51
Webový server Apache	0,00	0,38	0,46
Uživatelský systém	0,76	0,40	0,32

Tabulka 6.2: Implementovaná protiopatření na systémech v laboratorním prostředí

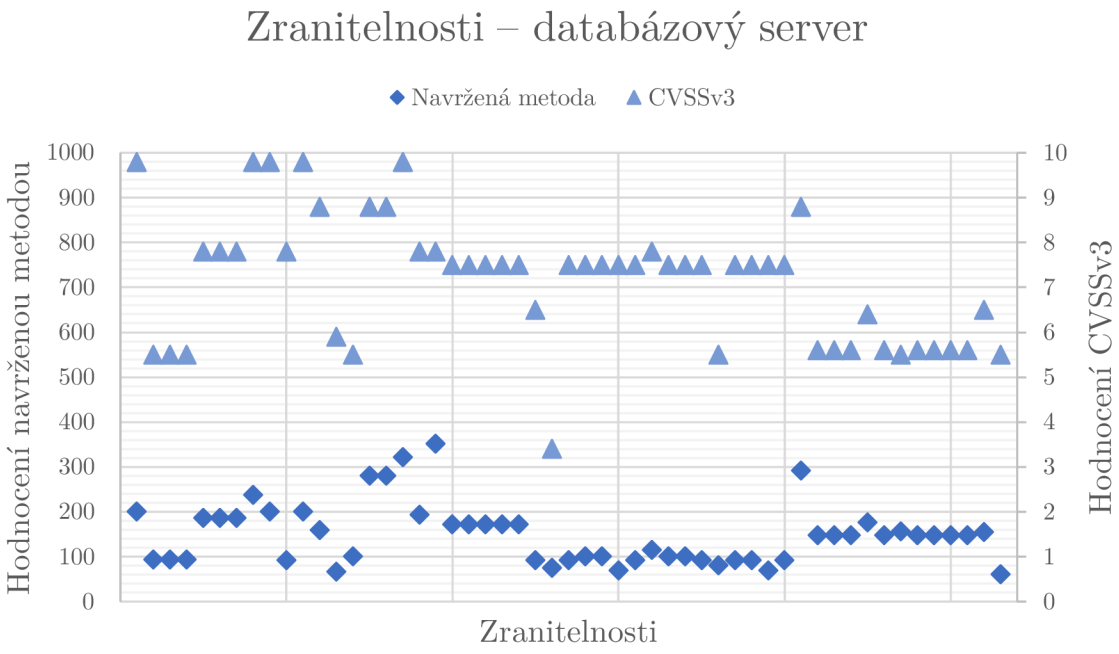
Aktivum	**Priorita po započítání ochrany důvěrnosti**	**Priorita po započítání ochrany integrity**	**Priorita po započítání ochrany dostupnosti**
Webový server IIS	0,72	0,65	1,00
Databázový server	0,72	0,58	0,80
Webový server Apache	0,72	0,72	1,00
Uživatelský systém	0,58	0,72	1,00

Na těchto systémech s výše uvedenou prioritou aktiva a po započítání implementovaných opatření, které poskytují ochranu prvků CIA triády, byl proveden sken zranitelností a zranitelnosti byly ohodnoceny jak pomocí CVSSv3, což umožňoval samotný skener zranitelností, tak pomocí navržené metody.

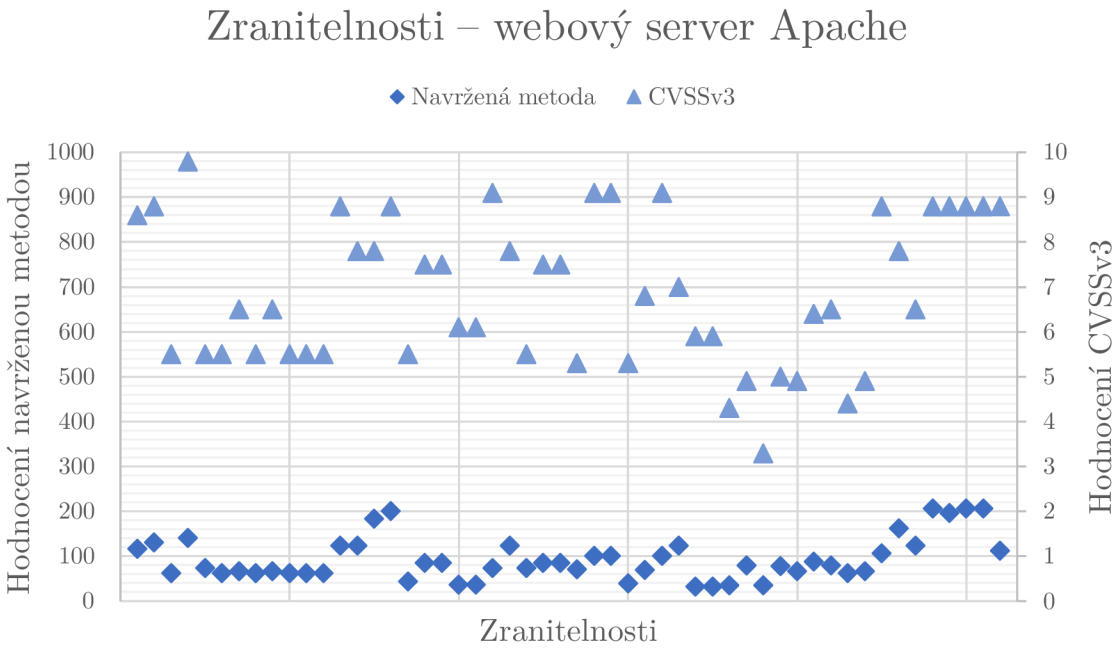
Kompletní přehled detekovaných zranitelností a jejich hodnocení jak pomocí navržené metody, tak pomocí CVSSv3, je uvedený v příloze E. Pro srovnání metody jsou data zanesena do grafů 6.1 až 6.4 dle jednotlivých systémů.



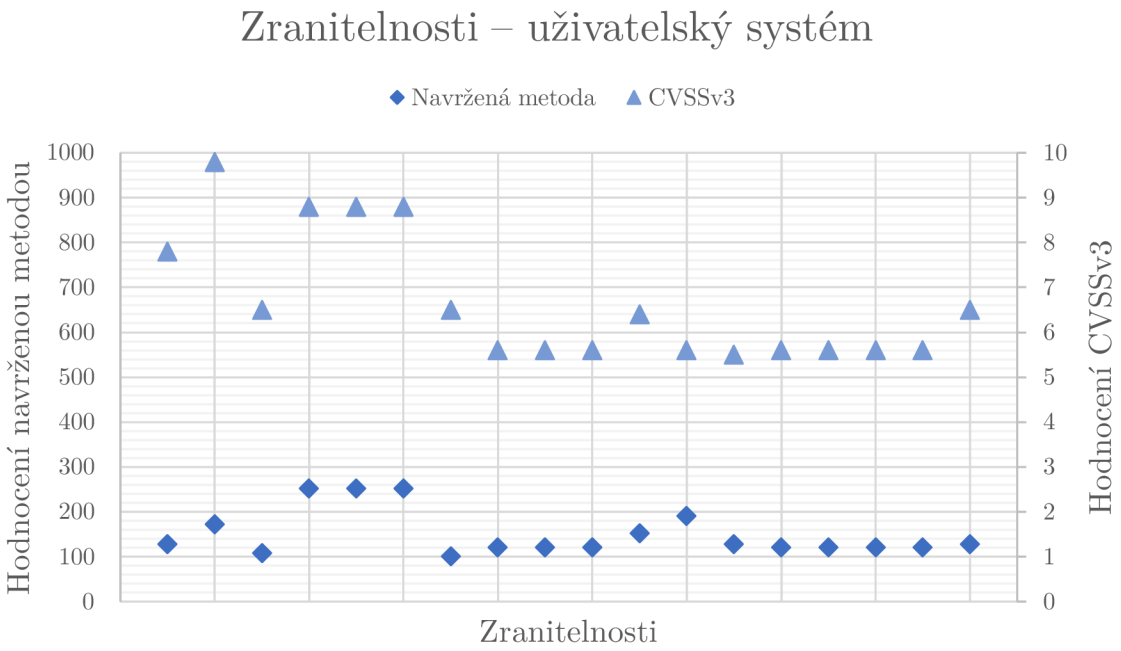
Obrázek 6.1: Srovnání CVSSv3 a navržené metody na webovém serveru IIS



Obrázek 6.2: Srovnání CVSSv3 a navržené metody na databázovém serveru



Obrázek 6.3: Srovnání CVSSv3 a navržené metody na webovém serveru Apache



Obrázek 6.4: Srovnání CVSSv3 a navržené metody na uživatelském systému

U konkrétních zranitelností lze velmi jednoduše pozorovat vliv parametrů, které v metodě CVSSv3 započítány nejsou, na výslednou prioritu zranitelnosti. Konkrétně se jedná o parametry Threat Intelligence, Exploitace a Dostupnost informací. V tabulce 6.3 níže jsou uvedeny tři různé zranitelnosti objevené na databázovém serveru. Pro všechny tři zranitelnosti jsou tedy priorita aktiva a ochranná protiopatření shodná, liší se pouze v stálých parametrech hodnocení zranitelnosti, a právě v aktuálních parametrech, které na uvedeném příkladě mají významný vliv na výslednou prioritu. Hodnocení jednotlivých parametrů je pro jednoduché srovnání v tabulce uvedeno číselně.

Tabulka 6.3: Srovnání hodnocení konkrétních zranitelností dle CVSSv3 a navržené metody

Parametr	**CVE-2016-0132**	**CVE-2020-0646**	**CVE-2017-8759**
Hodnocení CVSSv3	**9,8**	**9,8**	**7,8**
Threat Intelligence	0	0,75	1
Exploitace	0,11	0,56	1
Dostupnost informací	0,11	0,44	1
Interakce uživatele	1	1	0,4
Požadovaná oprávnění	1	1	1
Obtížnost zneužití	1	1	0,78
Dopad na důvěrnost	1	1	1
Dopad na integritu	1	1	1
Dopad na dostupnost	1	1	1
Výsledná priorita	**200**	**322**	**352**

Z tohoto srovnání vyplývá důležitost aktuálních parametrů zranitelnosti, které metoda CVSSv3 nezohledňuje, a jejich vliv na výslednou prioritu zranitelnosti. U zranitelnosti CVE-2017-8759, která je hodnocena dle CVSSv3 v porovnání s dalšími dvěma pouze 7,8 body, je priorita dle navržené metody nejvyšší právě kvůli nejvyšším možným hodnotám u aktuálních parametrů Threat Intelligence, Exploitace a Dostupnost informací.

7 Závěr

Cílem této práce bylo popsat stávající metody pro hodnocení zranitelností a na základě jejich analýzy navrhnout vlastní metodu, která bude zaměřena na prioritizaci zranitelností. Popis těchto metod je uveden v kapitole 2.

Hlavním cílem však byl návrh samotné metodiky. Ta pro prioritizaci zranitelnosti využívá devět parametrů popisujících zranitelnost, dále vlastnosti zranitelného systému, respektive požadavek aktiva na zajištění důvěrnosti, integrity a dostupnosti. Tyto tři zmíněné parametry metoda dále kombinuje s dopadem na důvěrnost, integritu a dostupnost tak, aby se vztah mezi požadavkem a dopadem odrážel ve výsledné hodnotě priority.

Metoda hodnotí zranitelnost pomocí zmíněných devíti parametrů, které jsou dále rozděleny do dvou skupin – aktuální a stálé. Mezi aktuální parametry spadá možnost a náročnost exploitace, dostupnost informací o zranitelnosti a informace ze služeb Threat Intelligence. Tyto tři parametry, jak je možné vidět v kapitole 6.3, jsou velmi důležité pro stanovení výsledné priority zranitelnosti a mají také nezanedbatelný vliv na hodnocení. Skupina stálých parametrů obsahuje obtížnost zneužití, požadavek na interakci uživatele, požadované oprávnění pro zneužití zranitelnosti a dále tři parametry hodnotící dopad na CIA triádu.

V metodě počítá s ohodnocením aktiva, na kterém se zranitelnost nachází. Pomocí dotazníku jsou vyhodnoceny požadavky na důvěrnost, integritu a dostupnost daného systému a všechny tři jsou číselně ohodnoceny. Tato číselná hodnota je pak provázána s dopadem na CIA triádu a výsledné číslo je započítáno do celkového skóre priority zranitelnosti.

Do metody vstupuje i hodnocení implementovaných protiopatření, které je stejně jako výše uvedená priorita aktiva provázáno s dopadem na CIA triádu. Protiopatření snižují riziko zneužití zranitelnosti a z tohoto důvodu jsou do metody zahrnuta. Stejně jako požadavky na zajištění CIA triády, tedy jinak řečeno kritičnost aktiva, mají významný vliv na výsledné hodnocení priority zranitelnosti, jak je možné vidět na výsledcích z testování uvedených v kapitole 6.3.

Formální výpočet priority je postaven na základních matematických operacích tak, aby byla metoda co nejjednodušší, ale zároveň aby její výsledky byly přínosné. Popis výpočtu priority je uveden v kapitole 4.

V kapitole 5 je uvedeno teoretické srovnání navržené metody a aktuálně velmi používané metody CVSSv3. Na základě těchto výsledků můžeme říct, že mezi hodnocením zranitelností dle navržené metody a dle CVSSv3 je určitá korelace, kterou zde můžeme najít. Navržená metoda je efektivnější z důvodu započítání požadavků na zajištění CIA triády aktiva.

Teoretické srovnání však nepostačuje při hodnocení efektivity této metody, která byla dále hodnocena na laboratorním prostředí sestávajícího ze čtyř systémů. Každý systém měl jiné požadavky na zajištění CIA triády, které vycházely z účelu systému a dat na něm uložených

nebo zpracovávaných. Dále byly na každém systému implementována jiná protiopatření, která mohou snížit výslednou prioritu zranitelnosti. Systémy v laboratorním prostředí vycházejí z reálného prostředí firmy, pouze byly uzpůsobeny rozsahu práce a možnostem testování.

V kapitole 6 je popsáno celé laboratorní prostředí, jednotlivé systémy, na kterých byly uměle vytvořeny zranitelnosti, a jejich účel a případná protiopatření. Výsledky testování popsané v této kapitole ukazují, že navržená metoda daleko lépe prioritizuje zranitelnosti díky třem parametrům – Threat Intelligence, Exploitace a Dostupnost informací. Zranitelnosti se stejným nebo podobným hodnocením dle CVSSv3 mají značně odlišné hodnocení dle navržené metody právě díky těmto třem parametrům, které se v čase mění. Priorita testovaných zranitelností byla zanesena do grafů a srovnána s hodnocením dle CVSSv3, z grafů vyplývá značná efektivita při započítání priority aktiva, respektive požadavků na zajištění CIA triády, a také při započítání vlivu implementovaných protiopatření.

Navržená metoda splnila očekávané předpoklady, kdy významný vliv na výslednou prioritu mají parametry proměnné v čase a vlastnosti zranitelného aktiva, respektive dat na něm uložených nebo zpracovávaných. Stejně tak bylo potvrzeno, že je vhodné vzít v potaz i implementovaná protiopatření, která mohou výslednou prioritu zranitelnosti snížit. Tím se dostane pozornosti systémům, které nemají taková protiopatření nebo nemají dokonce žádná protiopatření, a zranitelnosti na takových systémech mohou představovat daleko větší riziko.

Aby bylo možné přesně stanovit efektivitu navržené metody, bylo by vhodné její testování na daleko větším počtu systémů a větší a rozmanitější síti. I přesto bylo testování přínosné, neboť potvrdilo předpoklady definované v teoretickém srovnání navržené metody s CVSSv3.

Seznam použitých zdrojů

[1] 3 Things You Need To Know About Prioritizing Vulnerabilities. *Tenable* [online]. Columbia, 2019, 04. 12. 2019 [cit. 2019-12-08]. Dostupné z: https://lookbook.tenable.com/predictive-prioritization/ebook-3-things-to-know-about-prioritizing-vulnerabilities

[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-whitepaper-predictive-prioritization

[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, July 19, 2011 [cit. 2019-12-08]. Dostupné z: https://www.beyondtrust.com/blog/entry/why-exploitability-matters

[6] ISO/IEC 27005:2018. *Information technology — Security techniques — Information security risk management*. Třetí vydání. 2018.

[7] RFC 4949. *Internet Security Glossary*. Version 2. 2007.

[8] Vulnerabilities. *MDN web docs* [online]. 2019 [cit. 2019-12-08]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Vulnerabilities

[9] PECL, David a Martin DICKÝ. Řízení zranitelností není jen o výběru správného nástroje. *IT Systems* [online]. 2019(07-08) [cit. 2019-12-08]. Dostupné z: https://aec.cz/cz/ztisku/david-pecl+martin-dicky-rizeni-zranitelnosti-neni-jen-o-vyberu-spravneho-nastroje-it-systems-2019.pdf

[10] CVSS Adopters. *First Improving Security Together* [online]. 2019, March 12 [cit. 2019-12-08]. Dostupné z: https://www.first.org/cvss/v2/adopters

[11] 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

[12] Common Vulnerability Scoring System version 3.0. *First Improving Security Together* [online]. 2019 [cit. 2019-12-08]. Dostupné z: https://www.first.org/cvss/v3-0/

[13] CVSS v2 Archive: New version of Common Vulnerability Scoring System released. *First Improving Security Together* [online]. 2019 [cit. 2019-12-08]. Dostupné z: https://www.first.org/cvss/v2/

[14] Don't Substitute CVSS for Risk: Scoring System Inflates Importance of CVE-2017-3735. *McAfee* [online]. United States / English, 2019, Nov 24, 2017 [cit. 2019-12-08]. Dostupné z: https://securingtomorrow.mcafee.com/mcafee-labs/dont-substitute-cvss-for-risk-scoring-system-inflates-importance-of-cve-2017-3735/

[15] CVSS – Is 3 The Magic Number? *Risk Based Security* [online]. 2019, JUNE 5, 2017 [cit. 2019-12-08]. Dostupné z: https://www.riskbasedsecurity.com/2017/06/05/cvss-is-3-the-magic-number/

[16] SCARFONE, Karen a Peter MELL. An analysis of CVSS version 2 vulnerability scoring. 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE, 2009, 2009, 516-525. DOI: 10.1109/ESEM.2009.5314220. ISBN 978-1-4244-4842-5. Dostupné také z: http://ieeexplore.ieee.org/document/5314220/

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

[18] 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

[19] ASTAFYEU, Aliaksandr. Information Security Risk Assessment Methodologies in Vulnerability Assessment of Information Systems. 2015. Master thesis. Technical University of Denmark.

[20] IMPE, Koen Van. Simplifying Risk Management. *Security Intelligence Logo* [online]. 2019, March 28, 2017 [cit. 2019-12-08]. Dostupné z: https://securityintelligence.com/simplifying-risk-management/

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

[22] PECL, David. „Next-Gen" antiviry: Pokročilejší zabezpečení nebo jen buzzword? *DSM* [online]. 2018(3) [cit. 2019-12-08]. Dostupné z: https://aec.cz/cz/ztisku/david-pecl-next-gen-antiviry-pokrocilejsi-zabezpeceni-nebo-jen-buzzword-1-dil-dsm-2018.pdf

[23] ALMER, Lubomír. Management kybernetické bezpečnosti organizace: disertační práce. Brno: Univerzita obrany, 2019.

[24] FRUHWIRTH, Christian a Tomi MANNISTO. Improving CVSS-based vulnerability prioritization and response with context information. 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE, 2009, 2009, 535-544. DOI: 10.1109/ESEM.2009.5314230. ISBN 978-1-4244-4842-5. Dostupné také z: http://ieeexplore.ieee.org/document/5314230/

[25] CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: Security Vulnerability. *Microsoft* [online]. English (United States), 2019 [cit. 2019-

12-08]. Dostupné z: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[26] CVE-2019-0708 Detail. National Vulnerability Database [online]. [cit. 2019-12-08]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2019-0708

Seznam zkratek

CIA	důvěrnost, integrita a dostupnost
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CVSSv3	Common Vulnerability Scoring System verze 3
DMZ	demilitarizovaná zóna
DoS	Denial of Service attack
GSM	Global System for Mobile Communications
ISO	International Organization for Standardization
HR	Human Resources
LAN	Local Area Network, lokální počítačová síť
NVD	National Vulnerability Database
OS	operační systém
RDP	Remote Desktop Protocol
RFC	Request For Comments
USB	univerzální sériová sběrnice
WAN	Wide Area Network, počítačová síť, která pokrývá rozsáhlé území
Wi-Fi	standard popisující bezdrátovou komunikaci v počítačových sítích

Seznam příloh

Příloha A. Dotazník pro stanovení požadavků na CIA triádu aktiva a pro hodnocení protiopatření

Příloha B. Vyplněný dotazník se stanovením požadavků na CIA triádu – zranitelnost CVE-2019-0708

Příloha C. Hodnocení testovaných zranitelností pomocí CVSS a pomocí navržené metody – teoretické srovnání

Příloha D. Vyplněné dotazníky se stanovením požadavků na CIA triádu pro testované zranitelnosti – teoretické srovnání

Příloha E. Výsledky praktického srovnání