Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Zranitelnosti ProxyShell v podmínkách ČR

Lukáš Novotný

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Lukáš Novotný

Informatika

Název práce

Zranitelnosti ProxyShell v podmínkách ČR

Název anglicky

ProxyShell vulnerabilities in the Czech Republic

Cíle práce

Bakalářská práce je zaměřena na problematiku ProxyShell. Hlavním cílem práce je analýza zranitelností ProxyShell v podmínkách ČR společně se získáním bližších informací o potenciálně zranitelných serverech. Dílčí cíle jsou:
- poznání řešené problematiky skrze zpracování základních teoretických oblastí
- nalezení zranitelných serverů nacházejících se na území ČR
- získání bližších informací o těchto serverech
- vyhodnocení dat a nastínění možného řešení ve smyslu zabezpečení
- závěry a doporučení

Metodika

Metodika řešené problematiky bakalářské práce vychází z analýzy a studia odborných informačních zdrojů. V první části je nejprve uveden současný stav a historický vývoj. Dále je problematika ProxyShell charakterizována jako celek a poté se práce zaměřuje na jednotlivé zranitelnosti. Následně je představena reakce českých úřadů a aktéři, kteří zranitelností ProxyShell potenciálně mohli využít. V poslední části jsou shrnuty dostupné informace o nástroji Shodan, který slouží k vyhledávání zařízení připojených k internetu, jež lze filtrovat podle různých atributů, a tedy i zranitelností.

Po dokončení teoretických východisek následuje praktická část zabývající se především analýzou zranitelnosti ProxyShell v podmínkách ČR. Nejprve je sestaven seznam všech potenciálně zranitelných serverů a následně jsou k nim získány bližší informace. Práce si klade za úkol vycházet pouze z veřejně přístupných informací a citlivá data nebudou uváděna pro ochranu provozovatelů serverů, avšak budou sloužit pro akademické účely a pro vyhodnocení situace. Pomocí syntézy teoretické a praktické části jsou následně formulovány závěry bakalářské práce shrnující výsledky společně s nastíněním možného řešení.

Doporučený rozsah práce

40-50 stran

Klíčová slova

ProxyShell, Shodan, Microsoft Exchange Server, web shell, zranitelnost, kyberbezpečnost, vzdálené spuštění kódu

---

Doporučené zdroje informací

CHAUHAN, Sudhanshu a Nutan Kumar PANDA. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Saint Louis: Elsevier Science & Technology Books, 2015. ISBN 9780128019122.

ORTEGA, José Manuel. Mastering Python for Networking and Security: Leverage the Scripts and Libraries of Python Version 3. 7 and Beyond to Overcome Networking and Security Issues. Birmingham: Packt Publishing, Limited, 2021. ISBN 9781839216213.

SANDBU, Marius. Windows Ransomware Detection and Protection: Securing Windows Endpoints, the Cloud, and Infrastructure Using Microsoft Intune, Sentinel, and Defender. Birmingham: Packt Publishing, Limited, 2023. ISBN 9781803230610.

ZHOU, Jianying, Xiapu LUO, Qingni SHEN a Zhen XU. Information and Communications Security: ICICS 2019. Beijing: Springer International Publishing, 2020. ISBN 9783030415792.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zranitelnosti ProxyShell v podmínkách ČR" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Jiřímu Vaňkovi, Ph.D za odborné vedení mé bakalářské práce a za připomínky komise na bakalářském semináři.

Zranitelnosti ProxyShell v podmínkách ČR

Abstrakt

Tato bakalářská práce se zabývá problematikou zranitelností ProxyShell v podmínkách ČR. Práce charakterizuje zranitelnosti ProxyShell, které v minulosti představovaly značné riziko pro státní instituce, organizace i pro běžné obyvatelstvo. Autor práce aktuální situaci analyzoval, nalezl všechny IP adresy potenciálně zranitelných serverů, získal bližší informace, všechny organizace ručně prověřil a zvolil tři typové organizace, u kterých proběhlo dodatečné zkoumání problematiky. Práce se následně zabývá nastíněním možného řešení ve smyslu zabezpečení. Autor práce nenahlíží na problematiku pouze ze statického pohledu na minulost, ale návrhy na zlepšení lze implementovat do širokého spektra organizací a nezaměřuje se pouze na obranu proti sadě zranitelností ProxyShell. Navržené postupy snižují riziko kompromitace organizace i v budoucnu a nejedná se o prosté doporučení k instalaci bezpečnostních aktualizací. Výsledky této práce lze použít pro zlepšení kybernetické bezpečnosti v podmínkách ČR a jakožto upozornění na skutečnost, že se po uplynulých letech stále vyskytují organizace, které jsou potenciálně zranitelné a tento stav by mohl být zlepšen.

Klíčová slova: ProxyShell, Shodan, Microsoft Exchange Server, web shell, zranitelnost, kyberbezpečnost, vzdálené spuštění kódu

ProxyShell vulnerabilities in the Czech Republic

Abstract

This bachelor thesis deals with the issue of ProxyShell vulnerabilities in the Czech Republic. The thesis characterizes ProxyShell vulnerabilities that in the past posed a significant risk to government institutions, organizations and the general public. The author of the thesis analysed the current situation, found all IP addresses of potentially vulnerable servers, obtained more detailed information, manually scanned all organizations and selected three typical organizations for which additional investigation of the issue was carried out. The thesis then goes on to outline a possible solution in terms of security. The author of the thesis does not only look at the issue from a static view of the past, but the suggestions for improvement can be implemented in a wide range of organizations and does not only focus on defending against the ProxyShell vulnerability set. The suggested practices reduce the risk of an organization being compromised in the future and are not simply recommendations to install security updates. The results of this work can be used to improve cybersecurity in the Czech Republic and as a reminder of the fact that there are still organizations that are potentially vulnerable after the past years and this situation should be improved.

Keywords: ProxyShell, Shodan, Microsoft Exchange Server, web shell, vulnerability, cybersecurity, remote code execution

Obsah

1 Úvod

Práce se zabývá problematikou zranitelností ProxyShell na území České republiky. Téma bylo zvoleno z důvodu autorova zájmu v informačních technologiích a to především s důrazem na bezpečnost. Informační technologie se v dnešním rychle se rozvíjejícím světě nacházejí skoro na každém místě a tvoří důležitou součást našich životů. Opomíjeným aspektem se častokrát stává kybernetická bezpečnost a fakt, že se snadno opravitelná zranitelnost může stát velkou hrozbou.

V teoretické části práce jsou uvedeny základní oblasti z kybernetické bezpečnosti, definice klíčových termínů, současný stav problematiky a nástroj, prostřednictvím kterého lze vyhledávat potencionálně zranitelné zařízení. Nástroj Shodan tvoří důležitou součást práce a je následně použit v pozdější fázi zkoumání zranitelností ProxyShell.

V praktické části je problematika zasazena do prostřední České republiky a vytyčeným cílem práce je celkové zhodnocení situace a nastínění možného řešení. Nejprve je však sestaven seznam všech potenciálně zranitelných serverů a následně jsou k nim získány bližší informace. Získávání dodatečných informací nebude provedeno manuálně, neboť autor práce vnímá, že bude potřeba analyzovat velké množství serverů. Práce si klade za úkol vycházet pouze z otevřených zdrojů a citlivá data, která budou v průběhu analyzování shromážděna, nebudou veřejně prezentována. Obsahem práce bude také srovnání počtu potenciálně zranitelných serverů se sousedními státy. Závěrem autor práce navrhne doporučení, aby bylo možné lépe předcházet kybernetickým hrozbám.

2 Cíl práce a metodika

2.1 Cíl práce

Bakalářská práce je zaměřena na problematiku ProxyShell. Hlavním cílem práce je analýza zranitelností ProxyShell v podmínkách ČR společně se získáním bližších informací o potenciálně zranitelných serverech. Dílčí cíle jsou:

- poznání řešené problematiky skrze zpracování základních teoretických oblastí;
- nalezení zranitelných serverů nacházejících se na území ČR;
- získání bližších informací o těchto serverech;
- vyhodnocení dat a nastínění možného řešení ve smyslu zabezpečení;
- závěry a doporučení.

2.2 Metodika

Metodika řešené problematiky bakalářské práce vychází z analýzy a studia odborných informačních zdrojů. V první části je nejprve uveden současný stav a historický vývoj. Dále je problematika ProxyShell charakterizována jako celek a poté se práce zaměřuje na jednotlivé zranitelnosti. Následně je představena reakce českých úřadů a aktéři, kteří zranitelností ProxyShell potenciálně mohli využít. V poslední části jsou shrnuty dostupné informace o nástroji Shodan, který slouží k vyhledávání zařízení připojených k internetu, jež lze filtrovat podle různých atributů, a tedy i zranitelností.

Po dokončení teoretických východisek následuje praktická část zabývající se především analýzou zranitelnosti ProxyShell v podmínkách ČR. Nejprve je sestaven seznam všech potenciálně zranitelných serverů a následně jsou k nim získány bližší informace. Práce si klade za úkol vycházet pouze z veřejně přístupných informací a citlivá data nebudou uváděna pro ochranu provozovatelů serverů, avšak budou sloužit pro akademické účely a pro vyhodnocení situace. Pomocí syntézy teoretické a praktické části jsou následně formulovány závěry bakalářské práce shrnující výsledky společně s nastíněním možného řešení.

3 Teoretická východiska

3.1 Kybernetická bezpečnost

Kybernetická bezpečnost je způsob, jakým jednotlivci a organizace snižují riziko kybernetického útoku. Hlavním úkolem je ochrana zařízení, služeb a samotné infrastruktury před zneužitím, krádeží a poškozením. Také se jedná o mechanismus, který se snaží zabraňovat a předcházet neoprávněnému přístupu k obrovskému množství dat, která jsou na těchto zařízeních a online ukládána.[1] Kybernetická bezpečnost je nedílnou součástí informačních technologií, která musí být zejména flexibilní a adaptivní v dnešním světě rychle se rozvíjejících hrozeb.

3.2 CIA Triad

Jedním ze základních stavebních kamenů informační bezpečnosti je analýza rizik, při které je často využita CIA triáda. Confidentiality (Důvěrnost), Integrity (Integrita) a Availability (Dostupnost) představují tři pilíře CIA triády, modelu informačních technologií sloužícímu k ochraně citlivých informací před možnými úniky.[2] Slouží k vyhledávání zranitelností v systému a pro tvorbu metod pro vytváření řešení.[3] Model lze využívat i na jednotlivé části systému a lze hodnotit, jaký vliv a v jakém rozsahu na daný systém může mít porušení jednoho z pilířů.

CIA triáda se stala elementárním konceptem v oblasti kybernetické bezpečnosti. Je použita v mezinárodně platném a používaném standardu ISO 27001, ve kterém jsou definovány požadavky na informační bezpečnost systémů managementu.[4] Pro běžnou populaci je více známé nařízení Evropského parlamentu, General Data Protection Regulation (GDPR), které taktéž zmiňuje základní princip CIA triády v podobě důrazu na důvěrnost, integritu a dostupnost.[5] Model CIA triády je tedy ve světě velmi široce používán.

3.2.1 Confidentiality

Confidentiality je prvním z kompetentů CIA triády a lze tento pojem přeložit jako důvěrnost. Zachování důvěrnosti spočívá v tom, že by k datům měl přistupovat pouze ten, kdo je k tomu oprávněn a neautorizovaným osobám by se mělo k přístupu zabránit. Citlivé informace jsou uložené bezpečně a je k nim omezený přístup. Neoprávněně mohou k informacím přistupovat útočníci, ale i osoby v dané organizaci bez platného povolení.

K porušení principu důvěrnosti může docházet prostřednictvím přímých útoků, často se ale lze setkat s porušením neúmyslným. Lidské chyby, nedbalost a nedostatečné nároky na kybernetickou bezpečnost mohou také vést k úniku dat.[3]

V boji proti narušení důvěrnosti se používají různé metody, které mají za úkol takovým situacím předcházet. Citlivá data lze klasifikovat a označovat informace s omezeným přístupem. Přístupy lze regulovat a zavádět směrnice, které se zabývají bezpečností a informační bezpečností v rámci dané organizace. Data lze šifrovat a vyžadovat používání systémů s vícefaktorovým ověřením. Je také vhodné zajistit patřičné školení a vzdělávání, aby měli všichni potřebné znalosti a dokázali se ve světě informačních technologií orientovat.

3.2.2 Integrity

Integrity, česky integrita, je dalším elementem CIA triády. Odkazuje na úplnost společně s přesností dat a na schopnost organizace chránit data před kompromitací v podobě změny a úpravy.[2] I sebemenší změna by mohla mít rozsáhlé následky. Integrita dat je při ochraně informací velmi důležitým komponentem. Při posuzování integrity nehledíme na oprávněnost přístupu, nýbrž na to, jestli je samotná informace správná a nebyla dodatečně modifikována.

3.2.3 Availability

Availability, česky dostupnost, je posledním základním elementem CIA triády. Dostupnost znamená schopnost organizace přistupovat k datům podle potřeby.[3] U některých systémů je potřebný nepřetržitý provoz a není možné, aby nastal i sebemenší výpadek.

Pro uvedení příkladu, organizace se chystá přejít na Microsoft Exchange Server. Samotný Exchange Server z pohledu dostupnosti musí fungovat neustále a není možný jeho výpadek. Klientský přístup přes desktopové rozhraní na osobním počítači nacházejícím se v kanceláři není z pohledu dostupnosti prioritní a lze počítat s výpadkem na několik hodin. Uživatelé mohou do systému přistupovat pomocí dalších metod.

3.3 Terminologie kybernetické bezpečnosti

Pro orientaci ve světě kybernetické bezpečnosti je důležitá znalost základních pojmů a principů. Níže jsou charakterizovány základní pojmy pro pochopení zkoumané oblasti. Termíny jsou vysvětleny tak, aby konceptuálně zapadaly do tématu práce a umožnily náhled do problematiky bezpečnosti i z pohledu ochrany informací a analyzování aktérů.

3.3.1 Vektor útoku

Vektor útoku je způsob, prostřednictvím kterého se útočník dostane do systému nebo sítě.[6] Je to metoda využívána pro napadení počítačů, sítí nebo jiných zařízení. Mezi základní vektory útoku se řadí sociální inženýrství, krádež identity, zneužití zranitelností nebo nedostatečná ochrana proti vnitřním hrozbám.

3.3.2 Vulnerabilities

Vulnerabilities, česky zranitelnosti, jsou chyby v systému nebo v jeho architektuře, které umožnují útočníkovi neautorizovaný přístup, spouštění škodlivého kódu nebo jiné nekalé metody.[7] Jsou to slabá místa v systému, o jichž si není výrobce vědom, tedy ve většině případů. Při odhalení zranitelností dochází ze strany výrobce k vydávání bezpečnostních aktualizací, které slabiny opravují, pokud je to technicky možné.

Zranitelností existuje mnoho a objevují se stále nové. Z důvodu přehlednosti vznikl v minulém století systém CVE (Common Vulnerabilities and Exposures), seznam, ve kterém jsou veřejně odhalené bezpečnostní slabiny. Pokud někdo zmiňuje CVE, odkazuje na zranitelnost s přiděleným identifikačním číslem CVE.[8] Celý systém je spravován neziskovou organizací The MITRE Corporation podpořenou Ministerstvem vnitřní bezpečnosti Spojených států amerických. V českém prostřední na zranitelnosti upozorňuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

3.3.3 Exploit

Exploit je program nebo část kódu navržený pro vyhledávání a zneužívání chyb a zranitelností v jiném programu nebo v systému. Obvykle je použit pro instalaci malwaru, tedy škodlivého programu. [9] Mohlo by se zdát, že je exploit sám o sobě malwarem, ale není tomu tak.

Lze je rozdělit na známé a neznámé. Jakmile je exploit objeven, zranitelnost je opravena, aby zneužití nebylo možné. Úzce tedy toto téma navazuje na zranitelnosti jako takové. Pokud je exploit znám pouze lidem, kteří ho vyvinuli a nikomu jinému, je označován jako zero-day exploit. Tvoří tak poměrně závažnou hrozbu a ochrana proti němu není pouze v podobě aktualizovaného systému.

Nejvíce nebezpečným druhem je ovšem zero-click exploit, který představuje významnou hrozbu především pro mobilní telefony a dalších zařízení. Při zneužití tradičních exploitů se útočník snaží docílit oklamání oběti, zero-click exploit může infikovat zařízení nepozorovaně. Často se lze setkat s případem, kdy se uživateli pouze zobrazí notifikace o zmeškaném hovoru. Zero-click exploity jsou velmi ceněné zranitelnosti všemi aktéry kybernetických hrozeb, včetně pokročilých trvalých hrozeb (APT) a národních států. Převážně se používají pro doručení spywaru, tedy škodlivého programu, který tajně shromažďuje informace o osobách zájmu.[10] Takový druh softwaru už je v dnešní době běžný používaným.

Mediálně známým softwarem využívajícím právě zero-click exploitu je spyware od izraelské společnosti NSO zvaný Pegasus.[11] Totožním příkladem je i spyware Predator od společnosti Cytrox. Pegasus byl zacílen od počátku své existence na tisíce lidí.[12] Preciznost takového softwaru je naprosto nezbytná, protože je převážně využíván na osoby, jež možné kompromitovaní zařízení mohou očekávat. Využívání podobného softwaru je mnohdy kritizováno a považováno za nemorální, avšak existují i situace, kdy je použití nutné a bezpečnostní složky po celém světě mají především chránit běžné obyvatelstvo před nebezpečím a k tomu potřebují adekvátní a účinné metody.

Lze se pouze s určitou pravděpodobností domnívat, zda se v českém prostředí spyware jako je NSO Pegasus, Cytrox Predator, Candiru DevilsTongue a obdobné používají. Pokud by tomu tak nebylo, české zpravodajské služby by se dostávaly do nevýhody oproti protivníkům.

3.3.4 Payload

V kontextu kybernetické bezpečnosti je payload škodlivý kód, který je pomocí vektoru útoku a využití exploitu spuštěn na cíleném zařízení. Payload může být za použití stejného vektoru útoku a využití stejného exploitu různorodý. Škodlivost daného kódu závisí na

útočníkovi. Může se jednat o exfiltraci dat, ransomware, spyware nebo i pouhý žert, který je ve své podstatě nevinný a neškodný. To ovšem není častý případ.

3.3.5 Threat Actor a Cyber Threat Actor

Threat actor, někdy se lze setkat i s označeným cyber threat actor (CTA), je označení pro osobu nebo organizovanou skupinu lidí, kteří vědomě páchají akce, jejímž cílem je způsobit škodu v oblasti informačních technologií. Zneužívají zranitelnosti počítačů, sítí a systémů pro účely svých útoků.[13] Společností jsou vnímáni negativně, ač existují případy, kdy s nimi běžné obyvatelstvo soucítí. Příkladem může být skupina Anonymous.

Mnoho aktérů si nevolí přímo své cíle, ale spíše se zaměřují na vyhledávání slabin, které by mohli pro své působení využít. Objevují se i aktéři, kteří do svých činů zapojují své ideologické vyznání a prosazují své zájmy v podobě aktivismu v kybernetické prostoru prostřednictvím hackingu. Proto se také označují jako hacktivists, tedy spojení slov hacker a activists.[14] Někteří aktéři si své cíle záměrně vybírají a pohání je jiná motivace než ostatní. Mohou to být Advanced persistent threats (APT) prosazující obvykle zájmy cizí státní moci. Může docházet k tomu, že je aktérem přímo některý stát.

3.3.6 Advanced persistent threat

Advanced persistent threat, česky pokročilá přetrvávající hrozba, je druh aktéra, který je obvykle úzce spjatý a finančně podporovaný cizí státní mocí. Mnohdy může být využívaný pro operace zpravodajských služeb cizí moci s kterými velice často spolupracuje. Jedná se tedy o závažnou hrozbu, která především cílí na státní instituce a velké společnosti. Motivace aktéra bývá politická nebo ekonomická.

Mezi známé státy, jež jsou spojováni s působením APT, se řadí Čínská lidová republika, Ruská federace, Íránská islámská republika a Korejská lidově demokratická republika.[15] Na APT není nahlíženo pouze jakožto na zločinecké skupiny mimo EU/NATO. Příkladem APT finančně podporovanou našim spojencem je Equation Group.[16] Při přisuzování působení aktéra některé zemi a její zpravodajské službě či jiné státní instituci, je vhodné se pohybovat v rámci určité pravděpodobnosti. Obecně se nelze na základě otevřených zdrojů s jistotou rozhodovat o spojování aktérů, zemí a útoků.

Získávání informací, monitorování a analyzování APT obstarávají především zpravodajské služby a velké technologické společnosti.[15] Naše zpravodajské služby nejsou všemocné a pro boj proti nebezpečí, které APT představují, je důležitá mezinárodní

spolupráce.[17] Vyplývá to i z faktu, že mnoho útoků není pouze na jednu zemi a jedná se spíše o rozsáhlé kampaně proti více zemí zejména v EU/NATO.

Jelikož tato hrozba na sebe upíná mnoho pozornosti, zajímá se o ní logicky i celá řada společností působících na poli kybernetické bezpečnosti. V poslední době nastává problém v přehlednosti pojmenování těchto hrozeb. Existuje zažité označení pomocí zkratky APT spojené s číslem, avšak každá firma má pro jednotlivé aktéry své vlastní jméno, a tak vznikají dlouhé seznamy a leckdy se může stát, že jeden aktér těchto označení získá desítky.

Celá situace se zhoršuje i tím, že společnosti své označení v průběhu času mění. V letošním roce se pro tento postup rozhodl Microsoft, který donedávna pro APT používal pojmenování podle drahých kovů, od letošního roku proběhl přechod na pojmenování podle počasí.[18]

Běžný životní cyklus APT je rozdělený na 4 fáze: průzkum a sběr informací, počáteční kompromitace, vytvoření přístupu a následná exfiltrace dat.[19] Životní cyklus aktéra je také přizpůsobený podstatě jeho existence. Službě cizí státní moci. Aktér se zaměří na jeden konkrétní úkol. Pokusí se získat přístup do daného prostředí. Vektor útoku může být jakýkoliv. Prostřednictvím části kompromitovaného systému pronikne do sítě a nahraje dodatečný škodlivý obsah pomocí kterého naplní cíl svého útoku. Závěrečný krok je zamaskování stop. Firmy nebo i státní instituce se o proběhlém útoku mohou dozvědět až po několika měsících.

3.3.7 Atribuce

Atribuce představuje především proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka. Jedná se v první řadě o technické informace a analýzy, pod kterými si lze představit například analýzu síťového provozu nebo použitého škodlivého kódu.[17]

K atribuci útoku by se mělo přistupovat s rozvahou a mělo by se dbát na to, aby nedošlo k chybnému propojení.[20] Soukromé společnosti a státní instituce s rozvahou jednají a není častým jevem, že by docházelo k atribuci chybné. Celá problematika úzce navazuje na důvěryhodnost daných institucí a společností. Renomované kybernetické organizace atribuci označí jako neznámou než aby neprávem některou zemi nebo přímo některého aktéra obvinili. Chybná atribuce nepoškozuje pouze autora, ale i danou zemi, která na obvinění poté může adekvátně reagovat.

Při atribuci lze vytvořit pomocnou tabulku, kde se shrnou dosavadně získané indicie a na základě vybraného rozhodovacího modelu se lze rozhodnout, jestli existuje dostatek důkazů, že se jedná právě o zemi nebo aktéra, kterého podezříváme. Může se stát, že některé indicie budou

naznačovat i na jiné země a aktéry, poté je rozhodování velmi individuální a osoby zodpovědné za atribuci by měli postupovat obezřetně. Atribuovat útok dané zemi je vždy snazší a jedná se o začátek celého procesu. Poté se lze rozhodovat o aktérovi. Existuje možnost, že se bude jednat o neznámého útočníka, ale spíše se bude jednat o už existující CTA, popřípadě APT. Při znalosti konkrétního aktéra lze zkoumat napojení na cizí státní moc. Pokud je propojení na cizí státní moc prokazatelné, je to vždy ten horší případ.

V neposlední řadě, celá problematika se stává komplikovanější, když zodpovědné osoby musejí brát v úvahu i false flag operace. False flag operací se mohou v oblasti informačních technologií dopouštět naši spojenci i naši nepřátelé či neutrální státy.

3.3.8 Stupnice pravděpodobnosti

Při poskytování informací lze použít stupnice pravděpodobnosti. Ve světě kybernetické bezpečnosti a analyzování aktérů jsou podobné stupnice běžně používané. Stupnice mohou mít několik stupňů a při vybírání je vhodné zvážit osobní preference a intuitivnost dané stupnice. Mnoho subjektů v prostředí České republiky používá metodiku hodnocení používanou NÚKIB. Konkrétní stupnici lze vidět v tabulce 1, která zobrazuje procentuální vyjádření míry jistoty.

Název	Procentuální vyjádření
Téměř jistě	90-100%
Velmi pravděpodobně	75-85%
Pravděpodobně	55-70%
Reálná možnost	25-50%
Nepravděpodobně	15-20%
Velmi nepravděpodobně	0-10%

Tabulka 1 Stupnice pravděpodobnosti (zdroj: NÚKIB)

3.3.9 Traffic Light Protocol

Důležitou součástí sdílení dat, nikoliv jen o incidentech v oblasti kybernetické bezpečnosti, je ochrana informací. Stát disponuje složitým mechanismem skrze který problematiku utajovaných informací obstarává. V soukromé sféře se lze s utajovanými informacemi ve smyslu státního pojetí také setkat, ale častější jsou interní směrnice, podle kterých se zaměstnanci řídí a pro tento účel si mohou společnosti pomoci i světově rozšířeným protokolem Traffic Light Protocol (TLP). Tento fakt ovšem neznamená, že by se protokol TLP nepoužíval v rámci státní správy. Celá problematika ochrany dat a klasifikace informací je provázaná.

V České republice tvoří hlavní pilíř Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, který upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.[21]

TLP protokol byl vytvořen s cílem usnadnit a zabezpečit sdílení informací mezi organizacemi. Používá čtyři základní barvy, pomocí kterých označí konkrétní informaci a určí tak, jak může příjemce s danou informací zacházet a jak ji může dále používat.[22] Před zasláním citlivé informace musíme dbát na to, jestli protistrana je se systémem TLP seznámena a respektuje jej.[23] Pokud by tomu tak nebylo, mohlo by dojít k úniku dat.

Označení	Barva	Podmínky použití
TLP:RED	Červená	Informace je poskytnuta pouze určité osobě a nikomu dalšímu, další subjekty musejí být taxativně jmenováni. Původně musí souhlasit.
TLP:AMBER	Žlutá	Informace může být sdílena pouze v rámci organizace příjemce, s dalšími partnerskými subjekty příjemce pouze pokud splňují princip need to know. Původně může rozsah sdílení dále omezovat.
TLP:GREEN	Zelená	Informace může být sdílena v rámci organizace příjemce nebo s dalšími partnerskými subjekty příjemce, nikoliv však veřejnými kanály
TLP:WHITE	Bílá	Informace může být šířena a poskytována bez omezení

Tabulka 2 TLP (zdroj: NÚKIB)

V roce 2022 byla vydána aktualizovaná verze příznaků TLP. Do 31.12 2022 byl vyžadován ze strany NÚKIB přestup na novější verzi.[24] Došlo ke změně jména TLP:WHITE na TLP:CLEAR a TLP:AMBER byl rozšířen na dodatečný stupeň TLP:AMBER+STRICT, který informaci klasifikuje pouze pro organizaci a v rámci organizace se pracovníci řídí pravidlem need to know, tedy informace je dostupná pouze vybraných zaměstnancům.

3.4 Zranitelnosti ProxyShell

ProxyShell je zcela nová zranitelnost Microsoft Exchange Serveru, která byla v srpnu roku 2021 prezentována na konferenci BlackHat USA výzkumníkem Orange Tsai.[25] Zneužití ProxyShell je pro zasvěcené v oboru poměrně jednoduché a dává útočníkům přístup k shellu jakožto Windows NT Authority user.

ProxyShell funguje na základě série závažných zranitelností pro už zmiňovaný Microsoft Exchange Server. A to konkrétně pro jeho verzi 2013, 2016 a 2019. Zranitelné jsou všechny servery na této verzi, které jsou přístupné na portu 443 a od dubna 2021 nebyly aktualizované.[26] Jednotlivé zranitelnosti byly opravené bezpečnostními aktualizacemi z dubna 2021 (KB5001779 pro CVE-2021-34473 a CVE-2021-34523) a z května 2021 (KB5003435 pro CVE-2021-31207).

Na počátku roku 2022 mělo signifikantní množství organizací problém s aktualizací Exchange služeb. Přesněji se jednalo o 4,3 % serverů, u kterých nebyl nainstalován patch na ProxyShell zranitelnosti a 16 % serverů nemělo následující bezpečnostní aktualizace vydané od srpna 2021.[27]

3.4.1 CVE-2021-34473

Jedná se o zranitelnost umožňující vzdálené spuštění kódu skrze chybu ve zpracování požadavku. Přesněji jde o takzvaný server-side request forgery (SSRF), což znamená, že útočník může donutit zranitelný server vydávat požadavky jeho jménem. Není zde potřeba žádná autentizace, protože jsou požadavky prováděné koncovými body na backendové servery a důvěra mezi nimi zde už existuje. Tato zranitelnost vzniká v důsledku záměny cest kvůli nesprávnému analyzování URI.

To znamená, že zranitelnost umožňuje útočníkovi spustit další dvě zranitelnosti (CVE) přes poslaní na backendový server, který za normálních podmínek vyžaduje autentizaci, ale v našem případě jsou požadavky poslané jakožto NT Authority/System, což je uživatel v prostředí Windows s nejvyššími právy.[25]

3.4.2 CVE-2021-34523

Jedná se o zranitelnost oprávnění skrze chybu v Exchange PowerShell Remoting. Za pomocí této chyby můžeme získat přístup k PowerShell Remoting agentovi, který je dostupný skrze cestu /PowerShell/. Toto prostředí je však vysoce restriktivní a umožňuje pouze některé příkazy. Prostředí navíc nemůžeme jakožto systémový uživatel k našemu finálnímu účelu využít, protože nemáme poštovní schránku – potřebujeme se stát jedním z uživatelů daného

Exchange Serveru, a to tedy Exchange adminem. Toho docílíme pomocí toho, že je přístupový token zadaný jako X-Rps-CAT v dotazu deserializován a přidán jako hlavička X-CommonAccessToken do konečného požadavku, což nám umožní se za daného uživatele vydávat a můžeme dále postupovat v útoku.[25]

3.4.3 CVE-2021-31207

Proč se práce v minulém odstavci zmiňovala o poštovní schránce? Protože je to další součást ProxyShell útoku. Tato chyba nám umožnuje zápis souboru na server a vzdálené spouštění kódu.

Princip této části útoku spočívá v tom, že útočník může exportovat obsah poštovní schránky do cesty a přípony souboru, který si sám zvolí, i přesto že to za normálních okolností možné není. Útočník tedy ve finále může uložit WebShell zakořeněný v konceptu mailové zprávy a poté ji pomocí cmdlet New-MailboxExportRequest může exportovat v .NET formátech jako Active Server Pages (ASPX) do příslušných složek a skrze tento postup může spustit škodlivý kód.[25]

3.4.4 Detekce indikátorů potenciálního zneužití

Organizace by měla kompromitaci předcházet. Vhodné je použití technologií, které jsou již běžným standardem: NGFW (firewall a pokročilé filtrování provozu), SIEM (centrální uchovávání bezpečnostních logů), XDR (nejen antivirové endpoint řešení), SOAR (automatizace), IDS/IPS (pasivní monitorování nebo aktivní filtrování provozu, častokrát součástí jiného řešení), DLP (ochrana informací) a obdobné.

Organizace by měla prověřit indikátory potenciálního zneužití ProxyShell. Pokud organizace disponuje Exchange Serverem, který nebyl aktualizován a jedná se o charakterizovanou verzi z předchozích odstavců, je pravděpodobné, že zranitelnosti ProxyShell lze proti společnosti zneužít.

- *POST requesty obsahující "/PowerShell/", "/autodiscover/autodiscover.json" "/mapi/nspi/ v IIS logu;*
- *přítomnost nelegitimních .ASPX souborů ve složce "C:\inetpub\wwwroot\aspnet_client" (dle informací často o velikost 265KB);*
- *hXXps://Exchange-server/autodiscover/autodiscover.json?@foo.com/mapi/nspi/?&Email=autodiscover/autodiscover.json%3F@foo.com.*[26]

Administrátorům je doporučeno, aby byla bezodkladně provedena instalace poslední bezpečnostní aktualizace pro Exchange Server dle dokumentace Microsoft.[26] Pokud organizace objeví potenciální kompromitaci, kybernetický bezpečnostní incident by měla nahlásit na NÚKIB.

3.4.5 Reakce českých úřadů

Úřadem, který se problematikou nejvíce veřejně zajímal je bezesporu NÚKIB, jež se snažil před situací několikrát varovat a vydával přehledy a doporučení. NÚKIB na ProxyShell upozorňoval v srpnu 2021.[26] Následně i na podzim na začátku listopadu 2021, kdy se objevila vlna zneužívání zranitelností.[28] NÚKIB měl o situaci přehled i z důvodu, že jsou povinné subjekty ze zákona kybernetické bezpečností incidenty ohlašovat.

Zmínka o ProxyShell se také objevila ve Zprávě o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky z roku 2021 vydanou Ministerstvem vnitra.[29] Ministerstvo ovšem vychází z dat NÚKIB a data pouze charakterizuje vlastním textem a grafickým znázorněním vývoje kybernetických incidentů

3.5 Shodan

Shodan je vyhledávač zaměřený na zařízení připojené na internet. Většina z běžné populace si pod slovem vyhledávač představí například Google, Seznam nebo Bing, které jsou skvělé a práci ulehčující při vyhledávání webových stránek. Ovšem Shodan je zcela něco jiného a může nám poskytnout data například, o tom jaké země jsou nejvíce připojené na internet nebo jaká verze (zde lze doplnit téměř cokoliv) je zrovna populární a nejvíce používaná.[30] V této práci se ale budeme věnovat datům ohledně zranitelností, který tento vyhledávač také nabízí, a které jsou pro zaměstnance v informačních technologií velice důležité.

Shodan získává informace o všech zařízeních, které jsou přímo připojené do internetu. Když takové zařízení existuje, tak o něm Shodan získá množství zajímavých, a přesto veřejných informací. Může se jednat o malé IP kamery až po vodní elektrárnu.[31] Shodan v České republice užívá například Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Zakladatelem Shodan je počítačový programátor John Matherly. Shodan spatřil světlo světa poprvé v roce 2009, ač měl John myšlenky na vyhledávač pro zařízení připojená na internet už v roce 2003. Jméno tohoto vyhledávače je referencí na postavu ze série videoher System Shock zvanou SHODAN.[31] SHODAN (Sentient Hyper-Optimized Data Access Network) je hlavní antagonista a umělá inteligence.

Uživatelé Shodanu jsou zejména odborníci na kybernetickou bezpečnost, výzkumníci a státní bezpečnostní složky. Zatímco útočníci s nekalými úmysly mohou Shodan také využívat, tak to pro ně není moc výhodné a lukrativní, protože by mohli být detekováni a mají bezpečnější přístup k těmto datům – botnet sítě, které tento úkol také splní.

Shodan nabízí základní 4 produkty. Prvním z nich je už popisovaný vyhledávač, ale to není všechno, co může Shodan nabídnout. Dále je to i Shodan Monitor pro monitorování sítě, Shodan Maps pro zobrazení dat na mapě a Shodan API.[32] API slouží ke práci se Shodanem v našem kódu bez nutnosti použití webové stránky a pro automatizování daného procesu.

3.5.1 Rozdíl mezi filtrem verified a unverified

V prostředí Shodanu se můžeme setkat filtrem verified (potvrzené) a unverified (nepotvrzené). Nepotvrzené jsou takové zranitelnosti, které jsou vyjádřeny pomocí dat postavených na metadatech, který Shodan shromažďuje.

Shodan se snaží zranitelnosti jednotlivých zařízení potvrzovat, ale je to nad jeho síly, protože jich je opravdu mnoho. Nepotvrzené zranitelnosti ovšem mohou mít značný podíl falešně pozitivních případů a v potvrzených datech zase může mnoho chybět.[33]

3.5.2 Honeypot problematika v prostředí Shodan

Honeypot je zařízení, které je cíleně přístupné a zranitelné, sloužící pro účely výzkumu útočníků a jejich metod. Primární cíl je sběr dat, ale pokud bychom měli honeypot i v rámci sítě, lze jej využít jakožto slepou uličku pro útočníka.

Existuje reálná možnost, že je blíže nespecifikovaný počet zařízení ve vyhledávači Shodan honeypot, a ve skutečnosti se nejedná o potenciálně zranitelný server.

Dle čínských výzkumníků z konference Informační a komunikační bezpečnosti v Pekingu, kteří prováděli měření přístupnosti ICS (Industrial Control System), je existence pravděpodobná. Celkově 5 jejich honeypot zařízení, MirrorPot instancí, bylo ve vyhledávači Shodan k nalezení a mylně označené jako „Industrial Control System“. Pokus s určitou mírou předkládá informaci, že se ve vyhledávači Shodan zobrazují i honeypot zařízení a jsou efektivní.[34]

4 Vlastní práce

4.1 Metody pro nalezení zranitelných serverů na území ČR

Pro analýzu současného stavu problematiky ProxyShell je nutné získání potřebných dat, pomocí kterých se lze následně rozhodovat. Na začátku celého procesu je třeba charakterizovat možné metody, kterými lze data získat. Pro získání dat, přesněji IP adres, lze využít více postupů, které jsou rozdělené v dalších kapitolách.

Nejstěžejnější fází celé práce je samotné získání dat. Práce si klade za úkol získat IP adresy všech potenciálně zranitelných serverů společně s bližšími informacemi. Při zvážení všech možností lze sběr dat rozdělit do třech kategorií a pouze jedna je pro tento sběr dat vhodná. Do kritérií lze zařadit různé aspekty, podle kterých se lze rozhodovat, ale ten nejdůležitější je jednoznačně efektivita společně s bezpečností a souladem se zákony během celého procesu. Práce se soustředí na základní porovnání nákupu dat, využití vlastní infrastruktury a použití komerčního nástroje Shodan.

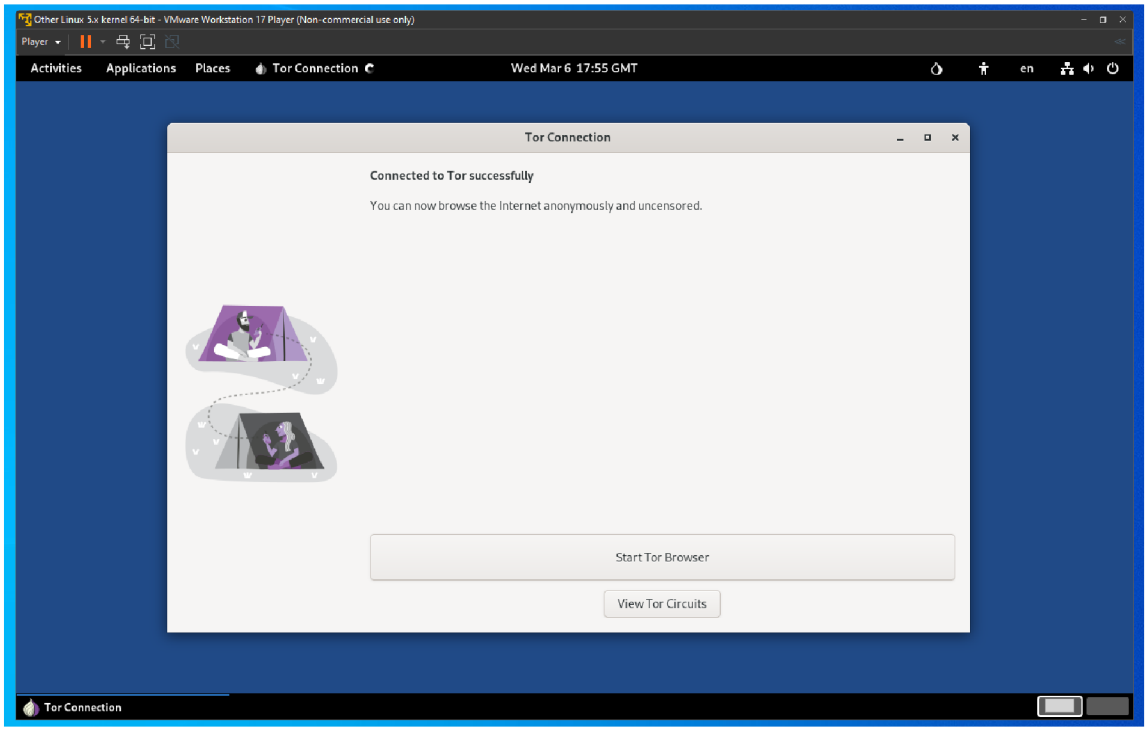
4.1.1 Nákup dat na Exploit.in

Jeden z postupů, který lze pro sběr dat využít, je nákup dat. Existuje mnoho míst, kde lze podobné služby, data, informace a malware nakoupit. Především se jedná o místa, která nejsou běžně dostupná z klasického internetu a prohlížeče, a na kterých se pohybují lidé, kteří nemají většinou dobré úmysly. Známou webovou stránkou, kterou lze pro tento účel využít, je ruskojazyčné fórum Exploit.in, jenž se řadí mezi nejznámější stránky s podobným obsahem.

Pokud by se práce ubírala tímto směrem, což z hlediska neefektivnosti daného řešení společně s morální stránkou věci, nebude, je důležité dbát na OPSEC (Operations security). OPSEC se snaží minimalizovat možná rizika kompromitace operace a aplikuje postupy ke snížení možného přiřazení aktivity k určité osobě, v tomto případě by se jednalo o spojení nákupu dat na ruskojazyčné webové stránce k osobě autora práce. Tak by došlo ke kompromitaci aktivity, která je v rámci práce vykonávaná. Pro snížení rizika kompromitace autora práce lze aplikovat mechanismy, které se snaží takovému výsledku zabránit. Na začátku procesu si osoba plánující využití stránky musí uvědomit, že je naprosto nezbytné se maximálně chránit a interakce na podobném místě není bezpečná a je nutné dodržování zákonů. Návštěva podobného webového serveru by měla sloužit pouze pro studijní účely.

Pro snížení rizika lze využít notebook bez předinstalovaného operačního systému, který byl nakoupen zásadně pomocí hotovostní platby a na místě nám neznámém s operačním

systémem Tails s použitím prohlížeče Tor a .onion verze Exploit.in. Autor práce nechce možné využití postupů pro OPSEC či PERSEC dále charakterizovat, protože by mohlo dojít ke zneužití informací pro trestnou činnost. Na obrázku 1 je vidět operační systém Tails a informace o úspěšném připojení do sítě.



Obrázek 1: Operační systém Tails (zdroj: autor)

Autor práce na virtualizovaný stroj pomocí softwaru VMware operační systém Tails nainstaloval, avšak poněvadž se práce nebude ubírat směrem, který by přímo vyžadoval zvýšenou bezpečnost při práci, nebyl dále využíván. Jelikož se jedná pouze o virtuální stroj, není jeho použití autorem práce doporučeno. Pokud by byl kompromitován hlavní počítač, na kterém je ona virtualizace spuštěna, operační systém na VMware postrádá význam.

Optimální využití Tails je při instalaci na flash disk, který lze kdykoliv vysunout a operační systém se při opětovném zapnutí spustí do původního stavu, což představuje výhodu proti kompromitaci systému či proti vnější škodlivé činnosti proti uživateli obdobného operačního systému.

Správně nastavený OPSEC neposkytuje ochranu pouze proti špatným aktérům na poli kybernetického prostoru, ale i proti bezpečnostním složkám, které nás především chrání a každý by měl jistým způsobem k ochraně naší země přispívat, a ne se vydávat cestou trestné a škodlivé činnosti. Peníze, které se velice často v podobě kryptoměn na webovém serveru zobchodují, mohou i nepřímo financovat útoky na naší zemi. Ruskojazyčné kyberkriminální prostředí je

velice obsáhlé a bylo by nesprávné se domnívat, že ani jeden člen Exploit.in nikdy nebyl zapojen do jakéhokoliv, s vlastní či motivací cizí státní moci, útoku na země EU/NATO.

ProxyShell je už veřejně známá a odhalená sada zranitelností. Pokud bychom chtěli získat informace o zranitelnostech, které nejsou ještě rozšířené ve veřejné bezpečnostní komunitě a jsou využívané zejména státními celky a aktéry, je průzkum kyberkriminálních komunit poměrně výhodná cesta. V nástroji Shodan podobná data nebudou a daný server by se mohl jevit jako poměrně dobře zabezpečený, ale mohl by obsahovat zranitelnost, přes kterou by mohl být snadno kompromitován. V nástroji Shodan a v komerčních produktech se takové zranitelnosti mohou projevit až s odstupem času, kdy je organizace už kompromitována. Proto také existují pracovní pozice s častým názvem "Threat Hunter". Člověk na obdobné pozici se snaží objevovat doposud neodhalené zranitelnosti a nástrojem, který lze pro obdobnou práci využít, jsou i servery podobné Exploit.in. Zejména se jedná o komunity, jež nejsou tak snadno dostupné jako zmiňovaný Exploit.in.

Využití webové stránky Exploit.in je neefektivní a data lze získat lepším způsobem. Jedná se také o podporu kyberkriminálního prostředí, nepřímá podpora ruských aktérů skrze fakt, že se jedná o ruskojazyčné fórum a mnoho uživatelů potenciálně může mít vazbu na podobné aktéry, nutnost dodržovat přísné bezpečnostní postupy a už zmiňovaná morálnost a legálnost celého řešení. Autor práce silně nedoporučuje, aby byla stránka Exploit.in jakkoliv použita či podpořena. Celý popis možné koupě dat slouží pouze pro akademické účely.

4.1.2 Využití vlastní infrastruktury

Pro získání a sběr dat lze využít i vlastní infrastrukturu. V porovnání s koupí dat se jedná o náročnější cestu a není lehké takového postupu využít. Aktér disponující s infrastrukturou pro nalezení všech potenciálně zranitelných serverů na území ČR, vlastní obdobnou infrastrukturu s určitým důvodem a v mnoha případech se nejedná o aktéra, který by podobnou činnost provozoval pro dobrý účel. Skenování možných cílů je častokrát první fází útoku a na základě získaných dat se aktér může dále rozhodovat, na kterou organizaci zaútočí nebo v opačném případě při zacílení jedné organizace nebo státní instituce se rozhoduje jakou zranitelnost a slabinu využije. Oba postupy jsou podobné, ale vyžadují odlišné myšlení.

Autor práce považuje druhou možnost jako méně náročnou ve fázi testování, ale složitější ve fázi kompromitace, protože není jisté, zda bude zranitelnost nalezena a jak složité bude její využití. Skenování jedné organizace a hledání možných slabin není náročné na vlastní infrastrukturu, ale pokud bychom chtěli oskenovat celou ČR, bez rozsáhlé vlastní infrastruktury, bylo by nutné použití nástrojů třetích stran, a to například Shodan. Hranice mezi

využití vlastní infrastruktury a nástrojem Shodan je velice zanedbatelná, protože při využívání vlastní infrastruktury také není vše vytvořeno pouze daným aktérem.

4.1.3 Využití komerčních nástrojů

Optimální metodou, kterou lze docílit nalezení potenciálně zranitelných serverů, je použití komerčního nástroje, který je svou efektivností vhodným řešením. Komerčních řešení existuje celá řada a práce se bude soustředit především na nástroj Shodan.

4.2 Využití nástroje Shodan

Pro účely získání IP adres potenciálně zranitelných serverů na zranitelnosti ProxyShell je využíván nástroj Shodan. Jedná se o velmi efektivní nástroj pro analyzování problematiky. Nákup dat je nevhodný, neefektivní a není nutné vytvářet vlastní infrastrukturu, protože do jisté míry již existuje, a to je právě nástroj Shodan.

Během analyzování serverů a společností je nutné uvědomění si jednoho důležitého faktu. Na zranitelnost, ať už ProxyShell nebo i jiné, může být zranitelný kdokoliv. Lze se setkat se soukromým sektorem v podobě malých a středně velkých firem či dokonce nadnárodních korporací. Na druhé straně stojí vrcholné státní instituce, bezpečnostní složky či kritická infrastruktura státu. Se zranitelností se lze setkat i u soukromých osob, kterými mohou být OSVČ či běžné obyvatelstvo.

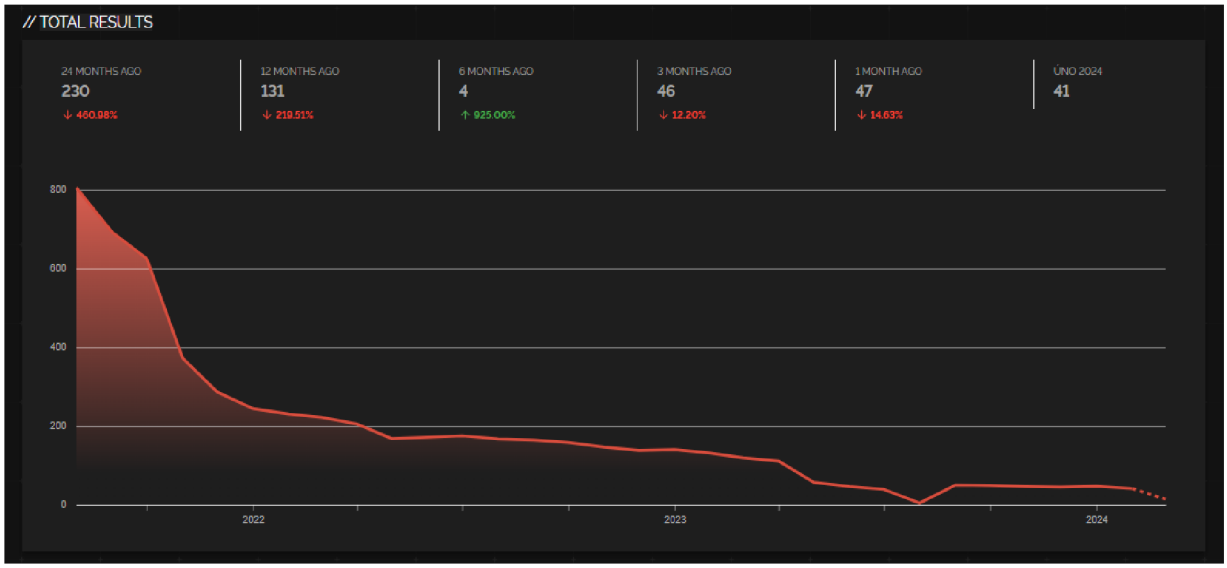
Jestliže by se mezi zranitelnými servery vyskytovala významná státní instituce či rozsáhlá soukromá společnost, jednalo by se o poměrně významné riziko oproti výskytu u lokální malé či středně velké firmy. V průběhu práce nebyla zaznamenána žádná významná instituce či společnost, která by na zranitelnosti byla zranitelná. Ačkoliv je sada zranitelností ProxyShell z roku 2021, lze se stále setkat i s nejednou zajímavou organizací, které se na seznamu potenciálně zranitelných serverů vyskytují.

4.2.1 Celkový pohled na problematiku na území ČR

Na území České republiky se nachází celkově 43 potenciálně zranitelných serverů a tento počet je do jisté míry neměnný. Mnoho organizací, kde je kybernetická bezpečnost na vysoké úrovni, již své servery zabezpečilo, když se o zranitelnostech začaly objevovat v bezpečnostní komunitě první zmínky.

Další velká vlna nastala při vydání doporučení NÚKIB. Problematika již v roce 2024 netvoří pro většinu organizací hrozbu, ale přesto lze dotčené servery stále nelézt. Situace je velmi podobná i v ostatních státech a nejedná se o specifickou situaci. V nástroji Shodan lze

získat mimo IP adresy a bližší informace o serverech, také i grafické znázornění výskytu zranitelností. Příkladem grafického zobrazení, který nástroj nabízí, je vidět na obrázku 2.



Obrázek 2: Historický vývoj ProxyShell v ČR (zdroj: Shodan.io)[35]

Konkrétně lze na obrázku 2 vidět historický vývoj zranitelností ProxyShell na území ČR. Prvním měsícem měření je srpen 2021, během kterého bylo dle nástroje Shodan celkově potenciálně zranitelných 805 serverů. Graf velmi strmě klesá a v aktuální době se počet pohybuje v nižších desítkách serverů. V srpnu 2023 pravděpodobně nastala chyba měření, protože bylo dle Shodan potenciálně zranitelných velmi málo serverů, konkrétně čtyři. Lze usuzovat, že se skutečně jedná o chybu, protože následující měsíc se počet opět navrátil na číslo 50 na kterém osciluje do dnešní doby.

4.2.2 Příklady potenciálně zranitelných organizací na území ČR

Jelikož je práce dostupná širší veřejnosti občanů, není vhodné všechny výsledky práce veřejně prezentovat. V metodice práce je uvedeno, že citlivé údaje nebudou zveřejněné, ale pro lepší pochopení problematiky a pro uvedení případu, je nutné, ač s využitím cenzury, některé zobecněné informace využít. Pro uvedení příkladu autor práce zvolil tři typové organizace, které se vyskytují na získaném seznamu potenciálně zranitelných organizací. Jak už bylo řečeno, na seznamu se nevyskytuje žádná významná organizace ani státní instituce, avšak některé společnosti mohou být zajímavé, i z důvodu, že se nejedná pouze o malé podniky, které jsou zcela bezvýznamné.

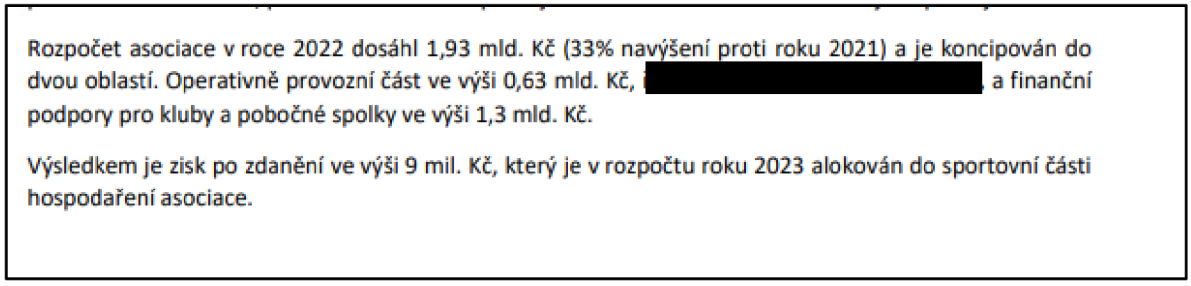
Autor práce zdůrazňuje, že se jedná pouze o potenciálně zranitelné servery a ve skutečnosti by útok využívající sadu zranitelností ProxyShell úspěšný být nemusel. Nástroj však musel zaznamenat indikátor na základě kterého data poskytuje a není zcela jisté kolik

falešně pozitivních nálezů se na seznamu může vyskytovat. Kdyby se o falešně pozitivní stopu jednalo, je pro organizaci vhodnější, když bude server zkontrolován, než kdyby neprobíhala údržba vůbec.

Blíže nespecifikovaná sportovní asociace

Na seznamu potenciálně zranitelných serverů se vyskytuje i blíže nejmenovaná sportovní organizace. Jedná se o organizaci, která zaměstnává lehce nad 100 pracovníků a roční tržby přesahují miliardu českých korun. Nese právní formu spolku se sídlem v Praze a má kořeny na začátku minulého století. Zaregistrovaní členové asociace jsou sportovní kluby a hráči, kterých je velmi vysoký počet. Podle všech dostupných informací se nejedná o organizaci, která by trpěla nedostatkem finančních prostředků, pozornosti běžného obyvatelstva a zcela jistě drží pevné místo v české společnosti, ač i tato organizace je, s údivem autora práce, na ProxyShell potenciálně zranitelná.

Jelikož se v asociaci pohybují vysoké finanční částky, představuje riziko kompromitace organizace poměrně velkou hrozbu. Poškození reputace nese riziko obdobné. Mezi sponzory asociace se řadí známé mezinárodní značky i české lokální společnosti. Jedná se například o Pepsi či Českou televizi jakožto mediálního partnera. Organizace má rozpočet nad miliardu českých korun, avšak není schopná odstranit své nedostatky v rámci své bezpečnosti. Na obrázku 3 jsou vidět podrobnější informace o finanční situaci asociace. Zranitelnosti jsou z roku 2021 a téhož roku došlo k vydání aktualizací. Obdobná organizace by takové nedostatky mít neměla. Je možné, že není Exchange a Outlook využíván, protože build serveru je z počátku roku 2021 a jedná se o verzi 2016. Jestliže je aktivně využíván, je zvláštní, že několik let nedošlo k jeho údržbě a spíše to vypadá, že se o IT infrastrukturu nikdo z organizace aktivně nestará.

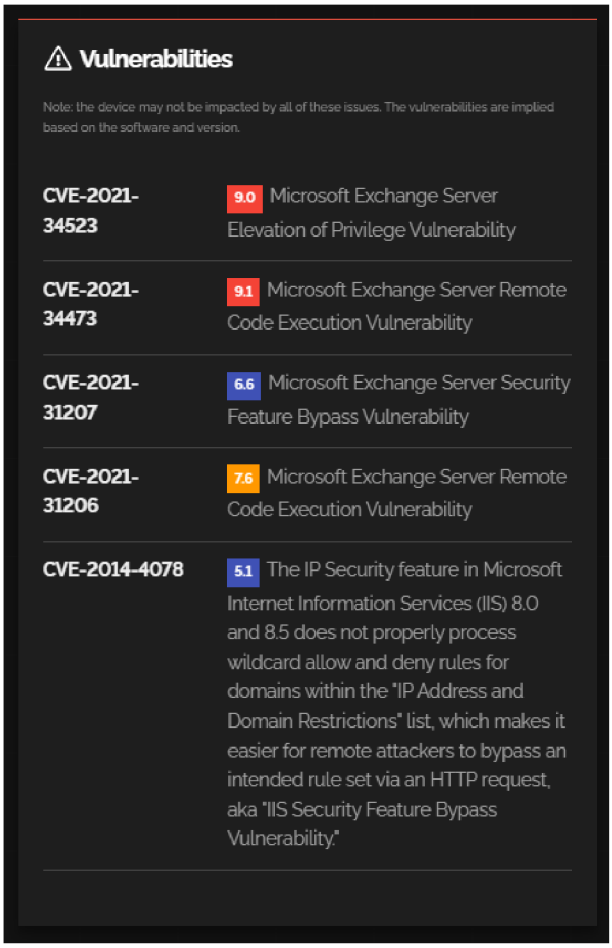

Rozpočet asociace v roce 2022 dosáhl 1,93 mld. Kč (33% navýšení proti roku 2021) a je koncipován do dvou oblastí. Operativně provozní část ve výši 0,63 mld. Kč, [redacted], a finanční podpory pro kluby a pobočné spolky ve výši 1,3 mld. Kč.

Výsledkem je zisk po zdanění ve výši 9 mil. Kč, který je v rozpočtu roku 2023 alokován do sportovní části hospodaření asociace.

Obrázek 3: Rozpočet asociace (zdroj: finanční výkaz nespecifikované asociace)

Dle Shodan má server dostupné následující porty 80, 179, 443 a 10443. Je potenciálně zranitelný na následující zranitelnosti CVE-2021-34523, CVE-2021-34473, CVE-2021-31207, CVE-2021-31206, CVE-2014-4078, z kterých první tři jsou ProxyShell. Na obrázku 4 lze vidět seznam všech zranitelností, na které nástroj upozorňuje. Mimo zranitelnosti Exchange serveru

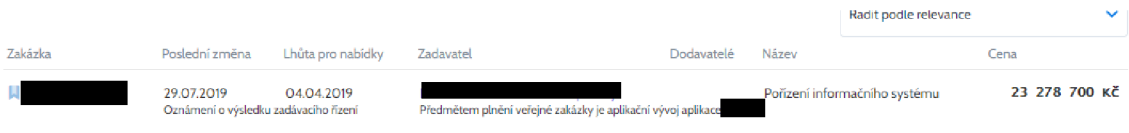
je potenciálně zranitelná i služba webového serveru Microsoft Internet Information, která by útočníkovi dovolila do jisté míry obejít sadu pravidel v IIS Security.



Obrázek 4: Seznam zranitelností serveru asociace (zdroj: Shodan.io)[35]

Dle Shodan lze z portu 10443 potenciálně zjistit, že organizace využívá Fortinet FortiGate-100F, což je NGFW firewall. Port 10443 je management port pro dané firewall řešení a není vhodné, aby byl takto dostupný z internetu.

Dle Hlídače státu se o asociaci lze dozvědět více informací. Jako podstatnou informaci lze považovat, že organizace v minulých letech vypsala veřejnou zakázku s odhadovanou hodnotou 50 000 000 českých korun na vývoj v informačních technologiích. Je to další náznak, že asociace netrpí finančními problémy a jistý přehled o informačních technologií musí v organizaci existovat, protože by v jiném případě podobná zakázka neexistovala. Na obrázku 5 lze vidět finální hodnotu veřejné zakázky, kterou asociace zaplatila dodavateli.



Obrázek 5: Veřejná zakázka (zdroj: Hlidacstatu.cz)[36]

V sekci dokumenty o zakázce lze získat veřejné i privátní klíče, které nejspíše sloužily k šifrování dokumentů pro potenciální dodavatele, avšak z principu věci, by neměl být privátní klíč veřejně dostupný. V takovém případě do jisté míry ztrácí svůj význam. Privátní klíč lze vidět na obrázku 6.

Obrázek 6: Privátní klíč pro dešifrování příloh veřejné zakázky (zdroj: autor)

Organizace by měla Exchange server aktualizovat na bezpečnou verzi, posílit oddělení informačních technologií, aby se situace již neopakovala a měla by dbát na další doporučení, které vedou ke zlepšení kybernetické bezpečnosti.

Blíže nespecifikovaný prestižní hotel

Mezi potenciálně zranitelné organizace lze zařadit i blíže nejmenovaný pětihvězdičkový hotel. Hotel má bohatou historii a je provozován už od začátku minulého století. Dle cen pokojů se nejedná o široce dostupný hotel a je zacílen především na zahraniční klientelu. Ačkoliv má hotel dlouholetou tradici, jeho aktuální provozovatel nese právní formu společnosti s ručením omezeným a je zapsána u Městského soudu v Praze. Jednatelem společnosti je občan Ruské federace a společník je společnost, která je zapsána v Moskvě v Ruské federaci.

Server má otevřené následující porty 25, 443, 444 a 5900 a je potenciálně zranitelný na následující zranitelnosti: CVE-2021-34523, CVE-2021-34473, CVE-2021-31207, CVE-2021-31206, CVE-2021-27065, CVE-2021-26858, CVE-2021-26857 a CVE-2021-26855. Všechny zranitelnosti souvisí s Exchange serverem a většina z nich spadá do kategorie "Remote Code Execution Vulnerability". Na obrázku 7 lze vidět seznam zranitelností z nástroje. Build Exchange serveru je dle Shodan velmi zastaralý, odpovídá Exchange serveru z roku 2013. Jestliže organizace aktivně server využívá a jeho skutečný stav

odpovídá stavu dle analýzy, je tento stav nedostačující a organizace by měla více dbát na kybernetickou bezpečnost.

Obrázek 7: Seznam zranitelností serveru hotelu (zdroj: Shodan.io)[35]

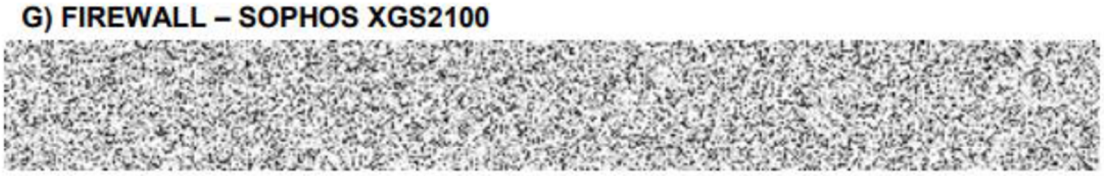
Organizace, ač je finančně zcela jistě dobře zabezpečena, do jisté míry opomíná bezpečnost kybernetickou, a proto je nutné, aby byl Exchange server aktualizován.

Blíže nespecifikovaný městský úřad

Často se lze setkat u veřejných institucí se zranitelnostmi způsobené zákonnou transparentností státních subjektů. Státní instituce musí do jisté míry poskytovat informace o svém fungování a mnohokrát lze z uveřejněných smluv na Registru smluv vyčíst podstatné informace o infrastruktuře, která je v rámci dané organizace využívána. Je zcela jasné, že organizace nechce, aby potenciálně útočník znal, jakou konkrétní verzi firewallu od konkrétního dodavatele používá.

Firewall lze označit jako příklad, protože v posledních měsících se objevilo několik zranitelností na produkty od společnosti FortiGate, útočník tedy i z Registru smluv zjistí, že je

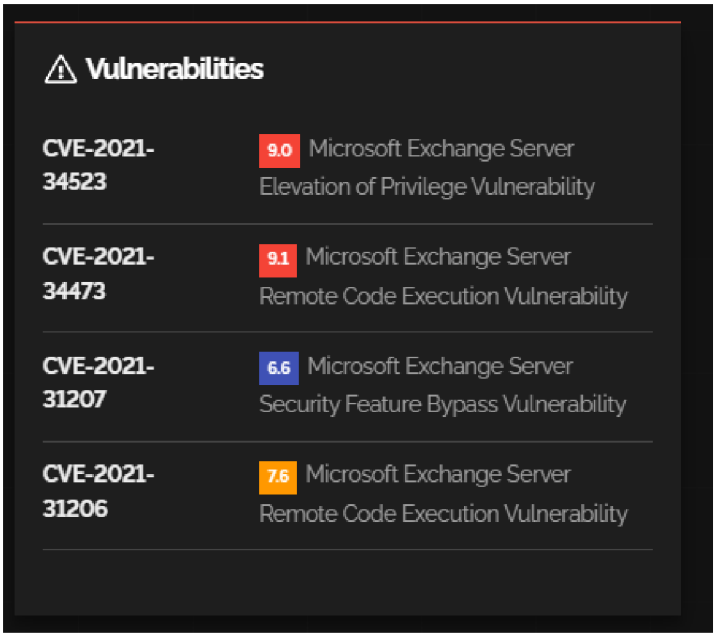
konkrétní řešení využíváno a má zranitelnost a lze tak započít útok. Bližší informace o FW jsou cenzurované, jak lze vidět na obrázku 8, ale během několika málo sekund si útočník může obstarat informaci o struktuře sítě, protože na Registru smluv lze dohledat i další produkty, které tento blíže nespecifikovaný úřad nakoupil a aktivně používá.



Obrázek 8: Informace o FW ve veřejné zakázce úřadu (zdroj: Hlidacstatu.cz)[36]

Příklad, který lze označit za nebezpečný, se objevuje pouze u malého počtu organizací. V Registru smluv se mohou vyskytovat i konkrétní jména pracovníků pracujících v kybernetické bezpečnosti. V dnešní době mnoho lidí využívá pracovní sociální sítě, jako je například LinkedIn, na které svou kariéru veřejně prezentují, ale pokud daný zaměstnanec nechce být spojován s působením v oblasti kybernetické bezpečnosti, je jeho kompromitace v podobě Registru smluv, nechtěná.

Dle nástroje Shodan má server otevřené následující porty 25, 80, 443, 587, 993, 1723 a 5222 a je potenciálně zranitelný na následující standardizované zranitelnosti CVE-2021-34523, CVE-2021-34473, CVE-2021-31207 a CVE-2021-31206, které lze vidět na obrázku 9. Jedná se konkrétně o verzi serveru z roku 2019, která byla naposledy aktualizovaná na začátku 2021.



Obrázek 9: Seznam zranitelností serveru úřadu (zdroj: Shodan.io)[35]

Na portu 1723 je dostupný Point-to-Point Tunneling Protocol (PPTP), který je z dnešního pohledu již zastaralý a není doporučováno ho využívat. Je používán ke vzdálenému přístupu pro implementování VPN. Informace získané z nástroje o protokolu PPTP lze vidět na obrázku 10. Základní specifikace neobsahuje šifrování dat a ani autentizaci. V roce 2012 bylo zabezpečení MS-CHAPv2, které PPTP protokol využíval, prolomeno. Na základě informací lze dodatečně zjistit, že úřad využívá síťové zařízení od společnosti MikroTik.

Obrázek 10: Otevřený port pro PPTP (zdroj: Shodan.io)[35]

Jelikož se jedná o městský úřad, měla by být dodržována bezpečnost na takové úrovni, aby nemohlo dojít ke kompromitaci citlivých údajů obyvatel a státu, či k poškození reputace ČR. Městský úřad by měl Exchange server aktualizovat a implementovat bezpečnější řešení, než je protokol PPTP.

4.3 Získání bližších informací o IP adresách

Pro získání bližších informací byl využit, v informačních technologiích, běžně využívaný WHOIS, pomocí kterého lze získat základní dodatečné informace. Jedná se ale především o velmi omezené informace, které se z velké části týkají ISP, kterého provozovatel serveru využívá ke připojení k internetu.

Všechny IP adresy autor práce dodatečně manuálně analyzoval a nevyskytuje se mezi nimi žádná státní instituce či nadnárodní společnost. Ač dané zranitelné společnosti mohou sloužit jakožto vektor útoku na zmiňované státní instituce či nadnárodní společnosti. Firmy, které se na seznamu vyskytují, mohou být v dodavatelském vztahu i s podstatnější a pro aktéry zajímavější obětí. Lze tedy obdobnou firmu kompromitovat a dále kompromitovat i následující společnost nebo pouze exfiltrovat data, které má dodavatel k požadované společnosti k dispozici.

Příklad WHOIS informací v tabulce 3 nejmenované společnosti potenciálně provozující zranitelný Exchange server na území ČR. Jedná se o informace, které nejsou z nástroje Shodan. Údaje jsou do jisté míry cenzurované, aby nemohlo dojít k přímému prorazení dotčeného serveru.

IP Adresa	Stát	Město	Země. šířka	Země. délka	ISP
85.93.X.X	CZ	Olomouc	49.XX	17.XX	Sprintel s.r.o.

Tabulka 3 Příklad WHOIS informací (zdroj: autor)

Využití API a Python scriptu

Pro usnadnění a částečnou automatizaci práce bylo pro získání bližších informací o IP adresách. zvoleno využití API a Python scriptu. Pokud bychom chtěli získávat informace bez jeho použití, celý proces by se časově prodloužil.

4.4 Překážky v rámci využití nástroje Shodan

Prvotní velkou překážkou, kterou musela práce překonat, je jednoznačně dostupnost nástroje. Celá řada nástrojů není přístupná zadarmo a je nutné takové produkty za nemalé náklady nakoupit a využívat licence. Shodan je právě jedním z podobných nástrojů a bylo nutné přístup obstarat. Autor práce si nebyl z počátku jistý, zda a za jakých podmínek to možné bude, ale po bližším průzkumu byla objevena možnost akademického členství, které lze pro účely bakalářské práce využít.

Využívání filtrů pro zranitelnosti jsou pro účely práce naprosto klíčové a bez přístupu není možné nástroj pro získání potenciálně zranitelných IP adres využít. Další překážkou je také i limitace zobrazení výsledků. Nástroj ve své bezplatné verzi tento počet limituje a je nutné dodatečné členství pro zobrazení. Limitován je i počet skenů, které je možné během jednoho měsíce vykonat.

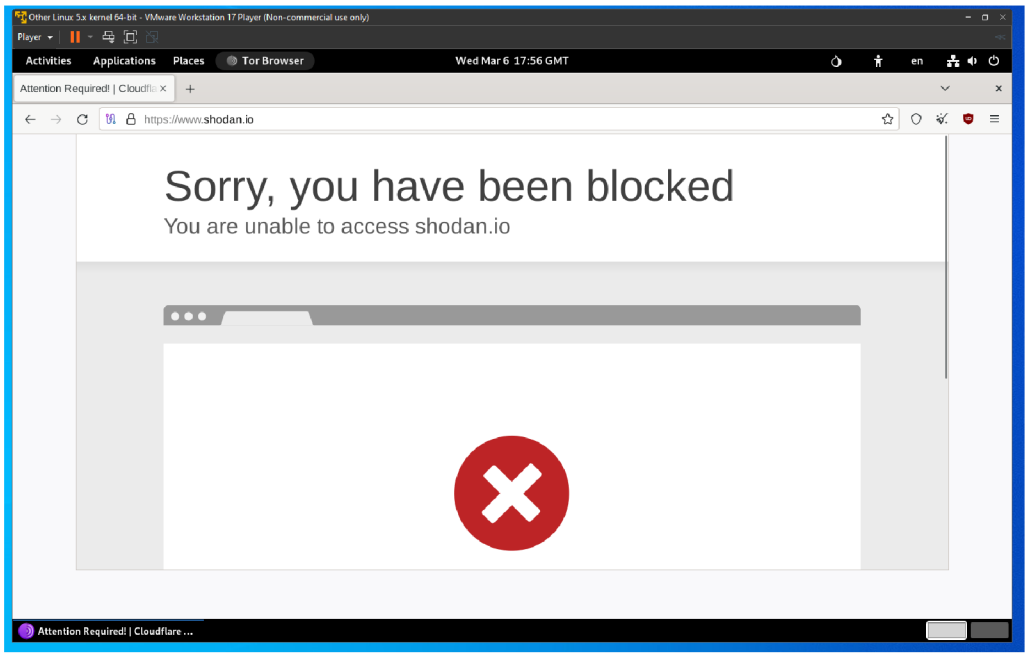
Aby autor práce přístup získal, musel kontaktovat přímo společnost stojící za Shodan. Společnost na webové stránce zmiňuje, že je celý proces usnadněn, pokud škola využívá doménu končící .edu, ač to není přímo podmínkou pro získání akademického členství. Celý proces udělení členství byl poměrně časově nenáročný a společnost po zhruba 10 dnech odpověděla a nástroj mohl být bezplatně používán

4.4.1 Bezpečnost při použití nástroje Shodan

V průběhu práce se nalezla dodatečná překážka a tou je zachování bezpečnosti při využití nástroje Shodan a čerpání informací z otevřených zdrojů. Určitým problémem by mohlo být

zpoplatnění nástroje i pro anonymnost a zachovávání OPSEC během analýzy problematiky. Společnost nenabízí platby v kryptoměně a bylo by nutné pro využití potřebných filtrů nakoupit členství, a to prostřednictvím platební karty, bankovní šeku nebo bankovním převodem. V takovém případě by společnost měla o uživateli nástroje mnoho citlivých informací.

Pokud je nástroj využit pro nelegitimní účely, je využita bezplatná verze bez registrace, která aktérům, i v této verzi, nabízí mnoho užitečných informací. Aktér nemusí skenovat porty a pomocí nástroje je získá během okamžiku. V případě použití pro akademické účely má poskytovatel nástroje přístup k univerzitní emailové schránce a následně k lokalitě, a tedy k zemi, jménu a na základě žádosti i k oboru studenta. Nástroj Shodan se aktivně také snaží zamezit připojení k nástroji z IP adres, které patří poskytovatelům VPN. Takovému připojení se snaží bránit. Situace není jiná ani u využití The Onion Router (Tor), u kterého k blokaci a nedostupnosti webové stránky také dochází.



Obrázek 11: Blokace Shodan na Tails v prohlížeči Tor (zdroj: autor)

Jestliže je toto chování požadované společností, není lehké ho obejít, protože všechny Tor Exit Nodes jsou veřejně známé a muselo by dojít ke kombinaci využití vícero řešení. Lze využít Tor bridge, který využívá serverů, které nejsou na seznamu Tor directory a nelze tedy všechny zablokovat.

Jednoduchý postup pro vyřešení situace by bylo připojení se z veřejné sítě. Pro účely práce je poskytovatel považován za bezpečného a pro umožnění přístupu disponuje citlivějšími údaji, než je IP adresa. Riziko ze strany ISP či bezpečnostních složek nepředstavuje hrozbu, protože je nástroj využíván pro legitimní účely.

4.4.2 Nedostupnost funkcionalit u API

Autor práce se snažil využít i API nástroje Shodan, ačkoliv bylo následně zjištěn fakt, že využití API není možné ani u akademického členství, respektive kombinace filtru pro zranitelnosti a API. Pokud by bylo možné API využívat, došlo by k zjednodušení celého procesu, jež by mohl být dokonce i automatizován. Rozhraní API lze využívat i pro pokročilejší případy, než je prosté zjednodušení procesu získání malého počtu IP adres. Pomocí rozhraní lze Shodan integrovat na jiné nástroje či do nástrojů vlastních. Práce by mohla být obohacena o zdokonalení celého procesu, ač je tento postup, jak už bylo řečeno, v případě malého počtu adres nepotřebný, došlo by otestování funkcionalit a lepšímu pochopení daného API, což by mělo pozitivní vliv, pokud by později autor práce integroval Shodan do nástrojů jako je Splunk, prostředí Azure, Gravwell či prostého nmap.

4.5 Nastínění možného řešení ve smyslu zabezpečení

Smyslem práce autora není pouze charakteristika historického stavu ve spojitosti se zranitelnosti ProxyShell. Každý den se objevují nové a nové zranitelnosti a organizace na tuto skutečnost musí reagovat. Během čerpání různorodých zdrojů došlo k závěru, že se u mnohých organizací lze setkat s typovými příklady nedostatků, které mohou organizaci oslabovat a pokud by došlo k jejich odstranění, organizace by mohla lépe odolat útoku, který využívá ProxyShell, ale také i obecně by se kybernetická bezpečnost zlepšila a organizace by byla připravená na nástrahy, které lze v budoucnosti očekávat. Autor práce se domnívá, že je nutné problematiku zlepšení kybernetické bezpečnosti charakterizovat podrobně, ačkoliv pro odstranění ProxyShell je zapotřebí pouze aktualizace serverů.

Nastínění možného řešení ve smyslu zabezpečení je součástí vlastní práce autora a výhradně autorova práce. Vychází ze syntézy předcházející části vlastní práce, teoretických východisek, zkušeností autora ze školního i pracovního prostředí, bakalářské praxe s vědomím existence zákonů: Zákona č. 412/2005 Sb., Zákona č. 181/2014 Sb. a Vyhlášky č. 82/2018 Sb., ač přímo z uvedených zákonů a vyhlášky nevychází.

4.5.1 Personální zabezpečení

Informační technologie a kybernetická bezpečnost je pouze tak silná jako jsou lidé, kteří je spravují, implementují a vytvářejí. Nejslabší součástí každého systému je vždy člověk. Proto je nezbytné, aby byla správně zavedena personální bezpečnost, ovšem na začátku celého cyklu se daný člověk musí o pracovní pozici ucházet. Nedostatek lidí na trhu práce na poli informačních technologií je znatelný, a proto jsou kapacity nedostatečné a personální

zabezpečení není naplněno a je poté i ztížena i personální bezpečnost. Obě problematiky spolu úzce souvisí. Pokud bude mít společnost nastavenou přísnou personální bezpečnost, například státní instituce a je potřebné psychologické vyšetření nebo i dokonce osvědčení z NBÚ, je nutné, aby byl dostatek uchazečů, jinak může docházet k tomu, že podmínkám nikdo nebude vyhovovat a daná pozice zůstane volná. Pro organizace je to riziko, při kterém vícero pozic musí vykonávat jedinec, který nemusí mít na potřebné technologie dostatečnou praxi či dostatek času.

Důležitým aspektem je i kvalita a zkušenosti zaměstnanců. Kvantita není vždy správná cesta. Více zaměstnanců si sice může povšimnout, že je jejich Exchange Server zranitelný na ProxyShell zranitelnosti, ovšem nemusí tomu tak vůbec být. Je lepší mít menší, ale kvalitou špičkový tým, nežli pracovníky, kteří v práci odpočítávají minuty, než půjdou domů, nechtějí se vzdělávat, nechodí na konference a školení a jejich rozvoj je nulový.

Pokud bude mít organizace dobře zabezpečenou obsazenost pracovních pozic, dojde k nepřímému navýšení kybernetické bezpečnosti a odolnosti na možná rizika, zranitelnosti a chyby. Největším problémem je nedostatek času, praxe, zkušeností a rozložení zodpovědnosti, když není zabezpečen dostatek zaměstnanců na poli informačních technologií v organizaci. V případě, kdyby organizace měla dostatek kvalifikovaných zaměstnanců a role kybernetické bezpečnosti, tak se autor práce domnívá, že dramaticky klesá pravděpodobnost, že by organizace byla zranitelná na ProxyShell.

4.5.2 Personální obsazení rolí kybernetické bezpečnosti

Zlepšit kybernetickou bezpečnost v organizaci lze i přes personální obsazení rolí dle zákona o kybernetické bezpečnosti. V současné době je personální zabezpečení IT sekcí společností složité. Na trhu je poměrně velký nedostatek lidí a pokud se uchazeč přeci jenom objeví, pro některé organizace může být složité jeho zaplacení a nemusí mít dostatek financí, aby mu dokázala obstarat požadované ohodnocení. V podoboru informačních technologií, který se zabývá především kybernetickou bezpečností je situace ještě více tristní. Problémová kombinace je kybernetická bezpečnost a státní správa. Úřady, ministerstva, bezpečnostní sbory a další státní instituce mají s obsazením, ne jenom rolí kybernetické bezpečnosti, ale všech zaměstnanců a příslušníků odborů a oddělení IT, nelehký úkol.

Pokud se budeme zaměřovat pouze na role kybernetické bezpečnosti dle zákona, jedná se o manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti, je naprosto vhodné, aby takové role existovaly. Pokud nejsou pro

organizaci povinné a organizace takové role nechce vytvářet, lze implementovat jejich ekvivalent.

Když bude organizace, subjekt podléhající zákonu, a bude absolvovat audit kybernetické bezpečnosti souladu se zákonem a vyhláškou o kybernetické bezpečnosti, či když bude audit probíhat i podle ISMS, dojde k nepříjemnému zjištění pro danou organizaci. Neobsazené role budou uvedené jakožto nálezy auditu, přitom se nemusí jednat pouze o zmiňované role. Nedostatečné personální zabezpečení informačních technologií jako celku se velice často v auditech také vyskytuje jakožto nález auditu. Takový nález je pro organizaci těžké napravit. Vedení si je takového problému často vědomo a nové zaměstnance personální oddělení hledá. Pokud dojde k situaci, že si takového problému vedení není vědomo, je tento nález z auditu dobrým hnacím motorem pro oddělení informačních technologií, jak na vedení vytvořit tlak, aby došlo k náboru nových zaměstnanců. Přeci jenom, někdo musí podepsat akceptační protokol ke zprávě z auditu a poté i s nálezy pracovat. Vytváří se tedy za toto rozhodnutí zodpovědnost, někdo ho musí nést, a to se může rozhodovat, že bude nejlepší volbou opravdu počet zaměstnanců posílit.

4.5.3 Architekt kybernetické bezpečnosti

Pro organizace je žádoucí, aby existoval člověk, který se zamýšlí nad celou koncepcí architektury bezpečnosti v daném podniku, specialista, který myslí do budoucna, bezpečnost rozvíjí a zlepšuje. Plánuje audity a certifikace ISMS a daný systém řízení bezpečnosti informací zavádí. Organizace, které takovou roli nemají, a kde řídí bezpečnost pracovník, který mimo bezpečnost má na starost řízení některého oddělení, ač to může být i právě kybernetická bezpečnost, nemusí mít dostatek času, aby se věnoval všemu potřebnému a může docházet ke zaměřování pozornosti na menší operativní činnost svých podřízeních, zabývání se byrokracií a další agendou vedenou z takové pozice. Horším příkladem může být osoba, která se zabývá správou a administrací systémů obohacenou i pro správu sítí. Sice do detailu problematice rozumí a zná technické podrobnosti, avšak opět se naráží na nedostatek času. Proto se autor práce domnívá, že je architekt kybernetické bezpečnosti pro organizaci vždy výhodou.

4.5.4 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je dalším klíčovým prvkem organizace. Osoba, která na problematiku bezpečnosti z této pozice nahlíží méně technickým pohledem, je však stejně důležitá jako architekt. Takový člověk by měl komunikovat s vedením společnosti a měl by poznatky prezentovat i lidem mimo informační technologie. Zároveň pro organizaci spravuje

interní směrnice a obstarává jejich vylepšování a odstavování nedostatků. Je nutno poznamenat, že samotné vytváření směrnic, nemusí přímo být jeho posláním. Spíše se jedná o určování obsahu a celkovém směřování směrnic a bezpečnostní dokumentace jako celku. Je vhodné, aby někdo určoval, jakým směrem se bude organizace na poli kybernetické bezpečnosti ubírat a technické zajištění poté navrhuje architekt.

V rámci struktury organizace by neměl být podřízen, oddělení informačních technologií, měl by se spíše nacházet ve struktuře vedení společnosti. Reprezentování organizace a komunikace, například s NÚKIBem a státními institucemi, je nedílnou součástí každé vetší organizace. Pokud by taková pozice neexistovala, jsou takové činnosti rozdrolené mezi ostatní pracovníky a dochází k zatěžování ředitele informačních technologií, který poté část takové agendy musí vykonávat a dochází leckdy k odpojení od vedení společnosti. Nebo se opět lze setkat s výkonem této práce zaměstnancem obstarávajícím kybernetickou bezpečnosti, který vede oddělení právě kybernetické bezpečnosti. Vykovávat svou práci, řídit několik pracovníků a zaštitovat roli manažera a architekta kybernetické bezpečnosti, není lehký úkol.

4.5.5 Auditor kybernetické bezpečnosti

Častokrát opomínanou rolí je auditor kybernetické bezpečnosti. Existují organizace, ve kterých efektivně fungují přechozí role, ale auditor by se hledal marně. I přesto že se jedná o stejně důležitou roli jako jsou role ostatní. V situaci, kdy organizace zaměstnává interního auditora kybernetické bezpečnosti, lze ušetřit na auditech externích. Audity vykonávané externím dodavatelem nemusí organizace obstarávat tak často než společnost, kde interní auditor nepůsobí. Celá problematika působí zvláštním dojmem, protože pro většinu větších firem je naprosto běžným faktem, že se v jejich strukturách nachází oddělení vnitřního auditu, které se zaměřuje především na finanční toky, podepsané smlouvy a celkové dění ve společnosti. Autor práce si tedy pokládá otázku, na kterou je těžké najít odpověď. Když je běžné oddělení vnitřního auditu, proč tedy není běžný i vnitřní auditor na kybernetickou bezpečnost nebo informační technologie jako celek?

4.5.6 Personální bezpečnost

Na problematiku personálního zabezpečení úzce navazuje i zmiňovaná personální bezpečnost. Personální bezpečnost je pro některé organizace naprosto klíčová a musí být nezbytně nutně nastavena na vysokou úroveň. Takové organizace jsou především vrcholné státní instituce a bezpečnostní sbory. Naproti tomu existují menší firmy a uskupení podnikajících osob, u kterých na personální bezpečnost není tak nutné nahlížet s vysokou

prioritou. Záleží na okolnostech a na informacích, se kterými se může budoucí zaměstnanec setkat.

Pokud bude budoucí zaměstnanec pracovat na místě, kde se bude seznamovat s utajovanými informacemi podle zákona 412/2005 Sb. nebo bude dokonce jejich původce a utajované informace bude vytvářet a klasifikovat, přistupovat do certifikovaných systémů dle NÚKIBu (dříve NBÚ) nebo utajované informace převážet a jakkoliv s nimi nakládat, je opravdu nezbytně nutné, aby byla personální bezpečnost na špičkové úrovni. Je vhodné, aby byla naddimenzovaná. Hodně parametrů vychází přímo ze zákona a je nutné osvědčení z NBÚ. Tento fakt státní institucím či firmám ulehčuje práci a jeden pilíř personální bezpečnosti je vytvořen. Lze požadovat i psychologické vyšetření a testování nebo implementovat podobné metody. Zaměstnanec by měl také svůj osobní a pracovní život žít v duchu principu nezbytné znalosti ("need to know") a popřípadě se dělit pouze o informace potřebné pro práce ostatních ("need to share"). Dále by měl ctít i pravidlo třetí strany a vždy chránit zdroj informací. Zaměstnanci v informačních technologií by měli rovněž znát TLP a řídit se podle něho a aplikovat ho při sdílení informací třetím stranám. Toto téma souvisí s klasifikací dat. Všechny problematiky jsou úzce spojené a nelze hovořit pouze o jedné zvlášť, tvoří nedělitelný komplexní celek.

Priorita personální bezpečnosti by se neměla určovat pouze podle informací, s kterými se může budoucí zaměstnanec seznamovat, ale i jaký aktér může na danou organizaci zaútočit, a na jaké zaměstnance se může zaměřit. V teoretické části práce autor zmiňuje aktéra úzce spjatého a finančně podporovaného cizí státní mocí, který může být dokonce i součástí cizí státní moci ve formě přímého napojení do struktury zpravodajské služby, tento aktér představuje vysoké riziko pro danou organizaci a pokud by organizace měla informace, že se na ní tento aktér může zaměřit, je vhodné mít nastavenou, u potřebných pracovníků, odpovídající personální bezpečnost.

Pokud není riziko kontaktu s klíčovými informacemi organizace či státu vysoké a nejedná se o informace podle zmiňovaného zákona, tak ve většině organizací existuje nulová personální bezpečnost. Ano, je pravda, že je požadován záznam z trestního rejstříku a dojde tak k vyfiltrování těch nejvíce rizikových osob, ale to nemusí být vždy dostatečné. Organizace ovšem musí postupovat podle zákona a jsou povinni ctít ochranu osobních údajů uchazeče. Některé otázky můžou být nemístné a nepochopitelné. Pokud personální bezpečnost obstarává personální oddělení, tak se velice často nejedná o personální bezpečnost, ale spíše o, častokrát nevhodné otázky, které nemají vypovídající charakter.

Riziko nespočívá pouze v infiltrace škodlivých zaměstnanců do organizace, ale i jejich možná manipulace a využití jejich slabin. Organizace si může pokládat různé otázky u kterých by si měla být jistá, že na daného zaměstnance neodpovídají. Pokud by byl zaměstnanec vydírán kompromitujícím materiálem, jak by se zachoval? Pokud by si k zaměstnanci v baru přisedla pohledná mladá slečna a po pár skleničkách alkoholu by se začala vyptávat na jeho práci, jak by zaměstnanec reagoval? Má zaměstnanec finanční problémy? Je závislý na alkoholu, drogách či hazardních hrách? Trpěl nebo stále trpí psychickými problémy? Má úzkosti? Cestoval v blízké době do zemí mimo EU/NATO? Žil dlouhodobě v zahraničí? Má blízko k cizí státní moci? Jak se projevuje na sociálních sítí? Jaké je jeho zámezí? Jaké jsou jeho finanční závazky a pohledávky?

V případě provozu Exchange serveru malou místní firmou jsou tyto otázky lehce nemístné, nejedná se o informační systém, který by zpracovával data s vysokou mírou důležitosti, u kterého je naprosto nezbytné, aby byla co nejméně narušena CIA (důvěrnost, integrita a dostupnost) Jedná se, přeci jenom, o emailový server malé společnosti a logicky z tohoto faktu vyplývá, že se nejedná o primární cíl aktérů, kteří mají takové zdroje, aby se takové otázky musely dopodrobna analyzovat. Riziko pro ochranu dat pro organizace nespočívá pouze v kybernetickém prostoru a je proto nutné na to nezapomínat.

Správně nastavená personální bezpečnost je důležitou součástí každé organizace. Snižuje se existence rizika, že by byla organizace v aktuální době zranitelná na ProxyShell. Pokud by některý aktér chtěl zneužít některé zranitelnosti, může k tomu využít i samotné pracovníky. Neznalost, neochotu ale i jejich slabost. Autor práce se domnívá, že je emailový server kritickou částí každé organizace a je důležité data ochraňovat a uvědomovat si rizika plynoucí z vlastních zdrojů.

4.5.7 Fyzická bezpečnost

Při tvorbě celkové koncepce kybernetické bezpečnosti organizace je nutné dbát i na bezpečnost fyzickou. Pokud bude primární cíl ochránit Exchange server, tak jeho aktualizování na nejnovější verzi, která už není zranitelná na ProxyShell, nemusí dostačovat. I v rámci organizace se lze setkat se záškodníky, kteří by se danou organizaci mohli snažit poškodit. Může se jednat o pouhého nespokojeného stávajícího pracovníka, ale i dopředu rozmyšlený útok vnitřního útočníka, který mohl být zmanipulován nebo do organizace přímo za takovým účelem pronikl. Pokud není dostatečně vyřešen přístup do budovy, může být vnitřní útočník i naprosto cizí člověk, který nemá se společností nic společného.

Vrcholné státní instituce a jiné státní celky, převážně v Praze, mají fyzickou bezpečnost na vysoké úrovni. Soukromý sektor se ve většině případů nenachází v podobné situaci. Fyzická bezpečnost podobných kvalit nedosahuje a je to dáno nejedním faktorem. Prvním z nich je častá neexistence oddělení, které by se přímo fyzickou bezpečností zabývala. Lze se setkat, že není personální bezpečnost řešena vůbec nebo jí obstarává do jisté míry oddělení informačních technologií. Mnoho organizací se nachází v rozlehlých kancelářských komplexech, u kterých se spoléhají na zajištění fyzické bezpečnosti právě provozovatelem těchto budov. Fyzická bezpečnost není pouze o vstupu do budovy ale i do jiných prostor a zaznamenávání neobvyklých situací a podobně. Dalšími faktory může být nedostatečná velikost organizace nebo nedostatek finančních prostředků či znalostí.

Při analyzování se autor práce nesetkal se žádnou velkou společností či významných veřejným subjektem, který by byl v současné době na ProxyShell zranitelný. Pokud by tedy útočník chtěl teto server kompromitovat, musí dojít k využití jiných vektorů k útoku. Neojedinělým způsobem může být i využití nedostatečné fyzické bezpečnosti a přímý fyzický přístup do místnosti se serverem.

Organizace by měla být rozdělena do zón s omezeným přístupem. Jednou z nich by měla být serverová místnost, kde se Exchange server nachází. Těchto místností může být několik. Přístup by neměl mít každý zaměstnanec a ani každý pracovník oddělní, které informační technologie obstarává. Tento přístup by měl být zaznamenáván a na základě těchto záznamů by se dala vytvořit behaviorální analýza v některém systému, která by automaticky sledovala neobvyklé chování, pokud by se fyzicky chtěl některý pracovník k Exchange serveru dostat a zkusil by to poprvé, může se jednat o chybu, ale pokud by došlo k vyzkoušení přístupu několikrát za sebou, může se jednat o pokus o průnik do dané místnosti.

Fyzické zabezpečení by nemělo být pouze u serverů, ale i jiných důležitých prostor organizace a lze takto zabezpečit celé oddělení a vytvořit zóny, do kterých mohou vstupovat pouze pověření zaměstnanci.

Autor práce se domnívá, že pouhé sledování trendů v kybernetické bezpečnosti a aktualizace serveru na nejnovější verzi, není dostatečná pro ochranu Exchange serveru a je vhodné implementovat do jisté míry i bezpečnost fyzickou.

4.5.8 Audit kybernetické bezpečnosti a penetrační testování

Penetrační testování je zcela zásadní a nedílná součást kybernetické bezpečnosti, ač je mnohokrát přehlížena a některé společnosti na penetrační testování nenahlíží s prioritou, která by byla odpovídající. Penetrační testy se nejčastěji uskutečňují při spouštění nového

informačního systému či jakékoliv zásadnějšího programu nebo většího zásahu do sítové infrastruktury. Není to ovšem pravidlo a testy lze provádět na jakékoliv aspekty kybernetické bezpečnosti a během jakýkoliv podmínek. Penetrační testy lze provést interně, ale mnohé společnosti nemají potřebné personální zdroje, nebo prostřednictvím externího dodavatele. Během testování jsou odhalované zranitelnosti, probíhá simulace aktéra snažícího se proniknout do systému a systém kompromitovat a je využito mnoho dalších metod.

Testy lze provádět jako black box, white box či gray box. Označení jsou velice intuitivní a naznačují s kolika informacemi bude jedinec nebo společnost disponovat během testování. Testování by mělo probíhat ve dvou vlnách, a to prvotní a poté kontrola, zda byly nálezy odstraněny a společnost už na dané nálezy není zranitelná.

Organizace pracující s citlivými informacemi mohou penetrační testování vnímat jako riziko. Pokud by se jednalo o rozsáhlé white box testování, dodavatel by disponoval informacemi, které by sice organizaci pomohly a na základě těchto informací by došlo ke zlepšení bezpečnosti, ale riziko by spočívalo právě v dodavateli. Organizace by měla sice podepsané patřičné smlouvy, ale jako vhodnou alternativu by mohl být NÚKIB, který bezplatně obdobné služby poskytuje a organizace by si byla jistá, že jsou citlivé informace u NÚKIBu v bezpečí a nehrozí vyzrazení a zneužití.

Během penetračního testování Exchange serveru by došlo bez pochyby ke zjištění, že je daný server zranitelný na zranitelnosti ProxyShell a byla by tato zranitelnost označena jako nález, který by organizace bezprostředně odstranila a během kontrolního testování by došlo ke zjištění, že daný server už zranitelný není. Autor práce silně doporučuje zakomponovat pravidelné penetrační testy do chodu společnosti

Penetrační testování a audity kybernetické bezpečnosti jsou v obdobné kategorii, i když se soustředí na rozdílné problematiky. Zatímco je penetrační testování velmi technického rázu a výsledkem jsou konkrétní technické nedostatky shrnuté v závěrečné zprávě, audit kybernetické bezpečnosti je rozdílný. Zaměřuje se především nepřímo na technickou stránku věci, bezpečnostní dokumentace, analýzy rizik, analyzování infrastruktury z pohledu použitých řešení, dbání zavedených a povinných standardů, přičemž není obvyklé, že by se během auditu technicky snažil někdo proniknout do auditovaného systému.

Audit kybernetické bezpečnosti se ve většině případů provádí na soulad se zákonem a vyhláškou o kybernetické bezpečnosti či na ISO 270001 a jako příprava na certifikaci ISMS. Auditor nemusí být ani přímo v organizaci a mít do organizace jakýkoliv přístup, i když takový postup by byl adekvátnější. Společnost může mít rozepsanou fyzickou bezpečnost místnosti se serverem, na kterém je daný informační systém, ale ne všechny informace musí nutně odpovídat

realitě. Proto je mimo audit kybernetické bezpečnosti také vhodné pro organizace zvážit interní provedení analýzy současného stavu a porovnání s veškerou dokumentací, kterou společnost disponuje.

Pokud by byl v organizaci proveden audit kybernetické bezpečnosti, snižuje se pravděpodobnost rizika výskytu zranitelností ProxyShell, a to tedy pokud organizace dbá na obsah vyhlášky a zákona a implementovala potřebné postupy a procesy. Oproti penetračnímu testování, zjištění zranitelností není jisté a jedná se spíše o nepřímý nástroj, který přispívá ke zvyšování kybernetické bezpečnosti.

4.5.9 Bezpečnost dodavatelského řetězce

Významný pilíř kybernetické bezpečnosti tvoří i bezpečnost dodavatelského řetězce, na kterou by se nemělo zapomínat. Výše jmenované součásti společně s dodavatelským řetězcem jsou naprosto klíčové v zajištění celkové bezpečnosti organizace. Během analyzování problematiky je důležité nezapomínat i na dodavatele a jejich implementaci bezpečnosti. Jsou rozdílné přístupy a lze se setkat pouze s dodáváním určitého softwaru, hardwaru, poradenských služeb, ale naproti tomu stojí i komplexní služby v informačních technologií. Takový dodavatel může spravovat infrastrukturu objednavatele, část infrastruktury nemusí být v přímé moci objednavatele a dodavatel se stává zásadním pro fungování organizace, která musí spoléhat na jeho dobře nastavenou bezpečnost.

To vlastně znamená, že personální bezpečnost a zabezpečení obsazenosti dostatkem zaměstnanců, provádění penetračních testů a auditů kybernetické bezpečnosti, sledování trendů kybernetické bezpečnosti a rozvoj informačních technologií v dané organizaci, není sledován pouze v rámci dotčené organizace, ale i u jejího dodavatele. Problematika se stává více komplexní a nepřehlednou, pokud se bude brát v potaz i subdodavatel, tedy dodavatel dodavatele. Celé spektrum faktorů, na které organizace musí spoléhat, a na kterých částečně stojí její bezpečnost, se rapidně zvyšuje.

Problematika zranitelností ProxyShell získává poměrově větší prostor a pravděpodobnost vyskytnutí a pozdního zareagování na situaci ve formě aktualizace, se zvyšuje, pokud je v každé organizaci provozován Exchange server, který na tuto zranitelnost může trpět. Organizace si musí být vědoma, že toto riziko existuje a pracovat s ním. V předchozí části práce bylo nalezeno mnoho potenciálně zranitelných serverů. Je na místě si uvědomit, že dané zranitelné organizace můžou na trhu vystupovat jakožto dodavatel pro ostatní.

Pokud by organizace, která sama neprovozuje celou svou infrastrukturu, chtěla provést interní či externí audit kybernetické bezpečnosti souladu se zákonem a vyhláškou

o kybernetické bezpečnosti nebo chtěla některý ze svých systémů certifikovat na ISMS, je situace obtížnější. Pro takové audity by byla nutná součinnost, protože logicky není část infrastruktury v její přímé moci a nemusí pro daný audit mít všechny potřebné informace.

4.6 Problematika Microsoft Exchange Server

Během praktické práce a při využití nástroje Shodan se autor práce setkával s faktem, že na Microsoft Exchange server existuje nespočet zranitelností a podobné postupy použité při analyzování situace lze aplikovat i na jiné zranitelnosti. Nastává otázka, zda je opravdu Exchange server navržen nedostatečně nebo problematika spočívá v jeho vysoké rozšířenosti. Exchange server lze najít v celé řadě společností a na světě ho používají desítky tisíc organizací. Dle nástroje Shodan je z internetu přístupných ke dni 24.02 2024 celkově 159 071 Outlook webových rozhraní, které lze, i graficky znárodněné, vidět na obrázku 12 Pokud budeme Microsoft srovnávat s konkurencí, dnes už velmi zřídka používanou, kterou je IBM a Domino server, zranitelnosti se nevyskytují s frekvencí jako tomu je u Microsoftu.

Celkový počet Exchange serverů bude větší, než je počet Outlook webových rozhraní, které Shodan zobrazuje. Není to zanedbatelný počet a mnohokrát lze právě Exchange server využít jakožto prvotní vektor útoku.

Obrázek 12: Počet Outlook klientů dostupných z internetu (zdroj: Shodan.io)[35]

Exchange server se každým rokem stává oblíbeným cílem aktérů, kteří obdobné zranitelnosti využívají pro svůj prospěch a k průniku do systému organizace. V poslední době lze jmenovat slavné sady zranitelností, mezi které se řadí převedším ProxyLogon

(CVE-2021-26855), ProxyShell (CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207) a ProxyNotShell (CVE-2022-41040 and CVE-2022-41082). Postup zjištění zranitelností a návrhy ve smyslu zabezpečení lze aplikovat na všechny jmenované zranitelnosti Exchange serveru.

4.6.1 Pohled na problematiku mimo ČR

Microsoft Outlook je široce využíván po celém světě a není tomu jinak ani u našich sousedních zemí. Vývoj, především v západní Evropě, postupuje značně odlišným tempem a častokrát se lze setkat s využíváním starší technologie v rámci České republiky, ačkoliv řešení od Microsoftu je velmi rozšířené i u nás. Důležité je dbát na to, aby nedocházelo k porovnání problematik, které nemají totožný základ.

Pokud by se v jiné zemi výrazně více používala některá technologie než u nás, je pravděpodobné, že bude existovat i více potenciálně zranitelných zařízení a nelze pouze nahlížet na velikost dané země a počet obyvatel. Jsou země, ve kterých existuje více organizací, více se zaměřují na technologie, více podnikají a více se v daném prostředí objevují zahraniční korporace. Lze ale i předpokládat, že bude kybernetická bezpečnost na lepší úrovni, a naopak bude počet zranitelných zařízení klesat.

Procentuální vyjádření potenciálně zranitelných serverů na počet obyvatel je srovnatelné s Německem. Polsko je sice větší země, ale počet potenciálně zranitelných serverů je výrazně menší. Zajímavým faktem, který je vidět na obrázku 13, je, že se v Praze nachází půlka všech českých serverů, zatímco v Berlíně se jedná pouze o zlomek celkového počtu, jež osciluje na úrovni 300, tedy zhruba osmkrát více než je celkový počet u nás.

Obrázek 13: ProxyShell a sousední státy (zdroj: Shodan.io)[35]

5 Zhodnocení a doporučení

Následující kapitola se zabývá zhodnocením situace, které lze charakterizovat jako nastínění uceleného pohledu na problematiku. Ve druhé části je uvedeno a shrnuto doporučení na základě možného návrhu zabezpečení, kterému se vlastní práce rovněž věnovala.

5.1 Zhodnocení situace

Mnohé organizace nevnímají kybernetickou bezpečnost jako prioritu a dochází k přerozdělování finančních a personálních zdrojů na jiná místa. Zlepšení kybernetické bezpečnosti nemusí být na první pohled viditelné a nedostatky mohou vyústit až k závažnému kybernetickému bezpečnostnímu incidentu u organizace. Incident takového rozsahu může způsobit nemalou finanční ztrátu, poškození reputace nebo i lidské životy, pokud se jedná o bezpečnostní sbory nebo zdravotnické zařízení.

Zhodnocení výsledků z nástroje Shodan tvoří náhled do českého prostředí informačních technologií. Potenciálně zranitelných serverů se na území ČR stále vyskytuje nezanedbatelné množství a situace je spíše statická, než aby docházelo ke snížení počtu serverů, které mohou na ProxyShell být zranitelné.

Zhodnocení situace se nezaměřuje pouze na území a podmínky v rámci ČR. Situace byla prozkoumána i v sousedních státech a práce dospěla k výsledku, že je situace obdobná, ač v okolních státech mohou být rozdílné podmínky a nelze přímo zranitelnosti ProxyShell porovnávat na počet obyvatel a velikost dané země.

5.2 Doporučení

Obrana proti ProxyShell je relativně jednoduchá a organizace už v prvních vlnách zneužívání této sady zranitelností mohli implementovat postupy, které bez větších problémů mohly kompromitaci předcházet. Na počátku stojí fakt, že organizace se musí o hrozbě a zranitelnosti, která se začíná nově objevovat, dozvědět. Nelze se efektivně bránit něčemu o čem organizace nemá informace, i když by správně postavená infrastruktura s vhodně zvoleními prvky a dobře navrženou a aplikovanou kybernetickou bezpečností, měla být schopná částečně odolávat i útokům, které jsou zcela neznámé. Organizace by proto měla sledovat nové informace a trendy v oblasti kybernetické bezpečnosti.

Všechny prvky by měly dostávat pravidelné aktualizace a nemělo by docházet k používání zastaralého zranitelného hardwaru a softwaru. Organizace by měla tedy včasně aktualizovat Exchange server na nejnovější verzi a pokud tomu při vydání nedošlo, měla by

poté dbát na upozornění pracovníků z Microsoftu a NÚKIBu, které na sadu zranitelností aktivně upozorňovali. Problematika není jednostranná a nejnovější aktualizace nemusí být vždy doporučené, proto je nutné dbát primárně na doporučení výrobce a aktuální kompozici prvků, která se v organizace využívá.

Organizace by do svého zabezpečení měla implementovat prvky personální bezpečnosti, personální zabezpečení, fyzickou bezpečnost, bezpečnost dodavatelského řetězce, provádění auditů kybernetické bezpečnosti, provádění penetračního testování a měla by komunikovat se státními institucemi.

Ve finální fázi by se organizace měla poučit a mělo by docházet ke zlepšování povědomí o kybernetické bezpečnosti. Vzdělávání není vhodné pouze pro pracovníky informačních technologií, ale i pro řadové zaměstnance a vrcholné vedení společnosti. Lze využít interní či externí školení, certifikace v oblasti kybernetické bezpečnosti, návštěvy konferencí a přednášek a celkový zájem o problematiku. Organizace, která všechny doporučení aplikuje do svých procesů, nebude odolná pouze na ProxyShell, ale bude mít silný základ i proti ostatním hrozbám.

6 Závěr

Během práce bylo zaznamenáno celkově 43 potenciálně zranitelných serverů, ke všem byly získané bližší WHOIS informace a autor práce ručně všechny IP adresy prověřil a následně 3 vybrané nespecifikované organizace blíže charakterizoval. Byl vybrán vzorek, který zachovával různorodost potenciálně zranitelných serverů, aby byla uchována prvotní myšlenka, že na ProxyShell může být zranitelný kdokoliv. Bezpečnost se proto nesmí opomínat v žádné organizaci.

Existuje přesto reálná možnost, že servery nemusí být skutečně zranitelné a jedná se o mylné označení ze strany Shodan, existuje i možnost výskytů honeypot serverů, práce uvedené skutečnosti reflektuje a pojednává pouze o potenciálně zranitelných serverech.

Nedostatky se mohou projevovat ve všech oblastech kybernetické bezpečnosti. Jedná se o problematiku komplexní a práce se na situaci zaměřuje z mnoha pohledů a nelze staticky charakterizovat pouze přímé souvislosti, které s ProxyShell souvisí. Všechny aspekty bezpečnost posilují a tvoří jeden komplexní celek, na kterém se nutně musí podílet celá řada zdrojů organizace. Zranitelnost nemusí být pouze technického charakteru a aktéři se na poli informačních technologií zaměřují na celé spektrum možností, pomocí kterých lze organizaci kompromitovat za účelem narušení důvěrnosti, integrity nebo dostupnosti.

Ačkoliv jsou organizace zranitelné na ProxyShell, existuje nespočet různých zranitelností a každým dnem se objevují nové. Nelze sledovat všechny nové informace a mnohdy dochází k souběhu několika projektů, na kterých se podílí i pracovníci provozní a infrastrukturní části oddělení informačních technologií. Problematika nespočívá pouze v nedostatku času, ale také i v nedostatku finančních prostředků, které nemusí vždy směřovat do provozní sekce organizace.

V průběhu práce by mohlo dojít k implementaci API rozhraní pro automatizaci procesu nebo k rozšíření práce i na praktické využití a simulaci útoku ProxyShell. Autor práce během praktické části analyzování zranitelností narazil na překážky, které se ovšem podařilo úspěšně překonat.

Jak bylo řečeno, práce pouze staticky necharakterizuje ProxyShell a lze poznatky, jež autor práce v průběhu získal, použít i obecně v rámci problematiky kybernetické bezpečnosti. Organizace, které jsou zranitelné, mohou své nedostatky napravit.

7 Seznam použitých zdrojů

1. NCSC, National Cyber Security Centre. What is cyber security? [online]. [cit. 2023-08-13]. Dostupné z: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
2. IT Governance. What Is the CIA Triad and Why Is It Important? [online]. [cit. 2023-08-13]. Dostupné z: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
3. Fortinet. What is the CIA Triad? [online]. [cit. 2023-08-13]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/cia-triad
4. ISO, International Organization For Standardization. ISO/IEC 27001 Information security management systems [online]. [cit. 2023-08-13]. Dostupné z: https://www.iso.org/standard/27001
5. EVROPSKÝ PARLAMENT. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. In: . ročník 2016, 2016/679. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679
6. Cloudflare. What is an attack vector? [online]. [cit. 2023-08-13]. Dostupné z: https://www.cloudflare.com/learning/security/glossary/attack-vector/
7. NIAZI, Mahmood. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study [online]. 2020 [cit. 2023-08-13]. Dostupné z: https://www.researchgate.net/publication/338419380_Cyber_Security_Threats_and_Vulnerabilities_A_Systematic_Mapping_Study
8. Red Hat. What is a CVE? [online]. 2021 [cit. 2023-08-13]. Dostupné z: https://www.redhat.com/en/topics/security/what-is-cve
9. Cisco. What Is an Exploit? [online]. [cit. 2023-08-13]. Dostupné z: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html
10. Check Point Software Technologies. What is a Zero Click Attack? [online]. [cit. 2023-08-13]. Dostupné z: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-zero-click-attack/

11. ENSIGN, Prescott. Privatized espionage: NSO Group Technologies and its Pegasus spyware [online]. 2022 [cit. 2023-08-13]. Dostupné z: https://www.researchgate.net/publication/365948186_Privatized_espionage_NSO_Group_Technologies_and_its_Pegasus_spyware
12. DIMITROV, Dimitar a Evgeni ANDREEV. Cyber Espionage: A New Era Of Intelligence Gathering And Threats [online]. 2023 [cit. 2023-08-13]. Dostupné z: https://www.researchgate.net/publication/371472221_CYBER_ESPIONAGE_A_NEW_ERA_OF_INTELLIGENCE_GATHERING_AND_THREATS. Vasil Levski National Military University.
13. Crowdstrike. What Is a Threat Actor [online]. [cit. 2023-08-13]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/threat-actor/
14. Trend Micro. Hacktivism 101: A Brief History and Timeline of Notable Incidents. [online]. 2015. [cit. 2023-08-16]. Dostupné z: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents
15. EuRepoC, The European Repository of Cyber Incidents. Advanced Persistent Threats (APTs) [online]. 2022. [cit. 2023-08-16]. Dostupné z: https://eurepoc.eu/advanced-persistent-threats-apts/
16. Malpedia Fraunhofer FKIE. Equation Group. [online]. 2022. [cit. 2023-08-16]. Dostupné z: https://malpedia.caad.fkie.fraunhofer.de/actor/equation_group
17. NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost. Vláda schválila strategii kybernetické bezpečnosti na následujících pět let [online]. 2020 [cit. 2023-08-13]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1657-vlada-schvalila-strategii-kyberneticke-bezpecnosti-na-nasledujicich-pet-let/
18. NARAINE, Ryan. Microsoft Will Name Threat Actors After Weather Events. [online]. 2023. [cit. 2023-08-16]. Dostupné z: https://www.securityweek.com/microsoft-will-name-apts-actors-after-weather-events/
19. Swiss Cyber Institute. 3 Advanced Persistent Threat (APT) Examples You Should Know About. [online]. 2021. [cit. 2023-08-16]. Dostupné z: https://swisscyberinstitute.com/blog/guide-of-advanced-persistent-threat-apt/
20. Carnegie Endowment for International Peace. Attribution and Characterization of Cyber Attacks.[online]. 2022. [cit. 2023-08-16]. Dostupné z: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698

21. Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.
22. CISA, Cybersecurity And Infrastructure Security Agency. Traffic Light Protocol (TLP) Definitions and Usage [online]. [cit. 2023-08-13]. Dostupné z: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage
23. NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost. Doporučení k používání protokolu TLP ke sdílení chráněných informací [online]. 2020 [cit. 2023-08-13]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/
24. NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost. Doporučení k používání protokolu TLP ke sdílení chráněných informací. [online]. 2022 [cit. 2023-08-19]. Dostupné z: https://nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/
25. ORANGE, Tsai. ProxyLogon is Just the Tip of the Iceberg: A New Attack Surface on Microsoft Exchange Server! [online]. (PDF). [cit. 2023-08-22]. Dostupné z: https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf
26. NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost. Upozornění na aktivní zneužívání zranitelnosti Microsoft Exchange Server - ProxyShell. [online]. 2021 [cit. 2023-09-01]. Dostupné z: https://nukib.cz/cs/infoservis/hrozby/1739-upozorneni-na-aktivni-zneuzivani-zranitelnosti-microsoft-exchange-server-proxyshell/
27. SANDBU, Marius. Windows Ransomware Detection and Protection: Securing Windows Endpoints, the Cloud, and Infrastructure Using Microsoft Intune, Sentinel, and Defender. Birmingham: Packt Publishing, Limited, 2023. ISBN 9781803230610. Dostupné z: https://ebookcentral.proquest.com/lib/czup/detail.action?docID=30406673
28. NÚKIB, Národní úřad pro kybernetickou a informační bezpečnost. Upozornění na kampaň zneužívající zranitelnosti Exchange Server. [online]. 2021 [cit. 2023-09-01]. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1766-upozorneni-na-kampan-zneuzivajici-zranitelnosti-exchange-server/

29. Ministerstvo vnitra České republiky. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2021. [online]. (PDF). 2022. [cit. 2023-09-01]. Dostupné z: https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-verejneho-poradku-a-vnitrni-bezpecnosti-na-uzemi-ceske-republiky-v-roce-2021.aspx
30. CHAUHAN, Sudhanshu a Nutan Kumar PANDA. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Saint Louis: Elsevier Science & Technology Books, 2015. ISBN 9780128019122. Dostupné z: https://ebookcentral-proquest-com.infozdroje.czu.cz/lib/czup/reader.action?docID=2025500
31. ORTEGA, José Manuel. Mastering Python for Networking and Security: Leverage the Scripts and Libraries of Python Version 3. 7 and Beyond to Overcome Networking and Security Issues. Birmingham: Packt Publishing, Limited, 2021. ISBN 9781839216213. Dostupné z: https://ebookcentral.proquest.com/lib/czup/reader.action?docID=6423660
32. Shodan. Shodan Products. [online]. [cit. 2023-09-01]. Dostupné z: https://www.shodan.io/about/products
33. Shodan. Understanding Shodan Vulnerability Assessment. [online]. [cit. 2023-09-01]. Dostupné z: https://help.shodan.io/mastery/vulnerability-assessment
34. ZHOU, Jianying, Xiapu LUO, Qingni SHEN a Zhen XU. Information and Communications Security: ICICS 2019. Beijing: Springer International Publishing, 2020. ISBN 9783030415792. Dostupné z: https://ebookcentral-proquest-com.infozdroje.czu.cz/lib/czup/detail.action?docID=6112944&query=9783030415792
35. Shodan. Shodan Search Engine. [online]. [cit. 2024-02-24]. Dostupné z: https://www.shodan.io/search
36. Hlídač státu. Výsledky vyhledávání. [online]. [cit. 2024-02-24]. Dostupné z: https://www.hlidacstatu.cz

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek