POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY
V PRAZE

BAKALÁŘSKÁ PRÁCE

2024 ANETA REJHONOVÁ

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra krizového řízení

Kyberútoky jako problém současnosti

Bakalářská práce

Cyberattacks as a current problem

Bachelor thesis

VEDOUCÍ PRÁCE

JUDr. Vladimír SOUČEK

AUTOR PRÁCE

Aneta REJHONOVÁ

PRAHA

2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 15. února 2024

Aneta Rejhonová

Poděkování

Ráda bych poděkovala svému vedoucímu bakalářské práce JUDr. Vladimíru Součkovi za odborné vedení, za pomoc a cenné rady při zpracování této práce. Také musím poděkovat své rodině za trpělivost a podporu během celého studia a Bc. Janu Nechutnému za podporu při psaní této práce.

Anotace

Bakalářská práce se zabývá kybernetickou bezpečností a hrozbami, které jsou v dnešní době čím dál častější. V práci jsou popsány nejčastěji se vyskytující typy kyberútoků. V druhé části práce jsou popsány subjekty státní správy spojené s problematikou kybernetické bezpečnosti a jejich role při řešení kybernetických útoků. Na základě případů kyberútoků jsou na závěr uvedeny opatření, které by mohly předejít nebo zmírnit dopady kyberútoků.

Klíčová slova

Kybernetický útok * Hacking * NÚKIB * Kybernetická obrana * kybernetická hrozba * opatření

Annotation

The bachelor thesis deals with cyber security and threats, which are becoming increasingly common nowadays. The thesis describes the most frequently occurring types of cyber attacks. The second part of the thesis describes the entities of public administration related to cyber security issues and their roles in addressing cyber attacks.

Keywords

Cyber attack * Hacking * NÚKIB * cyber defence * cyber threat * measures

Obsah

Úvod

Důvodem pro volbu tématu kyberútoků pro tuto bakalářskou práci byl fakt, že v digitální éře, v níž se lidé stále více spoléhají na moderní technologie, jsou kybernetické hrozby stále častější a sofistikovanější. Průběh a následky kybernetických útoků mohou ovlivnit spoustu lidí jak v pracovním, tak i osobním životě.

Cílem této bakalářské práce je přiblížit problematiku kybernetiky v České republice, posoudit současný stav a zpracovat opatření ke zlepšení stavu v oblasti kybernetické bezpečnosti.

Teoretická část vychází z odborné a populárně naučné literatury a je rozdělena do tří kapitol. První kapitola pojednává o právních předpisech a jiných dokumentacích. V této kapitole jsou představeny zákony a vyhlášky, které upravují problematiku kybernetiky. Druhá kapitola je věnována vysvětlení pojmů a terminologie nezbytné k porozumění problematice kybernetické bezpečnost. Třetí kapitola je nejobsáhlejší, a proto je rozdělena na dvě podkapitoly. První podkapitola se zabývá typy kyberútoků. Podrobně popisuje vybraných 8 druhů spolu s průběhem útoku. Druhá podkapitola se zabývá kyberútočníky, kde je definován kyberútočník a uvedeno rozdělení kyberútočníků.

Praktická část je rozdělena do čtyř kapitol. Čtvrtá kapitole se zaměřuje na posouzení připravenosti České republiky na aktuální hrozby kyberútoků. Tento rozbor zahrnuje hodnocení klíčových institucí zapojených do snah o kybernetickou bezpečnost, včetně Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), Národního centra kybernetické bezpečnosti, Vládního CERTu, týmu CSIRT.CZ a Vojenského zpravodajství. Pátá kapitola se zaměřuje na řešení kybernetických útoků v ČR, jsou zde také rozebrány doporučení, které je dobré dodržovat při kybernetickém útoku. Šestá kapitola je věnována SWOT analýze, kde jsou rozebrány silné a slabé stránky, příležitosti a hrozby. Sedmá kapitola obsahuje návrhy a opatření zaměřené na zlepšení stavu kybernetické bezpečnosti v České republice.

1. Právní předpisy a další dokumentace

V posledních letech se svět potýká čím dál více s kyberútoky, proto dochází k ohromnému nárustu mezinárodní právní úpravy, která se zaměřuje na kyberprostor a činnost osob pohybujících se v něm.

V České republice se problematika kybernetické bezpečnosti poprvé začala probírat v roce 2000, kdy Ministerstvo vnitra ČR vydalo Koncepci boje proti trestné činnosti v oblasti informačních technologii včetně Harmonogramu opatření. Tam rozpracovává otázky kybernetické bezpečnosti a uvádí – „*Je úlohou státních orgánů vytvářet stabilní a bezpečné prostředí, které dává občanům oprávněně pocit právní jistoty při využívání moderních informačních a komunikačních prostředků.“* [1]

V roce 2011 byla přijata Strategie pro oblast kybernetické bezpečnosti ČR na období let 2011 až 2015. V tuto dobu byla i převedena gesce na NBÚ z původního MVČR. [2]

NBÚ v polovině roku 2013 předložil Vládě návrh zákona o bezpečnosti, a jelikož legislativní proces byl bez větších připomínek, od 29. srpna 2014 byl platný zákon č. 181/2014 Sb., o kybernetické bezpečnosti, s účinností od 1. ledna 2015. Avšak od 5. srpna 2022 byl tento zákon nahrazen zákonem č. 226/2022, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento zákon stanovuje práva a povinnosti osob a rozsah pravomocí orgánů veřejné moci v oblasti kybernetické bezpečnosti. Tento legislativní akt zahrnuje odpovídající směrnici Evropské unie, a zároveň respektuje platné nařízení Evropské unie. Dále upravuje zabezpečení bezpečnosti elektronických komunikačních sítí a informačních systémů. [3]

Hlavními cíli zákona je stanovení minimálních standardů bezpečnostních opatření, vylepšení identifikace kybernetických bezpečnostních incidentů,

[1] Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření
[2] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
[3] Zákon č. 226/2022 Sb., o kybernetické bezpečnosti

implementování systému hlášení kybernetických bezpečnostních incidentů, zavedení postupů pro reakci na kybernetické bezpečnostní incidenty nebo také upravení pravomocí dohledových pracovišť.[4]

Co se týče právních aktů vydaných Evropským parlamentem a Radou o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, je zde směrnice NIS2. Tato směrnice přináší tak radikální novelizace, že se Národní úřad pro kybernetickou bezpečnost (dále jen NÚKIB) rozhodl připravit zcela nový zákon o kybernetické bezpečnosti, který by měl vstoupit v účinnost v říjnu 2024. [5]

Dalším zákonem EU je zákon o kybernetické solidaritě. Zákon má za úkol posílit schopnosti Evropské unie v odhalování, přípravě a reakci na vážné a rozsáhlé kybernetické hrozby a útoky. Tento návrh zahrnuje vytvoření evropského štítu kybernetické bezpečnosti, který spojuje bezpečnostní operační střediska propojená v celé EU, a komplexní nouzový mechanismus pro zlepšení kybernetického postavení Evropské unie.[6]

Výchozími dokumenty, které upravují zajištění kybernetické bezpečnosti ČR jsou Akční plán kybernetické bezpečnosti České republiky a Národní strategie kybernetické bezpečnosti.

V první části národní strategie kybernetické bezpečnosti ČR je popsáno, kdo a jak se podílí na systému zajištění kybernetické bezpečnosti. Především je zde uvedeno, že za řízení, fungování a zajištění celého bezpečnostního systému ČR je odpovědná vláda ČR. Gestorem a ústředním orgánem pro oblast kybernetické bezpečnosti je podle zákona 226/2022 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, NÚKIB. [7]

[4] NÚKIB. Návrh nového zákona o kybernetické bezpečnosti vstupuje do další fáze. Online. NÚKIB. ©2023. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1969-navrh-noveho-zakona-o-kyberneticke-bezpecnosti-vstupuje-do-dalsi-faze/. [cit. 2023-10-29].
[5] NÚKIB. Návrh nového zákona o kybernetické bezpečnosti vstupuje do další fáze. Online. NÚKIB. ©2023. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1969-navrh-noveho-zakona-o-kyberneticke-bezpecnosti-vstupuje-do-dalsi-faze/. [cit. 2023-10-29].
[6] The EU Cyber Solidarity Act. Online. EUROPEAN COMMISSION. European commission. ©2023. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity. [cit. 2023-10-29].
[7] Národní strategie kybernetické bezpečnosti České republiky 2021-2025

V části druhé jsou uvedeny vize a cíle na nadcházející roky. Cíle jsou zde rozděleny do tří skupin. Sebevědomě v kyberprostoru, kde probírá, že abychom byli i nadále bezpečnou a ekonomicky prosperující zemí, je nutné reagovat na nejnovější hrozby, kterým by mohla ČR čelit. Základem pro fungující obranyschopnost ČR je souvislý systém odhalování kybernetických hrozeb a spolupráce mezi bezpečnostními složkami. Při zodpovědném a sebejistém přístupu ke kybernetické bezpečnosti bude ČR prosperovat a bude i nadále silným spojencem pro zahraniční partnery. V dalších částech je popsáno, že bychom si měli udržovat silná a spolehlivá spojenectví na mezinárodní úrovni. Poslední část se zaměřuje na tzv. odolnou společnost 4.0, což znamená, že by byla celá společnost schopna využívat moderní technologie s minimalizací rizika kybernetických rizik.[8]

Akční plán kybernetické bezpečnosti České republiky považuje za hlavní cíl například vytvoření návrhu, který by umožňoval jednotný postup pro případ nahlášení kybernetických bezpečnostních incidentů a určit postup řešení odpovědným orgánům či zapracovat na spolupráci se soukromým sektorem, aby stouplo povědomí o působnosti a činnosti NÚKIB. Co se mezinárodní spolupráce týče, je důležité mezirezortně kooperovat při zahraničních aktivitách v oblasti kybernetické bezpečnosti. [9]

[8] Národní strategie kybernetické bezpečnosti České republiky 2021-2025

[9] PORADA, Viktor. Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-903-4.

2. Pojmy

Abychom mohli vůbec začít, je důležité si vysvětlit pár základních pojmů převzatých z Terminologického slovníku pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu:

Bezpečnost je stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. **Kybernetická bezpečnost** je souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. [10]

Kybernetický prostor je definován dle Terminologického slovníku definován jako digitální prostředí, které umožňuje vznik, zpracování a výměnu informací. Toto prostředí zahrnuje informační systémy, služby a sítě elektronických komunikací. Naopak dle zákona o kybernetické bezpečnosti je **kybernetický prostor** digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Bezpečnostní hrozba je potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

Kybernetická obrana je obrana proti kybernetickému útoku a zmírňování jeho následků. Také rezistence subjektu na útok a schopnost se účinně bránit.

Stav kybernetického nebezpečí je stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít

[10] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. Online. Ministerstvo vnitra ČR. 2016, 2016. Dostupné z: https://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx. [cit. 2023-11-07].

k porušení nebo by došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.[11]

Výbor pro řízení kybernetické bezpečnosti je organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů. [11]

Kybernetický útok je útok, který spouštějí kyberzločinci pomocí jednoho nebo více počítačů proti jednomu nebo více počítačům nebo sítím. Jeho cílem může být záměrné vypnutí počítačů, krádež dat nebo využití napadeného počítače jako výchozího bodu pro další útoky. Kyberzločinci používají různé metody, včetně malwaru, phishingu, ransomwaru, útoků typu "denial of service" a dalších. [12]

Dle zákona o kybernetické bezpečnosti je **kritická informační infrastruktura** je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,

[11] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. Online. Ministerstvo vnitra ČR. 2016, 2016. Dostupné z: https://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx. [cit. 2023-11-07].

[12] *What is a Cyber Attack?* Online. Check point. 2023. Dostupné z: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/. [cit. 2024-02-09].

3. Současné zhodnocení hrozeb kyberútoků

3.1 Typy kyberútoků

Kybernetické útoky se díky rychlému vývoji potýká s čím dál častějšími útoky a mají potenciál způsobovat velké škody. Právo s tím spojená rizika řadí mezi nejzávažnější, a to hned z několika důvodů. Jedním z nich je technická nenáročnost a zanedbatelné náklady oproti škodě, které může způsobit. Dokonce P. A. Yannakogeorgos ve své knize uvádí, že následky kybernetických útoků může způsobit větší škody než přírodní katastrofy či teroristické útoky. Mohou totiž narušit či způsobit selhání kritické infrastruktury. [13]

Je nesporné, že hrozba a potenciál stále poroste spolu s rostoucím počtem uživatelů zařízení připojených k internetu. Útoky, které byly v minulosti zcela výjimečné až nemožné, jsou v současnosti zcela běžné a dost snadné. Dříve totiž mělo minimum lidí možnost připojit se k internetu a většina důležitých dat bylo vedeno v písemné formě, takže drtivě převládal fyzický průnik do systému. [14]

Firmy se v posledních letech řídí heslem „kdykoli, odkudkoli a z jakéhokoli zařízení“. Proto jsou zaměstnanci přihlášení na internet a do informačního systému firmy nejen ze služebních zařízení, ale i ze svých soukromých. Tím se ovšem výrazně navyšuje riziko. Každý z nás má v průměru alespoň dvě elektronická zařízení připojená k internetu, mobilní telefon a počítač, což je v porovnání s dobou před 30 lety rozdíl, jelikož dříve tyto zařízení užívali většinou jen inženýři. V současné době je to běžný pracovní nástroj, takže s ním pracují naprosto všichni, a to včetně dětí, které ještě neumí kolikrát ani mluvit. [15]

Počet zařízení připojených k síti sice roste, ovšem to samé se nedá říct o bezpečnostních návycích, které většinu lidí i obtěžuje. Lze to vidět u vytváření hesel nebo na mobilním telefonu bez zabezpečovacího kódu či gesta. Dalším

[13] YANNAKOGEORGOS, Panayotis A. Conflict and Cooperation in Cyberspace The Challenge to National Security. CRC Press, 2013. ISBN 9781466592018.
[14] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
[15] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

může být bezhlavém zadávání údajů o platební kartě prakticky kamkoli či sdílení jiných osobních údajů. [16]

Dalším fakt, který útočníkům pomáhá je ten, že na internetu dnes najdete již opravdu vše a sdílení know-how není výjimkou. Při zadání správných slov do vyhledávače lze najít, jak na někoho vést kybernetický útok či si stáhnout nástroj pro napsání vlastního viru. Pro méně zdatné je možnost si útok na někoho za pár dolarů objednat. Této službě se říká CaaS, Crime as a servise, a je to kompletní služba včetně podpory. Lze s ní posílat zavirované emaily, nahrát na Appstore podvodnou aplikaci nebo napadnout server na druhé polokouli. [17]

Do kybernetické kriminality spadají především majetkové formy kriminality – podvody, klamání. Jsou ovšem i autoři, kteří sem řadí i narušení práv duševního vlastnictví. Jedním z nejběžnějších a nejrychleji se rozšiřujícím způsobem je krádež identity spotřebitele. Charakteristické je zcizení údajů o platební kartě pro přístup na bankovní účet či zneužití s tím spojených služeb.

3.1.1 Hacking

Původ pojmů „hacker“ a „hackeing“ sahají již do 50. let 20. století do USA. Hacking je úmyslná změna obvyklého chování počítače a připojených systémů. Obyčejně je páchán pomocí skriptů nebo programů, které manipulují s přenášenými daty, s cílem získat přístup k informacím ze systému. Hackeři útočí na počítače pomocí virů, červů, trojských koní, ransomware, rootkitů nebo neautorizovanými transformacemi v nastavení DNS serverů. Mohou také zahltit systém kvantem požadavků na jistou službu nebo stránku.

Hackerské programy si může na internetu volně stáhnout a upravovat kdokoliv. Trpělivý, motivovaný a schopný člověk se dokáže naučit tyto programy používat a může se pokusit získat vaše soukromé údaje, včetně přihlašovacích údajů do banky nebo jiných přístupových dat. Kromě začátečníků existuje také

[16] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
[17] SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

mnoho zkušených hackerů, kteří dokáží upravovat stávající programy a tvoří stále nové hackerské techniky. [18]

Pod pojmem hacker si tedy většina lidí představí něco špatného, opak je ale pravdou. Opravdový hacker je osoba, která má dokonalé znalosti v oblasti informačního systému a která dokáže záměrně hacknout webové stránky a upravit jejich obsah. Hacker své zkušenosti a vědomosti používá k pomoci člověka, tím je myšleno, že napadá stránky, aby byly zjištěny nedostatky zabezpečení. Hacker nemá zájem o citlivé a osobní informace. Hacker by měl umět také programovat, aby si dokázal napsat vlastní malware – škodlivé viry. [19]

Existuje mnoho druhů hackerů:

White hat hacker je člověk, který vše dělá legálně. Firma si ho najme, uzavře s ním smlouvu a on testuje aplikace či webové stránky. Poptávka zadaná od firmy u hackera se týká toho, aby zjistil, jestli je například hra a její software bezpečný a pokud zjistí, že ne, tak chyby nahlásí a ty se následně opraví. [20]

Black hat hacker tento druh hackera dělá svou činnost kompletně nelegálně. Snaží se dostat do systému firmy a tím jí uškodit. Může zde jít o stažení dat a následné prodání či smazání.[20]

Grey hat hacker je speciální druh. Jeho činnost je sice nelegální, avšak není pro firmu přímo nebezpečný. Snaží se pouze dostat do systému, ale následně už nijak neškodí. Dokonce většinou chybu nahlásí majiteli, aby si ji mohl opravit. [20]

Green hat hacker není na top úrovni, ale snaží se učit. Je to takzvaný učící se hacker. [20]

[18] RAYMOND, Eric Stevens. How to become a hacker. Online. 2001. Dostupné z: http://www.catb.org/~esr/faqs/hacker-howto.html. [cit. 2023-11-17].
[19] DAVID ŠETEK – HACKNI SVOU BUDOUCNOST. 1. Hacking a kybernetická bezpečnost – Co je to hacking. Online. YouTube. 2023. Dostupné z: https://www.youtube.com/watch?v=piri0l5lhWk. [cit. 2023-11-12].
[20] DAVID ŠETEK – HACKNI SVOU BUDOUCNOST. 2. Hacking a kybernetická bezpečnost – Kdo je to hacker a typy hackerů (white, grey a black hat). Online. YouTube. 2023. Dostupné z: https://www.youtube.com/watch?v=iWiIpmYkAvU. [cit. 2023-11-12].

Red hat hacker pracuje na straně dobra. Snaží se dostat Black hat hackera a předvést ho policii. Říká se o nich, že jsou nemilosrdní.[20]

Dalším dělením je red team a blue team. Tyto týmy se objevují ve firmách, kde mají za úkol zabezpečit firmu za pomoci jisté soupeřivosti.

Blue team za úkol mají zabezpečení firmy. Pracují uvnitř firmy a provádí hodnocení rizik, vzdělávají zaměstnance, monitorovací zařízení. [21]

Red team má za cíl porazit blue team. Útočí na lidi, procesy a technologii. Dříve se jím říkalo Tiger team. Teď se tak říká top hackerům, kteří testují něco specifického – například pokud by vláda vyvinula sledovací software, tak oni se ho snaží hacknout. [21]

Jelikož vlastnictví dvou týmů může být finančně velmi náročné, v dnešní době již existují externí firmy, které poskytují služby ve formě provádění testování pomocí dvou skupin hackerů. Existují také kurzy na red a blue teaming. [21]

Hacker se zaměřuje na slabiny počítačového systému. Přístup může být povolený, a to v případě, kdy chce firma zjistit, zda má její počítačový systém nějaké mezery a jestli je lehké systém prolomit. V tomto případě pak hacker chyby nahlásí a forma se podle toho zařídí. Přístup však může být i nepovolený, v tomto případě, jde hackerovi o to, aby se dostal dovnitř, získal nebo nějak poškodil data (vymazat, prodat).

Cílem hackera může být hned několik věcí:

- **Peníze** – získání informací za účelem prodeje či vydírání
- **Podniková špionáž** – jeden podnik chce získat informace od své konkurence
- **Politická špionáž** – státy mají své hackery, kteří zjišťují a analyzují situaci ostatních států a vytahují informace na státní představitele, které v případě nepříznivé situace či konfliktu následně použijí
- **Pomsta** – za účelem dané osobě či podniku ublížit, poškodit ho

[21] DAVID ŠETEK – HACKNI SVOU BUDOUCNOST. 3. Hacking a kybernetická bezpečnost – Blue team a red team v hackingu. Online. YouTube. 2023. Dostupné z: https://www.youtube.com/watch?v=sqHA_VXEwq4. [cit. 2023-11-12].

- **Haktivism**
- **Sláva** – dobrý pocit a pocit uznání, že dokázal prolomit systém a dostal se k jistým datům[22]

3.1.2 Trojský kůň

Trojský kůň je program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje.[23]

Ani jméno není náhoda, stejně jako historický předchůdce ze starořecké pověsti o dobytí Troji, i tento trojský kůň předstírá, že obnáší nějakou přidanou hodnotu jako jsou bezplatné programy, zábavu či užitečná funkce, proto je často pustí uživatel sám v dobré víře. Ve finále však způsobuje velké škody či krádež dat. [24]

Trojský kůň není ale klasický vir, ten se totiž dokáže šířit sám. Aby se trojský kůň šířil, jsou k tmu potřeba tzv. wormové, kteří napomáhají šíření, aniž by o tom měl uživatel tušení. Dalším způsobem šíření je přidání ho do již vytvořené aplikace a nabízení jí na warez serverech. [25]

Po jeho aktivaci může provádět různé škodlivé činnosti. Může umožnit útočníkovi vzdálený přístup k zařízení či počítači, což mu umožňuje získat citlivá data. Může také vést k nainstalování dalšího škodlivého softwaru na napadeném zařízení. Mohou být využity zdroje zařízení, jako jsou výpočetní kapacity nebo síťové prostředky, například k útokům nebo k těžbě kryptoměn.

[22] DAVID ŠETEK – HACKNI SVOU BUDOUCNOST. 3. Hacking a kybernetická bezpečnost – Blue team a red team v hackingu. Online. YouTube. 2023. Dostupné z: https://www.youtube.com/watch?v=sqHA_VXEwq4. [cit. 2023-11-12].
[23] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[24] Trojský kůň. Online. Avast. 2016. Dostupné z: https://www.avast.com/cs-cz/c-trojan. [cit. 2023-11-19].
[25] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

Nebo v neposlední řadě mohou být využity k sledování a sběru citlivých informací, jako jsou hesla, bankovní údaje nebo soukromé dokumenty. [26]

Nejlepší způsob, jak se proti trojskému koni bránit, je si stáhnout a dobře nakonfigurovat firewall a antivirus a pravidelně je aktualizovat. Dobré je takové použití funkce antitrojan, který vám odhalí přítomnost trojského koně. [26]

3.1.3 Cracking

Cracking je velmi propojený s počítačovým pirátstvím a hackingem. Označuje prolamování či obcházení ochranných prvků systému, programů nebo aplikací, s cílem jejich dalšího neoprávněného užití. Jiná definice říká, že to je metoda odstraňování nebo zakazování funkcí proprietárního softwaru, které jsou považovány za nežádoucí za pomoci techniky disassemblování. [27]

Cracking a warez scéna spolu hodně souvisí, cracking je totiž její součástí. Nejprve co je warez scéna – *celosvětová, podzemní, organizovaná síť pirátských skupin specializujících se na získávání a nelegální bezplatné vydávání digitálních médií před jejich oficiálním datem prodeje*.[27]

Bezpečnost je mnohdy prolamována i u velmi nákladných programů, které lze poté užívat bez koupené licence a lze s ním normálně pracovat. Běžně jsou takto ilegálně cracknuté grafické či projektovací programy, jedním z často napadaných je program Auto Cad. [28]

Cracking lze samozřejmě provádět mnoha formami, jednou z forem je „password cracking“ neboli prolamování hesel, který slouží ke zjištění přístupového hesla do licencovaného systému či programu. Cracker obyčejně vytvoří keygen či crack, který umožní pozdější užití programu. Další je „rootkit“,

[26] Trojský kůň. Online. Avast. 2016. Dostupné z: https://www.avast.com/cs-cz/c-trojan. [cit. 2023-11-19].
[27] Warez scene. Online. Wikipedia. 2020, 10. 9. 2023. Dostupné z: https://en.wikipedia.org/wiki/Warez_scene. [cit. 2023-11-14].
[28] Kdo je cracker. Online. Správa sítě – slovník pojmů. 2022. Dostupné z: https://www.sprava-site.eu/cracker/. [cit. 2023-11-16].

což je program, který skrývá výskyt viru či malwaru. Sniffing je napíchnutí na místní síť a následné provádění odposlechu. [29]

Cracker je osoba, která má stejnou jako hacker informovanost a zkušenosti v oboru informačních technologií, ale využívá je ve svůj užitek, a nikoliv pro užitek někoho druhého. Často jsou crackeři chybně zaměňovaný s hackry a souhrnně bývají obě skupiny označovány za hackery. Cracker ale na rozdíl od hackera zneužívá hackerských metod zpravidla k obohacení sebe sama. [30]

Jelikož povědomí lidí o této oblasti, často jsou zaměňovány pojmy hacking a cracking. Hacker původně totiž neznamená člověka provádějící nelegální činnost, kterou by škodil ostatním či kradl. Jejich cílem je se prolomit systém a dostat se do cizího systému a tím upozornit na chyby a rizika. Existuje ovšem další skupina, která se za hackery vydává. Pravý hackeří je popisují jako líně, málo chytré a nezodpovědné, jelikož proniknout skrz zabezpečení z nikoho nedělá hackera. Základním rozdílem tedy je, že hacker věci buduje, naopak cracker je ničí. [30]

3.1.4 Phishing

Phishing lze definovat jako kriminální jednání, kde je cílem podvodně získat či vylákat prostřednictví elektronické komunikace citlivé informace (přihlašovací údaje, hesla, údaje o karetních či debetních kartách) způsobem, že se pachatel vydává za věrohodnou organizaci či osobu. Tento pojem vychází z anglického slova „fishing“, což je v překladu rybaření. Funguje to tedy jako rybaření, pachatel nahodí návnadu a čeká, jaká oběť se na ni chytí.

Pachatel se u phishingu má za cíl získat neoprávněný přístup k bankovnímu účtu a platební kartě a poté z těchto zdrojů odcizit veškeré finance. V tomto případě útok nesměřuje na finanční instituci, ale přímo proti klientům.

[29] Kdo je cracker. Online. Správa sítě – slovník pojmů. 2022. Dostupné z: https://www.sprava-site.eu/cracker/. [cit. 2023-11-16].
[30] RAYMOND, Eric Stevens. How to become a hacker. Online. 2001. Dostupné z: http://www.catb.org/~esr/faqs/hacker-howto.html. [cit. 2023-11-17].

Oběťmi jsou tedy klienti finančních institucí, kteří díky své nevědomosti a nerozvážnosti sdělí pachateli své osobní údaje. [31]

Principem phishingu je „sociální inženýrství“. To znamená, že pachatel využívá k získání citlivých údajů a informací různé psychologické metody a techniky, proto se pachatel snaží získat důvěru oběti, aby mu oběť dala informace sama a dobrovolně. Prostřednictvím elektronické komunikace nepotřebuje pachatel velké komunikační schopnosti, navíc je zde mnohem větší anonymita než v reálném světě. Další výhodou elektronické komunikace pro pachatele je, že může jedním klikem napadnout velké množství potenciálních obětí a tím zvýšit svou šanci na úspěch. Nejčastěji se tak děje přes email, sociální sítě či různé obchodní portály.

Předchůdce phishingu je již z 19. století, kdy toto jednání známé pod názvem „španělský vězeň“. Během tohoto podvodného chování šlo o to, že jistý bohatý vězeň se o své bohatství podělí, pokud mu oběť přes svého důvěrníka pošle určitý obnos peněz na podplacení stráží, které ho hlídají ve vězení. Po uhrazení částky se ovšem objevily další komplikace a po oběti jsou vyžadovány další finanční prostředky.

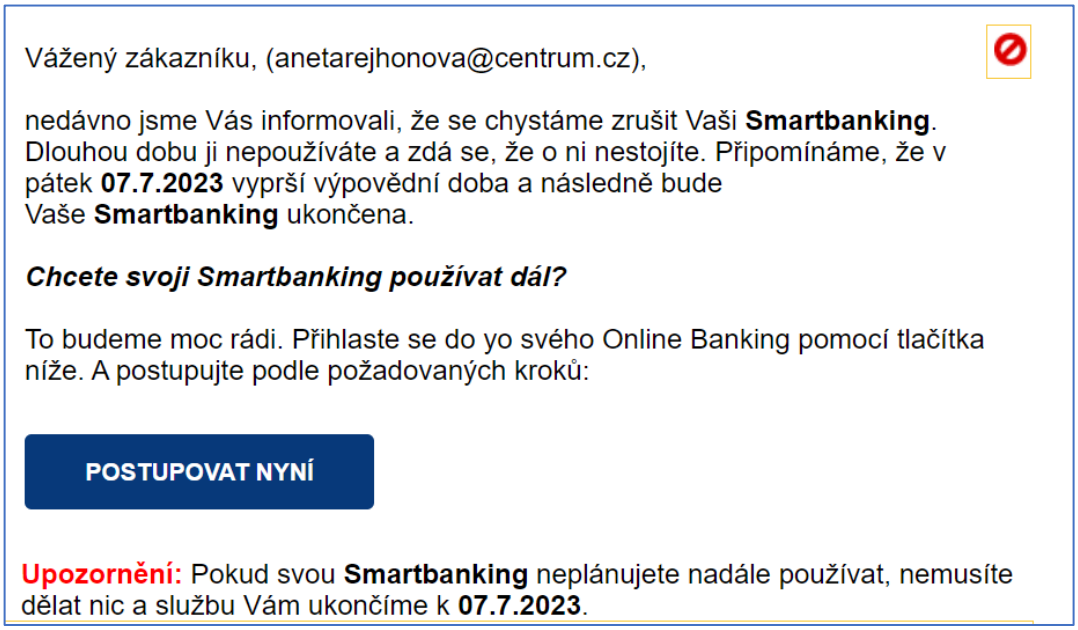
V této době by na takový příběh asi drtivá většina lidí neskočila, ale stačí poupravit příběh do dnešní doby a je zde další podvod. Právě španělským vězněm se inspirovali tvůrci tzv. nigerijských listů, známí také jako „419 scam“. Zde pachatelé využívají nízkého povědomí o politické a ekonomické situaci v Africe, proto je snadné vymyslet záminku, jak z lidí vylákat jejich úspory. Jedním z příběhů bývá historka o bohatých obchodnících či farmářích, kteří chtějí ze své země emigrovat kvůli ohrožení na životě, ale nechtějí přijít o všechny své úspory a majetek. Avšak má to různé háčky – je třeba založit účet u místní banky nebo zaplatit nejprve finančnímu úřadu za převod. Jakmile člověk částku pošle, tak mu pachatel slibuje, že mu peněžní obnos v příštích dnech pošle, avšak o pár dní později se vyskytnou další problémy a je potřeba zaslat další peníze. Oběť s vidinou zbohatnutí a vědomím, že už v tom má vložené vlastní peníze,

[31] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

další částku pošle a doufá, že tato částka byla už ta poslední a brzy zbohatne, opak je však pravdou.[32]

Velmi častým způsobem, jak oklamat oběť, je prostřednictvím emailu. Funguje to tak, že pachatel rozešle podvodný email totožný s emailem zaslaným například od banky. Je uváděno, že 3-11 % na takový email zareaguje. Je zde však většinou pár znaků, jak poznat, že se jedná o email podvodný. [33]

Já například v červenci 2023 obdržela tento email od banky Fio z emailové adresy fio@fio.cz, že se údajně chystají zrušit moje smartbanking, jelikož ho již dlouho dobu nepoužívám, a že pokud se přes tlačítko nepřihlásím, tak mi službu k danému dni ukončí.



Vážený zákazníku, (anetarejhonova@centrum.cz),

nedávno jsme Vás informovali, že se chystáme zrušit Vaši **Smartbanking**. Dlouhou dobu ji nepoužíváte a zdá se, že o ni nestojíte. Připomínáme, že v pátek **07.7.2023** vyprší výpovědní doba a následně bude Vaše **Smartbanking** ukončena.

Chcete svoji Smartbanking používat dál?

To budeme moc rádi. Přihlaste se do yo svého Online Banking pomocí tlačítka níže. A postupujte podle požadovaných kroků:

POSTUPOVAT NYNÍ

Upozornění: Pokud svou **Smartbanking** neplánujete nadále používat, nemusíte dělat nic a službu Vám ukončíme k **07.7.2023**.

Obrázek 1 – podvodný e-mail

Takový email by asi mohl být v pořádku, kdyby neměl několik chyb. Hned první je, že žádný účet u banky Fio nemám, tudíž mi nemají co rušit. Když pominu tento fakt, jsou tu pravopisné náležitosti. Měli bychom si dávat pozor na překlepy a pravopisné chyby, jako je zde v emailu například bezesmyslné slovo „yo“. Dále by pravá banka jistě nenapsala do oslovení mou emailovou adresu, ale mé celé jméno.

[32] Acta Universitatis Carolinae – Kybernetická kriminalita. 2012, roč. 58, č. 4. 2012. ISSN 0323-0619.
[33] ZAVRŠNIK, Aleš. Kyberkriminalita. Právní monografie (Wolters Kluwer ČR). Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-758-5.

3.1.5 Pharming

Pharming je propracovanější a nebezpečnější forma phishingu. Jde tu o útok na takzvaný DNS server, který přiřazuje k číselné IP adrese doménové jméno. V překladu to znamená, že se zde využívají speciální počítačové programy, jež jsou viry. Uživatel, který se přihlásí do svého internetového bankovnictví, se přepojí na stránku podvodnou. Ta je zpravidla velmi dobře imitovaná, takže se těžko rozpoznává, že nejde o pravou stránku. Uživatel s vědomím, že je to jeho banka, zadá své osobní údaje, které však získává pachatel. Druhou metodou pharmingu je přímé napadení počítače uživatele. Na napadeném počítači pouze upraví soubor Hosts obsahující URL, takže se rovnou přesměruje na pachatelovo podvodnou stránku. [34]

3.1.6 Spamming

Spam je jakýkoli druh nevyžádané masové digitální komunikace. Zahrnuje nepožadovaná reklamní sdělení doručovaná prostřednictvím e-mailů, SMS, komunikačních aplikací, sociálních sítí nebo diskusních fór, která jsou odesílána velkému množství adresátů nebo zveřejněna na různých místech na internetu. Zasílání nevyžádaných reklamních zpráv je trend již z minulého století. První známá masivní distribuce nevyžádaných zpráv, tzv. spamová kampaň, se objevila v roce 1978 na síti ARPANET a zasáhla zhruba 15 % uživatelů. Největší vzestup však nastal spolu s vydáním nového operačního systému Windows 95 v roce 1995. Tento operační systém již měl totiž i vlastní internetový prohlížeč. [35]

Spameři používají k automatickému rozesílání nechtěných zpráv počítačový program zvaný spambot. Ten podle svého algoritmu určuje, komu rozešle, jakou nevyžádanou zprávu. To znamená, že pro české emailové adresy bude používat český text a fráze. Do spammingu se také řadí řetězové zprávy a hoaxy, které se ale od typického spamu liší tím, že další šíření je mezi lidmi samotnými.

[34] SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.
[35] Spam. Online. , Eset software spol. s r.o. Eset. 2023. Dostupné z: https://www.eset.com/cz/spam/. [cit. 2023-11-21].

Dne 1. června 2002 nabyl účinnosti zákon 138/2002 Sb., který přináší změny a dodatky k zákonu č. 40/1995 Sb. ČR, o regulaci reklamy. Tyto nové ustanovení výrazně upravují pravidla pro osoby zadávající, zpracovávající a šířící reklamu. Mimo jiné říká, že „*šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje*.“ [36]

Kontrolu dodržování tohoto zákona provádějí živnostenské úřady (podle §7 písm. d). Lze očekávat, že na základě konkrétního a dostatečně konkrétního podání se tento dozorový orgán skutečně pokusí identifikovat skutečného šiřitele. S ohledem na současné technologie to však není jednoduchý úkol. [36]

Poznat, že jde o spam, je velmi jednoduché. V emailové či jiné schránce se začne pravidelně objevovat velké množství nevyžádaných zpráv. Obsahem jsou obvykle reklamy, které však mohou být spojené i s phishingem. Pokud se proto objeví ve schránce zpráva od příjemce nabízející nějaké zboží či službu, ale k jeho odběru jsme se nepřihlásili, jedná se o spam.

3.1.7 Ransomware

Ransomwarový útok představuje snahu o vydírání peněz od organizace výměnou za obnovení přístupu ke svým datům. Malé a střední podniky jsou stále častěji cílem ransomwarových útoků z několika důvodů. Tyto společnosti často uchovávají údaje, které mají vyšší hodnotu než běžní domácí uživatelé, ačkoliv nemají tak propracovaná bezpečnostní opatření jako velké korporace nebo instituce. Tato skutečnost činí tyto podniky atraktivními cíli pro útočníky, kteří hledají snadnější cesty k získání cenných dat a zároveň využívají jejich nedostatečnou ochranu k provedení ransomwarových útoků. Navíc manažeři

[36] Zákon, kterým se mění zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů, ve znění pozdějších předpisů, a zákon č. 79/1997 Sb., o léčivech a o změnách a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, § 2e

těchto menších firem si často myslí, že nejsou pro útočníky zajímaví, a tak pravidelně nezálohují svá data a nejsou na takové útoky připraveni. [37]

Ransomearový útočníci se již ale nespokojí pouze s vydíráním jednoho subjektu, a tak své metody násobí. Dvojité schéma funguje tak, že útočníci získají a zablokují citlivá data a následně subjektu vyhrožují zveřejněním, pokud nezaplatí výkupné. Trojnásobné schéma je způsob, jak získat více peněžních prostředků z výkupného od více osob. Útočnici v tomto případě požadují výkupné nejen od napadeného subjektu, ale i od subjektů, kterých se tyto citlivé informace týkají. Jako příklad lze uvézt útok mířený v roce 2020 na finskou psychoterapeutickou kliniku, kde útočníci požadovali výkupné od kliniky, ale i od pacientů pod výhružkou, že zveřejní údaje o jejich psychickém zdraví, pokud nezaplatí 200 eur. [37]

3.1.8. Eavesdropping

Útok pomocí odposlechu nastává, když hackeři zachytí, smažou nebo upraví data přenášená mezi dvěma zařízeními. Odposlech, též známý jako odchytávání nebo odposlouchávání, využívá nezabezpečených komunikací v síti k přístupu k datům přenášeným mezi zařízeními. Pro další vysvětlení definice "útok pomocí odposlechu" typicky nastává, když uživatel připojí k síti, v níž není provoz zabezpečen nebo šifrován, a odesílá citlivá obchodní data kolegovi. Data jsou přenášena přes otevřenou síť, což poskytuje útočníkovi příležitost využít zranitelnost a zachytit je různými způsoby. Útoky pomocí odposlechu často mohou být obtížně rozeznatelné. Na rozdíl od jiných forem kybernetických útoků přítomnost báglu nebo odposlechového zařízení nemusí negativně ovlivnit výkon zařízení a sítí. [38]

Odposlech může být pasivní nebo aktivní: V prvním případě hacker detekuje informace naslouchánim přenosu zpráv v síti, zatímco v druhém případě

[37] RANSOMWARE Bezpečnostní tipy pro malé a střední firmy. Online. Eset. 2022. Dostupné z: https://cdn-smartemailing.cz/15587/media/2023/ransomware/eset-ransomware-ebook-v4-cz-hyper.pdf?utm_medium=email&utm_content=ebook-ransomware&sid=ad87184e95694e69ac757ab230ea15cf&t=m. [cit. 2023-11-30].
[38] What is Eavesdropping? Online. FORTINET. 2023. Dostupné z: https://www.fortinet.com/resources/cyberglossary/eavesdropping. [cit. 2024-02-04].

aktivně získává informace tím, že se maskuje jako přátelské zařízení a zasílá dotazy stroji oběti. Tento druh odposlechu může zahrnovat sondování, skenování nebo neoprávněnou manipulaci. Detekce pasivních odposlechových útoků je často důležitější než detekce aktivních útoků, protože ty druhé vyžadují, aby útočník získal znalosti o síti a zařízení oběti předchozím pasivním odposlechem. Nejefektivnějším opatřením proti odposlechu je šifrování dat. [39]

3.2 Kyberútočníci

Kybernetický útočník je jedinec nebo skupina, která realizuje kybernetické útoky s úmyslem získat neoprávněný přístup k počítačovým sítím, zařízením či datům. Tyto osoby mohou mít různé motivace, jako je získání finančního prospěchu, provádění špionáže, poškození systémů či pouze dokazování si svých dovedností.

Při svých aktivitách útočníci využívají různých strategií a technik, včetně použití škodlivého softwaru, jako jsou viry, trojské koně, ransomware či phishing. Mohou se také spoléhat na sociální inženýrství, což zahrnuje manipulaci s lidským chováním za účelem získání přístupu k informacím.

Kybernetičtí útočníci mají různé úrovně znalostí a dovedností v oblasti počítačové bezpečnosti. Mohou se jednat o jednotlivce, skupiny se specializací na určité typy útoků, ale také o státní subjekty, které provádějí sofistikované útoky s politickým či vojenským záměrem.

Jejich cílem může být způsobit škodu, získat finanční výhody, získat citlivé informace, či zkrátka narušit funkčnost cílových systémů. Ochrana před kybernetickými útočníky je zásadní pro zachování bezpečnosti a integrity počítačových systémů a dat.

Vnitřní útočník je osoba, která má přímý přístup k vnitřní komunikační síti. Nejčastěji se jedná o vlastního zaměstnance případně někdo, kdo takového zaměstnance pod výhrůžkou či peněžní nabídkou přiměje ke spolupráci. V praxi

[39] What is Eavesdropping? Online. FORTINET. 2023. Dostupné z: https://www.fortinet.com/resources/cyberglossary/eavesdropping. [cit. 2024-02-04].

jde například o úmyslné nezálohování dat, poskytování citlivých údajů organizace konkurenci nebo protivníkovi. [40]

Vnější útočník je naopak osoba zvenčí, nemá fyzický přístup k vnitřní komunikační síti. Jakmile provádí svůj útok, musí čelit nástrahám a bezpečnostní ochraně, které jsou správcem sítě kladeny. [41]

Státem sponzorovaní útočníci zahrnuje velké množství různých útočníku s rozdílnými motivacemi. Jendo však mají společné, a to financování. Státní sponzoring může probíhat různě, avšak jádrem je vláda, kterou jsou také chráněni, proto je těžké je zastavit a postihnout. Typickými znaky jsou významné finanční prostředky, organizovanost a schopnost provádět náročné kybernetické útoky. Státem podporované útoky jsou zaměřeny na větší organizace, kde by mohl incident způsobit vážné poruchy provozu, jako jsou vládní instituce, neziskové organizace a další. Tyto entity obvykle uchovávají a spravují velmi cenná data, která poskytují hlubší vhled do politických strategií a vládních plánů. Motivace za takovými útoky je obvykle politická, ale může také sloužit jako ekonomická páka v budoucnosti. Soukromá sféra zpravidla nebývá zahrnuta mezi cíle státem podporovaných kybernetických útoků. [42]

Organizované kriminální gangy mají za cíl finanční prospěch, který aktuálně probíhá přes ransomware. Američtí analytici odhadují, že ransomware způsobí globální náklady na škody do roku 2031 ve výši 265 miliard dolarů. Ransomware je čím dál rozšířenější a dražší. Také výkupné po podnicích je vyžadováno stále vyšší, což útočníky motivuje k dalším útokům. [43]

Hacktivisté jsou skupina lidí, kteří aktivně a globálně usilují o změnu politického a sociálního světového vývoje. Cílí hlavně na země, které tyto myšlenky potlačují. Nejznámější skupinou současnosti jsou Anonymous,

[40] NĚMEČEK, Petr. Bezpečnost IT služeb ve veřejné správě. Bakalářská práce. Praha: AMBIS a.s, 2019.
[41] NĚMEČEK, Petr. Bezpečnost IT služeb ve veřejné správě. Bakalářská práce. Praha: AMBIS a.s, 2019.
[42] Tři typy kybernetických útočníků a jejich motivace. Online. Kurzy.cz. 2022, 18.11.2022. Dostupné z: https://www.kurzy.cz/zpravy/671723-tri-typy-kybernetickych-utocniku-a-jejich-motivace/. [cit. 2023-11-30].
[43] OPOJIŠTĚNÍ.CZ. Tři typy kybernetických útočníků a jejich motivace. Online. Kurzy.cz. 2022, 18.11.2022. Dostupné z: https://www.kurzy.cz/zpravy/671723-tri-typy-kybernetickych-utocniku-a-jejich-motivace/. [cit. 2023-11-30].

která byla založena v roce 2003, avšak nikdo neví, kolik má po celém světě členů. Například v roce 2015 skupina oznámila, že zveřejní jména s kontakty příznivců Ku-klux-klanu, což je organizace založená na rasové nesnášenlivosti. Po několika dnech Anynomous zveřejnila kontakty na 70 členů klanu. Díky této skutečnosti se o tyto zločiny začala zajímat média i policie. [44]

[44] HANÁČEK, Jan. Hodní a zlí hackeři, Anonymous a hybridní válka. Online. Akademie věd České republiky. 2022, 13. 05. 2022. Dostupné z: https://www.avcr.cz/cs/veda-a-vyzkum/vedy-o-zemi/Hodni-a-zli-hackeri-Anonymous-a-hybridni-valka/. [cit. 2023-11-30].

4. Stav a připravenost ČR na aktuální ohrožení kyberútoky

4.1 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost byl zřízen jako ústřední správní orgán pro oblast kybernetické bezpečnosti, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Jeho pravomoci zahrnují také regulaci veřejně poskytovaných služeb v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 v souladu se zákonem č. 205/2017 Sb., který modifikoval zákon č. 181/2014 Sb. o kybernetické bezpečnosti a souvisejících změnách v příslušných zákonech, vyřazením problematiky kybernetické bezpečnosti z Národního bezpečnostního úřadu. [45]

Hlavní činnosti NÚKIB vyplývají ze zákona o kybernetické bezpečnosti, jsou jimi především:

- Provoz vládního CERT ČR
- Spolupráce s ostatními národními a mezinárodními CERT týmy
- Stanovení kritérií pro určení klíčových informačních systémů z hlediska České republiky a jejich autoritativní určování v konkrétních případech
- Kontrola dodržování stanovených standardů u informačních systémů
- Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- Výzkum a vývoj v oblasti kybernetické bezpečnost
- Ochrana utajovaných informací v oblasti informačních a komunikačních systémů [46]

[45] NÚKIB. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2024. Dostupné z: https://nukib.gov.cz/cs/o-nukib/. [cit. 2024-02-04].
[46] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

4.1.1. Hlavní aktivity, které vyvíjel NÚKIB v roce 2022

Koordinované zveřejňování zranitelností (CVD) je proces, který zahrnuje dobrovolné odhalování zranitelností v produktech informačních a komunikačních technologií (ICT) třetími stranami, tzv. objeviteli. Tento proces zahrnuje zprávu vlastníkům nebo správcům ICT produktů o objevených zranitelnostech s cílem umožnit provedení bezpečnostních oprav. V České republice v současné době neexistuje komplexní přístup státu k CVD ani specifická právní úprava v této oblasti, proto Národní úřad pro kybernetickou a informační bezpečnost pracoval v roce 2022 na návrhu národního přístupu, který by umožnil zodpovědné a koordinované odhalování zranitelností, které by mohlo být využíváno orgány veřejné moci i soukromým sektorem. [47]

Projekt BIVOJ, tato zkratka znamená bezpečný, inovativní, pro veřejnou správu, odolný, jednotný. Cílem projektu je vytvoření jednotné, funkční a bezpečné sítě, která by poskytovala bezpečnostní a komunikační služby. Součástí by byly instituce veřejné správy či prvky kritické informační infrastruktury. Projekt obsahuje více jednotlivých odvětví, které chce zrealizovat do 5-7 let. Koordinátorem projektu je NÚKIB. [47]

Nastavování bezpečnostního rámce rozvoje 5G sítí. NÚKIB spolu s dalšími správními úřady vydal v únoru 2022 Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v ČR, které poskytuje podporu zejména pro dodávky do informačních a komunikačních systémů kritické infrastruktury České republiky. Představuje perspektivu státu, která se neomezuje pouze na konečnou technickou podobu dodávaného řešení, ale zohledňuje také netechnické aspekty, včetně podnikatelského, právního a politického prostředí, ve kterém se dodavatel pohybuje. [48]

4.1.2. Činnost NÚKIB v číslech

V roce 2022 bylo na NÚKIB nahlášeno celkem 764 oznámení o kybernetickém útoku, z nichž 146 vyhodnotil jako kybernetické bezpečnostní incidenty, které následně řešil. Po několika letech konstantního nárůstu

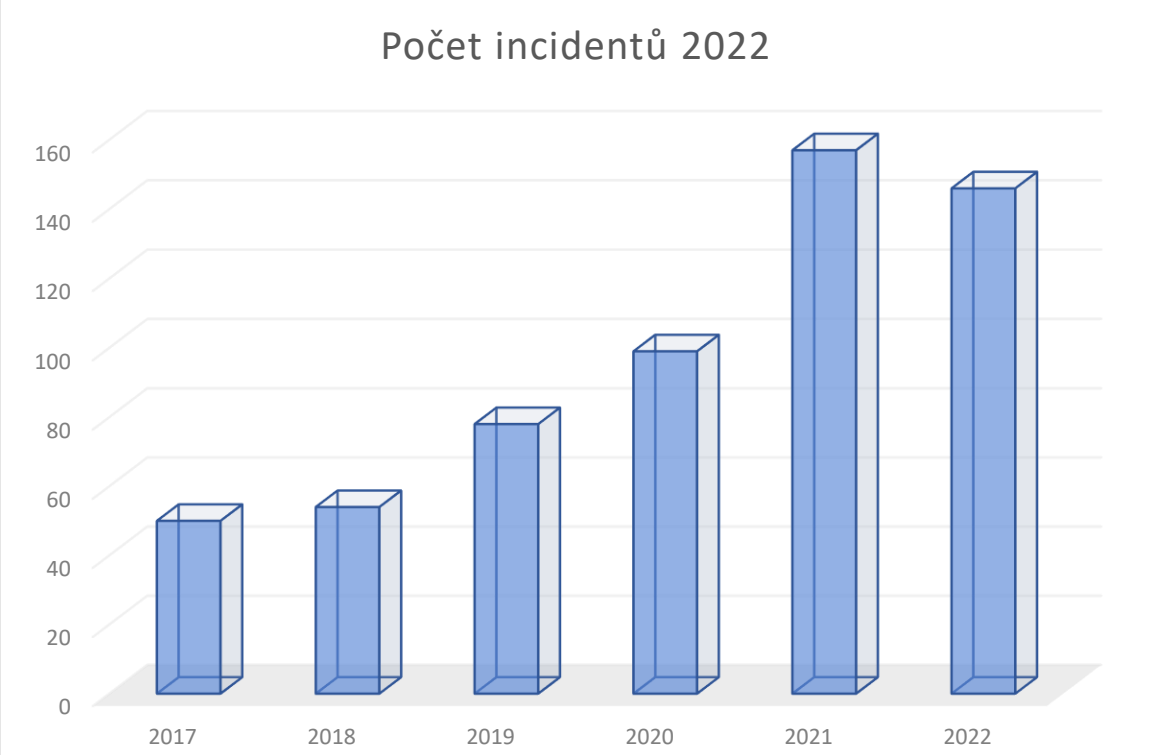
[47] Zpráva o činnnosti 2022, 2023. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_cinnosti_NUKIB-2022.pdf

se tak jednalo o první meziroční pokles. Je pravděpodobné, že za poklesem oproti roku 2021 stály především kampaně ProxyLogon a ProxyShell, zaměřené na široce používanou službu Microsoft Exchange Server. Ke konci roku 2021 byla také odhalena zranitelnost Log4Shell. V roce 2022 nebyla zjištěna žádná podobná zranitelnost s tak značným dopadem na bezpečnost. [48]

NÚKIB během roku 2022 provedl 20 auditů a kontrol kritických systémů a uspořádal 10 cvičení kybernetické bezpečnosti. Vyhodnotil také 169 materiálů posouzených v mezirezortním připomínkovém řízení.

4.1.3. Vývoj počtu incidentů registrovaných NÚKIB

Nejvíce kybernetických útoků bylo evidováno v roce 2022 v dubnu a v říjnu. Za tímto nárustem staly hlavně úroky ruských hacktivistických skupin. V obou případech útoky s největší pravděpodobností souvisely s českou podporou Ukrajiny. [49]



Obrázek 2 - graf počtu incidentů

[48] Zpráva o činnosti 2022, 2023. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_cinnosti_NUKIB-2022.pdf

[49] Zpráva o činnosti 2022, 2023. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_cinnosti_NUKIB-2022.pdf

4.1.4. Vedení úřadu

V čele Národního úřadu pro kybernetickou a informační bezpečnost je ředitel Ing. Lukáš Kintr. V roce 2015 začal pracovat jako auditor kybernetické bezpečnosti do Národního centra kybernetické bezpečnosti. Toto centrum bylo do roku 2017 součástí Národního bezpečnostního úřadu. Později přešel na Národní úřad pro kybernetickou a informační bezpečnost, kde zastával pozici vedoucího oddělení kontroly. Od září 2019 působil jako náměstek ředitele Národního úřadu pro kybernetickou a informační bezpečnost, kde měl na starosti řízení Národního centra kybernetické bezpečnosti. Tato sekce byla odpovědná za formulaci strategie pro zajištění a prosazování kybernetické bezpečnosti v České republice. Kromě toho měl na starosti činnost vládního CERT, jednání a spolupráci s národními a mezinárodními partnery a organizaci cvičení v oblasti kybernetické bezpečnosti. Od 1. července 2022 je ředitelem NÚKIB. Náměstky ředitele jsou Martin Smrčka z oddělení informačních systémů, Věra Vojáčková z oddělení personalistiky, práva a provozu, Pavel Štěpáník z oddělení strategických agend a spolupráce a Tomáš Krejčí z oddělení Národní centrum kybernetické bezpečnosti. [50]

4.2 Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti, jakožto výkonný orgán, představuje klíčovou instituci v rámci Národního úřadu pro kybernetickou a informační bezpečnost, která se zaměřuje na širokou škálu aktivit a opatření spojených s kybernetickou bezpečností v České republice.

4.2.1 Úkoly NCKB

Jedním z hlavních úkolů NCKB je prevence před hrozbami kybernetického prostoru, zejména proti kritické informační infrastruktuře a systémům poskytujícím základní služby. Tato prevence zahrnuje začlenění bezpečnostních opatření

[50] Vedení úřadu, 2022. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/vedeni-uradu/

a monitorování potenciálních hrozeb, aby se minimalizovala pravděpodobnost úspěchu kybernetických útoků. [51]

NCKB se taktéž zabývá řešením a koordinací kybernetických bezpečnostních incidentů, které mohou ohrozit kritickou infrastrukturu, provozovatele základních služeb a orgány veřejné správy. Tato koordinace je klíčová pro rychlou a efektivní reakci na kybernetické incidenty a minimalizaci jejich dopadu. [50]

Dalším důležitým pilířem činnosti NCKB je osvětová a vzdělávací činnost v oblasti kybernetické bezpečnosti. Tato aktivita má za cíl zvyšovat povědomí o kybernetických hrozbách mezi veřejností a poskytovat informace a nástroje pro ochranu před nimi. [52]

NCKB také úzce spolupracuje s národními i mezinárodními organizacemi zabývajícími se kybernetickou bezpečností, aby sdílelo informace, osvědčené postupy a koordinovalo společné úsilí v boji proti kybernetickým hrozbám. [51]

Kromě toho se NCKB podílí na pořádání a účasti na kybernetických cvičeních, která slouží k testování a zdokonalování reakčních schopností a postupů při kybernetických incidentech. [51]

V neposlední řadě se NCKB věnuje také výzkumu a vývoji v oblasti kybernetické bezpečnosti, aby mohlo aktivně přispívat k rozvoji nových technologií a metod pro ochranu kybernetické infrastruktury. [51]

4.3 Vládní CERT

V rámci ochrany kritické informační infrastruktury a významných informačních systému se můžeme setkat s klíčovými subjekty, jimiž jsou vládní CERT (Computer Emergency Response Team) a týmy CSIRT (Computer Security Incident Response Team). Úlohou každého státu, jež má svá data a systémy

[51] Co je NCKB. Online. Národní centrum kybernetické bezpečnosti. 2023. Dostupné z: https://www.govcert.cz/cs/. [cit. 2024-02-04].
[52] Co je NCKB. Online. Národní centrum kybernetické bezpečnosti. 2023. Dostupné z: https://www.govcert.cz/cs/. [cit. 2024-02-04].

propojené s internetem, je efektivně a důsledně vzdorovat bezpečnostním výzvám, reagovat na incidenty a organizovat efektivní řešení. [53]

Jako primární činnost vládního týmu CERT je řešení bezpečnostních incidentů. Poskytují technickou pomoc IT specialistům při nahlášení události, ale také dávají rady ohledně preventivního opatření.

Tým GovCERT.CZ poskytuje služby analýzy síťových dat a logů v rámci řešení incidentů, aby identifikoval způsob a dopady dané události. Pro subjekty s povinností také nabízí konzultace, které pomáhají rozlišit mezi incidenty a pouhými událostmi, za předpokladu, že jsou poskytnuty příslušné údaje nebo logy, na jejichž základě tým GovCERT.CZ provede odpovídající vyhodnocení. [54]

Povinnými subjekty jsou:

- Poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací
- Významné sítě
- Kritická informační infrastruktura
- Významné informační systémy
- Provozovatelé základních služeb
- Poskytovatelé digitálních služeb [55]

Vládní CERT v rámci své působnosti zpracovává několik projektů. Jedním z nich je projekt Systém detekce, který se týká kybernetické bezpečnostní události a metadata o síťovém provozu ve formě flow záznamů z perimetrů zapojených organizací. Záměrem projektu je dovednost detekce celkových problémů,

[53] Vládní CERT. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/. [cit. 2024-02-06].
[54] Poskytované služby. Online. NCKB. 2024. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/. [cit. 2024-02-06].
[55] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

které míří na více subjektů z řad povinných subjektů (viz výše), jež jsou zapojené do projektu. [56]

Dalším projektem vládního CERT je nasazování honeypotů. Zde je o to, že pomocí síťových pastí lze objevit pokus o nežádoucí přístup do systému či sledovat jednání útočníků. Pro aktivaci tohoto druhu monitorování lze použít síťovou past na IP adresu nebo adresy, které jste vyhradili. Pokud se subjekt rozhodne s vládním týmem utvořit spolupráci, může se zapojit do sdílení dat z těchto honeypotů.[57] Dle výroční zprávy o činnosti CSIRT.CZ za rok 2022 bylo zaznamenáno 4 501 registrovaných uživatelů a 33 768 024 spojení nebo útoků.

4.4 Tým CSIRT.CZ

Potřeba týmů zabývajících se ochranou sítě se navýšila v polovině 90. let, kdy došlo k velkému rozkvětu internetu mezi běžné uživatele, tedy i nárůstu kybernetické kriminality. Za tímto účelem začaly vznikat jednotky nazývané CSIRT (Computer Security Incident Response Team), jejichž úkolem bylo rychle identifikovat internetové útoky a minimalizovat případné škody. V dnešní době má téměř každá země, případně i větší organizace své bezpečnostní CSIRT týmy. [58]

Od 1. ledna 2011 tým CSIRT.CZ (Computer Security Incident Response Team České republiky) převzal roli Národního bezpečnostního týmu ČR. Toto rozhodnutí bylo učiněno Ministerstvem vnitra České republiky a bylo potvrzeno Memorandem o provozu Národního CSIRT.CZ, které bylo podepsáno mezi MV ČR a sdružením CZ.NIC v prosinci 2010. Tým CSIRT.CZ zastává roli národního CERT ČR podle Zákona o kybernetické bezpečnosti. Pole působnosti týmu CSIRT.CZ zahrnuje celou Českou republiku, což znamená, že všichni uživatele a sítě provozované v České republice jsou pod jeho dohledem. [59]

[56] Poskytované služby. Online. NCKB. 2024. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/. [cit. 2024-02-06].
[57] Poskytované služby. Online. NCKB. 2024. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/. [cit. 2024-02-06].
[58] Jak na internet. Online. Cz.nic. 2017. Dostupné z: https://www.jaknainternet.cz/page/1790/bezpecnostni-tymy/. [cit. 2024-02-09].
[59] O týmu CSIRT.CZ. Online. CSIRT.CZ. 2023. Dostupné z: https://csirt.cz/cs/o-nas/. [cit. 2024-02-09].

4.4.1 Úkoly týmu CSIRT.CZ

Tým CSCIRT.CZ má hned několik úkolů. Prvním z nich je udržování zahraničních vztahů, kdy tým spolupracuje se světovou komunitou CERT/CSIRT týmů a organizacemi, které podporují tuto komunitu. Dále spolupracuje se subjekty v rámci ČR, kterými jsou poskytovatelé internetových služeb, obsahovými provozovateli, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi v České republice. A v neposlední řadě poskytuje bezpečnostní služby v oblasti řešení a koordinace bezpečnostních incidentů, osvětová a školící činnost, proaktivní bezpečnostní služby. [60]

Pro představu, jak funguje tým CSIRT.CZ v praxi, lze uvést sérii kybernetických útoků v březnu roku 2013 na české internetové služby. Tento útok zapříčinil nedostupnost významných portálů, zpravodajských serverů a dalších služeb, včetně systémů pro elektronické bankovnictví některých bank. Napadenými subjekty byly například Seznam.cz, Česká národní banka, ČSOB, Novinky.cz, iDNES.cz či Česká spořitelna. Od samého začátku březnových útoků tým CSIRT.CZ aktivně působil jako poradce pro napadené společnosti, státní úřady a veřejnost. [61]

Tým CSIRT.CZ navázal komunikaci s postiženými subjekty, tj. organizacemi a subjekty, které utrpěly útoky. Nabídl jim specializovanou pomoc a poradenství, což zahrnovalo analýzu charakteru útoků, identifikaci zranitelných míst v jejich systémech a poskytování doporučení na zlepšení celkové kybernetické bezpečnosti. Dále nesměla chybět spolupráce se státní správou. CSIRT.CZ úzce spolupracoval s vládními orgány a úřady za účelem sdílení informací o útocích, koordinace reakcí a poskytování podpory při zajišťování celostátní kybernetické bezpečnosti. Tato spolupráce zahrnovala úzkou spolupráci s Ministerstvem vnitra a dalšími úřady s cílem zajistit, že opatření a strategie jsou prováděny koordinovaně a efektivně. Po provedení detailní analýzy probíhajících útoků se CSIRT.CZ snažil lépe pochopit jejich povahu a taktiky útočníků. Na základě

[60] O týmu CSIRT.CZ. Online. CSIRT.CZ. 2023. Dostupné z: https://csirt.cz/cs/o-nas/. [cit. 2024-02-09].
[61] Jak na internet. Online. Cz.nic. 2017. Dostupné z: https://www.jaknainternet.cz/page/1790/bezpecnostni-tymy/. [cit. 2024-02-09].

těchto analýz pak tým poskytoval doporučení a strategie pro budoucí prevenci a ochranu před podobnými útoky. [60]

4.5 Výbor pro kybernetickou bezpečnost

Výbor pro kybernetickou bezpečnost je stálým pracovním orgánem Bezpečnostní rady státu pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky. Výbor byl ustanoven usnesením vlády ze dne 10. května 2017. Výbor má 21 členů, přičemž jeho předsedou je předseda vlády a zároveň předseda Bezpečnostní rady státu. Jako výkonný místopředseda Výboru působí ředitel Národního úřadu pro kybernetickou a informační bezpečnost.[62]

Činnost spočívá v koordinaci plánování opatření pro zajištění kybernetické bezpečnosti České republiky. Tento výbor se zaměřuje na strategické otázky a opatření týkající se kybernetické bezpečnosti a sleduje vývoj v této oblasti, aby mohl poskytnout doporučení a rady vládě a dalším orgánům. Jeho úkoly zahrnují také monitorování aktuálních hrozeb a koordinaci reakce na kybernetické incidenty.[62]

4.6 Vojenské zpravodajství

Vojenské zpravodajství představuje jednotnou ozbrojenou zpravodajskou službu ČR, spojující jak rozvědnou, tak kontrarozvědnou činnost. Jeho kořeny sahají až do období první světové války, kdy bylo organizované zpravodajské oddělení československé armády založeno v listopadu 1918. Nynější Vojenské zpravodajství vzniklo v roce 2005 sloučením bývalého kontrarozvědného Vojenského obranného zpravodajství a rozvědné Vojenské zpravodajské služby. [63]

[62] Statut Výboru pro kybernetickou bezpečnost, ze dne 3. ledna 2024, Příloha č. 7, usnesení vlády
[63] Kdo jsme. Online. Vojenské zpravodajství. 2023. Dostupné z: https://vzcr.cz/kdo-jsme-35. [cit. 2024-02-11].

Vojenské zpravodajství spadá pod pravomoc Ministerstva obrany. V čele stojí ředitel, jenž je jmenován ministrem obrany po konzultaci s výborem Poslanecké sněmovny a souhlasem Vlády. Aktuální ředitelskou pozici zastává již od roku 2014 generálporučík Ing. Jan Beroun. [64]

Úkoly Vojenského zpravodajství jsou stanoveny Vládou České republiky, a za jejího vědomí také prezident. Jelikož je Česká republika členy NATO a Evropské unie, je Zpravodajství povinno plnit i úkoly, které vyplývají ze závazků k těmto organizacím. [62]

Během provádění svých úkolů je v rámci jistých podmínek oprávněno využít zpravodajské prostředky a disciplíny. Jimi jsou

- **HUMINT** – Zpravodajství lidských zdrojů, známé též jako Human Intelligence, je obor, který se zabývá sběrem a analýzou informací poskytovaných lidskými zdroji.
- **SIGINT** – Signálové zpravodajství, známé též jako Signal Intelligence, se zabývá zpracováním dat a informací získaných z elektromagnetického spektra, které vysílají komunikační i nekomunikační elektronické prostředky.
- **OSINT** – Zpravodajství z otevřených zdrojů, známé též jako Open Source Intelligence, analyzuje informace získané z veřejně dostupných zdrojů a dalších zdrojů s omezeným utajením, které jsou částečně nebo zcela zveřejněny.
- **IMINT –** Obrazové zpravodajství, známé též jako Imagery Intelligence, analyzuje informace z obrazových záznamů získaných různými typy senzorů, včetně fotografických, infračervených, termovizních, laserových. [65]

4.6.1 Zajišťování kybernetické obrany České republiky

Jelikož svět prochází významným společenským i technologickým vývojem, spolu s tím dochází ke změně tradičních metod a postupů pro zabezpečení

[64] Kdo jsme. Online. Vojenské zpravodajství. 2023. Dostupné z: https://vzcr.cz/kdo-jsme-35. [cit. 2024-02-11].
[65] Kdo jsme. Online. Vojenské zpravodajství. 2023. Dostupné z: https://vzcr.cz/kdo-jsme-35. [cit. 2024-02-11].

obrany. Konflikty poslední dekády jednoznačně naznačují rostoucí význam asymetrických forem konfliktů, ve kterých má klíčovou úlohu využití kyberprostoru. Útoky kyberprostorem mohou přijít nečekaně téměř z jakéhokoli místa na světě. Proto byl kybernetický prostor na summitu NATO, který se konal ve Varšavě v červenci roku 2016, označen vedle země, vzduchu, vody a vesmíru za další oblast, ve které může probíhat konflikt.[66]

Vládní přístup k této problematice označuje kybernetickou obranu jako samostatnou a specifickou složku celkového konceptu kybernetické bezpečnosti. Kybernetická obrana má za úkol zabezpečovat obranu státu v souladu se zákonem č. 222/1999 Sb., o zajišťování obrany České republiky. To zahrnuje ochranu svrchovanosti, územní celistvosti, principů demokracie a právního státu, a také ochranu životů občanů a jejich majetku před vnějšími hrozbami. Tato ochrana zahrnuje budování efektivního systému obrany státu, přípravu a nasazení vhodných sil a prostředků, a zapojení do kolektivního systému obrany. [64]

Dále je nutné si říct rozlišit kybernetickou obranu a bezpečnost. Hlavní rozdíly jsou hlavně v charakteru a intenzitě útoků a opatření, která na ně reagují, a to bez možnosti definovat zcela přesná kritéria. Připravenost na kybernetické útoky musí být komplexní a nesmí se omezovat pouze na oblast bezpečnosti. Je nezbytné budovat schopnosti, které umožní reagovat na útoky, jež by mohly vyžadovat aktivaci obrany státu. Aktivace kybernetické obrany bude tedy zvažována pouze při nejintenzivnějších útocích. Specifikem kybernetické obrany je, že může být prováděna jak při vyhlášení mimořádných stavů, kdy spolupracuje s ostatními složkami obrany České republiky, tak i mimo tyto situace, nepřetržitě. [64]

[66] Kybernetická obrana. Online. Vojenské zpravodajství. 2023. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46. [cit. 2024-02-11].

5. Řešení kybernetických útoků v ČR

V dnešní době nejsou kybernetické útoky jen hrozba, ale bohužel se staly neodmyslitelnou součástí digitálního světa. Nejen firmy a instituce, ale i fyzické osoby čelí stálému riziku stále více propracovanějších kybernetických hrozeb.

Česká republika zaostává v porovnání s ostatními zeměmi Evropy i světa v reakci na počet a závažnost kyberútoků a nedostatečně odolává kyberzločinu. Kromě firem jsou u nás častými cíli kyberútoků i státní instituce, zdravotnická zařízení, včetně velkých nemocnic, a univerzity. [67]

Kybernetické útoky mohou mít pro firmy široké spektrum následků a dopadů. Mezi hlavní rizika patří ztráta citlivých dat (odcizení, zničení nebo pozměnění dat, krádež identity), finanční ztráty (výkupné, náklady na obnovu a opravy systémů, ztráta příjmů z důvodu výpadku systémů, pokuty za porušení předpisů), poškození reputace (ztráta důvěry zákazníků, partnerů a investorů), právní důsledky (pokuty a soudní spory kvůli úniku citlivých dat), narušení obchodních aktivit (výpadky provozu, výroby, zpoždění dodávek, ztráta produktivity) a poškození IT infrastruktury s dlouhodobými dopady. [68]

Z těchto důvodů je tedy důležité jednat a dodržovat určitá doporučení, jakmile dojde ke kyberútoku jakékoli formy: [65]

Zachovat klid a reagovat hned. Tato rada se snáze říká, než dělá, avšak je velice nutná. V takové situace je důležité zvolit proaktivní postoj a hned aplikovat incidentní plán pro kybernetickou bezpečnost, který by měl obsahovat postup k izolaci postižených systémů, obnovu služeb a minimalizaci škod. Pokud však firma či instituce takový plán nemá, je nutné, aby osoba, která je pověřená koordinací kybernetické bezpečnosti, neprodleně kontaktovala odborníky na kybernetickou bezpečnost.

[67] Jak postupovat v případě kybernetických útoků: praktické rady pro řešení i nejčastější chyby, kterých se vyvarovat, 2023. Kurzy.cz [online]. [cit. 2024-02-16]. Dostupné z: https://www.kurzy.cz/zpravy/736770-jak-postupovat-v-pripade-kybernetickych-utoku-prakticke-rady-pro-reseni-i-nejcastejsi-chyby/

[68] Co dělat v případě kyberútoku: Klíčová je rychlá reakce a schopnost rozhodnout o dalším postupu, 2022. O2 CyberNews [online]. [cit. 2024-02-16]. Dostupné z: https://o2cybernews.cz/clanky/co-delat-v-pripade-kyberutoku-klicova-je-rychla-reakce-a-schopnost-rozhodnout-o-dalsim-postupu

Izolovat postižené systémy. Tento bod je velice snadný, je třeba totiž odpojit napadené systémy od sítě. Tím se minimalizuje možnost šíření a zároveň se zvýší pravděpodobnost zabránění dalšímu napadení a poškození dat a omezení ztráty citlivých informací.

Kontaktovat odborníky na kybernetickou bezpečnost. Prvním krokem by mělo být zapojení specialistů v oblasti kybernetické bezpečnosti, kteří mohou zhodnotit rozsah škod a asistovat při zabezpečení sítě proti dalším útokům. Zároveň mohou pracovat na identifikaci způsobu útoku na vaši síť a poskytnout důkazy pro budoucí vyšetřování.

Oznámit incident, komunikovat a spolupracovat. Příslušné právní předpisy a směrnice stanovují, zda je nutné nahlásit kybernetický incident dozorčím orgánům či regulačním institucím. O útoku je vhodné informovat jak interní týmy, tak klíčové externí partnery. Otevřená a pravidelná komunikace může předejít šíření dezinformací, udržet důvěru ve vaši organizaci a snížit možné budoucí škody. Pečlivé zabezpečení veškerých podrobností a důkazů spojených s útokem, které by mohly být užitečné při vyšetřování, by mělo být taktéž součástí postupu. Tyto informace mají klíčový význam pro vyšetření a prevenci budoucích incidentů. Organizace postižená kybernetickým útokem by měla úzce spolupracovat s kybernetickými bezpečnostními specialisty a právními orgány, aby mohla útok důkladně prověřit a identifikovat viníky.

Je však i důležité si říct, co rozhodně nedělat:[69]

Zanedbávat prevenci. Toto téma si podrobněji probereme v kapitole 8, avšak je nutné ji tu alespoň zmínit. Žádná instituce ani fyzická osoba by neměla podceňovat preventivní opatření.

Zamlčování incidentu. Ač to třeba může být pro daný subjekt nepříjemné přiznat skutečnost kybernetické napadení, nahlášení může být klíčové pro případné další útoky. Taktéž je nutné okamžité informování všech dotčených

[69] Jak postupovat v případě kybernetických útoků: praktické rady pro řešení i nejčastější chyby, kterých se vyvarovat, 2023. Kurzy.cz [online]. [cit. 2024-02-16]. Dostupné z: https://www.kurzy.cz/zpravy/736770-jak-postupovat-v-pripade-kybernetickych-utoku-prakticke-rady-pro-reseni-i-nejcastejsi-chyby/

osob, aby počítali s případnými následky a zároveň oznámení jim následných kroků, které povedou k řešení situace.

Jednání bez odborníků. To trochu souvisí s předchozím bodem. Ne každý je profesionální IT specialista či expert na kybernetickou bezpečnost, proto by se nikdo neměl ostýchat se na takové osoby obrátit. Absence jejich pomoci může situaci akorát zhoršit nebo minimálně prodloužit dobu řešení obnovy.

Placení výkupného. Nejen že tím jsou podporovány nelegální aktivity, které se tím akorát mohou stupňovat, ale ani po zaplacení výkupného nemusí být konec. Pachatel totiž sice data může vrátit, ale zašifrováním a následným dešifrováním může dojít ke ztrátě některých dat nebo jejich změně nebo může mít útočník v souborech skrytý malware, přes který může dále způsobovat nepříjemnosti a pohybovat se v IT systémech postiženého.

5.1 Vláda ČR

Dne 17. prosince 2021 byla bývalým prezidentem České republiky Milošem Zemanem jmenována Vláda ČR v čele s prof. PhDr. Petrem Fialou, Ph.D., LL.M. Programové prohlášení Vlády České republiky bylo schváleno vládou dne 6. ledna 2022. Na jednání 1. března 2023 kabinet schválil upravenou verzi tohoto programového prohlášení, které má 18 kapitol a pojednává od veřejných financí, přes digitalizaci, která je důležitá pro problematiku kybernetické bezpečnosti, až po spravedlnost a právo.

Vláda ve svém programu prohlašuje, že se ve svém funkčním období zaměří na zvýšení bezpečnosti v kybernetické oblasti ve veřejné i soukromé sféře. Taktéž mají v plánu vybudovat platformu, která umožní trvalou spolupráci mezi veřejnou správou a soukromým sektorem při ochraně sdíleného kybernetického prostoru. [70]

Dále avizovali zvýšení důležitosti a koordinace v oblasti informační a kybernetické bezpečnosti v rámci bezpečnostní politiky státu, což zahrnuje úzkou spolupráci mezi Národním úřadem pro kybernetickou a informační

[70] Programové prohlášení vlády, 2023. Vláda ČR [online]. [cit. 2024-02-18]. Dostupné z: https://vlada.gov.cz/cz/programove-prohlaseni-vlady-193547/#digitalizace

bezpečnost, Ministerstvem vnitra, Armádou České republiky a zpravodajskými službami, a to s ohledem na zachování práva na soukromí a svobody jednotlivce. [71]

V neposlední řadě Vláda ve svém programovém prohlášení apeluje na prohloubení spolupráce s EU, NATO a dalšími mezinárodními organizacemi, aby zůstal internet bezpečný a volný. Taktéž mluví o poskytnutí spolupráce s EU při řešení algoritmicky řízených platforem a sociálních sítí.[69]

V pátek 20. října 2023 se premiér Petr Fiala setkal s ředitelem Ing. Lukášem Kintrem při návštěvě NÚKIB v Brně. Premiér po návštěvě prohlásil, že význam tohoto úřadu roste, neboť kybernetická bezpečnost je dnes záležitostí všech. Vyjádřil poděkování řediteli úřadu Lukáši Kintrovi za jeho často nepřímo viditelnou práci. Premiér zdůraznil, že vládní kabinet přikládá kybernetické bezpečnosti mimořádný význam, což měla potvrdit i jeho návštěva.[72]

Premiér spolu s ředitelem úřadu projednávali mimo jiné i návrh zákona o kybernetické bezpečnosti, který vzniká především kvůli potřebě implementovat do české legislativy evropskou bezpečnostní směrnici do 18. října 2024. V rámci mezirezortního řízení obdržel úřad kolem 850 připomínek od více než 40 subjektů. Návrh zákona byl předložen 22. prosince 2023 Legislativní radě vlády. [73]

Další snahou Fialovy Vlády o zlepšení kybernetické bezpečnosti v České republice je spolupráce Vlády a fakulty elektrotechnické ČVUT v Praze. V souvislosti s tím bylo podepsáno 14, listopadu 2023 memorandu o jejich spolupráci ve Strakově akademii vedoucí Úřadu vlády ČR Mgr. Janou Kotalíková a děkanem FEL ČVUT profesorem Petrem Pátou.

"Úřad vlády České republiky se zavázal k dalšímu posilování svých kapacit v oblasti kybernetické bezpečnosti a pro dosažení tohoto cíle potřebujeme spolehlivého a nezávislého partnera s odbornými znalostmi v oblasti systémů

[71] Programové prohlášení vlády, 2023. Vláda ČR [online]. [cit. 2024-02-18]. Dostupné z: https://vlada.gov.cz/cz/programove-prohlaseni-vlady-193547/#digitalizace
[72] Význam NÚKIB roste, kyberbezpečnost se týká všech, řekl premiér Fiala, 2023. ČTK České noviny [online]. [cit. 2024-02-18]. Dostupné z: https://www.ceskenoviny.cz/zpravy/2429243
[73] Nová směrnice EU o kybernetické bezpečnosti „NIS2“ a návrh NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI, 2023. NÚKIB [online]. [cit. 2024-02-18]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

řízení informační bezpečnosti," uvedla vedoucí Úřadu vlády Jana Kotalíková v souvislosti s memorandem o porozumění. Dodala, že Fakulta elektrotechnická ČVUT disponuje potřebnými specialisty pro různé aspekty kybernetické bezpečnosti a řízení rizik a má také zkušenosti se vzděláváním dospělých. Díky tomu mohou odborníci z FEL aktivně přispět i k školení zaměstnanců Úřadu vlády ČR. [74]

Podle Ing. Jaroslava Burčíka, Ph.D., LL.M., vedoucího Centra kyberbezpečnosti na Fakultě elektrotechnického inženýrství by budoucí spolupráce mezi oběma institucemi měla zahrnovat několik klíčových bodů. Fakulta bude podporovat znalostní rozvoj pracovníků NÚKIB, poskytovat odborné poradenství a pomáhat s výběrem studentů technických oborů pro potřeby úřadu. Nový model spolupráce bude postaven na pilotním projektu, jehož cílem je zdokonalení vzájemných postupů, určení odpovědností a vyjasnění očekávání v oblasti informační bezpečnosti na Úřadu vlády. Plánovaná realizace projektu by měla proběhnout během několika měsíců. [72]

Jako příklad subjektu napadeného kybernetickými útoky si lze uvést české zdravotnictví, to je dle NÚKIB nejvíce napadaným odvětvím. Konkrétně tedy Fakultní nemocnici Brno, která se stala obětí kybernetických útoků v březnu 2020.

Ředitel nemocnice krátce po útoku uvedl, že kybernetický útok sice chod nemocnice omezil, avšak nepřerušil její provoz. Útok nastal kolem druhé hodiny ranní, kdy některý pracovník otevřel věrohodný mail, pachatel se tím dostal do systému, čímž postupně přestávaly fungovat. Proto sice bylo možné provádět většinu vyšetření, avšak nebylo možné přenášet informace z laboratoří do databáze. Nemocnice také přišla některá data, avšak k úniku dat o pacientech údajně nedošlo. Velké ztráty utrpěla také například transfuzní oddělení, kterému díky útoku selhal objednávací systém, díky jemuž nastal pokles dárců krve.

Útok sice proběhl před 4 lety, ale s následky se nemocnice vede boj doteď. Obnova nejzákladnějších systému trvala kolem dvou měsíců. Nutno také

[74] Úřad vlády a Fakulta elektrotechnická ČVUT zahájily spolupráci v oblasti kyberbezpečnosti, 2023. Fakulta elektrotechnická ČVÚT v Praze [online]. [cit. 2024-02-18]. Dostupné z: https://fel.cvut.cz/cs/aktualne/novinky/32738-urad-vlady-a-fakulta-elektrotechnicka-cvut-zahajily-spolupraci-v-oblasti-kyberbezpecnosti

podotknout, že tento incident se stalo za nouzového stavu, což mohlo ovlivnit výši trestu pachatele. Ten však nebyl dopaden, a proto byl pro nedostatek důkazů Policii ČR případ odložen.

6. SWOT analýza

Tato kapitola bude věnována SWOT analýze, tedy stanovení silný a slabých stránek a příležitostí s hrozbami, v českých nemocnicích. Tuto oblast jsem si vybrala, jelikož kybernetické útoky na nemocnice nejsou v České republice úplně ojedinělé viz kapitola 5.

Silné stránky

- Existence funkčního, základního a legislativního rámce pro kybernetickou bezpečnost.
- Národní centrum kybernetické bezpečnosti a vládní CERT disponují solidními kapacitami.
- Mezinárodní spolupráce v oblasti kybernetické bezpečnosti, zejména mezi CERT/CSIRT pracovišti, je velmi efektivní.
- Samotný systém zdravotní péče, který disponuje přirozenou odolností díky své koncepci. Česká republika disponuje kvalitní sítí zařízení poskytujících zdravotní péči, což znamená, že výpadek jednotlivých zařízení nemá zásadní vliv na schopnost celého systému poskytování zdravotní péče plnit svou funkci.
- Snaha Ministerstva zdravotnictví řídit jednotně kybernetickou bezpečnost, to také vedlo k rozvoji elektronického zdravotnictví.
- Rozmanitá spolupráce mezi zdravotnictvím a místním ICT prostředím, odborníky a firmami.
- Nemocnice splňují definici kritické infrastruktury. Kritičnost zdravotnictví, zejména velkých nemocnic, představuje pozitivní aspekt pro budoucí pokrok kybernetické bezpečnosti v tomto odvětví.
- Vznik Iniciativy pro koordinaci kybernetické bezpečnosti resortu zdravotnictví v roce 2020.

Slabé stránky

- Nedostatek zásad pro uplatnění odpovědnosti managementu jednotlivých institucí zapojených do poskytování zdravotní péče.
- Omezená míra sdílení informací, které by mohli pomoci rychlému jednání a snížení rizik typických pro zdravotnictví.

- Nedostatečné povědomí a kvalifikaci v oblasti kybernetické bezpečnosti.
- Jednou z větších slabých stránek je rozhodně finanční stránka. Díky tomu není možné zaměstnat dostatek odborníků na kybernetickou bezpečnost, ale také to například znemožňuje nákup a provoz technických prostředků.
- Nedostatečná motivace zaměstnanců vzdělávat se v oblasti kybernetické bezpečnosti.
- Absence systému řízení bezpečnosti informací, který by stanovil minimální požadavky pro zajištění kybernetické bezpečnosti.
- Různorodost aplikací a softwaru v prostředí informačních a komunikačních technologií komplikuje implementaci technologických prostředků pro zajištění kybernetické bezpečnosti.

Příležitosti

- Motivace odborníků na kybernetickou bezpečnost a ICT k zaměstnaní v této oblasti, které nebude omezeno tak finančními prostředky. Česká republika obdržela od EU dotace na kybernetickou bezpečnost ve výši 4,5 miliardy korun českých, což je mnohem více než v předchozím programovém období.
- Je nezbytné, aby zdravotnictví v ČR bylo připraveno na rostoucí trend využívání moderních technologií a dalších prostředků pro zpracování zdravotních informací. Jednou z možností v této oblasti je navázání spolupráce s komerčním sektorem kybernetické bezpečnosti, který je v České republice významný. Dále by mohla být využita spolupráce s vysokými školami a jejich výzkumnými kapacitami.
- Možnost se vzdělávat a přejímat trendy od nemocnic okolních státu, především tady těch západních.
- Začlenit se více do mezinárodních projektů v této oblasti.
- Vybudovat školící centra a pravidelné semináře pro běžné zaměstnance, ale i odborníky ICT a kybernetické bezpečnosti.

Hrozby

- Stále rostoucí počet kybernetických útoků a jejich různorodé cíle, zahrnující metody útoků a bezpečnostní slabiny.
- Neorganizované úsilí o digitalizaci zdravotních služeb, nedoprovázené schopností adekvátně posoudit a účinně řešit hrozby v oblasti kybernetické bezpečnosti.
- Hrozbou se naprosto přirozeně jeví nejen chybějící legislativní rámec, který jasně definuje povinnost vedení organizace se aktivně podílet na implementaci a dalším rozvoji systému řízení bezpečnosti informací, včetně zajištění odpovídajících zdrojů, a dále pravidelně tento systém řízení bezpečnosti informací vyhodnocovat a zlepšovat.
- Nouze o kvalifikované pracovníky v oboru může přispět k ohrožení kybernetické bezpečnosti nejen nemocnice.
- Nedostatečná inovace v oblasti nejen ICT, ale především procesů a systémů řízení, představuje hrozbu. Nesnesitelná situace, kdy organizace nedokáže adekvátně reagovat na moderní trendy a požadavky, zejména v oblasti analýzy velkých dat, zpracování a sdílení dat v reálném čase, může vést k nadměrnému tlaku na urychlenou modernizaci, což se stane místo plánovaného a postupného zavádění inovací a moderních postupů.

7. Návrhy a opatření ke zlepšení stavu v oblasti kybernetické bezpečnosti ČR

Zákon o kybernetické bezpečnosti uvádí v § 5 bezpečnostní opatření, která dělí na organizační a technická opatření.

Organizační opaření obsahují dle zákona *systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politika, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací, řízení přístupu osob, akvizice, vývoj a údržba, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrolu a audit*. [75]

Písmeno g) se zabývá bezpečností lidských zdrojů. Jelikož je člověk brán jako nejslabší článek kybernetické bezpečnosti, je kvůli tomu v prováděcím předpise věnovaná část právě edukaci uživatelů. Subjekty uvedené v § 3, písmene c) až f) ZoKB jsou podle Vyhlášky o kybernetické bezpečnosti povinni následující: [76]

Vzhledem k situaci a potřebám systému řízení bezpečnosti informací je navržen plánu rozvoje bezpečnostního povědomí, jehož účelem je zajistit adekvátní vzdělávání a zvýšení povědomí o bezpečnosti. Tento plán zahrnuje formu, obsah a rozsah:

- Informování uživatelů, správců, osob vykonávajících bezpečnostní role a dodavatelů o jejich povinnostech a bezpečnostní politice.
- Poskytnutí nezbytných teoretických a praktických školení uživatelům, správcům a osobám vykonávajícím bezpečnostní role.

S tím souvisí i stanovení odpovědné osoby, která bude mít na starosti jednotlivé úkoly uvedené v plánu rozvoje bezpečnostního povědomí.

Technická opatření tvoří s organizačními opatřeními základ bezpečnostních opatření. Na rozdíl od organizačních opatření, která se zaměřují na nastavení

[75] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
[76] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

pravidel v organizaci, technická opatření cílí na pravidla v oblasti nastavení informačních a komunikačních systému.

Obsahují *fyzickou bezpečnost, nástroje pro ochranu integrity komunikačních sítí, nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, nástroje pro ochranu před škodlivým kódem, nástroje pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů, nástroje pro detekci kybernetických bezpečnostních událostí, nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroje pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů*.[77]

Nástroj pro ověřování identity zajišťuje ověření identity před zahájením, a to heslem, otiskem, gestem či jinými způsoby a s tím spojený i omezený počet pokusů. Dále ukládání autentizačních údajů tak, aby byly odolné proti offline útokům.

Dle VoKB § 19 je nutné, aby heslo mělo hned několik náležitostí. Heslo by mělo mít u běžných uživatelů alespoň 12 znaků, u administrátorů a aplikací minimálně 17 znaků a s maximální délkou 64 znaků. Heslo by správně mělo obsahovat malá a velká písmena, číslice i speciální znaky. Měla by být možnost změnit heslo, s tím, že časový úsek mezi dvěma změnami nesmí být menší jak 30 minut.[78]

Při tvorbě hesla jako takového, aby bylo silné, je nutné se vyvarovat hned několika bodů. Rozhodně by heslo nemělo být podobné heslu předchozímu, ani by nemělo obsahovat jméno, příjmení, přezdívku, uživatelské jméno, název společnosti, a to ani pozpátku. Ani by to neměly být písmena či čísla po sobě jdoucí, např. 12345, abcd, yxcvb. Důležité taky je, abychom heslo nikomu neříkali a ani si ho nepsali na žádné viditelné místo či místo blízko zařízení. [79]

Správné silné heslo by tedy mělo obsahovat alespoň 12 znaků, obsahující malá, velká písmena, znaky i čísla. Heslo také může obsahovat pravopisné chyby,

[77] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
[78] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
[79] Jak vytvořit „silné“ heslo, 2021. DELL Technologies [online]. [cit. 2024-02-23]. Dostupné z: https://www.dell.com/support/kbdoc/cs-cz/000132376/jak-vytvo%C5%99it-siln%C3%A9-heslo

aby nebylo tak snadné na to přijít např. *Mám5broskvý!.* Nebo je také možné písmeno nahradit znakem či číslicí např. *A1f@_R0me0§*.

Policie ČR již třetím rokem propaguje kampaň *#nePINdej!*. Tato zkratka vychází z fráze „Pin nedej!“ Cílem této kampaně je zábavně a originálně seznámit veřejnost s nejčastěji se vyskytujícími podvody a naučit je, jak je rozpoznat a vyhnout se jim. Tento kybertest poskytuje několik možností, které demonstrují různé podvodné taktiky vhodné pro různé věkové skupiny. Kybernetická kriminalita cílí na různé věkové skupiny a neomezuje se pouze na seniory a osamělé jedince. Pachatelé se snaží oslovit co nejširší veřejnost bez ohledu na věk či vzdělání. Proto je cílem kampaně osvěta a vzdělávání veřejnosti, začínající s dětmi a mladými lidmi a pokračující přes dospělé až po seniory.[80]

Uvedené návrhy a doporučení doplňují výsledky mini průzkumu provedeného autorkou práce v jejím okolí v období února. Respondenti byly ve věku 18 až 28 let a byly oslovování na sociální síti s cílem zjistit jejich přístup k problematice hesel. Celkem bylo dotázáno 100 lidí.

Odpovědi na první otázku ukázaly, že 73 lidi ze 100 má jedno heslo k více účtům. To znamená, že jakmile hacker prolomí heslo k jednomu účtu a zkusí to k jinému, dostane se i tam a může spáchat mnohem větší škody. Zbylých 23 lidí uvedlo, že si heslo pokaždé minimálně trochu poupravuje.

Druhá otázka ukázala, že 97 lidí ze 100 tvoří hesla z malých, velkých písmen, znaků i čísel. Tento počet je docela překvapivý. Předpoklad byl, že to bude mnohem menší číslo. Avšak je pozitivní, že v tomto ohledu jsou lidé obezřetní a zodpovědní.

Třetí otázka byla, jak často respondenti mění svá hesla. Nikdy si heslo neměnilo 16 z nich. Naopak většina, 81 lidí, odpověděla, že si někdy heslo vyměnilo, avšak nedělají to absolutně pravidelně. A pouze jeden člověk odpověděl, že heslo mění pravidelně každé 3 měsíce.

[80] #nePINdej!, 2023. Policie České republiky [online]. [cit. 2024-02-29]. Dostupné z: https://www.policie.cz/clanek/nepindej.aspx

Poslední otázka zjišťovala, zdali lidem někdy někdo napadl účet, či se o to minimálně pokusil. 67 lidí z 100 odpovědělo, že se o to někdo v minulosti pokusil pomocí podvodných phishingových emailů. 23 lidí se přiznalo, že jim byl ukraden učet či dokonce odcizeny nějaké peníze. Zbylých 10 prý žádné zkušenosti s útoky nemá.

Tento mini průzkum ukazuje, že si lidé sice vytváří komplikovanější hesla, avšak to nestačí. Je také nutné heslo obměňovat, a hlavně nepoužívat jedno heslo k více účtům.

Závěr

Bakalářská práce se zabývala aktuálním problémem kyberútoků v České republice s cílem posoudit současný stav a zpracovat opatření ke zlepšení stavu v oblasti kybernetické bezpečnosti.

Teoretická část řešila právní předpisy a další dokumenty regulující oblast kybernetiky, vymezila pojmy a terminologie nezbytné k pochopení problematiky kybernetické bezpečnosti a definovala typy kyberútoků a kyberútočníků.

V praktické části byly nejprve představeny a hodnoceny klíčové instituce zapojené do snah o kybernetickou bezpečnost, zejména NÚKIB, vládní CERT či NCKB. Následně byly řešeny kybernetické útoky v ČR spolu s doporučeními, které by se měly dodržovat při kybernetickém útoku. Zároveň byly zkoumány a vymezeny silné a slabé stránky, příležitosti a hrozby kybernetické bezpečnosti v českých nemocnicích. Nakonec byla zpracována technická a organizační opatření ke zlepšení stavu v oblasti kybernetické bezpečnosti ČR.

Součástí návrhů a doporučení bylo vyhodnocení mini průzkumu provedeného autorkou práce v jejím okolí s cílem zjistit přístup lidí k tvorbě a využívání hesel. Bylo zjištěno, že většina z oslovených lidí sice nějaké povědomí o bezpečném vytváření a využívání hesel má, avšak i přesto nejsou dostatečně obezřetní a většina se již setkala s nějakou formou kybernetického útoku. Závěr je takový, že mezi lidmi panuje určité povědomí o kybernetické bezpečnosti, avšak není dostatečné, a proto by bylo dobré, aby již od ranných školních let na toto téma probíhala výuka a osvěta, aby každý věděl, jak kyberútokům předejít, případně jak se jim bránit.

Seznam zkratek

MVČR	Ministerstvo vnitra České republiky
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou bezpečnost
EU	Evropská unie
CaaS	Crime as a servise
DNS	Domain Name System
URL	Uniform Resource Locator
ICT	Informační a komunikační technologie
CVD	Koordinované zveřejňování zranitelností
BIVOJ	Bezpečný, inovativní, pro veřejnou správu, odolný, jednotný
NCKB	Národní centrum kybernetické bezpečnosti
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
IT	Informační technologie
NATO	Severoatlantická aliance (North Atlantic Treaty Organization)
HUMINT	Zpravodajství lidských zdrojů
SIGINT	Signálové zpravodajství
OSINT	Zpravodajství z otevřených zdrojů
IMINT	Obrazové zpravodajství
FEL	Fakulta elektrotechnická
ČVUT	České vysoké učení technické

ZoKB	Zákon o kybernetické bezpečnosti
VoKB	Vyhláška o kybernetické bezpečnosti

Prameny

Acta Universitatis Carolinae - Kybernetická kriminalita, 2012. ISSN 0323-0619.

Buďte připraveni na 10 nejčastějších kybernetických útoků!, 2022. *Forum media* [online]. [cit. 2024-02-04]. Dostupné z: https://www.forum-media.cz/premium/arch-zakladni/data-2022-8-23-950/doc/10-nejcastejsich-kybernetickych-utoku.pdf

Co je NCKB, 2023. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2024-02-04]. Dostupné z: https://www.govcert.cz/cs/

Co dělat v případě kyberútoku: Klíčová je rychlá reakce a schopnost rozhodnout o dalším postupu, 2022. O2 CyberNews [online]. [cit. 2024-02-16]. Dostupné z: https://o2cybernews.cz/clanky/co-delat-v-pripade-kyberutoku-klicova-je-rychla-reakce-a-schopnost-rozhodnout-o-dalsim-postupu

DAVID ŠETEK - HACKNI SVOU BUDOUCNOST, 2023. 1. Hacking a kybernetická bezpečnost - Co je to hacking. *YouTube* [online]. [cit. 2023-11-12]. Dostupné z: https://www.youtube.com/watch?v=piri0l5lhWk

DAVID ŠETEK - HACKNI SVOU BUDOUCNOST, 2023. 2. Hacking a kybernetická bezpečnost - Kdo je to hacker a typy hackerů (white, grey a black hat). *YouTube* [online]. [cit. 2023-11-12]. Dostupné z: https://www.youtube.com/watch?v=iWiIpmYkAvU

DAVID ŠETEK - HACKNI SVOU BUDOUCNOST, 2023. 3. Hacking a kybernetická bezpečnost - Blue team a red team v hackingu. *YouTube* [online]. [cit. 2023-11-12]. Dostupné z: https://www.youtube.com/watch?v=sqHA_VXEwq4

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

EUROPEAN COMMISSION, 2023. The EU Cyber Solidarity Act. In: EUROPEAN COMMISSION. *European commission* [online]. [cit. 2023-10-29]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

HANÁČEK, Jan, 2022. Hodní a zlí hackeři, Anonymous a hybridní válka. In: *Akademie věd České republiky* [online]. 13. 05. 2022 [cit. 2023-11-30]. Dostupné z: https://www.avcr.cz/cs/veda-a-vyzkum/vedy-o-zemi/Hodni-a-zli-hackeri-Anonymous-a-hybridni-valka/

Hrozby, 2023. KYBEZ [online]. [cit. 2024-02-16]. Dostupné z: https://kybez.cz/hrozby/

Jak na internet, 2017. *Cz.nic* [online]. [cit. 2024-02-09]. Dostupné z: https://www.jaknainternet.cz/page/1790/bezpecnostni-tymy/

Jak postupovat v případě kybernetických útoků: praktické rady pro řešení i nejčastější chyby, kterých se vyvarovat, 2023. Kurzy.cz [online]. [cit. 2024-02-16]. Dostupné z: https://www.kurzy.cz/zpravy/736770-jak-postupovat-v-pripade-kybernetickych-utoku-prakticke-rady-pro-reseni-i-nejcastejsi-chyby/

Jak vytvořit „silné“ heslo, 2021. DELL Technologies [online]. [cit. 2024-02-23]. Dostupné z: https://www.dell.com/support/kbdoc/cs-cz/000132376/jak-vytvo%C5%99it-siln%C3%A9-heslo

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6.

Kdo je cracker, 2022. *Správa sítě - slovník pojmů* [online]. [cit. 2023-11-16]. Dostupné z: https://www.sprava-site.eu/cracker/

Kdo jsme, 2023. *Vojenské zpravodajství* [online]. [cit. 2024-02-11]. Dostupné z: https://vzcr.cz/kdo-jsme-35

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, JUDr. Jan, 2010. Kybernetické útoky. In: *CESNET-CERTS* [online]. s. 22 [cit. 2023-11-12]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

Kybernetická obrana, 2023. *Vojenské zpravodajství* [online]. [cit. 2024-02-11]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46

Národní strategie kybernetické bezpečnosti České republiky 2021-2025

NĚMEČEK, Petr, 2019. *Bezpečnost IT služeb ve veřejné správě*. Praha. Bakalářská práce. AMBIS a.s.

Nová směrnice EU o kybernetické bezpečnosti „NIS2“ a návrh NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI, 2023. NÚKIB [online]. [cit. 2024-02-18]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

NÚKIB, 2024. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/

NÚKIB, 2023. Legislativa KB. In: *NÚKIB* [online]. [cit. 2023-10-29]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

NÚKIB, 2023. Návrh nového zákona o kybernetické bezpečnosti vstupuje do další fáze. In: *NÚKIB* [online]. [cit. 2023-10-29]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1969-navrh-noveho-zakona-o-kyberneticke-bezpecnosti-vstupuje-do-dalsi-faze/

O týmu CSIRT.CZ, 2023. *CSIRT.CZ* [online]. [cit. 2024-02-09]. Dostupné z: https://csirt.cz/cs/o-nas/

OPOJIŠTĚNÍ.CZ, 2022. Tři typy kybernetických útočníků a jejich motivace. In: *Kurzy.cz* [online]. 18.11.2022 [cit. 2023-11-30]. Dostupné z: https://www.kurzy.cz/zpravy/671723-tri-typy-kybernetickych-utocniku-a-jejich-motivace/

PORADA, Viktor, 2022. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie*. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-903-4.

Poskytované služby, 2024. *NCKB* [online]. [cit. 2024-02-06]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

Programové prohlášení vlády, 2023. Vláda ČR [online]. [cit. 2024-02-18]. Dostupné z: https://vlada.gov.cz/cz/programove-prohlaseni-vlady-193547/#digitalizace

RANSOMWARE Bezpečnostní tipy pro malé a střední firmy, 2022. *Eset* [online]. [cit. 2023-11-30]. Dostupné z: https://cdn-smartemailing.cz/15587/media/2023/ransomware/eset-ransomware-ebook-v4-cz-hyper.pdf?utm_medium=email&utm_content=ebook-ransomware&sid=ad87184e95694e69ac757ab230ea15cf&t=m

RAYMOND, Eric Stevens, 2001. *How to become a hacker* [online]. [cit. 2023-11-17]. Dostupné z: http://www.catb.org/~esr/faqs/hacker-howto.html

SMEJKAL, Vladimír, 2022. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-849-5.

Spam, 2023. In: *Eset* [online]. [cit. 2023-11-21]. Dostupné z: https://www.eset.com/cz/spam/

Statut Výboru pro kybernetickou bezpečnost, ze dne 3. ledna 2024, Příloha č. 7, usnesení vlády

Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025 - přílohy

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu, 2016. *Ministerstvo vnitra ČR* [online]. 2016 [cit. 2023-11-07]. Dostupné z: https://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx

Trojský kůň, 2016. *Avast* [online]. [cit. 2023-11-19]. Dostupné z: https://www.avast.com/cs-cz/c-trojan

Tři typy kybernetických útočníků a jejich motivace, 2022. *Kurzy.cz* [online]. 18.11.2022 [cit. 2023-11-30]. Dostupné z: https://www.kurzy.cz/zpravy/671723-tri-typy-kybernetickych-utocniku-a-jejich-motivace/

Úřad vlády a Fakulta elektrotechnická ČVUT zahájily spolupráci v oblasti kyberbezpečnosti, 2023. Fakulta elektrotechnická ČVÚT v Praze [online]. [cit. 2024-02-18]. Dostupné z: https://fel.cvut.cz/cs/aktualne/novinky/32738-urad-vlady-a-fakulta-elektrotechnicka-cvut-zahajily-spolupraci-v-oblasti-kyberbezpecnosti

Vedení úřadu, 2022. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/vedeni-uradu/

Vládní CERT, 2024. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2024-02-06]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/

Význam NÚKIB roste, kyberbezpečnost se týká všech, řekl premiér Fiala, 2023. ČTK České noviny [online]. [cit. 2024-02-18]. Dostupné z: https://www.ceskenoviny.cz/zpravy/2429243

Warez scene, 2020. *Wikipedia* [online]. 10. 9. 2023 [cit. 2023-11-14]. Dostupné z: https://en.wikipedia.org/wiki/Warez_scene

What is a Cyber Attack?, 2023. *Check point* [online]. [cit. 2024-02-09]. Dostupné z: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

What is Eavesdropping?, 2023. *FORTINET* [online]. [cit. 2024-02-04]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/eavesdropping

YANNAKOGEORGOS, Panayotis A, 2013. *Conflict and Cooperation in Cyberspace The Challenge to National Security*. 1. CRC Press. ISBN 9781466592018.

ZAVRŠNIK, Aleš, 2017. *Kyberkriminalita*. Praha: Wolters Kluwer. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Zpráva o činnosti 2022, 2023. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2024-02-04]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_cinnosti_NUKIB-2022.pdf

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Zákon č. 226/2022 Sb., o kybernetické bezpečnosti

Zákon, kterým se mění zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů, ve znění pozdějších předpisů, a zákon č. 79/1997 Sb., o léčivech a o změnách a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, § 2e

#nePINdej!, 2023. Policie České republiky [online]. [cit. 2024-02-29]. Dostupné z: https://www.policie.cz/clanek/nepindej.aspx