Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Incident management ve zdravotnictví

Bakalářská práce

Autor: Šimon Hlušička
Studijní obor: Informační a síťová bezpečnost

Vedoucí práce: Ing. Tomáš Svoboda, Ph.D.

Hradec Králové Srpen 2026

Prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval (pod vedením vedoucího bakalářské práce) samostatně a uvedl jsem všechny použité prameny a literaturu. V případě využití nástrojů umělé inteligence jsem uvedl jejich účel a rozsah použití a ověřil správnost takto získaných informací.

Při tvorbě bakalářské práce jsem využil nástroj umělé inteligence za účelem designu a zpracování tabulek v prostředí LaTeX.

Použitý model: Google Gemini.

V Hradci Králové dne 10. srpna 2026 Šimon Hlušička

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Tomášovi Svobodovi, Ph.D. za metodické vedení práce, odborné postřehy a vstřícnost při konzultacích. Dále mé díky patří Ing. Luboši Rejlovi za odbornou konzultaci. V neposlední řadě bych chtěl poděkovat svojí rodině za podporu a motivaci po celou dobu studia.

Abstrakt

Tato bakalářská práce se zabývá problematikou řízení kybernetických bezpečnostních incidentů v prostředí zdravotnické organizace jakožto poskytovatele regulované služby v režimu vyšších povinností podle vyhlášky č. 409/2025 Sb., a zákona č. 264/2025 Sb., o kybernetické bezpečnosti, které v České republice transponují Evropskou směrnici NIS2. Cílem této práce je analyzovat základní prvky a pojmy kybernetické bezpečnosti, novou právní úpravu kybernetické bezpečnosti v České republice, a její vztah se zdravotnictvím. Dále byly představeny právní požadavky, normy, standardy a další best-practices v oblasti řízení kybernetických bezpečnostních incidentů v oblasti zdravotnictví, a na jejich základě navržena metodika řízení, která byla simulována na modelové situaci kybernetického útoku.

Klíčová slova: Kybernetický bezpečnostní incident, zdravotnictví, aktivum, NIS2, řízení incidentů

Abstract

Title: Incident management in healthcare

This Bachelor thesis focuses on the matter of cybersecurity incident management in a healthcare environment as a regulated service under a regime of higher obligations in accordance to Decree no. 409/2025 Coll., and Act no. 264/2025 Coll., on Cybersecurity, which transpose the European Directive NIS2. The aim of this thesis is to analyze the fundamentals and concepts of cybersecurity, the new legal provision of cybersecurity in Czech republic, and its relation with healthcare. Furthermore, legal requirements, norms, standards, and other best-practices were introduced in the field of cybersecurity incident management in healthcare, upon which a methodology of incident management was conceived, which was then simulated on a model situation of a cybersecurity attack.

Key words: Cybersecurity incident, healthcare, asset, NIS2, incident management

Obsah

Seznam zkratek

CERT Computer emergency response team – „Tým pro reakci na počítačové nouzové situace“

CIA Confidentiality, Integrity, Availability – „Důvěrnost, Integrita, Dostupnost“

CSIRT Computer Security Incident Response Team — „Tým pro reakci na počítačové bezpečnostní incidenty“

CVE Common Vulnerabilities and Exposures

ČR Česká republika

DDoS Distributed Denial-of-service

DoS Denial-of-Service

ENISA Evropská agentura pro bezpečnost sítí a informací

EU Evropská unie

GDPR General Data Protection Regulation – „Obecné nařízení o ochraně osobních údajů“(Nařízení Evropského parlamentu a Rady (EU) 2016/679)

ICS Industrial Control Systems – „Průmyslové řídící systémy“

ICT Informační a komunikační technologie

IoMT Internet of Medical Things — „Internet zdravotnických věcí“

IP Internetový protokol

ISMS Information Security Management System – Systém řízení bezpečnosti informací

KBI Kybernetický bezpečnostní incident

KBU Kybernetická bezpečnostní událost

MKB Manažer kybernetické bezpečnosti

NIS Nemocniční informační systém

NIS2 Směrnice Evropského parlamentu a Rady 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

NIST National Institute of Standards and Technology – „Národní ústav standardů a technologií“

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

PDCA Plan, Do, Check, Act – Plánuj, Proveď, Zkontroluj, Jednej

SIEM Security Information and Event Management – „Správa bezpečnosti informací a událostí“

TLP Traffic Light Protocol

ÚOOÚ Úřad pro ochranu osobních údajů

VoBOvRNP Vyhláška č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

VoBOvRVP Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

VoRS Vyhláška č. 408/2025 Sb., o regulovaných službách

ZoKB Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, ze dne 11. června 2025

Seznam obrázků

Seznam tabulek

1 Úvod

Digitalizace ve zdravotnictví přinesla značný technologický posun a zlepšila dostupnost, kvalitu a rychlost poskytované lékařské péče. Elektronická zdravotnická dokumentace, Internet of Medical Things — „Internet zdravotnických věcí“ (IoMT), nebo telemedicína jsou technologie, které by bez digitalizace nemohly existovat. Nicméně s novými technologiemi se pojí i nová bezpečnostní rizika; zdravotní infrastruktura je závislá na nepřetržitém provozu, integritě a dostupnosti těchto technologií a elektronické dokumentace. Zatímco v ostatních odvětvích nedostupnost služby obvykle znamená finanční, nebo reputační ztrátu, narušení bezpečnosti ve zdravotnictví ohrožuje i zdraví a životy pacientů, kterým je zdravotní služba poskytována.

Kyberzločin je v současné době nejvýdělečnější forma zločinu, finanční ztráty způsobené kyberzločinem celosvětově činí odhadem 10,5 bilionu amerických dolarů.[1] Kybernetické útoky se neustále vyvíjí, existuje mnoho forem, zdravotnictví se potýká s obvyklými hrozbami, jako je phishing nebo ransomware, ale i se zranitelnostmi, jako je zastaralý software, nebo nedbalost zaměstnanců. Pokud dojde ke kompromitaci služby jedním z vektorů útoku, dochází k tzv. kybernetickému bezpečnostnímu incidentu, který je třeba co nejrychleji mitigovat a omezit jeho dopady na poskytování zdravotnických služeb a zdraví pacientů. Neexistuje ideální, všemuvzdorný systém kybernetické bezpečnosti, ale existuje několik technik, jejichž účelem je těmto nežádoucím situacím předcházet. Pro zvládání incidentů je klíčové řízení incidentů – incident management – stanovený proces, který pomocí přesně definovaných kroků napomáhá uvést provoz zpět do normálního stavu.

V České republice je 160 nemocnic akutní péče, poskytující zdravotní služby podle zákona č. 372/2011 Sb., o zdravotních službách.[2] Všechna tato zařízení jsou vystavená kybernetickým hrozbám, a proto je nutné je zabezpečit standardizovaným způsobem. V České republice je od roku 2025 právním základem kybernetické bezpečnosti nový Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, ze dne 11. června 2025 (ZoKB) a související vyhlášky, které transponují požadavky Evropské směrnice NIS2. V této práci bude představen přehled kybernetické bezpečnosti, její právní úpravy v ČR a jejich kontext ve zdravotnictví, životní cyklus a jeho řízení.

2 Cíl a metodika práce

2.1 Cíl práce

Cílem této bakalářské práce je návrh procesu řízení kybernetických bezpečnostních incidentů pro poskytovatele zdravotnictví jako regulované služby v režimu vyšších povinností podle vyhlášky č. 409/2025 Sb. v souladu s novým zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, který transponuje požadavky Evropské unie na zajištění ochrany digitální infrastruktury ve směrnici NIS2. Navržený proces řízení incidentů rámcově vychází z norem, standardů a best-practices organizací, které při řízení incidentů využívají podobné procesy. Výsledkem je metodika procesu, který by mohl být v praxi nasazen ve zdravotnickém zařízení pro účely řízení kybernetických bezpečnostních incidentů.

2.2 Metodika práce

Teoretická část byla zpracována literární rešerší a vychází tak z odborných článků, legislativních předpisů, norem a standardů, v této části je představena terminologie v oblasti kybernetické bezpečnosti, přehled nového zákona o kybernetické bezpečnosti a souvisejících prováděcích předpisů, a jakým způsobem je na ně vázáno zdravotnictví. Dále jsou v práci představeny různé klasifikační rámce kybernetických bezpečnostních incidentů, a samotný proces řízení kybernetického bezpečnostního incidentu vycházející ze standardů, norem a best-practices. Některé aspekty řízení incidentů vycházejí po konzultaci s manažerem kybernetické bezpečnosti z praktik skutečné organizace, nicméně vzhledem k faktu, že konkrétní bezpečnostní postupy jsou důvěrnými informacemi organizace, teoretický základ práce čerpá převážně z jmenovaných literárních zdrojů.
Praktická část pracuje s navrženým procesem řízení kybernetických bezpečnostních incidentů na modelové organizaci. Jednotlivé kroky při řízení jsou popsány jako reakce na simulovaný kybernetický útok. Byla identifikována aktiva a bezpečnostní role aktérů při řešení incidentu, a jakým způsobem mohou být jednotlivé fáze, které jsou zahrnuty v diagramu procesu řízení kybernetických bezpečnostních incidentů, implementovány v praxi.

3 Úvod do kybernetické bezpečnosti

„Kybernetická bezpečnost není pouze technickým problémem, ale komplexní výzvou vyžadující multidisciplinární přístup. Spolupráce mezi vládními institucemi, soukromým sektorem a občanskou společností je pro vytvoření odolného a bezpečného digitálního prostředí nezbytná.“[3]

Kybernetická bezpečnost, jakožto podmnožina bezpečnosti, nemá jednotně uznávanou definici. Jan Kolouch a Pavel Bašta (2019) definují kybernetickou bezpečnost jako: *„souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů, schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.“*[4] Kybernetická bezpečnost existuje v kyberprostoru, i mimo něj.[4]

Kromě pojmu kybernetická bezpečnost se můžeme setkat i s pojmem bezpečnost informací, který lze nalézt v technických normách. Standard ČSN ISO/IEC 27000:2020 uvádí bezpečnost informací jako *„zachování důvěrnosti, integrity a dostupnosti informací.“*[5] Lze tedy říct, že narušením jednoho z prvků důvěrnosti, integrity a dostupnosti dochází k narušení bezpečnosti informací. Bezpečnost informací sama o sobě není smyslem činnosti organizace, jde o podpůrnou, ale nezbytnou součást činnosti organizace, implementace se liší podle velikosti, kritičnosti a typu organizace; jinak bude k bezpečnosti informací přistupovat stát než obchodní společnost. Každá organizace si sama určí, které aspekty bezpečnosti informací jsou pro ni více kritické; zatímco dostupnost a integrita informací je klíčová pro organizaci, důvěrnost nemusí být tolik významná, pokud se jedná o veřejně přístupné informace. V jiném případě může být právě důvěrnost klíčová v případě zachování obchodního tajemství, jehož vyzrazení by mohlo ohrozit pozici organizace na trhu a způsobit značné finanční ztráty. Bezpečnost informací lze realizovat pomocí vhodných opatření zohledňujících různé hrozby bezpečnosti informací, a to prostřednictvím systému řízení bezpečnosti informací – ISMS. Bezpečnost informací se týká každé organizace, která shraňuje jakékoliv informace – citlivá data, jejichž neoprávněný únik, změna, nebo přístup mohou zásadně ohrozit její provoz.[6]

3.1 CIA Triáda

Při uplatňování kybernetické bezpečnosti se implementují tzv. triády kybernetické bezpečnosti, jejichž průnikem získáme bezpečnost informací. Pokud je jedna nebo více prvků narušena, je narušena bezpečnost informací. Nejpoužívanější triádou v rámci kybernetické bezpečnosti je triáda CIA. Ve zdravotnictví se jedná hlavně o ochranu bezpečnosti informací o zdravotním stavu[7], definovaných jako „*osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu*“ podle bodu 15) čl. 4 GDPR, která jsou zpracována pro účely poskytování zdravotní péče podle bodu i) čl. 9 GDPR.[8]

3.1.1 Důvěrnost

Důvěrnost je stav, kdy mají k informacím, datům, či technologiím přístup pouze autorizované subjekty, a nikdo jiný.[4] Smyslem zajištění důvěrnosti dat ve zdravotnictví je ochrana soukromí pacienta a prevence neoprávněného – úmyslného, nebo z nedbalosti – přístupu k datům, kdy může dojít k jejich úpravě, odcizení, nebo ztrátě. Abychom mohli určit míru důvěrnosti dat, můžeme využít TLP protokol, který využívá příznaky omezující sdílení dat sadou příznaků určujících omezení sdílení. TLP uvádí příznaky TLP:RED až TLP:CLEAR. [9] Příkladem útoku na důvěrnost dat je spearphishingový útok e-mailem, při kterém se útočník vydává za zaměstnance nemocnice s přístupem k datům s příznakem TLP:RED, a požaduje údaje o zdravotním stavu od skutečného zaměstnance, který z nedbalosti údaje útočníkovi poskytne.

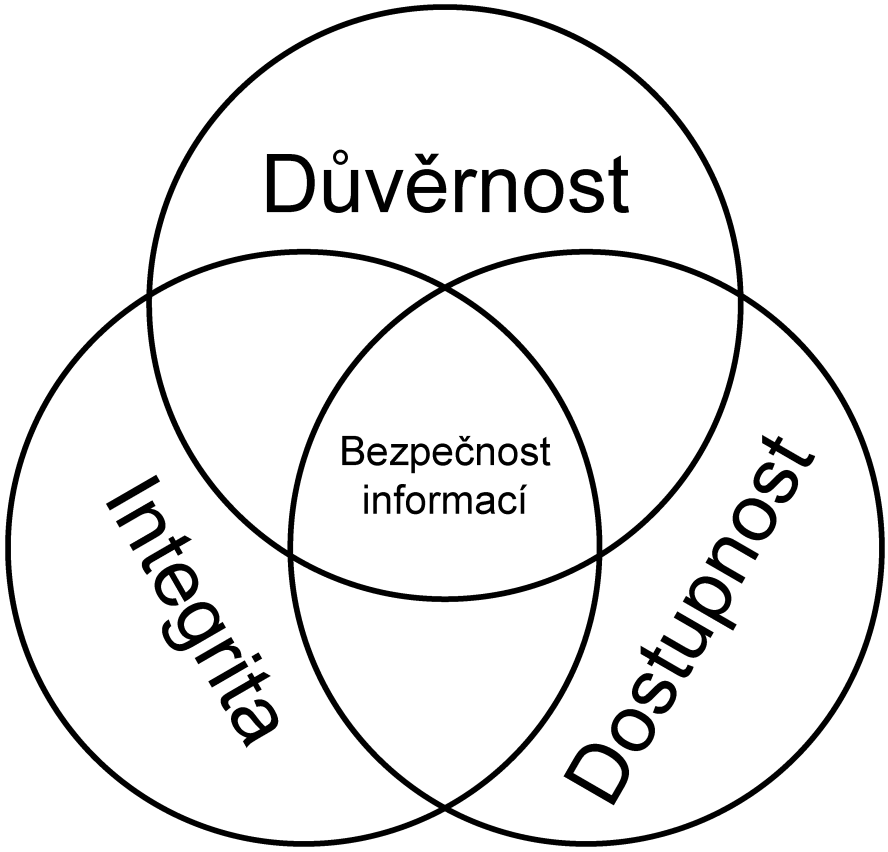
3.1.2 Integrita

Integrita, nebo také neporušenost, je nemožnost zásahu do informací, dat, technologií a jejich nastavení osobami jinými, než jsou k tomuto výkonu oprávněny. Lze tedy říct, že pokud jsou informace, nebo jiná aktiva, neoprávněně modifikovány, jedná se pak o narušení integrity. Pokud dojde k nežádoucí změně, může trvat velmi dlouho, než je tato nežádoucí změna odhalena.[4] Ve zdravotnictví může narušení integrity ohrozit život a zdraví pacientů prostřednictvím chybných, neplatných, nebo chybějících záznamů o pacientech. Integritu lze zajistit validací dat, zálohami, audit logy, digitálním podpisem nebo řízením přístupu.[7] Příkladem útoku na integritu dat je Data Tampering, který může být úmyslný, nebo z nedbalosti. Pokud data nejsou při vstupu do databáze validována, mohou obsahovat abnormální, nebo neplatná data. Dopadem jsou nesprávné

diagnostiky, které mohou ohrozit zdraví pacientů.

3.1.3 Dostupnost

Dostupnost je garance přístupu k informacím, datům, nebo technologiím v okamžiku, kdy je vyžadován přístup k nim. I přes ideální zajištění integrity a důvěrnosti aktiv v systému je systém nevyužitelný, pokud dostupnost neumožní přístup k datům.[4] Ve zdravotnictví se dostupností rozumí přístup ke zdravotním záznamům pacienta, bez kterých není možné poskytovat zdravotní péči. V případě výpadku nemocničního systému nemůže zaměstnanec nemocnice poskytnout zdravotní péči pacientovi jehož dopadem je ohrožení zdraví pacienta. Dostupnost lze zajistit redundancí síťových prvků a monitoringem síťového provozu. [7]



Obrázek 1: CIA Triáda [1]

[1] Vlastní tvorba

3.2 Kyberprostor

Kyberprostor je dynamický systém tvořený prvky ICT vytvářející celosvětovou počítačovou síť, ve které uživatelé pomocí jednotlivých počítačových systémů s touto globální sítí interagují. Jedná se o nehmotný prostor, virtuální realitu, závislou na materiální existenci hardware. Při změně fyzického média kyberprostoru, např. prvků sítě, počítačových systémů, cloudových úložišť atd. se dokáže těmto změnám kyberprostor přizpůsobit a existovat dále, avšak při zničení veškerého materiálního média dojde k úplnému kolapsu a zničení kyberprostoru. Mezi hlavní znaky kyberprostoru lze zařadit decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost a možnost ovlivňování mínění skrze uživatele. V současné době považují mnohé státy kyberprostor jako pátou doménu, po zemi, vodě, vzduchu a vesmíru, a proto se nejen ze strany vládních organizací klade čím dál větší pozornost této doméně.[4]
Kyberprostor lze rozdělit do tří vrstev: fyzická, logická a sociální.[10]

3.2.1 Fyzická vrstva

Protože by kyberprostor nemohl existovat bez fyzického média, první vrstvou kyberprostoru je fyzická vrstva, složená z geografické a fyzické síťové části. Geografickou částí se rozumí fyzické umístění síťových prvků. Přestože lze v kyberprostoru snadno překročit geopolitické hranice státních celků, jeho dosah je stále limitován fyzickou přítomností relevantních médií. Fyzická síťová část je složena z již zmíněné hardwarové infrastruktury a síťových prvků, které je propojují.[10]

3.2.2 Logická vrstva

Logická vrstva obsahuje komponenty logické sítě a logická spojení mezi síťovými uzly; např. počítači, mobilními telefony, atd. s vlastní IP adresou.[10]

3.2.3 Sociální vrstva

Protože s kyberprostorem interagují fyzické osoby, třetí vrstva je sociální, složená z komponent „kyberosoba“ a osoba. Kyberosoba je shluk jednoznačné osobní identifikace, např. e-mailová adresa, IP adresa počítače, telefonní číslo atd. Osoba je člověk využívající síť. Osoba a kyberosoba jsou spolu ve vztahu N:N, protože jedna osoba může být více kyberosob, např. použitím více různých e-mailových adres, a zároveň více osob může sdílet např. stejnou e-mailovou adresu.[10]

3.2.4 Vrstvy přístupu

Kyberprostor je vrstvený i podle dostupnosti a přístupu k datům pro běžného uživatele, proto jej lze rozdělit na služby a data:

- volně přístupná na síti pomocí internetu – Surface Web
- přístupná pouze v rámci konkrétních sítí a zařízení – Deep Web
- záměrně skrytá a přístupná pouze pomocí speciálních nástrojů – Dark Web[4]

4 Kybernetická bezpečnost v České republice

4.1 Zákon o kybernetické bezpečnosti

V České republice je legislativním základem kybernetické bezpečnosti zákon č.264/2025 Sb., o kybernetické bezpečnosti, účinný od 1. listopadu 2025, který nahrazuje předchozí zákon č.181/2014 Sb. a zavádí změny dané směrnicí Evropského parlamentu a Rady EU 2022/2555 NIS2.[11] Hlavním cílem návrhu nového ZoKB bylo vykonání řádné transpozice NIS2 a zajištění základní úrovně zabezpečení důvěrnosti, integrity a dostupnosti informací a dat v organizacích poskytujících služby ve společensky významných odvětvích. NIS2 rozšiřuje okruh regulovaných odvětví a služeb, cílem nového ZoKB bylo tyto požadavky zohlednit, a proto má dopad na výrazně větší počet organizací. ZoKB a související vyhlášky připravil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), vycházející z dosud shromážděných poznatků a zkušeností v oblasti kybernetické bezpečnosti.[11] ZoKB nově zavádí dvě úrovně regulace pro poskytovatele regulovaných služeb: vyšší a nižší. Rozdělení poskytovatelů do dvou úrovní vychází z principu "dvourychlostní kybernetické bezpečnosti"v souladu s NIS2, a jeho cílem je usnadnění menším a středním organizacím splnit požadovaná opatření. Pokud alespoň jedna služba organizace spadá do režimu vyšších povinností, všechny ostatní regulované služby poskytované organizací do tohoto režimu automaticky spadají také.[11]

4.2 Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB je ústřední správní orgán kybernetické bezpečnosti v ČR. Kromě kybernetické bezpečnosti zajišťuje NÚKIB ochranu informací v oblasti informačních a komunikačních systémů a kryptografické ochrany a má na starosti regulovanou službu v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 podle zákona č. 205/2017 Sb.[2][12]

[2] Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony

4.3 Vyhláška o regulovaných službách

Vyhláška č. 408/2025 Sb., o regulovaných službách je prováděcí právní předpis k ZoKB, který stanovuje seznam služeb a podmínky významnosti poskytovatele služby a rozdělení poskytovatelů podle poskytovaných regulovaných služeb, vymezených v ZoKB.[3][4] Tato odvětví jsou regulovaná směrnicí NIS2, a platí jednotně v celé EU. VoRS specifikuje konkrétní služby podléhající regulaci, podle velikosti a významnosti poskytovatele. Příloha VoRS stanovuje rozdělení poskytovatelů podle poskytovaných služeb do režimů povinností podle §8 odst. 1 ZoKB. V příloze je uvedeno 22 odvětví regulovaných služeb, z nichž je pro tuto práci relevantní uvést bod č.18 Zdravotnictví.[13]

Regulovaná služba	
Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
Poskytování zdravotní péče podle zákona o zdravotních službách	Poskytovatel zdravotních služeb poskytující zdravotní péči podle zákona o zdravotních službách je: • poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem • poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem Organizační složka státu zřízená ústředním orgánem státní správy, jíž bylo uděleno oprávnění k poskytování zdravotních služeb podle zákona o zdravotních službách, je poskytovatelem regulované služby v režimu vyšších povinností.

Tabulka 1: Bod č.18 přílohy VoRS – Zdravotnictví jako regulovaná služba

[3] §4 odst. 1 ZoKB
[4] §1 - 3 VoRS

5 Zdravotnictví v ČR jako regulovaná služba

5.1 Regulovaná služba

Regulovaná služba je zásadní činnost nutná pro fungování státu a veřejnosti, a jejíž narušení by mohlo mít významný dopad na bezpečnost a stabilitu státu, zdraví obyvatel, ekonomiku, nebo životní prostředí. Smyslem regulace služeb je zajištění odpovídající úrovně kybernetické bezpečnosti u poskytovatelů regulovaných služeb a umístění těchto subjektů do systému koordinovaného řešení kybernetických incidentů.[14] Zdravotnictví je jednou z regulovaných služeb, uvedená ve VoRS.

5.2 Poskytovatel regulované služby

Poskytovatel regulované služby je podle ZoKB subjekt poskytující regulovanou službu podle §3 až §5 ZoKB, a zároveň je středním, nebo velkým podnikem.[15] Poskytovatelé zdravotních služeb jsou zařazeni do režimu regulované služby v závislosti na charakteru poskytované služby a velikosti jejich podniku. O rozdělení do režimů rozhoduje Vyhláška č. 408/2025 Sb., o regulovaných službách (VoRS).[16] V případě poskytování zdravotních služeb se subjekt stává poskytovatelem regulované služby, pokud poskytuje mj. zdravotní péči podle zákona o zdravotních službách.[16]

5.3 Režimy poskytovatele regulované služby

Bod 15 směrnice NIS2 zavádí dvě nové kategorie subjektů regulovaných služeb: základní a důležité[17]. ZoKB přistupuje k tomuto rozdělení tak, že místo dvou subjektů zavádí pouze jeden: poskytovatele regulované služby se dvěma režimy.[18] Kromě transpozice NIS2 je motivací rozdělení také přizpůsobení rozsahu bezpečnostních povinností na základě významnosti poskytované služby tak, aby byla kybernetická bezpečnost regulovaných služeb přiměřená hrozbám a velikosti možných dopadů. Oba režimy vycházejí ze společného základu bezpečnostních opatření, liší se hloubkou a rozsahem implementace.[16] Oba režimy jsou právně definovány pomocí dvou samostatných vyhlášek:

- Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (VoBOvRVP)
- Vyhláška č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (VoBOvRNP)

5.3.1 Režimy poskytovatelů zdravotnictví jako regulované služby

O tom, do jakého režimu jsou poskytovatelé zdravotní péče poskytující služby podle zákona o zdravotních službách zařazeni, rozhoduje velikost podniku. V případě, že je poskytovatel velký podnik, je zařazen do režimu vyšších povinností, pokud se jedná o střední podnik, jsou zařazeni do nižších povinností. Výjimkou je organizační složka státu zřízená ústředním orgánem státní správy, která poskytuje zdravotní péči; ta je zařazena automaticky do režimu vyšších povinností.[13]

5.4 Povinnosti poskytovatele regulované služby

Poskytovatel regulované služby je povinnen v rámci stanoveného rozsahu zavést a provádět organizační a technická bezpečnostní opatření, která chrání poskytování regulované služby a kybernetickou bezpečnost aktiv organizace. Tato opatření jsou uzpůsobena režimu, do kterého poskytovatel regulované služby spadá; poskytovatelé ve vyšším režimu jsou povinni zavést 14 organizačních a 11 technických opatření, zatímco poskytovatelé v nižším režimu musí zavést celkem 13 opatření, která jsou v jedné skupině.

5.5 Organizační opatření poskytovatele regulované služby

5.5.1 Systém řízení bezpečnosti informací

Information Security Management System – Systém řízení bezpečnosti informací (ISMS)[19] je sada politik, směrnic a postupů, které umožňují organizaci chránit bezpečnost informací aktiv. Cílem ISMS je minimalizace rizik a zajištění kontinuity služby omezením dopadu na aktiva. Aby mohl být ISMS v praxi zaveden, je třeba určit jeho cíle: vybudování povědomí o nutnosti bezpečnosti informací, posouzení rizik, na jejichž základě budou vypracována bezpečnostní opatření, sestavení bezpečnostní politiky, aktivní prevence a detekce, a opakovaný audit bezpečnosti informací. Konkrétní postupy zavedení ISMS jsou uvedené v sadě norem ČSN EN ISO/IEC 27000.[6]
VoBOvRVP vyžaduje v rámci ISMS podobné požadavky, ve zdravotnickém prostředí je nutné alespoň jednou ročně vyhodnocovat účinnost ISMS mj. posouzením plánu zvládání rizik, auditu a revizi hodnocení rizik, a na jejím základě zpracovat zprávu o vyhodnocení účinnosti. [20]

5.5.2 Stanovení rozsahu řízení kybernetické bezpečnosti

§12 ZoKB vyžaduje u poskytovatelů stanovení rozsahu řízení kybernetické bezpečnosti – a to v obou režimech – ve třech krocích.

Prvním krokem je určení všech primárních aktiv v organizaci poskytovatele. Určí se všechna primární aktiva v podobě informací zpracovávaných organizací nebo poskytovaných služeb. Smyslem této identifikace je v dalším kroku rozhodnout, zda tato aktiva přímo souvisejí s regulovanou službou. Poté se u každého identifikovaného aktiva posoudí, zda s poskytováním regulované služby souvisí, nesouvisející aktiva jsou z rozsahu řízení kybernetické bezpečnosti vyloučena s odůvodněním a jsou evidována jako nesouvisející. Nakonec se po identifikaci souvisejících primárních aktiv se stanoví jednotlivá podpůrná aktiva pro každé primární aktivum.

Rozsah řízení kybernetické bezpečnosti se považuje za stanovený až po dokončení jeho dokumentace. Dokud tak není učiněno, platí výchozí rozsah kybernetické bezpečnosti obsahující všechna primární a podpůrná aktiva. Rozsah není statický a je třeba jej pravidelně aktualizovat, NÚKIB doporučuje aktualizaci alespoň jednou ročně, nebo při významných změnách v organizaci. [21]

5.5.3 Řízení aktiv

V návaznosti na stanovení rozsahu organizace rozhodne, jakým způsobem identifikuje a bude hodnotit svá aktiva. Primární aktiva jsou taková aktiva, jejichž ztráta nebo poškození by narušily provoz a poskytování služeb organizace. Při identifikaci je proto hlavní otázkou, zda může organizace bez identifikovaného aktiva být schopná provozu; pokud ne, jedná se o primární aktivum. Následně jsou identifikována podpůrná aktiva, která přímo souvisejí se svým primárním aktivem; zajišťují provoz a podporu primárních aktiv. Podpůrná aktiva mohou být software, hardware, databáze, nebo technické služby.[22]

Kromě identifikace je třeba stanovit metodiku identifikace aktiv. Při hodnocení aktiv sledujeme, jaký je význam dopadu na organizaci při narušení bezpečnosti informací. Vzhledem k tomu, že bezpečnost informací je zajištěním CIA, stejným způsobem je hodnocen dopad při narušení bezpečnosti informací na aktivum. Hodnocením důvěrnosti, integrity a dostupnosti podle definovaných tabulek lze určit významnost aktiva, resp. velikost dopadu na organizaci při narušení. Nejvyšší naměřená hodnota kritičnosti je zároveň celková hodnota významnosti aktiva. Při hodnocení důvěrnosti aktiv lze

vycházet z mezinárodního standardu TLP.

Poskytovatel regulované služby musí všechna svá aktiva evidovat; do evidence uvede seznam aktiv, jestli je aktivum primární – nebo v případě podpůrného aktiva – jaké je jeho primární aktivum, správce a garanta aktiva, a jeho hodnocení podle CIA metrik. Na hodnocení aktiv se podílí garanti aktiv společně s manažerem kybernetické bezpečnosti[23] Garant aktiva je osoba přímo odpovídající za dané aktivum ve společnosti. Příkladem garanta aktiva ve zdravotnictví je provozovatel IT služeb jakožto garant NIS.

Úroveň	Popis
Kritická	Aktiva nejsou veřejně přístupná a vyžadují zvláštní kategorii zabezpečení. Při sdílení se třetí stranou je aktivum označeno jako TLP:RED.
Vysoká	Aktiva nejsou veřejně přístupná, a jejich ochrana je vyžadována v bezpečnostní dokumentaci. Při sdílení se třetí stranou je aktivum označeno jako TLP:AMBER.
Střední	Aktiva nejsou veřejně přístupná, ale jejich ochrana není vyžadována v bezpečnostní dokumentaci. Při sdílení se třetí stranou je aktivum označeno jako TLP:GREEN.
Nízká	Aktiva jsou veřejně přístupná a narušení nijak neohrožuje poskytování regulované služby. Při sdílení se třetí stranou je aktivum označeno jako TLP:WHITE.

Tabulka 2: Hodnocení důvěrnosti aktiv [5]

Úroveň	Popis
Kritická	Aktivum vyžaduje ochranu integrity a narušení integrity vážně ohrožuje poskytování regulované služby.
Vysoká	Aktivum vyžaduje ochranu integrity a narušení integrity ohrožuje poskytování regulované služby.
Střední	Aktivum může vyžadovat ochranu integrity a narušení integrity může vést k ohrožení poskytování regulované služby.
Nízká	Aktivum nevyžaduje ochranu integrity a narušení integrity neohrožuje poskytování regulované služby.

Tabulka 3: Hodnocení integrity aktiv [6]

Úroveň	Popis
Kritická	Narušení dostupnosti aktiva není přípustné a i několikaminutový výpadek vážně ohrožuje poskytování regulované služby.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu v řádu hodin. Dlouhodobější výpadek ohrožuje poskytování regulované služby.
Střední	Narušení dostupnosti aktiva by nemělo překročit den. Dlouhodobější výpadek vede k možnému ohrožení poskytování regulované služby.
Nízká	Narušení dostupnosti aktiva v řádu týdnů má zanedbatelný dopad na poskytování regulované služby.

Tabulka 4: Hodnocení dostupnosti aktiv [7]

[5] Vlastní tvorba podle VoBOvRVP
[6] Vlastní tvorba podle VoBOvRVP
[7] Vlastní tvorba podle VoBOvRVP

5.5.4 Zvládání KBU a KBI

Pro zvládání KBU poskytovatel musí určit, jakým způsobem bude KBU detekován, logován, a vyhodnocen, včetně posouzení, zda se jedná o KBU, nebo KBI, a také které role budou za tyto postupy zodpovědné. Pro zvládání KBI zajistí poskytovatel proces zvládání KBI, koordinaci při jeho zvládání, hlášení, vytvoření zprávy o jeho vyřešení, a pokud byl posouzen jako významný, určí jeho příčinu a vyhodnotí účinnost řešení KBI a na základě vyhodnocení provede kroky k zamezení opakování řešeného KBI. U všech těchto aktivit určí, které role budou za ně zodpovědné. [20]

5.6 Technická opatření poskytovatele regulované služby

5.6.1 Detekce události

Veškerá data, která se pohybují v rámci interní komunikační sítě je třeba monitorovat pomocí centrálně spravovaného nástroje pro detekci KBU, který ověřuje, kontroluje a blokuje provoz v interní síti a chrání ji před škodlivým kódem. Pověřená osoba, např. bezpečnostní analytik, pomocí nástroje řídí spouštění obsahu vyměnitelných nosičů dat, oprávnění ke spuštění kódu, a detekuje KBU na základě chování uživatelů a technických aktiv připojených v síti.[20] Příkladem takového detekčního a monitorovacího nástroje je SIEM.

5.6.2 Zaznamenávání události

Poskytovatel regulované služby na základě řízení aktiv určí seznam technických aktiv, který pravidelně aktualizuje v závislosti na skutečném stavu aktiv v organizaci, a to buď v pravidelných intervalech, nebo významných změnách. U těchto aktiv zaznamenává (loguje) akce, jako jsou přihlašování (včetně neúspěšných pokusů), provedení a pokusy činnosti, která vyžaduje zvláštní práva(např. administrátorská), nebo manipulaci s účty. U těchto aktivit eviduje uživatelský účet a technické aktivum, ze kterého byly provedeny. Tyto záznamy osoba pověřená logováním pomocí SIEM shraňuje a ukládá alespoň 3 roky. U logů musí být zajištěna ochrana důvěrnosti a integrity před jakoukoliv změnou nebo neoprávněným přístupem.[20]

5.6.3 Vyhodnocování událostí

SIEM musí nepřetržitě sbírat, vyhledávat a seskupovat veškerý provoz v interní síti a v případě detekce KBU o tom okamžitě informovat bezpečnostní role a další relevantní osoby(např. bezpečnostního analytika nebo manažera kybernetické bezpečnosti) s cílem identifikace potencionálního KBI. SIEM musí být pravidelně aktualizován včetně jeho detekčních pravidel, a při vysokém výskytu false-positives, nebo naopak nízké přesnosti detekce musí být pravidla upravena, aby byly všechny skutečné KBU detekované. [20]

5.7 Hlášení kybernetických bezpečnostních incidentů

Povinnost hlásit KBI, právně vycházející z §15 ZoKB, platí pro všechny poskytovatele regulované služby v případě, že se projevily ve *stanoveném rozsahu*, mají původ v kyberprostoru, a nelze u nich do 24 hodin vyloučit úmyslné zavinění. Stanovený rozsah je pojem mající právní základ v §12 ZoKB, jde o seznam aktiv, které souvisí s poskytováním regulované služby. V případě vyloučení úmyslného zavinění při incidentech provozního, nebo operativního charakteru není povinné incident hlásit. Osoba, která není regulovaným subjektem, není povinna hlásit jakékoliv KBI.[24][16] Poskytovatelé regulované služby hlásí KBI také v závislosti na tom, jestli jsou zařazeni do režimu nižších, nebo vyšších povinností:

- Poskytovatelé regulované služby v režimu vyšších povinností jsou povinni hlásit veškeré KBI, pokud splňují podmínky pro hlášení.
- Poskytovatelé regulované služby v režimu nižších povinností jsou povinni hlásit pouze KBI, u kterých byl dopad na poskytování regulované služby vyhodnocen jako významný. Poskytovatel sám posoudí významnost dopadu KBI podle §14 VoBOvRNP.

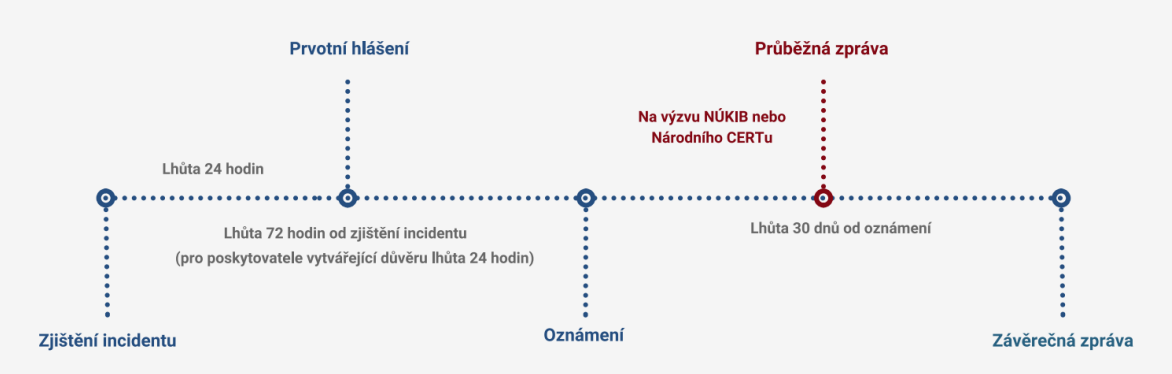
5.7.1 Průběh hlášení KBI

Poskytovatel regulované služby hlásí KBI na portál NÚKIB, e-mailem, nebo datovou schránkou do 24 hodin od okamžiku, kdy pověřená osoba(obvykle manažer kybernetické bezpečnosti nebo bezpečnostní analytik) vyhodnotí událost v organizaci jako KBI.[24]

Postup hlášení KBI se liší v závislosti na velikosti dopadu; Poskytovatel regulované služby v režimu vyšších povinností KBI nahlásí na NÚKIB, který vyhodnotí významnost dopadu; a podle toho rozhodne další postup. Pokud je dopad vyhodnocen

jako nevýznamný, poskytovatel nemusí podnikat další kroky. Pokud je dopad vyhodnocen jako významný, poskytovatel do 72 hodin od zjištění KBI zašle na NÚKIB oznámení; podrobnější zprávu o incidentu, a pokud jsou k dispozici, také uvede dopad a indikátory kompromitace.

Dále poskytovatel na výzvu NÚKIB nebo Národního CERT zašle průběžnou zprávu o změnách stavu zvládání KBI, a do 30 dnů od zaslání oznámení pošle závěrečnou zprávu o vyřešení KBI, kde uvede podrobný popis KBI, jeho závažnost, dopad, druh hrozby, příčinu KBI, a opatření k mitigaci dopadů. Pokud KBI není do 30 dnů vyřešen, poskytovatel odešle další průběžnou zprávu, dokud KBI není vyřešen.[24][16]



Obrázek 2: Průběh hlášení KBI [8]

5.8 Zvládání kybernetických bezpečnostních incidentů

NÚKIB nebo Národní CERT poskytne do 24 hodin od nahlášení vyjádření ke KBI, a na žádost dotčeného poskytovatele regulované služby poskytne metodickou podporu ke zvládání KBI. NÚKIB má právo si od poskytovatele vyžádat veškeré informace týkající se KBI. NÚKIB poté údaje zaeviduje do svojí evidence. [16]

5.9 Informační povinnost

Pokud to poskytovatel regulované služby v zájmu kontinuity poskytování služby uzná za vhodné, informuje uživatele regulované služby o existenci KBI s významným dopadem, který by mohl negativně ovlivnit poskytování služby. NÚKIB má právo uložit poskytovateli zákaz, nebo povinnost – ve vymezeném rozsahu – informovat dotčené uživatele o KBI. Ve zdravotnictví se uživatelem myslí pacient. Zároveň je poskytovatel povinnen informovat uživatele regulované služby, který může být postihnut významnou

[8] Převzato z: (24)

hrozbou, o tom, jaké kroky má podniknout, aby zminimalizoval dopad při využití této hrozby na uživatele. [16]

5.10 Vrcholné vedení a bezpečnostní role

Vrcholné vedení poskytovatele ve vyšším režimu je osoba, nebo skupina osob, zodpovědná za stanovení bezpečnostní politiky, zajištění finančních a technických prostředků potřebných pro zajištění a provoz kybernetické bezpečnosti a informování zaměstnanců o významu dodržování bezpečnostních pravidel. Vrcholné vedení musí být seznámeno s plánem zvládání rizik a výsledky auditů a kontrol kybernetické bezpečnosti. Vedení je zodpovědné za sestavení výboru pro řízení kybernetické bezpečnosti, jehož členové, odborně způsobilí k výkonu řízení kybernetické bezpečnosti, jsou minimálně jeden člen vrcholného vedení a manažer kybernetické bezpečnosti, a dále přidělí bezpečnostní role:

- Manažer kybernetické bezpečnosti, zodpovědný za řízení kybernetické bezpečnosti a informování vrcholného vedení o jeho stavu
- Architekt kybernetické bezpečnosti, zodpovědný na návrh implementace bezpečnostních opatření
- Garant aktiva, zodpovědný za bezpečnost aktiva
- Auditor kybernetické bezpečnosti, zodpovědný za nestranné provedení auditu kybernetické bezpečnosti

Osoby musí být k výkonu bezpečnostních rolí vyškoleny a prokázat způsobilost k řízení kybernetické bezpečnosti praxí. Obdobně je sestaveno vrcholné vedení i v režimu nižších povinností, s rozdílem, že VoBOvRNP nevyžaduje sestavení výboru ani určení bezpečnostních rolí.

6 Základní prvky kybernetické bezpečnosti

S postupem vývoje technologií a digitalizace se s problematikou řešení kybernetických bezpečnostních událostí a incidentů setkává prakticky každá společnost. Pro mnohé organizace může mít neřízený KBI velmi vážné důsledky; od značné finanční nebo materiální ztráty, nebo dokonce ohrožení lidských životů, přes poškození dobré pověsti, až po hrozbu pokuty při nedodržování zákona či povinnosti náhrady škody. Řízení KBI je oblast těsně související s celkovým řízením kybernetické bezpečnosti v rámci organizace, některé z nich jsou povinny v této oblasti plnit řadu právních požadavků. Pro pochopení řízení KBI je vhodné vymezit a definovat pojmy této problematiky. [6]

6.1 Definice pojmů

6.1.1 Aktivum

V kontextu kybernetické bezpečnosti je základním předmětem ochrany aktivum – jakýkoliv fyzická, nebo digitální entita mající význam a hodnotu pro organizaci. Organizace existuje a je provozuschopná díky jejím aktivům, a proto je pro ni důležité svoje aktiva chránit před kybernetickými útoky, které by mohly v případě narušení aktiva mít za následek finanční, nebo reputační ztrátu, ohrožení provozu organizace, nebo v případě poskytování zdravotní péče, ohrožení zdraví nebo života pacientů. Aktiva nemusí být nutně hmotná, může se jednat i o know-how, účty zaměstnanců, nebo dobrou pověst organizace, jejichž narušení by mohlo způsobit škodu organizaci, stejně jako při narušení fyzických aktiv, jako jsou servery, databáze, nebo v případě zdravotnických organizací, zdravotnické IoMT, dokumentaci, nebo NIS.[25]

S pojmem aktivum pracuje i ZoKB, který pro svoje účely definuje pojem aktivum, a dělí jej na primární, podpůrné a technické. Primární aktivum je informace, nebo poskytovaná služba, podpůrné aktivum zajišťuje funkci primárních aktiv – jedná se o budovy, klíčové zaměstnance, nebo dodavatele. Technickým aktivem se rozumí technické a programové prostředky nebo vybavení. [16]

6.1.2 Zranitelnost

Zranitelnost je slabina – chyba nebo nedostatek – v systému, která může při využití mít negativní dopad bezpečnost informací porušením důvěrnosti, integrity a dostupnosti.[26] Zranitelnosti mohou existovat buď jako úmyslné chyby v systému, nebo jako

neúmyslné slabiny v systému, které vznikly již při návrhu kybernetické bezpečnosti systému, pokud tato skutečnost není známa výrobci, jedná ze o tzv. zero-day zranitelnost.[27] Známé zranitelnosti jsou obvykle publikovány veřejnosti formou katalogu, např. CVE List, spravovaný organizací MITRE, obsahuje seznam zranitelností zveřejněných organizacemi po celém světě, které spolupracují s CVE. [28] Běžná zranitelnost v zdravotnické infrastruktuře je zastaralý software, který sám o sobě nemůže ohrozit bezpečnost informací, ale chyby v něm mohou být využity jako vektor útoku potencionálním útočníkem. S definicí zranitelnosti se můžeme setkat i v ZoKB, který jej definuje jako slabé místo aktiva, které může být zneužito hrozbou.[16]

6.1.3 Hrozba

Hrozba je potenciální příčina, nebo okolnost vedoucí k nežádoucí události, která může ohrozit aktiva a jejich uživatele využitím zranitelnosti.[26] Hrozby nelze zcela odstranit, ale je možné snížit pravděpodobnost jejich výskytu nebo omezit její dopad. Stejně jako zranitelnosti existují hrozby úmyslné (např. útok využitím zranitelnosti), nebo neúmyslné(např. přírodní katastrofy nebo nedbalost zaměstnanců).[29] ZoKB definuje hrozbu podobně, jako jiné zdroje. Dále bychom v legislativě našli i pojem významná hrozba, což je pojem, se kterým zákon pracuje i v souvisejících vyhláškách; jedná se o hrozbu, jejíž potenciál může závažně ovlivnit aktiva poskytovatele regulované služby a tím způsobit značnou újmu.[16] Největší hrozbou pro zdravotnictví je v současné době phishing.[30]
Příklady realizace hrozeb na CIA:

- **Důvěrnost** – Krádeže přístupových údajů nebo klíčů
- **Integrita** – Modifikace dat např. v databázi
- **Dostupnost** – DoS a DDoS útoky, výpadky proudu

[4]

6.1.4 Riziko

Riziko je pravděpodobnost, s jakou hrozba způsobí škodu organizaci využitím zranitelnosti aktiva.[26] Pro výpočet rizika můžeme využít rovnici, kterou publikoval NÚKIB[31]:

$$\textbf{Riziko} = Dopad \times Hrozba \times Zranitelnost$$

Rovnic existuje celá řada, od jednoduchých součinů až po složité matematické modely, záleží na organizaci, jakou metodu vyhodnocení rizik si zvolí, záleží na opakovatelnosti a přesnosti výpočtu. [29]

6.1.5 Analýza rizik

Analýza rizik je proces identifikace rizika a stanovení jeho úrovně.[26] Poskytovatel služby spadající do režimu vyšších povinností je povinnen provádět hodnocení rizik alespoň jednou ročně a zohlednit hrozby, zranitelnosti, předešlé KBI a možné dopady na aktiva.[20]Cílem analýzy je tedy zmapování rizik v organizaci, a to na základě stanoveného postupu, aby nedošlo k nahodilému hodnocení rizik. Po zmapování rizik by měla organizace rozhodnout, jak bude na jednotlivá rizika reagovat; pokud je riziko malé, nebo jeho mitigace je příliš drahá, může být rozhodnuto o jeho akceptování. Riziko lze snížit přijetím technických, nebo organizačních bezpečnostních opatřeních, nebo se mu lze vyhnout odstraněním činnosti, které se riziko dotýká.[6][29]

6.2 Hrozby a zranitelnosti ve zdravotnictví

Zdravotnictví patří mezi nejvíce lukrativní cíle kybernetických útoků, protože shromažďují velké objemy citlivých dat a jakožto poskytovatelé základní služby jsou subjektem kritické infrastruktury. Útočníci cílí na zdravotnické instituce, protože očekávají vyšší pravděpodobnost zaplacení výkupného v případě úspěšného útoku, neboť pro instituci je důležitější zdraví pacientů a rychlá obnova běžného provozu. Rychlá digitální transformace zdravotnického sektoru, mimo jiných zaváděním cloudových úložišť a technologií využívajících umělou inteligenci, dále rozšiřuje zranitelnosti a umožňuje nové vektory útoku.[32]

6.3 Kybernetické hrozby ve zdravotnictví

6.3.1 Phishing

Phishing (volně přeloženo jako „rybaření“) je podvodná technika usilující o odcizení digitální identity uživatele, přihlašovacích údajů, čísel bankovních karet a dalších využitelných dat za účelem jejich zneužití. Phishingové zprávy se nejčastěji šíří e-mailem, obvykle se jedná o podvržené zprávy vydávající se za legitimní. Příkladem phishingu je dotaz od napodobeniny legitimní banky, jejíž služeb příjemce využívá, o číslo účtu nebo

přístupový kód. Podvrženou stránku obvykle nelze rozeznat od legitimní, pokud příjemce neověří pravost webové stránky, a data odešle útočníkovi, phishing byl úspěšný a útočník získá data.[26] Ve zdravotnickém prostředí se phishing nejčastěji šíří prostřednictvím e-mailové komunikace, a to až v 63% případů, s cílem odcizení zdravotnických dat nebo získání přístupových dat.[30]

6.3.2 Ransomware

Ransomware je typ malware, který při instalaci zašifruje data na cílovém zařízení a pomocí kterého útočník požaduje výkupné výměnou za klíč, který data dešifruje. Uživatel bez tohoto klíče nemůže přistupovat k datům na infikovaném zařízení a obvykle samotné zařízení je nepoužitelné. Ransomwarový útok na zdravotnické zařízení může takto ohrozit data nebo zdraví pacientů.[33]

6.3.3 Kompromitace zdravotnických zařízení

Digitalizace lékařských záznamů a propojení datových toků mezi IoMT umožňuje real-time integraci dat a dálkovou péči o pacienty. Nicméně s tímto pokrokem přichází i nové vektory útoku skrz zdravotnická zařízení prostřednictvím zastaralého software, nebo chybějícího šifrování dat. Využitím zranitelnosti zastaralého software bez bezpečnostních záplat lze útočník buď přímo, nebo pomocí phishingu, získat přístup k digitalizovaným zdravotnickým datům a tím porušit důvěrnost dat. Dále může útočník porušit inegritu dat úmyslným tamperingem dat, které mohou vést v případě nesprávné diagnózy k ohrožení zdraví pacientů. [30]

6.3.4 Útok skrz dodavatele

Útok skrz dodavatele (tzv. Supply chain attack) spočívá ve vyhledání zranitelností v dodavatelském řetězci, pomocí kterého útočník cílí na hlavní organizaci spolupracující s dodavatelem. Příkladem je odběr software of dodavatele třetí strany, kterému organizace jako odběratel důvěřuje. Útočník vloží do software třetí strany škodlivý kód. Pokud se dodavatel o této změně kódu nedozví, a distibuuje jej odběratelům, útočník získá možnost útočit na vícero odběratelů zároveň. Obvyklým cílem tohoto útoku je právě zdravotnická dokumentace, kterou nemocnice sdílejí se svými externími dodavateli, jako jsou okresní kliniky, nebo skrz internetovou komunikaci formou telemedicíny.[34]

6.4 Kybernetické zranitelnosti ve zdravotnictví

6.4.1 Zastaralý software

Ve zdravotnických zařízeních zůstávají v provozu velké množství IoMT se zastaralými, již nepodporovanými operačními systémy, na které již nejsou vydávány žádné bezpečnostní záplaty. Vysoká cena zdravotnických přístrojů – jako jsou rentgeny, CT, nebo ultrazvuky – neumožňuje jejich častou výměnu, proto zůstávají v provozu i přes jejich nezáplatovaný operační systém (např. Windows XP).[33]

6.4.2 Nedostatečné školení zaměstnanců nemocnice

Zaměstnanci nemocničního zařízení, kteří nejsou seznámeni s bezpečnostní politikou nemocnice, a nezodpovědně zacházejí s přihlašovacími údaji (např. používáním hesla v Active Directory, které bylo v minulosti odcizeno na jiném účtu mimo nemocniční síť, nebo je na seznamu nejvíce používaných hesel), připojují do nemocniční sítě vlastní zařízení nebo přenosná média, nebo otevírají potenciálně nebezpečné přílohy e-mailu, jsou možné vektory útoku, pomocí kterých může útočník odcizit přihlašovací údaje, a získat tak přístup ke zdravotnické dokumentaci v nemocniční síti. [33]

6.4.3 Vzdálený přístup

Zaměstnanci přistupující k datům v nemocniční síti vzdáleně přes veřejné, nebo domácí síť, otevírají nové možnosti odcizení přihlašovacích údajů odesílaných přes nešifrovanou komunikaci. Útočník může odposlouchávat komunikaci sniffingem a tím získat nezašifrované přihlašovací údaje. Velké množství kybernetických útoků v roce 2020 bylo zaviněno právě nedostatečným zabezpečením externích internetových sítí. [33]

7 Kybernetická bezpečnostní událost a incident

Kybernetická bezpečnostní událost (KBU), která byla vyhodnocena jako stav narušující prvky důvěrnosti, dostupnosti a integrity, se považuje za Kybernetický bezpečnostní incident (KBI) s pravděpodobným negativním dopadem. KBI může ohrozit buď fungování celých států, proto je na jeho zvládnutí potřeba koordinovat několik různých bezpečnostních týmů a vynaložit značné prostředky, v případě lokálních dopadů na organizaci nebo její části jde o v porovnání relativně jednoduchou a nenákladnou mitigaci. V praxi se objevuje několik možných definicí KBU a KBI v závislosti na standardu, který jej definuje.[6]

7.1 Definice KBU

Norma ISO/IEC 27001 definuje KBU jako jakýkoliv zjištěný stav systému, služby, nebo sítě, poukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Také se může jednat o jinou, předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací. [35] Příručka NIST 800-61 definuje *událost* jako jakoukoliv pozorovatelnou situaci v systému, nebo síti. Kromě této velmi obecné definice, která zahrnuje i události bez negativního dopadu, definuje standard i pojem *nepříznivá událost*, která se vztahuje pouze na události charakteru bezpečnosti informací, nikoliv technické, nebo přírodní. [27] KBU právně definuje ZoKB definuje KBU pouze jako událost, která může vyústit v KBI. [16]

Obecně tedy z definic vyplývá, že KBU je stav bez zatím negativního dopadu, ovšem s potenciálem narušení bezpečnosti informací organizace. Ve zdravotnickém prostředí bychom mohli jako událost charakterizovat phishingovou e-mailovou zprávu určenou zaměstnanci nemocnice, která nebyla dosud otevřena. V tomto případě e-mailová zpráva sama o sobě nenarušuje bezpečnost, ale v případě otevření by k narušení mohlo dojít, a událost by vyústila v KBI.

7.2 Definice KBI

Stejně jako KBU definuje norma ISO/IEC 27001 také Kybernetický bezpečnostní incident (KBI), a to jako nechtěnou, nebo neočekávanou KBU, u které existuje vysoká pravděpodobnost kompromitace organizace a ohrožení bezpečnosti informací. [35] Velmi podobnou definici KBI bychom našli i v příručce NIST 800-61, která uvádí, že se

jedná o porušení, nebo bezprostřední hrozbu porušení bezpečnostních politik nebo standardních bezpečnostních praktik. [27] ZoKB pohlíží na KBI obecně jako na narušení bezpečnosti informací v kyberprostoru. [16]

Tyto definice se shodují, že KBI je původně událost, narušující bezpečnostní politiku organizace, a mající pravděpodobně negativní dopad na bezpečnost informací.

7.3 Taxonomie incidentů

Při návrhu a implementaci efektivního systému ochrany je třeba porozumět, jaké existují hrozby organizace a jakým způsobem jsou realizovány. Vzhledem k tomu, že v kyberprostoru bychom našli velké množství různých útoků, v praxi se uplatňuje několik klasifikací a taxonomií incidentů. Tyto taxonomie slouží k efektivní přípravě na útoky a incidenty a standardizaci reakce na určitý typ incidentu, sdílení informací o incidentu mezi externími CSIRT týmy organizace nebo v rámci bezpečnostní komunity. Využití taxonomie mimo jiné umožňuje i sledování trendů, pomocí kterých lze určit, které bezpečnostní aspekty je třeba posilovat. V oblasti taxonomie incidentů existuje hned několik dokumentů, standardů, a praktik. Taxonomie se obecně dělí do dvou základních skupin v závislosti na typu hrozby, tedy vektoru útoku, a typu dopadu incidentu. V praxi jsou pak častější taxonomie založené na typu hrozby, jelikož cílem procesu incident managementu je minimalizace počtu incidentů, je lepší se zaměřit na odstranění příčin incidentů – hrozeb.[6]

7.3.1 Taxonomie podle normy ČSN ISO/IEC 27035-2:2018

Norma ISO 27035 žádné klasifikační schéma incidentu neuvádí, pouze uvádí příklad klasifikačního schématu kategorie incidentu podle hrozeb ve formátu: kategorie hrozby, popis hrozby a jednotlivé příklady.

Kategorie	**Popis**	**Příklad**
Incident technického selhání	Ztráta bezpečnosti informací je způsobena chybami v informačních systémech, jejichž výsledkem je nedostupnost nebo zničení informačních systémů	Selhání hardware, software, zanedbání údržby.

Tabulka 5: Příklad kategorie incidentů bezpečnosti informací podle hrozeb

7.3.2 Taxonomie podle NIST 800-30

NIST je americká standardizační společnost, která mimo jiné vydala dokument NIST 800-30 [9], obsahující taxonomii posuzování rizik a klasifikační schéma založené na hrozbách. V dokumentaci NIST 800-30 je uvedena tabulka:

Typ zdroje hrozby	**Popis**	**Charakteristika**
ÚMYSLNÉ • Jednotlivec • Externí osoba • Interní osoba • Důvěryhodný interní pracovník • Privilegovaný interní pracovník • Skupina • Ad hoc • Zavedená • Organizace • Konkurent • Dodavatel • Partner • Zákazník • Stát	Jednotlivci, skupiny, organizace nebo státy, které se snaží zneužít závislost organizace na kybernetických zdrojích (tj. informace v elektronické podobě, informační a komunikační technologie a schopnosti zpracování a přenosu informací, které tyto technologie poskytují).	Schopnosti, záměr, cílení
NÁHODNÉ • Uživatel • Privilegovaný uživatel / administrátor	Chybné činnosti prováděné jednotlivci při plnění jejich každodenních pracovních povinností.	Rozsah dopadů

[9] Guide for Conducting Risk Assesments

Typ zdroje hrozby	Popis	Charakteristika
STRUKTURÁLNÍ • IT vybavení • Úložiště • Zpracování dat • Komunikace • Zobrazovací zařízení • Senzor • Řadič • Řízení prostředí • Regulace teploty/vlhkosti • Napájení • Software • Operační systém • Síťové prvky • Obecné aplikace • Aplikace specifické pro danou misi	Selhání zařízení, řízení prostředí nebo softwaru v důsledku stárnutí, vyčerpání zdrojů nebo jiných okolností, které překračují očekávané provozní parametry.	Rozsah dopadů
ENVIRONMENTÁLNÍ • Přírodní nebo člověkem způsobená katastrofa • Požár • Povodeň / tsunami • Vichřice / tornádo • Hurikán • Zemětřesení • Bombový útok • Překonání/obsazení (např. útokem) • Neobvyklý přírodní jev (např. sluneční skvrny) • Selhání infrastruktury / výpadek • Telekomunikace • Elektrická energie	Přírodní katastrofy a selhání kritické infrastruktury, na které je organizace závislá, ale které jsou mimo její kontrolu.	Rozsah dopadů

Tabulka 6: Taxonomie zdrojů hrozeb podle NIST 800-30

[36] Z tabulky je evidentní, že klasifikační rámec NIST je triviální a zastaralý, protože neobsahuje žádné aktuální hrozby související s moderními technologiemi. [6]

7.3.3 Taxonomie podle ENISA

ENISA je agentura EU koordinující aktivity národních týmů CERT/CSIRT členských zemí EU. ENISA rovněž zpracovala vlastní rámec pro klasifikaci bezpečnostních in-

cidentů, vycházející z podstatě incidentu jako takového, založeném na zkušenostech provozu CERT/CSIRT týmů.[6]

Klasifikace incidentu	**Příklad**	**Popis**
Škodlivý kód	Virus Červ Trojský kůň Spyware Dialer Rootkit	Různé druhy software záměrně vložené do informačnícho systému s cílem způsobení škody nebo narušení bezpečnosti informací.

Tabulka 7: Příklad kategorie incidentů bezpečnosti informací podle hrozeb dle ENISA

7.3.4 Taxonomie podle MITRE ATT&CK

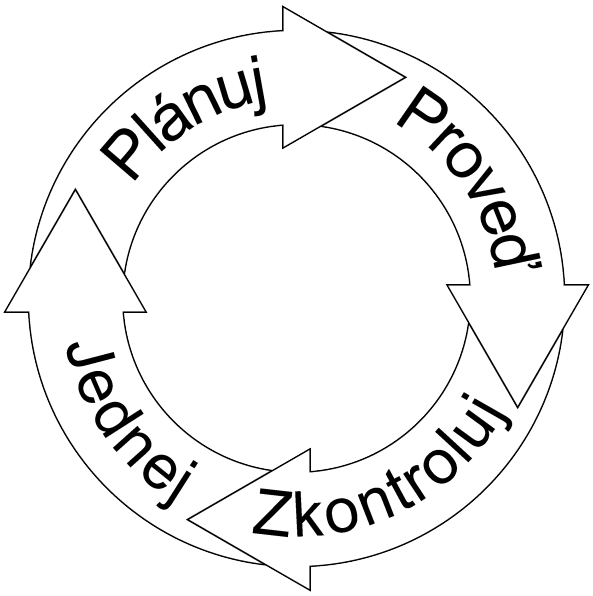
MITRE je americká nezisková organizace provádějící výzkum mimo jiných v oblasti kybernetické bezpečnosti. MITRE ATT&CK je celosvětově volně dostupná databáze vektorů útoků, hrozeb, zranitelností a technik pro mitigaci hrozeb vycházející ze skutečných scénářů. MITRE ATT&CK je definuje tři hlavní matice: Podnikovou(Enterprise), Mobilní(Mobile), a ICS. Každá matice obsahuje seznam taktik, které by mohl útočník potenciálně využít, tyto taktiky pak obsahují vektory útoku mající společný cíl. Nejedná se tedy o taxonomii podle vektoru útoku, nýbrž podle cíle útočníka. [6]

8 Řízení kybernetických incidentů

Řízení incidentů je proces zavedených postupů, které mají plánovat, detekovat, zaznamenat, posoudit, reagovat a vyhodnotit všechny kybernetické bezpečnostní události a incidenty. ZoKB přímo vyžaduje zvládání kybernetických bezpečnostních událostí a incidentů jakožto organizační opatření, které definuje jako: „*úkony vedoucí k prevenci, detekci, analýze, omezení dopadů incidentu, reakci na incident a následné obnově*“ a detekci kybernetických bezpečnostních událostí jakožto technické opatření regulované služby v režimu vyšších povinností. ZoKB neuvádí konkrétní normy, nebo postupy, ani návod na implementaci řízení KBI, proto existuje několik standardů a norem běžně používaných v praxi, podle kterých společnost vytvoří a implmementuje proces odpovídající jejich potřebám a prostředkům.[16]

8.1 PDCA Cyklus

Řízení KBI není statická šablona, je to opakující se proces, který by měl reagovat na změny v organizaci, nové hrozby nebo zranitelnosti, a nové poznatky a zkušenosti z provozu. Jednoduchým základem pro řešení událostí a incidentů je Demingův PDCA cyklus, který rozděluje proces do čtyř fází:[37]



Obrázek 3: PDCA Cyklus [10]

[10] Vlastní tvorba

8.2 Životní cyklus incidentu ve zdravotnictví

Univerzální podoba procesu řízení KBI, uplatnitelná v jakékoliv organizaci s maximální efektivitou, neexistuje. Níže je uveden možný návrh životního cyklu KBI, se kterým se pracuje v praktické části této práce. Celý tento proces rámcově vychází z norem běžně používaných v praxi: ČSN ISO/IEC 27035-2:2018, NIST SP.800-61, proces řízení ENISA a best-practices organizací zabývajících se kybernetickou bezpečností.

8.2.1 Příprava na incident

První fáze zahrnuje plánování a přípravu nutnou k úspěšnému zavedení procesu řízení KBI. Poskytovatel by měl nejdříve vypracovat politiku řízení KBI, která by měla obsahovat mimo jiné účel politiky, jejího vlastníka, proces řízení KBI, popis incidentů, proces jejich hlášení, definici rolí a požadavek na školení a vytváření povědomí o řízení KBI v organizaci. Dále je potřeba sestavit CSIRT tým zodpovědný za řešení KBI, který bude posuzovat události, vyhodnocovat, zda se jedná o KBI, koordinovat a řídit reakci na KBI, a využívat znalosti získané při řešení incidentu. Kromě vlastního CSIRT může poskytovatel využívat spolupráci s externími organizacemi; CSIRT týmy významných dodavatelů, nebo vládních organizací. V České republice je za pomoc při reakci na KBI při ochraně regulovaných služeb podle ZoKB zodpovědný vládní CERT GovCERT.cz. Nakonec se vytvoří systém školení a vytváření bezpečnostního povědomí o řízení KBI. Každý zaměstnanec musí znát svoji roli, správný postup a jaké kroky podniknout při identifikaci KBU. Tento proces je třeba pravidelně testovat a aktualizovat podle potřeby, aby byl i nadále plně funkční.[38][39]

8.2.2 Detekce a analýza incidentu

Druhá fáze se zabývá analýzou provozu v organizaci poskytovatele a detekcí KBU a identifikaci zranitelností. Klíčový je pro tuto fázi monitoring (např. pomocí SIEM) a logování komunikace v systémech a síti organizace. Pro zvýšení efektivity detekce je vhodné doplnit z externích zdrojů informace o nových metodách útoku, zjištěných zranitelnostech, nebo strategiích pro zmírnění dopadů kybernetických útoků. Norma ČSN/ISO 27035-2:2018 doporučuje evidovat výstupy z monitoringu do logů, které umožňují jejich zpětnou analýzu a posouzení.[38][39]

8.2.3 Klasifikace incidentu

Třetí fází je posouzení, na základě informací získaných v předchozí fázi, zda událost splňuje podmínky pro klasifikaci jako KBI, a rozhodnutí o tom, jestli zaznamenanou událost můžeme klasifikovat jako KBI. Pokud je u události vyhodnocen pravděpodobný negativní dopad na aktiva, vyhodnotí se jako KBI, a pokud splňuje podmínky vymezené ZoKB, poskytovatel je povinnen jej hlásit na NÚKIB. Vyhodnocují se důsledky, závažnost, a dopady na poskytování regulované služby. Pokud je identifikován KBI s dopadem na osobní údaje, je třeba postupovat v souladu s kritérii GDPR. KBI je v praxi klasifikován podle jednoho z klasifikačních schémat – taxonomií. Při posuzování KBI je třeba vycházet z již stanoveného plánu řešení incidentů, zdokumentovaného v interní dokumentaci poskytovatele; rozdělení odpovědností při posuzování informací a při rozhodování, a formálních postupů při hlášení po rozhodnutí o klasifikaci události jako KBI. Veškeré činnosti související s klasifikací je vhodné řádně logovat pro účely zpětné analýzy; po detailním přezkoumání KBI se může stát, že se jednalo o false-positive, které může sloužit jako ukazatel kvality systému – čím méně false positives, tím vyšší kvalita detekce.[38]

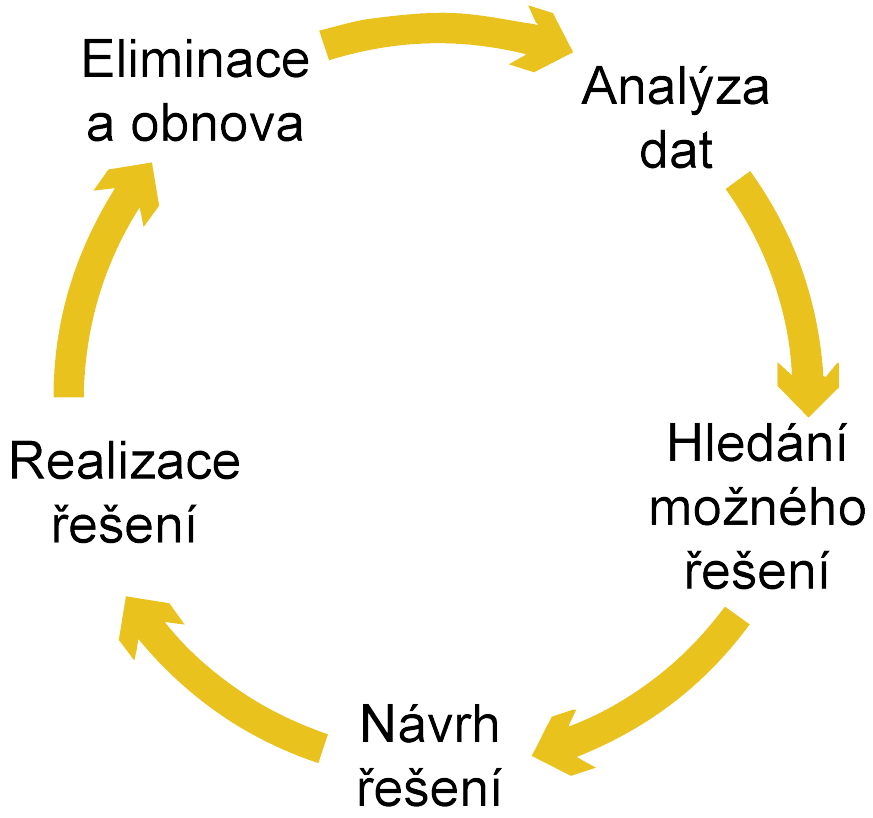
8.2.4 Prioritizace incidentu

Čtvrtou fází je určení priority KBI v závislosti na vyhodnoceném dopadu na aktiva poskytovatele a počtu dotčených pacientů. Podle definovaných matic vycházejících z předchozích KBI v interní dokumentaci se určí závažnost a relativní priorita. Smyslem prioritizace je alokace zdrojů incidentům s vyšší prioritou místo jejich chronologického zvládání.[38]

8.2.5 Odezva na incident

Pátou fází je samotné řešení KBI, kdy CSIRT tým podniká kroky procesu odezvy na incident. ENISA doporučuje ve svém dokumentu řízení incidentů postupovat podle cyklu řešení incidentu. [40] Při řešení KBI může tým přehodnotit jeho závážnost v rámci klasifikační matice, a podle toho vyhodnotit, zda je řešení KBI v rámci schopností týmu uvést jej pod kontrolou a jestli se jeho dopady dále nešíří. Pokud se však ukáže, že je dopad ve skutečnosti závažnější, než se předpokládalo, měl by být spuštěn proces krizového řízení a KBI eskalován. Eskalace je proces delegace řízení KBI na externí CSIRT tým, kterému jsou poskytnuty všechny logované informace o KBI, po-

kud externí CSIRT nezíská kontrolu nad KBI, je eskalován dále, např. spoluprací s Národním CERT.[38]



Obrázek 4: Cyklus odezvy na incident podle ENISA [11]

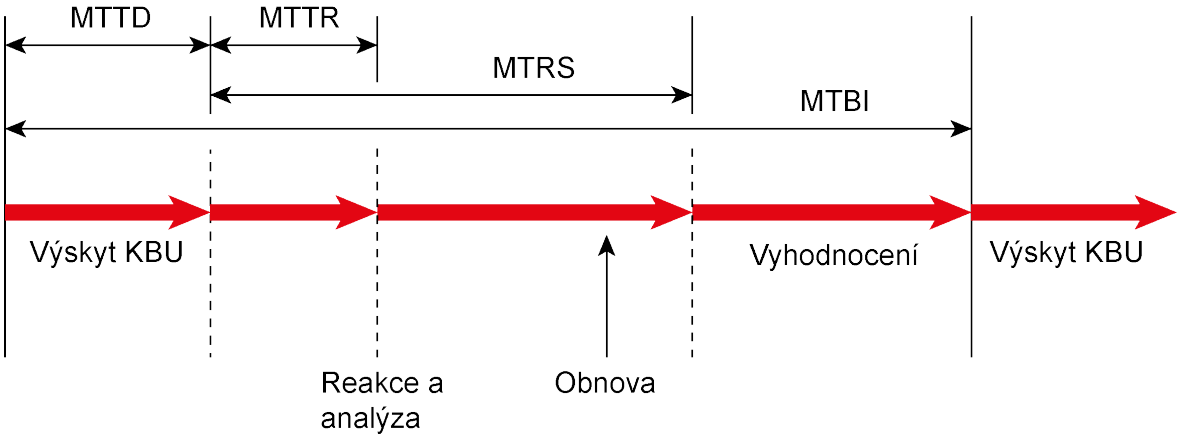
O průběhu řešení KBI je třeba informovat všechny zainsteresované stakeholdery: garanty a uživatele aktiv, vedení nemocnice a externí dodavatele. Pokud se KBI podaří zvládnout, stakeholders by měli být o této skutečnosti informováni. Průběh je také třeba podle ZoKB hlásit NÚKIB průběžnými zprávami, dokud není KBI vyřešen.[24]

8.2.6 Vyhodnocení incidentu

Na konci životního cyklu KBI se analyzuje postup řešení za účelem zlepšení procesu řízení KBI, a s ním sovisející procesy, jako je řízení rizik. Při analýze dat jednotlivých fází procesu řízení KBI se hledají trendy a vzory, podle kterých mohou být přijata preventivní opatření, která mají snížit riziko vzniku budoucích incidentů. Řízení KBI tak může odhalit slabá místa v zabezpečení nemocničního provozu, jako jsou nevyhovující parametry technických prostředků (např. firewall politiky), vadný software externího dodavatele, nebo politika řízení rizik. Nemocnice může v závislosti na této analýze

[11] Upraveno podle *Good Practice Guide for Incident Management*

podniknout kroky ke zlepšení kybernetické bezpečnosti, a to buď jako dlouhodobou strategii, která nemůže být ihned realizována, nebo ihned přijmout a implementovat konkrétní bezpečnostní opatření. Norma ČSN/ISO 27035-1:2018 také doporučuje zhodnotit efektivitu svého CSIRT týmu při řízení KBI. Veškeré informace o průběhu řešení KBI, změnách v dokumentaci, pravidlech nebo implementace kybernetické bezpečnosti je třeba zalogovat a uchovat v interním archivu pro účely další zpětné analýzy.[38]



Obrázek 5: Metrika řízení KBI [12]

Popis	Doba trvání
Doba mezi útokem a detekcí KBI (MTTD)	10 minut
Doba mezi detekcí a reakcí na KBI (MTTR)	20 minut
Doba mezi reakcí a vyhodnocením (MTRS)	30 minut
Doba mezi KBI (MTBI)	Stabilní trend

Tabulka 8: Metrika řízení významného KBI

[12] Vlastní tvorba podle [6]

8.3 Eskalační politika

Jak už bylo zmíněno, eskalace procesu je delegace řízení KBI na jinou osobu, nebo tým. Aby bylo jasné kdy, komu a jakým způsobem incident eskalovat, je třeba určit eskalační politiku. Může se stát, že první respondent KBI (např. manažer kybernetické bezpečnosti) nebude schopen vlastními silami KBI vyřešit, proto musí být jasně stanoveno, jakým způsobem předat řízení a shromážděné informace o incidentu jinému subjektu, a to v závislosti na závažnosti incidentu, nbo pokud je cílový čas vyřešení incidentu překročen.[41]

9 Praktická část

V praktické části se zaměříme na návrh procesu řízení KBI a jeho praktické využití při modelové situaci kybernetického útoku, jehož cílem je modelová zdravotnická organizace, ve které byla definovaná aktiva, bezpečnostní role a související odpovědnosti při řízení KBI, jednotlivé fáze samotného řízení a diagram samotného procesu. Při řízení KBI se obvykle postupuje podle playbooku v závislosti na druhu incidentu, v této ukázce jako playbook poslouží příloha č.3 knihy *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*

9.1 Modelová organizace

Subjektem, kterým bude modelová organizace praktické implementace řízení incidentů, je oblastní nemocniční zařízení s 1800 zaměstnanci, poskytující zdravotní služby podle zákona č. 372/2011 Sb., o zdravotních službách. Tato nemocnice je regulovaný subjekt spadající do režimu vyšších povinností podle VoRS, protože se jedná o velký podnik. Velkým podnikem se pak rozumí společnost s více než 250 zaměstnanci.[15]
Nemocnice disponuje technickými prostředky nezbytnými pro poskytování zdravotní péče, u kterých je nutné zajistit nepřetržitý provoz. Veškerá data jsou ukládána v datovém centru nemocnice v segmentované síti, do které mají přístup pouze zaměstnanci jak lokálně, tak vzdáleně. NIS je hlavní repozitář zdravotních karet pacientů, u kterých eviduje zdravotní stav, předepsané léky a osobní údaje, jako jsou rodná čísla. Zaměstnanci nemocnice se autentizují v nemocniční síti pomocí Active Directory, přes který mají přístup do NIS. Bezpečnostním pravidlem v nemocnici v zájmu dodržení ochrany osobních údajů je, že nahlížet do a upravovat záznamy pacienta v NIS může provádět pouze jeho vyšetřující lékař, a nikdo jiný. Dále nemocnice spravuje vlastní poštovní server s e-mailovými účty propojenými s Active Directory. Data jsou zálohována do lokálního zálohovacího úložiště, aby byla přístupná i v případě výpadku internetového provozu.

9.2 Bezpečnostní role a odpovědnosti

Před zvládáním KBI je nutné jednoznačně určit, kdo má při řízení jaké odpovědnosti, práva a povinnosti. Smyslem je jednoznačné a efektivní rozdělení zodpovědností pří řízení za účelem efektivního a správného vykonání procesu řízení KBI. Vzhledem k

tomu, ze subjekt je nemocniční zařízení v režimu vyšších povinností, je třeba myslet na právní požadavky pro stanovení rolí v ZoKB a VoBOvRVP. V této modelové organizaci jsou všechny osoby, jímž byly role přiděleny, zároveň zaměstnanci nemocnice. Při vypracování procesu řízení KBI byly identifikovány níže uvedené role:

9.2.1 Vedení nemocnice

Vedení nemocnice je v rámci kybernetické bezpečnosti zodpovědné za stanovení celkové strategie řízení KBI, dále určí zdroje a rozpočet. Při řízení KBI je v kontaktu s podřízenými rolemi a rozhoduje o zahájení krizového řízení.

9.2.2 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti (MKB) je zodpovědný za celý proces řízení KBI. Vyhodnocuje informace poskytnuté o detekované události, určí členy interního CSIRT týmu, dále podle významnosti KBI jej eskaluje, a koordinuje odezvu a vyhodnocení KBI. V případě potřeby informuje NÚKIB a podává průběžné zprávy o zvládání KBI. Pokud manažer usoudí podle závažnosti KBI potřebu sestavit CSIRT tým, jeho zodpovědnosti rozdělí mezi členy týmu.

9.2.3 Bezpečnostní analytik

Bezpečnostní analytik je zodpovědný za monitoring provozu v síti, analýzu detekovaných hrozeb a událostí, jejich dopadu, původu a metodu útoku. V případě detekce události analytik hledá zranitelnost, která byla pravděpodobně využita. Při řízení KBI je zodpovědný za posouzení a klasifikaci události. Pří řízení KBI je zodpovědný za detekci, analýzu, prioritizaci a následné vyhodnocení KBI.

9.2.4 Správce sítě

Správce sítě je zodpovědný za bezpečnost síťového provozu v nemocnici, segmentaci sítě a provoz interní komunikace. Při řízení KBI je odpovědný za potřebné změny v přístupu, izolaci síťového segmentu, nebo blokování přístupu do interní sítě z internetu.

9.2.5 Správce IT systémů

Správce IT systému zodpovídá za správu a provoz Active Directory, NIS, e-mailové služby a systému zálohování. Při řízení KBI je odpovědný za omezení přístupu do těchto

systému, vynucování změny hesel nebo blokace kompromitovaných zaměstnaneckých účtů.

9.2.6 CSIRT

Interní CSIRT je skupina osob zodpovědná za řízení KBI, kterou svolává manažer kybernetické bezpečnosti v závislosti na závažnosti a rozsahu KBI. CSIRT spolupracuje s manažerem při analýze, klasifikaci, prioritizaci, eskalaci, řešení a vyhodnocení KBI. Členové týmu mají specifické zodpovědnosti související s řízením KBI. Mezi členy CSIRT patří:

- **Velitel týmu** – zodpovědný za koordinaci aktivit týmu a komunikaci s vedením nemocnice, tuto pozici obvykle zastává manažer kybernetické bezpečnosti
- **Bezpečnostní analytik** – zodpovědný za přijmutí, posouzení a klasifikaci události
- **Správce sítě** – zodpovědný za správu nemocniční sítě
- **Správce IT systémů** – zodpovědný za správu a přistup k IT systémům
- **Právní konzultant** – zodpovědný za konzultaci v oblasti plnění právních povinností souvisejících s řízením KBI
- **Pověřenec pro ochranu osobních údajů** – zodpovědný za konzultaci v oblasti ochrany osobních údajů a hlášení na ÚOOÚ
- **PR manažer** – zodpovědný za komunikaci o KBI s veřejností

9.2.7 Krizový tým

Krizový tým je svolán vedením nemocnice při zahájení krizového řízení v případě závažného KBI. Členy krizového týmu jsou všichni členové interního CSIRT týmu společně s dalšími odborníky, které určí manažer kybernetické bezpečnosti.

9.2.8 Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti jako jediný z jmenovaných rolí není zaměstnancem nemocnice, jedná ze o stranově nezúčastněného odborníka v oblasti kybernetické bezpečnosti, který provádí v nemocnici bezpečnostní audit. Při řízení KBI poskytuje nezaujatou zpětnou vazbu na navrhované změny v oblasti řízení KBI.

9.3 Aktiva organizace

V modelové organizaci byla identifikována tato primární a podpůrná aktiva, u kterých se dále určí hodnocení jejich kritičnosti a garanti aktiv, a to podle dopadu narušení jejich důvěrnosti, integrity, nebo dostupnosti.

Aktivum	**Hodnocení**
Poskytování zdravotní péče	Kritická
Zdravotnická dokumentace	Kritická
Osobní údaje pacientů	Kritická
Provozní data	Vysoká

Tabulka 9: Primární aktiva nemocnice

Aktivum	**Skupina**
Klinické IoMT	Hardware
Periferní zařízení	Hardware
Síťové prvky	Hardware
NIS	Software
Provozní software	Software
Active Directory	Software
E-mailový systém	Software
Systém zálohování dat	Software
Zdravotnický personál	Zaměstnanci
IT personál	Zaměstnanci

Tabulka 10: Podpůrná aktiva nemocnice

9.4 Proces řízení incidentů

Cílem návrhu procesu řízení KBI je standardizace postupů a aktivit vykonaných v souvislosti se zvládáním KBI. Jedná se o vyvíjející se proces, který je po každém provedení zhodnocen a podle nalezených nedostatků upravován.
Seznam aktivit při řízení KBI vypadá takto:

Detekce

SIEM loguje veškerý provoz v nemocnici, logy analyzuje bezpečnostní analytik. Pokud je při logování vyhodnocena anomálie, analytik ji vyhodnotí a posoudí, zda by se mohlo jednat o potenciálně nežádoucí událost.

Posouzení události

Pokud analytik vyhodnotí neobvyklý provoz v síti jako KBU, informuje o této skutečnosti manažera kybernetické bezpečnosti, a pokud zjistí, že událost byla naplněna a bude mít negativní dopad, vyhodnotí ji jako KBI, poté určí pravděpodobný vektor útoku a velikost dopadu. Manažer kybernetické bezpečnosti o situaci informuje vedení nemocnice a pozastaví zálohování dat v NIS.

Klasifikace a prioritizace

Podle odhadovaného dopadu bezpečnostní analytik určí, zda se jedná o KBU, nebo KBI, klasifikuje incident a prioritizací určí cílovou odezvu. Pokud je při klasifikaci KBI vyhodnocen jako závažný, manažer kybernetické bezpečnosti odešle prvotní hlášení o incidentu na NÚKIB a pokud se zjistí pravděpodobný únik osobních dat, pověřenec pro ochranu osobních údajů ohlásí případ porušení zabezpečení osobních údajů podle GDPR na ÚOOÚ.

Posouzení schopnosti zvládnout KBI

Manažer kybernetické bezpečnosti posoudí, zda podnikne kroky k vyřešení KBI sám, svolá interní CSIRT tým, nebo řízení eskaluje a sestaví krizový tým.

Návrh a řešení KBI

Řešitel KBI navrhne kroky pro vyřešení incidentu, které jsou poté realizovány. Pokud kroky neuvedou situaci pod kontrolu, manažer kybernetické bezpečnosti kontaktuje další strany, vypracuje a odešle průběžnou zprávu o řešení incidentu na NÚKIB.

Obnova po KBI

Pokud se podaří KBI dostat pod kontrolu, manažer kybernetické bezpečnosti obnoví zálohování dat a podle potřeby obnoví postižená data. O vyřešení KBI informuje všechny zainteresované stakeholdery, sepíše závěrečnou zprávu a odešle ji na NÚKIB.

Vyhodnocení KBI

Nakonec manažer kybernetické bezpečnosti na základě sesbíraných dat o KBI a průběhu jeho řízení vyhodnotí efektivitu řízení KBI.
Tyto aktivity jsou zakresleny v diagramu procesu uvedeného v příloze.

9.5 Řízení modelového KBI

V této modelové situaci se podíváme na scénář útoku na Nemocniční informační systém (NIS) a jeho zvládání pomocí navrhovaného procesu řízení KBI.

9.5.1 Vektor a cíle útoku

Nemocnice byla napadena útočníkem, při kterém byl jako vektor útoku identifikován cílený spear-phishingový útok prostřednictvím e-mailu na zaměstnance nemocnice. Obsahem e-mailu, jehož odesílatel se vydává za Ministerstvo zdravotnictví, je výzva k aktualizaci interní metodiky nemocnice. Cílem tohoto útoku je získání přístupových údajů do nemocniční sítě a následné spuštění ransomware v NIS.

9.5.2 Detekce a analýza

Zaměstnanec otevřel odkaz v e-mailu, který zobrazil imitaci dialogového okna k přihlášení, prostřednictvím kterého odeslal útočníkovi přihlašovací údaje do nemocniční domény. Při analýze útočníka můžeme získat informace o odesílateli, jako je jeho jméno v hlavičce e-mailu, IP a URL adresu serveru, a podíváme se, jestli jsou na seznamu škodlivých webových stránek. Dále je třeba zjistit, kolik zaměstnanců otevřelo falešné dialogové okno a kolik jich vyplnilo přihlašovací údaje. SIEM zaznamenal nové přihlášení do Active Directory z neznámé IP adresy minutu po kliknutí na odkaz s přihlašovacími údaji, které se shodují s údaji zaměstnance, který se pokusil o přihlášení na phishingový server.[6] Bezpečnostní analytik tuto situaci vyhodnotil jako potenciální KBU s podezřením na neoprávněné vniknutí do nemocniční sítě s možností ohrožení bezpečnosti

dat v NIS, a informuje o situaci manažera kybernetické bezpečnosti, který okamžitě pozastavuje zálohování NIS.

9.5.3 Klasifikace a prioritizace

Po zjištění události je třeba na základě shromážděných informací ze SIEM logů posoudit, zda se jedná o KBU, nebo KBI. Dále je incident klasifikován na základě vektoru útoku podle klasifikačního schématu a prioritizován na základě dopadu na nemocnici. V tomto případě byl vektor útoku identifikován jako phishing. Tuto klasifikaci může vyhodnotit automaticky SIEM, nebo bezpečnostní analytik, s cílem určení relevantních postupů při řešení KBI, např. podle playbooku. Manažer kybernetické bezpečnosti informuje vedení nemocnice o detekci KBI v nemocničním prostředí a situaci ohlásí na NÚKIB, a protože existuje podezření na možný únik dat, pověřenec pro ochranu osobních údajů ohlásí podle čl.33 GDPR porušení zabezpečení osobních údajů na Úřad pro ochranu osobních údajů (ÚOOÚ).[8]

Po klasifikaci incidentu určíme prioritu incidentu v závislosti na jeho předpokládaném dopadu a cílovou dobu jeho vyřešení podle metrik určených v interní dokumentaci. Informace uvedené v klasifikačním schématu si organizace zpracuje sama podle svých potřeb. V následujících tabulkách je uveden případ hodnocení dopadu a prioritizace:

	Nízký	Střední	Vysoký
Dopad na bezpečí pacienta	Mírné poškození vyžadující minimální intervenci	Střední poškození vedoucí k profesionální intervenci	Vážné poškození vedoucí k prodloužení závislosti nebo invaliditě
	Prodloužení hospitalizace o 1 až 3 dny	Prodloužení hospitalizace o 4 až 13 dní	Prodloužení hospitalizace o >2 týdny

Tabulka 11: Matice dopadu incidentu

		Dopad		
		Vysoký	Střední	Nízký
Závažnost	Vysoká	5	4	3
	Střední	4	3	2
	Nízká	3	2	1

Tabulka 12: Matice prioritizace incidentu

Priorita	Popis	Cílová doba odezvy	Cílová doba uvedení pod kontrolu
5	Kritická	Okamžitá	do 1 hodiny
4	Vysoká	do 10 minut	do 4 hodin
3	Střední	do 1 hodiny	do 8 hodin
2	Nízká	do 6 hodin	do 1 dne
1	Minimální	do 1 dne	do 1 týdne

Tabulka 13: Hodnocení priorit incidentu

Vzhledem k tomu, že spearphishingový útok pravděpodobně cílí na NIS, tedy primární aktivum *Zdravotní dokumentace*, u kterého byla hodnota vyhodnocena jako *kritická*, můžeme říct, že se jedná o závažný KBI s kritickým dopadem na aktivum a je proto nutné na něj reagovat okamžitě a uvést jej pod kontrolu do 1 hodiny. Zaměstnanci IT podnikají okamžité kroky k omezení šíření škod způsobených KBI; správce IT systémů pozastavuje provoz NIS, správce sítě jej izoluje od zbytku nemocniční sítě a manažer kybernetické bezpečnosti doporučí vedení nemocnice přechod do fyzického režimu vedení zdravotnických záznamů.

9.5.4 Odezva

Manažer kybernetické bezpečnosti podle míry závažnosti rozhoduje, jestli KBI uzavře, řeší sám, nebo svolá pro řešení CSIRT tým. Protože byl incident vyhodnocen jako závažný, a tedy se očekává, že jeho vyřešení je mimo síly interního CSIRT týmu, manažer eskaluje incident a sestaví krizový tým, který podniká okamžité kroky k řešení incidentu. Pokud se ukáže, že KBI stále není pod kontrolou, je eskalován dále.

Analýza dat

Krizový tým si vyžádá shromážděná data o incidentu, na základě kterých rozhodne o formě odezvy. Zároveň informuje uživatele dotčených aktiv o existenci KBI.

Hledání možného řešení

Po analýze shromážděných dat členové týmu navrhnou možná řešení KBI a v závislosti na závažnosti se dohodnou co nejrychleji na nejelpší odezvě v rámci možností.

Návrh řešení

Potom, co se krizový tým dohodne na řešení, připraví seznam kroků k mitigaci probíhajícího útoku. S těmito kroky poté obeznámí všechny zúčastněné strany (např. poskytovatele internetových služeb, po jehož síti útok proběhl). Pokud tým spolupracuje se zaměstnanci, kteří nemají odborné znalosti v oblasti kybernetické bezpečnosti, je důležité, aby byly kroky k mitigaci dostatečně srozumitelné.
Navržené kroky odezvy na incident mohou vypadat takto:

- Zablokování škodlivé domény nastavením firewall pravidla
- Zablokování všech dalších spear phishingových e-mailů, pokud bylo cílem více osob
- Vynucení změny přístupových údajů u postiženého zaměstnance
- Informování zaměstnanců o aktuální hrozbě spear phishingu

Cílem útočníka bylo nahrání ransomware do NIS a zašifrování dat v něm. Pokud se krizovému týmu podaří zablokovat komunikaci včas, nemusí dojít k naplnění cíle útoku, pokud by však k zašifrování NIS došlo, znamenalo by to kompletní dopad na důvěrnost, integritu a dostupnost dat tohoto aktiva. Při kompletním výpadku NIS systém nahrazují fyzické záznamy na papír, nebo telefonicky. V takovém případě by musel krizový tým podniknout další kroky pro zvládnutí KBI, jako je pozastavení zálohování NIS, aby k nim neměl útočník přístup, a po zamezení komunikace obnova dat z těchto záloh.

Realizace řešení

Po naplánování kroků odezvy krizový tým začne jednotlivé kroky implementovat a kontrolovat, zda skutečně mitigují kybernetický útok. Pokud s krizovým týmem na řešení incidentu spolupracují další strany, tým musí počítat s možností neúplné, nebo jen částečné implementace některých kroků odezvy (např. poskytovatel internetových služeb nemusí komunikaci zcela zablokovat).

Eliminace a obnova

Pokud jsou vybrané kroky odezvy efektivní a incident se podaří dostat pod kontrolu, aby se dál nešířil, je třeba co nejrychleji obnovit všechna dotčená aktiva do původního stavu, aby mohla být služba znovu plně poskytována. Pokud může být vyloučena možnost přístupu útočníka do NIS, zdravotnická dokumentace, která byla v době výpadku vedena fyzicky na papír, správce IT systémů obnoví NIS ze zálohy, správce sítě jej připojí zpět do nemocniční sítě a zaměstnanci nemocnice doplní chybějící data, která byla v době výpadku vedena fyzicky. Veškerý postup řízení KBI je zaevidován do interní dokumentace, kde může být dále analyzován za účelem zlepšení bezpečnostních opatření i samotného procesu řízení KBI. Po uvedení KBI pod kontrolu manažer sepíše zprávu o vyřešení incidentu a odešle ji na NÚKIB, který tak incident považuje za uzavřený.

9.5.5 Vyhodnocení

Poté, co krizový tým podnikne všechny naplánované kroky k eliminaci KBI, a obnoví dotčená aktiva, celý proces řízení a reakce na něj se vyhodnotí pro určení efektivity celého procesu. Dále bezpečnostní analytik určí příčinu KBI a na základě toho sestaví mitigační opatření. Při analýze efektivity řízení KBI je třeba posoudit celkové množství práce, a dobu trvání KBI od detekce až po vyhodnocení a trvání jednotlivých fází. Pro tyto účely můžeme vytvořit metriku; tabulku s očekávanými dobami trvání, sestavenou z průměrných dob u předchozích KBI, nebo ideální hodnotu, se kterou bude současný KBI porovnán.

Popis	**Doba trvání**
Doba mezi útokem a detekcí KBI (MTTD)	14 minut
Doba mezi detekcí a reakcí na KBI (MTTR)	25 minut
Doba mezi reakcí a vyhodnocením (MTRS)	90 minut
Doba mezi KBI (MTBI)	Rostoucí trend

Tabulka 14: Příklad metriky řízení významného KBI

Na základě této metriky můžeme porovnat právě řešený KBI s předpokládanou dobou vyřešení celého incidentu, pokud byly naměřené hodnoty prodlev vyšší, než se očekávalo, proces je přezkoumán a hledají se nedostačující, nebo slabá místa jak v řízení KBI, tak i v kybernetické bezpečnosti jako celku.

Bezpečnostní analytik provedl analýzu vzniku incidentu a identifikoval jako způsob průniku odcizení přístupových údajů formou spear phishingu, tudíž hrozba byla realizována z nedbalosti a z důvodu absence anti-phishingového filtru, na základě čehož doporučil zavedení seznamu protiopatření, která budou implementována buď okamžitě, nebo do budoucna jako součást strategického plánu kybernetické bezpečnosti. Tuto zprávu zhodnotí auditor a posoudí, zda jsou požadavky v souladu s normami, nebo právními předpisy.

O celém průběhu manažer kybernetické bezpečnosti vypracoval podrobnou zprávu o řízení, kde zahrnul popis, typ a závažnost incidentu, datum detekce a vyřešení, jeho dopad na aktiva a provoz nemocnice, jednotlivé fáze řízení a jejich aktivity a všechny informované strany. Vzhledem k tomu, že incident byl ohlášen na NÚKIB, je třeba po vyřešení odeslat také závěrečnou zprávu, kterou NÚKIB zaeviduje do vlastní evidence KBI. Na základě sbíraných dat zhodnotíme i použitý playbook při odezvě na konkrétní druh KBI a případné nedostatky podle zkušeností z řízení upravíme.

Protiopatření	**Doba realizace**	**Odpovědnost za realizaci**
Povinnost dvoufázového ověření při přihlašování do Active Directory	Okamžitě	Správce IT systémů
Mimořádné školení zaměstnanců o phishingu a spear phishingu	Okamžitě	Manažer kybernetické bezpečnosti
Zavedení anti-phishingového filtru	Do budoucna	Správce sítě
Simulovaný phishingový test v síti	Do budoucna	IT zaměstnanci

Tabulka 15: Příklad návrhu obecně phishingových protiopatření

10 Shrnutí a diskuse

Řízení KBI je jen tolik účinné, jako je jeho aktuálnost a opakovatelná použitelnost. Proces může být jakkoliv dobře navržený, ale pokud není po opakovaném používání kontrolován, analyzován a zlepšován, neustále vyvíjející se hrozby v kybernetické bezpečnosti budou čím dál odolnější a nebezpečnější. Pokud však vedení nemocnice i zaměstnanci pochopí, jaké riziko činí kybernetické hrozby pro zdravotnictví, a jaký mají dopad kybernetické bezpečnostní incidenty při nedostatečné mitigaci, začnou sami dbát na dodržování bezpečnostních praktik. I přesto, že trend kybernetických bezpečnostních incidentů v České republice stabilně roste, mnoho organizací, včetně poskytovatelů regulovaných služeb, kybernetickou bezpečnost podceňují, proto je nutné bezpečnostní pravidla nejen zaznamenat do interní směrnice, ale i seznámit zaměstnance s jejím obsahem. Proces řízení KBI, stejně jako bezpečnostní politika nemocnice jako celek, by měl být pravidelně auditován i v případě minimálního výskytu zaznamenaných KBU, nebo KBI. Podcenění vhodné přípravy může ve zdravotnictví způsobit značný chaos, úniky nebo ztrátu dat o pacientech, nebo přímo ohrozit zdraví a životy pacientů.

11 Závěry a doporučení

V této práci byl představen teoretický přehled pojmů a praktik v oblasti kybernetické bezpečnosti, legislativní požadavky nového zákona o kybernetické bezpečnosti a prováděcích předpisů, a jakým způsobem se dotýkají bezpečnostních povinností poskytovatelů zdravotnictví jako regulované služby. Dále byly popsána terminologie kybernetické bezpečnosti a její návaznost na zdravotnictví, včetně častých hrozeb a zranitelností, které jim čelí, a jak na kybernetickou bezpečnost nahlíží běžně používané normy a standardy. V poslední části teorie byl popsán samotný proces řízení KBI, který rámcově vycházel z několika standardů běžně používaných v praxi. Následně byly v praktické části představeny praktické aspekty fází řízení KBI na simulovaném kybernetickém útoku na nemocniční zařízení. Zavedené postupy, normy a standardy, doporučení a další best practices z provozu nabízí osvědčené praktiky řízení KBI i kybernetické bezpečnosti jako takové, nicméně neexistuje univerzální postup, kterým by se měly všechny organizace řídit, naopak každá bezpečnostní implementace se liší v závislosti na prostředcích, nebo dokonce ochotě organizace bezpečnostní opatření vůbec zavádět.

12 Seznam použité literatury

1. DEEPSTRIKE. *Cybercrime-as-a-Service: Market Size and Growth* [online]. 2026. [cit. 2026-07-29]. Dostupné z: https://deepstrike.io/blog/cybercrime-as-a-service-statistics-2025.
2. ČESKÝ STATISTICKÝ ÚŘAD. *Zdravotní péče* [online]. 2025. [cit. 2026-07-29]. Dostupné z: https://csu.gov.cz/zdravotni-pece.
3. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024* [online]. 2025. [cit. 2026-03-06]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zpr%C3%A1va_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2024.pdf.
4. KOLOUCH, Jan; BAŠTA, Pavel. *CyberSecurity*. Praha : CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
5. TECHNICKÁ NORMALIZAČNÍ KOMISE: TNK 20 INFORMAČNÍ TECHNOLOGIE. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník* [online]. 2020. [cit. 2026-04-11].
6. FRANTIŠEK, Nonnemann; ČERVENÝ, Vlastimil; VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Praha: Wolters Kluwer ČR, 2022. ISBN 978-80-286-0331-1.
7. VELIBOR, BOŽIĆ. *Confidentiality, Integrity and Availibility in hospital* [online]. 2023. [cit. 2026-07-24]. Dostupné z: https://www.researchgate.net/publication/368880457_Confidentiality_Integrity_and_Availibility_in_hospital.
8. EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP)* [online]. 2016. [cit. 2026-07-24]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:02016R0679-20160504.
9. NÚKIB. *Doporučení pro sdílení informací a práci s nimi* [online]. 2025. [cit. 2026-07-24]. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/sdileni-informaci/.

10. U.S. ARMY TRAINING AND DOCTRINE COMMAND. *Cyberspace Operations Concept Capability Plan 2016-2028* [online]. 2010. [cit. 2026-03-16]. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf.

11. NÚKIB. *Průvodce novým zákonem o kybernetické bezpečnosti* [online]. 2025. [cit. 2026-03-06]. Dostupné z: https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti.

12. NÚKIB. *O NÚKIB* [online]. 2025. [cit. 2026-03-12]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/.

13. ČESKO. *Vyhláška č. 408/2025 Sb., o regulovaných službách* [online]. 2025. [cit. 2026-03-06]. Dostupné z: https://www.e-sbirka.cz/sb/2025/408/2025-11-01.

14. CYBRELA. *Regulované služby* [online]. 2025. [cit. 2026-02-19]. Dostupné z: https://www.zakonyprolidi.cz/blog/regulovane-sluzby.htm.

15. EVROPSKÁ KOMISE. *doporučení Komise 2003/361/ES ze dne 6. května 2003* [online]. 2003. [cit. 2026-07-18]. Dostupné z: https://eur-lex.europa.eu/CS/legal-content/glossary/small-and-medium-sized-enterprises.html.

16. ČESKO. *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti* [online]. 2025. [cit. 2026-03-06]. Dostupné z: https://www.e-sbirka.cz/sb/2025/264/2025-11-01.

17. EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Text s významem pro EHP)* [online]. 2022. [cit. 2026-03-23]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2555.

18. CYBRELA. *Bezpečnostní opatření pod lupou: Co všechno vyžaduje nový kyberzákon?* [online]. 2026. [cit. 2026-03-23]. Dostupné z: https://cybrela.com/bezpecnostni-opatreni-povinnosti-podle-kyberzakona/.

19. ISO/IEC. *ČSN ISO/IEC 27035-1:2018* [online]. 2018. [cit. 2026-07-27]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27035-1-369799-199823.html.

20. ČESKO. *Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností* [online]. 2025. [cit. 2026-03-06]. Dostupné z: https://e-sbirka.gov.cz/sb/2025/409/2025-11-01.

21. NÚKIB. *Stanovení rozsahu řízení kybernetické bezpečnosti* [online]. 2025. [cit. 2026-07-25]. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2025/10/24/podpurny-material-stanoveni-rozsahu-rizeni-kb_uid_68fb3ad3ad575.pdf.

22. ISO/IEC. *Jak identifikovat primární aktiva?* [online]. 2025. [cit. 2026-07-27]. Dostupné z: https://aptien.com/cs/kb/articles/how-to-identify-primary-information-assets.

23. NÚKIB. *Řízení aktiv* [online]. 2020. [cit. 2026-07-27]. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=4880.

24. NÚKIB. *Hlášení kybernetických bezpečnostních incidentů* [online]. 2026. [cit. 2026-07-25]. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2026/06/08/podpurny-material-ke-hlaseni-incidentu_v1-2_uid_6a267e393778b.pdf.

25. CYBRELA. *Aktivum* [online]. 2026. [cit. 2026-07-26]. Dostupné z: https://cybrela.com/slovnik/aktivum/.

26. JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti, Páté doplněné a upravené vydání* [online]. 2022. [cit. 2026-04-07]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

27. NIST. *Computer Security Incident Handling Guide* [online]. 2012. [cit. 2026-04-10]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

28. CVE PROGRAM. *About the CVE Program* [online]. 2026. [cit. 2026-07-31]. Dostupné z: https://www.cve.org/About/Overview.

29. CYBRELA. *Hrozby, zranitelnosti a rizika* [online]. 2025. [cit. 2026-07-31]. Dostupné z: https://www.zakonyprolidi.cz/blog/hrozby-zranitelnosti-a-rizika.htm.

30. RUBRIK. *Healthcare Cybersecurity Challenges & Threats - 2026 Update* [online]. 2026. [cit. 2026-07-27]. Dostupné z: https://www.rubrik.com/insights/healthcare-cybersecurity-challenges-threats-2025.

31. NÚKIB. *PRŮVODCE ŘÍZENÍM AKTIV A RIZIK DLE VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI* [online]. 2022. [cit. 2026-07-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf.

32. EVROPSKÁ KOMISE. *Kybernetická bezpečnost nemocnic a poskytovatelů zdravotní péče* [online]. 2026. [cit. 2026-07-27]. Dostupné z: https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_cs.

33. FORTINET. *Cyberattacks in the Healthcare Industry* [online]. 2022. [cit. 2026-04-11]. Dostupné z: https://www.fortinet.com/solutions/industries/healthcare/cyberattacks-in-the-healthcare-industry.

34. HEALTHIT. *Supply Chain Attacks in Healthcare* [online]. 2021. [cit. 2026-07-27]. Dostupné z: https://healthit.com.au/supply-chain-attacks-in-healthcare/.

35. ISO/IEC. *ISO/IEC 27001* [online]. 2022. [cit. 2026-07-27].

36. NIST. *Guide for Conducting Risk Assesments* [online]. 2012. [cit. 2026-04-10]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

37. INTELLIPERMIT. *Plan-Do-Check-Act (PDCA) in Safety Management: A Continuous Improvement Framework* [online]. 2025. [cit. 2026-07-21]. Dostupné z: https://www.intellipermit.com/blog/plan-do-check-act-in-safety-management/.

38. ISO/IEC. *ČSN ISO/IEC 27035-2:2018* [online]. 2018. [cit. 2026-07-27]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27035-2-369799-199824.html#.

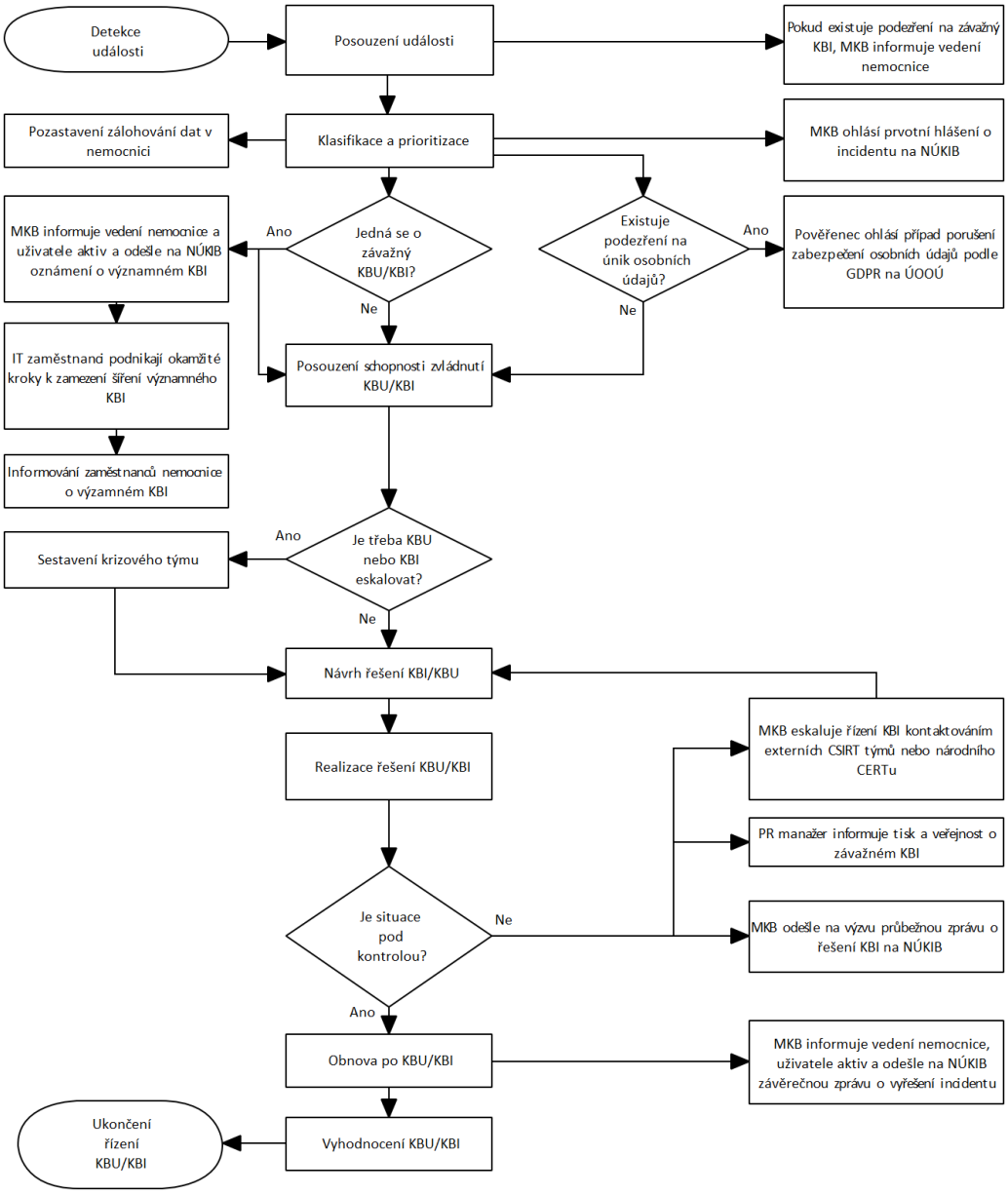
39. NIST. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* [online]. 2025. [cit. 2026-04-10]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

40. ENISA. *Good Practice Guide for Incident Management* [online]. 2010. [cit. 2026-07-31]. Dostupné z: https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf.

41. ATLASSIAN. *Escalation policies for effective incident management* [online]. 2026. [cit. 2026-07-31]. Dostupné z: https://www.atlassian.com/incident-management/on-call/escalation-policies.

13 Přílohy

13.1 Příloha č.1 – Vývojový diagram řízení KBI



UNIVERZITA HRADEC KRÁLOVÉ

Fakulta informatiky a managementu

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Šimon Hlušička**
Osobní číslo: **I2400040**
Studijní program: **B0612A140001 Informační a síťová bezpečnost**
Téma práce: **Incident management ve zdravotnictví**
Zadávající katedra: **Katedra informačních technologií**

Zásady pro vypracování

Cílem této bakalářské proce je popsat proces incident managementu z pohledu zajištění včasné reakce na incidenty s důrazem na zdravotnická zařízení. Práce se zaměří na identifikaci relevantních skakeholderů a na základě best-practise v dané oblasti bude výsledkem práce navržený proces zajištění identifikace, klasifikace, řešení a hlášení incidentu na relevantní autority.

Rozsah pracovní zprávy: **40**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

SCHNEPP, Rob, Ron VIDAL a Chris HAWLEY. *Incident Management for Operations*. 1. vyd. Sebastopol, CA: O'Reilly Media, 2017. ISBN 978-1-4919-1762-6

Vedoucí bakalářské práce: **Ing. Tomáš Svoboda, Ph.D.**
Katedra informačních technologií

Oponent bakalářské práce: **Ing. Patrik Urbaník, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **25. listopadu 2024**

L.S.

prof. Ing. Mgr. Petra Marešová, Ph.D., MBA v.r.
děkanka

doc. Ing. Pavel Čech, Ph.D. v.r.
vedoucí katedry

V Hradci Králové dne 25. listopadu 2024