Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Veřejné zakázky z pohledu informační a kybernetické bezpečnosti

Veronika Cábová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Veronika Cábová

Veřejná správa a regionální rozvoj – c.v. Litoměřice

Název práce

Veřejné zakázky z pohledu informační a kybernetické bezpečnosti

Název anglicky

Public procurement from the perspective of information and cyber security

---

Cíle práce

Hlavním cílem diplomové práce je na základě analýzy realizovaných veřejných zakázek v oblasti informační a kybernetické bezpečnosti identifikovat slabá místa a nedostatky v rámci provádění auditů kybernetické bezpečnosti a navrhnout vhodná nápravná opatření. Výstupem je pak návrh obecné metodiky pro výkon auditu kybernetické bezpečnosti a její implementaci do firemního prostředí.

Metodika

Práce bude rozdělena na část teoretickou a část praktickou. V teoretické části bude použita metoda literární rešerše a komparativní metoda výkladů odborné literatury, analýza právních předpisů, odborných článků a publikací týkajících se problematiky informační a kybernetické bezpečnosti.

Na základě získaných teoretických poznatků bude v praktické části diplomové práce použita metoda sběru dat u zvolené společnosti. Především pak analýza jednotlivých realizovaných veřejných zakázek v oblasti informační a kybernetické bezpečnosti. Na základě zjištěného stavu bude využitím metody deskripce, analýzy zpracovaných dat a komparace provedeno celkové vyhodnocení výstupů.

Výsledkem celého procesu bude návrh obecné metodiky pro plán a realizaci auditu kybernetické bezpečnosti a její implementace do firemního prostředí.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

audit kybernetické bezpečnosti, bezpečnost, bezpečnostní role, kybernetická bezpečnost, dokumentace, systém řízení bezpečnosti informací, veřejné zakázky, zákon o kybernetické bezpečnosti, vyhláška, zadávací řízení

Doporučené zdroje informací

BUGAN, A., Férové zadávání veřejných zakázek., Praha: Transparency International – Česká republika. 2019. 64 s. ISBN 978-80-87123-34-8

HRŮZA, P. a kolektiv, Kybernetická bezpečnost a kritická informační infrastruktura. Praha: Powerprint. 89 s. 2018. ISBN 978-80-7568-122-5

JIRÁSEK, P., NOVÁK, L., POŽÁR, J., Výkladový slovník kybernetické bezpečnosti, Praha: Policejní akademie České republiky. 240 s. 2015. ISBN 978-80-7251-436-6

KOLOUCH, J., BAŠTA, P. a kol. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8

MAISNER, M., VLACHOVÁ, B., Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a.s., 219 s. 2015. ISBN 978-80-7478-817-8

PAVEL, J. Veřejné zakázky a efektivnost. Praha: Ekopress, s.r.o., 123 s. 2013. ISBN 978-80-87865-04-0

SEDLÁK, P., Kybernetická (ne)bezpečnost., Brno: CERM, akademické nakladatelství. 429 s. 2021. ISBN 978-80-7623-068-2

ÚZ 1445. Svobodný přístup k informacím, Elektronické komunikace, EGOVERNMENT, Kybernetická bezpečnost., Ostrava-Hrabůvka: Sagit. 336 s. 2021. ISBN 978-80-7488-492-5

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

JUDr. Daniela Světlíková

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 7. 3. 2023

Ing. JUDr. Eva Daniela Cvik, Ph.D. et Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 13. 3. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 27. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Veřejné zakázky z pohledu informační a kybernetické bezpečnosti" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 29. března 2024 _____

Poděkování

Ráda bych touto cestou poděkovala JUDr. Daniele Světlíkové za její trpělivé vedení, odborné rady a věcné připomínky v průběhu celé tvorby diplomové práce. Děkuji rovněž společnosti BELCOM Digital za poskytnutí datových podkladů a obecnou podporu během mého studia. Dále bych ráda poděkovala své rodině za jejich trpělivost a vytvoření příznivého prostředí pro studium a psaní této práce.

Veřejné zakázky z pohledu informační a kybernetické bezpečnosti

Abstrakt

Diplomová práce je zaměřena na analýzu veřejných zakázek v oblasti informační a kybernetické bezpečnosti s důrazem na provádění auditů kybernetické bezpečnosti. Hlavním cílem je identifikovat slabá místa a nedostatky v rámci provedených auditů kybernetické bezpečnosti a navrhnout vhodná nápravná opatření.

Práce je rozdělena do dvou hlavních částí, a to na teoretickou a praktickou část. V teoretické části diplomové práce jsou objasněny základní pojmy související s problematikou kybernetické bezpečnosti a vymezena nejdůležitější ustanovení zákona, zejména Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Praktická část se zabývá sběrem dat, jejich analýzou a komparací nedostatků v rámci provedených auditů kybernetické bezpečnosti. V úvodu je představena konkrétní společnost, její hlavní oblasti působení a další relevantní informace. Následuje statistický přehled podaných nabídek na veřejné zakázky z oblasti informační a kybernetické bezpečnosti, kterých se vybraná společnost ve sledovaném období zúčastnila. Praktická část dále identifikuje nejčastější nedostatky v rámci provedených auditů kybernetické bezpečnosti. Výsledky statistické analýzy z období od počátku roku 2017 až do prosince 2022 jsou prezentovány pomocí tabulek a grafů vlastním zpracováním.

V závěru této práce jsou na základě vlastního šetření a statistického rozboru interpretovány zjištěné nedostatky a uvedena vhodná doporučení. Výstupem je pak návrh obecné metodiky pro výkon auditu kybernetické bezpečnosti a její implementace do firemního prostředí.

Klíčová slova: bezpečnost, zákon o kybernetické bezpečnosti, vyhláška, kybernetická bezpečnost, kybernetický útok, veřejné zakázky, informační bezpečnost, informační systém, hrozby, bezpečnost informací

Public procurement from the perspective of information and cyber security

Abstract

The diploma thesis is focused on the analysis of public contracts in the field of information and cyber security with an emphasis on the implementation of securtiy audits. The main objective is to identify weaknesses and deficienies in the conducted cybersecurity audits and to propose appropriate corrective measures.

The thesis is divided into two main parts, namely the theoretical nad practical part. The theoretical part of the thesis explains the basic concepts related to the issue cybersecurity and defines the most important provisions of the law, in particular Act No. 181/2014 Coll., on cybersecurity and on the amendments to related acts, as amended.

The practical part deals with collection of data, its analysis and comparison of shortcomigs within the framework of the conducted cybersecurity audits. In the introduction, a specific company, its main areas of aktivity and othe relevant information are presented. This is followed by a statistical overview of tenders submitted for public contractsin the field of information and cybersecurity in which the selected company participated in the period under review. The practical part also identifies the most frequent shorcomings in the cybersecurity audits performer. The results of the statistical analysis from the beginning of 2017 to December 2022 are presented using tables and graphs by our own processing.

At the end of this thesis, the identified gaps are interpreted based on the self-investigation and statistical analysis and appropriate recommendations are made. The output is then a proposal for general methodology for conducting a cybersecurity audit and its implementation in a corporate environment.

Keywords: security, cybersecurity law, regulation, cybersecurity, cyber-attack, public procurement, information security, information system, threats, information security

Obsah

1 Úvod

„Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.“[1]

V dnešní digitální éře se veřejné zakázky stávají více závislými na informačních technologiích. Tyto technologie přinášejí mnoho výhod v podobě efektivity, transparentnosti a rychlosti procesů. Avšak s tím roste také zranitelnost těchto systémů vůči kybernetickým hrozbám a útokům, které mohou mít závažné dopady na jednotlivce, firmy, veřejnou správu a celou národní infrastruktury. Včasné odhalení kybernetických útoků má zásadní význam pro zmírnění těchto hrozeb a může výrazně minimalizovat potenciální ztráty. S narůstajícím počtem digitálních hrozeb a útoků je nezbytné, aby organizace a veřejné instituce přijaly účinná opatření k ochraně svých informačních systémů a dat. Důsledná ochrana dat a informací není pouze etických požadavkem, ale také právní povinností veřejných institucí v souladu s příslušnou legislativou a předpisy. Jedná se především o Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů a její prováděcí Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech v podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Veřejné zakázky z oblasti informační a kybernetické bezpečností představují strategický nástroj pro zajištění kvalitních a bezpečných informačních systémů a služeb poskytovaných veřejným institucím. Současně s rostoucím důrazem na zabezpečení kritické informační infrastruktury vzniká potřeba provádění auditů kybernetické bezpečnosti jako prostředku k pravidelnému posuzování a zlepšování bezpečnosti informačních systémů. Audit kybernetické bezpečnosti je tak klíčovým nástrojem pro identifikaci potenciálních hrozeb a rizik a poskytuje organizacím nezbytné informace pro zlepšení svých bezpečnostních postupů a opatření.

Výběr tématu proběhl na základě praktických zkušeností s problematikou veřejných zakázek a realizací auditů kybernetické bezpečnosti. Autorka dlouhodobě pracuje ve společnosti, která se aktivně účastní zadávacích řízení v oblasti informační a kybernetické bezpečnosti s důrazem na provádění auditů kybernetické bezpečnosti. Proto se rozhodla

[1] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016. s. 474.

touto problematikou zabývat blíže a přinést ucelený pohled na celou oblast informační a kybernetické bezpečnosti.

Navzdory neustálému zvyšování investic do zabezpečení, aktéři hrozeb často úspěšně provádějí škodlivé či dokonce destruktivní kybernetické útoky. Je zřejmé, že k účinnému zvládání kybernetických hrozeb je proto nezbytné přijmout nový a efektivnější přístup. Kybernetické bezpečnosti nelze dosáhnout bez hluboké důvěry a spolupráce mezi veřejným sektorem a zbytkem společnosti. Pouze společně můžeme vytvořit opravdu otevřený a bezpeční kyberprostor, ve kterém budeme všichni prosperovat.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je na základě analýzy realizovaných veřejných zakázek v oblasti informační a kybernetické bezpečnosti identifikovat slabá místa a nedostatky v rámci provádění auditů kybernetické bezpečnosti a navrhnout vhodná doporučení. Výstupem je pak návrh obecné metodiky pro výkon auditu kybernetické bezpečnosti a její implementace do firemního prostředí.

2.2 Metodika

Diplomová práce je rozdělena na část teoretickou a část praktickou. V teoretické části je použita metoda literární rešerše a komparativní metoda výkladů odborné literatury, analýza právních předpisů, odborných článků a publikací vztahující se problematiky informační a kybernetické bezpečnosti. Jsou zde detailně vysvětleny základní pojmy nezbytné pro pochopení dané problematiky a definován právní rámec v České republice upravující informační a kybernetickou bezpečnost a otázky spojené s kritickou infrastrukturou. Na závěr této části je popsán samotný proces auditu kybernetické bezpečnosti.

Na základě získaných teoretických poznatků je v praktické části diplomové práce použita metoda sběru dat u zvolené společnosti. Především pak analýza jednotlivých realizovaných veřejných zakázek v oblasti informační a kybernetické bezpečnosti. Na základě zjištěného stavu je využitím metody deskripce, analýzy zpracovaných dat a komparace provedeno celkové vyhodnocení výstupů. Důraz je kladem především na identifikaci a komparaci nedostatků v rámci provedených auditů kybernetické bezpečnosti. Úvodní část práce je věnována představení vybrané společnosti, ve které autorka dlouhodobě pracuje, včetně hlavních oblastí činnosti a dalších relevantních informací. Statistické údaje o podaných nabídkách na veřejné zakázky z oblasti informační a kybernetické bezpečnosti jsou získány z interních dat vybrané společnosti ve zvoleném období od počátku roku 2017 do prosince 2022.

V rámci vlastního výzkumu je použita metoda sběru dat z interních dokumentů a závěrečných auditních zpráv. Výsledky z provedené analýzy jsou prezentovány pomocí tabulek a grafů a následně interpretovány. Ze získaných dat je provedena analýza vývoje

počtu podaných nabídek na veřejné zakázky dle jednotlivých oblastí informační a kybernetické bezpečnosti a dále dle finančního rozsahu. Prostřednictvím vlastního šetření a statistického rozboru jsou dále provedena identifikace a klasifikace nejčastějších a nejzávažnějších nedostatků v rámci provedených auditů kybernetické bezpečnosti. Zjištěná data za sledované období jsou poté komparována a výsledky těchto šetření jsou prezentovány přehlednými tabulkami, údaje graficky znázorněny a následně vyhodnoceny.

V závěru diplomové práce je využitím metody syntézy a klasifikace zpracovaných dat provedeno celkové vyhodnocení výstupů. Na základě získaných poznatků a jednotlivých skutečností vyplývající z výzkumného šetření jsou formulovány závěry. Ke každému závažnému nedostatku je autorkou navrženo vhodné doporučení. Výstupem celého procesu je návrh obecné metodiky pro výkon auditu kybernetické bezpečnosti a její implementace do firemního prostředí.

3 Teoretická východiska

Veřejné zakázky v oblasti informační a kybernetické bezpečnosti představují v současné době jedno z nejdiskutovanějších témat, která spojují dvě zásadní oblasti, a to veřejné zakázky (dále jen „VZ“) a bezpečnost informací. V době, kdy se naše společnost stále více spoléhá na digitální technologie a internetovou konektivitu, stává se bezpečnost informací, respektive kybernetická bezpečnost (dále jen „KB“), nezbytnou součástí naší každodenní existence. VZ nejen zajišťují to, že veřejné peníze jsou efektivně a zodpovědně využity, ale také pomáhají chránit národní bezpečnost a důvěrnost osobních údajů občanů. Dále musí být transparentní, spravedlivé a efektivní, což vyžaduje pečlivou analýzu potřeb, definici bezpečnostních požadavků a kompetenčního výběru dodavatelů. Tématu VZ je autorkou věnována bakalářská práce pod názvem „Veřejné zakázky z pohledu dodavatele ICT služeb“, ve které jsou vysvětleny základní pojmy, relevantní informace související s problematikou veřejných zakázek a vymezena nejdůležitější ustanovení Zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.[2]

Za účelem snadnějšího pochopení celé oblasti informační a kybernetické bezpečnosti je klíčové se seznámit se základními pojmy spojenými s touto problematikou. Proto v teoretické části této diplomové práce budou vymezena nejdůležitější ustanovení zákona a příslušných právních norem související s toho problematikou, především novelizovanému Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Získaná teoretická východiska jsou základní oporou k podpoře zpracování praktické části a dosažení hlavního cíle diplomové práce.

3.1 Principy informační a kybernetické bezpečnosti

Informační a kybernetická bezpečnost jsou v dnešním digitálním věku zásadními oblastmi, které hrají klíčovou roli v ochraně důvěrnosti, integrity a dostupnosti informací a systémů. S rostoucím významem digitálních technologií a internetu se stávají organizace a jednotlivci stále více závislými na digitálních systémech a komunikaci. Tato závislost vytváří nové výzvy a rizika, kterým je třeba čelit.

Informační bezpečnost se zaměřuje na ochranu dat a informací před neoprávněným přístupem, zneužitím a ztrátou. KB se na druhou stranu zaměřuje na ochranu počítačových

[2] CÁBOVÁ, V. *Veřejné zakázky z pohledu dodavatele ICT služeb.* Praha, 2022. Bakalářská práce (Bc). Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, Veřejná správa a regionální rozvoj, 2022-05-16.

systémů, sítí a zařízení před kybernetickými útoky a hrozbami, které mohou mít devastující dopady na společnost a ekonomiku.

Tento úvod do informační a kybernetické bezpečnosti nám poskytuje základní přehled o klíčových aspektech, jako jsou hrozby, zranitelnost, strategie obrany a nezbytnost vzdělání a osvěty v této oblasti. Důležité je i jakým způsobem je možnost chránit naše informace a digitální prostředí před hrozbami a útoky.

3.2 Právní úprava kybernetické bezpečnosti

Základním právním předpisem regulující v současné době problematiku kybernetické a informační bezpečnosti je Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“). Tento zákon vstoupil v účinnost dne 1. ledna 2015 a jde o jeden z prvních zákonů v České republice (dále jen „ČR“), který řeší celou sféru bezpečnosti. ZoKB vychází z Nařízení Evropské unie a upravuje práva a povinnosti osob a pravomoci orgánů veřejné moci v oblasti KB.[3] Cílem zákona je zajistit ochranu prostředí tvořeného informačními systémy (dále jen „IS“), sítěmi a službami elektronických komunikací s ohledem na prevenci ohrožení práva subjektů a zároveň zabránit zneužití národní kybernetické infrastruktury k útokům mimo území ČR.[4] Mimo to umožňuje vyhlášení stavu kybernetického nebezpečí, eventuálně následně nouzového stavu z důvodu kybernetického ohrožení zájmů státu.[5]

Součástí ZoKB je Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB“). Tato vyhláška stanovuje pravidla týkající se obsahu a struktury bezpečnostní dokumentace, a také upravuje požadavky na bezpečnostní opatření, kam patří povinnosti jejich aktualizace, typy, kategorie a hodnocení významnosti incidentů, způsob a náležitosti jejich hlášení, náležitosti oznámení

[3] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISE („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). [online]. 2019 [cit. 2023-08-30]. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument/souvislosti?celex=32019R0881&date=0.

[4] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 5.

[5] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.* Praha: Policejní akademie České republiky, 2020. s. 64.

o provedení reaktivního opatření a jeho výsledku, vzor a formu oznámení kontaktních údajů a způsob likvidace dat, provozních údajů, informací a jejich kopií.[6]

KB je úzce spjata s ochranou osobních údajů, utajovaných informací a IS veřejné správy. V současné době dochází ke stále většímu shromažďování dat a osobních údajů, a proto je nutné zajistit, aby veškeré tyto důvěrné informace byly řádně chráněny a nedocházelo tak k narušování našeho soukromí. V důsledku rozsáhlého sběru těchto informací může vznikat riziko sledování, a dokonce neoprávněného zveřejňování těchto citlivých informací. Tento zásadní problém se snaží řešit např. Nařízení o ochraně osobních údajů (EU) 2016/679 (dále jen „GDPR“). Hlavním cílem tohoto nařízení je snížit rizika spojená s neoprávněným nakládáním s těmito daty a osobními informacemi a zejména posílení práva jednotlivců. To zahrnuje i zjednodušené možnosti kontroly nad svými osobními údaji. I přes tato příslušná nařízení nelze zaručit úplnou a efektivní ochranu těchto dat, zejména v současné době, kdy dochází k obrovskému objemu zpracovávaných dat. Proto je třeba hledat podporu v různých technologiích, které mohou hrát klíčovou roli při ochraně osobních informací. Existuje celá řada nástrojů a technologií navržených k ochraně soukromí a tím zabezpečení těchto citlivých osobních údajů.[7]

Právě informace týkající se osobních údajů jsou častým cílem neoprávněného přístupu zejména s ohledem na rizika spojená s odhalenými zranitelnostmi systémů a kybernetickými útoky. Proto je klíčové, abychom chránili své osobní údaje a sdíleli je pouze tam, kde máme jistotu, že jsou řádně zabezpečeny. Je nezbytné provádět komplexní zabezpečení osobních údajů, které zahrnuje jak technické, tak organizační aspekty. Tato opatření musí být důkladná a průběžně monitorována, aby odpovídala rizikům a citlivosti těchto údajů.[8]

Následující obrázek znázorňuje přehledové schéma k ZoKB a jeho prováděcím předpisům.

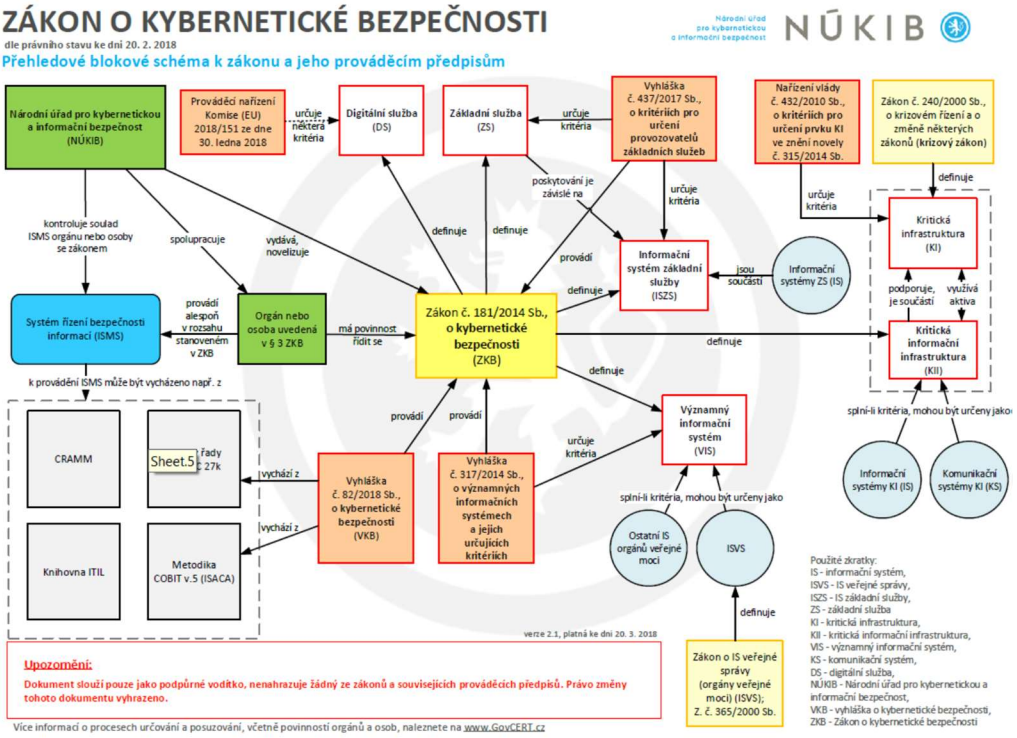
---

[6] § 1 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2018, částka 43.

[7] 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 [online]. 2016 [cit. 2023-08-30]. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument?celex=32016R0679#Sum.

[8] European Union Agency for Cyber Security. *Data Protection: Security of personal data*. [online]. 2005 [cit. 2023-08-30]. Dostupné z: https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection.

Obrázek 1 Přehledové blokové schéma k zákonu a jeho prováděcím předpisům



Zdroj: NÚKIB (2020)[9], zpracování: převzato

3.3 Definice základních pojmů

Zásadní součástí zákona je definice jednotlivých pojmů z oblasti informační a kybernetické bezpečnosti, které jsou důležité pro pochopení celé této problematiky.

3.3.1 Kybernetická bezpečnost

Pod pojmem KB rozumíme soubor opatření a prostředků, které jsou zaměřeny k zajištění ochrany kybernetické prostoru, zejména ochrany počítačových systémů, sítí, dat a digitálních zařízení před kybernetickými hrozbami a útoky.[10]

Cílem KB je zajištění integrity, dostupnosti a důvěrnosti digitálních prostředků a informací. KB se zabývá identifikací, prevencí, detekcí a reakcí na různé formy kybernetických útoků, k ochraně před kriminálním či neautorizovaným užitím

[9] Národní úřad pro kybernetickou a informační bezpečnost. *Přehledové blokové schéma k zákonu a jeho prováděcím předpisům*. [online]. 2020 (PDF). [cit. 2023-08-20]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-822/1schemazkb-cz.pdf.

[10] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 97.

elektronických dat a mnoho dalších neoprávněných aktivit. [11] *„S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnosti České republiky a zároveň práva jedinců na informační sebeurčení“.*[12]

Bezpečnost v kyberprostoru je zajišťována nejen v rámci tohoto prostoru samotného, ale také mimo něj.[13] Kybernetický prostor je nedílnou součástí našeho života. Stále vzrůstá trend digitalizace a dostupnosti k veškerým informacím kdykoliv a odkudkoliv.[14]

3.3.2 Kybernetický prostor/ Kyberprostor

Kybernetický prostor, který je také nazýván kyberprostorem, dle zákonné definice označujeme jako digitální prostředí, ve kterém se odehrávají interakce mezi digitálními systémy, počítačovými sítěmi, lidmi a technologiemi.[15]

Tento termín zahrnuje komunikaci, výměnu dat, informace a procesy, které se odehrávají v digitálním světě. Kyberprostor není fyzickým prostorem, ale je spíše virtuálním prostředím uměle vytvořené člověkem, ve kterém dochází ke zpracování a uchování informací a také především k jejich výměně a sdílení.[16]

S ohledem na rostoucí závislost společnosti na informačních technologiích (dále jen „IT“) dochází v kybernetickém prostoru k manipulaci s důvěrnými informacemi. Existuje významné riziko zneužití těchto informací.[17]

3.3.3 Bezpečnost informací

Dalším z pojmů, jež zákon definuje, je „bezpečnost informací“. Ta je chápána jako oblast KB, která se zaměřuje na ochranu důvěrnosti, integrity a dostupnosti informací v informačních a komunikačních technologiích (dále jen „ICT“). Zahrnuje opatření a postupy, které mají za cíl minimalizovat riziko, zneužití, neoprávněného přístupu nebo poškození dat a informací během jejich vzniku, zpracování, ukládání a přenášení,

---

[11] KOLOUCH J., BAŠTA P. a kol. *CyberSecurity*. Praha: CZ.NIC., 2019. s. 42.

[12] Národní úřad pro kybernetickou a informační bezpečnosti. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. 2017 (PDF). [cit. 2023-08-20]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

[13] KOLOUCH J., BAŠTA P. a kol. *CyberSecurity*. Praha: CZ.NIC., 2019. s. 45.

[14] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.* Praha: Policejní akademie České republiky, 2020. s. 30.

[15] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost.* Praha: CERM, 2021. s. 12.

[16] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 65.

[17] Tamtéž, s. 66.

a to jak ve fyzické, tak v digitální podobě. Bezpečnost informací se týká nejen firem a organizací, ale také jednotlivců a veřejných institucí.[18]

3.3.4 Kritická informační infrastruktura

Kritická informační infrastruktura (dále jen „KII“) představuje zákonem jasně vymezený komplex IS, jejichž narušení nebo nefunkčnost by mělo závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.[19]

Podle Směrnice ES/114/2008[20] a související tuzemské legislativy jsou klíčovými funkčními oblastmi činnosti státu, které vyžadují nepřetržitou funkčnost kritické infrastruktury, energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, veřejná správa atd.[21]

3.3.5 Významný informační systém

Mimo KII jsou také stanoveny tzv. významné informační systémy (dále jen „VIS“) orgánů veřejné moci. Toto stanovení probíhá podle ustanovení ZoKB, včetně jeho prováděcích právních předpisů, konkrétně vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.[22]

Tato kategorie je zvláště vyhrazena pro IS orgánů veřejné moci, jež mají klíčovou roli při výkonu veřejné správy. Do této kategorie patří všechny IS, které jsou spravovány orgány veřejné moci, ačkoli nejsou součástí kritické infrastruktury. Tyto systémy, byť nekritické, mohou svým narušením způsobit omezení nebo výrazné ohrožení efektivity výkonu orgánů veřejné moci.

V současné době je registrováno 92 takových systémů. Jedná se především o IS řízené ministerstvy a dalšími ústředními správními úřady. Mezi ně patří např. Centrální

---

[18] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 67.

[19] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.* Praha: Policejní akademie České republiky, 2020. s. 57.

[20] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu, [online]. 2008 [cit. 2023-08-28]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=cellar%3Aba51b03f-66f4-4807-bf7d-c66244414b10.

[21] Nařízení vlády č. 315/2014 Sb., Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů,* rok 2014, číslo 315.

[22] Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, In: *Sbírka zákonů,* rok 2014, částka 127.

registr vozidel, Registr živnostenského podnikání, Centrální evidence stíhaných osob nebo Centrální registr pojištěnců.[23]

3.3.6 Významná síť elektronických komunikací

Významnou sítí se označuje síť elektronických komunikací, která umožňuje přímé propojení se zahraničními veřejnými komunikačními sítěmi nebo přímý přístup ke KII. Tato síť elektronických komunikacích je definována v souladu s ustanoveními zákona o elektronických komunikacích.[24] Tato síť buď zajišťuje propojení kybernetického prostoru ČR s mezinárodním prostředím nebo zajišťuje připojení ke KII.[25]

3.4 Triáda CIA

Jedná se o model navržený pro KB, který definuje konkrétní zásady a bezpečnostní postupy, kterými by se měly řídit jak firmy, tak i jiné organizace pro zachování KB, zejména v oblasti ochrany dat a informací.[26]

V rámci KB jsou citlivé informace obvykle prioritně chráněny, neboť většina kybernetických útoků často vychází právě z úniku těchto informací. Osobní informace mohou obsahovat data o jméně, adrese, rodném čísle, zdravotní dokumentaci, finanční dokumentaci a dalších údajích. Získání informací může vést k podvodným aktivitám, jako je např. krádež identity osob. To může mít různé důsledky, například možností získání úvěru, prodeje nemovitostí nebo dokonce odcizení finančních prostředků z bankovního účtu.

Daleko závaznějšími následky může být například odhalení státních tajemství a jiných citlivých informací státních institucí, vlády, armády, policie, zpravodajských služeb, zdravotních institucí, bank a dalších subjektů. Tyto informace mohou zahrnovat válečné plány a dokumentace, utajenou identitu osob, informace získané zpravodajskou činností a jiné důvěrné údaje. V těchto případech jsou potenciální následky mnohem závažnější

[23] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 19.

[24] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikací), In.: *Sbírka zákonů,* rok 2005, částka 43.

[25] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 74.

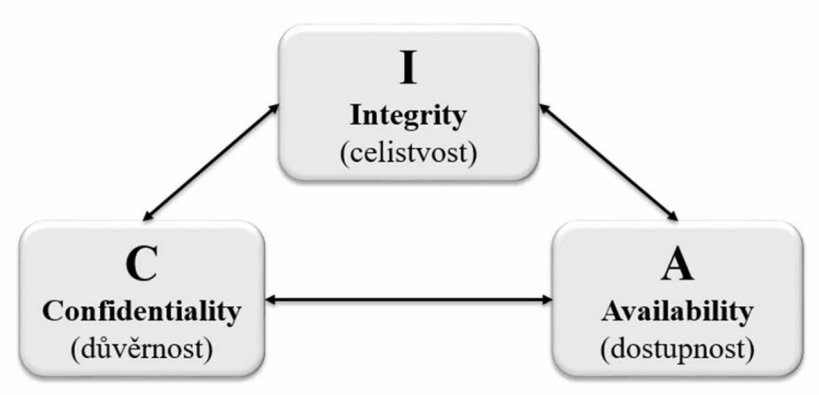
[26] KOLOUCH, J., BAŠTA, P., a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 45.

než pouze finanční ztráty, neboť může být ohrožen lidský život, zdraví a celková bezpečnost státu.[27]

3.4.1 Rozdělení CIA triády

CIA triáda je jeden ze základních konceptů IS, který integruje tři přístupy, které jsou navrženy s cílem přispět především k zabezpečení informací, jak nám znázorňuje následující obrázek.

Obrázek 2 Triáda CIA



Zdroj: *CyberSecurity* (2019)[28], zpracování: převzato

Tento model se zakládá na třech klíčových zásadách:

- C – *Confidentiality* (důvěrnost)
- I – *Integrity* (integrita/celistvost)
- A – *Availability* (dostupnost).[29]

Důvěrnost (Confidentiality)

U této zásady je kladen důraz na to, aby data, informace a vše, co s souvisí s ICT, byly dostupné pouze oprávněným osobám. Za tímto účelem se používá klasifikace těchto chráněných činností, a to prostřednictvím různých kategorizací, které jsou stanoveny například bezpečnostními standardy mezinárodně uznávané normy (dále jen „ISO/IEC“).[30]

[27] Science Direct. Parkerian Hexad: *What is Information Security?* [online]. 2014 [cit. 2023-08-30]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/parkerian-hexad.

[28] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 55.

[29] Coretelligent. *What is the CIA Triad, And Why Does Your Cybersecurity Position Depend on* It? [online]. 2022 [cit. 2023-08-30]. Dostupné z: https://coretelligent.com/insights/what-is-the-cia-triad-and-why-does-your-cybersecurity-position-depend-on-it/.

[30] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 48.

Na úrovni národního práva, například podle Zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, se předpisy týkají utajovaných informací a ty jsou rozděleny do různých stupňů utajení na:

a) *„**Přísně tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,*
b) ***Tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,*
c) ***Důvěrné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,*
d) ***Vyhrazené**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“*[31]

Integrita (Integrity)

Integrita znamená absolutní neporušitelnost. Jedná se o vlastnost, která garantuje, že s těmito daty nelze nijak manipulovat tak, aby se změnila jejich původní podoba. Obsahuje i další aspekty, zejména přesnost, a to v takové formě, že informace, která byla přijata, zůstane tak, jak byla původně vytvořena, sdílena nebo jinak předána. Když hovoříme o integritě systému, je tím myšleno, že systém funguje v souladu s čekáváním, bez příslušného oslabení a bez úmyslného nebo nahodilého neoprávněného zásahu do tohoto systému. V případě narušení integrity je důležité brát v potaz i to, že manipulace s daty, která by mohla nastat, nemusí být vždy snadno detekovatelná. Proto může trvat určitý čas, než bude případná manipulace odhalena.[32]

V rámci VoKB je integrita kategorizována do čtyř stupňů: nízký, střední, vysoký a kritický. Tyto stupně určují, jak by měla být chráněna ICT na základě jejich důležitosti a rozsahu. Kromě toho je u každého stupně integrity stanoveno, jaké prostředky nebo nástroje jsou vhodné pro daný stupeň ochrany. Důležitost ochrany a síla použitých prostředků roste směrem od nízkého stupně až po kritický.[33]

---

[31] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů,* ročník 2005, částka 143. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412.

[32] KOLOUCH, J., BAŠTA, P., a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 52, 53.

[33] Tab. 2: Stupnice pro hodnocení integrity k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů,* rok 2018, částka 43.

Dostupnost (Availability)

Dostupnost je zde myšlena ve vztahu k získání autorizovaného přístupu k informacím, datům nebo IS v okamžiku, kdy je tato možnost potřebná. VoKB rovněž definuje čtyři stupně kvalifikace dostupnosti: nízká, střední, vysoká a kritická. Tyto stupně se zabývají důležitostí oslabení dostupnosti ICT služeb a informací v závislosti na úrovni bezpečnosti, přičemž rozsah oslabení dostupnosti se pohybuje od nepodstatného v nízkém stupni až po nepřijatelné oslabení dostupnosti v úrovni kritické. Pro každý stupeň je také specifikováno, jak dlouho by maximálně mělo oslabení dostupnosti ICT služeb trvat vzhledem ke konkrétnímu stupni, resp. za jak dlouhou dobu by měla být dostupnost obnovena. Například pro nízký stupeň by měla být obnovena do sedmi dnů, zatímco pro střední stupeň do jednoho pracovního dne, pro vysoký stupeň do několika hodin a u kritického do několika minut. Dále je pro každý stupeň specifikováno, jaký typ ochrany je pro daný stupeň adekvátní. Jde zejména o zálohování dat, informací a počítačového systému jako takového. U nízkého stupně je požadováno pravidelné a systematické zálohování. U středního stupně je doporučeno provádět zálohy obvyklým způsobem zálohování a obnovy. U vysoké úrovně se požaduje použití záložních systémů, kdy znovuobnovení systému nebo služeb smí být za pomoci osoby k tomu určené nebo výměnou ICT komponentů. A u posledního kritického stupně je také nutné používat záložní systémy a obnova ICT služeb musí být automatizovaná bez potřeby zásahu jakékoli osoby. Tento požadavek je stanoven s cílem co nejrychlejší a nejefektivnější obnovy dostupnosti ICT systému po případném výpadku.[34]

3.5 Okruh povinných subjektů podle ZoKB

Ustanovení ZoKB vymezuje okruh povinných osob a orgánů, kterým jsou ukládány povinnosti související s KB. Kromě těchto subjektů se mohou do systému KB dobrovolně zapojit i další entity, např. soukromé osoby podnikající v oblasti IT.[35]

[34] Tab. 2: Stupnice pro hodnocení integrity k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů,* rok 2018, částka 43.

[35] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 75.

Kontrolu dodržování zákonem stanovených povinností provádí Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) u všech typů povinných subjektů, jak nám znázorňuje následující tabulka.

Tabulka 1 Povinné subjekty a bezpečnostní týmy – povinnosti

Povinný subjekt	Povinnost subjektu	Povinnost bezpečnostního týmu	Bezpečnostní tým odpovědný za skupinu povinných subjektů
Správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury Správci a provozovatelé významných informačních systémů Správci a provozovatelé systému základní služby	Hlásit kontaktní údaje příslušnému bezpečnostnímu týmu Hlásit kybernetické bezpečnostní incidenty příslušnému bezpečnostnímu týmy	Pomáhat řešit kybernetický bezpečnostní incident (např. obnovení provozu, eliminace útoku, dohledání zdroje útoku)	Vládní CERT
Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací Orgány nebo osoby zajišťující významnou síť Poskytovatelé digitální služby			Národní CERT

Zdroj: Kybernetická (ne)bezpečnost (2020)[36], zpracování: vlastní práce

[36] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky v Praze, 2020. s. 86.

Otázka KB je v rámci rychle se rozvíjejícího informačního a komunikačního sektoru stále aktuálnější. S postupujícím časem jsou využívány stále sofistikovanější informační a komunikační technologie. Zabezpečení a řízení KB se tak stává jedním z klíčových úkolů managementu v organizacích. Vzhledem k tomu, že všechny organizace musí zabezpečit a udržovat bezpečnost ve všech oblastech svého fungování, je toto téma zásadní.[37]

Poskytovatel služeb elektronických komunikací

Tímto poskytovatelem může být jakýkoli poskytovatel internetového připojení. ZoKB ukládá těmto subjektům pouze omezené povinnosti, jako je hlášení kontaktních údajů a dodržování opatření v případě kybernetického nebezpečí, která jsou stanovena NÚKIB.[38]

Orgán nebo osoba zajišťující významnou síť

Jde především o provozovatele významných páteřních komunikačních infrastruktur a vztahují se na ně stejná pravidla jako na poskytovatele, jak např. hlásit národnímu Computer Emergency Response Team (dále jen „CERT“) kontaktní údaje, kybernetické bezpečnostní incidenty (dále jen „KBI“), případně provádět reaktivní opatření za stavu kybernetického nebezpečí či nouzového stavu.[39]

Správce systému kritické informační infrastruktury

Správcem informačního a komunikačního systému (dále jen „IKS“) je systém orgánů nebo osoba, která určuje účel zpracování informací a podmínky provozování IKS. Těmto správcům jsou v rámci ZoKB uloženy povinnosti, jejichž plnění je stěžejní pro zajištění kybernetické bezpečnosti státu, zejména dodržování bezpečnostních opatření. Je tudíž nezbytné jednoznačně stanovit, kdo je k plnění těchto povinností vázán. Je zřejmé, že zodpovědnost nese ten, kdo určuje účel, principy a provoz daného systému.[40]

ZoKB na správce klade mnohem více povinností než poskytovatelům služeb elektronických komunikací, subjektům zajišťujícím síť elektronických komunikací

[37] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 9.

[38] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 75.

[39] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 206.

[40] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 73.

a osobám zajišťující významnou síť. To je způsobeno větší důležitostí těchto správců pro zabezpečení kybernetické bezpečnosti státu.[41]

U systémů KII jsou povinnosti výrazně rozšířeny. Stejně jako poskytovatelé musí nahlásit kontaktní údaje a dodržovat opatření vydaná NÚKIB. Nicméně, kromě toho musí hrát aktivní roli v detekci, dokumentaci a hlášení kybernetických bezpečnostních incidentů.[42]

Správce významného informačního systému

Správce má za povinnost jednak hlásit vládnímu CERT kontaktní údaje, kybernetický bezpečností incident, ale také implementovat a provádět bezpečnostní opatření, detekci kybernetických bezpečnostních událostí, provádět reaktivní a ochranná opatření.[43]

3.6 Systém zajištění kybernetické bezpečnosti

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Stále zřetelněji se projevuje závislost veřejného a soukromého sektoru na ICT. V dnešní době je sdílení a ochrana informací klíčová pro zabezpečení zájmů státu, obyvatelstva, ekonomiky a hospodářství. Přestože široká veřejnost nejčastěji vyjadřuje obavy finančních ztrát, úniku osobních dat a jejich zneužití, realita v oblasti KB je mnohem složitější. Existuje řada významných rizik, včetně kybernetické špionáže, ať už průmyslové, vojenské, politické či jiné, kde za těmito činnostmi stojí vlády a bezpečnostní orgány konkrétních států. Další nebezpečí představuje působení organizovaného zločinu v kyberprostoru, hacktivismus, cílená dezinformace s politickými nebo vojenskými záměry a potencionálně kyberterorismus. Aktuální hrozby nejsou omezeny pouze na časté kybernetické útoky prováděné za účelem např. ekonomického prospěchu. Dochází také k nechtěnému narušení sítí a bezpečnosti způsobené nezáměrně, například selháním lidského faktoru, živelnými katastrofami a dalšími faktory.[44]

[41] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 75.

[42] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 210.

[43] Tamtéž, s. 218.

[44] CDC DATA. *Co přináší NIS2 – nová směrnice o kyberbezpečnosti.* [online]. 2024 [cit. 2024-01-30]. Dostupné z: https://www.cdc.cz/cs/co-prinasi-nis2-nova-smernice-o-kyberbezpecnosti/.

3.6.1 Bezpečnostní opatření

Bezpečnostní opatření jsou ochranná opatření a postupy, které organizace, jednotlivci nebo subjekty přijímají k ochraně svých aktiv, informací, zařízení a infrastruktury před různými hrozbami a riziky. Dle ZoKB jsou rozdělena na organizační a technická. Tato opatření mají za cíl minimalizovat pravděpodobnost vzniku nebezpečných situací a maximalizovat reakci a odolnost v případě, že k takovým situacím dojde. Zahrnují různé strategie, technologie a pravidla, jež se v různých kontextech mohou lišit. Povinnosti, které se týkají zavedení systému bezpečnostních opatření, vycházejí z mezinárodně uznaných standardů. Netýkají se jen kategorií a funkčních parametrů jednotlivých typů bezpečnostních technologií, např. zavedením přístupových práv, logovacích nástrojů, kryptografických nástrojů. Patří sem rovněž organizace jednotlivých souvisejících procesů, zejména řízení lidských práv, ale také řízení akvizic nových technologií a organizační postupy pro řešení mimořádných událostí.[45]

Povinnost zavést a provádět bezpečnostní opatření není obecně uložena všem orgánům a osobám. Tuto povinnost mají pouze správci: informačního systému kritické infomační infrastruktury (dále jen „ISKII“), komunikačního systému kritické informační infrastruktury (dále jen „KSKII“), informačního systému základní služby (dále jen „ISZS“) a VIS. Jedná se IKS, jejichž provoz je klíčový pro zajištění kybernetické bezpečnosti státu. Bezpečnostní opatření nespočívá pouze v implementaci a dodržování, ale správci těchto systémů musí také vést a udržovat bezpečnostní dokumentaci.[46]

- ***Organizační opatření***

Organizační opatření stanovují požadavky na implementaci a provádění jednotlivých činností v rámci povinné osoby a její společnosti. Tyto činnosti jsou vzájemně propojené a jedna bez druhé by nezaručovala funkčnost systému bezpečnosti informací dané organizace. Proto je nezbytné řešit jejich implementaci napříč organizační strukturou povinné osoby.[47] Mezi organizační opatření ZoKB řadí:

a) „Systém řízení bezpečnosti informací,

b) řízení rizik,

[45] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 48.

[46] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 245.

[47] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 117.

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací,

i) řízení přístupu osob,

j) akvizice, vývoj a údržba,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit.“[48]

Zavedením organizačních opatření organizace prokazuje organizace svůj systémový přístup k ochraně kybernetické a informační bezpečnosti. Stanovení organizačních opatření poskytuje základ pro efektivní konfiguraci technických opatření a následné požití správných technických nástrojů ke splnění dosažení požadované úrovně KB v souladu se ZoKB.[49]

- ***Technická opatření***

Technická opatření a současně i protiopatření představují automatizované činnosti, které jsou prováděny IS prostřednictvím integrovaných mechanismů na zařízeních a jejich programech nebo na jejich částech.[50]

Technická opatření se od organizačních požadavků liší tím, že vyžadují od povinné osoby implementovat konkrétní opatření k ochraně daného subjektu před vnějšími hrozbami. I když často jedná o zavedení informačních a fyzických nástrojů, pravidel a postupů, které tyto činnosti provádějí, je na organizaci, jakým způsobem se rozhodne tyto požadavky naplnit.[51] ZoKB definuje jako technická opatření následující:

a)“Fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

[48] § 5 bod 2) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2014, částka 75.
[49] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 188.
[50] Tamtéž, s. 188.
[51] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 90.

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací,

l) bezpečnost průmyslových a řídicích systémů."[52]

Je nutné, aby každý provozovatel IKS, který může reálně nebo potencionálně ovlivnit chod státu, regionu, města nebo významné organizace, provedl následující kroky:

- ✓ provádět analýzu rizik;
- ✓ vypracovat plán minimalizace existujících rizik;
- ✓ navrhnout a implementovat preventivní opatření s cílem snížit identifikovaná rizika;
- ✓ monitorovat, vyhodnocovat a v případě potřeby upravit tato opatření.

3.6.2 Bezpečnost prvků kritické informační infrastruktury

Bezpečnost prvků KII je klíčovým aspektem pro zajištění stability, spolehlivosti a ochrany systémů a služeb, které jsou nezbytné pro fungování důležitých odvětví a minimalizaci rizik spojené s kybernetickými útoky a hrozbami. K zabezpečení těchto prvků lze využít sady bezpečnostních opatření, které můžeme nazvat druhy zajištění ochrany, jež jsou řazeny do jednotlivých oblastí.[53]

<u>*Personální bezpečnost*</u> – Personální bezpečnost se týká ochrany lidí pracujících v organizacích nebo institucích, a to jak fyzicky, tak i ohledně jejich kybernetického a informačního prostředí. Zahrnuje opatření zaměřená na zajištění jejich bezpečnosti, ochranu soukromí, a také prevenci a reakce na různé hrozby a rizika, která by mohla ohrozit

[52] § 5 bod 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2014, částka 75.

[53] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 42.

osobní integritu zaměstnanců nebo členů organizace. Je nezbytný řádný výběr osob, kteří mají pro organizaci pracovat. Organizace nesmí zanedbávat rozvoj jednotlivce, jeho výchovu a ochranu.

Průmyslová bezpečnost – Průmyslová bezpečnost je zaměřena na ochranu průmyslových zařízení, infrastruktury a procesů před různými oblastmi a hrozbami. Cílem průmyslové bezpečnosti je minimalizovat nebezpečí pro pracovníky, zařízení a životní prostředí a zabezpečit plynulý provoz průmyslových aktivit. Organizace pro svou činnost obvykle využívá nějaký komerční subjekt k výkonu svých činností, které nejsou součástí vlastního portfolia. V této souvislosti je důležité, aby každá organizace měla jasné povědomí o svých spolupracovnících, co jim umožňuje, kam mají přístup a jaké informace mohou získat.

Administrativní bezpečnost – Administrativní bezpečnost se týká opatření a postupů, které organizace a instituce provádějí k ochraně svých informací, zařízení a operací. Jedná se o řízení a správu bezpečnostních opatření prostřednictvím administrativních postupů, politik a pravidel. Administrativní bezpečnost hraje klíčovou roli při minimalizaci rizik a zajištění toho, že bezpečnostní opatření jsou prováděna a dodržována v celé organizaci. Pro správné fungování organizace je klíčové vytvořit systém opatření týkající se všech fází práce s informacemi, jako je tvorba, příjem, evidence, zpracování, odesílání, přeprava, sdílení, ukládání, archivace, případně dalších manipulací s informacemi.[54]

Fyzická bezpečnost – Fyzická bezpečnost se týká ochrany fyzických prostorů, zařízení, osob a majetku před neoprávněným přístupem, krádeží, poškozením nebo jinými nebezpečnými situacemi. Jedná se o opatření na zajištění bezpečnosti fyzických osob, které v těchto prostorách fungují nebo se pohybují. Fyzická bezpečnost hraje klíčovou roli při minimalizaci rizik a ochraně hodnotných zdrojů. Vlastní ochrana majetku organizace je souborem opatření, jehož cílem je omezit neoprávněným osobám přístup k majetku či informacím organizace, popřípadě se snažit o monitorování jakéhokoli pokusu nebo neoprávněného přístupu.

Bezpečnost informačních a komunikačních systémů – Bezpečnost IKS se týká ochrany digitálních dat, komunikačních kanálů, softwaru a hardwaru před kybernetickými hrozbami, zneužitím a neoprávněným přístupem. S narůstající digitalizací a propojeností organizací

[54] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 42.

a společností je bezpečnost IKS klíčová pro zajištění ochrany důvěrných informací, ochranu soukromí a udržení provozu kritických funkcí. Klíčová opatření systému se zaměřují na zajištění tří základních aspektů informací, s nimiž tyto systémy nakládají, a tím je důvěrnost, integrita a dostupnost. A zároveň i odpovědnost správy a uživatelů za jejich činnost v rámci informačního nebo komunikačního systému.

Kryptografická ochrana – Kryptografická ochrana je způsob, jakým způsobem se využívá kryptografie, tedy matematické techniky, pro zabezpečení komunikace, dat a informací. Kryptografie se používá k zašifrování dat tak, aby byla nečitelná pro ty, kteří nemají správný dešifrovací klíč. Tato metoda zajišťuje soukromí, integritu a autentizaci dat a komunikace. Je tvořena systémem opatření určených k ochraně informací. Tato opatření zahrnují využití kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání informací organizace.

Základním prvkem je především IS a jeho zabezpečení. V éře propojenosti firem prostřednictvím telekomunikační sítě internet, mobilních uživatelů a elektronického obchodování je nedílnou součástí návrhu IS i jeho zabezpečení. Tuto část systému nelze od ostatních zcela oddělit a musí být plně souladu s ostatními částmi celého IS. [55]

3.6.3 Kybernetická hrozba

Hrozbu lze jednoduše popsat jako potenciální událost nebo situaci, která má schopnost vyvolat neobvyklý nebo nepříznivý vývoj událostí a ovlivnit práva jiných subjektů. Jde o negativní chování, které může, ale nemusí být dokončeno.[56] VoKB v příloze č. 3 uvádí některé z hrozeb. Dle této vyhlášky je hrozbou:

- *„Porušení bezpečnostní politiky, provedení neoprávněních činností, zneužití oprávnění ze strany uživatelů a administrátorů;*
- *poškození nebo selhání technického anebo programového vybavení;*
- *zneužití identity;*
- *užívání programového vybavení v rozporu s licenčními podmínkami;*
- *škodlivý kód (například viry, spyware, trojské koně);*
- *narušení fyzické bezpečnost;*

[55] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 42, 43.

[56] KOLOUCH, J., BAŠTA, P., a kol., *CyberSecurity.* Praha: CZ.NIC, 2019. s. 74.

- *přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie;*
- *zneužití nebo neoprávněná modifikace údajů;*
- *ztráta, odcizení nebo poškození aktiva;*
- *nedodržení smluvního závazku ze strany dodavatele;*
- *pochybení ze strany zaměstnanců;*
- *zneužití vnitřních prostředků, sabotáž;*
- *dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb;*
- *nedostatek zaměstnanců s potřebnou odbornou úrovní;*
- *cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik;*
- *zneužití vyměnitelných technických nosičů dat;*
- *napadení elektronické komunikace (odposlech, modifikace).“*[57]

3.6.4 Kybernetická bezpečnostní událost

Kybernetická bezpečnostní událost se týká jakékoli události nebo incidentu, který může ohrozit bezpečnost, integritu, dostupnost nebo soukromí IS, dat nebo služeb. Tyto události mohou zahrnovat různé druhy kybernetických hrozeb, útoků nebo incidentů, které mají negativní dopad na organizace, firmy nebo jednotlivce.[58]

ZoKB ukládá určitým osobám povinnost detektovat bezpečnostní události. Těmito subjekty jsou orgány nebo osoby zajišťující významnou síť, správci ISKII, správci KSKII, správci ISZS a VIS. Těmto subjektům je uložena povinnost detekovat kybernetickou bezpečnostní událost.[59]

3.6.5 Kybernetický bezpečnostní incident

KBI již představuje skutečné narušení bezpečnosti informací nebo služeb v IKS s negativním dopadem. Tento incident může zahrnovat neoprávněný přístup, zneužití dat,

[57] Příloha č. 3 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. rok 2018, částka 43.

[58] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 300.

[59] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 100.

výpadek služeb nebo jiné hrozby, které mohou mít negativní dopad na organizaci, jednotlivce nebo společnost. KBI mohou mít různou závažnost a následky a vyžadují rychlou a koordinovanou reakci.[60]

Z formulace zákona vychází, že incident může být zapříčiněn jak úmyslným, tak nedbalostním jednáním člověka, ale i vyšší mocí. Klíčové je, že dojde k narušení bezpečnosti informací, nebo služeb a IKS s nimi spojených. Za určitou část KBI mohou také náhodné jevy, poruchy hardwaru, softwaru, konfigurační chyby prováděné administrátory či chyby uživatelů systémů aj.[61]

V současné době patří kybernetické incidenty za jedny z nejzávažnějších rizik a hrozeb pro společnost ve všech vyspělých zemích světa.[62] Je povinností správcem KII jednotlivé KBI stanoveným způsobem hlásit provozovateli národního CERT nebo NÚKIB.[63]

3.6.6 Kybernetický útok

Kybernetický útok je záměrný pokus o proniknutí do IS, sítě, zařízení nebo dat za účelem narušení, poškození, krádeže, zneužití nebo odcizení informací. Nejčastěji se používá v kontextu vojensky či politicky motivovaných útoků.[64]

Tato hrozba může zahrnovat širokou škálu technik, metod a strategií, které útočníci využívají k dosažení svých cílů. Kybernetické útoky se liší dle své povahy, cíle a způsobu provedení. Útočníci v současné době nepotřebují fyzický kontakt s vlastními technologiemi. Díky globálnímu propojení mají schopnost operovat z kterékoli části světa a díky řadě serverů po celém světě dosáhnout prakticky anonymity. Moderní strategie kybernetických útoků se dynamicky vyvíjí spolu s vývojem technologií. Tyto útoky se netýkají pouze málo chráněným jednotlivcům či lépe zabezpečených korporací, ale také zahrnují masivní útoky na kritickou infrastrukturu, které mohou zásadně ovlivnit obranné systémy či ekonomiku. V posledních několika letech se kyberprostor rychle rozrůstá a stává se zároveň zranitelnějším, protože obsahuje značné množství dat, často kritických.[65]

---

[60] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity,* Praha: CZ.NIC, 2019. s. 301.

[61] Tamtéž, s. 82.

[62] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky v Praze, 2020. s. 30.

[63] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 100.

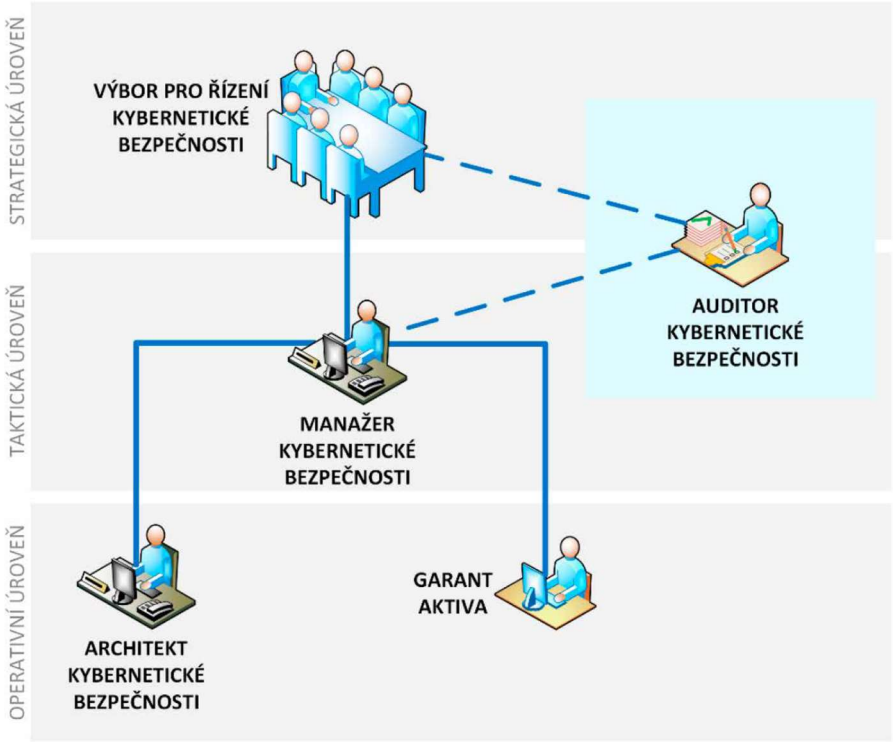
[64] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 100.

[65] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity,* Praha: CZ.NIC, 2019. s. 82.

3.7 Bezpečnostní role

Bezpečnostní role jsou definované role v souladu se ZoKB, znázorněny následujícím obrázkem a podrobně popsány v Příloze č. 6 VoKB.[66]

Obrázek 3 Bezpečnostní role



Zdroj: NÚKIB (2020)[67], zpracování: převzato

3.7.1 Výbor pro řízení kybernetické bezpečnosti

Jde o skupinu zpravidla interních odborníků nebo manažerů v organizaci, která je zodpovědná za strategické rozhodování, celkový dohled, řízení a rozvoj systému řízení bezpečnosti informací (dále jen „ISMS“). Jeho hlavním cílem je zajistit organizaci efektivní a koordinovaný přístup k ochraně svých IS, dat a aktiv před kybernetickými hrozbami a útoky.[68]

[66] Příloha č. 6 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), In: *Sbírka zákonů,* rok 2018, částka 43.

[67] Národní úřad pro kybernetickou a informační bezpečnost. Hierarchie bezpečnostních rolí. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. 2020 (PDF). [cit. 2023-08-27]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf.

[68] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 267.

3.7.2 Manažer kybernetické bezpečnosti

Manažer KB je klíčová role v organizaci, která má na starosti plánování, implementaci a dohled nad KB. Tato role má za úkol zajistit ochranu IS, sítí, dat a dalších kybernetických aktiv organizací před různými kybernetickými hrozbami a útoky.[69]

3.7.3 Architekt kybernetické bezpečnosti

Architekt KB je odborník, který se specializuje na návrhy a implementaci komplexních a efektivních bezpečnostních architektů a opatření v IS, sítích a infrastruktuře organizací. Tato role zahrnuje zodpovědnost za navrhování a implementaci strategií, které zajišťují ochranu před různými kybernetickými hrozbami a útoky. Jde o osobu, která má odbornou kvalifikaci pro tuto činnost a prokazuje svoji způsobilost prostřednictvím praxe.[70]

3.7.4 Auditor kybernetické bezpečnosti

Auditor KB je profesionál, který se specializuje na nezávislé a objektivní hodnocení a kontrolu bezpečnosti IS, sítí a procesů organizace. Hlavním cílem auditorské činnosti je zjistit, zda organizace dodržuje stanovené bezpečnostní standardy, postupy a regulace, a zjistila případné nedostatky nebo rizika v oblasti KB. Jde o osobu, která prošla odborným školením pro tuto činnost a dokazuje svou odbornou způsobilost praxí v oblasti provádění auditů KB.[71]

3.7.5 Garant aktiva

Termín "garant aktiva" se obvykle vztahuje k ochraně a zabezpečení určitého aktiva, jako jsou informace, majetek nebo další cenné prostředky. Garantem aktiva je osoba nebo entita, která je zodpovědná za zajištění bezpečnosti a ochrany tohoto aktiva před různými hrozbami a neoprávněným přístupem. Tato role zahrnuje monitorování, kontrolu a přijímání opatření k minimalizaci rizik.[72]

---

[69] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 56.

[70] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 25.

[71] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 57.

[72] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 271.

3.8 Hlášení kybernetického bezpečnostního incidentu

Jedním z hlavních cílů ZoKB je zajistit detekci kybernetických bezpečnostních událostí a následné hlášení KBI v KII a ve VIS. Tímto způsobem má být umožněna rychlá a efektivní reakce orgánů a subjektů ve spolupráci s vládním CERT. Vybrané skupiny orgánů a osob, konkrétně správci informačních nebo komunikačních systémů KII a správci VIS, mají povinnost nejen detekovat výskyt kybernetických bezpečnostních událostí pomocí příslušných bezpečnostních opatření, ale také povinnost následně nahlásit a předat údaje o zjištěných KBI vládnímu CERT. Vládní CERT po provedení potřebných analýz včetně ověření, zda incident nebyl hlášen současně z více zdrojů či různých částí KII nebo z VIS, zvolí další vhodné kroky v souladu s významem a rozsahem daného KBI.

ZoKB stanovuje osoby a orgány, které jsou povinny hlásit KBI. Tyto jištěné incidenty, které jsou vyhodnoceny jako KBI, je nutné bez prodlení nahlásit. Informace zpracovávané vládním CERT na základě hlášení KBI jsou vedeny v evidenci KBI, chráněny povinností mlčenlivosti a zpřístupněny k omezenému užití vybraným orgánům veřejné moci, národnímu CERT, orgánům vykonávajícím působnost v oblasti KB v zahraničí a jiným subjektům působícím v oblasti KB v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.[73]

Povinné osoby dle ZoKB mají povinnost hlásit KBI buď národnímu či vládnímu CERT, a to bezodkladně po jeho detekci.[74] Hlášení zahrnuje klíčové údaje, jako je klasifikace závažnosti incidentů, jeho typ, počet dotčených systémů a uživatelů nebo IP adresu systému. Součástí je také podrobný popis samotného incidentu a provedených reaktivních opatření. Pokud osoba povinná k oznámení nedodrží svou povinnosti, hrozí jí pokuta do výše 100 tisíc korun. Za neposkytnutí kontaktních údajů může být uložena pokuta až do výše 10 tisíc korun. Formulář je dostupný na webové adrese https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf.[75]

NÚKIB může sdílet informace o nahlášených incidentech s dalšími orgány veřejné správy v případech, kdy je to nebytné pro plnění úkonů v rámci jejich působnosti. Dále může NÚKIB sdílet informace také s obdobnými institucemi v jiných zemích a dalšími

[73] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 49.

[74] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 305.

[75] Národní úřad pro kybernetickou a informační bezpečnost. *Hlášení incidentů.* [online]. 2014 [cit. 2023-08-27]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/.

bezpečnostními subjekty, pokud to přispěje k ochraně kybernetického prostoru. V těchto případech jsou však data anonymizována tak, aby z nich nebylo možné identifikovat původce.

3.9 Evidence

Důkazy v kontextu KB se týkají sběru a uchovávání informací o kybernetických událostech, hrozbách, útocích a opatřeních, která jsou relevantní pro analýzu, vyšetřování a zlepšování bezpečnostních postupů. Správná evidence je klíčová pro pochopení, jaké události se staly, jaký byl dopad a jak lze zlepšit preventivní opatření.[76]

NÚKIB má dle ZoKB povinnost vést evidenci KBI. Součástí evidence těchto incidentů je:

- Vlastní hlášení KBI obsahující identifikaci odesílatele, datum a čas zjištění incidentu a popis incidentu;
- Identifikační údaje počítačového systému, proti kterému KBI směřoval;
- Údaje o zdroji či příčině KBI;
- Postup popisující řešení incidentu a jeho výsledek a další.[77]

Je nezbytné evidovat tyto údaje o KBI, zejména s ohledem na stanovení strategických postupů pro zajištění ochrany kybernetické bezpečnosti státu.

Údaje v databázi kybernetických bezpečnostních incidentů, kterou spravuje NÚKIB, mohou být v souladu se zákonem sdíleny s dalšími orgány veřejné moci. Mimo orgány veřejné moci, které mají pravomoc přístupu k těmto údajům v rámci své působnosti, mohou být tato data také předána dalším subjektům. Tato skupina zahrnuje provozovatele národního CERT, zahraniční orgány vykonávající působnost v oblasti KB a další osoby působící v této oblasti. Údajů mohou být sdíleny pouze v takovém rozsahu, který je nebytný pro zajištění ochrany kybernetického prostoru.[78]

[76] MAISNER, M., VLACHOVÁ, B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 105.

[77] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 312.

[78] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 106.

3.10 Opatření

Opatření v kontextu KB jsou preventivní, detekční nebo reaktivní kroky, které organizace, firmy a jednotlivci přijímají k ochraně svých IS, dat, sítí nebo služeb před kybernetickými hrozbami a útoky. Správná implementace bezpečnostních opatření je klíčová pro minimalizaci rizika kybernetických incidentů a zabezpečení digitálního prostoru.[79]

Opatření lze rozdělit do tří kategorií, a to na:

Varování

Varování je základním nástrojem opatření, které provádí NBÚ. Jde především o upozornění na možné hrozby, rizika nebo potenciální nebezpečí v digitálním prostoru. Tato varování mají za cíl informovat uživatele, organizace nebo veřejnost o aktuálních kybernetických hrozbách a poskytnout jim doporučení nebo kroky k prevenci a ochraně.[80]

Reaktivní opatření

Dalším z opatření, které slouží k ochraně a zabezpečení IKS, je reaktivní opatření. Tato opatření se týkají kroků, které organizace nebo jednotlivci podnikají pro zjištění kybernetického incidentu nebo útoku a jsou zaměřena na zastavení škod, minimalizaci dopadů a obnovu normálního provozu. Toto opatření má za cíl ochránit IS, služby a elektronické komunikační sítě před kybernetickými bezpečnostními událostmi či incidenty nebo aktivně řešit takové incidenty.[81]

Vykonávání reaktivních opatření je svěřeno příslušným povinným orgánům a osobám. Pro různé subjekty existuje rozdílný katalog povinností spojených s implementací reaktivních opatření. Povinnost provést reaktivní opatření je v plném rozsahu uložena správcům ISKII, KSKII a VIS.[82]

---

[79] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 109.

[80] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 200.

[81] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 112.

[82] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 320.

Ochranné opatření

Posledním z opatření dle ZoKB je ochranné opatření. Toto opatření je vydáváno formou opatření obecné povahy zaměřené na posílení bezpečnosti IKS, stejně jako služby a sítě elektronických komunikací. Mají za cíl ochránit IS, sítě, data a zařízení před neautorizovaným přístupem, zneužitím a poškozením. Jednotlivá opatření se provádí na základě vyhodnocení již vyřešeného KBI.[83]

Realizace ochranných opatření je pověřena příslušnými povinnými orgány a osobami. Katalog povinností spojený s implementací ochranných opatření, je individuální pro jednotlivé orgány a osoby. Zodpovědnost za provedení těchto opatření leží zcela na správcích ISKII, KSKII a VIS.[84]

3.11 Stav kybernetického nebezpečí

Stav kybernetického nebezpečí je termínem, který označuje situaci ohrožení bezpečnosti informací v IKS nebo aktuální míru rizika spojenou s kybernetickými hrozbami a útoky. Ohrožení musí dosáhnout takového rozsahu, kdy by mohlo narušit zájmy ČR, především jejích klíčových atributů – ústavnosti, územní jednotnosti a svrchovanosti, jakož i zajištění vnitřní a vnější bezpečnosti státu. Dále se také chrání ekonomika země a životní podmínky jednotlivců. Aktivace stavu kybernetického nebezpečí je posledním a nejzazším opatřením, které je platné v okamžiku, kdy nastalou situaci nelze vyřešit jinými prostředky.[85]

Vyhlásit stav kybernetického nebezpečí je oprávněn ředitel NÚKIB. Po dobu trvání tohoto stavu musí ředitel NBÚ informovat vládu o opatřeních k řešení situace a aktuálního stavu ohrožení, které vedly k vyhlášení tohoto stavu. Vyhlašuje se na dobu, která je nezbytně nutná, nejdéle však na 7 dnů s možností prodloužení. Souhrnná doba trvání však nesmí přesáhnout 30 dnů. Tato informace je zveřejněná na úřední desce NÚKIB a prostřednictvím rozhlasového a televizního vysílání.[86]

Pokud není možné odvrátit ohrožení bezpečnosti informací v IS, bezpečnosti služeb nebo integrity sítí elektronických komunikací v rámci vyhlášeného stavu kybernetického

[83] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 114.

[84] Tamtéž, s. 106.

[85] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 180.

[86] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 88.

nebezpečí, může ředitel NÚKIB požádat vládu o vyhlášení nouzového stavu. Stav kybernetického nebezpečí bude ukončen po uplynutí doby, na kterou byl vyhlášen, jeho zrušením nebo vyhlášením nouzového stavu.[87]

3.12 Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB je správním orgánem státní správy, který se zabývá koordinací a řízením opatření v oblasti kybernetické a informační bezpečnosti v dané zemi. NÚKIB má za úkol monitorovat kybernetické hrozby, analyzovat bezpečnostní rizika, poskytovat rady a doporučení pro ochranu proti kybernetickým hrozbám a spolupracovat s jinými subjekty v oblasti KB. Je také zároveň národním a vládním CERT týmem.[88]

Mezi klíčové pravomoci NÚKIB patří:

- *„Kybernetická bezpečnost;*
- *ochrana utajovaných informací pro oblast informačních a komunikačních systémů;*
- *kryptografická ochrana;*
- *problematika veřejně regulované služby navigačního systému Galileo (PRS).“*[89]

Na oficiální webové stránce NÚKIB jsou přístupné informace o kybernetických hrozbách prostřednictvím hlášení[90], dále nabízí doporučení pro řešení konkrétních situací[91] a zahrnuje také mnoho metodik a návodů.[92]

Každoročně publikuje NÚKIB Zprávu o stavu KB, která zahrnuje celou řadu kapitol týkající se činnosti úřadu, včetně odborných příloh, statistik a přehled hlášení.[93]

---

[87] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 323.

[88] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. s. 53.

[89] Národní úřad pro kybernetickou a informační bezpečnost. *O úřadu* [online] 2017 [cit. 2023-08-20]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/.

[90] Tamtéž, *Hrozby*. [online] 2017 [cit. 2023-08-20] Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/.

[91] Tamtéž, *Doporučení*. [online]. 2017 [cit. 2023-08-20] Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/.

[92] Tamtéž, *Podpůrné materiály*. [online]. 2017 [cit. 2023-08-20] Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

[93] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. s. 64.

Pro oblast KB lze uvažovat o použití nástroje strategického plánování a tím je SWOT analýza. Tato analýza spočívá v rozboru a hodnocení současného stavu ochrany KII, která je znázorněna v následující tabulce.

Tab. 1 SWOT analýza ochrany kritické informační infrastruktury

SILNÉ STRÁNKY	SLABÉ STRÁNKY
✓ Existence speciálního zákona ✓ Národní úřad pro kybernetickou a informační bezpečnost jako ústřední orgán a vládní a národní CERT ✓ Mezinárodní spolupráce a cvičení ✓ Velké množství CSIRT/CERT týmů v rámci České republiky ✓ Národní centrála proti organizovanému zločinu; sekce kyberkriminality ✓ Členství v Evropské agentuře pro bezpečnost sítí a informací a v dalších platformách	✓ Omezené finanční prostředky ✓ Nedostatek specialistů v oblasti informačních technologií ✓ Neochota hlásit kybernetické incidenty ✓ Podceňování kybernetických hrozeb ve státní správě ✓ Nízká připravenost na kyber-terorismus
PŘÍLEŽITOSTI	**HROZBY**
✓ Vzdělávání, školení ✓ Nábor a motivace odborníků ve státní správě ✓ Spolupráce se soukromým sektorem ✓ Dohody o spolupráce s Policí ČR	✓ Domino efekt ✓ Snadná dostupnost malware ✓ Nekázeň uživatelů ✓ Zranitelnost mobilních platforem ✓ Hardware trojani, zranitelnost internetu věcí

Zdroj: KOLEKTIV AUTORŮ (2020)[94], zpracování: vlastní práce

V rámci SWOT analýzy je užitečné hledat vzájemné vztahy mezi silnými a slabými stránkami, stejně jako příležitostmi a hrozbami. Tyto identifikované synergie lze následně využít pro formulaci strategie a rozvoje v oblasti ochrany KII.[95]

3.13 CERT týmy

Zákon ukládá zřízení dvou dohledových pracovišť, a to národního a vládního CERT, jejichž úkolem je vyhodnocování kybernetické bezpečnostní situace v IKS. Zároveň sem

[94] KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. s. 69.

[95] HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerprint, 2018. s. 62.

patří i ochrana těchto systémů před KBI. Základním smyslem fungování obou dohledových pracovišť je vyhodnocování informací o výskytu KBI.[96]

Koncept dvojího centrálního dohledového pracoviště zajistí ČR výhody díky kombinaci a využití užitečných informací z obou zmíněných oblastí, a to zejména formou výměny informací o řešení KBI. Obě dohledová pracoviště se můžou vzájemně podílet a spolupracovat na projektech výzkumu a vývoje, vzdělávání a dalších relevantních oblastech.[97]

Národní CERT

Národní CERT je specializovaný tým nebo organizace, která má za úkol reagovat na kybernetické incidenty, koordinovat bezpečnostní události a poskytovat podporu v oblasti KB na národní úrovni. Národní CERT funguje jako centrální bod pro sběr, analýzu a distribuci informací o kybernetických hrozbách a incidentech a podporuje různé subjekty v zemi v boji proti kybernetickým hrozbám.[98]

Vládní CERT

Vládní CERT je specializovaný tým nebo organizace, která má za úkol zabezpečovat KB, zpracovávat data o výskytu a řešení KBI a reagovat na kybernetické hrozby v rámci vládních a státních institucí. Případný únik těchto dat by mohl ohrozit bezpečnostní zájmy, práva orgánů a osob ČR.

Do evidence KBI jsou zahrnuty údaje týkající se původu KBI, údaje z hlášení o příslušném incidentu, včetně identifikačních údajů systému, ve kterém se zmiňovaný incident vyskytl. Tyto údaje podléhají povinnosti mlčenlivosti a jejich sdílené je možné pouze v omezeném rozsahu na základě výslovného zákonného oprávnění k poskytování dat. Pro potřeby vládního nebo národního CERT jsou následně zpracovány údaje týkající se jednotlivých KBI. Nejcitlivější částí těchto evidencí jsou statistická dat o frekvenci útoků na jednotlivé systémy, sítě a služby elektronických komunikací, a také data o způsobech řešení těchto incidentů.[99]

---

[96] MAISNER, M., VLACHOVÁ, B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 49.

[97] Tamtéž, s. 51.

[98] KROPÁČOVÁ, A. *CERT/CSIRT týmy a jejich role*. *Root.cz: Informace nejen ze světa Linuxu.* [online]. 2013 [cit. 2023-08-20]. Dostupné z: http:/www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

[99] MAISNER, M., VLACHOVÁ B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, 2015. s. 18.

3.14 Audity a bezpečnostní testování

Za účelem ověření stavu bezpečnosti informačního prostředí je nezbytné provádět bezpečnostní audity, které mají za cíl komplexně posoudit bezpečnost ve všech oblastech, včetně nastavení bezpečnostních charakteristik systémů s ohledem na osvědčené postupy a platnou legislativu. Například v reakci na nedávné změny v oblasti ochrany osobních údajů se tyto testy v současnosti často zaměřují na dodržování požadavků v souladu s GDPR. V případě orgánů veřejné správy pak uvedené audity zkoumají soulad s legislativou, jako je ZoKB. To zahrnuje zhodnocení bezpečnostních politik, směrnic, systému řízení a technických opatření odpovídající uvedenému zákonu. Dále mohou zkoumat bezpečnostní procesy a jejich nastavení, včetně náplně a obsazení bezpečnostních rolí. V technické oblasti jde většinou o zajištění stavu hardware nebo software, zabezpečení dat, konfigurace bezpečnostních prvků, bezpečnostního monitoringu a jeho nastavení, prověření vzdáleného přístupu nebo přístupu privilegovaných uživatelů. Někdy se audit zaměřuje i na kontrolu fyzické bezpečnosti nebo se soustředí na hodnocení prostředí třetích stran, včetně dodavatelů, a to i na bezpečnost jejich vývoje, kódování, případně interní nebo externí personální spolehlivost nebo hodnotí úroveň bezpečnostního povědomí a úroveň interního systému školení v oblasti informační bezpečnosti. Existují také specializované typy auditů, jako jsou penetrační testy, skeny zranitelností nebo testy odolnosti proti sociálnímu inženýrství, které provádějí praktické ověření reálného stavu v prostředí organizace.[100]

Audit kybernetické bezpečnosti

Audit KB je definován ZoKB jako systematický proces vyhodnocování, zjišťování a posuzování úrovně zabezpečení IS, sítí, aplikací a datových infrastruktur organizace.[101] Cílem tohoto procesu je identifikovat zranitelnost, nedostatky a hrozby spojené s KB a navrhnout opatření na zvýšení úrovně ochrany a minimalizace rizik.

VoKB dále stanovuje, že provádění auditu bude v pravidelném intervalu 2 nebo 3 let v závislosti na typu povinné osoby, a také bude prováděn významných změnách. Vyhláška umožňuje průběžný audit, ale v takovém případě musí být audit v celém rozsahu proveden

[100] § 25 odst. 1 písm. a) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In.: *Sbírka zákonů,* rok 2018, částka 43.

[101] § 5 odst. 2 písmeno m) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2014, částka 75.

do 5 let.[102] Audit KB může provádět pouze osoba, která splňuje požadavky pro bezpečnostní roli auditora KB. Požadavek na provedení auditu KB je specifikováno v § 3 písm. f). VoKB.[103]

Normy vztahující se k auditu kybernetické bezpečnosti

Bezpečnost informací se týká řada norem ISO (International Organization for Standardization – Mezinárodní organizace pro normalizaci) a norem IEC (International Electrotechnical Commission – Mezinárodní elektrotechnická komise).[104]

Z pohledu informační a kybernetické bezpečnosti jsou využívány především následující normy:

- *ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky*

Mezinárodně uznávaná norma ČSN ISO/IEC 27000 poskytuje základní přehled o ISMS, termínech a definic, které jsou obecně používány v rámci řady norem týkající se ISMS.[105]

- *ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky*

Tato mezinárodní norma byla vypracována s cílem poskytnout podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování v rámci systému řízení bezpečnosti informací. Přijetí systému by mělo být strategickým rozhodnutím organizace. Návrh a implementace ISMS v organizaci je podmíněno potřebami a cíli této organizace, stejně jako specifickými bezpečnostními požadavky, procesy, velikostí a strukturou organizace.[106]

---

[102] § 16 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), In: *Sbírka zákonů,* rok 2018, částka 43.

[103] § 3 písm. f) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), In: *Sbírka zákonů,* rok 2018, částka 43.

[104] KOLOUCH, J., BAŠTA, P., a kol., *CyberSecurity.* Praha: CZ.NIC, 2019. s. 46.

[105] SEDLÁK, P., KONEČNÝ, M., a kol., *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 24.

[106] KOLOUCH, J., BAŠTA, P. *CyberSecurity.* Praha: CZ.NIC, 2019. s. 46.

- *ČSN ISO/IEC 27002:2016 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci ISMS*

Tato norma poskytuje pokyny pro implementaci a provoz ISMS. Obsahuje návody a obecné zásady pro návrh, implementaci, udržení a zlepšení řízení ISMS v rámci organizace. Výběr opatření v rámci procesu zavádění ISMS vychází z předcházející normy ISO/IEC 27001.

- *ČSN ISO/IEC 27006:2016 Informační technologie – Bezpečnostní techniky – Požadavky na provádějící audit a certifikaci ISMS*

Norma ISO/IEC 27006:2015 je mezinárodně uznávaná norma, která se zaměřuje na provádění auditů bezpečnosti IS. Tato norma definuje konkrétní požadavky týkající se schopnosti a nezávislosti osob, které provádějí certifikační a akreditační auditní činnosti související s ISMS dle normy ISO/IEC 27001.

Tato norma podrobně specifikuje požadavky a poskytuje doporučení pro organizace a subjekty provádějící audit a certifikaci ISMS. Jejím hlavním účelem je zejména podpora procesu akreditace certifikačních orgánů poskytující certifikace ISMS. Dále může být použita jako referenční dokument pro proces akreditace, pro interní hodnocení nebo pro jiné auditní procesy související s bezpečností informací.[107]

- *ČSN ISO/IEC 27007:2020 Informační technologie – Bezpečnostní techniky – Směrnice pro audit ISMS*

Norma ISO/IEC 27007:2020 poskytuje rámec a směrnice pro provádění auditů ISMS a hodnocení, a to v souladu s normou ISO/IEC 27001. Tato norma podporuje auditní týmy a profesionály v oblasti KB při zlepšování auditních postupů a zajišťování konzistence, objektivity a účinnosti auditních procesů.[108]

Předmět auditu

Předmětem auditu je zkoumání a zjišťování konkrétní oblasti. V rámci kontextu KB a auditů IT je předmětem auditu především soubor IS, procesů, technologií nebo postupů, které budou podrobeny důkladné analýze a hodnocení. Na začátku auditu je klíčové přesně definovat předmět auditu, což by mělo odrážet cíle a požadavky organizace. Klíčové

[107] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 294.
[108] Tamtéž, s. 295.

je stanovit rozsah auditu tak, aby umožnil podrobnou analýzu, aniž by byl proces příliš rozsáhlý nebo naopak příliš omezený.[109]

Audit může zahrnovat různé aspekty KB, patří sem:

Informační systémy: Prověření zabezpečení konkrétních systémů, aplikací nebo databází.

Sítě: Provedení analýzy zabezpečení s důrazem na síťovou infrastrukturu, včetně firewallů, routování a bezdrátových sítí.

Datová úložiště: Posouzení bezpečnosti serverů, datových center a cloudových úložišť.

Ochrana dat: Prověřování metody šifrování, zálohování, správy přístupu a další relevantní faktory spojené s ochranou dat.

Identifikace a autentizace: Hodnocení procesů pro správu přihlašování, dvoufaktorové autentizace a identifikace uživatelů.

Zranitelnosti a penetrační testování: Identifikace zranitelnosti v systémech a realizace penetračních testů za účelem odhalení slabých míst.

Bezpečnostní politiky a postupy: Hodnocení shody s bezpečnostními politikami, směrnicemi a postupy dané organizace.

Reakce na incidenty: Prověření postupů reakce na kybernetické incidenty a mimořádné situace.

Odbornost týmu a kompetence: Posouzení schopností a znalostí členů auditorského týmu.

Soulad s normami a regulacemi: Zhodnocení, zda organizace splňuje požadavky příslušných norem, regulací nebo standardů v rámci kybernetické bezpečnosti.[110]

[109] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 295.

[110] Tamtéž, s. 296.

Klíčové prvky auditu kybernetické bezpečnosti

Klíčové prvky auditu KB zahrnují:

Identifikace zranitelnosti: Provádění technických skenů, testů proniknutí a zranitelností analýzy k odhalení existujících zranitelností v systémech a sítích.

Hodnocení opatření: Posouzení účinnosti stávajících kybernetických bezpečnostních opatření a politik.

Zjištění hrozeb: Identifikace aktuálních hrozeb a rizik spojených s KB včetně nových typů útoků a technik.

Kontrola: Ověření, zda jsou kybernetická bezpečnostní opatření v souladu s příslušnými normami, regulacemi a požadavky.

Analýza incidentů: Zhodnocení historických kybernetických incidentů, které mohou poskytnout informace o zranitelnostech a slabých bodech.

Ověření postupů: Posouzení toho, jak organizace reaguje na kybernetické hrozby a incidenty, včetně testování reakčních postupů a plánů.

Zpracování zjištění: Shromažďování, dokumentace a analýza výsledků auditu ke zjištění nedostatků a návrhu nápravných opatření.

Doporučení: Navrhování konkrétních opatření pro zlepšení KB a snížení identifikovaných rizik.

Kontrola kvality: Zajištění, že audit byl proveden systematicky, objektivně a při dodržení nejlepších postupů auditního procesu.

Sdílení výsledků: Prezentace výsledků auditu vedoucím pracovníkům a relevantním oddělením. A následná komunikace o opatřeních a změnách.

Cílem auditu KB je poskytnout organizaci objektivní pohled na současný stav svého zabezpečení, identifikovat slabiny a navrhnout strategii pro zvýšení úrovně ochrany. Je nezbytným nástrojem pro zajištění, že organizace je schopna efektivně reagovat na neustále se vyvíjející hrozby v kybernetickém prostoru.

Výsledky auditu slouží jako základ pro identifikaci nedostatků, doporučení, zlepšení a posouzení souladu s předepsanými normami, standardy nebo právními předpisy.[111]

[111] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost.* Praha: CERM, 2021. s. 295.

Kritéria auditu

Jde o soubor politik, postupů nebo požadavků, zahrnující směrnice, normy, bezpečnostní politiky, zákonné požadavky, které slouží jako referenční rámec pro srovnání s důkazy z provedeného auditu. Tyto reference slouží jako základní měřítko pro posouzení shody nebo souladu a mohou zahrnovat relevantní politiky, stanovené cíle, postupy, normy, legislativní požadavky, požadavky systémů managementu, smluvní požadavky, odvětvová pravidla chování nebo jiná plánovaná opatření[112].

V kontextu KB mohou kritéria auditu zahrnovat:

Normy a standardy: Jde o mezinárodně uznávané nebo interní normy, které určují požadavky týkající se KB. Příkladem je norma ISO/IEC 27001, která detailně definuje kritéria na řízení informační bezpečnosti.

Bezpečnostní politika: Vnitřní směrnice a postupy organizace zahrnující oblast KB, jako jsou hesla, přístupová práva, správa dat atd.

Technické normy: specifická technická opatření, například šifrování dat, firewall, aktualizace softwaru a další.

Regulace a zákony: Zákony a nařízení související s KB a ochrany osobních údajů.

Průmyslové standardy: Specifické standardy či směrnice přizpůsobené danému odvětví, které mohou ovlivnit KB.

Obchodní požadavky: Požadavky organizace na zajištění bezpečnosti informací a dat, jež jsou klíčové pro její provoz.

Nejlepší postupy (nejsou povinné): Navrhované postupy ze strany uznávaných odborníků a organizací zabývající se KB.

Soulad s předchozími auditními zjištěními: Kritéria, které vycházejí z předchozích auditů a jejich doporučení.

Program auditu

Program auditu neboli také auditní plán představuje detailní soubor procesů a činností, které je nutné během auditu dodržet.[113]

---

[112] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 296.

[113] Tamtéž, s. 297.

Hlavní prvky programu auditu mohou zahrnovat:

Cíle auditu: Stanovení konkrétních cílů, které lze auditem dosáhnout, jako například identifikace zranitelností, posouzení souladu s normami nebo bezpečnostními opatřeními.

Rozsah auditu: Vymezení konkrétních oblastí, systémů nebo procesů, které budou podrobeny auditem.

Harmonogram: Určení časového plánu pro realizaci jednotlivých fází auditu. Harmonogram zohledňuje dostupnost klíčových účastníků a minimalizuje narušení běžného provozu.

Odpovědnosti a role: Definování rolí a odpovědnost členů auditorského týmu, vedoucího auditu, pracovníků organizací a dalších zainteresovaných stran.

Metody a techniky auditu: Specifikace metodiky a techniky, které budou využity během průběhu auditu, jako například testování zranitelností, analýza dokumentace, rozhovory s pracovníky a další metody.

Sběr a analýza dat: Plán pro sběr dat, analýza a vyhodnocování dokumentace, testování systémů a další aktivity spojené s procesem shromažďování informací.

Komunikace a prezentace výsledků: Plán pro sdělení výsledků auditu vedoucím pracovníkům a dalším zainteresovaným stranám, včetně případných doporučení a návrhů na zlepšení.

Opatření na nápravu: Plán pro následné kroky, které budou provedeny na základě zjištění auditu, včetně implementace nápravných opatření a kontrolního auditu.

Důkazy z auditu

Důkazy z auditu jsou konkrétní informace, fakta, záznamy, dokumenty nebo materiály, které jsou shromážděny a analyzovány během auditního procesu s cílem potvrdit nebo vyvrátit platnost určité tvrzení, stanovisek nebo. Tyto důkazy slouží jako základ pro objektivní a důvěryhodné posouzení stavu, účinnosti, souladu nebo nedostatečnosti v předmětu auditu.[114]

[114] SEDLÁK, P., KONEČNÝ, M., a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 297.

Zjištění z auditu

Zjištění z auditu jsou konkrétní informace, skutečnosti nebo výsledky, které byly zjištěny během auditního procesu a poskytují důkazy o stavu v souladu nebo nedostatečnosti v předmětu auditu. Tato zjištění jsou výstupem zpracování a analýzy shromážděných důkazů a slouží k vyvození závěrů o auditované oblasti.

Auditní tým

Auditní tým přistupuje k plánování a provádění auditu s odborným skepticismem, což znamená, že si udržuje zdravou nedůvěru a provádí kritické posouzení platnosti získaných důkazních informací. Tým auditorů pečlivě zkoumá důkazní informace a věnuje zvláštní pozornost těm, které vylučují nebo zpochybňují spolehlivost dokumentů nebo prohlášení vedení, které jsou předmětem auditu.[115]

Vedoucí auditor: Vedoucí auditor, známý také jako hlavní auditor, je odborník s výraznými zkušenostmi a odpovědností, který má vedoucí roli v auditním týmu. Jeho hlavním úkolem je řídit celý proces auditu, zajistit kvalitu a konkrétní auditní činnosti a výstupy. Rovněž také komunikovat s klienty auditu a dalšími zainteresovanými stranami.

Člen týmu auditorů: Člen týmu auditorů je odborník, který je součástí auditního týmu a má úkol podílet se na provádění auditu nebo inspekce. Tito odborníci jsou zodpovědní za shromažďování informací, analýzu dat, hodnocení stavu a identifikaci nedostatků v rámci auditované oblasti. Každý člen týmu auditorů má specifické dovednosti a relevantní znalosti pro předmět auditu. Patří sem i podpora činností vedoucího auditora.

Technický expert: Technický expert je jedinec, který má hluboké znalosti, dovednosti a odbornost v určité technické oblasti. Tito odborníci jsou schopni porozumět komplexním technickým konceptům, procesům, zařízením nebo systémům a poskytovat odbornou radu, analýzu a řešení související s těmito oblastmi. Techničtí experti jsou často vyhledáváni pro své schopnosti vyřešit složité technické problémy a poskytnout specializovaný pohled na dané téma.

Pozorovatel: Pozorovatel je osoba nebo entita, která sleduje nebo zaznamenává určitou událost, situaci, proces nebo činnost. Pozorovatel může být přítomen fyzicky, vizuálně, auditivně nebo jinými smyslovými způsoby, nebo může sledovat události

[115] SEDLÁK, P., KONEČNÝ, M., a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 297.

prostřednictvím technických prostředků, jako jsou kamery, senzory nebo monitorovací systémy. Pozorovatelé mohou hrát důležitou roli v různých oblastech, jako je vědecký výzkum, bezpečnost, kontrola a monitorování.

Základní principy auditu

Principy auditu KB představují soubor pravidel, zásad a postupů, které definují správný a kvalitní způsob provedení auditu v oblasti KB. Tyto principy slouží k zajištění objektivity, důvěryhodnosti a efektivnosti celého procesu auditu a pomáhají identifikovat nedostatky, rizika a příležitosti pro zlepšení v systémech, sítích a procesech.[116]

Základní principy auditu KB:

Integrita: Integrita se v kontextu KB definuje jako zajištění nedotknutelnosti dat, informací a systémů před neoprávněnými změnami, poškozením nebo ztrátou. Je to stav, kdy jsou data a systémy chráněny tak, aby nebylo možné je nelegálně nebo neoprávněně modifikovat, což zajišťuje důvěryhodnost a spolehlivost informací či procesů v kybernetickém prostředí.[117]

Spravedlivé prezentování: Spravedlivé prezentování se týká způsobu, jakým jsou informace, údaje nebo výsledky zpracovávány a představovány tak, aby byly přesné, objektivní a nepřekroucené. Jde o zásadu, která zajišťuje, že prezentace informací nezkresluje skutečnost, nesnaží se manipulovat s vnímáním či hodnocením, a umožňuje lidem tvořit si vlastní nestranný názor na základě dostupných faktů.

Profesionální přístup: Profesionální přístup se vztahuje k způsobu, jakým jedinec nebo tým přistupuje k pracovním úkolům, povinnostem a interakcím. Jde o přístup, který je založen na zodpovědnosti, respektu, odbornosti a integritě. Profesionální přístup zahrnuje dodržování etických norem, komunikaci se zákazníky, kolegy a partnery s ohledem na vysokou kvalitu a slušnost, a také schopnost řešit problémy a výzvy s cílem dosáhnout nejlepších výsledků. V profesionálním přístupu se klade důraz na efektivní řešení úkolů, spolupráci a zachování dobrého jména a pověsti.[118]

---

[116] SEDLÁK, P., KONEČNÝ, M., a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 298.

[117] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 81.

[118] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 298.

Důvěrnost: Důvěrnost je principem ochrany informací, který zajišťuje, že citlivá data, informace nebo materiály nebudou neoprávněně sdíleny nebo zpřístupněny. Jde o zásadu, která se týká ochrany soukromí a omezuje přístup k informacím pouze na ty, kteří mají k tomu oprávnění. Důvěrnost je klíčovým aspektem v KB a v různých oblastech, jako je právní ochrana osobních údajů, obchodní tajemství, vládní tajemství a další citlivé informace. Důvěrnost zajišťuje, že informace jsou chráněny před zneužitím, krádeží nebo neoprávněným rozšířením.

Nezávislost: Audit by měl být prováděn nezávislým týmem odborníků, kteří nemají žádný osobní nebo finanční vztah k auditované organizaci. To zajišťuje, že auditní zjištění jsou nestranná a spolehlivá.

Průkaznost: Průkaznost se týká schopnosti prezentovat nebo prokázat platnost, pravdivost nebo oprávněnost nějaké informace, tvrzení, argumentu nebo faktu. Je to proces poskytování dostatečných a relevantních důkazů nebo indicií, které podporují dané tvrzení a umožňují věrohodně vyvozovat závěry.[119]

Proces auditu

Proces auditu je systematický a nezávislý postup, během kterého se provádí objektivní hodnocení, ověřování a posuzování určitého subjektu, činnosti, procesu, systému nebo účetních záznamů. Hlavním cílem auditu je získat důvěru věrohodnosti, spolehlivosti a úplnosti informací. Audit může být prováděn v rámci různých oblastí, jako jsou finanční záznamy, procesy, systémy řízení kvality, informační technologie nebo dokonce environmentální ochrana.

Proces auditu obvykle zahrnuje následující kroky:

Plánování: Plánování auditu se týká systematického procesu, během něhož se definuje příprava plánu auditu, sestavení harmonogramu, auditního týmu, vyžádání dokumentace a příprava podkladů.

Přezkum dokumentace: Přezkum dokumentace je proces, během něhož se důkladně posuzují a analyzují různé druhy písemných materiálů, dokumentů nebo záznamů. Tento proces může být prováděn z různých důvodů, jako je ověření přesnosti, hodnocení souladu s určitými normami nebo standardy, identifikace nedostatků, zajištění zákonného

[119] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 299.

splnění nebo shromažďování informací pro rozhodování. Přezkum dokumentace hraje důležitou roli při zajištění správného provádění procesů, dodržení standardů a shromažďování relevantních informací pro různé účely.[120]

Provádění činností při auditu: Při samotném průběhu auditu jde o souhrn činností jako je úvodní jednání, přidělení rolí a odpovědností, přezkoumání dokumentů v průběhu auditu, komunikace, shromažďování a ověřování. Dále zahrnuje zjištění z auditu, jako jsou shody/neshody, příležitost ke zlepšení či případné potenciální riziko.

Příprava protokolu: Příprava protokolu zahrnuje proces vytvoření oficiálního záznamu, ve kterém jsou zahrnuty údaje o organizaci, cíl a předmět auditu, místo a datum, plán a účastníci auditu, přehled auditovaných dokumentů, zjištění a manažerské shrnutí výsledků. Součástí jsou i uvedené závěry z auditu.

Ukončení auditu: Audit je dokončen, jakmile jsou provedeny všechny plánované auditní činnosti a klientem je schválen výstup z provedeného auditu.

Následný audit: Je forma auditu, která se provádí po ukončení hlavního auditu a jeho cílem je aplikovat nápravná opatření, poté ověření jejich dokončení a efektivnosti.[121]

Certifikační audit

Cílem certifikačního auditu je získat potvrzení ve formě certifikátu, který potvrzuje, že organizace, nebo jeho konkrétní část (například dle rozsahu ISMS) splňuje předepsané požadavky a zároveň má certifikovaný a dozorovaný systém managementu dle příslušné normy (např. ISO 27001).[122]

Platnost certifikátu ISMS je na 3 roky a je podmíněna každoročními dohledovými audity. ZoKB ani jeho příslušná vyhláška nekladou přímou povinnost na provedení certifikace. Tento audit je však požadován ze strany NÚKIB v případě, kdy organizace vykonává funkci správce a provozovatele KII, správce a provozovatele VIS, provozovatele základní služby nebo poskytovatele digitální služby.

[120] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 299.

[121] Tamtéž, s. 300.

[122] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. s. 41.

Dohledový audit – dohledový audit je prováděn pravidelně každý rok s cílem ověřit, zda se v průběhu tříletého certifikačního období dodržují zvolené standardy. V rámci tohoto auditu je nutné prokázat neustálé zlepšování.

Recertifikační audit – tento typ auditu je plánován a prováděn za účelem posouzení trvalého naplňování všech požadavků příslušné normy. Jeho cílem je potvrdit kontinuální shodu a účinnost ISMS jako celku a jeho dlouhodobou platnost a vhodnost pro konkrétní rozsah certifikace. Tento druh auditu probíhá v pravidelných tříletých intervalech.[123]

[123] SEDLÁK, P., KONEČNÝ, M. a kol. *Kybernetická (ne)bezpečnost*. Praha: CERM, akademické nakladatelství, 2021. s. 302.

4 Vlastní práce

Praktická část je zaměřena na analýzu veřejných zakázek v oblasti informační a kybernetické bezpečnosti. Práce je rozdělena na několik částí. V úvodu je nejprve představena společnost BELCOM Digital a.s. (dále jen „BDg“), ve které autorka dlouhodobě pracuje. Jsou zde uvedeny a popsány hlavní oblasti působení společnosti

V další kapitole je provedena analýza počtu jednotlivých VZ týkající se informační a kybernetické bezpečnosti, kterých se Společnost BDg zúčastnila. Jde o období od ledna 2017 do prosince 2022. Následuje analýza jednotlivých služeb v oblasti KB. Na základě zjištěných dat je provedena komparace údajů za jednotlivá období. Získaná data jsou graficky znázorněna a detailně vyhodnocena.

V závěrečné kapitole praktické části jsou interpretovány zjištěné nedostatky v rámci auditu KB, včetně jednotlivých doporučení k jejich řešení. Výsledkem celého procesu je návrh obecné metodiky pro plán a realizaci auditu KB a její implementace do firemního prostředí.

4.1 Charakteristika společnosti

Společnost BDg má více než dvacetiletou zkušenost jak na českém, tak i na zahraničním trhu a je uznávanou poradenskou firmou v oblasti ICT a KB. Její tým disponuje širokým spektrem odborných znalostí a dovedností v oblastech informační a kybernetické bezpečnosti, softwarového inženýrství, bezpečnostního auditu a řízení rizik. Společnost je držitelem certifikovaného systému pro systém managementu informací dle normy ISO/IEC 27001:2014 a získala pověření NBÚ, které jí umožňuje pracovat s utajenými informacemi na stupni Tajné. Je partnerem mnoha renomovaných světových i lokálních výrobců podnikových řešení a software v oblasti bezpečnosti, datové analytiky, softwarové robotizace a digitalizace firemních procesů.

4.1.1 Oblasti působení společnosti

Společnost BDg poskytuje rozsáhlé portfolio auditorských a konzultačních služeb, které zahrnuje manažerské poradenství, projektové řízení a řízení systému informační a kybernetické bezpečnosti. V současnosti se její činnost zaměřuje především na poradenství a auditorské činnosti v oblasti KB, včetně ochrany digitálních dat, sítí a systémů před různými hrozbami a útoky. Mimo to je společnost úspěšná při účasti v zadávacích

řízeních na klíčové zakázky v oblasti kybernetické a informační bezpečnosti. Dále poskytuje svým klientům poradenské služby v oblasti dotačního managementu a digitální transformaci procesů a obchodních aktivit. Současně se společnost zaměřuje i na oblast procesní automatizace a robotizace.

4.1.2 Popis jednotlivých nabízených služeb

V této části jsou blíže představeny nabízené služby ve společnosti BDg.

- **Služby ICT služeb**

V dnešním světě založeném na informací jsou organizace závislé na efektivním a kvalitním provozu ICT. Schopnost organizace dosahovat stanovených cílů a udržet svou konkurenceschopnost je částečně podmíněna schopností efektivně a kvalitně řídit své ICT služby při akceptovatelné úrovni nákladovosti a rychlosti implementace těchto služeb.

Společnost BDg poskytuje komplexní odborné služby nezbytné pro vytvoření a zajištění provozu a koncepčního prostředí ICT, především v oblastech zajištění podpory projektové kanceláře a řízení služeb, tvorby architektury, koncepce a procesů ICT, technologických řešení ICT, infrastruktury a serverového řešení.

Hlavním cílem je dosáhnout efektivního a spolehlivého poskytování ICT služeb, minimalizovat výpadky a potíže, optimalizovat využití ICT zdrojů a zvýšit spokojenost zákazníků či uživatelů.

- **Audit v oblasti ICT**

Audit v oblasti ICT je v mnoha ohledech velmi specifický. V dnešní době jsou ICT využívány ve všech oblastech činnosti organizace, a proto je nezbytné provést komplexní hodnocení ICT na všech úrovních. Toto hodnocení zahrnuje technické, organizační a procesní aspekty.

Společnost v oblasti ICT nejčastěji provádí následující druhy auditů, přičemž velmi často se jedná o kombinaci těchto druhů auditů podle požadavků klienta.

- ✓ *Audit systému řízení bezpečnosti informací (ISMS)* – posouzení stavu bezpečnosti informací v souladu s ustanoveními a požadavky norem řady ISO/IEC 27000.
- ✓ *Audit systému řízení IT služeb (ITSM)* – hodnocení dosažení úrovně plnění zákonných norem zaměřených na řízení IT služeb, případně IT Governance.

- ✓ *Audity v bankovním prostředí* – hodnocení, které zkoumá, do jaké míry jsou splněna regulační opatření zaměřených na ICT a dalších standardů ve specifickém bankovním prostředí.
- ✓ *Technické audity* – posouzení stavu v oblasti ICT, zejména konkrétních IS nebo technologií, v souladu s určitými standardy a doporučeními.

Audit v oblasti ICT představuje klíčový nástroj pro organizace, neboť pomáhá identifikovat slabá místa, rizika a nedostatky v rámci IT. Tím umožňuje přijmout opatření ke zlepšení bezpečnosti, efektivity a správy ICT zdrojů. Tímto způsobem organizace minimalizuje rizika a zajistí, že ICT infrastruktura plní své úkoly v souladu s očekáváním.

- ➢ **Řízení bezpečnosti informací**

Informace jsou dnes klíčovým faktorem, který ovlivňuje fungování a úspěch každé organizace. Je nezbytné chránit tyto informace, protože právě ony představují konkurenční výhodu a umožňují růst organizace. Implementace a provozování systému managementu bezpečnosti informací v souladu s normou ISO/IEC 27001 je účinným nástrojem pro zajištění dostupnosti a ochrany informací.

V současném digitálním světě se řízení bezpečnosti informací stává klíčovým prvkem. Organizace čelí stále rostoucím hrozbám a rizikům spojených s nedostatečnou ochranou citlivých informací a dat. Efektivní správa bezpečnosti informací organizacím umožňuje minimalizovat tato rizika a zajišťovat ochranu svých aktivit, a tím budovat důvěru u svých zákazníků a partnerů. Společnost BDg poskytuje poradenství v této oblasti a pomáhá při zavádění efektivního systému managementu bezpečnosti informací s využitím svých mnoholetých zkušeností s touto problematikou.

- ➢ **Bezpečnostní testy**

Pro testování bezpečnosti se v dnešní době často využívají standardizované metodiky. Cílem bezpečnostních testů je simulovat útoky a pokusy o neoprávněný přístup potenciálních útočníků s účelem zdokonalit celkovou bezpečnost organizace. Tyto testy mohou být realizovány interně samotnou organizací nebo externími bezpečnostními specialisty. Společnost BDg nejčastěji provádí následující typy testů:

- ✓ *Penetrační testy* – tento typ testů simuluje útoky na systémy organizace s cílem ověřit účinnost ochrany proti zranitelnostem. Penetrační testeři se snaží proniknout

do systémů a aplikací, identifikovat slabiny a navrhnout opatření na zajištění bezpečnosti.

- ✓ *Testy zranitelnosti* – testy zranitelnosti se zaměřují na odhalení známých i neznámých zranitelností v systémech. Testeři provedou skenování sítí a aplikací s cílem identifikovat potencionální slabiny, které mohou být zneužity útočníky.
- ✓ *Testy sociálního inženýrství* – tyto testy zkoumají povědomí zaměstnanců o bezpečnostních postupech a jejich odolnost vůči sociálnímu inženýrství. Testeři se snaží získat citlivé informace od zaměstnanců, často využívají techniky jako phishing.

Bezpečnostní testy představují klíčový nástroj pro organizace, které usilují o zlepšení svého bezpečnostního postavení a minimalizaci rizik spojených s útoky na IT systémy. Na základě výsledků těchto testů mohou organizace přijmout opatření s cílem posílit bezpečnost svých informačních aktiv.

- ➢ **Audit v oblasti kybernetické bezpečnosti**

Audit v oblasti KB je proces systematického a nezávislého vyhodnocení bezpečnostního stavu IS, sítí, aplikací a dalších prostředků s cílem identifikovat zranitelnosti, rizika a nedostatky v bezpečnostních opatřeních. Jeho hlavním cílem je poskytnout organizaci přehled o aktuálním stavu bezpečnosti, identifikovat potenciální hrozby a nedostatky a navrhnout opatření ke zvýšení úrovně ochrany před kybernetickými hrozbami.

Poskytované služby společnosti BDg zahrnují audit v oblasti KB dle požadavků ZoKB, VoKB, normy ISO 27001 a dalších relevantních zákonných předpisů. Konkrétně se jedná o hodnocení bezpečnostní politiky a postupů, kontrolu přístupových práv, zhodnocení zabezpečení sítí a infrastruktury, testování zranitelnosti, hodnocení incidentního řízení a kontrolu dodržování právních a regulačních požadavků. Také zahrnuje hodnocení úrovně školení a povědomí zaměstnanců o KB. Výsledky auditu jsou shrnuty ve zprávě obsahující zjištění, doporučení a plán kroků pro zlepšení bezpečnosti organizace. Kybernetický bezpečnostní audit hraje klíčovou roli v ochraně organizací před kybernetickými útoky a ztrátou citlivých informací.

- **Ochrana osobních údajů**

Ochrana osobních údajů má za cíl zejména zabezpečit právo jednotlivce na ochranu před neoprávněným zasahováním do jeho soukromí a stanovení podmínek pro bezpečné zpracování, uchovávání a likvidaci osobních údajů. Klíčovým principem ochrany osobních údajů, reflektovaným v povinnostech správce či zpracovatele, je skutečnost, že osobní údaje se zpracovávají za konkrétním účelem. Pro každý účel je proto nezbytné definovat a zdokumentovat, které konkrétní osobní údaje je nutné zpracovávat, a také operace, jež s nimi souvisejí. S ohledem na tyto požadavky musejí správci i zpracovatelé osobních údajů přijmout a zdokumentovat adekvátní technická a organizační opatření k zajištění ochrany osobních údajů v souladu se stanovenými zákonnými podmínkami.

Odborníci společnosti BDg poskytují součinnost při zavedení efektivního systém ochrany osobních údajů s využitím svých mnoholetých zkušeností s touto problematikou. V rámci činnosti externího pověřence pro ochranu osobních údajů dále poskytují poradenské a konzultační služby zahrnující ověření implementace požadavků GDPR a zákona o zpracování osobních údajů v organizaci, revizi postupů a procesů na ochranu osobních údajů, revizi předložené dokumentace k ochraně osobních údajů, ověření povědomí zaměstnanců o ochraně osobních údajů a prověření rizikovosti jednotlivých zpracování. Výstupem nabízené služby je komplexní zpráva o aktuálním stavu ochrany osobních údajů v organizaci z pohledu požadavků orgánů dohledu. Tato zpráva je doplněna o návrhy nápravných opatření.

- **Automatizace a robotizace**

Oba tyto koncepty jsou klíčovými prvky moderního průmyslu a technologického rozvoje. Automatizace a robotizace přinášejí výhody, jako je zvýšená produktivita, snížení nákladů, zlepšená kvalita a bezpečnost práce. Robotic Process Automation (dále jen „RPA“) označuje platformy a nástroje umožňující softwarovou automatizaci různých firemních procesů v oblastech jako finance, controlling, konsolidace, lidské zdroje, obchod, ICT, sklady a logistika apod. Tento nástroj nahrazuje lidskou práci „počítačem“ v případech, kdy je tato práce časově náročná, rutinní s minimální přidanou hodnotou, opakující se nebo velmi častá, s rizikem chyb z nepozornosti a pro většinu aktivit v procesu popsatelnou jasně stanovenými pravidly a postupy.

Společnost BDg je Certifikovaným partnerem společnosti nabízející dodávku licence platformy RPA včetně celkové podpory, update a řešení konfliktů při aktualizací apod.

- **Dotační management**

Dotační management se obvykle týká správy finančních prostředků, které jsou poskytovány za účelem podpory specifických aktivit, cílů nebo projektů. Tyto peníze mohou být poskytovány na veřejné služby, výzkum a vývoj, kulturu, vzdělání nebo jiné oblasti. Zahrnuje procesy správy a kontroly alokace finančních prostředků. To zahrnuje sledování využívání finančních prostředků, ověřování dosažení cílů a zajištění, že peníze jsou vynakládány efektivně a odpovědně. V rámci dotačního managementu je důležitá transparentnost v procesu poskytování dotací. Příjemci často musí podávat zprávy o tom, jak jsou finanční prostředky využívány a jsou odpovědní za dosažení stanovených cílů. Poskytování dotací zahrnuje rozhodovací proces, kde je nutné vyhodnotit žádosti o dotace, určit příjemce, stanovit podmínky a schvalovat alokaci finančních prostředků.

Společnost BDg poskytuje poradenské služby spočívající v podpoře řízení projektu a dozoru nad implementací projektu v souladu s platnou legislativou, pravidly příslušného operačního programu a konkrétní výzvy.

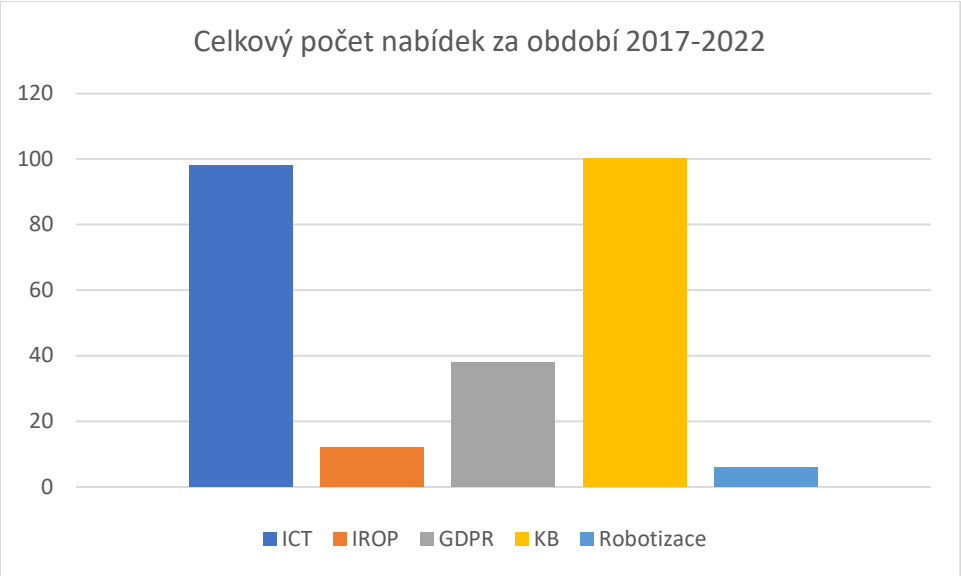
4.2 Přehled veřejné zakázky v oblasti informační a kybernetické bezpečnosti

Tato kapitola navazuje na teoretickou část diplomové práce a je zaměřena na analýzu počtu podaných nabídek na VZ v oblasti informační a kybernetické bezpečnosti. Následuje porovnání z hlediska finančního rozsahu jednotlivých veřejných zakázek, a to za období ledna 2017 až prosince 2022.

4.2.1 Počet nabídek na veřejné zakázky dle oblasti služeb v letech 2017-2022

Souhrnná data, ze kterých byla zpracována analýza počtu podaných nabídek na jednotlivé VZ v oblasti informační a kybernetické bezpečnosti, znázorňuje následující graf. Je porovnáváno sledované období 2017-2022.

Graf 1 Celkový počet nabídek na VZ dle oblasti služeb za období 2017-2022



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

Z uvedené komparace vyplývá, že největší počet podaných nabídek na VZ se týká nabízených služeb v oblasti KB. Ta zahrnuje různé služby a opatření navržené k ochraně IS, sítí a dat před kybernetickými hrozbami. Tyto služby jsou klíčové pro udržení integrity, dostupnosti a důvěrnosti informací v prostředích, kde je KB nezbytná pro ochranu citlivých dat a zajištění plynulého chodu operací.

Jedná se především o následující služby:

- *Ochrana proti malwaru:* Poskytování nástrojů a technik pro identifikaci, odstranění a prevenci malware, včetně virů, trojanů, spyware a ransomwaru.
- *Firewally a Prevention Systems:* Nasazení firewallů k monitorování a kontrole síťové komunikace a systémů pro detekci a prevenci neoprávněných přístupů a aktivit.
- *Bezpečnostní audit a monitorování:* Sledování a hodnocení bezpečnostních událostí a aktivit tak, aby bylo možné rychle identifikovat a reagovat na potenciální hrozby.
- *Zabezpečení sítí a koncových zařízení:* Implementace technologií a postupů pro zajištění bezpečnosti sítí, routerů, switchů a koncových zařízení, včetně antivirové ochrany.
- *Incident Response a krizový management:* Vypracování plánů a postupů pro rychlou a efektivní reakci na kybernetické incidenty a minimalizaci jejich dopadů.

- *Vzdělávání a školení v oblasti KB:* Poskytování školení a poučení pro zaměstnance a uživatele s cílem zvyšovat povědomí a kybernetických hrozbách a správných postupech pro bezpečné chování.
- *Penetrace testování:* Provádění simulovaných útoků s cílem identifikovat slabá místa a zranitelnosti v IS a sítích.
- *Řízení bezpečnostních událostí a incidentů (SIEM):* Implementace nástrojů a procesů pro shromažďování, analýzu a reakci na bezpečnostní události v reálném čase.

Nepatrně malý rozdíl je v nabídkách na služby v oblasti ICT. Tento segment zahrnuje širokou škálu služeb, které se týkají IS a komunikace. Zde jsou některé z hlavních nabízených služeb v oblasti ICT:

- *Vývoj software:* Zahrnuje návrh, vytváření a údržbu softwaru pro různé aplikace, od desktopových programů a mobilních aplikací po webové stránky a podnikové systémy.
- *Poradenské služby v oblasti ICT*: Poskytování odborných rad a konzultací v oblasti IS a strategií pro efektivní využívání IT zdrojů.
- *Technická podpora*: Poskytování technické podpory a řešení problémů pro uživatele v oblasti hardwaru a softwaru.
- *Interní audit v oblasti ICT*: Proces, který slouží k posouzení a hodnocení ICT ve firmě či organizaci. Jeho cílem je zajištění efektivity, bezpečnosti a souladu s předepsanými standardy a postupy.

Následují nabídky na VZ na služby v oblasti GDPR. Nabízené služby jsou zaměřeny na zajištění souladu s tímto nařízením a na ochranu osobních údajů a jde především o:

- *Zpracování údajů v souladu s GDPR:* Poskytování služeb pro zajištění, že veškeré zpracování osobních údajů je v souladu s principy a požadavky GDPR.
- *Audit GDPR:* Proces, který slouží k ověření a hodnocení dodržování GDPR ve firmě či organizaci. Jeho cílem je zajistit, že organizace spravuje osobní údaje svých subjektů zpracování v souladu s požadavky GDPR.
- *DPO (Data Protection Office):* Nabízení služeb DPO, který je odpovědný za dohled nad dodržováním GDPR ve společnosti.

Další kategorií jsou nabídky na VZ na služby zabývající se problematikou dotačního poradenství v oblasti Integrovaného regionálního operačního programu (dále jen „IROP“), které jsou součástí implementace strukturálních fondů Evropské unie. Tyto služby

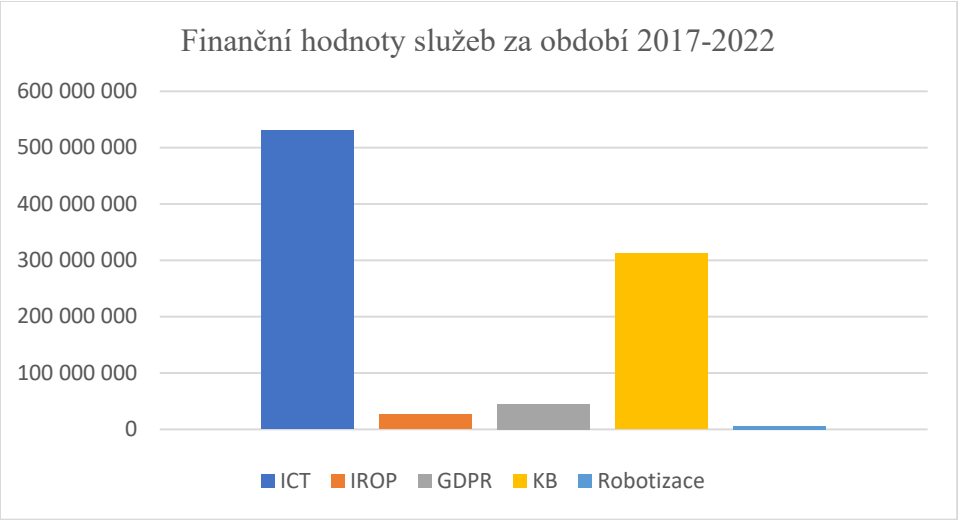
se zabývají plánováním a implementací projektů financovaných z evropských strukturálních fondů, poskytují podporu v oblasti finančního řízení projektů, sledování využívání finančních prostředků a zajištění transparentnosti a odpovědnosti. Pomáhají organizacím a subjektům při přípravě žádosti o financování, vyhodnocení jejich proveditelnosti a dodržování pravidel programu. Služby se také zabývají monitorováním a hodnocením pokroku dosaženého prostřednictvím projektů, a také zahrnují správu administrativních procesů spojených s projekty financovanými z IROP, včetně správy dokumentace, evidování změn a komunikace s příjemci dotací.

Nejméně podaných nabídek bylo v kategorii Automatizace a Robotizace. Tento rozdíl je patrný z důvodu, že tato služba je na trhu teprve krátkou dobu. Služby v oblasti robotizace a automatizace se zaměřují na využití technologií, aby se procesy a úkoly v organizace nebo průmyslu mohly provádět efektivněji a s minimální lidskou intervencí. Jde především o následující služby:

- *RPA (Robotic Process Automation):* Implementace softwarových robotů nebo botů, kteří mohou automatizovat opakující se a pravidelné úkoly v rámci podnikových procesů. RPA může simulovat lidskou interakci s digitálními systémy.
- *Automatizace dokumentace a procesů zpracování dat:* Využívání technologií pro automatické zpracování a organizace dokumentů a dat, čímž se urychlují administrativní a datové procesy.
- *Automatizace IT operací:* Používání automatizovaných nástrojů a systémů pro správu a monitorování IT infrastruktury, včetně správy serverů, síťových operací a správy cloudových prostředí.

Kromě počtu celkových podaných nabídek na VZ byly dále sledovány a graficky znázorněny hodnoty zakázek v jednotlivých oblastech činností. Přestože byl zaznamenán největší počet podaných nabídek na služby v oblasti KB, nejvyšší finanční hodnoty představují služby v oblasti ICT, což zachycuje následující graf.

Graf 2 Hodnoty VZ za jednotlivé služby za období 2017-2022

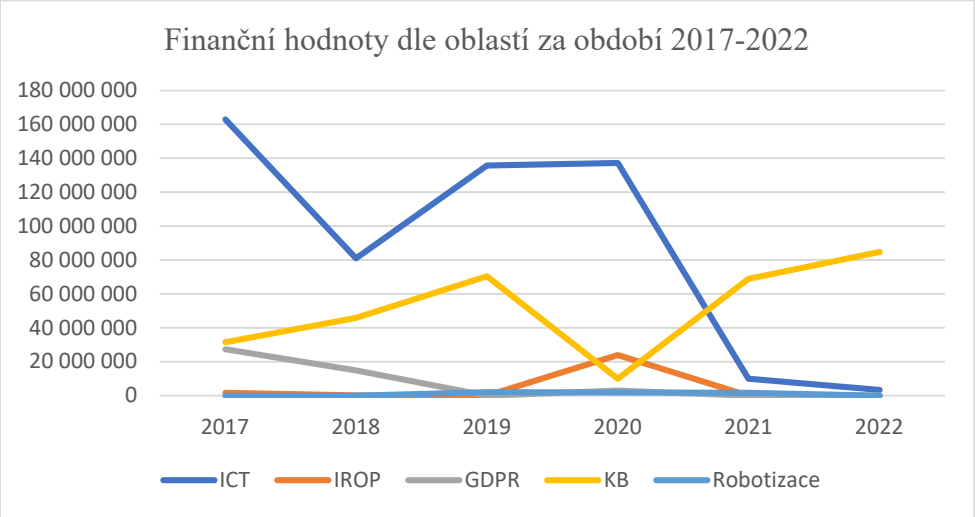


Zdroj: Interní data společnosti BDig, zpracování: vlastní práce

Jak je z grafu patrné, největší podíl z hlediska finančního rozsahu tvořily zakázky na služby v oblasti ICT, a to v celkové hodnotě 530 mil. Kč bez DPH. Důvodem vyššího finančního rozsahu oproti ostatním službám je poptávka služeb spojená s vytvořením návrhu, realizací a dodávkou rozsáhlejšího IS. Návrh, realizace navrženého systému a jeho nasazení tvoří vysoké finanční náklady a jeho provoz je rozprostřen do delšího časového období.

Dále následují zakázky v oblasti KB v celkové hodnotě 312 mil Kč bez DPH, kde z níže uvedeného grafu vyplývá, že tyto nabídky služeb postupně po roce 2020 převládají, jak počtem, tak i finanční hodnotou zakázek.

Graf 3 Vývoj finančních hodnot nabízených služeb v období 2017-2022



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

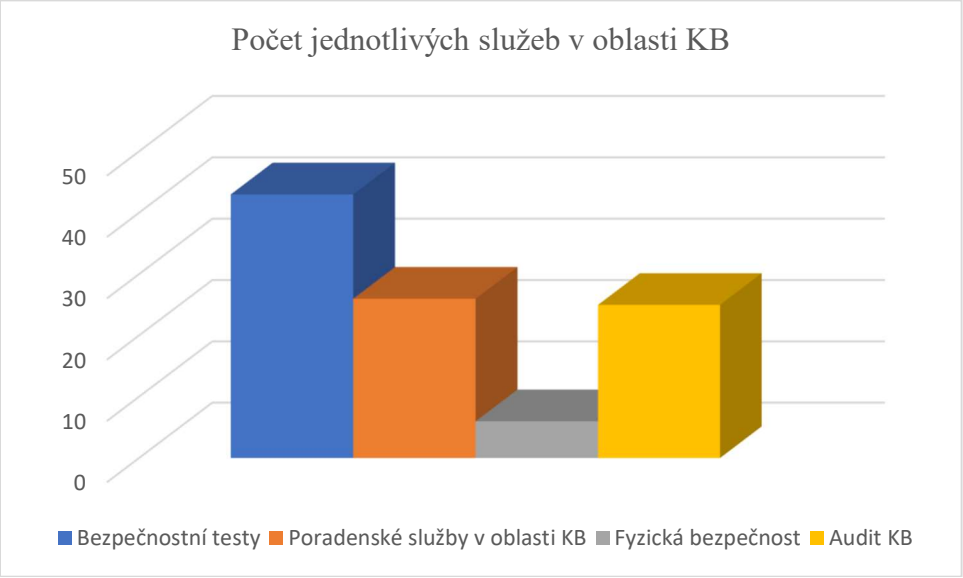
Z grafu je dále patrné, že v období 2019-2021 došlo k nárůstu zakázek na služby v oblasti IROP. Tento nárůst je ovlivněn možností čerpání finančních prostředků z dotačního programu představující Strategický rámec rozvoje veřejné správy ČR, konkrétně strategickým cílem 3: Zvýšení dostupnosti a transparentnosti veřejné správy, který reaguje na zvyšující se potřebu řešení KB a váže se na realizaci jediného specifického cíle, kterým je dobudování informačních a komunikačních systémů veřejné správy a realizace bezpečnostních opatření podle ZoKB prostřednictvím rozvoje využití a kvality systémů ICT. Celkový objem zakázek v této oblasti činil 26 mil. Kč bez DPH.

Nejmenší objem jak do počtu, tak i finanční hodnoty tvořily zakázky na služby v oblasti Robotizace, a to v celkové hodnotě 5 mil. Kč bez DPH. Jak již bylo zmíněno výše, tento segment služeb je poptáván na českém trhu relativně krátkou dobu.

4.2.2 Analýza počtu nabídek na VZ v oblasti KB

Souhrnná data, ze kterých byla zpracována analýza počtu podaných nabídek na jednotlivé nabízené služby v oblasti KB, znázorňuje následující graf. Rovněž je porovnáváno sledované období 2017-2022.

Graf 4 Celkový počet zakázek za jednotlivé oblasti KB za období 2017-2022



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

Jak je z grafu patrné největší počet podaných nabídek na VZ náleží kategorii bezpečnostních testů, které organizace provádějí k identifikaci a řešení bezpečnostních nedostatků a rizik. Patří sem především testování síťové bezpečnosti, bezpečnosti webových

aplikací, testování sociálního inženýrství, penetrační testování, testování zranitelnosti a odolnosti.

Následují zakázky v oblasti auditu KB, které se zaměřují na poskytování komplexního a systematického posouzení IS, sítí a prostředí organizace s cílem identifikovat a analyzovat potenciální kybernetická rizika a zranitelnosti. Tyto služby zahrnují zhodnocení současných bezpečnostních postupů a mechanismů, identifikaci slabých míst a nedostatků v systémech a navrhování doporučení pro zlepšení celkové KB. Součástí jednotlivých auditů bývají i zmiňované bezpečnostní testy. Cílem těchto služeb je poskytnout organizacím důkladné a objektivní hodnocení stavu jejich KB a doporučení pro zlepšení a ochranu proti moderním kybernetickým hrozbám. Tato oblast je dále podrobněji rozpracovaná v následující kapitole.

Další kategorii tvoří poradenské služby v oblasti KB. Jedná se např. o služby související s vytvořením řízené bezpečnostní dokumentace v souladu s požadavky zákona ZoKB a platného výkladu VoKB, kam patří návrh koncepce KB, analýza rizik zahrnující identifikaci a ohodnocení aktiv, hrozeb a zranitelnosti. Nejméně zakázek je v oblasti fyzické bezpečnosti, které se zaměřují na zajištění fyzické ochrany prostorů, majetku a osob před různými formami hrozeb a prevenci rizik. Všechny uvedené zakázky bývají zároveň součástí interního auditu KB.

4.3 Veřejné zakázky v oblasti auditu kybernetické bezpečnosti

Veřejné zakázky v oblasti auditu KB jsou specifické zakázky, které se zaměřují na posouzení a zlepšení úrovně KB ve veřejných institucích, organizacích nebo firmách. Charakterizují se několika klíčovými rysy:

- *Specifičnost požadavků:* Zakázky obvykle obsahují detailní specifikace požadavků, které poskytují jasné směrnice pro auditní proces. To může zahrnovat hodnocení sítí, systémů, aplikací a politik KB.
- *Ochrana citlivých informací:* Audit KB často zahrnuje přístup k citlivým informacím a datům. VZ musí zajistit, že účastníci budou schopni adekvátně zacházet s citlivými informacemi a že budou dodržovány veškeré bezpečnostní normy a postupy.
- *Odbornost a certifikace:* Zadavatelé VZ obvykle vyžadují odbornou kvalifikaci a certifikace od poskytovatelů auditních služeb v oblasti KB. To zajišťuje,

že audit bude prováděn odborníky se znalostí aktuálních hrozeb a bezpečnostních trendů.

- *Rozsah auditu:* Zakázky v oblasti auditu KB stanovují rozsah auditu, tj. co bude přesně hodnoceno. To může zahrnovat testování bezpečnostních mechanismů, analýzu zranitelností, hodnocení politiky a školení zaměstnanců v oblasti KB.
- *Dodržování právních předpisů:* Audit KB často musí respektovat příslušné právní předpisy. Které se týkají ochrany osobních údajů a KB. Veřejné zakázky by měly obsahovat ustanovení, která zajišťují dodržování všech relevantních právních normativů.
- *Nadstandardní služby:* Některé VZ mohou vyžadovat i nadstandardní služby, jako jsou doporučení pro zlepšení KB, školení zaměstnanců nebo podpora při implementaci bezpečnostních opatření.

Celkově lze říci, že veřejné zakázky v oblasti auditu KB mají za cíl posílit bezpečnostní postupy a zlepšit ochranu kybernetického prostoru ve veřejných institucích a organizacích.

4.4 Nejčastější nedostatky v rámci auditu kybernetické bezpečnosti

Cílem provedených auditů ve sledovaném období 2017-2022 bylo zjištění stavu a ověření souladu s požadavky ZoKB, respektive VoKB v následujících oblastech:

- ***Organizační opatření:*** jako soubor aktivit a procesů, které organizace provádí k minimalizaci rizik v oblasti KB a k ochraně svých IS, dat a aktiv proti kybernetickým hrozbám. Patří sem oblasti systému řízení bezpečnosti informací; politika a organizace bezpečnosti informací; řízení aktiv a rizik; bezpečnost provozu; řízení lidských zdrojů; řízení provozu a komunikací; akvizice, vývoj a údržba systémů; dodavatelské vztahy; řízení přístupu a bezpečné chování uživatelů; řízení incidentů bezpečnosti informací; aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací a kontrola a audit KII a VIS.
- ***Technická opatření:*** jako soubor technologických a technických prostředků, které organizace implementuje k minimalizaci rizik v oblasti KB a k ochraně svých IS, dat a aktiv proti kybernetickým hrozbám. Řadíme sem oblast fyzické bezpečnosti a bezpečnosti prostředí; nástroje pro ochranu integrity komunikačních sítí; nástroje pro ověřování identity uživatelů; nástroje pro řízení přístupových oprávnění; nástroje pro ochranu před škodlivým kódem; nástroj pro zaznamenávání činnosti KII a VIS,

jejich uživatelů a administrátorů; nástroje pro detekci kybernetických bezpečnostních událostí; aplikační bezpečnost; kryptografické prostředky; nástroj pro zajišťování úrovně dostupnosti.

- ***Bezpečnostní dokumentace:*** tato dokumentace je klíčová pro efektivní správu KB organizace a slouží jako základní referenční materiál pro implementaci a dodržování postupů a politik v rámci organizace. [124]

Pro větší přehlednost jsou v následující tabulce uvedena jednotlivá zjištění v prověřovaných oblastech a doplněna o jejich významnost, přičemž použitá klasifikace významnosti sestává ze čtyřstupňového hodnocení:

Tabulka 2 Klasifikace a popis úrovně rizika

Významnost	Popis úrovně rizika
Nízká	Drobné zjištěné skutečnosti, které vyplývají z rozdílů mezi vykonávanými činnostmi a předmětnými předpisy, ale ve svém důsledku nepředstavují významná rizika pro správce KII či VIS, a jsou způsobeny převážně lidským faktorem.
Střední	Systémové nedostatky, které však ve svém důsledku neohrožují činnosti správce KII či VIS, např. nesprávně nastavené postupy nebo jejich nedodržování.
Vysoká	Významné systémové nedostatky, které mají nebo by mohly mít negativní dopad nebo ohrozit činnosti správce KII či VIS, např. nesprávně nastaven vnitřní kontrolní systém nebo jeho nefunkčnost.
Kritická	Zjištění kritické významnosti se zásadním dopadem na funkčnosti činnosti, procesu nebo systému, např. neexistující plány pro řízení kybernetických incidentů nebo nedostatečné reakce na již zjištěné bezpečnostní incidenty.

Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

4.4.1 Souhrnná zjištění nedostatků v období 2017-2022

Souhrnná data, ze kterých byla zpracována analýza nedostatků v rámci provedených auditů KB, znázorňuje následující tabulka. Sledované období je od ledna 2017 do prosince 2022.

[124] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), In: *Sbírka zákonů,* rok 2018, částka 43.

Tabulka 3 Zjištěné nedostatky v rámci auditů kybernetické bezpečnosti

Nedostatky	Kalendářní rok					
	2017	2018	2019	2020	2021	2022
Kritická významnost	1	1	3	1	1	0
Vysoká významnost	4	6	11	3	3	1
Střední významnost	10	16	11	8	9	14
Nízká významnost	7	3	6	12	14	9

Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

Z výsledku tohoto šetření vyplývá, že nejvíce zjištěných nedostatků v rámci jednotlivých auditů jsou zaznamenány v roce 2019, a to celkem ve 31 případech. Zároveň v tomto roce byl i největší podíl nedostatků v kategorii kritické významnosti, které představují závažné riziko pro bezpečnost a integritu IS a dat organizace. Následuje rok 2021 s počtem 27 zjištění, z toho jeden na stupnici kritické významnosti a nejvíce pak v počtu 14 na nízké stupnici. V roce 2018 je to celkem 26 případů, z toho největší počet zjištěných nedostatků je na stupni střední významnosti. Shodně v počtu 24 zjištění je v roce 2020 a 2022. O jeden případ méně pak v roce 2021 a nejméně zjištěných nedostatků náleží prvnímu sledovanému roku 2017, a to v počtu 22 případů. Z uvedených dat dále vyplývá, že největší počet zjištěných nedostatků je na stupni střední významnosti.

Porovnáním údajů z výše uvedené tabulky jsou veškeré zjištěné nedostatky z provedených auditů pro větší přehlednost znázorněny i graficky po jednotlivých letech a data následně interpretována.

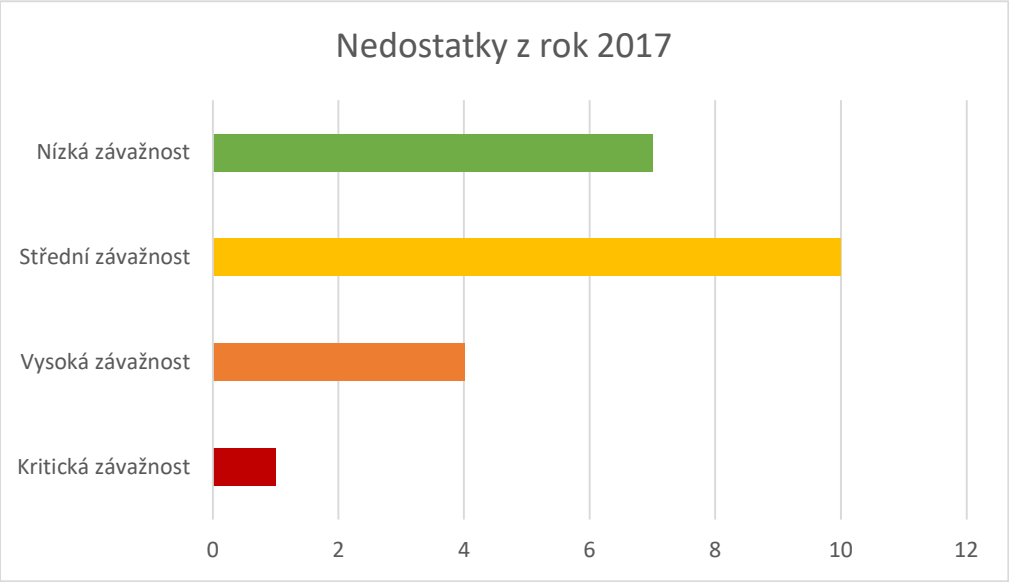
4.4.2 Vyhodnocení auditů za rok 2017

V průběhu roku 2017 bylo provedeno celkem sedm auditů KB. Ověřování zavedení procesů ISMS bylo zaměřeno na dualitu certifikovaného systému řízení bezpečnosti a bezpečnostní dokumentaci, obsazení bezpečnostních rolí a vzdělávání uživatelů, způsob dokumentace, přidělování a odebírání přístupových oprávnění a reakce na KBI. V rámci posuzování souladu vykonávaných činností se auditní tým zaměřil na porovnání aktuálního stavu vnitřních postupů organizace a konkrétní realizaci postupů na systémech tvořících KII s požadavky stanovenými ZoKB a výkladu VoKB.

Na základě provedených auditů lze konstatovat, že největší nedostatky v systémech, které tvoří KII a neodpovídají požadavkům stanoveným ZoKB a výkladu dle VoKB, představují v absenci systému pro sběr a vyhodnocování KBI a nedodržování stanovených požadavků na politiku hesel pro účty na úrovni komunikačních infrastruktury. Tato zjištění nejenže nejsou v souladu s požadavky ZoKB a výkladem VoKB, ale také představují závažné ohrožení nejen KII, ale i celé IT infrastruktury.

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 5 Přehled jednotlivých nedostatků v roce 2017



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci provedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

- ***Nedostatky kritické závažnosti*** spočívající v:
  - Nevyhovující struktuře řídící bezpečnostní dokumentaci.
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Absenci systému pro sběr a systematického vyhodnocení KBI;
  - Analýze rizik před uzavřením smlouvy s dodavatelem KII či VIS;
  - Monitorování a vyhodnocování auditních záznamů;
  - Nedodržování stanovených požadavků na politiku hesel pro účty na úrovni komunikační infrastruktury;
  - Nejednotné politice hesel a jejímu nerespektování.

- ***Nedostatky střední závažnosti*** spočívající v:
  - Stanovení a dokumentaci bezpečnostních požadavků;
  - Funkčnosti vazby mezi analýzou rizik a stanovením bezpečnostních požadavků;
  - Realizaci opatření na základě testů zranitelnosti;
  - Bezpečnostních požadavcích na dodavatele;
  - Sloučení role administrace systémů a správy uživatelů;
  - Nedostatečném zajištění autentizace uživatelů;
  - Nejednotných pravidlech a postupech pro evidenci a řešení incidentů;
  - Duální evidenci bezpečnostních incidentů;
  - Absenci pravidel pro zpracování bezpečnostních událostí a incidentů;
  - Zranitelnosti jednotné virtuální infrastruktury;
  - Konkrétních pravidlech pro zajištění bezpečnosti sítí a aplikací;
  - Plánování a evidenci vzdělávání uživatelů zastávajících role v oblasti KB;
  - Možném přiřazení téhož účtu dvěma různým externím uživatelům;
  - Nezahrnutí role architekta KB v metodice řízení projektů;
  - Neefektivnímu procesu sledování a vypořádávání zjištění v oblasti KB;
  - Neefektivnímu nakládání s utajovanými informacemi;
  - Nezapojení některých bezpečnostních rolí do práce výborů pro řízení KB;
  - Neúčinném plánování rozvoje bezpečnostního povědomí a vzdělávání uživatelů;
  - Neefektivní dokumentaci správy uživatelů a jejich kontroly.
- ***Nedostatky nízké závažnosti*** spočívající v:
  - Anonymizaci dat a testování v produkčních systémech;
  - Nejasnému požadavku na ustanovení o mlčenlivosti a poskytování informací;
  - Nekonzistentní terminologii a odkazech;
  - Neefektivnímu nastavení ISMS;
  - Absenci identifikace procesu řízení změn.

4.4.3 Vyhodnocení auditů za rok 2018

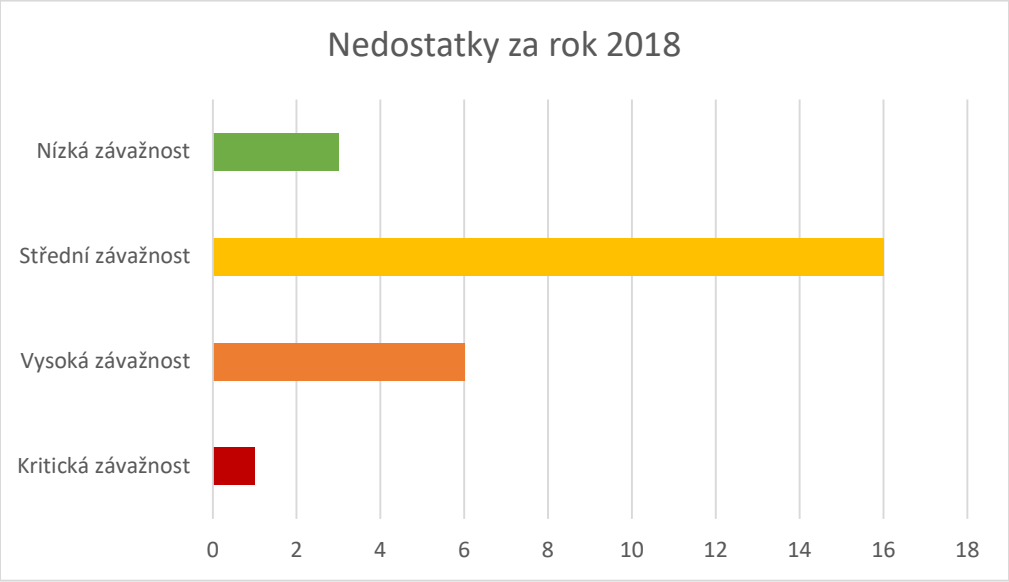
V průběhu roku 2018 bylo provedeno celkem šest auditů KB. Ověřování zavedení procesů ISMS bylo zaměřeno na řízení bezpečnosti informací a bezpečnostní dokumentaci, bezpečnost provozu a komunikací, zvládání kybernetických bezpečnostních událostí

a incidentů, bezpečnostní požadavky na dodavatele a uživatelé systémů, řízení přístupů a bezpečné chování uživatelů. V rámci posuzování souladu vykonávaných činností se auditorský tým zaměřil na porovnání aktuálního stavu vnitřních postupů v organizacích a konkrétních realizaci postupů na systémech tvořících KII, VIS s požadavky stanovenými ZoKB.

Na základě provedených auditů lze konstatovat, že největší slabiny v systémech tvořících KII vůči požadavkům stanovenými ZoKB a výkladu dle VoKB představuje absence přezkoumání ISMS, evidence bezpečnostních opatření, nedostatečná kapacita proxy serverů zabraňující včasnou reakci na hrozbu nákazy škodlivým kódem, absence postupů pro evidenci a systematického vyhodnocování KBI a absence analýzy rizik před uzavřením smlouvy s dodavatelem KII či VIS. Mimo nesoulad s požadavky dle ZoKB a výkladu VoKB představují uvedená zjištění i závažné ohrožení nejen KII, ale také celé IT infrastruktury.

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 6 Přehled jednotlivých nedostatků v roce 2018



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci uvedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

- ***Nedostatky kritické závažnosti*** spočívající v:
  - Nedostatečném řešení oblasti bezpečnosti informací včetně neaktuální analýzy rizik.
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Absenci systematického vyhodnocení KBI z jednotlivých aplikací;
  - Monitorování a vyhodnocování auditních záznamů;
  - Nedostatečné kapacitě serverů;
  - Nemožnosti blokovat nežádoucí síťovou komunikaci;
  - Nedostatečné ochraně komunikace jednotlivých aplikací.
- ***Nedostatky střední závažnosti*** spočívající v:
  - Stanovení a dokumentaci bezpečnostních požadavků;
  - Funkčnosti vazby mezi analýzou rizik a stanovením bezpečnostních požadavků;
  - Realizaci opatření na základě testů zranitelnosti;
  - Bezpečnostních požadavcích na dodavatele;
  - Sloučení role administrace systémů a správy uživatelů;
  - Nedostatečném zajištění autentizace uživatelů;
  - Duální evidenci bezpečnostních incidentů;
  - Absenci pravidel pro zpracování bezpečnostních událostí a incidentů;
  - Zranitelnosti jednotné virtuální infrastruktury;
  - Konkrétních pravidlech pro zajištění bezpečnosti sítí a aplikací.
- ***Nedostatky nízké závažnosti*** spočívajíc v:
  - Anonymizaci dat a testování v produkčních systémech;
  - Nejasnému požadavku na ustanovení o mlčenlivosti a poskytování informací;
  - Nekonzistentní terminologii a odkazech.

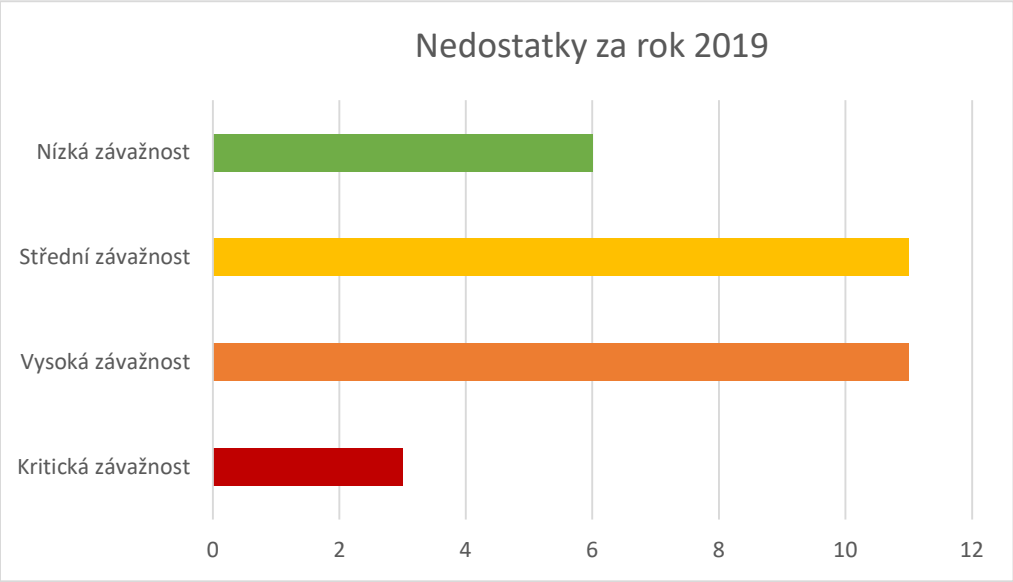
4.4.4 Vyhodnocení auditů za rok 2019

V průběhu roku 2019 bylo provedeno celkem sedm auditů KB. Na základě provedených auditů lze konstatovat, že nejkritičtějším zjištěním je nedostatečné zabezpečení bezdrátové sítě s přístupem do interní infrastruktury. Použitá hesla patří mezi ta, která jsou součástí slovníku uniklých hesel, jež útočníci velmi často využívají. Kromě toho bylo

zjištěno mnoho kritických bezpečnostních problémů na interní síti, zejména v souvislosti s nepodporovanými operačními systémy obsahující zranitelnosti, defaultní hesla na nejrůznějších administračních rozhraní a další zranitelnosti způsobené zejména absencí bezpečnostních aktualizací. V rámci provedených monitoringů lze konstatovat, že vlastnosti skenovaného prostředí a monitorované chování zaměstnanců jednotlivých správců KII a VIS hrubě nesplňují bezpečnostní požadavky stanovené ZoKB.

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 7 Přehled jednotlivých nedostatků v roce 2019



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci uvedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

- ***Nedostatky kritické závažnosti*** spočívající v:
  - Zabezpečení bezdrátové sítě;
  - Bezpečnosti interní sítě;
  - Bezpečnosti webového rozhraní.
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Nesouladu a neúčinném nastavení analýzy rizik;
  - Nejednotné politice hesel a jejímu nerespektování;
  - Monitorování a vyhodnocování auditních záznamů;

- Absenci nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
- Absenci realizace bezpečnostních testů před uvedením do provozu.

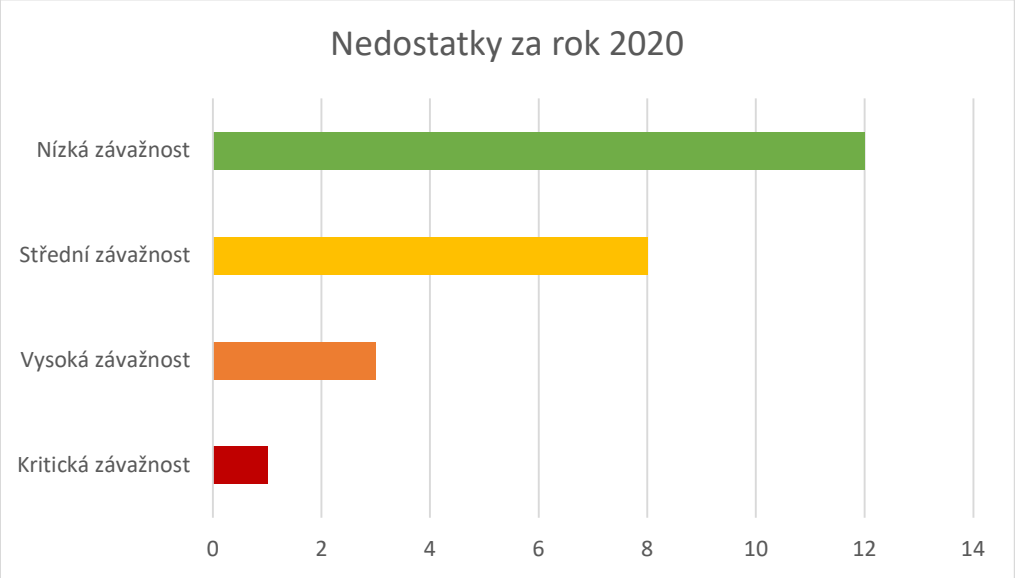
- ***Nedostatky střední závažnosti*** spočívající v:
  - Nastavení metodik pro výpočet rizika;
  - Nedostupnosti jednotné dokumentace autorizační politiky;
  - Nedostupné evidenci bezpečnostních událostí a incidentů pro systémy tvořící KII;
  - Absenci ochrany infrastruktury před škodlivým kódem;
  - Nerespektování politiky pro klasifikaci aktiv;
  - Nerespektování politiky řízení přístupů;
  - Absenci evidence bezpečnostních událostí a incidentů;
  - Bezpečnosti externího perimetru;
  - Sociálním inženýrství.
- ***Nedostatky nízké závažnosti*** spočívajíc v:
  - Obecných zásadách hodnocení důležitosti primárních aktiv;
  - Duplicitní definici požadavků na opatření fyzické bezpečnosti;
  - Absenci pravidel pro bezpečnostní dokumentaci.

4.4.5 Vyhodnocení auditů za rok 2020

V průběhu roku 2020 bylo provedeno celkem pět auditů KB. Na základě provedených auditů lze konstatovat, že největší slabiny v systémech tvořících KII vůči požadavkům stanovenými ZoKB a výkladu dle VoKB představuje nesystematické řešení oblasti informační bezpečnosti. Vytvořený formální rámec na úrovni bezpečnostního řádu a souvisejících dokumentů není řádně naplňován a není vedena příslušná dokumentace, není plně využito možností ochrany vnitřního prostředí před kritickými hrozbami útoků a nežádoucích aktivit.

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 8 Přehled jednotlivých nedostatků v roce 2020



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci uvedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

- ***Nedostatky kritické závažnosti*** spočívající v:
  - Nedostatečné struktuře řídící bezpečnostní dokumentaci.
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Nedostatečném definování plnohodnotné bezpečnostní strategie;
  - Aktuálním problematickém stavu na pozici Bezpečnostního manažera;
  - Nedostatečném systematickém řešení oblasti informační bezpečnosti.
- ***Nedostatky střední závažnosti*** spočívající v:
  - Řízení rizik spojených s dodavateli;
  - Neaplikovaném jednotném systematickém přístupu k hodnocení rizik;
  - Nepostupováním dle platné řídicí dokumentace dodavatelem služby;
  - Nevhodné kombinaci algoritmů dohod na klíči a šifrování klíčů;
  - Neúplném oddělení rozvoje a provozu;
  - Absenci katalogu poskytovaných služeb;
  - Nedostatečném nastavení procesů řízení včetně řízení incidentů a změn;
  - Absenci příslušné bezpečnostní dokumentace.
- ***Nedostatky nízké závažnosti*** spočívajíc v:
  - Struktuře plánu rozvoje bezpečnostního povědomí;

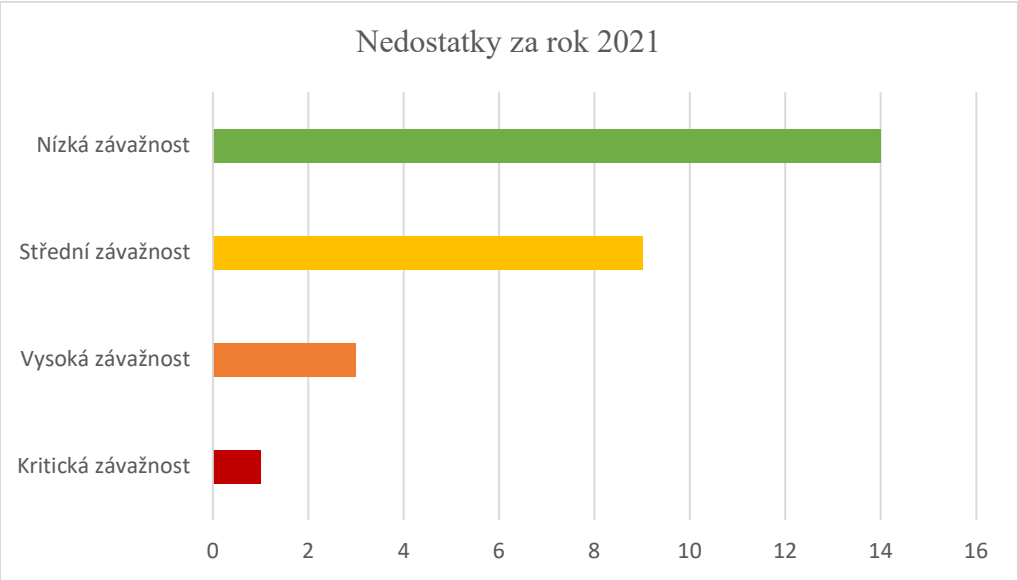
- Absenci řízení přístupu do sítě;
- Nedostatečné pravidelné aktualizaci OS a systematický hardening;
- Absenci bezpečnostního dohledu;
- Provozování historických technologií;
- Existenci špatných primárních skupin pro uživatele;
- Existenci účtů bez hesla;
- Vysokém počtu neaktivních / nepoužívaných účtů;
- Velmi vysokém počtu účtů bez expirace hesel.

4.4.6 Vyhodnocení auditů za rok 2021

V průběhu roku 2021 bylo provedeno celkem pět auditů KB. Na základě provedených auditů lze konstatovat, že největší slabiny v systémech tvořících KII vůči požadavkům stanovenými ZoKB a výkladu dle VoKB představuje nesystematičnost v bezpečnostní dokumentaci, bezpečnostní politika není formálně schválena a procesy řízení neprobíhají v souladu s touto politikou, nejsou zpracovány havarijní plány pro klíčovou infrastrukturu a zálohování a kontrola záloh neprobíhá všude v souladu s platnou řídící dokumentací.

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 9 Přehled jednotlivých nedostatků v roce 2021



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci uvedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

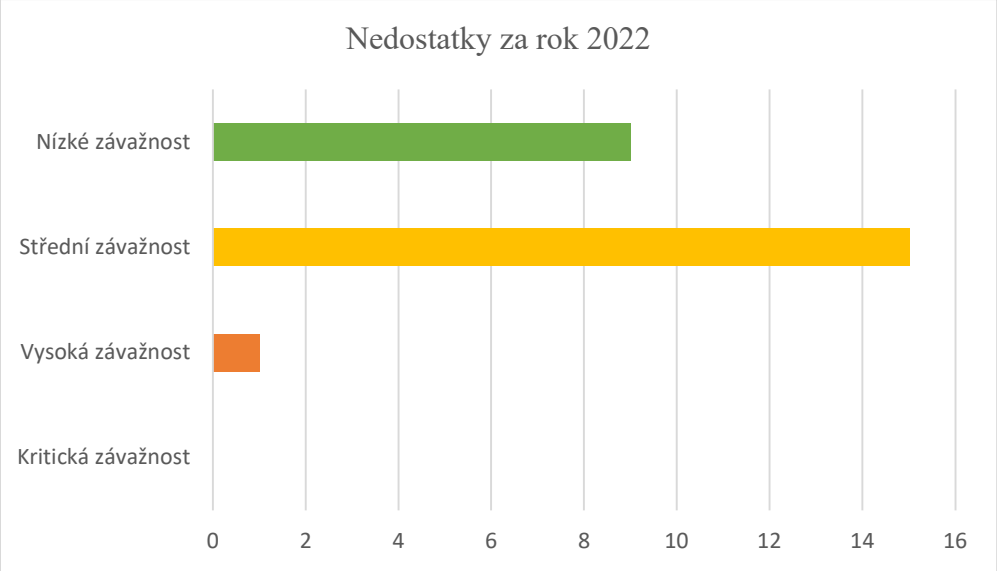
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Neshodě s bezpečnostní dokumentací v oblasti identifikace a hlášení bezpečnostních incidentů.
- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Absenci nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
  - Analýze rizik před uzavřením smlouvy s dodavatelem KII či VIS;
  - Monitorování a vyhodnocování auditních záznamů.
- ***Nedostatky střední závažnosti*** spočívající v:
  - Stanovení požadavků a dokumentaci bezpečnostních požadavků;
  - Funkčnosti vazby mezi analýzou rizik a stanovením bezpečnostních požadavků;
  - Realizaci opatření na základě testů zranitelnosti;
  - Bezpečnostních požadavcích na dodavatele;
  - Sloučení role administrace systémů a správy uživatelů;
  - Nedostatečném zajištění autentizace uživatelů;
  - Duální evidenci bezpečnostních incidentů;
  - Absenci pravidel pro zpracování bezpečnostních událostí a incidentů;
  - Zranitelnosti jednotné virtuální infrastruktury;
  - Konkrétních pravidlech pro zajištění bezpečnosti sítí a aplikací;
  - Používání Flash disků, které je z pohledu KB považováno za vysoce rizikové;
  - Nesystematickému řízení rizika při řízení změn;
  - Absenci vyhodnocování rizikovosti dodavatelů;
  - Nedostatečném zpracování plánu obnovy pro zajištění kontinuity činností.
- ***Nedostatky nízké závažnosti*** spočívajíc v:
  - Anonymizaci dat a testování v produkčních systémech;
  - Nejasnému požadavku na ustanovení o mlčenlivosti a poskytování informací;
  - Nekonzistentní terminologii a odkazech;
  - Nedostatečném rozpracování jednotlivých politik a jejich schvalování;
  - Požadavky VoKB nejsou aplikovány v celém rozsahu ISMS.

4.4.7 Vyhodnocení za rok 2022

V průběhu roku 2022 bylo provedeno celkem pět auditů KB. Na základě provedených auditů lze konstatovat, že největší slabinou v systémech tvořících KII vůči požadavkům stanovenými ZoKB a výkladu dle VoKB je absence nástroje pro sběr, monitorování a vyhodnocování kybernetických bezpečnostních incidentů a dále nenaplňování požadavků ochranného opatření NÚKIB vydaného dne 10.1.2023, které stanovuje způsoby ochrany IS a směřuje k zajištění důvěrnosti a integrity elektronické pošty a k zamezení podvržení elektronické pošty při komunikaci mezi povinnými osobami.[125]

V následujícím grafu jsou prostřednictvím statistického šetření detailně zobrazeny jednotlivé nedostatky v rámci provedených auditních šetření.

Graf 10 Přehled jednotlivých nedostatků v roce 2022



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

V rámci uvedené auditní akce zjistil auditorský tým následující nejčastější nedostatky:

V tomto roce nebyly identifikovány žádné nedostatky kritické závažnosti.

- ***Nedostatky vysoké závažnosti*** spočívající v:
  - Absenci nástroje pro sběr, monitorování a vyhodnocování KBI.
- ***Nedostatky střední závažnosti*** spočívající v:
  - Nenaplňování požadavku ochranného opatření NÚKIB;

[125] ISVS.CZ. *Ochranné opatření k zabezpečení e-mailové komunikace.* [online]. 2023 [cit. 2024-01-20]. Dostupné z: https://www.isvs.cz/ochranne-opatreni-k-zabezpeceni-e-mailove-komunikace/.

- Rozdílném havarijním plánu;
- Řadě nedostatků v rámci fyzické bezpečnosti;
- Absenci ověřování přístupových oprávnění;
- Absenci procesu pro kontrolu uniklých hesel uživatelů;
- Nedostatečné kontrole odchozí komunikace z vnitřního prostředí do externích sítí, a to včetně prostředí internetu;
- Nedostatečném antivirovém řešení;
- Absenci technologie proti škodlivému obsahu;
- Expirace bezpečnostních certifikátů;
- Absenci nastavení a konsolidace domény organizace;
- Absenci bezpečnostního dohledu.

- Nedostatky nízké závažnosti spočívajíc v:
  - Absenci ověřování identity na některá připojovaná zařízení;
  - Absenci nástroje na monitorování datových toků;
  - Absenci testování havarijních plánů;
  - Absenci dokumentace o bezpečnostních zónách;
  - Absenci provádění penetračního testování v rámci aplikační bezpečnosti.

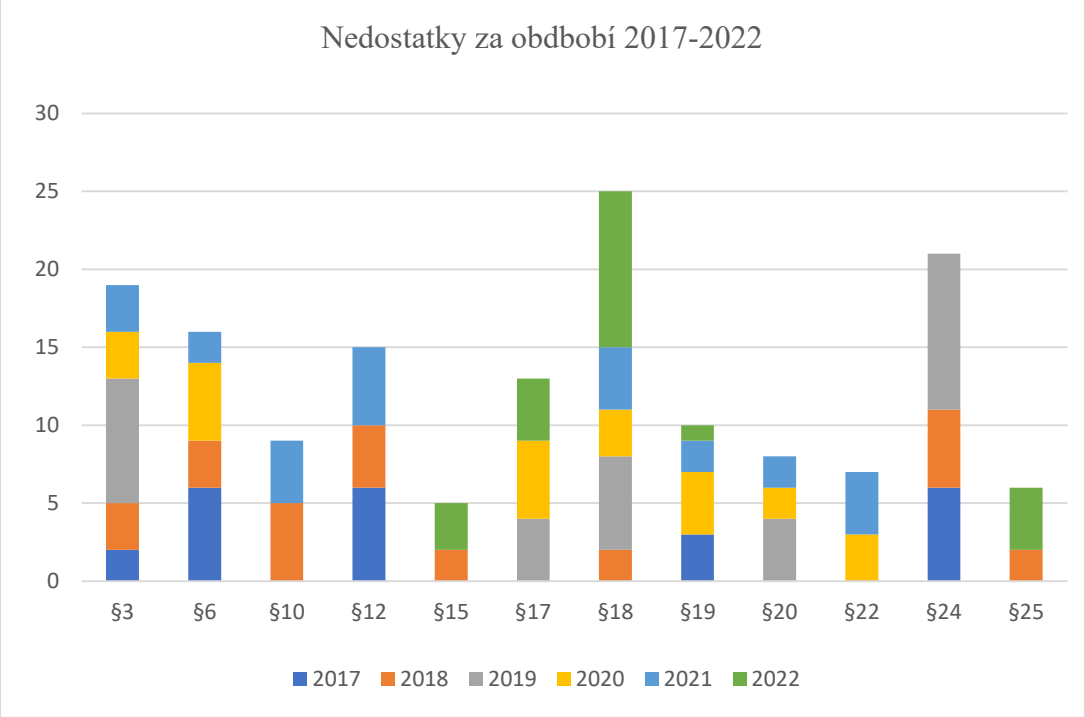
5 Zhodnocení a doporučení

V praktické části diplomové práce byla prostřednictvím sběru dat provedena analýza jednotlivých nedostatků v rámci realizovaných auditů KB za období 2017–2022. Následující kapitola uvádí klasifikaci a interpretaci závažných nedostatků, jež jsou v rozporu s požadavky ZoKB, resp. VoKB.

5.1 Shrnutí hlavních zjištěných nedostatků

Ve sledovaném období 2017–2022 byly zjištěné nedostatky komparovány a následně vytipovány nejčastěji se opakující. Ty jsou dále seřazeny dle míry závažnosti včetně vhodných navrhovaných doporučení. Celkové vyhodnocení jednotlivých oblastí je zobrazeno v následujícím grafu.

Graf 11 Nejčastější nedostatky za období 2017–2022



Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

Porovnáním dat z grafu je zřejmé, že největší počet nedostatků je identifikován v **§ 18**, a to v oblasti *„Bezpečnosti komunikačních sítí“*, která zahrnuje bezpečnostní opatření a technologie určené k ochraně dat, informací a komunikační infrastruktury před neoprávněným přístupem, manipulací a škodlivými útoky. Celkově bylo zjištěno dvacet pět pochybení a v této oblasti byl i největší počet kritických nálezů. O čtyři nedostatky méně bylo nalezeno v **§ 24** v oblasti *„Sběru a vyhodnocování kybernetických bezpečnostních*

událostí“. Jde o proces monitorování, analýzy a vyhodnocování kybernetických bezpečnostních událostí. Cílem je identifikovat a reagovat na bezpečnostní hrozby co nejrychleji a nejúčinněji. Následuje chybovost v devatenácti případech v **§ 3** v oblasti „*Systému řízení bezpečnosti informací“*. Jedná se o systematický přístup k ochraně důvěrných informací v organizaci zahrnující stanovení politik, identifikaci a hodnocení rizik, implementaci kontrol a opatření, pravidelnou revizi politik a vylepšování bezpečnostního povědomí. V **§ 6** bylo identifikováno šestnáct nedostatků, a to v oblasti „*Organizační bezpečnosti“* zabývající se implementací politik, procesů a postupů v organizaci pro ochranu aktiv, dat a informací před neoprávněným přístupem, škodlivými útoky a dalšími hrozbami. Patnáct pochybení bylo nalezeno v **§ 12** v oblasti „*Řízení přístupů a bezpečného chování uživatelů“* zaměřené na řízení přístupu k IS a podporou bezpečného chování uživatelů prostřednictvím autentizace, autorizace a vytváření povědomí o bezpečnostních hrozbách. V **§ 17** se chybovalo třináctkrát, a to v oblasti „*Fyzické bezpečnosti“* zaměřené na ochranu fyzických aktivit, infrastruktury a osob před neoprávněným přístupem, poškozením nebo zničením pomocí opatření jako jsou bezpečnostní kamery, alarmy či bezpečnostní služby. Deset nedostatků pak bylo identifikováno v **§ 19**, jde o oblast „*Správy a ověřování identit“* zahrnující procesy a technologie pro řízení přístupu uživatelů a zařízení k IS, včetně autentizace, autorizace a správy digitálních identit s cílem zajistit bezpečný a důvěryhodný přístup. V **§ 10** v oblasti „*Řízení provozu a komunikací“* zajišťující bezpečný provoz IKS a stanovující provozní pravidla a postupy pro zajištění bezpečného provozu IS KII, KS KII VIS, provádění pravidelného zálohování a prověřování použitelnosti provedených záloh bylo identifikováno devět nedostatků. Osm pochybení bylo zjištěno v **§ 20** v oblasti „*Řízení přístupových oprávnění“* zabývající se procesem správy a řízení přístupových práv uživatelů ke zdrojům IS prostřednictvím definování, správy a monitorování oprávnění a rolí. V **§ 22** v oblasti „*Zaznamenání událostí IKS, jeho uživatelů a administrátorů“* jako procesu monitorování, sběru a uchování informací o aktivitách přístupu a chování uživatelů a administrátorů IKS za účelem sledování bezpečnostních událostí, auditu a vývoje politik a postupů v oblasti KB bylo identifikováno sedm pochybení. V **§ 25** v oblasti „*Aplikační bezpečnost“* bylo zaznamenáno šest nedostatků. Tato oblast se zaměřuje na ochranu softwarových aplikací před různými bezpečnostními hrozbami a útoky prostřednictvím implementace bezpečnostních opatření, jako je kódování, autorizace a řízení přístupu s cílem minimalizovat rizika spojená s možnými zranitelnostmi a útoky. Nejméně, a to pět

nedostatků, bylo identifikováno v **§ 15,** oblasti *„Řízení kontinuity činností"* zahrnující plánování a implementaci opatření, která umožňují organizaci pokračovat v provozu, a i při výskytu mimořádných událostí či krizových situacích tak, aby minimalizovala dopady na svou činnost a zákazníky.

5.1.1 Bezpečnostní opatření

Bezpečnostní opatření se přijímají k minimalizaci rizika ztráty, poškození nebo neoprávněného přístupu k datům, informacím nebo systémům organizace. Hodnocení bezpečnostních opatření bylo provedeno v rozsahu rámce bezpečnostních opatření, která jsou vyžadována v souladu se ZoKB a jeho prováděcího právního předpisu VoKB. V následující tabulce je uveden počet nedostatků v jednotlivých oblastech získaný prostřednictvím komparace dat.

Tabulka 4 Nejčastější nedostatky v oblasti Bezpečnostní opatření za období 2017–2022

Paragraf	Oblast	Počet zjištění
§ 3	Systém řízení bezpečnosti informací	19
§ 6	Organizační bezpečnost	16
§ 10	Řízení provozu a komunikací	9
§ 12	Řízení přístupů	15
§ 15	Řízení kontinuity činností	5

Zdroj: Interní data společnosti BDg, zpracování: vlastní práce

Následuje interpretace klíčových nedostatků dle vybraných paragrafů včetně navrhovaných doporučení.

Z výše uvedené tabulky vyplývá, že největší počet nedostatků byl identifikován v **§ 3**, a to především v nedostatečném řízení bezpečnosti informací včetně neaktuální analýzy rizik, nekompletní bezpečnostní dokumentace a dalších návazných politik.

- *Zjištění kritické závažnosti – Nedostatečné nastavení systému řízení bezpečnosti informací, neprovedeno přezkoumání a absence pravidel či zastaralá bezpečnostní dokumentace a další návazná dokumentace*

Stávající nastavení systému řízení bezpečnosti informací je nedostatečné, bezpečnostní politika a další návazná dokumentace nejsou vytvořeny v souladu s požadavky ZoKB a VoKB. Není zajištěno vyhodnocení účinnosti systému, které obsahuje hodnocení stavu, posouzení výsledků provedených kontrol a auditů KB. Pravidla a postupy pro přezkoumání neobsahují hodnocení výkonnosti systému a stanovený způsob měření. Hlavní bezpečnostní

cíle nejsou rozpracovány do navazujících dokumentů nebo zcela chybí. Neprobíhá vyhodnocení řízení rizik a významné změny nejsou řízeny v rámci dokumentace jednotlivých systémů IS. Byly zjištěny výskyty vzájemně si odporující a zastaralá dokumentace, dále identifikovány nedostatky pokrytí rizik a bezpečnostních hrozeb, nedostatečná ochrana citlivých informací či nejasný plán krizového řízení.

Doporučení → Revidovat model nasazení nástroje pro podporu ISMS. Provést revizi a aktualizaci bezpečnostních politik a postupů organizace tak, aby plně odpovídaly požadavkům ZoKB a VoKB. Definovat jasné požadavky na tvorbu bezpečnostní dokumentace, např. podrobný popis zajištění technické bezpečnosti, analýzu bezpečnostních rizik a hrozeb včetně návrhu opatření. Revidovat nastavený způsob a realizovat pravidelné přezkoumání ISMS. Rozpracovat strategické cíle vyplývající ze ISMS a nadefinovat metriky pro jednotlivé cíle, které umožní pravidelné ověřování jejich plnění. Zajistit pravidelnou revizi a aktualizaci bezpečnostní dokumentace v souladu s aktuálními normami a požadavky VoKB. Implementovat postupy pro zálohování a archivaci bezpečnostní dokumentace tak, aby byla zajištěna integrita a dostupnost.

Následuje chybovost v § **6** v oblasti Organizační bezpečnosti, a to v nedostatečném určení bezpečnostních rolí a jejich zastupitelnosti či úplné absenci dokumentace jednotlivých pravomocí bezpečnostních rolí, jejich práv a povinností.

- *Zjištění vysoké závažnosti – Absence dokumentace rolí informačního systému, nezapojení bezpečnostních rolí do práce výborů, absence role architekta v metodice řízení projektů*

Není dostupný popis postupů administrace uživatelů a v IS chybí definice rolí. Projektový tým nedisponuje rolí odpovědnou za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena. Nezapojení některých bezpečnostních rolí do práce Výborů pro řízení KB, jako je role auditora, garantů aktiv či architekta KB. Taktéž chybí účinná kontrolní funkce pro sledování plnění přijatých nápravných opatření. Tento nedostatek představuje riziko omezené schopnosti reagovat na bezpečnostní hrozby.

Doporučení → Revidovat dokumentaci systému a zajistit, aby popis rolí a způsob jejich přidělování odpovídal reálnému nastavení rolí. Zahrnout osobu odpovědnou za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena. Nastavit

role a účast jednotlivých osob v rámci Výboru pro řízení KB tak, aby byla zajištěna jejich zastupitelnost a bylo možné realizovat plánovaná jednání výboru.

V **§ 12** jde především o nedostatečné zajištění přístupu a správy uživatelů či absence dokumentace správy uživatelů a rolí IS včetně jejich kontroly.

- *Zjištění kritické závažnosti – Nerespektování politiky řízení přístupů, neefektivní a nejednotná dokumentace správy uživatelů a jejich kontroly*

V některých systémech KII existují sdílené účty s různými typy oprávnění pro správu a nastavení systému, u kterých nelze jednoznačně identifikovat uživatele. Nejsou zdokumentovaná přístupová práva a identifikace uživatele. Pravidelné přezkoumání nastavení přístupových oprávnění není prováděno v souladu s vnitřními předpisy organizace, což zvyšuje riziko bezpečnostních incidentů.

Doporučení → Provést revizi a aktualizaci bezpečnostních politik a postupů organizace tak, aby plně odpovídaly požadavkům ZoKB a VoKB. Současně je třeba provést pravidelné přezkoumání nastavení přístupových oprávnění a sdílených účtů v systémech KII, s důrazem na odstranění neidentifikovaných uživatelů, včetně rozdělení jednotlivých uživatelů do přístupových skupin nebo rolí v souladu se stanovenou politikou. Dále je nezbytné stanovit jasné odpovědnosti a role v oblasti správy bezpečnostního systému a dokumentace, aby se minimalizovala možnost kolizí v odpovědnosti jednotlivých rolí. S ohledem na platné ustanovení bezpečnostní politiky oddělit přiřazení oprávnění jednotlivých uživatelů od vlastní administrace aplikace.

Nejčastějším pochybením v § **10** byla absence či neaktuální dokumentace provozních činností či postupů pro ověření bezpečnosti provozu a komunikace a postupu přidělování a odebírání přístupových oprávnění.

- *Zjištění vysoké závažnosti – Chybějící či neaktuální dokumentace provozních činností, přidělování a odebírání přístupů či nefunkční řízení kapacit, nedodržování zajištění odebrání přístupových oprávnění při ukončení nebo změně smluvního vztahu*

Při ověřování záznamů o provedených zálohách a jejich testování byl zjištěn nesoulad mezi dokumentem Politika řízení provozu a komunikací, Provozní pravidla a postupy pro IS KII a VIS a Provozní deník. Pro některé systémy nebyly doloženy dokumentace provozních postupů a v seznamu relevantních osob byly neplatné kontakty na pracovníky odboru IT.

Nebyly taktéž doloženy záznamy v provozním deníku o provedených zálohách a jejich testování za sledované období. Nejsou dodržována pravidla v odebírání přístupových oprávnění při ukončení či změně smluvních vztahů.

Doporučení → Dodržovat postupy stanovení vnitřními předpisy a jednotlivé provozní činnosti realizovat a dokumentovat formou záznamů či plánů v provozním deníku. Formalizovat a sjednotit postupy a pravidla pro řízení, schvalování a evidenci provozních změn. Revidovat nastavení procesu řízení kapacit a zahnout mimo technické zdroje rovněž i lidské zdroje. Provést a revidovat pravidla pro směrování komunikace v rámci jednotlivých sítí organizace. Aktualizovat přístupová oprávnění s ohledem na ukončení či změnu smluvního vztahu u jednotlivých zaměstnanců.

V **§ 15** bylo nejvíce nedostatků identifikováno v absenci systematického testování systému řízení kontinuity včetně havarijních plánů.

- *Zjištění vysoké závažnosti – Zranitelnost jednotné virtuální infrastruktury, konkrétní pravidla pro zajištění bezpečnosti sítí a aplikací*

V případě výpadku či napadení je současně postiženo celé prostředí virtuální infrastruktury včetně zálohovacích systémů. Správci tak nejsou schopni zajistit postupy dle havarijních plánů a nemusejí být o podstatě, příčinách a stavu výpadku relevantně informováni. K dispozici je jen omezená dokumentace kontinuity na úrovni havarijního plánu pro danou lokalitu obsahující nevyhovující postup obnovy v případě kritických situací. Nejsou prováděny testy kontinuity.

Doporučení → Zvážit nasazení technologií, které zajistí v případě napadení či chyby na úrovni virtuální infrastruktury její částečnou izolaci a zamezí nekontrolovanému šíření problému napříč všemi využitými fyzickými servery. Konsolidovat havarijní plány lokality pro dané oblasti v souladu se strukturou a obsahem předepsanou politikou havarijního plánování. Po konsolidaci dokumentace zajistit pravidelné testování havarijních plánů. Zajistit pravidelné seznamování pracovníků IT s dostupností, se strukturou a obsahem pro ně relevantní dokumentace při řešení obnovy kontinuity.

5.1.2 Technická opatření

Technická opatření jsou specifické postupy či metody používané k ochraně IS, dat nebo zařízení. Cílem je minimalizovat rizika spojená s bezpečností a zajištění integrity, dostupnosti a důvěrnosti dat a systémů. Hodnocení technických opatření bylo provedeno

v rozsahu rámce technických opatření, která jsou vyžadována v souladu se zákonem ZoKB a jeho prováděcího právního předpisu VoKB. V následující tabulce je uveden počet nedostatků v jednotlivých oblastech získaný prostřednictvím komparace dat.

Tabulka 5 Nejčastější nedostatky v oblasti Technická opatření za období 2017-2022

Paragraf	Oblast	Počet zjištění
§ 17	Fyzická bezpečnost	13
§ 18	Bezpečnost komunikačních sítí	25
§ 19	Správa a ověřování identit	10
§ 20	Řízení přístupových oprávnění	8
§ 22	Zaznamenání IKS, jeho uživatelů a administrátorů	7
§ 24	Sběr a vyhodnocování kybernetických bezpečnostních událostí	21
§ 25	Aplikační bezpečnost	6

Zdroj: vlastní zpracování, Interní data společnosti BDg, zpracování: vlastní práce

Následuje interpretace klíčových nedostatků dle vybraných paragrafů včetně navrhovaných doporučení.

Z výše uvedené tabulky vyplývá, že největší počet nedostatků byl identifikován v **§ 18**, a to především v pravidlech pro zajištění bezpečnosti sítí a aplikací a v nedostatečné ochraně IS a zabezpečení síťové infrastruktury.

- *Zjištění kritické závažnosti – Slabé zabezpečení WI-FI sítě, bezpečnost interní sítě a webového rozhraní*

Nejkritičtějším nálezem je slabé zabezpečení WI-FI sítě s přístupem do interní infrastruktury pomocí hesla, která jsou součástí slovníku uniklých hesel, jenž útočníci velmi často využívají. Mnoho kritických bezpečnostních problémů bylo zjištěno i na interní síti a webového rozhraní. Zejména nepodporované operační systémy, defaultní hesla na nejrůznějších administračních rozhraních a další zranitelnosti způsobené většinou absencí bezpečnostních aktualizací.

Doporučení → Zabezpečit WI-FI sítě bezpečnými hesly, omezit prostupy do interní infrastruktury, případně nasadit autentizaci uživatelů na WI-FI s prostupem do interní sítě. Změnit všechna defaultní hesla a konfigurovat systémy s ohledem na bezpečnost, včetně instalace bezpečnostních aktualizací. Pravidelně aktualizovat operační systémy. Monitorovat bezpečnostní události, pravidelně vyhodnocovat a odstraňovat detekované problémy nalezené v rámci penetračního testování.

O čtyři nedostatky méně pak bylo nalezeno v **§ 24** v nedostatečném nasazení a používání nástroje pro sběr a vyhodnocování jednotlivých bezpečnostních událostí a incidentů.

- *Zjištění kritické závažnosti – Nedostatečné monitorování a vyhodnocování auditních záznamů, nejednoznačná identifikace bezpečnostního incidentu, neprobíhající automatické vyhodnocení a nezaznamenání všech nalezených incidentů,*

Nástroj pro sběr a vyhodnocení KBI není plně implementován. Vyhodnocování incidentů probíhá nepravidelně s ohledem na čas a personální kapacity. Dokumentace jednotlivých IS týkající se KB není dostatečně podrobná a neupřesňuje postupy pro detekci, vyhodnocování a řešení incidentů. Řešení incidentů probíhá ad-hoc bez klasifikace a definovaných pravidel pro hlášení. To představuje riziko, kdy správci jednotlivých KII nejsou dostatečně připraveni na KBI a nebudou tak schopni včas zareagovat na probíhající útoky.

Doporučení → Dokončit stávající implementaci nástroje pro centralizované ukládání a správu systémových a bezpečnostních logů, který zajistí monitorování a vyhodnocování bezpečnostních záznamů KII a příslušné infrastruktury v reálném čase. Definovat pravidla a kritéria pro zaznamenání a hodnocení bezpečnostních incidentů a určení jejich závažnosti. Po dokončení implementace nástroje pro detekci realizovat výběr nástroje pro sběr a průběžné vyhodnocování KBI včetně včasného varování.

Třináct zjištění lze nalézt v **§ 17**, a to v nedostatečné ochraně vnitřního prostředí před hrozbami útoků a nežádoucích aktivit.

- *Zjištění kritické závažnosti – Není plně využito možností ochrany vnitřního prostředí před kritickými hrozbami útoků a nežádoucích aktivit, absence dokumentace a aplikace opatření v oblasti fyzické bezpečnosti včetně identifikace bezpečnostních zón*

Není realizovaná dostatečná segmentace a ochrana vnitřní sítě před připojením neoprávněných zařízení, zejména s ohledem na rozdílné bezpečnostní zóny. Nejsou dostatečně detekovány nežádoucí aktivity a kontrola hrozeb na vnitřní síti. Nebyla předložena dokumentace, která by zahrnovala stanovení zón v dané lokalitě a aplikovaná opatření fyzické bezpečnosti v jednotlivých zónách. Ani v serverovně není evidován vstup zaměstnanců s tím, že klíč ke vstupu je volně k dispozici všem pracovníkům IT. Serverovna je umístěna v prostorech, které pro tyto účely nejsou plně vyhovující.

Doporučení → Posílit ochranu vnitřního prostředí před kritickými hrozbami útoků a nežádoucích aktivit. Realizovat důslednou segmentaci vnitřní sítě tak, aby byla oddělena zařízení patřící do různých bezpečnostních zón. Jednotlivé bezpečnostní zóny důsledně oddělit firewallem s restriktivní bezpečnostní politikou. Využívat dostupné možnosti ochrany proti útokům. U všech aplikací využívat výhradně šifrovanou komunikaci. Zajistit řízení vstupu včetně automatizované identifikace vstupující osoby, záznamu o vstupu a pobytu osoby v serverovně a případné předávání těchto informací k záznamu a sledování centrálním dohledovým systémům. V rámci celé organizace připravit typizovaný vzor dokumentace, která by zahrnovala stanovení zón v dané lokalitě a aplikovaná opatření fyzické bezpečnosti v jednotlivých zónách. Zvážit úpravu použitých prostor případně jiné umístění serverovny.

Deset nedostatků bylo identifikováno v **§ 19** v oblasti Správa a ověřování identit.

- *Zjištění vysoké závažnosti – Nedodržování stanovených požadavků a nejednotná politika hesel, existence účtů bez hesla, vysoký počet neaktivních/nepoužívaných účtů, velmi vysoký počet účtů bez expirace hesla*

Jednotlivé bezpečnostní politiky udávají rozdílné nastavení politiky hesel, která jsou v některých případech v rozporu s platnou legislativou. Přístupové údaje pro technické účty nejsou generovány automaticky a dochází k jejich ručnímu zadávání. Existuje riziko kompromitace takto nastavených oprávnění. Nejsou stanoveny jednotné zásady pro obsluhu technických účtů v případě krizové situace. Pro aplikace a různé části infrastruktury existují odlišné postupy. Použití lokálních účtů není nijak omezeno ani sledováno. Hesla jsou generována správcem bez nastavených politik vynucujících délku a složitost (ta je kontrolována ručně). Pro účty je nastavena minimální délka hesla 8 znaků, což je v rozporu s požadavky VoKB. Při ověřování byl zjištěn vysoký počet nastavení účtů s absencí hesla. Toto nastavení představuje vysoké bezpečnostní riziko, protože účet není dostatečně chráněn. Byla zjištěna existence účtů, které mají nastavené heslo bez expirace a vysoký počet neaktivních účtů

Doporučení → Nastavit jednotnou politiku pro hesla v souladu s legislativou. Evidovat nastavené zásady a doplnit jednotné postupy pro technické účty a účty do komunikační sítě. V případech, kdy není technicky možné vynutit příslušné nastavení (například minimální doba platnosti hesla pro síťový prvek) aplikovat kontrolní mechanismy (automatický sběr a vyhodnocování auditních záznamů), které budou riziko zneužití uvedených účtů

eliminovat. Zvážit nastavení nového serveru, který bude navázán na již funkční procesy a bude sloužit k ověřování uživatelů a řízení přístupových identit. Provést změnu atributu u všech účtů, které nejsou používány. Revidovat počet neaktivních účtů a následně provádět průběžné sledování tohoto typu účtů s cílem maximálního omezení jejich počtu. Prověřit existující účty bez expirace a tam, kde to je možné, expiraci nastavit. Počet účtů bez expirace udržovat na co nejnižší úrovni.

V **§ 20** bylo nalezeno osm závažných zjištění, a to převážně v řízení přístupových oprávnění.

- *Zjištění vysoké závažnosti – Absence řízení přístupu do sítě, stáří hesla*

Není dostatečně kontrolována datová komunikace, která odchází z vnitřních sítí do externích prostředí včetně komunikace směřující do internetu. Kontrolována není zejména šifrovaná komunikace. Daný stav výrazně zvyšuje jedno z nejzásadnějších současných rizik, kterým je nežádoucí a nedetekovaný únik citlivých a důvěrných dat a informací mimo prostředí organizace.

Doporučení → Technologicky a procesně zajistit kontrolu datové komunikace odcházející z vnitřních sítí do externích prostředí, zejména potom do internetu. Vybudovat nebo posílit bezpečnostní monitoring tak, aby odpovědní správci měli včasnou informaci o případném probíhajícím útoku a mohli na něj účinně reagovat. U všech aplikací využívat výhradně šifrovanou komunikaci.

Celkem sedmkrát se chybovalo v **§ 22**, a to především v nedostatečném zaznamenání, zpracování a evidenci všech nalezených bezpečnostních incidentů.

- *Zjištění vysoké závažnosti – Absence pravidel pro zpracování a evidenci bezpečnostních událostí a incidentů, duální evidence bezpečnostních incidentů*

Informace o incidentech jsou posílány i elektronickou poštou a dokumentovány nahodile bez stanovených pravidel. Nejsou stanoveny pravidla či hranice, kdy mají být zaznamenány evidence bezpečnostních incidentů. Řešení KBI probíhá ad-hoc, prošetřování příčin je realizováno s ohledem na dostupné personální kapacity a znalosti. Opatření jsou aplikována s ohledem na dostupné zdroje. Nejsou zpracovány konkrétní postupy a kritéria, kdy je událost zaznamenána jako bezpečnostní incident, analyzována a na základě této analýzy jsou přijata nápravná opatření. Absence pravidel a jejich jasná komunikace směrem k uživatelům může vést buď k nadbytečnému hlášení jednotlivých bezpečnostních

událostí či jejich ignoraci. Opakované zadávání dat a evidence bezpečnostních incidentů ve dvou různých systémech je neefektivní, náročné na kapacitu pracovníků v bezpečnostních rolích a může vést k chybám při analýze a řešení bezpečnostních incidentů.

Doporučení → Formalizovat kritéria pro členění KBI do kategorií z hlediska důležitosti bezpečnostních incidentů do kategorií z hlediska důležitosti dotčených aktiv, dopadů na poskytované služby KII, dopadů na služby poskytovanými jinými IS, předpokládaných škod a dalších dopadů. Dopracovat konkrétní postupy a stanovit hranice, při jejichž překročení má být událost zaznamenána do evidence bezpečnostních událostí. S ohledem na omezené kapacity lidských zdrojů by bylo vhodné tyto eskalační procesy automatizovat. Komunikovat stanovená pravidla a hranice pro hlášení bezpečnostních událostí ze strany uživatelů IS v rámci programu zvyšování bezpečnostního povědomí. Revidovat model nasazení nástroje pro podporu ISMS tak, aby byla minimalizována nutnost manuálního zadávání dat a odstraněn problém duální evidence bezpečnostních událostí a incidentů.

Nejméně, a to v počtu pěti nedostatků bylo identifikováno v **§ 25** týkající se nepravidelného penetračního testování, včetně nedostatečné ochraně aplikací, informací a transakcí před neoprávněným zásahem.

- *Zjištění střední závažnosti – Omezené provádění bezpečnostního a penetračního testování, realizace opatření na základě testů zranitelnosti*

Provádění bezpečnostního testování je omezené, dlouhodobě není prováděno penetrační testování. Na základě dokumentace předložené auditovanými útvary není plně funkční vazba mezi testováním zranitelnosti a realizací nápravných opatření u jednotlivých aplikací. Na základě provedených penetračních testů nebyly nálezy zpracovány do plánu zvládání rizik do všech systémů.

Doporučení → Zajistit celkové testování bezpečnosti aplikací a jejich změn. Provádět pravidelné penetrační testování. Pro všechny aplikace realizovat opatření na základě provedených testů zranitelnosti, které budou pokrývat i samotné aplikace, nikoliv pouze jejich infrastrukturu. Dále sledovat tato nápravná opatření realizovaná na základě testování zranitelnosti a analýz rizik. Poskytnout odborným útvarům metodickou podporu a koordinovat jednotné bezpečnostní zásady a politiky, které mají být na jednotlivých systémech prosazovány.

Výstupem diplomové práce je návrh obecné metodiky pro výkon auditu kybernetické bezpečnosti. Zde je podoba celého návrhu:

OBECNÁ METODIKA PRO VÝKON AUDITU KYBERNETICKÉ BEZPEČNOSTI

I. Úvod

1.1 Účel dokumentu

Cílem této metodiky je popsat postupy plánování, provedení a vyhodnocení auditů systému řízení bezpečnosti informací (dále jen „SŘBI“) v podmínkách organizace. Audit SŘBI je procesem systematického a nezávislého ověření dodržování požadavků definovaných v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“), a zejména navazující vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB“).

Audit SŘBI představuje soubor organizačních a technických opatření, která zjišťují shromáždění a vyhodnocení informací o stavu bezpečnosti informací v souladu s předem stanoveným rozsahem.

Cílem auditu SŘBI je zejména:

- Získání informací o současném stavu SŘBI;
- Identifikace slabých míst a nedostatků SŘBI;
- Navržení doporučení, resp. nápravných opatření;
- Prověření splnění doporučení a účinnosti realizovaných nápravných opatření;
- Zlepšování a zvyšování efektivity SŘBI;
- Prověření, zda procesy a postupy SŘBI splňují požadavky vyhlášky;
- Prověření, zda procesy a postupy SŘBI odpovídají požadavkům na bezpečnost informací zadavatele.

1.2 Rozsah působnosti

Tato metodika stanovuje auditní postup pro zaměstnance odboru interního auditu a kontroly (dále jen „OIA“), a to jak v pracovním/služebním poměru, tak i zaměstnaných na základě dohod o pracích konaných mimo pracovní poměr. Dále je aplikovatelná pro všechny osoby a externí subjekty vykonávající audit pro zadavatele.

1.3 Seznam zkratek

Tabulka 6 Seznam zkratek

Zkratka	Popis
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
IKS	Informační a komunikační systém
IS	Informační systém
IT	Informační technologie
OIT	Odbor interního auditu
SŘBI	Systém řízení bezpečnosti informací
VIS	Významný informační systém
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zdroj: vlastní práce

II. Provedení auditu

2.1 Auditované oblasti

Audity SŘBI se provádí v rámci celé organizace.

Cílem jednotlivých auditů SŘBI je posouzení stavu v konkrétních oblastech bezpečnosti informací. To zahrnuje posouzení efektivity procesů SŘBI a prověření prosazení vybraných bezpečnostních nebo opatření bezpečnosti informací.

Posouzení efektivity procesů zahrnuje posouzení úrovně jednotlivých procesů potřebných pro zavedení, provoz a zlepšování SŘBI organizace a posouzení úrovně opatření týkající se bezpečnosti informací v souladu s VoKB. Jedná se následující procesy a opatření:

- § 3 – Systém řízení bezpečnosti informací;
- § 4 – Řízení aktiv;
- § 5 – Řízení rizik;
- § 6 – Organizační bezpečnost;
- § 7 – Bezpečnostní role;
- § 8 – Řízení dodavatelů;

- § 9 – Bezpečnost lidských zdrojů;
- § 10 – Řízení provozu a komunikací;
- § 11 – Řízení změn;
- § 12 – Řízení přístupu;
- § 13 – Akvizice, vývoj a údržba;
- § 14 – Zvládání kybernetických bezpečnostních událostí a incidentů;
- § 15 – Řízení kontinuity činností;
- § 16 – Audit kybernetické bezpečnosti;
- § 17 – Fyzická bezpečnosti;
- § 18 – Bezpečnost komunikačních sítí;
- § 19 – Správa a ověřování identit;
- § 20 – Řízení přístupových oprávnění;
- § 21 – Ochrana před škodlivým kódem;
- § 22 – Zaznamenání událostí IKS, jeho uživatelů a administrátorů;
- § 23 – Detekce kybernetických bezpečnostních událostí;
- § 24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí;
- § 25 – Aplikační bezpečnost;
- § 26 – Kryptografické prostředky;
- § 27 – Zajišťování úrovně dostupnosti informací;
- § 28 – Průmyslové, řídící a obdobné specifické systémy;
- § 29 – Digitální služby;
- § 30 – Bezpečnostní politika a bezpečnostní dokumentace.[126]

Rozhodujících kritériem pro provádění auditu jsou požadavky ZoKB a navazující VoKB uvedené v předmětných právních normách jako požadavky uvedené v § 3 písm. e) ZoKB a požadavky Bezpečnostní politiky informací zadavatele a navazující bezpečnostní dokumentace zadavatele.[127]

[126] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In.: *Sbírka zákonů,* rok 2018, částka 43.

[127] § 3 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2014, částka 75.

Při auditu bezpečnostních opatření je do auditu vždy nutné zařadit IS, které jsou zařazeny mezi KII dle. § 2 písm. b) a VIS dle § 2 písm. d). [128]

2.2 Způsob provedení auditu

Kritéria auditů SŘBI vycházejí z ustanovení Bezpečnostní politiky informací organizace, Plánu zvládání rizik bezpečnosti informací organizace, ustanovení ZoKB, resp. VoKB a cílů a strategie bezpečnosti informací organizace.

Audit se zaměřuje na hodnocení jednotlivých procesů SŘBI a oblastí bezpečnosti informací včetně identifikace relevantních zjištění a neshod a sledování implementace nápravných nebo preventivních opatření.

III. Organizace auditu

3.1 Plánování auditu

Audit SŘBI se provádí v souladu se střednědobým plánem auditních činností zadavatele v oblasti KB. Pro konkrétní kalendářní rok je střednědobý plán upřesněn ročním plánem auditních činností organizace v oblasti kybernetické bezpečnosti. Pro jednotlivé plánované činnosti OIA konkretizuje období provedení, název, cíl, typ a druh auditní akce a jejího personálního zajištění. V nutných a odůvodněných případech jsou tyto plány aktualizovány i v průběhu roku.

3.2 Příprava auditu

Nejméně 10 pracovních dnů před konáním konkrétního auditu stanoví interní auditor program auditu včetně projednání termínu s plánovanými účastníky. Program auditu je dokumentován do registru SŘBI do evidence auditů doplněním záznamu k plánovanému auditu. Záznam obsahuje termín provedení auditu a program auditu zahrnující doplňující informace o obsahu auditu, účastníků auditu a případně další požadavky.

Nejméně 5 pracovních dnů před konáním konkrétního auditu informuje interní auditor účastníky o termínu a předmětu auditu.

[128] § 2 písm. b) a d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), In.: *Sbírka zákonů,* rok 2014, částka 75.

3.3 Provedení auditu

Interní auditor stručně seznámí účastníky auditu s předmětem auditu a po dohodě s účastníky stanoví konkrétní časový plán a organizaci auditu.

Auditor v průběhu auditu shromažďuje informace a podklady formou rozhovorů s respondenty a posuzováním předložených dokumentů pro následné zpracování a vyhodnocení auditů.

3.4 Hodnocení vyzrálosti a vyhodnocení závěrů auditu

Hodnocení vyzrálosti je prováděno po jednotlivých procesech SŘBI a oblastech bezpečnosti informací dle tzv. modelu vyzrálosti, kdy je auditor hodnotí s přihlédnutím ke konkrétním činnostem pro procesy, cíle a opatření v rámci příslušné oblasti bezpečnosti informací. Hodnocení je auditorem prováděno pro následující stupně vyzrálosti.[129]

Tabulka 7 Hodnocení vyzrálosti

Stupeň vyzrálosti	Popis
Neexistence (Stupeň 0)	• Organizace si problematiku neuvědomuje a ani se jí interně nevěnuje. • Pravidla nejsou definována. • Žádný proces související s problematikou není možné rozpoznat. • Neexistují žádná sledování související s problematikou.
Náhodně (Stupeň 1)	• Je zřejmé, že organizace zjistila existenci problematiky a potřebu jejího pokrytí. Nicméně neexistuje konzistentní komunikace problematiky. • Existují hrubá pravidla, která nejsou dobře zdokumentována, zveřejněna a prosazována. • Existují ad-hoc přístupy aplikované individuálně případ od případu. Problematika není zastřešena nejvyšším vedením. • Monitorování je implementováno pouze reaktivně po incidentu, který způsobil organizaci nějaké ztráty.
Opakovatelně (Stupeň 2)	• V celé organizaci, kde je to přiměřené, existuje povědomí o problematice. • Existují jasně definovaná pravidla. • Související procesy jsou formálně prosazovány za aktivní podpory a dohledu managementu, ale nezahrnují celou organizaci. Neexistují výcvikové a komunikační standardy a odpovědnost je přizpůsobena individualitě.

[129] ČSN ISO/IEC 15504. *Úrovně zralosti v normě ISO/IEC 15504.* [online]. [cit. 2023-12-15]. Dostupné z: https://www.pdqm.cz/o-nas/terms/standardy/iso-15504

	• Management zjistil potřebu sledovat a metody a techniky hodnocení jsou ve stádiu vývoje.
Definovaně (Stupeň 3)	• Pochopení a respektování problematiky je vnímáno celou organizací. • Existují přesná a jednoznačná pravidla, která zohledňují jiné oblasti řízení. Při řešení je zvažováno řízení rizik. Pro některé prvky je použito řízení rizik. • Postupy jsou standardizovány, dokumentovány a aplikovány převážně v celé organizaci. Management prosazuje standardizované postupy a neformálně je stanoven plán odborné přípravy a školení. Obvyklé praktiky jsou formalizovány, přestože postupy nejsou zcela sofistikované. • Indikátory výkonu činností jsou zaznamenávány a sledovány, což vede ke zlepšování. Většina činností je posuzována vůči základním metrikám, nicméně odchylky jsou většinou řešeny individuální aktivitou jednotlivců a pouze výjimečně jsou detekovány managementem. Analýza příčin je používána pouze příležitostně.
Měřitelně (Stupeň 4)	• Existuje plné pochopení problematiky na všech odpovídajících úrovních. • Existují přesná a jednoznačná pravidla, která jsou vyžadována, plně integrována s jinými oblastmi. Při řešení je zvažováno řízení rizik. • Existuje jednoznačné vnímání zákazníka a jsou definovány odpovědnosti. V celé organizaci jsou procesy dobře definovány, integrovány a využívány. Je určen vlastník procesu, který prochází formální přípravou. Všichni vlastníci procesů jsou si vědomi rizik. • Zlepšování procesů je založeno především na kvantitativním vnímání a je možné sledovat a měřit soulad pomocí metrik. Management definoval tolerance, ve kterých se musí procesy pohybovat. Opatření jsou učiněna ve většině případů, kdy se zjistí, že proces nepracuje efektivně. Procesy jsou příležitostně zlepšeny a uvnitř organizace je prosazována nejlepší vžitá praxe. Analýza příčin je standardizována. Začíná proces trvalého zlepšování.
Optimalizovaně (Stupeň 5)	• Existuje hluboké a dlouhodobé porozumění problematiky. • Existují přesná a jednoznačná pravidla, která jsou vyžadována, plně integrována s jinými oblastmi a plně zahrnují řízení rizik. • Procesy jsou kultivovány na úrovni celosvětové nejlepší vžité praxe, což je výsledkem trvalého zlepšování a srovnáváním vyzrálosti s jinými organizacemi. Rizika a přínosy procesů jsou definovány, vzájemně vyváženy a rozšířeny v celé organizaci. Příprava, školení a vzájemná komunikace je aktuální. Implementace je vedena organizací, lidé a procesy se rychle přizpůsobí a plně podporují změny organizace.

	• Monitorování, sebehodnocení a komunikace problematiky je všudypřítomná v celé organizaci a pro podporu měření, analýz, komunikace a přípravy existuje optimální využití procesů a technologií. U všech problémů a odchylek jsou analyzovány příčiny a neprodleně jsou identifikována a zaváděna vhodná účinná opatření. Jsou využíváni externí odborníci a benchmarking.

Zdroj: (pdgm.cz)[130], zpracování: vlastní práce

Celkové shrnutí výsledů auditu uvádí souhrnnou přehledovou tabulku hodnocení pro jednotlivé procesy SŘBI a opatření bezpečnosti informací tak, jak jsou uvedeny v jednotlivých paragrafech vyhlášky. Každý vybraný proces/činnost a bezpečnostní opatření je hodnoceno v následující škále:

- Nezavedeno (N)
- V procesu zavádění (P)
- Zavedeno (Z)
- Neaplikováno (NA)

V případě identifikace neshod (formální, dílčí, systémová) nebo příležitostí ke zlepšení SŘBI jsou tyto skutečnosti předány k zavedení do evidence neshod a příležitostí v rámci registru SŘBI včetně odkazu na příslušný audit v evidenci auditů.

Po zaevidování neshody nebo příležitosti ke zlepšení navrhne bezpečnostní manažer přijetí nápravných a/nebo preventivních opatření nebo způsobu využití příležitosti. Toto dále zaznamená do registru SŘBI do evidence neshod a příležitostí k příslušným záznamům.

Shrnující komentář auditu SŘBI dává auditorovi prostor pro uvedení celkového komentáře, poznámek klíčových problémů v oblasti bezpečnosti informací apod. Struktura shrnujícího komentáře vychází z procesů SŘBI a z opatření bezpečnosti informací a má následující podobu:

- Písemné shrnutí stavu zavedení procesů SŘBI a naplnění vybraných opatření bezpečnosti informací za hodnocené období;
- Stav zavedení procesů SŘBI a naplnění opatření bezpečnosti informací v rozsahu dle kapitoly 2.1.

[130] ČSN ISO/IEC 15504. *Úrovně zralosti v normě ISO/IEC 15504.* [online]. [cit. 2023-12-15]. Dostupné z: https://www.pdqm.cz/o-nas/terms/standardy/iso-15504.

Audit SŘBI uvádí detailní přehledovou tabulku hodnocení úrovně jednotlivých procesů SŘBI a stavu realizace opatření bezpečnosti informací dle vybraných paragrafů vyhlášky s rozpadem až na úroveň hodnocení jednotlivých činností a opatření.

Závěrečná zpráva z auditu SŘBI musí obsahovat popis:

- Cíle a rozsahu auditu;
- Auditované oblasti;
- Auditního týmu a auditovaných útvarů;
- Použité metodiky auditu a hodnocení;
- Manažerského shrnutí hlavních nálezů a jejich odůvodnění;
- Všech nálezů auditů (Zjištění) včetně návrhů na jejich odstranění (Doporučení), popř. návrh na zlepšení účinnosti opatření (Návrh na zlepšení).

4 Závěrečná ustanovení

Za dodržování této metodiky odpovídají jednotliví vedoucí zaměstnanci OIA organizace v rámci vymezených kompetencí.

Za správnost a aktualizaci této metodiky odpovídá interní auditor.

V případě, že jsou činnosti uvedené v této metodice upraveny zvláštním právním předpisem, postupuje se podle tohoto předpisu.

4.1 Revize metodiky

Revize této metodiky se provádí v případě potřeby, minimálně jednou za tři roky. Cílem je zajistit, aby ustanovení dokumentu odpovídala požadavkům reálné praxe a stavu rozvoje SŘBI organizace.

4.2 Účinnost metodiky

Tato metodika nabývá účinnosti dnem podpisu.

6 Závěr

Předložená diplomová práce se zabývala analýzou veřejných zakázek v oblasti informační a kybernetické bezpečnosti s důrazem na realizaci auditů kybernetické bezpečnosti. Především pak identifikací zjištěných nedostatků a vytvořením vhodných doporučení. Výstupem práce bylo navrhnout obecnou metodiku pro výkon auditu kybernetické bezpečnosti a její využití v praxi.

Teoretická část diplomové práce vycházela ze studia odborných publikací a byla věnována výkladu a práci s literaturou, právními předpisy a literárními rešeršemi z oblasti kybernetické bezpečnosti, zejména Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů. Byly zde vysvětleny základní pojmy, které jsou stěžejní pro pochopení dané problematiky, jako je kybernetická bezpečnost, kritická informační infrastruktura, triáda CIA, bezpečnostní hrozby a systém řízení bezpečnosti informací. Na závěr byla popsán i samotný proces auditu kybernetické bezpečnosti.

Na teoretickou část diplomové práce úzce navazuje část praktická, ve které bylo provedeno výzkumné šetření zaměřené na analýzu podaných nabídek na veřejné zakázky v oblasti informační a kybernetické bezpečnosti, kterých se vybraná společnost zúčastnila, a to od ledna 2017 do prosince 2022. Z provedené analýzy lze konstatovat, že v průběhu celého sledovaného období byl největší počet podaných nabídek na veřejné zakázky v oblasti kybernetické bezpečnosti. Následně byla provedena analýza veřejných zakázek týkající se auditů kybernetické bezpečnosti. Důraz byl kladem především na identifikaci nejčastějších nedostatků v rámci realizovaných auditů kybernetické bezpečnosti a návrh vhodných doporučení. Cílem auditů bylo zjištění stavu a ověření souladu s požadavky ZoKB a VoKB. Data byla vyhodnocena dle jednotlivých let a následně provedena komparace údajů za sledované období šesti let. Tyto zjištěné nedostatky mohou představovat závažné ohrožení celé informační infrastruktury včetně kritické informační infrastruktury.

Nejvíce závažné nedostatky jsou hodnoceny na kritickém stupni významnosti a mají zásadní dopad na funkčnost celého procesu nebo systému. Nejvíce jich bylo identifikováno v oblasti „*Bezpečnosti komunikačních sítí*“, která představuje bezpečnostní opatření a technologie sloužící k zajištění ochrany dat, informací a komunikační infrastruktury před neoprávněným přístupem, manipulací a škodlivými útoky. Následují nedostatky

hodnoceny na vysokém stupni závažnosti v oblasti „*Sběru a vyhodnocování kybernetických bezpečnostních událostí*“, jenž mají za cíl identifikovat a následně reagovat na bezpečnostní hrozby. V oblasti „*Systému řízení bezpečnosti informací*“ docházelo k systematickým nedostatkům, jež jsou řazeny na středním stupni závažnosti. Jednalo se především o nedostatečné nastavení celého systému či nedostatečně zpracované příslušné bezpečnostní dokumentace a politiky. Za celé sledované období bylo právě těchto zjištěných nedostatků největší počet. Následovaly v kategorii „*Řízení přístupu a bezpečného chování* uživatelů“ v nízké míře závažnosti, které nepředstavují významná rizika a zjištěné drobné nedostatky jsou převážně způsobeny lidským faktorem.

Na základě výsledků ze zjištěných dat byla v závěru praktické části navržena vhodná doporučení. Jako hlavním nedostatkem autorka spatřuje v nedostatečném zabezpečení infrastruktury. Pro organizace je problematika ochrany a zabezpečení dat, s nimiž pracuje a která je třeba dále uchovávat, sdílet a jinak s nimi pracovat. S ohledem na aktuální trendy jsou proto často využívány nové formy ukládání dat, jako např. cloudová úložiště a sdílené online služby. Zvýšené používání těchto online služeb a cloudů však vede mnohdy k nedostatečné transparentnosti v oblasti řešení zabezpečení, což může zpochybnit jejich důvěryhodnost. Navrhovaným opatřením je nastavení kvalitnějších a přesnějších kontrolních systémů, v jehož důsledku vzrůstá potřeba provádět osvětu, seznamovat všechny klíčové aktéry s nejlepšími postupy a metodami na ochranu informační bezpečnosti, bezpečným nakládáním s informacemi a pomáhat je tak chránit před kybernetickými útoky.

S nárůstem počtu informačních a komunikačních technologií a rostoucím využívání internetu jak uživateli, tak samotnými zařízeními používanými v jednotlivých organizacích, roste i závislost na těchto technologiích a kritičnost jejich selhání, zejména u těch spadajících pod kritickou infrastrukturu. Zatímco počet zařízení připojených k internetu neustále narůstá, velké části uživatelů chybí povědomí o nezbytné digitální bezpečnosti, tedy o tom, jak se správně pohybovat v online prostředí a jak zabezpečit svá zařízení. Vhodným opatřením je kontinuálně provádět analýzu a monitoring hrozeb a rizik. Pravidelně provádět kontroly a zajišťovat odhalování chyb a zranitelnosti v informačních systémech a sítí. A v neposlední řadě zvyšovat možnosti, schopnosti a kapacity v oblasti aktivní ochrany a protiopatření proti kybernetickým útokům. S tím také souvisí průběžná a důsledná kontrola výstupních dokumentů.

Z výzkumu rovněž vyplývá nedostatek odborníků na kybernetickou bezpečnost. Je proto nezbytné zajistit dostatečné odborné kapacity a provést revizi vzdělávacích programů v oblasti kybernetické bezpečnosti pro vlastní zaměstnance tak, aby odpovídaly aktuálním požadavkům a trendům. Patří sem i pravidelná aktualizace bezpečnostní dokumentace a následných bezpečnostních politik.

Cíl diplomové práce byl splněn tím, že na základě identifikace a vyhodnocení nejčastějších nalezených nedostatků v rámci provedených auditů kybernetické bezpečnosti, byla dále navržena konkrétní vhodná doporučení. Tato doporučení by mohla podstatně snížit rizikovost potenciálních hrozeb a výrazně zvýšit úroveň kybernetické bezpečnosti organizace. V závěru této diplomové práce byla autorkou vypracována obecná metodika pro výkon auditu kybernetické bezpečnosti, která má za cíl poskytnout ucelený rámec pro realizaci auditu kybernetické bezpečnosti v souladu s konkrétními potřebami a prostředím každé organizace.

7 Seznam použitých zdrojů

7.1 Knižní zdroje

BUGAN, A. *Férové zadávání veřejných zakázek.* Praha: Transparency International – Česká republika, 2019. 64 s. ISBN 978-80-87123-34-8.

HRŮZA, P. a kol. *Kybernetická bezpečnost a kritická informační infrastruktura.* Praha: Powerpoint, 2018. 89 s. ISBN 978-80-7568-122-5.

JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 3. aktualizace. Praha: Policejní akademie ČR: Česká pobočka AFCEA, 2015. 240 s. ISBN 978-80-7251-436-6.

KOLEKTIV AUTORŮ. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Praha: Policejní akademie České republiky, 2020. 328 s. ISBN 978-80-7251-505-9.

KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, 2017. 524 s. ISBN 978-80-88168-15-7.

KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o., 2019. 560 s. ISBN 978-80-88168-34-8.

MAISNER, M., VLACHOVÁ, B. *Zákon o kybernetické bezpečnosti: Komentář.* Praha: Wolters Kluwer, a.s., 2015. 219 s. ISBN 978-80-7478-817-8.

PAVEL, J. *Veřejné zakázky a efektivnost.* Praha: Ekopress, s.r.o., 2013. 123 s. ISBN 978-80-8765-04-0.

SEDLÁK, P., KONEČNÝ, M. kol. *Kybernetická (ne)bezpečnost.* Praha: CERM, akademické nakladatelství, 2021. 429 s. ISBN 978-7623-068-2.

ÚZ 1445. *Svobodný přístup k informacím, Elektronické komunikace, EGOVERNMENT, Kybernetická bezpečnost.* Ostrava – Hrabůvka: Sagit, 2021. 336 s. ISBN 978-80-7488-492-5.

7.2 Internetové zdroje

CDC DATA. *Co přináší NIS2 – nová směrnice o kyberbezpečnosti*. [online]. 2024 [cit. 2024-01-30]. Dostupné z: https://www.cdc.cz/cs/co-prinasi-nis2-nova-smernice-o-kyberbezpecnosti/.

Coretelligent. *What is the CIA Triad, And Why Does Your Cybersecurity Position Depend on* It? [online]. 2022 [cit. 2023-08-30]. Dostupné z: https://coretelligent.com/insights/what-is-the-cia-triad-and-why-does-your-cybersecurity-position-depend-on-it/.

ČSN ISO/IEC 15504. *Úrovně zralosti v normě ISO/IEC 15504.* [online]. [cit. 2023-12-15]. Dostupné z: https://www.pdqm.cz/o-nas/terms/standardy/iso-15504.

Data Protection. Security of personal data. Enisa: *European Union Agency for Cyber Security* [online]. 2005 [cit. 2022-03-30]. Dostupné z: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies.

European Union Agency for Cyber Security. *Data Protection: Security of personal data*. [online]. 2005 [cit. 2023-08-30]. Dostupné z: https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection.

KROPÁČOVÁ, A., CERT/CSIRT týmy a jejich role. Root.cz: *Informace nejen ze světa Linuxu*. [online]. 2013 [cit.2023-08-28]. Dostupné z: http:/www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. 2022 (PDF). [cit. 2023-08-27]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Doporučení*. [online]. 2017 [cit. 2023-08-20]. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Hlášení incidentů.* [online]. 2014 [cit. 2023-08-27]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Hrozby*. [online] 2017 [cit. 2023-08-20]. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *O úřadu* [online] 2017 [cit. 2023-08-20]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Podpůrné materiály*. [online]. 2017 [cit. 2023-08-20] Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/.

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Přehledové blokové schéma k zákonu a jeho prováděcím předpisům*. [online]. 2020 (PDF). [cit. 2023-08-20]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-822/1schemazkb-cz.pdf

NBÚ, Národní úřad pro kybernetickou a informační bezpečnost. *Zpráva o stavu kybernetické bezpečnosti za rok 2017*. [online]. 2017 [cit. 2023-08-20]. Zdroj ve formátu PDF. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISE („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). [online]. 2019 [cit. 2023-08-30]. Dostupné z:
https://www.zakonyprolidi.cz/pravoeu/dokument/souvislosti?celex=32019R0881&date=0

Science Direct Parkerian Hexad: *What is Information Security?* [online]. 2014 [cit. 2023-08-30]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/parkerian-hexad.

Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. [online]. 2008 [cit. 2023-08-28]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=cellar%3Aba51b03f-66f4-4807-bf7d-c66244414b10.

ISVS.CZ: Ochranné opatření k zabezpečení e-mailové komunikace. [online]. 2023 [cit. 2024-01-20]. Dostupné z: https://www.isvs.cz/ochranne-opatreni-k-zabezpeceni-e-mailove-komunikace/.

7.3 Právní předpisy

Nařízení vlády č. 315/2014 Sb., Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (zákon o kybernetické bezpečnosti).

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

8.4 Seznam použitých zkratek

BDg	Zkoumaná společnost BELCOM Digital a.s.

CERT	Computer Emergency Response Team
DPH	Daň z přidané hodnoty
GDPR	General Data Protection
EU	Evropská unie
ICT	Informační a komunikační technologie
IEC	International Electrotechnical Commission
ISKII	Informační systém kritické informační infrastruktury
ISMS	Information Security Management System
ISO	International Organization
ISZS	Informační systém základní služby
IT	Informační technologie
ITSM	Information Technology Service Management
KB	Kybernetická bezpečnost
KBI	Kybernetický bezpečnostní incident
KII	Kritická informační infrastruktura
KSKII	Komunikační systém kritické informační infrastruktury
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
RPA	Robotic Process Automation
VIS	Významný informační systém
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech v podání v oblasti kybernetické bezpečnosti a likvidaci dat
VZ	Veřejné zakázky
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů