Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Zákon o kybernetické bezpečnosti a jeho dopady v praxi

Elvy Seidlerová

Bakalářská práce
2025

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2025/2026

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Elvy Seidlerová**
Osobní číslo:	**E22423**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Zákon o kybernetické bezpečnosti a jeho dopady v praxi**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce bude rozbor návrhu nového zákona o kybernetické bezpečnosti a jeho aplikace ve vybrané organizaci.

Osnova:
- Úvod do kybernetické bezpečnosti.
- Popis vývoje legislativy týkající se kybernetické bezpečnosti.
- Rozbor návrhu nového zákona o kybernetické bezpečnosti.
- Možnosti aplikace ve vybrané organizaci.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

KOLOUCH, Jan; BAŠTA, Pavel. *CyberSecurity*. *CZ.NIC*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80--88168-31-7.
SEDLÁK, Petr; KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
SMEJKAL, Vladimír; SOKOL, Tomáš; KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380--765-8.
ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. září 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

PROHLÁŠENÍ

Práci s názvem Zákon o kybernetické bezpečnosti a jeho dopady v praxi jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 25.4.2025

Elvy Seidlerová

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala své vedoucí práce Ing. Renatě Máchové, Ph.D. za její odborné vedení, cenné rady, trpělivost a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

Poděkování patří rovněž zaměstnancům Univerzity Pardubice, kteří mi umožnili absolvovat odbornou praxi a tím usnadnili možnost věnovat se zvolenému tématu.

Velké poděkování si zaslouží i má maminka za její podporu, povzbuzení a trpělivost, s níž zvládala mé nálady v průběhu studia.

ANOTACE

Bakalářská práce se věnuje zhodnocení dopadů změn zákona o kybernetické bezpečnosti. První část práce je úvodem do kybernetické bezpečnosti a rozborem legislativní stránky. V druhé části je rozebrán nový zákon a implementován do vybrané organizace.

KLÍČOVÁ SLOVA

Kybernetická bezpečnost, bezpečnost, kybernetika, zákon, Česká republika

TITLE

The Cyber Security Act and its impact in practice

ANNOTATION

The bachelor thesis is devoted to the evaluation of the impact of changes to the Cyber Security Act. The first part of the thesis is an introduction to cybersecurity and an analysis of the legislative aspect. The second part discusses the new law and implements it in a selected organization.

KEYWORDS

Cyber security, security, cybernetics, law, Czech Republic

OBSAH

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

AI	Umělá inteligence
ČR	Česká republika
EU	Evropská unie
ICT	Informační komunikační technologie
IS	Informační systém
MKB	Manažer kybernetické bezpečnosti
NIS	Síťová a informační bezpečnost
NÚKIB	Národní Úřad pro Kybernetickou a Informační Bezpečnost
nZoKB	Návrh zákona o kybernetické bezpečnosti
Odst.	Odstavce
PČR	Policie České republiky
Písm.	Písmene
Sb.	Sbírka zákonů
UPCE	Univerzita Pardubice
ZoKB	Zákon o kybernetické bezpečnosti

ÚVOD

Ve světě, kde je téměř každý aspekt lidského života propojen s digitálními technologiemi, už kybernetická bezpečnost nepředstavuje jen technické téma pro IT odborníky. Je také každodenní nutností pro státní sektor, soukromé organizace, vzdělávací instituce i jednotlivce. Útoky hackerů, úniky dat nebo výpadky služeb jsou realitou, která může mít vážné právní i finanční důsledky.

Aktuálnost tématu kybernetické bezpečnosti je umocněna neustálou digitalizací a nárůstem kybernetických hrozeb v globálním i národním měřítku. Směrnice NIS2 a s ní související novely legislativy představují zásadní krok k posílení odolnosti digitální infrastruktury v České republice.

Cílem práce je rozbor návrhu nového zákona o kybernetické bezpečnosti a jeho aplikace ve vybrané organizaci.

Práce se v úvodu nejdříve zaměří na vysvětlení základních pojmů a významu kybernetické bezpečnosti. Poté bude následovat přehled vývoje legislativy v České republice, který poskytne srovnání stávajícího zákona s připravovanou podobou a identifikací klíčových změn, které návrh přináší – jak z hlediska rozsahu povinností, tak dopadu na organizace.

Na tuto část bude navazovat praktická aplikace v prostředí vybrané organizace, kde na modelovém příkladu bude ukázáno, jak lze nové požadavky promítnout do vnitřních pravidel. Práce nabídne identifikaci dopadů a návrhy opatření, která mohou pomoci při přizpůsobování se nové legislativě.

1. ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI

Úvodní kapitola práce má seznámit čtenáře s definicí kybernetické bezpečnosti a poskytnout přehled o této problematice. Představuje základní pojmy, význam kybernetické bezpečnosti a jak kyberprostor přispívá ke zneužití. Zmiňuje nejčastější trestné činy a útoky, které se nacházejí v kyberprostoru, jejich podrobné vysvětlení, a zároveň je detailně popisuje.

Informační a komunikační technologie lze chápat jako souhrn technických prostředků a systémů, které se používají k práci s daty. Tento souhrn se zabývá jejich zpracováním, uchováním, správě a přenosu.

Kyberprostor označovaný také jako kybernetický prostor představuje digitální prostředí. Je tvořené informačními systémy či sítěmi elektronických komunikací, které umožňují vznik, zpracování, ukládání a výměnu dat. [1]

1.1. Definice kybernetické bezpečnosti

Termín „**kyber“** označuje **provázanost informačních a komunikačních technologií** s kyberprostorem. Existuje mnoho různých definic, kterými se označuje bezpečnost. Žádnou z nich však nelze považovat za správnou či univerzální. Níže jsou příklady, jak lze bezpečnost definovat:

„Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracovávání, úschově, distribuci a prezentaci informací.“ [2]

„Stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt a jeho zájmy a tento objekt je k eliminaci stávajících i potencionálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“ [3]

„Stav, ve kterém se individua, skupiny a státy necítí ohroženě vážnými hrozbami, popřípadě se před nimi považují za účinně ochráněné a svoji budoucnost mohou vytvářet podle vlastních představ.“ [1]

Kybernetická bezpečnost představuje jeden z klíčových prvků **ochrany společnosti v digitálním světě** internetu a je kriticky důležitá pro jeho každodenní fungování. V současnosti se jedná už o široce rozšířený pojem, který se stal nezbytnou součástí bezpečného společenského i pracovního života jak firem, tak každého jednotlivce. Postupná digitalizace vede k stále větší závislosti společnosti na fungování informačních a komunikačních

technologií, avšak současně se zvyšují požadavky na jejich spolehlivost. Bezpečnost je tedy klíčová pro ochranu citlivých dat, plynulosti podnikových procesů či soukromí jednotlivců.

Cílem kybernetické bezpečnosti je zajistit **dostupnost, důvěrnost a integritu** přenášených a zpracovaných dat počítačových systémů a sítí. Nejčastěji se označuje zkratkou CIA. V následujících bodech budou tyto atributy více přiblíženy: [4][5]

- **Confidentiality** (důvěrnost) – Zajištění, aby data byla chráněna před neoprávněným přístupem a aby přístup k nim měly pouze vybrané autorizované osoby. Pro dosažení důvěrnosti se používá šifrování dat, důsledná kontrola práv přístupu a mnoho dalších bezpečnostní opatření.
- **Integrity** (integrita nebo také celistvost) – Zajištění, že data zůstanou v neporušeném a nezměněném formátu od okamžiku odeslání až po moment přijetí před neoprávněnými osobami a kybernetickými útoky. Šifrováním komunikace se zabezpečuje obsah zprávy tak, aby pro neoprávněné osoby nebyl čitelný.
- **Availability** (dostupnost) – Jistota, že autorizované osoby mají vždy přístup do systému. Ochrana probíhá například pomocí záložních systémů a generátorů. Zahrnuje opatření proti výpadkům, které by mohly nastat, pokud útočník zahltí systém velkým množstvím přenosů a příkazů.

Kybernetická bezpečnost je způsob ochrany počítačů, telefonů a jiných elektronických zařízení. Jako přirovnání lze použít trezor v domě, do kterého se ukládají důležité věci, které potřebují být chráněné. Kybernetická bezpečnost funguje podobně – chrání data, fotografie nebo zprávy, které by měly vidět jen pověřené osoby, které k nim mají přístup.

1.2. Význam kybernetické bezpečnosti

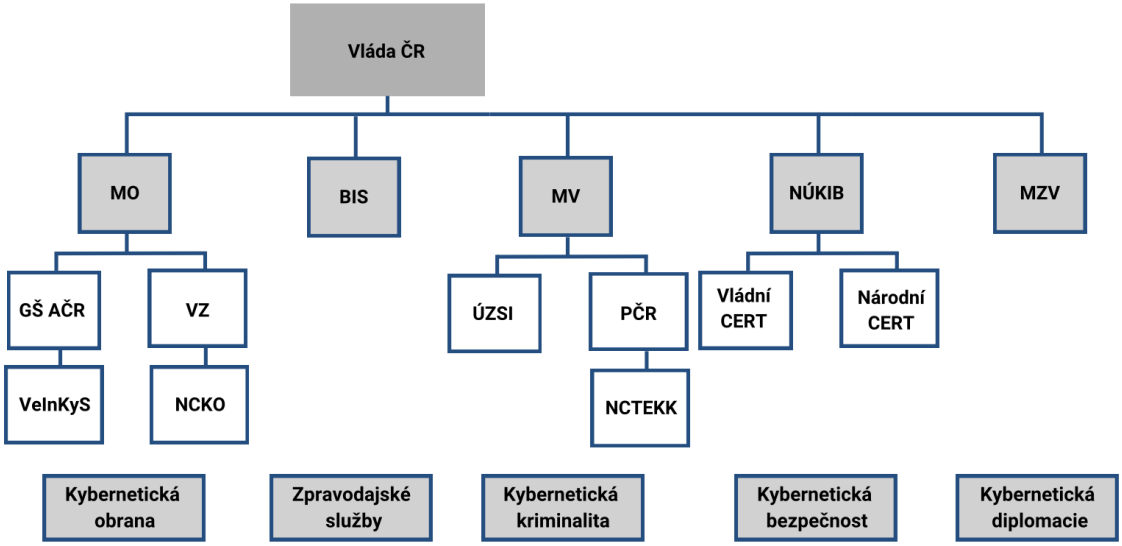
V dnešním digitálním světě se kybernetická bezpečnost **řadí mezi nejdůležitější oblasti** bezpečnostního zájmu. Vzhledem k rostoucí sofistikovanosti a frekvenci hrozeb se **investice stávají nepostradatelným prvkem** ochrany kyberprostoru.

Rozsah zájmu je obrovský. **Zabezpečuje ochranu citlivých dat** od jednotlivců až po národní, eventuelně nadnárodní organizace. Ochrana citlivých údajů spočívá v jejich zabezpečení proti krádeži, manipulaci nebo zneužití, což má zásadní význam pro fyzické osoby, spolky, organizace, ale i pro společnosti jako celek. **Přijatá opatření pomáhají minimalizovat ztráty** nejen finanční, ale také ztráty nehmotné, jako je ztráta důvěry či odliv zákazníků. Předpisy Evropské unie stanovují standardy kybernetické ochrany a zajišťují dodržování napříč členskými státy. Na globální úrovni hraje kybernetická bezpečnost klíčovou roli při ochraně

národní bezpečnosti a její kritické infrastruktury. Mezi významné body kybernetické bezpečnosti patří: ochrana citlivých údajů a soukromí, předcházení finančním ztrátám, podpora národní a globální bezpečnosti, ochrana kritické infrastruktury nebo snížení kyberkriminiality. [6]

1.3. Zajišťování kybernetické bezpečnosti v ČR

V České republice se na systému zajišťování kybernetické bezpečnosti podílí hlavně následující úřady a přiřazené organizace, jak je znázorněno na obrázku 1:



Obrázek č. 1: Hierarchie kybernetické bezpečnosti

Zdroj:[7]

Pod **Ministerstvo obrany** (MO) spadají zpravodajské služby, které se podílejí na systému zajišťování bezpečnosti. Jmenovitě jimi jsou Generální štáb Armády ČR (GŠ AČR), Velitelství informačních a kybernetických sil (VeInKyS), Vojenské zpravodajství (VZ) a Národní centrum kybernetických operací (NCKO). Společně zodpovídají za budování kybernetické obrany ČR. [7]

Bezpečnostní informační služba (BIS) je zpravodajskou službou, jejíž posláním je chránit občany před hrozbami, které by mohly ohrozit bezpečnost ČR. [8] Její fungování upravuje zákon č 154/1994 Sb. [9]

Ministerstvo vnitra České republiky je ústředním orgánem státní správy pro rozvoj a zajištění bezpečnosti digitálních služeb státu nebo spolupráce s dalšími subjekty. Jako příklad lze uvést školství, jehož vliv na vzdělávání a vzdělávací prostředí musí mít pro řádné fungování

zajištěnou kybernetickou bezpečnost. Pod Ministerstvo vnitra ČR spadá i Policie České republiky, u které nedávno vznikl útvar NCTEKK SKPV. [10]

Národní centrála proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování (NCTEKK SKPV) vznikla k 1.1.2023. Vznikla primárně vyčleněním dvou sekcí z Národní centrály proti organizovanému zločinu. Úkolem útvaru je zvýšení schopnosti policie v mnoha směrech. Především v oblasti terorismu, extremismu ale i v boji proti nejzávažnějším formám kybernetické kriminality, které útočí zejména na kritickou infrastrukturu. [11]

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost na území České republiky. Vznikl 1.8.2017 na základě účinnosti evropské směrnice NIS (2.4.1). Národní centrum kybernetické bezpečnosti (NCKB) bylo prvotně orgánem správy pro kybernetickou bezpečnost. Jednalo se o specializované pracoviště Národního bezpečnostního úřadu (NBÚ), které vzniklo na základě usnesení vlády ze dne 19.11.2011.[12]

Náplní centra je zajištění kybernetické bezpečnosti, pod kterou spadá i ochrana utajovaných informací v oblasti informačních a komunikačních systémů. Rovněž má úlohu koordinovat spolupráci na národní a mezinárodní úrovni při prevenci kybernetických útoků. Dále se také má podílet na navrhování a přijímání příslušných opatření. [13]

Vládní CERT (Computer Emergency Response Team) je zodpovědný za ochranu kritické informační infrastruktury a významných informačních systémů veřejné správy a samosprávy. Zaměřuje se na bezpečnostní incidenty, které mohou ohrozit nebo přímo ohrožují systémy těchto institucí. [14]

Národní CERT nebo také **CSIRT** (Computer Security Incident Response Team) se podílí na řešení incidentů týkajících se kybernetické bezpečnosti v České republice a má za úkol poskytovat pomoc a podporu při řešení incidentů mimo kritickou infrastrukturu. CSIRT tak plní roli kontaktního místa od orgánu až po povinné osoby. Společně s NÚKIB šíří osvětu a vzdělání v oblasti kybernetické bezpečnosti. [15]

Ministerstvo zahraničních věcí – zajišťuje ochranu zahraniční politiky a diplomacie v oblasti kybernetické bezpečnosti. Zabezpečuje vztahy mezi Českou republikou a ostatními státy a řídí české ambasády v zahraničí.

Na celkovém systému se však podílí spoustu dalších institucí, které se problematikou zabývají, jako je například i **Výbor pro kybernetickou bezpečnost** – jedná se o orgán

bezpečnostní rady státu pro zajištění opatření v rámci kybernetické bezpečnosti v České republice. V rámci působnosti zabezpečuje meziresortní spolupráci s jinými ústředními správními úřady a doporučuje jejich projednání v Bezpečnostní radě státu. Výbor má 21 členů složených ze zástupců ministerstev a úřadů. [16]

1.4. Trestné činy v kyberprostoru

Kybernetický útok je protiprávní jednání, které se odehrává v kyberprostoru. Řešení kybernetického útoku bývá složitý a časově náročný proces. Je však nutné reagovat rychle pro minimalizaci škod a ochranu systémů a dat organizací. Je nutné zmínit, že ne každý kybernetický útok je trestným činem, ale každý kybernetický trestný čin je zároveň kybernetickým útokem. Důvodem je absence trestněprávní normy. [17]

Faktory podporující zneužití kyberprostoru [18]:

- **Anonymita útočníka** – Ve většině případů je anonymita jen zdánlivá. Díky dostupným technologiím, které jsou dnes k dispozici, lze většinu útočníků dříve či později odhalit. Tato anonymita však dokáže vyvolat v pachateli pocit neporazitelnosti a nepostižitelnosti.
- **Lehce dostupné nástroje** – Na útoky, které jsou menšího rozsahu, postačí jako základ, díky cenové dostupnosti a rozšířenosti, mobilní telefon a internet. Díky této dostupnosti a propojenosti nástrojů vznikají nové možnosti poškození oběti rychleji než regulující pravidla.
- **Riskantní chování uživatele** – Opatrnost v kyberprostoru je podstatně nižší než v reálném světě. K riskantnímu chování přispívá i absence prevence a nízká informovanost jednotlivců o tom, co všechno se na sítích může odehrávat. Díky zdánlivé anonymitě jsou lidé na internetu odvážnější v rozebírání daleko citlivějších témat. Mezi velmi riziková chování patří i sdílení citlivých údajů nebo fotografií, které mohou být zneužity nebo pomocí nichž může být osoba terčem vydírání.

Dle zprávy NÚKIB byly pro rok 2023 nejčastějšími typy kybernetických útoků Phishing, Vishing, Ransomware nebo DDoS. [19]

Phishing – Původ slova je od autorů Jerryho Felixe a Chrise Haucka z knihy „Systems Security: A hacker's perspective" [20], kdy autoři přirovnali útok k rybolovu (anglicky fishing). Jedná se přirovnání, kdy **rybář „nahodí návnadu" a čeká, kdo se „chytí"**. Jedná se tedy nejčastěji o podvodné nebo klamavé jednání, které se snaží z uživatele dostat důvěrná data.

Obvykle podvod spočívá v žádosti šířené e-mailem nebo sms zprávou, ve které se nachází odkaz, který vyžaduje přihlašovací údaje. [21]

Vishing – Je forma phishingu uskutečněná prostřednictvím telefonního hovoru-takzvaný voice phishing, zkráceně vishing. Pachatelé využívají namluvené zprávy a generátory, pomocí kterých dokážou převádět text na řeč, nebo jsou rovnou uskutečněny živým volajícím. Cíl útoku je stejný jako u phishingu-pomocí podvodného jednání lze vylákat osobní nebo jiné citlivé údaje.[21]

Ransomware – Je kombinací dvou slov. „Ransom“, které označuje výkupné, a „ware“ jako zkratku software. Jedná se tedy o druh softwaru, který je škodlivý a jeho účelem je zašifrovat nebo jinak omezit přístup k datům nebo celému systému do doby, dokud nebude zaplaceno výkupné.[21]

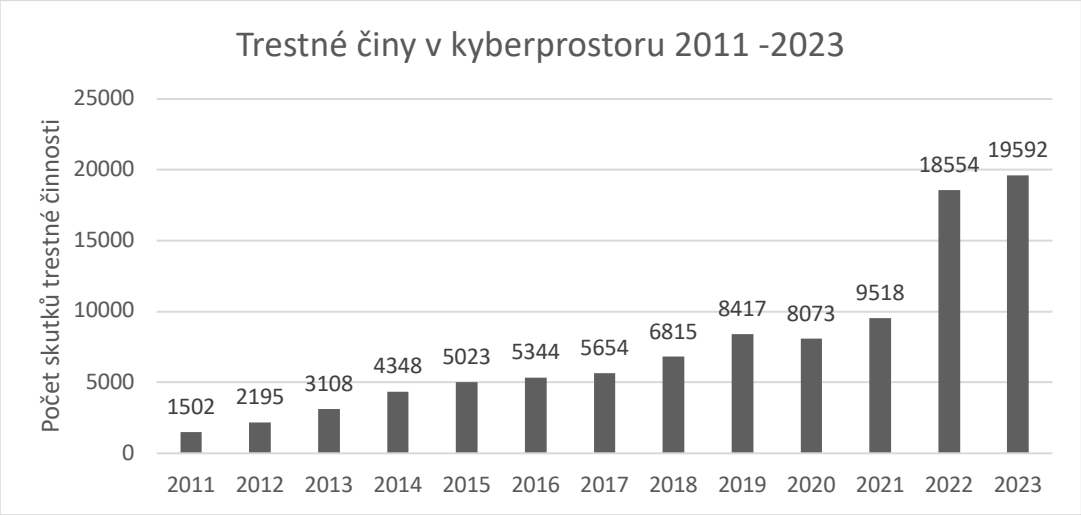
DDoS – Distributed Denial of Service je forma útoku, při kterém se útočník snaží narušit či poškodit stránku, aplikaci nebo web tím, že pošle obrovské množství požadavků. Tím dojde k přetížení systému, které omezí výkonost, některé funkce, případně celkový výpadek. [21]

1.5. Vliv umělé inteligence na kybernetickou bezpečnost

Je důležité také zmínit, že umělá inteligence je známá v angličtině pod zkratkou AI. V posledních letech se situace radikálně mění v oblastech například generování textů nebo zlepšování uživatelských funkcí. Umělá inteligence je **klíčovou podporou v detekci a vyhodnocování** kybernetických **útoků** jak aktuálních, tak minulých, ze kterých se umělá inteligence učí. Díky těmto krokům se výrazně zlepšuje obranyschopnost systémů. Nelze umělou inteligencí nahradit lidskými experty, ale umožňuje expertům zjednodušit pracovní vytíženost. Umělá inteligence může pomoci s jednoduššími výzvami a experti se potom mohou věnovat složitějším úlohám. Umělá inteligence exceluje díky algoritmům strojového učení v detekci potencionálních phishingových útoků nebo neznámých variant malware. Stává se z ní tak nezastupitelný pomocník v kyberbezpečnosti.

Umělá inteligence má také odvrácenou stranu. I když zatím nedosáhla dostatečné úrovně využitelnosti pro útočníky, je potencionální hrozbou při generaci škodlivého kódu, automatizaci a škálování útoků. Běžně dostupné umělé inteligence jako je ChatGPT, Copilot nebo Perplexity mají ochranu proti tvorbě nebo napomáhání útoků. Existují i takové umělé inteligence, které opatření dokážou obejít. Lze konstatovat, že v tuto chvíli stojí AI na straně obrany před útoky, ale je tu velká pravděpodobnost, že v budoucnu bude stát jak na straně útoku, tak na straně obrany. [22]

Podle dat Policie ČR (zobrazeno v grafu 1), kdy v roce 2023 proběhlo téměř 20 tisíc trestných činů v kyberprostoru. Mezi lety 2011 a 2021 byl růst pozvolný, avšak v roce 2022 přišel zlom a počet útoků v kyberprostoru se téměř zdvojnásobil. Tvořil více než 10 % trestných skutků toho roku. Rok 2023 přinesl další růst, ale už přiměřeně stabilizovaný. [23]



Graf č. 1: Vývoj registrovaných skutků trestné činnosti v kyberprostoru mezi lety 2011–2023

Zdroj: Vlastní zpracování podle [23]

2. VÝVOJ LEGISLATIVY TÝKAJÍCÍ SE KYBERNETICKÉ BEZPEČNOSTI

Tato kapitola se zaměřuje na vývoj právní úpravy v oblasti kybernetické bezpečnosti v České republice. Sleduje, jak se postupně formovala národní legislativa v reakci na rostoucí digitalizaci společnosti. Pozornost je věnována klíčovým bodům ve vývoji, které přispěly k ukotvení kybernetické bezpečnosti jako nedílné součásti právního systému.

Vývoj je zároveň posuzován i v kontextu evropské legislativy, zejména směrnic NIS a NIS2, které výrazně ovlivňují národní právní rámec a stanovují společné standardy kybernetické bezpečnosti v rámci Evropské unie.

2.1. Historie legislativy týkající se kybernetické bezpečnosti v České republice

Kybernetická bezpečnost se v České republice začala řešit na státní úrovni v roce 2000. Ministerstvo vnitra České republiky vytvořilo dokument "Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření [24]."

Tato koncepce byla primárně zaměřena na problematiku trestné činnosti v oblasti informačních technologií. I přes omezený rozsah se jednalo o první krok státu ve snaze vytvořit základní legislativní rámec v kybernetické oblasti. Dokument zdůrazňoval nutnost stabilního a bezpečného prostředí, které by občanům umožnilo pocit právní jistoty při používání informačních technologií.

Posun nastal 15. března 2010, kdy Vláda České republiky schválila **usnesení č. 205** [25], které se detailně **zabývalo problematikou kybernetické bezpečnosti**. Usnesení stanovilo Ministerstvo vnitra ČR gestorem a národní autoritou pro oblast kybernetické bezpečnosti. Rozhodnutí odráželo rostoucí **povědomí o důležitosti kybernetické bezpečnosti** jako klíčového faktoru pro ochranu kritické infrastruktury státu. V roce 2010 Ministerstvo vnitra ČR podepsalo Memorandum se sdružením CZ.NIC, při kterém byl zřízen Národní CSIRT (Popsán v kapitole 1.3 Zajišťování kybernetické bezpečnosti v ČR). [26]

Vláda ČR v roce 2011 zvolila usnesením gestorem problematiky kybernetické bezpečnosti Národní bezpečnostní úřad. Hlavním důvodem byla absence instituce, která by se na kybernetickou bezpečnost specializovala. Jedním z hlavních úkolů bylo vytvoření legislativního rámce. Stejným usnesením byla zřízena také Rada pro kybernetickou bezpečnost a byl schválen vznik Národního centra kybernetické bezpečnosti jako součást Národního bezpečnostního úřadu.

Národní centrum kybernetické bezpečnosti bylo pověřeno klíčovými úkoly, včetně **přípravy Zákona o kybernetické bezpečnosti** (ZoKB), [27] a dokončení plně funkčního centra-a to do konce roku 2015. V roce 2013 přišel první návrh ZoKB, který vstoupil v platnost roku 2014 pod označením 181/2014 Sb. s účinností od roku 2015. Tento zákon představoval **průlom pro kybernetickou bezpečnost**, neboť byl prvním zákonem, který definoval právní rámec pro ochranu kybernetického prostoru, stanovil podmínky pro provozovatele a pověřil NBÚ dozorem této oblasti. Samotný zákon bude více rozepsán v kapitole 2.2. [13]

Zásadními kroky u ZoKB byly dvě novelizace zákona č.104/2017 Sb. a č.205/2017 Sb.

Zákon **č.104/2017** Sb., [28], kterým se mění zákon č.181/2014 Sb., se zaměřuje na **zvýšení efektivity a koordinace** v oblasti kybernetické bezpečnosti. Hlavní změnou bylo zřízení NÚKIB jako ústředního orgánu státní správy odpovědného za kybernetickou bezpečnost. Tím převzal pravomoci, které dříve vykonávalo Národní centrum kybernetické bezpečnosti.

Zákon **č.205/2017** Sb.[29] byl přijat za účelem **zapracování** směrnice Evropského parlamentu a Rady 2016/1148, známé jako **směrnice NIS** (více uvedeno v kapitole 2.3.1), která stanovovala opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů.

Poslední platnou prováděcí vyhláškou ZoKB je vyhláška č.82/2018 Sb. [30], která byla vydána za účelem detailního rozpracování a konkretizace požadavků uvedených v tomto zákoně. Tato vyhláška zároveň slouží jako výchozí dokument pro porovnání s návrhem nové právní úpravy.

V roce 2023, před počátkem legislativního procesu nZoKB, se NÚKIB spojil s veřejností v rámci konzultace, která probíhala od 26.ledna do 23. března a týkala se 1. návrhu nového zákona. V průběhu více než 6 týdnů obdržel NÚKIB celkem 1144 připomínek a podmětů ke zveřejněným materiálům, ze kterých více než polovina byla zohledněna při aktualizaci návrhu nového zákona. [31]

2.2. Zákon číslo 181/2014 Sb. o kybernetické bezpečnosti

Přijetí ZoKB [27] bylo motivováno nárůstem používání informačních technologií a zvyšující se závislostí společnosti na jejich fungování. Díky tomuto nárustu vzrostl počet kybernetických útoků, hrozeb a zneužívání technologií. Jednou ze strategií Bezpečnostní strategie České republiky je prevence a potlačování kybernetických hrozeb, které by mohly ovlivnit bezpečnost nejen vnitřní, ale i vnější. [32]

Před vznikem tohoto ZoKB byla ochrana kyberprostoru řešena osobami a firmami samostatně díky absenci právního rámce. V průběhu roku 2014 byl přijat ZoKB a nabyl účinnosti dne 1.1.2015. Jeho hlavním cílem bylo stanovit minimální požadavky kybernetické bezpečnosti, které mají zefektivnit řešení kybernetických incidentů a vymezit oprávnění a povinnosti spolupráce mezi soukromým sektorem a veřejnou správou. Hlavním záměrem zákona je především ochrana kritické infrastruktury, jejíž narušení by mohlo vést k poškození či ohrožení národních zájmů. Jeho poslední platnou upravující vyhláškou je vyhláška č.82/2018 [1] [30]

2.3. Evropská legislativa

V České republice platí **povinnost plnit legislativní závazky**, které vyplývají z **členství v Evropské unii**. Většina právních předpisů je přijímána řádným legislativním procesem. Nejprve komise předloží návrh Evropskému parlamentu a následně Radě, která je složena ze zástupců členských států EU. Pro přijetí musejí oba orgány odsouhlasit znění daného předpisu. Parlamenty členských států obdrží legislativní návrhy Komise ve stejný čas jako Evropský parlament a Rada. Poté mají možnost podat k novele připomínky.[33]

2.3.1. Směrnice NIS

Směrnice NIS se celým oficiálním názvem nazývá „Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informací v Unii“ [35]. Jedná se o první ucelený **dokument o kybernetické bezpečnosti**, který vznikl na půdě Evropské unie. Cílem je zajistit vysokou míru bezpečnosti informačních systémů a bezpečnosti sítí. Za klíčové považuje dostupnost, autenticitu či důvěrnost dat a služeb. Do roku 2015 se praktická stránka kybernetické bezpečnosti mezi státy výrazně lišila. Bylo tak jisté, že je jen otázkou času, kdy se objeví oficiální doporučení nebo regulace ze strany EU. Směrnice NIS **vstoupila v platnost v srpnu 2016** a v průběhu 21 měsíců musely členské státy implementovat tuto směrnici do své národní legislativy. **Pouze tři státy v té době už právní rámec pro danou oblast měly, těmi jsou Česká republika, Estonsko a Maďarsko**. Díky ZoKB, který v České republice splňoval většinu pravidel, byl pouze upraven zákonem 207/2017 Sb.[29], čímž byla pokryta nedostatečně chráněná místa v zákoně. [36][37][38]

2.3.2. Směrnice NIS2

Směrnice 2022/2555, více známá jako NIS2 [39], **navazuje na předešlou směrnici NIS** [35] z roku 2016. Tato směrnice byla přijata jako reakce na rostoucí trestnou aktivitu v kyberprostoru. Hlavním úkolem NIS je **zvýšení úrovně kybernetické bezpečnosti** napříč evropskými státy. Požadavky se soustředí na technická opatření, soft skills nebo i školení zaměstnanců v oblasti kyberbezpečnosti. V prosinci roku 2022 byla zveřejněna oficiální evropská směrnice a v tuto chvíli se projednává Vládou ČR, kdy a za jakých podmínek bude implementována do národní legislativy.

Směrnice je **reakcí na odstranění rozdílů** mezi jednotlivými členskými státy Evropské unie. Rozdíly se objevují zejména na úrovni hlášení incidentů či jejich povinností. Zavedením jednotných opatření a povinností bude docíleno větší právní jistoty a stabilizovaného fungování vnitřního trhu. Směrnice **rozšiřuje** zejména **regulovaná odvětví a okruh povinných osob** (ukázáno na Obrázek č. 2). Regulované služby podle NIS2 zpřísňují požadavky CIA (jak bylo popsáno v kapitole 1.1) a zavádí přísnější sankce. NIS2 také klade větší důraz na mezinárodní spolupráci při kybernetických hrozbách a následných reakcích na kybernetické incidenty.

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential“.

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik“ a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik“ a „střední podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important“ (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022

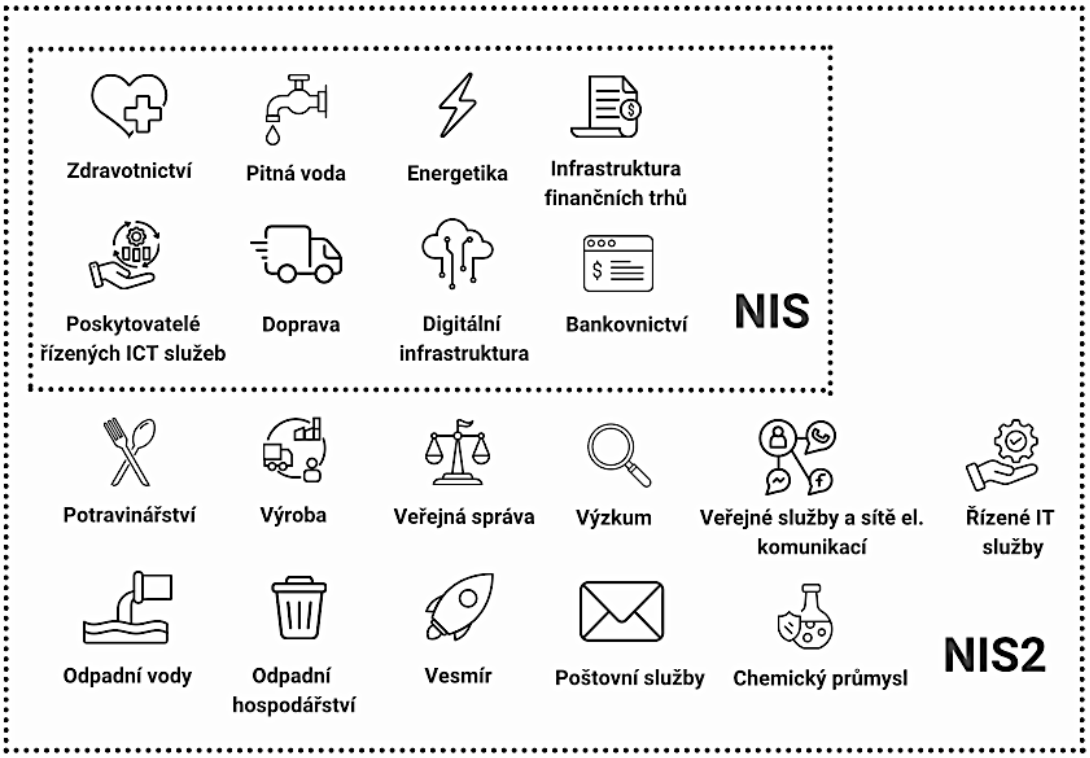
Zdroj: [40]

Obrázek č. 2: Regulované služby podle NIS2

Srovnání směrnice NIS a NIS2

Směrnice NIS [35] vstoupila v platnost v roce 2016 a vztahovala se převážně na úzkou skupinu subjektů. NIS2 [39]. Významně rozšířila počet subjektů a kategorií, jak je znázorněno na Obrázek č. 3, na které se vztahují nové povinnosti. Povinnosti se rozšiřují na potravinářství, výroby, veřejné služby a sítě elektrických komunikací (například na mobilní operátory), řízené IT služby (například na organizace spravující informační systém v nemocnicích), odpadní vody, odpadní hospodářství (například třídění odpadu), poštovní služby, chemický průmysl a další.

Zavedením přísnějších požadavků se musí zvýšit intenzita spolupráce mezi organizacemi a NÚKIB. Pokuty za nedodržení požadavků se rozlišují podle toho, jestli organizace spadá do bezpečnostních opatření s nižšími povinnostmi, může být uložena pokuta do 7 milionů eur nebo až 1,4 % z celosvětového ročního obratu. V případě organizací s vyššími povinnostmi se jedná 10 miliónů eur nebo až 2 % z celosvětového ročního obratu. Regulovaná odvětví se liší, protože dochází k úpravám, které musí odpovídat specifikům českého právního prostředí.[41][42]



Obrázek č. 3: Rozšíření regulovaných odvětví dle NIS2

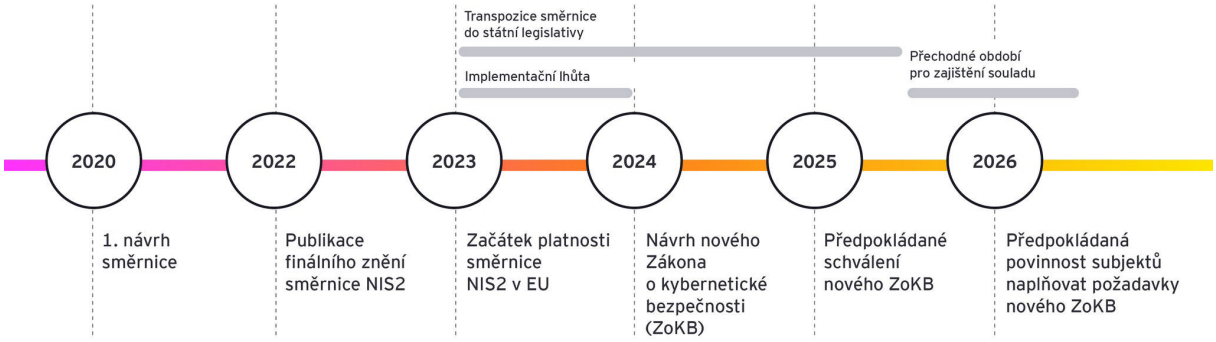
Zdroj: [43]

2.4. Návrh nového zákona o kybernetické bezpečnosti

Směrnice NIS2 (podrobněji popsána v kapitole 2.3.2) **přináší řadu podstatných změn oproti předchozímu regulačnímu rámci**, který reflektuje rostoucí intenzitu a sofistikovanost kybernetických hrozeb v evropském prostoru. Jedná se o reakci na zjištěné nedostatky implementace směrnice NIS a výrazné rozdíly přístupu jednotlivých států k zabezpečení sítí a informačních systémů. Směrnice NIS2 vstoupila v platnost v prosinci 2022 a od té doby běží osmnáctiměsíční transpoziční lhůta, do které členské státy EU musí implementovat znění směrnice do své národní legislativy.

V České republice byl touto **transpozicí pověřen NÚKIB**, který se rozhodl nepřistoupit k novelizaci stávajícího zákona 181/2014 Sb., ale k zpracování zcela nového návrhu zákona o kybernetické bezpečnosti. Důvodem byla především značná šíře nových povinností a potřeba přehledného a srozumitelného legislativního rámce. Návrh vychází z dosavadního znění [27] s novými povinnostmi, navíc zohledňuje zkušenosti a poznatky NÚKIB, které za dobu své existence získal.

Níže uvedená časová osa, zobrazená na Obrázek č. 4, zobrazuje vznik a implementaci NIS2, kdy v roce 2020 vyšel návrh revize směrnice, kterým byla upravena směrnice NIS. Oficiální znění směrnice NIS2 bylo publikováno až v prosinci 2022. V návaznosti na to byla spuštěna transpoziční lhůta 18 měsíců na implementaci zákona do vnitřní legislativy jednotlivých členských států, jejíž konec připadal na říjen 2024. Její implementace se však prodloužila a očekává se, že **vstoupí v platnost v průběhu roku 2025**, pravděpodobně v jeho druhé polovině. Pro většinu povinných subjektů se předpokládá, že budou mít ještě přechodné období do začátku roku 2026, kdy začne pravděpodobně platit plná účinnost zákona a s tím spojená možnost jeho vymáhání příslušnými orgány, zejména NÚKIB.



Obrázek č. 4: Časová osa ke vzniku a implementaci NIS2 do české legislativy

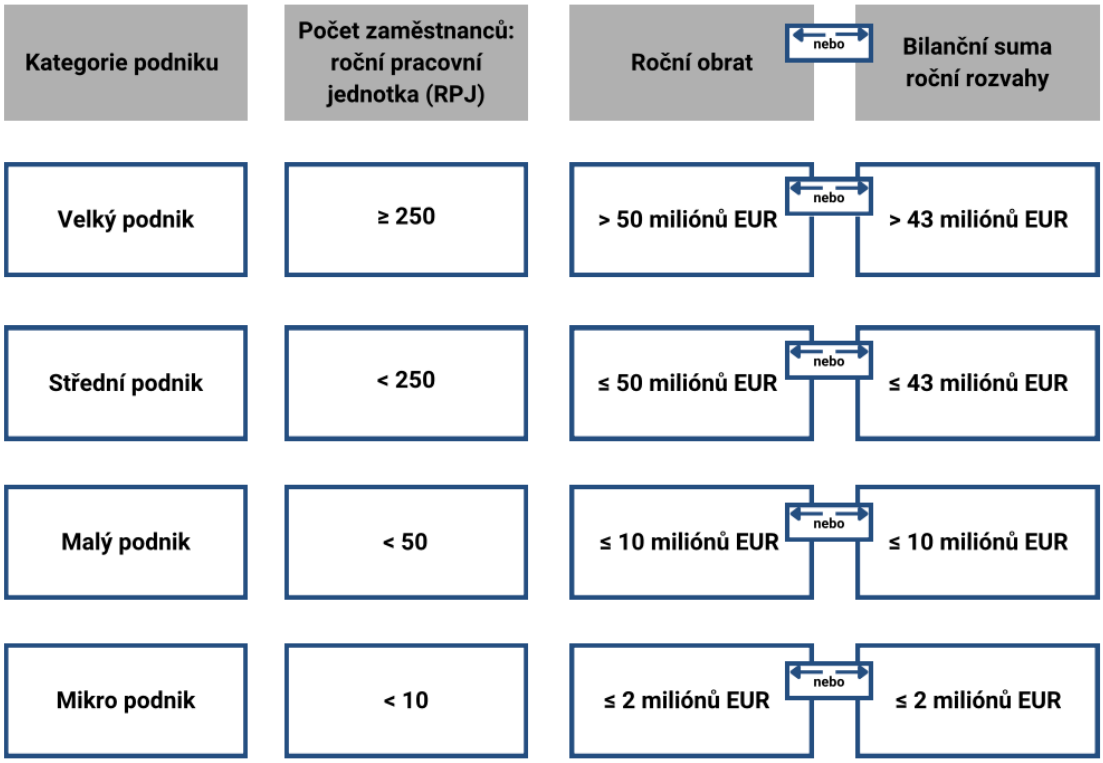
Zdroj: [44]

2.4.1. Rozdělení organizací podle významnosti a regulace

Návrh zákona o kybernetické bezpečnosti (nZoKB) [45] sdružuje typy povinných osob do jedné skupiny – tzv. poskytovatele regulované služby. Jedná se o organizace, které splňují podmínky k registraci. Podmínkou je, že organizace **působí v regulovaném odvětví** (zobrazeno na Obrázek č. 2), **poskytuje regulovanou službu**, která je ve Vyhlášce o regulovaných službách [45] nebo jsou **dostatečně významné**, tzn. splňují stejnou významnost jako regulované služby, většinou velikostí podniku, ročního obratu nebo jiného kritéria, které je taktéž obsaženo ve Vyhlášce o regulovaných službách [45].

Pokud je organizace regulovaná, musí plnit povinnosti, mezi které patří ohlášení služby organizace, zavádění bezpečnostních opatření, nahlášení kontaktních údajů zodpovědné osoby za kybernetickou bezpečnost v organizaci, hlášení kybernetických incidentů a provádění protiopatření, které vydává NÚKIB. [46]

Nutným měřítkem je zjistit velikost daného podniku (kategorizace na obrázku 5). **Velikost je vyhodnocena na základě počtu zaměstnanců a ročního obratu, nebo bilanční sumy roční rozvahy.** Při posuzování si organizace může sama vybrat, který ukazatel (roční obrat, nebo bilanční suma) je pro ni výhodnější. Vyjma dvou případů, a to, pokud dojde k překročení hranice počtem zaměstnanců automaticky, se velikost organizace posouvá na odpovídající vyšší velikost. Nebo pokud je počet zaměstnanců stejný, ale roční obrat i bilanční suma roční rozvahy jsou překročeny, musí organizace splnit pravidla vyššího podniku. V případě, že dojde k překročení pouze jednoho finančního ukazatele, status organizace zůstane stejný.



Obrázek č. 5: Ukazatel velikosti subjektu

Zdroj:[47]

Pro určení, zda se na danou organizaci vztahují požadavky nZoKB, musí dojít nejdříve k posouzení, zda organizace poskytuje **regulovanou službu a zároveň splňuje kritéria významnosti**. Tato kritéria jsou podrobně specifikována ve Vyhlášce o regulovaných službách [45], která stanovuje podmínky, za nichž je organizace považována za subjekt regulovaný ZoKB.

Režim **nižších povinností** přináší méně nových povinností a vyžaduje jen několik změn malého rozsahu. Důraz je kladen na zajištění přiměřené úrovně kybernetické bezpečnosti, a to zejména prostřednictvím základních technických a organizačních opatření.

Režim **vyšších povinností** je obsahově téměř třikrát delší, rozsáhlejší a přísnější. Vyžaduje více odborníků, řízení rizik, audity kybernetické bezpečnosti, vyhodnocování kybernetických bezpečnostních událostí a další.

2.4.2. Modelové příklady regulovaných služeb

Na základě výše uvedených kritérií budou následovat konkrétní příklady regulovaných služeb.

Zjištění tohoto statusu je klíčové pro znalost rozsahu povinností, které bude muset organizace splnit, a to včetně zavedení bezpečnostních opatření, hlášení incidentů nebo účasti na kontrolách. V případě, že si organizace není jista svým určením, je doporučeno se obrátit na NÚKIB, který je klíčovým centrem, pokud jde o kybernetickou bezpečnost nebo využít metodické podpory vydané k nZoKB.

Každá služba, která je ve vyhlášce uvedena, je pod konkrétním odvětvím. Například pod oblastí energetiky je zařazena služba „Těžba ropy“, u které je přesně určeno, jaká regulace bude platit v závislosti na **klasifikaci její velikosti** (zobrazeno v Tabulka č. 1). V rámci modelového příkladu se jedná o organizaci, která poskytuje službu v oblasti těžby ropy. Organizace spadá mezi regulované služby, pouze pokud se jedná o střední nebo velký podnik. Pokud se jedná o malý nebo mikro podnik, regulaci nepodléhají.

Tabulka č. 1: Ukázka č.1 regulované služby z Vyhlášky o regulovaných službách

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
3.1. Těžba ropy	Provozovatel zařízení na těžbu ropy je I. Poskytovatel regulované služby v režimu vyšších povinností v případě, že je **velkým podnikem.** II. Poskytovatel regulované služby v režimu nižších povinností v případě, že je **středním podnikem**.

Zdroj:[45]

Pro lepší pochopení dělení organizací budou představeny 3 fiktivní organizace v odvětví těžby ropy v návaznosti na Tabulka č. 1.

Příklad č.1: Organizace, která má 170 zaměstnanců, ročním obratem 65 miliónů eur a bilanční sumou 50 miliónů eur, bude považována za velký podnik, protože přesáhla roční obrat i bilanční sumu. Jako poskytovatel, který je velkým podnikem, spadá do režimu vyšších povinností.

Příklad č.2: Organizace s 8 zaměstnanci, ročním obratem 3 milióny eur a bilanční sumou 1 milión eur spadá pod mikro podnik a nespadá tak pod regulovanou službu.

Příklad č.3: Organizace s 40 zaměstnanci, ročním obratem 9 milionů eur a bilanční sumou 15 miliónů eur patří mezi malé podniky. I přes překročení bilanční sumy (15 mil.) se může považovat za mikro, protože podle ročního obratu strop nepřekračuje.

Tabulka č. 2: Ukázka č.2 regulované služby z Vyhlášky o regulovaných službách

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
18.2.Poskytování zdravotnické záchranné služby	Poskytovatel zdravotnické záchranné služby podle zákona o zdravotnické záchranné službě je poskytovatel regulované služby v režimu vyšších povinností.

Zdroj:[45]

Ve Vyhlášce o regulovaných službách **jsou** však **i služby, u kterých se nehledí na velikost**, a všechny organizace ji musí splňovat na stejné úrovni, jako je u služby 18.2. (zobrazeno v Tabulka č. 2). Zde se jedná o regulovanou službu v poskytování zdravotnické záchranné služby. Jedná se o jedinou službu v rámci zdravotnictví, u které její rozsah nehraje roli. Regulaci, která se vztahuje na všechny, najdeme například i u letecké dopravy, přesněji pak u služby Řízení letového provozu ve vzdušném prostoru České republiky nebo drážní dopravy při stavění vlakových cest a další podobné organizace.

3. ROZBOR NÁVRHU NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Prvním krokem pro zjištění změn mezi vyhláškou zákona 82/2018 Sb., dále uváděno jako ZoKB [30], a návrhem Zákona o kybernetické bezpečnosti (nZoKB) [45] byla důkladná komparace obou právních předpisů. **Cílem rozboru bylo identifikovat rozdíly**, které mohou mít dopad na aplikaci zákona. Nezbytně nutné jsou úpravy v organizačním a procesním nastavení subjektů, na které se zákon bude vztahovat. V této fázi je nutný rozbor jednotlivých paragrafů u obou předpisů, jejich vzájemné provázanosti a podobnosti, ale především odlišností, které reflektují nové požadavky a rozšířenou působnost zákona. Důležitou součástí tohoto procesu bylo porovnání znění jednotlivých právních opatření a rozbor jejich praktického dopadu, který bude ovlivňovat provozní prostředí dotčených organizací. **Rozbor se bude vztahovat na organizaci v režimu vyšších povinností.**

3.1. Motivace pro nový zákon

Hlavní motivací pro přijetí nového zákona byla nutnost **reagovat na rostoucí a propracovanější kybernetické hrozby** a zároveň zajistit systémový přís**tup k ochraně aktiv a digitálních služeb** v České republice. Návrh zohledňuje technické, právní i organizační prvky kybernetické bezpečnosti.

NÚKIB se přiklonil k sepsání nového zákona vzhledem k vysokému počtu změn, který by se pravděpodobně dal řešit skrz upravující vyhlášku, ale se zaimplementovanou vyhláškou by se zákon stal nepřehledným a zbytečně složitým. Návrh zákona **reflektuje i vývoj v oblasti mezinárodních standardů** a je rovněž nástrojem pro implementaci evropské směrnice NIS2, jejímž cílem je zajistit vysokou úroveň kybernetické bezpečnosti v celé Evropské unii.

Zákon přináší změny v rozsahu regulace – nově se bude vztahovat na širší okruh organizací soukromého i veřejného sektoru. Firmy budou muset zavádět nejen technická, ale i organizační bezpečnostní opatření, hlásit incidenty a minimalizovat dopady kybernetických rizik.

Další zásadní změnou je i přístup k samotné regulaci. Nový zákon se zaměřuje na celé organizace, nejen na vybrané IT složky. **Cílem je vytvořit odolnější digitální prostředí**, které bude schopné včasně reagovat na kybernetické incidenty a zajistit plynulé fungování klíčových služeb i v krizových situacích.[48][49]

3.2. Porovnání stávajícího zákona a návrhu nového

Jako první bylo zpracováno srovnání názvů paragrafů ZoKB a nZoKB (zobrazeno níže v Tabulka č. 3). Organizace, pro kterou bylo srovnání vytvořeno, je **v režimu vyšších povinností**. Pro systematické porovnání byly rozděleny podle oblastí opatření – organizační a technická. **Cílem je poskytnout základní orientaci v obsahu** obou právních opatření a umožnit první srovnání ještě před provedením podrobného rozboru. Tato část slouží jako základ pro znázornění konkrétních vazeb.

Tabulka č. 3: Srovnání názvů paragrafů ZoKB a nZoKB v režimu vyšších povinností

Srovnání názvů paragrafů ZoKB a nZoKB v režimu vyšších povinností				
Názvy paragrafů ZoKB			**Názvy paragrafů nZoKB**	
Organizační opatření			**Organizační opatření**	
§ 3	Systém řízení bezpečnosti informací		§ 4	Systém řízení bezpečnosti informací
§ 4	Řízení aktiv		§ 5	Povinnosti vrcholného vedení
§ 5	Řízení rizik		§ 6	Bezpečnostní role
§ 6	Organizační bezpečnost		§ 7	Řízení bezpečnostní politiky a bezpečnostní dokumentace
§ 7	Bezpečnostní role		§ 8	Řízení aktiv
§ 8	Řízení dodavatelů		§ 9	Řízení rizik
§ 9	Bezpečnost lidských zdrojů		§ 10	Řízení dodavatelů
§ 10	Řízení provozu a komunikací		§ 11	Bezpečnost lidských zdrojů
§ 11	Řízení změn		§ 12	Řízení změn
§ 12	Řízení přístupu		§ 13	Aktivizace, vývoj a údržba
§ 13	Akvizice, vývoj a údržba		§ 14	Řízení přístupu
§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů		§ 15	Zvládání kybernetických bezpečnostních událostí a incidentů
§ 15	Řízení kontinuity činností		§ 16	Řízení kontinuity činností
§ 16	Audit kybernetické bezpečnosti		§ 17	Audit kybernetické bezpečnosti
Technická opatření			**Technická opatření**	
§ 17	Fyzická bezpečnost		§ 18	Fyzická bezpečnost
§ 18	Bezpečnost komunikačních sítí		§ 19	Bezpečnost komunikačních sítí
§ 19	Správa a ověřování identit		§ 20	Správa a ověřování identit
§ 20	Řízení přístupových oprávnění		§ 21	Řízení přístupových oprávnění
§ 21	Ochrana před škodlivým kódem		§ 22	Detekce kybernetických bezpečnostních událostí
§ 22	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů		§ 23	Zaznamenávání událostí
§ 23	Detekce kybernetických bezpečnostních událostí		§ 24	Vyhodnocování kybernetických bezpečnostních událostí
§ 24	Sběr a vyhodnocování kybernetických bezpečnostních událostí		§ 25	Aplikační bezpečnost
§ 25	Aplikační bezpečnost		§ 26	Kryptografické algoritmy
§ 26	Kryptografické prostředky		§ 27	Zajišťování dostupnosti regulované služby
§ 27	Zajišťování úrovně dostupnosti informací		§ 28	Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv
§ 28	Průmyslové, řídicí a obdobné specifické systémy			
§ 29	Digitální služby			

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

Po vypsání paragrafů ZoKB a nZoKB bylo vytvořeno další srovnání (zobrazeno v Tabulka č. 4), kde je zobrazena vzájemná vazba mezi jednotlivými opatřeními z Tabulka č. 3, a to s cílem zjistit míru jejich shody a návazností. V rámci rozboru bylo sledováno, do jaké míry se názvy paragrafů vyhlášek shodují, zda jsou obsahově velmi podobné, nebo zda některé paragrafy postrádají odpovídající protějšek v druhé vyhlášce.

V případech, kdy názvy paragrafů **nebyly jednoznačně shodné**, bylo přistoupeno k bližšímu předběžnému rozboru obsahu – konkrétně k **porovnání prvních tří bodů** příslušných paragrafů. Tento postup umožnil přesněji určit, zda se jedná o obsahově související paragrafy, shodná opatření s odlišným názvem, nebo zda jde o zcela nově zavedené či naopak zrušené části vyhlášky. Vzhledem k tomu, že nZoKB vychází ze struktury původní, bylo ve většině případů možné poměrně rychle určit, zda mezi jednotlivými paragrafy existuje přímá návaznost, či nikoliv.

Tabulka č. 4: Vazby mezi paragrafy stávající a nové vyhlášky

Vazby mezi paragrafy stávající a nové vyhlášky	
Organizační opatření	
ZoKB	nZoKB
3	4
4	8
5	9
6	5
7	6
8	10
9	11
10	-
-	7
11	12
12	14
13	13
14	15
15	16
16	17

Vazby mezi paragrafy stávající a nové vyhlášky	
Technická opatření	
ZoKB	nZoKB
17	18
18	19
19	20
20	21
21	-
22	23
23	22
24	24
25	25
26	26
27	27
28	28
29	-

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

Na základě zjištění vazeb mezi texty ZoKB a nZoKB byla vytvořena **Pracovní srovnávací tabulka** (Tabulka č. 5). V této tabulce je zobrazena hierarchie každého opatření – paragraf, odstavec, písmeno, bod. Pracovní srovnávací tabulka sloužila jako nástroj pro identifikaci rozdílů mezi původní právní úpravou a novou právní úpravou.

Při tvorbě pracovní srovnávací tabulky byla dodržena následující pravidla:

1. Zachovat **přesné znění** jednotlivých textů u každé vyhlášky zvlášť.
2. Každému samostatnému bodu v rozboru byl **vyčleněn samostatný řádek**, ve kterém je uvedeno jeho znění a zároveň kompletní hierarchické označení vyhlášky. Místa, kde již číslování nepokračuje, jsou vyplněna pomlčkou.
3. V případech, kdy jedna vyhláška rozděluje jeden bod druhé do více bodů, je číslování rozděleno do více označení. (Ukázka v Tabulka č. 6)
4. Naopak tam, kde jedna vyhláška slučuje více bodů druhé vyhlášky do jednoho, je číslování sloučeno do jednoho označení. (Ukázka v Tabulka č. 7)

Tabulka č. 5: Ukázka pracovní srovnávací tabulky – srovnání §6 ZoKB a §5 nZoKB

Organizační opatření									
ZoKB					nZoKB v režimu vyšších povinností				
§	Odstavec	Písmeno	Bod	Požadavek	§	Odstavec	Písmeno	Bod	Požadavek
6	(1)	j	-	zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,	5	(1)	l)	-	zajistí, aby byla zachována mlčenlivost u všech relevantních osob (např. administrátorů, osob zastávajících bezpečnostní role, osob s přístupem k citlivým informacím, dodavatelů apod.)
6	(1)	k	-	pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a	5	(1)	m)	-	pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a
6	(1)	l	-	zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.	5	(1)	n)	-	zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.
-	-	-	-		5	(2)	-	-	Vrcholné vedení se prokazatelně seznamuje se
-	-	-	-		5	(2)	a)	-	zprávou o přezkoumání systému řízení bezpečnosti informací,
-	-	-	-		5	(2)	b)	-	zprávou o hodnocení rizik,
-	-	-	-		5	(2)	c)	-	výsledky analýzy dopadů v souladu s § 16 a
-	-	-	-		5	(2)	d)	-	výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.
6	(2)	-	-	Povinná osoba v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.	5	(3)	-	-	Vrcholné vedení v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti, bezpečnostní role, jejich práva a povinnosti související se systémem řízení bezpečnosti informací.
-	-	-	-		5	(4)	-	-	Jednání výboru pro řízení kybernetické bezpečnosti probíhají v pravidelném intervalu a o jejich průběhu je veden dokumentovaný záznam
6	(3)	-	-	Povinná osoba uvedená v § 3 písm. c), d) a f) zákona určí osobu, která bude zastávat bezpečnostní roli	5	(6)	-	-	Vrcholné vedení určí osobu, která bude zastávat bezpečnostní roli
6	(3)	a	-	manažera kybernetické bezpečnosti,	5	(6)	a)	-	manažera kybernetické bezpečnosti,
6	(3)	b	-	architekta kybernetické bezpečnosti,	5	(6)	b)	-	architekta kybernetické bezpečnosti,
6	(3)	c	-	garanta aktiva a	5	(6)	c)	-	garanta aktiva a
6	(3)	d	-	auditora kybernetické bezpečnosti.	5	(6)	d)	-	auditora kybernetické bezpečnosti.
6	(4)	-	-	Povinná osoba uvedená v § 3 písm. e) zákona určí role manažera kybernetické bezpečnosti a garanta aktiva. Ostatní bezpečnostní role podle odstavce 3 určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací.	-	-	-	-	
6	(5)	-	-	Povinná osoba uvedená v § 3 písm. c), d) a f) zákona zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 3 písm. a) a b).	5	(7)	-	-	Vrcholné vedení zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písm. a) a b).
6	(6)	-	-	Povinná osoba uvedená v § 3 písm. e) zákona zajistí zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti.	-	-	-	-	
6	(7)	-	-	Výbor pro řízení kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností, jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.	5	(5)	-	-	Výbor pro řízení kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností, jehož členem musí být alespoň jeden zástupce vrcholného vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.

Zdroj: Vlastní zpracování při porovnání [30][45]

Tabulka č. 6: Ukázka rozdělení jednoho bodu vyhlášky do více bodů

Organizační opatření									
ZoKB					nZoKB v režimu vyšších povinností				
§	Odstavec	Písmeno	Bod	Požadavek	§	Odstavec	Písmeno	Bod	Požadavek
3	g)	-	-	zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací,	4	(1)	f)	-	zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací alespoň jednou ročně, které obsahuje
					4	(1)	f)	1.	vyhodnocení cílů systému řízení bezpečnosti informací směřujících k zajištění bezpečnosti regulované služby,
					4	(1)	f)	2.	posouzení naplňování plánu zvládání rizik zpracovaného podle § 9 písm. g),
					4	(1)	f)	3.	hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik,
					4	(1)	f)	4.	posouzení výsledků provedených auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
					4	(1)	f)	5.	výsledky předchozích hodnocení účinnosti systému řízení bezpečnosti informací provedených podle tohoto písmena,
					4	(1)	f)	6.	posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby podle § 16 a na oblast kybernetické bezpečnosti a

Zdroj: Vlastní zpracování při porovnání [30][45]

Tabulka č. 7: Ukázka sloučení více bodů do jednoho bodu

Organizační opatření									
ZoKB					nZoKB v režimu vyšších povinností				
§	Odstavec	Písmeno	Bod	Požadavek	§	Odstavec	Písmeno	Bod	Požadavek
4	(1)	a)	-	stanoví metodiku pro identifikaci aktiv,	8	a)	-	-	stanoví metodiku pro identifikaci a hodnocení aktiv včetně stanovení úrovní aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,
4	(1)	b)	-	stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce					

Zdroj: Vlastní zpracování při porovnání [30][45]

Tento postup zajišťuje:

a) Že je každý jednotlivý bod snadno dohledatelný.

b) Že jsou vizuálně patrná chybějící místa.

c) Že výskyt těchto chybějících míst v rozboru slouží jako indikátor změněných nebo nově zaváděných povinností dle nZoKB.

Rozsah pracovní srovnávací tabulky, která obsahovala kompletní znění obou právních předpisů, **byl značný** a její pochopení by bylo časově náročné. Tabulka tvořila 404 jednotlivých řádků členěných podle paragrafů, odstavců, písmen a bodů. Z toho důvodu **bylo** tedy **přistoupeno k vytvoření zkrácené** a přehlednější **verze: Tabulky – Nově zavedené body (**část zobrazena v Tabulka č. 8, kompletní seznam změn je v Příloze 1). Tato Příloha 1 obsahuje všech 98 nově zavedených bodů, na které je nutné se zaměřit.

Tabulka č. 8: Ukázka z Přílohy 1: nově zavedená opatření (9 z 98 opatření)

Organizační opatření				
Opatření, která jsou přidaná v nZoKB				
§	**Odstavec**	**Písmeno**	**Bod**	**Požadavek**
4	(1)	k	-	stanoví proces řízení výjimek z pravidel stanovených podle písm. d).
5	(1)	a)	-	se prokazatelně účastní školení podle § 11 odst. 3 písm. a),
5	(1)	h)	-	se podílí na vypracování analýzy dopadů podle § 16,
5	(2)	-	-	Vrcholné vedení se prokazatelně seznamuje se
5	(2)	a)	-	zprávou o přezkoumání systému řízení bezpečnosti informací,
5	(2)	b)	-	zprávou o hodnocení rizik,
5	(2)	c)	-	výsledky analýzy dopadů v souladu s § 16 a
5	(2)	d)	-	výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.
5	(4)	-	-	Jednání výboru pro řízení kybernetické bezpečnosti probíhají v pravidelném intervalu a o jejich průběhu je veden dokumentovaný záznam

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

3.3. Klíčové novinky a změny

Nový zákon se bude vztahovat **především na střední a velké organizace**, ale zároveň bude působit v definovaných regulovaných oblastech. Zvýší se počet regulovaných organizací, nově budou organizace přímými subjekty odpovědnými za dodržování zákonných povinností. Tato část je zaměřena hlavně na změny, které mají zásadní dopad na činnost organizace a její povinnosti, které jsou v implementaci nejdůležitější.

V tabulkách níže jsou uvedené znatelné změny opatření, které jsou přidané v nZoKB.

Tabulka č. 9: Zobrazení paragrafu 7 a jeho 12 nových opatření

7	(1)	-	-	Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace
7	(1)	a)	-	stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5 k této vyhlášce a
7	(1)	b)	-	v provozní dokumentaci stanoví pravidla a postupy, které zohledňují relevantní oblasti z bezpečnostní politiky a bezpečnostní dokumentace.
7	(2)	-	-	Povinná osoba dodržuje pravidla a postupy stanovené podle odstavce 1.
7	(3)	-	-	Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlednění jejich relevantních oblastí v provozní dokumentaci.
7	(4)	-	-	Povinná osoba určí osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky, bezpečnostní dokumentace a zohlednění jejich relevantních oblastí v provozní dokumentaci podle odstavce 3.
7	(5)	-	-	Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly
7	(5)	a)	-	dostupné v elektronické nebo listinné podobě,
7	(5)	b)	-	komunikovány v rámci povinné osoby,
7	(5)	c)	-	přiměřeně dostupné dotčeným stranám,
7	(5)	d)	-	chráněny z pohledu důvěrnosti, integrity a dostupnosti a
7	(5)	e)	-	vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

§7 je novým paragrafem (výše uvedená Tabulka č. 9), který zavádí **nové požadavky na tvorbu, správu a přezkum bezpečnostní dokumentace**. Doporučuje role, které organizace

musí mít. Mezi ně patří manažer, architekt, auditor a garant kybernetické bezpečnosti, kdy každý má stanovené znalosti, zkušenosti, jejich vzdělání a praxe, u kterého je podmínka stejná – minimálně 3 roky praxe v oblasti informační nebo kybernetické bezpečnosti, anebo absolvování vysoké školy a rok praxe v oblasti.

Dokumentace musí být také aktuální, dostupná, chráněná a přehledná, tím zvyšuje důraz na její kvalitu a správu. Dokumenty taktéž musí být srozumitelné, jednoduše dohledatelné a úplné.

Tabulka č. 10: Část paragrafu 17 a jeho 7 nových opatření

17	(1)	-	-	Povinná osoba stanoví plán provádění auditu kybernetické bezpečnosti.
17	(3)	-	-	Povinná osoba zohlední výsledky auditu kybernetické bezpečnosti podle odstavce 2 v
17	(3)	a)	-	plánu zvládání rizik,
17	(3)	b)	-	prohlášení o aplikovatelnosti a
17	(3)	c)	-	plánu rozvoje bezpečnostního povědomí.
17	(4)	-	-	Povinná osoba stanoví případná nápravná opatření pro splnění požadavků podle odstavce 2.
17	(5)	c)	-	v souladu s plánem auditu kybernetické bezpečnosti.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

§17 (zobrazeno v Tabulka č. 10) udává, že každá organizace, která spadá pod zákon, musí mít **plán, jak a kdy bude provádět audity**. Audity jsou systematické kontroly a hodnocení, jejichž cílem je zjistit, jak dobře je organizace chráněná, zda dodržuje zákonné požadavky a jestli jsou nastavená opatření funkční. Povinná osoba tedy stanoví audity a zohlední jejich výsledky. Tento paragraf se soustředí na řízení auditu a následné kroky, které mají zajistit zlepšování bezpečnostních opatření v organizacích.

Tabulka č. 11: Část paragrafu 20 a jeho 8 nových opatření

20	(9)	-	-	Povinná osoba u administrátorského účtu určeného zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, musí vynucovat následující pravidla
20	(9)	a)	-	bezodkladně vynutí změnu výchozí hesla,
20	(9)	b)	-	heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
20	(9)	c)	-	délka hesla musí být alespoň 22 znaků,
20	(9)	d)	-	heslo musí být bezpečně uloženo,
20	(9)	e)	-	s účtem a jeho heslem mohou manipulovat pouze pověřené osoby a to v nezbytně nutných případech,
20	(9)	f)	-	musí být vynucena změna hesla po jeho použití, při jakékoli změně odpovědných osob nebo v intervalu maximálně po 18 měsících a
20	(9)	g)	-	eviduje manipulaci a pokusy o manipulaci s tímto účtem a jeho heslem.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 1*

§20 (zobrazeno v Tabulka č. 11) určuje **správu a ověřování identit**, kdy v odstavci 9 určuje pravidla pro hesla a účty. Pro technické a administrátorské účty je nutná délka hesla minimálně 22 znaků, musí být bezpečně uložena a pravidelně se měnit, a to minimálně každých 18 měsíců. Musí být také vedena evidence manipulace s účty a hesly nebo pokusy o manipulaci s nimi.

3.4. Identifikace dopadů na organizace

Dopady na organizace budou rozsáhlé. Budou se dotýkat **více než 8 000** soukromých i státních **organizací** v režimu nižších i vyšších povinností, což je přibližně **patnáctkrát více než bylo dosud**. V režimu nižších povinností by však měla být většina, a to téměř 7000 subjektů, v režimu vyšších povinností pak přes 1200 subjektů. [50]

Velkým problémem, který nastane během několika málo měsíců, bude **nepříznivý dopad nákladů na zavedení bezpečnostních opatření**. Z dostupných zdrojů NÚKIB se bude zavedení a provedení opatření pohybovat **mezi 800 tisíci a 1,5 miliónem Kč** vůči jednomu zabezpečovacímu systému. **Dané náklady se budou** však mezi organizacemi **lišit**. Některé mohou část opatření již splňovat, díky tomu pro ně dopady tak velké nebudou. Jiné organizace budou muset vlastnit víc systémů a náklady se jim tak zvýší. Analýza nákladů tedy není možná plošně. Je zde spousta proměnných, které předpokládané náklady mění–je jim například aktuální stav zajištění kybernetické bezpečnosti, soulad s aktuálním zněním ZoKB, počet regulovaných subjektů v organizaci a další. [51]

nZoKB přináší sankce, které musí být brány velmi vážně. Nejvyšším trestem je **zákaz výkonu řídící funkce** jakékoliv osobě, která má odpovědnost za výkon řídících funkcí (ředitel nebo zástupce v tomto sektoru). Pokud tato osoba opakovaně poruší povinnosti plnění rozhodnutí NÚKIB, zákaz výkonu se jí týká nejméně na 6 měsíců a může být prodloužen až do doby odstranění nedostatků. Tyto sankce lze uložit pouze u organizace, která spadá pod režim vyšších povinností. V případě **finančních sankcí** se pokuty pohybují v rozmezí **50 tisíc až 250 miliónů** nebo do výše **2 %** čistého celosvětového obratu. [52]

4. MOŽNOSTI APLIKACE VE VYBRANÉ ORGANIZACI

Pro zobrazení možnosti aplikace požadavků nového zákona jsem si vybrala **Univerzitu Pardubice**. Ač jako některé vysoké školy by mohla spadat pod režim nižších povinností, některými částmi jako je například **citlivý výzkum** (zobrazeno v Tabulka č. 12) nebo **počtem zaměstnanců**, kterých je téměř 1200 (podle přílohy 6.2 zdroje), spadá do režimu vyšších povinností. [52]

Tabulka č. 12: Ukázka č.3 regulované služby z Vyhlášky o regulovaných službách

19.1. Výzkum a vývoj	Výzkumná instituce, výzkumná organizace podle přímo použitelného předpisu Evropské unie, veřejná výzkumná instituce nebo vysoká škola je poskytovatelem regulované služby v režimu vyšších povinností v případě, že provádí citlivou výzkumnou činnost.

Zdroj:[45]

4.1. Návrhy opatření pro zajištění souladu s právní úpravou

Do UPCE směrnic **je potřeba zavést řadu změn**, zpřísnění nebo důkladnější specifikace požadavků. Vzhledem k tomu, že autor této práce nemá přístup k úplnému znění vnitřních směrnic pro zaměstnance, je předložený **návrh koncipován jako otevřený a částečně hypotetický**. Návrhy vychází z Přílohy 1 a celé jejich znění je vloženo v Příloze 2. Každý návrh začíná názvem okruhu, kterého se týká, a místo povinné osoby, která se uvádí v legislativních úpravách, je uvedena odpovědná osoba, která se ve finální verzi dá nahradit názvem pozice zaměstnance.

V návrhu uvedeném v Příloze 2 je **ke každému návrhu** znění směrnice **uvedený paragraf**, na který dané opatření navazuje. Tento přístup **umožňuje snadnou identifikaci příslušných změn** a jednotlivá opatření konkrétněji zasadit do existujících vnitřních směrnic UPCE. A zároveň ukázat, jak lze tyto právní požadavky převést do praxe. Návrhy jsou formulovány tak, aby sloužily jako pracovní základ pro úpravu nebo tvorbu nových pravidel. Ukázky z těchto návrhů lze vidět v Tabulka č. 13 (oblast vzdělání a školení), v Tabulka č. 14 (řízení fyzické bezpečnosti) a v Tabulka č. 15 (bezpečná komunikace).

Tabulka č. 13: Návrh opatření v rámci oblasti vzdělávání a školení

Název okruhu návrhu	Paragraf, na který návrh reaguje	Návrh
Vzdělávání a školení	§5 odst. (1) písm. a)	Vrcholné vedení se povinně a pravidelně účastní školení o bezpečnostní politice, řízení rizik a vypracování analýzy dopadů kybernetických incidentů. Odpovědná osoba stanoví plán rozvoje bezpečnostního povědomí s ohledem na stav a potřeby systému a zaměstnanců.
	§11 odst. (3) písm. a) a e)	Odpovědná osoba plánuje, realizuje a dokumentuje školení a jiné vzdělávací aktivity, včetně vstupního a průběžného testování zaměstnanců v oblasti kybernetické bezpečnosti. V případě porušení stanovených pravidel určí pravidla a postupy pro řešení.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 2*

Tabulka č. 14: Návrh opatření v rámci oblasti řízení fyzické bezpečnosti

Název okruhu návrhu	Paragraf, na který návrh reaguje	Návrh
Řízení fyzické bezpečnosti	§18 písm. c)	Odpovědná osoba v rámci fyzické bezpečnosti dokumentuje bezpečnostní perimetr, ve kterém jsou uchovávány nebo zpracovávány informace a data s ohledem na umístění technických aktiv a přidělení úrovně fyzické ochrany.
	§18 písm. d) bodu 4 a 5	Odpovědná osoba eviduje vstupy a přístupy do bezpečnostního perimetru a zajišťuje detekci jeho narušení.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 2*

Tabulka č. 15: Návrh opatření v rámci oblasti bezpečné komunikace

Název okruhu návrhu	Paragraf, na který návrh reaguje	Návrh
Bezpečná komunikace	§26	Odpovědná osoba zajišťuje bezpečnost technických aktiv a komunikace mezi nimi odolnými kryptografickými algoritmy a zohledňuje doporučení vydané na stránkách NÚKIB.
		Odpovědná osoba zajišťuje bezpečnou komunikaci v rámci organizace.
		Odpovědná osoba využívá pouze aktuálně odolné kryptografické klíče a certifikáty, umožní jejich kontrolu a audit a zajistí jejich důvěrnost a integritu.

Zdroj: Vlastní zpracování při porovnání [30][45] *vložené v Příloze 2*

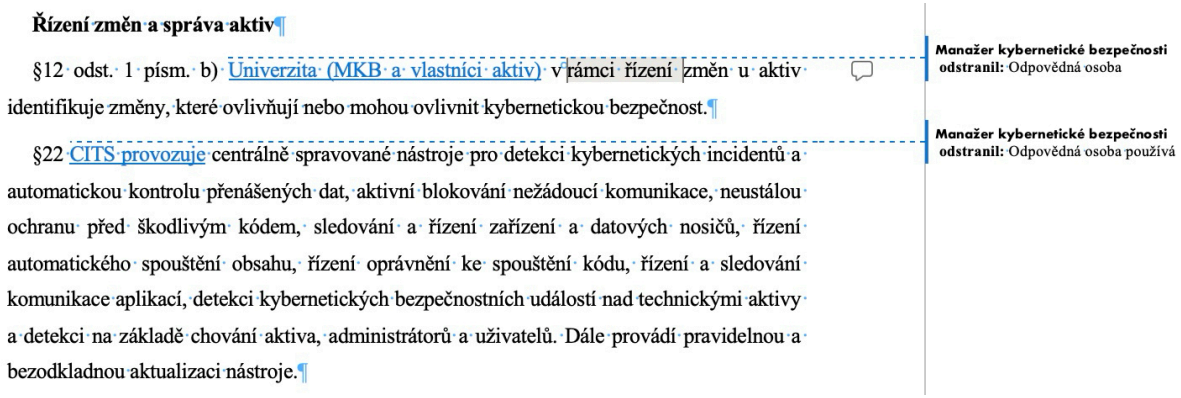
4.2. Návrh implementace bezpečnostních opatření

Tabulka nově zavedených bodů (v Příloze 1) a Návrh opatření pro zajištění souladu s právní úpravou (v Příloze 2) byly předány Manažerovi kybernetické bezpečnosti (MKB) Univerzity Pardubice. Jeho role je klíčová pro správné fungování systému řízení bezpečnosti informací a nese odpovědnost za jeho nastavení, udržování a rozvoj.

Zmíněné **porovnání sloužilo** MKB **jako podpůrný a orientační dokument**, který mu **umožnil** přesně **identifikovat a vyhodnotit rozdíly** mezi původní a navrhovanou legislativou. Na základě identifikovaných rozdílů obdržel také návrh úprav vnitřní směrnice UPCE, sestavený jako přehled doporučených změn s odkazy na konkrétní opatření právních předpisů.

V procesu přizpůsobení vnitřních předpisů aktualizoval MKB odpovědné osoby, které byly nahrazeny konkrétními rolemi (ukázáno na Obrázek č. 6). Tím byl zajištěn soulad vnitřní směrnice s legislativní terminologií používanou v nZoKB. Při té příležitosti upřesnil vybrané

formulace obsažené v poskytnutých návrzích tak, aby lépe odpovídaly reálnému prostření UPCE a legislativnímu kontextu.



Obrázek č. 6: Úpravy odpovědných osob pro implementaci návrhů do vnitřních směrnic

Zdroj: Vlastní zpracování podle přílohy 2 upravené MKB

Mezi další **návrhy implementace** je možné zařadit **osvětu a vzdělávání** nad rámec opatření. Mezi zásadní je možné zařadit **bezpečnostní školení pro všechny** nové zaměstnance a pravidelné školení stálých zaměstnanců. **Simulace phishingových emailů**, které budou nápomocné k vyhodnocení úrovně povědomí bezpečnosti a odhalení slabých míst v chování zaměstnanců. Zavést **tematické bezpečnostní měsíce** (například říjen je měsícem kybernetické bezpečnosti), kdy se mohou zapojit nejen zaměstnanci, ale i studenti do různých soutěží nebo kvízů. Tento způsob by zvyšoval povědomí o problematice nenásilnou formou.

Co v nZoKB bylo zmíněno, ale jeho implementace nebyla doslovně nařízena, je **Security Information and Event Management** (SIEM). Jedná se o **monitorovací software**, který slouží k analýze a detekci aktivit uživatelů, firemního software, aplikací nebo útočníků v rámci informačních systémů organizace. Tento systém bývá většinou nasazen přímo v počítačové síti organizace a pomáhá k odhalení hrozby, analýze a reakci dříve, než způsobí reálné škody v provozu firmy.

Posledním návrhem a doporučením je, aby byly **vnitřní normy**, bezpečnostní dokumentace a zavedené systémy **alespoň jednou ročně přezkoumány a podle potřeby aktualizovány**. Revize by měla zohledňovat nové legislativní požadavky, aktuální kybernetické hrozby, technologický vývoj a nasbírané praktické zkušenosti. **Cílem je zajistit, aby přijatá opatření odpovídala současným bezpečnostním požadavkům**, reflektovala nové hrozby a nadále plnila svou ochranu.

Z provedené analýzy a návrhu implementačních opatření vyplývá, že zavedení nového zákona o kybernetické bezpečnosti bude pro organizace představovat nejen administrativní zátěž, ale i potřebu komplexní změny v přístupu ke kybernetické bezpečnosti. Bude nutné zaměřit se na systematické řízení rizik, pravidelná školení zaměstnanců a efektivní interní komunikaci.

5. ZÁVĚR

Tato práce se zaměřila na ucelený rozbor problematiky kybernetické bezpečnosti, a to jak z pohledu její definice i významu, tak z pohledu vývoje příslušné legislativy na evropské i národní úrovni.

První část přinesla přiblížení pojmu kybernetická bezpečnost, její základní principy, nejčastější hrozby a útoky. Byla zakončena představením důležitých institucí zajišťujících bezpečnostní rámec v České republice.

Hlavní pozornost byla věnována srovnání stávajícího zákona o kybernetické bezpečnosti č. 181/2014 Sb. s návrhem nového zákona o kybernetické bezpečnosti, který vychází ze směrnice NIS2. Byla provedena komparace těchto dvou právních předpisů a vytvořena tabulka (Příloha 1), která obsahuje přehled nově zavedených opatření. Mezi hlavní zjištění patří rozšíření regulovaných subjektů, zavedení režimu nižších a vyšších povinností nebo zpřísnění požadavků na bezpečnostní opatření.

Ve další části byla aplikovaná teoretická zjištění na prostředí Univerzity Pardubice, která byla vybrána jako modelový subjekt, kterému bylo na základě rozboru navrženo několik konkrétních opatření a úprav interních směrnic (Příloha 2).

Součástí návrhů bylo také doporučení v oblasti školení, osvěty a technických nástrojů včetně využití systému SIEM (Security Information and Event Management), který, přestože není zákonem přímo vyžadován, představuje efektivní nástroj pro detekci a reakci na bezpečnostní incidenty.

Práce přináší hlubší porozumění legislativním změnám v oblasti kybernetické bezpečnosti a praktický návod k jejich zavedení do prostředí Univerzity Pardubice. Vytvořené tabulky a návrhy opatření mohou sloužit pro tvorbu či revizi interních směrnic a předpisů.

Zvýšením přehlednosti mezi stávajícím a novým zněním zákona přispívá práce k orientaci v nových povinnostech, zejména pro subjekty, které se připravují na implementaci směrnice NIS2. Významně také podporuje povědomí o důležitosti kybernetické bezpečnosti, a to nejen na úrovni řízení IT, ale napříč celou organizací. V neposlední řadě může sloužit jako podklad pro další výzkum a rozvoj v oblasti kybernetické legislativy a její praktické aplikace.

Výsledky práce ukazují, že implementace nového zákona o kybernetické bezpečnosti bude představovat významnou výzvu nejen z hlediska finančních nákladů, ale také z pohledu organizační změny a vzdělávání zaměstnanců. Úspěšné zvládnutí těchto požadavků bude vyžadovat strategické plánování, efektivní řízení rizik a trvalé zvyšování povědomí o

kybernetické bezpečnosti napříč organizací. Další vývoj v oblasti kybernetické bezpečnosti bude pravděpodobně zahrnovat přizpůsobování legislativy novým technologiím, zejména umělé inteligenci, a posilování spolupráce na mezinárodní úrovni.

POUŽITÁ LITERATURA

[1] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti [online]. Páté doplněné a upravené vydání*. Praha: Česká pobočka AFCEA, 2022 [cit. 2024-09-24]. ISBN 978-80-908388-4-0. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf

[3] ZEMAN, RNDr. Petr a kolektiv. *Česká bezpečnostní terminologie. Výklad základních pojmů*. Brno: Masarykova univerzita v Brně, 2002. [online]. [cit. 2025-03-24]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048

[4] VANĚK, Jiří. *Co je to CIA triáda a k čemu tento koncept slouží* [online]. 2023 [cit. 2024-11-28]. Dostupné z: https://blog.jirivanek.eu/cs/2023/07/23/co-je-to-cia-triada-a-k-cemu-tento-koncept-slouzi/

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

[6] FITZGERALD, Anna. *Cybersecurity Explained: What It Is & 13 Reasons Cybersecurity is Important* [online], 2024 [cit. 2025-03-15]. Dostupné z: https://secureframe.com/blog/why-is-cybersecurity-important

[7] NÚKIB, *Kybernetická bezpečnost v ČR* [online]. [cit. 2025-03-18]. Dostupné z: https://portal.nukib.gov.cz/informacni-servis/kyberneticka-bezpecnost-v-cr

[8] Bezpečnostní informační služba, *Naše poslání* [online]. [cit. 2025-03-22]. Dostupné z: https://www.bis.cz

[9] ČESKÁ REPUBLIKA, Zákon č. 154/1994 Sb. Zákon o bezpečnostní informační službě. [online. [cit. 2025-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/1994-154

[10] ŘEHKA, Ing. Karel. *Národní strategie kybernetické bezpečnosti České republiky*, [online]. 2020 [cit. 2025-03-22]. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[11] SCHÖN, KPT. David. *Od Nového roku začala fungovat Národní centrála proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování*, [online]. 2023, [cit. 2025-03-11]. Dostupné z: https://tydenikpolicie.cz/od-noveho-roku-zacala-fungovat-narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite-sluzby-kriminalni-policie-a-vysetrovani/

[12] NBÚ, *Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011* [online]. 2011, [cit. 2025-03-14]. Dostupné z: https://www.nbu.cz/cs/aktualne/867-994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/

[13] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o., 2019 [cit. 2024-09-25]. CZ.NIC. ISBN 978-80-88168-31-7. Dostupné z: https://www.nic.cz/files/edice/cybersecurity.pdf

[14] NÚKIB, *Vládní CERT*, [online]. [cit. 2025-02-28] Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[15] PAČKA, Roman. C*SIRT: v přední linii boje proti kybernetickým hrozbám*. Politologická řada. Brno: Centrum pro studium demokracie a kultury, 2019. [cit. 2025-16-03]. ISBN 978-80-7325-473-5.

[16] VLÁDA ČESKÉ REPUBLIKY, *Výbor pro kybernetickou bezpečnost*, [online] 2024, [cit. 2025-03-22] Dostupné z: https://vlada.gov.cz/cz/ppov/brs/pracovni-vybory/kyberneticka_bezpecnost/vybor-pro-kybernetickou-bezpecnost-212337/

[17] KOLOUCH, Jan. *CyberCrime*. CZ.NIC;. Praha: CZ.NIC, z.s.p.o., [online]. 2016. [cit. 2024-12-12]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/media/filer_public/4f/1e/4f1eeae6-b4e5-4553-8e74-5e0c6d014452/cybercrime.pdf

[18] Základní škola Jungmannova Kuřim. *Nebezpečí kyberprostoru* [online] 10 [cit.2024-09-29]. Dostupné z: https://www.zskj.cz/media/files/nebezpeci_kyberprostoru-2014.pdf

[19] NÚKIB. *Vláda schválila Zprávu o stavu kybernetické bezpečnosti ČR za rok 2023* [online]. 2024, 17.7.2024 [cit. 2024-10-31]. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2139-vlada-schvalila-zpravu-o-stavu-kyberneticke-bezpecnosti-cr-za-rok-2023/

[20] JERRY, Felix a Chris HAUCK. *System Security: A Hacker's Perspective*. In: INTEREX Conference Proceedings. 1987.

[21] ESET. *Slovník IT pojmů kybernetické bezpečnosti* [online]. [cit. 2024-10-31]. Dostupné z: https://www.eset.com/cz/slovnik/

[22] MUNI SCIRT – MU. *AI jako (ne)přítel v kybernetické bezpečnosti* [online]. [cit. 2024-10-31]. Dostupné z: https://security.muni.cz/clanky/ai-jako-nepritel-v-kyberneticke-bezpecnosti

[23] KINTR, Ing. Lukáš. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023* [online]. 2024, 52 [cit. 2025-02-21]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf

[24] Ministerstvo vnitra České republiky. *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření*, [online]. [cit. 2025-01-20]. Dostupné z: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://mv.gov.cz/soubor/koncepce-pdf.aspx&ved=2ahUKEwiytOWDvOSLAxX84AIHHSytAZ0QFnoECAgQAQ&usg=AOvVaw3JWeKBZetf-rZbX15Z9d-j

[25] Vláda České republiky. *Výsledky jednání vlády 15.března 2010*, [online]. 2010 [cit. 2025-03-22]. Dostupné z: https://vlada.gov.cz/cz/media-centrum/tiskove-zpravy/vysledky-jednani-vlady-15--brezna-2010-69537/#

[26] Cyber Security. *Kybernetická bezpečnost (Cyber Security)*. CyberSecurity [online]. 2017 [cit. 2024-10-07]. Dostupné z: https://www.cybersecurity.cz/basic.html

[27] ČESKÁ REPUBLIKA, Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) . In. Zákony pro lidi [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[28] ČESKÁ REPUBLIKA, Zákon č. 104/2017 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In. Zákony pro lidi [online] Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

[29] ČESKÁ REPUBLIKA, Zákon č. 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické

bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. In. Zákony pro lidi [online]. [cit. 2025-03-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[30] ČESKÁ REPUBLIKA. Zákon č. 82/2018 Sb., o kybernetické bezpečnosti. In: Zákony pro lidi [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[31] NÚKIB. *Vývoj zákona o kybernetické bezpečnosti*. [online]. [cit. 2025-03-21]. Dostupné z: Https://portal.nukib.gov.cz/informacni-servis/legislativa/vyvoj-zkb

[32] HROMADA, Martin, et al. *Kybernetická bezpečnost: teorie a praxe*. Powerprint, 2015. [online]. [cit. 2025-03-11]. Dostupné z: https://www.researchgate.net/profile/Petr-Hruza/publication/299489155_Cyber_Security_Theory_and_Practice/links/56fb969308ae3c0f264c9a84/Cyber-Security-Theory-and-Practice.pdf

[33] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[34] EVROPSKÁ KOMISE. *Přijímání právních předpisů EU*. In: European Commission [online]. [cit. 2025-03-11]. Dostupné z: https://commission.europa.eu/law/law-making-process/adopting-eu-law_cs

[35] EVROPSKÁ UNIE. *Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).* In: EUR-Lex [online]. [cit. 2025-03-11] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

[36] SystemOnline. *Nová legislativa EU o kyberbezpečnosti a ochraně dat*. Časopis IT Systems [online]. 2016, (1-2/2016) [cit. 2024-10-29]. Dostupné z: https://www.systemonline.cz/it-security/nova-legislativa-eu-o-kyberbezpecnosti-a-ochrane-dat.htm

[37] DURAČINSKÁ, Zuzana. *Co přináší nová směrnice EU o informační bezpečnosti?* Časopis IT Systems [online]. 2016, (10/2016) [cit. 2024-10-29]. Dostupné z: https://www.systemonline.cz/it-security/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm

[38] PETRŽELKA, Václav. *Kybernetická bezpečnost v EU a řízení bezpečnosti dle kybernetického zákona v ČR*. Časopis IT Systems [online]. 2016, (3/2016) [cit. 2024-10-

29]. Dostupné z: https://www.systemonline.cz/it-security/kyberneticka-bezpecnost-v-eu.htm

[39] EVROPSKÁ UNIE. *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive)* [online]. [cit. 2025-03-23]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[40] BLUE PARTNERS. *Co je směrnice NIS2?* [online]. 18.11.2024 [cit. 2025-02-03]. Dostupné z: https://www.bluepartners.cz/slovnik-it-pojmu/nis2

[41] NÚKIB. *Vzdělávací portál NÚKIB – NIS2 kurz* [online]. [cit. 2025-03-23]. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=168

[42] RASCASONE. *Co je směrnice NIS2 a jaké jsou její požadavky* [online]. [cit. 2025-03-23]. Dostupné z: https://www.rascasone.com/cs/blog/co-je-smernice-nis2-pozadavky

[43] NÚKIB. *Průvodce směrnicí NIS2* [online]. [cit. 2025-03-23]. Dostupné z: https://portal.nukib.gov.cz/pruvodce-smernici-nis2

[44] EY. *Co je NIS2 a zákon o kybernetické bezpečnosti* [online]. [cit. 2025-03-14]. Dostupné z: https://www.ey.com/cs_cz/services/cybersecurity/nis2

[45] ČESKÁ REPUBLIKA. *Návrh zákona o kybernetické bezpečnosti* [online]. 2023 [cit. 2025-03-23]. Dostupné z: https://odok.gov.cz/portal/services/download/attachment/ALBSD7F7MSH7/

[46] ÚJEZD.NET. *Co přinese nový zákon o kybernetické bezpečnosti?* [cit 2025-03-14]. Dostupné z: https://ujezd.net/co-prinese-novy-zakon-o-kyberneticke-bezpecnosti

[47] NÚKIB. *Významnost poskytovatele služby a počítání velikosti podniku* [online]. [cit. 2025-04-15]. Dostupné z: https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/6788d707e8e3c7573907a5d5

[48] NÚKIB. *Odůvodnění návrhu zákona o kybernetické bezpečnosti* [online]. [cit. 2025-03-23]. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2024/08/26/1b_Oduvodneni_Zakon-o-kyberneticke-bezpecnosti_uid_66cc4b982ff2d.pdf

[49] SVAZ PRŮMYSLU A DOPRAVY ČR. *Nový zákon o kybernetické bezpečnosti: proč je důležitý pro vaši firmu a na co se připravit* [online]. [cit. 2025-03-23]. Dostupné z:

https://www.spcr.cz/aktivity/z-hospodarske-politiky/16925-novy-zakon-o-kybernetickebezpecnosti-proc-je-dulezity-pro-vasi-firmu-a-na-co-se-pripravit

[50] DATARUN *Na koho dopadne zákon o kybernetické bezpečnosti?* [online]. [cit. 2025-04-25]. Dostupné z: https://www.datarun.cz/na-koho-dopadne-zakon-o-kybernetickebezpecnosti

[51] NÚKIB. *Finanční aspekty nového zákona o kybernetické bezpečnosti.* [online]. [cit. 2025-04-22] Dostupné z: https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/678a2ac3e8e3c7573907a644

[52] CYBRELA. *Nové sankce v kyberbezpečnosti. Za co hrozí vedení nejpřísnější postihy?* [online]. 2024 [cit. 2025-04-15]. Dostupné z: https://cybrela.com/nove-sankce-v-kyberbezpecnost-za-co-hrozi-pokuty/

[53] UNIVERZITA PARDUBICE. *Výroční zpráva o činnosti za rok 2023* [online]. Pardubice,2024 [cit. 2025-04-15]. Dostupné z: https://www.upce.cz/sites/default/files/global/2024-07/7552/Vyrocni%20zprava%20o%20cinnosti_2023_web_98367.pdf

SEZNAM PŘÍLOH

PŘÍLOHA 1

Organizační opatření				
Opatření, která jsou přidaná v nZoKB				
§	**Odstavec**	**Písmeno**	**Bod**	**Požadavek**
4	(1)	k	-	stanoví proces řízení výjimek z pravidel stanovených podle písm. d).
5	(1)	a)	-	se prokazatelně účastní školení podle § 11 odst. 3 písm. a),
5	(1)	h)	-	se podílí na vypracování analýzy dopadů podle § 16,
5	(2)	-	-	Vrcholné vedení se prokazatelně seznamuje se
5	(2)	a)	-	zprávou o přezkoumání systému řízení bezpečnosti informací,
5	(2)	b)	-	zprávou o hodnocení rizik,
5	(2)	c)	-	výsledky analýzy dopadů v souladu s § 16 a
5	(2)	d)	-	výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.
5	(4)	-	-	Jednání výboru pro řízení kybernetické bezpečnosti probíhají v pravidelném intervalu a o jejich průběhu je veden dokumentovaný záznam
7	(1)	-	-	Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace
7	(1)	a)	-	stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5 k této vyhlášce a
7	(1)	b)	-	v provozní dokumentaci stanoví pravidla a postupy, které zohledňují relevantní oblasti z bezpečnostní politiky a bezpečnostní dokumentace.
7	(2)	-	-	Povinná osoba dodržuje pravidla a postupy stanovené podle odstavce 1.
7	(3)	-	-	Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlednění jejich relevantních oblastí v provozní dokumentaci.
7	(4)	-	-	Povinná osoba určí osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky, bezpečnostní dokumentace a zohlednění jejich relevantních oblastí v provozní dokumentaci podle odstavce 3.
7	(5)	-	-	Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly
7	(5)	a)	-	dostupné v elektronické nebo listinné podobě,
7	(5)	b)	-	komunikovány v rámci povinné osoby,
7	(5)	c)	-	přiměřeně dostupné dotčeným stranám,
7	(5)	d)	-	chráněny z pohledu důvěrnosti, integrity a dostupnosti a
7	(5)	e)	-	vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné.
8	g)	vii)		pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidaci technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 3 k této vyhlášce.
9	(1)	h)	5.	výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
9	(1)	h)	6.	výsledky penetračního testování a skenování zranitelností.
11	(2)	d	-	pravidla tvorby bezpečných hesel v souladu s § 20,
11	(2)	e	-	relevantní témata uvedená v příloze č. 8 této vyhlášky.
11	(3)	a)	-	v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení vrcholného vedení o jeho povinnostech, o bezpečnostní politice zejména v oblasti systému řízení bezpečnosti informací a řízení rizik formou vstupních a pravidelných školení,
11	(3)	e)	-	určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu rozvoje bezpečnostního povědomí uvedeny
12	(1)	b)	-	stanoví pravidla, postupy a kritéria pro určení významných změn a
13	-	e)	-	dodržuje a vymáhá dodržování požadavků stanovených podle písmene c)
13	-	h)	-	je-li cílem provedení akvizice nebo vývoje technické aktivum užívající kryptografické algoritmy, plní požadavky podle § 26 odst. 1 písm. a) a odst. 3 písm. a).
16	(2)	-	-	Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § 34 zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod 2. tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.
17	(1)	-	-	Povinná osoba stanoví plán provádění auditu kybernetické bezpečnosti.
17	(3)	-	-	Povinná osoba zohlední výsledky auditu kybernetické bezpečnosti podle odstavce 2 v
17	(3)	a)	-	plánu zvládání rizik,
17	(3)	b)	-	prohlášení o aplikovatelnosti a
17	(3)	c)	-	plánu rozvoje bezpečnostního povědomí.
17	4)	-	-	Povinná osoba stanoví případná nápravná opatření pro splnění požadavků podle odstavce 2.
17	(5)	c)	-	v souladu s plánem auditu kybernetické bezpečnosti.

Celkem změn: 38

Technická opatření				
Opatření, která jsou přidaná v nZoKB				
§	**Odstavec**	**Písmeno**	**Bod**	**Požadavek**
18	-	c)	-	dokumentuje jednotlivé fyzické bezpečnostní perimetry podle písmena b) s ohledem na hodnocení umístěných technických aktiv a rozdělí je na jednotlivé úrovně fyzické ochrany,
18	-	d)	4.	pro zajištění detekce narušení fyzického bezpečnostního perimetru a
18	-	d)	5.	eviduje vstupy a přístupy do fyzického bezpečnostního perimetru
19	-	c)	-	zajistí řízení vzdáleného přístupu ke komunikační síti,
19	-	d)	-	zajistí řízení vzdálené správy technických aktiv
20	(6)	a)	3.	22 znaků pro účty technických aktiv,
20	(7)	-	-	Povinná osoba v souladu s odstavcem 6
20	(7)	a)	-	vytváří náhodné výchozí heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu a
20	(7)	b)	-	zajistí bezodkladnou změnu výchozího hesla technického aktiva,
20	(7)	c)	-	zajistí, aby uživatelé a administrátoři bezodkladně změnili svá výchozí hesla po prvním přihlášení,
20	(7)	d)	-	zajistí, že v rámci ověření identity technického aktiva bude jeho nové heslo vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků a
20	(7)	e)	-	bezodkladně vynutí změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci.
20	(8)	-	-	Povinná osoba bezodkladně zneplatní heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu po jeho prvním použití nebo uplynutí nejvýše 24 hodin od jeho vytvoření.
20	(9)	-	-	Povinná osoba u administrátorského účtu určeného zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, musí vynucovat následující pravidla
20	(9)	a)	-	bezodkladně vynutí změnu výchozí hesla,
20	(9)	b)	-	heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
20	(9)	c)	-	délka hesla musí být alespoň 22 znaků,
20	(9)	d)	-	heslo musí být bezpečně uloženo,
20	(9)	e)	-	s účtem a jeho heslem mohou manipulovat pouze pověřené osoby a to v nezbytně nutných případech,
20	(9)	f)	-	musí být vynucena změna hesla po jeho použití, při jakékoli změně odpovědných osob nebo v intervalu maximálně po 18 měsících a
20	(9)	g)	-	eviduje manipulaci a pokusy o manipulaci s tímto účtem a jeho heslem.
21	-	a)	-	využívá centralizovaný nástroj s ohledem na vazby mezi aktivy,
23	(2)	a)	-	detekované podle § 22,
22	(2)	-	-	Povinná osoba používá centrálně spravovaný nástroj s ohledem na vazby mezi aktivy pro detekci kybernetických bezpečnostních událostí, který u jednotlivých relevantních technických aktiv zajišťuje
22	(2)	a)	-	nepřetržitou a automatickou ochranu před škodlivým kódem,
22	(2)	b)	-	řízení a sledování používání vyměnitelných zařízení a datových nosičů,
22	(2)	c)	-	řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,
22	(2)	d)	-	řízení oprávnění ke spouštění kódu,
22	(2)	e)	-	řízení a sledování komunikace aplikací, jejich služeb a procesů,
22	(2)	f)	-	detekci kybernetických bezpečnostních událostí nad technickými aktivy a
22	(2)	g)	-	detekci na základě chování technického aktiva, administrátorů a uživatelů.
22	(3)	-	-	Povinná osoba provádí pravidelnou a bezodkladnou aktualizaci nástroje používaného podle odstavce 1 a 2, a to včetně jeho nastavení a detekčních pravidel.

23	(2)	b)	-	v rámci komunikační sítě,
23	(2)	c)	-	na síťovém perimetru a
23	(2)	d)	-	technických aktiv.
23	(3)	-	-	Povinná osoba aktualizuje rozsah technických aktiv určených podle odstavce 1 v pravidelných intervalech a při významných změnách
23	(5)	-	-	Povinná osoba v rámci zaznamenávání událostí podle odstavce 2 zaznamenává zejména následující informace o události
23	(8)	-	-	Povinná osoba v rámci zaznamenávání událostí podle odstavce 2, zejména zaznamenává
23	(9)	-	-	Povinná osoba používá centrální nástroj s ohledem na vazby mezi aktivy pro sběr a uchovávání záznamů událostí zaznamenaných podle odstavce 2
24	(2)	-	-	Povinná osoba v rámci používání nástroje v souladu s odstavcem 1 zajistí
25	(1)	-	-	Povinná osoba pro zajištění bezpečnosti regulované služby užívá technická aktiva, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí bezodkladné aplikování bezpečnostních aktualizací vydaných pro tato aktiva.
25	(2)	-	-	Povinná osoba do doby plnění odstavce 1 eviduje technická aktiva, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv.
25	(4)	-	-	Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby
25	(4)	a)	-	z interní a externí komunikační sítě a
25	(4)	b)	-	alespoň jednou ročně.
25	(5)	-	-	Povinná osoba zohlední výsledky skenů zranitelnosti v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků.
25	(7)	-	-	Povinná osoba zohlední výsledky penetračního testování v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků.
25	(8)	-	-	Povinná osoba provede opětovné otestování (retest) nálezu zjištěného na základě provedeného skenování zranitelnosti nebo penetračního testování za účelem ověření funkčnosti zavedených bezpečnostních opatření.
25	(9)	-	-	Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování a to alespoň jednou za dva roky.
25	(10)	-	-	Povinná osoba v odůvodněných případech, pokud nemůže provést penetrační testování v rozsahu nebo intervalu stanoveném v odstavci 9, může rozdělit toto penetrační testování do systematických celků. V takovém případě je nutno provést penetrační testování v rozsahu stanoveném v odstavci 6 nejpozději do 5 let.
26	(2)	-	-	Povinná osoba v souladu s odstavcem 1 zajišťuje bezpečnou
26	(2)	a)	-	hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace
26	(2)	b)	-	nouzovou komunikaci v rámci organizace.
26	(3)	-	-	Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá
27	(2)	-	-	Povinná osoba pro zajištění dostupnosti regulované služby v souladu s odstavcem 1 vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.
27	(3)	-	-	Povinná osoba u záloh vytvářených podle odstavce 2 zajistí
27	(3)	a)	-	pravidelné testování jejich integrity, dostupnosti a obnovitelnosti,
27	(3)	b)	-	dokumentování výsledků testů provedených podle odstavce 3 písm. a),
27	(3)	c)	-	ochranu ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, a to zejména šifrováním těchto záloh v souladu s § 26 a
27	(3)	d)	-	ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti.
27	(4)	-	-	Povinná osoba za účelem omezení šíření kybernetického bezpečnostního incidentu a snížení jeho dopadu odděluje zálohovací prostředí od jiných prostředí podle § 19 písm. a).
28	-	b)	-	omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům

PŘÍLOHA 2

Návrh opatření do UPCE směrnic		
Název okruhu návrhu	Paragraf, na který návrh reaguje	Návrh
Vzdělávání a školení	§5 odst. (1) písm. a)	Vrcholné vedení se povinně a pravidelně účastní školení o bezpečnostní politice, řízení rizik a vypracování analýzy dopadů kybernetických incidentů. Odpovědná osoba stanoví plán rozvoje bezpečnostního povědomí s ohledem na stav a potřeby systému a zaměstnanců.
	§11 odst. (3) písm. a) a e)	Odpovědná osoba plánuje, realizuje a dokumentuje školení a jiné vzdělávací aktivity, včetně vstupního a průběžného testování zaměstnanců v oblasti kybernetické bezpečnosti. V případě porušení stanovených pravidel určí pravidla a postupy pro řešení.
Audity a kontroly	§5 odst. (2)	Vrcholné vedení se prokazatelně seznamuje se zprávou o přezkoumání systému řízení bezpečnosti informací a o hodnocení rizik. Vedení se rovněž seznamuje s výsledky analýzy dopadů, auditů a kontrol v oblasti kybernetické bezpečnosti.
	§9 odst. (1) písm. h) body 5 a 6	Odpovědná osoba v rámci hodnocení a zvládání rizik zohlední výsledky auditů a kontrol v oblasti kybernetické bezpečnosti, penetračního testování a skenování zranitelností.
	§17 odst. (2) písm. a), (3) a (4)	Odpovědná osoba v rámci auditu kybernetické bezpečnosti posuzuje zavedenost bezpečnostních opatření požadována aktuálními zákony a vyhláškami.
Pravidla bezpečnostní dokumentace	§5 odst. (4)	Jednání výboru je uskutečňováno v pravidelném intervalu a je o něm veden záznam.
	§7	Odpovědná osoba stanoví bezpečnostní politiku a dokumentaci, provozní dokumentaci, kterou pravidelně přezkoumává, aktualizuje a chrání z hlediska důvěrnosti, integrity a dostupnosti.
Likvidace dat a technických aktiv	§8 odst. (1) písm. g) bodu 7	Odpovědná osoba určuje pravidla pro způsob likvidace informací, dat a technických aktiv podle jejich klasifikace.
Tvorba bezpečných hesel	§11 odst. 2 písm. d)	Stanovuje pravidla tvorby bezpečných hesel, pro které platí alespoň 12 znaků pro účty uživatele, 17 znaků pro účty administrátorů a 22 znaků pro účty technických aktiv.
	§20 odst. (7)	Výchozí heslo je náhodné a musí být do 24 hodin od prvního přihlášení změněno, poté se stává neplatným. Účty s privilegovaným přístupem podléhají navíc nutnosti změny každých 18 měsíců nebo při personálních změnách.
Řízení změn a správa aktiv	§12 odst. 1 písm. b)	Odpovědná osoba v rámci řízení změn u aktiv identifikuje změny, které ovlivňují nebo mohou ovlivnit kybernetickou bezpečnost.
	§22	Odpovědná osoba používá centrálně spravované nástroje pro detekci kybernetických incidentů a automatickou kontrolu přenášených dat, aktivní blokování nežádoucí komunikace, neustálou ochranu před škodlivým kódem, sledování a řízení zařízení a datových nosičů, řízení automatického spouštění obsahu, řízení oprávnění ke spouštění kódu, řízení a sledování komunikace aplikací, detekci kybernetických bezpečnostních událostí nad technickými aktivy a detekci na základě chování aktiva, administrátorů a uživatelů. Dále provádí pravidelnou a bezodkladnou aktualizaci nástroje.
Řízení fyzické bezpečnosti	§18 písm. c)	Odpovědná osoba v rámci fyzické bezpečnosti dokumentuje bezpečnostní perimetr, ve kterém jsou uchovávány nebo zpracovávány informace a data s ohledem na umístění technických aktiv a přidělení úrovně fyzické ochrany.
	§18 písm. d) bodu 4 a 5	Odpovědná osoba eviduje vstupy a přístupy do bezpečnostního perimetru a zajišťuje detekci jeho narušení.
Zranitelnosti a aktualizace technických aktiv	§25	Odpovědná osoba zajišťuje trvalou bezpečnost technických aktiv, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí schválené aktualizace vydané pro tato aktiva. V případě že bezpečnost technických aktiv nelze zajistit primárním způsobem, zavede bezpečnostní opatření, které zaručí stejnou nebo vyšší úroveň bezpečnosti těchto aktiv.
		Odpovědná osoba provádí minimálně jednou ročně skenování zranitelností technických aktiv v rámci komunikační sítě a zohlední výsledky při zavádění bezpečnostních opatření. Po zjištění nálezu zavede bezpečnostní opatření a provede opětovné otestování za účelem ověření funkčnosti.
		Odpovědná osoba provádí minimálně jednou za dva roky penetrační testování technických aktiv v komunikační síti, před uvedením do provozu nebo v souvislosti s významnou změnou. Po zjištění nálezu zavede bezpečnostní opatření a provede opětovné otestování za účelem ověření funkčnosti. Pokud nemůže provést testování ve stanoveném rozsahu může rozdělit testování do systematických celků a provést testování nejpozději do 5 let. Dále eviduje termín provedení a konkrétní osoby, které testování provádějí.
Bezpečná komunikace	§26	Odpovědná osoba zajišťuje bezpečnost technických aktiv a komunikace mezi nimi odolnými kryptografickými algoritmy a zohledňuje doporučení vydané na stránkách NÚKIB.
		Odpovědná osoba zajišťuje bezpečnou komunikaci v rámci organizace.
		Odpovědná osoba využívá pouze aktuálně odolné kryptografické klíče a certifikáty, umožní jejich kontrolu a audit a zajistí jejich důvěrnost a integritu.
Zálohování a obnova	§27 odst. (2), (3), (4)	Odpovědná osoba vytváří zálohy informací dat a konfigurací technických aktiv potřebných pro obnovu regulované služby v případě kybernetického bezpečnostního incidentu a chrání je před neoprávněným přístupem. Provádí pravidelné testování obnovy, integrity, dostupnosti záloh a dokumentuje výsledky testů.