**NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti**

**NIS2 and its causes on healthcare and other departments, new Cybersecurity law**

Projekt 4.

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D.

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2022/2023

**Z a d á n í P r o j e k t IV**

Student: **Šimon Kochánek**

Obor: Informatika a kybernetika ve zdravotnictví

Téma: **NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti**

Téma anglicky: **NIS2 and its causes on healthcare and other departments, new Cybersecurity law**

Z á s a d y p r o v y p r a c o v á n í :

Student představí NIS2 a také nový ZoKB. Poté zpracuje rešerši na změny řízení Kybernetické bezpečnosti ve zdravotních zařízeních, které budou podléhat novémeu zákonu. NIS2 začne platit od roku 2024 a výrazně zasáhne do oblast IT bezpečnosti.

Seznam odborné literatury:

1. <https://osveta.nukib.cz/course/view.php?id=145>
2. <https://www.isvs.cz/smernice-nis-2-koho-se-tyka-a-jak-ji-aplikovat-v-praxi/>
3. <https://www.epravo.cz/top/clanky/nis2-nova-regulace-kyberneticke-bezpecnosti-veu-115691.html>
4. <https://nis2.tech/>

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 12.3.2023

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedry

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 14.5.2023 …...….………...………………...

Jméno autora vč. titulů

**PODĚKOVÁNÍ**

Rád bych vyjádřil upřímné poděkování doktorce Brechlerové za její vedení mého semestrálního projektu. Cením si jejího přístupu, který mi umožnil pracovat na projektu s větší svobodou a bez přísných pravidel. Děkuji jí za vedení a motivaci, které mi pomohly rozvíjet své schopnosti a mé pracovní příležitosti v oblasti kyberbezpečnosti. Její přístup k mému zpracování byl otevřený a konstruktivní, a jsem jí za to velmi vděčný.

**ABSTRAKT**

NIS2 a dopady pro praxi zejména ve zdravotnictví, dopad na Zákon o kybernetické bezpečnosti

Tato semestrální práce se zaměřuje na detailní průzkum a analýzu nově implementovaných směrnic NIS2 a ZoKB, s důrazem na jejich dopad na řízení kybernetické bezpečnosti ve zdravotnických zařízeních. Nové směrnice představují zásadní změny v oblasti IT bezpečnosti, které budou mít významný dopad na zdravotnická zařízení. Směrnice NIS2, která začne platit od roku 2024, přináší řadu nových požadavků a standardů týkajících se kybernetické bezpečnosti. Souběžně s tím, práce zkoumá novou ZoKB, jež představuje další klíčový legislativní nástroj v tomto kontextu. Práce nabízí rešerši těchto změn a diskutuje jejich potenciální dopady na zdravotnická zařízení, která budou muset tyto nové požadavky splnit.

**Klíčová slova**

NIS2, ZoKB, Směrnice NIS2, nový ZoKB, NIS2 zdravotnictví

**ABSTRACT**

NIS2 and its causes on healthcare and other departments, new Cybersecurity law

This term paper focuses on detailed research and analysis of the newly implemented NIS2 and ZoKB guidelines, with an emphasis on their impact on cybersecurity management in healthcare facilities. The new directives represent major changes in IT security that will have a significant impact on healthcare facilities. The NIS2 Directive, which will come into force in 2024, introduces several new requirements and standards relating to cyber security. In parallel, the thesis examines the new ZoKB, which represents another key legislative instrument in this context. The thesis offers an exploration of these changes and discusses their potential impact on healthcare facilities that will have to comply with these new requirements.

**Keywords**

NIS2, ZoKB,Directive NIS2, new ZoKB, NIS2 healthcare

Obsah

[Seznam symbolů a zkratek 8](#_Toc137573284)

[1 Úvod 9](#_Toc137573285)

[1.1 Přehled současného stavu 10](#_Toc137573286)

[1.2 Cíle práce 10](#_Toc137573287)

[2 Metody 11](#_Toc137573288)

[2.1 Současný stav NIS1 a ZoKB 11](#_Toc137573289)

[2.1.1 NIS 1 11](#_Toc137573290)

[2.1.2 Zákon o Kybernetické Bezpečnosti č. 181/2014 12](#_Toc137573291)

[2.1.3 Vyhláška 82/2018 – Vyhláška o Kybernetické Bezpečnosti 13](#_Toc137573292)

[2.2 Důvod NIS2 14](#_Toc137573293)

[2.3 Nový zákon o kybernetické bezpečnosti 15](#_Toc137573294)

[3 Výsledky 18](#_Toc137573295)

[4 Diskuse 20](#_Toc137573296)

[5 Závěr 21](#_Toc137573297)

[Seznam použité literatury 22](#_Toc137573298)

[Příloha A: Požadavky na formátování práce 23](#_Toc137573299)

[Příloha B: Základní typografické zásady 24](#_Toc137573300)

[Příloha C: Další doporučení pro přehlednost textu 25](#_Toc137573301)

[Příloha D: Obsah přiloženého CD 26](#_Toc137573302)

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| NÚKIB | Národní Úřad pro Kybernetickou a Informační Bezpečnost |
| ZoKB  VoKB | Zákon o Kybernetické Bezpečnosti  Vyhláška o Kybernetické Bezpečnosti |

# Úvod

V digitálním věku, kdy společnosti stále více závisí na informačních a komunikačních technologiích, se otázka kybernetické bezpečnosti stala neoddělitelnou součástí našeho života. Direktiva o bezpečnosti sítí a informačních systémů (NIS1), která byla v roce 2016 přijata Evropskou unií, představovala první pokus o vytvoření soudržného rámcového práva pro zajištění kybernetické bezpečnosti v celé EU. Cílem bylo dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů v celé Unii, aby tak byla zajištěna její digitální rezistence.

Nicméně, jak se technologie rychle vyvíjejí a kybernetické hrozby se stávají sofistikovanějšími a diverzifikovanějšími, stává se jasné, že NIS1 již není schopna dostatečně řešit současné výzvy v oblasti kybernetické bezpečnosti. Důležité je zdůraznit, že od doby, kdy byla NIS1 implementována, došlo k dramatickým změnám v digitální krajině. Digitální technologie se staly integrální součástí našeho každodenního života a fungování ekonomiky, což znamená, že potenciální dopady kybernetických útoků jsou nyní mnohem větší než kdy dříve.

Vzhledem k těmto novým výzvám a příležitostem bylo nezbytné provést revizi NIS1. Cílem této revize bylo zajistit, že regulace EU v oblasti kybernetické bezpečnosti zůstane aktuální a efektivní vzhledem k rychlým změnám v digitální krajině.

Tato semestrální práce se proto zaměří na zkoumání NIS2, navrhované revize NIS1, s cílem zhodnotit její potenciál pro zlepšení kybernetické bezpečnosti v EU. Kromě toho se budu věnovat také analýze nového zákona o kybernetické bezpečnosti v České republice, který představuje náši národní odpověď na NIS2 a je klíčový pro integraci této evropské směrnice do našeho právního systému.

## Přehled současného stavu

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., v platném znění, představuje klíčový právní dokument pro řízení a zajišťování kybernetické bezpečnosti v České republice. Byl přijat s cílem ochránit kritickou infrastrukturu země a zajišťovat bezpečnost informačních systémů a sítí.

Tento zákon stanovuje rámec pro identifikaci a ochranu kritických informačních infrastruktur, stanovení bezpečnostních standardů a postupů a koordinaci mezi různými subjekty v oblasti kybernetické bezpečnosti. Zákon také zřizuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako hlavní regulační orgán v této oblasti.

Nicméně, i přes jeho význam, zákon čelí kritice za některé jeho aspekty. Někteří kritici poukazují na to, že zákon může být příliš obecný v některých svých ustanoveních, což může vést k nejednoznačnosti v jeho interpretaci a aplikaci. Dalšími oblastmi, které vyvolávají diskusi, jsou například otázky soukromí a ochrany osobních údajů v kontextu kybernetické bezpečnosti.

Je důležité poznamenat, že tento zákon byl přijat v roce 2014, a od té doby se digitální prostředí výrazně změnilo. Nové technologie, jako je cloud computing, Internet věcí (IoT) a umělá inteligence, přinášejí nové výzvy v oblasti kybernetické bezpečnosti, které tento zákon nemusí plně pokrýt. Proto je aktuální revize a aktualizace tohoto zákona klíčovou otázkou pro zajištění efektivní ochrany kybernetické bezpečnosti v České republice.

## Cíle práce

Prvním krokem je zjistit současný stav NIS1 a ZoKB. Je důležité porozumět, jak tyto systémy fungují nyní, aby bylo možné posoudit jakékoliv navrhované změny.

Následně je třeba se podrobně seznámit s NIS2. Je důležité pochopit důvody jejího zavedení a jaký význam má pro současný stav. To zahrnuje studium jak technických aspektů, tak i širšího kontextu.

Dalším krokem je procházet změny navrhované NÚKIBem a pochopit, jak se týkají nového ZoKB. To znamená nejen přečíst si navrhované změny, ale také se pokusit pochopit, jaké jsou jejich důsledky a jak mohou ovlivnit zavedení do praxe.

Nakonec nás čeká vyvození závěrů z předchozích cílů: Po prostudování a pochopení současného stavu NIS1 a ZoKB, pochopení důvodů pro zavedení NIS2 a jeho významu, a prozkoumání změn navrhovaných NÚKIBem týkajících se nového ZoKB, můžete vyvodit závěry. Tyto závěry by měly zohledňovat celkový dopad změn na kybernetickou bezpečnost, nové subjekty zodpovědné za řízení kybernetické bezpečnosti a jaké výzvy a příležitosti tyto změny přinášejí.

# Metody

## Současný stav NIS1 a ZoKB

Tři základní dokumenty pro Kybernetickou Bezpečnost v ČR:

- NIS1 – směrnice od EU 2016/1148

- ZoKB – Zákon o Kybernetické Bezpečnosti č.181/2014

- Vyhláška 82/2018 – Vyhláška o Kybernetické bezpečnosti

Pojďme si každý dokument představit:

### NIS 1

Směrnce o síťové a informační bezpečnosti (NIS), známá také jako NIS1, je první legislativní krok Evropské unie v oblasti kybernetické bezpečnosti. Byla přijata v červenci 2016 s cílem zvýšit celkovou úroveň kybernetické bezpečnosti v EU. NIS1 se zaměřuje na poskytování právních rámců pro zajištění bezpečnosti sítí a informací, zvláště u operátorů základních služeb (například v energetice, dopravě, bankovnictví a zdravotní péči) a poskytovatelů digitálních služeb (jako jsou online tržiště, cloudové služby a vyhledávače).

Směrnice stanovuje minimální bezpečnostní standardy a požadavky na oznámení incidentů pro tyto společnosti. Dále také požaduje, aby všechny členské státy EU zřídily nezávislý národní úřad pro kybernetickou bezpečnost, který by měl dostatečné zdroje na to, aby mohl reagovat na incidenty a monitorovat uplatňování těchto bezpečnostních opatření. Tento rámec také podporuje spolupráci mezi členskými státy EU v oblasti sdílení informací a nejlepších postupů.

### Zákon o Kybernetické Bezpečnosti č. 181/2014

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., který byl vyhlášen dne 29. srpna 2014 a nabyl účinnosti od 1. ledna 2015, je klíčovým předpisem České republiky, který se zabývá bezpečností kyberprostoru.

Tento zákon je úzce spojen s několika prováděcími předpisy, včetně Vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, Vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích a Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury1.

Základním cílem tohoto zákona je zvýšit bezpečnost kybernetického prostoru, zejména ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Tento zákon se však nesnaží řešit všechna rizika v kyberprostoru, jako je porušování autorských práv, různé podvodné aktivity, úniyk elektronických dat či šíření závadného elektronického obsahu.

Pro orgány a osoby, které určuje zákon, přibude řada nových povinností v oblasti zajištění bezpečnosti informačních a komunikačních systémů a komunikace s určenými kontaktními místy. Zákon také stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu.

Povinnosti plynoucí ze zákona se dotýkají jen vymezeného okruhu právnických osob, orgánů a podnikajících fyzických osob. To ale neznamená, že ostatních subjektů se potřeba chránit své informační a komunikační systémy před neustále narůstajícími kybernetickými hrozbami nijak netýká. Pro tyto subjekty může zákon a zejména vyhláška sloužit jako vhodná insprace nebo metodika.

Zákon také zavádí několik nových pojmů, včetně:

- "Kyberprostor" jako digitální prostředí umožňující zpracování informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.

- "Kritická informační infrastruktura" jako prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.

- "Významný informační systém" jako informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

### Vyhláška 82/2018 – Vyhláška o Kybernetické Bezpečnosti

Vyhláška č. 82/2018 Sb., známá také jako vyhláška o kybernetické bezpečnosti, byla vyhlášena dne 21. května 2018 a je účinná od 28. května 2018. Vyhláška je stanovena Národním úřadem pro kybernetickou a informační bezpečnost podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů [1].

Kybernetická bezpečnostní vyhláška je soubor pravidel a směrnic stanovených s cílem posílit ochranu proti hrozbám a útokům v kyberprostoru. Tato vyhláška určuje standardy a postupy pro ochranu systémů a dat, včetně implementace bezpečnostních protokolů, pravidelné aktualizace a údržby softwaru, školení zaměstnanců v oblasti kybernetické bezpečnosti a přijímání opatření pro řízení rizik. Navíc upravuje povinnosti a odpovědnosti organizací v oblasti hlášení a reakce na incidenty související s kybernetickou bezpečností.

## Důvod NIS2

- Rozšířená oblast působnosti:

NIS2 zahrnuje širší škálu odvětví než NIS1, včetně dalších průmyslových odvětví a poskytovatelů digitálních služeb.Mezi nová odvětví patří dodávky vody, potravin, digitální infrastruktura, online tržiště, vyhledávače a služby cloud computingu. Bude se pravděpodobně vztahovat na více než 6000 subjektů.

- Posílená opatření pro řízení bezpečnosti:

NIS2 zavádí další požadavky na řízení, včetně odpovědnosti vrcholového vedení za bezpečnostní standardy. (příslušné analýzy rizik, řešit bezpečnostní rizika v dodavatelském řetězci a procesy pro prevenci, odhalování, reakci a rychlé zotavení z bezpečnostních incidentů)

- Rozšířené povinnosti hlášení incidentů:

NIS2 upravuje kritéria pro to, co představuje "významný dopad", který je důvodem pro oznámení příslušným orgánům.Lhůta pro oznámení byla zkrácena ze 72 hodin na 24 hodin.NIS2 zavádí povinnost hlásit incidenty příjemcům služeb organizace a v nejzávažnějších případech i široké veřejnosti.

Zvýšení pokut a rozšíření sankcí:

NIS2 ukládá příslušným orgánům komplexnější soubor pravomocí, včetně stanovení maximální výše správních pokut na základě celosvětového obratu pro zásadní subjekty.

Nové možnosti vymáhání zahrnují právo orgánů provádět kontroly na místě, bezpečnostní audity, vyžadovat informace, nařizovat ukončení určitého jednání a nařizovat nápravu nevhodných opatření k řízení rizik.

## Nový zákon o kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti, který aktuálně čeká na schválení Parlamentem České republiky, je připravován v reakci na směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2. Tento zákon by měl nahradit stávající zákon o kybernetické bezpečnosti a jeho účinnost je plánována od druhé poloviny roku 2024[3].

Podle dostupných informací přináší směrnice NIS2 mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již nyní podle aktuálního zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely.

Nový přístup ZoKB rozděluje významné infrastruktury a kritické infrastruktury do dvou režimů: nižšího a vyššího, které se liší v několika klíčových aspektech[4]..

Nižší režim se vyznačuje sníženými požadavky a téměř beze změn oproti původnímu ZoKB. Oproti tomu vyšší režim zahrnuje povinnost hlásit všechny bezpečnostní incidenty s původem v kyberprostoru. Vyšší režim také zavádí pravidlo, že informace a data zpracovávaná v rámci stanoveného rozsahu musí být zpracována na vymezeném území.

Oba režimy vyžadují kontrolu, kterou v případě nižšího režimu provádí certifikovaní inspektoři nebo Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), zatímco v případě vyššího režimu kontrolu provádí přímo NÚKIB.

Zákon se dotýká různých sektorů, včetně elektrické energie, výrobního průmyslu, odpadového hospodářství, finančního trhu, vesmírného průmyslu, chemického průmyslu, vodní dopravy, vědy, výzkumu a vzdělávání, potravinářského průmyslu, letecké dopravy, zdravotnictví, veřejné správy, drážní dopravy, silniční dopravy, poštovních služeb, vodního hospodářství, digitální infrastruktury a služeb, vojenského průmyslu, ropného průmyslu, plynárenství, teplárenství a vodíkové energie.

Srovnání změn v bodech:

1. **Rozšířená působnost ZoKB**: Zákon nyní klade větší povinnosti na správce Významných a Kritických informačních systémů.
2. **Základní služby**: Služby závislé na komunikačních sítích nebo informačních systémech, jejichž narušení by mohlo mít významný dopad na klíčové společenské nebo ekonomické činnosti, jsou nyní zařazeny do působnosti ZKB. Tyto služby zahrnují odvětví jako Energetika, Doprava, Bankovnictví, Infrastruktura finančních trhů, Zdravotnictví, Dodávky a rozvody pitné vody, Digitální infrastruktura, Chemický průmysl a Veřejná správa.
3. **Digitální služby informační společnosti**: Nyní zahrnují internetové vyhledávače, cloud computing, a poskytování služby elektronického tržiště prostřednictvím internetové stránky.
4. **Zdravotnictví**: Nově je zařazena oblast zdravotnictví, která byla v současné verzi ZKB zařazena pouze u zdravotnických zařízení s kapacitou 2500 akutních lůžek.
5. **Digitální infrastruktura**: Novou oblastí je digitální infrastruktura internetových vyhledávačů, poskytovatelů eShopů a cloudových služeb (vyjma mikropodniků a malých podniků).
6. **Povinnost zabezpečení**: Všechny uvedené společnosti mají povinnost zajišťovat bezpečnost informačních systémů využívaných pro zajištění Digitální služby nebo Základní služby.
7. **Významné a kritické systémy**: Součástí změny vyhlášky jsou rovněž změny či významné doplnění požadavků kladených na stávající provozovatele významných a kritických informačních systémů.

### Časové rozmezí implementace zákona a jeho následků

Lhůta na transpozici NIS2 do českého práva a účinnosti ZoKB je do 17.10.2023.

Od této chvíle začíná 30 denní lhůta na provedení zápisů prvních poskytovatelů regulovaných služeb do evidence NÚKIB podle novely ZoKB. Poskytovatelé mají 30 dní na registraci v portálu NÚKIB.

Od ledna 2024 nám začíná probíhat jednoletá lhůta pro přípravu, po které musí nově určení provozovatelé regulované služby plnit povinnosti ze ZoKB.

Rok poté je náběh opatření u dalších určených subjektů a začátek vymáhání povinností od NÚKIB

# Výsledky

Po podrobném zkoumání NIS1, ZoKB a NIS2 jsem získal hluboké pochopení aktuálního stavu a budoucího směřování kybernetické bezpečnosti v Evropské unii. Pochopil jsem důvody pro zavedení NIS2, včetně jeho významu a účelu, a jak se tato nová regulace odráží v návrzích změn NÚKIBu pro nový ZoKB.

Tento dokument ve svých metodách uvádí jak jsem pochopil a zpracoval dostupné a uvedené dokumenty. Bohužel, jak jsem uváděl, ZoKB je stále nezavedený zákon, a může se stát, že se pozmění. Jak už také bylo řečeno bude nově platit pro více jak 6000 subjektů a tyto subjekty budou hledat to nejlevnější a nejjednodušší řešení.

Navíc jsem analyzoval nové subjekty zodpovědné za řízení kybernetické bezpečnosti a zhodnotil jejich roli a účinky změn, které přináší. Z těchto analýz jsem vyvodil závěry o celkovém dopadu těchto změn na kybernetickou bezpečnost, včetně výzev a příležitostí, které představují.

# Diskuse

V kontextu metod a výsledků mé práce jsem vytvořil tento dokument, aby byl základem pro pochopení nového zákona a jeho kontextu. Domnívám se, že nejlepším zdrojem informací je přímo NÚKIB. Někdo by mohl namítnout, že by bylo vhodnější provést tento projekt až v době, kdy ZoKB nabude plné planosti. Nicméně, považuji za nezbytné začít se již nyní připravovat na novou legislativu, vzhledem k tomu, že počet subjektů, na které se to vztahuje, stále roste. Tito subjekty často nemají dostatečné informace o relevantních legislativách a zákonech. Právě proto je důležité se na toto zaměřit již nyní a pomoci jim nejen vyhnout se pokutám za nesplnění povinností, ale také předejít kybernetickým incidentům.

# Závěr

Kybernetická bezpečnost prochází neskutečným rozmachem, který je daleko větší, než si kdokoli mohl představit. Tato práce mi poskytla nejen hluboký vhled do klíčových oblastí, ale také mi připravila cestu k porozumění nadcházejícím změnám v oblasti kybernetické bezpečnosti. Kromě toho tento dokument plánuji využít k vzdělávání ostatních, kteří se se mnou podílejí na šíření povědomí o kybernetické bezpečnosti.

# Seznam použité literatury

[1] s.r.o, Pixelfield, and Jana Blehová. “Co přináší zákon o kybernetické bezpečnosti.” T-SOFT, 13 Jan. 2015, https://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/.

[2] info@aion.cz, AION CS-. “82/2018 Sb. Vyhláška o kybernetické bezpečnosti.” Zákony pro lidi, https://www.zakonyprolidi.cz/cs/2018-82. Accessed 13 June 2023.

[3] Course: Nová Směrnice EU o Bezpečnosti Sítí a Informací. https://osveta.nukib.cz/course/view.php?id=145. Accessed 13 June 2023.

[4] info@aion.cz, AION CS-. “181/2014 Sb. Zákon o kybernetické bezpečnosti.” Zákony pro lidi, https://www.zakonyprolidi.cz/cs/2014-181. Accessed 13 June 2023