VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

Hodnocení připravenosti vybraných malých a středních podniků na plnění povinností dle zákona č. 264/2025 sb., o kybernetické bezpečnosti

Autor práce: Klára Mrázková, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Klára Mrázková, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Hodnocení připravenosti vybraných malých a středních podniků na plnění povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti

Název bakalářské práce v anglickém jazyce: Assessment of the readiness of selected small and medium-sized enterprises to fulfill their obligations under Act No. 264/2025 Coll., on cybersecurity

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): prosinec 2025

Cíl bakalářské práce: Cílem práce je vyhodnotit připravenost vybraných malých a středních podniků na plnění povinností stanovených zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění implementace směrnice NIS2, se zaměřením na proces registrace u NÚKIB a na určení režimu nižších či vyšších povinností.

Student: Klára Mrázková, DiS.	5. 12. 2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	11. 12. 25 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	17. 12. 2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11. 12. 2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20. 12. 2025 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MRÁZKOVÁ, K. *Hodnocení připravenosti vybraných malých a středních podniků na plnění povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 59 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetická bezpečnost, zákon o kybernetické bezpečnosti, NIS2, malé a střední podniky, Národní úřad pro kybernetickou a informační bezpečnost, regulovaná služba

Bakalářská práce se zabývá problematikou kybernetické bezpečnosti v souvislosti s novou právní úpravou vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, který implementuje směrnici NIS2 do českého právního řádu. V teoretické části jsou vysvětleny základní pojmy v oblasti kybernetické bezpečnosti a představeny vybrané evropské a mezinárodní nástroje upravující tuto problematiku, zejména směrnice NIS a NIS2, normy ISO/IEC řady 27000 a nařízení DORA. Následně je popsána právní úprava kybernetické bezpečnosti v České republice, včetně vybraných povinností subjektů, jako je posouzení poskytování regulované služby, určení režimu nižších či vyšších povinností a registrace u Národního úřadu pro kybernetickou a informační bezpečnost. Praktická část práce vychází z vlastního šetření provedeného formou strukturovaných rozhovorů s vybranými malými a středními podniky. Výsledky šetření poukazují zejména na úroveň informovanosti podniků o nové právní úpravě a jejich orientaci v legislativních požadavcích v oblasti kybernetické bezpečnosti.

ABSTRACT

MRÁZKOVÁ, K. *Assessment of the Readiness of Selected Small and Medium-Sized Enterprises to Fulfill their Obligations under Act No. 264/2025 Coll., on Cybersecurity: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2026. 59 s. pp. Supervisor: RNDr. Růžena Ferebauerová.

Key words: Cybersecurity, Cybersecurity Act, NIS2 Directive, Small and Medium-sized Enterprises, National Cyber and Information Security Agency, Regulated Service

The bachelor's thesis deals with the issue of cybersecurity in connection with the new legal framework arising from Act No. 264/2025 Coll., on Cybersecurity, which implements the NIS2 Directive into the Czech legal system. The theoretical part explains the basic concepts related to cybersecurity and introduces selected European and international instruments regulating this area, in particular the NIS and NIS2 directives, the ISO/IEC 27000 series standards and the DORA regulation. Subsequently, the legal regulation of cybersecurity in the Czech Republic is described, including selected obligations of entities, such as the assessment of providing a regulated service, determination of the regime of lower or higher obligations, and registration with the National Cyber and Information Security Agency. The practical part of the thesis is based on the author's own research conducted through structured interviews with selected small and medium-sized enterprises. The results of the research mainly indicate the level of awareness of enterprises about the new legal framework and their orientation in legislative requirements in the field of cybersecurity.

Obsah

Úvod

Kybernetická bezpečnost představuje v současné době jednu z nejvýznamnějších oblastí ochrany informačních systémů a digitální infrastruktury. Dnešní společnost je stále více závislá a informačních a komunikačních technologiích, které se staly nedílnou součástí každodenního fungování veřejné správy, podnikatelského sektoru ale i života jednotlivců. S rostoucí digitalizací samozřejmě narůstá i množství kybernetických hrozeb, které mohou mít podobu neoprávněného přístupu k datům, narušení dostupnosti informačních systémů nebo zneužití citlivých údajů. Kybernetické incidenty mohou způsobit ekonomické škody, narušit fungování organizací a v krajních případech ohrozit i bezpečnost státu. Z těchto důvodů se problematika kybernetické bezpečnosti stává stále významnějším tématem nejen v oblasti informační technologie, ale také v oblasti práva a veřejné správy.

Na rostoucí význam této problematiky reaguje také legislativa. A to především na úrovni Evropské unie, která postupně vytváří jednotný rámec a tím zajišťuje vysokou úroveň kybernetické bezpečnosti ve všech členských státech. Jedním z klíčových nástrojů v této oblasti je směrnice Evropského parlamentu a Rady Evropské unie (2022/255), známá jako směrnice NIS2. Tato směrnice navazuje na původní směrnici NIS a jejím cílem je posílit úroveň kybernetické bezpečnosti v rámci Evropské unie, zajistit jednotnou a vysokou úroveň ochrany ve všech členských státech a současně také zvýšit odolnost organizací vůči kybernetickým hrozbám. Povinnosti v oblasti kybernetické bezpečnosti se tak mohou nově týkat řady malých a středních podniků, které doposud nebyly v této oblasti regulovány v takovém rozsahu.

V České republice je směrnice NIS2 implementována prostřednictvím zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Tento zákon přestavuje nový legislativní rámec pro zajištění kybernetické bezpečnosti a stanovuje povinnosti pro organizace, které spadají do regulovaného režimu. Mezi nové povinnosti patří například určení režimu povinností nebo zavedení odpovídajících bezpečnostních opatření zaměřených na ochranu informačních a komunikačních systémů.

Problematika připravenosti podniků na plnění povinností v této oblasti proto představuje významné téma jak z hlediska právní regulace, tak z hlediska praktického fungování nejen podnikatelského prostředí. Zkoumání této problematiky může přispět

k lepšímu pochopení současného stavu implementace požadavků kybernetické bezpečnosti v praxi a zároveň poukázat na oblasti, ve kterých mohou organizace při naplňování nových legislativních požadavků čelit největším obtížím.

1 Cíl a metodika bakalářské práce

V první kapitole bakalářské práce, která má název Hodnocení připravenosti vybraných malých a středních podniků na plnění povinností dle zákona č. 264/2025 sb., o kybernetické bezpečnosti je vymezen cíl bakalářce práce a zvolená metodika zpracování. Hlavním cílem práce je vyhodnotit připravenost vybraných malých a středních podniků na plnění povinností stanovených zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění implementace směrnice NIS2, se zaměřením na proces registrace u NÚKIB a na určení režimu nižších či vyšších povinností.

V teoretické části bude za pomoci rešerše dostupné odborné literatury a právních předpisů vztahujících se k této problematice nejprve vymezena problematika kybernetické bezpečnosti a základní pojmy vztahující se k této oblasti. Dále bude pozornost věnována vybraným evropským a mezinárodním nástrojům, které upravují oblast kybernetické bezpečnosti. V této souvislosti budou představeny zejména směrnice NIS a NIS2, mezinárodní bezpečnostní normy řady ISO/IEC 27000 a nařízení DORA. V další kapitole teoretické části bude popsán zákon č. 264/2025 Sb., o kybernetické bezpečnosti a související prováděcí vyhlášky. V návaznosti na tuto právní úpravu budou představeny klíčové povinnosti subjektů vyplývající z tohoto zákona. Pozornost bude věnována především procesu registrace u Národního úřadu pro kybernetickou a informační bezpečnost, určení režimu vyšších nebo nižších povinností a základním bezpečnostním opatřením, která jsou s jednotlivými režimy spojena.

Praktická část bakalářské práce bude zaměřena na zjištění připravenosti vybraných malých a středních podniků na plnění povinností vyplývajících z nové právní úpravy. K dosažení cíle práce bude využita metoda strukturovaných rozhovorů. Rozhovory budou realizovány s podniky, které jsou klienty advokátní kanceláře a které působí v různých odvětvích podnikatelské činnosti. Celkem bude osloveno 25 podniků, které spadají do kategorie malých a středních podniků.

Získaná data budou následně zpracována a prezentována pomocí grafického znázornění pro lepší přehlednost. Součástí vyhodnocení bude také slovní interpretace získaných výsledků, která umožní lépe vysvětlit zjištěné skutečnosti a poukázat na oblasti, ve kterých mohou podniky při implementaci požadavků kybernetické bezpečnosti čelit největším obtížím.

Při zpracování budou rovněž využity profesní a praktické zkušenosti autorky práce získané při působení v advokátní kanceláři, která se ve své praxi zaměřuje především na poskytování právních služeb malým a středním podnikům. Tyto zkušenosti umožní lépe identifikovat praktické problémy, se kterými se podniky při plnění povinností v oblasti kybernetické bezpečnosti mohou setkávat.

2 Základní pojmy a definice v oblasti kybernetické bezpečnosti

Na začátku této práce autorka práce blíže vymezí pojmy, které se budou prolínat následujícími kapitolami. Vymezení pojmů v problematice kybernetické bezpečnosti je zcela zásadní. Jelikož pojmy jsou si na první pohled velmi podobné, avšak významově úplně odlišné. Vymezení těchto pojmů hned na začátku práce usnadní orientaci v dané problematice a přispěje k lepší přehlednosti celé bakalářské práce. Kapitola se proto zaměří na sjednocení pojmů, které plynou i z nové legislativy a pokud by nebyly dostatečně objasněny, tak by mohlo dojít k nepochopení tématu nebo k záměně pojmů. Terminologie používaná v oblasti kybernetické bezpečnosti vychází z několika různých zdrojů. Vedle právních předpisů se opírá také o technické standardy, odbornou literaturu a terminologii používanou v oblasti informačních technologií. Právě tato různorodost zdrojů může vést k tomu, že některé pojmy jsou v praxi používány nepřesně nebo jsou zaměňovány s jinými termíny. Současně je potřeba zdůraznit, že oblast kybernetické bezpečnosti se velmi rychle vyvíjí a tomu odpovídá i vývoj terminologie. Následující kapitoly se proto zaměří na vymezení vybraných pojmů, které mají pro tuto práci zásadní význam.

2.1 Kybernetická bezpečnost

V poslední době je mnohem více skloňován pojem kybernetická bezpečnost, a to hlavně díky novému zákonu o kybernetické bezpečnost, ale tomu se autorka práce bude věnovat v pozdější samostatné kapitole. Kybernetická bezpečnost bývá definována jako soubor nástrojů, politik, bezpečnostních konceptů, pokynů a přístupů k řízení rizik. Výkladový slovník kybernetické bezpečnosti tento pojem definuje takto: „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*.“[1] V širším kontextu je kybernetická bezpečnost chápána jako ochrana kybernetického prostoru, tedy virtuálního prostředí tvořeného informačními a komunikačními technologiemi. Kybernetický prostor je známý svou globální povahou bez fyzických hranic a vysokou provázaností jednotlivých systémů, což vytváří specifické bezpečnostní výzvy odlišné od klasického pojetí bezpečnosti. Z právního hlediska je kybernetická bezpečnost v České republice upravena zákonem

[1] JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. S. 97. ISBN 978-80-908388-4-0.

č. 264/2025 Sb., o kybernetické bezpečnosti, který implementuje směrnici NIS2. Primárním cílem kybernetické bezpečnosti je zajištění ochrany informací, informačních systémů a sítí před hrozbami pocházejícími z kybernetického prostoru.[2, 3]

2.2 Kybernetický incident

Kybernetický incident představuje neočekávanou událost, jejíž dopady mohou mít dopad na fungování informačních a komunikačních systémů, případně mohou ohrozit data, která jsou těmito systémy provozována. Mezi typické projevy kybernetického incidentu patří neoprávněný přístup k citlivým informacím, útoky typu odepření služby, šíření škodlivého softwaru nebo manipulace s daty. Pokud kybernetický incident zasáhne kritickou infrastrukturu může to ohrozit fungování celého státu. Na takovýto typ incidentu je potřeba součinnost různých týmů bezpečnostních expertů a vynaložení nemalých prostředků. Kybernetický incident se nemusí týkat pouze celého státu, může se týkat i jednotlivých institucí nebo jejich částí nebo i jednotlivců. Samozřejmě pro útočníka je větší výzva a adrenalin pokud zaútočí na celou organizaci nebo stát. Nejhorší jsou ty typy incidentů, které díky ochromení systémů ohrožují lidské životy, a to může být např. útok na nemocnici nebo na železniční a dopravní signály. Důsledky incidentů jsou nejen narušení fungování organizace, ale také to mohou být finanční ztráty, poškození reputace a úniky citlivých dat.[4, 5]

2.3 Kybernetický útok

Kybernetický útok představuje záměrné a cílené jednání, s cílem narušit, poškodit, získat neoprávněný přístup nebo jinak negativně ovlivnit informační a komunikační systémy, sítě a data. Na rozdíl od obecnějšího pojmu kybernetický incident, který zahrnuje jakoukoliv nežádoucí událost ohrožující bezpečnost informací, je kybernetický útok charakterizován jako úmyslné jednání útočníka, který sleduje konkrétní cíl. Cílem pro útočníka může být finanční zisk, špionáž, sabotáž nebo jinak ideologicky motivovaná akce. Mezi typické formy kybernetických útoků patří tzv. phishing, který představuje falešnou komunikaci, díky které získá citlivé údaje. Dále útoky typu ransomware,

[2] POLČÁK, R.; HARAŠTA, J. a STUPKA, V. *Právní problémy kybernetické bezpečnosti*. Spisy Právnické fakulty Masarykovy univerzity. Řada teoretická. Scientia. Brno: Masarykova univerzita, 2016. S. 18-26. ISBN 978-80-210-8426-1.
[3] ŠULC, V. *Kybernetická bezpečnost*. 2018. S. 9-11. ISBN 978-80-7380-737-5.
[4] NONNEMANN, F.; ČERVENÝ, V. a VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025. S. 9. ISBN 978-80-286-0331-1.
[5] SEDLÁK, P. a KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. S. 89-90. ISBN 978-80-7623-068-2.

při nichž dochází k zašifrování dat a následnému požadavku výkupného. Za specifikou formu kybernetického útoku lze považovat DDoS útoky (Distrubuted Denial of Service), které spočívají v masivním zahlcení cílového systému požadavky, a tím dochází k omezení nebo znemožnění jeho dostupnosti. Kybernetické útoky mohou být realizovány jednotlivci nebo organizovanými skupinami. Každý kybernetický útok, pokud je úspěšný se stává kybernetickým incidentem, avšak ne každý incident je důsledkem útoku.[6]

2.4 Rizika, hrozba a aktiva v kybernetickém prostoru

Pojmy riziko a hrozba jsou velmi úzce propojené, jelikož riziko vychází z existence hrozby. Samotná hrozba však neznamená vysoké riziko, neboť jeho míra se odvíjí od pravděpodobnosti realizace hrozby a rozsahu možných dopadů. Riziko v kybernetickém prostoru lze chápat jako kombinaci pravděpodobnost vzniku nežádoucí události a rozsahu možných dopadů na chráněná aktiva organizace. Riziko přitom nemůže existovat bez hrozby, jelikož bez potenciální nežádoucí události nelze stanovit ani pravděpodobnost jejího vzniku, ani posoudit možné následky. Hrozba je tak nezbytným předpokladem vzniku rizika. [7]

Pojem hrozba je Výkladovým slovníkem kybernetické bezpečnosti definována jako: „*Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“*[8] Mezi hrozby v kybernetickém prostoru lze zařadit úmyslné hrozby, kam patří kybernetické útoky, a to např. viry, trojské koně, phishing nebo již zmíněné DDoS útoky. A dále také neúmyslné hrozby mezi které patří chyby zaměstnanců, nesprávná konfigurace systémů anebo používání slabých hesel. [9]

Mezi aktiva se řadí cokoliv, co má nějakou hodnotu pro osobu, organizaci nebo stát a co je třeba chránit. Aktivum může mít různé podoby, může to být hmotná věc, a to třeba budova nebo zboží, a nehmotná věc například informace a data. Mezi aktiva může patřit i vlastnost nebo dobré jméno a reputace. Z hlediska typologie lze aktiva dělit do několika kategorií. V primárních aktivách jsou ty nejdůležitější věci, kvůli kterým

[6] JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. S. 59. ISBN 978-80-7251-397-0.
[7] KOLOUCH, J. a BAŠTA, P. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. S. 68. ISBN 978-80-88168-34-8.
[8] JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. S. 20. ISBN 978-80-7251-397-0.
[9] KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. S. 181. ISBN 978-80-88168-15-7.

organizace vůbec existuje. Zahrnuté jsou zde informace, data, která daná organizace zpracovává, jako jsou např. osobní údaje zákazníků, finanční záznamy nebo dokumentace, která je organizaci poskytnuta. Tato kategorie představuje právě to, co daná organizace chrání, neboť právě tyto informace jsou ty nejcennější. Podpůrná aktiva jsou ta, prostřednictvím kterých je zajišťováno fungování primárních aktiv, patří sem např. zaměstnanci, dodavatelé, technika nebo budovy. A do technických aktiv se řadí technické nebo programové prostředky, jako jsou např. servery, síťová zařízení nebo počítače.[10, 11]

3 Směrnice NIS, NIS2, ISO/IEC 27000 a nařízení DORA

Právní a normativní rámec kybernetické bezpečnosti tvoří na evropské i mezinárodní úrovni soubor vzájemně provázaných nástrojů, jejichž společným cílem je snaha o systematické řízení kybernetických rizik a zajištění odolnosti klíčových struktur. Pochopení těchto nástrojů je nezbytným předpokladem pro analýzu povinností, které z nich vyplývají pro malé a střední podniky na území České republiky. Na úrovni Evropské unie představovala směrnice NIS z roku 2016 první komplexní legislativní rámec. Její nedostatky v oblasti rozsahu působnosti a vymahatelnosti vedly k přijetí revidované směrnice NIS2. Ta výrazně rozšiřuje okruh regulovaných subjektů a zpřísňuje požadavky na řízení kybernetických rizik, hlášení incidentů a bezpečnostní opatření. Odlišnou funkci plní skupina norem ISO/IEC 27000. Jde o soubor dobrovolných mezinárodních standardů poskytujících metodický návod k budování a provozování systémů řízení bezpečnostních informací. V praxi slouží jako referenční rámec pro prokazování shody s legislativními požadavky. Specifické požadavky pro finanční sektor pak zavádí nařízení DORA, které harmonizuje přístup k řízení rizik informačních a komunikačních technologií napříč Evropskou unií.

3.1 Směrnice NIS

Směrnice NIS (Network Information Security) neboli zabezpečení sítí a informací, tvoří první komplexní legislativní nástroj přijatý na úrovni Evropské unie, s cílem zajištění jednotné a vysoké úrovně bezpečnosti sítí a informačních systémů ve všech členských státech. Vzhledem k tomu, že se jedná o legislativní nástroj vydaný

[10] KOLOUCH, J. a BAŠTA, P. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. S. 72. ISBN 978-80-88168-34-8.
[11] HRŮZA, P. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. S. 36-37. ISBN 978-80-7231-914-5.

ve formě směrnice, znamená to pro členské státy Evropské unie, že jim je stanoven cíl, kterého musí dosáhnout, avšak je ponechána určitá volnost v tom, jakým způsobem a jakými prostředky tento cíl naplní při jeho promítnutí do vnitrostátního právního řádu. Před přijetím této směrnice se národní přístupy k problematice kybernetické bezpečnosti výrazně odlišovaly, a to jak po formální stránce, tak v praktické rovině. Legislativní rámec pro oblast kybernetické bezpečnosti existoval pouze v omezeném počtu zemí a ne všechny členské státy disponovaly bezpečnostními týmy. „*Účelem směrnice je stanovit základní požadavky, které musí splňovat všechny členské státy EU*.“[12] Povinnosti vyplývající ze směrnice NIS lze rozdělit do dvou základních kategorií. Do první kategorie spadá organizační a legislativní povaha věci, která se vztahuje na členské státy jako takové. Do druhé kategorie patří povinnosti vztahující se na konkrétní kategorie subjektů definovaných směrnicí. Směrnice byla publikována v Úředním věstníku Evropské unie a vstoupila v platnost v srpnu 2016. Proto následně Česká republika do svého právního řádu implementovala směrnici NIS v rámci novelizace zákona č. 205/2017 Sb., o kybernetické bezpečností s účinností od 1. srpna 2017. Každý členský stát Evropské unie musel společně s implementací této směrnice zřídit nebo zvolit centrální orgán odpovědný za kybernetickou bezpečnost. Proto Česká republika společně s touto novelou zřídila Národní úřad pro kybernetickou bezpečnost (NÚKIB), který po Národním bezpečnostním úřadu (NBÚ) převzal práva a povinnosti v oblasti kybernetické bezpečnosti, a to včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů. Společně s touto novelizací byla také přijata Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 a její Akční plán. Mezi další povinnosti, které ukládala směrnice NIS patřila povinnost zřídit CSIRT tým. Tyto týmy poskytují podporu pro řešení kybernetických bezpečnostních incidentů. Působnost směrnice NIS vymezuje dvě základní kategorie regulovaných subjektů. Do první kategorie patří provozovatelé základních služeb, kteří působí v odvětvích zásadních pro fungování společnosti a ekonomiky. Mezi tato odvětví patří např. energetika, doprava, bankovnictví anebo zdravotnictví. Druhou kategorii představují poskytovatelé digitálních služeb, kam spadají provozovatelé online tržišť, internetových vyhledávačů a služeb cloud computingu.[13] [14]

[12] UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Směrnice NIS2*. Online. Dostupné z: https://www.utb.cz/kyberneticka-bezpecnost/nis/.. [cit. 2026-01-17].
[13] KOLOUCH, J. a BAŠTA, P. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. S. 94-98. ISBN 978-80-88168-34-8.
[14] RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Právní instituty. V Praze: C.H. Beck, 2023. S. 131-133. ISBN 978-80-7400-931-0.

3.2 Směrnice NIS2

NIS2 je nová směrnice Evropské unie, která nahrazuje směrnici NIS z roku 2016. Cílem této nové směrnice je podle portálu NÚKIB „*posílit kybernetickou bezpečnost organizací poskytujících klíčové služby pro společnost.“*[15] Směrnice NIS 2 přináší rozšířený soubor povinností zahrnujících ochranu informačních systémů, oznamování kybernetických bezpečnostních incidentů a systematické řízení rizik. Její působnost se vztahuje na podstatně širší okruh odvětví než původní směrnice NIS a současně klade důraz na posílení přeshraniční spolupráce mezi členskými státy Evropské unie. Směrnice byla schválena již v roce 2023 a implementace v České republice proběhla přijetím nového zákona o kybernetické bezpečnosti, který je účinný od 1. listopadu 2025. Povinnosti regulovaných subjektů nevychází přímo ze směrnice, nýbrž z vnitrostátní právní úpravy, která směrnici implementuje. Zákon také zavádí dva režimy regulací, nižší a vyšší podle odvětví a velikosti podniků. Vzhledem k tomu, že směrnice byla do českého právního řádu implementována prostřednictvím nového zákona o kybernetické bezpečnosti, bude podrobnější analýza konkrétních povinností regulovaných subjektů, procesu registrace u NÚKIB a rozlišení režimů vyšších a nižších povinností předmětem samostatné kapitoly věnované tomuto zákonu. V následující části práce tak bude pozornost zaměřena na vnitrostátní právní úpravu, která představuje bezprostřední právní základ pro povinnosti malých a středních podniků v oblasti kybernetické bezpečnosti.[16]

3.3 ISO/IEC 27000

Provázanost směrnice NIS2 s mezinárodními standardy pro řízení bezpečnosti informací je zásadní pro efektivní implementaci požadavků na kybernetickou bezpečnost. V tomto kontextu hrají klíčovou roli normy řady ISO/IEC 27000, které představují soubor mezinárodních standardů zaměřených na systémy řízení bezpečnosti informací (ISMS – Information Security Management Systems). Norma ISO/IEC 27000 vymezuje základní přehled a slovník pojmů pro celou řadu standardů systému řízení bezpečnosti informací, zatímco norma ISO/IEC 27001 specifikuje požadavky na zavedení, implementaci, udržování a neustálé zlepšování systému řízení bezpečnosti informací v organizaci. Význam normy ISO/IEC 27001 spočívá v jejím systémovém přístupu k řízení informační

[15] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce směrnicí NIS2*. Online. Dostupné z: https://portal.nukib.gov.cz/pruvodce-smernici-nis2. [cit. 2026-01-19].
[16] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce novým zákonem o kybernetické bezpečnosti*. Online. Dostupné z: https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti. [cit. 2026-01-19].

bezpečnosti. Organizace, která implementuje ISMS podle normy ISO/IEC 27001, systematicky identifikuje a hodnotí rizika pro svá aktiva a následně navrhuje a implementuje vhodná bezpečnostní opatření. Tento přístup, zahrnující řízení rizik, zvládání incidentů a bezpečnost dodavatelského řetězce, přímo koresponduje s mnoha požadavky směrnice NIS2. Přestože směrnice NIS2 explicitně nenařizuje certifikaci ISO/IEC 27001, implementace tohoto standardu může organizacím výrazně usnadnit prokazování souladu s legislativními nároky a vést k efektivnějšímu naplňování povinností vyplývajících z nové právní úpravy v oblasti kybernetické bezpečnosti.[17, 18]

Norma ISO/IEC 27001 je strukturována do několika hlavních částí, které definují požadavky na fungování systému řízení bezpečnosti informací v organizaci. Tyto požadavky se týkají zejména stanovení kontextu organizace, role vedení, plánování bezpečnostních opatření, podpůrných procesů apod. Struktura normy je přitom navržena tak, aby byla kompatibilní i s dalšími standardy systémů řízení, např. s normou ISO 9001. Díky tomu mohou organizace jednotlivé systémy řízení vzájemně propojit a vytvářet integrovaný systém řízení. Významným prvkem normy ISO/IEC27001 je proces certifikace, který umožňuje nezávislé ověření funkčnosti systému řízení bezpečnosti informací. Certifikaci provádějí akreditované certifikační orgány, které prostřednictvím auditů posuzují, zda organizace splňuje požadavky normy. Úspěšné získání certifikátu následně potvrzuje, že organizace zavedla a udržuje systém řízení bezpečnosti informací v souladu s mezinárodně uznávaným standardem. Certifikace je obvykle časově omezená a je pravidelně ověřována prostřednictvím dozorových auditů. Implementace této normy je přínosná nejen pro velké organizace, ale také pro malé a střední podniky. V praxi totiž pomáhá systematizovat přístup k ochraně informací, zlepšuje přehled o bezpečnostních procesech a podporuje odpovědný přístup zaměstnanců k práci s daty.[19 20]

3.4 Nařízení DORA

Nařízení DORA (Digital Operational Resilience Act) je podle České národní banky definováno takto: „*Nařízení DORA (Digital Operational Resilience Act) je stěžejní iniciativou EU v oblasti digitální provozní a kybernetické odolnosti, jejímž cílem je posílit bezpečnosti v sektoru finančních služeb a sjednotit požadavky pro jednotlivé druhy*

[17] DOUCEK, P.; KONEČNÝ, M. a NOVÁK, L. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. S.37. ISBN 978-80-88260-39-4.
[18] EDWARDS, J. a WEAVER, G. *The Cybersecurity Guide to Governance, Risk, and Compliance.* John Wiley, 2024. S. 209. ISBN 978-1-394-25019-6.
[19] WATKINS, S. *Iso/iec 27001: 2022*. IT Governance, 2022. S. 40-45. ISBN 1787784037.
[20] CALDER, A. *ISO 27001/ISO 27002*. IT Governance, 2017. S.109. ISBN 978-1787784932.

dohlížených subjektů."[21] Cílem tohoto nařízení je zabezpečit, aby finanční instituce byly schopny efektivně odolávat kybernetickým incidentům, adekvátně na ně reagovat a plně se z nich zotavit. Působnost tohoto nařízení se primárně zaměřuje na vymezené finanční instituce, avšak jeho dopad se rozšiřuje i na dodavatele informačních a komunikačních technologií (IKT), kteří poskytují služby těmto institucím. Ačkoli dodavatelé IKT služeb nejsou obecně přímo regulováni nařízením DORA, je zdůrazněna možnost, že mohou spadat pod jiné právní rámce, například pod směrnici NIS2, resp. nový zákon o kybernetické bezpečnosti. Výjimku tvoří tzv. kritičtí dodavatelé, kteří jsou určeni na celoevropské úrovni a podléhají přímé regulaci ze strany evropských dozorových orgánů vzhledem k jejich významnému podílu na poskytování IKT služeb v rámci celé Evropské unie. Nařízení na rozdíl od směrnice nevyžaduje převod do vnitrostátního práva, ale uplatňuje se přímo ve všech členských státech Evropské unie. V případě nařízení DORA to znamená, že jeho pravidla začalo platit automaticky, obdobně jako tomu bylo např. u nařízení GDPR. Přímá použitelnost však neznamená, že by nebyla potřeba žádná právní úprava na národní úrovni. V České republice proto dne 15. února 2025 v souvislosti s nařízením DORA nabyl účinnosti zákon o digitalizaci finančního trhu č. 31/2025 Sb., který vymezil Českou národní banku jako příslušný orgán dohledu a svěřil jí pravomoc kontrolovat dodržování stanovených povinností a ukládat sankce za jejich porušení.[22]

Nařízení DORA zajišťuje digitální provozní odolnost organizací prostřednictvím 5 klíčových požadavků, a to: řízení rizik v oblasti IKT, řízení, klasifikace a hlášení incidentů souvisejících s IKT, testování digitální provozní odolnosti, řízení dodavatelů a sdílení informací. První ze zmíněných oblastí řízení rizik v oblasti IKT si můžeme představit tak, že finanční instituce mají povinnost komplexně integrovat řízení rizik souvisejících s IKT a digitální provozní odolností do svých stávajících rámců a procesů pro řízení rizik. Tato povinnost zahrnuje používání a udržování aktuálních systémů, protokolů a IKT nástrojů, které musí vyhovovat požadavkům stanovených v článku 7 nařízení DORA. Pod druhou zmíněnou oblastí pro řízení, klasifikace a hlášení incidentů souvisejících s IKT se skrývají povinnosti vymezit, zavést a důsledně uplatňovat proces řízení incidentů s cílem efektivní detekce, řízení a hlášení těchto

[21] ČESKÁ NÁRODNÍ BANKA. *DORA – Digitální provozní odolnost finančního trhu*. Online. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/dora-digitalni-provozni-odolnost-financniho-trhu/. [cit. 2026-01-17].
[22] PATTISON, A. *DORA: a guide to the EU digital operational resilience act*. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2024. S. 11-18. ISBN 978-1-78778-451-2.

událostí. Subjekty jsou povinné informovat o významných incidentech Českou národní banku jakožto dozorový orgán. Ve třetí oblasti pro testování digitální provozní odolnosti jsou subjekty povinny implementovat testovací programy, které slouží k průběžnému ověřování digitální provozní odolnosti. Čtvrtá oblast týkající se řízení dodavatelů je jeden z ústředních pilířů nařízení DORA, vycházející z předpokladu, že finanční instituce často outsourcují značnou část svých IKT činností. Nařízení podrobně specifikuje požadavky na celý životní cyklus dodavatelů. A v poslední oblasti sdílení informací se skrývá podpora sdílení relevantních informací o kybernetických hrozbách, incidentech a dalších významných skutečnostech. Tyto informace si instituce vyměňují mezi sebou a některé jsou rovněž reportovány orgánům dohledu, tj. v České republice Česká národní banka.[23]

[23] NONNEMANN, F.; ČERVENÝ, V. a VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025. S. 72. ISBN 978-80-286-0331-1.

4 Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a s ním spojené vyhlášky

Nový zákon o kybernetické bezpečnosti vznikl v České republice zejména, protože vznikla potřeba implementovat do českého právního řádu novou směrnici Evropské unie NIS2, zároveň, ale také vznikla potřeba zákon o kybernetické bezpečnosti aktualizovat. Nový zákon, vycházející ze směrnice NIS2 byl 4. srpna 2024 publikován ve Sbírce zákonů a účinnost nabyl k 1. listopadu 2025. Většina požadavků nového zákona vychází právě ze směrnice NIS2, ale jelikož směrnice stanovuje zpravidla pouze minimální požadavky, státy tak mohou jít nad rámec požadavků. V souvislosti s primárním zákonem č. 264/2025 Sb., o kybernetické bezpečnosti byl přijat ještě doprovodný zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti, případně doplňuje další zákony, které s touto problematikou souvisí a bez těchto úprav by regulace nefungovala. Legislativní úprava kybernetické bezpečnost v České republice prošla významným vývojem, který odráží dynamicky se měnící povahu digitálních hrozeb a rostoucí závislost společnosti na informačních technologiích. Mezi hlavní změny, které se promítly do nového zákona patří: rozšíření počtu povinných osob, změna způsobu identifikace povinných osob, větší odpovědnost vrcholového vedení, nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce apod.[24]

Prvním komplexním právním předpisem u nás se stal zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který představoval reakci na potřebu systematického přístupu k ochraně kritické informační infrastruktury a významných informačních systémů. Tento zákon zároveň implementoval do českého právního řádu směrnici Evropské unie NIS, která poprvé sjednocovala minimální standardy kybernetické bezpečnosti na úrovni Evropské unie. S postupem času a rostoucím počtem kybernetických incidentů se ukázalo, že je směrnice nedostatečná vzhledem k bezpečnostním výzvám, a proto vznikla směrnice NIS2, kterou Česká republika také implementovala do svého právního řádu pomocí nového zákona o kybernetické bezpečnosti a nahradila tak původní zákon z roku 2014.[25]

[24] ČESKO. *Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/264?zalozka=text. [cit. 2026-03-14].
[25] SMEJKAL, V.; SOKOL, T. a KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. S. 33. ISBN 978-80-7380-765-8.

Nový zákon reaguje na vývoj kybernetických hrozeb a přenášení téměř všeho do digitálního prostředí. Mezi jeho hlavní cíle patří posílení kybernetické odolnosti Evropské unie jako celku a zajištění vysoké společné úrovně kybernetické bezpečnosti napříč všemi členskými státy. Důvodem pro novou právní úpravu je především potřeba rozšířit působnost regulace na větší okruh subjektů, zpřísnit požadavky na řízení rizik kybernetické bezpečnosti a incidentů a sjednotit postupy v rámci Evropské unie. Základními principy, na nichž je tato úprava postavena, jsou princip proporcionality, princip řízení rizik a princip odpovědnosti vedení organizací za kybernetickou bezpečnost. Tyto principy mají zajistit, že povinnosti budou odpovídat reálným rizikům a velikosti subjektů, kdy aktivní role v managementu kybernetické bezpečnosti je přesunuta na nejvyšší úroveň řízení. To znamená, že vrcholný management je odpovědný za to, že subjekt, kterého se zákon týká, implementuje a bude dodržovat všechna opatření, která jsou nezbytná pro zajištění souladu. Členové statutárních orgánů musí projít školením, které je provede principy kybernetické bezpečnosti. Odpovědnost platí bez ohledu na technickou kvalifikaci daného člověka a nelze se jí zprostit ani ji smluvně omezit. Toto opatření by mělo vést k reálnému zvýšení odolnosti podniků vůči kybernetickým hrozbám, jelikož pokud by porušovali některé pravidla hrozily by členům statutárních orgánů velmi vysoké sankce.[26, 27]

4.1 Vyhlášky spojené s novým zákonem č. 264/2025 Sb., o kybernetické bezpečnosti

Pro praktickou aplikaci zákona je zapotřebí přijetí navazujících právních předpisů, které konkretizují jeho obecná ustanovení. Tyto vyhlášky jsou klíčové v definování praktických požadavků na povinné subjekty a v zajišťování jednotného přístupu k implementaci kybernetické bezpečnosti. Jejich účelem je především měnit nekonkrétní zákonné principy na specifické, měřitelně, reálně uchopitelné a vynutitelné povinnosti. Jednou ze zásadních vyhlášek je vyhláška č. 408/2025 Sb., o regulovaných službách. Regulovaná služba je podle zákona o kybernetické bezpečnosti taková služba, která spadá do zákonem vymezených odvětví a je z hlediska fungování státu, společnosti nebo ekonomiky významná. Tento předpis stanovuje detailní kritéria, které identifikují

[26] HANZEL, P. *Kyberbezpečnost se stává osobní odpovědností jednatelů*. Online. Dostupné z: https://arws.cz/novinky-v-arrows/kyberbezpecnost-se-stava-osobni-odpovednosti-jednatelu. [cit. 2026-01-17].
[27] DENTONS EUROPE CS LLP. *Za selhání v kyberbezpečnosti ponese osobní zodpovědnost management. Už od listopadu*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/za-selhani-v-kyberbezpecnosti-ponese-osobni-zodpovednost-management-uz-od-listopadu. [cit. 2026-01-18].

regulované subjekty, spadající do působnosti vyšších či nižších povinností. Tato kategorizace umožňuje rozlišit požadavky na kybernetickou bezpečnost podle úrovně rizika, které daný subjekt představuje a podle významu služeb, které poskytuje. Mezi kritéria patří např. velikost organizace, počet zaměstnanců, ale i roční obrat a především význam a dopad potenciálního narušení integrity, dostupnosti a důvěrnosti jím poskytovaných služeb. Pro každý z režimů je vydán samostatný předpis, a to vyhláška o bezpečnostních opatřeních pro vyšší režim a vyhláška o bezpečnostních opatřeních pro nižší režim. První z nich specifikuje rozsah a typ bezpečnostních opatření, která musí povinné osoby zařazené do vyššího režimu implementovat. Jedná se o soubor technických, organizačních a procesních požadavků. Tyto požadavky zahrnují například řízení rizik, zvládání incidentů, ale i bezpečnost dodavatelského řetězce nebo požadavky na šifrování. Vyhláška pro subjekty spadající do nižšího režimu a s ní spojené povinnosti představují významný krok pro zvýšení celkové kybernetické bezpečnosti navzdory tomu, že jsou požadavky v tomto režimu výrazně nižší. Vyhláška dále stanovuje specifické postupy a pravidla pro identifikaci kybernetických incidentů s významným dopadem, které jsou směrodatné pro účely jejich hlášení NÚKIB. Tím je zajištěno zejména to, že na vytváření celkového přehledu o aktuálním prostředí kybernetických hrozeb podílejí i menší subjekty, což zároveň přispívá k včasné a efektivní reakci na vzniklé incidenty.[28]

Nedílnou součástí vyhlášek je i ta o Portálu NÚKIB č. 334/2025 Sb., ta si klade za cíl standardizovat a elektronizovat komunikační a administrativní procesy mezi povinnými subjekty a NÚKIB. Vyhláška upravuje technické, ale i procesní náležitosti elektronického Portálu NÚKIB, který slouží jako primární nástroj pro hlášení údajů o subjektech, oznamování kybernetických incidentů a jako přístup k informacím. Zavedení tohoto portálu má sloužit k zefektivnění administrativy, zrychlení výměny informací a zajištění plnění povinností ze strany regulovaných subjektů. Mezi připravované předpisy patří také návrh nařízení vlády o nepominutelných funkcích stanoveného rozsahu, který má vymezit, jaké funkce a aktiva jsou natolik významné, že na nich bude uplatňován mechanismus prověřování bezpečnosti dodavatelského řetězce. Dalším připravovaným předpisem je návrh nařízení vlády o strategicky významných službách, který má vymezit, jaké subjekty a služby budou považovány za strategicky

[28] ČESKO. *Vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/408?zalozka=text. [cit. 2026-03-14].

významné a na koho se bude vztahovat mechanismus prověřování bezpečnosti dodavatelského řetězce.[29]

Celkově lze konstatovat, že tyto vyhlášky tvoří důležitou součást nového legislativního rámce kybernetické bezpečnosti, jelikož převádějí obecné požadavky do konkrétních a v praxi použitelných pravidel. Jejich význam spočívá v tom, že umožňují regulovaným subjektům správně porozumět svým povinnostem, a pomáhají tyto povinnosti efektivně plnit.[30, 31]

5 Klíčové povinnosti vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti

Předchozí kapitola se věnovala nové právní úpravě kybernetické bezpečnosti v České republice jako celku a jejímu zakotvení v širším evropském kontextu vycházejícím ze směrnice NIS2. Pro naplnění cíle této bakalářské práce je však zásadní zaměřit se na konkrétní povinnosti, které z této právní úpravy vyplývají pro regulované subjekty, zejména pro malé a střední podniky. Tato kapitola se proto soustředí na zásadní povinnosti stanovené tímto zákonem, které mají přímý dopad na fungování podniků. Pozornost je věnována zejména povinnostem souvisejícím s registrací u Národního úřadu pro kybernetickou a informační bezpečnost, kritériím pro určení režimu nižších a vyšších povinností a základním požadavkům na organizační a technická opatření. Podle § 11 až § 23 mezi hlavní povinnosti všech poskytovatelů regulované služby patří:

- *ohlášení regulované služby,*
- *ohlášení kontaktních údajů,*
- *stanovení rozsahu řízení kybernetické bezpečnosti,*
- *zavádění bezpečnostních opatření,*

[29] ČESKO. *Vyhláška č. 334/2025 Sb. Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/334?zalozka=text. [cit. 2026-03-14].
[30] NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025. S. 79. ISBN 978-80-286-0331-1.
[31] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Portál NÚKIB*. Online. Dostupné z: https://portal.nukib.gov.cz/. [cit. 2026-01-17].

- *hlášení kybernetických bezpečnostních incidentů,*
- *informování uživatelů o incidentech a hrozbách,*
- *zavádění protiopatření vydaných NÚKIB.*[32]

5.1 Registrace u NÚKIB

Základním předpokladem pro plnění povinností podle zákona o kybernetické bezpečnosti je registrace poskytovatele regulované služby u NÚKIB. Samotný proces registrace probíhá prostřednictvím Portálu NÚKIB, jehož technické a procesní náležitosti upravuje samostatná vyhláška. Zástupce nebo statutární orgán poskytovatele regulované služby vyplní registrační formulář po přihlášení skrze Národní bod pro identifikaci a autentizaci (NIA). V rámci hlášení kontaktních údajů je nutné určit kontaktní osoby, přičemž subjekt může mít libovolný počet kontaktních osob, které se mohou lišit u různých služeb. Zástupce se automaticky stává kontaktní osobou, avšak kontaktní osoba nemusí být zástupcem. Kontaktní osobou však, ale musí být vždy fyzická osoba, není přípustné, aby to byla osoba právnická. Cílem hlášení těchto kontaktních údajů je zpřehlednění vztahu mezi úřadem a povinnou osobou a nastavení přímé komunikační linky. Po ohlášení úřad potvrdí registraci regulované služby a poskytovatele. A následně doručením registrace startují přechodné lhůty pro ostatní povinnosti, jako např. lhůta pro ohlášení kontaktů, která byla stanovena na 30 dnů od doručení rozhodnutí o registraci a další přechodná lhůta je na zavedení bezpečnostních a hlášení incidentů a ta je stanovena na 1 rok od doručení rozhodnutí o registraci. Pokud by subjekt začal poskytovat regulovanou službu později, tak jsou ty lhůty obdobné.[33]

Subjekty, které poskytují regulovanou službu měli lhůtu 60 od nabytí účinnosti nového zákona na ohlášení regulované služby. Tato lhůta tedy vypršela 31. prosince 2025 a podle portálu vseonis2.cz se mělo ohlásit odhadovaných 6 000 podniků, avšak k datu článku, který je 1. ledna 2026 se zaregistrovalo pouze přibližně 1 500 podniků. *„Firmy, které nestihly registraci provést v daném čase, mohou stále dodatečně ohlásit regulovanou službu přes portál NÚKIB, avšak hrozí jim sankce až do výše 250 milionů Kč. NÚKIB doporučuje co nejdřív kontaktovat úřad a využít dostupné*

[32] Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/264/2025-11-01?f=264%2F2025&zalozka=text#par_6-odst_2. [cit. 2026-03-14].
[33] KUČÍNSKÝ, A. *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti*. Online. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2025/11/20/videoprenaska-nzkb_uid_691ee0e537a80.pdf. [cit. 2026-01-17].

průvodce na portal.nukib.gov.cz. V roce 2026 firmy čeká plná implementace bezpečnostních opatření, včetně hlášení incidentů."[34]

5.2 Určení režimu vyšších či nižších povinností

Určení režimu poskytovatele regulované služby je klíčovým krokem, který stanovuje rozsah povinností, které musí daný subjekt plnit. Kritéria pro stanovení režimu jsou upravena ve vyhlášce 408/2025 Sb., o regulovaných službách, která rozlišuje vyšší a nižší režim. Základním kritériem pro tzv. samoidentifikaci jak již bylo zmíněno výše je velikost podniku, přičemž regulace se primárně týká středních a velkých podniků. Při posuzování velikosti subjektu se postupuje v souladu s příslušnými předpisy upravujícími kategorizaci podniků. Zařazení do konkrétního režimu má přímý dopad na rozsah bezpečnostních opatření, která musí poskytovatel regulované služby zavést a provádět. Pro každý z režimů existuje samostatná vyhláška o bezpečnostních opatřeních, která specifikuje detailní požadavky. Zákon rozlišuje dva způsoby identifikace regulovaných osob. Prvním je tzv. samoidentifikace podle § 4 zákona o kybernetické bezpečnosti, kdy subjekt sám posoudí, zda naplňuje alespoň jedno kritérium pro identifikaci regulované služby stanovené vyhláškou o regulovaných službách. Druhým způsobem je určení regulátorem podle § 5 zákona, kdy NÚKIB rozhodnutím stanoví, že určitá služba je regulovanou službou na základě kritérií pro určení regulované služby. V první zmíněném způsobu identifikace v tzv. samoidentifikaci je klíčová otázka velikost podniku a otázka, zda firma poskytuje některou z regulovaných služeb uvedenou ve vyhlášce o regulovaných službách. Při počítání velikosti se subjekt řídí doporučením komise 2003/361/ES o definici mikropodniků, malých a středních podniků, a pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel (počet zaměstnanců nebo rozvaha nebo obrat). Pro zjištění zda se subjektu regulace týká je také možné využít kalkulačku na portálu NÚKIB. Pokud organizace splňuje podmínky pro registraci podle § 5 zákona o kybernetické bezpečnost a je jako regulovaná služba identifikována regulátorem, nemusí jednat z vlastní iniciativy. V takovém případě ji NÚKIB sám osloví a zahájí s ní správní řízení, v jehož rámci prověřuje, zda organizace

[34] EXCLUSIVE NETWORKS. *Vypršela lhůta pro registraci regulované služby, hrozí pokuty*. Online. Dostupné z: https://vseonis2.cz/vyprsela-lhuta-pro-registraci-regulovane-sluzby-hrozi-pokuty/. [cit. 2026-01-16].

skutečně naplňuje zákonem stanovená kritéria. Nelze se tedy dostat do situace, kdy by se dotčený subjekt o své regulovatelnosti nedozvěděl.[35]

5.3 Povinnosti subjektů v režimu vyšších povinností

Každý z režimů je upraven v samostatné vyhlášce, pro subjekty, které jsou zařazeny do režimu vyšších povinností platí vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Poskytovatelé regulovaných služeb, kteří jsou zařazení do režimu vyšších povinností podléhají nejkomplexnějšímu souboru požadavků na zajištění kybernetické bezpečnosti. Do tohoto režimu jsou zařazené organizace, které jsou výrazně ekonomicky, společensky nebo bezpečnostně významné pro Českou republiku. Jedná o subjekty, které splní nejméně jedno z následujících kritérií: velikost a dosah, kritičnost pro odvětví, systémová závislost, rizikový provoz, kritická infrastruktura. Mezi tyto subjekty se můžou řadit např. velké nemocnice, energetické společnosti, ústřední orgány státní správy, poskytovatelé telekomunikačních služeb apod. Subjekty zařazené do režimu vyšších povinností musí plnit veškeré povinnosti stanovené pro režim nižších povinností a současně další kvalifikované požadavky, které reflektují jejich zvýšený význam pro kybernetickou bezpečnost státu. Náročnější požadavky jsou kladeny zejména, protože případné selhání subjektů by mělo závažnější následky než u subjektů v nižším režimu. Jak již bylo psáno, tak základním rozlišovacím kritériem určení režimu povinností je velikost podniku. Do režimu vyšších povinností spadají automaticky velké podniky, které zaměstnávají více než 250 zaměstnanců nebo ty, kterých roční obrat přesahuje 50 milionů EUR, případně ty, kterých bilanční suma rozvahy přesahuje 43 milionů EUR. Toto kritérium vychází z definice velkého podniku podle přílohy I nařízení Komise Evropské unie č. 651/2014. Toto nařízení současně předpokládá, že velký podnik má dostatečné zdroje pro implementaci náročnějších bezpečnostních opatření. Druhým určujícím faktorem je odvětví, ve kterém podnik působí. Zákon rozlišuje odvětví s vysokou mírou rizika a ostatní odvětví. Do režimu vyšších povinností logicky spadají podniky působící v odvětví s vysokou kritičností bez ohledu na jejich velikost, pokud splňují alespoň kritérium středního podniku. Mezi tato odvětví patří např. energetika, doprava, bankovnictví, zdravotnictví, dodávky a distribuce pitné vody, odpadní vody atd. Zákon

[35] ČESKO. *Vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/408?zalozka=text. [cit. 2026-03-14].

dále stanoví, že do režimu vyšších povinností spadají bez ohledu na velikost také některé specifické kategorie subjektů, a to zejména poskytovatelé služeb systému doménových jmen, poskytovatele registru internetových domén nejvyšší úrovně, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center apod. Tahle kategorizace reflektuje kritický význam uvedených služeb pro fungování digitální ekonomiky, jelikož poskytovatelé těchto služeb představují potenciální jednotné body selhání, jejichž narušení by mohlo ovlivnit velké množství dalších subjektů závislých na jejich službách. NÚKIB má navíc pravomoc zařadit do režimu vyšších povinností i subjekt, který by jinak spadal do režimu nižších povinností, pokud je to odůvodněno významem jeho služby pro společnost nebo ekonomiku, potenciálním dopadem incidentu nebo jeho postavením jako jediného poskytovatele dané služby v České republice.[36]

5.3.1 Stanovení bezpečnostních rolí

Subjekty v režimu vyšších povinností musí implementovat komplexní systém řízení bezpečnosti informací. Jedním ze základních požadavků vyhlášky je určit osobu, která bude za kybernetickou bezpečnost v organizaci skutečně odpovědná. Tato osoba by měla mít přímý kontakt s vedením a zároveň dostatečný prostor prosazovat potřebná bezpečnostní opatření. Na rozdíl od režimu nižších povinností je v tomto režimu povinnost, aby tato osoba byla zaměstnancem organizace a není možné ji přenést na externího dodavatele. Vyhláška o režimu vyšších povinností stanoví v § 4 odst. 4 toto: *„Vrcholné vedení určí osoby, včetně vymezení jejich práv a povinností souvisejících se systémem řízení bezpečnosti informací, které budou zastávat bezpečnostní role*

a) manažera kybernetické bezpečnosti,

b) architekta kybernetické bezpečnosti,

c) garanta aktiva a

d) auditora kybernetické bezpečnosti.“[37]

V následujícím odstavci vyhláška stanoví, že vrcholné vedení musí zajistit zastupitelnost bezpečnostních rolí uvedených v odstavci 4 písm. a) a b). První

[36] ČESKO. *Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/409?zalozka=text. [cit. 2026-03-14].

[37] ČESKO. *Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/409?zalozka=text. [cit. 2026-03-14].

ze zmíněných, tj. manažer kybernetické bezpečnosti má na starosti řízení systému bezpečnostních informací, na tuto pozici musí být osoba vyškolena a musí prokázat odbornou způsobilost praxí s řízením kybernetické bezpečnost anebo s řízením bezpečnosti informací nejméně po dobu 3 let. Manažer kybernetické bezpečnosti je odpovědný za informování vrcholného vedení o činnostech, které spadají do jeho odpovědnost a o aktuálním stavu systému řízení bezpečnostních informací. Architekt kybernetické bezpečnosti má na starosti návrh a zavedení bezpečnostních opatření tak, aby byla regulovaná služba postavena na bezpečné a funkční architektuře. Tuto roli může vykonávat pouze osoba, která doloží svou způsobilost praktickými zkušenostmi s navrhováním a implementací bezpečnostních opatření a se zajišťováním bezpečné architektury, a to nejméně po dobu 3 let. Garant aktiva se zaměřuje na rozvoj, použití a bezpečnost aktiv. A auditor kybernetické bezpečnosti má na starosti provádění auditu kybernetické bezpečnosti. Auditor se také zaručí, že provedení auditu je nestranné a zároveň auditor nesmí být pověřen výkonem jiných bezpečnostních rolí. [38]

5.3.2 Technická opatření

Mezi technická opatření patří požadavky na zabezpečení sítí a informačních systémů na vyšší úrovni než v režimu nižších povinností. Podle § 17 vyhlášky č. 409/2025 Sb., je subjekt povinen zajistit osobu, která má na starosti fyzickou bezpečnost, např. předcházení poškození, odcizení nebo zneužití aktiv. Součástí povinností této osoby je vymezení fyzických bezpečnostních prostorů, ve kterých jsou uchovány nebo zpracovány informace a data, případně kde se nacházejí technická aktiva. Tyto fyzické bezpečnostní perimetry musí být následně rozděleny do jednotlivých úrovní fyzické ochrany podle významu a citlivosti umístěných technických aktiv. Následně je tyto stanovené perimetry nutné řádně dokumentovat.

V oblasti bezpečnostních komunikačních sítí je povinná osoba podle § 18 vyhlášky o bezpečnostních opatřeních odpovědná za zajištění ochrany komunikační sítě, a to včetně jejího síťového perimetru. Základním požadavkem je vhodně navržené a zdokumentované rozdělení sítí, které odděluje jednotlivá prostředí a přispívá ke snížení rizika šíření bezpečnostních incidentů. Současně musí být také nastavena pravidla pro řízení komunikace, vzdáleného přístupu, přičemž povolená komunikace je omezena pouze na nezbytný rozsah.

[38] NICHOLS, L. *Cybersecurity Architect's Handbook*. De Gruyter GmbH, Walter, 2024. S. 82. ISBN 978-1803235844.

Podle následujícího § 19 je pověřená osoba povinná zajistit správu a ověřování identit uživatelů, administrátorů i technických aktiv. V praxi to znamená, že organizace musí mít přehled o tom, kdo a za jakých podmínek má přístup k systémům a datům, a že je přístup vždy umožněn pouze až po řádném ověření identity. Součástí těchto opatření je také ochrana přihlašovacích údajů, omezení počtu neúspěšných pokusů o přihlášení a opětovné ověření identity po určité době nečinnosti. Pokud je ověřování identity založeno na heslech, musí být hesla dostatečně silná, pravidelně měněná a nesmí být opakovaně používané.

V § 21 stejné vyhlášky je osoba povinná zajistit včasnou detekci kybernetických bezpečnostních událostí prostřednictvím vhodných technických nástrojů. Tyto nástroje jsou určené ke kontrole a ověřování přenášených dat v rámci komunikační sítě a zároveň umožňují aktivně blokovat nežádoucí nebo podezřelou komunikaci. Důležitou součástí je také schopnost odhalovat bezpečnostní události nejen na základě technických indikátorů, ale i podle chování uživatelů, administrátorů a samotných systémů. Používané nástroje musí být samozřejmě pravidelně aktualizované, a to jak z pohledu softwaru, tak i nastavení detekčních pravidel, aby byly schopné reagovat na aktuální hrozby a nové typy útoků. Podle § 23 musí organizace poskytující regulovanou službu průběžně vyhodnocovat kybernetické bezpečnostní události, které byly detekovány podle § 21. K tomuto účelu je využíván nástroj, který shromažďuje a propojuje relevantní záznamy, poskytuje průběžné informace o zjištěných událostech a umožňuje včasné varování odpovědných osob. Cílem tohoto procesu je rozlišit, zda se jedná o běžnou bezpečnostní událost nebo již o kybernetický bezpečnostní incident.

Podle § 26 je organizace povinná poskytující regulovanou službu přijmout taková bezpečnostní opatření, která zajistí její dostupnost i v případě nepříznivých situací. To znamená, že služba má být dostupná v souladu s předem stanovenými cíli, odolná vůči hrozbám a zranitelnostem. Součástí těchto opatření je také pravidelné vytváření záloh technických aktiv, informací a dat, která jsou nezbytná pro obnovu regulované služby v případě kybernetického bezpečnostního incidentu. Pro omezení šíření kybernetického bezpečnostního incidentu a snížení dopadů je také požadováno oddělení zálohovacího prostředí od ostatních prostředí, zejména od provozní části infrastruktury.

Režim vyšších povinností klade na regulované subjekty výrazně přísnější nároky nejen v oblasti technických a organizačních opatření, ale také v oblasti reakce na kybernetické bezpečnostní incidenty a následné kontroly plnění povinností. Povinnost

hlášení incidentů je v tomto režimu nastavena velmi podrobně a časově striktně. Významné kybernetické bezpečnostní incidenty musí být hlášeny na NÚKIB do 24 hodin od jejich zjištění a poté do 72 hodin musí být nahlášeny podrobnosti o tomto incidentu a do jednoho měsíce závěrečná zpráva o incidentu. V závěrečné zprávě je obsažena zejména analýza příčiny incidentu, přijatá opatření a poučení do budoucna. Subjekty v režimu vyšších povinností jsou zároveň povinny podrobovat se pravidelnému auditu kybernetické bezpečnosti, který musí být prováděn nezávislým auditorem nejméně jednou za 2 roky. Výsledky jsou následně předány NÚKIB a cílem tohoto auditu je ověření souladu zavedených opatření s požadavky zákona a prováděcích předpisů. NÚKIB je také oprávněn provádět kontroly plnění povinností, a to samozřejmě jak plánované, tak neohlášené. V rámci kontroly může požadovat přístup k dokumentaci, informačním systémům i prostorám organizace. Celkově lze shrnout, že režim vyšších povinností představuje komplexní a náročný systém požadavků, který klade důraz na prevenci, včasnou detekci, schopnost reakce a průběžnou kontrolu kybernetické bezpečnosti. Právě tento rozsah povinností má zásadní význam pro hodnocení připravenosti malých a středních podniků, kterou mohou mít s naplněním těchto požadavků omezené personální, technické či finanční kapacity.[39, 40]

5.4 Povinnosti subjektů v režimu nižších povinností

Druhým režimem regulace kybernetické bezpečnosti zavedeným zákonem č. 264/2025 Sb., o kybernetické bezpečnosti je režim nižších povinností. Tento režim je určen pro poskytovatele regulovaných služeb, kteří jsou klasifikování jako důležité subjekty ve smyslu směrnice NIS2, a dále pro některé další kategorie vymezené zákonem. Do režimu nižších povinností spadají všechny regulované subjekty, které nepatří do režimu vyšších povinností. Může se jednat např. o střední firmy v regulovaných odvětvích nebo o obce s rozšířenou působností. Konkrétně se jedná o podniky, které mají 50 až 249 zaměstnanců nebo rozvahu vyšší než 10 milionů EUR nebo roční obrat vyšší než 10 milionů EUR. Pokud podnik přesáhne jedno z kritérií tak se ho regulovaná služba bude týkat. Podniky poskytují služby v oblastech jako je digitální struktura, správa služeb informačních a komunikačních technologií, poštovní a kurýrní služby, nakládání

[39] ČESKO. *Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/409?zalozka=text. [cit. 2026-03-14].

[40] KRAITA.IO. *Režim vyšších nebo nižších povinností: Kam spadá vaše firma podle nového zákona?* Online. Dostupné z: https://www.kraita.io/blogove-prispevky/rezim-vyssich-nebo-nizsich-povinnosti-kam-spada-vase-firma-podle-noveho-zakona.. [cit. 2026-01-16].

s odpady, výroba a distribuce chemických látek nebo třeba výroba a distribuce potravin. Vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností stanovuje pro tyto subjekty konkrétní technická a organizační opatření, která jsou ve srovnání s režimem vyšších povinností méně rozsáhlá, avšak stále zajišťují adekvátní úroveň ochrany regulovaných služeb před kybernetickými hrozbami.[41]

5.4.1 Bezpečnostní opatření

V rámci zajištění kybernetické bezpečnosti povinná osoba vytváří přehled bezpečnostních opatření, který poskytuje ucelený pohled o tom, jaká opatření byla v organizaci již zavedena, jaká jsou plánována a která zavedena nejsou, včetně důvodů jejich nezavedení. U plánovaných opatření musí být stanovena priorita, termíny realizace a odpovědné osoby. Tento přehled je nutné alespoň jednou ročně aktualizovat a vyhodnocovat účinnost zavedených opatření, a současně je organizace povinna tyto dokumenty uchovávat po stanovenou dobu. Součástí zajištění minimální kybernetické bezpečnosti je také existence bezpečnostní politiky a související dokumentace, která upravuje pravidla a postupy v této oblasti. Tato pravidla musí být pravidelně přezkoumávána, aktualizována a jejich dodržování musí být v organizaci důsledně vynucováno.

Vyhláška v režimu nižších povinností klade významný důraz na roli vrcholného vedení při zajišťování kybernetické bezpečnosti. Vedení je odpovědné za to, aby měla určená osoba pověřená kybernetickou bezpečností odpovídající odborné znalosti, případně by byla povinná absolvovat stanovené odborné školení. Tato osoba musí mít dostatečné pravomoci k řízení a rozvoji dané oblasti, k dohledu nad jejím stavem a ke komunikaci s vedením organizace. Současně zajišťuje dostupnost zdrojů potřebných ke kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření a prosazuje neustálé zlepšování zajišťování kybernetické bezpečnosti. Osoba stanovuje i prioritu obnovy primárních aktiv.

V oblasti bezpečnosti lidských zdrojů se vyhláška zaměřuje především na chování osob, které s informačními systémy a daty pracují. Organizace má povinnost stanovit pravidla bezpečného chování uživatelů a vytvořit systém rozvoje bezpečnostního chování

[41] ČESKO. *Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/410?zalozka=text. [cit. 2026-03-14].

pro vrcholové vedení, ale i běžné uživatele, administrátory společně s osobou pověřenou kybernetickou bezpečností. Do těchto pravidel spadají i zásady týkající se tvorby a používání hesel, které bývají často podceňované. Důraz je v tomto případě kladen na prevenci, ale také na schopnost reagovat na situace, kdy k porušení bezpečnostních pravidel dojde. Prevence je prováděna hlavně formou školení a to jak vstupních, tak i pravidelných. Školení musí být zajištěna také pro administrátory a pro osobu odpovědnou za kybernetickou bezpečnost, a to samozřejmě v rozsahu odpovídajícím pracovní náplni. O všech provedených školeních je nutné vést přehled a evidenci školených osob.[42]

Vyhláška ukládá organizacím také povinnost zajistit základní schopnost detekovat kybernetické bezpečnostní události a včas na ně reagovat. Do toho patří zejména kontrola přenášených dat na síťovém perimetru, včetně blokování nežádoucí nebo podezřelé komunikace. Součástí těchto opatření je také využívání nástrojů pro nepřetržitou ochranu technických aktiv před škodlivým kódem, a to především na serverech. Subjekt také musí zajistit, aby bezpečnostní události byly průběžně vyhodnocovány a aby se o nich včas dozvěděly odpovědné osoby. Nedílnou součástí je také zaznamenávání bezpečnostních událostí. U zaznamenaných událostí musí být uchovány informace, jako datum a čas, typ činnosti, jednoznačná identifikace technického aktiva a identifikace účtu původce a informace o tom, zda byla činnost úspěšná či nikoliv. Záznamy se uchovávány po dobu, kterou si organizace stanoví podle svých bezpečnostních potřeb a slouží jako podklad pro vyhodnocování bezpečnostních událostí a případných incidentů.

Nedílná součást vyhlášky je § 10 o řešení kybernetických bezpečnostních incidentů, který organizacím ukládá povinnost mít nastavený systematický postup pro řešení kybernetických bezpečnostních událostí a incidentů. Základem je, aby povinná osoba zajistila, že v případě neobvyklého chování technických aktiv nebo při jakémkoliv podezření na jakoukoliv zranitelnosti budou uživatelé, administrátoři a další zaměstnanci tuto činnosti oznamovat. Podnik musí mít vypracovanou metodiku pro posuzování kybernetických bezpečnostních událostí a incidentů, která umožní vyhodnotit jejich závažnost a případný dopad na poskytovatele služeb. Na základě této metodiky jsou bezpečnostní události průběžně detekovány, vyhodnocovány a v případě potřeby

[42] KRAITA.IO. *Režim vyšších nebo nižších povinností: Kam spadá vaše firma podle nového zákona?* Online. Dostupné z: https://www.kraita.io/blogove-prispevky/rezim-vyssich-nebo-nizsich-povinnosti-kam-spada-vase-firma-podle-noveho-zakona.. [cit. 2026-01-16].

klasifikovány jako kybernetické bezpečnostní incidenty. V případě incidentu s významným dopadem je subjekt povinen zajistit jeho oznámení v souladu se zákonem o kybernetické bezpečnosti a následně zpracovat závěrečnou zprávu o jeho řešení. Zpráva slouží jako podklad pro vyhodnocení přijatých opatření a poučení pro budoucí zlepšení úrovně kybernetické bezpečnosti. [43]

5.4.2 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Stanovení významnosti dopadu kybernetického bezpečnostního incidentu je upraveno § 14 vyhlášky, který stanoví povinnost organizací předem nastavit způsob hodnocení dopadů incidentů na poskytování regulované služby. Základem tohoto hodnocení je určení tzv. únosné míry újmy, což představuje hranici, kdy při jejím nepřekročení ještě nedochází k ohrožení života nebo zdraví osob ani k narušení schopnosti organizace plnit své závazky. Vyhláška stanoví i oblasti pro posouzení významnosti dopadu těchto incidentů, přičemž hodnocení se zaměřuje zejména na provozní dopad incidentu na povinnou osobu a její schopnost poskytovat regulovanou činnost. Dále se zohledňuje počet uživatelů a dalších subjektů, které byly incidentem dotčeny, časové a technické nároky nezbytné k obnově poskytování služeb. V případě, že je příčina incidentu známa, přihlíží se také k tomu, zda se jednalo o lidskou chybu, technickou závadu nebo úmyslné jednání. Dopad incidentu na poskytování regulované služby je významný pokud podle § 14 odst. 2

a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně

b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.[44]

Režim nižších povinností stanovený vyhláškou č. 410/2025 Sb., představuje ucelený rámec požadavků na kybernetickou bezpečnost, který je přizpůsoben potřebám a možnostem středních podniků a dalších podniků označených za důležité subjekty. Jednotlivé povinnosti pokrývají všechny klíčové oblasti řízení kybernetické bezpečnosti od systémového přístupu k řízení bezpečnosti informací přes technická opatření až

[43] ČESKO. *Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/410?zalozka=text. [cit. 2026-03-14].
[44] ČESKO. *Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/410?zalozka=text. [cit. 2026-03-14].

po organizační aspekty. Ačkoliv jsou požadavky v režimu nižších povinností méně detailní než v režimu vyšších povinností, stále vyžadují od subjektů ucelený přístup k řízení kybernetické bezpečnosti. Pro tyto podniky, které doposud nemusely plnit požadavky zákona, představuje naplnění těchto povinností významnou výzvu vyžadující alokaci odpovídajících finančních, personálních a technických zdrojů. [45]

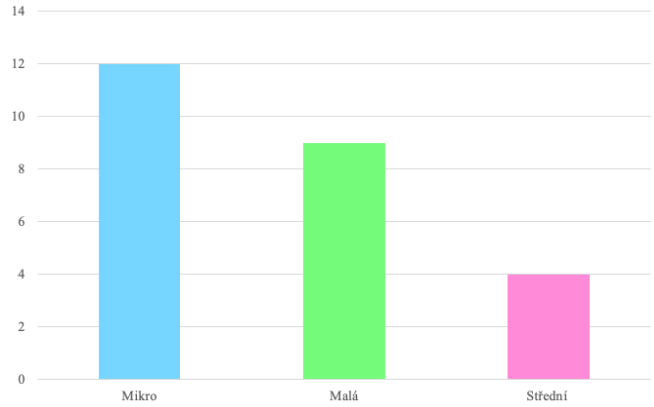
[45] ČESKO. *Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/410?zalozka=text. [cit. 2026-03-14].

6 Výzkumná část práce

Praktická část bakalářské práce je zaměřena na zjištění aktuální připravenosti vybraných malých a středních podniků na plnění povinností vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Hlavním cílem práce je vyhodnotit míru připravenosti těchto podniků na nové legislativní požadavky. Součástí praktické části je také identifikace nejčastějších nedostatků v praktickém naplňování požadavků vyplývajících z tohoto zákona. Na základě získaných poznatků autorka práce v závěru praktické části navrhuje opatření, která mohou přispět ke zvýšení souladu malých a středních podniků s legislativními požadavky v oblasti kybernetické bezpečnosti.

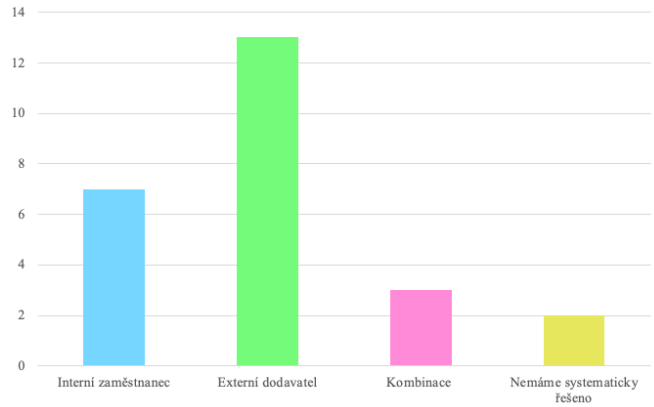
Výzkum vychází z vlastního šetření autorky práce, které bylo realizováno v únoru 2026. Cílem tohoto šetření bylo zjistit připravenost malých a středních podniků na plnění povinností vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Pro účely šetření byli osloveni klienti advokátní kanceláře Mgr. Alexandry Mára Paurové. Autorka práce s klienty realizovala celkem 25 strukturovaných rozhovorů, které vycházely z předem připraveného dotazníku s uzavřenými otázkami. Získané odpovědi byly následně kvantitativně vyhodnoceny a pro přehlednost jsou v práci prezentovány pomocí grafů. Většinu respondentů tvořili jednatelé nebo osoby ve vedoucích pozicích, které mají přehled o fungování organizace a jejích povinnostech v oblasti kybernetické bezpečnosti. Vzhledem k tomu, že si respondenti nepřáli být v práci jmenováni, jsou všechny získané odpovědi zpracovány anonymně. Celý soubor otázek a možnosti odpovědí jsou dále uvedeny v Příloze I.

Graf č. 1: Jak je velká organizace, ve které pracujete?[46]



První otázka byla zaměřena na zjištění velikosti organizace, ve které respondenti působí. Z celkového počtu 25 dotázaných tvořily největší skupinu mikro podniky s počtem zaměstnanců od 1 do 9, které představovaly 12 respondentů. Malé podniky s počtem zaměstnanců od 10 do 49 byly zastoupeny 9 respondenty. Nejmenší skupinou jsou střední podniky s počtem zaměstnanců od 50 do 249, které byly zastoupeny pouze 4 respondenty. Výsledky reflektují zaměření advokátní kanceláře, které je spíše na menší podniky. Ty často nedisponují rozsáhlými interními kapacitami pro řízení kybernetické bezpečnosti, což může mít vliv na jejich schopnost reagovat na nové legislativní požadavky.

Graf č. 2: Jak máte zajištěnu IT správu?[47]

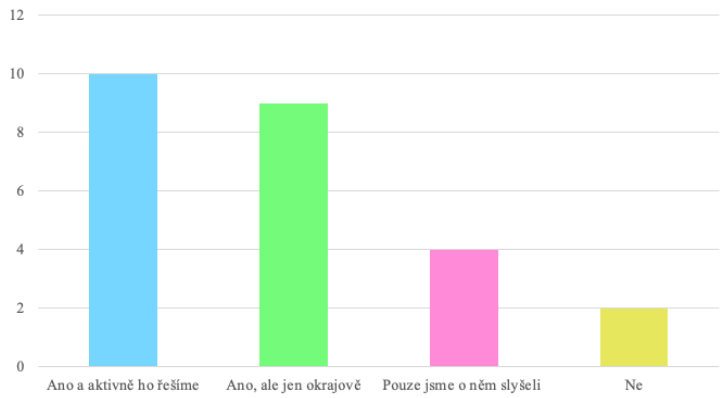


Druhá otázka byla zaměřena na způsob zajištění IT správy v jednotlivých organizacích. Z výsledků vyplynulo, že největší část podniků využívá externího dodavatele IT služeb, což uvedlo 13 dotázaných. Interního zaměstnance zodpovědného za IT správu uvedlo 7 organizací a kombinaci interní a externí správy využívají pouze

[46] Vlastní zpracování
[47] Vlastní zpracování

3 podniky. Ve dvou případech bylo dokonce uvedeno, že IT správa není řešena vůbec systematicky. Výsledky ukazují, že malé a střední podniky často spoléhají na externí poskytovatele IT služeb, což je vzhledem k jejich velikosti a omezeným personálním kapacitám poměrně běžné. V některých případech to může představovat komplikace, jelikož pokud organizace spoléhá především na externí správu, tak nemusí mít vždy dostatečný přehled o legislativních požadavcích nebo o tom, zda se na ně vztahují konkrétní povinnosti.

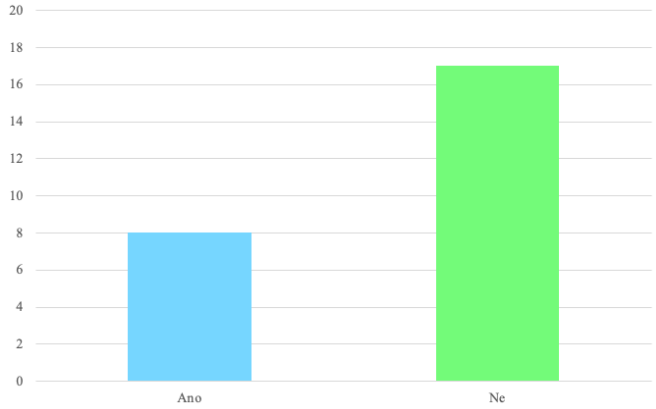
Graf č. 3: Slyšeli jste o novém zákoně o kybernetické bezpečnosti (ZoKB/NIS2)?[48]



Třetí otázka byla zaměřena na zjištění míry povědomí o novém zákoně č. 264/2025 Sb., o kybernetické bezpečnosti, který do českého právního řádu implementuje směrnici NIS2. Z celkového počtu oslovených, uvedlo 10 osob, že se novým zákonem aktivně zabývá. Devět dotázaných uvedlo, že se se zákonem setkali pouze okrajově, čtyři osoby o něm pouze slyšeli a dokonce dvě uvedly, že se s tímto zákonem dosud vůbec nesetkaly. To ukazuje, že povědomí o nové právní úpravě mezi podniky sice existuje, avšak jeho úroveň se výrazně liší. Pouze část organizací se novým zákonem aktivně zabývá, zatímco značná část podniků má o této legislativě pouze omezené informace. Tento výsledek může naznačovat, že přestože nový zákon o kybernetické bezpečnosti již vstoupil v účinnost, část malých a středních podniků si stále plně neuvědomuje rozsah povinností, které z něj pro ně mohou vyplývat. Nedostatečné povědomí o nové legislativě tak může představovat jednu z hlavních překážek při jejím praktickém naplňování.

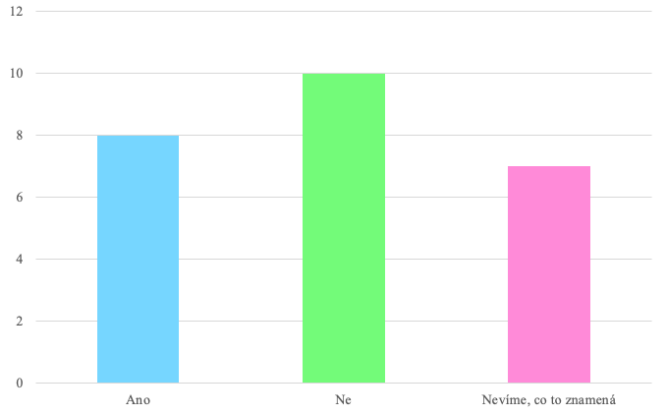
[48] Vlastní zpracování

Graf č. 4: Slyšeli jste o směrnici ISO/IEC 27001?[49]



Tato otázka zjišťovala, zda se oslovené osoby setkaly se směrnicí ISO/IEC 27001, která představuje mezinárodně uznávaný rámec pro řízení bezpečnosti informací. Pouze 8 z oslovených uvedlo, že se se směrnicí setkali, ostatní uvedli, že nikoliv. Toto lze do jisté míry považovat za očekávatelný výsledek, jelikož ISO/IEC 27001 je dobrovolným mezinárodním standardem pro řízení bezpečnosti informací a jeho zavedení není pro podniky obecně povinné. Přesto může být tento rámec pro podniky vhodným vodítkem pro systematické řízení kybernetické bezpečnosti, organizaci to může pomoci nastavit základní bezpečnostní procesy a zároveň usnadnit splnění legislativní požadavky v případě, že by se na ně v budoucnu regulace vztahovala.

Graf č. 5: Posuzovali jste, zda poskytujete regulovanou službu podle Zákona o kybernetické bezpečnosti?[50]

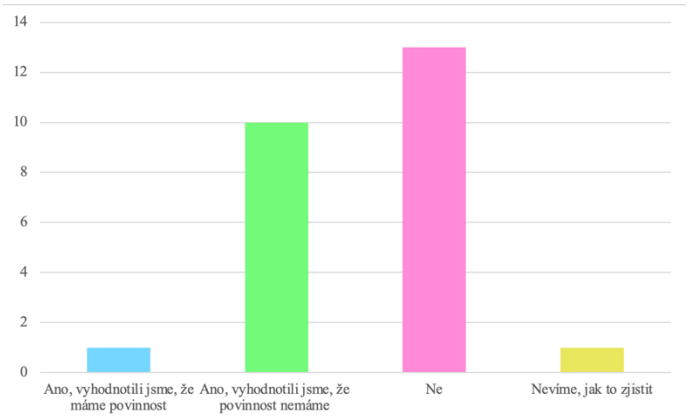


Tato otázka zjišťovala, jestli podniky posuzovaly poskytování regulované služby ve smyslu zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Z celkového počtu dotázaných, uvedlo 10 osob, že tuto skutečnost neposuzovalo. Sedm osob, což

[49] Vlastní zpracování
[50] Vlastní zpracování

představuje 28 % všech oslovených uvedlo, že neví co to znamená. Což je velmi překvapivé, jelikož právě posouzení, zda organizace poskytuje regulovanou službu je jeden z klíčových kroků při určování povinností podle zákona o kybernetické bezpečnosti.

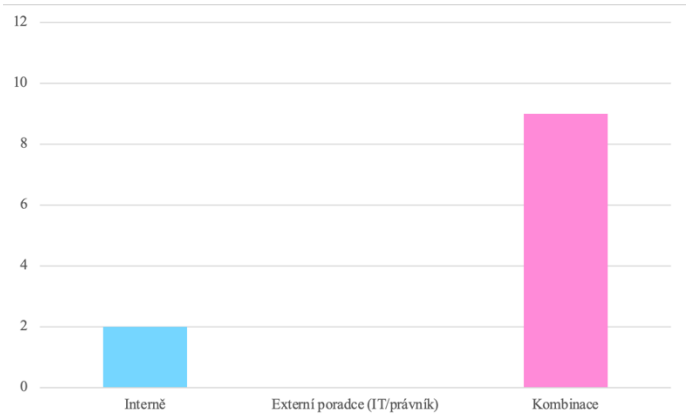
Graf č. 6: Posuzovali jste povinnost registrace u NÚKIB?[51]



Otázka č. 6 byla zaměřena na zjištění, zda podniky posuzovaly svou případnou povinnost registrace u Národního úřadu pro kybernetickou bezpečnost (NÚKIB). Z odpovědí vyplynulo, že 40 % z oslovených organizací vyhodnotilo, že se na ně povinnost nevztahuje, jelikož neposkytují regulovanou službu. Pouze 1 z oslovených organizací uvedla, že poskytují regulovanou službu, tzn. že mají povinnost registrovat se u NÚKIB. Zajímavým zjištěním však bylo, že jedna organizace uvedla, že neví, jak zjistit, zda se na ně povinnost registrace u NÚKIB vztahuje. To lze považovat za poměrně dost překvapivé, protože pokud organizace již posoudila, zda poskytuje regulovanou službu či nikoliv, měla by být zároveň schopna vyhodnotit, zda se na ni vztahuje povinnost registrace u NÚKIB.

[51] Vlastní zpracování

Graf č. 7: Kdo posouzení provedl?[52]

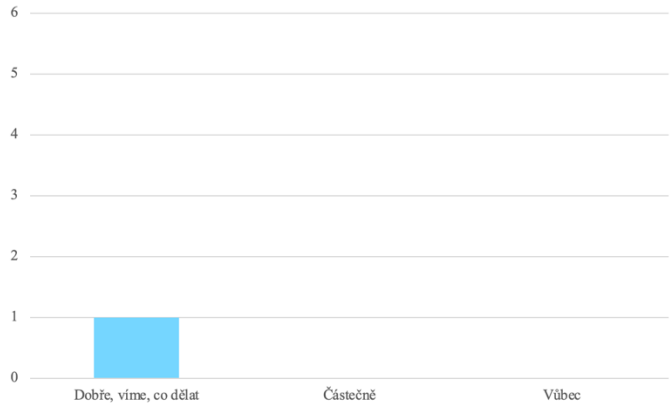


Otázka č. 7 zněla „Kdo posouzení provedl?“, autorka práce touto otázkou chtěla zjistit, zda posouzení poskytování regulované služby proběhlo interně, externě anebo kombinací obojího. Tato otázka navazovala na předchozí, ve které bylo zjišťováno, zda podniky tuto povinnost vůbec posuzovaly. Z odpovědí vyplynulo, že tuto skutečnost posuzovalo celkem 11 organizací. Na tuto otázku tak odpovídaly pouze tyto organizace, jelikož ostatní podniky uvedly, že neposuzovaly povinnost registrace u NÚKIB. Ve většině případů bylo posouzení zajištěno kombinací interních zaměstnanců a externích poradců, například právníků. Pouze 2 podniky uvedly, že posouzení bylo provedeno výhradně interně.

Tento výsledek naznačuje, že podniky při posuzování povinností v oblasti kybernetické bezpečnosti si raději nechají poradit od odborníka na danou problematiku, což může souviset i s komplexností právních a technických požadavků vyplývajících z nové právní úpravy.

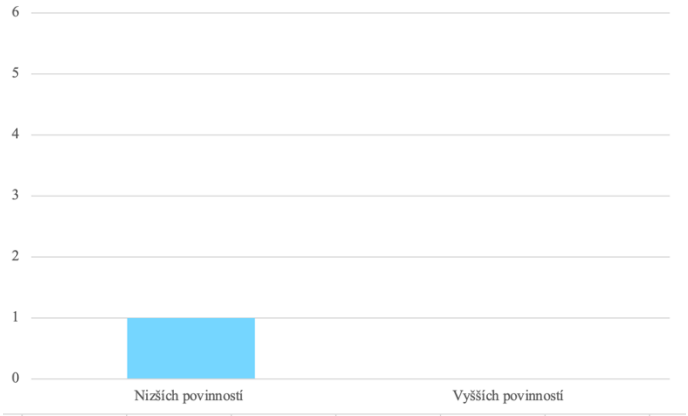
[52] Vlastní zpracování

Graf č. 8: Jak dobře rozumíte procesu registrace u NÚKIB?[53]



Otázka č. 8 byla zaměřená na porozumění procesu registrace u NÚKIB, touto otázkou autorka práce chtěla prověřit, jak je tento proces pro samotné organizace srozumitelný a zda mají dostatečné povědomí o jeho průběhu. V návaznosti na odpovědi z otázky č. 6 však vyplynulo, že pouze jedna organizace poskytuje regulovanou službu a vztahuje se na ní povinnost registrace u NÚKIB. Ostatní dotázané organizace procesem registrace neprocházely. Tato organizace uvedla, že procesu registrace rozumí a ví, jak postupovat. Skutečnost, že organizace s praktickou zkušeností hodnotí proces jako srozumitelný, může poukazovat na to, že je proces registrace ze strany NÚKIB nastaven přehledně a srozumitelně. Zároveň však nelze vzhledem k omezenému počtu odpovědí vyvozovat obecnější závěry.

Graf č. 9: Do kterého režimu regulované služby vaše organizace spadá?[54]

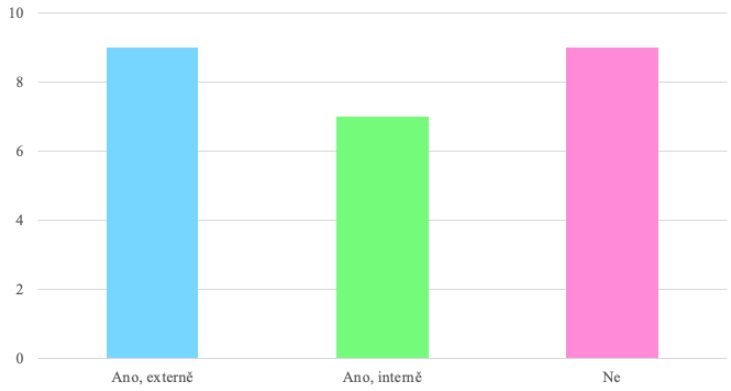


V rámci rozhovorů se tato otázka zaměřovala na zjištění, do kterého režimu regulované služby organizace spadá. Z předchozích otázek vyplynulo, že pouze jedna z

[53] Vlastní zpracování
[54] Vlastní zpracování

dotazovaných organizací poskytuje regulovanou službu a proto pouze pro tuto jednu organizaci byla tato otázka relevantní. V daném případě bylo uvedeno, že organizace spadá do režimu nižších povinností. Zařazení do nižšího režimu znamená i nižší míru povinností pro danou firmu. Celkově to také odpovídá klientele advokátní kanceláře, která je zaměřená spíše na menší a střední podniky.

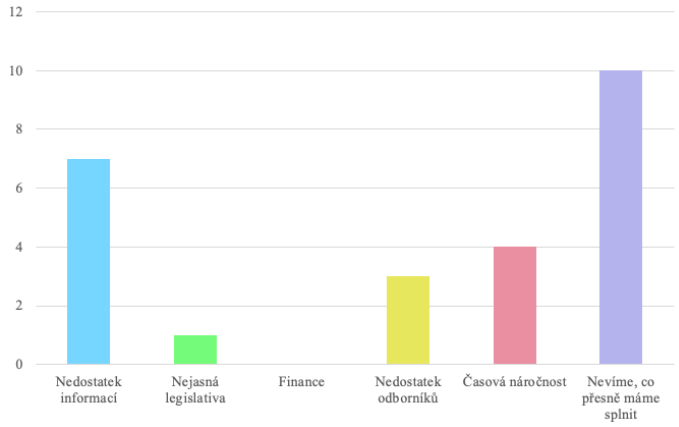
Graf č. 10: Má vaše organizace určenou osobu odpovědnou za kybernetickou bezpečnost?[55]



V rámci odpovědí na tuto otázku měli oslovení možnost uvést, zda je tato osoba určena interně, externě anebo že určenou osobu vůbec nemají. Z odpovědí je zřejmé, že 7 organizací má osobu odpovědnou za kybernetickou bezpečnost určenou interně a 9 organizací externě. Avšak 9 z dotázaných, což představuje 36 % žádnou takovou osobu nemá. To naznačuje, že zejména menší podniky často nepřistupují k řízení kybernetické bezpečnosti systematicky. Lze předpokládat, že taková organizace otázky kybernetické bezpečnosti řeší operativně nebo ad hoc. V praxi to může znamenat, že je problém anebo potřeba řešena až v momentě kdy nastane, nikoli na základě předem nastaveného systému. Pokud organizace nemá žádnou odpovědnou osobu může to představovat i potencionální riziko, a to zejména v případě, že by na tyto organizace v budoucnu dopadaly povinnosti vyplývající ze zákona.

[55] Vlastní zpracování

Graf č. 11: Co vám nejvíce brání splnit požadavky Zákona o kybernetické bezpečnosti?[56]

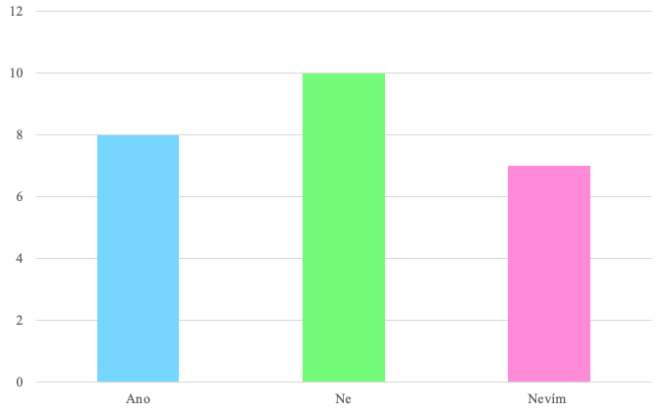


V rámci rozhovorů měli oslovení možnost vybrat více odpovědí, jelikož překážek při naplňování požadavků zákona o kybernetické bezpečnosti může být více současně. Mezi nabízené možnosti patřil například nedostatek informací, nejasná legislativa, finanční náročnost, nedostatek odborníků, časová náročnost nebo skutečnost, že organizace přesně neví, jaké povinnosti se na ni vztahují nebo by se na ni vztahovali. Na tuto otázku mohly odpovídat všechny oslovené organizace, a to i v případě, že regulovanou službu neposkytují. Odpovědi tak vycházely z jejich teoretického pohledu na problematiku a z představy, jaké překážky by mohly při naplňování požadavků zákona o kybernetické bezpečnosti pociťovat, pokud by se na ně tato právní úprava vztahovala.

Z odpovědí vyplynulo, že mezi nejčastěji zmiňované překážky patří především nedostatek informací o nové právní úpravě a také nejasnost samotných legislativních požadavků. Část oslovených osob rovněž uvedla, že přesně neví, jaké konkrétní povinnosti by jejich organizace měla splnit. Tyto výsledky naznačují, že pro malé a střední podniky může být hlavním problémem především orientace v nové právní úpravě a pochopení praktických dopadů zákona o kybernetické bezpečnosti.

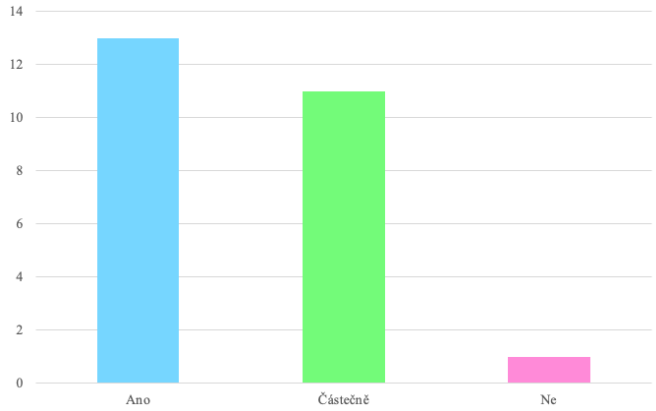
[56] Vlastní zpracování

Graf č. 12: Má vaše organizace zpracovaný postup pro řešení kybernetického incidentu?[57]



V rámci rozhovorů se autorka práce dále zaměřila na to, zda mají organizace zpracovaný postup pro řešení kybernetického incidentu. Získané odpovědi ukazují, že takový postup nemá 40 % oslovených organizací. Tento výsledek může představovat potenciální komplikaci, protože absence předem stanoveného postupu může v případě vzniku kybernetického incidentu vést k nejasnostem při řešení vzniklé situace a k pomalejší reakci organizace. V kontextu celkových výsledků šetření lze tento výsledek opět spojit s tím, že menší podniky často nepřistupují k řízení kybernetické bezpečnosti systematicky.

Graf č. 13: Má vaše organizace přehled o svých klíčových IT aktivech (systémy, data, služby)?[58]

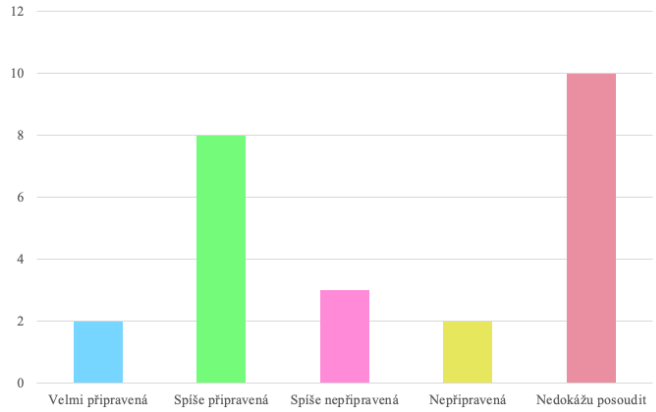


Tato otázka se v rámci provedených rozhovorů zaměřovala na to, zda mají organizace přehled o svých klíčových IT aktivech, tedy o systémech, datech a službách, které jsou pro jejich fungování zásadní. Z odpovědí vyplynulo, že 13 organizací, což

[57] Vlastní zpracování
[58] Vlastní zpracování

představuje 52 % z celkového počtu dotázaných, uvedlo, že má přehled o svých klíčových IT aktivech. Dalších 11 organizací uvedlo, že má přehled alespoň částečný. Pouze jedna organizace uvedla, že takový přehled nemá. Tento výsledek lze hodnotit poměrně pozitivně, protože naznačuje, že většina oslovených podniků má alespoň základní přehled o svých informačních systémech, datech a službách, které jsou pro jejich fungování zásadní.

Graf č. 14: Jak byste celkově zhodnotili připravenost vaší organizace na plnění povinností Zákona o kybernetické bezpečnosti?[59]



Poslední otázka v rámci provedených rozhovorů směřovala k posouzení připravenosti organizací na plnění povinností vyplývajících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Oslovené osoby měly uvést, jak by svou organizaci z hlediska této připravenosti hodnotily. Na tuto otázku odpovídaly všechny oslovené organizace, a to i přesto, že z předchozích odpovědí vyplynulo, že pouze jedna firma poskytuje regulovanou službu. Ostatní podniky tedy odpovídaly z jejich subjektivního a teoretického hodnocení, jak by byly na plnění povinností připraveny v případě, že by se na ně tato právní úprava vztahovala.

Odpovědi na tuto otázku lze hodnotit poměrně pozitivně. Celkem 10 dotázaných uvedlo, že by jejich organizace byla na plnění povinností podle zákona o kybernetické bezpečnosti velmi připravená nebo spíše připravená. Výsledek naznačuje, že firmy vnímají svou úroveň řízení kybernetické bezpečnosti jako dostatečnou a předpokládají, že by byly schopné se případným legislativním požadavkům poměrně dobře přizpůsobit. Dále pouze 5 z dotázaných uvedlo, že jsou spíše nepřipravení anebo nepřipravení. A 10 z dotázaných svou připravenost nedokázali posoudit.

[59] Vlastní zpracování

Diskuze a vyhodnocení výsledků

Výzkumné šetření bylo provedeno formou strukturovaných rozhovorů s celkem 25 podniky, které spadají do kategorie malých a středních podniků. Jednalo se o klienty advokátní kanceláře Mgr. Alexandry Mára Paurové, kteří působí v různých odvětvích podnikatelské činnosti. Rozhovory byly vedeny převážně s jednateli společnostní nebo s osobami ve vedoucích pozicích, které mají přehled o fungování organizace a o jejích povinnostech v oblasti informačních technologií a kybernetické bezpečnosti. Všechny odpovědi byly zpracovány anonymně a získaná data byla následně kvantitativně vyhodnocena a prezentována pomocí grafů.

Výsledky šetření ukazují kolik skutečností, které lze porovnat s teoretickými poznatky uvedeními v předchozích kapitolách práce. Jedním z významných zjištění je to, že část oslovených podniků nemá dostatečné povědomí o nové právní úpravě kybernetické bezpečnosti. Někteří respondenti totiž uvedli, že o novém zákoně č. 264/2025 Sb., o kybernetické bezpečnosti slyšeli pouze okrajově anebo dokonce neslyšeli vůbec. Tento výsledek je překvapivý hlavně s ohledem na to, že právní úprava je účinná již několik měsíců. Odborná literatura přitom zdůrazňuje, že význam kybernetické bezpečnosti v posledních letech rapidně roste a organizace jsou stále více nuceny věnovat této oblasti systematickou pozornost. Autoři zabývající se řízením kybernetické bezpečnosti například uvádějí, že ochrana informačních systémů a dat představuje důležitý předpoklad pro stabilní fungování organizací v digitálním prostředí.

Z odpovědí respondentů také vyplynulo, že mezi organizacemi je relativně nízká znalost standardu ISO/IEC 27001. Pouze menší část z dotázaných uvedla, že se s tímto standardem setkala. Tento výsledek lze do jisté míry považovat za očekávaný, jelikož implementace tohoto standardu není povinná. Na druhou stranu je však norma považována za jeden z nejvýznamnějších mezinárodních rámců pro řízení bezpečnosti informací a může organizacím pomoci při systematickém zavádění bezpečnostních opatření. Nízké povědomí organizací může souviset s tím, že menší podniky často nemají personální ani finanční kapacity pro komplexní řízení kybernetické bezpečnosti.

Výsledky šetření také ukazují, že část oslovených podniků neposuzovala, zda poskytuje regulovanou službu podle zákona o kybernetické bezpečnosti, případně neměla jasnou představu o významu tohoto pojmu. Tento poznatek je poměrně překvapivý, protože právě posouzení poskytování regulované služby je základním krokem při určování rozsahu povinností podle zákona. Zjištění naznačuje, že některé podniky

se nemusí dostatečně orientovat v základních pojmech nové právní úpravy, což samozřejmě může ztěžovat správné vyhodnocení jejich případných povinností.

Specifickým zjištěním výzkumu je také to, že pouze jedna z oslovených organizací poskytuje regulovanou službu ve smyslu zákona o kybernetické bezpečnosti. Tudíž pouze u této jediné organizace bylo možné zkoumat povinnost registrace u NÚKIB. Tato jediná firma uvedla, že spadá do režimu nižších povinností a s procesem registrace u NÚKIB neměla žádné potíže a věděla si s ním rady. Z odpovědí zároveň vyplynulo, že v případě, že by ostatní organizace regulovanou službu poskytovaly, pouze malá část by spadala do režimu nižších či vyšších povinností. Naopak značná část podniků nedokázala posoudit, do kterého režimu by spadaly. Tento fakt naznačuje, že podniky nemají dostatečnou orientaci v nové právní úpravě ani v systému určování jednotlivých režimů povinností.

Pozitivní zjištění je, že většina oslovených podniků má určenou odpovědnou osobu za oblast kybernetické bezpečnosti, a to buď interně nebo prostřednictvím externího dodavatele. Avšak co se týče zpracování postupu pro řešení kybernetického incidentu, tam situace není tak příznivá. Část respondentů sice uvedla, že takový postup mají, avšak u některých organizací nebylo zcela zřejmé, zda je tento postup skutečně formálně zpracován, neboť osoby poskytující odpovědi si nebyly jeho existencí jisté. Absence takového postupu může mít velké následky, protože pokud chybí zpracovaný postup, tak to může vést k nejasnosti, jak se v takovém případě zachovat. Odborné zdroje zdůrazňují, že právě schopnost rychlé a koordinované reakce na bezpečnostní incidenty představuje jeden ze zásadních prvků efektivního řízení kybernetické bezpečnosti.

Zajímavé souvislosti se objevily při porovnání odpovědí týkajících se překážek při naplňování požadavků zákona o kybernetické bezpečnosti a celkového hodnocení připravenosti organizací. Na tuto otázku měly možnost odpovědět všechny organizace, bez ohledu na to, zda poskytují regulovanou službu či nikoliv. U těch, které regulovanou službu neposkytují, což je většina, tak odpovědi odrážely pouze hypotetické vnímání možných problémů, které by podniky mohly při naplňování požadavků pociťovat v případě, že by se na ně tato regulace vztahovala. Jako nejčastější odpověď byl uváděn zejména nedostatek informací a nejasnost samotných legislativních požadavků. Což na pozadí vyplývá i z odpovědí na ostatní otázky. Část firem také uvedla, že přesně neví, jaké konkrétní povinnosti by se na jejich organizaci mohly vztahovat. Celkově tyto odpovědi ukazují, že pro malé a střední podniky nepředstavuje problém samotná

implementace opatření, ale především orientace v legislativním rámci a pochopení praktických dopadů zákona o kybernetické bezpečnosti. Avšak při celkovém zhodnocení připravenosti organizací na plnění povinností dle zákona, a to ať už v podobě čistě teoretické, tak v jednom případě i reálné, se ukázalo, že větší část respondentů považuje svou organizaci za poměrně dobře připravenou, což lze považovat za dobrý výsledek. Ale byly zde i organizace, které vůbec nedokázaly posoudit jejich připravenost.

Celkové výsledky ukazují, že mnoho malých a středních podniků stále vnímá kybernetickou bezpečnost jako problematiku, která se týká především velkých organizací nebo státních institucí. V praxi se často objevuje názor, že menší podniky nejsou pro kybernetické útočníky dostatečně atraktivním cílem. Nedostatečná prevence v konečném důsledku může vést k výrazně vyšším nákladům spojeným s řešením následků kybernetického incidentu, než by stála prevence. Významnou roli může také, ale hrát nedostatek odborníků v oblasti kybernetické bezpečnosti.

Na základě získaných poznatků autorka práce navrhuje několik opatření, která by mohla přispět ke zvýšení souladu malých a středních podniků s legislativními požadavky. Za nejdůležitější lze považovat především zvýšení informovanosti podniků o nové právní úpravě. Informace o povinnostech vyplývajících ze zákona by měly být dostupné v jednoduché a srozumitelné formě, aby jim porozuměli i podnikatelé bez hlubších právních nebo technických znalostí. K tomu mohou přispět například odborné semináře, školení nebo přehledné metodické materiály zaměřené na menší podnikatele. Autorka práce dále doporučuje, aby podniky přistupovaly k otázkám kybernetické bezpečnosti systematičtěji. I menší organizace by měly mít alespoň základně určenou odpovědnou osobu, která bude tuto oblast koordinovat a zjišťovat aktuální novinky. V neposlední řadě může být pro podniky přínosné využívání metodických rámců a standardů pro řízení bezpečnosti informací. Tyto přístupu mohou organizacím pomoci lépe identifikovat bezpečnostní rizika a nastavit vhodná opatření. I když zavedení těchto standardů může být pro menší podniky náročné i nákladné, stále to nebude dosahovat takové míry, jaké by dosahovala obnova po kybernetickém incidentu.

Závěr

Bakalářská práce se zabývala problematikou připravenosti malých a středních podniků na plnění povinností vycházejících ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, prostřednictvím kterého byla implementována směrnice NIS2 do českého právního řádu. Cílem této práce bylo vyhodnotit, jak jsou vybrané podniky připraveni na plnění těchto povinností se zaměřením na proces registrace u NÚKIB a na určení režimu nižších či vyšších povinností.

Na základě provedené rešerše odborné literatury, právních předpisů a výsledků vlastního šetření lze konstatovat, že stanovený cíl práce byl naplněn. Výzkum umožnil vyhodnotit připravenost vybraných malých a středních podniků na plnění povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Samotné podniky se hodnotily jako spíše připravené, pouze malá část z nich se cítila být na plnění povinností zcela nepřipravená. Z celkových výsledků výzkumu autorka práce však vnímá připravenost podniků jako nižší, a to s ohledem např. na skutečnost, že část respondentů uvedla, že se s novým zákonem setkala pouze okrajově, případně se s ním dosud nesetkala vůbec. Tento rozdíl naznačuje, že vnímaná připravenost podniků nemusí vždy plně odpovídat jejich skutečné úrovni připravenosti v praxi.

Teoretická část práce vymezila základní pojmy kybernetické bezpečnosti a představila hlavní evropské a mezinárodní nástroje upravující tuto oblast, zejména pak směrnice NIS, NIS2 a normy řady ISO/IEC 27000. Následně byl popsán vývoj nového zákona o kybernetické bezpečnosti a vybrané povinnosti, které z něj pro regulované subjekty vyplývají, včetně určení režimu povinností a základních bezpečnostních opatření.

Praktická část práce byla zaměřena na zjištění aktuální úrovně informovanosti a připravenosti malých a středních podniků, jakožto klientů vybrané advokátní kanceláře. Výsledky šetření ukázaly, že podniky často nemají dostatek informací o nové právní úpravě ani o tom, jaké povinnosti by se na ně mohly vztahovat pokud by regulovanou službu poskytovaly. Na druhou stranu bylo zjištěno, že některé podniky již mají zavedené alespoň základní prvky řízení kybernetické bezpečnosti, například přehled o svých klíčových IT aktivech anebo že mají určenou osobu odpovědnou za kybernetickou bezpečnost.

Autorka práce se proto domnívá, že jedním ze zásadních kroků ke zvýšení připravenosti podniků by mělo být především zvýšení informovanosti o nové právní úpravě. A to v jednoduché a srozumitelné formě pro každého běžného podnikatele. Přínos této práce spočívá zejména v tom, že poskytuje základní přehled o úrovni informovanosti a připravenosti vybraných malých a středních podniků na novou právní úpravu v oblasti kybernetické bezpečnosti a zároveň poukazuje na oblasti, ve kterých mohou podniky při plnění legislativy požadavků čelit největším obtížím. Získané poznatky mohou být využitelné jak pro samotné podniky, tak pro širokou odbornou veřejnost, která se touto problematikou zabývá.

Seznam použitých zdrojů

Literární zdroje

1. CALDER, A. *ISO 27001/ISO 27002*. IT Governance, 2017. 86 S. ISBN 978-1787784932.
2. DOUCEK, P.; KONEČNÝ, M. a NOVÁK, L. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. 272 S. ISBN 978-80-88260-39-4.
3. EDWARDS, J. a WEAVER, G.. *The Cybersecurity Guide to Governance, Risk, and Compliance*. John Wiley, 2024. 672 S. ISBN 978-1-394-25019-6.
4. HRŮZA, P. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. 90 S. ISBN 978-80-7231-914-5.
5. JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. 93 S. ISBN 978-80-7251-397-0.
6. JIRÁSEK, P.; NOVÁK, L. a POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. 352 S. ISBN 978-80-908388-4-0.
7. KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. 526 S. ISBN 978-80-88168-15-7.
8. KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. 560 S. ISBN 978-80-88168-34-8.
9. NICHOLS, L. *Cybersecurity Architect's Handbook.* De Gruyter GmbH, Walter, 2024. 494 S. ISBN 978-1803235844.
10. NONNEMANN, F.; ČERVENÝ, V. a VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025. 280 S. ISBN 978-80-286-0331-1.
11. PATTISON, A. *DORA: a guide to the EU digital operational resilience act.* Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2024. 107 S. ISBN 978-1-78778-451-2.
12. POLČÁK, R.; HARAŠTA, J. a STUPKA, V. *Právní problémy kybernetické bezpečnosti.* Spisy Právnické fakulty MU (řada teoretická). Brno: Masarykova univerzita, 2016. 270 S. ISBN 978-80-210-8426-1.
13. RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Právní instituty. V Praze: C.H. Beck, 2023. 268 S. ISBN 978-80-7400-931-0.
14. SMEJKAL, V.; SOKOL, T. a KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. 378 S. ISBN 978-80-7380-765-8.

15. SEDLÁK, P. a KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. 440 S. ISBN 978-80-7623-068-2.
16. ŠULC, V. Kybernetická bezpečnost. 2018. 148 S. ISBN 978-80-7380-737-5.
17. WATKINS, S. *Iso/iec 27001: 2022*. IT Governance, 2022. 384 S. ISBN 1787784037.

Elektronické zdroje

1. ČESKÁ NÁRODNÍ BANKA. *DORA – Digitální provozní odolnost finančního trhu*. Online. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/dora-digitalni-provozni-odolnost-financniho-trhu/. [cit. 2026-01-17].
2. ČESKO. *Vyhláška č. 334/2025 Sb. Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/334?zalozka=text. [cit. 2026-03-14].
3. ČESKO. *Vyhláška č. 408/2025 Sb. Vyhláška o regulovaných službách*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/408?zalozka=text. [cit. 2026-03-14].
4. ČESKO. *Vyhláška č. 409/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/409?zalozka=text. [cit. 2026-03-14].
5. ČESKO. *Vyhláška č. 410/2025 Sb. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/410?zalozka=text. [cit. 2026-03-14].
6. ČESKO. *Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti*. Online. Dostupné z: https://www.e-sbirka.cz/sb/2025/264?zalozka=text. [cit. 2026-03-14].
7. DENTONS EUROPE CS LLP. *Za selhání v kyberbezpečnosti ponese osobní zodpovědnost management. Už od listopadu*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/za-selhani-v-kyberbezpecnosti-ponese-osobni-zodpovednost-management-uz-od-listopadu. [cit. 2026-01-18].
8. EXCLUSIVE NETWORKS. *Vypršela lhůta pro registraci regulované služby, hrozí pokuty*. Online. Dostupné z: https://vseonis2.cz/vyprsela-lhuta-pro-registraci-regulovane-sluzby-hrozi-pokuty/. [cit. 2026-01-16].
9. HANZEL, P. *Kyberbezpečnost se stává osobní odpovědností jednatelů*. Online. Dostupné z: https://arws.cz/novinky-v-arrows/kyberbezpecnost-se-stava-osobni-odpovednosti-jednatelu. [cit. 2026-01-17].
10. KRAITA.IO. *Režim vyšších nebo nižších povinností: Kam spadá vaše firma podle nového zákona?* Online. Dostupné z: https://www.kraita.io/blogove-prispevky/rezim-vyssich-nebo-nizsich-povinnosti-kam-spada-vase-firma-podle-noveho-zakona.. [cit. 2026-01-16].

11. KUČÍNSKÝ, A. *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti*. Online. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2025/11/20/videoprenaska-nzkb_uid_691ee0e537a80.pdf. [cit. 2026-01-17].
12. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Portál NÚKIB*. Online. Dostupné z: https://portal.nukib.gov.cz/. [cit. 2026-01-17].
13. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce novým zákonem o kybernetické bezpečnosti*. Online. Dostupné z: https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti.. [cit. 2026-01-19].
14. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce směrnicí NIS2*. Online. Dostupné z: https://portal.nukib.gov.cz/pruvodce-smernici-nis2. [cit. 2026-01-19].
15. UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Směrnice NIS2*. Online. Dostupné z: https://www.utb.cz/kyberneticka-bezpecnost/nis/.. [cit. 2026-01-17].

Seznam zkratek

1. DDoS – Distributed Denial of Service
2. DORA – Digital Operational Resilience Act
3. EU – Evropská unie
4. GDPR – General Data Protection Regulation
5. IKT – informační a komunikační technologie
6. ISMS – Information Security Management Systems
7. NIA – Národní bod pro identifikaci a autentizaci
8. NIS – Network Information Security
9. NIS2 – Network Information Security 2
10. NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

Seznam příloh

Přílohy

Příloha I – Otázky a varianty odpovědí použité při strukturovaných rozhovorech

1. Jak velká je organizace, ve které pracujete?

   a) Mikro (1-9 zaměstnanců)
   b) Malá (10-49 zaměstnanců)
   c) Střední (50-249 zaměstnanců)

2. Jak máte zajištěnu IT správu?

   a) Interní zaměstnanec
   b) Externí dodavatel
   c) Kombinace
   d) Nemáme systematicky řešeno

3. Slyšeli jste o novém zákoně o kybernetické bezpečnosti (ZoKB/NIS2)?

   a) Ano a aktivně ho řešíme
   b) Ano, ale jen okrajově
   c) Pouze jsme o něm slyšeli
   d) Ne

4. Slyšeli jste o směrnici ISO/IEC 27001?

   a) Ano
   b) Ne

5. Posuzovali jste, zda poskytujete regulovanou službu podle ZoKB?

   a) Ano
   b) Ne
   c) Nevíme, co to znamená

6. Posuzovali jste povinnost registrace u NÚKIB?

   a) Ano - vyhodnotili jsme, že máme povinnost
   b) Ano - vyhodnotili jsme, že povinnost nemáme
   c) Ne
   d) Nevíme, jak to zjistit

7. Kdo posouzení provedl?

   a) Interně
   b) Externí poradce (IT/právník)
   c) Kombinace
   d) Neřešili jsme

8. Jak dobře rozumíte procesu registrace u NÚKIB?

   a) Dobře, víme, co dělat
   b) Částečně
   c) Vůbec

9. Víte, do kterého režimu by vaše organizace spadala, pokud by poskytovala regulovanou službu?

a) Nižších povinností
b) Vyšších povinností
c) Nevíme
d) Nespadá ani do jednoho

10. Má vaše organizace určenou osobu odpovědnou za kybernetickou bezpečnost?

a) Ano, interně
b) Ano, externě
c) Ne

11. Co vám nejvíce brání splnit požadavky ZoKB?

a) Nedostatek informací
b) Nejasná legislativa
c) Finance
d) Nedostatek odborníků
e) Časová náročnost
f) Nevíme, co přesně máme splnit
g) Nespadáme do žádného režimu
h) Časová náročnost

12. Má vaše organizace zpracovaný postup pro řešení kybernetického incidentu?

a) Ano
b) Ne
c) Nevím

13. Má vaše organizace přehled o svých klíčových IT aktivech (systémy, data, služby)?

a) Ano
b) Částečně
c) Ne

14. Jak byste celkově zhodnotili připravenost vaší organizace na plnění povinností ZoKB?

a) Velmi připravená
b) Spíše připravená
c) Spíše nepřipravená
d) Nepřipravená
e) Nedokážu posoudit