VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

APLIKACE ZAVEDENÍ SHODY S VYHLÁŠKOU KYBERNETICKÉ BEZPEČNOSTI DO SPOLEČNOSTI

APPLICATION AND DEPLOYMENT OF COMPLIANCE WITH CYBERSECURITY REGULATION INTO COMPANY

ZÁVĚREČNÁ PRÁCE

FINAL THESIS

AUTOR PRÁCE **Mgr. Radek Vymazal**

AUTHOR

VEDOUCÍ PRÁCE **Ing. Petr Sedlák**

SUPERVISOR

BRNO 2025

ZADÁNÍ ZÁVĚREČNÉ PRÁCE

ABSTRAKT

Závěrečná práce se zabývá implementací shody s vyhláškou o kybernetické bezpečnosti ve společnosti působící v různých odvětvích prostřednictvím holdingové struktury.

V první části práce je uveden teoretický rámec problematiky kybernetické bezpečnosti a právních požadavků vyplývajících z vyhlášky o kybernetické bezpečnosti.

Druhá část se zaměřuje na analýzu současného stavu a popisuje samotný proces implementace shody s vyhláškou pomocí softwarového nástroje ESKO-SW.

Závěrečná část obsahuje diskuzi a zhodnocení navržených opatření a komentář k dosaženým výsledkům v kontextu plnění požadavků vyhlášky o kybernetické bezpečnosti.

KLÍČOVÁ SLOVA

NIS2, Zákon o kybernetické bezpečnosti, vyhláška o kybernetické bezpečnosti, shoda s VKB, kritická informační infrastruktura, významné informační systémy.

ABSTRACT

The thesis focuses on the implementation of compliance with the Cybersecurity Decree within a company operating across multiple sectors through a holding structure.

The first part provides a theoretical framework for the issue of cybersecurity and the legal requirements arising from the Cybersecurity Decree.

The second part analyzes the current state and describes the implementation process of compliance using the ESKO-SW software tool.

The final part presents an economic assessment of the proposed measures and a commentary on the achieved results in the context of fulfilling the requirements of the Cybersecurity Decree.

KEYWORDS

NIS2, Cybersecurity Act, Cybersecurity Decree, Compliance with Cybersecurity Requirements, Critical Information Infrastructure, Significant Information Systems.

ROZŠÍŘENÝ ABSTRAKT

Dne 14 prosince 2022 byla publikována směrnice NIS2, která byla transponována do české legislativy, nejdříve do Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a později ji nahradil nový zákon č. 264/2025 Sb. O kybernetické bezpečnosti. Dané kroky představují zásadní změnu v oblasti řízení kybernetické bezpečnosti, neboť zavádí nové povinnosti a postupy pro široký okruh organizací v České republice.

Podle odhadů Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) se nové povinnosti dotknou více než 7 000 subjektů, které budou muset implementovat opatření kybernetické bezpečnosti do svých procesů a infrastruktury. To vytváří významnou společenskou i ekonomickou výzvu a současně otevírá prostor pro vznik podpůrných metodik, nástrojů a aplikací, které mohou organizacím celý proces usnadnit.

Téma této závěrečné práce je proto zaměřeno na analýzu a návrh struktury procesů souvisejících s transpozicí směrnice NIS2 do české legislativy a na aplikaci těchto poznatků ve vybrané společnosti. Z praktického hlediska je cílem ukázat postup, který lze využít nejen u jednoho konkrétního subjektu, ale také jako vzor pro další organizace v České republice a potenciálně i v rámci Evropské unie.

BIBILIOGRAFICKÁ CITACE

VYMAZAL, Radek. Aplikace zavedení shody s vyhláškou kybernetické bezpečnosti do společnosti [online]. Brno, 2025. Závěrečná práce. Vysoké učení technické v Brně, Fakulta, podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená závěrečná práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským). Také prohlašuji, že jsem užil nástrojů generativní inteligence primárně pro výpomoc s opravou stylistických a gramatických chyb při psaní textů. Jednalo se o nástroj ChatGPT a jazykový model GPT-5. Prohlašuji, že veřejně poskytuji dobrovolně část teoretickou, označenou v záhlaví indexem TLP: CLEAR svobodně k šíření a současně oznamuji, že praktická část označená TLP: AMBER je vzhledem ke svému obsahu zakázáno jakkoliv sdílet veřejně z bezpečnostních důvodů. V případě porušení bezpečnosti šíření informací této práce mohou být vymáhané právní důsledky, protože závěrečná práce podléhá smluvní mlčenlivosti.

V Brně dne 17. listopadu 2025

……

podpis studenta

PODĚKOVÁNÍ

Tímto bych chtěl poděkovat Ing. Terezce Tesařové, kolegům studujícím se mnou na oboru MBA, Ing. Petrovi Sedlákovi a ostatním účastníkům, kteří se na realizaci studia spolupodíleli. Drobné poděkování patří i Vildovu atomovému kufříku plném inspirace.

Obsah

1. TEORETICKÁ ČÁST 16

1.1 ÚVOD 16
1.2 ZÁKLADNÍ POJMY KYBERNETICKÉ BEZPEČNOSTI 18
1.2.1 Aktivum 18
1.2.2 Kybernetická bezpečnostní událost 18
1.2.3 Kybernetický bezpečnostní incident 18
1.2.4 Opatření 18
1.2.5 Dopad 18
1.2.6 Dopadové kritérium 19
1.2.7 Hrozba 19
1.2.8 Zranitelnost 19
1.2.9 Kybernetické riziko 19
1.3 EVROPSKÉ SMĚRNICE NIS A NIS2 20
1.3.1 Definice směrnice 20
1.3.2 Směrnice NIS 20
1.3.3 Směrnice NIS2 20
1.3.3.1 Příloha I – Odvětví vysoké kritičnosti 21
1.3.3.2 Příloha II – Další kritická odvětví 23
1.4 OBECNÁ STRUKTURA ZÁKONA 25
1.4.1 Definice zákona 25
1.4.2 Název zákona 25
1.4.3 Úvodní ustanovení 25
1.4.4 Části 25
1.4.5 Hlavy, díly, oddíly a pododdíly 25
1.4.6 Paragrafy (§) 26
1.4.7 Přechodná a závěrečná ustanovení 26
1.4.8 Přílohy 27
1.4.9 Příklad (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti) 27
1.4.10 Rozšířený přehled částí zákona o kybernetické bezpečnosti 27
1.5 OBECNÁ STRUKTURA VYHLÁŠEK 29
1.5.1 Definice vyhlášky 29
1.5.2 Název vyhlášky 29
1.5.3 Úvodní ustanovení 29
1.5.4 Části a hlavy 29
1.5.5 Paragrafy (§) 29
1.5.6 Přílohy 30
1.5.7 Přechodná a závěrečná ustanovení 30
1.5.8 Příklad (Vyhláška č. 82/2018 Sb.) 30
1.6 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI 32
1.6.1 Historický vývoj 32
1.6.2 Významné novelizace ZKB 32

1.6.3 Nový zákon o kybernetické bezpečnosti (nZKB) ... 33
1.6.3.1 Přehled hlavních změn a povinností u nZKB (264/2025 Sb.) ... 34
1.7 VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI (VKB) ... 36
1.7.1 Struktura a přehled VKB ... 36
1.7.2 Technická opatření a příklady implementace ... 38
1.7.3 Rozdílnost mezi ZKB a VKB ... 39
1.7.4 Pojem „shoda s vyhláškou o kybernetické bezpečnosti“ ... 40
1.7.5 Detailnější popis hlavních kroků procesu VKB ... 44
1.8 DEFINICE A VYMEZENÍ VELIKOSTI PODNIKU ... 45
1.8.1 Počet zaměstnanců ... 45
1.8.2 Roční obrat ... 47
1.8.2.1 Ukázka tržeb ... 47
1.8.3 Bilanční suma ... 49
1.8.3.1 Ukázka bilanční sumy ... 49
1.8.4 Tabulka hodnocení velikosti podniku ... 53
1.8.5 Příklad výpočtu velikosti podniku a vliv ekonomického kritéria. ... 54
1.8.6 Příklad výpočtu velikosti podniku a vliv kritéria počtu zaměstnanců ... 55
1.8.7 Struktura dle velikosti podniků ... 56
1.8.7.1 Nezávislý podnik ... 56
1.8.7.2 Příklad nezávislého podniku ... 57
1.8.7.3 Partnerský podnik ... 57
1.8.7.4 Propojený podnik ... 60
1.8.8 Sumace a srovnání rozdílnosti vlastnictví podniků ... 62
1.9 VYHLÁŠKA O REGULOVANÝCH SLUŽBÁCH ... 63
1.9.1 Proces samoidentifikace podle vyhlášky o regulovaných službách ... 65
1.9.2 Srovnání vyšších a nižších režimů a jejich povinností ... 67
1.9.3 Společné povinnosti pro všechny režimy ... 67
1.9.4 Rozdíly v povinnostech mezi oběma režimy ... 68
1.9.5 Hlášení incidentů ... 68
1.9.6 Sankce ... 68
1.10 ISMS ... 71
1.10.1 Definice ISMS ... 71
1.10.2 Celkový proces zavádění ISMS ... 72
1.10.3 Rozsah ISMS ... 74
1.10.4 Politiky (bezpečnostní směrnice) ... 74
1.10.5 Vzájemný vztah a vazba mezi ISMS a VKB ... 75
1.11 DEFINICE AKTIV A JEJICH HODNOCENÍ ... 77
1.11.1 Definice aktiv ... 77
1.11.2 Hodnocení aktiv ... 77
1.11.2.1 Důvěrnost ... 78
1.11.2.2 Integrita ... 78
1.11.2.3 Dostupnost ... 78
1.11.3 Hodnotící atributy aktiv ... 78
1.11.3.1 Tabulka hodnocení dostupnosti ... 79
Výpočet hodnoty aktiva ... 79
1.12 PRIMÁRNÍ AKTIVA ... 81
1.12.1 Obecná charakteristika primárních aktiv ... 81

1.12.2 Identifikace primárních aktiv ... 81
1.12.3 Evidence primárních aktiv ... 82
1.12.4 Hodnocení primárních aktiv ... 82
1.13 PODPŮRNÁ AKTIVA ... 84
1.13.1 Obecná charakteristika podpůrných aktiv ... 84
1.13.2 Kategorizace podpůrných aktiv ... 84
1.13.3 Identifikace podpůrných aktiv ... 85
1.13.4 Evidence podpůrných aktiv ... 85
1.13.5 Hodnocení podpůrných aktiv ... 86
1.13.6 Příklad rozdílu mezi primárním a podpůrným aktivem ... 86
1.14 VAZBY MEZI PRIMÁRNÍMI A PODPŮRNÝMI AKTIVY ... 87
1.14.1 Vzájemná vazba mezi primárními aktivy ... 87
1.14.2 Vazba mezi primárními a podpůrnými aktivy ... 87
1.14.3 Metodika hodnocení vazeb mezi aktivy ... 88
1.15 PRAVIDLA PRO NAKLÁDÁNÍ S AKTIVY ... 90
1.15.1 Různé úrovně opatření pro nakládání s aktivy ... 90
1.15.2 Nakládání s aktivy ... 91
1.16 LIKVIDACE DAT ... 92
1.17 KLASIFIKACE INFORMACÍ ... 93
1.17.1 Traffic Light Protocol (TLP) ... 93
1.17.2 Permissible Actions Protocol (PAP) ... 94
1.17.2.1 Úrovně PAP ... 95
1.17.3 Kombinace TLP a PAP ... 97
1.17.3.1 Příklady kombinovaného použití TLP a PAP ... 98
1.18 ZRANITELNOSTI ... 100
1.18.1 Definice zranitelnosti ... 100
1.18.2 Příčiny zranitelností ... 100
1.18.2.1 Příklady zranitelností z praxe ... 101
1.18.3 Metodika hodnocení zranitelností ... 101
1.18.4 Struktura metrik CVSS ... 101
1.18.4.1 Příklad hodnocení ... 102
1.18.4.2 Klasifikace skóre ... 103
1.18.5 Stupnice hodnocení zranitelností ... 104
1.18.6 Katalog zranitelností ... 104
1.19 HROZBY ... 106
1.19.1 Definice hrozby ... 106
1.19.2 Klasifikace hrozeb dle původu ... 106
1.19.3 Klasifikace hrozeb dle účelu ... 106
1.19.4 Klasifikace hrozeb dle lokality působnosti ... 107
1.19.5 Pravděpodobnost výskytu hrozeb ... 107
1.19.6 Stupnice hodnocení hrozeb ... 108
1.19.7 Risk matrix: kombinace pravděpodobnosti a dopadu ... 109
1.19.8 Katalog hrozeb ... 109
1.20 ANALÝZA A ŘÍZENÍ RIZIK ... 112
1.20.1 Řízení rizik ... 112
1.20.1.1 Definice dopadu ... 112

1.20.1.2 Definice rizika 112
1.20.2 Klasifikace rizik 113
1.20.3 Matice dopadů 113
1.20.3.1 Účel a význam matice dopadů 113
1.20.3.2 Obecná struktura matice dopadů 114
1.20.4 Hodnocení rizik 114
1.20.5 Metodika řízení rizik 115
1.20.6 Kritéria akceptovatelnosti rizik 115
1.20.7 Zpráva z hodnocení rizik 116
1.20.8 Prohlášení o aplikovatelnosti 116
1.20.9 Plán zvládání rizik 117
1.20.10 Zavádění opatření 118
1.21 ŘÍZENÍ KONTINUITY ČINNOSTÍ 120
1.21.1 Definice pojmu 120
1.21.2 Životní cyklus řízení kontinuity 120
1.21.3 Základní požadavky pro řízení kontinuity 121
1.21.4 RTO a RPO 122
1.21.5 Business Continuity Management (BCM) 123
1.21.6 Disaster Recovery (DR) 123
1.21.7 Vizuální schéma rozdílností mezi RTO a RPO 124
1.22 STANOVENÍ BEZPEČNOSTNÍCH ROLÍ 125
1.22.1 Úvod o řízení bezpečnostních rolí 125
1.22.2 Výbor pro řízení kybernetické bezpečnosti 125
1.22.3 Manažer kybernetické bezpečnosti 125
1.22.4 Architekt kybernetické bezpečnosti 126
1.22.5 Auditor kybernetické bezpečnosti 126
1.22.6 Odbor bezpečnostní 127
1.23 RACI MATICE 128
1.23.1 Úvod a obecný základ RACI matice 128
1.23.2 Výhody využití RACI matice 128
1.23.3 Nevýhody využití RACI matice 129
1.23.4 Příklad RACI matice 129
1.24 ŘÍZENÍ DODAVATELŮ 131
1.24.1 Úvod k řízení dodavatelů 131
1.24.2 Povinnosti organizace v oblasti řízení dodavatelů 131
1.24.3 Politika řízení dodavatelů 132
1.24.4 Významný dodavatel a provozovatel 132
1.24.5 Prokazatelné informování dodavatele 132
1.24.6 Obsah smluv s významnými dodavateli 133
1.24.7 Proces řízení dodavatelů 134
1.25 BEZPEČNOST LIDSKÝCH ZDROJŮ 136
1.25.1 Úvod do bezpečnosti lidských zdrojů 136
1.25.2 Plán rozvoje bezpečnostního povědomí 136
1.26 ŘÍZENÍ PROVOZU A KOMUNIKACÍ 138
1.27 ŘÍZENÍ ZMĚN 140

1.28 ŘÍZENÍ PŘÍSTUPŮ (IDENTITY ACCESS MANAGEMENT) 142
1.28.1 Základní principy řízení přístupu 142
1.28.2 Opatření k ochraně přístupů 143
1.28.3 Politika hesel a autentizace 143
1.28.4 Správa a životní cyklus přístupů 144
1.28.5 Privilegované účty a bezpečnostní politika 145
1.29 OCHRANA PŘED ŠKODLIVÝM KÓDEM, ZAZNAMENÁVÁNÍ A DETEKCE UDÁLOSTÍ, ZVLÁDÁNÍ INCIDENTŮ A KRYPTOGRAFIE 146
1.29.1 Ochrana před škodlivým kódem 146
1.29.2 Zaznamenávání událostí, retence a synchronizace času 146
1.29.3 Detekce a vyhodnocování kybernetických událostí 147
1.29.4 Řízení bezpečnostních incidentů 147
1.29.5 Aplikační a síťová bezpečnost 148
1.29.6 Kryptografické prostředky 148
1.30 AUDIT 149
1.30.1 Definice auditu 149
1.30.2 Audit kybernetické bezpečnosti 149
1.31 PDCA CYKLUS 151
1.31.1 Definice pojmu 151
1.31.2 Struktura PDCA cyklu 152
1.31.3 PDCA cyklus v kontextu ISMS 152
1.31.4 Aplikace PDCA cyklu v praxi 153
1.31.4.1 Fáze *Plan* (Plánuj) 153
1.31.4.2 Fáze *Do* (Udělej) 154
1.31.4.3 Fáze *Check* (Zkontroluj) 155
1.31.4.4 Fáze *Act* (Jednej) 155

1. Teoretická část

1.1 Úvod

Kybernetická bezpečnost se v posledních letech stala jedním z nejdiskutovanějších témat nejen v oblasti informačních technologií, ale také ve veřejné správě, kritické infrastruktuře a soukromém sektoru. Rychlý rozvoj digitalizace a závislost organizací na informačních a komunikačních systémech vedou k tomu, že výpadky služeb či úspěšné kybernetické útoky mohou mít závažné dopady nejen ekonomické, ale i společenské a bezpečnostní. Evropská unie proto vydala aktualizovanou směrnici **NIS2** [1], která zásadním způsobem rozšiřuje rámec požadavků na bezpečnost sítí a informačních systémů a zavádí povinnosti pro širší okruh subjektů v rámci Evropské unie. Česká republika směrnici transponovala do národní legislativy prostřednictvím zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen *ZKB*), a prováděcí vyhlášky č. 82/2018 Sb. (dále jen *VKB*). ZKB byl dne 01.11.2025 nahrazen novým zákonem o kybernetické bezpečnosti č. 264/2025 Sb. (Dále jen nZKB).

Teoretická část této práce se proto zaměřuje na podrobnou analýzu a systematické vysvětlení jednotlivých požadavků, které z uvedené legislativy vyplývají se zaměřením na shodu s VKB. Cílem je vytvořit přehledný rámec, jenž umožní pochopit nejen samotné právní požadavky, ale také jejich metodické a praktické naplnění prostřednictvím systému řízení bezpečnosti informací (ISMS). Práce vychází jak z právních předpisů, tak z podpůrných metodických materiálů Národního úřadu pro kybernetickou a informační bezpečnost (dále jen NÚKIB) a z mezinárodních standardů, zejména řady **ISO/IEC 2700***.

Struktura teoretické části je rozdělena do několika na sebe navazujících celků. Nejprve jsou představeny základní pojmy a institucionální rámec kybernetické bezpečnosti v České republice a Evropské unii. Následně je pozornost věnována jednotlivým oblastem definovaným ZKB a VKB, které tvoří páteř povinností pro regulované subjekty. Detailně jsou rozpracovány kapitoly týkající se **řízení aktiv**, **řízení rizik**, **řízení dodavatelů**, **řízení**

kontinuity činností, **zvládání incidentů** či **auditu kybernetické bezpečnosti**. Každá kapitola je doplněna o praktické vysvětlení významu daného požadavku, metodické přístupy k jeho naplnění, související vazby na mezinárodní standardy a nejlepší praxi.

Praktická část se poté věnuje aplikaci teoretických poznatků na jeden konkrétní subjekt v ČR. Závěrečná diskuzní část propojuje jednotlivé oblasti a utváří shrnutí s přihlédnutím k náročnosti realizace, benefitů z nich plynoucích i zátěží vyplývajících z nových opatření spolu s přihlédnutím k ekonomické stránce celé problematiky.

1.2 Základní pojmy kybernetické bezpečnosti

1.2.1 Aktivum

Aktivem se rozumí jakýkoli hmotný nebo nehmotný prvek, který má pro organizaci hodnotu a je nezbytný pro zajištění její činností. Aktivem může být například hardware, software, data, know-how či lidský zdroj [2, § 7 písm. f), g)].

1.2.2 Kybernetická bezpečnostní událost

Kybernetická bezpečnostní událost (KBU) je stav systému, služby nebo sítě, který může naznačovat možné narušení bezpečnostních politik, selhání bezpečnostního opatření nebo jinou neznámou situaci, jež může mít vliv na bezpečnost [2, § 7 odst. 1].

1.2.3 Kybernetický bezpečnostní incident

Kybernetický bezpečnostní incident (KBI) je událost, která má prokazatelný negativní dopad na bezpečnost sítě nebo informačního systému, zejména na její důvěrnost, integritu nebo dostupnost [3, § 7 odst. 2,3].

Může se jednat o:

- Nehodu v informačním systému.
- Formu narušení bezpečnosti a integrity sítě elektronických komunikací.
- Formu narušení bezpečnosti užívané služby.

1.2.4 Opatření

Opatřením se rozumí soubor činností nebo úkolů, jejichž cílem je eliminace nebo zmírnění identifikovaného rizika.

1.2.5 Dopad

Dopad označuje měřitelný efekt, který má dané aktivum, událost nebo opatření na cílové skupiny, organizace či společnost. Dopad může být pozitivní i negativní, přímý nebo nepřímý, krátkodobý i dlouhodobý.

1.2.6 Dopadové kritérium

Dopadové kritérium představuje konkrétní ukazatel, pomocí něhož se hodnotí, zda a v jaké míře bylo daného dopadu dosaženo. Slouží k objektivnímu posouzení výsledků ve vztahu k definovaným cílům.

1.2.7 Hrozba

Hrozbou se rozumí potenciální příčina kybernetické bezpečnostní události nebo incidentu, která může způsobit škodu [2, § 2 písm. e)].

1.2.8 Zranitelnost

Zranitelností se rozumí slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami [2, § 2 písm. p)].

1.2.9 Kybernetické riziko

Kybernetické riziko je možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu [2, § 2 písm. h)].

1.3 Evropské směrnice NIS a NIS2

1.3.1 Definice směrnice

Směrnice (též direktiva) je právní akt Evropské unie, který je závazný pro členské státy z hlediska výsledků, kterých má být dosaženo, přičemž konkrétní forma a prostředky transpozice jsou ponechány na jednotlivých státech. Směrnice je součástí sekundárního práva EU a vychází z cílů stanovených v primárním právu [4].

1.3.2 Směrnice NIS

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (tzv. směrnice NIS) představovala první právní rámec EU v oblasti kybernetické bezpečnosti. Jejím cílem bylo rozvíjet schopnosti v oblasti kybernetické bezpečnosti, zmírňovat hrozby pro informační systémy poskytující základní služby a zajistit kontinuitu jejich fungování [5].

1.3.3 Směrnice NIS2

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (tzv. směrnice NIS2) navazuje na původní směrnici NIS a výrazně rozšiřuje její rozsah.

Hlavní změny oproti NIS zahrnují: [6]

1. Rozšíření okruhu regulovaných subjektů – V případě ČR to zahrnuje více než 7 000 organizací rozdělených na „essential“ a „important entities“.
2. Posílení odpovědnosti managementu – Tedy povinnost vzdělávání a vyšší míra zodpovědnosti vedení organizací.
3. Nové požadavky na hlášení – Možnost dobrovolného hlášení hrozeb, zranitelností a incidentů.

4. Specifické povinnosti pro registrátory domén a infrastrukturu DNS.

5. Důraz na sdílení informací mezi povinnými osobami.

6. Zvýšení sankcí za nedodržení povinností.

V rámci NIS2 je provedeno systematické rozdělení organizací podle odvětví a jejich velikosti. Toto rozdělení je definováno v přílohách I a II směrnice [1, annex I, annex II]:

1.3.3.1 Příloha I – Odvětví vysoké kritičnosti

Tabulka 1: Seznam odvětví vysoké kritičnosti (převzato z [1], annex I])

Sektor	Podsektor	Velké subjekty	Střední subjekty	Malé a mikropodniky
Energetika	Elektřina; teplárenství, plyn, vodík, ropa, včetně poskytovatelů nabíjecích služeb	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Doprava	Letecká, železniční, silniční, námořní	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Bankovnictví	Úvěrové instituce (DORA lex specialis)	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Finanční trhy	Obchodní místa, protistrany EU	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH

	(DORA lex specialis)			
Zdravotnictví	Poskytovatelé zdravotní péče, výzkum léčiv, farmaceutická výroba	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Pitná voda	Poskytovatelé služeb	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Odpadní voda	Pouze pokud tvoří součást hlavní činnosti	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH
Digitální infrastruktura	Poskytovatelé služeb důvěry, DNS, registry domén nejvyšší úrovně	ZÁSADNÍ	ZÁSADNÍ	VÝZNAMNÉ
Veřejná správa	Ústřední orgány státní správy (volitelně i místní)	VÝZNAMNÉ	VÝZNAMNÉ	VÝZNAMNÉ
Vesmír	Provozovatelé pozemní infrastruktury (podle rozhodnutí členských států)	ZÁSADNÍ	VÝZNAMNÉ	MIMO ROZSAH

1.3.3.2 Příloha II – Další kritická odvětví

Tabulka 2: Další kritické odvětví (převzato z [1, annex II])

Sektor	Podsektor	Velké subjekty	Střední subjekty	Malé a mikropodniky
Poštovní a kurýrní služby		VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH
Odpadové hospodářství	Pouze pokud tvoří hlavní ekonomickou činnost	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH
Chemický průmysl	Výroba, distribuce	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH
Potravinářství	Výroba a zpracování potravin ve velkoobchodním a průmyslovém měřítku	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH
Výroba	ICT vybavení, dopravní prostředky, zdravotnické přístroje	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH

Digitální služby	Online tržiště, vyhledávače, sociální sítě	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH
Výzkum	Výzkumné organizace (volitelně i vzdělávací instituce)	VÝZNAMNÉ	VÝZNAMNÉ	MIMO ROZSAH

Členské státy měly transpoziční lhůtu 21 měsíců na zapracování směrnice NIS2 do své legislativy. S účinností od 16. ledna 2023 se NIS2 stala impulsem pro aktualizaci českého zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a vedla ke vzniku jeho nové verze, Zákona č. 264/2025 Sb. [7]. Tato nová verze byla dne 26. června 2025 podepsána prezidentem ČR s předpokládanou účinností od 1. listopadu 2025 [8].

1.4 Obecná struktura zákona

1.4.1 Definice zákona

Zákon je právní předpis nejvyšší právní síly po Ústavě, vydávaný Parlamentem České republiky, který upravuje základní společenské vztahy a je závazný pro všechny subjekty na území státu [9].

Každý zákon jako právní předpis musí splňovat požadavky stanovené v **Legislativních pravidlech vlády** [10]. Struktura zákona není nahodilá, ale je systematicky rozčleněna do hierarchických jednotek, které mají usnadnit orientaci, čtení i praktickou aplikaci předpisu.

1.4.2 Název zákona

Název zákona vždy obsahuje označení právního předpisu, jeho číslo ve Sbírce zákonů a stručnou charakteristiku obsahu. Typickým příkladem je **„Zákon č. 181/2014 Sb., o kybernetické bezpečnosti“**. V praxi se běžně používají i zkrácené názvy, které se následně užívají v textu práce či odborné literatury (např. „Zákon o kybernetické bezpečnosti“ nebo „ZKB“).

1.4.3 Úvodní ustanovení

Úvodní ustanovení zákona vymezují účel, cíl a rámec právní úpravy. Tyto ustanovení zpravidla obsahují i definici základních pojmů, na něž se dále odkazuje v dalších částech zákona. Tím vytvářejí základní interpretační rámec celého předpisu.

1.4.4 Části

Části představují nejvyšší organizační jednotku zákona. Každá část se věnuje určité oblasti regulace, například obecným ustanovením, právům a povinnostem, procesním otázkám, sankcím či změnám jiných právních předpisů.

1.4.5 Hlavy, díly, oddíly a pododdíly

V rámci částí může být struktura dále členěna na hlavy, díly, oddíly a pododdíly. Toto členění slouží k systematickému seskupování paragrafů podle tematických okruhů.

- **Hlavy** – seskupují paragrafy k určité oblasti (např. bezpečnostní opatření, incidenty, kontrolní mechanismy).
- **Díly** – umožňují detailnější tematické členění uvnitř hlav.
- **Oddíly a pododdíly** – slouží pro ještě jemnější rozdělení a zpřehlednění právní úpravy.

Použití této vyšší granularity závisí na rozsahu a složitosti zákona. U jednodušších předpisů se tyto nižší úrovně nemusí uplatnit.

1.4.6 Paragrafy (§)

Paragrafy tvoří základní normativní jednotku zákona. Každý paragraf je označen symbolem „§“ a pořadovým číslem. Obsahují jednotlivé právní normy a ty mohou být dále členěny na:

- **odstavce** (číslované v závorkách – (1), (2), …),
- **body** (číslované arabskými čísly – 1., 2., …),
- **písmena** (označené abecedně – a), b), …).

Tento systém členění umožňuje jednoznačně citovat konkrétní ustanovení.

1.4.7 Přechodná a závěrečná ustanovení

Součástí většiny zákonů jsou přechodná a závěrečná ustanovení. Přechodná ustanovení stanovují pravidla pro aplikaci zákona na situace, které vznikly ještě před jeho účinností, zatímco závěrečná ustanovení určují den nabytí účinnosti a vymezují, které právní předpisy nebo jejich části se ruší.

1.4.8 Přílohy

Pokud je to nezbytné, zákon může obsahovat i přílohy. Ty tvoří jeho nedílnou součást a obsahují zejména technické detaily, tabulky, seznamy nebo metodické postupy.

1.4.9 Příklad (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti)

Pro ilustraci je zde uváděn zjednodušený přehled struktury první části zákona:

- **ČÁST PRVNÍ – Kybernetická bezpečnost**
- *Hlava I – Základní ustanovení*
    - § 1 – Předmět úpravy
    - § 2–3 – Vymezení pojmů
    - § 3a – Zástupce poskytovatele digitálních služeb
- *Hlava II – Systém zajištění kybernetické bezpečnosti*
    - § 4–6a – Bezpečnostní opatření
    - § 7–8 – Kybernetická bezpečnostní událost a incident

Tento příklad ukazuje, jak systematické členění umožňuje přehlednou orientaci a současně usnadňuje praktickou aplikaci zákona.

1.4.10 Rozšířený přehled částí zákona o kybernetické bezpečnosti

Níže v tabulce 3 je konkrétní ukázka struktury členění ZKB.

Tabulka 3: Struktura členění ZKB

Část	Paragrafy	Popis
ČÁST PRVNÍ	§ 1–§ 33	Kybernetická bezpečnost: předmět úpravy, definice pojmů, povinné subjekty, bezpečnostní opatření, události a incidenty, reaktivní opatření aj.
ČÁST DRUHÁ	§ 34	**Zrušeno**.
ČÁST TŘETÍ	§ 35	Změny souvisejících zákonů (např. zákon o elektronických komunikacích).
ČÁST ČTVRTÁ	§ 36	**Zrušeno**.
ČÁST PÁTÁ	§ 37	Změny souvisejících zákonů (např. zákon o provozování rozhlasového a televizního vysílání).
ČÁST ŠESTÁ	§ 38	Účinnost.

Z původně širšího členění byly i některé části zrušeny, jak je vidět v tabulce 4.

Tabulka 4: Části zrušené ze ZKB

Část	Změna
Druhá část	§ 34 zrušen
Čtvrtá část	§ 36 zrušen

Pouze první část je dále systematicky členěna do hlav, které tematicky seskupují příslušná ustanovení.

1.5 Obecná struktura vyhlášek

1.5.1 Definice vyhlášky

Vyhlášky jsou právní předpisy podzákonné povahy. Vydávají je orgány výkonné moci na základě a v mezích zákona. Slouží k provedení zákona a konkretizují jeho ustanovení [9].

Vyhláška je právní předpis **nižší** právní síly než zákon a je vydávaný například ministerstvem nebo správním orgánem na základě zmocnění v zákoně. Stanovuje podrobnosti k jeho provedení, které je závazné na celém území České republiky. Typické části vyhlášek v rámci struktury jsou podobné zákonům. Obsahují:

1.5.2 Název vyhlášky

Název zpravidla uvádí vydavatele (např. „Ministerstvo vnitra“), číslo ve Sbírce zákonů a stručný obsah (např. „Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních…“).

1.5.3 Úvodní ustanovení

Tato část vymezuje předmět úpravy, základní pojmy a rámec působnosti. Často obsahuje i odkazy na zákon, na jehož základě byla vyhláška vydána.

1.5.4 Části a hlavy

U rozsáhlejších vyhlášek je text rozdělen do částí a hlav, přičemž každá se zaměřuje na určitou oblast (např. organizační opatření, technická opatření, proces hlášení incidentů).

1.5.5 Paragrafy (§)

Základní stavební jednotku vyhlášek tvoří paragrafy označené symbolem „§“ a pořadovým číslem. Tyto paragrafy mohou být podobně jako u zákonů dále členěny na:

- **odstavce** – (1), (2), …
- **body** – 1., 2., …

- **písmena** – a), b), …
- **Přílohy**

1.5.6 Přílohy

obsahují zejména technické detaily, tabulky, vzory dokumentů nebo metodické postupy. Jsou nedílnou součástí vyhlášky.

1.5.7 Přechodná a závěrečná ustanovení

Přechodná ustanovení stanovují lhůty a podmínky pro zavedení nových požadavků, zatímco závěrečná ustanovení určují účinnost vyhlášky a mohou obsahovat i zrušovací klauzule k předchozím předpisům.

1.5.8 Příklad (Vyhláška č. 82/2018 Sb.)

Struktura vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních [2] může sloužit jako typická ukázka. Její obsah je následující:

- **ČÁST PRVNÍ – Úvodní ustanovení**
- § 1 – Předmět úpravy
- § 2 – Vymezení pojmů
- **ČÁST DRUHÁ – Organizační a technická opatření**
- Hlava I – Organizační opatření (§ 3–16)
- Hlava II – Technická opatření (§ 17–29)
- **ČÁST TŘETÍ – Dokumentace a hlášení** (§ 30–32)
- **ČÁST ČTVRTÁ – Reaktivní opatření a kontakty** (§ 33–34)

- **ČÁST PÁTÁ – Přechodná a závěrečná ustanovení** (§ 35–37)

1.6 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen **ZKB**) [3], představuje základní právní rámec kybernetické bezpečnosti v České republice. Zákon vymezuje povinné subjekty, stanovuje jejich práva a povinnosti, určuje působnost a pravomoci orgánů veřejné moci a vytváří základ pro prováděcí předpisy.

Zákon o kybernetické bezpečnosti byl přijat dne 23. července 2014 a nabyl účinnosti 1. ledna 2015.

1.6.1 Historický vývoj

Počátky systematického řešení kybernetické bezpečnosti v ČR sahají do roku 2011, kdy vláda přijala **Strategii kybernetické bezpečnosti České republiky na období 2012–2015** [11]. Protože v té době neexistovala instituce odpovědná za tuto oblast, bylo usnesením vlády č. 781 ze dne 19. října 2011 [12] stanoveno, že gestorem problematiky se stane **Národní bezpečnostní úřad (NBÚ).** Stejným usnesením byla zřízena **Rada pro kybernetickou bezpečnost** a založeno **Národní centrum kybernetické bezpečnosti (NCKB)**.

Na základě těchto kroků byl přijat ZKB, který vytvořil první ucelený legislativní rámec v oblasti kybernetické bezpečnosti v České republice.

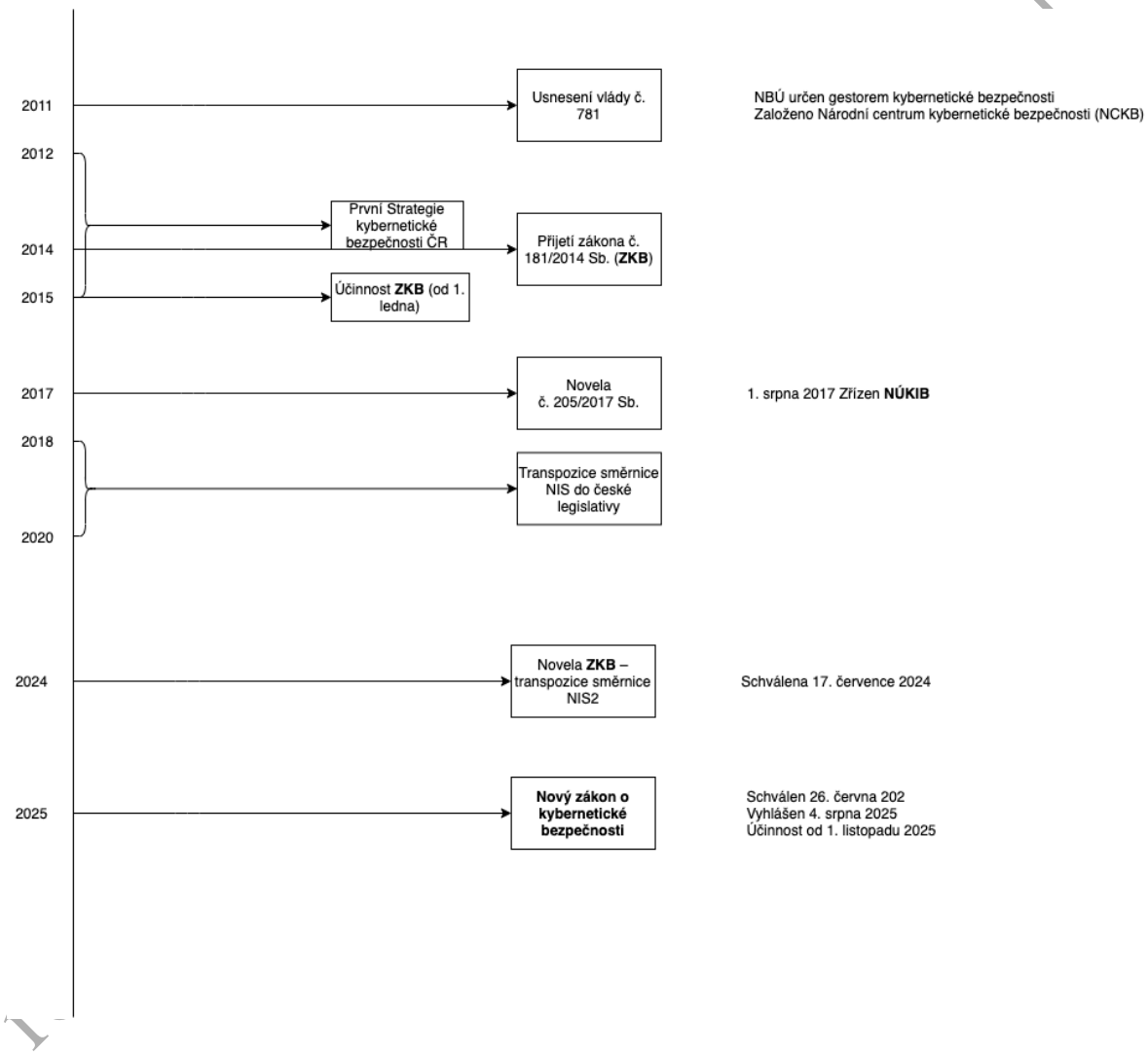
1.6.2 Významné novelizace ZKB

V rámci různých aktualizací v průběhu času vznikla takto časová osa, která mapuje různé novelizace v čase:

1. **Vznik NÚKIB** – Dne 1. srpna 2017 vstoupil v účinnost zákon č. 205/2017 Sb.[13], který zřídil **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)** jako ústřední správní orgán v oblasti kybernetické bezpečnosti [14].

2. **Transpozice směrnice NIS** – Novela ZKB provedla zapracování evropské směrnice NIS (2016/1148/EU) [5] do české legislativy.

3. **Transpozice směrnice NIS2** – V roce 2024 byla přijata novela ZKB, která implementovala směrnici NIS2 [1]. Novelu Poslanecká sněmovna schválila dne 17. července 2024 a později byl zákon přijat dne 23. července 2024 a nabyl účinnosti 1. ledna 2025. Níže je na obrázku 1 dodáno granulární rozkreslení jednotlivých změn v čase.



Obrázek 1: Časová osa vývoje ZKB

1.6.3 Nový zákon o kybernetické bezpečnosti (nZKB)

V návaznosti na aktualizaci směrnice NIS2 byl přijat nový zákon o kybernetické bezpečnosti (nZKB) [7], který představuje zásadní aktualizaci původního rámce. Tento zákon byl

schválen Parlamentem ČR a podepsán prezidentem dne 26. června 2025 a vyhlášen ve Sbírce zákonů 4. srpna 2025. Jeho nabytí účinnosti je od 1. listopadu 2025. nZKB reflektuje nové požadavky vyplývající z NIS2 a klade důraz na vyšší odpovědnost vedení organizací, širší okruh regulovaných subjektů a výrazně přísnější sankce.

1.6.3.1 Přehled hlavních změn a povinností u nZKB (264/2025 Sb.)

Ze zkoumání zákona lze konstatovat, že v obecné rovině jsou následující změny:

1. **Rozšíření** působnosti nZKB na více subjektů (například oblast digitálních služeb a digitální infrastruktury).
2. **Upřesnění** nebo zjednodušení některých pojmů či procesů (Například jasná definice vyšší a nižší povinnosti, s opatřeními, které jsou povinna k aplikací. Také je upřesněna definice velikosti podniku).
3. **Konsolidace** problematiky mechanismu k prověřování dodavatelského řetězce.

Mezi přehled hlavních povinnosti dle NÚKIBu [15] patří povinnosti popsané detailněji v tabulce č. 5.

Tabulka 5: Přehled hlavních povinností dle NÚKIBu [15]

Povinnost	Vysvětlení
Ohlášení regulované služby	Subjekt poskytující regulovanou službu má povinnost ji ohlásit NÚKIB. Termín: do 60 dnů od naplnění podmínek prostřednictvím Portálu NÚKIB. Výstup je rozhodnutí o registraci.
Hlášení kontaktních a dalších údajů	Subjekt musí poskytnout aktuální kontaktní a další údaje. Termín je do 30 dnů od rozhodnutí o registraci prostřednictvím Portálu NÚKIB.

Stanovení rozsahu řízení kybernetické bezpečnosti	Organizace určí primární a podpůrná aktiva spojená s regulovanou službou. Pokud rozsah nestanoví, regulace se vztahuje na celou organizaci.
Zavádění bezpečnostních opatření	Subjekt musí zavést opatření podle režimu (vyšší/nižší) do 1 roku od rozhodnutí o registraci začít implementovat.
Hlášení kybernetických bezpečnostních incidentů	Organizace musí hlásit incidenty odpovědným orgánům do 1 roku od rozhodnutí o registraci přes Portál NÚKIBu. Vyšší režim se hlásí NÚKIBu, nižší režim pak Národnímu CERT.
Informování zákazníků o incidentech a hrozbách	Regulovaná organizace může informovat zákazníky o významných incidentech/hrozbách. NÚKIB může uložit povinnost nebo zákaz informovat dle okolností.
Provádění protiopatření vydaných NÚKIB	Organizace musí reagovat na výstrahy, varování a reaktivní opatření vydané NÚKIBem a to ihned dle lhůty v opatření. Ohlášení se provádí přes Portál, pokud není stanoveno jinak.
Povinnosti z mechanismu bezpečnosti dodavatelských řetězců	Poskytovatelé strategicky významných služeb musí prověřovat své dodavatele bezpečnostně významných dodávek a to do 1 roku od označení služby za strategicky významnou.
Zajištění dostupnosti strategicky významné služby z ČR	Strategicky významné služby musí být dostupné z území ČR v nezbytném rozsahu, čase a kvalitě a to do 1 roku od označení služby za strategicky významnou.

1.7 Vyhláška o kybernetické bezpečnosti (VKB)

Vyhláška č. 82/2018 Sb**.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a o likvidaci dat (dále jen **VKB**) [2], představuje prováděcí předpis k zákonu o kybernetické bezpečnosti. Jejím účelem je detailně specifikovat technické a organizační požadavky, které musí regulované subjekty implementovat pro naplnění zákonných povinností.

VKB rozlišuje dvě hlavní kategorie opatření:

1. organizační (§ 3–16).
2. technická (§ 17–29).

Organizační opatření se zaměřují na řízení informační bezpečnosti na úrovni procesů a odpovědností.

Technická opatření určují minimální standard zabezpečení informačních a komunikačních systémů.

Cílem VKB je zavést jednotný postup řízení kybernetické bezpečnosti, který je přezkoumatelný a prokazatelný při výkonu dozoru ze strany NÚKIBu.

1.7.1 Struktura a přehled VKB

Níže, tabulka 6 popisuje strukturu vyhlášky spolu s popisem podstaty obsahu dané části.

Tabulka 6: Přehled struktury VKB

ČÁST	HLAVA	PARAGRAF	NÁZEV	OBSAH/PODSTATA
ČÁST PRVNÍ		§ 1–2	Předmět úpravy a	Vymezuje účel vyhlášky, rámec její působnosti a základní terminologii (např.

			vymezení pojmů	aktivum, hrozba, riziko, ISMS).
ČÁST DRUHÁ	**HLAVA I**	§ 3–16	Organizační opatření	Požadavky na ISMS, řízení aktiv a rizik, organizační bezpečnost, stanovení rolí a odpovědností, správu dodavatelů, lidských zdrojů, provozu a komunikace, řízení změn a audity.
	HLAVA II	§ 17–29	Technická opatření	Požadavky na fyzickou bezpečnost, bezpečnost sítí, správu identit a přístupů, detekci a reakci na incidenty, kryptografii, zajištění dostupnosti, ICS/OT systémy a digitální služby.
ČÁST TŘETÍ	**HLAVA III**	§ 30–32	Dokumentace a hlášení	Obsahuje pravidla pro zpracování dokumentace, kategorizaci incidentů a formální požadavky na jejich hlášení.
ČÁST ČTVRTÁ		§ 33–37	Reaktivní opatření, kontakty, přechodná ustanovení	Upravuje povinnosti při zavádění reaktivních opatření, požadavky na kontaktní údaje, přechodná ustanovení a účinnost vyhlášky.

1.7.2 Technická opatření a příklady implementace

V následující tabulce 7 jsou ilustrována vybraná technická opatření, jejichž provedení se odvíjí od konkrétního kontextu organizace a výsledků analýzy rizik:

Tabulka 7: Vybraná technická opatření z VKB

§	Název	Příklady technických opatření
17	Fyzická bezpečnost	Perimetrická ochrana, zamykatelné racky, kontrola vstupu, kamerové systémy, evidence a audit fyzického přístupu.
18	Bezpečnost komunikačních sítí	Segmentace sítě (VLANy), firewall s inspekcí stavů, užití DMZ a řízení komunikace mezi nimi.
19	Správa a ověřování identit	Centrální adresář (např. Active Directory), správa identit a přístupů (IAM), vícestupňová autentizace, bezpečná správa hesel.
20	Řízení přístupových oprávnění	Princip nejmenších oprávnění, role-based access control (RBAC), pravidelné obnovy a audity přístupů, just-in-time přístupy.
21	Ochrana před škodlivým kódem	Antiviry, EDR, řízení aktualizací, sandboxing, filtrování e-mailové a webové komunikace.
22	Zaznamenávání událostí IKS	Centralizované logování, synchronizace času, uchování a ochrana integrity logů, SIEM s detekčními scénáři.
23	Detekce kybernetických bezpečnostních událostí	IDS/IPS, síťová detekce anomálií, DLP nástroje.

24	Sběr a vyhodnocování kybernetických bezpečnostních událostí	SOC procesy, automatizace reakce (SOAR), metriky účinnosti, eskalační mechanismy.
25	Aplikační bezpečnost	Bezpečný vývojový cyklus, testování (SAST, DAST, IAST), code review, penetrační testy, ochrana proti OWASPs Top 10 hrozbám.
26	Kryptografické prostředky	Správa životního cyklu klíčů, šifrování dat, správa a obnova certifikátů uživatelů, serverových, přístupových.
27	Zajišťování dostupnosti informací	Redundance kritických komponent, zálohování a pravidelná obnova, HA/DR architektury, testy kontinuity.
28	Digitální služby	Specifické povinnosti pro poskytovatele digitálních služeb, včetně hlášení incidentů a aktualizace kontaktních údajů.

1.7.3 Rozdílnost mezi ZKB a VKB

Zákon o kybernetické bezpečnosti (ZKB) a Vyhláška o kybernetické bezpečnosti (VKB) představují vzájemně provázané, avšak hierarchicky odlišné právní předpisy. **ZKB** stanovuje základní rámec, obecné zásady a povinnosti v oblasti kybernetické bezpečnosti. Na něj navazuje **VKB** jako prováděcí právní předpis, který tato pravidla rozvádí do konkrétní podoby organizačních a technických opatření, lhůt, postupů a dokumentačních požadavků.

Následující tabulka 8 shrnuje klíčové rozdíly mezi těmito dvěma předpisy:

Tabulka 8: Klíčové rozdíly mezi ZKB a VKB

Zákon o kybernetické bezpečnosti (ZKB/nZKB)	**Vyhláška o kybernetické bezpečnosti (VKB)**
Stanovuje obecné zásady a rámec kybernetické bezpečnosti, včetně působnosti a povinností regulovaných subjektů.	Konkretizuje, jak mají být tyto povinnosti plněny prostřednictvím technických a organizačních opatření.
Má vyšší právní sílu – je přijímán Parlamentem a vyhlašován ve Sbírce zákonů.	Má nižší právní sílu – je vydáván správním orgánem (NÚKIB) jako prováděcí předpis.
Určuje „co“ musí povinné subjekty zajistit (např. povinnost zavést bezpečnostní opatření, hlásit incidenty).	Specifikuje „jakým způsobem“ se mají povinnosti plnit (např. detailní postupy hlášení incidentů, lhůty, technické a organizační standardy).
Vymezuje pravomoci orgánů veřejné moci, zejména NÚKIB.	Stanovuje detailní požadavky, které regulované subjekty musí implementovat v praxi.

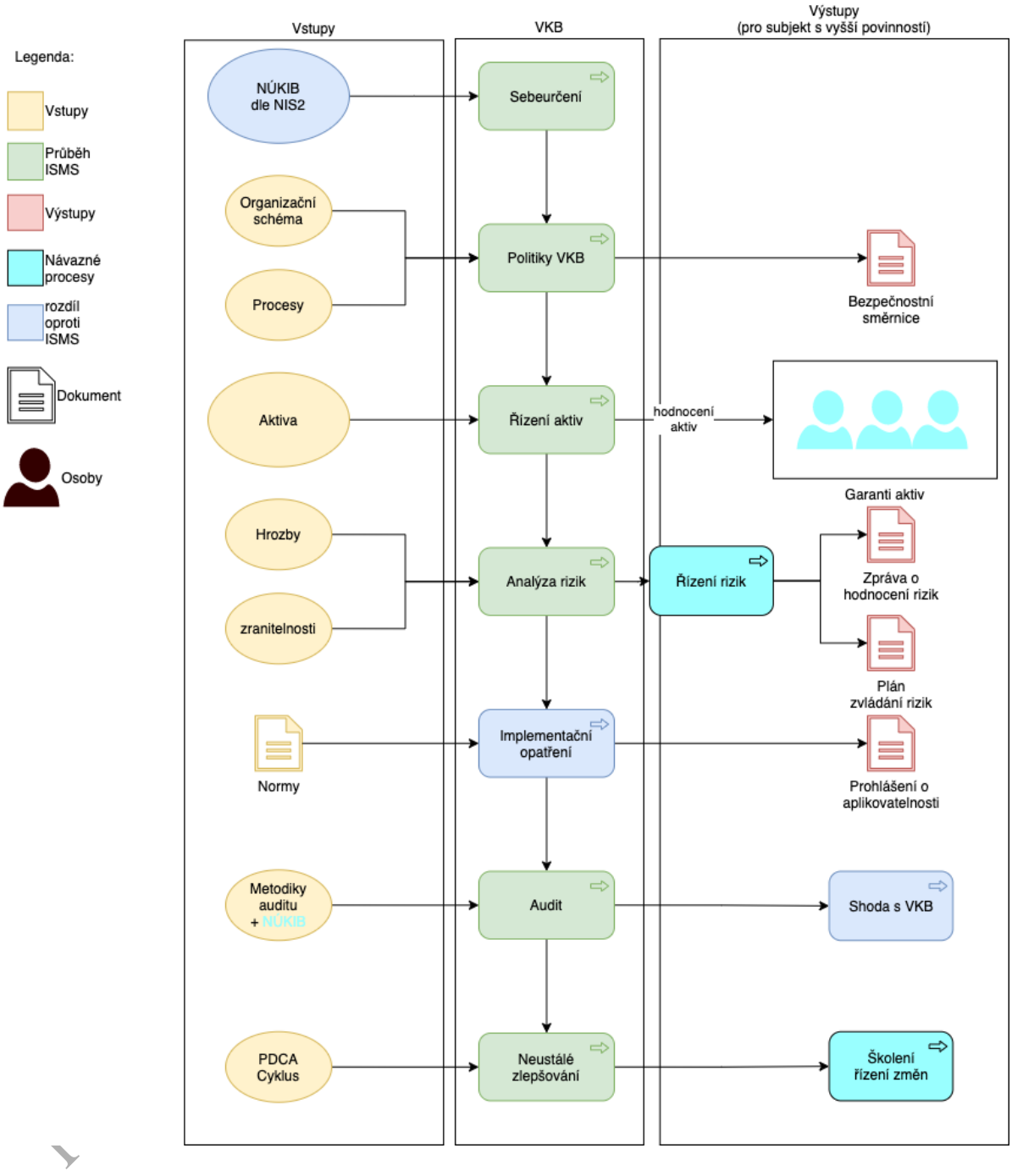
1.7.4 Pojem „shoda s vyhláškou o kybernetické bezpečnosti“

Shoda s vyhláškou o kybernetické bezpečnosti (VKB) představuje stav, kdy organizace prokazatelně splňuje všechny povinnosti stanovené vyhláškou č. 82/2018 Sb., vydanou na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB).

Jinými slovy, „shoda s VKB“ znamená, že organizace implementovala, dokumentovala a udržuje bezpečnostní opatření, která jsou závazná pro správu a provoz informačních a komunikačních systémů podle § 4 ZKB — tedy zejména systém řízení bezpečnosti informací

(ISMS), bezpečnostní role, řízení rizik, ochranu aktiv, lidské zdroje, provoz, přístupy, dodavatele, incidenty a další oblasti.

Následující obrázek 2 proto ilustruje hlavní procesní linku kroků vedoucích k implementaci požadavků VKB. Vizualizuje vstupy, výstupy a celkový průběh. Tento průběh byl v komerční podobě autorem této práce zpracován v samostatnou webovou prezentaci dostupnou pod https://nukibator.cz [16].



Obrázek 2: Schéma procesu VKB

Legenda k obrázku 2:

- **Vstupy** (žlutě): Jedná se o podklady z organizace (organizační schéma, procesy, seznam aktiv, hrozby, zranitelnosti), externí požadavky (od NÚKIBu, plynoucí z norem, metodiky auditu, PDCA cyklu).

- **VKB (proces)** (zeleně/modře): Jedná se o vlastní implementační kroky, tedy *sebeurčení, Stanovení politik VKB, Řízení aktiv, Analýzu rizik, Implementační opatření, Audit, Neustálé zlepšování,* a to včetně *Řízení rizik* jako průřezové činnosti.

- **Výstupy** (červeně): to jsou dokumenty a výsledky, tedy *bezpečnostní směrnice, garanti aktiv, zpráva o hodnocení rizik, plán zvládání rizik, prohlášení o aplikovatelnosti, školení a řízení změn.*

1.7.5 Detailnější popis hlavních kroků procesu VKB

Shoda s VKB je nejdůležitější pojem a proto je popisována detailněji v tabulce 9.

Tabulka 9: Detailnější popis kroků realizace shody s VKB

Krok	Popis
Sebeurčení	Subjekt na základě požadavků NÚKIB a kritérií transponované směrnice NIS2 identifikuje svou roli a povinnosti v oblasti kybernetické bezpečnosti. Provede nahlášení NÚKIBu.
Politiky VKB	Na základě organizační struktury a procesů se stanovují cíle, zásady a postupy řízení bezpečnosti. Politiky vytvářejí rámec pro implementaci opatření.
Řízení aktiv	Probíhá systematická identifikace, evidence a hodnocení aktiv. Významnou roli hrají garanti aktiv, kteří nesou odpovědnost za správu a bezpečnost. Hodnocení probíhá podle atributů CIA (důvěrnost, integrita, dostupnost).
Analýza rizik a řízení rizik	Na základě hrozeb a zranitelností se provádí analýza rizik. Výstupem je zpráva o hodnocení rizik a rozhodnutí o přijetí, snížení, přenesení nebo odmítnutí rizika. Navazuje na implementaci opatření.
Implementační opatření	Provádí se zavedení opatření dle katalogu VKB s cílem adresovat rizika identifikovaná v analýze. Tento proces je právě označován jako **„splnění shody s VKB“.**
Audit a neustálé zlepšování	Pravidelný audit prověřuje plnění povinností a efektivitu opatření. Proces neustálého zlepšování (PDCA) umožňuje průběžně adaptovat systém na měnící se podmínky v čase.

1.8 Definice a vymezení velikosti podniku

Vymezení velikosti podniků vychází z **Doporučení Komise 2003/361/ES** ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků [17]. Na toto doporučení navázalo **Ministerstvo průmyslu a obchodu** vyhlášením českého znění definice ze dne 5. ledna 2023 [18] takto:

> „Podnikem se rozumí každý subjekt vykonávající hospodářskou činnost bez ohledu na právní formu, tedy včetně osob samostatně výdělečně činných.“ [18 strana 4.]

Velikost podniku se posuzuje podle tří klíčových ukazatelů:

1. Počet zaměstnanců
2. Roční obrat
3. Bilanční suma

1.8.1 Počet zaměstnanců

Počet zaměstnanců udává, kolik pracovníků podnik zaměstnával v posuzovaném účetním období. Základní jednotkou je pracovník na **hlavní pracovní poměr** po celé období (FTE). U osob, které nepracovaly na plný úvazek či po celé období, je nutné **poměrné převedení** (částečné úvazky, DPČ, DPP, sezónní práce, nástupy/odchody). Do počtu se **započítávají** i vlastníci/společníci, pokud funkci vykonávají. Působí-li vlastnící/společníci ve více propojených či partnerských podnicích, započítají se pouze jednou.

Příklad výpočtu (rok 2019):

Rok 2019 měl 251 pracovních dnů, standardní pracovní doba je 8 hodin denně, tj.:

2008 hod./zaměstnanec/rok

10 zaměstnanců na HPP po celý rok:

$$10 \times 100\% = 10 \text{ FTE}$$

1 zaměstnanec od 1. 1. do 30. 6. (124 dní = 992 hod.):

$$x = \frac{992}{2008} \times 100\% \approx 49{,}4\%$$

1 zaměstnanec od 1. 1. do 30. 4. (664 hod.):

$$x = \frac{664}{2008} \times 100\% \approx 33\%$$

2 zaměstnanci na 0,5 úvazku po celý rok:

$$2 \times 50\% = 1 \text{ FTE}$$

1 zaměstnanec na DPP (300 hod. za rok):

$$x = \frac{300}{2008} \times 100\% \approx 15\%$$

1 zaměstnanec na DPČ (15 hod./týden, 52 týdnů):

$$780 \text{ hod.} = 52 \times 15$$

$$x = \frac{780}{2008} \times 100\% \approx 38{,}8\%$$

1 majitel vykonávající funkci statutárního orgánu:

$$+1 \text{ FTE}$$

Součet:

$$10 + 0{,}49 + 0{,}33 + 1 + 0{,}15 + 0{,}38 + 1 = 13{,}35 \text{ FTE}$$

V uvedeném příkladu podnik spadá do kategorie **malý podnik**.

1.8.2 Roční obrat

Roční obrat představuje celkový objem peněžních prostředků, které podnik získá z prodeje zboží a služeb za dané účetní období. V účetních výkazech se obvykle uvádí v položce **„Čistý obrat za účetní období“** (v tisících Kč).

1.8.2.1 Ukázka tržeb

Společnost **SATOS Prostějov a.s.** ve výroční zprávě za rok 2023 [19] uvádí ve výkazu zisků a ztrát (k 31. 12. 2023) žlutým označením řádku č. 56 v bilanční rozvaze u obrázku 4, kde výpočet čistého obratu vychází i z hodnot z obrázku 3 následujícím způsobem:

$$\text{Čistý obrat za účetní období} = I. + II. + III. + IV. + V. + VI. + VII. = 144346 \text{ tis. Kč}$$

Označení a	TEXT b	Číslo řádku c	Skutečnost v účetním období běžném 1	Skutečnost v účetním období minulém 2
I.	**Tržby z prodeje vlastních výrobků a služeb**	01	**819**	**451**
II.	**Tržby za prodej zboží**	02	**142 449**	**142 793**
A.	**Výkonová spotřeba (ř. 04 + 05 + 06)**	03	**95 417**	**88 874**
1.	Náklady vynaložené na prodané zboží	04	85 276	78 561
2.	Spotřeba materiálu a energie	05	1 307	1 260
3.	Služby	06	8 834	9 053
B.	**Změna stavu zásob vlastní činnosti (+/-)**	07		
C.	**Aktivace (-)**	08		
D.	**Osobní náklady (ř. 10 + 11)**	09	**11 143**	**11 137**
1.	Mzdové náklady	10	8 213	8 309
2.	Náklady na sociální zabezpečení, zdravotní pojištění a ostatní náklady (ř. 12 + 13)	11	2 930	2 828
2. 1	Náklady na sociální zabezpečení a zdravotní pojištění	12	2 646	2 515
2. 2	Ostatní náklady	13	284	313
E.	**Úpravy hodnot v provozní oblasti (ř. 15 + 18 + 19)**	14	**410**	**695**
1.	Úpravy hodnot dlouhodobého nehmotného a hmotného majetku (ř. 16 + 17)	15	294	525
1. 1	Úpravy hodnot dlouhodobého nehmotného a hmotného majetku - trvalé	16	294	525
1. 2	Úpravy hodnot dlouhodobého nehmotného a hmotného majetku - dočasné	17		
2.	Úpravy hodnot zásob	18	116	170
3.	Úpravy hodnot pohledávek	19		0
III.	**Ostatní provozní výnosy (ř. 21 + 22 + 23)**	20	**192**	**174**
III. 1	Tržby z prodaného dlouhodobého majetku	21	0	0
2	Tržby z prodaného materiálu	22		
3	Jiné provozní výnosy	23	192	174
F.	**Ostatní provozní náklady (ř. 25 až 29)**	24	**367**	**281**
1.	Zůstatková cena prodaného dlouhodobého majetku	25	0	0
2.	Prodaný materiál	26		
3.	Daně a poplatky v provozní oblasti	27	13	11
4.	Rezervy v provozní oblasti a komplexní náklady příštích období	28		
5.	Jiné provozní náklady	29	354	270
*	**Provozní výsledek hospodaření (+/-) (ř. 01 + 02 - 03 - 07 - 08 - 09 - 14 + 20 - 24)**	30	**36 123**	**42 431**

Obrázek 3: Satos Prostějov a.s. – výkaz zisků a ztrát

Označení a	TEXT b	Číslo řádku c	Skutečnost v účetním období běžném 1	Skutečnost v účetním období minulém 2
IV.	**Výnosy z dlouhodobého finančního majetku - podíly (ř. 32 + 33)**	31	**0**	**0**
IV. 1	Výnosy z podílů - ovládaná nebo ovládající osoba	32		
2	Ostatní výnosy z podílů	33		
G.	**Náklady vynaložené na prodané podíly**	34		
V.	**Výnosy z ostatního dlouhodobého finančního majetku (ř. 36 + 37)**	35	**0**	**0**
V. 1	Výnosy z ostatního dlouhodobého finančního majetku - ovládaná nebo ovládající osoba	36		
2	Ostatní výnosy z ostatního dlouhodobého finančního majetku	37		
H.	**Náklady související s ostatním dlouhodobým finančním majetkem**	38		
VI.	**Výnosové úroky a podobné výnosy (ř. 40 + 41)**	39	**91**	**0**
VI. 1	Výnosové úroky a podobné výnosy - ovládaná nebo ovládající osoba	40		
2	Ostatní výnosové úroky a podobné výnosy	41	91	
I.	**Úpravy hodnot a rezervy ve finanční oblasti**	42		
J.	**Nákladové úroky a podobné náklady (ř. 44 + 45)**	43	**0**	**250**
1.	Nákladové úroky a podobné náklady - ovládaná nebo ovládající osoba	44		
2.	Ostatní nákladové úroky a podobné náklady	45		250
VII.	**Ostatní finanční výnosy**	46	**795**	**2 411**
K.	**Ostatní finanční náklady**	47	**847**	**1 633**
*	**Finanční výsledek hospodaření (+/-) (ř. 31 - 34 + 35 - 38 + 39 - 42 - 43 +46 - 47)**	48	**39**	**528**
**	**Výsledek hospodaření před zdaněním (+/-) (ř. 30 + 48)**	49	**36 162**	**42 959**
L.	**Daň z příjmů (ř. 51 + 52)**	50	**6 857**	**8 150**
1.	Daň z příjmů splatná	51	6 885	8 182
2.	Daň z příjmů odložená (+/-)	52	-28	-32
**	**Výsledek hospodaření po zdanění (+/-) (ř. 49 - 53)**	53	**29 305**	**34 809**
M.	Převod podílu na výsledku hospodaření společníkům (+/-)	54	0	0
***	**Výsledek hospodaření za účetní období (+/-) (ř. 53 - 54)**	55	**29 305**	**34 809**
*	**Čistý obrat za účetní období = I. + II. + III. + IV. + V. + VI. + VII**	56	**144 346**	**145 829**

Obrázek 4: Satos Prostějov a.s. - Bilanční rozvaha

1.8.3 Bilanční suma

Bilanční suma je součet **všech aktiv** nebo **všech pasiv** v rozvaze k rozvahovému dni. V rozvaze platí rovnost *aktiva* = *pasiva* (po korekcích).

1.8.3.1 Ukázka bilanční sumy

Přehled aktiv/pasiv v sekci hospodářská činnost je zpravidla uveden ve výroční zprávě, jak je zaevidováno na obrázku 5, kde přehled pasiv je detailněji vidět na obrázku 6 a přehled aktiv je detailněji viděn na obrázku 7. Z vizualizací je zřetelné, že aktiva jsou ekvivalentní pasivům.

Hospodářská činnost

Ve sledovaném období společnost SATOS Prostějov a.s. dosáhla hospodářského výsledku po zdanění, ve výši 29 305 tis. Kč, což oproti roku 2022 znamená snížení o 5 504 tis. Kč.
Nejpodstatnější položkou z pohledu tržeb jsou tržby za prodej zboží, které dosáhly hodnoty 142 449 tis. Kč při souběžně vynaložených nákladech na prodané zboží ve výši 85 276 tis. Kč. Finanční hodnota ostatních provozních výnosů ve sledovaném období dosáhla výše 192 tis. Kč, ostatní provozní náklady dosáhly částku 267 tis. Kč.
Ve sledovaném účetním období spravovala obchodní společnost aktiva a pasiva ve výši 111 328 tis. Kč, což oproti roku 2022 znamená snížení o 23 349 tis. Kč.

Obrázek 5: Satos Prostějov a.s. - Výkaz zisků a ztrát

označ		PASIVA	řád	běžné období	minulé období
a		b	c	5	6
		PASIVA CELKEM (ř. 83 + 104 + 147)		**111 328**	**134 677**
A.		**Vlastní kapitál (ř. 84 + 88 + 96 + 99 + 102 - 103)**	083	**107 114**	**117 809**
A.	I.	**Základní kapitál (ř. 85 až 87)**	084	**5 000**	**5 000**
	1	Základní kapitál	085	5 000	5 000
	2	Vlastní podíly (-)	086		
	3	Změny základního kapitálu	087		
A.	II.	**Ážio a kapitálové fondy (ř. 89 + 90)**	088	**0**	**0**
A.	II. 1	Ážio	089		
	2	Kapitálové fondy (ř. 91 až 95)	090	0	0
	2.1	Ostatní kapitálové fondy	091		
	2.2	Oceňovací rozdíly z přecenění majetku a závazků	092		
	2.3	Oceňovací rozdíly z přecenění při přeměnách obchodních korporací	093		
	2.4	Rozdíly z přeměn obchodních korporací (+/-)	094		
	2.5	Rozdíly z ocenění při přeměnách obchodních korporací (+/-)	095		
A.	III.	**Fondy ze zisku (ř. 97 + 98)**	096	**0**	**0**
A.	III. 1	Ostatní rezervní fondy	097		
	2	Statutární a ostatní fondy	098		
A.	IV.	**Výsledek hospodaření minulých let (+/-) (ř. 100 + 101)**	099	**72 809**	**78 000**
A.	IV. 1	Nerozdělený zisk nebo neuhrazená ztráta minulých let	100	72 809	78 000
	2	Jiný výsledek hospodaření minulých let (+/-)	101		
A.	V. 1	**Výsledek hospodaření běžného účetního období (+/-) /ř.01 - (+ 84 + 88 + 96 + 99 - 103 + 104 + 147)/**	102	**29 305**	**34 809**
	2	**Rozhodnuto o zálohách na výplatě podílu na zisku (-)**	103		
B. + C.		**Cizí zdroje (ř. 105 + 110)**	104	**4 214**	**16 868**
B.	I.	**Rezervy (ř. 106 až 109)**	105	**0**	**0**
B.	I. 1	Rezerva na důchody a podobné závazky	106		
	2	Rezerva na daň z příjmů	107		
	3	Rezervy podle zvláštních právních předpisů	108		
	4	Ostatní rezervy	109		
C.		**Závazky (ř. 111 + 126)**	110	**4 214**	**16 868**
C.	I.	**Dlouhodobé závazky (ř. 112 + 115 až 122)**	111	**60**	**60**
C.	I. 1	Vydané dluhopisy (ř.113 + 114)	112	0	0
	1.1	Vyměnitelné dluhopisy	113		
	1.2	Ostatní dluhopisy	114		
	2	Závazky k úvěrovým institucím	115		
	3	Dlouhodobé přijaté zálohy	116	60	60
	4	Závazky z obchodních vztahů	117		
	5	Dlouhodobé směnky k úhradě	118		
	6	Závazky - ovládaná nebo ovládající osoba	119		
	7	Závazky - podstatný vliv	120		
	8	Odložený daňový závazek	121		
	9	Závazky - ostatní (ř. 123 až 125)	122	0	0
	9.1	Závazky ke společníkům	123		
	9.2	Dohadné účty pasivní	124		
	9.3	Jiné závazky	125		

Obrázek 6: Bilanční rozvaha – Pasiva společnosti Satos Prostějov a.s.

označ	AKTIVA	řád	běžné období			minulé období
			Brutto	Korekce	Netto	Netto
a	b	c	1	2	3	4
	AKTIVA CELKEM (ř. 02 + 03 + 37 + 74)	001	**118 943**	**-7 615**	**111 328**	**134 677**
A.	Pohledávky za upsaný základní kapitál	002			0	
B.	**Stálá aktiva (ř. 04 + 14 + 28)**	003	**7 438**	**-7 294**	**144**	**403**
B. I.	**Dlouhodobý nehmotný majetek (ř. 05 + 06 + 09 až 11)**	004	**473**	**-473**	**0**	**14**
B. I. 1	Nehmotné výsledky vývoje	005			0	
2	Ocenitelná práva (ř. 07 + 08)	006	473	-473	0	14
2.1	Software	007	473	-473	0	14
2.2	Ostatní ocenitelná práva	008			0	
3	Goodwill	009			0	
4	Ostatní dlouhodobý nehmotný majetek	010	0	0	0	
5	Poskytnuté zálohy na dlouhodobý nehmotný majetek a nedokončený dlouhodobý nehmotný majetek (ř. 12 + 13)	011	0	0	0	0
5.1	Poskytnuté zálohy na dlouhodobý nehmotný majetek	012			0	
5.2	Nedokončený dlouhodobý nehmotný majetek	013			0	
B. II.	**Dlouhodobý hmotný majetek (ř. 15 + 18 až 20 +24)**	014	**6 965**	**-6 821**	**144**	**389**
B. II. 1	Pozemky a stavby (ř. 16 + 17)	015	0	0	0	0
1.1	Pozemky	016			0	
1.2	Stavby	017			0	
2	Hmotné movité věci a jejich soubory	018	6 965	-6 821	144	389
3	Oceňovací rozdíl k nabytému majetku	019			0	
4	Ostatní dlouhodobý hmotný majetek (ř. 21 + 22 + 23)	020	0	0	0	0
4.1	Pěstitelské celky trvalých porostů	021			0	
4.2	Dospělá zvířata a jejich skupiny	022			0	
4.3	Jiný dlouhodobý hmotný majetek	023			0	
5	Poskytnuté zálohy na dlouhodobý hmotný majetek a nedokončený dlouhodobý hmotný majetek (ř. 25 + 26)	024	0	0	0	0
5.1	Poskytnuté zálohy na dlouhodobý hmotný majetek	025			0	
5.2	Nedokončený dlouhodobý hmotný majetek	026			0	0
B. III.	**Dlouhodobý finanční majetek (ř. 28 až 34)**	027	**0**	**0**	**0**	**0**
B. III. 1	Podíly - ovládaná nebo ovládající osoba	028			0	
2	Zápůjčky a úvěry - ovládaná nebo ovládající osoba	029			0	
3	Podíly - podstatný vliv	030			0	
4	Zápůjčky a úvěry - podstatný vliv	031			0	
5	Ostatní dlouhodobé cenné papíry a podíly	032			0	
6	Zápůjčky a úvěry - ostatní	033			0	
7	Ostatní dlouhodobý finanční majetek (ř. 35 + 36)	034	0	0	0	0
7.1	Jiný dlouhodobý finanční majetek	035			0	
7.2	Poskytnuté zálohy na dlouhodobý finanční majetek	036			0	

Obrázek 7: Bilanční rozvaha – Aktiva společnosti Satos Prostějov a.s.

Vizualizované korekce na obrázku 7 s číselným označením „2“ se rozumí přechod z hodnot **brutto** na **netto** na základě:

- opravných položek (přechodné snížení hodnoty v důsledku poklesu tržní ceny).
- odpisů (dlouhodobý hmotný/nehmotný majetek).
- oprávek (trvalé snížení hodnoty vlivem opotřebení).

1.8.4 Tabulka hodnocení velikosti podniku

Originální finanční ukazatele prahové hodnoty pro hodnocení velikostí podniků jsou stanoveny v **eurech**. Pro potřeby českého prostředí se částky převádějí kurzem ČNB k **31.12.** předcházejícího roku. Pokud podnik účtuje v jiné měně než CZK, převádí se nejprve na EUR [18, kapitola 4.6 příručky, strana 17].

Tabulka 10: Prahové hodnoty pro výpočet velikosti podniku (převedeno z [18, strana 4])

Parametry velikosti subjektu	**Počet zaměstnanců**	**Roční obrat (v tis.)**	**Bilanční suma (v tis.)**
Střední podnik	51 < 250	250 001 < 1 250 000	250 001 < 1 075 000
Malý podnik	11 < 50	50 001 < 250 000	50 001 < 250 000
Mikropodnik	0 < 10	0 < 50 000	0 < 50 000

Kde platí, že:

$$\text{Identifikátor velikosti podniku} = \text{Počet zaměstnanců} \wedge (\text{Čistý obrat} \vee \text{Bilanční suma})$$

Kdy:

- Kritérium **počtu zaměstnanců** je závazné.
- Mezi **tržbami** a **bilanční sumou** lze volit výhodnější ukazatel.
- Pro výslednou kategorizaci se uplatní **nejvyšší** dosažené (relevantní) kritérium.

1.8.5 Příklad výpočtu velikosti podniku a vliv ekonomického kritéria.

Podnik **Connectica s.r.o.** má následující fiktivní parametrizaci uvedenou v tabulce 11:

Tabulka 11: Modelový příklad parametrů pro výpočet u společnosti Connectica s.r.o.

Parametr	**Hodnota**
Počet zaměstnanců	9
Tržby	55 mil. EUR
Bilanční suma	9 mil. EUR

Kritéria vyhodnocení jsou uvedena v tabulce 12 následně:

Tabulka 12: Kritéria a vyhodnocení Connectica s.r.o.

Kritérium	**Hodnocení**
Zaměstnanci	**mikropodnik**
Tržby	**velký podnik**
Bilanční suma	**malý podnik**

Výsledek hodnocení pak zní, že podnik si zvolí mezi tržbami a bilanční sumou **bilanční sumu** (je pro něj výhodnější). Výsledná kategorie je definována jako **malý podnik** (vyšší ekonomické kritérium totiž přepíše mikrokategorii danou počtem zaměstnanců).

1.8.6 Příklad výpočtu velikosti podniku a vliv kritéria počtu zaměstnanců

Fiktivní podnik **Connectica Investments s.r.o.** má následující parametry uvedené v tabulce 13.

Tabulka 13: Modelový příklad parametrů pro výpočet u společnosti Connectica Investments s.r.o.

Parametr	**Hodnota**
Počet zaměstnanců	49
Tržby	2,5 mil. EUR
Bilanční suma	1,9 mil. EUR

Kritéria vyhodnocení jsou z tabulky 14 následná:

Tabulka 14: Kritéria a vyhodnocení Connectica Investments s.r.o.

Kritérium	**Kategorie**
Zaměstnanci	**malý podnik**
Tržby	**malý podnik**
Bilanční suma	**mikropodnik**

Výsledek: Podnik by dle zvolené ekonomické metriky (bilanční suma) vycházel jako **mikropodnik**, ale rozhodující a závazné je kritérium **počtu zaměstnanců,** a tedy konečná kategorizace je **malý podnik**.

1.8.7 Struktura dle velikosti podniků

Podniky svojí velikostí a vzájemným provázáním mohou být trojího druhu:

1. Nezávislý podnik
2. Partnerský podnik
3. Propojený podnik

1.8.7.1 Nezávislý podnik

Podnik je **nezávislý**, pokud splňuje následující podmínky:

- **(a) Samostatnost**
    1. Nemá žádný podíl v jiných podnicích.
    2. Žádný jiný podnik nemá podíl v daném podniku.
- **(b) Částečné vlastnictví do 24,99 %**
    1. Vlastní méně než 25 % základního kapitálu či hlasovacích práv v jednom nebo více podnicích.
    2. Je vlastněn méně než 25 % základního kapitálu či hlasovacích práv jiným podnikem.
- **(c) Ostatní, specifické případy**

Nezávislý podnik je nezávislým podnikem, pokud není propojen s jiným podnikem přes fyzickou osobu [17, čl. 3 odst. 1, strana 43].

1.8.7.2 Příklad nezávislého podniku

Podnik je vlastněný pěti investory po **20 %**. Žádný jednotlivý držitel nepřesahuje 25 % a proto podnik je **nezávislý**.
Výjimky, kdy je podnik považován za nezávislý i při 25–50 % podílu investora jsou:

- společnosti rizikového kapitálu
- univerzity
- institucionální investoři
- samosprávy s rozpočtem < 10 mil. EUR a < 5 000 obyvatel (za podmínky absence vzájemného propojení) [17 písm d), strana 49].

1.8.7.3 Partnerský podnik

Podnik je **partnerský**, pokud:

1. drží **25–50 %** podílu v jiném podniku, a současně
2. není **propojen** (tj. bez rozhodujícího vlivu > 50 %).

1.8.7.3.1 Příklad partnerského podniku

V následující tabulce 15 jsou uvedeny výchozí hodnoty pro posouzení podniku:

Tabulka 15: Hodnoty pro partnerský podnik

Podnik	Počet zaměstnanců
A	8
B	1
C	9
D	100

Vlastnické vztahy jsou vizualizovány na obrázku 8 takto:

- Podnik A vlastní **33 %** podniku C
- Podnik A vlastní **49 %** podniku D
- Podnik B vlastní **25 %** podniku A

Obrázek 8: Vizualizace vazeb a vztahů vlastnictví pro výpočet partnerského podniku

Pak výpočet pro podnik B je následující:

Podnik C má 9 zaměstnanců → podíl u podniku A je 33 % ≈ **3** „ekvivalentní“ zaměstnanci. Podnik D má 100 zaměstnanců → podíl u podniku A je 49 % = **49** zaměstnanců. Podnik A má 8 vlastních + (3 + 49) = **60** zaměstnanců. Podnik B drží **25 %** podniku A → **15** zaměstnanců z podniku A + **1** vlastní zaměstnanec = **16** zaměstnanců.

Podnik B by vlastní velikostí spadal do mikropodniku, ale po započtení podílů spadá do kategorie **malý podnik**.

1.8.7.4 Propojený podnik

Propojené podniky tvoří skupinu, v níž jeden podnik vykonává **rozhodující vliv** nad jiným (typicky přímé či nepřímé držení **50 %** kapitálu/hlasů), případně má právo jmenovat/odvolat většinu členů orgánů nebo tento vliv vyplývá ze smlouvy či dohody společníků.

Propojení nastává zejména tehdy, když:

1. Podnik vlastní **více než 50 %** jiného podniku.
2. Má právo jmenovat/odvolat většinu orgánů.
3. Smluvní ujednání přiznává rozhodující vliv.
4. Dohoda umožňuje ovládat většinu hlasovacích práv jiného podniku.

1.8.7.4.1 Příklad propojeného podniku

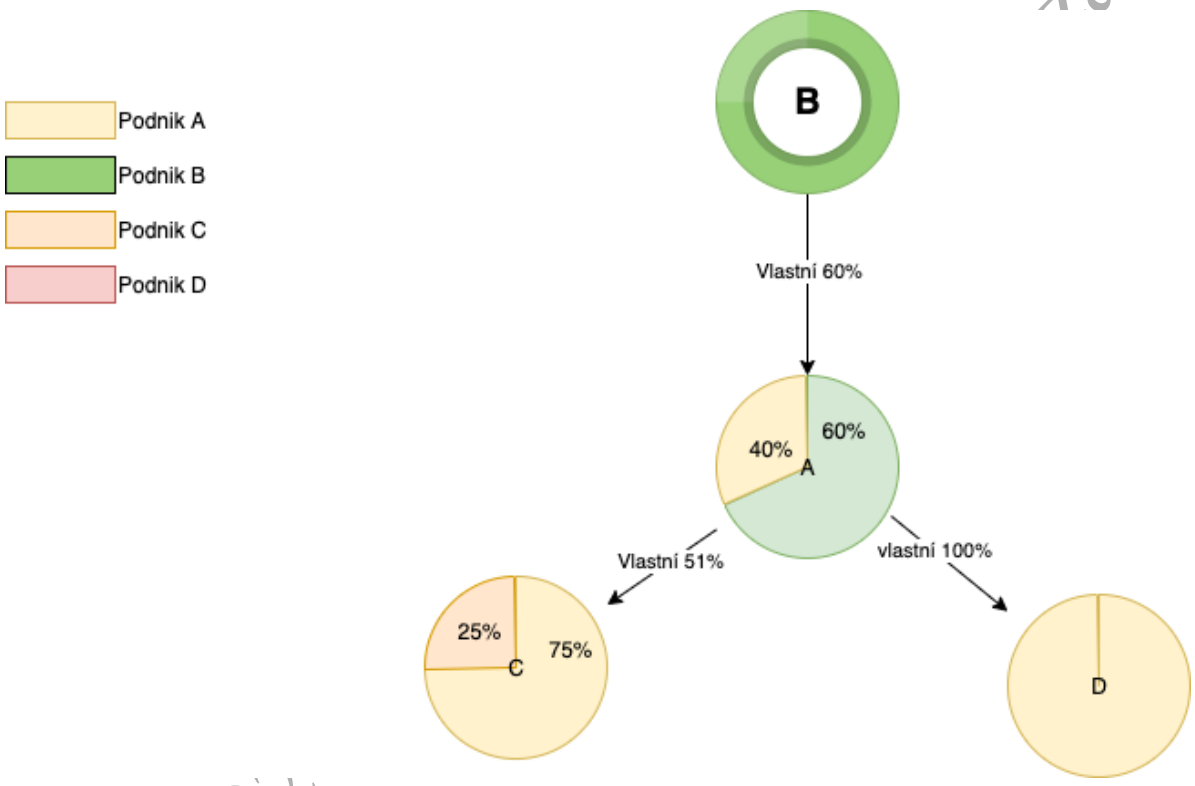
V následující tabulce 16 jsou uvedeny výchozí hodnoty pro posouzení podniku:

Tabulka 16: Hodnoty pro propojený podnik

Podnik	Počet zaměstnanců
A	8
B	1
C	9
D	100

Vlastnické vztahy jsou vizualizovány na obrázku 9 takto:

- Podnik A vlastní **51 %** podniku C
- Podnik A vlastní **100 %** podniku D
- Podnik B vlastní **60 %** podniku A



Obrázek 9: Vizualizace vazeb a vztahů vlastnictví pro výpočet propojeného podniku

Výpočet pro podnik B:

Podíly **50 %** se započítávají **100 %**. Podnik B ovládá podnik A (60 %), Podnik A ovládá podnik C i D, proto k podniku B se zaměstnanci přičítají takto:

$$A(8) + C(9) + D(100) = 117 + 1 = 118$$

Podnik B tedy spadá do kategorie **střední podnik** (přestože má sám jen jednoho zaměstnance).

1.8.8 Sumace a srovnání rozdílnosti vlastnictví podniků

Hodnotí-li se tedy pouze srovnání vlastnictví dle procentuálního zastoupení, pak, jak je uvedeno v tabulce 17, je takto možné zobecnit sumaci dle procentuálního vlastnictví a logicky ji seřadit:

Tabulka 17: Sumace srovnání rozdílnosti vlastnictví podniků

Druh podniku	Vlastní jiný podnik	Je vlastněn jiným podnikem
Nezávislý	0 % < 24,99 %	0 % < 24,99 %
Partnerský	25 % < 49,99 %	25 % < 49,99 %
Propojený	≥ 50 %	≥ 50 %

1.9 Vyhláška o regulovaných službách

V souvislosti s návrhem nového zákona o kybernetické bezpečnosti byl ve sněmovním tisku 759/0 ze dne 25. července 2024 předložen soubor šesti prováděcích vyhlášek [20]. Tyto předpisy konkretizují požadavky zákona a zaměřují se na různé oblasti jeho praktické implementace. Přehled jednotlivých vyhlášek je uveden v tabulce 18.

Novelizované vyhlášky s platností od **01.11.2025** jsou:

- Vyhláška č. 412/2025 Sb. *Vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu [24].*
- Vyhláška č. 334/2025 Sb. *Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony [22].*
- Vyhláška č. 408/2025 Sb. *Vyhláška o regulovaných službách [21].*

Tabulka 18: Přehled jednotlivých vyhlášek o regulovaných službách v nZKB

Název vyhlášky	**Popis**
Vyhláška o regulovaných službách [21]	Stanovuje pravidla pro určování regulovaných a strategicky významných služeb. Implementuje koncept *essential* a *important entities* ze směrnice NIS2 a upravuje proces samoidentifikace.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Upravuje povinnosti subjektů klasifikovaných jako *essential* podle NIS2. Je obsahově shodná s Vyhláškou o kybernetické bezpečnosti.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	Stanovuje povinnosti subjektů klasifikovaných jako *important*. Představuje mírnější variantu režimu nižších povinností.
Vyhláška o Portálu NÚKIB [22]	Specifikuje způsoby a náležitosti hlášení bezpečnostních incidentů prostřednictvím portálu NÚKIB.
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Upravuje povinnosti poskytovatelů veřejných komunikačních sítí a služeb elektronických komunikací.
Vyhláška o kritériích rizikovosti dodavatele	Stanovuje kritéria pro hodnocení rizikovosti dodavatelů a způsob jejich posuzování.

1.9.1 Proces samoidentifikace podle vyhlášky o regulovaných službách

Ilustrativním příkladem může být společnost **A, s.r.o.**, která provozuje vodovod podle zákona č. 274/2001 Sb., o vodovodech a kanalizacích [21, § 2 odst. 5]. Podle přílohy *Kritéria pro identifikaci regulované služby* tato činnost spadá do sekce **10 –** Vodní hospodářství, jak je vidět z výňatku na obrázku 10 .

10. Vodní hospodářství

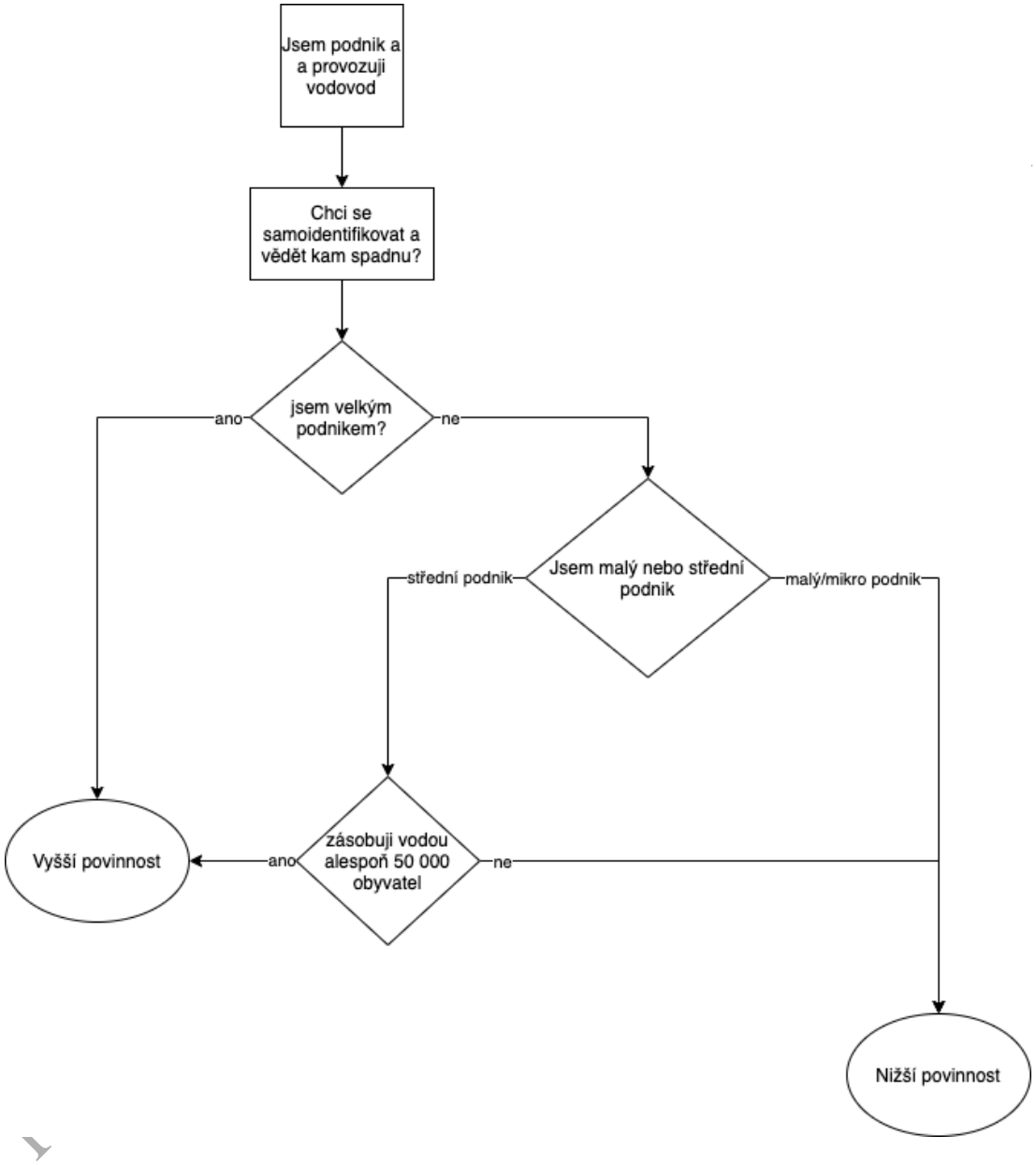
Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
10.1. Provozování vodovodu	Provozovatel vodovodu podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) zásobuje pitnou vodou alespoň 50 000 obyvatel, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
10.2. Provozování kanalizace	Provozovatel kanalizace podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) poskytuje služby odvádění nebo čištění odpadních vod alespoň 50 000 obyvatelům, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Obrázek 10: Kritéria pro identifikaci regulované služby (sekce 10 – Vodní hospodářství)

Z kritérií vyplývá, že:

- Poskytovatel vodovodu je zařazen do **režimu vyšších povinností**, pokud je velkým podnikem nebo zásobuje pitnou vodou alespoň 50 000 obyvatel.
- Do **režimu nižších povinností** spadá v případě, že jde o střední podnik.

Na základě těchto kritérií organizace provádí tzv. **samoidentifikaci**, jejímž výsledkem je registrace u NÚKIB a rozhodovací proces je vizualizován na obrázku 11.



Obrázek 11: Rozhodovací diagram procesu samoidentifikace na příkladu vodárny

Pokud subjekt poskytuje více regulovaných služeb, je vždy rozhodující režim s vyššími povinnostmi. To znamená, že pokud organizace provozuje čtyři služby, z nichž jedna spadá

do režimu vyšších povinností a tři do nižších, na všechny čtyři se vztahují požadavky vyššího režimu při samoidentifikaci.

1.9.2 Srovnání vyšších a nižších režimů a jejich povinností

Režim povinností podle nového zákona o kybernetické bezpečnosti rozlišuje dva základní typy subjektů – **subjekty v režimu vyšších povinností** a **subjekty v režimu nižších povinností**. Rozdíl mezi nimi spočívá především v rozsahu požadavků, které musí organizace plnit a v úrovni odpovědnosti vůči NÚKIBu [25].

1.9.3 Společné povinnosti pro všechny režimy

Bez ohledu na to, zda organizace spadá do **režimu vyšších** nebo **nižších povinností**, existuje soubor požadavků, které musí plnit všechny regulované subjekty podle zákona o kybernetické bezpečnosti. Tyto povinnosti představují základní rámec zajištění bezpečného provozu informačních a komunikačních systémů a umožňují efektivní komunikaci s NÚKIBem [25].

Každá povinná osoba musí zejména:

- **Ohlásit poskytovanou regulovanou službu** prostřednictvím elektronického formuláře dostupného v **Portálu NÚKIB [22]**, čímž formálně vstupuje do evidence regulovaných subjektů.
- **Nahlásit a udržovat aktuální kontaktní údaje** organizace prostřednictvím Portálu NÚKIB, a to **nejpozději do 30 dnů** od doručení rozhodnutí o registraci.
- **Stanovit rozsah řízení kybernetické bezpečnosti**, tj. vymezit, na které systémy, služby a procesy se bezpečnostní opatření vztahují.
- **Zavést bezpečnostní opatření** odpovídající svému režimu povinností podle prováděcí vyhlášky o kybernetické bezpečnosti.

- **Zajišťovat hlášení kybernetických bezpečnostních incidentů**, včetně jejich evidence, kategorizace a komunikace s příslušnými orgány.

- **Dodržovat případná ochranná nebo reaktivní opatření**, která může NÚKIB vydat v souvislosti s hrozbou nebo probíhajícím kybernetickým incidentem.

1.9.4 Rozdíly v povinnostech mezi oběma režimy

Subjekty zařazené do režimu vyšších povinností musí zavádět **rozsáhlejší soubor bezpečnostních opatření** stanovený prováděcí vyhláškou, zatímco subjekty v nižším režimu mají povinnosti přiměřeně zjednodušených opatření. Každý režim je tedy spojen s odlišným okruhem požadavků na řízení rizik, ochranu informací a provozní bezpečnost.

1.9.5 Hlášení incidentů

Klíčovým rozdílem je **způsob a rozsah hlášení kybernetických bezpečnostních incidentů**.

- Organizace v režimu **vyšších povinností** hlásí incidenty přímo **NÚKIB**.

- Organizace v režimu **nižších povinností** hlásí incidenty **národnímu CERT**.

  V obou případech se hlášení provádí jednotně prostřednictvím **Portálu NÚKIB**, který zajišťuje evidenci a správu hlášení.

1.9.6 Sankce

V rámci režimu vyšších povinností lze uložit **přísnější sankce**, a to jak finanční, tak i administrativní. Vedle pokut může jít například o **pozastavení platnosti certifikace** nebo **dočasný zákaz výkonu funkce člena statutárního orgánu**. Režim nižších povinností sice podléhá kontrole, avšak sankční mechanismus je zde mírnější a více zaměřen na nápravu než na represivní postih.

Detailnější rozdíly mezi oběma režimy shrnuje tabulka 19.

Tabulka 19: Detailnější srovnání rozdílů mezi režimem vyšší a nižší povinnosti

Služby v režimu vyšších povinností	**Služby v režimu nižších povinností**
a) Organizační opatření	
1. Systém řízení bezpečnosti informací	a) Systém zajišťování minimální kybernetické bezpečnosti
2. Požadavky na vrcholové vedení	b) Požadavky na vrcholové vedení
3. Stanovení bezpečnostních rolí	
4. Řízení bezpečnostní politiky a dokumentace	
5. Řízení aktiv	c) Řízení aktiv
6. Řízení rizik	d) Řízení rizik
7. Řízení dodavatelů	
8. Bezpečnost lidských zdrojů	e) Bezpečnost lidských zdrojů
9. Řízení změn	
10. Akvizice, vývoj a údržba	
11. Řízení přístupu	g) Řízení přístupu
12. Zvládání kybernetických událostí a incidentů	j) Řešení kybernetických incidentů
13. Řízení kontinuity činností	f) Řízení kontinuity činností
14. Provádění auditu kybernetické bezpečnosti	

b) Technická opatření	
1. Fyzická bezpečnost	
2. Bezpečnost komunikačních sítí	k) Bezpečnost komunikačních sítí
3. Správa a ověřování identit	
4. Řízení přístupových práv a oprávnění	
5. Detekce kybernetických událostí	i) Detekce a zaznamenávání kybernetických událostí
6. Zaznamenávání událostí	
7. Vyhodnocování kybernetických událostí	
8. Aplikační bezpečnost	l) Aplikační bezpečnost
9. Kryptografické prostředky	m) Kryptografické prostředky
10. Zajišťování dostupnosti regulované služby	
11. Zabezpečení průmyslových, řídicích a obdobných specifických systémů	

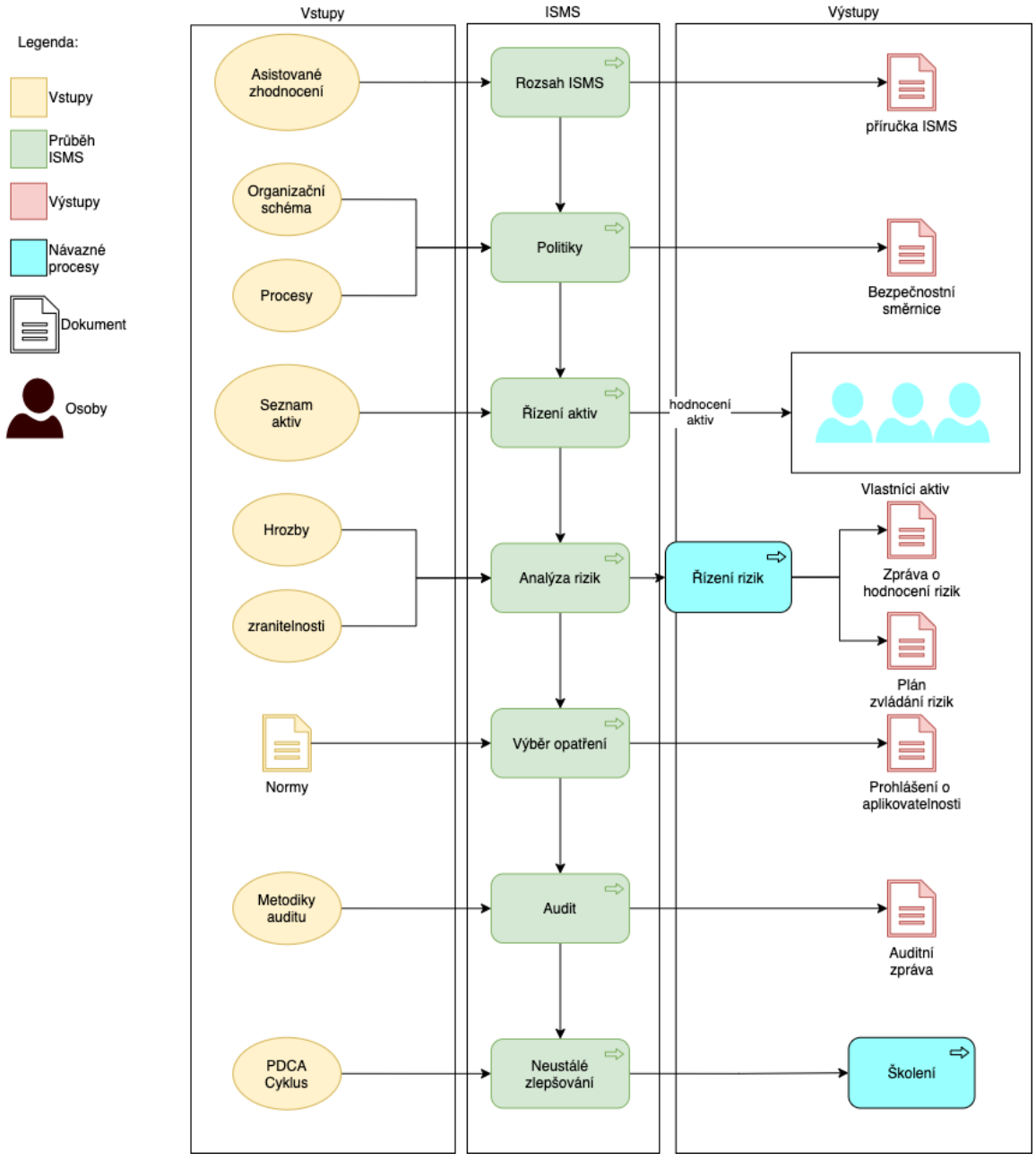
1.10 ISMS

1.10.1 Definice ISMS

Zkratka **ISMS** označuje Systém řízení informační bezpečnosti (**I**nformation **S**ecurity **M**anagement **S**ystem). Jde o dokumentový i procesní rámec, který je součástí celkového řízení organizace a je založen na systematickém **řízení rizik**. Účelem ISMS je **ustanovení, zavádění, provoz, monitorování, udržování, zlepšování a přezkoumávání** bezpečnosti informací. Cílem je minimalizace rizik ztráty, poškození nebo nedostupnosti informačních aktiv [26]. Normativní základ tvoří zejména řada **ISO/IEC 27000**, především **ČSN EN ISO/IEC 27001:2023** [27].

1.10.2 Celkový proces zavádění ISMS

Následující obrázek 12 ilustruje hlavní kroky implementace ISMS, jejich vstupy a výstupy.



Obrázek 12: Schéma procesu zavádění ISMS

Legenda:

- **Vstupy** (žlutě): Jedná se o podklady, požadavky, seznamy aktiv, hrozeb a zranitelností, normy a metodiky. Též výstupy z PDCA cyklu sem vstupují jako vstupy.

- **ISMS (proces)** (zeleně): Jedná se o vlastní implementační kroky, tedy *Rozsah ISMS, stanovení politik, řízení aktiv, analýza rizik, výběr opatření, audit, neustálé zlepšování* – včetně *řízení rizik* jako průřezové činnosti.

- **Výstupy** (červeně/modře): Dokumenty a artefakty, tedy *příručka ISMS, bezpečnostní směrnice, vlastníci aktiv, zpráva o hodnocení rizik, plán zvládání rizik, prohlášení o aplikovatelnosti (SoA), auditní zpráva, školení*.

Pro přehlednost je logika diagramu shrnuta detailněji v tabulce 20.

Tabulka 20: Sumace logiky procesu shody s ISMS

Vstupy	Proces ISMS	Typické výstupy
Asistované zhodnocení, organizační schéma, procesy	Rozsah ISMS	Příručka ISMS
Seznam aktiv	Řízení aktiv	Vlastníci aktiv, hodnocení aktiv
Hrozby, zranitelnosti	Analýza rizik / Řízení rizik	Zpráva o hodnocení rizik, Plán zvládání rizik
Normy (např. ISO/IEC 27001/27002)	Výběr opatření	Prohlášení o aplikovatelnosti (SoA)
Metodiky auditu	Audit	Auditní zpráva

PDCA cyklus	Neustálé zlepšování	Školení, aktualizace politik a procesů

1.10.3 Rozsah ISMS

Rozsah ISMS vymezuje, **které části organizace, aktiva, procesy a technologie** jsou zahrnuty do systému řízení bezpečnosti informací. Správné vymezení je klíčové pro přezkoumatelnost, případné rozšíření i jednotný výklad v organizaci. Nedostatečně zvolený rozsah (opomenutí kritických aktiv či podpůrných prostředků) může vést k nesouladu s **§ 4 odst. 2 ZKB** [2].

Rozsah může být:

- **celopodnikový** (týká se celé organizace), nebo
- **částečný** (vymezen na oblast související s regulovanou/službou kritickou z hlediska KB).

Výstupem definovaného rozsahu je **Příručka pro zavádění ISMS**, která v logice **PDCA cyklu** odpovídá fázi *Plan* (naplánuj).

1.10.4 Politiky (bezpečnostní směrnice)

Vstupem pro tvorbu politik jsou **organizační schémata, procesy a kontext** (odvětví, primární účel, infrastruktura). Z těchto podkladů se odvozují **cíle**, které se transformují do **bezpečnostních směrnic**. Každá směrnice má vymezený cíl a inkrementální kroky jeho naplnění.

Politiky mají svojí povinnou strukturu, která je shrnuta v tabulce 21:

Tabulka 21: Povinná struktura politik VKB

Povinná část politik	Popis	Příklad
Číselné označení	Jednoznačná identifikace dokumentu	Bezpečnostní směrnice 1.8
Název směrnice	Věcné označení obsahu	Bezpečné chování uživatelů
Metadata povinností	Hierarchie závaznosti (musí/mělo by/nesmí)	„Musí“ = bezpodmínečně závazné
Obecný popis	Kontext a účel směrnice	Postupy pro nakládání s aktivy, hesly
Cíl směrnice	Bezpečnostní záměr	Ochrana aktiv přístupných uživatelům
Kroky k cíli	Inkrementální opatření	Vlastník aktiva školí uživatele, definuje postupy apod.

1.10.5 Vzájemný vztah a vazba mezi ISMS a VKB

Implementační kroky ISMS – především analýza rizik, výběr a zavádění opatření, prohlášení o aplikovatelnosti (SoA), audit a proces neustálého zlepšování – tvoří praktický mechanismus, **jak naplnit požadavky VKB** a prokazovat soulad vůči dohledu [2].

Z porovnání obrázku 12 a obrázku 2 vyplývá, že **ISMS a shoda s VKB mají velmi obdobnou strukturu a logiku**, avšak s dílčími rozdíly. Například:

- **ISMS** je rámcový a vychází z mezinárodní normy ISO/IEC 27001, přičemž poskytuje obecný metodický návod.

- **VKB** je závazný právní předpis, který klade konkrétní povinnosti a vyžaduje jejich doložení.
- VKB navíc obsahuje sebeurčení a implementační opatření, které v ISMS nejsou explicitně popsány.
- Výstupy VKB jsou orientovány na shodu s legislativními požadavky, zatímco ISMS se zaměřuje na celkový rámec řízení informační bezpečnosti.

Oba systémy se tak vzájemně doplňují.

ISMS poskytuje metodický rámec a mezinárodní uznání, zatímco VKB stanovuje konkrétní povinnosti a umožňuje jejich kontrolu v podmínkách České republiky.

VKB požaduje pravidelné vyhodnocování účinnosti ISMS (revize rizik, dopady incidentů), řízení významných změn a evidence činností ISMS.

Adaptovala-li dříve organizace ISMS, poté je shoda s VKB administrativně i energeticky snazší k implementaci, a to právě z důvodu blízkosti překryvu obou procesů.

1.11 Definice aktiv a jejich hodnocení

1.11.1 Definice aktiv

V oblasti informační bezpečnosti je aktivum chápáno jako jakýkoli prvek, který má pro organizaci hodnotu a jehož ochrana je nezbytná pro zajištění kontinuity činností. Podle normy ČSN EN ISO/IEC 27001:2023 je aktivem „cokoli, co má pro organizaci hodnotu a je nutné chránit“ [27].

Aktiva lze členit na primární a podpůrná aktiva.

Primární aktiva zahrnují procesy, služby a informace, které tvoří podstatu podnikání organizace.

Podpůrná aktiva jsou naopak prostředky, které zajišťují funkčnost aktiv primárních – typicky technická infrastruktura, lidské zdroje, software nebo služby dodavatelů.

1.11.2 Hodnocení aktiv

Pro účely řízení bezpečnosti informací je nezbytné stanovit hodnotu aktiv, a to:

- kvalitativně (užitečnost, význam pro organizaci)
- kvantitativně (finanční vyjádření hodnoty).

Podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti [2], se doporučuje hodnotit aktiva na základě tří klíčových atributů, tzn. „CIA”:

- Důvěrnost (**C**onfidentiality)
- Integrita (**I**ntegrity)
- Dostupnost (**A**vailability)

1.11.2.1 Důvěrnost

Důvěrnost vyjadřuje, že informace je zpřístupněna pouze oprávněným osobám. Například veřejná webová prezentace vykazuje nízké nároky na důvěrnost, zatímco citlivý dokument určený omezenému okruhu osob vyžaduje nejvyšší ochranu. Zveřejnění vysoce důvěrného dokumentu na veřejném kanálu představuje pak v tomto příkladu úplnou ztrátu důvěrnosti.

1.11.2.2 Integrita

Integrita vyjadřuje správnost, úplnost a neporušenost informace. Změna obsahu (úmyslná či neúmyslná) snižuje její vypovídací hodnotu. Mechanismy typu řízení verzí, kontrolní součty či podpisy zvyšují jistotu, že data nebyla neoprávněně modifikována.

1.11.2.3 Dostupnost

Dostupnost znamená, že informace a služby jsou k dispozici v okamžiku potřeby. Neplánovaná nedostupnost (např. výpadek aplikace) má dopady úměrné významu aktiva pro provoz organizace.

1.11.3 Hodnotící atributy aktiv

Každý z atributů disponuje specifickými indikátory, které vyjadřují míru ztráty či poškození aktiva, jak je rozepsáno v tabulce 22.

Tabulka 22: Hodnotící atributy míry poškození aktiva

Atribut	Klíčový indikátor
Dostupnost	Míra ztráty aktiva v důsledku jeho časové nedostupnosti
Integrita	Míra ztráty nebo poškození aktiva z hlediska jeho celistvosti
Důvěrnost	Míra ztráty nebo poškození aktiva v důsledku jeho potenciálního vyzrazení

1.11.3.1 Tabulka hodnocení dostupnosti

Příloha č.1 doporučená vyhláškou č. 82/2018 Sb. [2] uvádí čtyři úrovně hodnocení dostupnosti aktiv, doslovné převzetí je sepsáno v tabulce 23:

Tabulka 23: Doporučené úrovně hodnocení dostupnosti aktiv

Úroveň	**Popis**	**Příklady ochranných opatření**
Nízká	Výpadek je tolerovatelný (cca do 1 týdne).	Pravidelné zálohování.
Střední	Výpadek nesmí překročit 1 pracovní den.	Běžné metody zálohování a obnovy.
Vysoká	Výpadek nesmí přesáhnout několik hodin a je nutná okamžitá reakce.	Záložní systémy, obnova často vyžaduje zásah obsluhy.
Kritická	Nedostupnost není přípustná ani v minutách.	Automatizované záložní systémy s krátkodobou obnovou.

Analogické hodnocení je aplikováno na hodnocení integrity i důvěrnosti. Přesný obsah je uveden v tabulce 1 a tabulce 2 přílohy 1 VKB.

Výpočet hodnoty aktiva

Pro kvantifikaci hodnoty aktiva lze využít různé metody, a to:

- Aritmetický průměr
- Prostý součet
- Prosté násobení

Bude-li definice proměnných stanovena takto:

- (A) = dostupnost (*availability*),
- (C) = důvěrnost (*confidentiality*),
- (I) = integrita (*integrity*),
- (H) = výsledná hodnota aktiva.

Pak **Aritmetický průměr** lze spočítat:

$$H = \frac{A + C + I}{3}$$

a **Prostý součet je počítán:**

$$H = A + C + I$$

Prosté násobení lze vypočítat jako:

$$H = A \times C \times I$$

Výběr konkrétní metody závisí na potřebách organizace a na charakteru posuzovaných aktiv. Například aritmetický průměr poskytuje vyvážený pohled na hodnotu aktiva, zatímco prosté násobení zdůrazňuje kritičnost – pokud je jeden atribut nulový, je nulová i výsledná hodnota.

1.12 Primární aktiva

1.12.1 Obecná charakteristika primárních aktiv

Primární aktiva představují prvky, které tvoří samotný základ činnosti organizace a přímo souvisejí s jejími službami, obchodními procesy a strategickými cíli. Jejich správná ochrana a řízení jsou nezbytné pro zachování kontinuity provozu a pro plnění legislativních požadavků v oblasti kybernetické bezpečnosti.

Typicky se rozlišují dva základní typy primárních aktiv:

1. **Služby** – zahrnující například zdravotnickou péči, bankovní transakce či výrobní procesy.

2. **Informace** – jako jsou databáze klientů, technická dokumentace, obchodní tajemství nebo know-how.

Do kategorie primárních aktiv lze dále zařadit také klíčové **obchodní procesy** a **právní závazky** vyplývající z uzavřených smluv či regulatorních povinností. Má-li potenciální ztráta nebo narušení těchto aktiv přímé důsledky, a to jak ekonomické, tak reputační či právní.

1.12.2 Identifikace primárních aktiv

Identifikace primárních aktiv je proces, při němž organizace systematicky určuje, která aktiva jsou pro její činnost klíčová. Tento proces by měl v ideálním světě probíhat za účasti zástupců vedení i odborných útvarů, aby byla zajištěna komplexnost a správnost výsledku [28].

Příklady primárních aktiv:

- Elektronická zdravotnická dokumentace ve zdravotnickém zařízení.

- Bankovní informační systém v peněžním ústavu.

- Software poskytovaný formou služby (SaaS) ve společnosti zaměřené na vývoj aplikací.

1.12.3 Evidence primárních aktiv

Evidence primárních aktiv je povinná a musí být vedena v souladu s vyhláškou č. 82/2018 Sb. Minimální požadované údaje zahrnují [25, strana 34]:

- **Jednoznačný identifikátor aktiva (ID)**.
- **Název a popis aktiva** včetně jeho účelu a rozsahu použití.
- **Gestora nebo garanta aktiva**, který nese odpovědnost za jeho správu a ochranu.
- **Hodnocení atributů důvěrnosti, integrity a dostupnosti (CIA)**.
- Další doplňující informace (např. lokalita, technické parametry, právní vazby).

Takto vedená evidence slouží jako základní nástroj pro řízení rizik a plánování bezpečnostních opatření.

1.12.4 Hodnocení primárních aktiv

Hodnocení primárních aktiv je zaměřeno na určení dopadů, které by přinesla jejich ztráta, poškození nebo nedostupnost. Podle vyhlášky č. 82/2018 Sb. se posuzují zejména atributy **důvěrnosti, integrity a dostupnosti** s vhodně stanoveným výpočtem dle preference organizace [2, § 4 odst 1, písm e)].

Primární aktiva jsou obvykle hodnocena jako **kritická**, protože jejich ohrožení má bezprostřední a zásadní vliv na fungování celé organizace. Výsledkem hodnocení je stanovení **úrovně kritičnosti**, která následně slouží jako vstup pro proces řízení rizik a výběr adekvátních bezpečnostních opatření.

Podle § 4 odst. 2 vyhlášky č. 82/2018 Sb. musí hodnocení zahrnovat i posouzení širších dopadů, a to například:

- rozsah a význam zpracovávaných osobních údajů či obchodního tajemství,
- plnění právních povinností a smluvních závazků,
- narušení vnitřních kontrolních a řídicích činností,
- potenciální finanční ztráty a dopady na obchodní či veřejné zájmy,
- vliv na poskytování služeb důležitých pro fungování společnosti,
- přerušení běžných provozních činností,
- ohrožení pověsti a dobrého jména organizace,
- rizika pro bezpečnost a zdraví osob,
- možné negativní důsledky pro mezinárodní vztahy,
- dopady na uživatele informačního a komunikačního systému.

Tento vícerozměrný přístup zajišťuje, že hodnocení není pouze technické, ale zahrnuje i právní, ekonomické a společenské aspekty.

1.13 Podpůrná aktiva

1.13.1 Obecná charakteristika podpůrných aktiv

Podpůrná aktiva představují prostředky, které umožňují provoz a správné fungování aktiv primárních. Sama o sobě obvykle nevytvářejí přímou hodnotu ani službu, avšak jejich spolehlivost je zásadním předpokladem pro chod organizace. Typickými příklady jsou technologická infrastruktura, lidské zdroje, software, fyzické objekty či služby externích dodavatelů [25, strana 52].

Selhání podpůrných aktiv (například výpadek napájení, nedostupnost serveru nebo odchod klíčového zaměstnance) má okamžitý dopad na kontinuitu činností a může způsobit dominový efekt i v dalších oblastech. Proto je jejich správné řízení součástí celkového systému řízení informační bezpečnosti.

1.13.2 Kategorizace podpůrných aktiv

Podpůrná aktiva lze podle doporučení NÚKIB členit do následujících kategorií, [25, strana 52] jak je uvedeno u extrahované tabulky 24.

Tabulka 24: Extrakce doporučené členění podpůrných aktiv [28, strana 52]

Kategorie	Příklady
Technické vybavení	Servery, pracovní stanice, mobilní zařízení
Komunikační prostředky	Routery, switche, přístupové body Wi-Fi
Programové vybavení	Operační systémy, aplikační software, ERP systémy
Objekty	Serverovny, kancelářské prostory, sklady
Lidské zdroje	Administrátoři, vývojáři, management

Dodavatelé	Poskytovatelé hardwaru, softwaru a souvisejících služeb
Externí systémy a služby	Cloudové platformy (např. Azure, AWS), SaaS aplikace

1.13.3 Identifikace podpůrných aktiv

Proces identifikace podpůrných aktiv vyžaduje detailní znalost prostředí organizace a jeho technických, organizačních i smluvních vazeb. V praxi zahrnuje:

- mapování všech prostředků podporujících provoz primárních aktiv,
- posouzení relevance aktiva pro daný proces,
- zohlednění časových a finančních možností při stanovování detailnosti evidence.

Cílem je stanovit optimální úroveň podrobnosti tak, aby identifikace byla prakticky využitelná a současně ekonomicky přiměřená.

1.13.4 Evidence podpůrných aktiv

Evidence podpůrných aktiv slouží jako nástroj pro jejich řízení a propojení s primárními aktivy. Minimální záznamy by podle doporučení NÚKIB měly obsahovat: [28, strana 56]

- jednoznačný identifikátor (ID),
- název a detailní popis,
- garanta aktiva,
- hodnocení atributů důvěrnosti, integrity a dostupnosti,
- doplňková metadata (např. lokalitu, vlastnictví, SLA, smluvní vazby).

U podpůrných aktiv je často zásadní role dodavatelů a třetích stran. Proto je vhodné doplnit také údaje o poskytovaných službách, SLA nebo smluvních závazcích.

1.13.5 Hodnocení podpůrných aktiv

Hodnota podpůrného aktiva je zpravidla odvozena od významu aktiv primárních, která jsou jimi podporovány. Hodnocení by proto mělo zohledňovat:

- kritičnost primárního aktiva,
- spolehlivost a odolnost podpůrného aktiva,
- závislost na třetích stranách a smluvních vztazích,
- možnost náhrady či existence redundance.

Stejně jako u primárních aktiv se při hodnocení podpůrných aktiv využívá model „CIA“ (confidentiality, integrity, availability). Rozsah kritičnosti podpůrných aktiv se může lišit – od běžného pracovního počítače až po centrální serverový cluster. Klíčové je proto také mapování vzájemných závislostí mezi aktivy.

1.13.6 Příklad rozdílu mezi primárním a podpůrným aktivem

Společnost *A s.r.o.* vyvíjí a licencuje software, který používá zdravotnická organizace *B s.r.o.*:

- **Primárním aktivem** společnosti A je samotný software poskytovaný zákazníkům.
- **Podpůrná aktiva** tvoří například:
    - vývojový tým a administrátoři,
    - servery, síťové prvky a fyzickou infrastrukturu,
    - zabezpečení serverovny (EZS, přístupové systémy).

Z pohledu společnosti B se společnost A stává dodavatelem, jehož podpůrná aktiva mají přímý vliv na zajištění zdravotnických služeb společnosti B.

1.14 Vazby mezi primárními a podpůrnými aktivy

Aktiva v organizaci neexistují izolovaně, ale jsou navzájem propojena prostřednictvím vztahů a závislostí. Tyto vazby mají zásadní význam pro řízení bezpečnosti, protože narušení jednoho aktiva se může řetězově promítnout do funkčnosti dalších. Vazby lze rozdělit do dvou základních kategorií:

1. **Vzájemná vazba mezi primárními aktivy**
2. **Vazba mezi primárními a podpůrnými aktivy**

1.14.1 Vzájemná vazba mezi primárními aktivy

Primární aktiva jsou často propojena prostřednictvím obchodních procesů a informačních toků. Typickým příkladem je situace, kdy obchodní proces využívá více služeb nebo informačních systémů, které zajišťují jeho realizaci.

Pokud například klíčová služba zdravotnického zařízení závisí na elektronické dokumentaci pacientů, pak výpadek systému pro správu dokumentace (primární aktivum) může způsobit přerušení poskytování zdravotní péče (jiné primární aktivum).

Mapování těchto vazeb je nezbytné pro identifikaci kritických míst, jejichž selhání by vedlo k dominovému efektu v rámci celé organizace.

1.14.2 Vazba mezi primárními a podpůrnými aktivy

Významnější roli, než vzájemné vztahy mezi primárními aktivy sehrávají vazby mezi aktivy primárními a podpůrnými. Každé primární aktivum je podporováno řadou podpůrných prostředků – od technické infrastruktury a softwaru až po dodavatelské služby.

Pokud dojde k selhání podpůrného aktiva, projeví se tento dopad přímo na aktivum primární a to může řetězením mít vliv na jiné primární aktivum. Například výpadek napájení (podpůrné aktivum) znemožní provoz databázového serveru což může narušit poskytování

koncové služby zákazníkům (primární aktivum) a tato koncová služba může mít vliv na jiné, blízké primární aktivum či jiná aktiva.

Proto je systematické mapování vazeb mezi primárními a podpůrnými aktivy **klíčové**. Tyto vztahy musí být zohledňovány zejména při hodnocení rizik a plánování bezpečnostních opatření.

1.14.3 Metodika hodnocení vazeb mezi aktivy

Pro posuzování vztahů mezi primárními a podpůrnými aktivy existují tři hlavní přístupy [28, strana 58]:

1. **Dědičnost hodnoty primárního aktiva** – podpůrné aktivum přebírá hodnotu primárního, které podporuje.
2. **Individuální hodnocení podpůrných aktiv** – každé podpůrné aktivum je posuzováno samostatně.
3. **Vzorcové mapování** – podpůrné aktivum získává hodnotu z primárního prostřednictvím definovaného vzorce.

Srovnání těchto metod uvádí následující tabulka 25:

Tabulka 25: Srovnání metodiky pro hodnocení dědičnosti vazeb mezi primárními a podpůrnými aktivy

Varianta	Popis	Klady	Zápory
A	Podpůrná aktiva dědí hodnoty primárních aktiv	+ Minimální časová náročnost + Vysoký stupeň automatizace	- Riziko zkreslení hodnot - Možnost nadhodnocení a vyšších nákladů na opatření
B	Podpůrná aktiva jsou posuzována individuálně s ohledem na hodnotu primárních aktiv	+ Nejvyšší přesnost + Zohlednění specifických podmínek	- Vysoké časové a kapacitní nároky - Obtížná aplikace při velkém počtu aktiv
C	Podpůrná aktiva přebírají hodnoty prostřednictvím vzorce	+ Možnost automatizace + Vyváženost mezi variantami A a B	- Náročnost na vytvoření vhodného vzorce - Riziko chybné parametrizace

V praxi se často kombinuje více přístupů současně. Například pro méně významná aktiva může být efektivní varianta A, zatímco u kritických aktiv je vhodnější individuální hodnocení (varianta B).

1.15 Pravidla pro nakládání s aktivy

1.15.1 Různé úrovně opatření pro nakládání s aktivy

Nakládání s informačními aktivy je jedním ze stěžejních prvků řízení informační bezpečnosti. Každé aktivum musí být spravováno v souladu se svou klasifikací a úrovní důvěrnosti. Smyslem tvorby pravidel je zajištění, aby ochrana byla přiměřená hodnotě a významu daného aktiva pro organizaci, jak je vizualizováno na obrázku 17 později. Podle vyhlášky č. 82/2018 Sb. a doplňujících metodických dokumentů od NÚKIBu se pravidla vztahují nejen na elektronické soubory, ale také na listinné dokumenty a technická média [2, příloha č. 5, odst 1, pododst 1.1, písm d)].

Modelově lze rozlišit čtyři základní úrovně opatření, které podobně kopíruje i TLP z tabulky 26:

- **Veřejná aktiva** nevyžadují zvláštní bezpečnostní opatření, jelikož jejich dostupnost je cílená.
- **Interní aktiva** podléhají základní ochraně, zejména prostřednictvím řízení přístupu a evidence.
- **Citlivá aktiva** vyžadují zavedení šifrování komunikace, sledování přístupů a důsledné uplatňování zásady *need-to-know*.
- **Diskrétní aktiva** jsou spravována v nejpřísnějším režimu, zahrnujícím šifrování, detailní logování a schválení původce při každém sdílení.

Pravidla je vhodné nejméně jednou za dva roky přezkoumávat a aktualizovat, aby odpovídala aktuálnímu stavu hrozeb a technologií.

1.15.2 Nakládání s aktivy

Proces nakládání s aktivy zahrnuje tři klíčové činnosti:

- Označování
- manipulaci
- správu výměnných médií

Označování slouží k jasnému určení klasifikace. U dokumentů je požadováno vyznačení úrovně důvěrnosti na viditelném místě (např. na titulní straně), přičemž u citlivých a diskrétních dokumentů má být označení uvedeno na každé stránce. Elektronické soubory mají být opatřeny odpovídajícími metadaty. Více k této části je uvedeno v samostatné kapitole 1.17.1.

Manipulace s aktivy se řídí principem proporcionality: čím vyšší úroveň klasifikace, tím přísnější omezení. Zatímco u veřejných dokumentů je možné volné kopírování, u citlivých a diskrétních aktiv je požadována evidence každé kopie a jejich sdílení podléhá přísné kontrole.

Správa médií zahrnuje evidenci všech nosičů obsahujících citlivá či diskrétní informace, jejich bezpečné ukládání a řízení životního cyklu. Tato opatření minimalizují riziko ztráty nebo neoprávněného úniku dat.

1.16 Likvidace dat

Likvidace dat a jejich nosičů je regulována přílohou č. 4 vyhlášky č. 82/2018 Sb [2]. Zvolený způsob závisí na klasifikaci aktiva:

- **Veřejná aktiva** mohou být pouze vyhozena do odpadu.
- **Interní aktiva** mohou být likvidována běžnými postupy (mazání, skartace, přepis zařízení).
- **Citlivá aktiva** vyžadují fyzickou likvidaci (skartace příčným řezem, spálení, rozložení).
- **Diskrétní aktiva** musí být likvidována pod dohledem a opatřena protokolárním potvrzením.

V případě elektronických médií (např. HDD, SSD, optické disky) se využívá víceúrovňové přepsání dat, kryptografická likvidace nebo fyzické zničení. Pro cloudové služby je nezbytné smluvně stanovit podmínky likvidace a doporučuje se využívat šifrování v kombinaci s následným zničením klíčů [2, příloha 4].

1.17 Klasifikace informací

Správné nakládání s informacemi vyžaduje jejich systematickou klasifikaci podle citlivosti a okruhu oprávněných příjemců. V praxi se k tomuto účelu uplatňují standardizované protokoly, které jednoznačně vyjadřují pravidla pro **šíření** a **použití** informací. Nejrozšířenějšími rámci jsou:

- **TLP (Traffic Light Protocol)**
- **PAP (Permissible Actions Protocol)**

Aplikace těchto protokolů podporuje efektivní výměnu informací, posiluje důvěru mezi partnery a snižuje riziko neautorizovaného zveřejnění či nevhodného nakládání s obsahem.

1.17.1 Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) představuje mezinárodně uznávaný rámec publikovaný organizací FIRST. Cílem je definovat pravidla **šíření** citlivých informací. Verze 2.0 (2022) je k dispozici i v českém jazyce [29].
TLP pracuje s barevnou škálou, která signalizuje míru omezení šíření, její granulární popis je uveden v tabulce 26. Označení zvolené odesílatelem stanoví, komu a v jakém rozsahu lze informaci dále poskytovat.

Tabulka 26: Označení a pravidla užívání šíření dat při užití TLP

Označení	Význam	Pravidla šíření
TLP:RED	Nejvyšší omezení	Poskytnutí výlučně adresátovi; jakékoli další sdílení pouze s výslovným souhlasem původce.
TLP:AMBER+STRICT	Přísné interní sdílení	Sdílení výhradně **uvnitř** organizace příjemce a pouze osobám splňujícím

		zásadu *need-to-know*; externí distribuce se nepřipouští.
TLP:AMBER	Omezené cílené sdílení	Sdílení uvnitř organizace a s nezbytnými partnerskými subjekty a vždy pouze osobám s prokazatelnou potřebou seznámení.
TLP:GREEN	Komunitní (neveřejné) sdílení	Sdílení v rámci širší profesní komunity/odvětví; nikoli veřejnými kanály; vyžaduje důvěrný přenos.
TLP:CLEAR	Bez omezení šíření	Volné zveřejnění; respektují se případná práva duševního vlastnictví a právní regulace.

TLP se běžně využívá při výměně informací o hrozbách, indikátorech kompromitace a dalších bezpečnostních poznatcích mezi veřejnými institucemi a soukromým sektorem [30].

1.17.2 Permissible Actions Protocol (PAP)

Permissible Actions Protocol (PAP) je klasifikační mechanismus, který **ne**stanovuje, **komu** lze informaci předat (to řeší TLP), nýbrž vymezuje, **jaké akce** je dovoleno s informací provádět. Protokol vznikl v komunitě projektu MISP a slouží k řízení **použití** informací v prostředí sdílení kybernetických poznatků [31].

1.17.2.1 Úrovně PAP

Klasifikační úrovně PAP sumarizované v tabulce 27 jsou podobné TLP uvedeném v tabulce 26.

Tabulka 27: Převzaté označení a podmínky užití PAP [30].

Označení	Význam	Podmínky použití
PAP:RED	Nejvyšší omezení použití	Pouze **nedetekovatelné** pasivní úkony v oddělené, kontrolované infrastruktuře (forenzní/investigativní účely). Aktivní využití v sítích připojených k internetu se **nepřipouští**.
PAP:AMBER	Silně omezené použití	Dovoleny **pasivní** akce (např. ověření přes externí služby typu WHOIS, CESNET NERD; monitoring; honeypot). Aktivní interakce s cílem se **neprovádí**.
PAP:GREEN	Omezené (aktivní) použití	Mimo vlastní infrastrukturu **jen neinvazivní** kroky (např. ping, blokace provozu, specifická konfigurace honeypotu); v rámci interní infrastruktury je povoleno plné využití.
PAP:CLEAR	Bez omezení použití	Volné použití bez dodatečných restrikcí; vždy se respektují obecné právní povinnosti a práva duševního vlastnictví.

Pro úplnost původu strojově čitelné vyjádření taxonomie PAP je zveřejněno na GitHubu [32].


```
{
  "namespace": "PAP",
  "expanded": "Permissible Actions Protocol",
  "description": "The Permissible Actions Protocol - or short: PAP - was
designed to indicate how the received information can be used.",
  "version": 3,
  "exclusive": true,
  "predicates": [
    {
      "value": "RED",
      "expanded": "(PAP:RED) Non-detectable actions only. Recipients may not use
PAP:RED information on the network. Only passive actions on logs, that are not
detectable from the outside.",
      "colour": "#ff2b2b",
      "uuid": "35c5f1fa-c244-504e-bdd8-a6e98f502ab7"
    },
    {
      "value": "AMBER",
      "expanded": "(PAP:AMBER) Passive cross check. Recipients may use PAP:AMBER
information for conducting online checks, like using services provided by third
parties (e.g. ripe whois), or set up a monitoring honeypot.",
      "colour": "#ffc000",
      "uuid": "09f19595-73dc-5cc2-8e56-48a8403e4053"
    },
    {
      "value": "GREEN",
      "expanded": "(PAP:GREEN) Active actions allowed. Recipients may use
PAP:GREEN information to ping the target, block incoming/outgoing traffic
from/to the target or specifically configure honeypots to interact with the
target.",
      "colour": "#33ff00",
      "uuid": "52ef05b9-08cf-56fb-aaec-82093f6dc677"
    },
```

```
    {
      "value": "CLEAR",
      "expanded": "(PAP:CLEAR) No restrictions in using this information.",
      "colour": "#ffffff",
      "uuid": "cd72ec20-215c-5cd3-a3a7-06755f81d6bb"
    },
    {
      "value": "WHITE",
      "expanded": "(PAP:WHITE) No restrictions in using this information.",
      "colour": "#ffffff",
      "uuid": "6b973638-eafb-5265-bf70-b96bd06ddfdb"
    }
  ],
  "uuid": "8d7472b0-8a76-5be9-bfe0-185cc9ca9c30"
}
```


1.17.3 Kombinace TLP a PAP

V praxi kybernetické bezpečnosti je uplatňováno současné použití protokolů Traffic Light Protocol (TLP) a Permissible Actions Protocol (PAP).

PAP je tedy komplementární k TLP. Společně umožňují přesně určit jak okruh oprávněných příjemců, tak i povolené způsoby práce s obsahem [30] .

- TLP určuje, *komu* je možné danou informaci předat.
- PAP stanovuje, *jakým způsobem* může být tato informace využita.

Použití obou protokolů současně zajišťuje, že příjemce má jasně vymezen jak okruh oprávněných osob, tak i způsoby práce s informacemi. Tento přístup je využíván ke zvýšení konzistence, důvěryhodnosti a jednoznačnosti při sdílení citlivých informací v národním i mezinárodním kontextu.

1.17.3.1 Příklady kombinovaného použití TLP a PAP

Pro ilustraci praktického uplatnění protokolů TLP a PAP uvádíme několik modelových scénářů. Tyto příklady vycházejí z doporučených postupů NÚKIB, a byly přeformulovány a adaptovány pro účely této práce [33, strana 10] jak je vizualizováno v tabulce 28.

Tabulka 28: Příklady použití kombinací TLP a PAP

TLP + PAP	Modelový scénář použití
TLP:RED + PAP:RED	Národní CSIRT informuje bankovní instituci o tom, že útočníci mají aktivní přístup do interní sítě. Organizace je instruována, aby informace sdílela výhradně v rámci úzkého bezpečnostního týmu a aby prováděla pouze pasivní analýzy kompromitovaných stanic v kontrolovaném prostředí.
TLP:AMBER+STRICT + PAP:GREEN	Energetická společnost je upozorněna na kritickou zranitelnost používaného firewallu. Informace může být sdílena pouze uvnitř organizace, přičemž je povoleno provádění bezpečných technických kroků (např. aplikace bezpečnostních záplat nebo blokace podezřelé komunikace).
TLP:AMBER + PAP:AMBER	Dodavatel IT služeb je informován o podezření na kompromitaci části sítě zákazníka. Je doporučeno provést pasivní prověření rozsahu napadení, avšak bez blokování nebo přímé interakce s útočníkem. Sdílení informací je možné pouze s osobami, které mají pracovní potřebu tyto údaje znát.

TLP:GREEN + PAP:AMBER	Ve zdravotnickém sektoru se objevuje škodlivá kampaň cílená na nemocnice. Organizace obdrží návod, jak útok detekovat. V případě zjištění není doporučeno útočníka blokovat, ale kontaktovat centrální autoritu.
TLP:GREEN + PAP:CLEAR	Univerzitní síť je informována o probíhající phishingové kampani. Organizace může informaci sdílet v rámci celého akademického sektoru a zároveň provést školení uživatelů o rizicích.
TLP:CLEAR + PAP:CLEAR	Veřejně dostupná zpráva shrnuje počet incidentů řešených v národní úrovni za uplynulý rok, včetně agregovaných statistik. Tato informace je volně publikovatelná bez omezení.

1.18 Zranitelnosti

1.18.1 Definice zranitelnosti

Zranitelnost představuje inherentní vlastnost aktiva, která může být zneužita hrozbou k narušení důvěrnosti, integrity nebo dostupnosti informací. Jinými slovy, zranitelnost je slabina systému, aplikace, infrastruktury nebo procesů, která umožňuje útočníkovi provést akci vedoucí k narušení bezpečnosti. Zranitelnosti jsou přirozeným důsledkem rostoucí komplexity informačních a komunikačních technologií a jejich vzájemné provázanosti.

1.18.2 Příčiny zranitelností

Příčiny vzniku zranitelností lze rozdělit do několika kategorií:

- **Hardwarové zranitelnosti** (např. chyby návrhu architektury procesorů).
- **Softwarové zranitelnosti** (nedostatky v implementaci aplikací).
- **Síťové zranitelnosti** (nesprávná konfigurace síťových prvků či služeb).
- **Zranitelnosti způsobené lidským faktorem** (slabá hesla, chyby administrátorů).
- **Dosud neznámé zranitelnosti (tzv. zero-day)**, které nebyly identifikovány nebo zveřejněny.

1.18.2.1 Příklady zranitelností z praxe

Tabulka 29: Příklad zranitelností z praxe

Typ zranitelnosti	Popis
Hardwarové	Zranitelnost *Spectre* [34] umožňuje útočníkovi číst data z cache procesoru a tím získat citlivé informace z jiných procesů.
Softwarové	Chybně napsaný kód aplikace umožňující zneužití technikou *SQL injection [35].*
Síťové	Nesprávně nakonfigurovaný firewall s otevřeným portem 3389 (RDP) přístupným z internetu na neaktualizovaný Windows server.
Lidský faktor	Používání továrního hesla na firewallu přístupném zvenčí přes porty 80/443.

1.18.3 Metodika hodnocení zranitelností

Pro hodnocení závažnosti zranitelností se používá **Common Vulnerability Scoring System (CVSS)**, což je průmyslový standard umožňující přiřadit číselnou hodnotu v rozmezí 0–10. Čím vyšší hodnota, tím vyšší je závažnost zranitelnosti. CVSS je spravován organizací FIRST [36] a od svého vzniku v roce 2005 prošel několika verzemi. Nejnovější verzí je CVSS v4.0.

1.18.4 Struktura metrik CVSS

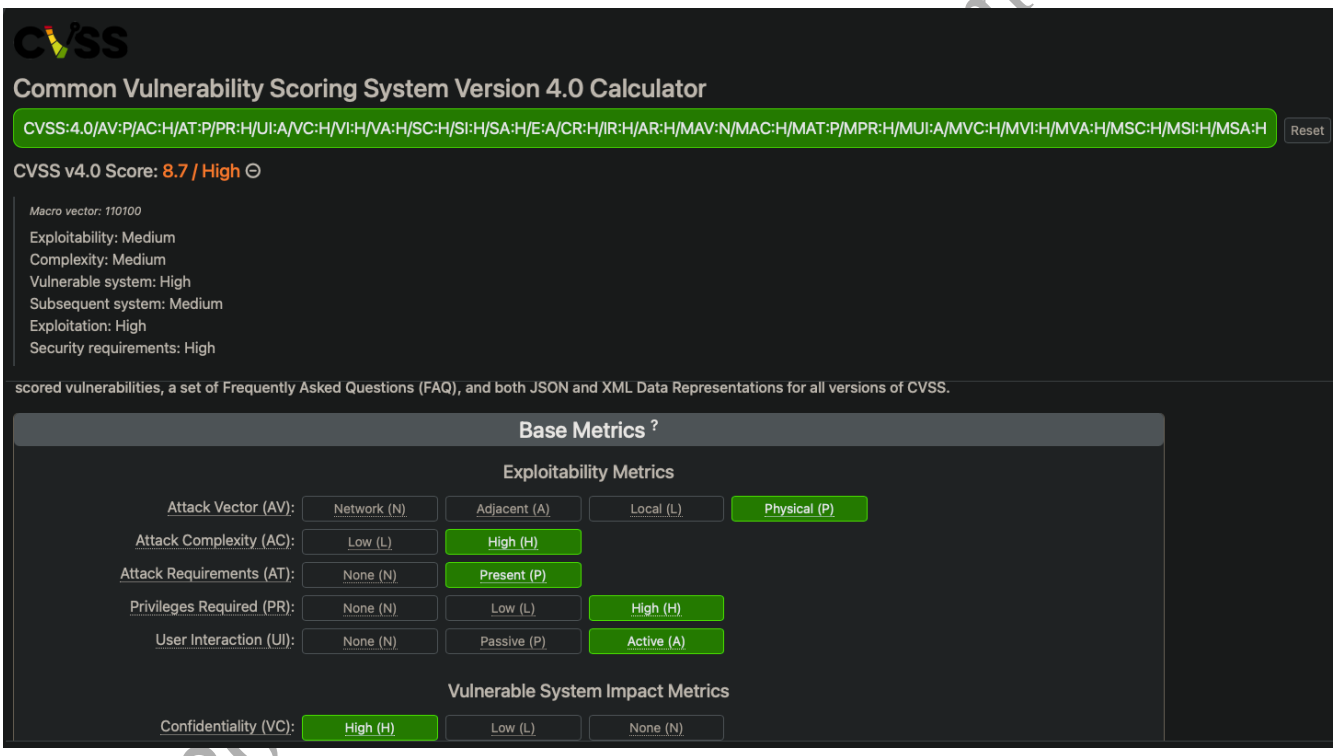
Hodnoticí metriky CVSS v4.0 jsou rozděleny do následujících skupin [33, strana 5]:

1. **Základní metriky (Base Metrics)** – inherentní charakteristiky zranitelnosti, které se nemění v čase ani prostředí.

2. **Metriky potenciálu vzniku hrozby (Threat Metrics)** – zohledňují, zda je zranitelnost aktivně zneužívána.

3. **Metriky prostředí (Environmental Metrics)** – reflektují konkrétní prostředí, ve kterém se aktivum nachází.

4. **Doplňkové metriky (Supplemental Metrics)** – poskytují dodatečné informace o charakteru zranitelnosti.

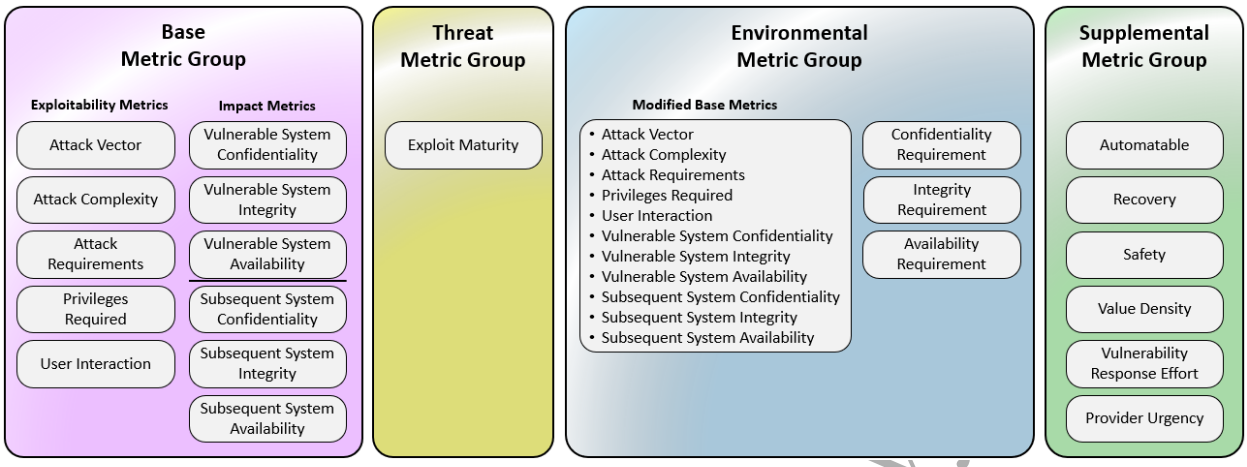


Obrázek 13: Struktura metrik CVSS 4.0 [37]

Každá z těchto skupin obsahuje podrobnější indikátory, jejichž kombinací je vypočítáno výsledné skóre. Praktické hodnocení lze provést pomocí oficiální kalkulačky CVSS 4.0 [37].

1.18.4.1 Příklad hodnocení

Pokud je zranitelnost schopna umožnit útočníkovi spuštění libovolného kódu s administrátorskými oprávněními na cílovém systému, bude její skóre velmi vysoké.



Obrázek 14: Ukázkové hodnocení CVSS převzaté z [36 strana 5, figure 1].

1.18.4.2 Klasifikace skóre

Výsledné skóre je interpretováno následující kvalitativní stupnicí uvedené v tabulce 30:

Tabulka 30: Kvantitativní stupnice CSVV skóre převzaté z [36, strana 27, table 22]

CVSS Score	Kvalitativní hodnocení
0.0	Žádné (None)
0.1 – 3.9	Nízké (Low)
4.0 – 6.9	Střední (Medium)
7.0 – 8.9	Vysoké (High)
9.0 – 10.0	Kritické (Critical)

1.18.5 Stupnice hodnocení zranitelností

Příloha č. 2 Vyhlášky č. 82/2018 Sb. [2] uvádí relativní stupnici hodnocení zranitelností sumarizované v tabulce 31:

Tabulka 31: Relativní stupnice hodnocení zranitelností [2, příloha 2, tabulka 3].

Úroveň	Popis
Nízká	Zranitelnost prakticky neexistuje, pravděpodobnost zneužití je minimální. Opatření dokážou detekovat pokusy o zneužití.
Střední	Pravděpodobnost zneužití je nízká až střední. Opatření jsou zavedena, avšak jejich účinnost je omezená a detekce pokusů je nedostatečná.
Vysoká	Zneužití je pravděpodobné. Opatření nejsou dostatečně komplexní a jejich kontrola není pravidelná. Jsou známy dílčí úspěšné útoky.
Kritická	Zneužití je velmi pravděpodobné až jisté. Opatření buď neexistují, nebo jsou neúčinná. Jsou známy úspěšné pokusy o zneužití.

1.18.6 Katalog zranitelností

Dle § 5 odst. 1 písm. b) u Vyhlášky č. 82/2018 Sb. je nutné vytvořit katalog zranitelností s využitím přílohy číslo 3. Vyhlášky č. 82/2018 Sb. [2] konkrétní, doslovné znění zranitelností je sepsáno v tabulce 32.

Tabulka 32: Obsah katalogu zranitelností dle přílohy č.3 VKB [2]

Číselné označení.	**Název kategorie**
1	Nedostatečná údržba informačního a komunikačního systému
2	Zastaralost informačního a komunikačního systému
3	Nedostatečná ochrana vnějšího perimetru
4	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů
5	Nevhodné nastavení přístupových oprávnění
6	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
7	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování
8	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí
9	Nedostatečná ochrana aktiv
10	Nevhodná bezpečnostní architektura
11	Nedostatečná míra nezávislé kontroly
12	Neschopnost včasného odhalení pochybení ze strany zaměstnanců

Po vyjmenování zranitelností se provádí mapování zranitelností na aktiva.

1.19 Hrozby

1.19.1 Definice hrozby

Hrozba představuje potenciální jev nebo událost, která může vyvolat nežádoucí incident a ohrozit informační aktiva, procesy či infrastrukturu organizace. Systematická klasifikace hrozeb umožňuje jejich efektivnější identifikaci, vyhodnocení a následné řízení [35].

1.19.2 Klasifikace hrozeb dle původu

1. **Přírodní hrozby** – vznikají v důsledku přírodních jevů a katastrof. *Příklady:* povodně, požáry, zemětřesení, vichřice, pandemie.
2. **Hrozby vyplývající z lidského faktoru** – souvisejí s činností člověka, ať již vědomou nebo nevědomou. *Příklady:* nedbalost zaměstnance (smazání dat), úmyslný útok insidera, phishing, útoky hackerů.

1.19.3 Klasifikace hrozeb dle účelu

1. **Náhodné hrozby** – vznikají bez záměru způsobit škodu. *Příklady:* selhání hardware, porucha napájení, softwarová chyba.
2. **Úmyslné hrozby** – cílené jednání s úmyslem poškodit organizaci. *Příklady:* ransomware, distribuované DoS útoky, průmyslová špionáž.
3. **Přirozené hrozby** – plynou z přirozeného opotřebení nebo životního cyklu aktiv. *Příklady:* stárnutí serverů, degradace diskových polí, zastaralost softwaru.
4. **Kryté hrozby** – skryté aktivity, jejichž účelem je zakrýt skutečný záměr. *Příklady:* malware maskovaný jako legitimní aplikace, backdoor v softwaru.

1.19.4 Klasifikace hrozeb dle lokality působnosti

1. **Vnější hrozby** – pramení z prostředí mimo organizaci. *Příklady:* kybernetické útoky z internetu, fyzické živelní pohromy, krádeže vybavení.

2. **Vnitřní hrozby** – mají původ uvnitř organizace. *Příklady:* chybné nastavení přístupových práv, úmyslné jednání zaměstnanců, nedostatečné školení personálu.

1.19.5 Pravděpodobnost výskytu hrozeb

Hodnota hrozby je určena nejen její povahou, ale také pravděpodobností realizace. Pro tento účel se často využívá čtyřstupňová škála uvedené v tabulce 33.

Tabulka 33: Pravděpodobnost realizace hrozby

Úroveň	**Popis**
Nízká	Hrozba prakticky neexistuje nebo je málo pravděpodobná. Předpokládaný výskyt není častější než jednou za 5 let.
Střední	Pravděpodobnost výskytu je nízká až střední. Očekávaný výskyt jednou za 1–5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Očekávaný výskyt jednou za 1 měsíc až 1 rok.
Kritická	Hrozba je velmi pravděpodobná až téměř jistá. Výskyt častější než jednou za měsíc.

1.19.6 Stupnice hodnocení hrozeb

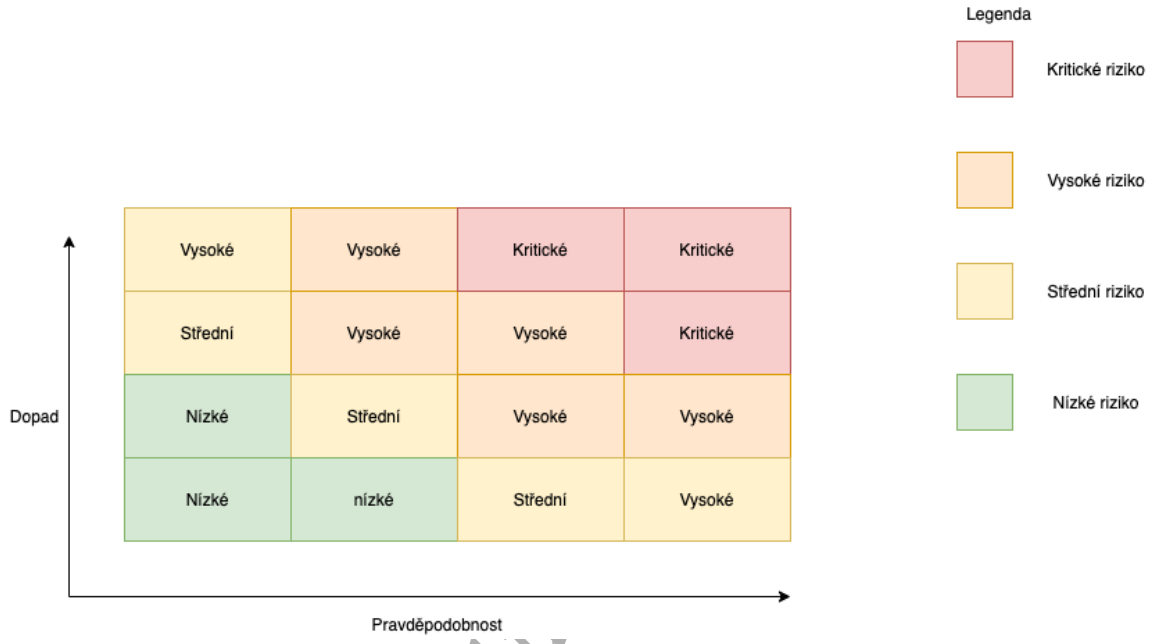
Na základě přílohy č. 2 vyhlášky č. 82/2018 Sb. [2]lze hrozby hodnotit pomocí relativní stupnice uvedené v tabulce 34. Tato tabulka 34 je obdobné té, která se používá pro hodnocení zranitelností s detailní vizualizací v Tabulka 31, a to je také velmi stejné jako tabulka 33.

Tabulka 34: Stupnice hodnocení hrozeb dle vyhlášky č. 82/2018 Sb.

Úroveň	**Popis**
Nízká	Hrozba prakticky neexistuje nebo její realizace je vysoce nepravděpodobná. Existují účinná opatření schopná její včasné odhalení.
Střední	Realizace hrozby je málo pravděpodobná až pravděpodobná. Opatření existují, ale jejich účinnost je omezená a kontrola probíhá nepravidelně.
Vysoká	Realizace hrozby je pravděpodobná až velmi pravděpodobná. Opatření nejsou dostatečně komplexní a jejich účinnost není pravidelně ověřována.
Kritická	Realizace hrozby je velmi pravděpodobná až téměř jistá. Bezpečnostní opatření nejsou zavedena nebo jsou vysoce neúčinná.

1.19.7 Risk matrix: kombinace pravděpodobnosti a dopadu

Pro vizualizaci rizika se v praxi běžně používá **matice rizik**, která kombinuje pravděpodobnost hrozby a závažnost dopadu.



Obrázek 15: Risk matrix (pravděpodobnost × dopad)

Matice poskytuje rychlý přehled o kritických kombinacích (např. vysoká pravděpodobnost a vysoký dopad, tedy červená zóna) a slouží jako nástroj pro prioritizaci opatření.

1.19.8 Katalog hrozeb

Dle § 5 odst. 1 písm. b) u Vyhlášky č. 82/2018 Sb. je nutné vytvořit katalog hrozeb s využitím přílohy číslo 3. Vyhlášky č. 82/2018 Sb. [2] konkrétní, doslovné znění hrozeb je převzaté v tabulce 35.

Tabulka 35: Převzaté konkrétní hrozby z přílohy č.3 VKB [2]

Číselné označení	Popis hrozby
1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů
2	Poškození nebo selhání technického anebo programového vybavení
3	Zneužití identity
4	Užívání programového vybavení v rozporu s licenčními podmínkami
5	Škodlivý kód (například viry, spyware, trojské koně)
6	Narušení fyzické bezpečnosti
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
8	Zneužití nebo neoprávněná modifikace údajů
9	Ztráta, odcizení nebo poškození aktiva
10	Nedodržení smluvního závazku ze strany dodavatele
11	Pochybení ze strany zaměstnanců
12	Zneužití vnitřních prostředků, sabotáž
13	Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní

15	Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
16	Zneužití vyměnitelných technických nosičů dat
17	Napadení elektronické komunikace (odposlech, modifikace)

Po vyjmenování hrozeb nastává mapování hrozeb na zranitelnosti. Tím vzniká triáda provázání **hrozba-zranitelnost-aktivum** v kontextu k hodnocení důvěrnosti, integrity a dostupnosti. Ne všechny hrozby i zranitelnosti působí na různá aktiva stejně. Proto vhodnou kombinatorikou vznikají účelné kombinace, které definují potenciální scénář rizik u patřičných aktiv s určitou prioritizací a tím je pak možné efektivně řídit rizika, ke které pomáhá i již zmíněný risk matrix z obrázku 15.

1.20 Analýza a řízení rizik

1.20.1 Řízení rizik

1.20.1.1 Definice dopadu

Dopad představuje hodnotu škody, která by vznikla u aktiva v případě narušení bezpečnosti informací (tedy triády důvěrnosti, integrity, dostupnosti) [28].

1.20.1.2 Definice rizika

Riziko představuje **možnost vzniku nežádoucí události**, která by mohla negativně ovlivnit informační aktiva, procesy či infrastrukturu organizace. Podle normy ISO/IEC 27005 je riziko definováno jako *kombinace pravděpodobnosti výskytu bezpečnostního incidentu a jeho dopadu* [39]. V kontextu kybernetické bezpečnosti se riziko zpravidla chápe jako funkce hodnoty aktiva, působící hrozby a úrovně zranitelnosti definované následujícím vztahem:

$$R = H \times T \times V$$

kde:

- R = výsledná hodnota rizika,
- H = dopad aktiva (vyplývá z CIA hodnocení aktiv),
- T = pravděpodobnost nebo intenzita hrozby (threat),
- V = míra zranitelnosti (vulnerability).

Tento vztah vyjadřuje, že i vysoce hodnotné aktivum nemusí být kriticky ohrožené, pokud hrozba neexistuje nebo je míra zranitelnosti minimální. Naopak kombinace vysoké hodnoty aktiva, silné hrozby a výrazné zranitelnosti vede k riziku nejvyšší kategorie [28].

1.20.2 Klasifikace rizik

Klasifikace rizik slouží k jejich přehlednému uspořádání a umožňuje organizaci stanovit priority pro zavádění bezpečnostních opatření. Nejčastěji se používá kombinace **kvalitativního** a **kvantitativního hodnocení**, kde:

- **Kvalitativní přístup** znamená, že rizika jsou hodnocena na škále (např. nízké, střední, vysoké, kritické). Výhodou je jednoduchost a rychlost, nevýhodou je určitá subjektivita hodnocení.
- **Kvantitativní přístup** naopak rizika vyčísluje numericky (např. na základě finančních ztrát). Tento přístup poskytuje detailnější pohled, ale vyžaduje více dat a přesnější vstupy.

Klasifikace obvykle probíhá s využitím **rizikové matice**, která na jedné ose zobrazuje pravděpodobnost výskytu a na druhé osa dopad. Výsledkem je vizuální mapa rizik, umožňující rychlou identifikaci prioritních oblastí.

1.20.3 Matice dopadů

Matice dopadů, někdy nazývaná *impact matrix* nebo *consequence matrix*, je nástroj používaný v procesu hodnocení rizik, který se soustředí výhradně na **závažnost následků** (dopadů) určité události, pokud ke ní dojde. Zatímco riziková matice (risk matrix) kombinuje dopad s pravděpodobností, matice dopadů rozebírá jednotlivé úrovně dopadu detailněji, odděleně od otázky pravděpodobnosti.

1.20.3.1 Účel a význam matice dopadů

Matice dopadů umožňuje systematickou klasifikaci dopadů rizik z pohledu různých dimenzí (např. finanční ztráty, reputace, právní dopady, provozní výpadky). Proto slouží jako podklad pro stanovení stupňů závažnosti, které později mohou být využity v rizikové matici jako osa „dopad“ a tím pomáhá zajistit, že hodnocení dopadů není paušální, ale zohledňuje různé aspekty a kontext dané organizace.

1.20.3.2 Obecná struktura matice dopadů

Matice dopadů bývá obvykle uspořádána jako jednorozměrné schéma interpretované v tabulce 36.

Tabulka 36: Matice dopadů

Úroveň dopadu	Popis dopadu	Možné příklady
Minimální / zanedbatelný	Dopad je tak slabý, že nemá praktický význam	kosmetická chyba, dočasné výpadky podpůrných služeb
Nízký	Dopad je patrný, ale zvládnutelný	menší finanční škoda, krátkodobý výpadek
Střední	Dopad je významný a vyžaduje zásah	narušení části služby, zvýšené náklady
Vysoký	Dopad má široký rozsah a závažné důsledky	rozsáhlá finanční ztráta, ztráta důvěry uživatelů
Kritický	Dopad je extrémní, ohrožuje existenci organizace	rozsáhlý výpadek, právní postih, ztráta provozu

Každá organizace si v praxi přizpůsobuje popisy úrovní podle své domény, rozsahu činnosti, legislativních požadavků a rizikového prostředí.

1.20.4 Hodnocení rizik

Hodnocení rizik je systematický proces, při kterém se identifikovaná rizika analyzují z hlediska pravděpodobnosti a dopadu. Cílem je určit úroveň rizika a porovnat ji s akceptovatelnými mezemi organizace [27].

V rámci vyhlášky č. 82/2018 Sb. je hodnocení rizik přímo propojeno s evidencí aktiv a zahrnuje posouzení jejich důvěrnosti, integrity a dostupnosti. Výstupem je **zpráva o hodnocení rizik**, která dokumentuje metody, výsledky a závěry celého procesu.

1.20.5 Metodika řízení rizik

Metodika řízení rizik vychází z mezinárodních norem (ISO/IEC 27001 [27], ISO/IEC 27005 [39]) a z požadavků vyhlášky o kybernetické bezpečnosti. Základním rámcem je cyklus:

1. **Identifikace rizik** – určení aktiv, hrozeb a zranitelností.
2. **Analýza rizik** – určení pravděpodobnosti a dopadu, výpočet rizika.
3. **Hodnocení rizik** – srovnání výsledků s kritérii přijatelnosti.
4. **Zvládání rizik** – rozhodnutí o způsobu reakce (přijetí, snížení, přenesení, odmítnutí).
5. **Monitorování a přezkoumání** – průběžná kontrola účinnosti a adaptace na nové podmínky.

Metodika řízení rizik tak slouží jako most mezi analytickou částí (zjištění stavu) a praktickou implementací opatření (zlepšení stavu).

1.20.6 Kritéria akceptovatelnosti rizik

Součástí metodiky řízení rizik je stanovení kritérií akceptovatelnosti rizik, která vymezují hranici mezi riziky tolerovanými a riziky, jež musí být aktivně řešena. Podle ISO/IEC 27005 představují kritéria akceptovatelnosti *soubor předem definovaných podmínek, na jejichž základě se rozhoduje, zda je riziko přijatelné, či nikoli* [39].

Kritéria stanovuje management organizace s ohledem na regulatorní rámec, vlastní strategii, ekonomické možnosti a ochotu přijímat potenciální ztráty. V praxi může být kritériem například maximální přípustná finanční škoda, maximální délka výpadku kritické služby nebo limitní úroveň reputačního dopadu.

Stanovení kritérií akceptovatelnosti úzce souvisí s **plánem zvládání rizik**. Pokud hodnota rizika nepřesáhne stanovené kritérium, lze jej akceptovat, monitorovat a nepřijímat další opatření. Naopak v případě, že riziko kritérium překračuje, musí být navržena opatření ke snížení, přenesení či odmítnutí rizika.

1.20.7 Zpráva z hodnocení rizik

Výsledkem hodnocení rizik je **zpráva z hodnocení rizik**. Tento dokument musí obsahovat zejména [40]:

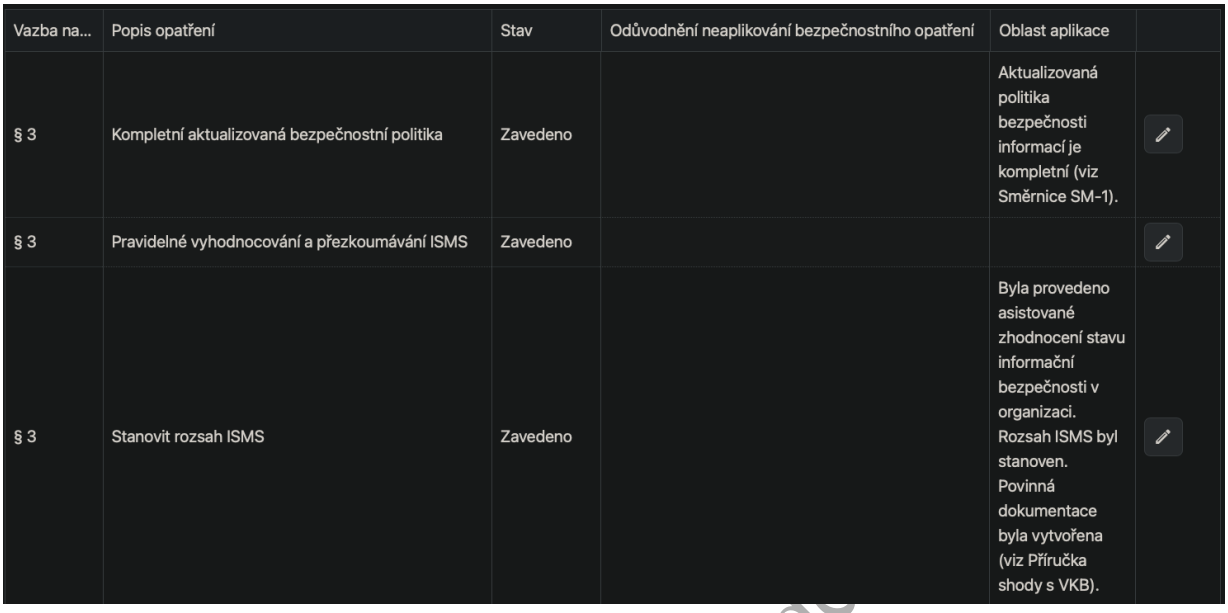
- seznam identifikovaných rizik,
- popis použitých metod hodnocení,
- výsledky analýzy (včetně klasifikace rizik),
- závěry a doporučení pro řízení rizik.

Zpráva slouží nejen jako vnitřní nástroj řízení, ale také jako doklad pro orgány dohledu a pro pozdější interní či externí audit.

1.20.8 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti (SoA, Statement of Applicability) představuje klíčový dokument systému řízení bezpečnosti. Obsahuje seznam všech bezpečnostních opatření, která byla z katalogu opatření vybrána, s uvedením důvodů jejich zahrnutí či vyloučení, jak je vizualizováno na obrázku 16.

SoA tak prokazuje, že organizace vycházela z výsledků hodnocení rizik a přizpůsobila jim výběr opatření. Tento dokument je zásadní pro audity a dohled, protože ukazuje vazbu mezi identifikovanými riziky a přijatými opatřeními [27].



Vazba na...	Popis opatření	Stav	Odůvodnění neaplikování bezpečnostního opatření	Oblast aplikace	
§ 3	Kompletní aktualizovaná bezpečnostní politika	Zavedeno		Aktualizovaná politika bezpečnosti informací je kompletní (viz Směrnice SM-1).	
§ 3	Pravidelné vyhodnocování a přezkoumávání ISMS	Zavedeno			
§ 3	Stanovit rozsah ISMS	Zavedeno		Byla provedeno asistované zhodnocení stavu informační bezpečnosti v organizaci. Rozsah ISMS byl stanoven. Povinná dokumentace byla vytvořena (viz Příručka shody s VKB).	

Obrázek 16: Příklad prohlášení o aplikovatelnosti (vlastní zdroj z ESKO-SW)

1.20.9 Plán zvládání rizik

Plán zvládání rizik stanovuje konkrétní opatření, odpovědnosti, zdroje a časový harmonogram pro implementaci kontrol, které mají rizika snížit na akceptovatelnou úroveň. Typické způsoby zvládání rizik zahrnují:

- přijetí rizika (risk acceptance),
- snížení rizika (risk mitigation),
- přenesení rizika (risk transfer, např. pojištění, outsourcing),
- odmítnutí rizika (risk avoidance).

Plán zvládání rizik je živým dokumentem, který se musí pravidelně aktualizovat v návaznosti na změny prostředí a nově vznikající hrozby [28].

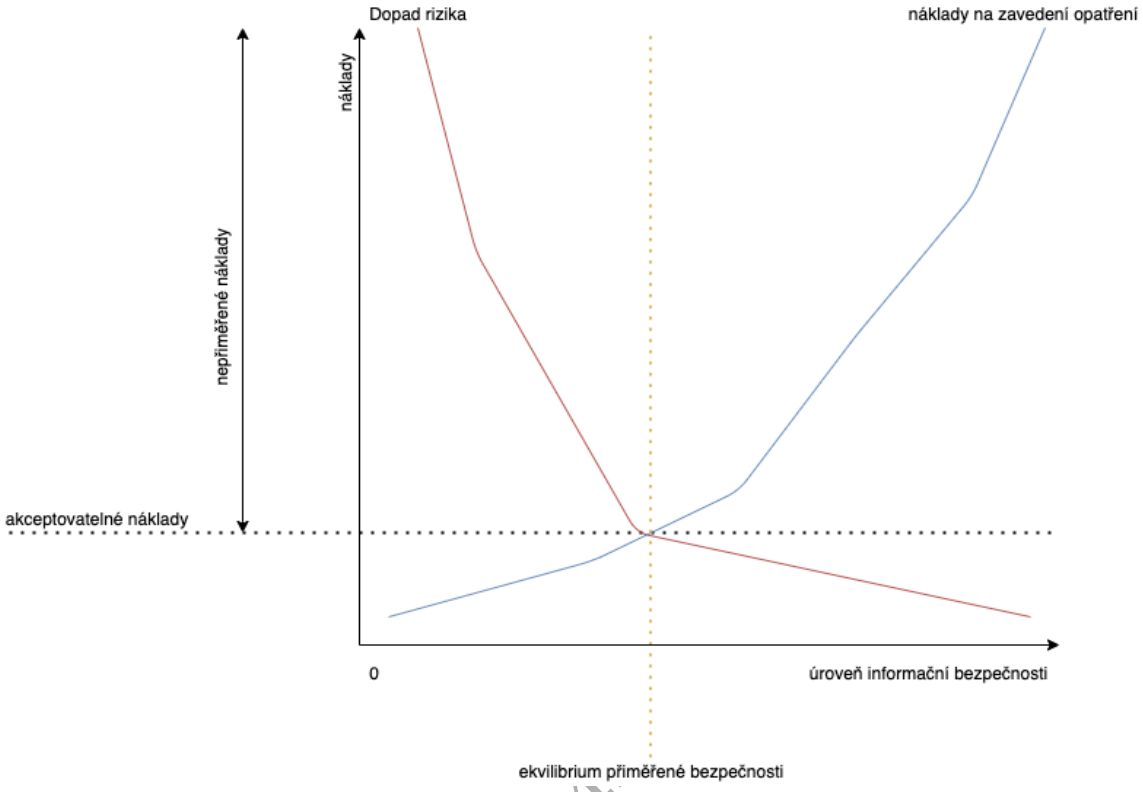
1.20.10 Zavádění opatření

Proces zavádění opatření představuje praktickou realizaci plánu zvládání rizik. Na základě katalogu bezpečnostních opatření vyhlášky č. 82/2018 Sb. organizace implementuje technická a organizační opatření, která odpovídají výsledkům analýzy a hodnocení rizik.

Úspěšné zavedení opatření se posuzuje nejen podle jejich formální existence, ale i podle jejich účinnosti a udržitelnosti v praxi. V tomto smyslu je klíčovým výstupem **shoda s VKB**, tedy stav, kdy lze prokázat, že opatření byla implementována v souladu s legislativními požadavky.

Při zavádění opatření se v praxi bere v potaz, aby bezpečnostní opatření byla ekonomicky smysluplná a přiměřená v porovnáním s potenciálním rizikem u daného aktiva či skupiny aktiv.

Vhodně daný vztah ilustruje obrázek 17.



Obrázek 17: Vztah zavádění opatření v kontextu k nákladům a úrovni informační bezpečnosti

Na vodorovné ose (osa x) obrázku 17 je znázorněna **úroveň informační bezpečnosti**, tedy relativní míra implementace opatření. Na svislé ose (osa y) jsou vyjádřeny **náklady**. Červená křivka představuje **dopad rizik** – při nízké úrovni bezpečnosti je dopad rizika vysoký, avšak se zaváděním opatření postupně klesá. Modrá křivka vyjadřuje **náklady na zavedení opatření** – ty jsou na počátku nízké, ale s rostoucí úrovní zabezpečení výrazně stoupají.

Průsečík obou křivek označuje **ekvilibrium přiměřené bezpečnosti** – bod, ve kterém jsou náklady na opatření vyváženy snížením dopadů rizik. Tento bod je zároveň místem, kde jsou celkové náklady organizace (součet dopadů rizik a nákladů na opatření) nejnižší. Oblast nad úrovní přiměřenosti představuje **nepřiměřené náklady**, kdy dodatečná opatření již nepřinášejí odpovídající snížení rizika, zatímco oblast pod ekvilibriem ukazuje na **nedostatečné zabezpečení**.

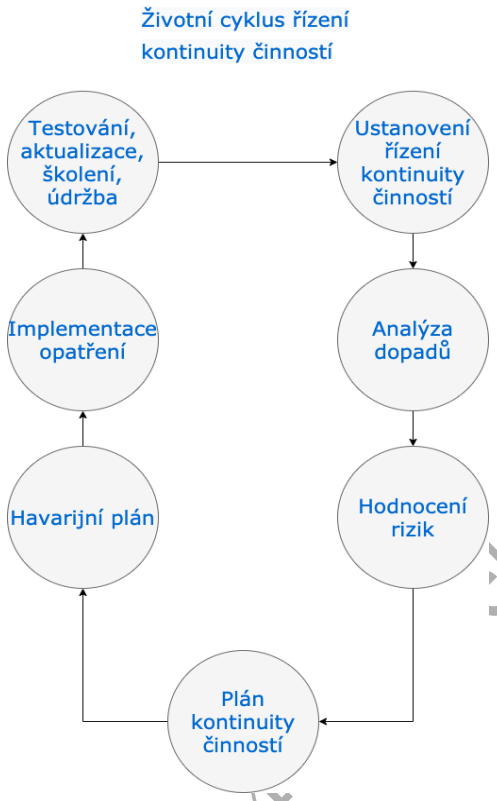
1.21 Řízení kontinuity činností

1.21.1 Definice pojmu

Řízení kontinuity činností představuje procesní rámec, jehož cílem je vytvořit postupy, podle kterých bude možné zajistit funkčnost klíčových procesů, obnovu dat a provoz organizace na předem stanovené minimální úrovni služeb v případě výskytu kybernetického bezpečnostního incidentu či jiné krizové situace [41].
V podmínkách kybernetické bezpečnosti jde především o minimalizaci dopadů incidentů na provoz informačních a komunikačních systémů a služeb, které na nich závisí [2, § 15].

1.21.2 Životní cyklus řízení kontinuity

Řízení kontinuity činností je chápáno jako **cyklický proces**, který zahrnuje fáze plánování, implementace, testování, vyhodnocování a zlepšování. V praxi se opírá o PDCA cyklus **(Plan-Do-Check-Act)**, který zajišťuje, že kontinuita není jednorázovým úkolem, ale dlouhodobě udržovaným systémem. Celý cyklus kontinuity je vizualizován na obrázku 18.



Obrázek 18: Jednotlivé kroky životního cyklu řízení kontinuity činností vycházející z PDCA cyklu

1.21.3 Základní požadavky pro řízení kontinuity

Podle vyhlášky č. 82/2018 Sb.[2, § 15] je povinná osoba v rámci řízení kontinuity činností povinna:

- stanovit práva a povinnosti administrátorů a osob v bezpečnostních rolích, čímž se zajišťuje jasné vymezení odpovědností při řešení krizových situací.
- vyhodnotit a dokumentovat dopady kybernetických incidentů prostřednictvím hodnocení rizik a analýzy dopadů na činnost organizace,
- na základě těchto výstupů stanovit cíle řízení kontinuity činností, které zahrnují:
- minimální úroveň poskytovaných služeb – nejnižší přijatelnou úroveň dostupnosti a funkčnosti systémů a služeb.

- dobu obnovení (Recovery Time Objective, RTO) – maximální čas, ve kterém musí být po incidentu obnovena minimální úroveň poskytovaných služeb.

- bod obnovení dat (Recovery Point Objective, RPO) – časový rozsah, za který musí být data po incidentu či selhání obnovena.

- stanovit politiku řízení kontinuity činností, která kromě cílů zahrnuje i pravidla a odpovědnosti pro vrcholové vedení, dodavatele a další relevantní subjekty,

- vypracovat, testovat, aktualizovat a distribuovat plány kontinuity činností a havarijní plány, aby byla zajištěna připravenost organizace na různé scénáře ohrožení,

- realizovat opatření ke zvýšení odolnosti informačních a komunikačních systémů vůči incidentům a výpadkům dostupnosti (např. redundantní připojení, záložní zdroje energie, geografická diverzifikace datových center).

1.21.4 RTO a RPO

Při řízení kontinuity činností hrají klíčovou roli ukazatele **RTO (Recovery Time Objective)** a **RPO (Recovery Point Objective)**:

- **RTO** představuje maximální dobu, po kterou může být služba nebo systém nedostupný po incidentu, aniž by došlo k nepřijatelnému narušení činnosti organizace.

- **RPO** vyjadřuje časový bod v minulosti, ke kterému lze obnovit data. Jinak řečeno – určuje, kolik dat může být maximálně ztraceno, aniž by to zásadně ohrozilo činnost.

Tyto ukazatele společně definují rámec pro **strategie zálohování, disaster recovery a obnovu služeb**. Příliš krátké RTO/RPO mohou znamenat vysoké náklady, zatímco příliš dlouhé hodnoty ohrozí kontinuitu a důvěru uživatelů [42] [43].

1.21.5 Business Continuity Management (BCM)

Business Continuity Management (BCM) představuje integrovaný přístup, který organizaci umožňuje předvídat, připravit se, reagovat a zotavit se z událostí, jež mohou přerušit její činnosti. BCM zahrnuje jak ICT infrastrukturu, tak klíčové procesy a lidské zdroje.

BCM obvykle zahrnuje:

- Analýzu dopadů na podnikání.
- Stanovení priorit a kritických procesů.
- Plány kontinuity činností, které vymezují role, odpovědnosti a kroky při přerušení provozu.
- Pravidelné testování a cvičení plánů, jejich distribuci a průběžnou aktualizaci.

1.21.6 Disaster Recovery (DR)

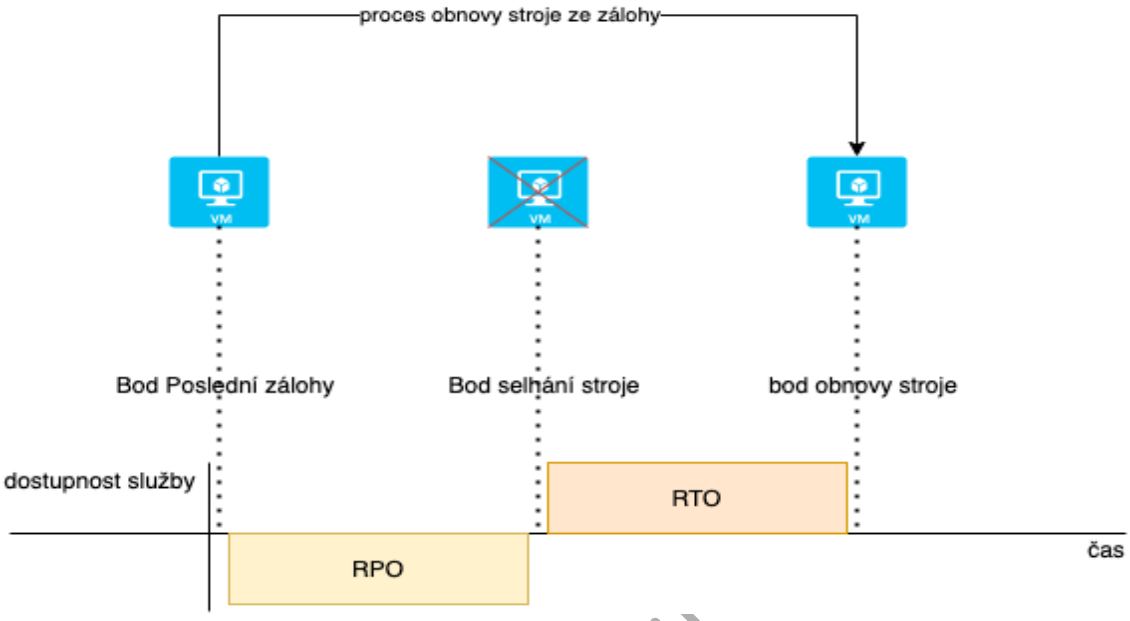
Disaster Recovery (DR) je specifickou součástí BCM, zaměřenou na technickou obnovu IT infrastruktury a dat po incidentu.

Typické prvky DR zahrnují:

- Zálohování a obnova dat.
- Plány obnovy IT infrastruktury (servery, sítě, aplikace).
- Postupy pro návrat k běžnému provozu.

DR tak představuje praktickou realizaci parametrů RTO a RPO. Pokud BCM definuje, že klíčový systém musí být obnoven do 4 hodin (RTO) a ztráta dat nesmí přesáhnout 30 minut (RPO), DR určuje konkrétní technologie a postupy, kterými bude těchto cílů dosaženo.

1.21.7 Vizuální schéma rozdílností mezi RTO a RPO



Obrázek 19: Vztah mezi RTO a RPO

Na obrázku 19 je na vodorovné ose x znázorněna časová osa. Osa y reprezentuje úroveň provozní dostupnosti. Vzniklý incident způsobí přerušení služby a pokles dostupnosti.

Pak:

- **RPO** určuje časový bod, ke kterému je možné data obnovit (zpětně od incidentu).
- **RTO** představuje časový interval potřebný k obnovení minimální úrovně poskytovaných služeb.

1.22 Stanovení bezpečnostních rolí

1.22.1 Úvod o řízení bezpečnostních rolí

V rámci systému řízení kybernetické bezpečnosti (ISMS) vymezeného zákonem č. 181/2014 Sb., o kybernetické bezpečnosti [3], a prováděcí vyhláškou č. 82/2018 Sb. [2] je nezbytné jasně definovat klíčové bezpečnostní role. Tyto role vytvářejí organizační rámec pro efektivní implementaci a dohled nad bezpečnostními opatřeními a jejich správným fungováním. Jejich podrobný popis je specifikován v příloze č. 6 k vyhlášce č. 82/2018 Sb. Dle § 6 VKB odstavce 5. je povinné zajištění zastupitelnosti bezpečnostních rolí.

Následující část se zaměřuje obecněji na pět zásadních rolí [44]:

- Výbor pro řízení kybernetické bezpečnosti.
- Manažera kybernetické bezpečnosti.
- Architekta kybernetické bezpečnosti.
- Auditora kybernetické bezpečnosti.
- Bezpečnostní odbor.

1.22.2 Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti představuje kolektivní orgán, jehož úkolem je koordinovat a řídit aktivity v oblasti ochrany informačních a komunikačních systémů. Členy výboru jsou zástupci vrcholového vedení a **manažer kybernetické bezpečnosti**, doplnění o odborníky z oblasti ICT a bezpečnosti. Výbor zajišťuje strategické směřování, koordinaci činností a nastavuje prioritní opatření v souladu s právními požadavky i potřebami organizace. Jeho existence zajišťuje, že rozhodování o bezpečnostních otázkách probíhá na adekvátní úrovni řízení a má podporu vedení.

1.22.3 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je klíčovou rolí. Jeho hlavní odpovědností je dohled nad implementací bezpečnostních opatření a zajištění jejich kontinuálního fungování. Tato role vyžaduje nejen odbornou způsobilost doloženou praxí či certifikací, ale také schopnost pravidelně informovat vrcholové vedení o stavu kybernetické bezpečnosti. Manažer působí jako spojovací článek mezi strategickou a operativní úrovní, čímž umožňuje efektivní přenos informací a rozhodnutí. Vzhledem k významu této pozice je nezbytné, aby byla nezávislá na provozních ICT rolích, a tím se minimalizovalo riziko střetu zájmů.

1.22.4 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti se zaměřuje na návrh a implementaci bezpečné architektury ICT prostředí. Jeho úkolem je zajistit, aby informační a komunikační systémy byly vystavěny v souladu s principy důvěrnosti, integrity a dostupnosti. Architekt se podílí na koncepčních návrzích bezpečnostních opatření, od úrovně infrastruktury až po aplikační vrstvu, a garantuje, že zavedená řešení odpovídají legislativním a normativním požadavkům. Tato role vyžaduje vysokou míru odbornosti a schopnost reagovat na aktuální hrozby i technologický vývoj. V praxi je často architektem kybernetické bezpečnosti architekt IT nebo vedoucí pracovník IT.

1.22.5 Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti představuje nezávislou roli, jejímž hlavním úkolem je provádět audity v oblasti kybernetické bezpečnosti a hodnotit účinnost zavedených opatření. Auditor musí disponovat odbornou způsobilostí, praxí a znalostí auditních metodik. Jeho nezávislost na ostatních bezpečnostních rolích zajišťuje objektivitu hodnocení a poskytuje vedení organizace důvěryhodnou zpětnou vazbu o stavu kybernetické bezpečnosti. Výsledky práce auditora tvoří důležitý podklad pro rozhodování výboru a manažera kybernetické bezpečnosti a společně tak přispívají k neustálému zlepšování.

1.22.6 Odbor bezpečnostní

Bezpečnostní odbor (v širším smyslu organizační útvar zajišťující kybernetickou a informační bezpečnost) integruje jednotlivé role a poskytuje institucionální rámec pro jejich fungování. Zajišťuje procesní, metodickou i provozní podporu a disponuje odpovídajícími pravomocemi i rozpočtovými zdroji. Jeho úkolem je nejen realizace opatření v souladu s interními směrnicemi a legislativními požadavky, ale i systematický rozvoj bezpečnostního povědomí zaměstnanců. Odbor bezpečnostní tak představuje klíčový prvek z hlediska dlouhodobé udržitelnosti a zralosti celého systému řízení bezpečnosti.

1.23 RACI matice

1.23.1 Úvod a obecný základ RACI matice

RACI matice představuje široce využívaný nástroj projektového a procesního řízení, jehož cílem je jednoznačné vymezení rolí a odpovědností jednotlivých aktérů v rámci určité aktivity nebo projektu. Zkratka **RACI** je tvořena počátečními písmeny čtyř anglických pojmů, které vymezují klíčové role [44]:

- **Responsible** – osoby nebo týmy, které jsou přímo odpovědné za provedení daného úkolu či aktivity. Nesou odpovědnost za samotnou realizaci, nikoli však za konečný výsledek.
- **Accountable** – jednotlivec, který nese konečnou odpovědnost za úkol a jeho výsledek. Tento subjekt je autoritou, která úkol schvaluje a garantuje jeho správné provedení.
- **Consulted** – osoby či skupiny poskytující rady, odborné znalosti nebo doporučení. V praxi se jedná o konzultační roli, která obvykle probíhá formou obousměrné komunikace.
- **Informed** – subjekty, které by měli být o průběhu a výsledcích informovány, aniž by aktivně vstupovaly do rozhodovacího nebo realizačního procesu. Zpravidla se jedná o jednosměrnou komunikaci.

1.23.2 Výhody využití RACI matice

Mezi hlavní přínosy zavedení RACI matice patří zejména zvýšení transparentnosti při řízení projektů, minimalizace nejasností v odpovědnostech a snadnější koordinace týmové spolupráce i komunikace. Jasné rozdělení rolí zároveň umožňuje předejít duplicitám a sporům, kdo je zodpovědný za konkrétní výstup. V kontextu komplexních projektů je tak RACI matice efektivním prostředkem pro podporu komunikace a řízení očekávání zainteresovaných stran.

1.23.3 Nevýhody využití RACI matice

Na druhou stranu se s využitím tohoto přístupu pojí i určité nevýhody. Jedná se především o riziko nadměrného formalismu, kdy matice může být vnímána jako byrokratická zátěž, zejména v dynamickém prostředí s rychle se měnícími prioritami. Údržba matice si vyžaduje pravidelnou aktualizaci, jinak hrozí její zastarání a ztráta relevance. Dalším limitem je i možnost nesprávné interpretace jednotlivých rolí, což může vést k neefektivnímu využívání tohoto nástroje a v neposlední řadě u velkých projektů může být RACI matice velmi složitá a tím neposkytovat cílený efekt.

1.23.4 Příklad RACI matice

Činnosti	Výbor KB	Odbor bezpečnostní	Manažer KB	Auditor KB	Architekt KB	Gestor PrA	Gestor PoA	Garant PrA	Garant PoA	Pověřenec pro OOÚ	Odbor ICT	Další osoby
												(osoby, které řeší incidenty a události)
Vytvoření katalogu zranitelností		A	R		R	R	R	R	R	C	C	C (osoby, které řeší incidenty a události)
Schválení metodiky pro identifikaci a hodnocení rizik	A	R	I	I	I	I	I	I	I	I	I	
Identifikace kombinací aktiv, hrozeb a zranitelností (výstup – identifikovaná rizika)		A	R		R	R	R	R	R			
Stanovení konkrétní hodnot hrozeb a zranitelností pro aktiva		A	R		C	R	R	R	R			
Výpočet výsledné hodnoty rizika, návrh způsobu zvládání rizik a výběr bezpečnostních opatření do plánu zvládání rizik		A	R		R	R	R	R	R			
Vytvoření plánu zvládání rizik		A	R		C	C	C	C	C			
Schválení plánu zvládání rizik	A	R	I	I	I	I	I	I	I		I	
Vytvoření zprávy o hodnocení aktiv a rizik	I	A	R		I	I	I	I	I		I	
Souhlas se zbytkovými riziky	A, R											
Vytvoření prohlášení o aplikovatelnosti	I	A	R		C	C	C	C	C			
Zavádění bezpečnostních opatření		A	R		R	C	C	C	C		C	
Sledování a přezkoumávání rizik, zohlednění výstupů interního auditu a významných změn, zohlednění opatření podle § 11 ZKB, pravidelná aktualizace celého procesu řízení aktiv a rizik	I	A	R		C	C	C	C	C	C	C	

Obrázek 20: RACI matice převzatá z [25, Strana 27]

Legenda k obrázku 20:

Levý první sloupec nám definuje seznam činností k realizaci.

V horní části prvního řádku jsou definovány jednotlivé zájmové strany a ve společném průniku je definice zodpovědností.

Pak například pro schválení metodiky pro identifikaci a hodnocení rizik je vykonavatelem odbor bezpečnosti, výbor KB je zodpovědný za kontrolu doručené metodiky a její správnost. Ostatní strany jsou jen informovány o průběhu.

1.24 Řízení dodavatelů

1.24.1 Úvod k řízení dodavatelů

Řízení dodavatelů představuje klíčovou součást systému řízení kybernetické bezpečnosti, jelikož dodavatelé a externí partneři mají často přímý nebo nepřímý přístup k informačním a komunikačním systémům organizace. Správně nastavené vztahy s dodavateli, jejich evidence a řízení rizik spojených s jejich činností jsou zásadní pro zajištění odolnosti celého prostředí [28].

1.24.2 Povinnosti organizace v oblasti řízení dodavatelů

Podle § 8 vyhlášky č. 82/2018 Sb. [2] je povinná osoba povinna stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací, a tato pravidla prokazatelně komunikovat všem dodavatelům, zejména těm, kteří jsou klasifikováni jako významní. Současně je nutné vést evidenci významných dodavatelů a pravidelně kontrolovat, zda jsou stanovená pravidla i smluvní podmínky skutečně dodržovány.

Mezi hlavní povinnosti patří zejména:

- stanovení pravidel pro dodavatele, která zahrnují požadavky na bezpečnostní opatření a procesy v souladu s ISMS,
- evidence významných dodavatelů a jejich **prokazatelné písemné informování** o této skutečnosti,
- seznamování dodavatelů s bezpečnostními pravidly a vyžadování jejich dodržování,
- řízení rizik spojených s dodavateli, a to jak v rámci předsmluvní analýzy, tak v průběhu spolupráce,
- zajištění smluvních ujednání o bezpečnostních opatřeních a odpovědnostech (zejména v souladu s přílohou č. 7 VKB),

- pravidelné přezkoumávání plnění smluv a kontrola realizace bezpečnostních opatření.

1.24.3 Politika řízení dodavatelů

Organizace musí mít zpracovanou politiku řízení dodavatelů, jejíž obsah je vymezen v příloze č. 5 odst 1.4 Vyhlášky č. 82/2018 Sb. [2]. Tato politika představuje ucelený rámec, jenž stanovuje pravidla, povinnosti a principy pro řízení dodavatelských vztahů. Minimální obsah politiky zahrnuje:

1. Pravidla a principy pro výběr dodavatelů,
2. Pravidla pro hodnocení rizik souvisejících s dodavateli,
3. Náležitosti smlouvy o úrovni služeb (SLA) a stanovení odpovědnosti za realizaci opatření,
4. Pravidla pro provádění kontroly zavedení bezpečnostních opatření,
5. Pravidla pro hodnocení dodavatelů.

1.24.4 Významný dodavatel a provozovatel

Zvláštní pozornost je věnována institutu **významného dodavatele**, který je definován v § 2 písm. n) VKB [2] jako subjekt, jehož vztah s povinnou osobou je významný z hlediska bezpečnosti informačního a komunikačního systému.

Do této kategorie dodavatelů spadá také **provozovatel**, tj. orgán nebo osoba zajišťující funkčnost technických a programových prostředků či komunikačních systémů. Provozovatel je tak **podmnožinou** významných dodavatelů.

1.24.5 Prokazatelné informování dodavatele

Pokud je dodavatel vyhodnocen jako významný, musí být o této skutečnosti **prokazatelně informován**. Dokumentace musí obsahovat minimálně:

1. identifikaci správce nebo provozovatele,
2. identifikaci informačního a komunikačního systému,
3. identifikaci významného dodavatele,
4. vyrozumění o skutečnosti, že dodavatel je evidován jako významný (popřípadě i jako provozovatel),
5. obsah pravidel, která musí dodavatel dodržovat.

Optimální praxí je začlenění těchto informací přímo do dokumentu seznamujícího dodavatele s pravidly, a to s písemným potvrzením, které prokazuje, že byl s pravidly a svou významností seznámen.

1.24.6 Obsah smluv s významnými dodavateli

Vyhláška č. 82/2018 Sb. [2] rovněž stanovuje prostřednictvím přílohy č. 7 konkrétní bezpečnostní požadavky pro smluvní vztahy s významnými dodavateli. Obsah smluv musí zahrnovat především:

- ustanovení o ochraně informací (důvěrnost, dostupnost, integrita),
- ustanovení o oprávnění užívat data,
- ustanovení o autorských právech k programovému kódu a licencích,
- ustanovení o možnosti kontroly a auditu dodavatele, včetně pravidel zákaznických auditů,
- ustanovení o řetězení dodavatelů s povinností přenést závazky i na poddodavatele,
- ustanovení o dodržování bezpečnostních politik povinné osoby nebo o jejich schválení ze strany povinné osoby,

- ustanovení o řízení změn,
- ustanovení o souladu smlouvy s právními předpisy,
- povinnost dodavatele informovat o kybernetických bezpečnostních incidentech, způsobech řízení rizik, významných změnách vlastnictví nebo ovládání,
- specifikaci podmínek při ukončení smlouvy (např. migrace dat, přechodné období při ukončení služby),
- podmínky pro začlenění dodavatelů do plánů kontinuity činností,
- podmínky pro předávání dat a provozních informací správci,
- pravidla pro likvidaci dat,
- ustanovení o právu odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem,
- ustanovení o sankcích za porušení povinností.

Tyto požadavky mají zajistit, aby smluvní vztahy nebyly pouze formální, ale obsahovaly konkrétní a vymahatelná bezpečnostní ujednání, která významně posilují bezpečnostní postavení povinné osoby.

1.24.7 Proces řízení dodavatelů

Metodika NÚKIB definuje proces řízení dodavatelů jako sled kroků, které musí povinná osoba realizovat, tedy:

- stanovit politiku řízení dodavatelů,
- evidovat a informovat významné dodavatele,
- provádět analýzy rizik a předsmluvní posouzení,

- zahrnout bezpečnostní požadavky do smluvních vztahů,
- provádět pravidelné hodnocení a kontrolu plnění opatření (např. prostřednictvím zákaznických auditů).

Důsledné řízení dodavatelů je nezbytné nejen z hlediska souladu s legislativou, ale také pro zajištění důvěryhodnosti a odolnosti organizace jako celku. Nedostatečná kontrola dodavatelských vztahů může vést k významným bezpečnostním incidentům, neboť právě dodavatelé často představují nejslabší článek v dodavatelském řetězci spolu s lidskými zdrojemi.

1.25 Bezpečnost lidských zdrojů

1.25.1 Úvod do bezpečnosti lidských zdrojů

Lidské zdroje představují jednu z důležitých oblastí kybernetické bezpečnosti, protože zaměstnanci, administrátoři i externí dodavatelé mohou být současně největším přínosem i slabinou organizace. Z pohledu systému řízení bezpečnosti informací je proto nezbytné zavést mechanismy, které zajistí jak prevenci, tak i průběžnou kontrolu jejich činností. Právě v této oblasti klade § 9 vyhlášky č. 82/2018 Sb. [2] důraz na plán rozvoje bezpečnostního povědomí, pravidelná školení, evidenci a postupy při porušení pravidel. Mezi naprosto výborné školení ze strany NUKIB patří online kurz "Dávej kyber" [45], který svým rozsahem pokrývá minimální potřebný základ pro proškolení zaměstnanců.

1.25.2 Plán rozvoje bezpečnostního povědomí

Plán rozvoje bezpečnostního povědomí je koncepční dokument, který stanovuje formu, obsah a rozsah vzdělávání uživatelů, administrátorů, osob zastávajících bezpečnostní role i dodavatelů. Jeho cílem je (v teorii) zajistit, aby všichni aktéři rozuměli svým povinnostem a byli schopni předcházet rizikům spojeným s provozem informačních a komunikačních systémů.

Podle doporučení NÚKIBu by plán měl obsahovat zejména: [46]

- obsah a termíny poučení uživatelů, administrátorů a osob v bezpečnostních rolích,
- obsah a termíny školení nových zaměstnanců,
- přehledy s uvedením předmětu školení a seznamem osob, které školení absolvovaly,
- způsoby hodnocení účinnosti plánu a jednotlivých školení,
- stanovení odpovědnosti za tvorbu a aktualizaci plánu i za realizaci činností.

V praxi se vedením a aktualizací tohoto plánu zpravidla zabývá **manažer kybernetické bezpečnosti**. Plány bývají uloženy v personálních systémech organizace, kde jsou vedeny údaje o termínech školení, jejich náplni a výsledcích (splněno/nesplněno, případně s výstupním testem).

1.26 Řízení provozu a komunikací

Jedním ze základních pilířů bezpečného fungování informačních a komunikačních systémů je správně nastavené řízení provozu a komunikací a s ním úzce související řízení změn. Tyto procesy zajišťují, aby systémy byly provozovány konzistentně, bezpečně a aby každá provedená změna byla řádně posouzena z hlediska rizik i možných dopadů na kybernetickou bezpečnost.

Řízení provozu a komunikací se zaměřuje na každodenní provozní pravidla a postupy, jejichž cílem je zajistit bezpečný a stabilní chod informačních systémů. Podle § 10 vyhlášky č. 82/2018 Sb. musí povinná osoba stanovit a udržovat soubor provozních pravidel, která zahrnují zejména [2]

- dokumentování práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role,
- postupy pro spuštění a ukončení chodu systémů, včetně restartů a obnovy po selhání,
- pravidla pro detekci a vyhodnocování kybernetických bezpečnostních událostí a ochranu záznamů o těchto událostech,
- pravidla pro ochranu před škodlivým kódem (antivirová strategie),
- procesy řízení technických zranitelností, například prostřednictvím pravidelného skenování,
- jasně definované kontaktní osoby odpovědné za technickou a systémovou podporu,
- pravidla pro řízení a schvalování provozních změn,
- postupy pro sledování, plánování a řízení kapacit lidských a technických zdrojů,
- pravidla pro ochranu informací a dat během celého životního cyklu,

- postupy pro instalaci a správu technických aktiv,
- pravidelné zálohování, testování čitelnosti záloh a zajištění jejich bezpečného uložení,
- pravidla pro zajištění bezpečnosti síťových služeb.

Důležitým požadavkem je rovněž **oddělení vývojového, testovacího a provozního prostředí**, aby se předešlo nechtěným zásahům do produkčních systémů. Testovací prostředí by mělo co nejvěrněji simulovat prostředí produkční, přičemž testovací data musí být anonymizována.

Aktualizace provozních pravidel a postupů musí probíhat vždy v návaznosti na provedené změny systému, aby byla zachována jejich aktuálnost a účinnost.

1.27 Řízení změn

S řízením provozu úzce souvisí také proces řízení změn, jehož cílem je zajistit, aby každá významná změna v systému byla předem posouzena z hlediska bezpečnosti a aby její realizace neohrozila stabilitu a funkčnost prostředí.

Podle § 11 vyhlášky č. 82/2018 Sb. [2] je povinná osoba povinna:

- přezkoumávat možné dopady změn a určovat, zda se jedná o **významnou změnu**,
- dokumentovat řízení významných změn,
- provádět analýzu rizik a přijímat opatření k minimalizaci nepříznivých dopadů,
- aktualizovat související bezpečnostní politiku a dokumentaci,
- zajistit testování změn před jejich uvedením do provozu,
- zavést mechanismy pro návrat do původního stavu (tzv. roll-back).

Za **významnou změnu** se považuje taková změna, která může mít zásadní vliv na kybernetickou bezpečnost a představuje vysoké riziko [2, § 11, písm o)]. Posouzení je vždy v kompetenci organizace.

Příklady významných změn zahrnují:

- akvizici nového systému nebo modulu,
- změnu významného dodavatele, se kterým dosud nebyla zkušenost,
- reakci na varování NÚKIB před novou hrozbou,
- změny v organizační struktuře ovlivňující řízení bezpečnosti,
- úpravy topologie v síti,

- výměnu či pořízení nových bezpečnostních nástrojů (firewall, SIEM, DDoS ochrana) nebo obnova hardwaru (servery, switche apod.).

Na základě analýzy rizik může být navíc rozhodnuto o provedení penetračního testování nebo testování zranitelností, zejména pokud změna zasahuje důležitá aktiva.

1.28 Řízení přístupů (Identity access management)

Řízení přístupu představuje jednu ze stěžejních oblastí kybernetické bezpečnosti, neboť zajišťuje, aby se k informačním a komunikačním systémům dostaly pouze oprávněné osoby a prostředky. Cílem je minimalizovat riziko neoprávněného přístupu a zneužití autentizačních údajů, což je potřebné pro zachování důvěrnosti, integrity a dostupnosti dat.

V kontextu k řízení přístupů jsou tři základní pojmy:

1. Autorizace
2. Autentizace
3. RBAC

Autentizace je proces, kdy se ověří, že osoba přihlašující se k různým systému je onou danou osobou. Například s využitím loginu, hesla a MFA.

Autorizací se rozumí autorizace a přiřazení práv pro přístupy k různým zdrojům.

RBAC (Role-Based Access Control), neboli *řízení přístupu na základě rolí*, představuje jeden z nejrozšířenějších modelů řízení přístupových oprávnění. Tento model přiřazuje oprávnění **nikoli jednotlivým uživatelům**, ale **rolím**, které odrážejí pracovní pozice nebo funkce v organizaci. Každý uživatel je následně zařazen do jedné nebo více rolí, čímž automaticky získává odpovídající oprávnění dle jeho pracovní pozice. RBAC model také platí pro systémové účty.

1.28.1 Základní principy řízení přístupu

Podle § 12 vyhlášky č. 82/2018 Sb. [2] musí povinná osoba řídit přístup na základě provozních a bezpečnostních potřeb. Každému uživateli, administrátorovi, aplikaci i technickému účtu je přidělen **jednoznačný identifikátor**, který umožňuje zpětně dohledat vykonavatele operací v systému. Přístupová práva se spravují prostřednictvím **RBAC**, čímž se zajišťuje systematické a přehledné přiřazování oprávnění.

Mezi základní typy účtů patří:

- **privilegované účty**, které umožňují administrátorské úkony,
- **uživatelské účty**, sloužící k běžné práci,
- **technické účty**, využívané aplikacemi nebo službami.

Specifickou oblastí je také využívání soukromých zařízení (*Bring Your Own Device – BYOD*). V takových případech je žádoucí zavést **Mobile Device Management (MDM)**, který umožňuje správu konfigurace, distribuci aktualizací, monitoring či zálohování mobilních zařízení připojených do firemní infrastruktury.

1.28.2 Opatření k ochraně přístupů

Organizace je povinna zavést soubor opatření, která zajišťují autentizaci, autorizaci a brání zneužití přístupů. Tato opatření zahrnují:

- Zavedení bezpečnostních opatření pro používání mobilních zařízení, včetně těch, která nejsou ve správě organizace.
- Omezení přidělování privilegovaných oprávnění pouze na úroveň nezbytně nutnou (*princip need-to-know*).
- Pravidelnou kontrolu a přezkoumávání všech přístupových oprávnění, včetně jejich rozdělení do skupin a rolí.
- Zavedení pravidel pro používání softwaru a hardwaru, který by mohl narušit bezpečnost (např. kontrola USB zařízení, antivirová opatření nebo i bossware).

1.28.3 Politika hesel a autentizace

Minimální bezpečnostní standard i VKB [2, § 19] stanovují povinnosti v oblasti správy a používání hesel. Tyto požadavky lze shrnout následovně:

- **Minimální délka hesla**:
- 12 znaků pro běžné uživatele
- 17 znaků pro administrátory a technické účty
- **Maximální délka**: možnost použít alespoň 64 znaků
- **Komplexita**: systém nesmí omezovat použití malých a velkých písmen, číslic a speciálních znaků.
- **Správa hesel**: zákaz použití běžně známých či opakujících se hesel, paměť pro minimálně 12 posledních hesel, povinná změna nejméně jednou za 18 měsíců.
- **První použití hesla**: po prvním přihlášení musí být heslo bezodkladně změněno.
- **Obnova hesla**: dočasná hesla pro obnovu přístupu musí mít omezenou platnost (max. 60 minut).

V případě, že je autentizace založena pouze na heslech, je nutné doplnit ji o další opatření, například kryptografické klíče nebo vícefaktorovou autentizaci (MFA).

1.28.4 Správa a životní cyklus přístupů

Správně nastavený systém řízení přístupů zahrnuje celý životní cyklus účtů a oprávnění:

1. **Registrace a vytvoření identity** – uživateli nebo administrátorovi je přidělen identifikátor a odpovídající oprávnění.
2. **Aktivní fáze** – pravidelné využívání účtu a přidělených oprávnění, která jsou průběžně kontrolována.
3. **Změna role či pracovní pozice** – při přesunu zaměstnance na jinou pozici se provádí úprava oprávnění.

4. **Ukončení smluvního vztahu** – přístupová oprávnění musí být okamžitě odebrána, aby nedošlo k jejich zneužití.

Veškeré procesy přidělování a odebírání přístupových oprávnění musí být **dokumentovány**, aby byla zajištěna dohledatelnost a možnost auditu.

1.28.5 Privilegované účty a bezpečnostní politika

Zvláštní pozornost si zaslouží **privilegované účty**. Ty nesmí být sdílené a každý administrátor musí mít kromě privilegovaného účtu i účet běžného uživatele pro činnosti, které privilegia nevyžadují. V rámci politiky řízení přístupu je nezbytné stanovit jasná pravidla pro:

- Omezení používání privilegovaných účtů.
- Využívání nástrojů pro správu a ověřování identity a pro řízení přístupových oprávnění.
- Prosazování bezpečného používání autentizačních údajů (hesel, certifikátů, kryptografických klíčů, MFA).

1.29 Ochrana před škodlivým kódem, zaznamenávání a detekce událostí, zvládání incidentů a kryptografie

1.29.1 Ochrana před škodlivým kódem

Ochrana před škodlivým kódem představuje preventivní opatření pro zajištění bezpečného provozu informačních a komunikačních systémů. Povinné osoby musí implementovat nepřetržitou automatickou ochranu všech klíčových aktiv – koncových stanic, serverů, mobilních zařízení, úložišť, sítí a síťových prvků. Jinými slovy – používat antivir.

Současně musí být monitorováno používání výměnných médií a potlačeno automatické spouštění obsahu z těchto zařízení. Pro zajištění integrity prostředí je vhodné omezit oprávnění ke spouštění kódu pouze na důvěryhodné aplikace.

Doporučení od NÚKIBu [47] je užívat:

- segmentaci sítí (oddělení provozní a správcovské části pomocí VLAN),
- instalaci nástrojů pro detekci a odstranění malware,
- denní aktualizaci antivirových databází,
- testování aktualizací v izolovaném prostředí,
- zákaz neschváleného softwaru v produkčním prostředí,
- blokování vzdáleného spouštění kódu mimo řízené prostředí.

1.29.2 Zaznamenávání událostí, retence a synchronizace času

Zaznamenávání událostí je klíčovým prvkem pro zajištění forenzní dohledatelnosti a bezpečnostního auditu. Povinné osoby jsou povinny zaznamenávat všechny bezpečnostní a provozní události důležitých aktiv, včetně přihlášení, správy účtů, administrátorských činností, chybových hlášení a pokusů o manipulaci s logy.

Vyhláška stanovuje povinnost:

- uchovávat záznamy **nejméně 18 měsíců** (resp. 12 měsíců u vybraných subjektů),
- synchronizovat systémový čas minimálně 1× za 24 hodin,
- chránit logy před neoprávněným čtením a úpravou.

1.29.3 Detekce a vyhodnocování kybernetických událostí

Detekce kybernetických událostí slouží k včasné identifikaci nežádoucí aktivity v síti. Vyhláška požaduje využití nástroje, který umožňuje:

- ověření a kontrolu přenášených dat,
- blokování nežádoucí komunikace,
- detekci hrozeb v rámci koncových stanic, serverů a síťových prvků.

Na vyšší úrovni má být zaveden nástroj pro sběr a nepřetržité vyhodnocování událostí (SIEM), který umožňuje korelaci dat, včasné varování a identifikaci potenciálních incidentů. Důležitá je také pravidelná aktualizace detekčních pravidel a zpětná analýza výstupů.

1.29.4 Řízení bezpečnostních incidentů

Efektivní řízení incidentů zahrnuje kategorizaci, evidenci a testování reakčních procesů. Povinné osoby musí být schopny:

- rozpoznat kybernetický incident,
- zajistit jeho okamžité ohlášení příslušnému orgánu,
- dokumentovat jeho průběh a dopady,
- analyzovat příčiny a přijmout nápravná opatření.

Podle doporučení NÚKIB je vhodné mít formálně zpracovanou Politiku zvládání kybernetických bezpečnostních incidentů, která určuje odpovědnosti, kontaktní osoby, eskalační schéma a způsob testování plánů [47].

1.29.5 Aplikační a síťová bezpečnost

V oblasti aplikační bezpečnosti musí být provedeno penetrační testování před uvedením systému do provozu i po významných změnách. Povinná osoba zajišťuje trvalou ochranu aplikací, informací a transakcí proti neoprávněné činnosti a zneužití.

Součástí je i zajištění bezpečnosti síťových služeb a oddělení vývojového, testovacího a produkčního prostředí [47].

1.29.6 Kryptografické prostředky

Ochrana citlivých aktiv je zajištěna pomocí kryptografických prostředků. Povinná osoba musí:

- používat aktuálně odolné kryptografické algoritmy a klíče,
- mít implementovaný systém správy klíčů a certifikátů,
- zajistit auditovatelnost všech operací s kryptografickými materiály,
- prosazovat bezpečné nakládání s kryptografickými klíči a certifikáty.

NÚKIB doporučuje šifrování disků, přenosných médií a bezpečné ukládání hesel [47].

1.30 Audit

1.30.1 Definice auditu

Pojem *audit* pochází z latinského slova *audire*, což znamená „naslouchat“ nebo „slyšet“. Historicky se jednalo o proces, při kterém auditor naslouchal výpovědím o správě majetku a ověřoval jejich správnost. V moderním kontextu se audit vyvinul v systematický proces **ověřování, zda určité činnosti, záznamy nebo systémy odpovídají stanoveným požadavkům, normám nebo pravidlům** [48].

Audit je dle autora definován jako

> „Systematické a nezávislé zkoumání, jehož cílem je stanovit, zda činnosti a související výsledky odpovídají plánovaným opatřením, zda jsou tato opatření účinně zaváděna a zda jsou vhodná k dosažení stanovených cílů“ [48].

Obecně lze audit chápat jako nástroj zajišťování důvěry a prověřování kvality – auditor třetí straně poskytuje nezávislý pohled na dodržování pravidel, kvalitu procesů či správnost údajů.

Audit se uplatňuje v mnoha oblastech, od finančního řízení, přes management kvality, environmentální řízení, až po oblast informační a kybernetické bezpečnosti. Společným prvkem všech auditů je důraz na nezávislost hodnotitele, systematičnost postupu a schopnost poskytnout věrohodný závěr.

1.30.2 Audit kybernetické bezpečnosti

V oblasti informační a kybernetické bezpečnosti se audit stal zásadním nástrojem pro ověřování správnosti a účinnosti zavedených bezpečnostních opatření. Vyhláška č. 82/2018 Sb. definuje auditora kybernetické bezpečnosti a k němu povinnosti jako například provádět pravidelná a nezávislá přezkoumání.

Audit tedy provádí osoba splňující požadavky stanovené v § 7 odst. 4 VKB (tedy Auditor kybernetické bezpečnosti), který hodnotí soulad organizace s právními předpisy, interními dokumenty, smluvními závazky a nejlepší praxí [2, § 16].

Účelem auditu kybernetické bezpečnosti je nejen kontrola shody s VKB, ale také identifikace nesouladů a jejich náprava. Výsledky auditu musí být zohledněny v plánu zvládání rizik a v plánu rozvoje bezpečnostního povědomí, čímž se audit stává nedílnou součástí procesu neustálého zlepšování. Audit tak neslouží pouze jako nástroj dozoru, ale i jako mechanismus zvyšování odolnosti organizace vůči novým hrozbám.

Audit VKB je vhodné realizovat v pravidelných intervalech

- jednou za tři roky v celém rozsahu požadavků v případě správce a provozovatele významného informačního systému,
- jednou za dva roky v případě ostatních povinných osob,
- kdykoliv, kdy dojde k významné změně.

1.31 PDCA cyklus

1.31.1 Definice pojmu

PDCA cyklus, známý také jako *Demingův cyklus*, představuje model neustálého zlepšování procesů. Akronym vychází z anglických výrazů:

1. **P**lan (*naplánuj*)
2. **D**o (*udělej*)
3. **C**heck (*zkontroluj*)
4. **A**ct (*jednej*)

Jedná se o iterativní mechanismus, jehož cílem je systematická optimalizace procesů prostřednictvím plánování, implementace, kontroly výsledků a následné úpravy postupů. Model se uplatňuje ve výrobě, řízení kvality i v oblasti informační bezpečnosti.

Autorem a popularizátorem konceptu je **William Edwards Deming** [49], který jej sám připisoval svému mentorovi **Walteru Shewhartovi** [50].

1.31.2 Struktura PDCA cyklu

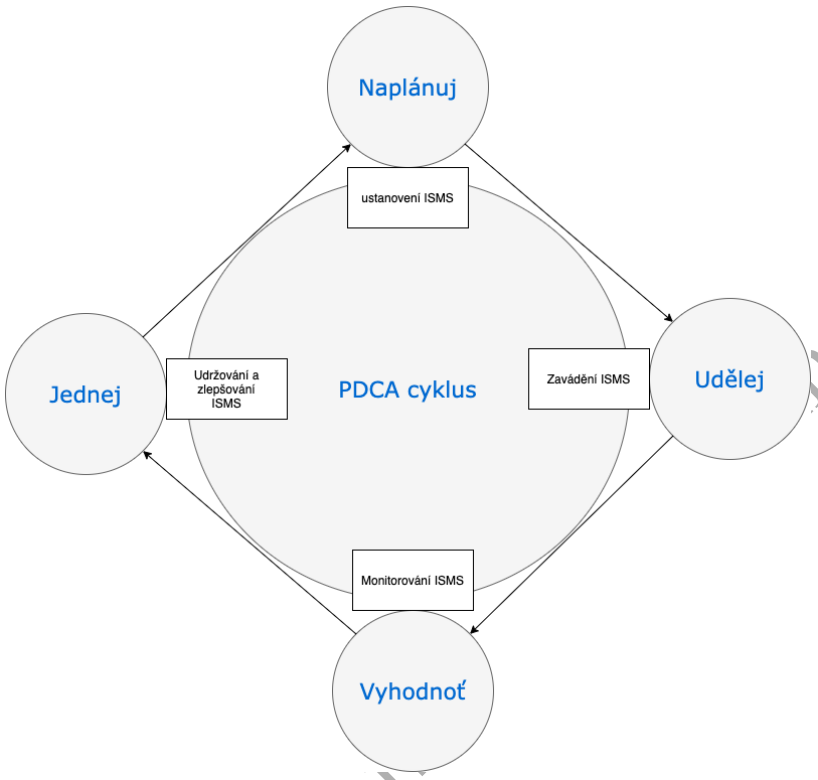
Jednotlivé fáze cyklu jsou popsány v tabulce 37 spolu s charakteristikou popisu dané fáze.

Tabulka 37: Podrobnější popis jednotlivých fází PDCA cyklu

Fáze (EN)	Fáze (CZ)	Charakteristika
Plan	Naplánuj	Identifikace problémů, sběr dat, návrh nápravných opatření.
Do	Udělej	Realizace a implementace navržených kroků.
Check	Zkontroluj	Vyhodnocení výsledků, porovnání s plánem, analýza efektivity.
Act	Jednej	Zavedení opatření ke zlepšení a zpřesnění budoucího plánování.

1.31.3 PDCA cyklus v kontextu ISMS

V oblasti **řízení informační bezpečnosti (ISMS)** slouží PDCA cyklus jako základní rámec pro zavádění a neustálé zlepšování systému řízení bezpečnosti informací, jak je vizualizováno na obrázku 21. Umožňuje organizaci reagovat na nové hrozby, adaptovat bezpečnostní opatření a plnit legislativní požadavky.



Obrázek 21: PDCA cyklus v kontextu k ISMS

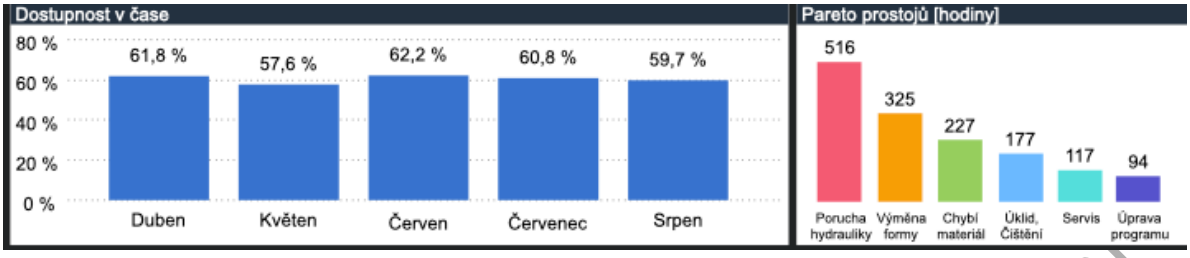
1.31.4 Aplikace PDCA cyklu v praxi

Praktickou ukázku může představovat fiktivní společnost **Hydraulikoservis s.r.o.**, výrobce hydraulických komponent pro automobilový průmysl. Společnost provozuje přibližně 100 strojů v režimu 24/7, přičemž monitoring opakovaně odhalil prostojové situace způsobené poruchami hydraulických systémů.

1.31.4.1 Fáze *Plan* (Plánuj)

Na základě historických dat byly jako nejčastější příčina prostojů identifikovány poruchy hydrauliky. Cílem plánování se stalo snížení průměrného počtu prostojů na maximálně 2

hodiny měsíčně u jednoho stroje. Posbíraná data jsou na obrázku 22.



Obrázek 22: Modelová ne/dostupnost strojů v čase a k tomu přidružená Paretův princip analýzy prostojů

Navržená opatření k nápravě mohou být:

- krátkodobá: pravidelná kontrola oleje, školení pracovníků, zavedení protokolů,
- střednědobá: SLA s dodavatelem na rychlou výměnu dílů,
- dlouhodobá: vývoj kvalitnějších komponent nebo změna dodavatele.

1.31.4.2 Fáze *Do* (Udělej)

Byla zavedena denní kontrola hydraulického oleje, týdenní vyhodnocování protokolů, přidělení odpovědných osob a školení zaměstnanců.

1.31.4.2.1 SMART cíl

Je definován takto:

- **Specifický:** snížit prostoje způsobené poruchami hydrauliky.
- **Měřitelný:** redukce z 17,2 hodin prostojů denně u 100 strojů.
- **Dosažitelný:** díky novým kontrolním mechanismům.
- **Relevantní:** historická data potvrzují kritičnost problému.
- **Časově ohraničený:** implementace probíhá denně a týdně.

1.31.4.3 Fáze *Check* (Zkontroluj)

Probíhá průběžné sledování účinnosti opatření a porovnání dosažených výsledků s plánovanými cíli.

1.31.4.4 Fáze *Act* (Jednej)

Na základě vyhodnocení byla zavedena nová opatření. Bylo například zjištěno, že ačkoli výměny oleje snížily poruchovost, současně zvýšily náklady a nároky na skladování. Tyto poznatky byly použity jako vstup do dalšího cyklu

Citace

[1] EUROPEAN PARLIAMENT AND COUNCIL. *Směrnice (EU) 2022/2555 (NIS2)* [online]. 2022 [vid. 2025-10-25]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.CES

[2] ZÁKONY PRO LIDI. *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. § 16 Audit kybernetické bezpečnosti.* [online]. 2018 [vid. 2025-10-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[3] ZÁKONY PRO LIDI. Zákon 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi* [online]. 2014 [vid. 2025-10-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[4] EUROPEAN PARLIAMENT AND COUNCIL. EUR-Lex – Access to European Union law. *EUR-Lex – Access to European Union law* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://eur-lex.europa.eu/CS/legal-content/glossary/directive.html

[5] EUROPEAN PARLIAMENT AND COUNCIL. *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)* [online]. 2016 [vid. 2025-10-25]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

[6] NÚKIB. Průvodce novým zákonem o kybernetické bezpečnosti - obecné informace o NIS2. *NÚKIB* [online]. 2025 [vid. 2025-10-26]. Dostupné z: https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-obecne-informace-o-smernici-nis2

[7] ZÁKONY PRO LIDI. Zákon 264/2025 Sb. Zákon o kybernetické bezpečnosti (nový). *Zákony pro lidi* [online]. [vid. 2025-10-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-264

[8] NÚKIB. *NÚKIB - Nový zákon o kybernetické bezpečnosti byl podepsán prezidentem* [online]. 2025 [vid. 2025-10-27]. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2274-novy-zakon-o-kyberneticke-bezpecnosti-byl-podepsan-prezidentem/

[9] *Základy správního práva: učební text pro bakalářské studium*. 2. vydání. Brno: Masarykova univerzita, 2017. ISBN 978-80-210-8517-6.

[10] ÚŘAD VLÁDY ČR. *Legislativní pravidla vlády* [online]. 2023 [vid. 2025-10-25]. Dostupné z: https://vlada.gov.cz/assets/jednani-vlady/legislativni-pravidla/Legislativni-pravidla-vlady-s-prilohami-platna-od-1--unora-2023.pdf

[11] NÚKIB. Strategie pro oblast kybernetické bezpečnosti [online]. nedatováno. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/strategie_kb_2012-2015.pdf

[12] NBÚ. *NBÚ - Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011* [online]. 2011 [vid. 2025-10-27]. Dostupné z: https://www.nbu.cz/cs/aktualne/867-994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/

[13] ZÁKONY PRO LIDI. Zákon 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících záko... *Zákony pro lidi* [online]. 2017 [vid. 2025-10-27]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[14] *NÚKIB - Vznik* [online]. 2025 [vid. 2025-10-27]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/

[15] NÚKIB. Průvodce novým zákonem o kybernetické bezpečnosti. *NÚKIB* [online]. 2025 [vid. 2025-10-26]. Dostupné z: https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti

[16] RADEK VYMAZAL. Web projektu nukibator.cz. *NUKIBATOR* [online]. [vid. 2025-10-27]. Dostupné z: https://nukibator.cz/

[17] EUROPEAN COMMISSION, DG GROW. *Uživatelská příručka k definici MSP* [online]. 2019 [vid. 2025-10-25]. Dostupné z: https://data.europa.eu/doi/10.2873/4104. ECGuide:2019

[18] MINISTERSTVO PRŮMYSLU A OBCHODU (MPO). *Příručka k použití definice malých a středních podniků* [online]. B.m.: Ministerstvo průmyslu a obchodu ČR. 2021 [vid. 2025-10-25]. Dostupné z: https://mpo.gov.cz/assets/cz/podnikani/dotace-a-podpora-podnikani/oppik-2014-2020/spolecne-prilohy-dotacnich-programu-op-pik/2021/1/Prirucka-k-pouziti-definice-MSP.pdf. MPOGuide:2021

[19] MINISTERSTVO SPRAVEDLNOSTI ČESKÉ REPUBLIKY. *Veřejný rejstřík a Sbírka listin - Ministerstvo spravedlnosti České republiky* [online]. 2025 [vid. 2025-10-26]. Dostupné z: https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=82790709&subjektId=553561&spis=687875

[20] ZÁKONY PRO LIDI. *Sněmovní tisk 759/0 – Návrh zákona o kybernetické bezpečnosti* [online]. 2024 [vid. 2025-10-25]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=9&t=759

[21] ZÁKONY PRO LIDI. Vyhláška 408/2025 Sb. Vyhláška o regulovaných službách. *Zákony pro lidi* [online]. [vid. 2025-10-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-408

[22] ZÁKONY PRO LIDI. Vyhláška 334/2025 Sb. Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na někter... *Zákony pro lidi* [online]. [vid. 2025-10-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-334

[23] ZÁKONY PRO LIDI. Zákon 274/2001 Sb. Zákon o vodovodech a kanalizacích. *Zákony pro lidi* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2001-274

[24] ZÁKONY PRO LIDI. Vyhláška 412/2025 Sb. Vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů clou... *Zákony pro lidi* [online]. [vid. 2025-10-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2025-412

[25] NÚKIB. *NÚKIB - Režim povinností podle zákona o kybernetické bezpečnosti* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://portal.nukib.gov.cz/rezim-povinnosti

[26] NÚKIB. *NÚKIB - Podpůrný materiál - Systém a rozsah ISMS v1.0 (Podpůrný materiál)* [online]. 2022 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Podpurny_material_system_a_rozsah_ISMS_v1.0.pdf

[27] ČAS – ČESKÁ AGENTURA PRO STANDARDIZACI. *ČSN EN ISO/IEC 27001 (369797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky* [online]. Norma. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) / Česká agentura pro standardizaci. 2023 [vid. 2025-10-25]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27001-369797-250275.html

[28] NÚKIB. *NÚKIB - řízení dodavatelů* [online]. 2023 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Metodika-rizeni-dodavatelu.pdf

[29] FIRST.ORG, INC. Traffic Light Protocol (TLP) Version 2.0 [online]. 2022, (FIRST:TLPv2) [vid. 2025-10-25]. Dostupné z: https://www.first.org/tlp/docs/v2/tlp-v2-cz.pdf

[30] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). NÚKIB - Doporučení pro sdílení informací a práci s nimi. *Doporučení pro sdílení informací a práci s nimi* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/sdileni-informaci/#zkracene-zneni-tlp-protokolu-pro-e-mailovou-komunikaci-v-anglicke-verzi

[31] MISP PROJECT. *PAP Taxonomy* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://www.misp-project.org/taxonomies.html#_pap

[32] MISP PROJECT. *PAP Taxonomy – machinetag.json* [online]. 2025 [vid. 2025-10-25]. Dostupné z: https://raw.githubusercontent.com/MISP/misp-taxonomies/refs/heads/main/PAP/machinetag.json

[33] NÚKIB. *NÚKIB - Podpůrný materiál - Doporučení ke sdílení informací a práci s nimi* [online]. 2025. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Doporuceni-ke-sdileni-informaci-ke-stazeni.pdf

[34] NIST. *NVD -SPECTRE - cve-2017-5753* [online]. [vid. 2025-10-27]. Dostupné z: https://nvd.nist.gov/vuln/detail/cve-2017-5753

[35] W3 SCHOOLS. *SQL Injection* [online]. [vid. 2025-10-27]. Dostupné z: https://www.w3schools.com/sql/sql_injection.asp

[36] FIRST.ORG, INC. *Common Vulnerability Scoring System v4.0: Specification Document* [online]. 2024 [vid. 2025-10-25]. Dostupné z: https://www.first.org/cvss/v4.0/specification-document

[37] Common Vulnerability Scoring System Version 4.0 Calculator. *FIRST — Forum of Incident Response and Security Teams* [online]. [vid. 2025-10-27]. Dostupné z: https://www.first.org/cvss/calculator/4-0

[38] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru* [online]. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2. Dostupné z: https://www.knihydobrovsky.cz/kniha/kyberneticka-ne-bezpecnost-problematika-bezpecnosti-v-kyberprostoru-429539892

[39] ČAS – ČESKÁ AGENTURA PRO STANDARDIZACI. *ČSN ISO/IEC 27005 (369790) Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací* [online]. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) / Česká agentura pro standardizaci. 2019 [vid. 2025-10-25]. Dostupné z: https://www.technicke-normy-csn.cz/csn-iso-iec-27005-369790-199779.html

[40] NÚKIB. *NÚKIB - Podpůrný materiál - PŘÍLOHA 9: ZPRÁVA O HODNOCENÍ RIZIK – MINISTERSTVO PRO CERTIFIKACI SENZORŮ* [online]. 2022 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Ploha%209%20-%20Vzorov%20zprva%20o%20hodnocen%20rizik.pdf

[41] NÚKIB. *Kurz - Šéfuj kyber 25: Paragraf - 15* [online]. 2025 [vid. 2025-10-26]. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=4035

[42] NAKIVO. RTO vs RPO: Key Differences Explained. *NAKIVO* [online]. 26. září 2022 [vid. 2025-10-26]. Dostupné z: https://www.nakivo.com/blog/rpo-and-rto-difference/

[43] LIUZZO, Maria. RPO and RTO: What's the Difference? *Veeam Software Official Blog* [online]. 2. únor 2024 [vid. 2025-10-26]. Dostupné z: https://www.veeam.com/blog/recovery-time-recovery-point-objectives.html

[44] NÚKIB. *NÚKIB - Podpůrný materiál - Bezpečnostní role a jejich začlenění v organizaci (verze 3.1)* [online]. 2022 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/bezpenostn-role_v3.1.pdf

[45] NÚKIB. *Kurz - Dávej kyber 25: Přivítání, vstupní informace, nejčastější dotazy* [online]. 2025 [vid. 2025-10-27]. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=4043

[46] NÚKIB. *Kurz - Šéfuj kyber 25: Paragraf - 9* [online]. 2025 [vid. 2025-10-26]. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=4029

[47] NÚKIB. *NÚKIB - Podpůrný materiál - Minimální bezpečnostní standard v1.2* [online]. 2023 [vid. 2025-10-25]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[48] SEDLÁČEK, Jaroslav. *Základy auditu* [online]. 1. vyd. Brno: Masarykova univerzita, 2006. ISBN 978-80-210-4168-4. Dostupné z: https://www.digitalniknihovna.cz/mzk/view/uuid:bd7c1e50-87c3-11e7-b92d-005056827e51?page=uuid:854da950-97df-11e7-8dbe-005056827e51

[49] ISNIAH, Sarah, Humiras PURBA a Fransisca DEBORA. Plan do check action (PDCA) method: literature review and research issues. *Jurnal Sistem dan Manajemen Industri* [online]. 2020, **4**, 72–81. Dostupné z: doi:10.30656/jsmi.v4i1.2186

[50] *PDCA* [online]. 2025 [vid. 2025-10-27]. Dostupné z: https://en.wikipedia.org/w/index.php?title=PDCA&oldid=1306478463

Seznam použitých zkratek

Zkratka	Celý název
ZKB	Zákon o kybernetické bezpečnosti
nZKB	nový Zákon o kybernetické bezpečnosti
VKB	Vyhláška o kybernetické bezpečnosti
IS	Informační systém
NIS2	Network and Information Security 2
KBU	Kybernetická bezpečnostní událost
KBI	Kybernetický bezpečnostní incident
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
KB	Kybernetická bezpečnost/kybernetické bezpečnosti
FTE	Full time employment (Práce ha hlavní pracovní poměr)
PAP	Permissible Actions Protocol
TLP	Traffic light protocol
DR	Disaster recovery
BCM	Business continuity management
NÚKIB	Národní ústav pro kybernetickou bezpečnost

Seznam obrázků

Obrázek 1: Časová osa vývoje ZKB 33
Obrázek 2: Schéma procesu VKB 42
Obrázek 3: Satos Prostějov a.s. – výkaz zisků a ztrát 48
Obrázek 4: Satos Prostějov a.s. - Bilanční rozvaha 49
Obrázek 5: Satos Prostějov a.s. - Výkaz zisků a ztrát 50
Obrázek 6: Bilanční rozvaha – Pasiva společnosti Satos Prostějov a.s. 51
Obrázek 7: Bilanční rozvaha – Aktiva společnosti Satos Prostějov a.s. 52
Obrázek 8: Vizualizace vazeb a vztahů vlastnictví pro výpočet partnerského podniku 59
Obrázek 9: Vizualizace vazeb a vztahů vlastnictví pro výpočet propojeného podniku 61
Obrázek 10: Kritéria pro identifikaci regulované služby (sekce 10 – Vodní hospodářství) 65
Obrázek 11: Rozhodovací diagram procesu samoidentifikace na příkladu vodárny 66
Obrázek 12: Schéma procesu zavádění ISMS 72
Obrázek 13: Struktura metrik CVSS 4.0 [37] 102
Obrázek 14: Ukázkové hodnocení CVSS převzaté z [36 strana 5, figure 1]. 103
Obrázek 15: Risk matrix (pravděpodobnost × dopad) 109
Obrázek 16: Příklad prohlášení o aplikovatelnosti (vlastní zdroj z ESKO-SW) 117
Obrázek 17: Vztah zavádění opatření v kontextu k nákladům a úrovní informační bezpečnosti 119
Obrázek 18: Jednotlivé kroky životního cyklu řízení kontinuity činností vycházející z PDCA cyklu 121
Obrázek 19: Vztah mezi RTO a RPO 124
Obrázek 20: RACI matice převzatá z [25, strana 27] 129
Obrázek 21: PDCA cyklus v kontextu k ISMS 153
Obrázek 22: Modelová ne/dostupnost strojů v čase a k tomu přidružená Paretův princip analýzy prostojů 154

Seznam tabulek

Tabulka 1: Seznam odvětví vysoké kritičnosti (převzato z [1], annex I]).....21
Tabulka 2: Další kritické odvětví (převzato z [1, annex II]).....23
Tabulka 3: Struktura členění ZKB.....28
Tabulka 4: Části zrušené ze ZKB.....28
Tabulka 5: Přehled hlavních povinností dle NÚKIBu [15].....34
Tabulka 6: Přehled struktury VKB.....36
Tabulka 7: Vybraná technická opatření z VKB.....38
Tabulka 8: Klíčové rozdíly mezi ZKB a VKB.....40
Tabulka 9: Detailnější popis kroků realizace shody s VKB.....44
Tabulka 10: Prahové hodnoty pro výpočet velikosti podniku (převedeno z [18, strana 4]) 53
Tabulka 11: Modelový příklad parametrů pro výpočet u Connectica s.r.o.....54
Tabulka 12: Kritéria a vyhodnocení Connectica s.r.o.....54
Tabulka 13: Modelový příklad parametrů pro výpočet u Connectica Investments s.r.o.....55
Tabulka 14: Kritéria a vyhodnocení Connectica Investments s.r.o.....55
Tabulka 15: Hodnoty pro partnerský podnik.....58
Tabulka 16: Hodnoty pro propojený podnik.....60
Tabulka 17: Sumace srovnání rozdílnosti vlastnictví podniků.....62
Tabulka 18: Přehled jednotlivých vyhlášek o regulovaných službách v nZKB.....64
Tabulka 19: Detailnější srovnání rozdílů mezi režimem vyšší a nižší povinnosti.....69
Tabulka 20: Sumace logiky procesu shody s ISMS.....73
Tabulka 21: Povinná struktura politik VKB.....75
Tabulka 22: Hodnotící atributy míry poškození aktiva.....78
Tabulka 23: Doporučené úrovně hodnocení dostupnosti aktiv.....79
Tabulka 24: Extrakce doporučené členění podpůrných aktiv [28, strana 52].....84
Tabulka 25: Srovnání metodiky pro hodnocení dědičnosti vazeb mezi primárními a podpůrnými aktivy.....89
Tabulka 26: Označení a pravidla užívání šíření dat při užití TLP.....93
Tabulka 27: Převzaté označení a podmínky užití PAP [30].....95
Tabulka 28: Příklady použití kombinací TLP a PAP.....98
Tabulka 29: Příklad zranitelností z praxe.....101
Tabulka 30: Kvantitativní stupnice CSVV skóre převzaté z [36, strana 27, table 22].....103
Tabulka 31: Relativní stupnice hodnocení zranitelností [2, příloha 2, tabulka 3].....104
Tabulka 32: Obsah katalogu zranitelností dle přílohy č.3 VKB [2].....105
Tabulka 33: Pravděpodobnost realizace hrozby.....107
Tabulka 34: Stupnice hodnocení hrozeb dle vyhlášky č. 82/2018 Sb.....108
Tabulka 35: Převzaté konkrétní hrozby z přílohy č.3 VKB [2].....110
Tabulka 36: Matice dopadů.....114
Tabulka 37: Podrobnější popis jednotlivých fází PDCA cyklu.....152

Seznam příloh

Příloha 01 - P01_Seznamy_aktiv.pdf
Příloha 02 - P02_Analyza_rizik.pdf
Příloha 03 - P03_Prehled_bezpecnostnich_opatreni.pdf
Příloha 04 - P04_PoA.pdf
Příloha 05 - P05_Plan_zvladani_rizik.pdf
Příloha 06 - P06_technicke_zranitelnosti.pdf
Příloha 07 - SM-1_Systém řízení IB a KB.docx
Příloha 08 - SM-2_Řízení aktiv.docx
Příloha 09 - SM-3_Organizační bezpečnost.docx
Příloha 10 - SM-4_Řízení dodavatelů.docx
Příloha 11 - SM-5_Bezpečnost lidských zdrojů.docx
Příloha 12 - SM-6_Řízení provozu a komunikací.docx
Příloha 13 - SM-7_Řízení přístupu.docx
Příloha 14 - SM-8_Bezpečné chování uživatelů.docx
Příloha 15 - SM-9_Zálohování a obnovy a archivace.docx
Příloha 16 - SM-10_Bezpečné předávání a výměny informací.docx
Příloha 17 - SM-11_Řízení technických zranitelností.docx
Příloha 18 - SM-12_Bezpečné používání mobilních zařízení.docx
Příloha 19 - SM-13_Akvizice vývoj a údržba.docx
Příloha 20 - SM-14_Ochrana osobních údajů.docx
Příloha 21 - SM-15_Fyzická bezpečnost.docx
Příloha 22 - SM-16_Bezpečnost komunikační sítě.docx
Příloha 23 - SM-17_Ochrana před škodlivým kódem.docx
Příloha 24 - SM-18_Nasazení a používání nástroje pro detekci BU.docx
Příloha 25 - SM-19_Využití a_údržba nástroje.docx
Příloha 26 - SM-20_Kryptografická_ochrana.docx
Příloha 27 - SM-21_Řízení změn.docx
Příloha 28 - SM-22_Formular_hlaseni_incidentu.pdf*
Příloha 29 - SM-22_Zvládání kybernetických bezpečnostních incidentů.docx
Příloha 30 - SM-23_Řízení kontinuity činností.docx