

OBSAH

O autorech XI

Seznam použitých zkratk XIII

Úvod XVIII

Část první Kybernetický incident z pohledu IT

1. Základní pojmy 3

1.1 Základní pojmy 3

1.2 Bezpečnost informací 5

1.3 Systém řízení informační bezpečnosti (ISMS) 6

1.4 Incident bezpečnosti informací 7

1.5 Řízení incidentů bezpečnosti informací 9

1.6 Shrnutí základních pojmů 10

2. Taxonomie incidentů 13

2.1 Taxonomie incidentů podle normy ČSN ISO/IEC 27035-2:2024 14

2.2 Taxonomie incidentů podle NIST 17

2.3 Taxonomie incidentů podle ENISA 19

2.4 Taxonomie incidentů podle MITRE ATT&CK 21

2.5 Výběr vhodné taxonomie pro konkrétní organizaci 24

3. Technická bezpečnostní opatření 27

3.1 Klasifikace informací 27

3.2 Řízení přístupu 28

3.3 Kryptografie 30

3.4 Provozní bezpečnost 30

3.5 Logování a monitoring 32

3.6 Řízení zranitelností 32

3.7 Celkový kontrolní rámec 33

Část druhá Řízení kybernetických incidentů

1. Standardy a normy pro řízení incidentů 39

1.1 Standard 39

1.2 Řízení incidentů bezpečnosti informací podle normy ČSN ISO/IEC 27035-1:2024 a normy ČSN ISO/IEC 27035-2:2024 40

1.2.1	Plánování a příprava	41
1.1.2	Detekce a podávání zpráv	44
1.1.3	Posouzení a rozhodnutí	44
1.1.4	Odezva	46
1.1.5	Poučení se	47
1.1.6	Shrnutí řízení incidentů podle normy ČSN ISO/IEC 27035-1:2024 a normy ČSN ISO/IEC 27035-2:2024	48
1.2	Řízení incidentů podle NIST SP.800-61	49
1.2.1	Organizační aspekty řízení incidentů	50
1.2.2	Zvládání incidentů podle NIST SP.800-61	52
1.3	Další normy a metodiky pro řízení kybernetických incidentů	59
1.4	Výběr standardu pro řízení kybernetických incidentů v praxi	61
1.5	Rozvoj technologií a kybernetické incidenty	63
1.6	Využití generativní umělé inteligence při řízení kybernetických bezpečnostních incidentů	64
1.6.1	AI z pohledu útočníka	65
1.6.2	AI z pohledu obránce	66
1.6.3	Možnosti použití generativní AI v procesech řízení kybernetických bezpečnostních incidentů	66
1.6.4	Dílčí závěr	68
1.7	Kontrolované a bezpečné využití AI	69
1.7.1	Typická rizika AI	70
1.7.2	Jak čelit AI rizikům?	72
1.7.3	ISO norma	72
1.7.4	Systém řízení umělé inteligence (AIMS)	73
1.7.5	Pro koho je vhodná certifikace dle ISO/IEC 42001:2023?	75
1.7.6	Zavedení AIMS v praxi	76

Část třetí Kybernetický incident z pohledu compliance

1.	Stručně o compliance management systému	81
1.1	Kybernetický incident a compliance: dva úhly pohledu	82
1.2	Kybernetický incident a compliance systém v praxi	84
1.3	Compliance jako proces, nikoliv stav	85
1.4	Individuální řešení místo šablonovitého přístupu	87
1.5	Compliance systém zavedený do praxe	89
2.	Základní prvky compliance systému	91
2.1	Čtyři klíčové fáze compliance	91
2.2.1	Plánuj	92
2.2.2	Proved'	93
2.2.3	Zkontroluj	93
2.2.4	Jednej	94

3. Poznej svoji organizaci	97
3.1 Jak na to?	97
3.2 Co potřebujeme poznat?	98
3.3 Hlavní činnost organizace	99
3.4 IT architektura a prostředí	100
3.5 Datové toky	101
3.6 Identifikace klíčových dodavatelů	101
3.7 Řízení informačních aktiv	102
3.8 Právní požadavky a závazky organizace	104
3.9 Hrozby	105
3.10 Zavedená opatření	106
4. Analýza rizik	109
4.1 Jak na analýzu rizik?	110
4.2 Metodika	111
4.3 Hodnocení jednotlivých rizik	112
4.4 Ochota podstupovat riziko (rizikový apetit)	113
4.5 Identifikace rizik	113
4.6 Rozhodnutí o riziku	115
4.7 Aktualizace rizikové analýzy	117
4.7.1 Jak často je nutno rizikovou analýzu aktualizovat?	117
5 Opatření ke snížení rizika	119
5.1 Opatření	119
5.2 Kontroly	120
5.3 Nápravná opatření	121
5.4 Společná pravidla pro opatření	121
5.4.1 Opatření odpovídající podmínkám v organizaci	121
5.4.2 Chytré a efektivní řešení	122
5.4.3 Skutečná realizace opatření	123
5.4.4 Dokumentace opatření	123
5.4.5 Aktualizace opatření	124
5.5 Druhy bezpečnostních opatření pro řízení kybernetických incidentů	124
5.5.1 Technická opatření	124
5.5.2 Organizační opatření	125
5.5.3 Administrativní opatření	125
5.5.4 Personální opatření	125
5.5.5 Procesní opatření	126
5.6 Organizační opatření v detailu	126
5.6.1 Nastavení strategie a cílů v oblasti ochrany před kybernetickými incidenty	127
5.6.2 Plánování v oblasti informační bezpečnosti a řízení kybernetických incidentů	128

5.6.2	Určení rolí a odpovědností	129
5.7	Administrativní opatření	131
5.7.1	Vnitřní předpisy	131
5.7.2	Dokumentace k řízení rizik	132
5.7.3	Evidence kybernetických incidentů	132
5.7.4	Další dokumentace a evidence	133
5.8	Personální opatření	134
5.8.1	Popis pracovních pozic	134
5.8.2	Pravidla pro další zaměstnance	135
5.8.3	Školení zaměstnanců	135
5.8.4	Kontrola zaměstnanců před nástupem (Background check)	136
5.8.5	Monitoring zaměstnanců	137
5.9	Další procesní opatření	138
6	Kontroly a hodnocení compliance systému	141
6.1	Jak kontrolovat?	141
6.2	Co je cílem kontroly?	142
6.3	Frekvence kontroly	142
6.4	Role a odpovědnosti	143
6.5	Automatická nebo manuální kontrola?	143
6.6	Hodnocení compliance systému jako celku	144
6.7	Další zdroje pro hodnocení compliance systému	146
6.8	Dokumentace kontrol	147
 Část čtvrtá Praktické aspekty řízení kybernetických incidentů		
1	Praktické aspekty řízení kybernetických bezpečnostních incidentů	151
2	Podpora vedení organizace	153
3	Pojištění kybernetické bezpečnosti	157
4	Outsourcing	159
5	Monitoring	161
6	Klasifikace a prioritizace incidentu	163
7	Hodnocení reakce na incident	165
8	Zpráva o incidentu	167

Část pátá Kybernetický incident a právo

1	Vymezení kybernetického bezpečnostního incidentu v právu	171
1.1	Kybernetický incident	171
1.2	Jak právo kybernetický incident definuje?	172
2	Nová regulace kybernetické bezpečnosti	175
2.1	Právní úprava	175
2.2	Směrnice NIS2 a její česká implementace	176
2.2.1	Směrnice NIS2	176
2.2.2	Česká implementace směrnice NIS2	177
2.3	Nařízení DORA	178
3	Kybernetický incident v regulovaném prostředí	181
3.1	Ochrana osobních údajů	181
3.2	Kybernetická bezpečnost	183
3.3	Významné incidenty podle nařízení pro poskytovatele digitálních služeb	185
3.4	Poskytování platebních služeb	187
3.5	Služby elektronických komunikací	188
3.6	Veřejná správa	190
4	Přesahy a styčné body různých regulací	193
4.1	Souběžná aplikace více právních předpisů na jeden incident	193
4.2	Praktické důsledky	194
4.3	Hrozí za jeden incident více pokut?	194
5	Právní povinnosti související s kybernetickým incidentem	197
5.1	Povinnosti při řešení kybernetického incidentu	197
5.2	Právní následky kybernetického incidentu	197
5.2.1	Oznámení incidentu dozorovému úřadu nebo dotčeným osobám	198
5.2.2	Smluvní povinnosti	198
5.2.3	Odpovědnost za způsobenou újmu a náhrada újmy	198
5.2.4	Dokumentace kybernetických incidentů	200
5.2.5	Přijetí nápravných opatření	201
5.2.6	Spolupráce s policií, výkupné	201
5.2.7	Veřejnoprávní sankce (pokuty)	202
6	Oznámení kybernetického incidentu	205
6.1	Obecná oznamovací povinnost	205
6.2	Notifikace kybernetického incidentu v regulovaném prostředí	206
6.2.1	Ochrana osobních údajů – dozorový úřad	206

6.2.2	Ochrana osobních údajů – subjekty údajů	208
6.2.3	Kybernetická bezpečnost	210
6.2.4	Finanční instituce	211
6.2.5	Služby elektronických komunikací	212
7	Právní požadavky na řízení dodavatelů	213
7.1	Požadavky na řízení dodavatelů	213
7.2	Ochrana osobních údajů	214
7.3	Regulace kybernetické bezpečnosti	215
7.4	Finanční instituce	217
7.5	Odolnost kritických subjektů	218
7.6	Veřejná správa	220
8	Další právní souvislosti	223
8.1	Trestněprávní aspekty	223
8.2	Ochrana soukromí zaměstnanců	225
8.3	Dopady do autorskoprávní ochrany	226
8.4	Certifikační schémata	227
8.5	Hromadné žaloby	227
	Přílohy	232
	Závěr	251
	Seznam použité literatury a zdrojů	253