

# OBSAH

O autorech .....	XI
Seznam použitých zkratek .....	XII
Úvod .....	XVII

## ČÁST PRVNÍ: KYBERNETICKÝ INCIDENT Z POHLEDU IT ..... 1

<b>1 Základní pojmy .....</b>	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 pojmu .....	10
<b>2 Taxonomie incidentů .....</b>	13
2.1 Taxonomie incidentů podle normy ČSN ISO/IEC 27035-2:2018 .....	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
<b>3 Technická bezpečnostní opatření .....</b>	25
3.1 Klasifikace informací .....	25
3.2 Řízení přístupu .....	26
3.3 Kryptografie .....	27
3.4 Provozní bezpečnost .....	28
3.5 Logování a monitoring .....	29
3.6 Řízení zranitelností .....	30
3.7 Celkový kontrolní rámec .....	31

## ČÁST DRUHÁ: ŘÍZENÍ KYBERNETICKÝCH INCIDENTŮ ..... 33

<b>1 Standardy a normy pro řízení incidentů .....</b>	35
1.1 Standard .....	35

1.2	Řízení incidentů bezpečnosti informací podle normy ČSN ISO/IEC 27035-1:2018 a normy ČSN ISO/IEC 27035-2:2018 .....	36
1.2.1	Plánování a příprava na incident .....	37
1.1.2	Zjišťování incidentů a podávání zpráv .....	40
1.1.3	Posouzení incidentu a rozhodnutí o dalším postupu .....	40
1.1.4	Odezva na incident .....	41
1.1.5	Poučení z minulosti .....	43
1.1.6	Shrnutí řízení incidentů podle normy ČSN ISO/IEC 27035-1:2018	43
1.2	Řízení incidentů podle NIST SP.800-61 .....	45
1.2.1	Organizační aspekty řízení incidentů .....	46
1.2.2	Zvládání incidentů podle NIST SP.800-61 .....	48
1.3	Další normy a metodiky pro řízení kybernetických incidentů .....	54
1.4	Výběr standardu pro řízení kybernetických incidentů v praxi .....	57
1.5	Rozvoj technologií a kybernetické incidenty .....	59

## **ČÁST TŘETÍ: KYBERNETICKÝ INCIDENT Z POHLEDU COMPLIANCE .....** 61

### **1 Stručně o compliance management systému .....** 63

1.1	Kybernetický incident a compliance: dva úhly pohledu .....	64
1.2	Kybernetický incident a compliance systém v praxi .....	66
1.3	Compliance jako proces, nikoliv stav .....	67
1.4	Individuální řešení místo šablonovitého přístupu .....	69
1.5	Compliance systém zavedený do praxe .....	70

### **2 Základní prvky compliance systému .....** 71

2.1	Čtyři klíčové fáze compliance .....	71
2.1.1	Plánuj .....	72
2.1.2	Proved'	73
2.1.3	Zkontroluj .....	73
2.1.4	Jednej .....	74

### **3 Poznej svoji organizaci .....** 77

3.1	Jak na to? .....	77
3.2	Co potřebujeme poznat? .....	78
3.3	Hlavní činnost organizace .....	79
3.4	IT architektura a prostředí .....	80
3.5	Datové toky .....	81
3.6	Identifikace klíčových dodavatelů .....	81
3.7	Řízení informačních aktiv .....	82
3.8	Právní požadavky a závazky organizace .....	84
3.9	Hrozby .....	85
3.10	Zavedená opatření .....	86

<b>4</b>	<b>Analýza rizik</b>	89
4.1	Jak na analýzu rizik?	90
4.2	Metodika	91
4.3	Hodnocení jednotlivých rizik	92
4.4	Ochota podstupovat riziko (rizikový apetit)	93
4.5	Identifikace rizik	93
4.6	Rozhodnutí o riziku	95
4.7	Aktualizace rizikové analýzy	97
<b>5</b>	<b>Opatření ke snížení rizika</b>	99
5.1	Opatření	99
5.2	Kontroly	100
5.3	Nápravná opatření	101
5.4	Společná pravidla pro opatření	101
5.4.1	Opatření odpovídající podmínkám v organizaci	101
5.4.2	Chytré a efektivní řešení	102
5.4.3	Skutečná realizace opatření	103
5.4.4	Dokumentace opatření	103
5.4.5	Aktualizace opatření	104
5.5	Druhy bezpečnostních opatření pro řízení kybernetických incidentů	104
5.5.1	Technická opatření	104
5.5.2	Organizační opatření	105
5.5.3	Administrativní opatření	105
5.5.4	Personální opatření	106
5.5.5	Procesní opatření	106
5.6	Organizační opatření v detailu	106
5.6.1	Nastavení strategie a cílů v oblasti ochrany před kybernetickými incidenty	107
5.6.2	Plánování v oblasti informační bezpečnosti a řízení kybernetických incidentů	108
5.6.3	Určení rolí a odpovědností	109
5.7	Administrativní opatření	111
5.7.1	Vnitřní předpisy	111
5.7.2	Dokumentace k řízení rizik	112
5.7.3	Evidence kybernetických incidentů	112
5.7.4	Další dokumentace a evidence	113
5.8	Personální opatření	114
5.8.1	Popis pracovních pozic	114
5.8.2	Pravidla pro další zaměstnance	115
5.8.3	Školení zaměstnanců	115
5.8.4	Kontrola zaměstnanců před nástupem (Background check)	116
5.8.5	Monitoring zaměstnanců	117
5.9	Další procesní opatření	118

<b>6</b>	<b>Kontroly a hodnocení compliance systému</b>	121
6.1	Jak kontrolovat?	121
6.2	Co je cílem kontroly?	122
6.3	Frekvence kontroly	122
6.4	Role a odpovědnosti	123
6.5	Automatická nebo manuální kontrola?	123
6.6	Hodnocení compliance systému jako celku	124
6.7	Další zdroje pro hodnocení compliance systému	126
6.8	Dokumentace kontrol	127

## **ČÁST ČTVRTÁ: PRAKTIKÉ ASPEKTY ŘÍZENÍ KYBERNETICKÝCH INCIDENTŮ** ..... 129

<b>1</b>	<b>Praktické aspekty řízení kybernetických bezpečnostních incidentů</b>	131
<b>2</b>	<b>Podpora vedení organizace</b>	133
<b>3</b>	<b>Pojištění kybernetické bezpečnosti</b>	137
<b>4</b>	<b>Outsourcing</b>	139
<b>5</b>	<b>Monitoring</b>	141
<b>6</b>	<b>Klasifikace a prioritizace incidentu</b>	143
<b>7</b>	<b>Hodnocení reakce na incident</b>	145
<b>8</b>	<b>Zpráva o incidentu</b>	147

## **ČÁST PÁTÁ: KYBERNETICKÝ INCIDENT A PRÁVO** ..... 149

<b>1</b>	<b>Vymezení kybernetického bezpečnostního incidentu v právu</b>	151
1.1	Kybernetický incident	151
1.2	Jak právo kybernetický incident definuje?	152
<b>2</b>	<b>Kybernetický incident v regulovaném prostředí</b>	155
2.1	Ochrana osobních údajů	155
2.2	Kybernetická bezpečnost	157
2.3	Poskytování platebních služeb	158

2.4	Služby elektronických komunikací .....	160
2.5	Veřejná správa .....	162
<b>3</b>	<b>Přesahy a styčné body různých regulací .....</b>	<b>163</b>
3.1	Souběžná aplikace více právních předpisů na jeden incident .....	163
3.2	Praktické důsledky .....	164
3.3	Hrozí za jeden incident více pokut? .....	164
<b>4</b>	<b>Právní povinnosti související s kybernetickým incidentem .....</b>	<b>167</b>
4.1	Povinnosti při řešení kybernetického incidentu .....	167
4.2	Právní následky kybernetického incidentu .....	167
4.2.1	Oznámení incidentu dozorovému úřadu nebo dotčeným osobám .....	168
4.2.2	Smluvní povinnosti .....	168
4.2.3	Odpovědnost za způsobenou újmu a náhrada újmy .....	168
4.2.4	Dokumentace kybernetických incidentů .....	170
4.2.5	Přijetí nápravných opatření .....	171
4.2.6	Spolupráce s policií, výkupné .....	171
4.2.7	Veřejnoprávní sankce (pokuty) .....	172
<b>5</b>	<b>Oznámení kybernetického incidentu .....</b>	<b>175</b>
5.1	Obecná oznamovací povinnost .....	175
5.2	Notifikace kybernetického incidentu v regulovaném prostředí .....	176
5.2.1	Ochrana osobních údajů – dozorový úřad .....	176
5.2.2	Ochrana osobních údajů – subjekty údajů .....	178
5.2.3	Kybernetická bezpečnost .....	179
5.2.4	Poskytovatelé platebních služeb – notifikace dozorovému úřadu .....	180
5.2.5	Poskytovatelé platebních služeb – dotčené osoby .....	181
5.2.6	Služby elektronických komunikací .....	182
<b>6</b>	<b>Právní požadavky na řízení dodavatelů .....</b>	<b>183</b>
6.1	Požadavky na řízení dodavatelů .....	183
6.2	Ochrana osobních údajů .....	184
6.3	Regulace kybernetické bezpečnosti .....	185
6.4	Platební styk .....	187
6.5	Veřejná správa .....	188
<b>7</b>	<b>Další právní souvislosti .....</b>	<b>191</b>
7.1	Trestněprávní aspekty .....	191
7.2	Ochrana soukromí zaměstnanců .....	193
7.3	Dopady do autorskoprávní ochrany .....	194

<b>8 Legislativní změny na obzoru</b>	195
8.1 Rozšíření požadavků kybernetické bezpečnosti	195
8.2 Digitální odolnost finančního sektoru	196
8.3 Hromadné žaloby	196
<b>Závěr</b>	198
<b>Přílohy</b>	201
<b>Seznam použité literatury a zdrojů</b>	221
<b>Věcný rejstřík</b>	226