

OBSAH

PŘEDMLUVA	9
1. ÚVOD	11
1.1 ZÁKLADNÍ NÁZVOSLOVÍ	12
1.2 ZÁKLADNÍ POJMY	15
1.2.1 Teorie informací	15
1.2.2 Matematická teorie informací	22
1.2.3 Shannonovy teorémy	23
1.3 NORMY	24
1.3.1 Řada norem Systém řízení bezpečnosti informací – Information Security Management System (ISMS)	24
1.3.2 Normy NIST	27
1.4 KRITICKÁ INFRASTRUKTURA	29
2. HISTORIE	33
2.1 KYBERNETICKÁ BEZPEČNOST VE SVĚTĚ V POSLEDNÍCH LETECH	38
2.2 KYBERNETICKÁ BEZPEČNOST V ČR V POSLEDNÍCH LETECH	42
2.2.1 Národní strategie kybernetické bezpečnosti ČR	44
2.2.2 Akční plán kybernetické bezpečnosti ČR	46
2.2.3 Kauza Huawei a ZTE	47
2.2.4 Kauza Solar Winds	48
3. KYBERPROSTOR A KYBERNETICKÁ BEZPEČNOST	51
3.1 VÁŽNOST A UKOTVENÍ BEZPEČNOSTI V KYBERPROSTORU	52
3.1.1 Budoucnost kybernetické bezpečnosti	54
3.1.2 Řízení kybernetických rizik	55
3.2 KYBERPROSTOR A KYBERNETICKÁ BEZPEČNOST JAKO PODMNOŽINA INFORMAČNÍ BEZPEČNOSTI?	57
4. PRÁVNÍ PROSTŘEDÍ	61
4.1 PRÁVNÍ PROSTŘEDÍ EU	62
4.1.1 Provozovatel základních služeb	62
4.1.2 Poskytovatel digitálních služeb	65
4.1.3 Agentura ENISA	67
4.2 PRÁVNÍ PROSTŘEDÍ ČR	68
4.2.1 Zákon o kybernetické bezpečnosti – ZKB	69
4.2.2 Povinné subjekty podle ZKB	76

4.2.3	Kybernetická obrana	83
4.3	ROLE NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST	84
5.	KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT	89
5.1	DEFINICE A KATEGORIZACE	91
5.1.1	Role CSIRT, CERT a SOC	91
5.1.2	Řízení incidentů	93
5.1.3	Security Information and Event Management (SIEM)	95
5.2	KONTINUITA ČINNOSTI ORGANIZACE	97
5.2.1	Základní pojmy	97
5.2.2	Hlavní zásady	99
5.2.3	Plán obnovy po havárii	103
6.	KYBERNETICKÉ ÚTOKY	107
6.1	TYPY ÚTOKŮ	108
6.2	ŽIVOTNÍ CYKLUS KYBERNETICKÉHO ÚTOKU	113
6.3	ZRANITELNOSTI	114
7.	KYBERNETICKÁ VÁLKA	119
7.1	TALLINSKÝ MANUÁL	121
8.	VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI	123
8.1	METODIKA BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ SAE	124
8.2	KYBERNETICKÁ HYGIENA	126
9.	INTERNET VĚCÍ	133
9.1	IoT – INTERNET OF THINGS	134
9.2	IIoT – INDUSTRIAL INTERNET OF THINGS	138
9.3	NoT – NETWORK OF THINGS	139
9.4	BEZPEČNOSTNÍ DOPORUČENÍ PRO IoT	140
10.	UMĚLÁ INTELIGENCE – AI	147
10.1	ZÁKLADNÍ POJMY	148
10.2	PRINCIPY	149
10.3	AI A KYBERNETICKÝ PROSTOR	155
10.4	ODPOVĚDNOST ZA ŠKODU ZPŮSOBENOU UMĚLOU INTELIGENCÍ	156
10.5	ČASTÉ OMYLY VE VZTAHU K UMĚLÉ INTELIGENCI	157
11.	VELKÁ DATA	159
11.1	PROBLEMATIKA VELKÝCH DAT	160
11.2	NÁZVOSLOVÍ A ZÁKLADNÍ POJMY	162
11.3	NORMY PRO VELKÁ DATA	165

11.4	ZDROJE VELKÝCH DAT	167
11.5	BEZPEČNOST VELKÝCH DAT (BIG DATA SECURITY)	168
11.6	EVROPSKÁ DATOVÁ STRATEGIE	173
12.	PROBLEMATIKA ZÁLOHOVÁNÍ	175
12.1	ZÁLOHOVÁNÍ ZAŘÍZENÍ	179
12.2	ZÁLOHOVÁNÍ DAT	180
13.	PROBLEMATIKA CLOUDOVÝCH ŘEŠENÍ	187
13.1	BEZPEČNOST CLOUDU	192
13.2	BEZPEČNOST DAT V CLOUDU	194
13.3	CLOUD JAKO BEZPEČNOSTNÍ ŘEŠENÍ	195
13.4	BEZPEČNOST CLOUDOVÝCH TECHNOLOGIÍ	199
13.4.1	Virtualizace	200
13.4.2	Kontejnerizace	201
13.4.3	SDP-ZTN	205
13.4.4	SD-WAN a SASE	210
13.5	eGOVERNMENT CLOUD	219
14.	ZABEZPEČENÍ A OCHRANA DAT	223
14.1	OCHRANA SOUKROMÍ A REGULACE	226
14.2	POJEM PRIVACY BY DESIGN	229
15.	VĚDECKÉ METODY PŘÍSPÍVAJÍCÍ KE ZVYŠOVÁNÍ BEZPEČNOSTI	233
15.1	BEHAVIORÁLNÍ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI	234
15.2	VĚDECKÉ METODY	239
16.	MANAŽERSKÁ BEZPEČNOST	245
16.1	MANAŽERSKÉ BEZPEČNOSTNÍ DOVEDNOSTI	247
16.1.1	Ekonomické vnímání kybernetické bezpečnosti	249
16.1.2	Znalostní dovednosti manažera	251
16.2	MANAŽERSKÉ BEZPEČNOSTNÍ POVĚDOMÍ	252
17.	BEZPEČNOSTNÍ INŽENÝRSTVÍ	255
18.	INTERNETOVÁ BEZPEČNOST	259
18.1	ZÁKLADNÍ BEZPEČNOSTNÍ DOPORUČENÍ PŘI PRÁCI NA INTERNETU	262
18.2	OSINT – OPEN SOURCE INTELLIGENCE	264
18.3	HROZBY	266
18.3.1	Internetové hrozby	266
18.3.2	Pokročilé trvalé hrozby (Advanced Persistent Threat – APT)	270
18.3.3	Hrozby dle VKB	273

19. ZRALOSTNÍ MODEL V OBLASTI KB	275
19.1 CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)	277
19.2 VYUŽITÍ ZRALOSTNÍHO MODELU V PRAXI	291
20. AUDIT KYBERNETICKÉ BEZPEČNOSTI	293
20.1 NÁZVOSLOVÍ A ZÁKLADNÍ POJMY	296
20.2 ZÁKLADNÍ PRINCIPY AUDITU	298
20.3 PROCES AUDITU	299
20.4 CERTIFIKAČNÍ AUDIT	301
20.5 EVROPSKÝ RÁMEC CERTIFIKACE KYBERNETICKÉ BEZPEČNOSTI	303
20.6 PENETRAČNÍ TESTY	304
21. BEZPEČNOST DODAVATELSKÉHO ŘETĚZCE	311
21.1 BEZPEČNOST DODAVATELSKÉHO ŘETĚZCE Z POHLEDU KYBERNETICKÉHO ZÁKONA	312
21.2 BEZPEČNOST DODAVATELSKÉHO ŘETĚZCE PODLE BEST PRACTICES	315
21.3 ZÁKLADNÍ POJMY	317
22. FORENZNÍ VNÍMÁNÍ KYBERNETICKÉ BEZPEČNOSTI	321
23. PŘÍPADOVÉ STUDIE	331
23.1 ASISTOVANÉ ZHODNOCENÍ	332
23.2 SW NÁSTROJ PRO ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI	335
23.3 NOVODOBÝ RANSOMWARE	341
23.4 TOR	347
23.5 BLOCKCHAIN JAKO ÚLOŽIŠTĚ	349
23.5.1 Základní pojmy	350
23.6 FYZICKÉ ZABEZPEČENÍ OBJEKTU KI	356
23.7 BEZPEČNOST DIGITÁLNÍHO OBSAHU	371
23.8 KYBERNETICKÁ BEZPEČNOST V PRŮMYSLOVÉM PROSTŘEDÍ	376
23.9 ZÁSADY NÁVRHU SÍTĚ MCN	384
23.10 ISO/OSI MODEL A BEZPEČNOST	388
24. REJSTŘÍK POJMŮ	391
25. PŘEHLED PLATNÝCH BEZPEČNOSTNÍCH NOREM	403
25.1 ŘADA VYBRANÝCH NOREM 27000	404
25.2 ŘADA VYBRANÝCH NOREM NIST SP 800	405

26. SEZNAM ZKRATEK	407
27. SEZNAM OBRÁZKŮ	413
28. SEZNAM TABULEK	419
29. POUŽITÁ LITERATURA	423
ELEKTRONICKÉ ODKAZY	429

Publikace je určena pracovníkům v managementu informačních a komunikačních technologií, správcům sítí a odborné veřejnosti, která se problematikou kybernetické bezpečnosti zabývá.

Pojem kybernetické bezpečnosti je zasazen do širších souvislostí a uchopen z pohledu aktuálního řešení bezpečnosti v kyberprostoru a vývoje nových technologií včetně vnímání systémové integrace kybernetické bezpečnosti.
V publikaci nechybí ani malý výlet do nedávné historie.

Od kapitoly 9 je problematika kybernetické bezpečnosti rozebrána z pohledu prostředí, kam má být nebo je implementována s důrazem na specifika, která jsou těmto prostředím vlastní.

Kapitola 23 je ukázka případových studií, které mají za úkol čtenáři pomoci uchopit problematiku kybernetické bezpečnosti a její šíři záběru v praxi.

Závěr publikace tvoří rejstřík pojmů, přehled bezpečnostních norem, seznamy zkratk, obrázků, tabulek použitých v textech a seznam použité literatury.

Tato publikace není koncipována jako vyčerpávající zdroj informací, ani nemá ambice stát se návodem, jak si s problematikou bezpečnosti v kyberprostoru poradit. Její cíl je ozřejmit závažnost celé problematiky a upozornit na klíčové aspekty kybernetické bezpečnosti, která se evidentně týká téměř všech.

Kdyby se některé kapitoly zdály být opakováním již něčeho, tak to není náhoda, protože byly třeba zopakovat, případně doplnit k lepšímu komplexnímu vnímání konkrétních témat. A navíc stále platí staré známé přísloví „opakování je matka moudrosti“.

Varovný nádech publikace již od jejího názvu není náhodný!

Publikace vznikla díky aktivitám Fakulty podnikatelské Vysokého učení technického v Brně.

Publikace je výstupem projektu specifického výzkumu FP-S-20-6376 „Modelování a optimalizace podnikových procesů v podmínkách digitální transformace“.