
Obsah

1 ČO JE TO BEZPEČNOSŤ?	1
ZÁVISLOSŤ OD SPÄTNEJ VÄZBY	1
ŽIVOTNÉ PRIESTORY	1
BEZPEČNOSŤ AKO MERATELNÝ STAV	2
INFORMAČNÁ ALEBO KYBERNETICKÁ BEZPEČNOSŤ?	4
NEMÝLME SI OBJEKT SO SUBJEKTOM	5
ABSTRAKTNÝ MODEL BEZPEČNOSTI	6
KYBERBEZPEČNOSŤ AKO MODERNÝ VÝRAZ	7
2 ÚVOD K PROBLEMATIKE BEZPEČNOSTNÝCH OPATRENÍ	8
ČO ZNAMENÁ SLOVO „OPATRENIA“?	8
GENERICKÉ ROZDELENIE OPATRENÍ	9
PRÁVNE ZAKOTVENIE BEZPEČNOSTNÝCH OPATRENÍ	10
OPATRENIA PODĽA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI	12
KONCEPT SEKTOROVÝCH OPATRENÍ	15
VŠEOBECNÉ PRINCÍPY NÁVRHU BEZPEČNOSTNÝCH OPATRENÍ	17
3 ORGANIZÁCIA INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI	19
ZODPOVEDNOSŤ VEDENIA ORGANIZÁCIE	19
RIADENIE A VÝKON BEZPEČNOSTNÝCH PROCESOV	20
HLAVNÉ ZÁSADY V ORGANIZÁCIÍ BEZPEČNOSTI	21
MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI	22
ALOKÁCIA ZODPOVEDNOSTÍ	22
RIADENIE VÝNIMIEK	23
ZARADENIE BEZPEČNOSTI V ORGANIZAČNEJ ŠTRUKTÚRE	23
4 RIADENIE RIZÍK INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI	28
INFORMAČNÝ MAJETOK	28
GRANULARITA INFORMAČNÉHO MAJETKU	29
RIZIKÁ PÔSOBIACE NA INFORMAČNÉ AKTÍVA	30
LOGICKÉ OBJEKTY V RIADENÍ RIZIKA	31
PROCES RIADENIA RIZÍK	33
STANOVENIE KONTEXTU A IDENTIFIKÁCIA RIZIKA	34

METÓDY HODNOTENIA RIZIKA	37
ANALÝZA RIZIKA	38
OHODNOTENIE RIZIKA	40
IMPLEMENTÁCIA PROCESU RIADENIA RIZÍK	42
5 PERSONÁLNA BEZPEČNOSŤ	44
POUŽÍVATEĽ AKO PRVOK KYBERNETICKÉHO PRIESTORU	44
BEZPEČNOSŤ PRED ZAČATÍM ZMLUVNÉHO VZŤAHU	44
PODMIENKY ZAMESTNANIA A STANOVENIE PRACOVNEJ NÁPLNE	45
PERSONÁLNA BEZPEČNOSŤ POČAS TRVANIA ZMLUVNÉHO VZŤAHU	46
DISCIPLINÁRNE PROCESY	47
BEZPEČNOSŤ PO SKONČENÍ PRACOVNÉHO POMERU	47
6 RIADENIE PRÍSTUPOV	49
DIGITÁLNA IDENTITA A IDENTIFIKÁCIA	49
AUTENTIZÁCIA	51
PROCES RIADENIA DIGITÁLNYCH IDENTÍT A PRÍSTUPOV	52
SINGLE SIGN-ON	54
POŽIADAVKY NA RIADENIE PRÍSTUPOV	55
7 RIADENIE BEZPEČNOSTI VO VZŤAHOCH S TRETÍMI STRANAMI	56
INSOURCING ALEBO OUTSOURCING?	56
SLUŽBA MÔŽE BYŤ POSKYTOVANÁ AJ VIRTUÁLNE	56
IDENTIFIKUJTE RIZIKO SKÔR, NEŽ VYBERIETE DODÁVATEĽA	59
ZMLUVA O PLNENÍ BEZPEČNOSTNÝCH OPATRENÍ	60
KVALITA POSKYTOVANEJ SLUŽBY	61
VENDOR LOCK-IN V OBSTARÁVANÍ	61
JE MOŽNÉ UDRŽAŤ BEZPEČNOSŤ V SIETI DODÁVATEĽOV?	62
8 RIADENIE BEZPEČNOSTI PREVÁDZKY	63
KYBERNETICKÁ ODOLNOSŤ	63
RIADENIE ZMIEN	65
RIADENIE KAPACÍT	65
ZÁLOHOVANIE A OBNOVA INFORMÁCIÍ	66
INŠTALÁCIA SOFTVÉRU A ZARIADENÍ	66
PREVÁDZKA ZÁSADNÝM SPÔSOBOM SÚVISÍ S BEZPEČNOSŤOU	66

9 HODNOTENIE ZRANITELNOSTÍ A BEZPEČNOSTNÉ AKTUALIZÁCIE	68
VZŤAH RIZÍK A ZRANITEENOSTÍ	68
ZRANITELNOSTI NULOVÉHO DŇA	69
IDENTIFIKÁCIA ZRANITEENOSTÍ	69
RIADENIE ZRANITEENOSTÍ	69
RIADENIE ZÁPLAT A AKTUALIZACÍÍ	72
PREČO JE POTREBNÉ RIADENIE ZRANITEENOSTI?	72
10 OCHRANA PROTI ŠKODLIVÉMU KÓDU	73
ČO JE TO MALVÉR?	73
BEŽNÉ TYPY MALVÉRU	73
OCHRANA PRED ŠKODLIVÝM KÓDOM	74
AKO FUNGUJE ANTIMALVÉROVÝ SOFTVÉR?	75
DOBRÁ PRAX V OCHRANE PRED MALVÉROM	78
11 SIEŤOVÁ A KOMUNIKAČNÁ BEZPEČNOSŤ	80
SIETE NIE SÚ LEN DIGITÁLNE	80
RIADENIE BEZPEČNOSTI ELEKTRONICKEJ KOMUNIKÁCIE	80
RIADENIE PRÍSTUPOV	81
SEGREGÁCIA PODĽA DÔVERY	81
MONITORING POKUSOV O PRIENIK	83
AK NA DIAVKU, POTOM IBA BEZPEČNE	83
SPEVŇOVANIE HRADIEB	86
OBSAH JE ROZHODUJÚCI	86
ÚPRATOVANIE A INVENTÚRA	86
12 AKVIZÍCIA, VÝVOJ A ÚDRŽBA INFORMAČNÝCH SYSTÉMOV	87
BEZPEČNÝ SYSTÉM NEJESTVUJE	87
ROZDIEL MEDZI VÝVOJOVÝMI A PREVÁDZKOVÝMI FÁZAMI SDLC	89
AKO VYVÍJAĚ BEZPEČNÉ SYSTÉMY?	90
BEZPEČNOSŤ VÝVOJOVÉHO PROSTREDIA	91
MANAŽMENT VÝVOJA SOFTVÉRU	91
VEDOMOSTI A ZRUČNOSTI VÝVOJÁROV	91
METODIKA VÝVOJA	92
OBSTARAŤ ALEBO VYVINÚŤ?	94

KAŽDÁ TECHNOLOGIA POTREBUJE ÚDRŽBU	94
VÝHODY BEZPEČNÉHO VÝVOJA SYSTÉMOV	95
13 ZAZNAMENÁVANIE UDALOSTÍ A MONITOROVANIE	96
ZAZNAMENÁVANIE UDALOSTÍ	96
METÓDY BEZPEČNOSTNÉHO MONITORINGU	96
TYPY LOGOV	97
SYNTAKTICKÁ NORMALIZÁCIA A PARSING	98
SÉMANTICKÁ NORMALIZÁCIA	98
ROTÁCIA A ARCHIVÁCIA LOGOV	98
AGREGÁCIA LOGOV	98
KORELÁCIA	99
SCENÁRE POUŽITIA BEZPEČNOSTNÉHO MONITORINGU	102
PROBLÉM FALOŠNÝCH HLÁSENÍ O UDALOSTIACH	105
ÚČEL MONITOROVANIA	106
14 FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ PROSTREDIA	107
FYZICKÁ BEZPEČNOSŤ	107
ORGANIZAČNÉ OPATRENIA VO FYZICKEJ BEZPEČNOSTI	107
TECHNICKÉ OPATRENIA VO FYZICKEJ BEZPEČNOSTI	108
RIADENIE A KONTROLA VSTUPU A POHYBU V CHRÁNENOM PRIESTORE	111
KONTINUITA ČINNOSTÍ VO FYZICKEJ BEZPEČNOSTI	111
AKO FYZICKÁ BEZPEČNOSŤ SÚVISÍ S KYBERNETICKOU BEZPEČNOSŤOU?	111
15 RIEŠENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV	112
ČO JE TO INCIDENT?	112
UDALOSŤ VERZUS INCIDENT	112
DETEKCIA INCIDENTOV	114
KATEGÓRIE INCIDENTOV	114
INCIDENT V KONTEXTE KVALITY IT SLUŽBY	116
ATRIBÚCIA ALEBO IDENTIFIKÁCIA PRÍČINY INCIDENTU PODĽA ZDROJA	117
ZÁKLADNÉ PRÍČINY INCIDENTOV	118
STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU	119
PROCESY RIEŠENIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV	121
DETAILNÉ FÁZY PROCESU RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV	122
ESKALAČNÉ PROCEDÚRY	122

PLÁN REAKCIE NA INCIDENT	123
JEDNOTKY CSIRT	124
AKÉ SÚ DÔVODY A MOTIVÁTORY PRE VZNIK A ČINNOSŤ CSIRT?	124
16 KRYPTOGRAFICKÉ OPATRENIA	127
AKO FUNGUJE ŠIFROVANIE?	127
ELEKTRONICKÝ PODPIS	128
AKÝ JE VZŤAH PODPISU A ELEKTRONICKÉHO PODPISU?	130
TERMINOLOGICKÉ ROZDIELY MEDZI PODPISOM A ELEKTRONICKÝM PODPISOM	131
ROZDIELY Z HĽADISKA PRÁVNÝCH ÚČINKOV	133
VÝHODY A NEVÝHODY ELEKTRONICKÉHO PODPISU V PRAXI	135
POŽIADAVKY ZÁKONA NA KRYPTOGRAFICKÉ OPATRENIA	137
BEZPEČNOSŤ KRYPTOGRAFICKÝCH OPATRENÍ	137
DÔVERYHODNÉ SLUŽBY	138
QUBIT A BUDÚCNOSŤ KRYPTOGRAFIE	139
17 RIADENIE KONTINUITY ČINNOSTÍ	140
KONTINUITA JE NIELEN CIEĽ, ALE NAJMÄ PROCES	140
KAŽDÁ KRÍZA MÁ SVOJ SCENÁR	141
JE LEPŠIE SA BÄŤ, AKO SA ZĽAKNÜŤ	141
PRIORITY SÜ PREDURČENÉ DOPADMI	142
HAVARIJNÄ OBNOVA	143
RIADENIE KONTINUITY AKO CYKICKÄ ČINNOSŤ	144
POŽIADAVKA NA PLÄNOVANIE KONTINUITY V REGULÄCII	145
AKO NA BCM?	146
18 AUDIT KYBERNETICKEJ BEZPEČNOSTI	147
POŽIADAVKA NA AUDITING	147
ČO JE TO AUDIT?	147
KTO MÔŽE VYKONAŤ AUDIT?	148
METODIKA PRE VÝKON AUDITU KYBERNETICKEJ BEZPEČNOSTI	149
URČENIE ROZSAHU AUDITU KYBERNETICKEJ BEZPEČNOSTI	150
VÝKONATEĽNOSŤ AUDITU	151
19 RIADENIE SÜĽADU A KONTROLNÉ ČINNOSTI	152
METÖDY OVEROVANIA ÜROVNE BEZPEČNOSTI	152
TESTOVANIE V RÄMCI ŽIVOTNÉHO CYKLU VÝVOJA SYSTÉMOV	154

METÓDY TESTOVANIA BEZPEČNOSTI SOFTVÉROVÉHO KÓDU	154
TESTOVANIE V RÁMCI PROCESOV RIADENIA KONTINUITY ČINNOSTÍ	155
OVEROVANIE BEZPEČNOSTI S CIEĽOM RIADENIA SÚLADU	156
SYSTÉM VNÚTORNEJ KONTROLY	157
20 BEZPEČNOSTNÁ DOKUMENTÁCIA	158
VŠEOBECNÝ RÁMEC BEZPEČNOSTNEJ DOKUMENTÁCIE	158
ZÁKONOM POŽADOVANÁ ŠTRUKTÚRA INTERNÝCH RIADIACICH AKTOV	160
BEZPEČNOSTNÁ STRATÉGIA	162
BEZPEČNOSTNÝ PROJEKT ITVS	165
21 ARCHITEKTÚRA NULOVEJ DÔVERY	167
DÔLEŽITOSŤ NEDÔVERY V SÚČASNOM PROSTREDÍ	167
KĹÚČOVÉ KOMPONENTY ARCHITEKTÚRY NULOVEJ DÔVERY	167
VÝHODY ARCHITEKTÚRY NULOVEJ DÔVERY	168
AKO IMPLEMENTOVAŤ ARCHITEKTÚRU NULOVEJ DÔVERY	168
UDRŽIAVANIE A AKTUALIZÁCIA ARCHITEKTÚRY NULOVEJ DÔVERY	170
LITERATÚRA	171
ZOZNAM ILUSTRÁCIÍ	175
ZOZNAM TABULIEK	177
REGISTER POJMOV A SKRATIEK	178
SKRATKY	197