

Obsah

Informačná bezpečnosť je súčasť nášho života	12
Techniky sociálneho inžinierstva	15
Techniky	16
Útoky zamerané na fyzický kontakt	17
Najčastejšie virtuálne typy útokov	21
Príbehy zo školy: Zničený počítač	31
Sociálne inžinierstvo a riadenie bezpečnosti organizácie	31
Príbehy zo školy: Phishing na škole	33
Bezpečnostná legislatíva	34
Príbehy zo školy: Za phishing na súd!	36
Normy ako návod na riadenie informačnej bezpečnosti	36
Systém noriem ISO 27000	39
ISO 27001	39
ISO 27002	42
ISO 27003	42
ISO 27004	43
ISO 27005	43
ISO 27017	43
ISO 27018	43
Príbehy zo školy: Návod na riadenie bezpečnosti	43
Pojednanie o stratégii informačnej bezpečnosti	44
Ukazovatele, ktoré musí napĺňať stratégia	46
Stratégia informačnej bezpečnosti	49
Príbehy zo školy: Kto tú stratégiu nakoniec urobí?	51
Norma ISO 27002:2013	52
Politiky informačnej bezpečnosti	52
Príbehy zo školy: Politka informačnej bezpečnosti alebo trest?	54
	54
Organizácia informačnej bezpečnosti	54
Roly a zodpovednosti v informačnej bezpečnosti	57
Príbehy zo školy: Politika informačnej bezpečnosti alebo trest?	60
Oddelenie právomoci	60
Riadenie kontaktu s orgánmi moci	61

Riadenie kontaktu so špeciálnymi záujmovými skupinami	64
Informačná bezpečnosť v projektovom riadení	64
Mobilné zariadenia a práca na diaľku	65
Politika pre mobilné zariadenia	65
Práca na diaľku	66
Príbehy zo školy: Politika informačnej bezpečnosti alebo trest?	70
Personálna bezpečnosť	70
Príprava pred nástupom do zamestnania	71
Doba zamestnania	74
Ukončenie zamestnania alebo zmena zamestnania	80
Príbehy zo školy: Politika informačnej bezpečnosti alebo trest?	82
Riadenie aktív	83
Zodpovednosť za aktíva	83
Inventárny zoznam aktív	84
Vlastníctvo aktív	84
Aktíva je potrebné používať vhodne	85
Vrátenie aktív	86
Príbehy zo školy: Nič nenič!	87
Klasifikácia informácií	87
Príklad klasifikácie informácií	88
Označovanie informácií vo fyzickej podobe	89
Zaobchádzanie s aktívami	90
Zaobchádzanie s médiami	90
Príbehy zo školy: Tajný dokument, hotová pohroma.	92
Riadenie prenosných médií	92
Likvidácia médií	93
Fyzický prenos médií	94
Príbehy zo školy: Začiatok konca pracovného neporiadku.	95
Riadenie prístupov	96
Politika riadenia prístupov	97
Prístup do sietí a sieťových služieb	97
Riadenie používateľských prístupov	98
Registrácia a deregistrácia používateľov	99
Poskytovanie používateľských prístupov	100
Riadenie prístupov privilegovaných používateľov	103
Riadenie utajených autentizačných údajov	103

Preskúmanie prístupových práv	104
Odstránenie alebo prispôsobenie prístupových práv	105
Zodpovednosť používateľov za autentifikačné údaje	105
Používanie a utajenie autentifikačných údajov	106
Riadenie systémových a aplikačných prístupov	107
Obmedzenie prístupu k informáciám	108
Bezpečné postupy prihlasovania	108
Systém riadenia hesiel	108
Používanie privilegovaných programov	110
Riadenie prístupu k zdrojovým kódom programu	111
Kryptografia a kryptografické opatrenia	112
Príbehy zo školy: Používatelia, ako ich svet nevidel.	112
Úvod do kryptológie	113
Od úvodu do kryptografie k aplikovaniu kryptografických opatrení	118
Príbehy zo školy: Rnqd ufs wnfinyjq,	124
Fyzická bezpečnosť	124
Zabezpečené oblasti	125
Zariadenia	132
Príbehy zo školy: Ukradnem informácie odčítaním cez okno.	137
Bezpečnosť prevádzky	138
Prevádzkové postupy a zodpovednosti	139
Oddelenie vývojových, testovacích a prevádzkových prostredí	142
Ochrana voči malvéru	144
Zálohovanie	148
Riadenie prevádzkového softvéru	153
Riadenie technických zraniteľností	155
Príbehy zo školy: Nefunguje počítač v kuchyni!, prestali vydávať obedy...	159
	160
Komunikačná bezpečnosť	161
Úvod do sietí	161
Útoky v počítačovej sieti	166
Riadenie sieťovej bezpečnosti	169
Prenos informácií	179
Príbehy zo školy: Pozor bezpečnostný útok je tu!	184
Nákup, vývoj a údržba informačných systémov	185
Projekty na nákup alebo vývoj informačných systémov	187

Bezpečnostné požiadavky na informačný systém	193
Bezpečnosť procesov vývoja a údržby	196
Testovacie dáta	203
Príbehy zo školy: Vývíjať, vývíjať, vyvíjať....	205
Riadenie vzťahov s dodávateľmi	206
Informačná bezpečnosť vo vzťahoch s dodávateľmi	206
Manažment dodávateľských služieb	211
Príbehy zo školy: Čo spôsobilo nepokoj riaditeľa Pokojného?	215
Riadenie incidentov informačnej bezpečnosti	215
Riadenie incidentov informačnej bezpečnosti a zlepšovania	216
Zodpovednosť a postupy	218
Informovanie o udalostiach informačnej bezpečnosti	219
Informovanie o slabinách informačnej bezpečnosti	220
Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich	220
Reakcia na incidenty informačnej bezpečnosti	221
Poučenie z incidentov informačnej bezpečnosti	222
Incidenty a trestné konanie, zber dôkazov	223
Prvky informačnej bezpečnosti v riadení kontinuity biznisu	224
Príbehy zo školy: Ako ransomvér za rohom číhal	224
Čo je to riadenie kontinuity biznisu?	224
Plánovanie kontinuity informačnej bezpečnosti	230
Implementácia kontinuity informačnej bezpečnosti	231
Verifikácia a ohodnotenie kontinuity informačnej bezpečnosti	232
Redundancie	232
Príbehy zo školy: Ako zmizol aj posledný obláčik a aj cloud.	233
Súlad s právnymi a zmluvnými požiadavkami	233
Identifikácia platnej legislatívy a zmluvných požiadaviek	234
Práva duševného vlastníctva	234
Ochrana záznamov	235
Súkromie a ochrana osobných údajov	236
Nariadenie o šifrovacích opatreniach	238
Revízie informačnej bezpečnosti	238
Nezávislá revízia informačnej bezpečnosti	238
Súlad s bezpečnostnými politikami a štandardmi	239
Revízia technického súladu	240
Príbehy zo školy: Haló!, nenastal koniec sveta, začal „len“ audit...	241

Otázky pre testovanie znalostí

242

Správne odpovede testov

254