Obsah

Sociálne inžinierstvo 11
Základné pojmy, súhrn predošlých znalostí 12
Útoky využívajúce manipulatívne techniky 16
Prejavy útoku 17
Dopad útoku 20
Príklady útokov 20
Čo nám pomôže odhaliť útok? 24
Rodiny pod tlakom sociálneho inžinierstva 25
Súčasné útoky a očakávané trendy útokov 25
Najčastejšie útoky 26
Predpokladateľný vývoj 28
Nové typy útokov 28
Útoky pomocou umelej inteligencie 29
Útoky na hráčov hier 32
Útoky v metaverse 33
Princípy prevencie pred útokmi 34
Jednotlivec alias čo by mal vedieť každý používateľ 34
Ako postupovať pri podvode? 35
Manažment rizík 37
Manažment rizík - opakovanie 38
Riziko 39
Rozdelenie zodpovednosti 42
Jednotlivé prvky rizika 45
Aktívum 45
Hrozba 47
Zraniteľnosť 48
Vzájomný vzťah jednotlivých prvkov 50
Ako merať riziko? 53
Proces a životný cyklus 60
Identifikácia rizika 60
Posúdenie rizika 63
Reakcia na riziko 63
Inherentné vs. reziduálne riziko 67
Monitorovanie rizík a opatrení. Reportovanie 68
Risk manažment v riadení informačnej bezpečnosti 71
Cloud 73
Čo je to Cloud computing? 74
fast food 79
reštaurácia 80
domáce stravovanie 80
Prvky, z ktorých je zložený cloud 83
Služby cloudu 84
Stavebné prvky Cloudu (architektúra) 86
Hlavné charakteristiky Cloud-u 87
Zodpovednosť za prevádzkovanie Cloudu 89
Cloud a bezpečnosť 91
Rozdelenie zodpovednosti 93
Požiadavky na bezpečnosť Cloud služieb 96
Prečo je to tak? 96
Izolácia dát 98
Čo je to izolácia dát v prípade Cloudu? 98
Riziká Cloud-u a ich riadenie 100
Štandardizované bezpečnostné opatrenia pre Cloud služby 105
Cloud Access Security Broker (CASB) 106
Posture management 107
Odchod (EXIT) z Cloudu 108
Podmienky pre EXIT 108
OWASP TOP 10 113
Etika v rámci kybernetickej bezpečnosti a OWASP TOP 10 114
Základy fungovania webových aplikácií 114
Inštalácia prostredia 119
A01 Broken Access Control 119
Chýbajúca alebo nedostatočná autorizácia 120
Path traversal 121
Zverejnenie citlivých dát 122
Problémy s oprávneniami 123

Cross-site request forgery (CSRF) 124
A02 Cryptographic Failures 125
Používanie nešifrovaných protokolov 125
Použitie trvale nastaveného šifrovacieho kľúča 126
Slabé algoritmy, krátke kľúče, nízka entropia 126
HSTS 128
Soľ, korenie a hašovacie funkcie 129
A03 Injection 130
HTML injection a cross-site scripting 130
SQL injection 133
OS command injection 134
Validácia vstupu a parametrizácia dotazov 135
A04 Insecure Design 136
Nevhodný dizajn alebo aplikovanie privilégií 136
Sprístupnenie citlivých údajov 137
Nechránený upload súborov 139
Spoliehanie sa na bezpečnosť klienta 139
Security through obscurity 140
Chyby v biznis logike 141
Ako odhaliť chyby v dizajne 141
A05 Security Misconfiguration 142
Cookie flags a nešifrované citlivé dáta v cookies 142
Prihlasovacie údaje v súboroch alebo premenných prostredia 143
HTTP hlavičky 144
Zhrnutie 145
A06 Vulnerable and Outdated Components 146
Operačný systém, DBMS, aplikačný server, programovací jazyk a framework 146
Knižnice a závislosti 146
A07 Identification and Authentication Failures 148
Brute-force, credentials stuffing a politika hesiel 148
Nedostatočná validácia certifikátov 149
Slabý mechanizmus pre obnovu hesla 151
A08 Software and Data Integrity Failures 152
Nedostatočná verifikácia autentickosti dát 152
Stiahnutie kódu bez kontroly integrity 154
Deserializácia nedôveryhodných dát 155
A09 Security Logging and Monitoring Failures 155
Nedostatočné logovanie 156
Nedostatočná sanitizácia dát pred zápisom do logov 158
Zápis citlivých dát v logoch 160
A10 Server Side Request Forgery 161
Zhrnutie 162
Umelá inteligencia v optike informačnej bezpečnosti 163
Čo si predstaviť pod umelou inteligenciou? 165
Základné delenia systémov umelej inteligencie 168
Neurónové siete 173
Základné algoritmy strojového učenia 177
Hľadanie nových riešení 181
Limity a riziká súčasných systémov umelej inteligencie 184
Zraniteľnosti, slabiny a klamanie systémov strojového učenia 186
Bezpečnosť procesov 197
Spoločenské a psychologické riziká 199
Vybrané riziká generatívnych systémov 201
Pohľad pod kapotu umelej inteligencie 202
Softvér 203
Hardvér 206
Umelá inteligencia a etika 209
Interdisciplinárny rámec ako základ 209
Umelá inteligencia zameraná na dobro človeka 210
Dôveryhodná umelá inteligencia 211
Niektoré etické požiadavky na dôveryhodné systémy umelej inteligencie 213
Oblasti implementácie etických princípov a regulácií 214
Špecifické odporúčania pre algokraciu a armádne využitie 216
Legislatívne kroky a regulácie 220
Otázky pre testovanie znalostí 229
Správne odpovede testov 242