Obsah

Úvod 5
1. kapitola – Kybernetická bezpečnost 9
1.1 Vývoj informační bezpečnosti v České republice 11
1.2 Dopady kybernetických útoků 12
2. kapitola – Data, informace a znalosti 14
2.1 Typy dat a informací 16
2.2 Životní cyklus informace 17
2.3 Bezpečnost dat a informací 19
2.3.1 Důvěrnost 19
2.3.2 Integrita 22
2.3.3 Dostupnost 24
3. kapitola – Kybernetické útoky 26
3.1 Sociální inženýrství 30
3.2 Cílené a plošné útoky 32
3.2.1 Cílené útoky 37
3.2.2 Plošné útoky 38
3.3 Malware 40
3.3.1 Drive by-download malware 42
3.3.2 Malvertising 43
3.3.3 Watering holes 45
3.4 Botnet 46
3.5 Ransomware 49
3.5.1 Ransomware šifrující soubory 50
3.5.2 Ransomware blokující počítač 51
3.6 Trojanizované aplikace 52
3.7 DDoS 52
3.8 APT 56
3.8.1 Příprava k útoku 58
3.8.2 Průnik 59
3.8.3 Kompromitace 60
3.8.4 Dokončení 60
3.9 Vektory útoku 62
3.9.1 SPAM 63
3.9.2 Phishing 68
3.9.3 Praktický příklad 71

4. kapitola – Řízení informační bezpečnosti 86
4.1 Aktiva 88
4.2 Hrozby 90
4.3 Zranitelnosti 93
4.3.1 Zranitelnost nultého dne 95
4.3.2 Hodnocení zranitelnosti 96
4.4 Bezpečnostní politika 98
5. kapitola – Základní sada bezpečnostních opatření 101
5.1 Typy opatření 101
5.2 Identifikace 104
5.3 Autentizace 106
5.3.1 Autentizace založená na znalosti sdíleného tajemství 106
5.3.2 Autentizace založená na biometrických charakteristikách .. 111
5.3.3 Autentizace založená na vlastnictví předmětu 121
5.4 Autorizace 123
5.5 Auditing a monitoring 124
5.6 Zálohování a archivace 130
5.7 Antimalware 131
5.8 Šifrování 132
5.9 Hashování 134
Závěr 136
Summary 138
Literatura 139
Věcný rejstřík 143