Innhold

Forord 15

Kapittel 1
Grunnleggende begreper for informasjonssikkerhet 17
1.1 Terminologi rundt informasjonssikkerhet 17
1.2 Betydninger av begrepet sikkerhet 18
1.3 Hva er sikkerhet? 19
1.4 Hva er informasjonssikkerhet? 20
1.5 Kilder til krav om informasjonssikkerhet 22
1.6 Trusler, sårbarheter, verdier, hendelser og risikoer 23
1.7 Tiltak for informasjonssikkerhet 25
1.8 KIT-sikkerhetsmålene 27
1.8.1 Konfidensialitet 27
1.8.2 Dataintegritet 28
1.8.3 Systemintegritet 29
1.8.4 Tilgjengelighet 29
1.9 Andre sikkerhetsmål 30
1.9.1 Autentisering 30
1.9.2 Sporbarhet og ubenektelighet 33
1.9.3 Pålitelighet 34
1.10 Autorisering og tilgangskontroll 34
Oppgaver til kapittel 1 36

Kapittel 2
Angrepsvektorer og skadevare 39
2.1 Angrepsvektorer 39
2.1.1 Phishing 40
2.1.2 Drive-by-angrep 41
2.1.3 Falske nettsider 41
2.1.4 Deepfake 41
2.1.5 Direkte angrep mot sårbare systemer og applikasjoner 42
2.1.6 Leveransekjedeangrep 42
2.1.7 Skadelige eksterne enheter 43
2.1.8 Hacking av upatchede sårbare IoT-enheter 44

2.1.9 Uvitende installering av skadevare 44
2.1.10 Innsideangrep 44
2.2 Skadevare 45
2.2.1 Datavirus 45
2.2.2 Løsepengevirus 46
2.2.3 Spionvare 46
2.2.4 Bott-programvare 46
2.2.5 Exploit 47
2.2.6 Makro-virus 47
2.2.7 Trojaner 47
2.2.8 Dataorm 48
2.2.9 Rootkit 48
2.2.10 Bakdør 48
2.2.11 Skadelige JavaScript 48
2.2.12 Logisk bombe 48
Oppgaver til kapittel 2 49

Kapittel 3
Systemsikkerhet 51
3.1 Systemarkitektur 51
3.2 Viktigheten av systemsikkerhet 52
3.3 Håndtering av sårbarheter i systemer og programvare 53
3.4 Privilegienivåer for prosesser i mikroprosessoren 55
3.5 Sårbarheten buffer overflow, utnyttelser og mottiltak 57
3.6 Virtualisering 60
3.6.1 Virtuelle maskiner 61
3.6.2 Virtualiseringsarkitekturer 62
3.6.3 Sikkerhetsaspekter ved virtualisering 63
3.7 Tiltrodd beregning (Trusted Computing) 64
3.8 Sikker oppstart 64
3.9 Intel Management Engine 66
3.10 Sidekanaler og skjulte kanaler 67
3.11 «Datamaskin» – et uheldig ord 68
Oppgaver til kapittel 3 69

Kapittel 4
Kryptografi 71
4.1 Hva er kryptografi? 71
4.2 Kryptografiske funksjoner 72
4.3 Symmetriske algoritmer 72
4.4 Krypteringsmodus for blokkchiffer 74
4.4.1 ECB: Elektronisk kodebok 75
4.4.2 CTR: Tellermodus 75
4.5 Hash-funksjoner og MAC 76

4.6 Diffie-Hellman nøkkelutveksling 78
4.6.1 Tradisjonell Diffie-Hellman 78
4.6.2 ECDH: Elliptisk kurve Diffie-Hellman 79
4.7 Asymmetriske algoritmer 80
4.7.1 RSA-algoritmen 81
4.7.2 Hybrid kryptering 82
4.7.3 Digital signatur 84
4.7.4 Autentisert kryptering med fremoverhemmelighold 86
4.8 Kryptografiens historie 87
4.8.1 Klassiske chiffer 87
4.8.2 Chiffer i middelalderen 88
4.9 Chiffer frem mot første verdenskrig 89
4.9.1 Kerckhoffs-prinsippet 89
4.9.2 Engangsnøkkel 89
4.10 Chiffer rundt andre verdenskrig 90
4.10.1 Rotorchiffer fra andre verdenskrig 90
4.10.2 Shannons teori om kryptografi 91
4.11 Chiffer frem mot år 2000 93
4.12 Chiffer etter år 2000 94
4.12.1 Blokkchiffer: Erstatte en gammel og sliten hest med en ung og sterk 94
4.12.2 Hash-funksjoner: Det trengtes nye svamper 94
4.12.3 Postkvantekrypto: En redningsbåt i tilfelle skipet synker 95
4.13 Kryptografi og energiforbruk 97
4.13.1 TLS overalt 97
4.13.2 Kryptovaluta 98
Oppgaver til kapittel 4 100

Kapittel 5
Nøkkelhåndtering og PKI 101
5.1 Nøkkelhåndtering 101
5.1.1 Nøkkeltyper 101
5.1.2 Kryptoperioder 102
5.1.3 Nøkkelstørrelser 103
5.1.4 Livssyklus for nøkler 105
5.2 PKI 106
5.2.1 Nøkkeldistribusjonsproblemet 106
5.2.2 X.509-sertifikater og PKI-komponenter 107
5.2.3 Generering av X.509-sertifikater 109
5.2.4 Validering av X.509-sertifikater 110
5.2.5 Tillitsmodeller for PKI 111
5.3 Utfordringer og løsninger for PKI 112
5.3.1 PKI støtter kun tillit til autentisitet 112
5.3.2 Sertifikatrevokering 113

5.3.3 CA-autorisering og sertifikattransparens 114
5.4 Bruk av blokkjeder 114
Oppgaver til kapittel 5 115

Kapittel 6
Nettverkssikkerhet 117
6.1 Datanett og internett 117
6.2 Kommunikasjonssikkerhet 122
6.2.1 TLS – Transport Layer Security 123
6.2.2 IPSec – Internet Protocol Security 126
6.2.3 VPN – Virtuelle private nett 127
6.2.4 Steganografi 129
6.3 Datanettsikkerhet 129
6.4 Brannmurer 130
6.4.1 Tilstandsløst pakkefilter 131
6.4.2 Tilstandsbasert pakkefilter 131
6.4.3 Applikasjonsbrannmur 131
6.5 Inntrengningsdeteksjon 132
6.5.1 Signaturbasert deteksjon 132
6.5.2 Anomalibasert deteksjon 133
6.6 Nettverksarkitektur for sikkerhet 133
6.7 TLS-inspeksjon 134
Oppgaver til kapittel 6 137

Kapittel 7
Trådløs sikkerhet 139
7.1 Radiokommunikasjon 139
7.1.1 Radiosignaler 139
7.1.2 Radiospekteret 140
7.2 Sikkerhet i wifi 142
7.2.1 Grunnleggende wifi-konsepter 142
7.2.2 Utvikling av sikkerhet i wifi 142
7.2.3 Sikker nettverkstilgang med WPA 143
7.2.4 SAE (Simultaneous Authentication of Equals) 145
7.3 Sikkerhet i blåtann 145
7.3.1 Blåtannteknologier 146
7.3.2 Paring og tilkobling 148
7.3.3 SSP og autentisering mellom enheter 148
7.3.4 Sikkerhetsråd for blåtann 149
7.4 Sikkerhet i mobilnett 150
7.4.1 Teknologier for mobilnett 150
7.4.2 Sikkerhetsarkitektur i 2G 151
7.4.3 IMSI-fanger 152
7.4.4 Sikkerhet i 4G 154

7.4.5 Sikkerhet i 5G 154
7.4.6 SIM, eSIM og iSIM 156
Oppgaver til kapittel 7 157

Kapittel 8
Brukerautentisering 159
8.1 Hva er brukerautentisering? 159
8.2 Autentiseringsmetoder 160
8.3 Kunnskapsbaserte autentikatorer: passord og lærte mønster 160
8.3.1 Beskyttelse av passord mot cracking 160
8.3.2 Råd om sterke passord 164
8.4 Eierskapsbaserte autentikatorer: enheter 164
8.4.1 OTP-brikker 165
8.4.2 Brukerautentisering med online-enheter 166
8.4.3 Adgangs- og ID-kort 167
8.4.4 Sekundære kanaler 168
8.5 Egenskapsbaserte autentikatorer: biometri 169
8.5.1 Krav til biometriske systemer 170
8.5.2 Virkemåte og komponenter i biometriske systemer 170
8.5.3 Kvalitetsaspekter ved biometriske systemer 172
8.5.4 Trygghetsaspekter ved biometriske systemer 174
8.6 Flerfaktor-autentisering 174
8.7 Veiledere for autentisering 175
Oppgaver til kapittel 8 178

Kapittel 9
IAM – identitets- og tilgangshåndtering 179
9.1 Definisjon av IAM 179
9.2 Identitetshåndtering 181
9.2.1 Identitet 181
9.2.2 Silomodell for identitetshåndtering 183
9.2.3 Føderert identitetshåndtering 184
9.2.4 Protokoller for ID-føderering 185
9.2.5 OpenID Connect 186
9.2.6 Identitetsføderasjonene ID-porten, Altinn og FEIDE 187
9.2.7 Identitetsføderasjonene Facebook, Twitter, Google etc. 189
9.2.8 Kategorisering av identitetsføderering 190
9.3 Tilgangskontroll 193
9.3.1 DAC: Navnebasert tilgangskontroll 193
9.3.2 MAC: Merkebasert tilgangskontroll 194
9.3.3 RBAC: Rollebasert tilgangskontroll 196
9.3.4 ABAC: Attributtbasert tilgangskontroll 197
9.4 OAuth og distribuert tilgangsstyring 198
9.4.1 OAuth i sosiale nettverk 198

9.4.2 OAuth for tilgang og samhandling mellom helseinstitusjoner 199
Oppgaver til kapittel 9 200

Kapittel 10
Personvern 201
10.1 Hva er forskjellen mellom personvern og personopplysningsvern? 201
10.2 Personvern i den digitale tidsalderen 202
10.3 Personverninvaderende teknologier 203
10.3.1 Sporing med informasjonskapsler 204
10.3.2 Sporing med e-postadresser og telefonnummer 206
10.3.3 Sporing med plattformfingeravtrykk 206
10.3.4 Sporing med mobilapper 207
10.4 Blokkering av sporing 208
10.5 GDPR og personopplysningsloven 209
10.6 Roller i GDPR 210
10.6.1 Den registrerte og tilhørende personopplysninger 211
10.6.2 Den behandlingsansvarlige 212
10.6.3 Databehandleren 212
10.6.4 Personvernombudet 212
10.6.5 Tilsynsmyndigheten og straff ved overtredelse av GDPR 212
10.7 Spesielt relevante artikler i GDPR 213
10.7.1 Artikkel 5: Prinsipper for behandling av personopplysninger 213
10.7.2 Artikkel 6: Behandlingens lovlighet 215
10.7.3 Artikkel 25: Innebygd personvern 216
10.7.4 Artikkel 32: Sikkerhet ved behandlingen 217
10.7.5 Schrems II-dommen og Artikkel 45 og 46 om overføring av personopplysninger til land utenfor EU/EØS 218
10.8 Artikkel 35: Vurdering av personvernkonsekvens – DPIA 220
10.8.1 Prosessen rundt DPIA 220
10.8.2 Når er det nødvendig å utføre en DPIA? 221
10.8.3 Trusselaktører som element i vurdering av risiko 222
10.8.4 Hvem skal utføre DPIA? 222
10.8.5 Trinnene i DPIA 223
10.9 Varsling ved brudd på personopplysningssikkerhet 226
10.10 Terminologi for personvern 226
Oppgaver til kapittel 10 227

Kapittel 11
Innebygd informasjonssikkerhet 229
11.1 Innebygd informasjonssikkerhet 229
11.2 Innebygd personvern 230
11.3 De syv fasene av innebygd informasjonssikkerhet 231
11.3.1 Opplæring 231
11.3.2 Krav til informasjonssikkerhet og personvern 233

11.3.3 Sikkert design . . . 233
11.3.4 Sikker koding . . . 233
11.3.5 Sikkerhetstesting av programvare . . . 234
11.3.6 Produksjonssetting . . . 235
11.3.7 Forvaltning . . . 236
11.4 Sikker programvareutvikling . . . 237
11.4.1 Fossefallmetoden . . . 237
11.4.2 Smidig programvareutvikling . . . 237
11.4.3 Sikker smidig programvareutvikling . . . 238
11.4.4 Sikkerhets-champion . . . 239
11.5 Identifisering av trusler under programvareutvikling . . . 240
11.5.1 Trusselmodellering . . . 240
11.5.2 Brukerhistorier og bruksmønster . . . 241
11.5.3 Angriperhistorier og trusselscenarioer . . . 241
11.5.4 STRIDE trusselmodellering i programvareutvikling . . . 242
11.6 Applikasjonssikkerhet . . . 243
11.6.1 Web-applikasjoners eksponering mot trusler . . . 243
11.6.2 OWASP: The Open Web Application Security Project . . . 244
11.6.3 OWASP Top 10 . . . 244
11.6.4 OWASP ASVS . . . 245
11.7 Eksempel på angrep mot applikasjoner . . . 246
11.7.1 SQL-injeksjon . . . 246
11.7.2 XSS: Cross-Site Scripting . . . 247
11.8 Sikkerhet i skyen . . . 248
11.8.1 Skytjenester . . . 248
11.8.2 Skysikkerhet . . . 250
11.8.3 DevOps . . . 252
11.8.4 Cloud Security Alliance . . . 253
11.9 Sikkerhet i digitale leveransekjeder . . . 253
Oppgaver til kapittel 11 . . . 254

Kapittel 12
Styring og ledelse av informasjonssikkerhet . . . 255
12.1 Styringsnivåer for informasjonssikkerhet . . . 255
12.1.1 Styring av informasjonssikkerhet . . . 256
12.1.2 Spørsmål som styret og toppledelsen bør stille seg . . . 258
12.1.3 Ledelse av informasjonssikkerhet . . . 259
12.1.4 Administrasjon og drift av informasjonssikkerhet . . . 259
12.2 Standarder og rammeverk for styring og ledelse av informasjonssikkerhet . . . 260
12.3 ISO/IEC 27000-serien med standarder . . . 261
12.3.1 Historien bak ISO/IEC 27001 og 27002 . . . 261
12.3.2 ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet (ISMS) – krav . . . 263
12.3.3 Prosessyklus for ISMS . . . 266

12.3.4 ISO/IEC 27002 Informasjonssikkerhetstiltak 268
12.3.5 27000-familien av standarder 269
12.4 Grunnprinsipper for IKT-sikkerhet 271
12.5 NIST Cybersecurity Framework 272
12.6 Modenhet i styring av informasjonssikkerhet 274
Oppgaver til kapittel 12 275

Kapittel 13
Sikkerhetskultur 277
13.1 Definisjon av sikkerhetskultur 277
13.2 Bygging av sikkerhetskultur 278
13.3 Innsidetrusselen 279
13.3.1 Personlig integritet 280
13.3.2 Ledelsens ansvar for håndtering av innsidetrusselen 282
13.4 Sosial manipulering 283
13.5 Tekno-sosial manipulering 283
13.5.1 Phishing-angrep 283
13.5.2 Deteksjon av phishing-angrep 284
13.5.3 Hvis du er blitt offer for sosial manipulering 285
13.6 Fysisk sosial manipulering 285
13.6.1 Angrepsstrategier for fysisk sosial manipulering 285
13.6.2 Forsvar mot fysisk sosial manipulering 287
13.7 Sikkerhetsbrukervennlighet og sikkerhetslæring 289
Oppgaver til kapittel 13 291

Kapittel 14
Risikostyring for informasjonssikkerhet 293
14.1 Tolkning av risiko og risikostyring 293
14.1.1 Definisjon av informasjonssikkerhetsrisiko 294
14.1.2 Modeller for informasjonssikkerhetsrisiko 295
14.1.3 Definisjon av risikostyring for informasjonssikkerhet 298
14.2 Prosess for risikostyring 298
14.2.1 Kontekstetablering 299
14.2.2 Risikovurdering 300
14.2.3 Risikohåndtering 301
14.2.4 Risikohåndteringsplan og akseptert risiko 303
14.3 Prosess for risikovurdering 304
14.4 Risikoidentifisering 304
14.4.1 Identifisering av verdier 305
14.4.2 Trusselmodellering: Identifisering av trusler 306
14.4.3 Identifisering av konsekvenser 307
14.4.4 Registrering av risikoer 308
14.5 Risikoanalyse 308
14.5.1 Kvalitativ risikoanalyse 309

14.5.2 Relativ risikoanalyse 310
14.5.3 Kvantitativ risikoanalyse 312
14.6 Risikoevaluering og rapportering 313
Oppgaver til kapittel 14 314

Kapittel 15
Lover og regelverk for informasjonssikkerhet 317
15.1 Viktigheten av regelverk om informasjonssikkerhet 317
15.1.1 Regelverk som kilde til krav om informasjonssikkerhet 317
15.1.2 Ansvar 318
15.2 Grunnleggende begreper om regelverk 319
15.2.1 Hierarki av regelverk og krav 319
15.2.2 Formål og virkeområde til lover og forskrifter 320
15.2.3 Sammenheng mellom lover og forskrifter 320
15.3 Sentrale lover for informasjonssikkerhet 321
15.3.1 Sikkerhetsloven 321
15.3.2 Andre relevante lover og forskrifter for informasjonssikkerhet 322
15.3.3 Regelverk fra EU 323
Oppgaver til kapittel 15 325

Kapittel 16
Beredskap og hendelseshåndtering 327
16.1 Bakgrunn for beredskap og hendelseshåndtering 327
16.2 Beredskapsprinsippene 329
16.3 Tekniske beredskapsbegreper 330
16.4 Beredskapsplanlegging 331
16.5 Hendelseshåndtering 332
16.6 Digital etterforskning 335
16.7 NCSC og sektorvise responsmiljøer 337
Oppgaver til kapittel 16 338

Kapittel 17
Cyberoperasjoner 339
17.1 Avanserte cybertrusler 339
17.1.1 APT: Avansert vedvarende trussel 339
17.1.2 Cyber Kill Chain – en modell for APT-angrep 340
17.2 CTI: Digital trusseletterretning 341
17.2.1 Kategorier og nivåer av digital trusseletterretning 342
17.2.2 MITRE ATT&CK 344
17.2.3 Syklus for CTI 345
17.2.4 Deling av CTI 347
17.2.5 Representasjon og bruk av CTI 348
17.3 Sikkerhetstesting av systemer, nettverk og virksomheter 349
17.3.1 Pentesting 349

17.3.2 Red-teaming og blue-teaming 349
17.3.3 TIBER 350
17.4 Cyberkrigføring 351
17.4.1 Sammenligning av våpen 352
17.4.2 Cyberavskrekking og cyberkaperfart 353
17.4.3 IT-sektorens rolle i cyberkrigføring 355
Oppgaver til kapittel 17 356

Forkortelser 357

Oversettelser: engelsk – norsk 360

Oversettelser: norsk – engelsk 363

Stikkord 366