

Innhold

Forord	13
Kapittel 1 Introduksjon til digital sikkerhet	15
<i>Ronny Windvik</i>	
1.1 Digitalisering	19
1.2 Sikkerhet	19
1.3 Sikkerhetsmål	21
1.3.1 Konfidensialitet	21
1.3.2 Integritet	22
1.3.3 Tilgjengelighet	22
1.4 Kryptografi	24
1.4.1 Krypteringsnøkler	25
1.4.2 Symmetrisk kryptering	26
1.4.3 Asymmetrisk kryptering	27
1.4.4 Hash-funksjoner	29
1.4.5 MAC-funksjoner	30
1.5 Oppsummering og tips	31
Oppgaver	32
Referanser	32
Kapittel 2 Sikkerhetskultur	33
<i>Bjarte Malmedal</i>	
2.1 Innledning	33
2.2 Hva er kultur?	34
2.3 Digital sikkerhetskultur	35
2.4 Digital sikkerhetskultur – grunnleggende faktorer	35
2.4.1 Fellesskap	37
2.4.2 Styring og kontroll	37
2.4.3 Tillit	38

2.4.4	Risikooppfattelse	39
2.4.5	Optimisme for teknologi og digitalisering	40
2.4.6	Kompetanse	40
2.4.7	Interesse for teknologi og IT	41
2.4.8	Adferdsmønstre	42
2.5	Forandre en digital sikkerhetskultur	43
2.6	Oppsummering og tips	44
	Oppgaver	46
	Referanser	46
Kapittel 3 Sikkerhet i et digital-etisk perspektiv		47
<i>Leonora Onarheim Bergsjø</i>		
3.1	Innledning	47
3.1.1	Etikk, dilemmaer og ny teknologi	48
3.2	Digital etikk	49
3.2.1	Er ikke teknologien nøytral?	49
3.2.2	Når algoritmene får bestemme	50
3.2.3	Teknologi som utfordrer	51
3.2.4	Digital-etisk refleksjon over ny teknologi	52
3.3	Digital-etiske vurderinger	53
3.3.1	Digital-etisk risikovurdering	53
3.3.2	Lovlig, etisk og robust teknologi	54
3.3.3	Etiske prinsipper for god teknologi	55
3.3.4	Verdier i konflikt	56
3.4	Etikk i et globalt perspektiv	56
3.4.1	Etikk er gresk for meg	57
3.4.2	Reflektert etikk	57
3.4.3	Applisert etikk	58
3.4.4	Moralske maskiner?	59
3.4.5	Hva slags samfunn vil vi ha?	60
3.5	Oppsummering og tips	61
	Oppgaver	61
	Referanser	62
Kapittel 4 Identifikasjon, autentisering og aksesskontroll		63
<i>Geir M. Køien</i>		
4.1	Innledning – tillit og usikkerhet	63
4.1.1	En tankevekker – nordmenn er elendige på passord	63
4.1.2	Om behovet for identifikasjon og autentisering	63
4.1.3	Personer og prosesser	64

4.1.4	Sjekking av identitet	65
4.1.5	Sjekking av rettigheter	65
4.2	Identifikatorer	65
4.2.1	Entiteter, identitet og identifikatorer	65
4.2.2	Egenskaper	67
4.3	Autentisering og kryptografiske nøkler	67
4.3.1	Angripere	68
4.3.2	Ærlige deltakere	68
4.3.3	Grenser for tillit	68
4.3.4	Typer av autentisering	69
4.3.5	Faktorer	70
4.3.6	Autentiseringsprotokoller	71
4.3.7	Et autentiseringseksempel	72
4.4	Sikker tilstand	75
4.4.1	Om å etablere <i>sikker tilstand</i> («security context»)	75
4.4.2	Levetider	76
4.4.3	Lengder	76
4.4.4	Nøkkelhierarki	77
4.5	Autorisasjon og aksesskontroll	78
4.5.1	Autorisasjon	78
4.5.2	Rettigheter	78
4.5.3	Klarering og autorisasjon	79
4.5.4	Aksesskontroll	80
4.5.5	Sikkerhetsfilosofi	81
4.6	Oppsummering og tips	82
	Oppgaver	83
	Referanser	84
Kapittel 5 Digitalt personvern, ID-tyveri og anonymitet		85
<i>Lasse Øverlier</i>		
5.1	Innledning	85
5.2	Digitalt personvern	86
5.2.1	Overvåkning og informasjonskilder	87
5.2.2	Personverninvaderende teknologier	88
5.2.3	Datamaskin på Internett	93
5.2.4	Smarttelefon	94
5.2.5	«Smartbil»	95
5.2.6	Sosial kredittverdighet	95
5.3	Identitetstyveri	96
5.4	Anonymitet	98

5.4.1	Digital anonymitet.	100
5.4.2	Nettanonymitet	101
5.5	Oppsummering og tips.	105
	Oppgaver.	106
	Referanser.	107
Kapittel 6 Lover og ansvar.		109
<i>Gullik Gundersen</i>		
6.1	Innledning	109
6.1.1	Hvorfor jus i en bok om digital sikkerhet?	110
6.1.2	Generelt om rettslig regulering av digital sikkerhet	110
6.2	Personopplysningsloven og personvernforordningen	112
6.2.1	Introduksjon til personvern	112
6.2.2	Informasjonssikkerhet og personvern	113
6.2.3	Prinsipper	114
6.3	Sikkerhetsloven	117
6.4	Ansvar	120
6.5	Felles regler	120
6.5.1	Dokumentert sikkerhetsstyring.	120
6.5.2	Risikostyring og risikovurdering.	121
6.5.3	Avvikshåndtering og -rapportering	123
6.6	Særregler for behandling av personopplysninger	123
6.6.1	Vurdering av personvernkonsekvenser	123
6.6.2	Innebygd personvern.	124
6.7	Oppsummering og tips.	125
	Oppgaver.	126
	Referanser.	126
Kapittel 7 Sårbarheter i IKT-systemer.		129
<i>Nils Agne Nordbotten</i>		
7.1	Innledning	129
7.2	Hva er en sårbarhet?.	130
7.3	Ulike typer sårbarheter.	134
7.3.1	Eksempel 1: Mulige sårbarheter ved bruk av tjeneste over Internett.	134
7.3.2	Eksempel 2: Sårbarheter i trådløse nettverk	137
7.4	Hvordan kan man redusere sårbarheten i egne systemer?	139
7.5	Oppsummering og tips.	141
	Oppgaver.	142
	Referanser.	142

Kapittel 8 Trusler og etterretning	145
<i>Kristian Malmkvist Eie</i>	
8.1 Innledning	145
8.2 Begreper	146
8.2.1 Hva er en trussel?	147
8.2.2 Hva er forskjellen på en bevisst og en ubevisst trussel? . . .	148
8.2.3 Hvilke faktorer utgjør en trussel?	148
8.2.4 Hva eller hvem er en trusselaktør?	151
8.2.5 Hva betyr Advanced Persistent Threat (APT)?	154
8.2.6 Forskjellen på data, informasjon og etterretning	155
8.3 Digital trusseletterretning	156
8.3.1 Fire sentrale ferdigheter	157
8.3.2 Etterretning som prosess	161
8.3.3 Etterretning som produkt	166
8.4 Å handle basert på etterretning	179
8.5 Oppsummering og tips	181
Oppgaver	182
Referanser	182
 Kapittel 9 Funksjonsbasert risikovurdering	 185
<i>Janita A. Bruvoll, Kjersti Brattekås og Kjell Olav Nystuen</i>	
9.1 Innledning	185
9.2 Hva er risiko?	188
9.3 Standardisert risikovurdering	190
9.4 Hva er systemet og funksjonene, og hvem skal ha kjennskap til det?	193
9.4.1 Verdier og avhengighet	193
9.5 Funksjonsbasert tilnærming til risiko	194
9.5.1 Kritiske samfunnsfunksjoner og infrastrukturer	195
9.5.2 Jernbanen – et eksempel	196
9.5.3 Resiliente funksjoner / resiliens	198
9.6 Oppsummering og tips	200
Oppgaver	201
Referanser	201
 Kapittel 10 Den kommersielle IKT-sikkerhetsbransjen	 203
<i>Thomas Tømmernes</i>	
10.1 En bransje i endring	203
10.2 Kommersiell IKT-kriminalitet	206

10.3 IKT-sikkerhetsbransjen	207
10.3.1 Produsenter	207
10.3.2 Distributører	209
10.3.3 Salg	209
10.4 Fra statusanalyse til avhending	210
10.5 Oppsummering og tips	213
Oppgaver	215
Referanser	215
Kapittel 11 Programvaresikkerhet	217
<i>Martin Gilje Jaatun</i>	
11.1 Hva er programvaresikkerhet?	217
11.2 Alle feil er ikke født like	219
11.3 Måling av sikkerhet	220
11.3.1 Arkitekturanalyse	222
11.3.2 Penetrasjonstesting	225
11.4 OWASP Top Ten	225
11.5 Unngå designfeller	227
11.6 Kan små virksomheter ha en programvaresikkerhetsgruppe?	228
11.7 Lisens til å kode?	229
11.8 Oppsummering og tips	230
Oppgaver	230
Referanser	230
Kapittel 12 Sikkerhetsovervåkning og deteksjon	233
<i>Lasse Rosenvinge og Eirik Nesbakken</i>	
12.1 Kunnskap og visibilitet	234
12.2 Deteksjonsteknologier	237
12.2.1 Nettverk – NIDS	239
12.2.2 Nettverk – logger fra brannmur	241
12.2.3 Nettverk – flowdata (trafikkdata)	241
12.2.4 Nettverk – Passiv DNS	243
12.2.5 Nettverk – Passiv TLS	244
12.2.6 Nettverk – webtrafikklogg – HTTP-logg	246
12.2.7 Nettverk – e-postlogg	247
12.2.8 Klient og server – PC og serverlogger	248
12.2.9 Klient og server – HIDS	249
12.2.10 Dataanalyse – filanalyse ved hjelp av sandkasse	252

12.2.11 Dataanalyse – Security Information and Event Management – SIEM	256
12.2.12 Anomali – anomalideteksjon	259
12.3 Sikkerhetsovervåkning	261
12.4 Deteksjonsevne	262
12.5 Oppsummering og tips	265
Oppgaver	266
Referanser	266
Kapittel 13 Hendelseshåndtering og opprydding	267
<i>Håkon Bergsjø</i>	
13.1 Innledning	267
13.2 De ulike trinnene	269
13.2.1 Forbered virksomheten på håndtering av hendelser (trinn 1)	269
13.2.2 Vurdering og kategorisering (trinn 2)	270
13.2.3 Kontrollere og håndtere hendelsen (trinn 3)	272
13.2.4 Evaluering og læring (trinn 4)	276
13.3 Oppsummering og tips	277
Oppgaver	278
Referanser	278
Engelsk-norsk ordliste	279
Forfatterromtaler	281
Stikkordregister	285