

Innhold

Forord Eldar Lorentzen Lillevik	13
Forord	15
Kapittel 1 Hva er datasikkerhet?	17
1.1 Dagens situasjon	18
1.2 Datasikkerhet	25
1.3 Ledelse	27
Kapittel 2 Trusler på internett	31
2.1 Hacktivisme	33
2.2 Digital kriminalitet	34
2.3 Spionasje	35
2.4 Sabotasje	36
2.5 Bruk av datainnbrudd i krise og krig	38
2.6 Oppsummering og tips	39
Kapittel 3 Metoder ulike aktører bruker	41
3.1 Innbrudd via e-post	42
3.2 Innbrudd via vannhull	43
3.3 Innbrudd via skyleverandører	44
3.4 Innbrudd via gammelt utstyr	45
3.5 Innbrudd via Internett of Things (IoT)	46
3.6 Innbrudd via nettsider og databaser	47
3.7 Innbrudd via ditt eget passord	47
3.8 Innbrudd ved bruk av innsidere	49
3.9 Direktørsvindel og klassisk svindel	49

3.10	Innbrudd gjennom avlytting og tilgang til trafikk	51
3.11	Oppsummering og tips.	52
Kapittel 4 Kartlegging og vurdering av verdier.		55
4.1	Fremgangsmåte for kartlegging og vurdering av verdier.	56
4.2	Eksempel på bruk av fremgangsmåten	59
4.3	Klassifisering av datasystemer og data	64
4.4	Avhengigheter	71
4.5	Oppsummering og tips.	74
Kapittel 5 Risikoanalyse – internkontroll i praksis		75
5.1	Eksempler	77
5.2	Sette risikovurdering inn i mal.	79
5.3	Overføring av risikovurdering til risikoreduserende tiltak.	80
5.4	Hendelser med flere konsekvenser.	80
5.5	Ledelsens fokus	81
5.6	Standarder for arbeidet og maler	81
5.7	Internkontroll i praksis / systematiske aktiviteter	82
5.8	Risikovurdering og risikohåndtering	83
5.9	Overvåkning og hendelseshåndtering	83
5.10	Måling, evaluering og revisjon.	83
5.11	Kompetanse og kulturutvikling	84
5.12	Ledelsens styring og oppfølging	84
5.13	Etterarbeid	85
5.14	Andre grunner til å gjennomføre risikovurdering	86
5.15	Sette det i sammenheng	87
5.16	Grunnprinsipper for IKT-sikkerhet	87
5.17	Oppsummering og tips.	87
Kapittel 6 Personvern		89
6.1	Hva er personopplysninger?.	90
6.2	Ledelsens plikter	91
6.3	Behandling av sensitive personopplysninger.	92
6.4	Internkontroll for personopplysninger	92
6.5	Se det i sammenheng med internkontroll for datasikkerhet.	94
6.6	Eier av flere virksomheter	95
6.7	Utsetting av tjenester	95

6.8	Nye personvernregler gjeldende fra 2018	96
6.9	Når man starter en ny virksomhet	98
6.10	Oppsummering og tips	99
Kapittel 7 E-post		101
7.1	E-postkontoen sin rolle i hverdagen	101
7.2	E-postsikkerhet	105
7.3	Phishing	111
7.4	Spam	116
7.5	Oppsummering og tips	120
Kapittel 8 Mobiltelefoner og nettbrett		123
8.1	Operativsystemer	124
8.2	Sårbarheter og datainnbrudd	125
8.3	Apper som overvåker deg	129
8.4	Egensikring av mobiltelefoner og nettbrett	130
8.5	Oppsummering og tips	130
Kapittel 9 Passord		131
9.1	Tilgang til datasystemer	132
9.2	Passordkneking	138
9.3	Håndtering av passord i hverdagen	141
9.4	Oppsummering og tips	144
Kapittel 10 Innsidetrusselen		145
10.1	Hva menes med en innsidetrussel?	145
10.2	Ledelse og personellsikkerhet	150
10.3	Modenhetsnivåer innen personellsikkerhet	157
10.4	Oppsummering og tips	158
Kapittel 11 Reise		161
11.1	Risikovurdering	161
11.2	Ulike faser av reisen	162
11.3	Bruk av trådløse nett	166
11.4	Kriminalitet og terror	167
11.5	Oppsummering og tips	167

Kapittel 12 Tjenesteutsetting og sky	169
12.1 Tjenesteutsetting	170
12.2 Skytjenester	170
12.3 Ulike typer skytjenester	171
12.4 Lovgrunnlag	172
12.5 Personvernloven	172
12.6 Bokføringsloven	175
12.7 Arkivloven	176
12.8 Sikkerhetsloven – kritisk infrastruktur og samfunnsfunksjoner	176
12.9 Sektorregelverk	178
12.10 Oppsummering og tips	178
Kapittel 13 Enkle tiltak for økt datasikkerhet	179
13.1 Datamaskiner	179
13.2 Mobiltelefoner og nettbrett	182
13.3 Sosiale medier	185
13.4 Passord	186
13.5 E-post	188
13.6 Web	190
13.7 Data	190
13.8 Rutiner	192
Kapittel 14 Kostnader	195
14.1 Hva koster dårlig datasikkerhet?	195
14.2 Hva koster god datasikkerhet?	197
14.3 Oppsummering og tips	204
Kapittel 15 Hendelseshåndtering	205
15.1 Indikatorer på at noen har brutt seg inn	205
15.2 De første timene	207
15.3 Situasjonsforståelse og lederstøtte	208
15.4 Grov handlingsplan	208
15.5 Hvordan be om hjelp?	209
15.6 Logger	210
15.7 Samarbeid med de som hjelper	211
15.8 Hvordan kommunisere og dokumentere når systemet er tatt over? ..	211
15.9 Merkevarer under angrep	211

15.10 Anmeldelse	213
15.11 Personvern	213
15.12 Holde aktørene ute	214
15.13 Hvem står bak?	215
15.14 Oppsummering og tips	215
Kapittel 16 Hvor får man hjelp?	217
16.1 Eget ansvar	217
16.2 Støtte fra offentlige virksomheter	218
16.3 Sektorvise responsmiljøer	220
16.4 NSMs kvalitetsordning	222
16.5 Hvor kan jeg få informasjon om datasikkerhet?	222
16.6 Oppsummering og tips	223
Referanser	225
Stikkord	235