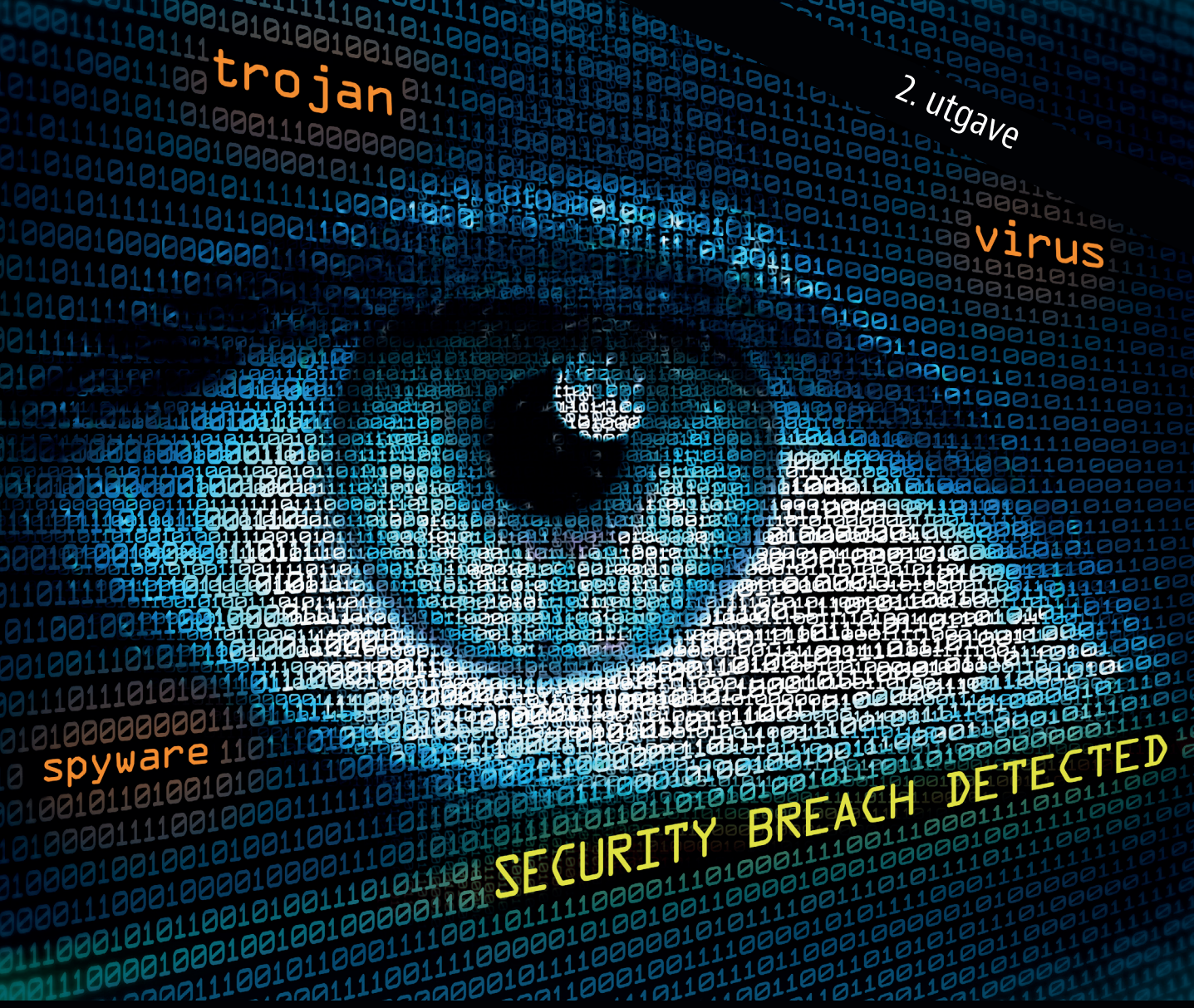


Tom Heine Nätt og Christian F. Heide

DATASIKKERHET

Ikke bli svindlerens neste offer

GYLDENDAL

Tom Heine Nätt og Christian F. Heide

Datasikkerhet

Ikke bli svindlerens neste offer

GYLDENDAL

© Gyldendal Norsk Forlag AS 2021
2. utgave, 1. opplag 2021

ISBN 978-82-05-556485-5

Omslagsdesign: Gyldendal Akademisk
Layout: HAVE A BOOK
Figurer: David Keeping
Omslagsbilde: Ulya Erdem/Istock
Bilderedaktør: Anette Badendyck
Bildene på side 103, 117, 135, 206, 210, 211n, 218, 302, 303 og 392: © forfatterne
Sats: HAVE A BOOK
Brødtekst: Minion Pro 10,5/15 pkt

Alle henvendelser om boken kan rettes til
Gyldendal Akademisk
Postboks 6730 St. Olavs plass
0130 Oslo

www.gyldendal.no/akademisk
akademisk@gyldendal.no

Forfatterne har mottatt støtte fra Det faglitterære fond

Det må ikke kopieres fra denne boken i strid med åndsverkloven eller avtaler om kopiering inngått med KOPINOR, interesseorgan for rettighetshavere til åndsverk. Kopiering i strid med lov eller avtale kan medføre erstatningsansvar og inndragning, og kan straffes med bøter eller fengsel.

FORORD

Takk for at du tar deg tid til å lese denne boka!

Den har som mål at du skal bli mer bevisst på datasikkerhet i dagliglivet. Vi ønsker å gjøre deg oppmerksom på hvilke farer som lurer, hvordan du oppdager dem, og hvordan du avverger dem. Med andre ord: Vi ønsker å gi deg en sikrere hverdag.

For å gjøre boka aktuell både over tid og på tvers av ulikt utstyr og programvare vil ikke boka ha detaljerte fremgangsmåter for helt spesielle angrep mot enkeltversjoner av programvare eller operativsystemer. Farer endrer seg konstant, så vårt mål er å lære deg til å tenke selv, ikke å følge oppskrifter.

Innholdet vil derfor gi deg en mer generell sikkerhetstankegang som gjør at du kan oppdage og avverge nye farer som måtte dukke opp, og svindel som er skreddersydd mot enkeltbrukere. Vi har med andre ord ønsket å lage en bok som gjør deg sikkerhetsbevisst.

Som vi alle vet, endrer teknologi seg svært raskt. Derfor kan eksempler, skjermbilder og fremgangsmåter være endret etter at boka ble publisert. Der vi omtaler produkter og tjenester, er dette bare for å illustrere generelle prinsipper. Disse omtalene er ikke ment som anbefalinger.

Selv om det ikke stilles store krav til forkunnskaper, vil enkelte deler av innholdet kunne fremstå noe teknisk. Husk da at det viktige er å forstå hva som kan gjøres, ikke hvordan det gjøres. Du trenger ikke å forstå alle detaljene som en hacker må kunne. Det er hva farene innebærer for deg, og hvordan du avverger dem, som er viktig.

Denne bokas mål er selvsagt ikke å utdanne hackere. For å kunne beskytte seg er det imidlertid viktig å vite hvordan hackere tenker, og til en viss grad hvordan angrep utføres. Denne boka vil derfor inneholde beskrivelser av mye som kan benyttes til å skade andre.

Vi vil på det sterkeste fraråde noen å utnytte kunnskapen de får gjennom denne boka, til å utføre kriminelle handlinger eller handlinger som kan skade andre. Husk at også ting som er ment som en spøk, kan være kriminelt.

HVEM ER DENNE BOKA FOR?

Denne boka er for deg! Enten du er deltaker på et kurs, student ved en høgskole eller et universitet, elev på videregående, ansatt i en bedrift eller en privatperson. Flink i IT eller ei. Alle har behov for å lære mer om datasikkerhet, for dette angår alles hverdag.

BOKAS OPPBYGNING

Boka er inndelt tematisk, der hvert kapittel tar for seg områder som nettsider, e-post, sosiale medier, datalagring og netthandel. I tillegg er det et kort introduksjonskapittel som tar for seg dagens datasikkerhet på mer generelt grunnlag.

I de senere kapitlene i boka blir det brukt begreper og teknikker som er forklart i tidligere kapitler. Det skal likevel være helt uproblematisk å lese bare enkeltkapitler. Ordlisten bak i boka kan da være til hjelp.

Gjennom boka finnes det flere typer informasjonsbokser:

Nerdestoff: Disse boksene inneholder informasjon som kan utdype temaet dersom du sitter inne med mer avansert IT-kunnskap. Typisk inneholder boksene henvisning til programkode.

Bedrifter: Disse boksene tar for seg noen utfordringer som spesielt gjelder forholdet mellom ansatte og bedrifter.

Eksempel: Her presenterer vi relevante eksempler som illustrerer de ulike angrepsformene.

På siden: Disse seksjonene har innhold som kan knyttes til temaet, men som ikke er helt sentralt.

Sjekkliste: Her kommer noen gode råd og oppsummering av hva du kan gjøre for å beskytte deg.

Bakerst i boka finner du en ordliste for litt mer tekniske begreper og et stikkordregister.

Vi vil også gjøre oppmerksom på at vi i boka bruker en del fiktive nettadresser og e-postadresser i våre eksempler, som `http://www.vgnet.no/` og `ola@avsender.no`. Disse adressene var ikke i bruk da boka ble skrevet, men det er umulig for oss å gi en garanti for at ikke noen på et senere tidspunkt registrerer enkelte av adressene og tar dem i bruk.

Videre gjør vi oppmerksom på at noen av skjermbildene vi bruker, er konstruert spesielt for denne boka, og dermed ikke er skjermbilder av reelle hendelser. Det er for å anonymisere hendelsene eller for å oppnå en høyere kvalitet til trykk.

NYTT I 2. UTGAVE

I 2. utgave av boka er det foretatt en generell oppdatering av innholdet. Vi har også skrevet tre nye kapitler.

Det første av disse heter Nettvett, og er tenkt som en hjelp for alle som er på nett, med fokus på vanlige svindler man kan bli utsatt for, og hvordan man kan unngå å gå i disse fellene.

Det andre nyskrevne kapittelet er om barn og unge og hvordan man som foreldre og lærere skal kunne hjelpe barn til å beskytte seg mot svindlere og overgripere på nettet.

Det tredje er spesielt rettet mot bedrifter og organisasjoner, men vi tror mye av stoffet i dette kapittelet kan være av interesse også for privatpersoner. I tillegg er kapitlene om sosiale medier skrevet om og samlet i ett kapittel.

TAKK TIL

Først vil vi takke vår arbeidsgiver Høgskolen i Østfold og Det faglitterære fond for at de hadde tro på ideen, og for at de har gjort prosjektet mulig å gjennomføre.

I tillegg vil vi få takke følgende personer for at de tok seg tid til å lese og gi tilbakemeldinger på manus for første utgave: Ole Anders Danielsen, Kristoffer Møgster Berge, Henrik Heide, Jim Melby og Tor Moltu.

OM FORFATTERNE

Forfatterne av denne boka arbeider til daglig ved Høgskolen i Østfolds avdeling for informasjonsteknologi, der de blant annet underviser i emnene «Innføring i datasikkerhet», «Informasjonssikkerhet» og «Datasikkerhet i utvikling og drift».

Tom Heine Nätt har en mastergrad i informatikk fra Høgskolen i Østfold. Han er en ettertraktet foredragsholder og har formidlet datasikkerhet i en årrekke.

Christian F. Heide er sivilingeniør fra NTNU. Han har tidligere arbeidet ved Televerkets forskningsinstitutt blant annet med datasikkerhet, og har også arbeidet i konsulentbedriftene Scandpower og Commitment.

INNHOLD

KAPITTEL 1
DATASIKKERHET OG DATAKRIMINALITET **17**
- Datakriminalitet **18**
- Hvem står bak? **19**
  - Hva vil de? **23**
  - Tilgang **24**
- Brukernes kunnskap og holdninger **25**
  - Det skjer ikke meg **26**
  - Uønskede sikkerhetstiltak **27**
  - Teknisk datasikkerhet **28**
- Sosial manipulering **28**
  - Hvorfor fungerer sosial manipulering? **31**
  - Psykologi **31**
  - Informasjon **35**

KAPITTEL 2
E-POST **37**
- Forfalskning av e-post **38**
- E-post og svindel **43**
  - Klassisk svindel **44**
  - Nettfiske **46**
  - Spredning av skadevare **52**
  - Svindlernes e-postlister **53**
  - Å oppdage søppelpost **55**
- Sporing gjennom e-post **56**
- Avlytting **56**
  - E-postklienter **57**
  - Mellomledd **57**
  - Kryptering av e-post **59**

KAPITTEL 3
NETTSIDER 65
Nettsvindel 66
Kopier av nettsider 66
Nettsider for nettfiske 68
Informasjonstyveri 72
Klassisk svindel 73
Spredning av skadevare 73
Sikkerhetsfiltre for nettsider 75
Hackede nettsider 76
Nettadresser 78
Oppbygning 78
Kortadresser 81
Omdirigering 82
HTTPS 83
Kryptering 84
Autentisering 84
Hvorfor benyttes fortsatt HTTP? 85
Hvor kan ting gå galt med HTTPS? 86
Publisering på nett 87

KAPITTEL 4
PASSORD OG BRUKERKONTOER 91
Hva er et godt passord? 92
Unngå passord med personlig informasjon 92
Unngå vanlige passord 92
Unngå ordlistepassord 93
Unngå korte passord med enkle tegn 94
Hvordan lage et godt passord? 95
Begrensninger i systemene 97
Gjenbruk av passord 98
Verktøy for å knekke passord 100
Personlig håndtering av passord 101
Ikke gi passordet til andre 104
Tjenesters håndtering av passord 105
Glemt passord 105
Passordhint 106
Klartekstpassord 106
Tofaktorautentisering 109
Elektronisk identitet 110
Urettmessig tilgang til brukerkontoer 111
Passiv bruk 111
Aktiv bruk 113
Hvilke brukerkontoer har vi? 114

KAPITTEL 5
MASKINER, PROGRAMVARE OG DATALAGRING **115**
Fysisk tilgang **115**
Omgå autentisering **116**
Maskinvare **117**
Podslurping **120**
Svakheter i programvare **120**
Mangel på oppdateringer **121**
Fjernstyring **122**
Sikker oppbevaring av data **123**
Kryptering av data **124**
Sikkerhetskopier **125**
Å kvitte seg med maskinvare **126**
Metadata i filer **128**
Bruk av andres maskiner **133**
Skytjenester **134**
Tjenesteleverandørene **135**
Beskyttelse av data **137**
Tilgang på data **137**
Brukeren **137**
Datamaskiner er ikke lenger en PC **138**
Enheter i hjem og kontor **138**
Kjøretøy **141**

KAPITTEL 6
DATATRAFIKK OG NETTVERK **145**
Avlytting og modifikasjon av datatrafikk **146**
Skadevare **148**
Kablede lokalnett **149**
Trådløse nett **150**
Sporing av datatrafikk **155**
DNS **157**
DNS-forfalskning **160**
Modifiserte DNS-oppslag **162**
DNS-kapring **162**
DNS-avlytting **163**
Nettverksutstyr **164**
Brannmurer **167**

KAPITTEL 7
SKADEVARE 169
Skadevarens oppbygning 169
Spredning og infeksjon 170
Virus 170
Orm 171
Trojaner 172
Drive-by-download 173
Makrovirus 174
Inkubasjon 176
Nyttelast 177
Hærverk 177
Økonomisk vinning 178
Spredning av propaganda og reklame 180
Spionvare 180
Rootkits 181
Deteksjon, kamuflasje og fjerning 182
Signaturbasert deteksjon 183
Heuristikk 184
Snubletråder 184
Utfordringer og svakheter ved antivirusprogrammer 185
Fjerning 187
Nye typer skadevare 189
Tillitvekkende skadevare 189
Manuell skadevare 189
Intelligent skadevare 190
Skreddersydd skadevare 190
Selvoppdaterende skadevare 191
Utviklingsverktøy og maler for skadevare 191
Sosiale medier 191
Botnett 192
Hoax 193

KAPITTEL 8
MOBILE ENHETER 197
Applikasjoner 198
Tilgangsrettigheter 200
Mobil skadevare 202
Økonomisk svindel 203
Ukjente kilder 203
Falske apper 206

Fysisk tilgang og sikring ... 207
Skjermlås ... 207
USB-tilkobling ... 210
Minnekort ... 211
Sporing og fjernsletting ... 212
Kast og salg av mobile enheter ... 214
Kommunikasjon ... 216
Mobiltrafikk ... 216
Trådløse nett ... 216
Blåtann ... 217
Overvåkning ... 219
Tilstedeværelse ... 221
SMS ... 221
SMS-svindel ... 222
Telefonoppringninger ... 224
Jailbreaking og rooting ... 224

KAPITTEL 9
NETTVETT ... 227
Informasjon – svindlernes gull ... 228
Hvem har tilgang til vår informasjon? ... 229
Hva deler andre om meg? ... 237
Skjult informasjon i tjenester ... 239
Identitetstyveri ... 242
Konkurranser og undersøkelser ... 242
Falsk informasjon ... 249
Utpressing ... 251
Opplevd anonymitet ... 253
Raske penger ... 255
Nettdating ... 257
Noen generelle tips ... 258
Ikke la følelsene styre ... 259
Gjør enkle nettsøk ... 259
Ikke alt som ser bra ut, er det ... 260
Er det for godt til å være sant, så 260
Ikke stol på alt du ser ... 260
Ikke stol på kjente ... 261
Ikke stol på teknologien ... 261
Innse at du kan bli et offer ... 261
Når skaden har skjedd ... 262

KAPITTEL 10
SOSIALE MEDIER ... 265
Profiltyverier ... 266
Fysisk tilgang ... 266
Nettfiske ... 267
Venner og kontakter ... 269
Venneforespørsler fra ukjente ... 270
Profilkopier ... 271
Svindel fra «venner» ... 273
Oppsøkte kontakter ... 276
Kontakt fra fremmede ... 276
Personverninnstillinger ... 278
Standardinnstillinger ... 280
Tredjepartstjenester / eksterne aktører ... 280
Apper ... 280
Nettsider og programvare ... 284
Klikkapring ... 285
Hva «liker» og deler vi egentlig? ... 287
Overvåkning og personvern ... 290

KAPITTEL 11
NETTHANDEL OG NETTBANK ... 293
Kjøp av varer og tjenester ... 293
Skuffende varer ... 294
Farlige varer ... 294
Ikke-eksisterende varer ... 294
Vaklende butikker ... 295
Kopier av eksisterende nettbutikker ... 295
Mangel på rettigheter ... 295
Kamuflerte butikker ... 295
Oppdage svindelbutikker ... 297
Auksjonstjenester, annonsetjenester og markedsplasser ... 300
Betaling på nett ... 301
Lagring av kortdata ... 304
Verifisering ... 305
Logosvindel ... 306
Spionvare og keyloggers ... 306
La andre ta risikoen ... 306
Nettbank ... 308
Nettfiske ... 308
Skadevare ... 311
Kodebrikker og identifisering ... 312

KAPITTEL 12
BARN OG UNGE **313**
Digital deltakelse **315**
Overordnede trusler **317**
Mobbing **317**
Overvåkning **317**
Økonomiske svindler **318**
Informasjon på avveie **320**
Nettovergrep **322**
Utpressing **324**
Falsk informasjon **324**
Ulovlige handlinger **325**
Regler og regelbrudd **326**
Begrunnelse og identifiserbarhet **326**
Rimelighet **328**
Håndheving og oppfølging **328**
Hvordan følge med og kontrollere? **329**
Holdninger og kunnskap **331**
Hjelp når noe skjer **332**
Temaer til samtale **333**

KAPITTEL 13
NÅR ANDRE SVIKTER **335**
Hvorfor går det galt? **335**
En komponent brukes mange steder **336**
Ingen lang fagtradisjon **338**
Å dysse ned er bedre enn å fikse og avsløre feilene **339**
Sikkerhet nedprioriteres **339**
Kompleksitet **341**
Stillingskrig **342**
Gammel teknologi som ikke lar seg endre **342**
Andre hensyn **342**
Hva kan vi som brukere gjøre? **343**
Fremtidsutsikter **344**

KAPITTEL 14
BEDRIFTER OG ORGANISASJONER **347**
Hvorfor hører man lite om sikkerhetshendelser? **349**
Informasjonssikkerhet **350**
Ord og begreper **351**
Trusselmodellering **353**
Risikostyring **354**

Planlegge og organisere 355
Lage kategorier av sannsynligheter 355
Lage kategorier av konsekvenser 355
Definere akseptabel risiko 356
Identifisere hendelser 356
Estimere sannsynlighet og konsekvens for hver hendelse 357
Beregne risiko for hver hendelse 357
Lage prioriteringsliste 358
Utarbeide risikoreduserende tiltak 358
Utarbeide tiltaksplan 358
Gjennomføre og teste 358
Evaluere og dokumentere 359
Gevinster og utfordringer ved risikoanalyse 359
Beredskapsplaner, øvelser og rutiner 361
Sikkerhetsstandarder 363
ISO/IEC 27000-serien 364
Sikkerhetskultur, opplæring og personellsikkerhet 365
Sikkerhet overfor leverandører 368
Lovverk 368
Personopplysningsloven – GDPR 370

KAPITTEL 15
WEBTEKNOLOGI 377
Innloggede sesjoner 377
Stjele informasjonskapsler? 379
Sosial manipulering 380
Sesjonenes utløpstid 380
Sporing via informasjonskapsler 381
Nettsider med parametere 382
Manipulasjon av visning 383
Stjele data 384
Overvåkning 385
Hackede nettjenester 385
Cross-site scripting (XSS) 386
Cross-site request forgery (CSRF) 390

ORDFORKLARINGER 394
STIKKORD 411

KAPITTEL 1

DATASIKKERHET OG DATAKRIMINALITET

Datasikkerhet er ikke noe vi har eller ikke har, noe som er påskrudd eller avskrudd. Det er ikke noe vi kan tenke på en gang i uken eller få hjelp av en nabo til å oppnå. Datasikkerhet er din egen bevissthet om hva hackere og svindlere kan gjøre, samt hvordan du kan hindre at det skjer. Datasikkerhet er også bevissthet om hvordan du oppdager at noe galt alt har skjedd, og hvordan du kan minimere skadene. Datasikkerhet er både kunnskap og en måte å tenke på.

Å sikre et bygg kan innebære mange ulike typer av tiltak. I noen tilfeller er det nok med en dørlås eller et gjerde, mens det i andre tilfeller kreves alarm, vakthund eller vektere. På samme måte vil datasikkerhet ha mange ulike nivåer for å kunne forebygge og for å kunne rydde opp.

Maskiner, e-post, nettsider som besøkes og programvare er mulige veier inn til din informasjon for en hacker, og bør i størst mulig grad være satt opp for å hindre angrep. Dessverre finnes det også en annen vei inn, som i mange tilfeller er langt lettere for en hacker å bruke. Denne veien er deg. Du er faktisk selv en av de største truslene for din egen datasikkerhet.

Det hjelper ikke med all verdens gode systemer for å beskytte din informasjon dersom du gladelig gir ut den samme informasjonen ved å svare på en falsk e-post som tilsynelatende kommer fra politiet, eller når du betaler for varer i en nettbutikk som er ren svindel. Det er derfor viktig å være klar over at datasikkerhet vel så mye er kunnskap om hvordan du selv skal unngå å bli

svindlet, som å kjenne til og benytte ulike tekniske hjelpemidler, for eksempel antivirusprogrammer.

I dag er kunnskap om datasikkerhet viktigere enn noen gang. Vi omgir oss med en mengde enheter som kan angripes – mobiler, PC-er og nettverksutstyr. Vi er stort sett alltid pålogget Internett og dermed alltid tilgjengelig for hackere. Vi er blitt avhengig av datamaskiner både på jobb og privat, og de fleste er flittige brukere av tjenester som sosiale medier, netthandel og nettbank. Vi er derfor enda mer sårbare for dataanngrep og konsekvensene av dem enn tidligere.

På siden

I engelsk finnes det to begreper for sikkerhet: *safety* og *security*. Safety tilsvarer omtrent det norske ordet pålitelighet, altså at vi ønsker å unngå at systemer feiler av seg selv under normal bruk fordi de inneholder feil eller mangler.

Denne boka tar for seg sikkerhet i betydningen security, altså når noen aktivt forsøker å svindle oss.

DATAKRIMINALITET

Kriminelle og svindlere finnes overalt, har funnes til alle tider og vil heller ikke forsvinne. Innbruddstyver, bankranere, uærlige dørselgere, skattesnytere, mafia og narkotikaselgere er bare noen eksempler.

Datakriminalitet kan defineres som straffbare handlinger som begås ved utnyttelse av informasjonsteknologi. Motiver som økonomisk gevinst, hevn, status, utpressing og gjentjenester er dermed like gjeldende for datakriminalitet som for kriminalitet ellers. I prinsippet er bare verktøy som brekkjern og metoder som personlig oppmøte byttet ut med skjerm, tastatur og en Internett-forbindelse.

Datakriminalitet skiller seg likevel på visse punkter fra den mer generelle kriminaliteten. Følgende liste er en utvidelse av Bruce Schneiers[1] tre opprinnelige hovedpunkter *automation*, *action at a distance* og *technique propagation*:

- **Avstand**: En person kan nå potensielle ofre over hele verden. Internett har ingen overordnede regler på tvers av landegrenser, så angrepet kan utføres fra et land med dårlig lovgivning og rettsvesen.

1 Bruce Schneier er en kjent person innen datasikkerhet og har skrevet mange bøker om temaet.

- **Automatisering**: Maskinkraften gjør at programmer automatisk kan forsøke å svindle hundretusenvis av brukere samtidig. Selv om bare en liten andel av ofrene lar seg lure, har bakmennene likevel oppnådd et kjemperesultat. Dette er for eksempel tilfellet med svindel i form av søppelpost. Ved hjelp av automatisering er det også enklere å inkludere personlige opplysninger om offeret, noe som gjør at svindelen virker mer realistisk (såkalt *målretting* eller *targeting*).
- **Teknologisk spredning**: Etter hvert som hackere lager verktøy, spres de svært effektivt, slik at alle hackere nærmest øyeblikkelig får nye muligheter. Det tar lengre tid å få laget og distribuert sikkerhetsfikser til brukerne.
- **Lett å skjule spor**: Digital informasjon lar seg avlytte og kopiere uten fysiske spor, slik det ofte blir om noen trykker falske sedler eller driver med skimming av bankkort. Selv endring av data gir få spor, i motsetning til hva det ville gjort for eksempel ved forfalskning av et trykt vitnemål. Mange av mekanismene for deteksjon av endringer som er gjort, for eksempel logging, kan dyktige hackere manipulere til ikke å vise tegn etter angrepet.
- **Møter aldri offeret**: Det at gjerningsmennene aldri ser ofrene i øynene, slik de gjør under et bankran, gjør at de får mindre problemer med samvittigheten. For en hacker er offeret bare et «dårlig sikret system». Dette er også en av grunnene til at mange anser hacking for å være «snill» kriminalitet, selv om dette selvsagt er feil.

HVEM STÅR BAK?

Når vi snakker om «motstanderen» i forbindelse med datasikkerhet, tenker de fleste med en gang på begrepet *hacker*. Likevel har de fleste ulik oppfatning av hvem dette faktisk er. Ofte er bildet basert på filmscener og medieoppslag. For mange vil en hacker typisk være en blek og usosial person mellom 20 og 30 år. Personen har mye fritid og begrensede ressurser, men er svært dyktig innenfor IT. Linux er operativsystemet, og alt foregår i såkalt terminalmodus, gjerne med grønn skrift på svart bakgrunn – med andre ord det som i manges øyne faller inn under betegnelsen «datanerd».

Å utføre et hackerangrep består i dette bildet av å bestemme seg for et mål, skrive inn noen få kommandoer og så sitte og se på at skjermen overstrømmes av utskrifter etter hvert som maskinen stadig kommer nærmere målet. Gjerne da også med en slags fremdriftsindikator som viser hvor langt på vei prosessen er mot 100 % suksess.