Bliv sikker på nettet

PC- og onlinesikkerhed

Om truslerne fra Internettet mod sikkerheden på din pc, smartphone og tablet, og hvordan du beskytter dig mod dem.

Lars Laursen

FORLAGET STAR

Bliv sikker på nettet

PC- og onlinesikkerhed

Om truslerne fra Internettet mod sikkerheden på din pc, smartphone og tablet, og hvordan du beskytter dig mod dem.

Af Lars Laursen

FORLAGET STAR

Lars Laursen

Om forfatteren

Lars Laursen er født i Vejle i 1961 og bor nu i Bagsværd. Gennem en årrække har han arbejdet som programmør i softwareudviklingsfirmaerne UniComal A/S i Søborg og Prolog Development Center i Brøndby. Han har en uddannelse som datamatiker bag sig.

Han har undervist i IT for begyndere siden begyndelsen af år 2012, først for seniorer i Høje Gladsaxe og siden som ansat af kommunen til at undervise førtidspensionister i grundlæggende IT bl.a. i Gladsaxe Kulturhus – også kaldet Telefonfabrikken – i Søborg.

Han har fået indsigt i typiske problemer, som seniorer (og mange andre) slås med dagligt på pc'en, ved at være IT-frivillig i en datastue gennem flere år. Undervisningserfaringen har han bl.a. fået ved at designe, tilrettelægge og afholde en række grundlæggende IT-brugerkurser. Han skriver selv sit materiale til mange af kurserne. Denne bog er udsprunget af et af dem.

Bliv sikker på nettet – PC- og onlinesikkerhed, 1. udgave

Udgivet i 2018.

Research & tekst:
Lars Laursen, Wikipedia.org, politiet og en række danske og udenlandske nyheds- og sikkerhedshjemmesider.

Layout og tilrettelæggelse:
Per Tiljevang og Lars Laursen

Forside:
Colourbox.com

Udgiver:

FORLAGET STAR

Værebrovej 30, 2., 2
2880 Bagsværd
E-mail: info@forlagetstar.dk
Web: www.forlagetstar.dk
Facebook: www.facebook.com/ForlagetStar/
Blog: BlivSikkerPaaNettet.blogspot.com

Trykt bog: ISBN 978-87-996133-1-1
PDF e-bog: ISBN 978-87-996133-6-6

Tryk:

ScandinavianBook

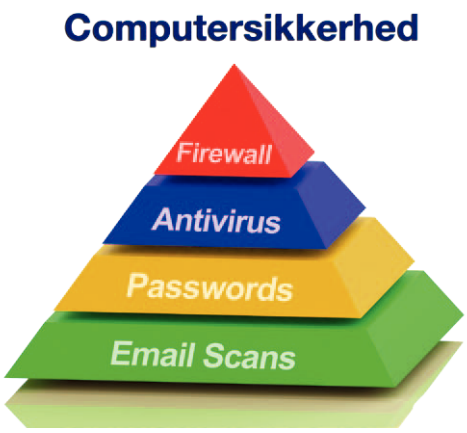
ScandinavianBook, Århus.

KAPITLER I BOGEN

Indledning

I den første periode med den personlige computer fra starten af firserne var pc-brugerne sikre. Der var ingen trusler mod brugeren eller pc'en. Det var en enklere tid end i dag. Man købte et program, installerede det og så kørte man det. Man havde et ret enkelt styresystem i **PC-DOS/MS-DOS** (***D***isk ***O***perating ***S***ystem), som dog for en dels vedkommende voldte besvær, fordi det ikke var så brugervenligt og intuitivt. Men havde man først lært at bruge pc'en og f.eks. et menuprogram, tekstbehandlingsprogrammet **WordPerfect** og eventuelt et regneark som **Lotus 123**, så kørte den, uden at man behøvede at bekymre sig mere om den.

Mens vi anvendte styresystemet PC-DOS begyndte der at dukke såkaldte computervira op (fra ca. 1984). De kunne følge med disketter med gratis programmer, som blev købt billigt. Satte man en sådan diskette i pc'en, kunne et virusprogram hæfte sig til et andet program, f.eks. WordPerfect, uden at man rigtigt lagde mærke til det. Satte man nu en ny (tom) diskette i pc'en, risikerede man, at der blev lagt en kopi af virussen ud på den. Og blev disketten flyttet til en anden pc, kunne dennes programmer blive inficeret på tilsvarende måde.



Nogle vira var forholdsvis uskadelige – de spredte sig blot eller kom med en besked på skærmen. Andre var mere ondsindede og slettede filer på pc'en – både systemfiler og brugerskabte filer. Man blev derfor nødt til at gøre noget for at sikre sig mod disse skadelige og uinviterede stykker software.

Dengang begyndte man at anvende antivirusprogrammer. Og lige siden har alle pc-brugere været nødt til at have et sådant program på deres pc'er, idet truslerne er blevet stadigt mere omfattende.

Computervira har udviklet sig siden dengang sammen med udviklingen af styresystemet Windows og især udbredelsen af det verdensomspændende datanetværk, **Internettet**.

Der er kommet nye aktører til, som sender millioner af e-mails ud uden at oplyse den rigtige afsenderadresse. Til dette kræves tusindvis af intetanende brugeres pc'er til postudsendelsen – såkaldt **spam**. Der er også kommet internetkriminelle, der forsøger at få bl.a. kreditkortoplysninger ud af de intetanende pc-brugere, som så sælges for små penge til andre kriminelle ude i verden, der benytter disse oplysninger til at fremstille betalingskort og betale for varer og ydelser på nettet for andres penge.

Computervira er blevet så stort et problem, at Windowsleverandøren Microsoft har været nødt til at redesigne sit styresystem fra bunden, så det blev mindre sårbart for vira – det skete med **Windows Vista** i 2007. Den tidligere udgave af styresytemet, **Windows XP** fra 2001 blev berygtet for ikke at yde ret god beskyttelse mod disse trusler.

Der findes nu på verdensplan en hel industri af sikkerhedsvirksomheder, som beskæftiger sig med at holde virus ude og væk fra pc'erne – både i private hjem og i virksomheder. Denne industri tager hånd om mange aspekter af sikkerhed – lige fra at stoppe virus fra at komme ind på pc'en til at sikre den mod angreb fra såkaldte ***botnet*** med måske tusindvis af kaprede pc'er, der sender et stort antal anmodninger til firmaers hjemmesideservere for at bringe dem i knæ – de

såkaldte DDoS-angreb (***D***istributed ***D***enial ***o***f ***S***ervice – overbelastningsangreb).

I denne bog bliver der beskrevet de forskellige typer af trusler, en pc-bruger kan komme ud for i dag. Vi skal se på hvad, der kan gøres for at sikre sig mod dem – både på det personlige, adfærdsmæssige plan, men også med programværktøjer som ***antivirus***, ***firewall***, ***e-mail-scanning*** og ***antispyware***. Man skal heller ikke forglemme betydningen af vanskeligt knækbare adgangskoder til sine internettjenester.

Antivirus beskytter mod computervirus.

Sådan kan denne bog læses

Bogen oplyser om rigtigt mange emner relateret til pc- og internetsikkerhed. Der er noget om:

- Hvad forskellige typer malware er.
- Hvad de foretager sig.
- Hvem der skaber dem, og hvad de får ud af dem.
- Valutaen Bitcoins medvirken ved IT-kriminalitet.
- Der er en gennemgang af hvilke antivirusprogrammer, der er bedst – både under Windows, Mac OS, Linux og Android.
- Hvad en firewall er.
- Skal man også have et antispywareprogram?
- Der er fyldige beskrivelser af farerne ved e-mailbedrageri.
- Hvordan man spotter e-mailbedrageri.
- Hvad phishing er, og hvordan man sikrer sig mod det.
- Social engineering: sociale narreteknikker.
- Hvad man kan gøre mod identitetstyveri.
- Er cookies farlige?
- Farer ved fildelingsprogrammer.
- Hvor sikkert er NemID egentligt?
- Hvordan man kan blive udsat for farer på sociale medier som Facebook.
- Falske nyheder på sociale medier.
- Værktøjer til at redde en malwareinficeret pc.
- Sikkerhedskopiering af dine dyrebare filer.
- Onlinebeskyttelse af børn på Internettet.
- Hvordan du holder din pc opdateret.
- Farer for malware på smartphones og tablets.
- Gode adgangskoder.
- IT-virksomheders overvågning af dig på nettet.
- Nationalstaters brug af malware over for borgere og andre nationer.
- Digitalt selvforsvar.
- Falske netbutikker og falske domænenavne.
- Receptpligtig medicin købt online.
- Nogle af de farer, som virksomheder og andre organisationer kan komme ud for.
- Der er mange eksempler fra det virkelige liv, som de er blevet beskrevet i artikler i medierne.

Det kan virke som overvældende mange emner, og forfatteren forventer da heller ikke, at alt læses af alle. Bogen kan benyttes som et opslagsværk med udgangspunkt i enten den fyldige indholdsfortegnelse eller **stikordsregistret** bagerst i bogen fra side 461.

Hvem henvender bogen sig til?

Bogen kommer ind på mange emner. Nogle er beskrevet i et let tilgængeligt sprog, mens andre bedst forstås af mennesker med et vist kendskab til styresystemer og deres virkemåde – de kan virke en smule tekniske. Derfor er det også en forholdsvis bred skare, der kan have gavn af bogen. Den kan med fordel læses af:

- Sikkerhedsbekymrede borgere.
- Mennesker, der gerne vil vide, hvordan de sikrer sig mod at blive ofre for hackere og it-kriminelle.
- De, der gerne vil vide, hvilket antivirusprogram de med fordel kan anvende.
- De, der er usikre på om NemID og netbank er sikre at bruge.
- De, der har hørt om nogle af de ord og begreber, som deres bekendte taler om vedrørende IT-sikkerhed, og som gerne vil forstå dem bedre.
- IT-undervisere.
- Studerende på gymnasier og videregående uddannelser.
- De, der vil lære nogle tips og tricks til at redde computere fra malware.
- De, der vil sikre deres data ved at sikkerhedskopiere deres dokumenter, billeder, musik og videoer.
- Forældre, der vil vide, hvordan de kan sikre deres børn på pc'en, smartphonen, tabletten og internettet og eventuelt begrænse deres brug af den.
- De, der vil vide, hvordan man holder sin pc, styresystem og programmer sikkerhedsopdaterede.
- Ansatte i virksomheder. Der er emner i bogen, som fortrinsvis ansatte i virksomheder og organisationer kan blive udsat for. Men der er kun få specielle sikkerhedsløsninger beskrevet, som henvender sig specifikt til systemadministratorer.

Du kan finde de 16 vigtigste sikkerhedsråd i denne bog opsummeret i **Kapitel 36** på siderne 449-457.

Der kan være farer på computeren og på Internettet. Grafik: Colourbox.

Kapitel 1 - Hvad er computervirus for noget?

Dette store kapitel beskriver vira af forskellige slags, vigtigheden af at beskytte sig mod disse former for skadelige programmer, der under ét kaldes malware (malicious software – ondsindet eller skadelig software), og som det er nyttigt at kende til. Vi kommer ind på en række begreber, som egentlig er "eksotiske" computerprogrammer:

- Virus – programmer, der integrerer sig selv i andre programfiler og kan "smitte" andre computere.
- Orme – uønskede programmer, der spredes via netværk.
- Trojanske heste – programmer, der kommer med en skadelig og uønsket "ladning".
- Ransomware – programmer, der opkræver betaling af en løsesum for at slippe en enhed fri.
- "Zombier" i botnet til masseudsendelse af spam og udførelse af overbelastningsangreb.
- Rootkits – malware, der skjuler sig i styresystemet.
- Spyware – opsnapning af fortrolige oplysninger fra din enhed.
- Adware – visning af (for mange) reklamer i programmer og på hjemmesider.

På de følgende sider er beskrevet nøjere, hvad de forskellige typer malware kan og gør, og hvad der adskiller dem fra hinanden.

Malware-spredning kan ske i forbundne datanetværk over hele kloden. Grafik: Colourbox.

1.1 Virus

En computervirus er et malwareprogram, som når det eksekveres, kopierer sig selv ved at indsætte kopier af sig selv (muligvist modificerede) i andre computerprogrammer, datafiler eller i boot-sektoren på harddisken (hvorfra styresystemet hentes). Når denne selvkopiering lykkes, siges de påvirkede områder at være "inficerede". Vira udfører ofte en slags skadelig aktivitet på de inficerede værter, såsom at stjæle harddiskplads eller processortid, få adgang til private oplysninger, beskadige data, vise politiske eller humoristiske budskaber på brugerens skærm, spamme hans/hendes kontaktpersoner eller at logge (notere) deres indtastninger via tastaturet. Men ikke alle vira bærer en destruktiv ladning eller forsøger at skjule sig – viras særlige karakteristika er, at de er selvkopierende computerprogrammer, som installerer sig uden brugerens samtykke.

Virusforfattere benytter det, der på engelsk kaldes social engineering (sociale narreteknikker, se side 198) og udnytter detaljeret viden om sikkerhedssårbarheder for at opnå adgang til deres værters (uforvarende pc-brugeres) computerressourcer. Det store flertal af vira er målrettet systemer, der kører styresystemet Microsoft Windows, og anvender forskelligartede mekanismer til at inficere nye værter og benytter ofte komplekse antidetekterings/skjulnings-strategier for at undgå antivirusprogrammer. Motivet til at skabe vira kan være at opnå profit; ønsket om at sende et politisk budskab; personlig morskab; at demonstrere, at en sårbarhed findes i software; til sabotage og overbelastning af computersystemer; eller simpelthen fordi de ønsker at udforske kunstigt liv og evolutionære algoritmer.

Computervira koster for tiden milliarder af kroner i økonomiske skader hvert år, fordi systemer bringes til at fejle, spilde computerressourcer, beskadige data, forøge vedligeholdelsesudgifter, medarbejderes mistede produktivitet, osv. Som modsvar på dette er der udviklet gratis, opensource antivirusværktøjer, og en mange milliarder-kroners industri for antivirussoftwareleverandører er opstået, som sælger virusbeskyttelse til brugere af forskellige styresystemer, af hvilke Windows ofte er det største offer, delvis pga. af sin overordentlige store popu-

laritet. Intet eksisterende antivirusprogram kan fange alle computervira (især ikke nye). Computersikkerhedsforskere søger aktivt efter nye måder at gøre antivirusløsningerne mere effektive til at detektere nye vira, før de er blevet vidt udbredte.

1.2 Orme

Ordet "orm" blev første gang brugt i computersammenhæng i den britiske forfatter **John Brunners** roman fra 1975, **The Shockwave Rider**. I denne roman designer og udsender Nichlas Haflinger en *"dataindsamlingsorm"* som hævn mod de magtfulde mænd, der driver et nationalt elektronisk informationsnetværk, som bevirker masseensretning blandt befolkningen. Citat fra bogen: *"I har den største orm nogensinde løs i nettet, og den saboterer automatisk ethvert forsøg på at overvåge den… Der har aldrig været en orm med så barsk et hoved eller så lang en hale!"*

Den 2. november 1988 slap **Robert Tappan Morris**, en datalogistuderende ved Cornell Universitetet i USA, det, der blev kendt som **Morris**-ormen, løs og forstyrrede derved et stort antal computere, der dengang var på Internettet – der blev gættet på 10 % af alle tilsluttede computere. Under Morris' appelsag vurderede **U.S. Appelretten** omkostningerne til at fjerne virussen fra hver computerinstallation til at ligge i omegnen af 200-530.000 dollar. Morris selv blev den første person, der blev retsforfulgt og dømt under loven **1986 Computer Fraud and Abuse Act** (Computerbedrageri- og -misbrugsloven af 1986).

En tegners opfattelse af en "computerorm", der spredes via netværk.

1.2.1 Hvad er en computerorm?

En computerorm er et enkelt malware-computerprogram, som kopierer sig selv for at spredes til andre computere. Ofte benytter det et datanetværk til at spredes og er afhængig af sårbarheder i sikkerheden på målcomputeren for at få adgang til den. I modsætning til en computervirus behøver den ikke at hæfte sig til et eksisterende program. Orme forårsager næsten altid nogen grad af skade på netværket, også selvom de kun forbruger båndbredde, hvorimod computervira næsten altid beskadiger eller modificerer filer på en målcomputer.

Mange orme er blevet skabt og designet til kun at spredes og ikke gøre forsøg på at ændre systemet, de passerer igennem. Men som Morris-ormen og **Mydoom** viste, kan selv disse "ladningsfrie" orme forårsage større forstyrrelser ved at øge netværkstrafikken og andre utilsigtede virkninger. En "ladning" er programkode i ormen, der er designet til at gøre mere end at sprede ormen – den kan slette filer på værtssystemet (f.eks. **ExploreZip**-ormen), kryptere filer i et såkaldt *kryptoviralt pengeafpresningsangreb* (ransomware) eller sende dokumenter via e-mail. En meget almindelig ladning for orme er at installere en såkaldt **bagdør** på den inficerede computer for at gøre den til en *zombie*-computer under kontrol af ormens forfatter. Netværk af sådanne maskiner kaldes ofte for *botnet* og benyttes meget ofte af spam-udsendere til at sende uopfordrede e-mails eller til at skjule deres hjemmesides adresse. Spammere menes derfor at være en kilde til finansieringen af skabelsen af sådanne orme, og der er ormeforfattere, der er blevet fanget for at sælge lister over IP-adresser (en slags "telefonnumre", der identificerer enheder på netværket) på inficerede maskiner. Andre prøver at afpresse firmaer ved at true med DDoS-angreb (***D***istributed ***D***enial ***o***f ***S***ervice – distribuerede overbelastningsangreb).

Pc-brugere kan minimere sådanne trusler fra orme ved at holde deres computeres styresystemer og anden software opdaterede og undgå at åbne uopfordret tilsendt e-mail og e-mail fra ukendte kilder og have firewall- og antivirussoftware installeret.

Kapitel 21 - Sociale medier

Sociale medier (også forkortet **SoMe**) er kort fortalt en række steder på internettet, hvor indholdet bliver genereret ved brugernes egen interaktion med resten af internettet. Hele idéen er, at andre skal kunne se og reagere på det, der lægges ud. Det gælder f.eks. *Skype*, *Facebook*, *Flickr*, *Twitter*, *Digg*, *YouTube*, *Stumbleupon*, *LinkedIn*, *Google+*, *MySpace*, *Snapchat*, *InstaGram*, *WhatsApp* og *Pinterest*. Mange hjemmesider tillader at dele deres indhold via en række sociale medier.

På mange sociale medier kan man benytte såkaldte *hashtags* (f.eks. **#sød**, **#fødselsdag**, **#MeToo**, **#dkpol**) i indlæg, som der kan søges efter og vises. Sociale medier findes både på pc'en, smartphonen og tabletpc'en.

Nogle af tjenesterne er især beregnet til brug på smartphones. Herunder introduceres nogle af de mest populære sociale medier i Danmark. Der er opgjort antallet af månedlige, aktive brugere i september 2017.

Facebook er det største og nok det mest udviklede af de sociale medier. Der 2,06 milliarder brugere fra hele verden og over 3,7 millioner i Danmark. Her kan man skrive opslag; kommentere andres opslag; afgive synes-om-tilkendelser; dele andres opslag og artikler fra Internettet; tage kontakt til sine venner, familie, nuværende og tidligere kolleger, skole- og studiekammerater. Der er en chat-tjeneste kaldet **Messenger**, så man kan kommunikere lige nu med en anden person via tekst, lyd- eller videosamtale; man kan lægge billeder og videoer ud; spille spil; invitere andre til en begivenhed og til at spille spil. Anvendes af alle aldre.

Instagram er en fotodelingstjeneste med ca. 700 millioner brugere, der tillader dem at dele billeder og videoer enten offentligt eller privat til forud valgte følgere. Brugerne kan anvende forskellige fotofiltre til at ændre fotos, der deles, og tilføje geografiske data. Anvendes især af de unge.

Snapchat er en chatfacilitet til smartphones og tablets med ca. 255 millioner brugere, som gør det muligt at tage fotos, videoer og tilføje tekst og tegninger og derefter sende dem til venner. Der er både tekst- og videobaseret chat. Beskederne er synlige et vist antal sekunder og destruerer derefter sig selv. Disse beskeder kaldes *snaps*. Anvendes især af de unge.

YouTube er en gratis videodelingstjeneste med 1,5 milliarder brugere, som står for en stor del af Internettets samlede datatrafik. Her kan ses musikvideoer, spilvideoer, filmtrailere, instruktions- og undervisningsvideoer, virale reklamer, klip fra alverdens tv-udsendelser og film, videoer om nuttede dyr. Enhver kan selv gratis uploade videoer.

WhatsApp er en app til smartphones med 1,3 milliarder brugere til at sende SMS-lignende beskeder og foretage gruppechat, sende dokumenter og geografisk opholdssted, billed-, lyd- og videobeskeder mellem dem.

Twitter er en nyhedstjeneste med ca. 328 millioner brugere, som er blevet kaldt Internettets SMS-tjeneste. Her kan sendes beskeder (kaldet *tweets*) op til 280 tegns længde, men dog med både links, billeder og videoer. Den amerikanske præsident Donald Trump er blevet berømt/berygtet for at benytte dette medie i sit embede.

LinkedIn er et erhvervs- og karriereorienteret socialt medie med 106 millioner månedlige brugere. Her kan man fortælle om sin uddannelse og professionelle kvalifikationer; tilbyde sine tjenester; skabe forbindelser til andre og få anbefalinger; og søge job bl.a. via sine forbindelser.

Skype er med ca. 300 millioner brugere en chat-, telefoni- og videosamtaletjeneste, der i mange tilfælde er gratis at benytte. Mange danskere benytter den til at føre gratis videosamtaler med familie og venner i ind- og udland. Man kan føre samtaler mellem to

eller flere brugere i videokonferencer og dele en andens skærmbillede live.

På de efterfølgende sider ses på, hvilke farer man som bruger af tjenesterne kan blive udsat for.

21.1 Farer på sociale medier

[30] I og med at verden i stigende grad bliver forbundet via Internettet og andre teknologier, er det som om, der ikke er noget sikkert sted for de cyberkriminelles sigtekorn. I de senere år har pc-brugere og virksomheder set hackere bryde ind i alle former for mål, deriblandt den enkeltes pc, mobile enheder, salgsterminaler (POS) og virksomhedsnetværk i almindelighed. For nyligt synes der dog at være en stigende tendens til, at sorthatte (engelsk: **black hats** – hackere med skadelige hensigter) har udvidet rækkevidden af deres angreb til at omfatte ikke kun traditionelle angrebsmidler, men også sociale medier.

Når man ser det fra en hackers synspunkt, er det let at forstå, hvorfor sociale netværk bliver det næste fornuftige mål. Som regel går cyberkriminelle derhen, hvor de har adgang til den største gruppe af ofre. Med sociale medie-hjemmesider som

Facebook (2,06 mia. månedlige brugere),
WhatsApp (1,3 mia.),
Instagram (700 mio.),
LinkedIn (106 mio.),
Twitter (328 mio.)

og andre, der til stadighed øger deres brugerantal, er det ikke vanskeligt at forstille sig, at hackere benytter disse platforme til deres skadelige aktiviteters fordel.

Men helt nøjagtigt hvordan udnytter cyberkriminelle sociale medier til deres angreb? Lad os undersøge denne stigende tendens, såvel som hvordan brugerne kan beskytte sig.

21.2 Sociale Medier: Port til vandhulsangreb

Angreb via sociale medier minder om løver, der angriber ved et vandhul, hvor dyrene kommer for at drikke – et vandhuls-angreb.

I de senere år har angribere benyttet hjemmesider, der besøges af et eller flere medlemmer af målgruppen, for at inficere disse individer og deres apparater med malware. Hvis f.eks. en sorthat forsøger at gå efter en bestemt virksomhed og bemærker, ved at iagttage netværksaktiviteter, at et antal ansatte ofte benytter en oplysende hjemmeside relateret til den industri, kan hackeren placere malware på webstedet – eller skabe en legitimt udseende falsk webside – for at lokke medarbejdere til det inficerede netværk.

Kaspersky Lab-direktøren for global B2B-markedsføring, Mark Bermingham, fortalte i 2015 magasinet **PCWorld**, at der ville være en stigning i såkaldte *vandhulsangreb* ved brug af sociale medier.

Disse vandhulsangreb, som sikkerhedsforskere kalder dem, minder om angreb, hvor en løve lægger sig på lur ved et vandingshul og venter på, at potentielle ofre dukker op for at slukke deres tørst.

Vandhulsangreb er oftest målrettede: Angriberne udvælger websteder, som de udvalgte ofre sandsynligvis vil besøge. De aktuelle angreb ser ud til at være rettet mod personer med interesse i menneskerettigheder og ytringsfrihed. Således tilhører et vandhul, der er blevet forgiftet, organisationen **Journalister uden grænser**.

Tidligere angreb gik ud over politiske partier i Hong Kong og Taiwan samt menneskerettighedsorganisationer tilknyttet Tibet.

Angrebene udnytter de seneste sikkerhedshuller i Java og Internet Explorer. Begge huller er lukket, men hvis man ikke har installeret opdateringerne, risikerer man at få inficeret sin pc, hvis man besøger et inficeret vandingshul.

[30] Kilde: blog.trendmicro.com/social-media-malware-on-the-rise/

Ofrenes pc'er inficeres med fjernstyringssoftware, der giver bagmændene adgang til data på dem.

"Sikkerhedsforanstaltningerne kan ikke få bugt med stjålne log-ind-oplysninger og klik på tvivlsomme links," påpeger Mark Bermingham.

Desuden vurderede sikkerhedsforskere ved **Proof-point**, at der i 2015 ville være en stigning på 400 % i indhold af skadelig art på sociale medier.

21.3 Angreb med trojansk hest på Facebook

Tilstedeværelsen af et angreb fra en trojansk hest, der angriber brugere via Facebook, synes at støtte eksperters forudsigelser om en stigende mængde angreb på sociale medier. I februar 2015 opdagede sikkerhedsforskere en pornografibaseret trojansk hest, der inficerede brugere på det populære sociale medie, rapporterede bladet **IT Pro**.

Angrebet lokker brugere til at blive inficeret ved at love vovet indhold via et link. Når ofrene én gang har klikket på linket, kan de se en forfilm af det pornografiske indhold, men videoen stopper halvvejs igennem og beder brugerne om at downloade en opdateret udgave af tilføjelsesprogrammet **Adobe Flash Player** for at fortsætte. Dette program er imidlertid et skadeligt bedrag, der inficerer ofrene og sætter hackere i stand til at kontrollere tastatur og musebevægelser. Når malwaren én gang er installeret, sender det skadelige links til offerets Facebook-væg og tagger brugerens venner, hvorved alle andre, der klikker på dem, inficeres. Malwaren kan også sende private beskeder til offerets venner og derved sprede infektionen yderligere.

I februar 2015 vurderedes angrebet at have inficeret 110.000 Facebook-brugeres pc'er over en todages periode. Efter opdagelsen udsendte en Facebook-talsperson en meddelelse, der sagde, at webstedet benyttede flere automatiserede teknologier til at lokalisere og mildne skaderne af sådanne skadelige links.

"I dette tilfælde er vi klar over disse forskellige former for malware, som typisk skyldes webbrowser-tilføjelsesprogrammer og udbredes ved brug af links på hjemmesider for sociale medier," gjorde Facebook-talspersonen opmærksom på. *"Vi blokerer links til denne svindel og tilbyder muligheder for at blive renset og bruger andre midler til at sikre, at folk fortsætter med at have en tryg oplevelse på Facebook."*

21.4 Oprørere lokker fjender med honningkrukke-malware-hjemmesider

Facebook-trojaneren er ikke den første gang risikabelt indhold blev benyttet til at lokke ofre til malware-infektion. Teknologihjemmesiden **Ars Technica** rapporterede, at denne teknik er blevet udnyttet mod syriske oprørere så sent som februar 2015 til at stjæle følsomme oplysninger fra oprørssoldater.

I angrebene udnyttede hackere social medie-svindel og Skype-konti, der syntes at tilhøre kvindelige støtter til syriske oprørsgrupper. Disse *"kvinder"* benyttes til at narre oprørssoldater til at downloade malware, som får fat på en række personlige oplysninger fra pc'er og Android-enheder.

"Angriberen bad om et foto af målet og sendte så et billede af sig selv – et billede, som offeret havde for travlt med at sidde og drømme om til at blive klar over, at det kom sammen med malware," gør Ars Technica-bidragsyderen Sean Gallagher opmærksom på.

Sikkerhedsforskere opdagede at ved at anvende denne fremgangsmåde kunne hackere få adgang til personlige oplysninger om deres mål, såvel som kampplaner og andre militære efterretninger, der kom fra de syriske regeringstropper.

Inden for efterretningstjenesterne benyttes tilbud om sex som middel til bl.a. at lokke oplysninger ud af udvalgte personer. Det kaldes en honningkrukkefælde. Modelfoto: Colourbox.

21.5 Beskyttelse handler om årvågenhed og rettidig omhu

Sociale medie-angreb kan være meget sværere at beskytte sig mod, idet de ofte i høj grad er forklædte. Af denne grund må brugerne være meget omhyggelige og være sikre på, at de forstår risiciene.

"Større årvågenhed og agtpågivenhed er det bedste forsvar," bemærkede PCWorld-bidragsyder Tony Bradley.

At holde sig orienteret om de seneste sociale mediebaserede angreb og være på vagt over for mistænkelige links, vedhæftede filer til e-mails og indlæg kan hjælpe brugere til at undgå at blive ofre for denne slags infektioner. En række antivirusprogrammer har linkbeskyttelse, som også beskytter sociale medier som Facebook.

21.6 Falske nyheder på (sociale) medier på Internettet

Stemnings- og opinionsstyring via sociale medier er i stigende grad en risiko for nyhedsstrømmen og meningsdannelsen i demokratiske lande. En række aktører og fremmede nationers regeringer forsøger at påvirke den folkelige opinion via falske plantede nyheder i både trykte medier og (sociale) medier på nettet.

Det er ikke nyt med misinformationskampagner styret af fremmede nationer. Vi oplevede det under den kolde krig, hvor Sovjetunionen og østlande forsøgte at påvirke opinionen i Danmark via påvirkningsagenter. Nu oplever vi en genkomst af fænomenet via bl.a. sociale medier som Facebook og Twitter.

I 2016 blev præsidentkandidaternes kampagner i USA på begge sider ramt af falske nyheder, som bl.a. havde til formål at påvirke meningsdannelsen og dermed præsidentvalget.

Falske nyheder er en fare for åbne samfund som de vestlige demokratier, hvor vi har været vant til forholdsvis pålidelige nyhedsunderretninger, som er tjekkede og faktabaserede.

De handler om at underminere en modstanders opbakning i samfundet, således at denne mister støtte. Det så vi i 2016 under den amerikanske præsidentvalgskampagne. Man har kaldt fænomenet, hvor sociale mediers såkaldte nyheder også bliver nyheder i selv seriøse medier, for det *postfaktuelle samfund* – i modsætning til faktuelle samfund, hvor man i ret høj grad kan stole på de nyheder, der bliver udsendt. Vi ser nu i flere lande en tendens til, at der dukker faktatjekkende instanser op – medier, som undersøger sandheden og fakta bag en række nyheder og udtalelser fra offentlige personer. Vi kender det selv fra Danmarks Radios DR2-udsendelsesrække **Detektor**. Under den amerikanske valgkamp opstod grupper, der faktatjekkede både kampagnernes falske nyheder og præsidentkandidaternes udtalelser.

Magasinet TIME's forside fra april 2017 om falske nyheder og benægtelse af fakta: Er sandheden død?

Man kan sige, at denne slags nyheder gør det mere usikkert at færdes på Internettet og sociale medier. Læseren risikerer at blive fanget af følelser for forhold, som ikke har noget på sig. Det kan være vanskeligt at ændre holdninger pga. sådanne følelser, når nyheden bliver falsificeret af andre medier. Derfor kan falske nyheder være en bombe under f.eks. valgkampagner og kontroversielle forhold i samfund rundt om i verdens lande.

21.8 Artikel: "Troldefabrik" som hemmeligt våben

[32] ***Rusland: En hær af russiske internettrolde planter misinformation fra Kreml i debatterne på internettet. Ruslands hybridkrig i cyberspace har sendt Vesten i tænkeboksen.***

MOSKVA/BRUXELLES – Da oppositionspolitikeren Boris Nemtsov for en måned siden blev myrdet en sen aften på en bro lige foran Kreml, var det ikke kun pressens folk, der kom på overarbejde.

På Savusjkin Gaden i en forstad til Ruslands næststørste by, Skt. Petersborg, fik hundreder af såkaldte *internettrolde* – skribenter, som under dække af falske profiler og aliasser blander sig i debatterne på nettet – strenge ordrer om at komme til tasterne og rubbe neglene:

"Vi skal skabe en opfattelse af, at ukrainske aktører kan være indblandet i den russiske oppositionspolitikers død," fremgik det af en instruks til troldene den 28. februar, morgenen efter mordet.

"Dette er en åbenbar provokation beregnet på at skabe et udbrud af utilfredshed blandt oppositionens folk," lød en anden del af det budskab, som de ansatte skulle sprede i debatfora på netmedier og på Facebook, Twitter og russiske sociale medier.

400 ansatte

Instruksen findes blandt en stribe dokumenter, som avisen **Moj Raion** i Skt. Petersborg for nyligt har offentliggjort som del af en stor undersøgelse af virksomheden på Savusjkin Gaden.

Centret, der ifølge avisen har 400 ansatte, drives af selskabet **Internet Research Agency** og finansieres via strukturer med forbindelse til Kreml.

Det er en særdeles velorganiseret operation, hvor de vellønnede skribenter i 12-timers skift hver forventes at sende over 100 korte kommentarer ud.

Og troldene får virkelig noget fra hånden.

"Under teksterne om drabet på Nemtsov er der hundreder og nogle steder tusinder af kommentarer: Mordet er en provokation. Kreml er ikke indblandet. Det er oppositionen, som dræbte sin egen mand," fortæller Aleksej, en anonym eks-trold til avisen.

Tegneren Woody Hearns opfattelse af en almindelig enlig "trold", som påvirker tonen i negativ retning i et forum. Man plejer at sige: "Fodr ikke trolden!" – for så risikerer læseren selv at blive som trolden. På troldefabrikker forsøger troldene at påvirke meningsdannelsen f.eks. ved et valg i et andet land, ved politiske beslutninger eller opfattelsen af en begivenhed – de er kort sagt propagandister og spreder misinformation.

Sofistikeret strategi

Troldene i Skt. Petersborg er en væsentlig del af den skjulte, men sofistikerede strategi, som Kremls spindoktorer har udtænkt.

Informationskrigens artilleri i form af nyhedsbureauer eller tv-stationer som RT, der sender russisk propaganda målrettet et vestligt publikum, er ikke svær at få øje på og dermed mulig at modgå med argumenter.

Men dens fodfolk, udrustet med hver sit lille våben, kan operere mere eller mindre uset og under radaren. Alligevel kan deres samlede effekt være stor.

De organisationer, som kommanderer rundt med en hærskare af trolde, er også leve-

[32] Kilde: www.jp.dk/protected/premium/international/ECE7613910/Troldefabrik-som-hemmeligt-v%C3%A5ben
Af Heidi Plougsgaard og Poul Funder Larsen, Jyllands-Postens korrespondenter, 10. april 2015.

21.16 Hvordan påvirker sociale medier os så?

Medstifteren af den hedengangne musikdelingstjeneste **Napster** og den første Facebook-præsident, **Sean Parker**, har tænkt en del over den rolle, han har spillet i at bringe sociale medier til verden. Han sagde ved en begivenhed arrangeret af mediefirmaet Axios i 2017, at han anser sig selv for at være en *"samvittighedsfuld modstander"* af sociale medier.

"Da Facebook var ved at komme op i omdrejninger, oplevede jeg mennesker, der kom til mig og sagde, 'Jeg er ikke på de sociale medier.' Og jeg sagde, 'Okay, men det kommer du.' Og de ville sige, 'Nej, nej, nej. Jeg værdsætter samspil med mine relationer i det virkelige liv. Jeg værdsætter nære forhold.' Og jeg sagde, 'Vi vil få dig på i sidste ende,'" sagde Parker. Og han tilføjede, at de første mål for firmaer som Facebook var at sikre, at brugerne tilbragte så meget tid som muligt på deres websteder. Samspil såsom **synes-om-**tilkendegivelser og kommentarer tjente til at få folk dybere ind på webstedet, om hvilket Parker sagde, *"Det er en kontant social feedback-løkke … lige sådan en ting, som en hacker som jeg ville finde på, fordi man udnytter en sårbarhed i den menneskelige psykologi."*

Sean Parker sagde, at stifteren af Facebook, Mark Zuckerberg, og andre forstod dette, ***"Og vi gjorde det alligevel."*** Nu undrer han sig over, om den udbredte brug af sociale medier som Facebook har ændret vores produktivitet, ligesom de har ændret vores sociale relationer. *"Kun Gud ved, hvad det gør ved vores børns hjerner,"* sagde han.

Facebooks tidligere vicepræsident for brugervækst, Chamath Palihapitiya, har sagt, at han føler *"overvældende skyld"* over det selskab, han har været med til at skabe. *"Jeg mener, vi har skabt redskaber, der er ved at ødelægge grundlaget for, hvordan samfundet virker,"* sagde Palihapitiya til en forsamling på **Standford Graduate School of Business**, som han anbefalede at tage *"en hård pause"*

Her er en satireartikel fra RokokoPosten i Jyllands-Posten om, hvor svært det kan være at gøre dét på smartphonen, man gerne vil, uden at blive "suget" ind af sociale medie-apps.

Smartphonebruger ville se, hvad klokken var – og så, hvad klokken var

Onsdag lykkedes det en kvinde fra Gladsaxe at se, hvad klokken var, på sin smartphone helt uden at tjekke Facebook, mail eller andre apps.
"Det var en helt fantastisk følelse af at tage kontrollen over mit liv tilbage."
Sådan beskriver den 33-årige Sophie Bennetsen fra Gladsaxe sin oplevelse, da hun onsdag eftermiddag tog sin smartphone frem for at se, hvad klokken var. For i stedet for at lade sig distrahere af push-beskeder fra Facebook, Snapchat, mail og hendes mange andre apps, kiggede hun blot på uret.
"Jeg huskede endda, hvad klokken var, så jeg ikke skulle have telefonen frem igen for at kigge," siger hun, tydeligt overrasket over sin egen bedrift.

Nyhederne ikke noget savn
Sophie Bennetsen fortæller, at hun ikke engang savnede nyhederne fra Facebook, som hun ellers plejer at falde over som det første, når hun vil se, hvad klokken er. Hun så ganske vist, at der var et par notifikationer, både fra Facebook, Twitter, Instagram og Snapchat, men af grunde, som hun ikke kan forklare, ignorerede hun dem.
"Jeg så bare på uret, og så lagde jeg telefonen væk igen," siger hun.
Hvordan det gik til, at hun ikke, som man ellers altid gør, brugte flere minutter på at tjekke sine apps for derefter at opdage, at hun havde glemt at se, hvad klokken var, ved hun ikke:
"Jeg spørger stadig mig selv, hvad der skete, men jeg kan slet ikke forklare det."

"Som om det kunne ske"
Efter hændelsen lavede Sophie Bennetsen et Facebook-opslag, hvor hun fortalte om sin mærkværdige oplevelse. Allerede samme aften var opslaget blevet delt flere end 1.000 gange, og mange har reageret med overraskelse, respekt og skepsis.
Facebook-brugeren Kasper Jespersen skriver, at han slet ikke forstår, hvordan det kunne lade sig gøre.
"Jeg fatter ikke, at du kunne. Jeg glemmer altid at se på klokken," skriver han.
Flere giver Kasper Jespersen ret, mens enkelte mener, at Sophie Bennetsen overdriver eller ligefrem lyver.
"Som om det kunne ske," skriver 16-årige Jasmin Møller Andersen.
Sophie Bennetsen selv understreger, at det bestemt ikke er løgn, men at hun ikke lavede sit opslag for at prale.
"Jeg forventer på ingen måde, at det sker igen. Det var bare så underligt, at jeg blev nødt til at dele oplevelsen med nogen," slutter hun.

Når en pc skal reddes fra malware...

Kapitel 22 - Værktøjer til at redde en pc, der er inficeret med malware

Hvis din pc er blevet inficeret med malware, hvad kan du så gøre? Der er en hel række tiltag, der kan gøres afhængig af, hvor "slem" malwaren er. Med "slem" menes, i hvor høj grad malwaren modsætter sig fjernelse.

Det første skridt er at køre en fuld scanning af pc'en med det installerede antivirusprogram. Det kan tage op til et par timer at gennemføre. Antivirusprogrammet tilbyder at fjerne malwaren (eller i det mindste at sætte den i "karantæne"), og dermed er pc'en "kureret" eller reddet, og du kan som bruger ånde lettet op – problemet er klaret.

Nogle gange er malwaren så slem, at den kan afholde dig fra at scanne pc'en med antivirusprogrammet; den kan gøre det umuligt at benytte en webbrowser til at søge efter hjælp til fjernelse af malwaren på Internettet; den kan endog fjerne muligheden for at starte programmer op eller installere programmer, der kunne afhjælpe situationen.

I denne situation opdager man, at det ikke kun er prisen på antivirussoftwaren, der betyder noget. Den service, som leverandøren af antivirusprogrammet kan levere, betyder også noget. Nogle antivirusleverandører tilbyder fjernsupport via Internettet, hvor en medarbejder hos firmaet kan se din skærm og styre din mus og tastatur, således at han/hun kan foretage ændringer på pc'en. Prisen er måske lidt højere for antiviruspakken med denne service, men det kan vise sig at være en billig måde at redde pc'en på.

Hvis man selv vil gøre noget for at redde pc'en, er der en række ting, der er nyttige at være bekendt med. Der er nogle ting, du kan foretage dig nu og nogle ting, som du kan vende tilbage til denne bog og læse om, hvis du skulle komme ud for malware.

Der er bl.a. følgende muligheder at overveje:

- At **oprette en genoprettelsesdisk/-USB-nøgle**, så du kan starte computeren fra et andet medie end harddisken, hvis computeren er ramt af virus. Med denne metode kan du fjerne malware fra systemharddisken, uden at den er aktiv.
- Hvis pc'en ikke kan starte, kan du foretage **reparation eller genoprettelse af styresystemet** ved at trykke på en særlig tast under opstart. Her kan styresystemet enten repareres, eller det kan genetableres på harddisken.

Kapitel 23 - Sikkerhedskopiering – sikkerhed for dine filer

Computere er noget af det, en indbrudstyv foretrækker – det er letomsættelige tyvekoster.

Nogle siger: "**Rigtige mænd tager ikke backup – de græder!**"

Underforstået, at først for sent finder de ud af, at det er en rigtig god idé at foretage backup – på dansk sikkerhedskopiering. Der er eksempler på virksomheder, som ikke har taget backup, og som, da de mistede deres data i form af kundedatabaser og anden vigtig information for deres forretning, ikke har fundet sig i stand til at fortsætte deres virksomhed – de måtte dreje nøglen om pga. manglende data.

Der er også eksempler på, at virksomheden HAR taget backup, men over på tape, som senere, da de havde mistet data, viste sig at være dårlig, så en genetablering af data ikke kunne lade sig gøre. En virksomheds eksistens kan altså afhænge af backup.

Så slemt går det nok ikke for private, men det kan være et stort følelsesmæssigt slag at miste sine billeder og digitale minder – det kan være bryllupsbilleder, billeder af børn og børnebørn og fra ferier og fester. Mange finder nok desværre først ud af vigtigheden af backup netop, når de har mistet en større mængde data – f.eks. ved at harddisken eller pc'en er holdt op med at fungere. Eller der kan være sket vandskade, brand eller tyveri af pc'en i hjemmet eller ude. Det er brandærgerligt at miste sine minder i form af billeder, videoklip, redigerede film, adressebog og dokumenter. En pc inficeret med ransomware får ofte alle nævnte filtyper krypteret og kræver derefter løsepenge for at dekryptere dem! Har du en nylig backup af filerne og licensnøgler, kan du vende tilbage til pc'ens fabrikstilstand og geninstallere alle programmer og filer – uden at skulle betale løsepenge.

Backup er mange ting nu om dage: det kan være backup til en ekstern harddisk; til en NAS-enhed (***N***etwork ***A***ttached ***S***torage – en lille boks med harddiske tilsluttet netværket); til et clouddrev på nettet eller til en rendyrket onlinebackuptjeneste på Internettet.

Der findes også flere typer af backup. Der kan foretages en fuldstændig backup af hele harddisken (varer måske timer) eller kun backup af ændringer siden sidste backup (sekunder eller minutter).

Selvom man har backup af sine data, virker genetablering *(restore)* så? Det er noget, der kan være en rigtig god idé at teste.

Skybrud er blevet forholdsvis hyppige – med indtrængen af vand i huse og kældre til følge – her Vesterbro i København.

Er uheldet ude, og man har en harddisk, der har været udsat for skade af den ene eller anden art, så findes der firmaer, der har specialiseret sig i at redde data fra den. Det koster, men det kan som regel lade sig gøre.

Sådan kan det gå – brandskade på computeren – så er gode råd dyre.

Kapitel 24 - Børn og onlinesikkerhed

For en del forældre er den digitale verden, deres børn og teenagere færdes i, ny, og de har ikke selv nogen erfaring med fra deres egen barndom og ungdom, om hvordan de på passende vis kan forholde sig til og tale med deres egne børn om den. De har ofte ikke tilstrækkelig viden eller indsigt i hvilke gode ting, der er for børnene på pc'en og nettet, og heller ikke hvilke farer det er godt at rådgive dem om – og ikke mindst med hvilken indstilling, man med fordel kan henvende sig til dem om det. Desuden er mange børn og unge overladt til sig selv på pc'en, smartphonen og tablet-pc'en uden overvågning fra forældre. Mange forældre er ikke opmærksomme på deres børns brug af disse apparater, apps og internettjenester, og børnene fortæller dem ofte heller ikke noget om det. Børnene og de unge går ofte alene med deres tanker.

I de følgende afsnit belyses forskellige aspekter, der er nyttige at kende til for forældre og andre voksne, der har med børn og deres udvikling at gøre. Der er tale om følgende emner:

- Samtale mellem forældre og børn om onlinesikkerhed.
- At sætte grænser for sit barns tidsforbrug på pc'en; hvilke hjemmesider, der må besøges; og hvilke apps, der må benyttes.
- Forældrekontrol med børns brug af smartphones; spærrede hjemmesider; spærring af køb i spil; begrænsning af tidsforbruget på apps og Internettet; og undgåelse af børnenes omgåelse af reglerne for brug.

24.1 Samtale mellem forældre og børn om onlinesikkerhed

[35] Hvordan starter du bedst en samtale med dine børn om et kompliceret emne som onlinesikkerhed? Kan mor og far få dem til at forstå det? I denne artikel vises nogle nemme måder at starte samtalen på, og hvordan du holder en løbende dialog i gang i din familie.

[35] Kilde: dk.norton.com/the-talk/article – En artikel fra antivirusfirmaet Symantec om forældresamtale med børn.

Kapitel 26 - Hackeres tyveri af log-ind-oplysninger fra hjemmesider

I de senere år har der været en række tilfælde af store datatyverier fra store firmaers hjemmesider. Det gælder det store softwarehus **Adobe** og e-mailtjenesten **Yahoo**, som har fået stjålet log-ind-oplysninger for millioner af deres brugere. Dette er alvorligt, især fordi mange mennesker benytter det samme bruger-id (deres e-mailadresse) og adgangskode til mange tjenester på nettet. Har hackerne først fået fat i disse oplysninger et sted fra, kan de i princippet gå på brugernes Facebook-konti, udenlandske netbanker og e-mailkonti. Dette er én af grundene til, at det er godt at have mere end én adgangskode til de tjenester, du benytter, så du ikke kun benytter den samme alle steder.

At brugernavne og adgangskoders afsløring kan have store konsekvenser, viser et hackerindbrud foretaget af hackergruppen **The Impact Team** hos den canadiske utroskabstjeneste www.ashleymadison.com. Hackere har fået fat på bruger-id'er, adgangskoder, e-mailadresser og kreditkortnumre for 37 millioner brugere fra mere end 40 lande. De gav tjenesten en måned til at lukke. Det gjorde den ikke. Så offentliggjorde hackerne alle 30 gigabyte data på fildelingsnetværk. Andre igen har gjort dataene søgbare. Lækket er søgbart på hjemmesiden ashley.cynic.al. Læs om forløbet herunder for at forstå de mulige konsekvenser af et sådant hackerindbrud.

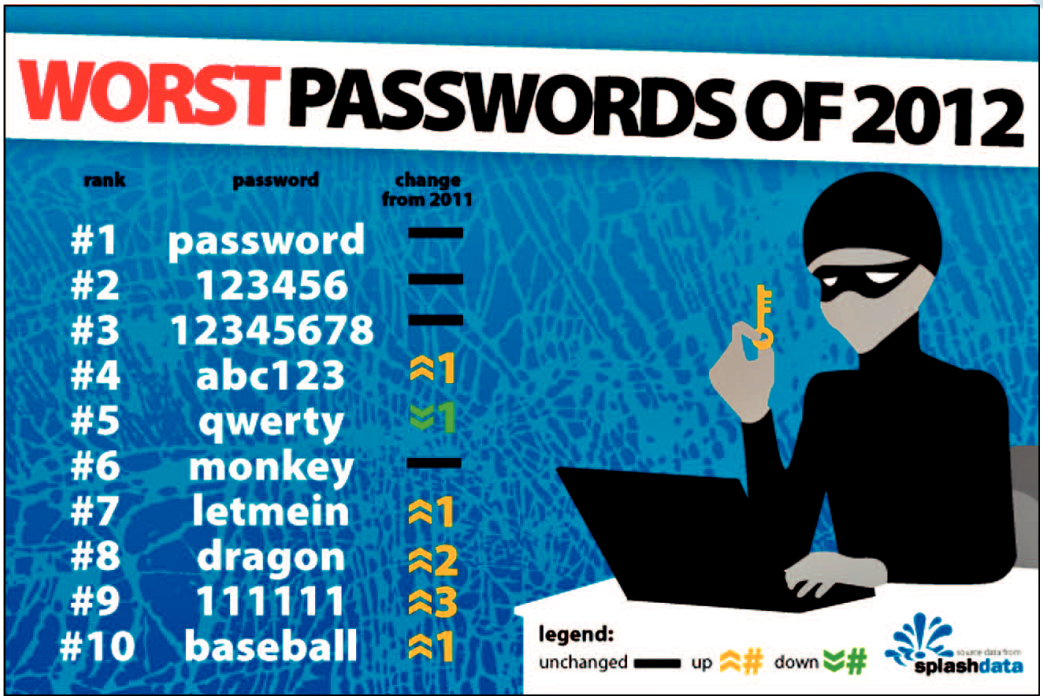
26.1 Hackersagen om utroskabshjemmesiden Ashley Madison

Oplysninger om 36 millioner utro mænd og kvinder fra hjemmesiden Ashley Madison blev lagt online. Hvad har denne skandale ført med sig?

En amerikansk journalist, Brian Krebs, havde i flere år ajourført en populær internetsikkerhedsblog (KrebsOnSecurity.com), hvor han bl.a. skrev om datalæk af brugerkontooplysninger fra store firmaers hjemmesider. En anonym henvendelse til ham per e-mail listede nogle links til et datalæk. Dette førte til en af hans livs største nyheder, som hurtigt blev taget op af mange andre medier. Den drejede sig om sidespringshjemmesiden Ashley Madison.

"Livet er kort – hav en affære" er mottoet for Ashley Madison. Hjemmesiden blev oprettet i 2008 for at formidle affærer for gifte personer. Den reklamerer med, at brugerne er *"anonyme"*, og der er *"100 % diskretion"*. Abonnementet er gratis for kvinder, mens mænd betaler et månedligt gebyr.

Den 12. juli 2015 blev ansatte i firmaet bag Ashley Madison, **Avid Life Media**, konfronteret af en meddelelse på deres computere fra hackerne, da de loggede på. Budskabet blev ledsaget af musik: AC/DCs **Thunderstruck**. Avid Life Media udlovede en dusør på 500.000 canadiske dollars for oplysninger, der kunne føre til identifikation af hackerne. Firmaet udtalte, at de var fortrøstningsfulde over for, at politiet ville pågribe hackerne og retsforfølge dem.



De ti "værste" adgangskoder anvendt i 2012 rangeret efter hyppigheden for anvendelse. Disse bør undgås. Kilde: Splashdata.

Kapitel 27 - Valg af gode adgangskoder for at styrke sikkerheden

Hvordan håndterer danskerne egentligt deres adgangskoder? Bliv klogere af denne statistik:

35 % af danskerne skifter aldrig eller yderst sjældent deres kodeord, bl.a. fordi det er svært at huske nye.

34 % bruger ofte de samme faste kodeord til netbanken, de sociale medier og sider, hvor de e-handler.

4 % har for en sikkerheds skyld gemt et foto af deres NemID-nøglekort på mobilen.

4 % har skrevet kodeord ned og lagt sedlen i deres pung eller taske [40].

Af og til læser man i pressen, at der er sket et stort læk af log-ind-oplysninger fra en stor netbutik eller en anden tjeneste på Internettet. Det sker med måneders mellemrum. Her har hackere fået adgang til (i nogle tilfælde) millioner af menneskers bruger-id'er (typisk e-mailadresser) og adgangskoder. Disse bliver enten solgt videre til lave priser per 100 styk til andre kriminelle eller offentliggjort på hjemmesider. Læs **artiklen** om dette på side 82 og om **tyveri af adgangskoder** på siderne 359-373.

Da dette er en reel risiko ved at benytte sine log-ind-oplysninger på Internettet, har sikkerhedseksperter nu i en årrække anbefalet (især virksomheders medarbejdere) at benytte nogle ret skrappe regler for koder:

- Ændring af adgangskoder hver måned eller hver tredje måned.
- Undgå at vælge en adgangskode, der har været anvendt før på en tjeneste.
- Vælg lange, svært knækbare adgangskoder med både store og små bogstaver, cifre og specialtegn.
- Hav forskellige adgangskoder til hvert program eller internettjeneste.
- Undlad at benytte adgangskoder, som mennesker, der ved noget om dig, let vil kunne finde ud af. Det kan være hunden eller kattens navn, et navn på et familiemedlem eller et mellemnavn, du sjældent benytter.

[40] Kilde: **TNS Gallup** for Nordea i 2015. Baseret på 1.055 interview med personer i alderen 18-65 år. Se den fulde undersøgelse her: www.nordea.com/Images/34-113950/Digital%20adfærd%202015.pdf

Kapitel 28 - Nationalstaters brug af malware

Cyberspionageangreb sponsoreret af nationalstater bliver mere og mere sofistikerede og er målrettet omhyggeligt definerede brugere med komplekse modulære værktøjer og holder sig godt under radaren for stadig mere effektive opdagelsessystemer, konkluderer **Kaspersky Lab**-eksperter.

Vi skal på de kommende sider se på et eksempel på malware, som ramte den iranske atomkraft/atomvåben-industri – kaldet **Stuxnet**. Den blev beskrevet i pressen, da den blev opdaget.

- I tysktalende lande har man også benyttet såkaldte *statstrojanere* til spionageformål.
- Vi vil også se på et værktøj til overvågning af mistænkte personer, som politiet i flere lande har benyttet.
- Der er beskrevet noget om, hvad amerikanske NSA og CIA er i stand til med malwareangreb.
- Endelig skal vi også se på inficering af harddiskcontrollere med en nærmest "udødelig" virus.

28.1 Stuxnet og iranske nukleare centrifuger

[41] **Stuxnet** er en computerorm, som blev opdaget i juni 2010. Den er designet til at angribe industrielle *programmable logic controllers* (programmerbare logiske styringsenheder), også kaldet PLC'er – det er en lille computer brugt til automatisering af maskiner i industriel produktion.

28.1.1 Iranske PLC'er ramt af Stuxnet

PLC'er tillader automatisering af elektromekaniske processer såsom dem, der benyttes til at styre en fabriks samlebånd, udstyr i forlystelsesparker, eller centrifuger til adskillelse af nukleart materiale. Der benyttes centrifuger til at adskille f.eks. materiale med de to uranisotoper, det mere almindelige ^{238}U (kan ikke benyttes til kernespaltning) og det sjældnere ^{235}U (kan bruges til kernespaltning). Ved at udnytte fire nuldages-sikkerhedshuller fungerer Stuxnet ved at være målrettet maskiner, der benytter Microsoft Windows-styresystemer og -netværk, og udsøger sig derefter **Siemens Step7**-softwaren. Stuxnet har angiveligt kompromitteret iranske PLC'er, der indsamlede informationer om industrielle systemer, og forårsagede ødelæggelser på hurtigt roterende centrifuger, så de faldt fra hinanden. Stuxnets design og arkitektur er ikke specifik

[41] Kilde: en.wikipedia.org/wiki/Stuxnet

Kapitel 29 - Digitalt selvforsvar

Internetrevolutionen har medført, at de fleste mennesker i den vestlige og mange i den øvrige verden benytter e-mail, hjemmesider, lytter til musik og ser video over nettet. Vi lægger i stigende grad fotos og dokumenter ud på nettet i fototjenester og cloud-drev (fillager på nettet). Google og andre store annoncetjenester registrerer vores søgninger, og det vi klikker på, og lagrer det hele for at skabe en profil om os, så annoncører bedre kan målrette deres annoncer til os.

Føler du dig overvåget på Internettet?

29.1 Overvågning på nettet

Vi hører whistlebloweren **Edward Snowden** afsløre, at NSA (***N***ational ***S***ecurity ***A***gency), en amerikansk efterretningsorganisation, elektronisk opsnapper, hvem du telefonerer med, dine e-mails, Facebook-vægges indhold, Twitter-beskeder og måske også indholdet af cloud-drev, som vi i stigende grad benytter os af – især med **OneDrive** i Windows; **iCloud** på Mac, iPhone og iPad; **Google Drev** hos Google og **Dropbox**. De såkaldte *cookies*, som mange hjemmesider efterlader på pc'er og mobile enheder, kan benyttes til at indsamle oplysninger. Klik på en hjemmeside fungerer endog på en sådan måde, at den hjemmeside, du kommer til ved et klik, kan registrere, hvilken hjemmeside du kommer fra.

Der findes firmaer, der har specialiseret sig i at indsamle oplysninger om os alle, såkaldte *databrokere* (datasælgere), og som sælger disse oplysninger videre til dem, der er interesserede i dem – det kan være annoncører, der vil målrette annoncer; det kan være forsikringsselskaber; det kan endog være efterretningstjenester. Der kan indsamles op til 1.500 stykker information per borger på denne måde. Så hvis du på Facebook skriver noget om en sygdom, kan et forsikringsselskab indhente oplysninger om dette hos en databroker. Dette har især betydning i USA, hvor det normale er at have private sundhedsforsikringer.

29.2 Se hvilke oplysninger Google indsamler om dig

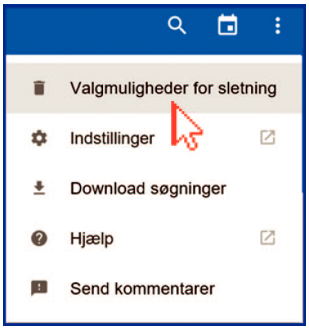
Hvis du har en Google-konto, kan du få adgang til at se de oplysninger, som Google indsamler om dig på Googles hjemmesider, bl.a. www.google.dk, www.youtube.com, www.blogspot.com og www.gmail.com.

F.eks. kan du se, hvilke søgninger du har foretaget gennem den seneste tid. Log ind med din Google-konto på www.google.dk og gå til webadressen for web- og app-aktivitet: https://myactivity.google.com/myactivity

En menu med adgang til yderligere oplysninger. Se f.eks. Placeringshistorik – en oversigt over hvor du har været geografisk, vist på et kort.

Så får du en liste over dine søgninger – hvilke søgeord, du har brugt, og hvilke links i listen over søgeresultater, du har klikket på. Disse anføres med tidspunkt, og hvis de er sket fra en mobiltelefon eller en PC med Wi-Fi, også hvor det skete geografisk.

Du kan slette historien om din web- og app-aktivitet ved at klikke på menuen med de tre lodrette prikker. Så får du mulighed for at slette søgehistorikken for en periode eller for altid (se her til højre).



Klik på menuen med de tre prikker for at få valgmulighederne for sletning af historikken.

Så kan du slette din aktivitet hos Google.

Klikker du på menuen med de tre streger, får du yderligere mulighed for at se, hvad Google har af oplysninger om dig (se herover). Googles data bliver delvist anonymiserede efter 18 måneder.

Du kan se Googles kendskab til dine interesser på: www.google.com/settings/ads

29.3 Træt af it-selskabers indsamling af oplysninger?

Danske teleselskaber logger lokationsdata ved sending af SMS'er og MMS'er. De kan eller vil ikke skelne mellem disse typer meddelelser og logning af mobilbrugerens andre lokationsdata ved anden mobildatatrafik. Det betyder, at firmaerne indsamler oplysninger om, hvor du har været i løbet af dagen – det kan være over 100 oplysninger i løbet af en dag. Det har tidligere i Danmark været et krav til teleselskaberne, at de skulle logge oplysninger om alle websider, der besøges, og alle e-mails, der sendes og modtages. Efter en EU-dom, må myndighederne ikke mere forlange dette af selskaberne.

Store it-firmaer som Google og Apple logger også en mængde oplysninger. Google indsamler lokationsdata og data om, hvordan du bruger dine apps på en Android-telefon mange gange i løbet af en dag. Apple gør noget tilsvarende for iPhone-brugere.

Hvis du ikke synes om, at Google registrerer oplysninger om dine søgninger og interesser til brug ved målrettede reklamer, findes der alternative søgemaskiner, der ikke registrerer noget om dig. De kan give neutrale i modsætning til personaliserede søgeresultater som Googles. Et par stykker, hvis popularitet er stigende, er: