DKCERT Trendrapport 2012

Status på informations-sikkerhed i året der gik

DeiC DANISH e-INFRASTRUCTURE COOPERATION

Redaktion: Shehzad Ahmad, Jens Borup Pedersen og Torben B. Sørensen, DKCERT, DeIC

Grafisk arbejde: Kirsten Tobine Hougaard, DeIC

Foto: Jens Borup Pedersen

ISBN 978-87-87036-36-8

Om DKCERT

Det er DKCERTs mission at skabe øget fokus på informationssikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DKCERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DKCERT bygger på en vision om at skabe samfundsmæssig værdi i form af øget informationssikkerhed. Det sker gennem offentliggørelse af viden om it-sikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen, samt internationale samarbejdspartnere.

Denne viden benytter DKCERT til at udvikle services, der skaber merværdi for DKCERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DKCERT, det danske Computer Emergency Response Team, blev oprettet i 1991 som en afdeling af UNI-C, Danmarks it-center for uddannelse og forskning, der er en styrelse under Ministeriet for Børn og Undervisning.

I dag hører DKCERT under DeIC, Danish e-Infrastructure Cooperation. DeIC har til formål at understøtte Danmark som e-science-nation gennem levering af e-infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DeIC er etableret under Ministeriet for Forskning, Innovation og Videregående Uddannelser og hører organisatorisk under Styrelsen for Forskning og Innovation.

Fysisk er DKCERT placeret på DTU's campus nord for København.

DKCERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om informationssikkerhed med grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DKCERT om informationssikkerhed i Danmark. DKCERT er medlem af FIRST (Forum of Incident Response and Security Teams).

Forord

De ringer. De mailer. De skriver via Facebook og Twitter.

Sjældent har jeg oplevet større interesse for informationssikkerhed end i denne tid. Vi bliver kontaktet af journalister, af it-folk og helt almindelige borgere. De spørger om den seneste trussel på nettet, hvordan den berører dem, og hvad de skal gøre.

Henvendelserne er udtryk for en klar tendens: Informationssikkerhed er ikke længere et område, der kun interesserer nogle få indviede. I dag interesserer det os alle – fordi det berører os alle. Den øgede interesse er positiv. Men den kommer på en dyster baggrund.

Væksten i interessen afspejler nemlig en tilsvarende vækst, når det gælder mængden af sikkerhedshændelser. Når vi renser tallene for portscanninger, steg mængden af reelle sikkerhedshændelser, DKCERT registrerede i 2012, med 45 procent. Mængden af nye sårbarheder i it-systemer steg 27 procent på verdensplan.

Derfor er det ikke så mærkeligt, at flere er blevet mere interesserede i sikkerhed. Informationssikkerhed har fået betydning i vores dagligdag. Vi risikerer, at vores pc bliver inficeret med malware, som giver forbrydere adgang til netbanken. Vores smartphones er blevet angrebsmål, og inden længe ser vi de første angreb på fjernsyn og anden intelligent elektronik med internetadgang.

Så der er brug for DKCERT og de øvrige organisationer, der arbejder for en bedre informationssikkerhed. Mere end nogensinde.

Ved årets slutning overgik DKCERT sammen med flere andre aktiviteter fra UNI-C til DeIC (Danish e-Infrastructure Cooperation). DeIC blev dannet i april ved en fusion af Forskningsnettet og Dansk Center for Scientific Computing.

Dermed forlod vi altså UNI-C, som stod bag stiftelsen af DKCERT helt tilbage i 1991. Vi har været glade for at være en del af UNI-C-familien, så det var et vemodigt farvel.

”Her venter mange spændende udfordringer inden for informationssikkerhed i de kommende år, ikke mindst inden for områder som big data og BYOD.”

Set udefra betyder overgangen ikke de store ændringer: Vi bor fortsat på DTU’s campus nord for København og er fortsat CERT for Forskningsnettet. Men på længere sigt ser jeg fordele ved, at DKCERT nu er knyttet endnu tættere til universitetssektoren. Her venter mange spændende udfordringer inden for informationssikkerhed i de kommende år, ikke mindst inden for områder som big data og BYOD
(Bring Your Own Device).

God fornøjelse med læsningen af DKCERTs Trendrapport 2012!

Shehzad Ahmad, chef for DKCERT

Indholdsfortegnelse

1. Resume

DKCERT behandlede 15.560 sikkerhedshændelser i 2012. Det er 65 procent færre end året før. Faldet skyldes primært et fald i indrapporterede portscanninger. Renser man tallene for den type hændelser, steg mængden af sikkerhedshændelser 45 procent.

Sager om piratkopiering udgjorde 23,7 procent af hændelserne og var dermed den form for sikkerhedshændelse, der var flest af.

Der var 1.211 tilfælde, hvor danske webservere blev brugt til at huse falske login-sider. De indgår i såkaldt phishing, hvor svindlere narrer folk til at tro, at de er inde på en webside, de kender. Her lokkes offeret til at indtaste brugernavn, adgangskode og kreditkortinformationer, som bagmændene derefter kan udnytte. Megen phishing gav sig ud for at være mails fra Skat eller store banker.

629 hændelser handlede om pc'er, der deltog i botnet. Det vil sige, at de var inficeret med skadelige programmer, som internetkriminelle kunne bruge til at fjernstyre dem med. Ofte bliver pc'erne i botnettet misbrugt til udsendelse af spam eller angreb på andre computere.

"Når ubudne gæster vil ind på pc'er og servere, går vejen ofte gennem velkendte sårbarheder."

Når ubudne gæster vil ind på pc'er og servere, går vejen ofte gennem velkendte sårbarheder. 2012 bød på en trist rekord her: Der blev på internationalt plan fundet 5.293 sårbarheder, det er det højeste antal siden 2009. Fokus var i høj grad på de sikkerhedshuller, der udnyttes, før der findes en rettelse til dem, de såkaldte zero day-sårbarheder. Et zero day-hul i Java fik således DKCERT til i juni at fraråde brugen af Java.

Næsten hver fjerde nye sårbarhed findes i web-software. Det er problematisk, fordi websystemer som hovedregel er frit tilgængelige fra internettet. Derfor har angribere let ved at udnytte deres sårbarheder.

DKCERT scannede i årets løb 3.421 computere på Forskningsnettet for sårbarheder. Der blev fundet sårbarheder på næsten hver fjerde af dem. Tre ud af fire af sårbarhederne lå i websystemer.

Efter en gennemgang af statistikker baseret på vores egne og andres tal bringer trendrapporten en oversigt over nogle af de centrale nyheder fra it-sikkerhedsområdet i det forgangne år. Det var et år, der blev præget af hacktivisme, exploit kits og zero day-sårbarheder.

Fire artikler fra eksterne bidragydere dækker aktuelle udfordringer i de it-ansvarliges hverdag: De ansattes brug af eget udstyr, beredskabsplanlægning, sikkerhedsstandarden ISO27000 og plysningskampagner.

Efter en status over informationssikkerheden i 2012 og i fremtiden rundes rapporten af med tre sæt anbefalinger til henholdsvis borgerne, de it-ansvarlige og beslutningstagerne.

2. Indledning

Med temaet *"sammen er vi sikre hver for sig"* ønsker vi med dette års Trendrapport at sætte fokus på løsningen af individuelle behov ud fra et fællesskabsperspektiv. I trafikken fungerer det kun, hvis vi alle følger de samme spilleregler. Det gælder, hvad enten vi kører i en Fiat eller en Ferrari, skal til Nakskov eller Nørre Sundby. Sådan er det også med informationssikkerhed.

"Selv om vi kan have forskellige behov, systemer og løsninger, er det grundlæggende de samme trusler, vi udsættes for."

Selv om vi kan have forskellige behov, systemer og løsninger, er det grundlæggende de samme trusler, vi udsættes for. Ydermere er vi underlagt den samme lovgivning og de samme standarder. Her er effektiv videndeling og samarbejde væsentlige elementer i transformationen af det fælles til det individuelle. I sidste ende er målsætningen også den samme: At vi for færrest mulig penge får mest mulig anvendelighed og sikkerhed af vores løsninger. Eller sagt på en anden måde, at vores informationssystemer og data skaber mest mulig positiv værdi.

Temaet skal også ses i lyset af sammenlægning af Forskningsnettet og Dansk Center for Scientific Computing (DCSC) i det nyetablerede DeIC (Danish e-Infrastructure Cooperation), som DKCERT er en del af. Også her handler det om at gå sammen om det, som er fælles, mens varetagelse af det enkelte universitets specifikke behov overlades til dem selv. DeICs opgave er at sikre en stabil leverance af e-infrastrukturer, der er fælles for de danske forskningsinstitutioner, samt at arbejde for en bæredygtig udvikling af e-science i Danmark.

Både nationalt og internationalt samarbejdes der for at imødegå den fælles trussel fra transnationale internetkriminelle grupperinger. Det afspejles blandt andet ved den nylige oprettelse af Rådet for Digital Sikkerhed, samt ved en fælleseuropæisk harmonisering af lovgivning vedrørende internetkriminalitet. For som justitsminister Morten Bødskov (S) udtalte i forbindelse med, at sidstnævnte blev sendt til formel godkendelse i Europa-Parlamentet:

"Angreb på informationssystemer udgør en stigende udfordring for vores samfund. (...) De kriminelles metoder til at begå disse forbrydelser bliver mere og mere sofistikerede."

Vi har i år ændret strukturen af rapporten, så den i større grad afspejler de trusler, vi udsættes for. Således er der sket en opdeling af emner i rapportens første afsnit, hvor vi med tal og statistikker gør rede for hændelser, der blev rapporteret til DKCERT. Der tages her udgangspunkt i data, der primært dækker hændelser på de netværk, som DKCERT overvåger, suppleret og perspektiveret med eksterne data og statistikker.

I rapportens følgende afsnit bringer vi artiklerne fra årets tre tidligere kvartalsrapporter efterfulgt af nye artikler om fjerde kvartals hændelser. Rapporten afspejler således i højere grad begivenheder fra hele året. Tilsammen er artiklerne med til at give et billede af internetkriminalitet som en trussel, alle i dag er underlagt. Det hvad enten man agerer som enkeltindivid eller i en organisatorisk sammenhæng.

Herefter har vi ladet en række eksterne aktører komme til orde for at fortælle om deres udfordringer med hensyn til informationssikkerhed. Her kan du for eksempel læse om, hvordan man på de danske universiteter takler overgangen til ISO 27000-standarden, udfærdigelse og implementering af beredskabsplaner som en integreret del af sikkerhedspolitikken, samt brugere der ønsker at benytte deres eget udstyr til arbejdsrelaterede opgaver.

I afsnit 9 giver vi et samlet opsummerende billede af de trusler, vi har kunnet identificere, samt de heraf afledte problemstillinger. Vi beskriver, hvordan internetkriminaliteten har udviklet sig gennem 2012, og hvordan vi forventer, at den vil udvikle sig fremover. Herved forsøger vi at åbne perspektivet på brugen af teknologien og de udfordringer, vi i fremtiden skal imødegå. Afsnittet afrundes med vores bud på de væsentligste tendenser med hensyn til informationssikkerhed. Det gør vi ved at liste de vigtigste tendenser for 2012 og de tendenser, som vil præge informationssikkerhedsarbejdet de kommende år.

Rapporten afrundes med vores anbefalinger til, hvordan vi i fællesskab kan bidrage til at sikre danskernes it-aktiver. Hvad enten det handler om at beskytte mod misbrug af borgernes kreditkortinformationer, at sikre at forretningskritiske data ikke ryger i de forkerte hænder eller sikre oppetiden på centrale installationer, er vi nemlig alle del af den samme internetkriminelle fødekæde.

Det er derfor vores håb, at du finder vores anbefalinger til henholdsvis borgerne, organisationerne og beslutningstagerne brugbare. Spørgsmålet er nemlig, om det ikke er, når vi står sammen og lærer af hinanden, at vi er mest sikre, også når vi agerer som individer hver for sig.

Eu2012, 2012; "*Nye EU-regler om straffe for it-kriminalitet*".

3. 2012 - året i tal

Dette afsnit beskriver årets sikkerhedshændelser og nye sårbarheder med udgangspunkt i de tal og statistikker, som er tilgængelige for DKCERT.

Fokus er på data, der er gjort tilgængelige for os i vores rolle som CERT (Computer Emergency Response Team) for institutioner på Forskningsnettet, der er en landsdækkende netinfrastruktur for universiteter og forskningsinstitutioner. Data vedrørende institutioner på Forskningsnettet er suppleret med hændelser vedrørende det øvrige danske internet, som blev rapporteret til DKCERT i løbet af året.

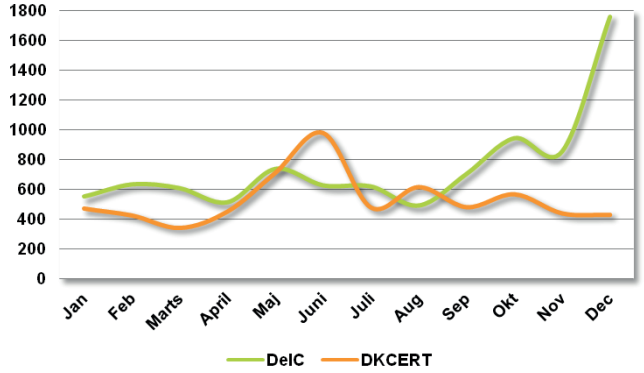
Yderligere data fra internettets åbne kilder benyttes til at supplere og/eller perspektivere egne data. Derfor mener vi, at afsnittet afspejler udviklingen på hele det danske internet i 2012.

Afsnittet begynder med en oversigt over de sikkerhedshændelser, vi modtog henvendelse om i årets løb. Derefter ser vi på de ten-denser, statistikkerne viser: Hvordan var udviklingen inden for skadelige programmer, spam, phishing og andre trusler mod informationssikkerheden?

Til slut gennemgår vi sårbarheder ud fra to perspektiver. Først ser vi på de nye sårbarheder i it-systemer, der blev opdaget i 2012. Derefter analyserer vi resultaterne af de sikkerhedsscanninger, som vi i årets løb har gennemført for institutioner på Forskningsnettet.

3.1 Årets sikkerhedshændelser

DKCERT behandlede væsentligt færre sikkerhedshændelser i 2012 i forhold til året før. Vi modtog 18.903 henvendelser, der førte til registrering af 15.560 hændelser (Figur 1). Det er et fald på 65 procent i forhold til de 44.829 hændelser i 2011.

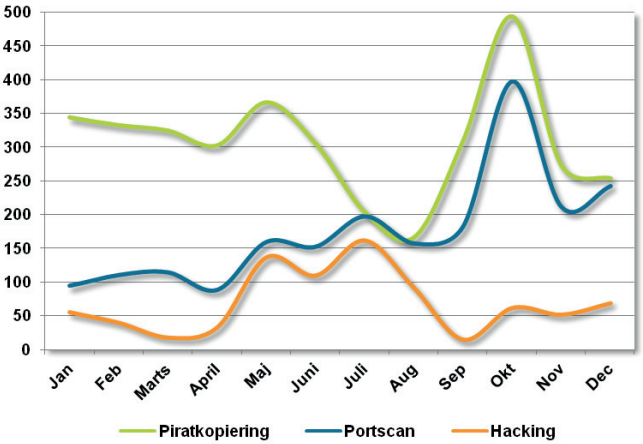


Figur 1. Hændelser for DeIC (Forskningsnettet) og øvrige Danmark.

Faldet skyldes, at registrerede portscanninger er faldet voldsomt: Hvor vi i 2011 havde 35.535 portscanninger, var der i 2012 kun 2.114. Dette fald skyldes sandsynligvis ændringer i opsætningen hos de institutioner, der indrapporterer portscanninger. Man får derfor et mere retvisende billede ved at rense tallene for portscanninger.

Gør man det, var der en stigning i mængden af hændelser på 45 procent fra 2011 til 2012. Mængden af hændelser steg gennem maj og juni og igen i slutningen af året. Disse tal og de følgende statistikker bygger på data fra DKCERTs interne rapporteringssystem, medmindre andet er angivet.

Sager om piratkopiering tegnede sig for 23,7 procent af årets hændelser og var dermed den hyppigst forekommende type hændelse (Figur 2). Mange af disse sager udspringer af kollegier tilsluttet Forskningsnettet. Derfor så vi sæsonmæssige udsving. Mængden af hændelser falder, når de studerende er til eksamen eller væk på ferie.



Figur 2. Hændelser med piratkopiering, portscanninger og hacking.

Stigningen i portscanninger i oktober og november kan måske skyldes, at hackere har søgt efter web- og mail-servere til brug ved svindel op til juletid. Højtiden er også højsæson for svindel: Ofrene er villige til at bruge penge og bekymrer sig mere om, om julegaverne når frem i tide, end om de kan stole på den butik, de køber hos.

Når en hændelse kategoriseres som hacking i DKCERTs system til håndtering af sikkerhedshændelser, kan der være tale om meget andet end egentlig hacking. Ved flere hændelser er der således ikke tale om reelle manuelle hackingforsøg, hvor en hacker bryder ind på et system. Vi må erkende, at nogle af hændelserne er fejlkategoriseret og reelt burde have været kategori-seret som for eksempel brute force, scanning eller botnetinfektion.

3.2. Malware

Antivirusfirmaet F-Secure opdagede 5.536 skadelige filer på danskeres computere i 2012. 40 procent af de skadelige programmer var trojanske heste (Figur 3).

Exploits har tidligere udgjort under tre procent af de fundne programmer, men deres andel steg i 2012 til 8,6 procent. Et exploit er et angrebsprogram, der udnytter en sårbarhed til at få kontrol med pc'en.

Forklaringen på den stigende mængde exploits kan være, at der er kommet flere såkaldte exploit kits på nettet. Det er serverprogrammer, der afprøver en lang række kendte exploits i forsøget på at inficere de besøgende computere. I årets løb var der stigende opmærksomhed på det problem.

Det mest udbredte exploit kit hedder Blackhole. Ifølge sikkerhedsfirmaet Sophos tegnede det sig for 28 procent af de web-baserede trusler, firmaet registrerede fra oktober 2011 til marts 2012.

"Flere sikkerhedsfirmaer rapporterer om en stigende mængde afpresningsprogrammer."

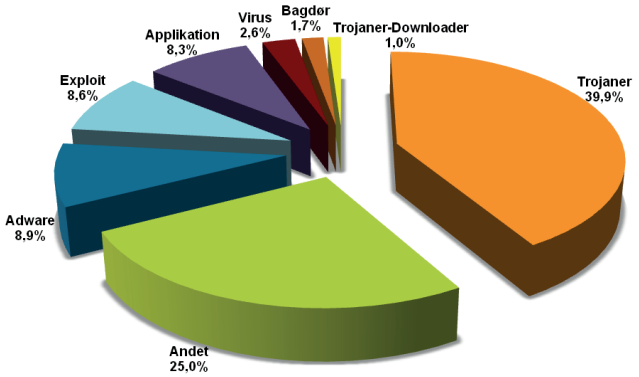
Flere sikkerhedsfirmaer rapporterer om en stigende mængde afpresningsprogrammer. Det er skadelig software, der tager brugerens data som gidsel. En besked på skærmen fortæller, at alle data er krypteret, og at man skal betale for at få adgang til dem igen.

En udbredt variation over dette tema er politi-ransomware. Her får brugeren at vide, at adgangen er spærret af politiet, fordi brugeren er blevet taget i at bruge piratkopier eller børneporno. Lader man sig narre af det budskab, sikre en kombination af autoritetstro og frygten for at andre tror at der er noget om snakken, at man ikke konsulterer andre. For mange efterlader det kun en mulighed: At betale bøden.

Udbredelsen af politi-ransomware var blandt de mest synlige tendenser i 2012. Vores forventning er den type malware vil fortsætte med at stige i udbredelse. I 2012 var der to grupper, der havde målrettet deres kode til det danske marked og andre vil sandsynligvis udnytte denne trend.

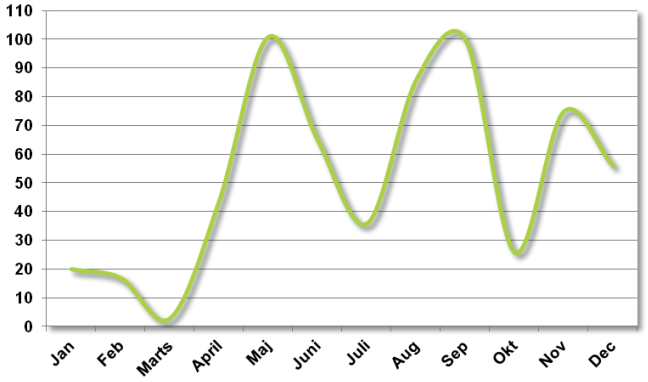
I stedet for at betale ved en eventuel inficering, bør man proaktivt investere i backup af sine date. Der er ingen garanti for at man modtager en kode der låser maskinen op eller at den efterfølgende er fri for malware.

Malware er ikke længere begrænset til traditionelle computere. Der var en kraftig stigning i skadelige programmer rettet mod smartphones med Android som styresystem. Tallene varierer, men firmaet Trustgo fandt for eksempel 28.707 forskellige skadelige Android-programmer i september 2012. Året før var tallet 4.951. At det primært er Android, som rammes skyldes blandt andet, at Android giver mulighed for installation af applikationer uden om Google Play.



Figur 3. Malware-infektioner fordelt på typer. Kilde: F-Secure.

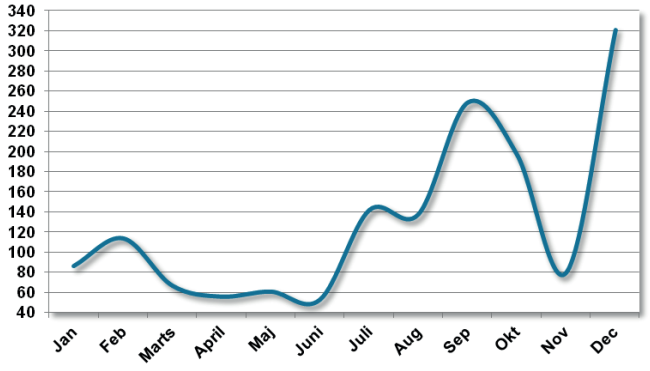
Når en pc bliver inficeret med skadelig software, er det i dag snarere reglen end undtagelsen, at den indrulleres i et botnet. Det vil sige, at bagmændene bag programmet kan fjernstyre pc'en uden ejeres vidende. DKCERT registrerede 629 hændelser, hvor pc'er var opdaget som deltagere i botnet (Figur 4). De store udsving over året skyldes, at infektionen typisk opdages, når en af bagmændenes servere (Command & Control server) bliver beslaglagt og data analyseres. Så modtager vi og andre CERT'er en større mængde IP-adresser på inficerede pc'er.



Figur 4. Hændelser med botnet-inficerede danske computere i 2012.

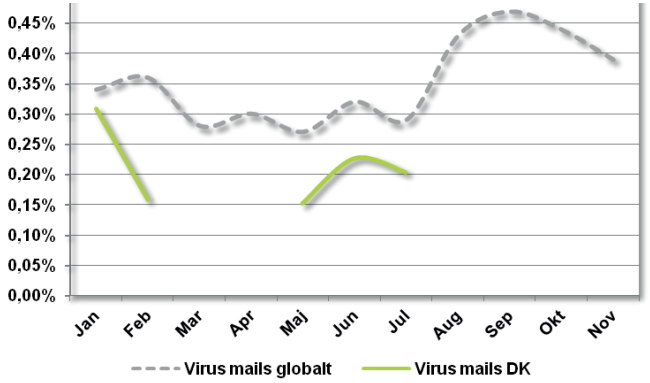
Megen malware spredes i dag ved, at offeret besøger en inficeret webside, hvor et exploit kit forsøger at inficere pc'en. Det afspejler sig i en stigning i antallet af inficerede websteder. DKCERT registrerede 1.564 hændelser, hvor danske websteder var inficeret med skadelige programmer (Figur 5). Det er en stigning på 46 procent i forhold til 2011. Tallet omfatter også websider, der videresender besøgende til sider med phishing eller malware. Tendensen til stigning i december kan skyldes, at de it-kriminelle generelt bliver mere aktive op mod jul.

Stigningen i september og oktober er sværere at forklare, men den svarer godt til udviklingen på globalt plan inden for virusinficerede mails (Figur 5).



Figur 5. Hændelser med malware-inficerede danske hjemmesider i 2012.

Sikkerhedsfirmaet Symantec finder typisk virus i mellem 1,5 og 3 promille af alle mails, der sendes til danskere (Figur 6). Dermed ligger Danmark lidt under det generelle niveau på 3,5 promille på verdensplan.



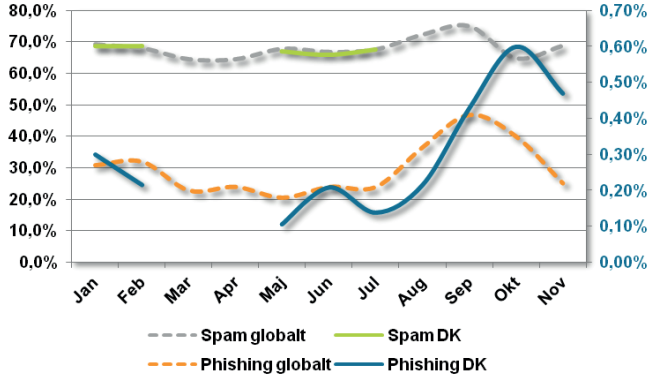
Figur 6. Andelen af virusspredende mails gennem 2012. Kilde: Symantec.

Symantec; "*Globale trusler*".
Symantec; "*Symantec intelligence reports*".
F-secure; "*F-Secure Security Lab - virus world map*".
Thenextweb, 2012; "*In one year, Android malware up 580%, 23 of the top 500 apps on Google Play deemed 'High Risk'*".

3.3. Spam og phishing

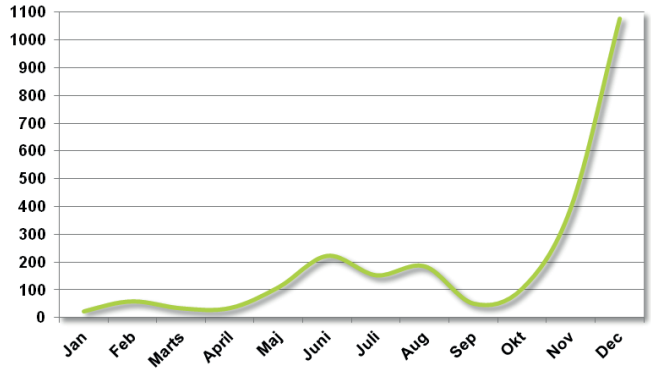
Mens virusmails måles i promiller, måler man spam i procenter: 68 procent af alle mails sendt i 2012 var ren spam, altså uønskede mails med kommercielt indhold (Figur 7). Her lå Danmark på linje med resten af verden, viser Symantecs tal.

I gennemsnit 2,6 promille af alle mails på verdensplan var forsøg på at lokke modtageren til at besøge et forfalsket websted. Formålet med den slags phishing er at narre fortrolige oplysninger fra offeret. Med 3,0 promille lå Danmark her en smule over det globale gennemsnit.

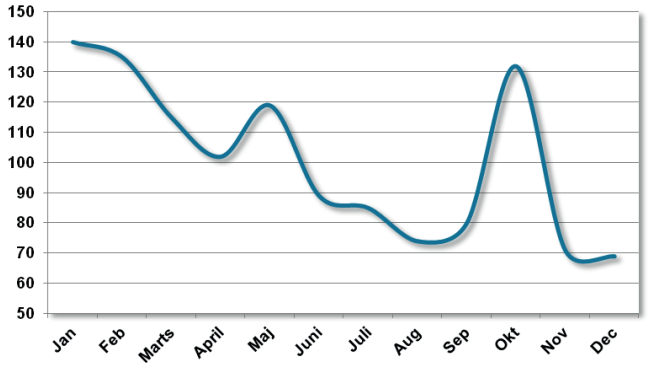


Figur 7. Spam- og phishing-mails sendt til danskerne i 2012. Kilde: Symantec.

DKCERT modtog 2.481 henvendelser om spam- eller phishingmails (Figur 8). Der var en lille stigning i sommerperioden, men den helt store mængde kom i november og december. Det er muligt, at nogle af disse mails havde til formål at lokke ofre til websteder, der er inficeret med malware – dem var der også flest af i december.



Figur 8. Spam- og phishing-mails rapporteret til DKCERT.



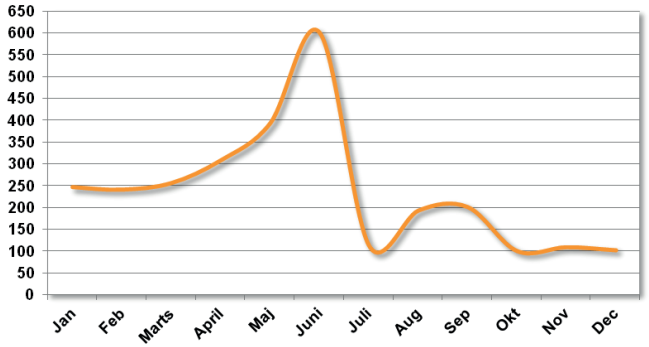
Figur 9. Hændelser med danske phishing-sider gennem 2012.

Danske webservere lægger også diskplads til phishing-sider. DKCERT behandlede 1.211 hændelser om phishing-sider (Figur 9). Mange af dem forsøgte at få fat i kreditkortinformationer, men banker og Skat var også populære.

Symantec; "*Globale trusler*".
Symantec; "*Symantec intelligence reports*".

3.4. Brute force-angreb

Ved et brute force-angreb afprøver en angriber en lang række mulige brugernavne og passwords i et forsøg på at finde en kombination, der giver adgang.



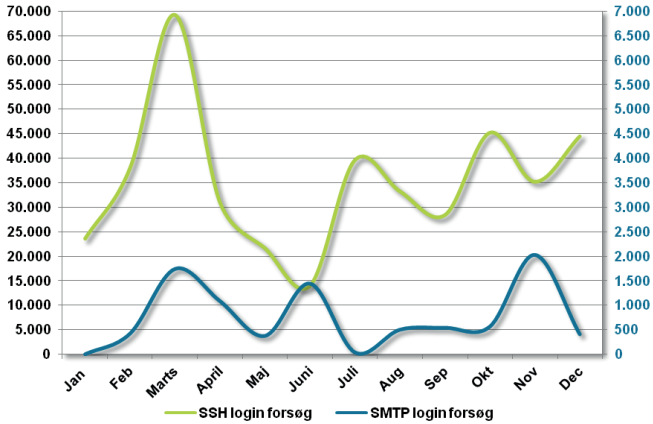
Figur 10. Hændelser med brute force-angreb gennem 2012.

DKCERT behandlede 2.875 hændelser om brute force-angreb, heraf handlede 335 om angreb på danske systemer (Figur 10). Det drejer sig primært om SSH-servere (Secure Shell) på danske universiteter og forskningsinstitutioner tilknyttet DeIC. De øvrige hændelser var forsøg på angreb på systemer i udlandet, der kom fra danske IP-adresser. Angrebene var primært rettet mod SSH og SMTP (Simple Mail Transfer Protocol), der bruges til at sende mail med.

At SSH og SMTP er populære angrebsmål fremgår også af tal fra en ny datakilde. DKCERT har sat et såkaldt honeynet i drift. Det er en digital lokkekrukke, der har til formål at tiltrække hackerangreb, så vi opbygger mere viden om deres aktiviteter.

Statistikken viser store udsving hen over året. I gennemsnit var der over 35.000 forsøg på at få adgang til honeynettets SSH-tjenester pr. måned (Figur 11). Men i marts nået tallet tæt på 70.000.

Angreb på SMTP lå noget lavere: I snit 776 forsøg om måneden, men også her med store udsving måned for måned.



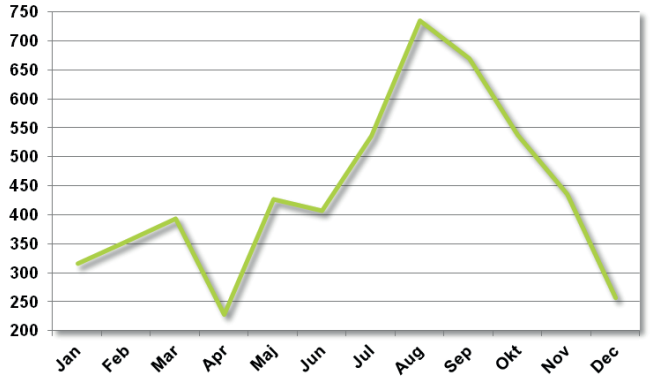
Figur 11. SSH og SMTP brute force login-forsøg gennem 2012.

Angriberne afprøver meget udbredte brugernavne i deres angreb: Root, admin, user og oracle er nogle typiske eksempler. Det samme gælder passwords: Her koncentrerer de sig om den type passwords, som brugeren ikke har brugt mange kræfter på et udtænke. Typiske eksempler er password, root, 123456 og lignende.

3.5. Årets nye sårbarheder

I 2012 blev der fundet 5.293 nye sårbarheder. Tallet dækker over sårbarheder, der i 2012 blev registreret i USA's National Vulnerability Database og udstyret med et CVE-nummer (Common Vulnerabilities and Exposures). Antallet i 2012 er det højeste siden 2009, ellers har tendensen de seneste år været faldende. Det høje tal dækker dog over store månedlige variationer (Figur 12).

I årets løb var der megen fokus på såkaldte zero day-sårbarheder. Det er sårbarheder, som angribere udnytter, før producenten har nået at udsende en rettelse, der lukker sikkerhedshullet. Med andre ord går der nul dage, fra sårbarheden er kendt, og til den udnyttes i praksis.



Figur 12. Nye CVE-nummererede sårbarheder gennem 2012.

Et eksempel på en zero day-angreb stammer fra slutningen af december, hvor et websted tilhørende USA's Council on Foreign Relations begyndte at sprede skadelige programmer til dem, der besøgte det. Det skyldtes, at webstedet selv var blevet inficeret med et skadeligt program. Og dette program havde udnyttet en hidtil ukendt sårbarhed i Internet Explorer 8 til at inficere webstedet med.

Microsoft reagerede ved at udsende en foreløbig rettelse, der lukkede for muligheden for at udnytte sårbarheden. En egentlig rettelse, der fjerner sårbarheden, kom ikke i 2012.

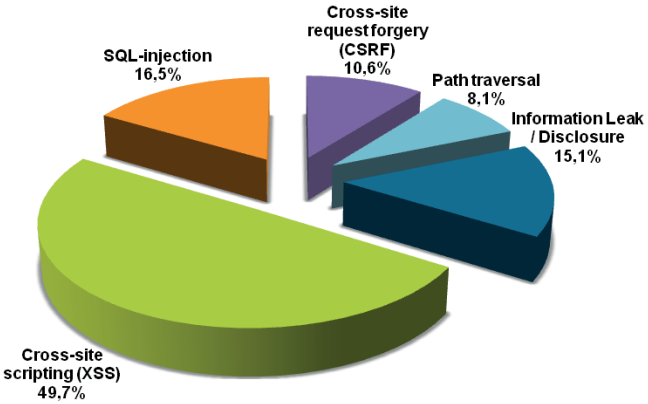
Andre eksempler på zero days i 2012 var et hul i Java, der blev udnyttet i august, og et i Internet Explorer fra september.

"En undersøgelse fra Carnegie Mellon University (CMU) udført af forskere fra sikkerhedsfirmaet Symantec viste, at der kan være flere zero day-sårbarheder, end vi hidtil har troet."

En undersøgelse fra Carnegie Mellon University (CMU) udført af forskere fra sikkerhedsfirmaet Symantec viste, at der kan være flere zero day-sårbarheder, end vi hidtil har troet. Forskerne analyserede skadelige programmer fundet på pc'er. De undersøgte, hvor mange af programmerne, der udnyttede sårbarheder, som ikke var kendt på tidspunktet for infektionen.

I alt fandt de 18 zero day-sårbarheder. Og 11 af dem har man hidtil ikke vidst blev udnyttet, før der kom en rettelse til dem. Hvis billedet er repræsentativt, kan der altså være en del flere zero day-angreb i omløb, end vi har været klar over.

Godt en fjerdedel af årets nyopdagede sårbarheder lå i webapplikationer. Sårbarheder i webapplikationer udgør ofte en høj risiko, fordi websystemer i sagens natur er frit tilgængelige fra internettet. Dermed har angribere let ved at finde potentielle angrebsmål og afprøve forskellige metoder mod dem.



Figur 13. Nye CVE-nummererede websårbarheder i 2012.

Halvdelen af de web-relaterede sårbarheder var af typen cross-site scripting (Figur 13). Det er en type sårbarhed, der gør det muligt at køre scriptkode i brugerens browser. Resultatet kan være, at en angriber kan opsnappe cookies, der giver adgang til brugerens session på et websted.

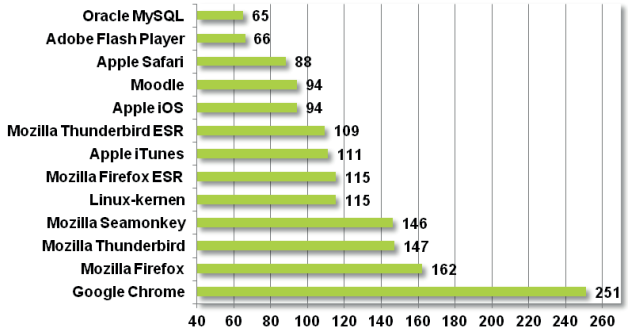
En anden udbredt sårbarhedstype er SQL-injection. Det går ud på, at angriberen indtaster databasekommandoer direkte i et felt på en webside. Kommandoerne overføres til databaseserveren, der udfører dem. På den måde kan uvedkommende få adgang til fortrolig information.

Både cross-site scripting og SQL-injection skyldes manglende validering af de input, der indsendes fra browseren. Løsningen er derfor øget kvalitetskontrol, så softwareudviklere sørger for at tjekke input, før de bliver sendt videre i systemet.

Flest sårbarheder blev der fundet i webbrowserne Google Chrome og Mozilla Firefox (Figur 14). Medregnet Mozillas kommercielle ESR version, Apples Safari browser og tilføjelses programmet Adobe Flash Player, var det systemer derbruges til at læse indhold fra webservere, der blev fundet flest sårbarheder i. Nedenfor følger en kronologisk gennemgang af udvalgte sårbarheder, der blev registreret i årets løb.

Den 10. januar udsendte Adobe en opdatering (APSB12-01), der fjernede seks alvorlige sårbarheder i Adobe Reader og Acrobat. Sårbarhederne giver en angriber mulighed for at afvikle programkode. Foruden sikkerhedsrettelserne indeholder de nye versioner af programmerne de rettelser til Flash Player, som blev udsendt i november, samt en ny sikkerhedsfunktion, der gør det muligt at slå

JavaScript til i dokumenter, som organisationen har tillid til.



Figur 14. Nye CVE-nummererede sårbarheder i softwareprodukter i 2012.

Oracles kvartalsvise opdatering den 23. januar rettede i alt 78 sårbarheder i syv produkter. Kun en blev vurderet at udgøre en høj risiko. To af sårbarhederne var i firmaets databaseserversoftware, mens der var 17 i tidligere Sun-produkter, 27 i MySQL og 11 i Fusion Middleware. Flere af sårbarhederne kan udnyttes over nettet af en uautentificeret angriber.

2. februar udsendte Apple en opdatering til Mac OS X Snow Leopard og Lion, der lukker en række alvorlige sikkerhedshuller i styresystemet. De 39 rettelser, der indgår i OS X Lion 10.7.3 og Security Update 2012-001 til OS X Snow Leopard 10, fjerner i alt 52 sårbarheder. 19 af dem retter alvorligere sårbarheder.

En opdatering lukkede den 14. februar 14 sikkerhedshuller i Oracle Java SE. Fem af sårbarhederne fik virksomhedens højeste risikovurdering. Fejlene er rettet i Java 6 Update 31 og Java 7 Update 3. Der er også udsendt rettelser til Java 5 og tidligere versioner.

Den 17. februar udsendte Adobe en opdatering (APSB12-03) til Flash Player 11.1 og tidligere versioner til Windows, Macintosh, Linux, Solaris og Android. Opdateringen rettede syv kritiske sårbarheder, som gør det muligt at afvikle programkode. En sårbarhed gør det muligt at udføre kommandoer via cross-site scripting. Den er set udnyttet via links i e-mails.

En opdatering af Chrome 17 rettede den 4. marts i alt 17 CVE-nummererede sårbarheder. 16 af sårbarhederne fik Googles næsthøjeste risikovurdering. Med opdateringen fulgte den nyeste version af Flash Player.

Adobe udsendte den 5. marts en ekstraordinær opdatering (APSB12-05) til Flash Player. Opdateringen rettede to kritiske sårbarheder (CVE-2012-0768 og CVE-2012-0769) i Flash 11.1 og tidligere til Windows, Macintosh, Linux, Solaris og Android. På tidspunktet for opdateringen var der ingen programmer, som udnyttede sårbarhederne.

Den 12. marts udsendte Apple en opdatering af browseren Safari til Mac OS X og Windows. Opdateringen til version 5.1.4 retter 83 sårbarheder i browseren. Flere af fejlene er alvorlige. De fleste sårbarheder findes i web-biblioteket WebKit, der også benyttes i browseren til iOS og i iTunes. Mange af rettelserne er de samme, som tidligere er blevet opdateret i disse programmer.

Den 14. marts udsendte Microsoft en rettelse til en alvorlig sårbarhed (CVE-2012-0002) i Remote Desktop Protocol, der bruges til fjernstyring af Windows-computere. Rettelsen indgik i månedens opdateringer til Microsofts operativsystemer og programmer, som rettede i alt seks CVE-nummererede sårbarheder. Sårbarheden blev opdaget 10 måneder tidligere. Mindre end en uge efter offentliggørelsen blev det første exploit udsendt. Det gør det muligt at udføre Denial of Service på sårbare systemer.

Microsofts april-opdateringer indeholdt rettelser til 11 sårbarheder, hvoraf flere fik virksomhedens højeste risikovurdering. Størst prioritet fik opdateringen til Windows Common Controls ActiveX-kontrol, som rettede en kritisk sårbarhed (CVE-2012-0158), der tidligere er udnyttet. Derudover lukker en opdatering til Internet Explorer fem sårbarheder, hvoraf tre er kritiske. En opdatering til Windows fjerner en kritisk sårbarhed (CVE-2012-0151) i kontrol af digital signering. Endelig fjerner opdateringerne sårbarheder i .NET Framework, Forefront Unified Access Gateway, Office og Works. Med opdateringerne offentliggjorde Microsoft, at de stopper supporten på Windows XP og Office 2003 i april 2014.

Den sjette april blev der frigivet en opdatering til Java til Mac OS X, der førte den op på samme version som Oracles versioner til Windows og Linux (1.6.0_31). Herved lukkedes 12 sikkerhedshuller, hvoraf det mest alvorlige (CVE-2012-0507) gjorde det muligt at afvikle kode uden for Javas sandkasse. Sårbarheden blev blandt andet udnyttet af det skadelige program Flashback, som angiveligt havde cirka 600.000 inficerede Macintosh-computere i sit botnet.

Oracle udsendte den 17. april sine kvartalsvise opdateringer, der lukkede 88 sårbarheder i virksomhedens produkter. Mest kritisk var en sårbarhed i Java-værktøjet JRockit (CVE-2012-1695), som fik højeste CVSS score 10. Ud over Oracles egne produkter som for eksempel Database Server, Fusion Middleware, Enterprise Manager Grid Control og E-Business Suite indeholdt opdateringen rettelser til de tidligere Sun-produkter Solaris og MySQL.

I alt 14 CVE-nummererede sårbarheder blev rettet med Mozillas opdatering til Firefox 12 den 25. april. Halvdelen af sårbarhederne er vurderet som kritiske og kan medføre kørsel af programkode fra et angribende websted. Ud over opdateringen af Firefox frigav Mozilla rettelser til Thunderbird og SeaMonkey. Hidtil har Mozillas opdateringer været underlagt Microsofts UAC (User Account Control). Efter Firefox i version 12 sker opdateringer uden at kræve brugerens accept.

Den fjerde maj udsendte Adobe en opdatering af Flash Player til

Windows, Macintosh, Linux og Android (APSB12-09). Den nye version fjerner en sårbarhed, som er set udnyttet (CVE-2012-0779). Sårbarheden gør det muligt for en angriber at få fuld kontrol over den sårbare pc.

Den ottende maj udsendte Microsoft sine månedlige opdateringer. De indeholdt syv opdateringer, der fjerner 23 sårbarheder i virksomhedens produkter. Mest kritisk var sårbarhederne CVE-2012-0183 i Word samt CVE-2012-0160 og CVE-2012-0161 i .NET Framework. De gør det muligt at afvikle kode på den sårbare maskine.

Derudover blev en opdatering, der lukker ti sårbarheder i Office, Windows, .NET Framework og Silverlight vurderet som kritisk. De øvrige opdateringer retter sårbarheder i .NET Framework, Office, Visio Viewer 2010, TCP/IP-stakken i Windows samt Windows Partition Manager.

Apple udsendte den 9. maj opdateringer, som retter 36 sårbarheder i Mac OS X samt fire i Safari. Med OS X Lion version 10.7.4 og Security Update 2012-002 til version 10.6.8 rettes blandt andet en omtalt sårbarhed (CVE-2012-0652), der giver adgang til passwords ved brug af Filevault. Den nye version af Safari (5.1.7) retter blandt andet en række cross-site scripting-sårbarheder i WebKit.

Den 23. maj udsendte Google en opdatering til Chrome 19, som var blevet frigivet en uges tid forinden. Opdateringen til version 19.0.1084.52 på Windows, Macintosh og Linux retter 13 sårbarheder. Ni sårbarheder fik Googles næsthøjeste risikovurdering, mens ingen blev vurderet som kritiske.

Den ottende juni udsendte Adobe en opdatering af Flash Player (APSB12-14) til alle platforme. Den fjernede syv sårbarheder, heraf seks alvorlige.

Oracles kvartalsvise opdateringer den12. juni lukkede 14 sårbarheder i Java til Windows, Mac OS X, Solaris og flere Linux-varianter. Seks sårbarheder fik højeste risikovurdering.

Juni-opdateringerne fra Microsoft indeholdt i alt rettelser til 26 sårbarheder. De syv opdateringer retter flere alvorlige sårbarheder i Windows, Internet Explorer, .Net Framework, Lync og Dynamics AX. Højest prioriterede opdatering lukker 13 sårbarheder i Internet Explorer og en i Remote Desktop Protocol (RDP) i Windows. En sårbarhed til Internet Explorer (CVE-2012-1875), der indgik i Microsofts juni-opdateringer, blev senere set udnyttet.

Den 20 juni udsendte Cisco opdateringer, der lukkede fire sårbarheder i VPN-klientprogrammet AnyConnect Secure Mobility Client. Sårbarhederne giver mulighed for at afvikle programkode eller nedgradere til en tidligere version. Tre sårbarheder findes i versionerne til både Windows, Mac OS X og Linux, mens den fjerde kun berører 64-bit Linux.

Juli-opdateringerne fra Microsoft indeholdt ni rettelser, der fjernede i alt 16 sårbarheder i blandt andet Visual Basic for Applications, Windows, SharePoint og Office for Mac. Mest kritiske var sårbarheder i Microsoft XML Core Services (CVE-2012-1889), Internet Explorer (CVE-2012-1522 og CVE-2012-1524) og Microsoft Data Access Components (CVE-2012-1891). De tillader alle ekstern afvikling af kode.

De kvartalsvise opdateringer fra Oracle den 17. juli rettede i alt 87 sårbarheder i blandt andet Oracle Database, Fusion Middleware, Enterprise Manager og Sun-produkterne. Flere sårbarheder i Fusion Middleware giver mulighed for ekstern afvikling af kode og findes gennem komponenten Outside In. Den benyttes til at konvertere mellem filformater og anvendes også af programmer fra andre producenter, som derfor også er sårbare. Blandt de berørte produkter er Microsofts Exchange og FAST Search Server 2010 for SharePoint.

Mozilla udsendte også opdateringer den 17. juli. De indeholdt 15 rettelser til 19 forskellige sårbarheder i Firefox, Thunderbird og Seamonkey. Fem opdateringer blev vurderet som kritiske og rettede i alt ni sårbarheder (CVE-2012-1948, CVE-2012-1949, CVE-2012-1951 - CVE-2012-1954, CVE-2012-1959, CVE-2012-1962 og CVE-2012-1967). Flere af disse giver mulighed for ekstern afvikling af kode.

Apple udsendte den 25. juli version 6 af browseren Safari til Mac OS X. Den lukkede mere end 120 sikkerhedshuller, hvoraf de fleste var i det tilknyttede browserbibliotek WebKit. Der blev ikke samtidig udsendt en ny version af Safari til Windows, som derfor sandsynligvis stadig er sårbar. Det ser ud til, at Apple er holdt op med at markedsføre Windows-udgaven, men den gamle, sårbare version kan stadig hentes på firmaets websted.

Med Googles frigivelse af Chrome 21 den 31. juli blev der rettet i alt 15 sårbarheder. En sårbarhed (CVE-2012-2859), som kun var tilgængelig i Linux-versionen, blev vurderet som kritisk. Seks sårbarheder, hvoraf flere vedrørte visning af PDF-filer, fik Googles næsthøjeste risikovurdering.

Den 14. august udsendte Microsoft deres månedlige opdateringer, der fjernede i alt 26 sårbarheder. Opdateringer til Windows Common Controls (MS12-060), Internet Explorer (MS12-052), Remote Administration Protocol (MS12-054) og Remote Desktop Protocol under Windows XP (MS12-053) blev vurderet som kritiske og rettede i alt ni sårbarheder. Derudover rettede en kritisk opdatering (MS12-058) 13 sårbarheder i Exchange Server 2007 og 2010, der vedrører brugen af Oracles Outside In-produkt.

Adobe udgav den 21. august en opdatering (APSB12-19), der lukkede syv sårbarheder i Flash Player til alle platforme. Sårbarhederne (CVE-2012-4163 – 68 og CVE-2012-4171), hvoraf fem har højeste risikovurdering, kan udnyttes til at få det berørte system til at gå ned og potentielt eksekvering af kode.

Firefox 15 fra den 29. august indeholdt 17 opdateringer, som rettede i alt 33 sårbarheder i den tidligere version. Syv rettelser vurderes som kritiske og giver blandt andet mulighed for eksekvering af kode på det sårbare system. Med opdateringen rettes samtidig fejl i Thunderbird og Seamonkey.

I slutningen af august kunne man på flere blogs læse om en endnu ikke offentliggjort sårbarhed i Java, som blev udnyttet i mindre angreb. Den 28. august blev der observeret større angreb. Det blev konstateret, at sårbarheden (CVE-2012-4681) nu indgik i exploit kittet BlackHole.

Derfor anbefalede blandt andre vi, at man deaktiverede Java. Sårbarheden, der er risikovurderet som kritisk, kan udnyttes til afvikling af kode på det sårbare system. Den 30. august udsendte Oracle ekstraordinært Java version 7 update 7. Den rettede fire sårbarheder, heriblandt CVE-2012-4681. Siden kom det frem, at også den opdaterede version indeholdt en sårbarhed, der dog ikke var set udnyttet.

En opdatering af Chrome version 21 rettede den 30. august otte sårbarheder. Tre af sårbarhederne (CVE-2012-2866, CVE-2012-2869 og CVE-2012-2871) fik Googles næsthøjeste risikovurdering.

Den 6. september udsendte Apple en sikkerhedsrettelse til Mac OS X. Den fjernede en kritisk sårbarhed i Java 6. Sårbarheden (CVE-2012-4681) var den samme, som en uge tidligere var blevet opdateret til de øvrige platforme af Oracle.

En lille uge senere udsendte Apple den 12. august iTunes 10.7 til Windows. Den lukker 163 sårbarheder i programmets indbyggede browserkomponent, WebKit. Sårbarhederne kan medføre nedbrud af iTunes eller afvikling af skadelig kode.

Den 16. september offentliggjorde sikkerhedsforskeren Eric Romang fundet af et angrebsprogram, der udnyttede en hidtil ukendt sårbarhed i Internet Explorer 6, 7, 8 og 9. Programmet blev fundet på en server, der blev benyttet af samme bande, som cirka tre uger tidligere havde udnyttet en sårbarhed i Java. Programmet udnyttede sårbarheden gennem en Flash-fil indlejret på en HTML-side og medførte installation af programmer på den sårbare maskine.

Dagen efter udsendte Microsoft en advarsel om sårbarheden (CVE-2012-4969), der blev vurderet som kritisk. Derfor advarede den tyske regering og en række sikkerhedsorganisationer mod brugen af Internet Explorer, da man forventede angreb, der udnyttede sårbarheden. Den 19. september kom Microsoft med en midlertidig løsning på problemet i form af programmet Fix It. Den 21. september udsendte de en endelig opdatering af Internet Explorer, der rettede sårbarheden.

To dage før salget af iPhone 5 startede den 21. september, udsendte Apple telefonens styresystem iOS 6. Den nye version af iOS fjerner mere end 100 sårbarheder, hvoraf hovedparten findes i browserkomponenten WebKit. Samtidig udsendtes en ny version af browseren Safari, samt en række sikkerhedsrettelser til Mac OS X. Safari version 6.01 fjerner i alt 60 sårbarheder. Også her er de fleste i browserkomponenten WebKit. Sikkerhedsopdateringerne til Mac OS X fjerner 26 sårbarheder, hvoraf 15 ligger i tredjepartssoftware som Apache, BIND og PHP.

Den 21. september udgav ERP-producenten (Enterprise Ressource Planning) SAP en kritisk opdatering, som rettede i alt 27 sårbarheder. De to mest kritiske sårbarheder gav mulighed for afvikling af kode gennem RFC (Remote Function Call), mens ni sårbarheder var af typen cross-site scripting.

Google udsendte Chrome 22 den 25. september. Den nye version lukkede over 40 sikkerhedshuller, hvoraf et enkelt fik firmaets højeste risikovurdering.

I slutningen af september oplyste sikkerhedsfirmaet Security Explorations, at de havde fundet et alvorligt hul i alle versioner af Oracles Java. De frigiver ikke yderligere information, før Oracle har lukket hullet. Sikkerhedsforskeren bag opdagelsen mener, at fejlen kan rettes på en halv time. Oracle regner med at have en rettelse klar i februar 2013.

Den 4. oktober udsendte VMware rettelser til VMware vCenter Operations, CapacityIQ og Movie Decoder. Opdateringerne fjernede sårbarheder, der i nogle tilfælde gav mulighed for at afvikle programkode eller overtage en administrators session.

Adobe lukkede 25 sikkerhedshuller i Flash Player i starten af oktober. Samtidig udsendte Microsoft en rettelse, der lukkede hullerne i den Flash, som er indbygget i Windows 8. Et par dage senere kom Microsofts månedlige samling rettelser, denne gang med syv rettelser til i alt 20 sårbarheder.

Cisco lukkede den 10. oktober 12 sikkerhedshuller fordelt på ASA 5500 Adaptive Security Appliances og Catalyst 6500 ASA Services Module samt Cisco WebEx Recording Format player. Sårbarhederne gav angribere mulighed for at genstarte enheden eller afvikle programkode på den.

Den 16. oktober udsendte Oracle to samlinger af sikkerhedsrettelser. Den ene indeholdt 109 rettelser til en lang række af virksomhedens produkter. Den anden havde 30 rettelser til Java. 10 af de 30 fik firmaets højeste risikovurdering.

I juli udsendte softwarehuset Sybase rettelser til 12 sårbarheder, som sikkerhedsfirmaet TeamShatter havde opdaget. Men i slutningen af oktober offentliggjorde TeamShatter, at 10 af sårbarhederne fortsat kan udnyttes, selvom man har installeret rettelserne. Den 6. november lukkede Adobe syv alvorlige sikkerhedshuller i Flash Player. Ved samme lejlighed oplyste firmaet, at det fremover udsender rettelser til Flash Player på den anden tirsdag i måneden. Dermed følger de samme skema som Microsoft.

Novembers seks rettelser fra Microsoft lukkede 19 sikkerhedshuller. Blandt dem var de første rettelser til de nye styresystemer Windows 8 og RT. Derudover var der rettelser til Internet Explorer, Excel og IIS (Internet Information Services).

Apple udsendte QuickTime 7.7.3 til Windows i november. Den lukkede ni alvorlige sikkerhedshuller.

Mozilla udsendte Firefox 17 den 20. november. Den nye version

indeholdt 16 rettelser, der hver lukkede et eller flere sikkerhedshuller. Seks af dem fik firmaets højeste risikovurdering. De tilsvarende fejl i Thunderbird og Seamonkey blev også rettet.

Den 26. november advarede US-CERT om, at printere fra Samsung har en sårbarhed, som kan give uvedkommende kontrol over dem. Sårbarheden ligger i implementeringen af SNMP (Simple Network Management Protocol), og den er også til stede, selvom man slår SNMP fra. Samsung oplyste, at printere udsendt efter den 31. oktober ikke havde sårbarheden.

Den 11. december lukkede Adobe tre alvorlige sårbarheder i Flash Player til Windows, Macintosh og Linux. Sårbarhederne ramte også Adobe AIR.

Samme dag udsendte Microsoft december måneds syv sikkerheds-rettelser, der lukkede 12 huller. En af rettelserne viste sig senere at give problemer for nogle brugere, idet de ikke kunne bruge visse typer fonte. Rettelsen blev rettet med en ny version den 20. december.

Et hold sikkerhedsforskere offentliggjorde, at de havde fundet flere sårbarheder i fjernsyn fra Samsung. Sårbarhederne ligger i Smart-TV-funktionerne, der giver mulighed for at gå på nettet. Ved at udnytte sårbarhederne kunne forskerne få fat i filer og informationer.

Også smartphones fra Samsung var sårbare. En forsker opdagede, at det var muligt at få fuld adgang til alle data med privilegier som administrator (root). Det gjaldt for udstyr baseret på Exynos, som er Samsungs hardware-platform for en række smartphones og tablets.

Adobe, august 2012; "*Security updates available for Adobe Flash Player*".
Adobe, december 2012; "*Security updates available for Adobe Flash Player*".
Adobe, februar 2012; "*Security update available for Adobe Flash Player*".
Adobe, maj 2012; "*Security update available for Adobe Flash Player*".
Adobe, marts 2012; "*Security update available for Adobe Flash Player*".
Adobe, januar 2012; "*Security updates available for Adobe Reader and Acrobat*".
Adobe, juni 2012; "*Security update available for Adobe Flash Player*".
Adobe, november 2012; "*Security updates available for Adobe Flash Player*".
Adobe, oktober 2012; "*Security updates available for Adobe Flash Player*".
Apple, 2012; "*About the security content of iTunes 10.7*".
Apple, 2012; "*About the security content of Java for OS X 2012-005 and Java for Mac OS X 10.6 Update 10*".
Apple, 2012; "*About the security content of Java for OS X Lion 2012-002 and Java for Mac OS X 10.6 Update 7*".
Apple, 2012; "*About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004*".
Apple, 2012; "*About the security content of OS X Lion v10.7.3 and Security Update 2012-001*".
Apple, 2012; "*About the security content of OS X Lion v10.7.4 and Security Update 2012-002*".
Apple, 2012; "*About the security content of Safari 5.1.4*".
Apple, 2012; "*About the security content of Safari 5.1.7*".
Apple, 2012; "*About the security content of Safari 6*".
Apple, 2012; "*APPLE-SA-2012-09-19-1 iOS 6*".
Apple, 2012; "*APPLE-SA-2012-09-19-3 Safari 6.0.1*".
Carnegie Mellon University, 2012; "*Before we knew it*".
Cisco, 2012; "*Multiple Vulnerabilities in Cisco AnyConnect Secure Mobility Client*".
Cisco, 2012; "*Multiple vulnerabilities in Cisco ASA 5500 series adaptive security appliances and Cisco Catalyst 6500 series ASA services module*".
Cnet, 2012; "*German government tells public to stop using Internet Explorer*".
Computerworld, 2012; "*Apple patches Mac Java zero-day bug*".
DKCERT; "*DKCERT Sårbarhedsdatabase*".
Eric Romang, 2012; "*Zero-Day season is really not over yet*".
Erpscan, 2012; "*SAP critical patch update September 2012*".
FireEye, 2012; "*Java zero-day - first outbreak*".
FireEye, 2012; "*Zero-day season is not over yet*".
Google, 2012; "*Google Chrome releases*".
Google, 2012; "*Stable channel release*".
Microsoft, 2012; "*Microsoft security advisory (2757760)*".
Microsoft, 2012; "*Microsoft security advisory (2794220)*".
Microsoft, 2012; "*Microsoft security bulletin summary for april 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for august 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for december 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for july 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for june 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for march 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for may 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for november 2012*".
Microsoft, 2012; "*Microsoft security bulletin summary for october 2012*".
Microsoft, 2011; "*Microsoft security intelligence report volume 11*".
Microsoft, 2012; "*More information on security advisory 2757760's Fix It*".
Microsoft, 2012; "*MS12-063: Cumulative security update for Internet Explorer: September 21, 2012*".
Microsoft, 2012; "*Proof-of-Concept code available for MS12-020*".
Mozilla, 2012; "*Mozilla Foundation security advisories*".
Mozilla, 2012; "*Security Advisories for Firefox*".
National Institute of Standards and technology (NIST); "*CVE and CCE statistics query page*".
Oracle, 2012; "*April 2012 critical patch update released*".
Oracle, 2012; "*Oracle critical patch update advisory - april 2012*".
Oracle, 2012; "*Oracle critical patch update advisory - January 2012*".
Oracle, 2012; "*Oracle critical patch update advisory - July 2012*".
Oracle, 2012; "*Oracle critical patch update advisory - october 2012*".
Oracle, 2012; "*Oracle Java SE critical patch update advisory - february 2012*".
Oracle, 2012; "*Oracle Java SE critical patch update advisory - june 2012*".
Oracle, 2012; "*Oracle Java SE critical patch update advisory - october 2012*".
Oracle, 2012; "*Oracle security alert for CVE-2012-4681*".
Seclists, 2012; "*[SE-2012-01] New security issue affecting Java SE 7 Update 7*".
Security Explorations, 2012; "*Critical security issue affecting Java SE 5/6/7*".
Sophos, 2012; "*IE remote code execution vulnerability being actively exploited in the wild*".
TeamShatter, 2012; "*Sybase – Disclosed But Unpatched Vulnerabilities*".
The Register, 2012; "*Samsung's smart TVs 'wide open' to exploits*".
Websense, 2012; "*New Java 0-day added to Blackhole Exploit Kit*".
VMware, 2012; "*VMware vCenter Operations, CapacityIQ, and Movie Decoder security updates*".

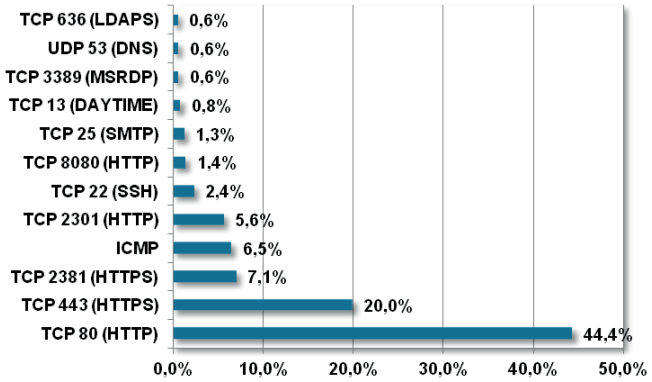
3.6. Sårbarhedsstatistik fra DKCERTs scanninger

Gennem året har DKCERT sikkerhedsscannet computere på danske universiteter og forskningsinstitutioner tilknyttet DeIC. Der blev udført 62 førstegangsscanninger.

Vi forsøgte at forbinde os til over 66.000 IP-adresser. Heraf kom der svar fra 3.421 adresser. De blev så udsat for en nærmere undersøgelse. Den viste, at der var sårbarheder på næsten hver fjerde computer, nemlig 826.

I alt fandt scanningerne frem til 7.795 sårbarheder. I gennemsnit var der 9,4 sårbarheder på hver sårbar IP-adresse. 19,6 procent af sårbarhederne blev risikovurderet højt, 67,8 procent udgjorde en mellemrisiko, mens 12,6 procent havde lav risiko. I gennemsnit blev der fundet en alvorlig sårbarhed på hver sårbar computer.

Der blev fundet sårbarheder på 78 forskellige porte/protokoller (Figur 15). Tre ud af fire sårbarheder lå i websystemer. Dermed svarer billedet til de internationale tendenser, hvor web-systemer tegner sig for en stadig større del af sårbarhederne.



Figur 15. Hyppigste sårbare porte konstateret ved scanning.

7,1 procent af sårbarhederne havde forbindelse til TCP-port 2381. Den anvendes af software til systemadministration fra HP. Samme software bruger også port 2301, som tegnede sig for 5,6 procent.

4. Artikler fra første kvartal

Du kan her læse eller genlæse vores artikler fra fø rste kvartals trendrapport. Artiklerne bidrager til at beskrive udviklingen af de trusler, vi som danskere prøvede at beskytte os mod i 2012. Men også hvordan det virkede at stå imod og i fællesskab ytre sin utilfredshed eller at holde på sin ret til egne persondata.

Kvartalet åbnede med protesterne mod et amerikansk lovforslag, som internetsamfundet så som både protektionistisk og bagstræverisk. Protesterne medførte, at lovforslaget blev trukket tilbage. I fortsættelse heraf fulgte protester mod den internationale handelsaftale ACTA, som Danmark underskrev den 26. januar.

Siden fulgte det hidtil største vellykkede angreb på en dansk netbank. Det fik igen debatten om NemID til at blusse op herhjemme. Netbankerne var dog ikke de eneste, der blev beskudt.

Også SCADA-industrisystemer viste sig sårbare. De havde tidligere været ramt af Stuxnet. I starten af året var der flere historier om sårbare SCADA-systemer, som ikke var designet til at være koblet til internettet.

Herhjemme lykkedes det en dansker at få medhold i en klage over Facebooks måde at håndtere gruppetilmeldinger på. Med lovgivningen i hånden viste han, at det kan betale sig at stå imod mastodonten, hvis den ikke følger spillereglerne.

Hacktivisme var en af årets tendenser i 2011. Flere tusinde samledes i aktioner mod alt, der havde antydning af censur og krænkelse af menneskerettigheder og ytringsfrihed. Samtidig stod globale virksomheder som mål for angreb, der havde til formål at udstille deres utilstrækkelighed, øjensynligt i det hellige grins navn. Tendensen fortsatte i første kvartal af 2012.

En væsentlig aktør var Anonymous-bevægelsen, som vi forsøgte at tegne et billede af. Det var ikke nemt, da der ikke er tale om en entydig og fasttømret gruppe. Et eksempel er den danske gruppe ”UN1M4TR1X0,” der i 2012 sprang på Anonymous-vognen.

4.1. Den internationale kamp mod piratkopiering

Sjældent har et amerikansk lovforslag givet anledning til så meget furore. Protesten mod SOPA medførte demonstrationer, underskriftindsamlinger, mørklægning af Wikipedia og hackerangreb mod FBI og Universal Music. Utilfredsheden med den internationale handelsaftale om bekæmpelse af forfalskning (ACTA) blev ikke mindre.

Den 26. oktober 2011 introducerede formanden for den juridiske komite under Repræsentanternes Hus i USA, Lamar Smith, lovforslaget Stop Online Piracy Act (SOPA). Lovforslaget var bakket op af en tværpolitisk gruppe bestående af 12 medlemmer af Repræsentanternes Hus. Det gav anledning til de mest omfattende og vidtrækkende protester ,vi hidtil har set. Siden er SOPA blevet trukket tilbage.

Lovforslaget var oprindeligt udfærdiget for at sikre amerikanernes intellektuelle rettigheder og omfattede mere end piratkopiering af film, musik og lignende. Det er dog bekæmpelsen af disse emner, der hovedsageligt nåede offentligheden.

Blandt de væsentligste kritikpunkter af SOPA var, at en internettjeneste kunne blive holdt juridisk ansvarlig for links til kopibeskyttet materiale, som var placeret af tjenestens brugere, og at rettighedshaverne selv kunne føre dom over en krænkende tjeneste. Det fik blandt andet Wikipedia, Reddit og Wordpress til den 18. januar 2012 at mørklægge deres tjenester.

Derudover samlede SOPA protester fra virksomheder som Mozilla, Facebook, Yahoo, eBay, American Express og Google. 130 erhvervsledere underskrev et brev til Kongressen, og tusinder samledes i fysiske demonstrationer rundt omkring i USA. Yderligere medførte lovforslaget DDoS-angreb mod blandt andet FBI og Universal Music, angiveligt udført af Anonymous-bevægelsen.

Som SOPA har også den internationale Anti-Counterfeiting Trade Agreement (ACTA) været udsat for kritik om at begrænse ytringsfriheden og krænke privatlivets fred. Kritikere af ACTA har kaldt den værre end SOPA. Blandt andet fordi den ikke kan ophæves og den forhandles uden offentlig indsigt. Modsat SOPA har kritikken derfor været baseret mere på spekulationer om betydningen i de lande, der tiltræder aftalen.

Stop Online Piracy Act (SOPA)

SOPA blev fremsat af Lamar Smith i Repræsentanternes Hus den 26. oktober 2011. Lovforslaget udvidede myndigheder og rettighedshaveres beføjelser til at gribe ind over for deling af og handel med ophavsretligt beskyttede værker og forfalskede produkter. De digitale rettighedsorganisationer i USA tog hurtigt lovforslaget til sig og gjorde det til et våben i kampen mod piratkopiering af film, musik og lignende.

Lovforslagets fulde titel er:

“To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes.”

I kølvandet på lovforslaget rejste sig en protest af hidtil usete dimensioner. Flere af internetindustriens mastodonter gik forrest, og lovforslaget er nu udskudt på ubestemt tid.

På trods af protester både herhjemme og i udlandet underskrev Danmark som et af 22 europæiske lande den 26. januar 2012 ACTA. Aftalen skulle træde i kraft fra juni 2012, forudsat at den blev vedtaget ved en afstemning i EU-parlamentet. Men her blev den nedstemt den 4. juli.

At protesterne mod ACTA først for alvor blussede op, efter at SOPA blev trukket tilbage, kan skyldes den lukkethed, hvormed aftalen er blevet

forhandlet. Som borger var man simpelthen ikke klar over aftalens eksistens, omfang og betydning, før den blev sammenstillet med den mere vidtrækkende SOPA. Måske gav den lukkede proces omkring forhandlingerne bagslag, da aftalen blev sammenstillet med SOPA.

Under alle omstændigheder har forløbene vist internettets styrke i en demokratisk sammenhæng. Internettet gjorde det muligt at informere og mobilisere folket i protester, som i omfang ikke tidligere er set. Det er nok ikke sidste gang, at vi ser internetsamfundet påvirke lokale og internationale beslutningsprocesser. I sidste ende er det vel demokrati i sin yderste konsekvens.

Anti-Counterfeiting Trade Agreement (ACTA)

ACTA er en multinational aftale om etablering af standarder for opretholdelse af intellektuelle rettigheder. Formålet er at etablere en international ramme til bekæmpelse af forfalskede varer, generiske lægemidler og krænkelse af ophavsretten på internettet. Aftalen er på mange områder blevet sidestillet med den amerikanske SOPA.

Aftalen blev oprindeligt underskrevet af Australien, Canada, Japan, Marokko, New Zealand, Singapore, Sydkorea og USA i oktober 2011. Den 26. januar 2012 tiltrådte Danmark sammen med 21 andre EU-lande ACTA, som – forudsat at den blev vedtaget i EU-parlamentet – ville træde i kraft fra juni 2012. Men den 4. juli blev aftalen nedstemt i parlamentet. 478 stemte imod, 39 stemte for, 165 undlod at stemme.

Betydningen af ACTA har der herhjemme været delte meninger om.

Forbes, 2012; *"SOPA, ACTA and the TPP: Lessons for a 21st century trade agenda"*.
Gizmodo, 2012; *"What is SOPA?"*.
Repræsentanternes Hus; 2011; *"Stop Online Piracy Act"*.
Version 2, 2012; *"SOPA er død: Lovforslag trukket"*.
Wikipedia; *"ACTA"*.
Wikipedia; *"Stop Online Piracy Act"*.

4.2. Angrebsprogrammer udnytter sårbare SCADA-systemer

Sårbarheder i en række udbredte industrikontrolsystemer er nu lette at udnytte for angribere. Der er sårbarheder i de systemer, der holder Holland tørt.

I januar offentliggjorde sikkerhedsforskere en række sårbarheder i udbredte industrikontrolsystemer. Det er it-systemer, der styrer og overvåger fysisk infrastruktur såsom vandforsyning, elforsyning og renseanlæg. Styringen sker gerne via computere, der kommunikerer med de PLC'er (Programmable Logic Controller), som for eksempel kontrollerer elektromekaniske motorer.

Men forskerne nøjedes ikke med at fortælle om sårbarhederne. I et samarbejde med firmaet Rapid7 udsendte de grydeklare angrebsmoduler til rammeværket Metasploit. Dermed kan enhver bruger af Metasploit bruge det til at foretage angreb på såkaldte SCADA-systemer (Supervisory Control And Data Acquisition).

Der er foreløbig udviklet moduler, som kan angribe udstyr fra General Electrics, Rockwell Automation, Schneider Modicon og Koyo/Direct LOGIC. Nogle af modulerne giver adgang til at fjernstyre systemerne, andre kan sætte dem ud af drift.

"Offentliggørelsen er med til at øge opmærksomheden på den trussel, hackerangreb udgør mod samfundets kritiske infrastruktur."

Offentliggørelsen er med til at øge opmærksomheden på den trussel, hackerangreb udgør mod samfundets kritiske infrastruktur. Samtidig er den også med til at gøre det lettere for hackere at udføre angreb.

Angreb på kritisk infrastruktur var senest i offentlighedens søgelys, da ormen Stuxnet hærgede i 2010. Det viste sig, at formålet med ormen var at sabotere iranske centrifuger, som blev brugt til landets atomprogram. Det gjorde ormen ved at ændre på programmeringen af industrikontrolsystemer fra Siemens.

I februar blev truslen mod SCADA-systemer nærværende for borgerne i Holland. Sikkerhedsforsker Oscar Kouroo opdagede, at en række kritiske infrastruktursystemer var registreret i databasen Shodan. Den gør det let at finde sårbare it-systemer.

Forskeren opdagede, at en angriber på den måde kunne styre de sluser og pumpestationer, der holder vandet bag digerne. I en tv-udsendelse demonstrerede han sårbarhederne på en mere uskadelig måde: Han loggede sig ind på systemet i Frelsens Hærs nationale hovedkvarter og skruede ned for varmen. En talskvinde for organisationen bekræftede, at der var blevet koldt på hovedkvarteret.

De hollandske systemer er ikke noget særsyn. I 2011 blev der rapporteret 215 sårbarheder i industrikontrolsystemer. Det er flere sårbarheder end i de foregående ti år lagt sammen. Og sikkerhedsforsker Sean McBride fra firmaet Critical Intelligence mener, at de offentliggjorte sårbarheder knap nok skraber overfladen på alle de sårbarheder, der reelt eksisterer.

Samtidig går udviklingen imod stadig større dataudveksling mellem it-systemer. Og medarbejderne får mobilt udstyr til at udføre deres arbejde. Det er med til at åbne for endnu flere mulige angrebsveje ind i de SCADA-systemer, hvis sikkerhed i forvejen ofte er mangelfuld.

Rapid7, 2012; *"New Metasploit module to exploit GE PLC SCADA devices"*.
Tofino Security, 2012; *"Cyber security nightmare in the netherlands"*.
Tofino Security, 2012; *"S4 SCADA security symposium takeaway: Time for a revolution"*.
Wikipedia; *"Stuxnet"*.

4.3. Netbank-kunder bestjålet ved real time phishing

I starten af februar blev otte netbank-kunder hos Danske Bank udsat for tyveri af næsten 700.000 kr. Forud for angrebet blev en større mængde brugere inficeret med den benyttede malware. Angrebet blev udført som real time phishing, mens brugerne var logget på deres netbank-konto.

Det er ikke første gang siden indførelsen af NemID, at det er lykkedes at misbruge danskeres netbank-konti. I september 2011 blev flere konti i Nordea misbrugt efter et phishing-angreb. I begge tilfælde er der tale om angreb, hvor kontoinformationer blev fisket i real tid, hvorefter der blev overført penge til udlandet. Her stopper ligheden dog også.

I det tidligere angreb blev informationerne opsnappet på en webside, der til forveksling lignede Nordeas netbank, efter at brugeren havde klikket på et link i en phishing-mail. Ved det seneste angreb blev informationerne fisket på brugerens computer, der var inficeret med malware.

Efter normal login på netbanken præsenterede malwaren brugerne for en falsk NemID-autentificeringsboks, som interagerede med NemID-løsningen. Herefter var der adgang til bruger-ID, adgangskode og talkoden fra NemID-nøglekortet.

"Den type malware er ikke ny, men det er første gang, vi har set den interagere med NemID-løsningen."

Den type malware er ikke ny, men det er første gang, vi har set den interagere med NemID-løsningen. Malwaren er kendt under navne som Enchanim, TROJ_GLUPINS og BankEasy.A. Koden kan spores tilbage til en bank-trojaner, der blev brugt mod spanske banker i november 2011. Den falske NemID-autentificeringsboks er en tilføjelse rettet specifikt mod danske netbank-kunder.

Når beløbet denne gang var så højt, skyldes det, at bagmændene forinden havde udvalgt sig de bedste konti at misbruge. Angrebet er et led i udviklingen af mere målrettede og avancerede angreb, hvor de it-kriminelle lægger tid, tanker og planlægning ind i processen og går målrettet efter de mest lukrative mål.

I ingen af tilfældene var det NemID, der blev kompromitteret. Angrebene lykkedes, fordi de berørte kunder ikke fulgte almindelig god sikkerhedspraksis. Det vil blandt andet sige at holde sine systemer opdaterede og ikke at reagere på mails, der angiver at komme fra banken og opfordrer til indtastning af kontooplysninger eller login. Det seneste angreb har dog været yderst vanskeligt at opdage for brugerne. Danske Bank valgte efterfølgende ekstraordinært at kompensere de berørte kunder for deres tab.

Selv om NemId har været under voldsom kritik, har det indtil videre været kunderne, som var det svageste led. NemId kan utvivlsomt blive bedre, men indtil videre må vi konstatere, at løsningen generelt har tilført mere brugervenlighed og sikkerhed til login på kritiske tjenester.

I kølvandet på de seneste angreb er der flere selskaber, der nu markedsfører en forsikring mod netbank-tyveri rettet mod små og mellemstore virksomheder.

Nets, 2012; "*Netbanksvindel ved brug af NemID*".
Version 2, 2012; "*Danske Bank: Vi har fortsat fuld tillid til NemID2*".
Version 2, 2012; "*Netbanktyve bryder gennem NemID igen: Stjæler 700.000*".

4.4. Klager over persondataretten kan betale sig

Det kan betale sig at klage over brud på persondataretten. Direktøren for den danske virksomhed Nensome ApS, Mikael Hertig, har efter en klage fået Facebook til at foretage ændringer, så brugere først fremstår som medlemmer af en gruppe, efter at de har accepteret invitationen til den.

Sådan har det ikke været før. Det positive udfald af klagen er et opløftende eksempel på, at det nytter at henvende sig til myndighederne for at få eksisterende retsregler respekteret, også når det gælder store internationale koncerner som for eksempel Facebook eller Google.

Mikael Hertig henvendte sig i marts 2011 til datatilsynet i Irland, hvor Facebooks europæiske hovedsæde er placeret. Han klagede over den måde gruppefunktionen i Facebook fungerer på, og henviste til, at en bruger kan melde sine Facebook-venner ind i en gruppe uden de pågældendes forudgående tilladelse. Faktisk er det den måde, folk typisk tilmeldes grupper på. Det fandt Mikael Hertig i strid med det danske persondatadirektivs artikel 7 og 8. Klagen indgik i en større revision af Facebook efter forhandlinger med den irske datamyndighed i samarbejde med EU.

"Forelagt hans klage har Facebook meddelt myn-dighederne, at det fra udgangen af marts 2012 ikke længere vil være muligt at fremstå som medlem af en gruppe uden brugerens godkendelse."

I december 2011 modtog Mikael Hertig svar fra det irske datatilsyn. Forelagt hans klage har Facebook meddelt myndighederne, at det fra udgangen af marts 2012 ikke længere vil være muligt at fremstå som medlem af en gruppe uden brugerens godkendelse. En bruger, som modtager en invitation til en gruppe, vil således først blive vist som medlem af gruppen, når vedkommende har besøgt den. På den måde foreligger der en slags samtykke, før medlemskabet er offentligt.

Ændringen skulle nu være trådt i kraft. Samtidig er der etableret en nemmere måde at forlade Facebook-grupper på.

Berlingske, 2012; "*Dansker får standset Facebook-fejl*".

4.5. Vi er Anonymous

Den tredje januar annoncerede Anonymous-bevægelsen #opeurope. Siden har den blandt andet proklameret nye angreb hver fredag. Hvad der startede som elektronisk mobning på et af internettets mørkere afkroge, har udviklet sig til hvad der ligner en global protestbevægelse.

Oprettelsen af 4chan i 2003 blev startskuddet for organiseringen af en række unge mænd i et løst sammenknyttet anarkistisk netværk. Den fælles interesse var internettet og de bizarre indslag, der trives på 4chan. Et bulletin board uden regler, hvor alle benytter det fælles navn Anonymous og indhold og logfiler ikke gemmes i mere end 24 timer.

Med det hånlige grin som gevinst blev 4chan udgangspunktet for drillerier, som havde til formål at udstille og latterliggøre personer, der tog sig selv for højtideligt. Man fungerede som en internettets hånende jantelov, der i mange tilfælde tog overhånd. For eksempel fik en 11-årig pige i 2010 politibeskyttelse, efter at brugere af 4chan havde offentliggjort hendes adresseoplysninger på internettet og sendt hende mordtrusler.

4chan var også udgangspunkt for mere kuriøse indslag som fænomenet "Rickrolling" fra 2007. Joken var at få folk til at klikke på links, der førte til en video med Rick Astley-sangen "Never Gonna Give You Up". Fænomenet spredte sig til den fysiske verden, og sangen indgik som fast indslag ved de senere protester mod Scientology.

I januar 2008 optrådte Tom Cruise i et interview produceret af Scientology på YouTube. Det blev startskuddet for Anonymous. Brugere på 4chan fandt videoklippet og Scientologys senere forsøg på at fjerne det fra internettet latterlige.

Som en protest mod censur og for at latterliggøre en organisation, der var 4chans diametrale modsætning, besluttede de cirka 200 brugere i et chatforum at iværksætte et DDoS-angreb mod Scientologys webside. Som svar blev der produceret et videoklip med Anonymous som afsender. Den blev afsluttet med sætningen:

"We are legion. We do not forgive. We do not forget. Expect us."

Den 10. februar 2008 deltog tusinder i protester arrangeret af Anonymous foran Scientologys hovedkvarterer i 142 byer over hele verden. Siden har protesten mod Scientology udmøntet sig i websiden WhyWeProtest, som samler de fysiske protester for menneskerettigheder og mod censur. Den er blevet et centralt sted for kampen mod blandt andet Scientology, ACTA og for demokrati i mellemøsten.

I 2010 kom "blåstemplingen" af den politiske del af Anonymous. Først ved et DDoS-angreb mod sammenslutninger af amerikanske rettighedshavere efter anklager om, at de havde udført tilsvarende angreb på fildelingstjenesten The Pirate Bay. Siden da de udførte DDoS-angreb på Paypal og Mastercard efter blokeringen af pengeoverførelser til Wikileaks. Her deltog angiveligt mere end 6.000 mennesker efter opfordringer på 4chan.

Det er Davids kamp mod Goliat, hvor en væsentlig faktor er muligheden for at udstille de bedrevidende og selvhøjtidelige magthavere og -udøvere. Den hånligt grinende Guy Fawkes-maske, som også benyttes af Occupy-bevægelsen, er blevet symbolet for Anonymous. De hånende grin (Lulz) er dog nu i mindre grad motivationsfaktoren. Som reaktion på det dannedes i 2011 hackergruppen LulzSec. Efterfølgende er fulgt en række angreb, som har fået massiv medieomtale.

Bevægelsens metoder spænder over digital chikane, defacement, hacking samt DDoS-angreb. Målene har været alt fra tilfældige individer, pædofile, Scientology, den katolske kirke, myndigheder, politiske partier, sikkerhedsorganisationer og private virksomheder i alle brancher. Enhver med en "sag" kan udføre angreb og tilskrive det Anonymous. Eller som Impervas sikkerhedsdirektør Rob Rachwald udtaler:

"Who is Anonymous? Anyone can use the Anonymous umbrella to hack anyone at anytime."

Anonymous kan ikke afskrives som en flok utilpassede teenagedrenge, der lever deres sociale liv på internettet og udfolder det gennem mere eller mindre perfide jokes. Spørgsmålet er heller ikke, hvorvidt Anonymous er aktivister, frihedskæmpere, terrorister eller balladamagere og hærværksmænd. Svaret er nemlig, at de på samme tid er det hele og ingen af dem.

Fra et kommunikationssynspunkt er det både bevægelsens svaghed og styrke. De forskelligartede angreb gør holdningerne og budskaberne uklare, hvilket forstærkes ved manglen på en veldefineret afsender. Omvendt gør det truslen for angreb mere latent og skræmmende, når vi ikke ved hvorfra den kommer. Om end mål og metoder er anderledes, er frygten for Anonymous ligeså nærværende som frygten for Al-Qaeda, for som bevægelsen har udtalt:

"You can't cut off the head of a headless snake."

Anholdelsen den 6. marts af seks medlemmer af LulzSec medførte et Anonymous-angreb på mere end 30 subdomæner hos Panda Security. Det skete som reaktion på en medarbejders blogindlæg med titlen "Where is the Lulz now?" Blandt de anholdte var lederen "Sabu", som gennem længere tid havde samarbejdet med FBI.

Har vi så grund til at frygte Anonymous? Svaret er både ja og nej. Så længe vi herhjemme har globalt fokus på menneskerettigheder og opretholdelsen af de demokratiske principper, er der nok ikke den store risiko for, at vi påkalder os de oprindelige Anonymousers vrede. Derimod er risikoen for at danske interesser kan blive mål for skaren af sympatisører steget, da de nu kan "legitimere" deres aktiviteter under Anonymous-fanen. For som forfatteren Cole Stryker udtaler:

"Anonymous is a handful of geniuses surrounded by a legion of idiots."

#OpEurope

Den tredje januar lagde Anonymous-bevægelsen en video på YouTube, der med vanlig maskinstemme annoncerede starten på Operation Europe. Operationen ville have europæiske skoler, universiteter og myndigheder som mål. I videoen fortælles blandt andet:

"We will publish e-mails and data to prove that there is corruption in Europe."

Med videoen fulgte offentliggørelse af login-data til en skole i Østrig. Siden har der været stille om #OpEurope.

Anonymous-angreb i 2012

19/1. DDoS mod bl.a. FBI og Universal Music som protest mod SOPA/PIPA og lukningen af MegaUpload.
27/1. Copyrightalliance.org blev gjort utilgængelig som protest mod ACTA.
30/1. Defacement af politikeren Morten Messerschmidts (DF) hjemmeside som protest mod ACTA.
3/2. Angreb mod Salt Lake City Police, Boston Police og Texas Police som protest mod et anti-graffiti-lovforslag, anklager om politibrutalitet og en betjent der blev undersøgt i forbindelse med børnepornografi.
3/2. Aflytning af telefonmøde mellem FBI og Scotland Yard-medarbejdere.
3/2. Hacking af advokatfirmaet Puckett & Faraj, som forsvarer amerikanske soldater anklaget for overgreb på civile i Irak.
8/2. Kompromittering og offentliggørelse af kildekode fra Symantec.
8/2. Kompromittering og offentliggørelse af data fra Syriens Ministry of Presidential Affairs som protest mod styret.
10/2. DDoS-angreb mod CIA gjorde deres webside utilgængelig.
29/2. Kompromittering og offentliggørelse af data fra Patent- og Varemærkestyrelsen som protest mod ACTA.
29/2. DDoS-angreb på Interpols hjemmeside efter anholdelse af 25 personer der menes at have tilknytning til Anonymous-bevægelsen.
6/3. Kompromittering og offentliggørelse af data fra Panda Security efter arrestation af seks medlemmer af LulzSec.

New York Times, 2012; "*In attack on Vatican web site, a glimpse of hackers' tactics*".
New York Times, 2012; "*One on one: Cole Stryker, author of 'Epic win for Anonymous'*".
Pastebin, 2012; "Anonymous - #opeurope".
Securityweek, 2012; "*Following LulzSec arrests, AntiSec supporters attack Panda Security*".
The Huffington Post, 2012; "*Anonymous and the war over the internet*".
The Huffington Post, 2012; "*Anonymous and the war over the internet (Part II)*".
Urlesque, 2010; "*The Jessi Slaughter scandal - An unbalanced 11-year-old girl's ongoing fight with internet trolls*".
Wired, 2009; "*The assclown offensive: How to enrage the Church of Scientology*".
Wired, 2012; "*Anonymous promises regularly scheduled friday attacks*".

4.6. Danske medier ramt af hackerangreb

Den 28. marts skaffede en dansk hacktivist-gruppe sig adgang til 18 FTP-servere tilhørende danske nyhedssider. Gruppen "UN1M4TR1X0" der står bag angrebet, beskriver sig selv som en del af Anonymous-bevægelsen.

Angrebet skete ved udnyttelse af en SQL-injection sårbarhed på en server hos mediebureauet Ritzau. Herfra fik man adgang til oplysninger om FTP-servere tilhørende en række danske medier. Peter Kruse fra CSIS udtalte sig efterfølgende.

"*Der er tale om et angreb, der rammer næsten alle de store medier i Danmark*".

Angrebet kompromitterede ikke umiddelbart følsomme data hos de berørte medier ud over de publicerede FTP-konti. Potentielt kunne oplysningerne benyttes til upload af materiale på de berørte servere. Herved var der mulighed for ændring af tekst og billeder.

Angrebet skete ifølge gruppen selv som et led i kampen mod korruption, uretfærdighed og censur. På traditionel Anonymous-vis blev der lagt en video på YouTube og de kompromitterede FTP-adgange blev publiceret på Pastebin.

I en meddelelse om angrebet på Pastebin beskriver den nystartede hacktivist-gruppe sig som en del af Anonymous-bevægelsen. Dermed tilhører den en voksende skare af aktivister, som tilskriver deres handlinger Anonymous-bevægelsen uden anden relation end et muligt meningsfællesskab.

Angiveligt er det ikke det sidste, vi har hørt til "UN1M4TR1X0". I meddelelsen skriver de yderligere:

"*Vi vil over de næste par måneder offentliggøre og synliggøre alt fra politikeres korruption, til religiøse sekters magtmisbrug.*"

Den samme gruppe stod angiveligt bag kompromittering af Patent- og Varemærkestyrelsens systemer den 29. februar. Herfra lækkede de information om 17.000 brugerprofiler. Ifølge gruppen skete offentliggørelsen her for at vise sympati med de danskere, der weekenden inden havde demonstreret imod ACTA.

Computerworld, 2012; "*Flere danske medier ramt af stort hackerangreb*".
Pastebin, 2012; "*Untitled*".
Politiken, 2012; "*Hackere stjæler flere hundrede danskeres passwords*".

5. Artikler fra andet kvartal

Heller ikke i andet kvartal blev vi forskånet for malware. Denne gang var det den trojanske hest Flame, som ramte mediernes overskrifter. Ligesom Stuxnet var Flame sandsynligvis udviklet for eller af den amerikanske stat. Denne gang med det formål at opsamle informationer fra de inficerede systemer. Det bemærkelsesværdige var, at den tilsyneladende havde huseret i mere end to år uden at blive opdaget.

I starten af juni måned fortalte den sociale netværkstjeneste LinkedIn, at en fil med 6,5 millioner passwords til tjenesten var blevet lækket. Skaden var dog umiddelbart ikke så stor. For eksempel indeholdt filen ikke de tilhørende brugernavne.

Omvendt måtte hosting-leverandøren Surftown senere på måneden afvise en mistanke om, at deres bagvedliggende systemer var kompromitteret. Surftown øgede sikkerheden, men kunne med fordel også have kigget på, hvordan udbyderne af cloud-tjenester har øget transparensen af deres tjenester.

Malware til Android-smartphones var i eksplosiv vækst. Udviklingen lignede den, vi tidligere har set til både Windows og Macintosh. Mængden af enheder der benytter platformen og tilgængeligheden af udviklingsværktøjer betød, at den var blevet interessant for de internetkriminelle.

"... samfundets brug af informationsteknologi er under stadig udvikling og hermed også de trusler, vi står over for."

Historierne fra andet kvartal er tilsammen med til at skitsere, hvordan samfundets brug af informationsteknologi er under stadig udvikling og hermed også de trusler, vi står over for. Et stigende krav om digitalisering medfører samtidig, at vi digitaliserer aktiver, som også har værdi for andre end os selv. Det stiller nye krav til lovgivningen og de måder, vi gør tingene på.

5.1. Danske myndigheder under angreb

Den 26. april varslede GovCERT de statslige organisationer om, at et ministeriums installationer var blevet kompromitteret, og man forventede yderligere angreb på danske myndigheder. Siden ramte historien pressen, og den 30. april fortalte GovCERT og Statens It, at angrebene nu var imødegået. Men hvad der egentlig skete, står stadig uklart for offentligheden.

Om eftermiddagen den 26. april konstaterede den statslige varslingstjeneste GovCERT et indbrud i et it-system hos en styrelse under Erhvervs- og Vækstministeriet. Indbruddet var af en sådan karakter, at man forventede yderligere angreb på andre myndigheder. Herefter udsendte GovCERT en advarsel til de statslige organisationer, hvori man opfordrede til skærpet opmærksomhed og logning.

Dagen efter ramte historien medierne, og GovCert advarede igen de statslige organisationer. Denne gang indeholdt advarslen oplysninger om tre udenlandske IP-adresser, som angiveligt havde relation til hændelserne. Siden er det kommet frem, at Sikkerhedsstyrelsen, Søfartsstyrelsen og Erhvervsstyrelsen alle blev ramt af angrebet og i større eller mindre grad havde været nødsaget til at lukke deres systemer ned.

Den 30. april kom den officielle udmelding fra henholdsvis GovCERT og Statens IT. Tre styrelser under Erhvervsministeriet havde været udsat for angrebet, som nu var blevet inddæmmet. Hændelsen var blevet politianmeldt, og man havde blandt andet iværksat øget overvågning af de statslige systemer. Derudover understregede GovCERT sine tidligere anbefalinger om:

"... at der er aktiveret logning på alle it-systemer."

Tilbage står en række ubesvarede spørgsmål om hvem, hvad og hvorfor. Hvorvidt angrebene har relation til Anonymous-bevægelsens tidligere trusler mod blandt andet danske myndigheder, står derfor hen i det uvisse. Det er således ikke muligt at vurdere, om der var tale om en enkeltstående hændelse, eller den skal tages som udtryk for en generel større trussel mod danske interesser.

"Tilbage står en række ubesvarede spørgsmål om hvem, hvad og hvorfor."

Selvfølgelig er det ikke muligt at informere i detaljer, da hændelsen er blevet politianmeldt og til dels vedrører rigets sikkerhed. Information kan dog have værdi ved risikovurdering på de øvrige danske installationer. Organisationer ud over de berørte har således ingen mulighed for at drage nytte af de erfaringer, der blev gjort i forhold til risikovurdering, fremtidig sikring, beredskab, korrigerende handlinger med mere.

Govcert, 2012; "*Angreb på Erhvervs- og Vækstministeriet*".
Statens it, 2012; "*Erhvervs- og Vækstministeriet angrebet af hackere*".
Version 2, 2012; "*GovCERT slår alarm: Advarer alle ministerier mod hackerangreb*".
Version 2, 2012; "*Hackerangreb lammer ministerium*".
Version 2, 2012; "*Hackerangreb plager ministerium på 4. døgn*".

5.2. Nye muligheder for brug af cloud-tjenester i det offentlige

Tidligere har brug af tjenester i skyen stort set været forbeholdt private virksomheder, der ikke behandlede og lagrede personfølsomme oplysninger i tjenesterne. Blandt de springende punkter har været usikkerhed om, hvor og hvordan data blev lagret. Fra flere kanter ser der nu ud til at være en opblødning undervejs.

Den 28. maj annoncerede Google, at deres cloudbaserede kontorpakke til erhvervslivet var blevet certificeret efter ISO 27001-standarden. Dermed trådte Google Apps for Business et væsentligt skridt nærmere at blive benyttet af danske organisationer og myndigheder.

Også Microsoft har underkastet sig standarden for deres cloudbaserede kontorpakke Office 365. De har forpligtet sig til at lade sikkerheden i selve løsningen og i datacentrene underkaste audit (revision), som udføres i overensstemmelse med ISO 27001. Blandt andet derfor har Datatilsynet delvist åbnet for, at myndigheder og virksomheder herhjemme kan bruge Office 365. Også når det gælder personfølsomme oplysninger.

For begge tjenester gælder, at man nu har mulighed for at sikre sig, at behandlingen af persondata følger EU's regler. Hos både Google og Microsoft kan man underskrive kontrakter, der opfylder EU-Kommissionens krav til databehandlere. Ved at følge EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til en databehandler i et tredjeland er de første spadestik taget til brug af cloudbaserede tjenester i det offentlige.

Med Datatilsynets behandling af Microsoft Office 365 er det blevet mere gennemskueligt, hvad der kræves, før man kan bruge tjenester placeret i skyen. I kombination med et stigende marked for cloudbaserede løsninger, der overholder EU-Kommissionens kontraktkrav, kan det være med til at skubbe flere offentlige tjenester ud i skyen.

På længere sigt vil det være til gavn for ikke bare økonomien og miljøet, men også for sikkerheden. For som Director of Security i Google, Eran Feigenbaum, udtalte i forbindelse med certificeringen af Google Apps for Business:

"... businesses are beginning to realize that companies like Google can invest in security at a scale that's difficult for many businesses to achieve on their own."

Datatilsynet, 2012; *"Behandling af personoplysninger i cloud-løsningen Office 365"*.
Digitaliseringsstyrelsen, 2011; *"Cloud computing og de juridiske rammer"*.
Google, 2012; *"Google Apps receives ISO 27001 certification"*.
Version 2, 2012; *"Google på vej til at fjerne EU-barriere for Google Apps til danske myndigheder"*.

5.3. Fornyet kritik af logningsbekendtgørelsen

Ved angrebet på tre styrelser under Erhvervs- og Vækstministeriet i april lød rådet fra GovCERT blandt andet, at man aktiverede og skærpede logningen. På politisk plan er der ønske om det modsatte: En lempelse af logningsbekendtgørelsen. Argumentet er, at loggede data kun sjældent bliver brugt.

Det er ikke ualmindeligt, at afdækningen af en sikkerhedshændelse stopper ved, at der ikke er foretaget tilstrækkelig logning. For eksempel i tilfælde, hvor IP-adressen på en malware-inficeret computer peger på en NAT-adresse, et WI-FI- hotspot eller lignende, oplever vi ofte, at det ikke er muligt at opspore og rense den inficerede computer.

På virksomhedsniveau er der generelt forståelse for at, logning er nødvendig. Både i forhold til gældende standarder som for eksempel ISO 27001 og i forhold til afklaring og dokumentation af sikkerhedshændelser. Med den lovpligtige logning af tele- og internettrafik forholder det sig dog anderledes. De virksomheder, der står med den administrative og økonomiske byrde, har ikke selv nogen interesse i loggen.

Derfor er der fra flere sider herhjemme sat spørgsmålstegn ved, om logningsdirektivet er blevet overimplementeret i forhold til EU's retningslinjer. For eksempel fik en opgørelse, der viste, at politiet havde efterspurgt internetoplysningerne 170 gange i 2010, politikere fra både Enhedslisten og Venstre til at udtale, at de ville stille beslutningsforslag om helt at afskaffe sessionslogningerne.

Forslag om en eventuel lempelse af logningsbekendtgørelsen tager primært udgangspunkt i antallet af gange, politiet har benyttet logfilerne. Der stilles således ikke spørgsmål til, om de kunne være benyttet mere og hvorfor de eventuelt ikke blev det, eller hvordan det eventuelt kan se ud i fremtiden.

Ud over at afskaffelsen af sessionslogning kan være et dårligt signal at sende til organisationerne, kan der i fremtiden vise sig at være større behov for dem, end der er i dag. For eksempel udtalte politiinspektør Magnus Andresen til avisen Information om en stigende mængde data og tjenester placeret i skyen:

"Det kunne gøre, at man i fremtiden fik et større behov for analyse af sessionslogninger."

Tilbage står, at logning er et centralt element i forhold til sikkerhedsarbejdet. I forbindelse med en sikkerhedshændelse er loggen ofte det eneste sted at finde svar på spørgsmål om, hvad der skete. De svar kan være med til at forhindre fremtidige hændelser. Det blev delvist illustreret ved aprils angreb på styrelser under Erhvervs- og Vækstministeriet, hvor GovCERT rådede til, at man aktiverede og skærpede logningen.

På trods af et bredt politisk ønske om ændring af logningsbekendtgørelsen kunne dronning Margrethe den 18. juni underskrive en lovændring, der udsatte revisionen af bekendtgørelsen til folketingsåret 2012-13.

Information, 2012; *"Størstedelen af internet-logningen kan sløjfes"*.
Retsinformation, 2012; *"Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige"*.
Version 2, 2012; *"Massiv logning af danskernes internetbrug - men politiet bruger kun IP-adressen"*.

5.4. Flame – malware som spionageværktøj

I slutningen af maj fortalte flere kilder om et nyopdaget skadeligt program. Nogle kaldte det Flame, andre Flamer, SkyWiper eller Wiper. FN-organet ITU (den internationale teleunion) havde hyret sikkerhedsfirmaet Kaspersky Lab til at undersøge et angreb, som var gået ud over computere hos Irans olieministerium. Angrebet førte i april til, at Iran koblede flere olieterminalers netværk fra internettet. Kaspersky Lab fandt frem til programmet, de kaldte Flame.

Med en samlet størrelse på omkring 20 megabyte er Flame langt større end typiske eksempler på malware. Programmet ser ud til at være skrevet til at udføre målrettet spionage. Ifølge avisen Washington Post er Flame udviklet af USA og Israel med det formål at forsinke Irans atomprogram. Avisen citerer unavngivne kilder for, at Flame blev brugt til at indsamle information.

Hvis det er korrekt, kan den indsamlede information senere have været brugt i et sabotageangreb, hvor ormen Stuxnet saboterede centrifuger, der blev brugt i atomprogrammet. Kaspersky Lab har fundet fælles programkode i Flame og Stuxnet.

Teknisk set er Flame interessant ved, at den udnytter en hidtil ukendt form for kryptografisk kollisionsangreb på MD5-algoritmen. Det gør det muligt for bagmændene at udarbejde et certifikat, der ser ud til at være udstedt af Microsoft. Med dette certifikat stemplede de dele af programkoden. Derved blev det muligt at få det skadelige program installeret via Windows Update-funktionen, da programmet så ud til at være signeret af Microsoft. Microsoft udsendte 3. juni en sikkerheds-advarsel og tog flere skridt til at forhindre, at tricket kunne gentages.

"Trods den megen omtale udgør Flame ikke nogen fare for hovedparten af de danske netbrugere."

Trods den megen omtale udgør Flame ikke nogen fare for hovedparten af de danske netbrugere. Det skyldes, at programmet er beregnet til målrettede spionageangreb. Derfor er det ikke særlig udbredt – Kaspersky Lab anslog i maj, at kun 1.000 computere på verdensplan var inficeret.

Derimod er Flame væsentlig som et eksempel på, hvordan skadelige programmer nu indgår i værktøjskassen hos militær og efterretnings-væsener i jagten på fortrolige informationer.

Centrum Wiskunde & Informatica, 2012; "*CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*".
Kaspersky lab, 2012; "*Back to Stuxnet: the missing link*".
Microsoft, 2012; "*Microsoft releases Security Advisory 2718704*".
New York Times, 2012; "*Facing cyberattack, Iranian officials disconnect some oil terminals from internet*".
Washington Post, 2012; "*U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*".
Wikipedia, 2012; "*Flame (malware)*".

5.5. 6,5 millioner passwords til LinkedIn blev lækket

"Our team is currently looking into reports of stolen passwords. Stay tuned for more."

Sådan lød en Twitter-besked fra det sociale netværk LinkedIn den 6. juni. I tiden derefter viste det sig, at rygterne holdt stik: På et russisk websted var der placeret filer med i alt 6,5 millioner passwords til LinkedIn.

Passwordene var lagret i form af hashværdier. Man kunne altså ikke direkte læse de enkelte passwords. Men hvis man gættede sig til et password, kunne man se, om det fandtes på listen. Ifølge sikkerhedsfirmaet Sophos blev 60 procent af passwordene gættet i løbet af det første døgn.

Filerne indeholdt ikke de brugernavne, som hørte til de berørte passwords. LinkedIn nulstillede passwords for de konti, hvis passwords befandt sig på listen. Firmaet oplyser, at det ikke har hørt fra brugere, hvis konti er blevet kompromitteret som følge af offentliggørelsen.

Ifølge et blogindlæg fra direktør Vicente Silveira, LinkedIn, havde firmaet i nogen tid arbejdet på at forbedre sikkerheden. Således var der allerede før offentliggørelsen indført et system, hvor passwords ikke kun beskyttes med en hash-funktion. Nu bliver der også tilføjet et såkaldt salt. Det gør det vanskeligere at finde frem til, hvilket password der gemmer sig bag en hashværdi. Det ser altså ud til, at de offentliggjorte passwords ikke var helt nye.

Affæren illustrerer både styrker og svagheder ved autentificering baseret på passwords. Hvis man har et stærkt password, vil det være vanskeligt at knække. Men man risikerer, at webtjenester lagrer ens password på en måde, der gør styrken ligegyldig: Hvis et password er gemt i klartekst, er det ligegyldigt hvor stærkt det er, hvis hackere får fat i det.

Derfor er det vigtigt, at man ikke genbruger passwords på tværs af tjenester. Hvis man har brugt et unikt password til sin LinkedIn-konto, tager det ikke mange sekunder at skifte til et nyt. Men hvis man har gen-brugt det samme password til en række andre tjenester, vil det være en større opgave at logge ind på dem alle og ændre password.

LinkedIn, 2012; "*An update on taking steps to protect our members*".
Sophos, 2012; "*LinkedIn confirms hack, over 60% of stolen passwords already cracked*".
Twitter, 2012; "*LinkedIn*".

5.6. Balladen om Surftown

I juni måned satte Version 2 gentagne gange spørgsmålstegn ved sikkerheden på Surftowns webhotel-løsninger. Surftown afviste kritikken og øgede sikkerheden. Sagen rummer dog nogle generelle aspekter om, hvad vi som kunder kan forvente af vores leverandører og hvordan det kommunikeres.

Rene Madsen fra Online Marketing udtalte den 20. juni til nyhedssitet Version 2, at han havde oplevet flere hackede hjemmesider på samme IP-adresse. Problemet var ikke specifikt for Surftown, det var blot det seneste tilfælde. Hans konklusion var, at angrebet var sket gennem en root-adgang til webhotellets underliggende systemer. Det blev afvist af Kresten Bach Søndergaard, der er kommunikationschef hos Surftown.

En uges tid efter kunne Surftown gentage afvisningen. Man havde nu undersøgt, om der var hold i anklagerne og var i gang med at kigge på logfiler. På baggrund af anklagerne hævede Surftown på nogle områder sikkerheden og forbedrede overvågningen.

Dagen efter kunne Version 2 fortælle, at der også havde været lækket lister med brugernavne og passwords til PHPmyadmin hos Surftown. Det blev fejlagtigt tolket som, at den oprindelige anklage måtte være sand. Ved en senere opdatering af artiklen viste det sig, at det kun drejede sig om en enkelt kundes databaseadgang med PHPmyadmin.

I den aktuelle sag har Surftown afvist alle anklager og kan herefter henvise deres kunder til aftaleteksten for deres webhotelløsninger:

"Surftown påtager sig i øvrigt intet ansvar for uvedkommendes overvågning eller opsamling af eller adgang til kundens trafik eller data."

I samme aftale fraskriver Surftown sig ansvaret for kundernes eventuelle tab:

"... medmindre Surftown har handlet forsætligt til skade for Kunden eller groft uagtsomt."

"Selv om Surftown har handlet ansvarsfuldt, og der ikke har været et problem på deres ydelser, står kunderne tilbage med tvivlen."

Den manglende dialog og totale ansvarsfraskrivelse er måske det store problem i denne sag. Selv om Surftown har handlet ansvarsfuldt, og der ikke har været et problem på deres ydelser, står kunderne tilbage med tvivlen.

Problemet er, at kunderne ikke kan gennemskue, hvilken sikkerhed de får af leverandøren, og hvad der er deres eget ansvar. Et væsentligt punkt er udformningen af aftalerne, hvor leverandøren bør beskrive deres ansvar, og hvad de gør for at leve op til det. Her kunne man lære af for eksempel cloud-leverandørerne, som på mange områder er i gang med at standardisere deres tjenester. Som her bør den enkelte hosting-udbyder kunne tilbyde sikkerhed, der overgår den enkelte kundes muligheder, da der for alle kunder er tale om samme standardiserede produkt.

Den nyligt stiftede Brancheforening for IT-hostingvirksomheder i Danmark (BFIH) ser ud til at være et skridt i den retning. Den arbejder for at højne kvalitets- og sikkerhedsniveauet på hosting-ydelser samt gøre det lettere at gennemskue og sammenligne ydelsernes kvalitet og sikkerhed. Et væsentligt aspekt af det arbejde hedder standardisering og certificering.

Vi har tidligere været efter hosting-udbyderne for ikke i tilstrækkelig grad at tage vare på kundernes sikkerhed. Vores kritik har primært været rettet mod, hvorvidt og hvor hurtigt der blev reageret, når vi havde konstateret en sikkerhedshændelse. Vores generelle indtryk er, at vi er på vej i den rigtige retning. Vi har i den periode, hvor kritikken af Surftown har været rejst, ikke kunnet konstatere flere hændelser end normalt vedrørende phishing-sider og malware hos Surftowns kunder.

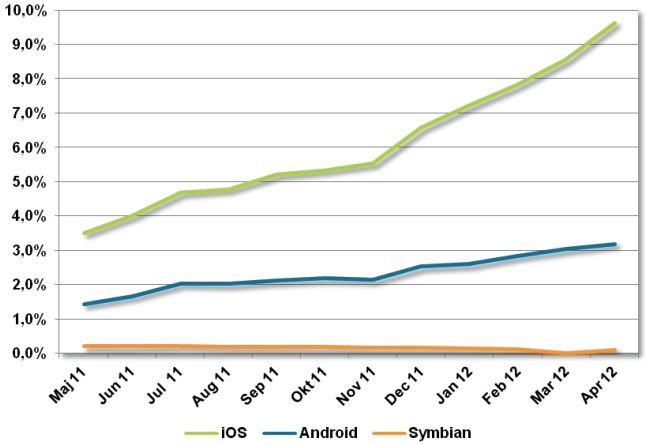
Brancheforeningen for IT-hostingvirksomheder i Danmark (BFIH), 2012; *"Om BFIH"*.
Version 2, 2012; *"Password til Surftown-konto lækket af Anonymous - i marts"*.
Version 2, 2012; *"Mystiske hackerangreb hos Surftown-kunder: Hvordan kommer de ind?"*.
Version 2, 2012; *"Surftown afviser definitivt interne hackerangreb - men hæver sikkerheden"*.

5.7. Android – historien der gentager sig

Gennem det seneste år er brugen af bærbare enheder mere end fordoblet. Næsten 13 procent af de danske websider som danskerne kiggede på i april, blev set fra en mobiltelefon eller tavle-pc. Det har betydet, at særligt Android er blevet mål for malware. Det er der mange forklaringer på, og udviklingen ligner noget, vi har set før.

Apples iPhone og iPad, der begge benytter styresystemet iOS, stod ifølge Foreningen af Danske Interaktive Medier (FDIM) for 9,6 procent af de danske sidevisninger i april 2012. De forskellige enheder, der benytter Android, stod for 3,2 procent (Figur 16). Selv om udbredelsen og brugen af Android ikke overgår iOS, er der herhjemme sket en fordobling i antallet af danskernes visninger af websider fra danske medier gennem perioden maj 2011 til april 2012.

Mens iOS stort set har været forskånet for malware, eksploderer mængden af skadelig kode til Android. Således modtog F-Secure i første kvartal 2012 i alt 3.063 skadelige Android-pakker (APK-filer) mod kun 139 i samme periode året før. Samtidig er kompleksiteten af den fundne malware steget både med hensyn til spredning og funktionalitet.



Figur 16. Andel af sidevisninger med mobile enheder på danske websites.

84 procent af de malware-varianter, som blev opdaget til Android i første kvartal 2012, var trojanske heste. Nogle varianter indeholdt desuden botnet-funktionalitet eller evnen til at installere yderligere programmer, foretage opkald og afsende overtakserede sms'er. Derudover var det ikke ualmindeligt, at de fundne malware-varianter for eksempel kryp-

terede data eller gemte dem i billedfiler.

Når de mobile enheder er interessante for malware-udviklerne, skyldes det flere faktorer. Mobiltelefoner og tavle-pc'er er reelt små computere, der benyttes til alt fra e-mail, spil og webtrafik til e-handel. Data på en mobil enhed er i dag lige så værdifulde som data på en traditionel computer. De mobile enheder slukkes sjældent, og den stigende udbredelse gør dem i sig selv til et attraktivt mål. Derudover har teknologien nået en modenhed, så der findes flere udviklingsmiljøer, der gør det lettere at udvikle malware.

Mange opfatter ikke deres mobil som et potentielt mål for internetkriminalitet. Derfor er det hovedsageligt i erhvervslivet, der i øjeblikket er et marked for kryptering, antivirus og lignende.

Den stigende mængde mobile enheder med adgang til stadig hurtigere mobilt netværk vil sandsynligvis medføre udvikling af endnu mere malware rettet mod de mobile enheder.

At det er Android, de kriminelle har kastet sig over, skyldes platformens åbenhed i forhold til iOS. Her skal alle applikationer godkendes, inden de lægges til download fra Apples App Store. Det er langt lettere at lægge skadelige applikationer på Android Market.

Udviklingen ligner den, vi tidligere har set for både Windows og Macintosh. Mens udbredelsen af internetopkoblede Windows-computere steg op gennem 1990'erne, steg også mængden af orme og virus, hvis udvikling var muliggjort af en stigende mængde tilgængelige udviklingsplatforme. Samme udvikling har vi de senere år set for Macintosh-computerne, der tidligere var forskånet for malware.

De stigende markedsandele i kombination med at mange brugere har ment, at det ikke var nødvendigt med antivirus-software til Macintosh, har gjort platformen til et attraktivt mål. Gennem de seneste år er malware, der også rammer denne platform, derfor eksploderet i antal.

F-secure, 2012; "*Mobile Threat Report Q1 2012*".
Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".

6. Artikler fra tredje kvartal

Nedenstående artikler fra vores trendrapport for tredje kvartal 2012 illustrerer hvordan digitaliseringen af samfundet har medført nye digitale problemstillinger og risici.

I Danmark har vi taget informationsteknologien til os, hvilket har givet bankerne, erhvervslivet og det offentlige mulighed for at udvikle nye digitale selvbetjeningsplatforme. Det har øget effektiviteten og fleksibiliteten i vores samfund, men sam-tidig introduceret nye problemstillinger. Hvor informationsteknologien på mange måder har gjort vores dagligdag mere enkel, er verden nemlig samtidig blevet mere sammenhængende og kompleks.

Hvordan skal man for eksempel som borger forholde sig til ikke at kunne indberette ledighed til sin a-kasse, fordi dens hjemmeside er sat ud af drift af folk, som er uenige med dens måde at agere på? Når østeuropæiske hackere stjæler penge fra ens bankkonto, blot fordi man benyttede netbank? Eller når maskinen låser og en besked på skærmen fortæller, at man skal betale 100 euro for at få den låst op?

”Udbredelse af informationsteknologi har nemlig også en bagside.”

Ovenstående skitserer nogle af de problemstillinger, vi som borgere og samfund stod over for i tredje kvartal. Problemstillinger som ikke er ukendte i erhvervslivet. Ud over selv at være mål for it-kriminalitet er organisationerne nemlig en del af både problemet og dets løsning. Den stigende digitalisering af vores aktiver øger vores sårbarhed for, at data kommer i de forkerte hænder. Udbredelse af informationsteknologi har nemlig også en bagside.

Blandt andet derfor havde EU-kommissionen udfærdiget et forslag til revision af databeskyttelsesdirektivet, som ventes til førstebehandling til februar 2013. Ud over at stille større krav til organisationernes behandling af forbrugerdata skal det blandt andet sikre, at forbruger-data ikke kan kompromitteres, uden at forbrugeren informeres rettidigt.

Mens nogle af disse problematikker kan løses teknisk eller gennem ændret lovgivning og kontrol, vil andre kræve mere åbenhed og stigende information. Det er nemlig i fællesskabet, vi skal forstå og forme vores digitale fremtid. Også når det gælder informationssikkerhed.

6.1. Hacktivisme i skyggen af Restaurant Vejlegården

Efter at fagforeningen 3F i flere måneder havde blokeret Restaurant Vejlegården, blev dens hjemmeside den 19. juli udsat for et Denial of Service-angreb. Angrebet gjorde hjemmesiden utilgængelig og berørte fagforeningens dagpengemodtagere. Det illustrerer en tendens mod større global opbakning til lokale aktioner under signaturen Anonymous.

Baggrunden for angrebet var, at restauranten havde tegnet en overenskomst med Kristelig Fagforening, som 3F mener forringer de ansattes arbejdsforhold. Måneder efter konfliktens begyndelse ramte historien de landsdækkende medier. Herefter tog begivenhederne fart. Politikere valfartede til restauranten for at tilkendegive deres sympatier, og ethvert villigt interviewoffer havde sine egne holdninger og sympatier i forhold til de stridende parter.

Den 19. juli blev 3F’s hjemmeside udsat for et Denial of Service-angreb, der gjorde den utilgængelig i flere dage. Angiveligt deltog folk fra blandt andet USA, Mexico, Brasilien, Spanien, Tyskland, Portugal og Australien i angrebet, som i første omgang blev proklameret af Twitter-brugeren Elan0r. Angrebene ramte siden både LO og HK’s hjemmesider og berørte cirka 30.000 dagpengemodtageres mulighed for indberetning af ledighed med forsinket udbetaling af dagpenge til følge.

Til TV 2 fortalte en anonym hacker, at angrebet var løbet af sporet, fordi mange deltagere ikke var ”rigtige” Anonymous. Senere belærte en video på YouTube os om, at det slet ikke var de ”rigtige” Anonymous, der stod bag angrebet. Også denne video var signeret Anonymous og kaldte deltagerne i angrebet for forrædere.

Hvordan man i en løstknyttet global bevægelse uden formelle strukturer, regler eller medlemslister kan definere nogle som mere rigtige end andre, skal her stå hen i det uvisse. Flere steder på nettet kan man finde udsagnet om, at alle kan være Anonymous, eller som det kan læses på hjemmesiden anonkbh.dk:

”Anonymous er en idé, et ideal, et catch-all for en kultur, der er opstået på internettet. Anonymous er et navn som selvstændige grupper kan påtage sig, når de handler i hvad de mener er dette ideals ånd.”

Om hacktivisme:

Sammentrækning af hacking og aktivisme, eller på dansk ”politisk motiveret hacking”. Hacktivister forfølger politiske mål gennem brugen af internettet. De kan overordnet opdeles i tre bevægelser:

Anonymous, der støtter det frie internet og er den mest synlige og aktive gruppering. Deres metoder involverer hacking, DDoS-angreb, informationstyveri og offentliggørelse af personlige eller fortrolige informationer.

Cyberoccupiers er de traditionelle aktivister, der primært benytter internettet til propaganda og informationsdeling. Med henvisning til Occupy-bevægelsen er de for et mere transparent demokrati og imod korruption.

Cyberkrigerne er folk, der kæmper for en sag, hvad enten det er religion, nationalstater eller ekstremistiske bevægelser. Benytter sig primært af webgraffiti og DDoS-angreb.

Uenigheden om hvorvidt angrebene mod 3F var udført af Anonymous

eller ej, illustrerer to ting. Dels at der en vilje til at aktionere, hvis man mener, at nogen opfører sig på en måde, der ikke er i overensstemmelse med egne holdninger. Dels at Anonymous ikke er en hackergruppe, men snarere en idé eller bevægelse som man kan tilslutte sig efter forgodtbefindende.

"Det er ikke første gang, vi ser hacktivister udføre angreb i Danmark. Imidlertid er det første gang, at en sag, der har så lokal interesse, øjensynlig opnår global opbakning."

Det er ikke første gang, vi ser hacktivister udføre angreb i Danmark. Imidlertid er det første gang, at en sag, der har så lokal interesse, øjensynlig opnår global opbakning. Den udvikling er muliggjort af Anonymous' massive medieomtale, synligheden af deres kommunikationskanaler og en global interesse for at indgå i dette virtuelle fællesskab. Resultatet af ens protester er nemlig her meget synlige.

Ved at forstå og reagere på Anonymous som en global gruppe med et fælles fokus og mål overser man mangfoldigheden af angrebsmotiver fra grupper eller individer, som sætter signaturen Anonymous på deres handlinger. De mere eller mindre politisk motiverede angreb har altid eksisteret. Ved at kalde det Anonymous har man nu fået mulighed for at få global tilslutning til angreb, der primært vedrører lokale forhold.

DKCERT mener:

Med signaturen Anonymous som den mest fremtrædende har hacktivisme gennem de seneste år været blandt de store nye tendenser. Vi ser en stigning i politisk motiverede angreb som en tendens, der vil fortsætte. Både globalt og lokalt.

Vi mener, at man ikke bør frygte Anonymous, men i stedet overveje, om organisationens forretning, handlinger og data kan give anledning til, at man bliver mål for lokalt betingede angreb, og bruge det aktivt i forhold til den løbende risikovurdering.

Anonymous København; *"Velkommen til Anonymous København"*.
Berlingske, 2012; *"3F-hacker-angreb rammer dagpengene"*.
BT, 2012; *"Anonymous: 3F-hackerne er forrædere"*.
McAfee, 2012; *"Hacktivism - Cyberspace has become the new medium for political voices"*.
TV 2, 2012; *"3F's hjemmeside lagt ned af hackere"*.
TV 2, 2012; *"Anonym hacker: Operationen er kørt af sporet"*.

6.2. NemID-angreb afværget i Sydbanks netbank

Den 14. august informerede Sydbank sine kunder om, at bankens netbankløsning var under angreb. Som ved årets tidligere netbankindbrud var de uheldige bankkunders computere inficeret med malware, der ved login interagerede med NemID-løsningen.

Ved et realtime man-in-the-middle-angreb lykkedes det i løbet af juli og august måned hackere at logge ind på 13 Sydbank-kunders netbankkonti. Normal login på netbanken ledte ved hjælp af en trojansk hest kunderne til en ny login-side. Den var imidlertid falsk og gav angriberne mulighed for at etablere en ny NemID-session mod netbankløsningen. Pengeoverførslerne blev dog opdaget og afværget af Sydbanks systemer til fraud detection.

"Angrebet bliver sandsynligvis ikke det sidste, vi ser på danske netbanker. Det illustrerer truslerne mod NemID's fortsatte succes. Den afhænger af brugernes tillid til løsningen."

Angrebet bliver sandsynligvis ikke det sidste, vi ser på danske netbanker. Det illustrerer truslerne mod NemID's fortsatte succes. Den afhænger af brugernes tillid til løsningen. Her er det væsentligt, at man er i stand til at afværge kommende angreb, hvilket dog også er brugernes eget ansvar. For at angrebene lykkes, kræver det nemlig, at man er i stand til forinden at inficere deres computere med malware.

Usikkerhed om Java-platformen er en yderligere problemstilling, som man står over for. Hvordan skal man for eksempel som bruger forholde sig til 0-dags sårbarheder i Java, som den vi i august advarede mod? At man ikke har været i stand til at få et dansk domænenavn til NemID, hvis hjemmeside i dag hedder www.nemid.nu, er tilsvarende med til at skabe uklarhed.

NemID-løsningen har siden den blev introduceret i 2010 været udsat for kritik. Den har blandt andet gået på, at løsningen ikke var brugervenlig nok, var for central og omfattede adgang til både det offentlige og private, blev udviklet og drevet i privat regi og generelt ikke var sikker nok. Særligt har der været kritik af Java, som er valgt som platform for løsningen. Java bliver vurderet som usikker og kan ikke benyttes på alle mobile platforme.

Hvad enten kritikken er berettiget eller ej, er mangfoldigheden af synspunkter med til at sikre, at NemID formes, så den også i fremtiden er både brugervenlig og sikker. I sidste ende handler det om, at vi som brugere har tillid til en løsning, som også er brugervenlig.

Også brugeren selv har et medansvar for at login-proceduren ikke kompromitteres af tredjepart. Det vil primært sige, at den benyttede computer holdes opda-teret og sikker. Belært af det seneste års erfaringer står vi her med en udfordring, som primært er af kommunikativ karakter.

DKCERT mener:

Med et par 2012 på bagen er teknologien og brugsmønstrene for NemID efterhånden velkendte. Også i de internet-kriminelle miljøer. Derfor har vi i år set flere netbankangreb, hvor det er lykkedes at omgå sikkerheden i NemID. Vi venter, at de angreb vil stige i antal.

Vi mener grundlæggende, at NemID er en både sikker og brugervenlig løsning. Det skal dog ikke give anledning til, at vi hviler på laurbærrene, da der er plads til forbedringer. Både i forhold til den benyttede teknologi, hvor og hvordan den benyttes, samt hvorledes løsningen kommunikeres til brugerne. I sidste ende handler det om, at vi har tillid til løsningen.

DKCERT, 2012; "*Alvorligt hul i Java står åbent*".
Sydbank, 2012; "*Angreb på Sydbanks NetBank*".
Version 2, 2012; "*Domæne-chok: DanID taber retten til nemid.dk med et brag*".
Version 2, 2012; "*Hackere angriber Sydbanks netbank med virus*".
Version 2, 2012; "*Hackere snyder NemID igen: Sydbank stopper massivt angreb*".

6.3. Krav om informationspligt ved tab af data

Sidst i august kritiserede flere personer i sikkerhedsbranchen de danske organisationer for at holde hackerangreb skjult. Ønsket om større åbenhed blev siden taget op af politikere fra både Venstre og Socialdemokratiet, der ikke ville love regulerende lovgivning. Den er dog på vej ind ad bagdøren gennem EU-kommissionens udkast til en revision af databeskyttelsesdirektivet.

Ifølge tal fra Danmarks Statistik svarede syv procent af danske virksomheder med mere end ti ansatte, at de i 2010 var udsat for ødelæggelse af data på grund af virus eller uautoriseret adgang. Seks procent havde oplevet forstyrrelser i it-systemer på grund af denial-of-service-angreb og lignende. Hertil kommer forsøg på angreb, som enten ikke blev opdaget eller ikke gav anledning til forstyrrelser eller tab af data. Det er relativt store tal, som langt overstiger antallet af politianmeldelser.

Vi har gennem en årrække givet udtryk for et ønske om indberetningspligt ved brud på informationssikkerheden. Dels skylder man sine kunder at orientere dem, og dels betyder den nuværende adfærd, at vi ikke har reel viden om problemernes omfang. Herved blokeres for læring, som i sidste ende også vil komme virksomhederne til gode. Det kommenterede direktør Lars Neupart fra Neupart A/S i en artikel i Berlingske:

"... når der ikke er en åben kommunikation om sikkerhedshændelser, bliver vi ikke klogere som fagfolk."

I dansk lovgivning om behandling af personoplysninger er virksomhederne ikke forpligtede til at informere om læk af personfølsomme oplysninger, medmindre de selv vurderer, at der er behov for det. Det står i kontrast til blandt andet flere amerikanske delstater, hvor virksomhederne skal informere både offentligheden og personer, hvis data er berørt. Denne praksis vil et udkast til en revision af EU's databeskyttelsesdirektiv indføre.

EU-kommissionens udkast blev offentliggjort den 25. januar. Det styrker borgernes retsstilling og giver i højere grad ejerskab af egne data. Blandt andet betyder det, at borgeren har krav på at blive orienteret, hvis dennes data kompromitteres af tredjepart, ligesom virksomhederne har pligt til at orientere en lokal tilsynsførende myndighed. Ansvaret for overholdelse af lovgivning påhviler herhjemme Datatilsynet, hvis direktør Janni Christoffersen blandt andet udtalte:

"For virksomheder og organisationer er der større krav om at tage ansvar for databeskyttelse. Der strammes op med nye forpligtelser for at øge fokus på databeskyttelse."

Hvis lovændringen indføres, vil det betyde et større økonomisk incitament for organisationerne til at tage ansvar for informationssikkerheden. Ud over indirekte omkostninger som prestigetab kan kompromittering af virksomhedernes data betyde bøder eller erstatning, som håndhæves i stil med markedsføringslovens §6 vedrørende spam. Derudover pålægges det organisationer med over 250 ansatte at udpege en databeskyttelsesansvarlige, der skal medvirke til organisationens overholdelse af forordningen.

DKCERT mener:

De seneste år har sat fokus på offentliggørelse af kompromitterede data. Data flyder og lagres på tværs af landegrænser. Derfor hilser vi en europæisk harmonisering af reglerne om databeskyttelse velkommen.

Vi mener, at en skærpet informationspligt ikke blot vil sikre borgernes rettigheder, men også øge organisationernes fokus på informationssikkerhed. I et bredere perspektiv giver informationspligten muligheder for videnindsamling og -deling omkring aktuelle trusler, som ikke er mulig i dag. Alt sammen til borgernes, organisationernes og samfundets bedste.

Berlingske, 2012; "*IT-indbrud holdes skjult for dig*".
Berlingske, 2012; "*Politikere ønsker mere åbenhed om hackerangreb*".
Danmarks Statistik, 2011; "*Danske virksomheders brug af it - 2011*".
Datatilsynet, 2012; "*EU-Kommissionens reformpakke om databeskyttelse*".
Datatilsynet, 2012; "*Udtalelse om EU-Kommissionens forslag til forordning om databeskyttelse*".
Europa-kommissionen, 2012; "*Commission proposes a comprehensive reform of the data protection rules*".
Europa-kommissionen, 2012; "*Opinion 01/2012 on the data protection reform proposals*".
Version 2, 2012; "*Opråb til danske virksomheder: Skjul ikke hackerangreb*".
Version 2, 2012; "*Pas på nye privacy-regler: Datatilsynet får kæmpe bødehammer*".

6.4. Når malware tager data som gidsel

Din computer er låst, indtil du har betalt en bøde for at se børneporno, med venlig hilsen politiet. Det er den korte version af en type malware, der gennem de seneste år er steget i antal. Politi-ransomware er blevet en god forretning, der i juli måned også blev

målrettet danskerne.

Politi-ransomware er blandt de hurtigst voksende trusler på internettet. Derfor har både FBI og Europol i år advaret specifikt mod den. At det også er en god forretning, viser bagmændenes egne statistikker. En enkelt variant blev den 17. maj spredt til 2.116 computere alene i Frankrig. I 79 tilfælde (3,7 procent) valgte brugerne at betale "bøden". I alt betalte 322 personer fra hele verden denne dag, hvilket indbragte 28.000 euro. Dagen efter var indtjeningen 44.000 euro.

Ved hjælp af exploit kits som for eksempel BlackHole spredes malwaren fra kompromitterede hjemmesider ved drive-by-download til de besøgendes computere. Ofte efterprøves flere sårbarheder i for eksempel Java, Flash eller Adobe Reader. Lykkes det at inficere computeren, hentes koden, der ved for eksempel kryptering låser computeren. Herefter præsenteres brugeren for kravet om at betale en bøde for at få låst maskinen op. Den mest kendte variant, Reveton, installerer samtidig en trojansk hest og indeholder funktionalitet til indsamling af brugernavne og kodeord fra computeren.

I juli måned kom det første tilfælde af den type malware målrettet danskere. Et vindue med overskriften "Computeren er blevet blokeret for at overtræde lovgivningen i Danmark" fortalte, at man havde set børnepornografisk materiale og piratkopieret ophavsretsbeskyttet materiale. Derfor var maskinen blevet låst, indtil man via betalingstjenesten Ukash havde betalt en bøde på 100 euro. Beskeden var udført på dårligt dansk og uden en egentlig afsender, hvorfor de fleste gennemskuede, at der var tale om malware.

Som falske telefonopkald fra Microsoft er politi-ransomware delvist et skridt i evolutionen af falske antivirusprodukter. De præsenterer de inficerede for et vindue, der fortæller, at maskinen er inficeret med malware, som kun kan fjernes ved køb af et specifikt "antivirusprodukt". For at øge incitamentet til at købe det falske antivirusprodukt har malwaren i stigende grad "låst" den inficerede computer.

"De færreste har lyst til at fortælle naboen eller kollegaen, at man har fået en bøde for at kigge på børneporno. Det hvad enten det er tilfældet eller ej."

Med en kombination af en ubrugelig maskine, brugerens skyldfølelse og pres fra "myndighederne" har politi-ransomware skruet op for brugen af social engineering. Det skal i sidste ende få brugeren til at betale uden at konsultere andre. De færreste har lyst til at fortælle naboen eller kollegaen, at man har fået en bøde for at kigge på børneporno. Det hvad enten det er tilfældet eller ej. Mens inficeringer med falske antivirusprodukter ifølge McAfee falder, er ransomware derfor i vækst.

Vi har endnu ikke set troværdige eksempler på ransomware, der udgiver sig for at komme fra de danske myndigheder. Om det skyldes, at vi rent sprogligt udgør et relativt lille "marked", manglende udbredelse af anonyme betalingsmidler eller at vores computere er mere sikre end i de andre europæiske lande, ved vi ikke. Det seneste eksempel fra juli måned giver dog en forventning om, at det er et problem, som også herhjemme vil vokse i både troværdighed og mængde. Der er trods alt tale om en god forretning.

DKCERT mener:

Ransomware er den hurtigste og nemmeste måde at omsætte sin kode til rede penge på. Når malwaren er distribueret til download, er det blot at vente på, at pengene ruller ind på kontoen. I modsætning til andre typer malware er der ingen data, der efterfølgende skal bearbejdes eller forsøges omsat til penge.

Derfor venter vi, at væksten af denne type af malware vil fortsætte – også målrettet danskere. Så længe der er computere, som ikke er beskyttet, er der brugere, der er villige til at betale for igen at få adgang til deres computer og data. Det hvad enten det er "politiet" eller andre, der har låst den.

Ransomware:

Malware, der tager brugernes data som gidsel, indtil der er betalt løsepenge (ransom) med anonyme betalingssystemer som for eksempel Ukash, Paysafe og MoneyPak. Oftest sker gidseltagningen ved at kryptere indhold på den inficerede computer, hvorfor malwaren blandt andet også benævnes kryptovirus. Malwaretypen er ikke ny og har i flere år floreret særligt i Rusland. En af de første trojanske heste, AIDS- eller PC Cyborg-trojaneren fra 1989, havde samme funktionalitet.

Politi-ransomware er det seneste skud på stammen. Den spredes ved drive-by-download. Brugeren præsenteres for en besked fra den lokale politimyndighed, der fortæller, at maskinen er låst på grund af download af børneporno, kopibeskyttet materiale og tilsvarende. Maskinen låses op ved betaling af en bøde på typisk 100 euro, pund eller dollars.

Computerworld, 2012; "*Her er den første afpresnings-software på dansk*".
KrebsonSecurity, 2012; "*Inside a 'reveton' ransomware operation*".
McAfee, 2012; "*'Police ransomware' preys on guilty consciences*".
McAfee, 2012; "*'McAfee threats report: Second quarter 2012*".
Wikipedia; "*Ransomware (malware)*".
Wikipedia; "*Rogue security software*".

6.5. Angreb udnyttede hul i Internet Explorer

Et hidtil ukendt sikkerhedshul i Internet Explorer blev brugt i begrænsede, målrettede angreb. Programmet benyttes til halvdelen af danskernes internetsurf, så truslen var potentielt alvorlig. I medierne blev den præsenteret som meget alvorlig.

Den 16. september skrev sikkerhedsforsker Eric Romang på sin blog,

at han havde fundet et angrebsprogram på en server. En nærmere analyse viste, at angrebet udnyttede et hidtil ukendt sikkerhedshul i Internet Explorer. Dagen efter bekræftede Microsoft, at sårbarheden findes i Internet Explorer 6, 7, 8 og 9. Den 19. september udsendte Microsoft en midlertidig rettelse af typen Fix It. Den 21. september kom en sikkerhedsrettelse, der fjernede denne og fire andre sårbarheder i Internet Explorer.

Sårbarheden lå i browserens behandling af objekter, der bliver slettet. Angribere kunne udnytte den til at afvikle programkode. Kort tid efter offentliggørelsen blev der udsendt et modul til Metasploit, der udnyttede sårbarheden i praksis. Der er kun observeret få angreb, der udnytter sårbarheden.

"Medierne skruede op for sensationen i dækningen af sårbarheden. Flere talte om en kommende virus, skønt der kun var tale om en sårbarhed."

Medierne skruede op for sensationen i dækningen af sårbarheden. Flere talte om en kommende virus, skønt der kun var tale om en sårbarhed. Det gav øget opmærksomhed hos borgerne, hvilket er en god ting. Men det medførte også, at nogle borgere blev mere bekymrede, end der var grund til.

Når medierne taler om virus, skyldes det nok, at begrebet sårbarhed eller sikkerhedshul ikke er kendt. Her har sikkerhedsbranchen en informationsopgave, så befolkningen lærer at forstå begreberne sårbarhed, virus og angrebsprogram.

I dette tilfælde er der tale om en potentielt alvorlig sårbarhed, der dog endnu ikke har været brugt til særlig mange angreb. Det korrekte budskab burde derfor være, at brugerne så vidt muligt skulle undlade at bruge Internet Explorer, indtil Microsoft kom med en rettelse. Kunne det ikke lade sig gøre, kunne man følge de råd, som Microsoft giver i sin sikkerhedsadvarsel: Installer EMET (Enhanced Mitigation Experience Toolkit) eller sæt sikkerheden for zonen Internet til Høj.

Det sidste råd er umiddelbart nemmest at følge, men i praksis medfører det, at mange websteder ikke fungerer. Derfor risikerer man, at brugerne hurtigt dropper indstillingen og dermed bliver sårbare igen.

Nogle organisationer kan med et tryk på en knap ændre sikkerhedsindstillingen i Internet Explorer for alle brugere. For andre kræver det, at hver enkelt medarbejder modtager en mail og følger anvisningerne i den. Naturligvis er den første metode mest effektiv.

DKCERT mener:

Når der opdages en sårbarhed i et så udbredt program som Internet Explorer, er det afgørende at kommunikere korrekt om den. Informationen skal på den ene side fortælle, hvor alvorlig sårbarheden er, på den anden side skal den ikke skræmme ved at overdrive konsekvenserne. Organisationer skal derfor nøje overveje, hvordan de informerer deres brugere om truslen, og hvad de bør gøre.

Vi mener, at denne type sårbarhed viser, hvor vigtigt det er at have centrale værktøjer til administration. Derfor bør organisationer lette deres sikkerhedsarbejde ved at indføre central administration af sikkerhedspolitikker.

DKCERT, 2012; "*Microsoft lukker huller i IE og Flash*".
Foreningen af Danske Interaktive Medier (FDIM); "*Browserbarometer*".
Microsoft, 2012; "*Microsoft security advisory (2757760)*".
Erik Romang, 2012; "*Zero-Day Season Is Really Not Over Yet*".

6.6. Hackere lækkede data fra universiteter

Ved at udnytte SQL-injection-sårbarheder fik hackere fat i data fra en række universiteters databaser. De lagde oplysninger om godt 40.000 brugerkonti ud på nettet. Årsagen er angiveligt, at man er utilfreds med udviklingen af uddannelsessystemerne.

Den 1. oktober lagde en hackergruppe ved navn Teamghostshell data fra universiteter ud på forskellige websteder. Ifølge gruppen selv er der tale om data fra verdens top 100 universiteter, der ikke før har været lækket. Tidligere har Anonymous-bevægelsen fremsat trusler mod uddannelsesinstitutioner i Europa, og selvom der ingen danske universiteter er blandt de hackede institutioner, illustrerer det, at også de kan blive mål for angreb.

De lækkede data er for eksempel mail-adresser og brugernavne på ansatte og studerende. I nogle tilfælde optræder også passwords, ofte dog kun som hashværdier. Det ser således ud til, at der ikke var kritiske data i lækagen. Danskere der har været tilknyttet udenlandske institutioner, bør dog tjekke, om deres data optræder på listerne.

Hackergruppen skriver, at den fandt langt flere data, men at den har valgt at begrænse offentliggørelsen af dataposter. På mange af de kompromitterede servere fandt de efter eget udsagn også skadelige programmer (malware).

Stikprøver viser, at data typisk er hentet ved at udnytte SQL-injection-sårbarheder i web-applikationer. Den slags sårbarheder er ofte relativt nemme at fjerne. Med tanke på at webgrænsefladen er blandt de mest angrebne, kan man derfor undre sig over, at så store organisationer overhovedet havde den slags sårbarheder.

Angrebet er et eksempel på hacktivisme i stil med den, vi også kender fra Anonymous-bevægelsen. Teamghostshell begrunder lækagen med,

at gruppen er kritisk over for udviklingen af uddannelsessystemerne og hvordan de interagerer med den øvrige verden. Eller som de blandt andet selv skriver på webstedet Pastebin:

"... we have ventured from learning valuable skills that would normally help us be prepared in life, to just, simply memorizing large chunks of text in exchange for good grades."

Angrebet viser, at selvom man ikke har profit som mål og i egen selvopfattelse arbejder til samfundets bedste, kan der være nogle, der har en anden holdning til, hvordan man udfører sine gerninger. Som med angrebet på 3F's hjemmeside i juli bør det medføre et større fokus på databeskyttelse. Også i organisationer der ikke traditionelt opfattes som oplagte mål.

DKCERT mener:

Globaliseringen har medført en stigende mangfoldighed i motiver og muligheder for digitale angreb. Således viser det aktuelle angreb, at det i dag er de færreste organisationer, der kan afskrives som mål. Mange af de sårbarheder der blev udnyttet, er nemme at fjerne og burde ikke have været der.

Det er en god anledning til at tjekke, om ens egen it-sikkerhed er på plads. Her mener vi, at angrebet bør medføre, at man også i den akademiske verden sætter større fokus på sårbarheder i sine webapplikationer. Det er oftest dem, der udnyttes, hvad enten det handler om at stjæle data eller kompromittere sidens besøgende.

Identityfinder, 2012; "*Large-Scale Coordinated SQLi Attack on Higher Education*".
Teamghostshell, 2012; "*#ProjectWestWind - Today's education!*".
Threatpost, 2012; "*Team Ghost Shell claims to publish records from thousands of universities*".

7. Temaer i fjerde kvartal

Vi runder her året af med de historier, vi har fundet væsentlige for fjerde kvartal 2012. Et kvartal, der på mange måder stod i de anonyme hackeres tegn. Både herhjemme og i Sverige oplevede vi angreb, som var underskrevet den løst sammenknyttede bevægelse Anonymous, omend angrebenes motiver og udførelse var forskellige.

Hvor DDoS-angrebet på flere svenske myndigheders hjemmesider ligger i direkte forlængelse af bevægelsens tidligere angreb, virkede angrebet på cpr.dk mere tilfældigt. Både målet i sig selv og det, bevægelsen efterfølgende kommunikerede om angrebet, kunne på mange måder anfægtes. I sidste ende kan den manglende røde tråd og troværdighed vise sig at blive starten på enden for Anonymous-bevægelsen.

Modsat angrebet på cpr.dk blev der vist større kompromisløshed, da ukendte gerningsmænd midt i november offentliggjorde 30.000 brugernavne og kodeord fra datingsiden sex.dk. Angrebet var underskrevet #anondk. Også her manglede et gennemskueligt motiv bag handlingen.

Cpr-nummeret kom igen i fokus, da det viste sig, at flere mobilselskabers hjemmesider kunne bruges til at få oplyst brugernes cpr-nummer. Miseren skyldtes, at nummeret blev benyttet i autentificeringsprocessen, hvilket er problematisk.

Sidst i november så et nyt råd dagens lys. Rådet for Digital Sikkerhed samler trådene for en bred vifte af aktører inden for informationssikkerhed og skal bidrage til en sikker digitalisering af Danmark. Herfra ønsker vi rådet velkomment og god vind på rejsen. Der er nemlig nok at tage fat på.

I afsnittets sidste historie sætter vi beløb på internetkriminaliteten og sammenligner med traditionel berigelseskriminalitet som bankrøveri. Afsnittet anskueliggør, at internetkriminalitet er en god forretning, som ved større professionalisering og effektivisering er blevet en stadig mere tilgængelig karrierevej. Set i det lys har vi en forventning om, at problemet vil tage til i omfang.

7.1. Koordinerede angreb på svenske myndigheder

Personer med tilknytning til Anonymous-bevægelsen angreb i oktober flere svenske myndigheder. Det var en protest mod en politirazzia hos et hosting-firma, der var mistænkt for at være involveret i ulovlig fildeling.

Den 1. oktober foretog svensk politi en razzia mod hosting-firmaet PRQ, som er stiftet af folk med baggrund i Pirate Bay. Samtidig skete der et nedbrud hos Pirate Bay, så man ikke kunne komme i forbindelse med webstedet. De to hændelser havde øjensynlig intet med hinanden at gøre, men nogle internetaktivister så dem som tegn på myndighedernes forfølgelse af fildeling.

Derfor truede ukendte personer, der hævdede at udtale sig på vegne af Anonymous-bevægelsen, med angreb mod flere svenske websteder. Angrebene kom i flere bølger. Den 3. oktober blev der varslet et angreb til start samme aften klokken 23. Men allerede omkring 21:45 blev regeringens, nationalbankens og rigsdagens websteder ramt sammen med flere andre. Webstederne havde lange svartider eller svarede slet ikke.

Et senere angreb blev varslet til fredag den 5. oktober klokken 14:30. Her havde man på forhånd udpeget 19 angrebsmål, heriblandt Antipiratbyran.se og Domstol.se. Om eftermiddagen var otte af dem nede. Samme dag skrev en person på vegne af Anonymous-bevægelsen til aktivisterne, at de skulle høre inde med angrebene. Derefter døde angrebene ud.

Angrebet medførte voldsom stigning i internettrafik mod Sverige, som blandt andet kunne aflæses på NORDUnets routere.

DKCERT mener:

Angrebet viser, at hacktivisme er en reel trussel mod myndigheder og virksomheder. Man kan også blive ramt, selv om man ikke er part i den konflikt, som er årsag til angrebet. Samtidig illustrerer det, hvor vanskeligt det er at beskytte sig mod et DDoS-angreb.

Ved sådanne angreb er forberedelse afgørende. Derfor mener vi, at enhver organisation bør have en beredskabsplan for, hvordan den vil håndtere for eksempel et DDoS-angreb, hvis den bestyrer websteder, som det er afgørende, at kunder og borgere kan nå.

Nyheter24, 2012; *"Anonymous-attackerna helt avblåsta"*.
Nyheter24, 2012; *"Polisrazzia mot webbhotellet PRQ"*.
Version 2, 2012; *"Cyberangreb på Sverige: Statsbaner og nyhedsbureau DDoS'et"*.

7.2. Mulig datalækage fra Cpr.dk

Den sjette november kunne man i de danske medier læse, at Anonymous-bevægelsen havde skaffet sig adgang til det danske cpr-register. Rigtigheden af dette blev senere dementeret og satte spørgsmålstegn ved bevægelsens motiver og troværdighed.

Som en fejring af Guy Fawkes-dag den femte november proklamerede Anonymous-bevægelsen på Pastebin, at de fra cpr.dk havde skaffet sig adgang til cpr-registrets database. Den indeholder samtlige danskeres navne, adresser, cpr-numre med mere.

Angrebet var sket for at illustrere, at it-sikkerheden i Danmark er dårlig, og som en protest mod myndighedernes påståede krig mod Anonymous-bevægelsen. Navne på 90 tabeller i databasen under cpr.dk blev offentliggjort som bevis på angrebets ægthed og alvorlighed.

Efterfølgende kunne kontorchef Carsten Grage fra Økonomi- og indenrigsministeriets Cpr-kontor bekræfte, at cpr.dk havde været genstand for et angreb. Hjemmesiden giver dog ikke adgang til personfølsomme oplysninger. Skaden var derfor ikke så stor, for som

han videre fortalte til Danmarks Radio:

"Selve cpr-systemet er helt adskilt fra hjemmesiden, og det har ikke været genstand for hacking."

Ved efterfølgende ikke at anskueliggøre, at man rent faktisk havde fået fingre i danskernes cpr-numre, står Anonymous-bevægelsen med et troværdighedsproblem. Havde man haft adgang til danskernes persondata, kunne man nemt have offentliggjort dele af dem i maskeret form uden at gå på nævneværdigt kompromis med vores privatliv.

Ikke blot virkede angrebet umotiveret, men troværdigheden af det, som blev kommunikeret, kunne også anfægtes. Tilsvarende var det med et angreb på den danske it-virksomhed Atea, der blev offentliggjort sammen med angrebet på cpr.dk. Her udtalte it-direktør Henrik Arndt efterfølgende:

"Vi kan se, at de har prøvet, og vi har brugt meget tid på at undersøge det, men vi har ikke fundet noget."

Nøglen til Anonymous-bevægelsens succes har hidtil været dens evne til at skabe medieomtale om aktiviteter, der kunne sættes i sammenhæng med kampen for et frit internet, mod storkapitalen og censur. Hvad enten målet var internationale virksomheder, offentlige myndigheder eller andre, var det den lilles kamp mod de uretfærdige undertrykkere. En historie der blev kommunikeret effektivt og som var velfortalt og letforståelig. Angrebet på cpr.dk faldt på mange måde uden for denne kontekst.

"Hvis aktiviteterne blot udføres, fordi man kan, vil det betyde opløsning af den lim, der binder bevægelsen og dens støtter sammen."

Hvis bevægelsen fortsat skal finde støtte til sine aktiviteter, kræver det et fælles mål i form af en sag, en fjende eller et problem, man ønsker at løse. Hvis aktiviteterne blot udføres, fordi man kan, vil det betyde opløsning af den lim, der binder bevægelsen og dens støtter sammen.

Når man ydermere kan anfægte korrektheden af det, som kommunikeres i bevægelsens navn, forstærkes denne effekt. På længere sigt kan det betyde, at Anonymous-bevægelsen decimeres. Hvis deres aktiviteter ikke indgår i en større sammenhæng, er der jo blot tale om tilfældige drengestreger.

Der vil altid være kræfter, der ønsker destabilisering og anarki, men de mange der indtil videre har tilsluttet sig kampen for et frit internet og mod censur, vil muligvis betakke sig for at blive associeret med bevægelsen. På mange måder kan man derfor håbe, at bevægelsens succes samtidig betyder dens fald. I modsat fald kræver det som et minimum, at det som kommunikeres i bevægelsens navn ikke kan anfægtes.

DKCERT mener:

Angrebet på cpr.dk illustrerer kommunikationens betydning for Anonymous-bevægelsens identitetsskabelse og opbakning. Hvis ikke man kommunikerede, at man havde fået adgang til samtlige danskeres cpr-numre, ville angrebet i global skala være uinteressant. Hvorvidt det var sandt eller ej, betød angiveligt ikke så meget, blot man kunne sandsynliggøre og kommunikere det.

DKCERT mener, at angrebet på cpr.dk viser Anonymous-bevægelsens sårbarhed. Kan vi stille spørgsmålstegn til angrebenes motiver og resultater, kan man håbe, at de grupperinger der ellers ville associere sig med bevægelsen, vil undlade deres forehavende. Hvis midlet er identitetsskabende kommunikation, må vi svare tilbage med korrekt kommunikation.

DR, 2012; *"Cpr.dk angrebet af hackere"*.
Pastebin,2012;*"Dear citizens of Denmark"*.
Version 2, 2012; *"Anonymous slår til i Danmark: Vi har hacket CPR.dk og Atea"*.
Version 2, 2012; *"Dansk it-firma udsat for 'voldsom trafik' og flere forsøg på indbrud fra Anonymous"*.

7.3. Dating-tjenesten Sex.dk lækkede profiler

Brugernavne og passwords for over 30.000 brugere af datingtjenesten Sex.dk blev lækket på nettet efter et hackerangreb. Tjenesten kan ikke afvise, at dataene kan være blevet misbrugt.

Den 15. november lagde en person oplysninger om Sex.dk-brugere ud på Pastebin. Personen underskrev sig som #anondk, hvilket kan tyde på, at vedkommende opfatter sig som en del af Anonymous-bevægelsen. Men i modsætning til de fleste Anonymous-angreb er dette ikke begrundet med et ønske om at fremme en bestemt udvikling. Den eneste begrundelse for offentliggørelsen lød:

"Vi elsker alle sex, og her er 30.000, som søger det via sex.dk."

Administratorerne af Sex.dk opdagede lækken ved 12-tiden samme dag. De blokerede for alle de berørte profiler. Brugerne fik besked om, at de skulle bruge et nyt password ved næste login.

Bo Jacobsen, der er chef for Sex.dk, oplyser til Version2, at hackeren sandsynligvis har udnyttet SQL-injection til at få fat i dataene. Det vil sige, at der har været en sårbarhed i webstedets behandling af input fra brugerne, så indtastede data blev overleveret ufiltreret til databasen.

"For hver af de 31.385 berørte brugere oplyste listen brugernavn og password, der optrådte i klartekst. Det betyder, at de berørte brugere kan risikere at blive ofre for identitetstyveri."

For hver af de 31.385 berørte brugere oplyste listen brugernavn og

password, der optrådte i klartekst. Det betyder, at de berørte brugere kan risikere at blive ofre for identitetstyveri. Det kan ske, hvis de har brugt samme brugernavn (i dette tilfælde e-mailadresse) og password til andre tjenester. Så kan hackere afprøve kombinationerne af brugernavn og password på mail-tjenester, Facebook og andre tjenester, indtil der er gevinst.

Var hændelsen sket efter indførelsen af EU's kommende regler om personsikkerhed, kunne det være blevet en dyr fornøjelse for virksomheden bag Sex.dk. Det ville i så fald have medført et krav om, at samtlige af de berørte brugere skulle have været informeret. Endvidere kunne virksomheden være blevet pålagt en bøde.

DKCERT mener:

Organisationens websted er dens digitale ansigt udadtil, men ofte er det også blandt dens mest sårbare punkter. Ved lækagen af brugerdata fra Sex.dk var der som så ofte tidligere tale om en sårbarhed af typen SQL-injection, der blev udnyttet. Uden et egentligt motiv tyder det derfor på, at angrebet blev udført, blot fordi man kunne.

Vi mener, at de seneste års mange datalækager bør medføre et skærpet fokus på sikkerhed på organisationernes web- og databaseservere. Det gælder både løbende opdatering af software og tjek for kendte sårbarhedstyper. Der bør være skærpet fokus på sårbarheder som SQL- injection, da de potentielt kan give adgang til data i den bagvedliggende database.

Version 2, 2012; *"Datingchef indrømmer: Brugernavne og kodeord på Sex.dk kan være blevet misbrugt"*.
Version 2, 2012; *"Hackere afslører 30.000 danske brugere og kodeord fra Sex.dk"*.

7.4. Hul hos teleselskaber gav cpr-adgang

Webportaler hos teleselskaber gjorde det muligt at gætte sig frem til en persons cpr-nummer ud fra fødselsdatoen. Skønt hullet blev kendt i maj måned, fandtes det et halvt år senere stadig hos et par teleselskaber.

En række teleselskaber havde et sikkerhedshul, der gav uvedkommende adgang til at finde en persons cpr-nummer. Man skulle blot kende personens fødselsdato. Det udgør en sikkerhedsrisiko, fordi borgere ofte bliver bedt om at oplyse cpr-nummer for at legitimere sig. Dermed kan uvedkommende misbruge cpr-nummeret over for det offentlige.

Sikkerhedshullet lå i en proces til verificering af kundeoplysninger. En ny kunde hos teleselskabet skal indtaste sit cpr-nummer og adresse. Derefter tjekker systemet, at oplysningerne svarer til dem, der står i cpr-registret.

En uvedkommende kunne udnytte systemet ved at afprøve en fødselsdato sammen med en række muligheder for de sidste fire cifre. Efter en række forsøg kan man på den måde finde frem til personens cpr-nummer.

To studerende på IT-Universitet skrev i maj et program, der demonstrerede sårbarheden. Efter at de havde offentliggjort deres resultater, rettede nogle teleselskaber i deres løsning, så de efter tre forgæves forsøg lukker for adgangen i en halv time.

Men det betyder kun, at det tager to dage at finde et cpr-nummer, hvor det før kunne gøres på fem minutter, udtalte en af de studerende til Computerworld.

I oktober fandtes hullet fortsat hos teleselskaberne Oister og OK-Mobil. Juridisk direktør Nicholai Kramer Pfeiffer fra Telenor, der driver OK-Mobil, lovede, at selskabet inden årsskiftet ville hæve sikkerhedsniveauet.

Cpr-nummeret er grundlæggende en unik identifikation af den enkelte borger. Derfor bør det ikke benyttes som hverken brugernavn eller password til diverse webtjenester, der i flere tilfælde har vist sig at være sårbare. I forbindelse med NemID anbefales det for eksempel, at man ikke benytter sit cpr-nummer som bruger-ID, og det må ikke benyttes som password.

DKCERT mener:

Et sikkerhedshul i teleselskabernes brug af cpr-oplysninger illustrerer et grundlæggende problem med måden, cpr-nummeret mange steder benyttes på: Cpr-nummeret blev benyttet som kundeautentifikation og gav herved uvedkommende potentiel adgang til andres cpr-oplysninger. Det er et problem, fordi cpr-nummeret forventes holdt hemmeligt.

Cpr-nummeret er en unik borgeridentifikation, som grundlæggende bør holdes hemmelig. Derfor mener vi ikke, at det skal benyttes ved autentifikation på diverse webtjenester, hvor det ikke kan suppleres med anden legitimation. Grundlæggende bør borgeridentifikation som minimum foregå krypteret ved to-faktor identifikation ved noget, man ved (eventuelt cpr-nummeret), der suppleres med noget, man har (sygesikringsbevis, kørekort og lignende).

Computerworld, 2012; *"Stort sikkerhedshul: Så nemt kan man stjæle dit cpr-nummer"*.
Computerworld, 2012; *"Telefirmaer taget med bukserne nede: Anede intet om CPR-huller"*.
NemID; *"Bruger-id og adgangskode"*.
Version 2, 2011; *"Prosa advarer medlemmer om CPR-login i NemID - brugte det selv"*.

7.5. Nyt råd for informationssikkerhed så dagens lys

En række stærke organisationer står bag det nystiftede Rådet for Digital Sikkerhed. Rådet har til formål at samle indsatsen for bedre it-sikkerhed og privacy i Danmark.

Fredag den 23. november stiftede en række fremtrædende personer fra it-sikkerhedsverdenen Rådet for Digital Sikkerhed. Det er en privat forening, der har til formål at skabe en stærk og bred platform for en

kvalificeret debat og udspil til offentligheden. Det handler først og fremmest om, hvad der skal til, for at Danmark fortsat kan udnytte teknologiens muligheder på en tryg måde.

Den stiftende generalforsamling valgte Birgitte Kofod Olsen, CSR-chef i Tryg, som formand. Shehzad Ahmad, der er chef for DKCERT, blev næstformand.

Bag initiativet står Forbrugerrådet, DI ITEK, IT-Branchen, Dansk ITs Råd for IT- og Persondatasikkerhed og Rådet For Større IT-Sikkerhed. Dermed er der tale om den hidtil bredest forankrede indsats for it-sikkerhed i Danmark.

Rådet vil arbejde på at få indflydelse på den samlede it-sikkerhed i Danmark. Dermed bliver det en efterfølger for de råd og udvalg, Forskningsministeriet tidligere har haft på området.

Ministeriets råd havde en officiel rådgivende rolle. De forskellige råd i privat regi har forsøgt at påvirke udviklingen gennem rådgivning og offentlige udmeldinger. Som noget nyt kan organisationerne bag dem nu tale med én stemme. Nogle af initiativtagerne vil fremover lægge al deres indsats i det nye råd. Andre vil sideløbende have egne aktiviteter.

DKCERT mener:

Vi har tidligere efterspurgt mere samarbejde mellem de forskellige råd og udvalg, der herhjemme arbejder med informationssikkerhed. Derfor hilser DKCERT Rådet for Digital Sikkerhed velkomment. Rådet blev oprettet i november måned og er en platform for samarbejde og kommunikation om, hvordan vi i fællesskab løser borgernes og organisationernes udfordringer på internettet. Med fælles viden kan der nemlig skabes rum for bedre individuelle løsninger.

Vi mener, at rådets største fordel, at danske it-sikkerhedsinteresserede nu kan tale med én stemme. Initiativtagerne er bredt forankret i erhvervsliv og organisationsverdenen, så rådet kan udtale sig med stor vægt. Derfor venter vi, at der bliver lyttet til rådets anbefalinger.

Digital Sikkerhed, 2012; "*Nyt it-råd skal sikre tryg digitalisering*".

7.6. Det handler om penge

Netbanktyverier samt tyveri og misbrug af kreditkortinformationer koster hvert år et tocifret millionbeløb i Danmark alene. Det er mere indbringende og risikoen er mindre i forhold til traditionel kriminalitet. Udviklingen af specialiserede værktøjer og tjenester har medført, at det ikke kræver de samme tekniske færdigheder som tidligere.

I de første tre kvartaler af 2012 blev 131 danske netbankkonti tømt for i alt 3.640.279 kroner, hvilket er det højeste beløb siden indførelsen af NemID. Overordnet set var der tale om tre angreb, hvor kontohavernes computere blev inficeret med avanceret malware. Bagmændene formodes at operere fra udlandet. Indtil videre er ingen blevet fanget.

Til sammenligning blev der i hele 2011 begået 116 røverier mod danske pengeinstitutter. Det typiske udbytte var ifølge TV 2 på mellem 30.000 kr. og 50.000 kr. Det giver et estimeret samlet udbytte på cirka 5.000.000 kr. To tredjedele af bankrøverierne bliver ifølge Finansrådet opklaret.

"Ovenstående illustrerer, at internetkriminalitet i sammenligning med traditionel kriminalitet er en god forretning."

Ovenstående illustrerer, at internetkriminalitet i sammenligning med traditionel kriminalitet er en god forretning. Særligt i betragtning af, at både straffen og risikoen er mindre, og det gennemsnitlige udbytte ved bankrøverier er faldende.

I tillæg til ovenstående blev 7.328 dankort i 2011 misbrugt til handel på internettet til en værdi af i alt 10.866.000 kr. Det vil sige dankort, hvor kortinformationerne er fremskaffet ved phishing, afluret med malware på brugernes computer eller ved hacking af netbutikker, hoteller og lignende, som modtager og opbevare denne type informationer i deres it-systemer.

Beløbet er gennem de sidste år steget. I første halvdel af 2012 blev der på denne måde misbrugt dankort for 8.168.000 kroner. Hertil kommer misbrug af internationale kreditkort som for eksempel MasterCard og Visa.

Selvom den internetkriminelle værdikæde er lang, og bagmændenes profit i sidste ende måske kun er halvdelen af udbyttet, er der tale om en god forretning. Også når man tager i betragtning, at denne kriminalitetsform er global og kan udføres stort set risikofrit samtidig i flere lande.

Vi har en forventning om, at problemet vil vokse. Særligt når man tager i betragtning, at specialisering af den internetkriminelle værdikæde har medført, at der i dag ikke stilles de samme krav til den kriminelles tekniske færdigheder. Som et eksempel på denne specialisering er udbredelsen og brugen af avancerede exploit kits som blandt andet BlackHole.

BlackHole gør det muligt fra en kompromitteret hjemmeside at udnytte flere sårbarheder på de besøgendes maskiner med det formål at inficere dem med malware. Exploit kittet, der af Sophos blev vurderet at være ansvarlig for 28 procent af alle webrelaterede trusler i perioden oktober 2011 til maj 2012, kom i september i en ny version. Et abonnement på BlackHole inkluderer support og løbende opdatering med nye exploits. En hostet løsning koster 500 euro for en måned eller 1.500 euro for et helt år, hvis man selv hoster exploit kittet.

Tilsvarende kan de programmer, man ønsker at inficerer brugerne med, ifølge en rapport fra Trend Micro købes i den russiske undergrund. Som eksempel kan trojanske heste eller ransomware købes for helt ned til

otte dollars.

DKCERT mener:

Tyveri og misbrug af kreditkortinformationer samt netbankindbrud er en god forretning, der er næsten risikofri i forhold til for eksempel bankrøverier. Angrebene kan udføres samtidig i flere lande, uden at man konfronteres med potentielle ofre. Når udviklingen har gjort, at de tekniske barrierer for indtræden på en internet kriminel løbebane er faldet, medfører det, at problemet er stigende.

DKCERT mener, at oplysning er vejen frem, da det ofte er borgernes uvidenhed, uopmærksomhed eller uforsigtighed, der er årsag til, at de ender som ofre for internetkriminalitet. Hvordan vi gør det mest effektivt, eller i hvilket regi awareness rettet mod borgerne skal udføres, er til diskussion. I sidste ende er det både i bankernes, kreditkortselskabernes, det offentliges og det øvrige erhvervslivs interesse, at deres brugere benytter teknologien med viden og omtanke.

Finansrådet, 2012; *"Netbankindbrud - statistik"*.
Finansrådet, 2012; *"Røveristatistik"*.
Nets, 2012; *"Dankort-misbrug de første seks måneder af 2012"*.
Softpedia, 2012; *"BlackHole Exploit Kit 2.0 Made available, price remains the same"*.
Sophos, 2012; *"Exploring the Blackhole Exploit Kit"*.
Trendmicro, 2012; *"Russian underground 101"*.
TV 2, 2012; *"Bankrøvere får mindre i udbytte end før"*.

7.7. Norge fik national strategi for it-sikkerhed

Den norske regering har indført en national strategi for informationssikkerhed. Med strategien følger en handlingsplan, der angiver, hvor der skal sættes ind og prioriteres.

Den 17. december udsendte Norges regering et dokument på 32 sider: "Nasjonal strategi for informasjonssikkerhet." Dermed har landet nu en samlet strategi for, hvordan det vil øge informationssikkerheden.

Samtidig kom der et supplement i form af en handlingsplan. Den indeholder en prioriteret liste over, hvor der skal sættes ind.

Bag strategien står fire ministerier: Justits- og beredskabsministeriet, Forsvarsministeriet, Trafikministeriet og Fornyelses-, administrations- og kirkeministeriet.

Strategien har fire formål:

- Alle aktører skal kende risikobilledet og sikre deres systemer og netværk ud fra det.
- Myndighederne skal sørge for, at den nationale it-infrastruktur er godt sikret. Det skal ske gennem organisering, tilstrækkelig brug af ressourcer, gode rammevilkår og effektive tiltag.
- Private og offentlige virksomheder skal indbygge sikkerhed og robusthed i deres informationsinfrastruktur. Det skal både ske for at sikre deres egen virksomhed og for at beskytte kunder og brugere.
- Den enkelte skal tage et selvstændigt initiativ for at beskytte sin identitet, sine personoplysninger og økonomiske værdier på nettet.

Blandt de nye udfordringer for informationssikkerheden, som strategien skal tage hånd om, nævnes blandt andet mobile enheder, øget brug af internet, og at nedbrud er mere kritiske for samfundet. Endvidere giver nye tjenester og platforme uigennemsigtighed, der er øget brug af udenlandske tjenesteudbydere, markedet for it-kriminalitet vokser, og truslen fra spionage og sabotage øges.

Handlingsplanen lægger op til, at alle it-tjenester, der er kritiske for samfundet, skal kortlægges og risikovurderes. Landets nationale sikkerhedsmyndighed (NSM) skal udvikles, så den kan arbejde mere helhedsorienteret. Det kræver bedre datagrundlag, hvor de forskellige sektorer opretter CSIRT-enheder (Computer Security Incident Response Services), der rapporterer til NSM.

Det er anden gang, Norge lægger en national strategi på sikkerhedsområdet. Den første kom i 2003. Bag den stod Erhvervs- og handelsministeriet, Forsvarsministeriet og Justits- og politiministeriet.

DKCERT mener:

Det er imponerende, at Norge kan skabe fælles fodslag om en samlet national strategi for informationssikkerhed. Den tilhørende handlingsplan konkretiserer de gode intentioner og øger sandsynligheden for, at de faktisk bliver ført ud i livet.

DKCERT mener, at den danske regering med fordel kan kigge mod nord og lade sig inspirere til en tilsvarende dansk strategi. Det har vi opfordret til flere gange, specielt i sidste års trendrapport, hvor vores anbefaling til beslutningstagerne var, en national it-strategi, der inkluderer det offentliges, organisationernes og borgernes informationssikkerhed.

Norsk regering, 2012; *"Nasjonal strategi for informasjonssikkerhet"*.
Norsk regering, 2012; *"Nasjonal strategi for informasjonssikkerhet - Handlingsplan"*.

8. Det eksterne perspektiv

Hvert år bruger danske organisationer millioner af kroner på at beskytte deres systemer og data, således at både tilgængelighed, integritet og fortrolighed kan opretholdes. På tværs af forretningsområder, standarder og systemer er det grundlæggende de samme problemstillinger, man står overfor. Variationen ligger i de enkelte organisationers risikovillighed og aktuelle behov.

Derfor har vi i nærværende afsnit givet ordet til en række eksterne skribenter, der fortæller om, hvordan de konkret håndterer specifikke aspekter af informationssikkerhed. Målet er at gøre vores perspektiv på informationssikkerhed mere åbent og brugbart. Selv om deres løsninger ikke passer til alles behov, håber vi, at du kan lære af deres overvejelser.

Bring Your Own Device (BYOD) er et begreb, der i disse år vinder indpas, også i danske organisationer. Fra Roskilde Universitet fortæller it-sikkerhedskonsulent Henrik Jensen om, hvilke overvejelser det her har givet anledning til, at brugerne i stigende grad ønsker at bruge deres eget udstyr i arbejdsmæssige sammenhænge. For hvordan er det med sikkerheden, når det ikke længere er universitetet, der ejer udstyret? Hvem ejer for eksempel de data og applikationer, som placeres på brugernes udstyr?

Herefter fortæller informationssikkerhedschef Henrik Larsen fra Københavns Universitet om, hvordan man her har organiseret sit sikkerhedsberedskab. Hvordan man på universitetet benytter en erfaringsbaseret tilgang til risikovurdering, som danner grundlag for udfærdigelse af konkrete beredskabsplaner. Et væsentligt aspekt af dette arbejde er at udbrede kendskabet til og forståelsen for beredskabsplanerne, således at man sikrer, at de også bliver fulgt, når det er aktuelt.

It-sikkerhedsansvarlig Morten Als Pedersen fra Danmarks Tekniske Universitet (DTU) fortæller herefter om deres udfordringer ved at skulle overgå fra DS484 til ISO-standarden. Hvordan de ved overgangen til den nye standard forsøger at integrere en række nye centre og institutter i en eksisterende decentral sikkerhedsstruktur. Ledelsens aktive involvering og udbredelse af politikkerne til universitetets ansatte og brugere er her centrale udfordringer.

På mange måder er viden, bevidsthed og kommunikation gennemgående temaer for afsnittets tre første artikler. Det hvad enten det handler om at ekstrahere viden fra tidligere erfaringer, som benyttes ved udfærdigelse af risikovurderinger, politikker eller beredskabsplaner, eller hvordan sikkerhedsbevidste medarbejdere er en forudsætning for beskyttelse af en perimeter, der i stigende grad er flyttet til deres egne enheder og installationer.

Netop dette aspekt berører den sidste artikel i dette afsnit. Gennem de sidste mange år er der med varierende succes gennemført awareness-kampagner rettet mod danske organisationers ansatte. Nogle har været en succes, mens andre er fejlet, fordi vi ikke forstod den grundlæggende præmis: At informationssikkerhed ikke er relevant, blot fordi det er det, der bliver kommunikeret om. Igen er der andre kampagner, vi ikke ved noget om, fordi det er vanskeligt efterfølgende at lave effektmålinger, da vi ikke kan dokumenterer sammenhænge mellem årsager og virkninger.

Til at belyse dette emne giver Caspar Bock fra reklamebureauet DDB Copenhagen sine perspektiver på virkemidlerne i den vellykkede oplysnings- og holdningskampagner. Langt hen ad vejen handler det om at tage udgangspunkt i brugeren snarere end den omgivende kontekst for herved at gøre emnet aktuelt, relevant og brugbart for modtageren. At tale til den enkeltes følelser i stedet for at formidle informationssikkerhed i en teknologisk sammenhæng.

Vi håber, at ovenstående perspektiver vil bidrage med aspekter af informationssikkerhed, som er brugbare for dig.

8.1. De ansattes brug af eget udstyr på RUC

Af Henrik Jensen, it-sikkerhedskonsulent, Roskilde Universitet (RUC)

En rapport fra Gartner beskriver Bring Your Own Device (BYOD) som en trend, der er kommet for at blive. Trenden har skabt nye muligheder for organisationer, der ønsker at øge produktiviteten gennem mobile medarbejdere og eksterne kontorer. De opfordrer organisationerne til at styrke deres sikkerhedspolitikker.

Også på Roskilde Universitet (RUC) er der en tendens til, at brugerne ønsker at benytte deres eget udstyr. At give de ansatte mulighed for at få adgang til universitetets e-mail, forretningskritiske applikationer og data vil gøre dem mere produktive og effektive. Det giver de omkostningstunge kostcentre, som vores it-afdelinger også er, en kærkommen forstærkning i form af sparede udgifter til indkøb af hardware og support.

På RUC har vi derfor accepteret præmisserne omkring BYOD og ser os nødsaget til at udforme en strategi, som har fokus på at reducere risici og administration. Det betinger den rigtige balance mellem fleksible løsninger og informationssikkerhed. Strategien skal sikre, at der er balance mellem risiko og fordele ved BYOD og belyse universitetets muligheder for at:

- Genvinde bevidsthed og kontrol med administration af data.
- Udbrede kendskab til begrænsninger og forpligtelser på personlige enheder.
- Dele informationer og data sikkert.
- Beskytte data, uanset om udviklingen går mod context-aware sikkerhed.

Med et paradigmeskift for vores it-anvendelse har vi fået lejlighed til at bringe informationssikkerhed på dagsordenen. Vi bliver nemlig nødt til at gentænke den måde, hvorpå vi udnytter og sikrer de mange

informationer og data, som de fleste organisationer bygger deres forretningsmodel på.

Stjålne og bortkomne enheder er blandt de udfordringer, som blinker rødt hos de fleste informationssikkerhedsansvarlige i forbindelse med accepten af BYOD. Men også de juridiske problemstillinger omkring, hvem der ejer data, som opbevares på enheder, der ejes af medarbejderen, og ikke mindst hvordan dette håndteres, når medarbejderen forlader universitetet, bør tages alvorligt.

De fleste sikkerhedsteknologier er designet og installeret til at stoppe hackere, spioner, phishere og svig. De kan dog blive ineffektive og give falsk tryghed, eller kan blive kompromitteret af menneskelige svagheder som uopmærksomhed, uvidenhed eller inkompetence. En teknisk sårbarhed kan udbedres, men mennesker uden basal bevidsthed (awareness) og uddannelse repræsenterer de største sårbarheder i en ellers godt teknisk sikret infrastruktur.

Efterhånden som nye teknologier kommer på markedet, er det derfor vigtigt at sikre sig, at medarbejderne forstår, hvordan man trygt bruger dem. Et ofte overset spørgsmål i forbindelse med indførelsen af ny teknologi er, at grænsen mellem det personlige og professionelle liv er sløret. Mobilitet og sociale medier repræsenterer på RUC to yderst relevante risikoområder, der i stigende grad kan involvere overtrædelser af lov- og myndighedskrav. Det er vores erfaring, at mange overtrædelser er resultatet af manglende bevidsthed blandt medarbejderne.

"Vi har den holdning, at bevidsthedstræning er en del af informationssikkerheden, som ikke kun skal beskytte informationer og data på arbejdspladsen, men også på medarbejderens private enheder."

På RUC er uddannelse og bevidstheden naturlige elementer i vores informationssikkerhedsstrategi. Vi har den holdning, at bevidsthedstræning er en del af informationssikkerheden, som ikke kun skal beskytte informationer og data på arbejdspladsen, men også på medarbejderens private enheder. Efter vores erfaringer fungerer det nemlig bedst, når medarbejderne opfordres til at tænke på informationssikkerhed i forbindelse med hjem og familie.

En central udfordring ved BYOD er, at når en enhed sluttes til netværket, kan vi ikke være sikre på, hvad den er eller hvordan den vil opføre sig. Problemet bliver ikke mindre, hvis medarbejderne henter potentielt usikre programmer til enhederne og dermed øger risikoen for kompromittering af virksomhedens data. På RUC planlægger vi derfor en handleplan for håndhævelse og udarbejdelse af politikker for behandling af informationer og data.

Handleplanens målsætning er at skabe bevidsthed om arbejdet med informationer og data og skal indarbejdes i alle forretningsgange. Den går i korte træk ud på at gøre det klart og nemt for medarbejderne at vide, hvornår, hvorfor og hvordan de kan få adgang til informationer og data.

Følgende forretningsgange påtænkes for eksempel indført for dels at mindske sandsynligheden for tab af data og dels som støtte til medarbejdernes tilgang til BYOD:

- Indføre og håndhæve en enkel og forståelig BYOD-politik. Er der for eksempel kun bestemte enheder, som er tilladt? Hvem skal eje og betale for enhederne, og hvordan supporteres de? Hvilke applikationer er tilladt og hvilke er forbudt? Niveauer af support?
- Klarhed over hvem der ejer hvilke applikationer og data. Skal universitetet for eksempel erstatte personlige musikfiler, programmer eller billeder, der fjernslettes på en tabt eller stjålet enhed?
- Beskyttelse med adgangskode og regler for at slette enhedens indhold efter for eksempel 10 forkerte forsøg.
- Indførelse af teknologi som Mobile Device Management (MDM), der kan adskille personlige og virksomhedsspecifikke data og give kontrol med organisationsspecifik data.
- Forretningsgange til håndtering af fratrædelser. For eksempel sletningen af organisationsspecifikke applikationer, informationer og data fra enheder på BYOD-platformen under hensyntagen til medarbejderens egne applikationer, informationer og data.

Der er mange løsninger til Mobile Device Management (MDM) og Mobile Application Management (MAM), som vurderes på RUC. Vurderingskriterierne indeholder parametre, som kan tilgodese, hvordan de organisationsspecifikke systemer, informationer og data beskyttes og tage hensyn til, hvem der ejer enheden.

På RUC mener vi, at et MDM-system blandt andet skal udføre og lette følgende administrative opgaver:

- Kryptering af data på mobile enheder.
- Fjernlåsning og/eller -sletning af enheden.
- Realtidsfjernbetjening og -administration. Herunder lockdown af kamera, SD-kort, Bluetooth og Wi-Fi.
- Begrænse adgangen til enhedens applikationer, data og informationer.
- Håndhæve adgangskontrol, enhedens synlighed og blokering af adgang til enhedens e-mail med mere.
- Vedligeholdelse af log og revisionsspor.
- Sporing af tabte og stjålne enheder.

Ovennævnte funktioner er effektive, når enheden ejes af organisationen, men der er juridiske problemstillinger, som skal adresseres, når enhederne tilhører de ansatte. Derfor ser vi et MDM-system som en sandkasseløsning, hvor organisationens systemer, informationer og data er "låst" i en kasse, der er dedikeret for anvendelse af organisationen.

Sandkasseløsningen tænkes fulgt op af en samtykkeerklæring, som præciserer retningslinjerne for installation og brug, tillige med roller og ansvar i forbindelse med adgangen til organisationens systemer og data fra den privatejede enhed.

De tekniske løsninger er i mange situationer gode værktøjer, men bør ikke stå alene. Det hele begynder med brugernes tilgang til brugen af applikationer, informationer og data. Ud over den teknologiske vinkel bør der fokuseres på brugere og processer, der indgår i det nye mønster for fleksibel udnyttelse og adgangen til applikationer, informationer og data.

BYOD er et paradigmeskift i forhold til, hvordan vi anvender systemer, informationer og data, hvordan hardwaren anvendes, finansieres og supporteres, samt hvor ejerforholdet er placeret. Organisationens perimeter er rykket ud hos brugerne og har gjort sandsynligheden for eksponering af organisationens intellektuelle ejendom større. Hermed sker der også et skift i tilgangen til beskyttelse af virksomhedens systemer, informationer og data. Det giver de sikkerhedsansvarlige muligheder for at sætte informationssikkerhed på dagsordenen.

De sikkerhedsmæssige udfordringer grundet den mindre synlige perimeter er ikke et isoleret problem for den enkelte organisation. Derfor er et nationalt fokus på informationssikkerhed, især i relation til mobile enheder og sammensmeltningen af privat- og arbejdsliv relevant for alle, og også et fælles ansvar. Især med tanke på de juridiske problemstillinger, som vil dukke op i kølvandet på, at brugerne benytter deres eget udstyr. Her tænkes især på de tvister, der vil opstå mellem arbejdsgiver og arbejdstager omkring, hvem der ejer hvad.

Gartner, 2012; "*Gartner survey shows BYOD is top concern for enterprise mobile security*".

8.2. Beredskabsplanlægning på KU – et udviklingsområde

Af Henrik Larsen, informationssikkerhedschef, Københavns Universitet (KU)

Københavns Universitet (KU) bygger sin informationssikkerhed på den internationale standard ISO 27001 og har en risikobaseret tilgang til sikkerhedsarbejdet. Beredskabsplanlægningen bygger således på et system af lokalt udarbejdede risikovurderinger.

Informationssikkerhedsorganisationen på KU er opbygget med decentral forankring. Det vil sige, at der er udpeget en lokal informationssikkerhedsansvarlig på hvert institut, selvstændige forskningscenter eller forvaltningsafdeling. Efter de seneste organisationsændringer er der cirka 70 lokale informationssikkerhedsansvarlige.

Risikovurderingerne foretages dels af de lokale informationssikkerhedsansvarlige, der vurderer forretningsrisikoen, dels af den driftsansvarlige for det enkelte informationsaktiv. Blandt andet på baggrund af de hændelser, der er registreret i den foregående periode og på erfaringer i øvrigt vurderes sandsynligheden for brud på informationssikkerheden. Såvel forretningsrisiko som sandsynlighed vurderes for hvert enkelt informationsaktiv særskilt for brud på fortrolighed, integritet og tilgængelighed.

Forretningsrisiko, her forstået som alvorligheden for den daglige forretningsdrift ved et brud på et sikkerhedselement for en enheds informationsaktiver, ganget med sandsynligheden for et sådant brud giver en risikofaktor. Den danner grundlag for udformning af den enkelte enheds beredskabsplan.

KU har for nogle år siden med hjælp fra konsulentfirmaet Devoteam udarbejdet en drejebog og skabelon for beredskabsplaner. Hver af de cirka 70 enheder i informationssikkerhedsorganisationen udarbejder og vedligeholder årligt beredskabsplaner ud fra et business continuity-perspektiv. Fokus er på at imødegå virkningerne af et større brud på informationssikkerheden og at videreføre de forsknings-, undervisnings- og formidlingsmæssige samt administrative funktioner i videst muligt omfang. Derfor er der særlig fokus på tilgængeligheden til vitale informationsaktiver.

Enheder, der har ansvaret for driften af informationsaktiver, udarbejder desuden beredskabsplaner med et disaster recovery-perspektiv. Det er især, men ikke kun, Koncern-it og de fire fakultet-it-afdelinger. Fokus er på at genetablere normal drift efter et potentielt sikkerhedsbrud. Der er blandt andet udarbejdet specifikke disaster recovery-planer for de større it-systemer.

Det seneste år har givet erfaringer med brug af beredskabsplanen i forbindelse med et par større it-nedbrud. De opsamlede erfaringer indgår i revisionen af ikke mindst Koncern-its beredskabsplan. Hændelserne har dog også vist nødvendigheden af, at de lokale enheder vedligeholder og i situationen anvender beredskabsplaner med fokus på at videreføre de løbende opgaver. For eksempel gennemførelsen af eksaminer uden adgang til for eksempel lokalefordelingssystemet, som det var tilfældet i januar 2012.

"Når man oplever et større it-brud eller et andet væsentligt brud på informationssikkerheden, mindskes følgevirkningerne bedst gennem rettidig, fyldestgørende og ærlig kommunikation til alle berørte parter."

Erfaringen fra hændelserne er, at der skal lægges særlig vægt på en effektiv kommunikationsplan som en del af beredskabsplanen. Når man oplever et større it-brud eller et andet væsentligt brud på informationssikkerheden, mindskes følgevirkningerne bedst gennem rettidig, fyldestgørende og ærlig kommunikation til alle berørte parter. Det opnår man bedst, hvis man har forberedt sig. kommunikationsplanen skal tage stilling til, hvem der har ansvaret for at kommunikere og hvem, der skal orienteres om situationen. Og telefonlister skal vedligeholdes!

En væsentlig, fremadrettet opgave for informationssikkerheds-organisationen på KU er løbende at videreudvikle konceptet for beredskabsplanlægning, at udbrede forståelsen for betydningen af gode, risikobaserede planer og ikke mindst at udbrede kendskabet til planerne og sikre at de bliver brugt, når uheldet er ude.

Målet nås bedst gennem en løbende erfaringsudveksling, såvel internt mellem KUs interessenter som med eksterne samarbejdspartnere, ikke mindst i universitetssektoren.

KUs Informationssikkerhedsorganisation:

Informationssikkerhedsorganisation (ISO) på Københavns Universitet består af en lokal informationssikkerhedsansvarlig på hvert institut, selvstændige forskningscenter eller forvaltningsafdeling. De cirka 70 lokale informationssikkerhedsansvarlige indgår i lokale informationssikkerhedsudvalg på fakultetsniveau.

De fem lokale informationssikkerhedsudvalg er repræsenteret i Informationssikkerhedsudvalget (ISU), der desuden består af universitetsdirektøren som formand, vicedirektøren for koncern-it og repræsentanter for Hovedsamarbejdsudvalgets B-side. Informationssikkerhedschefen er sekretær for udvalget og repræsenterer desuden det ene lokale udvalg.

Informationssikkerhedsudvalget (ISU) refererer til KUs Ledelsesteam, der består af rektor, prorektor, universitetsdirektøren og dekanerne for de seks fakulteter. Hermed sikres den ledelsesmæssige forankring af informationssikkerhedsarbejdet, som ISO 27001 foreskriver.

Københavns Universitet; *"Beredskabsstyring"*.
Københavns Universitet; *"Informationssikkerhedsorganisationen ISO"*.

8.3. DTU's overgang til ISO27001-standarden

Af Morten Als Pedersen, it-sikkerhedsansvarlig, Danmarks Tekniske Universitet (DTU)

Som alle andre statsinstitutioner kan DTU forvente at blive mødt med krav om at overgå fra DS484 til ISO27001 med den næste revision af ISO-standarden. Den forventes at foreligge i løbet af 2013. Overgangen vil forventeligt blive krævet færdiggjort inden for 12 måneder fra det tidspunkt, hvor den nye version foreligger.

DTU har valgt at implementere sit informationssikkerhedssystem i al væsentlighed på institutniveau. Det betyder, at der på universitetsniveau kun findes en fælles informationssikkerhedspolitik, en fælles regelsamling samt nogle få fælles procedurer. Eneste personaleressource på universitetsniveau har indtil for nylig været en it-sikkerhedskoordinator.

Resultatet af den igangværende revision af ISO er ikke kendt i detaljer. Den forventes dog ikke at medføre grundlæggende strukturelle ændringer i ISO27000-serien. DTU valgte derfor at påbegynde overgangen i midten af 2012. Det arbejde forløber i to spor:

Det ene gælder nydannede institutter/centre, der er etableret ved organisatoriske ændringer i løbet af det seneste år. De har medført dannelsen af en række nye enheder, som i forvejen stod med opgaven at etablere et it-sikkerheds-styresystem, da de ikke længere er underlagt de tidligere organisatoriske rammer. De nydannede enheder har valgt at etablere informationssikkerhedssystem efter ISO2700X.

Det andet spor omfatter de eksisterende institutter/centre. De har alle veletablerede og velintegrerede systemer til håndtering af informationssikkerheden, som er etableret i overensstemmelse med DS484. For de enheder er der valgt en anden implementeringsstrategi – løbende revision af enkelte elementer efterhånden som de alligevel skal revideres som del af processen med dokumentrevision i DS484. En forudsætning for dette arbejde er tre opgaver:

- Etablering af et system, der skal sikre ledelsens aktive og personlige deltagelse i arbejdet med at udvikle, implementere og formidle informationssikkerheden.
- Fornyelse/revision af den eksisterende risikovurdering – med den forøgede ledelsesfokus og involvering, der kræves i ISO2700X.
- En plan for den trinvise implementering af konsekvenserne ved den SOA (Statement of Applicability), der skal udarbejdes på baggrund af risikovurderingen.

"De første tidlige erfaringer med det arbejde er, at der efter en periode med reel skepsis og modstand imod den forøgede ledelsesindsats kan spores en vis entusiasme."

De første tidlige erfaringer med det arbejde er, at der efter en periode med reel skepsis og modstand imod den forøgede ledelsesindsats kan spores en vis entusiasme. Særligt ved udsigten til, at diskussionen af informationssikkerhed i højere grad får karakter af forretningsmæssigt interessante aspekter end informationsteknologiske forhold. Håbet er, at vi med ISO får en tættere kobling begge veje i styresystemet:

- Større gennemsigtighed for ledelsen, der fremover skal forholde sig til ledelsesmæssige parametre som for eksempel afvejning af økonomi, risiko for imagetab og et oplevet it-serviceniveau.
- At it-afdelingen vil opleve klarere udmeldinger om ledelsens forventninger, så det ikke som hidtil har været nødvendigt for it-afdelingen at påtage sig risikoen ved at oversætte ledelsens krav til operationelle parametre i hverdagen.

En konkret udfordring i det kommende arbejde er formidlingsopgaven, hvor ledelsen med overgangen til ISO får et mere konkret og direkte ansvar. Formidlingen skal sikre kendskab til procedurer og forretnings-

gange, men mindst lige så vigtigt: at der er den fornødne opmærksomhed på vigtigheden af, at alle medarbejdere støtter op om den fælles opgave. Det er vores erfaring, at det er vigtigt at have gode tekniske sikringsforanstaltninger. Den store forbedring af informationssikkerheden opnås dog kun ved at kombinere dem med awareness-aktiviteter. For at sikre udbredelse af politikkerne til medarbejderne i både ord og handling, vil der derfor være fokus på formidling.

En konsekvens af den måde, DTU i dag har implementeret DS484 på er, at der findes cirka 25 relativt uafhængige informationssikkerhedsstyresystemer. De er alle udarbejdet på den snævre fælles basis, men er tilpasset det enkelte instituts selvstændige risikovurdering. Her har ledelsen på de enkelte institutter inddraget det lokale trusselsbillede i etableringen af sikringsforanstaltninger, udarbejdelse af it-sikkerhedshåndbogens procedurer med videre.

Det har på den ene side som konsekvens, at der lokalt er foretaget ledelsesmæssig stillingtagen på baggrund af det lokale trusselsbillede, som det fordres under ISO2700X. På den anden side har opdelingen også medført, at der ikke er tilstræbt en så høj grad af harmonisering i valget af sikringsforanstaltninger og implementeringen af disse, som det egentlig var muligt. Det risikerer at påvirke mulighederne for etableringen af for eksempel fælles overvågningssystemer eller fælles arkiveringsløsninger i negativ retning.

Det er ikke tanken at ændre på den decentrale struktur, men der vil i den kommende proces med fordel kunne fokuseres på mulighederne for at samordne lokale løsninger på en måde, der i højere grad tillader etableringen af fælles sikringsforanstaltninger. Ud over den åbenlyse økonomiske fordel ved stordrift vil det også gøre det muligt at stimulere videndeling og deling af personaleressourcer på tværs af institutionen. Tilsvarende vil man formentlig også koordinere awareness-kampagner på tværs af institutter/afdelinger.

Også bredere inden for universiteterne i Danmark kan man med fordel afsøge mulighederne for harmonisering som baggrund for opbygning af fælles systemer. Der er i høj grad tale om sammenfaldende problemstillinger i denne sektor både inden for den traditionelle it-drift og inden for arbejdet med informationssikkerhed. Der er i dag et samarbejde, og denne samarbejdsflade vil blive søgt integreret i det kommende arbejde med informationssikkerhed på DTU.

8.4. Oplysnings- og holdningskampagner på lavinteresseområder

Af Caspar Bock, Creative, DDB Copenhagen

Mange oplysnings- og holdningskampagner på lavinteresseområder slår fejl. Således også inden for informationssikkerhedsområdet. Heldigvis er der masser af eksempler på det modsatte.

Historien er fyldt med beviser på, hvordan god vinkling og kreativ tænkning har gjort alt fra forsikringssammenligning til kapitalpension til interessante samtaleemner omkring middagsbordene.

Spørgsmålet er så, hvordan vi gør det samme for informationssikkerheden? Og ikke bare omkring middagsbordene, men også i kantinerne rundt omkring i de danske organisationer, hvor de ansatte har muligheden for at bidrage.

Lad os nå til den vigtigste erkendelse først: Informationssikkerhed er ikke et begreb, der sender pulsen i vejret hos den almindelige dansker. Vil man have nogen til at lukke ørerne på stedet, skulle der til gengæld være ret gode chancer: *"Nu skal du høre lidt om sikkerhed på nettet"*...

Hvis man selv brænder for emnet og alle de mange spændende facetter, det utvivlsomt rummer, vil det kræve en vis tolerance at nå til denne erkendelse. At forbrugerne og organisationernes ansatte dybest set er ligeglade. At det ikke ændrer adfærd blot at informere.

Men erkendelsen er afgørende. God kommunikation handler som bekendt om at tale til menneskers følelser. Og hvis emnet ikke gør det i sig selv, kan vi kun nå i mål ved at bygge et lag oven på informationen, der gør.

"Lidt provokerende sagt har kriminelle hjerner formentlig haft større held med at vække forbrugernes interesse for informationssikkerhed end hidtidige oplysningskampagner på området."

Et godt sted at starte her vil være ved at vende problemstillingen på hovedet og forstå, at området først bliver relevant for de fleste, når skaden er sket. Lidt provokerende sagt har kriminelle hjerner formentlig haft større held med at vække forbrugernes interesse for informationssikkerhed end hidtidige oplysningskampagner på området.

Tag f.eks. netbanken. Du logger på en almindelig tirsdag aften og opdager, at der er blevet overført 22.000 kr. til en konto i Hviderusland.

Eller du støder på dine private feriebilleder på nettet en måned efter at have gemt dem på Dropbox.

Der skal i princippet ikke meget til, før informationssikkerhed på et splitsekund går fra lav-interesse til absolut top-prioritet. En god oplysningskampagne formår at levendegøre dette.

Et andet eksempel, der er værd at fremhæve, er Anonymous. Bevægelsens erklærede kamp for frihed og retfærdighed i en global krisetid har nærmest Star Wars-lignende dimensioner, og deres fremgangsmåde resonerer smukt med en tidsånd fuld af apati over for samfundets magtinstitutioner. Anonymous-bevægelsen leverer storytelling på et højere plan end de fleste globale brands, uanset hvad man så måtte mene om deres aktiviteter i øvrigt.

De ovenstående eksempler tjener som bevis for, at det nemt kan lade

sig gøre at bringe informationssikkerhed på dagsordenen, når man pakker kernebudskabet ind i et emotionelt og relevant omsvøb.

Lad mig komme med et eksempel på, hvordan vi tidligere har løst lignende problemstillinger på DDB. I 2011 fik vi til opgave at promovere Krak.dk's nye søgefunktion. Briefen var simpel: få folk til at søge efter produkter på Krak.

Udfordringen var, som det også er tilfældet med informationssikkerhed, at vi havde at gøre med et budskab, som forbrugerne overhovedet ikke var interesserede i. Traditionel kommunikation havde været spild af kundens penge, og vi måtte tænke i en indpakning, der talte til forbrugerens nysgerrighed og følelser, før vi kunne komme igennem med vores kernebudskab.

I Kraks tilfælde indspillede vi "Jagten". En 25-minutters internet-road-movie med Casper Christensen i hovedrollen. Konceptet var simpelt: Casper vågner med hukommelsestab på en strand i Vestjylland og skal tilbage til København inden for 24 timer. Flere gange undervejs på hans tur sidder han fast – og brugerne skal finde produkter på Krak for at hjælpe ham videre.

Forskellige produkter gav forskellige (og dermed unikke) handlingsforløb, og kampagnen demonstrerede dermed dybden i Kraks database samt det lokale aspekt i søgefunktionen. Og dette helt uden at snakke om det produkt, vi promoverede. Over 5 procent af den danske befolkning spillede Jagten, og vi opnåede mere end en million søgninger på Krak.

Jagten var den rigtige løsning for Krak. For læserne af denne rapport vil den rigtige løsning være en anden, når der i fremtiden skal oplyses om informationssikkerhed. Vigtigst er det, at man har overskuddet til at anerkende de ansattes manglende interesse for emnet i sig selv, tænke ud over blot at informere, og arbejde seriøst med at finde den rigtige emotionelle indpakning til at formidle sit kernebudskab. Trods alt er organisationens informationssikkerhed også i de ansattes interesse.

9. Status på informationssikkerhed

Med et tilbageblik på 2012 giver vi her en status på informationssikkerheden i Danmark. Det vil sige en status på i hvilken retning, de internetkriminelle trak os i løbet af året, der gik.

Der tages udgangs-punkt i data og historier fra 2012. For eksempel kan vi konstatere, at flere af sidste års forudsigelser af fremtidige tendenser for internetkriminalitet gik i opfyldelse. Blandt andet blev de første sårbarheder i 2012 offentliggjort til Samsungs smart-tv-platform, hacktivisterne med Anonymous-bevægelsen som bannerførere var igen med til at sætte dagsordnen, og mængden af malware til de mobile platforme steg.

Et tilbageblik er hovedsageligt interessant, hvis det skitserer en udvikling, der peger fremad. Derfor forsøger vi at beskrive internetkriminalitetens evolution med henblik på at identificere de kommende års væsentligste risici og trusler.

"Overordnet set har de internetkriminelles motiver og virkemidler ikke forandret sig væsentligt og vil sandsynligvis heller ikke gøre det fremover. Deres fokus er blot flyttet til de teknologier, vi benytter og deres virkemidler er blevet forfinet, mere sofistikerede og målrettede."

Overordnet set har de internetkriminelles motiver og virkemidler ikke forandret sig væsentligt og vil sandsynligvis heller ikke gøre det fremover. Deres fokus er blot flyttet til de teknologier, vi benytter, og deres virkemidler er blevet forfinet, mere sofistikerede og målrettede. Samme tendens vil vi nok se i fremtiden. Så snart en given teknologi vinder tilstrækkelig udbredelse, vil den blive forsøgt udnyttet og med tiden med større og større dygtighed. Flere af de tendenser vi beskriver, er derfor ikke nye, men har fået ny næring ved teknologiens ibrugtagning og udbredelse.

Vores beskrivelse af internetkriminalitetens udvikling giver anledning til en beskrivelse af de udfordringer, udviklingen afstedkommer for os, der arbejder med at beskytte danskernes it-aktiver. Udfordringer, der til dels også skyldes ændringer i brug og udbredelse af teknologi samt de krav, samfundet og borgerne stiller til organisationerne. For eksempel har mange i dag en forventning om at kunne benytte deres egen computer til arbejdsrelaterede opgaver. En forventning, som i organisationerne ses som både en mulighed og en udfordring.

Selvfølgelig vil det primære fokus være at opretholde integritet, fortrolighed og tilgængelighed for systemer og data. Dog ændrer rammerne for det arbejde sig ligesom tilgængeligheden af værktøjer, der kan hjælpe os i det arbejde. For eksempel skal offentlige organisationer overgå til en ny standard for udfærdigelse af informationssikkerhedspolitikker, og EU arbejder på ny lovgivning vedrørende beskyttelse af borgernes data.

Afsnittet sluttes med, at vi i listeform angiver de tendenser, vi så som de mest tydelige i 2012, samt de nye tendenser vi tror, vi i de kommende år skal forholde os til. Om det billede af fremtiden holder stik, må være op til individuel vurdering og tiden at vise. Det er dog vores håb, at du finder inspiration i vores perspektiver, således at de kan baggrund for det fortsatte arbejde med at beskytte vores it-aktiver.

9.1. Internetkriminalitetens udvikling

Det digitale trusselsbillede er under forandring. Med udgangspunkt i rapportens tidligere afsnit giver vi her et billede af denne forandring. Hvilke tendenser ser vi lige nu, og hvad driver udviklingen? Forståelse for det giver grobund for at kunne imødegå de trusler, der lurer i horisonten.

Betragtet hen over året der gik tegner der sig et billede af flere overordnede tendenser, som peger fremad og vil have betydning for vores kommende udfordringer med hensyn til informationssikkerhed. Mest fremtrædende var udbredelsen af exploit kits som for eksempel Blackhole. De beskrives af sikkerhedsvirksomheden Sophos som en af de største trusler lige nu. De bruges af it-kriminelle til at afsøge og udnytte sårbarheder på maskiner, der besøger en webside, der er blevet inficeret med det pågældende exploit kit.

I 2012 betød det, at sårbarheder blev forsøgt udnyttet mere bredt. Det enkelte angreb forsøgte at udnytte flere sårbarheder, hvortil der var inkluderet exploit-kode i det valgte kit. Det betød kortere tid før, at et exploit til en ny sårbarhed blev udnyttet. Samlet set gav brugen af exploit kits en effektivisering af den internetkriminelle værdikæde og tegner et billede af stigende professionalisering hos de internetkriminelle.

Kigger vi fremad, venter vi, at de forskellige exploit kits får endnu flere funktioner end i dag. Også antallet af exploits og hastigheden hvormed exploit-kode til nye sårbarheder inkluderes, vil blive en konkurrenceparameter. Det vil igen betyde, at tiden fra en ny sårbarhed opdages, til den benyttes i angreb, falder. Det så vi allerede i 2012, hvor exploit-kode til zero day-sårbarheder ganske kort efter offentliggørelsen af sårbarheden blev indlemmet i blandt andet Blackhole.

"Brugen af exploit kits giver malwareudviklerne mulighed for at fokusere på deres egen kode."

Brugen af exploit kits giver malwareudviklerne mulighed for at fokusere på deres egen kode. De kan for eksempel benyttes til at afprøve kode, før den benyttes i egentlige angreb. Det vil medføre malware, der er mere robust end tidligere. Det vil sige malware, som dels er langt mere målrettet og effektiv i sine grundlæggende funktioner, og dels vanskeligere at detektere og fjerne. Den type malware var i 2012 blandt andet målrettet NemID-løsningen, som blev brugt på de danske netbanker.

På den ene side vil den udvikling føre til malware, som er målrettet

enkeltorganisationer og deres data. Tyveri af kundedata blev allerede sidste år i en undersøgelse foretaget af Ponemon Institute angivet som det væsentligste mål for internetkriminelle. Mere end halvdelen af respondenterne i USA, England og Tyskland angav tab af sensitiv information som konsekvens af målrettede angreb. Selvom kreditkort-informationer er det mest oplagte mål, kan andre data, der kan benyttes til social engineering og identitetstyveri, være et mål, ligesom produkt- og kundedata kan i forbindelse med industrispionage.

På den anden side tror vi, at vi kommer til at se mere malware, der er målrettet mobile platforme. En udvikling der også beskrives i en rapport fra Georgia Institute of Technology. Særligt enheder, der benytter Android, er her i farezonen. Det så vi sidste år, hvor mængden af malware rettet mod Android-enheder steg eksplosivt. Kontrollen med nye applikationer som lægges til download på Google Play, er mindre end på for eksempel Apples App Store. I tillæg hertil har Android-enheder mulighed for installation af applikationer uden om Google Play.

Mobile enheder er på mange områder et reelt alternativ til den traditionelle computer. Med alle vores kontakter, relationer og korrespondancer samlet er de blevet den primære kilde til det sociale og arbejdsmæssige liv på internettet. Dermed er smartphonen for mange blevet sværere at undvære end computeren. Virker computeren ikke, har man ofte adgang til en anden. Det gælder ikke for smartphonen. Derfor vil vi i de kommende år se ransomware, der er målrettet mobile enheder, da presset for at betale her er større, end hvis det var computeren, der blev ramt.

Som de foregående år vil vi stadig se angreb, der signeres Anonymous-bevægelsen. Tidligere har de angreb været proklameret fra, hvad der kan ligne centralt hold, og herefter udført med lokal tilslutning for at gøre opmærksom på magtfuldkommenhed, uretfærdighed eller for at fremme et frit internet. Gennem 2012 har der været en ændring i dette mønster.

Afhængigt af synsvinklen blev aktiviteter, der i 2012 blev udført med Anonymous-bevægelsen som afsender, mere anarkistiske eller demokratiske. Stadig flere angreb blev udført på initiativ af den store gruppe af personer, som associerer sig med bevægelsens idealer, og som tidligere blot har deltaget. Det medførte angreb, der nogle gange primært havde lokal interesse, og hvor der efterfølgende opstod diskussion om, hvorvidt angrebet var udført af bevægelsen. Det så vi blandt andet ved angrebet på 3F, som blev udført som reaktion på fagforbundets blokade af Restaurant Vejlegården.

De kommende år vil utvivlsomt bringe flere af den type angreb, som primært har lokal interesse. Enhver med en sag, ligegyldig hvor lille eller lokal den er, kan udføre et angreb og underskrive det Anonymous. Udefra set kan det ligne en fragmentering af Anonymous-bevægelsens motiver og mål. Resultatet er dog, at ingen helt kan sige sig fri for at være et potentielt mål, da det ikke længere kun er myndigheder, magthavere og storkapitalen, der har bevægelsens opmærksomhed.

I 2012 modtog vi flere henvendelser fra borgere, hvis online tjenester var blevet misbrugt. Ved de fleste henvendelser om identitetstyverier handlede det om en e-mailkonto eller en konto på sociale medier, som blev brugt til chikane af kontoens ejer. Da den type hændelser er i strid med straffeloven, blev efterforskningen overladt til politiet. Vi har derfor ikke har kendskab til, hvordan man havde skaffet sig adgang til den misbrugte tjeneste.

Det er dog et problem, at det ofte er brugerens e-mailadresse, der benyttes som brugernavn. Særligt når vi har en tendens til at vælge et kodeord, der er let at huske, og genbruger det på tværs af tjenester. Når først kodeordet til en tjeneste er afluret, gættet eller opsnappet af malware, er der således fri adgang til samtlige tjenester.

Identifikationstyveri og infiltration af vores netværk på de sociale medier kan være midler til at få os til at sænke paraderne. Trods alt har vi større tillid til information, der kommer fra mennesker, vi kender, eller som blot er en del af vores netværk. Det tror vi i stigende grad vil blive udnyttet af de internetkriminelle til alt fra udsendelse af spam, spredning af malware og phishing til andre typer svindel. Godt hjulpet på vej af den stigende mængde informationer vi selv deler og publicerer på de sociale medier og en udbredt brug af URL-forkortelser.

Derfor vil vi se flere forsøg på at få adgang til vores online tjenester. Enten med kvalificerede gæt ud fra informationer vi selv har gjort tilgængelige, eller ved at inficere vores computere med malware.

Også henvendelser og anmodninger om at indgå i vores netværk på de forskellige sociale medier fra profiler, vi ikke kender i den fysiske verden, vil stige. Her har vi en tendens til at acceptere anmodningen, blot fordi profilen er medlem af det samme faglige forum eller indgår i vores øvrige netværk. Det på trods af, at vi ikke har direkte kendskab til profilen. Den type kontakt kan efterfølgende bruges til yderligere social engineering. Enten for at skaffe sig adgang til vores personlige data eller i forbindelse med målrettede angreb mod vores arbejdsgiver og dennes data.

Den første kontakt vil i færre tilfælde foregå som tilfældige massehenvendelser, men blive udført med brug af information om os selv, som vi har lagt ud på for eksempel de sociale medier. Det har til formål at øge troværdigheden.

Implementeringen af den nye HTML5-standard bringer nye muligheder for dem, som udvikler kode og ny funktionalitet for os som brugere. HTML5 er allerede i dag det foretrukne middel til præsentation af video og andet interaktivt webbaseret indhold på nettet, og mulighederne for at udnytte den er endnu uklare.

Vi vil derfor se angreb, der specifikt udnytter HTML5-standardens svagheder. Det kan for eksempel være det fælles scripting-API, brugen af local storage eller andre sårbarheder i browsernes implementering af standarden, der vil blive udnyttet til for eksempel spredning af malware.

Som HTML5 byder andre nye teknologier også på både muligheder og udfordringer.

Gennem de seneste år har mange danskere investeret i nye tv, der understøtter præsentation af andet indhold end tv-signalet. Smart-tv'et, spilkonsollen og smart netopkoblet forbrugerelektronik fungerer på mange måder som den traditionelle pc. Dog uden at vi har samme mulighed for sikkerhed. For eksempel er der ikke mulighed for installation af antivirussoftware og lignende på smart-tv'et.

Desværre har teknologien i 2012 vist sig at være sårbar. Her blev de første sårbarheder til Samsungs smart-tv-platform offentliggjort. Vi tror, det kun er et spørgsmål om tid, inden der offentliggøres sårbarheder til de øvrige producenters enheder.

Det har tidligere vist sig, at det er et spørgsmål om, hvornår en given teknologi opnår en kritisk masse, før det kan betale sig at udnytte den. Det har vi blandt andet set på Apples Macintosh-computere, som nu også er blevet mål for malware. Den samme udvikling vil ske med den smarte forbrugerelektronik. I takt med stigende udbredelse af betalingstjenester, der benytter og lagrer data på smart-tv'et eller spilkonsollen, vil de blive genstand for angreb, der har til formål at stjæle kodeord, kreditkortinformationer med mere.

Rejsekortet er et elektronisk billetsystem, der kan bruges i busser, tog og metro. Det bruges i dag i nogle områder, men skal senere i drift over hele landet. Den elektroniske billet består af et kort med en RFID-chip (Radio Frequency Identification). Når passageren påbegynder sin rejse, holdes kortet hen til en enhed, der registrerer, hvor rejsen er påbegyndt. Når rejsen afsluttes, tjekker passageren ud på samme måde, hvorefter beløbet for rejsen trækkes fra kontoen.

I januar 2010 demonstrerede Christian Panton, der var studerende ved Datalogisk Institut på Københavns Universitet, i TV-Avisen, hvordan han let kunne få adgang til og ændre i de data, der lå på kortet. Det skyldes sårbarheder i kortets Mifare-krypteringsprotokol, som forskere demonstrerede allerede i 2007.

I januar 2012 konstaterede Christian Panton, at Rejsekort A/S ikke har ændret i teknologien i systemet. Dermed er det sandsynligt, at hackere uden større besvær vil kunne udnytte sårbarheder i systemet til at rejse gratis. Efterhånden som systemet bliver taget i brug i hele landet, øges risikoen for misbrug. Foreløbig er muligheden for at snyde sig til gratis rejser den mest oplagte form for misbrug, men der vil utvivlsomt dukke andre op.

Også andre betalingsmidler vil som rejsekortet og vores kreditkort blive forsøgt misbrugt. Mest synlig er her de løsninger, der i øjeblikket udbredes og/eller udvikles til mobilbetaling fra vores smartphones.

Gennem det seneste år har vi både herhjemme og i udlandet set en optrapning af midlerne der benyttes til informationsindsamling og krigsførelse på internettet. Således medførte et politisk forlig i december måned en fordobling af bevillingerne til det danske cyberforsvar. Et forsvar, som det tidligere har været fremme, skal være både reaktivt og proaktivt.

De cirka 75 millioner kroner, som de næste fire år er bevilget til Center for Cybersikkerhed under Forsvarsministeriet, falder efter en risikovurdering fra Forsvarets Efterretningstjeneste af de største trusler mod Danmark i oktober. Her udtalte chefen Thomas Ahrenkiel blandt andet:

"Der er en stigende trussel mod Danmark i cyberspace. I takt med, at vi bliver mere digitaliserede, bliver vi også mere sårbare, og derfor kræver truslen fra cyberspace mere opmærksomhed. Vi oplever, at danske interesser og danske myndigheder mere eller mindre konstant er under angreb i cyberspace."

Selvfølgelig er der i krigssituationer en interesse i at kunne ramme modstanderens forsyninger, informationer og kommunikationskanaler. Trods alt handler det om at svække fjenden og mindske egne tab. Med cyberkrigen er der på mange måder tale om et fokusskift, der har været undervejs i flere år. Det er en fortsættelse af udviklingen med brugen af ubemandende droner til overvågning og strategiske præcisionsangreb.

I stigende grad har vi også set cyberkrigen udfolde sig i fredstid. Og desværre også med uskyldige civile ofre. Både Stuxnet og Flame ramte ikke blot de mål, de var designet til at ramme, men også virksomheder og borgere over det meste af kloden.

Her kan vi frygte, at den globale optrapning medfører stigende civile tab. Fraværet af sørgende krigsenker synes nemlig at have gjort internettet til en legal skueplads for krigsførelse, også i fredstid. Vi frygter, at fremtiden byder på flere utilsigtede infektioner og nedbrud af computere og industrianlæg i den vestlige verden som følge af cyberkrig. Så kan vi blot håbe, at det ikke er vores egne computere, vand- eller elforsyning som rammes.

Berlingske, 2012; *"Cyberkrig er større trussel mod Danmark end terror"*.
Geogia Tech, 2012; *"Emerging cyber threats report 2013"*.
Information, 2012; *"En ny strategi for USA's militær"*.
Panton, 2012; *"Rejsekortet: Sikkerhed som vi pensionerede i 90'erne"*.
Ponemon Institute, 2012; *"The impact of cybercrime on business"*.
Sophos, 2013; *"Security threat report 2013"*.
Version 2, 2012; *"Forlig fordobler bevilling til danske cyberkrigere"*.

9.2. De afledte udfordringer

De kommende år byder på en række trusler, der medfører nye udfordringer og fokusskift for eksisterende informationssikkerhedstiltag. Vi mener grundlæggende, at de fleste af dem bør løses gennem strategiske initiativer for samarbejde og kommunikation. Det er nemlig, når vi står sammen og deler vores erfaringer og viden, at vi er mest sikre, også hver for sig. Eller som de på Georgia Institute of Technology skriver i introduktionen til den rapport, der blev udgivet som resultat af deres årlige Cyber Security Summit i sommeren 2012:

"If we are going to prevent motivated adversaries from attacking our systems, stealing our data and harming our critical infrastructure, the broader community of security researchers—including academia, the private sector, and government—must work together to understand emerging threats and to develop proactive security solutions to

safeguard the Internet and physical infrastructure that relies on it."

Blandt de væsentligste udfordringer er bekæmpelse af malware, som ofte spredes til brugernes computere fra kompromitterede websteder. For eksempel modtog mange sidst i november en falsk kvittering fra iTunes, der skulle narre brugerne til et sådant websted.

Selvom nummeret har været brugt tidligere, var der mange, som klikkede på linket i kvitteringen for at finde ud af, hvad det drejede sig om. Herefter blev deres computer forsøgt inficeret med den trojanske hest Zeus/ZBot. Mailen var nemlig blot endnu et udspil fra de internetkriminelle.

Samme problem gør sig gældende, når de samme brugere frivilligt afgiver deres kontooplysninger på baggrund af en mail eller et telefonopkald. De fleste ved ikke, hvordan man skal navigere i mængden af informationer, som internettet har gjort tilgængelig. Med et godt hjerte og tillid til afsenderens gode intentioner lader man sig narre af udspekulerede kriminelle, som bliver stadig dygtigere. Det er simpelthen blevet vanskeligere at kontrollere validiteten af en stigende mængde henvendelser og informationer.

"...hvordan kommunikerer vi til borgerne, at informationssikkerhed ikke kun handler om teknologi? At det ikke er nok at have installeret et antivirusprogram."

Ovenstående skitserer en reel udfordring. For hvordan kommunikerer vi til borgerne, at informationssikkerhed ikke kun handler om teknologi? At det ikke er nok at have installeret et antivirusprogram. At det i lige så høj grad handler om at opdatere sine programmer, og man ved simpel omtanke selv kan bidrage.

Samme problematik gør sig til dels gældende i organisationerne, hvor mange ikke har en grundlæggende forståelse for, hvordan man bør behandle potentielt fortroligt materiale. Derfor bliver udkast til forretningsplaner, kundelister og lignende placeret på for eksempel Dropbox eller sendt til den private Gmail-konto, når der er behov for at arbejde på det derhjemme. Og værre er det, hvis der er tale om personfølsomme oplysninger, der behandles på denne måde.

Det er en væsentlig udfordring for organisationerne at klassificere en stigende mængde data og information og sikre at de behandles efter informationssikkerhedspolitikkens forskrifter. Kan man ikke klassificere, hvad der er følsomt, er det vanskeligt at lave konsekvens- og risikovurdering, som skal føre til regler og procedurer. Eller at opstille reelle alternativer som medarbejderne både kan og vil bruge, at implementere systemer til Data Leak Prevention (DLP), eller på anden vis begrænse de ansattes adgang til følsomme data.

Problematikker om medarbejdernes kopiering af data og information har altid eksisteret. I takt med stigende mængder data og mangfoldigheden af muligheder er den dog blevet mere nærværende. Og en ting er, hvad der på organisationens eget udstyr kan sikres og kontrolleres, en anden er, når det handler om brugernes eget udstyr. Her bringer brugernes ønske om at benytte deres udstyr endnu en problemstilling på banen. Eller som sikkerhedsvirksomheden Sophos skriver i deres rapport om trusler fra sidste år og fremtiden:

"BYOD can be a win-win for users and employers, but the security challenges are real while boundaries between business and private use are blurring."

Bring Your Own device (BYOD) er for nogle organisationer et middel til at skabe større effektivitet. De primære fordele er besparelser på udgifter til fælles indkøb, drift og support samt medarbejdere der kan vælge det udstyr, der gør dem i stand til bedst muligt at udføre deres opgaver. Det giver imidlertid også anledning til en række problematikker om, hvordan medarbejdernes eget udstyr og data på det skal varetages inden for organisationens og juraens rammer.

Mens det er naturligt at begrænse, kontrollere og overvåge medarbejderne på organisationens eget udstyr, er det juridisk vanskeligere, når det er tale om deres eget udstyr. For eksempel kan det være vanskeligt at stille krav om, at de ansatte ikke må installere applikationer på deres egne smartphones, bærbare computere og lignende.

Det handler her om at risikovurdere de konfigurationer og enheder, der benyttes, og sørge for, at der udfærdiges politikker på området. Samtidig bør man overveje, om følsomme data skal kunne overføres til mobile enheder, som står uden for organisationens ejerskab og kontrol, samt hvordan man eventuelt vil håndhæve det. Generelt fordrer BYOD politikker, regler og procedurer, som er mere gensidige i forhold til medarbejderen.

Mange af de problematikker, der knytter sig til BYOD, gælder for så vidt også for organisationer, hvis medarbejdere får udleveret for eksempelvis smartphones og tavle-pc'er. Det kan nemlig være vanskeligt at begrænse, hvilke data og applikationer der lagres og installeres på dem. Systemer til Mobile Device Management (MDM) og Mobile Application Management (MAM) bør derfor under alle omstændigheder indgå i organisationernes overvejelser om, hvordan man ønsker at sikre sine data, ligesom software til kryptering.

Med den næste udgave af ISO-standarden, der forventes at komme i 2013, står mange organisationer over for en revision af deres informationspolitik. Den vil ikke blot lægge beslag på organisationens ressourcer, men også anskueliggøre et behov for aktivt at involvere ledelsen i arbejdet med at sikre organisationens aktiver. Det forventes standarden at stille større krav til, end vi er vant til fra DS484.

Der bør være fokus på, at informationssikkerhedspolitikken ikke kun er et statisk dokument, der udfærdiges for at tilfredsstille revisionen. Den skal også løbende revideres og efterleves i både ord og handling. Compliance-diskussioner bør ikke kun have fokus på det skrevne ord,

men i ligeså høj grad på, hvordan organisationen og dens medarbejdere agerer samt inddrage elementer af uddannelse og oplysning. Det arbejde er kun troværdigt, hvis ledelsen indgår aktivt i arbejdet med for eksempel risikovurdering og står som afsender af relevant information og oplysning til de ansatte. Det er nemlig i stigende grad deres udstyr og informationer, som har de internetkriminelles fokus.

Et væsentligt element af informationssikkerhedspolitikken er en troværdig beredskabsplan. At der er klarhed over, hvem der gør hvad og hvorfor, når tingene ikke går, som vi havde forestillet os. Når vi på trods af alle modforanstaltninger alligevel rammes af nedbrud eller tyveri af data. At der for eksempel er klarhed over, hvem der har ansvaret for at afværge yderligere følgevirkninger, og hvem der er ansvarlig for rettidig og troværdig kommunikation til de berørte interessenter.

En god beredskabsplan indeholder også alternative måder at gøre de ting på, som ikke længere er mulige. Der bør derfor udarbejdes nødplaner, der sikrer, at organisationen i en eller anden grad kan forsætte sit arbejde på trods af den aktuelle situation. Også for situationer, hvor det ikke nødvendigvis handler om, at vi er blevet kompromitteret, men måske er i forhold til foranstaltninger vi foretager for ikke at blive det.

Hvordan håndterer man for eksempel en situation, hvor det kan være nødvendigt at deaktivere forretningskritiske applikationer eller komponenter på de ansattes udstyr? Den seneste tid har vi set exploits til Java-sårbarheder, der blev medtaget i udbredte exploit kits, inden der var nogen rettelse til sårbarheden. Kan vi i de tilfælde centralt deaktivere Java på de ansattes udstyr, også hvis det er ejet af dem selv? Og hvad gør vi, hvis Java er nødvendig for at køre vores forretningsapplikationer? Og når der efterfølgende kommer en rettelse til den sårbare applikation, kan vi så sikre, at den også bliver installeret?

”I det perspektiv bør vi accepterer, at perimeteren er flyttet til brugernes computer, hvor krigen køres i browseren.”

I det perspektiv bør vi acceptere, at perimeteren er flyttet til brugernes computer, hvor krigen køres i browseren. Dermed står vi tilbage med et polymorft trusselsbillede, som bør adresseres strategisk. Informationssikkerhed er nemlig ikke længere et vilkår, der blot omhandler organisationens egne systemer og data, men bør betragtes som en del af forretningen.

Det illustreres blandt andet ved den kommende indførelse af EU’s databeskyttelsesdirektiv. Heri kan organisationer pålægges bøder ved læk af kundedata, og kunderne skal orienteres rettidigt. Under alle omstændigheder rummer ibrugtagningen af ny teknologi eller udviklingen af nye systemer strategiske perspektiver, som bør inddrage elementer af informationssikkerhed. Derfor mener vi, at informationssikkerhed bør betragtes som et strategisk aktiv, hvis det skal have det fornødne fokus hos beslutningstagerne.

Hvis ikke informationssikkerhed flyttes til et strategisk niveau, er det tilsvarende vanskeligt at forestille sig, at man kan opbygge en kultur, hvor medarbejderne er oplyste og bevidste omkring informationssikkerhed. I den proces bør man lytte til medarbejdernes stemme og prioritere uddannelse. Hvis varetagelsen af informationssikkerheden skal stå mål med et mangefacetteret trusselsbillede, kræver det en kultur, hvor medarbejderne må, kan og vil tage ansvar.

Med flydende grænser mellem arbejde og fritid bliver vi nødt til at tænke informationssikkerhed i en helhed. Som på Roskilde Universitet er det et godt udgangspunkt her også at adressere sikkerheden på medarbejderens private enheder. Herved bliver indsatsen nærværende og i de ansattes egen interesse. Erfaringerne fra tilsvarende oplysningskampagner fortæller nemlig, at de fungerer bedst, når vi opfordres til at relatere budskaberne til det nære.

Udviklingen og brugen af teknologien og i samfundet som helhed vil til stadighed udfordre de måder, hvorpå vi tænker og udfører informationssikkerhed. En forudsætning for at vi også fremover kan sikre danskernes it-aktiver er en prioritering af uddannelse, videndeling og samarbejde. På samme måde som organisationerne har et medansvar for at uddanne og oplyse deres medarbejdere, har vi som samfund en forpligtelse til at opretholde fødekæden af uddannet arbejdskraft.

Vi bør ikke lade økonomi være argumentet for en nedprioritering af informationssikkerhed. Lad os i stedet samarbejde om løsninger, som i første omgang højner sikkerheden og på sigt muliggør, at vi kan gøre det mere effektivt. Det handler nemlig om, at vi sammen er sikre hver for sig.

Geogia Tech, 2012; *“Emerging cyber threats report 2013”*.
Sophos, 2013; *“Security threat report 2013”*.

9.3. Tendenser fra året der gik

Det forgangne år bød på både gamle trusler, som fik ny udbredelse, gamle trusler i ny forklædning og helt nye tendenser, som vi endnu kun kan gisne om perspektivet og omfanget af. Flere af årets tendenser er muliggjort af teknologiens udvikling og udbredelse samt større forbundenhed og kompleksitet i de informationer, vi benytter og modtager. Det er simpelthen blevet vanskeligere at vurdere validiteten af de informationer, vi modtager.

Vellykket kriminalitet har altid handlet om at udnytte sårbarheder i de systemer, man ønsker at angribe. Således også på internettet. I 2012 ramte overskrifter om sårbarheder i it-systemer, der blev udnyttet, inden de var offentliggjort, flere gange medierne. Det er kritisk, da der således ikke er nogen rettelse til sårbarhederne. Truslen forstærkes ved den stigende brug af exploit kits til automatiseret afprøvning af flere sårbarheder. Et enkelt exploit kan her centralt udbredes til flere angreb. I takt med stigende konkurrence på markedet for denne type programmer vil hastigheden for, hvor hurtigt et exploit til en ny sårbarhed inkluderes, blive en konkurrenceparameter.

Blandt de programmer der havde 0-dagssårbarheder, var Oracles Java, der er en forudsætning for afvikling af NemID. Det var dog ikke 0-dagssårbarheder, som var årsag til de malwareinficeringer, der medførte, at bankerne i 2012 led de største tab ved netbankindbrud siden indførelsen af NemID. En del af ansvaret må her ligge hos netbankkunderne, der blev bedt om at genindtaste deres NemID-kode. Men hvordan kan man vide, om en fejl, ændringer i netbankens procedurer eller ondsindede internetkriminelle er årsagen?

Langt hen ad vejen var det en anden malwaretype, som i 2012 fik sit store gennembrud. Politi-ransomware var blandt de hurtigst voksende trusler på internettet. At det også var en god forretning, viste bagmændenes egne statistikker. Ransomware er en hurtig og nem måde at omsætte sin kode til rede penge på. Ved at lade politiet stå som afsender på budskabet om, at man havde downloadet børneporno, narrede svindlerne mange til at undlade at henvende sig til kollegaen, naboen, vennerne eller andre, der potentielt kunne hjælpe. Heldigvis var de versioner, som var målrettet danskere, ikke helt så troværdige som de udenlandske.

”Hvor der på den traditionelle computer er flere platforme, der er mål for malware, er det hovedsageligt Android, der er mål for malware til mobile platforme.”

Hvor der på den traditionelle computer er flere platforme, der er mål for malware, er det hovedsageligt Android, der er mål for malware til mobile platforme. 99 procent af de mobile trusler var ifølge Kaspersky Lab rettet mod Android-enheder i 2012. Mængden af ny malware til Android steg kraftigt i forhold til året før. Kaspersky Lab identificerede i gennemsnit 6.300 nye varianter om måneden. Der var hovedsageligt tale om SMS-trojanere, bagdørsprogrammer og spyware.

De mobile enheder var også mål for andre, mindre tekniske betonede angreb. Ved kun at lade telefonen ringe en enkelt gang undgik svindlerne, at den blev taget. Mange valgte herefter at ringe tilbage til nummeret, der fremgik af opkaldslisten. Senere opdagede de så, at der var tale om et overtakseret nummer. Det samme udspillede sig ved hjælp af tomme eller kryptiske SMS’er, der fik folk til at sende en SMS tilbage for at høre, hvad det drejede sig om.

Selv om der flere gange i medierne blev advaret mod engelsktalende ”Microsoft-ansatte”, der ringede for at hjælpe med sikkerhedsproblemer på danskernes computere, fortsatte danskerne med at lade sig ”hjælpe”. De første opkald kom allerede sidst i 2011, men tog gennem 2012 til i antal. Den venlige ”Microsoft-ansatte”, der ville hjælpe med at fjerne malware fra computeren, var i virkeligheden ude på selv at installere malware på den eller blot få adgang til offerets kreditkort-informationer.

Også i 2012 steg mængden af information, som vi delte og publicerede på et stadig stigende antal online tjenester. På flere af dem er det brugerens e-mailadresse, der benyttes som brugernavn, mens kodeordet genbruges på tværs af tjenester. Når først kodeordet til en tjeneste var afluret, gættet eller opsnappet af malware, var der således fri adgang til samtlige tjenester.

I 2012 steg antallet af henvendelser fra borgere, hvis online tjenester var blevet misbrugt af andre. Det handlede primært om drengestreger og chikane. Andre igen havde økonomiske motiver til at udnytte vores online tjenester, der kunne øge troværdigheden af deres budskaber. Det hvad enten det handlede om at sende spam og phishing-beskeder eller sprede malware. På de sociale medier øges risikoen ved den udbredte brug af URL-forkortere.

Hvor Anonymous tidligere har fremstået som en samlet gruppe, blev fragmenteringen af bevægelsens mål og midler gennem 2012 stadig mere klar. Anonymous-bevægelsen viste sig som en demokratisk platform, hvor alle kunne foreslå og igangsætte operationer eller blot efterfølgende underskrive deres angreb Anonymous. En hver med en sag kunne udføre angreb og tilskrive dem bevægelsen. Herved er der sket en mental retfærdiggørelse af angreb, som måske ikke tidligere ville blive udført. Det betyder en større vilkårlighed i mål og motiver, således at ingen i dag kan sige sig fri for at være et potentielt mål.

Selv om noget tyder på, at det ikke tilfældet, blev den iranske regering i første omgang anklaget for at stå bag et virusangreb på det saudiarabiske oliefirma Saudi Aramco. Virussen slettede i august data på en stor del af virksomhedens computere. Angrebet er utvivlsomt indgået som argument for den optrapning af midlerne til online krigsførelse, som gennem det seneste år har kunnet konstateres. Herhjemme fik et nyt Center for Cybersikkerhed under forsvarsministeriet i december fordoblet midlerne til cybersikkerhed. I den forbindelse udtalte forsvarsminister Nick Hækkerup (S) til TV 2:

”Vi skal have en cyberkapacitet, der kan bruges til angreb, hvis det er nødvendigt.”

Nedenfor kan du på listeform læse de tendenser, vi fra et dansk perspektiv fandt mest toneangivende i 2012:

1. **Flere zero day-sårbarheder nåede offentligheden**. Sårbarheder i Java og Internet Explorer blev i 2012 udnyttet, inden de var offentliggjort. De gav anledning til overskrifter og advarsler i medier, der ikke traditionelt beskæftiger sig med informationsteknologi. Desuden viste en undersøgelse, at der findes flere zero day-sårbarheder, end man hidtil har vidst.
2. **Eksploit kits medførte hurtig udnyttelse af sårbarheder**. Udbredelsen af exploit kits har givet de internetkriminelle adgang til at udnytte flere sårbarheder end tidligere. I kombination med, at de som udvikler exploit kits har en interesse i hurtigt at inkludere nye exploits, har det medført tidligere udnyttelse af sårbarheder. For eksempel blev et exploit til en Java-sårbarhed (CVE-2012-4681) inkluderet i Blackhole exploit kit mindre end en måned efter offentliggørelsen.

3. **Avanceret malware narrede brugerne og NemID**. Avanceret malware fik netbankbrugere til at indtaste deres NemID-kode i en falsk autentificeringsboks. Det gav de internetkriminelle adgang til deres bankkonti. Selv om angrebet i nogle tilfælde blev afværget af bankens systemer, oplevede vi i 2012 de største tab ved netbankindbrud siden indførelsen af NemID. Selv om NemId har været under kritik, har det indtil videre været kunderne, som var det svageste led.
4. **Ransomware tog data som gidsel**. I sidste halvår af 2012 oplevede mange, at deres computer blev låst med en meddelelse om, at den havde været benyttet til at downloade kopibeskyttet materiale og børneporno. Angiveligt kom meddelelsen fra politiet, der kunne låse maskinen op, hvis man betalte en bøde. Der var tale om en malwaretype, som ikke er ny, men fik en opblomstring i 2012.
5. **Vækst i malware til Android**. Med stigende udbredelse og brug følger også uønsket opmærksomhed. Således er mængden af malware målrettet Android-enheder eksploderet i 2012. Det meste spredes via inficerede applikationer, der installeres uden om Google Play.
6. **Telefonopkald fik folk til at ringe til overtakserede numre**. Korte telefonopkald som man ikke kunne nå at besvare og kryptiske SMS'er fra ukendte telefonnumre var et andet middel til at lokke pengene op af danskernes lommer. Mange ringede bagefter selv op til nummeret eller besvarede SMS'en for efterfølgende at finde ud af, at der var tale om en overtakseret tjeneste.
7. **Telefonopkald fra Microsoft**. Mange danskere blev i løbet af året ringet op af engelsktalende repræsentanter fra Microsoft eller tilsvarende organisationer. De tilbød at hjælpe med at rense en computer, som de kunne konstatere, var inficeret med malware. Der var tale om svindel. Målet var at få folk til at købe virkningsløse eller i forvejen gratis sikkerhedsprodukter, installere malware på deres computer eller få adgang til deres kreditkortoplysninger.
8. **Identifikationstyveri på online tjenester**. I 2012 så vi stigende misbrug af online tjenester, hvortil der var skaffet adgang ved brug af malware eller ved at gætte kodeordet. Målet var alt fra chikane og afsendelse af spam til social engineering. På flere tjenester benyttes e-mailadressen som brugernavn. Når kodeord genbruges på tværs af tjenester, giver det let adgang for uvedkommende. Det er et problem, da e-mailtjenester og sociale medier i stigende grad integreres med andre tjenester eller hardwareenheder som for eksempel smartphones.
9. **"Demokratisering" af aktiviteter i Anonymous**. I den løst sammenknyttede bevægelse uden formelle strukturer, regler eller medlemslister kan alle tage initiativ til angreb og underskrive det Anonymous. Som vi så det i konflikten med restaurant Vejlegården, tror vi, at fremtiden vil byde på flere lokalt betingede angreb, som udføres under signaturen Anonymous. Det medfører også, at kun de færreste kan fraskrive sig truslen.
10. **Global optrapning af ressource til cyberkrig**. Amerikanerne, israelerne, iranerne og kineserne har alle angiveligt udført avancerede statsstøttede angreb i cyberspace. I 2012 optrappede vi også herhjemme ressourcerne til aktiviteter for krigsførelse på internettet. Oprettelsen af Center for Cybersikkerhed under forsvarsministeriet mere end fordoblede bevillingerne til det danske cyberforsvar, som i modsætning til tidligere skal kunne agere både defensivt og offensivt.

Bloomberg, 2012; *"Code in Aramco cyber attack indicates lone perpetrator"*.
Finansrådet, 2012; *"Netbankindbrud - statistik"*.
Kaspersky Lab, 2013; *"Kaspersky Security Bulletin 2012. The overall statistics for 2012"*.
TV 2, 2012; *"Danmark klar til angreb på nettet"*.

9.4. Fremtidige trends

Flere af de tendenser vi har identificeret for 2012, vil fortsætte de kommende år. Når de ikke fremgår af vores trends for de kommende år, skyldes det den manglende nyhedsværdi, samt at de i medieomtale og opmærksomhed vil blive overskygget af andre og nyere tendenser.

For eksempel er det vanskeligt at forestille sig, at de som har associeret sig med Anonymous-bevægelsen og dens selvproklamerede kamp for frihed og retfærdighed, vil holde sig i ro. Internettet har vist sig som et effektivt medie at aktionere på, hvis man ønsker sine synspunkter bredt ud, også internationalt. Vi tror derfor, at hacktivisme er en aktionsform, som vi også i de kommende år bliver nødt til at forholde os til.

Derimod er det vanskeligt at forestille sig, at denne form for samfundsprotest vil bevæge sig i helt nye retninger. Trods alt er størstedelen af aktivisterne velkvalificerede vestlige mænd fra middelklassen. De har ingen interesse har i at nedbryde samfundet, højest at udstille dets svagheder.

Indtil videre har vi ikke set en digital pendant til fortidens Rote Armee Fraktion, som ønsker en helt ny samfundsstruktur i den vestlige verden. Det kan også være vanskeligt at forestille sig, at de på internettet vil opnå samme effekt som ved for eksempel mord, kidnapning, bombeattentater og flykapring. Indtil videre har internettet derfor primært tjent som medie til meningsudveksling og rekruttering for de rabiate grupperinger.

"Vi tror, at mange af dem som har associeret sig med Anonymous-bevægelsen, i fremtiden også vil være aktive på lokalt plan."

Vi tror, at mange af dem som har associeret sig med Anonymous-bevægelsen, i fremtiden også vil være aktive på lokalt plan. Bevægelsens diffuse rammer giver mulighed for, at alle kan udføre angreb og tilskrive dem bevægelsen. Som med angrebet på 3F i sommer, tror vi, at stadig flere angreb udføres som resultat af konflikter, der kun har lokal interesse. Herved er det ikke længere kun myndig-hederne og storkapitalen, der er potentielle mål. Det kan lige så vel være den virksomhed, man blev afskediget fra, eller en organisation, som i medierne fremstår som at have optrådt på en måde, man er uenig i.

Med exploit kits har de internetkriminelle fået et værktøj, der giver dem mulighed for nemt at udnytte flere sårbarheder og udføre målrettede angreb. Herved har de også fået mulighed for at fokusere på deres kerneforretning. Det kan betyde en mere målrettet indsats på udviklingen af skadelig kode, som derved blive mere robust. Samtidig giver det mulighed for at afprøve kode målrettet et specifikt system, teknologi eller geografi, inden den benyttes i et egentligt angreb. Vi tror, at det giver anledning til udvikling af malware, som er mere målrettet, bedre til at skjule sig, vanskeligere at fjerne og generelt bedre til at udføre de opgaver, det er designet til.

Et resultat af malware-udviklernes bedre muligheder for at fokusere på koden bliver ransomware, der er målrettet smartphones. Smartphonen er for mange blevet vanskeligere at undvære end computeren. Det er her vi har vores kontakter, lever det digitale liv på de sociale netværkstjenester og besvarer e-mails relateret til både privat- og arbejdsliv. Det lægger pres på ejeren af en inficeret enhed, som kan få ham til at betale for igen at få adgang til smartphonen. Derfor venter vi, at mobile enheder bliver mål for denne type malware. Der vil primært være tale om enheder, der benytter Android. De giver mulighed for installation af applikationer uden om Google Play, som i øvrigt har en mindre restriktiv procedure om nye applikationer end for eksempel Apples App Store.

Derudover tror vi, at værdien af de stigende mængder af data, som organisationerne indsamler og lagrer, i stigende grad vil få de internetkriminelles fokus. Det vil ikke blot handle om fortrolige data vedrørende organisationernes produkter og processer, der kan have værdi for konkurrenter eller andre, der ønsker at kopiere dem. Også informationer om organisationens kunder og ordrer kan have en værdi til målretning af phishing og andre former for svindel. Det vil betyde en stigende mængde malware, som er målrettet enkelte organisationer og deres nøglemedarbejdere.

Her tror vi, at identitetstyveri og overvågning af informationer og relationer, vi selv offentliggør på sociale medier, vil tjene som middel til at nedbryde vores mentale forsvarsværker. Beskeder, der inddrager informationer om os selv fra folk i vores netværk, har trods alt større troværdighed end de åbenlyst massegenererede beskeder, vi dagligt fodres med.

En udbredt genbrug af password på tværs af online tjenester, der benytter e-mailadresser som brugernavn, gør det i mange tilfælde nemt at skaffe sig adgang. Derfor vil vi i stigende grad se identitetstyverier udført med det formål at skaffe sig adgang til ressourcer i vores netværk. Det hvad enten det endelige mål er at skaffe sig adgang til kreditkortinformationer eller fortrolige virksomhedsdata.

HTML5 har efterhånden vundet indpas og er blevet en de-facto standard til præsentation af video og andet interaktivt webbaseret indhold på nettet. Derfor vil det også være naturligt, at standardens muligheder for misbrug undersøges af grupperinger, der for eksempel ønsker at benytte den til spredning af malware. Sårbarheder i det fælles scripting-API kan for eksempel udnyttes til at ramme på tværs af platforme og browsere. Vi tror derfor, at vi i fremtiden vil se angreb, der specifikt udnytter HTML5-standardens svagheder.

Indførelsen af ny teknologi betyder både nye muligheder og udfordringer. Således har smart-tv-platformen og anden netopkoblet forbrugerelektronik givet os ny funktionalitet, som for mange er blevet en bekvem del af hverdagen. Et smart-tv kan for eksempel installere applikationer, streame betalingsindhold, betjenes via telefonen og meget mere.

Desværre har teknologien også vist sig at være sårbar, og ofte er der kun ringe mulighed for selv at konfigurere og overvåge sikkerheden. Det har tidligere vist sig, at det blot er et spørgsmål om, hvornår en given teknologi og/eller platform opnår en kritisk masse, før det kan betale sig at udnytte den. I takt med stigende udbredelse af betalingstjenester, der benytter og lagrer data på smart-tv'et eller spilkonsollen, forudser vi derfor, at de bliver genstand for angreb.

Som andre elektroniske betalingsformer vil både rejsekortet og de kommende mobile betalingsløsninger i takt med udbredelsen blive udsat for forsøg på misbrug. Det er endnu for tidligt at gætte på, hvordan et misbrug konkret vil foregå, da løsningerne endnu ikke er udviklet og/eller tilstrækkeligt udbredte. Et oplagt gæt er, at vi vil se malware målrettet de mobile betalingsplatforme, mens rejsekortet i første omgang primært vil blive misbrugt til gratis rejser. Andre former for misbrug kan dog på sigt være muligt.

Den samfundsmæssige afhængighed af informationsteknologi har blandt andet medført, at it er blevet en del af den kritiske infrastruktur på linje med broer, el- og vandforsyning med mere. Således er teknologien også blevet et potentielt mål for terror og krigsaktiviteter og indgår som element af forsvaret både herhjemme og i udlandet.

Gennem de seneste år har der været flere eksempler på proaktive cyberforsvarsaktiviteter rettet mod fjendtligsindede regimer, også i fredstid. Vi frygter derfor, at den globale optrapning af ressourcerne til cyberkrig som vi også har set herhjemme, vil medføre infektioner og nedbrud af computere og industrianlæg i den vestlige verden. Vi venter, at virksomhederne og almindelige borgere utilsigtet kan blive berørt, som vi for eksempel så det med Stuxnet og Flame.

Herunder kan du læse mere om de tendenser, vi tror vil præge vores arbejde med informationssikkerhed de kommende år. Trusselsbilledet er nemlig ikke en statisk størrelse:

1. **Angreb underskrevet Anonymous-bevægelsen, der skyldes lokale konflikter**. Gennem de seneste år har flere vist vilje til ikke blot at indgå i den globale Anonymous-bevægelse, men også til på lokalt plan at påtage sig rollen som internettets retfærdighedssøgende hævner. De angreb underskrives Anonymous-bevægelsen, som man associerer sig til. Vi tror, at der kommer flere af den type angreb, der skyldes konflikter, som kun har lokal interesse.
2. **Mere robust malware som følge af exploit kits**. Mange funktioner

i de internetkriminelles værdikæde varetages i dag af exploit kits, der giver malwareudviklerne mulighed for at fokusere på deres kernekompetencer. Det vil give malware, som har potentialet til at være mere målrettet, skjult og robust.

3. **Ransomware til smartphones**. Smartphonen udgør et væsentligt redskab både i forhold til privatliv og arbejde. Det er herfra, vi opdaterer vores profiler på de sociale medier, læser e-mails med mere. Smartphonen er for mange mere uundværlig end computeren. Vi tror derfor, at vi vil se ransomware rettet mod smartphones, der primært benytter Android-styresystemet.
4. **Malware målrettet organisationer**. Jo længere man kan trænge ind i organisationens infrastruktur, des større værdi har de data og systemer, man kan få adgang til. Derfor tror vi, at vi vil se mere malware designet til at ramme medarbejderne i specifikke organisationer. Det hvad enten målet er den enkelte medarbejder eller de systemer og data, denne måtte have adgang til.
5. **Professionelle identitetstyverier på online tjenester**. Beskeder fra kontakter i vores netværk øger meddelelsens troværdighed. Identitetstyverier på online tjenester kan have til formål at indsamle personlige oplysninger til brug ved social engineering eller til spredning af maware. Vi tror, at fremtiden bringer flere eksempler på det.
6. **Angreb der udnytter HTML5**. Udbredelsen af HTML5 gør standarden til et attraktivt mål for internetkriminelle. Vi tror derfor, at vi vil se kode, der specifikt udnytter browsernes håndtering af standarden til spredning af malware.
7. **Angreb på smart hjemmeelektronik**. I 2012 blev de første sårbarheder til Samsungs smart-tv offentliggjort. Vi tror, at de kommende år byder på flere sårbarheder, også på de øvrige producenters enheder. Smart hjemmeelektronik benyttes i stigende grad til betalingstjenester og lignende. Derfor tror vi, at de bliver mål for angreb. Det vil primært handle om spilkonsollen, smart-tv'et og smart-tv-bokse, der potentielt indeholder data, der kan misbruges.
8. **Misbrug af betaling til mobiltelefoner**. I øjeblikket arbejdes der fra flere sider på at gøre betaling mulig fra vores smartphone. Med udbredelse af teknologierne øges også risikoen for misbrug. Derfor forudser vi, at de kommende mobile betalingsløsninger vil blive udsat for misbrug. En mulighed vil være i form af malware, som vi har set det i forhold til netbankløsninger og NemID.
9. **Misbrug af rejsekortet**. Som andre betalingsmidler er også rejsekortet et oplagt mål for misbrug. Det er tidligere vist, at en sårbarhed i kortets krypteringsprotokol gør det muligt at få adgang til og ændre data på kortet. Det er mest oplagt, at misbrug vil ske i form af tyveri af rejser.
10. **Global optrapning af cyberkrig vil ramme uskyldige**. Tryk avler modtryk. Derfor kan Danmark og dennes allierede meget vel blive genstand for et modsatrettet fokus på internettet. Vi tror, at de stigende investeringer i cyberkrig vil ramme uskyldige. Det er tidligere set med for eksempel Stuxnet og Flame. Det kan få alvorlige konsekvenser.

Berlingske, 2012; "*Hackerne er ude efter dit TV*".

10. Anbefalinger

Her lader vi rapportens konklusioner danne grundlag for en række anbefalinger til, hvordan du som almindelig computerbruger, it-ansvarlig eller beslutningstager kan være med til at sikre de danske it-aktiver. Ligegyldig hvilken rolle vi varetager, kan vi bidrage positivt til den fælles informationssikkerhed ved at tage ansvar for de løsninger og data, vi har mulighed for at påvirke.

Som meget andet i samfundet er vores systemer og data forbundne. Mangelfuld sikkerhed et sted kan betyde kompromitteringer et helt andet sted. Det hvad enten der er tale om malware, der spredes fra et usikkert websted, eller kreditkortinformationer der stjæles fra en internetbutik. Det er derfor vores håb, du vil tage anbefalingerne til dig, således at de kan bidrage til refleksioner, der på tværs af organisationer, brancher og sektorer kan bidrage til den fælles informationssikkerhed.

10.1. Anbefalinger til borgerne

Selvom teknologien og måden vi benytter den på, er under forandring, er det grundlæggende de samme ting, vi som borgere skal være på vagt overfor. Derfor har vi igen i år valgt at videregive de samme fem råd til beskyttelse af borgenes computere som videregives af "Netsikker nu!" kampagnen og via sitet "Opdater din PC". Kampagnen bliver til i et samarbejde mellem Digitaliseringsstyrelsen og en række danske virksomheder og organisationer, der alle har fokus på danskernes informationssikkerhed.

Rådene er almengyldige og omfatter også smartphones og tavle-pc'er, der reelt er små computere og bør behandles som sådan. De benyttes blandt andet også til at surfe på nettet, læse mail, tjekke Facebook, netbank med mere. Nedenstående fem råd gælder derfor også de bærbare og mobile enheder.

Beskyt dine enheder:

1. **Beskyt din pc mod ondsindede programmer**. Brug firewall og opdateret antivirusprogram.
2. **Hold dine programmer opdateret**. Brug automatisk opdatering, hvor det er muligt. Opdater også tredjepartsprogrammer og tilføjelsesprogrammer til browseren, eventuelt ved brug af programmer som for eksempel PSI fra Secunia.
3. **Slå krypteringen til på dit trådløse netværk**. Brug som minimum WPA2-kryptering, og brug et sikkert password (se også anbefaling nummer 7).
4. **Indstil sikkerhedsniveauet i din browser**. Herved kan du sikre dig, at du som minimum bliver spurgt inden overførsel af informationer, filer og programmer.
5. **Installer kun programmer, du har brug for**. Sårbarheder i ubrugte programmer udgør også en risiko, særligt hvis de ikke holdes opdateret.

Da informationssikkerhed handler om mere end blot den enkelte pc, har vi valgt at supplere de fem anbefalinger med råd om, hvordan man selv kan agere sikkert på internettet.

Opdatering af sårbare systemer giver kun ringe beskyttelse, hvis der er en nemmere måde at tilgå data på. Hvis andre har adgang til computeren eller den bærbare enhed, hjælper ovenstående råd derfor ikke i forhold til at beskytte adgangen til de data, der er placeret på den. Derfor handler det også om at beskytte adgangen til data med en adgangskode. Særligt på de bærbare enheder, der oftere glemmes eller stjæles med risiko for at andre kan læse de data, som er gemt på dem eller misbruge SIM-kortet til dyre opkald.

Beskyt dine data med adgangskode og kryptering:

6. **Brug passwordbeskyttelse på dine enheder, og benyt om muligt kryptering af data**. Husk, at dine bærbare enheder ofte også giver adgang til mail-kontoen, Facebook, Dropbox og lignende. Beskyt derfor adgangen til dine enheder med password og benyt eventuelt kryptering. Beskyt også SIM-kortet med en adgangskode, så det ikke kan misbruges ved tyveri af enheden.

Brug af standard-passwords og/eller passwords der er nemme at gætte, udgør en lige så stor risiko som ikke opdaterede systemer. Særligt på tjenester, der er placeret på nettet, hvor du ikke selv kan beskytte dem på anden vis. Kompromittering af en tjeneste kan ofte også give anledning til kompromittering af andre tjenester, der benytter samme password. Det gælder især de tjenester, hvor ens e-mailadresse udgør brugernavnet.

Brug passwords der er svære at gætte:

7. **Brug unikke og sikre passwords på alle tjenester**. Et sikkert password består af minimum otte tegn indeholdende både store og små bogstaver, tal og specialtegn. Undgå standardbrugernavne og -passwords og husk, at brugernavne og passwords er personlige. Benyt eventuelt et program, der kan huske passwords til alle dine tjenester.

Spam og phishing-mails er i dag et problem, som de fleste kender til. De uopfordrede henvendelser er dog blevet mere professionelt udført og kommer også som telefonopkald, SMS'er eller som venne-anmodninger på de sociale netværkstjenester. Fælles for dem er, at man bør være kritisk og undlade at svare, hvis man er i tvivl. Ofte handler det nemlig om, at man vil få os til at købe et produkt, vi ikke har behov for, franarre os kreditkortoplysninger, få os til at ringe til et overtakseret telefonnummer eller lægge spam på vores Facebook-væg.

Vær kritisk over for uopfordrede henvendelser:

8. **Undlad at besvare uopfordrede henvendelser**. Hverken banken, kreditkortselskabet, Google eller Microsoft vil bede dig bekræfte dine kontooplysninger. Undlad derfor at besvare mails eller

telefonopkald, der beder dig gøre dette. Tilsvarende kan links i uopfordrede mails føre dig til websider med skadelig kode, og vedlagte filer kan indeholde virus og lignende. Slet mailen, hvis du er i tvivl, og undlad at svare tilbage på mærkelige SMS'er og telefonopkald, da der kan være tale om overtakserede betalingstjenester.

Sociale medier er i dag også et middel til spredning af spam og malware samt indsamling af personlige oplysninger, som kan benyttes til social engineering. Vær derfor opmærksom på, hvilke oplysninger du giver andre adgang til, venneanmodninger fra folk du ikke kender, samt links til applikationer, hjemmesider med mere, som kan være inficeret med malware.

Brug af sociale netværkstjenester:

9. **Beskyt dine oplysninger og vær kritisk over for andres informationer og motiver**. Vær opmærksom på, hvem du giver adgang til. Brug privatlivsindstillinger til at beskytte dine personlige oplysninger og benyt tredjepartsapplikationer med omtanke. Vær desuden opmærksom på informationer, du modtager fra andre. Sender dine venner ikke normalt links til videoklip med spektakulære titler, anbefalinger af applikationer og lignende, kan det være en god idé at ignorere det.

De personlige data vi selv deler og lægger på nettet, kan af og til misbruges eller benyttes i sammenhænge, som kan være vanskelige at overskue. Mange data er vi ikke selv herre over, om ender på nettet. Desuden gælder, at læserbreve, debatindlæg, deltagerlister fra diverse aktiviteter samt billeder fra julefrokosten eller din seneste ferie ofte vil være tilgængelige på internettet, selv om du sletter dem. De kan på et tidspunkt blive set af nogen, som du ikke ønsker skal se dem, eller sat i en sammenhæng du ikke ønskede. Vær derfor kritisk, inden du trykker på upload-knappen.

Beskyt dit privatliv på nettet:

10. **Læg kun oplysninger på nettet, som alle til enhver tid må se**. Vær også opmærksom på de oplysninger, du afgiver til andre. Sørg for at læse aftalevilkår igennem og vær kritisk, så du ved, hvordan dine data bruges og hvad andre publicerer om dig. Tilsvarende skal du spørge, inden du lægger billeder og oplysninger ud om andre end dig selv.

Udvikling og brug af informationsteknologi er under konstant udvikling. Selv om ovenstående anbefalinger følges, vil der derfor være risici, som det kan være vanskeligt at overskue og vejlede om. Derfor bør man som udgangspunkt forholde sig kritisk til mediet og de informationer, der modtages og sendes. Brug derfor teknologien og medierne med omtanke. Tænk dig om og brug din sunde fornuft.

Opdaterdinpc; *"Gode råd"*.
ecunia; *"Download - Secunia Personal Software Inspector (PSI)"*.

10.2. Anbefalinger til it-ansvarlige

Mens det er den enkelte borger, der har ansvaret for sikkerheden på de installationer og tjenester, han benytter, bliver denne rolle i organisationerne varetaget af de it-ansvarlige. Det er dem, som ud fra retningslinjerne i organisationens informationssikkerhedspolitik varetager den praktiske del af sikkerheden på systemer, hvor udvikling og drift ikke er blevet outsourcet eller erstattet af tjenester i skyen. Det er således de it-ansvarlige, som har ansvar for, at organisationens systemer og data er tilgængelige, samtidig med at integriteten og fortroligheden opretholdes.

De it-ansvarlige bør fungere som ledelsens sparringspartnere og forlængede arm på udførelse og implementering af organisationens informationssikkerhedspolitik. Ofte vil det være dem, som er i stand til at bidrage kvalificeret til de konsekvens- og risikovurderinger, som i sidste ende skal føre til de forskellige politikker, regler og procedurer.

En ikke uvæsentlig del af organisationens systemer udgøres af de ansattes arbejdsstationer, bærbare computere og mobile enheder. At holde dem opdaterede og sikre udgør en væsentlig del af it-afdelingens arbejde. Som en naturlig del af informationssikkerhedspolitikken bør der implementeres procedurer, der sikrer, at medarbejdernes udstyr er sikret mod angreb.

Anbefalingerne til borgerne om hvordan man beskytter sin computer, kan tjene som en rettesnor, men skal selvfølgelig tilpasses den enkelte organisation og dennes behov.

Sikkerhed på de ansatte enheder:

1. **Hold brugernes enheder opdaterede**. Implementer procedurer, der sikrer, at der benyttes automatisk opdatering på alle enheder, samt at der benyttes centralt styret firewall og opdateret antivirusprogram.

Informationspolitikken bør tjene som rettesnor for, hvorledes organisationen sikrer sine aktiver og i praksis udfører sikkerhedsarbejdet. Ofte handler det om prioriteringer, der bør tages ud fra forretningsmæssige hensyn. Derfor er det væsentligt, at ledelsen involveres i arbejdet med, hvad der skal prioriteres og hvorfor.

Organisationens informationssikkerhedspolitik:

2. **Forlang aktiv involvering af ledelsen**. Det er ledelsen, der ud fra forretningsmæssige kriterier skal bidrage med konsekvensvurderinger på systemer og klassificering af data. Det er det, som bør være styrende for prioriteringen af organisationens informationssikkerhedsarbejde. Uden ledelsens involvering og engagement vanskeliggøres dette.
3. **Beredskabsplaner ved kritiske hændelser**. Et godt kriseberedskab kan afværge mange katastrofer. Brug derfor organisationens risikovurderinger som input til i samarbejde med ledelsen at udfærdige beredskabsplaner. Udbred kendskabet til beredskabsplanerne til alle relevante aktører. Husk at en væsentlig del af

beredskabet også handler om at kommunikere ærligt og troværdigt til potentielt berørte medarbejdere, kunder, leverandører og/eller pressen.

4. **Informationssikkerhedspolitikken er ikke statisk**. I takt med omgivelsernes, medarbejdernes og forretningens ændrede krav til brug af teknologien bør informationssikkerhedspolitikken opdateres. Fastlæg løbende intervaller for opdatering. Sørg for, at aktuelle trusler inkluderes, og at brugerne er bekendte med ændringerne. Awareness handler også om, at brugerne er opdateret med de retningslinjer, de skal følge, og ikke mindst hvorfor.

Der kan være mange argumenter både for og imod at lade brugerne selv stå for indkøb af udstyr til brug i arbejdsmæssige sammenhænge. En sådan politik er dog ikke uproblematisk. Som minimum kræver det, at der på baggrund af risikovurdering udfærdiges politikker, regler og procedurer for brugen af eget udstyr på organisationens installationer.

Smartphones og tavle-pc'er indgår i mange organisationer som naturlige redskaber på lige fod med computeren. I modsætning til denne er der dog ofte kun ringe mulighed for at begrænse brugernes udfoldelser med hensyn til for eksempel installation og brug af applikationer. Hvad enten organisationen har en politik om, at dens ansatte må medbringe og benytte deres eget udstyr eller ej, vil man derfor have de samme problemstillinger inde på livet.

Bring Your Own Device (BYOD) er kommet for at blive. Problematikkerne herfra gælder dog også for virksomhedsudleverede smartphones og tavle-pc'er.

BYOD-problematikker gælder også smartphones og tavle-pc'er:

5. **Inkluder BYOD-problematikker i informationssikkerheds-politikken**.
   Tag aktivt stilling og lav retningslinjer i for brug af medarbejdernes eget udstyr på organisationens installationer. Inkluder organisationsudleverede smartphones og tavle-pc'er, og gør det klart, hvordan et stigende krav om brug af og tilgængelighed fra multiple platforme ønskes håndteret. Udfærdig de nødvendige regler og procedurer, der sikrer adgangen til net og data.

Fortrolighed af data vedrører ikke kun organisationen selv. Hvis kunder, leverandører og samarbejdspartnere skal bevare tilliden til organisationen, skal data vedrørende dem vedblive at være fortrolige. Overvej derfor, hvem der må tilgå data og hvordan. Tænk kryptering ind i alle scenarier, også for medarbejdernes eget udstyr.

Giv sikre alternativer til at sende data over Gmail-kontoen, Dropbox eller noget helt tredje, hvor man ikke har kontrol over sikkerheden, når data skal benyttes uden for arbejdspladsen. Med indførelsen af EU's kommende databeskyttelsesdirektiv kan en eventuel datalækage blive dyr, ikke bare i tabt arbejdstid, salg og renomme.

Fortrolighed af data:

6. **Overvej adgang til data og brug kryptering**. Begræns adgangen til det nødvendige og brug systemer til Data Leak Prevention og kryptering af forretningskritiske data. Det gælder både data placeret i skyen, på egne servere, i transaktionen og ved anden transport på for eksempel bærbare computere, smartphones og andre mobile enheder.

Vidende og opmærksomme medarbejdere er ofte det bedste værn mod flere af de trusler, vi ser i dag. En væsentlig del af informationssikkerheden handler derfor om at holde medarbejderne opdateret og på vagt over for de aktuelle trusler. At gøre det klart hvorfor noget er en trussel og hvad motiverne bag er. I den kontekst vil de fleste kunne forstå de regler og begrænsninger, som informationssikkerhed jo også er.

Her spiller de it-ansvarlige en central rolle i forhold til at komme med input til den løbende opdatering af medarbejderne. De har haft indflydelse på udfærdigelse af organisationens informationssikkerhedspolitik, og det er oftest dem, som først oplever unormaliteter på net og installationer.

Awareness:

7. **Hold organisationens ansatte opdateret**. Hold løbende organisationens ansatte opdateret med aktuelle informationssikkerhedsproblematikker, der er relevante for netop dem. Gør dem klart, hvorfor noget er en trussel og motivet bag, og beskriv det i en kontekst af organisationens egne politikker og regler.

Det er ikke kun organisationens ansatte og deres enheder, som udgør en risiko for informationssikkerheden. I stigende grad har vi set, at organisationernes forretningssystemer har været mål for angreb. Det være sig angreb, der har til formål at stjæle data, denial of service-angreb eller angreb, som har til formål at benytte dem til hosting af malware eller phishing-sider.

Særlig SQL- injection på webapplikationer har været målet. Derfor bør man skærpe fokus på også at holde organisationens forretningssystemer opdaterede og sikre mod angreb.

Organisationens forretningssystemer:

8. **Skærp fokus på organisationens webapplikationer**. Valider alle brugersendte data inden eksekvering og/eller lagring. Brug automatisk softwareinspektion samt periodiske scanninger og penetrationstests til afklaring af sårbarheder. Luk for services, som ikke benyttes, da de også kan være sårbare.
9. **Giv kun mulighed for brug af stærke passwords**. Svage passwords er også en potentiel adgang til kompromittering af data. Giv derfor kun mulighed for brug af stærke passwords på alle leverandør-,

medarbejder- og kundeadgange. Implementer procedurer der sikrer, at der kun er mulighed for at definere stærke passwords lokalt såvel som på organisationens forretningssystemer.

Tænk sikkerhed ind i hele forsyningskæden. Undersøg markedet og stil krav til leverandørerne, således at sikkerhed indføres i kontrakterne. Betragt organisationens kunder og leverandører som samarbejdspartnere og tænk sikkerheden i relationen. Det er altid nemmere at inkludere sikkerhed på projektstadiet end at skulle putte det på efterfølgende.

Samarbejdsrelationer og leverandører:

10. **Tænk sikkerhed ind i relationen til leverandører og kunder**. Sørg for, at sikkerhed inkluderes allerede på projektstadiet. Brug organisationens risikovurderinger i udfærdigelse af kravspecifikationer og kontrakter. Tænk leverandører som en kilde til viden og inspiration til, hvordan sikkerheden kan indbygges i de færdige løsninger og få tilstrækkelig information og uddannelse. Det er trods alt leverandørerne, der har den største erfaring og viden om netop deres ydelse.

10.3. Anbefalinger til beslutningstagere

I organisationerne såvel som i det politiske liv er det beslutningstagerne, der skaber de strategiske og økonomiske rammer for, hvordan vi ønsker at udvikle samfundet ved brug af informationsteknologi. Hermed er det også dem, der har ansvar for at skabe de overordnede rammer for, hvordan vi ønsker at beskytte borgernes, organisationernes og nationens data. Det hvad enten det handler om på nationalt plan at udfærdige lovgivning, så den tilpasses den teknologiske udvikling, eller at udfærdige politikker og regler for organisationernes ansatte.

Informationsteknologi har særligt gennem de seneste 10 år været midlet til at udbrede velfærdsydelser på en nemmere og mere effektiv måde. Således kan vi fra dagligstuen for eksempel selv beregne og ændre vores skatteoplysninger, ansøge om nyt pas eller genlåne bøger på biblioteket.

På samme vis har teknologien været en vækstmotor for det private erhvervsliv. Den har effektiviseret mange af deres administrative opgaver og introduceret produkter og tjenester, som for kun få år tilbage syntes som ren science fiction.

Hvem havde bare i midt-halvfemserne forestillet sig, at vi i dag kunne se udsendelser på vores fjernsyn, når vi havde lyst, og ikke når de blev sendt. At et satellitbaseret system ikke blot kunne vise vej, men også finde ny og hurtigere vej, når der var kø. Eller at vi kunne surfe på internettet fra vores smartphone. Ja, dengang havde vi aldrig hørt om en smartphone, og internettet var bestemt ikke noget, alle havde kendskab til.

Teknologien har dog også introduceret nye risici. Vi ønsker, at udviklingen af teknologien fortsætter, men mener også, at vi bliver nødt til at adressere nogle af de farer, der lurer i den digitale verden. Derfor mener vi grundlæggende, at informationssikkerhed bør inkluderes i strategierne for, hvordan vi benytter informationsteknologien som vækstskaber.

Informationssikkerhed er i stigende grad blevet en forretningsparameter, som blandt andet bruges til at vælge eller fravælge leverandører og samarbejdspartnere. Tænk blot på markedet for cloud-baserede løsninger. Her har manglende garantier om sikkerhed og placeringen af data samt manglende efterlevelse af dansk lovgivning medført fravalg af en lang række udenlandske leverandører af cloud-baserede tjenester.

Oven på de seneste års mange hændelser med læk af fortrolige data breder fokus på informationssikkerheden sig. Også ved valget af leverandører og samarbejdspartnere i andre brancher. Det er derfor oplagt at betragte informationssikkerhed som et integreret element i diskussionen om, hvordan vi benytter informationsteknologien som vækstskaber.

Informationssikkerhed som del af forretningen:

1. **Informationssikkerhed som forretningsparameter**. Informationssikkerhed handler om at skabe tryghed. Troværdig kommunikation om organisationens informationssikkerhedstiltag vil derfor underbygge kundens tillid til organisationen og dens produkter. Også i det som kommunikeres til organisationens kunder, leverandører og samarbejdspartnere.
2. **Informationssikkerhed som strategielement**. Gør en dyd af rettidig omhu og inkluder informationssikkerhed i de langsigtede strategier for udvikling og brug af teknologi. Strategier for udvikling af markeder, produkter og tjenester bør samtidig tage højde for eventuelle nye risici og beskrive organisationens retningslinjer for, hvordan man ønsker at tilpasse informationssikkerheden hertil.

I ovenstående sammenhænge mener vi, at software- og tjenesteleverandører bør være deres ansvar voksent og skærpe fokus på at udvikle robuste og sikre løsninger. En ensidig fokus på added value, release-datoer og lignende har medført, at den cyklus, hvormed vi i dag installerer nye versioner af vores programmer, er blevet kortere. Særligt hvis vi samtidig ønsker at benytte programmer, der også er sikre, eller benytte de online tjenester, som kun understøtter den seneste version af browseren eller dennes plugins. Selvfølgelig undgår vi nok aldrig helt at skulle installere nye versioner eller opdatere eksisterende programmer, det er trods alt menneskeligt at fejle.

Sikkerhed i produkter og tjenester:

3. **Tænk sikkerheden ind fra starten**. Informationssikkerhed er i nogen grad i dag det samme som anvendelighed. Tænk derfor mulige scenarier for informationssikkerhed ind i hele produktets livscyklus. Brug frameworks, der sikrer produktets robusthed, og lav løbende review af koden og foretag de nødvendige test.

I sidste ende er det jeres kundegrundlag, der risikerer at blive kompromitteret.

Informationssikkerhedspolitikken konkretiserer og operationaliserer strategiernes overordnede målsætninger. Det er her, organisationens forretningsaktiver risikovurderes og der beskrives tiltag for, hvordan man ønsker at sikre dem. Som ved budgetter og regnskaber foretages der periodisk ekstern revision af politikken. En godkendt revision bør dog ikke være et mål i sig selv. Det er derfor vigtigt, at politikken løbende opdateres og følges.

Skab rammer, der synliggør organisationens tiltag og indbyg procedurer, der sikrer, at de efterleves. Vi mener, at der bør være transparens omkring denne proces, således at organisationens ansatte bidrager, kender, forstår og følger beslutninger om brugen af organisationens it-aktiver. I modsat fald kan det medføre kompromittering af systemer og data med mistet tillid og omdømme til følge.

Informationssikkerhed i et perspektiv af god selskabsledelse:

4. **Skab synlighed af ledelsens involvering i informationssikkerhed**. Ledelsesinvolvering er en afgørende faktor for, at informationssikkerhedspolitikken ikke bare følger gældende standarder og kan revideres, men at den rent faktisk også følges. Derfor skal ledelsen involvere sig og skabe synlighed om den.
5. **Prioriter og synliggør risikostyring**. Lad risikostyringsaktiviteter være en naturlig og synlig del af ledelsens arbejde, også på informationssikkerhedsområdet. Trods alt er det jo ledelsen, der bedst er i stand til at vurdere de forretningsmæssige konsekvenser ved brud på sikkerheden.
6. **Afsæt de fornødne ressourcer til uddannelse**. Viden og erfaring er grundlæggende fundamenter for opretholdelse af informationssikkerheden. Ledelsen bør derfor prioritere de ansattes uddannelse og styrke aktiviteter til oplysning, videndeling og samarbejde. Herved synliggøres, at sikkerhed er et område, der prioriteres.
7. **Skab samarbejdsrelationer omkring informationssikkerhed**. Informationssikkerhed implementeres og udvikles ikke i lukkede fora. Skab rammer for samarbejder, der inkluderer de ansatte, leverandører, kunder og øvrige interessenter. Det handler om gensidig videndeling og forventningsafstemning, der gavner helheden.

Informationssikkerhed er en afvejning af risici, konsekvenser og økonomi. I anvendelighedens hellige navn vil det ofte betyde, at man på nogle områder må gå på kompromis med informationssikkerheden. Det er derfor nødvendigt at vide, hvordan skaden begrænses, når det går galt.

Som ved andre krisesituationer er det ofte beslutningstagerne, der er blandt de første, som bliver orienteret, når systemerne ikke er tilgængelige, eller organisationens data kompromitteres. Eller sådan bør det i hvert fald være, da det er dem, der kan afsætte de fornødne ressourcer til at afværge en krisesituation. Ofte er det også beslutningstagerne, der efterfølgende skal orientere leverandører, kunder og presse, indgå i forhandlinger om eventuel bod og lignende. Et ordentligt kriseberedskab er derfor afgørende, når det går galt.

Vær beredt:

8. **Hav beredskabsplanen på plads**. Sørg for, at der er udfærdiget fyldestgørende beredskabsplaner for kritiske forretningsaktiver, der klart beskriver arbejds- og kommunikationsgange. Hav nødplaner parat, så kommunikationskanaler og produktion kan opretholdes under krisen, og sørg for løbende at efterprøve beredskabet.

Der er gennem de seneste års finanskrise blevet effektiviseret og skåret i budgetterne til investeringer i informationsteknologi. Det er ofte budgettet til informationssikkerheden, der står for skud, da investeringer her ikke skaber værdi for forretningen. Det kan på sigt vise sig at være en dyr beslutning, når organisationens systemer kompromitteres.

Informationssikkerhed koster:

9. **Brug de fornødne ressourcer**. At spare på informationssikkerheden kan i det lange løb være en dyrt. Et ønske om at effektivisere bør ikke give anledning til at gå på kompromis med de grundlæggende principper for informationssikkerhed. De midler man bruger her, skal jo fortsat stå mål med værdien af det, man ønsker at sikre. I sidste ende kan besparelser på informationssikkerhed nemlig koste langt mere end det, som er sparet. Overvej derfor, om der er råd til at spare på informationssikkerhed.

Der kan argumenteres for, at borgernes informationssikkerhed er deres eget ansvar, ligeså vel som det er organisationernes eget ansvar at opretholde den nødvendige sikkerhed. I en stadig mere kompleks verden er de nødvendige forholdsregler dog blevet vanskeligere at gennemskue for borgeren. Vi mener, at en optrapning af midlerne til også offensiv krigsførelse introducerer nogle risici, som i sidste ende kan ramme borgerne. Det er jo også deres data, som er placeret i de offentlige systemer, der kan blive mål for angreb, eller deres internetforbundne systemer, der utilsigtet kan blive ramt.

Borgernes informationssikkerhed:

10. **Glem ikke borgerne i cyberkrigen**. I takt med optrapningen af ressourcer til både offensiv og defensiv krigsførelse på internettet bør vi ikke glemme borgernes sikkerhed. Vores frygt er nemlig, at en global optrapning utilsigtet vil ramme borgernes systemer og data. Hvor vi tidligere byggede beskyttelsesrum og informerede om, hvordan man skulle forholde sig ved atomangreb og lignende, er der på internettet ikke taget tilsvarende foranstaltninger til at beskytte borgerne. Inddrag derfor internetudbyderne i arbejdet med at sikre borgernes systemer og data.

11. Ordliste

Anonymous-bevægelsen: En løst defineret internetbaseret gruppe, som i 2003 opstod via hjemmesiden 4chan.org. Gruppen benytter sig blandt andet af DDoS angreb i deres kamp for ytringsfrihed og mod hvad de anser som censur og misbrug af nettet. Er særlig kendt for dens modstand mod Scientology Kirken og for sin støtte til Wikileaks og The Pirate Bay. Gruppen stod også bag operation AntiSec i foråret 2011.

Awareness: Betegnelse for tiltag eller aktiviteter, der skaber opmærksomhed og påvirker ansattes eller borgeres viden og adfærd i forhold til it-sikkerhed.

BYOD: Bring Your Own Device, dækker over at et stigende antal organisationer lader de ansatte selv stå for indkøb og drift af deres eget udstyr. Det giver på den ene side større fleksibilitet, men på den anden side introducerer det en række problemstillinger i forhold til informationssikkerheden.

Botnet: Et botnet er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Navnet kommer af "robot" og "net". Ejerne af computerne ved ikke, at deres pc er inficeret med et botnet-program og indgår i botnettet. Angriberen udnytter gerne sine "robotter" til at foretage koordinerede denial of service-angreb eller udsende spam- og phishing-mails.

Brute force: Dækker i datalogien over en udtømmende afsøgning af et løsningsrum. Inden for it-sikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord, ofte ud fra foruddefinerede lister og ordbøger.

Cloud computing: Services distribueret i en sky af primært virtuelle ressourcer. Skyen giver mulighed for, at man får adgang til ressourcer efter behov. Skalerbarhed og pris vil ofte være de væsentligste argumenter for at lade sine services outsource til skyen. Overordnet skelnes mellem tre forskellige typer af cloud-services: Software as a Service (SaaS), Platform as a Service (PaaS) og Infrastructure as a Service (IaaS).

Command & control server: Et botnets centrale servere, hvorigennem det er muligt at sende kommandoer, som udføres af computere i botnettet, der er inficeret med botnet-programmer.

Cross-site request forgery (CSRF): En metode, der muliggør at uautoriserede parametre og kommandoer eksekveres på serveren gennem henvendelser fra en bruger, som websitet har tillid til. Metoden kan for eksempel medføre overtagelse af brugerens session til det enkelte site.

Cross-site scripting (XSS): En sårbarhed på et websted, der gør det muligt at afvikle scriptkode i browseren hos en bruger, der besøger det. Der er forskellige former for cross-site scripting, som gør det muligt at udføre komplekse angreb. Metoden kan for eksempel anvendes til phishing, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website, som en bruger har tillid til, til at få adgang til fortrolig information.

CVE, CVE-nummer: Common Vulnerabilities and Exposures, forkortet CVE, er en liste over offentligt kendte sårbarheder i software. Listen dækker sårbarheder i de fleste kendte og alment udbredte programmer, men ikke i skræddersyet eller internt udviklet software, der ikke er i distribution, såsom de fleste webapplikationer.

Compliance: Overensstemmelse eller efterlevelse af gældende regler. I it-sikkerhedssammenhæng beskriver compliance organisationernes evne til at efterleve krav til informationssikkerhed efter gældende lovkrav eller godkendte standarder som for eksempel DS 484, ISO 27001 eller lignende.

Data Leak Prevention, DLP: System, der på grundlag af centralt definerede politikker identificerer, overvåger og beskytter data, der er lagret, i bevægelse eller i brug, mod uautoriseret brug og tab. Beskyttelsen sker ved dybdegående analyse af data og et centralt styret management framework. DLP beskytter også organisationer mod social engineering og intern misbrug af data.

Defacement: Defacement eller web-graffiti, betegner et angreb, hvor websider tagges (overskrives) med angriberens signatur og ofte også et politisk budskab.

DeIC: Danish e-Infrastructure Cooperation - blev dannet i april 2012 ved en sammenlægning af Forskningsnettet og Dansk Center for Scientfiic Computing (DCSC). DeIC er etableret som et resultat af Infrastruktur Roadmapprocessen i regi af Styrelsen for Forskning- og Innovation, og gennem en national samarbejdsaftale om koordinering og etablering af fælles e-Infrastruktur til e-Science for alle forskningsområder. Aftalen er indgået mellem Styrelsen for Forskning- og Innovation og alle universiteterne i efteråret 2011. DeIC skal sikre den bedst mulige nationale ressourceudnyttelse på e-Infrastrukturområdet.

Denial of Service (DoS): Et angreb der sætter en tjeneste, funktion eller et system ud af drift eller på anden måde gør det utilgængeligt for brugerne. Et eksempel kan være et angreb, der overbelaster en webserver ved at sende mange forespørgsler. Disse angreb udføres ofte fra flere computere samtidig. Det kaldes distributed denial of service (DDoS).

Drive-by attacks, drive-by download: Angreb hvor tilfældige besøgende på en kompromitteret hjemmeside forsøges inficeret med skadelige programmer. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til, og infektionen foregår uden dennes vidende. Infektionen udnytter som regel sårbarheder i programmer på brugerens pc, ofte browseren eller udvidelser som Flash og Java.

E-infrastruktur: Videnskabelige redskaber og faciliteter baseret på computerteknologier; til indsamling af data, transport og lagring af data elektronisk, databehandling samt værktøjer til visualisering og

simulering. De vigtigste elementer af e-Infrastruktur er elektroniske netværk og dedikerede gridfaciliteter, high-performance-computerfaciliteter samt databanker.

E-science: Indsamling, behandling og anvendelse af videnskabelig information i dataform.

Exploit: Et program som forsøger at udnytte sårbarheder i software med det formål at kompromittere systemet.

Exploit kit: Software der placeres på et website og afsøger de besøgendes computer for sårbarheder i browseren og tilhørende programmer. Er computeren sårbar, kompromitteres den med et af programmets exploits. Indeholder ofte også funktioner til opdatering, statistik med mere.

Forskningsnettet: Et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner DeIC forskningsinstitutionerne med en række tjenester til e-Infrastruktur og e-Science.

God selskabsledelse: Corporate governance, på dansk god selskabsledelse, opstod som følge af en række erhvervsskandaler i England og USA og bredte sig op gennem 1990'erne til resten af Europa. God selskabsledelse skal sikre en hensigtsmæssig rolle- og ansvarsfordeling i forbindelse med kontrol og styring af organisationen. Et væsentligt element af god selskabsledelse omhandler risikostyring og revision. It governance er en integreret del af corporate governance, der har til formål at sikre strategisk udnyttelse af brugen af it, således at it både understøtter organisationens effektivitet og medvirker til at udvikle organisationen.

GovCERT: GovCERT-funktionen (Government Computer Emergency Response Team), der i Danmark er placeret under Forsvarsministeriet, skal sikre, at der i staten er overblik over trusler og sårbarheder i produkter, tjenester, net og systemer. På den baggrund skal tjenesten foretage en løbende vurdering af itsikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler.

Hacker: På dansk betyder hacker en person, der uden foregående tilladelse forsøger at kompromittere computersystemers sikkerhed. På engelsk kan man skelne mellem en hacker og en cracker eller whitehat hacker og blackhat hackere, afhængigt af om aktivitetens formål er at forbedre kode og/eller sikkerhed, eller det er at udføre it-kriminalitet.

Hacktivisme: Sammentræning af hack og aktivisme, eller på dansk "politisk motiveret hacking." Det vil sige forfølgelse af politiske mål gennem brugen af midler som defacement, DDoS-angreb, informationstyveri og lignende.

Identitetstyveri: Identitetstyveri betegner brugen af personlige informationer til misbrug af en andens identitet. Det modsvares i den juridiske terminologi af dokumentfalsk og bedrageri. Personlige informationer indsamles og misbruges ved phishing, hacking eller infektion med trojanske heste. Informationerne kan fx være kreditkortinformationer, personnumre eller adgangsoplysninger til mailkonti, internetbutikker, sociale netværkssider, onlinespil og lignende.

ISO/IEC 27001/2: En normativ standard for it-sikkerhed, der i staten helt skal erstatte brugen af DS 484. I familien indgår ud over de to normative standarder ISO 27001/2 og ISO 27006 en række standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder.

LulzSec: Hackergruppe, der udspringer af Anonymous. Navnet er en forvanskning af LOLs (Laughing Out Loud) og security. Gruppen oplyste, at dens formål var at have det sjovt, men har enkelte gange offentliggjort politiske budskaber. Er kendt for højt profilerede DDoS-angreb samt hacking og efterfølgende offentliggørelse af fortrolige informationer fra myndigheder og store virksomheder.

MAM: Mobile Application Management beskriver software der benyttes til central kontrol og godkendelse af tilgængelige mobil applikationer.

Malware, skadelig kode: Sammentrækning af malicious software eller på dansk ondsindede programmer. Malware er en samlebetegnelse for virus, orme, trojanske heste, keyloggere, spyware, adware, botnet-programmer og lignende.

Man-in-the-browser: Et angreb relateret til Man-in-the-middle angreb, hvor en trojansk hest kan modificerer websider og indhold af transaktioner uden brugerens viden. Man-in-the-browser funktioner kan være at overtage sessionen til netbanken, overføre penge fra brugerens konto og herefter ændre indholdet i browseren, således at overførelsen ikke fremgår af kontooversigten.

Man-in-the-Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes vidende, videresendes gennem en mellemmand, der aktivt kan kontrollere kommunikationen. I praksis kan et Man-in-the-middle-angreb for eksempel foregå ved en ændring af DNS-registrering på enten DNS-serveren eller ved ændring af hosts-filen.

MDM: Mobile Device Management er software, der benyttes til centralt administration og sikkerhed på enhedsniveau af mobile enheder.

NemID: NemID er en fælles certifikatbaseret dansk login-løsning til netbanker og offentlige hjemmesider, der baserer sig på den offentlige digitale signatur. Løsningen, som består af en personlig adgangskode og et nøglekort, kan benyttes fra en hvilken som helst computer uden foregående installation af software. NemID blev sat i drift 1. juli 2010 og bliver drevet af firmaet Nets DanID.

NORDUnet: NORDUnet er et fællesnordisk samarbejde om drift af nordisk og international e-infrastruktur og tjenester mellem forsknings og uddannelsesnetværk i Danmark, Finland, Island, Norge og Sverige.

Orm: Et program, der spreder sig i netværk ved at udnytte sårbarheder i

dets computere. I TCP/IP-verdenen sker det typisk ved, at ormeprogrammet kontakter den port, som det sårbare program lytter på.

Phishing: Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på phishing optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank, kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

Pirate Bay: The Pirate Bay blev grundlagt i slutningen af 2003, som en del af det svenske Piratbyrån. Den er i dag verdens største Bittorrent-tracker. Den åbne server indeholder links til torrent-filer og hoster således ikke selv ophavsretsligt beskyttet materiale. Den 26. november 2008 stadfæstede landsretten en kendelse om at filtrere adgangen til The Pirate Bay for alle abonnenter hos internetudbyderen Tele2. Siden har de fleste danske internetudbydere fulgt trop og filtreret adgangen til The Pirate Bay.

Ransomware: Sammentrækning af ordene ransom (løsesum) og malware. Skadelig kode, der tager data som gidsel, ofte ved kryptering.

Scanning, portscanning: Kortlægning af åbne porte på internettet, der har til formål at identificere sårbare services knyttet til dem. En portscanning foregår typisk ved, at der forespørges efter mange porte på få maskiner, eller én port på mange maskiner. Oftest benyttes et program til at foretage portscanninger. Brugen af firewalls vil som udgangspunkt lukke for adgangen til maskinens åbne porte.

Social engineering: Manipulation, der har til formål at få folk til at bidrage med informationer eller at udfører handlinger, som fx at klikke på links, svare på mails eller installere malware.

Spam: Uopfordrede massedistribuerede reklamemails med henblik på salg af produkter eller services.

SQL-injection: Et angreb der ændrer i indholdet på en webside ved at sende kommandoer til den bagvedliggende SQL-database gennem usikre input-felter på websiden, som for eksempel søgefelter eller kommentarfelter, eller gennem usikre parametre i websidens URL'er.

Stuxnet: Stuxnet er blandt de hidtil mest avancerede orme. Ormen spreder sig via USB-nøgler ved at udnytte en sårbarhed i Windows' behandling af genveje. Herefter angriber den industrielle Siemens WinCC SCADA-systemer. Den menes at være udviklet til at sabotere Irans atomprogram.

Sårbarhed: En fejl i et it-system, som en angriber kan udnytte til at få adgang til systemet, forhindre det i at fungere eller på anden måde misbruge det.

Sårbarhedsscanning: Kortlægning af kendte sårbarheder knyttet til services på et systems åbne porte. Benyttes ofte efter foregående scanning.

Trojansk hest: Et program der har andre, ofte ondartede, funktioner end dem som det foregiver at have. Trojanske heste indeholder ofte dialer-, bagdørs- eller keylogger-funktionalitet, eller benyttes til installation af virus, botnetprogrammer og lignende. Trojanske heste identificeres ofte af antivirus- og antispywareprogrammer.

Virus: Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virussen, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde virus, men dokumenter med makroer kan også gøre det. Virus spredes ofte som mail vedlagt en trojansk hest, der indeholder virussen selv.

Warez, piratsoftware: Begrebet dækker over computerprogrammer, musik, film og lignende, der distribueres illegalt og i strid med rettigheder og licensbetingelser. Warez er en sproglig forvanskning af flertalsformen af software.

Websårbarheder: En sårbarhed på en webapplikation, eller et tilknyttet system, som kan udnyttes gennem webapplikationen.

12. Figuroversigt

13. Referencer

Adobe, august 2012; "*Security updates available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-19.html

Adobe, december 2012; "*Security updates available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-27.html

Adobe, februar 2012; "*Security update available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-03.html

Adobe, januar 2012; "*Security updates available for Adobe Reader and Acrobat*"; adobe.com/support/security/bulletins/apsb12-01.html

Adobe, juni 2012; "*Security update available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-14.html

Adobe, maj 2012; "*Security update available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-09.html

Adobe, marts 2012; "*Security update available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-05.html

Adobe, november 2012; "*Security updates available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-24.html

Adobe, oktober 2012; "*Security updates available for Adobe Flash Player*"; adobe.com/support/security/bulletins/apsb12-22.html

Anonymous København; "*Velkommen til Anonymous København*"; anonkbh.dk/info/

Apple, 2012; "*About the security content of iTunes 10.7*"; support.apple.com/kb/HT5485

Apple, 2012; "*About the security content of Java for OS X 2012-005 and Java for Mac OS X 10.6 Update 10*"; support.apple.com/kb/HT5473

Apple, 2012; "*About the security content of Java for OS X Lion 2012-002 and Java for Mac OS X 10.6 Update 7*". support.apple.com/kb/HT5228

Apple, 2012; "*About the security content of OS X Lion v10.7.3 and Security Update 2012-001*"; support.apple.com/kb/HT5130

Apple, 2012; "*About the security content of OS X Lion v10.7.4 and Security Update 2012-002*"; support.apple.com/kb/HT5281

Apple, 2012; "*About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004*"; support.apple.com/kb/HT5501

Apple, 2012; "*About the security content of Safari 5.1.4*"; support.apple.com/kb/HT5190

Apple, 2012; "*About the security content of Safari 5.1.7*"; support.apple.com/kb/HT5282

Apple, 2012; "*About the security content of Safari 6*"; support.apple.com/kb/HT5400

Apple, 2012; "*APPLE-SA-2012-09-19-1 iOS 6*"; prod.lists.apple.com/archives/security-announce/2012/Sep/msg00003.html

Apple, 2012; "*APPLE-SA-2012-09-19-3 Safari 6.0.1*"; prod.lists.apple.com/archives/security-announce/2012/Sep/msg00005.html

Berlingske, 2012; "*3F-hacker-angreb rammer dagpengene*"; b.dk/nationalt/3f-hacker-angreb-rammer-dagpengene

Berlingske, 2012; "*Cyberkrig er større trussel mod Danmark end terror*"; b.dk/nationalt/cyberkrig-er-stoerre-trussel-mod-danmark-end-terror

Berlingske, 2012; "*Dansker får standset Facebook-fejl*"; b.dk/tech/dansker-faar-standset-facebook-fejl

Berlingske, 2012; "*Hackerne er ude efter dit TV*"; b.dk/tech/hackerne-er-ude-efter-dit-tv

Berlingske, 2012; "*IT-indbrud holdes skjult for dig*"; b.dk/nationalt/it-indbrud-holdes-skjult-for-dig

Berlingske, 2012; "*Politikere ønsker mere åbenhed om hackerangreb*"; b.dk/politiko/politikere-oensker-mere-aabenhed-om-hackerangreb

Bloomberg, 2012; "*Code in Aramco cyber attack indicates lone perpetrator*"; bloomberg.com/news/2012-10-25/code-in-aramco-cyber-attack-indicates-lone-perpetrator.html

BT, 2012; "*Anonymous: 3F-hackerne er forrædere*"; bt.dk/politik/anonymous-3f-hackerne-er-forraedere

Carnegie Mellon University, 2012; "*Before we knew it*"; users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

Centrum Wiskunde & Informatica, 2012; "*CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*"; cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware

Cisco, 2012; "*Multiple Vulnerabilities in Cisco AnyConnect Secure Mobility Client*"; tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac

Cisco, 2012; "*Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module*"; tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121010-asa

Cnet, 2012; "*German government tells public to stop using Internet Explorer*"; news.cnet.com/8301-10805_3-57515312-75/german-government-tells-public-to-stop-using-internet-explorer/

Computerworld, 2012; "*Apple patches Mac Java zero-day bug*"; www.computerworld.com/s/article/9225837/Apple_patches_Mac_Java_zero_day_bug

Computerworld, 2012; "*Flere danske medier ramt af stort hackerangreb*"; computerworld.dk/art/215384

Computerworld, 2012; "*Her er den første afpresnings-software på dansk*"; computerworld.dk/art/220175

Computerworld, 2012; "*Stort sikkerhedshul: Så nemt kan man stjæle dit cpr-nummer*"; computerworld.dk/art/221204

Computerworld, 2012; "*Telefirmaer taget med bukserne nede: Anede intet om CPR-huller*"; computerworld.dk/art/221213

Danmarks Statistik, 2011; "*Danske virksomheders brug af it - 2011*"; dst.dk/pukora/epub/upload/15242/dkit.pdf

Datatilsynet, 2012; "*Behandling af personoplysninger i cloud-løsningen Office 365*"; datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/

Datatilsynet, 2012; "*EU-Kommissionens reformpakke om databeskyttelse*"; datatilsynet.dk/nyheder/nyhedsarkiv/artikel/eu-kommissionens-reformpakke-om-databeskyttelse/

Datatilsynet, 2012; "*Udtalelse om EU-Kommissionens forslag til forordning om databeskyttelse*"; datatilsynet.dk/nyheder/nyhedsarkiv/artikel/udtalelse-om-eu-kommissionens-forslag-til-forordning-om-databeskyttelse-1/

DKCERT; "*DKCERT Sårbarhedsdatabase*"; sdb.cert.dk/login.php

Digitaliseringsstyrelsen, 2011; "*Cloud computing og de juridiske rammer*"; digitaliser.dk/resource/2274097/artefact/Cloud+computing+og+de+juridiske+rammer.pdf

Digital Sikkerhed, 2012; "*Nyt it-råd skal sikre tryg digitalisering*"; digitalsikkerhed.dk

DKCERT, 2012; "*Alvorligt hul i Java står åbent*"; https://www.cert.dk/nyheder/nyheder.shtml?12-08-27-13-02-46

DKCERT, 2012; "*Microsoft lukker huller i IE og Flash*"; https://cert.dk/nyheder/nyheder.shtml?12-09-24-08-56-11

DR, 2012; "*Cpr.dk angrebet af hackere*"; dr.dk/Nyheder/Indland/2012/11/06/132959.htm

Eric Romang, 2012; "*Zero-Day season is really not over yet*"; eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/

Erpscan, 2012; "*SAP critical patch update September 2012*"; erpscan.com/press-center/news/sap-critical-patch-update-september-2012/

Eu2012, 2012; "*Nye EU-regler om straffe for it-kriminalitet*"; eu2012.dk/da/NewsList/Juni/Uge-26/cybercrime

Europa-kommissionen, 2012; "*Commission proposes a comprehensive reform of the data protection rules*"; ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Europa-kommissionen, 2012; "*Opinion 01/2012 on the data protection reform proposals*"; ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

Finansrådet, 2012; "*Netbankindbrud - statistik*"; finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx

Finansrådet, 2012; "*Røveristatistik*"; finansraadet.dk/tal--fakta/statistik-og-tal/roeveristatistik.aspx

FireEye, 2012; "*Java zero-day - first outbreak*"; blog.fireeye.com/research/2012/08/java-zero-day-first-outbreak.html

FireEye, 2012; "*Zero-day season is not over yet*"; blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

Foreningen af Danske Interaktive Medier (FDIM); "*Browserbarometer*"; fdim.dk/Statistik/teknik/browserbarometer

Forbes, 2012; "*SOPA, ACTA and the TPP: Lessons for a 21st century trade agenda*"; forbes.com/sites/edblack/2012/02/29/sopa-acta-and-the-tpp-lessons-for-a-21st-century-trade-agenda/

F-secure; "*F-Secure Security Lab - virus world map*"; f-secure.com/en_EMEA/security/worldmap/

Gartner, 2012; "*Gartner survey shows BYOD is top concern for enterprise mobile security*"; gartner.com/it/page.jsp?id=2048617

Geogia Tech, 2012; "*Emerging cyber threats report 2013*"; gtsecuritysummit.com/pdf/2013ThreatsReport.pdf

Gizmodo, 2012; "*What is SOPA?*"; gizmodo.com/5877000/what-is-sopa

Google, 2012; "*Google Apps receives ISO 27001 certification*"; googleenterprise.blogspot.dk/2012/05/google-apps-receives-iso-27001.html

Google, 2012; "*Google Chrome releases*"; googlechromereleases.blogspot.com/

Google, 2012; "*Stable channel release*"; googlechromereleases.blogspot.ca/2012/07/stable-channel-release.html

Govcert, 2012; "*Angreb på Erhvervs- og Vækstministeriet*"

Identityfinder, 2012; "*Large-Scale Coordinated SQLi Attack on Higher Education*"; identityfinder.com/blog/post/Large-Scale-Coordinated-SQLi-Attack-on-Higher-Education.aspx

Information, 2012; "*En ny strategi for USA's militær*"; information.dk/289890

Information, 2012; "*Størstedelen af internet-logningen kan sløjfes*"; information.dk/301785

Kaspersky Lab, 2012; "*Back to Stuxnet: the missing link*"; securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link

Kaspersky Lab, 2013; "*Kaspersky Security Bulletin 2012. The overall statistics for 2012*"; securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012

KrebsonSecurity, 2012; "*Inside a 'Reveton' ransomware operation*"; krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

Københavns Universitet; "*Beredskabsstyring*"; informationssikkerhed.ku.dk/is-haandbogen/14_beredskabsstyring/

Københavns Universitet; "*Informationssikkerhedsorganisationen ISO*"; informationssikkerhed.ku.dk/organisation/

McAfee, 2012; "*Hacktivism - Cyberspace has become the new medium for political voices*"; mcafee.com/us/resources/white-papers/wp-hacktivism.pdf

McAfee, 2012; "'*Police ransomware' preys on guilty consciences*"; blogs.mcafee.com/mcafee-labs/police-ransomware-preys-on-guilty-consciences

McAfee, 2012; "'*McAfee threats report: Second quarter 2012*"; mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf

Microsoft, 2012; "*Microsoft security advisory (2757760)*"; technet.microsoft.com/en-us/security/advisory/2757760

Microsoft, 2012; "*Microsoft security advisory (2794220)*"; technet.microsoft.com/en-us/security/advisory/2794220

Microsoft, 2012; "*Microsoft security bulletin summary for april 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-apr

Microsoft, 2012; "*Microsoft security bulletin summary for august 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-aug

Microsoft, 2012; "*Microsoft security bulletin Summary for december 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-dec

Microsoft, 2012; "*Microsoft security bulletin summary for july 2012*";technet.microsoft.com/en-us/security/bulletin/ms12-jul

Microsoft, 2012; "*Microsoft security bulletin summary for june 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-jun

Microsoft, 2012; "*Microsoft security bulletin summary for March 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-mar

Microsoft, 2012; "*Microsoft security bulletin summary for may 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-may

Microsoft, 2012; "*Microsoft security bulletin Summary for november 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-nov

Microsoft, 2012; "*Microsoft security bulletin summary for october 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-oct

Microsoft, 2011; "*Microsoft security intelligence report volume 11*"; microsoft.com/security/sir/

Microsoft, 2012; "*More information on security advisory 2757760's Fix It*"; blogs.technet.com/b/srd/archive/2012/09/19/more-information-on-security-advisory-2757760-s-fix-it.aspx

Microsoft, 2012; "*MS12-063: Cumulative security update for Internet Explorer: September 21, 2012*"; support.microsoft.com/kb/2744842

Microsoft, 2012; "*Proof-of-Concept code available for MS12-020*"; blogs.technet.com/b/msrc/archive/2012/03/16/proof-of-concept-code-available-for-ms12-020.aspx

Microsoft, 2012; "*Microsoft releases Security Advisory 2718704*"; blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx

Mozilla, 2012; "*Mozilla Foundation security advisories*"; mozilla.org/security/announce/

Mozilla, 2012; "*Security advisories for Firefox*"; mozilla.org/security/known-vulnerabilities/firefox.html

NemID; "*Bruger-id og adgangskode*"; nemid.nu/support/bruger-id_og_adgangskode/

Nets, 2012; "*Dankort-misbrug de første seks måneder af 2012*"; www.nets.eu/dk-da/Om/om-virksomheden/nets-i-tal/misbrugstal/Pages/default.aspx

Nets, 2012; "*Netbanksvindel ved brug af NemID*"; www.nets.eu/dk-da/Om/nyheder-og-presse/Pages/Netbanksvindel-ved-brug-af-NemID.aspx

New York Times, 2012; "*Facing cyberattack, Iranian officials disconnect some oil terminals from internet*"; nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html

New York Times, 2012; "*In attack on Vatican web site, a glimpse of hackers' tactics*"; nytimes.com/2012/02/27/technology/attack-on-vatican-web-site-offers-view-of-hacker-groups-tactics.html

New York Times, 2012; "*One on one: Cole Stryker, author of 'Epic win for anonymous'*"; bits.blogs.nytimes.com/2011/09/02/one-on-one-cole-stryker-author-of-epic-win-for-anonymous/

National Institute of Standards and technology (NIST); "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Norsk regering, 2012; "*Nasjonal strategi for informasjonssikkerhet*"; regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf

Norsk regering, 2012; "*Nasjonal strategi for informasjonssikkerhet - Handlingsplan*"; regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf

Nyheter24, 2012; "*Anonymous-attackerna helt avblåsta*"; nyheter24.se/nyheter/internet/727883-anonymous-attackerna-avblasta-snalla-sluta-upp

Nyheter24, 2012; "*Polisrazzia mot webbhotellet PRQ*"; nyheter24.se/nyheter/internet/727351-polisrazzia-mot-webbhotellet-prq

Opdaterdinpc; "*Gode råd*"; opdaterdinpc.tdc.dk/publish.php?dogtag=opdaterdinpc_raad

Oracle, 2012; "*April 2012 critical patch update released*"; blogs.oracle.com/security/entry/april_2012_critical_patch_update

Oracle, 2012; "*Oracle critical patch update advisory - april 2012*"; www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html

Oracle, 2012; "*Oracle critical patch update advisory - January 2012*"; www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Oracle, 2012; "*Oracle critical patch update advisory - July 2012*"; www.oracle.com/technetwork/topics/security/cpujul2012-392727.html

Oracle, 2012; "*Oracle critical patch update advisory - October 2012*"; www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html

Oracle, 2012; "*Oracle Java SE critical patch update advisory - February 2012*"; www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html

Oracle, 2012; "*Oracle Java SE critical patch update advisory - june 2012*"; www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html

Oracle, 2012; "*Oracle Java SE Critical Patch Update Advisory - October 2012*"; www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html

Oracle, 2012; "*Oracle security alert for CVE-2012-4681*"; www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html

Panton, 2012; *"Rejsekortet: Sikkerhed som vi pensionerede i 90'erne"*; christian.panton.org/post/16458741723/rejsekort
Pastebin, 2012; "*Anonymous - #opeurope*"; pastebin.com/aUuuhLyD

Pastebin,2012;*"Dear citizens of Denmark"*; pastebin.com/UZJGwHjp

Pastebin, 2012; "*Untitled*"; pastebin.com/A33r79pe

Politiken, 2012; "*Hackere stjæler flere hundrede danskeres passwords*"; politiken.dk/erhverv/ECE1556987/hackere-stjaeler-flere-hundrede-danskeres-passwords/

Ponemon Institute, 2012; "*The impact of cybercrime on business*"; checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf

Rapid7, 2012; "*New Metasploit module to exploit GE PLC SCADA devices*"; www.rapid7.com/news-events/press-releases/2012/2012-new-metasploit-module-to-exploit.jsp

Repræsentanternes Hus, 2011; "*Stop Online Piracy Act*"; judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf

Retsinformation, 2012;"*Lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige*"; www.retsinformation.dk/Forms/R0710.aspx?id=142399

Seclists, 2012; "*[SE-2012-01] New security issue affecting Java SE 7 Update 7*"; seclists.org/bugtraq/2012/Aug/225

Security Explorations, 2012; "*Critical security issue affecting Java SE 5/6/7*"; seclists.org/fulldisclosure/2012/Sep/170

Secunia; "*Secunia Personal Software Inspector (PSI)*"; secunia.com/vulnerability_scanning/personal/

Securityweek, 2012; "*Following LulzSec arrests, AntiSec supporters attack Panda Security*"; securityweek.com/following-lulzsec-arrests-antisec-supporters-attack-panda-security

Softpedia, 2012; "*BlackHole Exploit Kit 2.0 Made available, price remains the same*"; news.softpedia.com/news/BlackHole-Exploit-Kit-2-0-Made-Available-Price-Remains-Same-291881.shtml

Sophos, 2012; "*Exploring the Blackhole Exploit Kit*"; sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf

Sophos, 2012; "*IE remote code execution vulnerability being actively exploited in the wild*"; nakedsecurity.sophos.com/2012/06/19/ie-remote-code-execution-vulnerability-being-actively-exploited-in-the-wild/

Sophos, 2013; "*Security threat report 2013*"; sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

Statens it, 2012; "*Erhvervs- og Vækstministeriet angrebet af hackere*"; statens-it.dk/omstatensit/nyheder/916.html

Sydbank, 2012; "*Angreb på Sydbanks NetBank*"; sydbank.dk/privat/artikler/netbankindbrud
Symantec; "*Globale trusler*"; symanteccloud.com/da/dk/globalthreats/

Symantec; "*Symantec intelligence reports*"; symanteccloud.com/da/dk/globalthreats/overview/r_mli_reports

Teamghostshell, 2012; "*#ProjectWestWind - Today's education!*"; pastebin.com/AQWhu8Ek

TeamShatter, 2012; "*Sybase – Disclosed But Unpatched Vulnerabilities*"; www.teamshatter.com/topics/general/team-shatter-exclusive/sybase-disclosed-but-unpatched-vulnerabilities/

The Huffington Post, 2012; "*Anonymous and the war over the internet*"; huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html

The Huffington Post, 2012; "*Anonymous and the war over the internet (Part II)*"; huffingtonpost.com/2012/01/31/anonymous-war-over-internet_n_1237058.html

The Register, 2012; "*Samsung's smart TVs 'wide open' to exploits*"; theregister.co.uk/2012/12/12/smart_tv_pwned/

Thenextweb, 2012; "*In one year, Android malware up 580%, 23 of the top 500 apps on Google Play deemed 'High Risk'*": thenextweb.com/google/2012/10/25/in-one-year-android-malware-up-580-23-of-the-top-500-on-google-play-deemed-high-risk/

Threatpost, 2012; "*Team Ghost Shell claims to publish records from thousands of universities*"; threatpost.com/en_us/blogs/team-ghost-shell-claims-publishe-records-thousands-univerisities-100212

Tofino Security, 2012; "*Cyber security nightmare in the Netherlands*"; tofinosecurity.com/blog/cyber-security-nightmare-netherlands

Tofino Security, 2012; "*S4 SCADA security symposium takeaway: Time for a revolution*"; tofinosecurity.com/blog/s4-scada-security-symposium-takeaway-time-revolution

Trendmicro, 2012; *"Russian underground 101"*; trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

TV 2, 2012; "*3F's hjemmeside lagt ned af hackere*"; nyhederne.tv2.dk/article.php/id-51969246

TV 2, 2012; "*Anonym hacker: Operationen er kørt af sporet*"; nyhederne.tv2.dk/article.php/id-52040255

TV 2, 2012; *"Bankrøvere får mindre i udbytte end før"*; nyhederne.tv2.dk/article.php/id-54240364

TV 2, 2012; *"Danmark klar til angreb på nettet"*, nyhederne.tv2.dk/article.php/id-61100129

Urlesque, 2010; "*The Jessi Slaughter scandal - An unbalanced 11-year-old girl's ongoing fight with internet trolls*"; urlesque.com/2010/07/19/jessi-slaughter/

Version 2, 2012; "*Anonymous slår til i Danmark: Vi har hacket CPR.dk og Atea*"; version2.dk/48716

Version 2, 2012; *"Cyberangreb på Sverige: Statsbaner og nyhedsbureau DDoS'et"*; version2.dk/48034

Version 2, 2012; "*Danske Bank: Vi har fortsat fuld tillid til NemID2*"; version2.dk/43521

Version 2, 2012; "*Dansk it-firma udsat for 'voldsom trafik' og flere forsøg på indbrud fra Anonymous*"; version2.dk/ 48794

Version 2, 2012; "*Datingchef indrømmer: Brugernavne og kodeord på Sex.dk kan være blevet misbrugt*"; version2.dk/48900

Version 2, 2012; "*Domæne-chok: DanID taber retten til nemid.dk med et brag*"; version2.dk/47523

Version 2, 2012; "*Forlig fordobler bevilling til danske cyberkrigere*"; version2.dk/49207

Version 2, 2012; "*Google på vej til at fjerne EU-barriere for Google Apps til danske myndigheder*"; version2.dk/45835

Version 2, 2012; "*GovCERT slår alarm: Advarer alle ministerier mod hackerangreb*"; version2.dk/45130

Version 2, 2012; "*Hackerangreb lammer ministerium*"; version2.dk/45129

Version 2, 2012; "*Hackerangreb plager ministerium på 4. døgn*"; version2.dk/45159

Version 2, 2012; "*Hackere angriber Sydbanks netbank med virus*"; version2.dk/46985

Version 2, 2012; "*Hackere afslører 30.000 danske brugere og kodeord fra Sex.dk*"; version2.dk/48883

Version 2, 2012; "*Hackere snyder NemID igen: Sydbank stopper massivt angreb*"; version2.dk/46990

Version 2, 2012; "*Massiv logning af danskernes internetbrug - men politiet bruger kun IP-adressen*"; version2.dk/45584

Version 2, 2012; "*Netbanktyve bryder gennem NemID igen: Stjæler 700.000*"; version2.dk/43471

Version 2, 2012; "*Opråb til danske virksomheder: Skjul ikke hackerangreb*"; version2.dk/47137

Version 2, 2012; "*Pas på nye privacy-regler: Datatilsynet får kæmpe bødehammer*"; version2.dk/43148

Version 2, 2011; "*Prosa advarer medlemmer om CPR-login i NemID - brugte det selv*"; version2.dk/32572

Version 2, 2012; "*SOPA er død: Lovforslag trukket*"; version2.dk/ 43055

Washington Post, 2012; "*U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*"; washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Websense, 2012; "*New Java 0-day added to Blackhole Exploit Kit*"; community.websense.com/blogs/securitylabs/archive/2012/08/28/new-java-0-day-added-to-blackhole-exploit-kit.aspx

Wikipedia; "*ACTA*"; da.wikipedia.org/wiki/ACTA

Wikipedia, 2012; "*Flame (malware)*"; en.wikipedia.org/wiki/Flame_%28malware%29

Wikipedia; "*Ransomware (malware)*"; en.wikipedia.org/wiki/Ransomware_(malware)

Wikipedia; "*Rogue security software*"; en.wikipedia.org/wiki/Rogue_security_software

Wikipedia; "*Stop Online Piracy Act*"; da.wikipedia.org/wiki/Stop_Online_Piracy_Act

Wikipedia; "*Stuxnet*"; en.wikipedia.org/wiki/Stuxnet

Wired, 2009; "*The assclown offensive: How to enrage the Church of Scientology*"; wired.com/culture/culturereviews/magazine/17-10/mf_chanology/

Wired, 2012; "*Anonymous promises regularly scheduled friday attacks*"; wired.com/threatlevel/2012/02/anonymous-friday-attacks/

VMware, 2012; "*VMware vCenter Operations, CapacityIQ, and Movie Decoder security updates*"; vmware.com/security/advisories/VMSA-2012-0014.html

Kontakt:

DKCERT, DeIC
DTU, Centrifugevej, Bygn. 356
2800 Kgs. Lyngby