DK•CERT

Trendrapport

It-sikkerhed i første kvartal 2012

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad og Jens Borup Pedersen, DK•CERT

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

Om DK•CERT

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

DK•CERT 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 DK•CERT til at udvikle services, der skaber merværdi for DK•CERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DK•CERT, 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.

DK•CERT 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 DK•CERT om informationssikkerhed i Danmark.

DK•CERT samarbejder med GovCERT (Government Computer Emergency Response Team), der er den danske stats internetvarslingstjeneste. DK•CERT bidrager med information rettet mod borgerne og mindre virksomheder om aktuelle trusler og sikkerhedshændelser.

Indholdsfortegnelse

1.	**Resume**	3
2.	**Første kvartal 2012 i tal**	4
	2.1. Kvartalets sikkerhedshændelser	4
	2.2. Malware og andre trusler	5
	2.3. Sårbarheder	7
3.	**Overskrifter fra første kvartal 2012**	10
	3.1. Den internationale kamp mod piratkopiering	10
	3.2. Angrebsprogrammer udnytter sårbare scada-systemer	11
	3.3. Netbank-kunder bestjålet ved real time phishing	12
	3.4. Klager over persondataretten kan betale sig	13
	3.5. Vi er anonymous	14
	3.6. Danske medier ramt af hackerangreb	16
4.	**Ordliste**	18
5.	**Figuroversigt**	21
6.	**Referencer**	22

1. Resume

Danske websteder bliver i stigende grad misbrugt til at sprede skadelige programmer og falske hjemmesider. DK•CERT modtog rapporter om 668 tilfælde af den type misbrug i første kvartal. Det er en stigning på 83 procent i forhold til foregående kvartal.

Misbruget foregår på den måde, at hackere trænger ind på et legitimt websted. Det kan de typisk gøre ved at udnytte en række velkendte sikkerhedshuller: Passwords til administration af webstedet kan være lette at gætte, eller der kan være sårbarheder i web-softwaren. Når de først har fået adgang, lægger de skadeligt indhold ind, typisk enten malware (skadelige programmer) eller phishing-sider.

Malware vil ofte blive lagt ind i form af programpakker, der afprøver en række angrebsmetoder mod dem, der besøger webstedet. Hvis en besøgende har en pc, der ikke er opdateret med nyeste version af for eksempel Flash Player, kan angriberen udnytte det til at få fuld kontrol over pc'en, uden at brugeren opdager noget. Dermed går webstedets dårlige sikkerhed ud over dets gæster.

Phishing-sider giver sig ud for at være websteder, som brugerne har tillid til. Det kan være en webbutik eller en netbank. Sidstnævnte var også i fokus i første kvartal, da det ved en kombination af malware og phishing lykkedes it-kriminelle at få fat i over 700.000 kroner fra danske netbank-kunder.

DK•CERTs sikkerhedsscanninger af Forskningsnettet fandt frem til flere servere med sårbare programmer. Hver tiende af de IP-adresser, der svarede på scanningen, havde således en eller flere sårbarheder. 80 procent af sårbarhederne var tilknyttet webservere og -applikationer.

På globalt plan blev der offentliggjort lidt færre nye sårbarheder i første kvartal i forhold til det foregående. Som noget nyt er systemer til industrikontrol (SCADA, Supervisory Control And Data Acquisition) begyndt at dukke op på listerne. Det kan hænge sammen med en gruppe sikkerhedsforskeres målrettede indsats for at udvide kendskabet til sårbare SCADA-systemer. De udsendte ligefrem grydeklare angrebsmoduler til det populære Metasploit-værktøj.

Endelig var kvartalet præget af megen omtale af Anonymous-bevægelsen og anholdelsen af seks medlemmer af den tilknyttede hackergruppe LulzSec. I denne kvartalsrapport bringer vi en gennemgang af bevægelsens historie og baggrund.

God fornøjelse med læsningen!

Shehzad Ahmad

Chef for DK•CERT

2. Første kvartal 2012 i tal

"De fleste sikkerhedshuller, kan lukkes ved relativt simple midler."

Som i 2011 stod også det første kvartal af 2012 i hacktivismens tegn. Året startede med omfattende protester mod et amerikansk lovforslag og en international handelsaftale. Begge havde til formål at sikre rettighedshavere mod misbrug.

En rapport fra Verizon viser, at 97 procent af datatabene forsaget af hacktivister i 2011 kunne være undgået uden vanskelige eller dyre modforanstaltninger. Selvom vi i første kvartal kun blev sporadisk ramt herhjemme, er billedet nok det samme. De fleste sikkerhedshuller, kan lukkes ved relativt simple midler.

Herhjemme er det under halvdelen af brugerne af Microsofts seneste operativsystemer, der også benytter softwareproducentens browser. Mens Windows 7 i februar blev benyttet af knap 45 procent af de besøgende på websider tilknyttet Foreningen af Danske Interaktive Medier (FDIM), var der kun små 28 procent der benyttede Internet Explorer 9, som udelukkende kan køres fra Windows Vista og Windows 7. De monopollignende tilstande synes ovre. Det kan have betydning for sikkerheden, da udnyttelse af sårbarheder i browseren ikke længere rammer så bredt.

I dette afsnit beskriver vi første kvartal med udgangspunkt i data fra de systemer og netværk, som DK•CERT har adgang til. Afsnittet beskriver primært hændelser på det danske net til forsknings- og uddannelsesinstitutioner, Forskningsnettet. Der suppleres og perspektiveres med data fra internettets åbne kilder. Afsnittet afspejler derfor til dels udviklingen på hele den danske del af internettet. Billedet vi tegner, vil dog aldrig være fuldkomment.

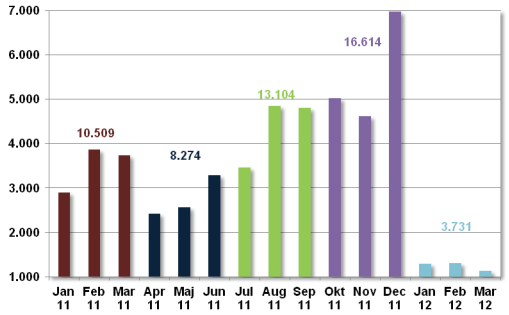
Afsnittet indledes med en overordnet beskrivelse af de hændelser, der gennem kvartalet er blevet rapporteret til DK•CERT. Mange af kvartalets hændelser er relateret til malware, som beskrives i afsnittets anden del. Her giver vi en status på udvikling og spredning af malware, samt de heraf afledte hændelser som spam og phishing. Vi afslutter med at beskrive udviklingen med hensyn til de sårbarheder, de it-kriminelle forsøger at udnytte på vores it-systemer. Det vil sige kvartalets nye sårbarheder og de sårbarheder, som blev forsøgt udnyttet, samt de sårbarheder vi fandt ved scanning af vores kunders systemer og netværk.

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Browserbarometer*".
Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*".
Verizon, 2012; "*2012 data breach investigations report*".

2.1. Kvartalets sikkerhedshændelser

Øjensynligt er der i første kvartal sket et drastisk fald i sikkerhedshændelser, som blev rapporteret til DK•CERT (Figur 1). Det skyldes bortfaldet af en række scannings-hændelser, som tidligere blev rapporteret og behandlet automatisk. I alt blev der således kun rapporteret 327 hændelser, der blev kategoriseret som scanninger i første kvartal 2012 mod 12.518 i kvartalet inden. For øvrige hændelsestyper har det ingen betydning for sammenligneligheden med tidligere.

I alt modtog vi i første kvartal 3.731 rapporter, som førte til registrering af 3.068 unikke sikkerhedshændelser. De havde deres udspring i 1.859 forskellige IP-adresser. Af dem udgjorde uretmæssige download af kopibeskyttede værker fra fil-



Figur 1. Sikkerhedshændelser rapporteret til DK•CERT.

delingstjenester den største del (Figur 2). I alt registrerede vi 977 hændelser, hvor repræsentanter for rettighedshaverne gjorde opmærksom på pirat-download af film, musik og software. Hændelserne havde rod i 285 forskellige IP-adresser på det danske Forskningsnet.

Hændelser, hvor kompromitterede danske websites blev udnyttet til hosting af malware og phishing-sider, er som den eneste kategori steget i forhold til fjerde kvartal 2011. De udgjorde denne gang 668 hændelser, hvilket er det højeste antal, vi hidtil har registreret. Det er en stigning på næsten 83 procent i forhold til fjerde kvartal 2011, og mere end en fordobling i forhold til tidligere kvartaler. Til det billede hører, at sårbare legale websites er en væsentligste kilde til spredning af malware.

På flere af de kompromitterede websites modtog vi henvendelser fra flere forskellige kilder. I enkelte tilfælde blev samme host på ny kompromitteret, efter at hostingudbyderen var informeret. Selvom problemet øjensynligt er stigende, er det dog vores oplevelse, at flere udbydere i dag tager henvendelserne alvorligt. Også det igangværende branche-samarbejde mellem hostingudbyderne kan være med til at sætte yderligere fokus på problemet.

Derudover dækkede kvartalet over 113 hændelser, der blev kategoriseret som hacking og 734 brute force angreb. Her blev det forsøgt at logge på en tjeneste ved systematisk at afprøve kombinationer af brugernavne og password. Ved 385 af disse hændelser blev der forsøgt fra udlandet at logge på danske SSH-tjenester. I de øvrige hændelser som blev kategoriseret som brute force-angreb, var det danske computere, som forsøgte at logge på udenlandske tjenester, primært SSH- og mail-tjenester.

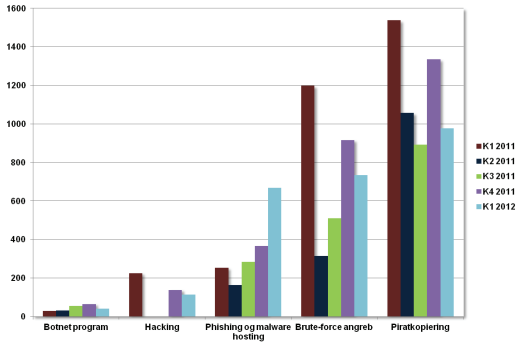
I flere tilfælde blev DK•CERT gjort opmærksom på danske computere, som deltog i botnet-relateret trafik. Alle henvendelser kom fra udlandet, hvor der i enkelte tilfælde var skaffet adgang til en af botnettets centrale Command & Control-servere. I alt registrerede vi 40 danske IP-adresser, som var inficeret med botnetprogrammer. Det er et fald i forhold til fjerde kvartal 2011, hvor vi registrerede 66 hændelser, der blev kategoriseret som botnet-inficeringer.

2.2. Malware og andre trusler

I kølvandet på hacktivismen har de traditionelle hackermetoder og DDoS-angreb i stigende grad ramt mediernes overskrifter. Det betyder ikke, at truslen fra stadig mere kompliceret og udspekuleret malware er blevet mindre. Det er stadig malware, der benyttes til at skaffe sig adgang til for eksempel vores mailkonti eller kreditkortinformationer. Det benyttes af de organiserede it-kriminelle.

For eksempel var det malware, der i februar måned gjorde det muligt at tømme otte danske netbank-konti for i alt 700.000 kr. Trojaneren der er kendt under navne som Enchanim, TROJ_GLUPINS og BankEasy.A, havde forinden inficeret mange flere danske computere.

Ifølge sikkerhedsfirmaet Norman og antivirusproducenten Kaspersky er Danmark blandt de lande i verden med den mindste infectionsrate af malware. Opgørelserne stammer fra scanninger med Normans Malware Cleaner og Kasperskys tilsvarende produkter. I Normans undersøgelse medførte scanninger i Finland, der havde færrest infektioner, malware-identifikation i 24,3 procent af tilfældene.



Figur 2. Væsentligste sikkerhedshændelser rapporteret til DK•CERT.

I første kvartal 2012 identificerede antivirusproducenten F-Secure 334 malware-infektioner på danske computere. I forhold til tidligere er dette tal meget lavt og kan ikke stå alene som et udtryk for den generelle sikkerhedsstatus herhjemme. For eksempel vil forskydninger i markedsandele have betydning for sammenligneligheden af data. Også fordelingen af de identificerede malware-typer har ændret sig dramatisk i forhold til tidligere.

Trojanske heste stod således for kun 5,4 procent af de danske malware-inficeringer, som blev registreret af F-secure, mod op til 40 procent i tidligere kvartaler (Figur 3). Den største del af inficeringerne skyldtes adware efterfulgt af malware som ikke lod sig entydigt identificere. Disse udgjorde henholdsvis 38,3 og 28,1 procent. Kun en marginal andel af malwaren på de danske computere besidder evnen til at sprede sig selv.

Mens antallet af malware-inficerede danske computere øjensynligt har været lavt i første kvartal, er der sket en stigning i danske websider, der er blevet kompromitteret med det formål at inficere besøgende og/eller franarre dem følsomme informationer (Figur 4). Således registrerede vi 668 sikkerhedshændelser, hvor danske websites var kompromitteret af trojanske heste eller phishing-sider. Det er en stigning på 83 procent i forhold til fjerde kvartal 2011. Følger angrebene det globale mønster, skyldes de fleste kompromitteringer SQL-injection.

Globalt set blokerede Symantec i februar 2.305 malware-inficerede websider. Det er en stigning på små ti procent i forhold til januar måned. Før det skal vi mere end et år tilbage for at finde færre blokeringer. På trods af en stigende mængde malware, er der færre websites der blokeres. Kun lidt under en tredjedel af de blokerede domæner var således nye i februar.

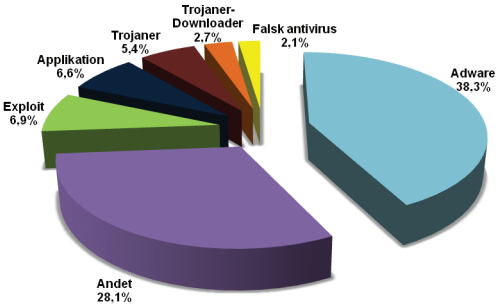
URL-forkortelser, søgemaskineoptimering og spam på mail og sociale netværkstjenester er blandt de foretrukne måder at lokke os til malware-inficerede websider. Den udbredte brug af URL-forkortelser på de sociale netværkssider gør det vanskeligt at gennemskue, hvor et link fører hen. Det får i mange tilfælde brugere til at klikke på links, de ellers ikke ville have klikket på. Det gør sociale netværkssteder til et yndet middel til spredning af malware.

Ved brug af for eksempel PHP-scripts på angribernes web-servere dannes der unikke malware-mutationer for hver enkelt forespørgsel. Server-side genereret malware vanskeliggør opdagelse ved brug af traditionel signaturbaseret detektion. Ifølge blokeringer af Symantecs cloud-baserede heuristiske malware-scannere udgjorde denne type malware i februar 41,1 procent af al malware, som blev spredt via e-mails.

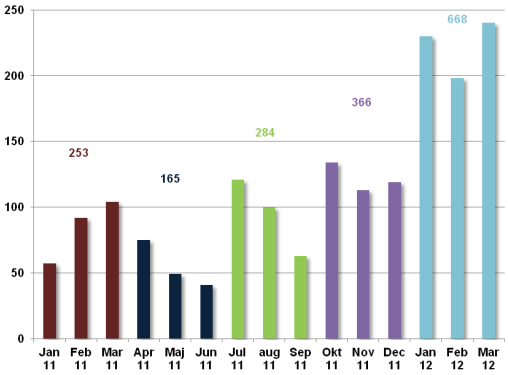
Ifølge Symantecs rapporter har andelen af spam-mails sendt til danskerne holdt sig konstant på små 70 procent siden november måned 2011. Andelen har været svagt faldende gennem det seneste år (Figur 5). Herved følger Danmark den globale udvikling. Når tallene for procentdelen af henholdsvis af spam-, phishing- og virusmails i december og januar er de samme i figuren, skyldes det, at det er et gennemsnit for begge måneder.

Mere end 85 procent af de reklamerede produkter og tjenester i spam faldt i februar inden for kategorierne erotiske sider og sexdating, medicin, ure og smykker samt vægttab. Små 60 procent var afsendt fra et com-domæne.

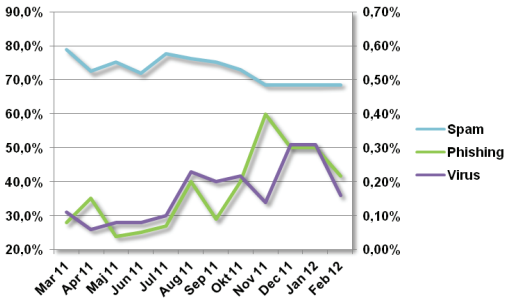
Mens mængden af phishing- og virus-mails herhjemme steg op mod julen, har vi i første kvartal været relativt forskånet i forhold til globale forhold. Andelen af virusmails var i februar på 0,16 procent af alle e-mails herhjemme, mens den glo-



Figur 3. Danske malware-infektioner identificeret af F-Secure i første kvartal i 2012.



Figur 4: Danske websites med trojanske heste og phishing-sider rapporteret til DK•CERT.



Figur 5. Danske e-mail-trusler det seneste år registreret af Symantec.

balt var på 0,36 procent. Tilsvarende gjorde sig gældende med phishingmails, om end det her er mindre udtalt. Her var andelen herhjemme i februar på 0,22 procent, mens den globalt set var på 0,28 procent.

I januar kom de første bølger af spam, der benyttede valentinsdag den 14. februar til at reklamere for alt fra Viagra og falske designertasker til elektroniske valentinskort. Det medførte i perioder store stigninger i den globale spammængde. Siden har nyheden om Whitney Houstons død været udnyttet til spredning af malware, og sommerens olympiske lege i London bliver udnyttet til distribution af malware og falske lotterigevinster.

F-secure, 2011; "*F-Secure security lab– virusworld map*".
Norman, 2012; "*Global malware rates – is your country among the safest or most infected?*".
Securelist, 2012; "*Monthly malware statistics: February 2012*".
Securelist, 2012; "*Spam report: January 2012*".
Symantec; "*Intelligence reports*".

2.3. Sårbarheder

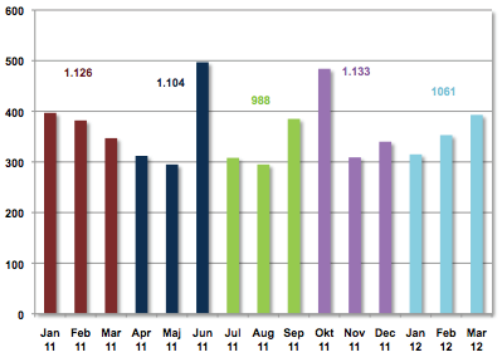
Der blev i første kvartal offentliggjort 1.061 nye CVE-nummererede sårbarheder (Figur 6). Det er et fald på seks procent i forhold til kvartalet inden. Også antallet af CVE-nummererede sårbarheder, som typisk er tilknyttet webapplikationer, faldt til i alt 305 (Figur 7). De udgjorde i første kvartal 29 procent af alle nye sårbarheder. Af dem var næsten halvdelen sårbarheder af typen Cross-site scripting (XSS).

Apple, Google, Oracle og Mozilla topper listen over producenter med flest nye CVE-nummererede sårbarheder i deres produkter i første kvartal 2012 (Figur 8). Statistikken medtager dog ikke versionsnumre. For eksempel har Google siden frigivelsen af Chrome version 16 den 13. december 2011 udgivet 3 nye versioner. Hvor mange sårbarheder der er i de aktuelle versioner er således ikke angivet. Desuden fortæller statistikken ikke, hvor mange sårbarheder, der går igen på den enkelte producents produkter. For eksempel er flere sårbarheder i Mozilla Firefox, Seamonkey og Thunderbird reelt de samme. På samme måde kan iTunes-sårbarheder også figurere som sårbarheder i Apples forskellige operativsystemer.

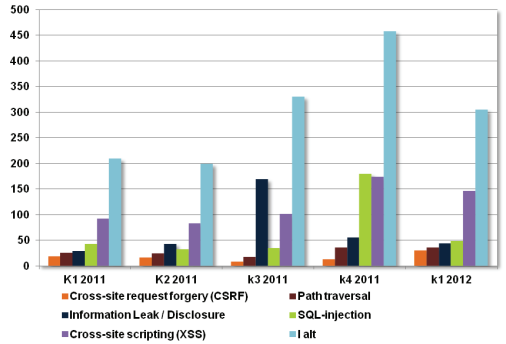
Flest sårbarheder blev der offentliggjort til Apples iTunes efterfulgt af Google Chrome og Oracle MySQL. Mere interessant er det, at flere sårbarheder denne gang knytter sig til industrikontrolsystemer. Sårbarheder til SCADA-interfaces fra både Advantech og Siemens er at finde blandt de produkter, hvortil der blev offentliggjort flest nye CVE-nummererede sårbarheder. Derimod er de traditionelle browser-plugins denne gang fraværende i toppen af listen.

Antallet af sårbarheder som offentliggøres, er ikke et direkte udtryk for den enkelte applikations generelle sikkerhedsstatus. Antallet fortæller i lige så høj grad noget om udbredelsen af applikationen, samt producentens fokus på sikkerhed. Mange producenter vælger for eksempel først at offentliggøre sårbarheder, når de samtidig frigiver en opdatering.

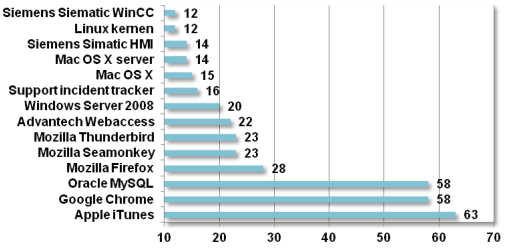
Tilgængeligheden af exploits der udnytter sårbarhederne, eller den potentielle kompromitteringsgrad er heller ikke inkluderet i tallene. Sikkerhedsfirmaet Secunia har påvist en sammenhæng mellem udbredelsen af en applikation og tilgængeligheden af exploits. Overordnet kan det betyde, at der til de mest udbredte applikationer også findes flere sårbarheder og udvikles flere exploits. Des mere udbredt en applikation er, des vigtigere er det således at opdatere den hurtigt. I



Figur 6. Nye CVE-nummererede sårbarheder offentliggjort af NIST.



Figur 7. Nye CVE-nummererede websårbarheder offentliggjort af NIST.



Figur 8. Nye CVE-nummererede produktsårbarheder offentliggjort i første kvartal 2012.

sidste ende er det producentens evne til at fjerne sårbarheder og forbrugernes evne og villighed til at opdatere applikationerne, der afgør produktets aktuelle sikkerhedsstatus.

I første kvartal 2012 udførte vi 24 sårbarhedsscanninger mod institutioner på det danske net til forskning og uddannelse, Forskningsnettet. I alt omfattede scanningerne 30.736 forskellige IP-adresser, hvoraf 2.689 på scanningstidspunktet var tilgængelige fra internettet. På 279 af disse blev der konstateret i alt 2.286 CVE-nummererede sårbarheder, hvoraf 357 blev vurderet at udgøre en høj risiko. Det svarer til, at 10 procent af de svarende IP-adresser i gennemsnit havde otte CVE-nummererede sårbarheder, hvoraf to var kritiske.

Sårbarhederne blev konstateret på i alt 28 forskellige porte og/eller protokoller (Figur 9). Ikke overraskende var det igen webapplikationer, der typisk lytter på TCP-port 80 (HTTP) og 443 (HTTPS), der var de mest sårbare. Næsten 80 procent af sårbarhederne blev konstateret på disse porte. Derudover fandt vi sårbarheder på en række andre porte, som også benyttede HTTP-protokollen. Også på SSH (TCP-port 22), DNS (UDP-port 53) og FTP (TCP-port 21) blev der konstateret sårbarheder.

Ifølge en rapport fra Secunia står programmer, der ikke var udviklet af Microsoft, for 79 procent af sårbarhederne i de programmer, som er installeret på den almindelige brugers pc. For 72 procent af sårbarhedernes vedkommende var der en opdatering tilgængelig samme dag, som sårbarheden blev offentliggjort. For eksempel benyttede 61 procent ifølge en rapport fra virksomheden Zscaler en sårbar version af Adobe Reader i fjerde kvartal 2011.

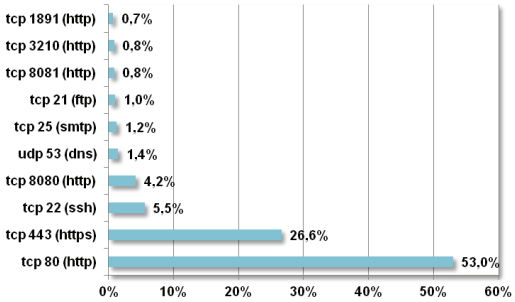
Ifølge Secunias rapport havde halvdelen af brugerne i 2011 mere end 66 forskellige programmer installeret fra mere end 22 forskellige producenter. Det giver et billede af, at den almindelige computerbruger sandsynligvis har mange sårbare programmer installeret og derfor udsætter sig selv for unødig risiko for malware-inficering og lignende. For den almindelige bruger er det simpelthen for vanskeligt at sikre, at alle programmer er opdateret, når man selv skal ud at finde rettelserne. Når mindre end en procent af angrebene i første halvdel af 2011 ifølge Microsoft skyldes udnyttelse af sårbarheder, som der endnu ikke var en rettelse til, angiver det manglende opdateringer som et væsentligt problem for sikkerheden.

Den 10. januar udsendte Adobe en opdatering (APSB12-01), der fjernede seks alvorlige sårbarheder i Adobe Reader og Acrobat. Sårbarhederne gør det muligt at afvikle programkode på det berørte system. Foruden sikkerhedsrettelserne indeholder nye versioner af programmerne 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.

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, der potentielt giver en angriber mulighed for at afvikle programkode.

Den 8. februar udgav Google version 17 af Chrome til Windows, Mac og Linux. Den



Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i første kvartal 2012.

nye version af browseren rettede i alt 20 CVE-nummererede sårbarheder, hvoraf én (CVE-2011-3961) blev vurderet som kritisk. Den gør det muligt at eksekvere kode på det sårbare system. Flere af sårbarhederne udløste kontante belønninger til finderne via Googles Chromium-program.

En opdatering lukkede den 14. februar 14 sikkerhedshuller i Oracle Java SE. Fem af sårbarhederne fik virksomhedens højeste risikovurdering. Alle sårbarhederne kan udnyttes af uautentificerede brugere. 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. Tre sårbarheder udløste en ekstraordinær dusør på 10.000 dollars til tre sikkerhedsforskere. 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.

Adobe, februar 2012; "*Security update available for Adobe Flash Player*".
Adobe, marts 2012; "*Security update available for Adobe Flash Player*".
Adobe, 2012; "*Security updates available for Adobe Reader and Acrobat*".
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 Safari 5.1.4*".
DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*".
Google, 2012; "*Google Chrome releases*".
Microsoft, 2012; "*Microsoft security bulletin summary for March 2012*".
Microsoft, 2011; "*Microsoft security intelligence report volume 11*".
Microsoft, 2012; "*Proof-of-Concept code available for MS12-020*".
Nvd.nist.gov; "*CVE and CCE statistics query page*".
Oracle, 2012; "*Oracle critical patch update advisory - January 2012*".
Oracle, 2012; "*Oracle Java SE critical patch update advisory - February 2012*".
Secunia, 2012; "*Secunia Yearly Report 2011*".
Zscaler, 2012; "*State of the web - quarter 4, 2011 report*".

3. Overskrifter fra første kvartal 2012

"En væsentlig aktør er Anonymous-bevægelsen, som vi forsøger at tegne et billede af. Det er ikke nemt, da der ikke er tale om en entydig og fasttømret gruppe."

Vi beskriver her nogle af de emner, der optog os i første kvartal 2012. Et kvartal, der åbnede med protesterne mod et amerikansk lovforslag, som internetsamfundet så som både protektionistisk og bagstræverisk. Protesterne medførte, at lovforslaget indtil videre er 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 har 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 de store 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 er fortsat i 2012.

En væsentlig aktør er Anonymous-bevægelsen, som vi forsøger at tegne et billede af. Det er 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.

Tilsammen er historierne med til at beskrive udviklingen af de trusler, vi som danskere prøver at beskytte os mod. Men også hvordan det virker at stå imod og i fællesskab ytre sin utilfredshed eller at holde på sin ret til egne persondata.

3.1. 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. Bland 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 være end SOPA. Blandt andet fordi den ikke kan ophæves og den forhandles uden offentlig indsigt. Modsat SOPA har kritikken derfor være baseret mere på spekulationer om betydningen i de lande, der tiltræder aftalen.

På trods af protester både herhjemme og i udlandet underskrev Danmark som et af 22 europæiske lande den 26. januar 2012 ACTA. Aftalen træder i kraft fra juni 2012, forudsat at den vedtages ved en afstemning i EU-parlamentet. Hvad det reelt kommer til at betyde for danskerne, har der siden været delte meninger om.

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.

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*".
Version2, 2012; "*SOPA er død: Lovforslag trukket*".
Wikipedia; "*Stop Online Piracy Act*".
Wikipedia; "*ACTA*".

3.2. 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

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.

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 vedtages i EU-parlamentet – træder i kraft fra juni 2012.

Betydningen af ACTA har der herhjemme været delte meninger om.

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. 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*".

3.3. 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.

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

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. 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*".
Version2, 2012; "*Danske Bank: Vi har fortsat fuld tillid til NemID2*".
Version2, 2012; "*Netbanktyve bryder gennem NemID igen: Stjæler 700.000*".

3.4. 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.

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

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.

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*".

"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."

3.5. 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 løstknyttet 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 balladeмagere 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

#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.

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.*"

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*".

3.6. 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*

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.

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*".

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

4. Ordliste

Adware: Software, der viser reklamer mens applikationen afvikles. Adware betegner både legale applikationer, som er gratis at benytte mod fremvisning af reklamer, samt malware der har til formål at eksponere reklamer på den inficerede computer.

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.

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.

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.

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

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 samtidigt, og kaldes i de tilfælde for distributed denial of service (DDoS).

Exploit: Et eksploit er kode, som forsøger at udnytte sårbarheder i software med det formål at kompromittere systemet.

Forskningsnettet: Et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner Forskningsnettet brugerne med en række tjenester til forskning, samarbejde og kommunikation.

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.

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.

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-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 fx foregå ved en ændring af DNS-registrering enten på DNS-serveren eller ved ændring af hosts-filen.

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.

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.

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.

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.

The 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.

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.

5. Figuroversigt

Figur 1. Sikkerhedshændelser rapporteret til DK•CERT. 4

Figur 2. Væsentligste sikkerhedshændelser rapporteret til DK•CERT. 5

Figur 3. Danske malware-infektioner identificeret af F-Secure i første kvartal i 2012. 6

Figur 4. Danske websites med trojanske heste og phishing-sider rapporteret til DK•CERT. 6

Figur 5. Danske e-mail-trusler det seneste år registreret af Symantec. 6

Figur 6. Nye CVE-nummererede sårbarheder offentliggjort af NIST. 7

Figur 7. Nye CVE-nummererede websårbarheder offentliggjort af NIST. 7

Figur 8. Nye CVE-nummererede produktsårbarheder offentliggjort i første kvartal 2012. 7

Figur 9. CVE-nummererede sårbarheder konstateret ved scanning i første kvartal 2012. 8

6. Referencer

Adobe, februar 2012; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb12-03.html

Adobe, marts 2012; "*Security update available for Adobe Flash Player*"; www.adobe.com/support/security/bulletins/apsb12-05.html

Adobe, 2012; "*Security updates available for Adobe Reader and Acrobat*"; www.adobe.com/support/security/bulletins/apsb12-01.html

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 Safari 5.1.4*"; support.apple.com/kb/HT5190

Berlingske, 2012; "*Dansker får standset Facebook-fejl*"; www.b.dk/tech/dansker-faar-standset-facebook-fejl

Computerworld, 2012; "*Flere danske medier ramt af stort hackerangreb*"; www.computerworld.dk/art/215384/flere-danske-medier-ramt-af-stort-hackerangreb

DK•CERT, 2011; "*DK•CERT Sårbarhedsdatabase*"; http://sdb.cert.dk/login.php

F-Secure, 2011; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Forbes, 2012; "*SOPA, ACTA and the TPP: Lessons for a 21st century trade agenda*"; www.forbes.com/sites/edblack/2012/02/29/sopa-acta-and-the-tpp-lessons-for-a-21st-century-trade-agenda/

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Browserbarometer*"; www.fdim.dk/Statistik/teknik/browserbarometer

Foreningen af Danske Interaktive Medier (FDIM), 2011; "*Operativsystemer*"; www.fdim.dk/Statistik/teknik/operativsystemer

Gizmodo, 2012; "*What is SOPA?*"; gizmodo.com/5877000/what-is-sopa

Google, 2012; "*Google Chrome releases*"; googlechromereleases.blogspot.com/2012/02/stable-channel-update.html

The Huffington Post, 2012; "*Anonymous and the war over the internet*"; www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html

The Huffington Post, 2012; "*Anonymous and the war over the internet (Part II)*"; www.huffingtonpost.com/2012/01/31/anonymous-war-over-internet_n_1237058.html

Microsoft, 2012; "*Microsoft security bulletin summary for March 2012*"; technet.microsoft.com/en-us/security/bulletin/ms12-mar

Microsoft, 2011; "*Microsoft security intelligence report volume 11*"; www.micro-

soft.com/security/sir/

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

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; "*In attack on Vatican web site, a glimpse of hackers' tactics*"; www.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/

Norman, 2012; "*Global malware rates – is your country among the safest or most infected?*"; blogs.norman.com/2012/for-consumption/global-malware-rates-is-your-country-among-the-safest-or-infected

Nvd.nist.gov, 2011; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

Oracle, 2012; "*Oracle critical patch update advisory - January 2012*"; www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Oracle, 2012; "*Oracle Java SE critical patch update advisory - February 2012*"; www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html

Pastebin, 2012; "*Anonymous - #opeurope*"; pastebin.com/aUuuhLyD

Pastebin, 2012; "*Untitled*"; pastebin.com/A33r79pe

Politiken, 2012; "*Hackere stjæler flere hundrede danskeres passwords*"; politiken.dk/erhverv/ECE1556987/hackere-stjaeler-flere-hundrede-danskeres-passwords/

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

Secunia, 2012; "*Secunia yearly report 2011*"; secunia.com/?action=fetch&filename=secunia_yearly_report_2011.pdf

Securityweek, 2012; "*Following LulzSec arrests, AntiSec supporters attack Panda Security*"; www.securityweek.com/following-lulzsec-arrests-antisec-supporters-attack-panda-security

Tofino Security, 2012; "*Cyber security nightmare in the Netherlands*"; www.tofino-security.com/blog/cyber-security-nightmare-netherlands

Tofino Security, 2012; "*S4 SCADA security symposium takeaway: Time for a revolution*"; www.tofinosecurity.com/blog/s4-scada-security-symposium-takeaway-time-revolution

Securelist, 2012; "*Monthly malware statistics: February 2012*"; www.securelist.com/en/analysis/204792223/Monthly_Malware_Statistics_February_2012

Securelist, 2012; "*Spam report: January 2012*"; ww.securelist.com/en/analysis/204792220/Spam_report_January_2012

Symantec; "*Intelligence reports*"; www.symanteccloud.com/da/dk/globalthreats/overview/r_mli_reports

Urlesque, 2010; "*The Jessi Slaughter scandal - An unbalanced 11-year-old girl's ongoing fight with internet trolls*"; www.urlesque.com/2010/07/19/jessi-slaughter/

Verizon, 2012; "*2012 data breach investigations report*"; www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Version2, 2012; "*Danske Bank: Vi har fortsat fuld tillid til NemID2*"; www.version2.dk/artikel/danske-bank-vi-har-fortsat-fuld-tillid-til-nemid-43521

Version2, 2012; "*Netbanktyve bryder gennem NemID igen: Stjæler 700.000*"; www.version2.dk/artikel/breaking-netbanktyve-bryder-gennem-nemid-igen-stjaeler-700000-43471

Version2, 2012; "*SOPA er død: Lovforslag trukket*"; www.version2.dk/artikel/sopa-er-doed-lovforslag-trukket-43055

Wikipedia; "*ACTA*"; da.wikipedia.org/wiki/ACTA

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*"; www.wired.com/culture/culturereviews/magazine/17-10/mf_chanology/

Wired, 2012; "*Anonymous promises regularly scheduled friday attacks*"; www.wired.com/threatlevel/2012/02/anonymous-friday-attacks/

Zscaler, 2012; "*State of the web - quarter 4, 2011 report*"; www.zscaler.com/state-of-web-q4-2011.html

Kontakt:

DK•CERT, UNI•C
Centrifugevej, Bygn. 356
Kgs. Lyngby 2800

Tel. +45 3587 8887
URL: https://www.cert.dk
Email: cert@cert.dk