DK•CERT

Trendrapport 2010

It-kriminalitet og sikkerhed i året der gik

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

Tryk: Rosendahls - Schultz Grafisk a/s

Om DK•CERT

Det er DK•CERTs mission at skabe øget fokus på it-sikkerhed 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 it-sikkerhed. 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 Undervisningsministeriet.

DK•CERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om it-sikkerhed med grundidé i CERT/CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DK•CERT om it-sikkerhed 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.

Forord

Under temaet "styrk forskellene og dyrk samarbejdet" byder jeg velkommen til DK•CERTs Trendrapport 2010. Formålet med rapporten er at give et overblik over it-sikkerheden i Danmark i 2010. Det overblik suppleres med kig på udvalgte emner fra resten af verden. Internettet er verdensomspændende, og det giver sjældent mening at se isoleret på et enkelt land, når man skal identificere tendenser.

Styrk forskellene. Alle vi, der arbejder med it-sikkerhed, er forskellige. Nogle er ansat i virksomheders it-funktion, andre sidder i det offentlige eller hos internetudbydere. Nogle har it-sikkerhed som deres eneste arbejdsopgave, mens det for andre er en opgave blandt mange. Og så er der en stor gruppe af frivillige, der uden aflønning bruger timer og dage på at sikkerhedsteste applikationer og systemer.

Alle disse forskellige spillere er med til at højne sikkerheden. Vi deltager i en fælles kamp mod de it-kriminelle, der udnytter tekniske sårbarheder og menneskelig ubetænksomhed til personlig vinding. Uanset vores indbyrdes forskelle kan vi ikke undvære nogen af spillerne i kampen for bedre sikkerhed. Så lad os holde fast ved de forskelle, der er vores individuelle styrker.

Dyrk samarbejdet. Alle vore forskellige styrker kan kun udnyttes, hvis vi samarbejder. Derfor har det også været en glæde for mig, at DK•CERT i 2010 kunne indgå i et samarbejde med statens nyoprettede GovCERT. DK•CERT står for opgaven med at informere borgere og mindre virksomheder, når der dukker nye trusler op.

Også internationalt samarbejder vi. DK•CERT har i mange år været medlem af FIRST (Forum of Incident Response and Security Teams), hvor vi løbende udveksler viden om sikkerhedshændelser og arbejdsmetoder. I 2010 tog EU initiativ til at øge samarbejdet mellem CERT'er i EU-landene. Det glæder vi os til at deltage i.

I samarbejdets ånd har vi inviteret nogle af vores partnere til at bidrage med indlæg i Trendrapport 2010. Jeg vil gerne sige tak til teknisk sikkerhedschef Lars Højberg, TDC, it-sikkerhedsansvarlig Steen Pedersen, DTU, områdeleder Thomas Kristmar, GovCERT og chefkonsulent Henning Mortensen, DI ITEK, for deres indlæg.

Jeg ønsker dig god fornøjelse med læsningen. Hvis du har spørgsmål eller kommentarer, er du velkommen til at kontakte mig.

Med venlig hilsen

Shehzad Ahmad, DK•CERT

Indholdsfortegnelse

1. Resume

Den samlede mængde sikkerhedshændelser der blev anmeldt til DK•CERT faldt en smule i 2010: I alt blev der anmeldt 36.199 hændelser mod 37.535 i 2009. Det skyldes blandt andet et fald i anmeldelser af portscanninger. Til gengæld var der flere sager, som krævede flere ressourcer i sagsbehandlingen. Det gælder fx sager om distribution af piratkopieret materiale.

Samlet set var 2010 et hårdt år for it-sikkerheden. Aldrig er der kommet så mange varianter af skadelige programmer på et enkelt år. Ifølge antivirusfirmaet Pandalabs blev 34% af al *malware*, der har eksisteret, skrevet i 2010. En af de hidtil mest avancerede trusler så dagens lys i 2010: *Stuxnet-ormen*, der muligvis havde til formål at sabotere det iranske atomprogram.

Til gengæld faldt mængden af registrerede *sårbarheder* i programmer fra 5.734 i 2009 til kun 4.640 i 2010. Men der var flere eksempler på, at *sårbarheder* blev udnyttet hurtigt, efter at de var blevet kendt. I flere tilfælde måtte Microsoft bryde med sit normale skema og udsende sikkerhedsrettelser, så snart de var klar, for at lukke alvorlige sikkerhedshuller. Angribere fokuserede især på at udnytte *sårbarheder* i browsere og udbredte hjælpeprogrammer såsom Adobe Reader og Flash Player.

DK•CERT foretog proaktive *scanninger* af næsten 60.000 IP-adresser. Knap 19% af disse var tilgængelige fra internettet og hver ottende af dem havde *sårbarheder*. I gennemsnit var der 17 *sårbarheder* på hver sårbare maskine, og over halvdelen af *sårbarhederne* har været kendt i over et år. tallene viser, at mange forsømmer at holde deres systemer opdateret.

Mængden af websteder med *trojanske heste* eller *phishing*-svindel som blev anmeldt til DK•CERT, i 2010 til 482 mod 565 i 2009. Det svarer ikke til den globale tendens, hvor blandt andre sikkerhedsfirmaet Dasient har set en fordobling i mængden af inficerede websteder, der spreder skadelige programmer.

Danmark er et *spam*land. I 2010 var 93,2% af alle e-mails sendt til danskere *spam*, hvorved Danmark blev nummer to på listen over de mest *spammede* lande. Globalt set udgjorde *spam* mellem 84 og 89% af alle mails. Mellem 80 og 90% af al *spam* udsendes via *botnet*.

Netop *botnet* er et område, som vakte opmærksomhed i 2010. Flere *botnet* blev lukket og nogle bagmænd blev arresteret. Alligevel udgør fænomenet stadig et så stort problem, at EU-kommissionen nævner det separat i et udspil til, hvordan man kan forbedre it-sikkerheden i EU. Organisationen planlægger at etablere et fælles europæisk center, der skal koordinere indsatsen mod it-kriminalitet. Det danske ISP-Sikkerhedsforum, hvor internetudbydere samarbejder om sikkerhed, har taget flere tiltag mod *botnet* og arbejder på at udvikle nye metoder.

Rapporten slutter med DK•CERTs anbefalinger af, hvad borgere, virksomheder og myndigheder kan gøre for at øge it-sikkerheden. Et nøgleord her er samarbejde.

2. Indledning

"Cybercrime is emerging as a very concrete threat. Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats we will ever face."[1]

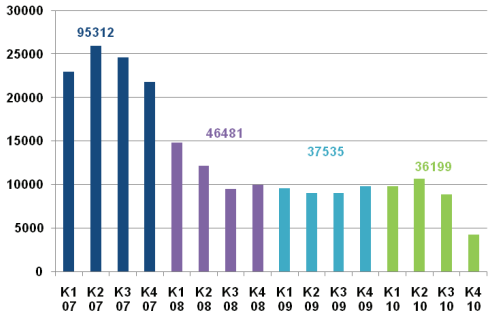
Vi indleder årets trendrapport med et citat af generalsekretær i Interpol, Ronald K. Noble. Ordene faldt som en del af åbningstalen ved Interpols første konference om it-sikkerhed, der i september 2010 fandt sted i Hongkong. Citatet skal tages som udtryk for en stadig mere nærværende trussel, hvor to ud tre adspurgte voksne ifølge Norton har været udsat for it-kriminalitet[2], men også for en trussel som stiger i både professionalisme og kompleksitet. Heldigvis har vi muligheden for i samarbejde at afværge truslen fra it-kriminalitet. I samarbejdets ånd har vi derfor igen i år inviteret en række eksterne parter til at give deres perspektiv på it-sikkerheden i Danmark.

Vi starter dog et helt andet sted med at beskrive de målelige resultater af it-kriminaliteten. Som tidligere år tager vi udgangspunkt i tal og statistikker fra 2010. Afsnittets konklusioner er hovedsageligt taget på baggrund af data udtrukket fra vores egne systemer. De dækker hændelser på de netværk, som DK•CERT overvåger. Ved at lægge et udviklingsperspektiv på beskrivelsen af nøgletal og enkeltstående begivenheder mener vi dog, at det er dækkende for hele den danske del af internettet.

På trods af, at de offentlige myndigheder fra 2008 til 2009 styrkede it-sikkerheden med hensyn til standardisering, beredskabsplaner og uddannelse, oplevede man samtidig en vækst i angreb, der forårsagede økonomiske tab (Figur 1). Mest interessant i den sammenhæng var en stigning i mængden af organisationer, der som resultat af målrettet økonomisk it-misbrug oplevede økonomiske tab. Noget kan dog tyde på at bøtten er vendt. Mens de økonomiske tab som følge af indbrud i de danske netbanker gennem de seneste år har været stigende, knækkede kurven i 2010. Således var der til og med tredje kvartal kun registreret seks vellykkede netbank-indbrud med et samlet tab på 433.043 kr. Dette er væsentligt mindre end de i alt 63 indbrud, som i 2009 gav de danske banker et tab på i alt 6.790.191 kr.[4].

Sammenhængen mellem it-kriminalitetens årsager, metoder og virkninger forsvinder i komplekse strukturer og mønstre. Vi forsøger alligevel i rapportens næste afsnit at sætte en finger på nogle emner, som vi mener prægede 2010. Vi beskriver faktorer, der havde betydning for udviklingen og lader de enkelte underafsnit pege fremad. Således giver afsnittet en pejling på hvad vi skal forholde os til i de kommende år.

Fx er *cloud computing* af konsulentvirksomheden Gartner blevet identificeret som den væsentligste strategiske it-teknologi for 2011[5]. Vi er tilbøjelige til at give dem ret. Mens *cloud computing* de tidligere år er blevet diskuteret som en fremtidig mulighed, placerer flere organisationer i dag tjenester i skyen. Det giver nogle udfordringer, som vi har valgt at behandle separat. Nummer 2 på Gartners liste er



Figur 1. Offentlige myndigheder, der har registreret sikkerhedshændelser[3].

1 Interpol, 2010; *"1st INTERPOL information security conference"*.

2 Norton.com, 2010; *"Norton cybercrime report: The human impact"*.

3 Danmarks Statistik, 2010; *"Den offentlige sektors brug af it 2009"*.

4 Finansrådet; *"Netbankindbrud - statistik"*.

5 Gartner, 2010; *"Gartner identifies the top 10 strategic technologies for 2011"*.

mobil-applikationer og tavle-pc'er. Vi anser også disse teknologier for væsentlige og i vækst, men har i modsætning til tidligere valgt ikke at beskrive dem særskilt. Som Gartner betragter vi nemlig mobile enheder som små computere.

Derimod beskrives, hvordan *malware* har udviklet sig til at være højt specialiseret kode, der i distribution og (mis)brug målrettes offeret og de data man ønsker at indsamle. I relation til at kun 19% nye *malware*-angreb ifølge virksomheden Cyveillance stoppes af antivirusprogrammerne, er dette et problem[6]. Problemet forstærkes yderligere ved, at meget *malware* spredes via websites, brugerne kender og har tillid til. Derfor tager vi fat ved nældens rod og beskriver problemet sårbare legale webapplikationer.

Truslen er midlertidig ikke kun skabt af "onde kriminelle hackere". Vi har alle haft et medansvar for udviklingen. Derfor kan du læse om, hvordan vi i jagten på synlighed og personlige relationer har sænket paraderne og givet afkald på vores privatliv og sunde skepsis. En ændring i adfærd, som har givet de it-kriminelle nye kort på hånden og været medvirkende til at ændre både deres mål og midler.

Målet har dog ikke kun været penge. I løbet af 2010 var der flere eksempler på, at it blev brugt i en "større" sags tjeneste. Fx så vi angreb, der havde til formål at knægte demokratiet ved at blokere adgangen til fri information. Selv om vi som tidligere år ikke har haft nævneværdige angreb på frie demokratiers infrastruktur, forudser mange, at cyberwarfare og cyberterrorisme bliver begreber, vi i fremtiden bliver nødt til at forholde os til.

Sikkerhedsbranchen har selvfølgelig ikke siddet udviklingen overhørig. Vi samler op på de begivenheder fra 2010, som havde betydning for danskernes it-sikkerhed. En væsentlig del af denne afhænger af, at vi som myndigheder, ISP'er, sikkerhedsbranche, organisationer og borgere er i stand til at samarbejde og udveksle erfaringer. Netop på dette område har 2010 budt på interessante perspektiver.

Rapportens følgende afsnit samler op og forsøge at åbne dit perspektiv på de tendenser, vi mener, vi som borgere, organisationer og samfund i de kommende år bør være opmærksomme på. Kun ved at være forberedte kan vi implementere de tekniske og organisatoriske løsninger, der er nødvendige for at sikre vores it-aktiver i forhold til den aktuelle konfiguration af data, teknologi, processer og mennesker. It-sikkerhed er nemlig ikke kun et spørgsmål om teknologi, men i lige så høj grad om mennesker og hvordan vi agerer i forhold til teknologien. Denne proces handler om at tilegne sig tilstrækkelig og rigtig viden og omsætte den til løsninger, men også om samarbejde og videndeling.

I dette lys håber vi, at du vil tage sidste afsnits anbefalinger til henholdsvis borgeren, organisationernes it-ansvarlige og beslutningstagerne til dig. Vi håber, at du vil bruge dem som baggrund for refleksion og diskussion over, hvilke løsninger der nu og i fremtiden er de rigtige, således at vi i fællesskab kan sikre danskernes it-aktiver. Problemets omfang taget i betragtning mener vi nemlig ikke, at der er tilstrækkelig fokus på at beskytte danske borgere og organisationer mod it-kriminalitet.

God læselyst.

6 Net-security.org, 2010; *"AV vendors detect on average 19% of malware attacks"*.

3. 2010 - året i tal

I dette afsnit beskriver vi 2010 på baggrund af de tal og statistikker, som er tilgængelige for DK•CERT. For at supplere, generalisere og perspektivere vores egne data har vi benyttet data leveret af tredjepart, samt internettets åbne kilder. Afsnittet beskriver således primært it-sikkerhed på baggrund af de netværk som vi overvåger. Det vil sige hovedsageligt UNI•Cs egne netværk og Forskningsnettet. Vi mener på trods af dette, at afsnittet kan bruges som en indikator for udviklingen på hele den danske del af internettet.

Antallet af sikkerhedshændelserder blev anmeldt til DK•CERT, steg en smule i årets første to kvartaler for herefter at falde, således at året endte på niveau med 2009 (Figur 2). 2010 endte med i alt 36.199 anmeldelser. Bortset fra 4. kvartal 2010 har der været et næsten konstant antal anmeldelser gennem de seneste 10 kvartaler.

Kigger vi nærmere på tallene, har der dog været forskydninger. Mens antallet af sager klassificeret som hacking eller web-sites inficeret med *trojanske heste* eller *phishing*-sider er faldet svagt, er der sket en markant stigning i sager om distribution af kopibeskyttet materiale (Figur 3). Også antallet af sager som det har været vanskeligt at klassificere, er steget markant. Således var der i 2010 2184 sager, som blev klassificeret som "andet", mod 159 i 2009. Alt i alt har denne udvikling betydet, at der i 2010 blev benyttet flere ressourcer til registrering og behandling af sikkerhedshændelser. Igen i 2010 faldt antallet af anmeldte *scanninger*, som for en stor dels vedkommende anmeldes og behandles automatisk. Der blev således i 2010 anmeldt 20.270 *scanninger* mod 33.761 i 2009.

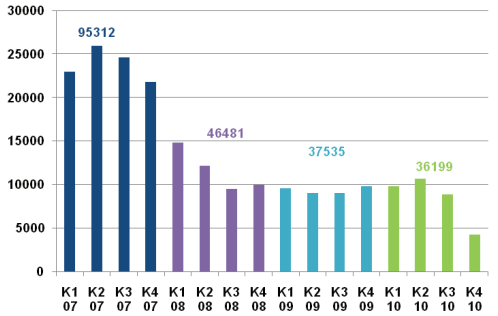
Også offentliggjorte nye *CVE-nummererede sårbarheder* faldt i 2010 i antal. Hvor der i 2009 blev offentliggjort 5.734 nye *sårbarheder*, var tallet i 2010 kun 4.640. Hurtigere udnyttelse af nye *sårbarheder* udgør et stigende problem i forhold til både organisationernes og borgernes sikkerhed.

Vi har igen i år fokus på tre emner, som afspejler DK•CERTs egne data og dermed de netværk, systemer og ydelser, vi i øjeblikket overvåger, benytter og leverer. Vi mener dog at, udviklingen med hensyn til *sårbarheder*, *scanninger* og *malware* kan stå for sig selv og er med til at pege fremad mod, hvad vi i fremtiden skal være opmærksomme på. Afsnittet indledes med data om årets offentliggjorte *sårbarheder*, aktualiseret med statistik over de *sårbarheder* vi konstaterer ved *scanninger* på *Forskningsnettet*. Igen i år har vi lagt fokus på de *sårbarheder*, som udnyttes på legale webapplikationer. Herefter beskriver vi udviklingen med hensyn til de *scanninger*, som i løbet af 2010 blev anmeldt til DK•CERT og sammenligner med tidligere. Afslutningsvis beskriver vi den *malware*, som i 2010 så dagens lys. Fælles for den er, at den som forventet er blevet mere målrettet og avanceret i både sine mål og midler.

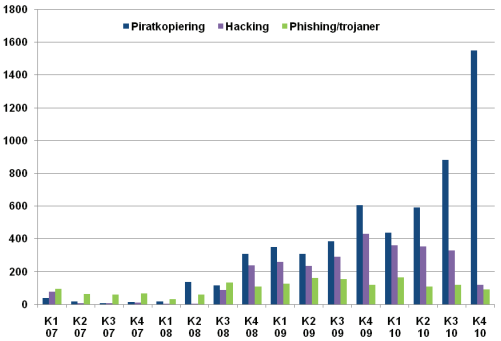
3.1. De sårbare it-systemer

Sårbarheder i it-systemer udgør den væsentligste årsag til systemkompromittering og spredning af *malware*. I 2010 blev der af den amerikanske tjeneste NVD[7] (National Vulnerability Database) offentliggjort i alt 4.640 nye *CVE-nummererede* (Common Vulnerability and Exposures) *sårbarheder*, hvilket er et fald i forhold til årene inden (Figur 4). NVD samler og katalogiserer *CVE-nummererede sårbarheder*

7 nvd.nist.gov; *"National Vulnerability Database version 2.2"*.



Figur 2. Sikkerhedshændelser anmeldt til DK•CERT.



Figur 3. Væsentligste hændelsestyper anmeldt til DK•CERT.

i standard it-systemer og benyttes af DK•CERT.

At der offentliggøres stadig færre *CVE-nummererede sårbarheder*, bør ikke tages som udtryk for, at der er færre *sårbarheder* i standard it-systemer, men snarere at der bruges færre ressourcer på at afklare og beskrive *sårbarheder*. Med større diversitet i platforme, flere nye it-produkter og versioner må det formodes, at antallet af *sårbarheder*, der endnu ikke er opdaget og offentliggjort, er flere end nogensinde før. Vi tror at de, der finder *sårbarheder* med udnyttelse for øje, har koncentreret indsatsen på tredjeparts-browserkomponenter som fx Flashafspilleren Flash Player og PDF-læseren Adobe Reader og lignende, samt på ikke standard it-systemer som fx sociale netværkssider og de applikationer, der benyttes i forbindelse med dem. Denne udvikling forklarer til dels også, at andelen af offentliggjorte *CVE-nummererede websårbarheder* er faldet (Figur 5), på trods af at legale webapplikationer er den væsentligste spredningskilde for *malware*.

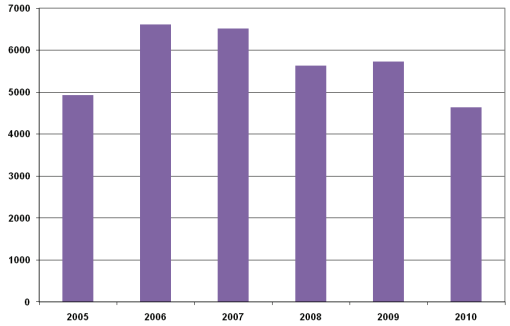
Mængden af *CVE-nummererede sårbarheder* af typerne *SQL-injection*, *cross-site scripting*, *cross-site request forgery* og information leak, der hovedsageligt relaterer sig til webapplikationer, udgjorde således i 2010 kun 29% mod 36% i 2009. Den største andel af disse var i 2010 *cross-site scripting sårbarheder* (Figur 5), der også udgør 51% af de *websårbarheder*, som i 2010 blev afdækket af sikkerhedsvirksomheden Veracode[9].

Det er dog ikke alle *websårbarheder*, der udgives med et *CVE-nummer*. De fleste *websårbarheder* findes i organisationsspecifikke webapplikationer. Tredjeparts-applikationer og komponenter på disse viste sig ifølge virksomheden Veracode mere sårbare end de applikationer, der blev udviklet internt i organisationerne[9]. De væsentligste årsager til *sårbarheder* i webapplikationer skal ifølge den hollandske *GovCERT* findes i mangelfuld inputvalidering, mangelfuld viden og erfaring med sikkerhed hos programmører og fraværet af udviklingsstandarder[10].

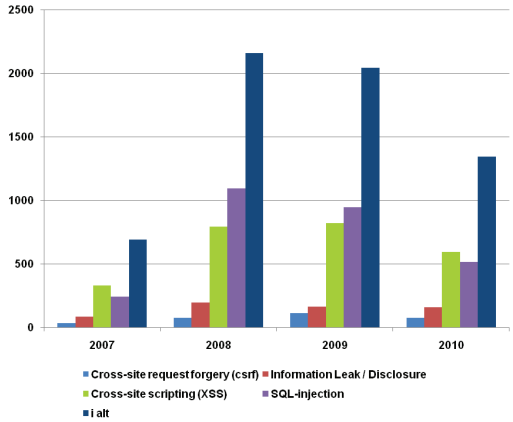
Selvom der stadig findes og offentliggøres mange *sårbarheder* i operativsystemerne, er den generelle tendens som sidste år, at *sårbarheder* i applikationer, der kører oven på operativsystemet, er i overtal[11]. De store operativsystemer fra Microsoft og Apple ligger dog sammen med Linux kernen stadig i toppen af listen over de programmer, der offentliggøres flest nye *sårbarheder* i. Det gælder også internetbrowsere fra både Apple og Mozilla (Figur 6). Microsofts browser Internet Explorer er placeret lige uden for listen på en 19. plads.

På henholdsvis 14. og 18. pladsen befinder PDF-læseren Adobe Reader og Adobes Flash Player sig. Begge er produkter, hvori *sårbarheder* har været blandt de hyppigst udnyttede i 2010. Endnu har ingen af de store operativsystemer til mobile platforme fundet vej til toppen af listen. Først på en 33. plads optræder Apples operativsystem til iPhone og iPad, IOS.

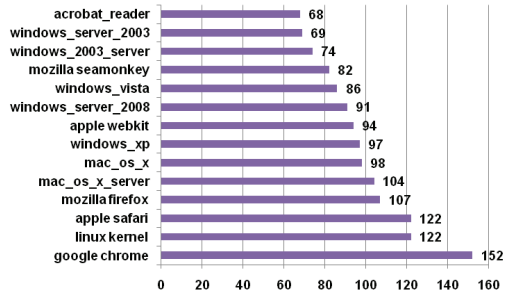
At der i stigende grad findes og udnyttes *sårbarheder* i forbrugerprogrammer som fx Adobe Reader, Adobes FlashPlayer eller QuickTime, er en forsættelse af en tendens, vi har set de seneste år. Sammen med browserne udgør *sårbarheder* i disse programmer, der ofte også fungerer som plugin til browseren, den største



Figur 4. Offentliggjorte CVE-nummererede sårbarheder[8].



Figur 5. Offentliggjorte CVE-nummererede websårbarheder.



Figur 6. CVE-nummererede sårbarheder offentliggjort i 2010 fordelt på produkter.

8 nvd.nist.gov; *"CVE and CCE statistics query page"*.

9 Veracode.com, 2010; *"State of software security report"*.

10 GovCERT.nl, 2010; *"2010 national cyber crime and digital safty trend report"*.

11 Sans.org, 2009; *"The top cyber security risks"*.

trussel. Tendensen forstærkes, når vi som tidligere år har set, at *sårbarheder* udnyttes stadig hurtigere, og ofte inden der er kommet en rettelse. Overordnet set er det for organisationerne blevet vanskeligere at vurdere den risiko den enkelte *sårbarheder*ne udgør, da de består af flere interagerende både tekniske og ofte også menneskelige lag.

I 2010 foretog DK•CERT *scanning* af næsten 60.000 forskellige IP-adresser, hovedsageligt placeret på *Forskningsnettet*. Resultateterne viste, at næsten 19% af de scannede adresser var tilgængelige fra internettet. Af disse blev der på hver ottende maskine konstateret i gennemsnit 17 *CVE-nummererede sårbarheder*. Af disse *sårbarheder* var flere end 50% blevet offentliggjort mere end et år tidligere.

I alt blev der konstateret *CVE-nummererede sårbarheder* på 124 forskellige porte og/eller protokoller. Ikke overraskende blev der også i 2010 konstateret flest *sårbarheder* på webapplikationer, der lytter på TCP-port 80 og 443 (Figur 7). Til de *CVE-nummererede sårbarheder* skal på disse porte lægges *sårbarheder*, der er specifikke for den enkelte webapplikation. Disse *sårbarheder*, der fx er forårsaget af mangelfuld inputvalidering, er der ikke testet for.

Overordnet set tegner DK•CERTs *scanninger* et billede af, at organisationerne ikke har en fast procedure for håndtering og rettelse af *sårbarheder*. Når *sårbarheder* først rettes sent udsættes organisationen og dennes brugere for unødvendige risici. Flere organisationer vil derfor have problemer med at overholde egen it-sikkerhedspolitik samt gældende standarder som fx *DS 484*, *ISO 27001*.

14. januar publicerede Microsoft en *sårbarhed* i Internet Explorer (*CVE*-2010-0249). *Sårbarheden* var tidligere blevet udnyttet i et større angreb, hvor blandt andre Google var målet. Angrebet blev siden kendt under navnet Aurora. *Sårbarheden* i browserens objekthåndtering gjorde det muligt at afvikle kode på den sårbare maskine.

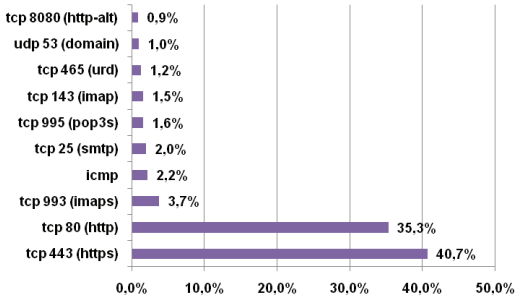
Årets måske væsentligste *sårbarhed* blev offentliggjort af Microsoft den 16. juni. *Sårbarheden* (*CVE*-2010-2568), der blev klassificeret som kritisk, muliggjorde eksekvering af kode ved at udnytte en fejl i Windows' måde at håndtere genveje på. *Sårbarheden* var tilgængelig i Windows XP og senere versioner af Windows. Inden Microsoft den 2. august frigav en rettelse til *sårbarheden*, var den flere gange blevet udnyttet af *malware*. Blandt andet blev *sårbarheden* udnyttet til spredning af *Stuxnet* via USB-nøgler.

Derudover blev der i løbet af 2010 offentliggjort en række væsentlige *sårbarheder* i både PDF-læseren Adobe Reader og Adobes Flash-afspiller, som muliggjorde kompromittering. Flere af dem blev udnyttet til spredning af *malware*, enkelte inden *sårbarheden* blev offentliggjort. Særligt udnyttelse af *sårbarheder* i PDF blev af IBM vurderet som værende en væsentlig trussel i første halvår af 2010[12]. Fælles for disse er, at udnyttelsen havde til formål at placere *malware* på den almindelige internetbrugers pc.

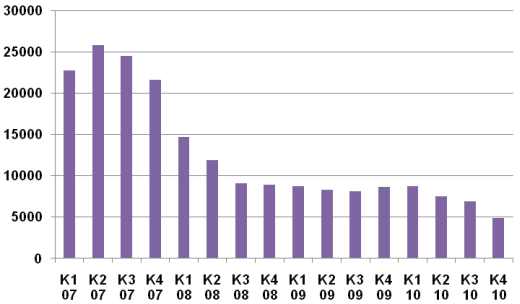
3.2. Scanninger

Igen i 2010 faldt antallet af *scanninger*, som blev anmeldt til DK•CERT (Figur 8). En væsentlig årsag til dette er, at kompromitteringen af it-systemer i 2010 foregår med midler, der er mere effektive og vanskeligere at opdage og afværge. Således

12 IBM, 2010; *"X-Force 2010 mid-year trend and risk report"*.



Figur 7. Fordeling af CVE-nummererede sårbarheder konstateret ved scanning.



Figur 8. Scanninger anmeldt til DK•CERT.

så vi i 2010 ingen væsentligere *orme*-udbrud, som tidligere har haft ansvaret for store dele af scanningsaktiviteten. Samme tendens gør sig ifølge Shadowserver.org gældende internationalt[13].

De 28.750 *scanninger*, der i 2010 blev anmeldt DK•CERT, fordeler sig på 453 forskellige porte og protokoller, mod kun 152 i 2009. Dette kunne være et billede på større diversitet i antallet af applikationer der forsøges udnyttet. Årsagen skal dog nok nærmere findes i en stigning i mængden af *malware*, særligt *botnet*-programmer og *trojanske heste*, som lytter på mere eller mindre vilkårlige porte, hvortil der ikke som standard er knyttet en applikation.

Antallet af anmeldelser om ICMP-ping af store netsegmenter enten alene eller i kombination med andre porte er faldet fra 30,8% i 2009 til 10,1% i 2010. Det forstærker billedet af større målrettethed: Det er ikke længere interessant at vide, om der er en maskine, men i højere grad om der er en maskine, som er inficeret med bestemt *malware* eller andre værktøjer, som gør det muligt at skaffe sig adgang til maskinen. Således er andelen af *scanninger* mod TCP-port 1024 og 1027 steget til i alt 20,1% af alle de anmeldte *scanninger* (Figur 9). Hvor port 1024 benyttes af programmer til fjernadministration, har bl.a. den *trojanske hest* ICQ-killer benyttet sig af port 1027. Derudover kommer *scanninger* mod SSH-tjenesten på TCP-port 22, der ligeledes kan benyttes til at skaffe sig adgang til den scannede maskine. De anmeldte *scanninger* på denne port dækker delvist over *brute-force* angreb, hvor der forsøges at logge på tjenesten ved at "gætte" kombinationer af brugernavn og kodeord.

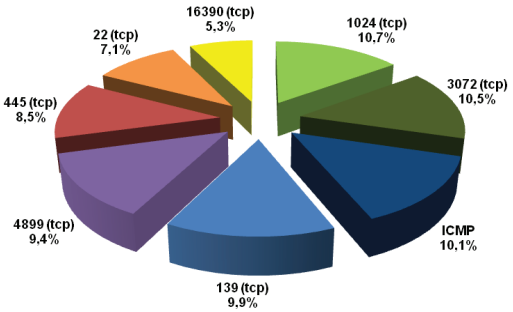
Scanninger mod TCP-port 3072, som var den næstmest scannede port i 2010, kan tilsvarende dække over målrettede angreb, der har til formål at skaffe sig adgang til ressourcer på en *malware*-inficeret maskine. Porten der blandt andet benyttes til monitorering af storage-løsninger, er tilsvarende blevet brugt af både en IRC-bot og en *trojansk hest*. Mest interessant er rapporter om at porten benyttes af en *trojansk hest*, der via IRC initiere *DDoS*-angreb[14].

Også i 2010 blev der anmeldt mange *scanninger* mod services, der benyttes af Windows-systemer på hhv. TCP-port 139 og 445. Derimod har vi ikke tidligere set så mange *scanninger* mod TCP-port 16390, som benyttes til Voice over IP (VoIP), blandt andet af IP telefoner fra Cisco.

Scanningerne blev foretaget fra næsten 16.000 forskellige IP-adresser. De mest aktive IP-adresser var placeret i Kina, Danmark og USA, med en hollandsk adresse som den mest aktive.

I slutningen af 2009 oplevede vi de første anmeldelser om *scanninger* fra tjenester i Amazons cloud, EC2. Siden er antallet vokset til i alt ca. 50 anmeldelser i 2010. Selvom *scanninger* udført fra tjenester placeret i skyen stadig er et overkommeligt problem, venter vi, at det vil eskalere, efterhånden som flere både legale og ondsindede tjenester placeres i skyen.

Scanninger foretages ikke længere for blindt at afsøge store netsegmenter for mulige sårbare hosts. Målet med *scanningerne* har flyttet sig og dermed også de midler der bruges. Således er det i dag unødvendigt for angriberne at benytte sig af større scanningsapplikationer, hvis man kun ønsker information om maskiner, der har en specifik *sårbarhed* eller er inficeret med bestemt *malware*. Oftest vil



Figur 9. Hyppigst scannede portnumre i 2010, DK•CERT.

13 Shadowserver.org, 2010; *"Scan charts"*.

14 Pc-library.com; *"TCP & UDP Port 3072 Information"*.

en målrettet søgning på Google kunne løse opgaven, uden at man på netværket eller den afsøgte host vil kunne se det. Umiddelbart synes truslen fra *scanninger* af større netsegmenter at være aftagende. Vi tror imidlertid, at disse erstattes af målrettede *scanninger* mod fx mobile enheder, som er koblet til et åbent trådløst netværk, som dem vi ser på cafeer, hoteller, i lufthavne og lignende.

3.3. Malware-trusler i 2010

Også i 2010 blev verden ramt af et større angreb fra en ny *orm*. I modsætning til tidligere var det denne gang ikke borgernes pc'er som blev ramt. Derimod blev flere virksomheder plaget af *Stuxnet*, som var den eneste væsentlige *orm* i 2010. Som tidligere var det de *trojanske heste*, der udgjorde den største trussel mod vores sikkerhed. I første halvdel af 2010 var den *trojanske hest* Trojan.AutorunINF. Gen ifølge BitDefender den største enkeltstående *malware*-trussel. Den *trojanske hest* udgjorde således mere end 11% af alle infektioner med *malware*. På toptilisten fandtes desuden fire andre *trojanske heste*[15].

I slutningen af juli måned udsendte Microsoft en advarsel mod *ormen Stuxnet*, der udnyttede en *sårbarhed* i den måde, Windows behandler genveje på. *Ormen* er blandt de mest målrettede og avancerede *orme*, vi endnu har set, og der var på daværende tidspunkt ingen rettelse til *sårbarheden*, som blev udnyttet. Den avancerede *orm* indeholder en *trojansk hest*. Den angriber Siemens WinCC SCADA, der blandt andet anvendes i elforsyning og industriproduktion. Om *ormen* skrev Ali Mesdaq fra sikkerhedsviksomheden Websense:

"Stuxnet has the same surgical capabilities as a stealth bomber."[16]

I første omgang spredte *ormen* sig hovedsagelig i Asien og Mellemøsten, men senere blev også danske virksomheder ramt. Således blev det i pressen beskrevet, hvordan man i A.P. Møller-Mærsk gennem flere uger måtte slås med oprydningen, efter at 300 computere var blevet ramt. Udbruddet skabte ifølge virksomheden selv, ikke afbrydelser i forretningen[17].

Instant messenger-*ormen* Worm.P2P.Palevo.DP ramte i maj 2010 ubeskyttede Yahoo Messenger og Windows Live, og installerede efterfølgende en *spam*bot på de inficerede maskinener. Kun en uge senere ramte Backdoor.Tofsee Skype og Yahoo Messenger[15].

Meget omtalte mediebegivenheder som fx naturkatastrofer, sportsbegivenheder, valentinesdag og lignende udnyttes til spredning af *malware*. For at øge effektiviteten bruges søgemaskineoptimering kombineret med script-baserede webangreb på større mediesites, hjemmesider oprettet til formålet, e-mail-kampagner og falsk antivirus. Søgning efter nyheder og trends udgjorde ifølge virksomheden Websense den største risiko for at blive udsat for links med skadelig kode. Ca. 22% af disse søgeresultater førte til links med skadelig kode. Generelt udgjorde søgninger, der ikke var specifikt arbejdsrelateret den største risiko[18]. I gennemsnit var levetiden på en *malware*-kampagne er 11 dage[19].

15 Bitdefender.com, 2010; *"H1 2010 E-threat landscape report"*.

16 Websense.com, 2010; *"2010 threat report"*.

17 Version2.dk, 2010; *"Viruskrig på to fronter: Mærsk også ramt af genvejsvirus på kontrolsystemer"*.

18 Websense.com, 2010; *"2010 threat report"*.

19 Dasient.com, 2010; *"Web-based malware infections double since last year"*.

Også i 2010 oversteg mængden af nye *malvare*-varianter den legitime software i mængde. *Malware* benyttes i dag ved stort set alle former for it-kriminalitet og udgør det væsentligste problem for vores online sikkerhed. *Trojanske heste* havde også i 2010 vind i sejlene. De udgjorde næsten halvdelen af al *malware*, som i årets første 9 måneder blev identificeret på danskernes pc'er af F-Secure (Figur 10). Dette er et mindre fald i forhold til 55% i 2009. Fælles er, at den meste *malware* ikke besidder evnen til at sprede sig selv. Sårbare legale webapplikationer, sociale netværkssteder og P2P-netværk er stadig væsentlige medier for spredning af *malware*.

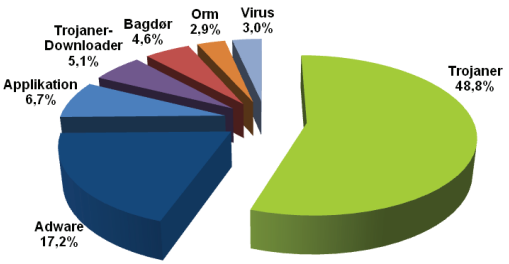
Den hollandske stats CERT estimerer, at mellem 0,5 og 5% af alle computere som er koblet på internettet er inficeret med *botnet*-programmer[21]. Selvom vi ikke i DK•CERT har modtaget specifikke rapporter om danske computere, som var inficeret med *botnet*-programmer og heller ikke F-secure har registreret danske inficeringer (Figur 10), må vi gå ud fra at de er der. Når vi ikke ser dem, skyldes det sandsynligvis at de ikke bliver fundet. Når de findes, rapporteres de ikke eller kategoriseres ikke som *botnet*-programmer. De fleste inficeringer indeholder nemlig også anden *malware*, og mange *botnet*-programmer indeholder funktionalitet, der gør, at de måske kategoriseres som fx en *trojansk hest*. Således må det formodes, at nogle af de inficeringer, som herhjemme blev kategoriseret som *trojanske heste*, reelt dækkede over *botnet*-programmer.

Herhjemme faldt antallet af anmeldelser om legale websites, der var inficeret med *phishing*-sider eller *trojanske heste*, til 482 mod 565 i 2009 (Figur 11). Når antallet af inficerede websites igen i december måned steg, tager vi det som et udtryk for, at man har forsøgt at udnytte julens øgede internethandel til at sprede *malware* og/eller indsamle kreditkortoplysninger. Når man ved, at kreditkortet snart skal bruges til julegaveindkøb, er man måske mere tilbøjelig til lade sig narre, af frygt for at ens kort ikke virker.

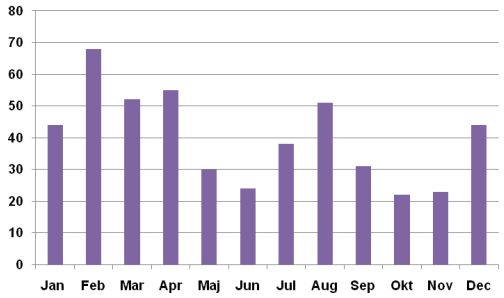
Mens vi har oplevet et mindre fald i websites, der udnyttes til spredning af *malware*, tegner andre organisationer et andet billede. Fx estimerede virksomheden Dasient, at der i andet kvartal af 2010 på verdensplan var 1,3 millioner websites, der var inficeret med skadelig kode. Det er en fordobling i forhold til kvartalet inden[22]. Tilsvarende blokerede Symantec i september et stigende antal websites, der var blevet inficeret med *malware*, der i mere end en femtedel af tilfældene var ny. I alt blev der dagligt blokeret 2.997 websites[23].

De fleste *phishing*-sider formodes at blive hostet i *botnet*, hvor *phishing*-sidens levetid mangedobles[24]. I 2009 blev 61% af alle *phishing*-sider ifølge RSA hostet i *botnet*, der benyttede fast-flux teknologi[25]. Dette formodes at være steget i 2010. Det forklarer til dels faldet i legale websites, der var anmeldt for at hoste *phishing*-sider eller *trojanske heste*. De fleste *phishing*-sider blev hostet i USA og Sverige med henholdsvis 45% og 37%. Tyskland var på en tredjeplads med kun 2%[26].

Ud over skadelig kode udgjorde uønskede mails også i 2010 et væsentligt problem.



Figur 10. Danske malware-infektioner identificeret af F-Secure i de første tre kvartaler af 2010[20].



Figur 11: Websites med trojanske heste og phishing-sider anmeldt til DK•CERT i 2010.

20 F-secure.com, 2010; "*F-Secure Security Lab - Virus World Map*".

21 Govcert.nl, 2010; *"2010 national cyber crime and digital safety trend report"*.

22 Dasient.com, 2010; *"Continued growth in web-based malware attacks"*.

23 Messagelabs.com, 2010; *"MessageLabs intelligence september 2010"*.

24 Havard.edu, 2009; *"The economics of online crime"*.

25 RSA, 2009; *"RSA online fraud report, august 2009"*.

26 Websense.com, 2010; *"2010 threat report"*.

I 2010 var 93,2% af alle e-mails sendt til danskere *spam*, hvorved Danmark er nummer to på listen over de lande hvortil der sendes mest *spam*. Globalt set var andelen af *spam* ifølge Symantec 89,1%[27] af alle mails, mens den af Websense blev opgjort til 84,3%[28]. Mellem 80 og 90% af al *spam* blev ifølge Symantec udsendt via *botnets*. Mod slutningen af året faldt andelen dog til 77%. Symantec anslår, at faldet skyldes lukningen af *spam*firmaet *Spam*it i september. Dette kan være årsag til en udvikling i den geografiske fordeling af, hvor *spam* kommer fra. Mens det meste *spam* i starten af 2010 kom fra Asien og Sydamerika, har Europa mod slutningen af året overtaget føringen[29].

Ifølge Websense udgjorde *phishing* i 2010 0,6% af alle *spam* mails[28]. Sammenholdt med en svag stigning i antallet af *spam* gennem de seneste år, må antallet af *phishing* mails tilsvarende være stigende. Der har dog gennem de seneste år været store udsving,med en mangedobling af *phishing*-niveauet hen over sommeren[30]. For månederne juni-oktober 2010 opgjorde Symantec den globale andel af *spam*-, *phishing*- og *virus*-mails til henholdsvis 86,4, 0,3 og 0,2%.

De fleste *phishing* mails skrives stadig på engelsk, men større målrettethed betyder, at de oftere er udført på det sprog, der er naturligt for modtageren. Således var 3% af alle *phishing*-mails i første halvdel af 2010 på svensk[31]. Selvom det i de fleste tilfælde er banker og andre finansielle institutioner, der er målet for *phishing*, opleves også kampagner målrettet mailsystemer, online casinoer, -butikker og -rollespil. DK•CERT behandler kun anmeldelser om *spam*, der vedrører de netværk, DK•CERT overvåger, og har således ingen repræsentative data vedrørende *spam* og *phishing* i Danmark.

Sociale netværk er en nyere kilde til udbredelse af *malware* i form af skadelig kode og/eller uønsket reklame og *phishing*. I 2010 var der links på 40% af alle statusmeddelelser på Facebook. 10% af disse var enten *spam* eller førte til sider med skadelig kode[28]. Vi ser dette som et problem i vækst og venter, at vi i fremtiden vil se mere *malware* målrettet sociale netværk.

I 2010 blev mængden af skadelig software til Android firedoblet. For smartphones generelt var der 33% flere tilfælde af infektioner med skadelige programmer i 2010 i forhold til året før. Mængden af trusler mod Java-baserede smartphones voksede 45%. Til gengæld faldt mængden af trusler mod iPhone og Symbian. Det fremgår af tal fra sikkerhedsfirmaet AdaptiveMobile[32].

I august dukkede det første kendte eksempel på en SMS-*trojansk hest* til Android op i Rusland. Hvis man installerer programmet, optræder det under navnet Movie Player på telefonens liste over applikationer. Programmet sender overtakserede SMS'er til to telefonnumre. Hver SMS koster knap 30 kroner, oplyser sikkerhedsfirmaet Kaspersky[33].

---

27 MessageLabs Intelligence, 2010; *"MessageLabs intelligence: 2010 annual security report"*.

28 Websense.com, 2010; *"2010 threat report"*.

29 MessageLabs Intelligence, 2010; *"MessageLabs intelligence: 2010 annual security report"*.

30 IBM, 2010; *"X-Force 2010 mid-year trend and risk report"*.

31 Bitdefender.com, 2010; *"H1 2010 E-threat landscape report"*.

32 AdaptiveMobile.com, 2010; *"Cyber criminals target Smartphones as malware increases by a third in 2010, reveals AdaptiveMobile"*.

33 Kaspersky, 2010; *"First SMS Trojan for Android"*.

4. Status på 2010

2010 var generelt ikke et godt år, når det gælder it-kriminalitet, og fremtidsudsigterne er dystre. Det europæiske politisamarbejde Europol anslår, at it-kriminalitet globalt koster virksomheder 750 milliarder euro om året. Hver dag menes 148.000 pc'er at få kompromitteret sikkerheden, fx via *virus* eller *botnet* programmer[34].

Som i 2009 blev året åbnet med et *orme*-angreb, der kom bag på mange af de berørte organisationer. Denne gang hed *ormen Stuxnet*. Den udgjorde både ved sin avancerede brug af teknologien og sin målrettethed endnu et skridt i it-kriminalitetens evolution.

En opgørelse fra EU's statistikkontor Eurostat viste, at 6% af de danske organisationer oplevede, at deres services var utilgængelige som følge af udefrakommende angreb. For 6% af organisationerne resulterede udefrakommende angreb og *malware* i, at data blev ødelagt[35]. Med introduktionen af nye og mere målrettede angreb som fx *Stuxnet* er der umiddelbart ingen grund til at tro, at dette har ændret sig i 2010, selvom de danske netbanker synes at være gået fri.

I dette afsnit runder vi nogle af de overskrifter og emner, som var med til at præge vores opfattelse af it-sikkerhed i 2010. Med udgangspunkt i udviklingen for 2010 tager vi fat i nogle overordnede temaer og sammenhænge, som vi mener peger fremad og vil have betydning for hvordan vi tænker og handler inden for it-sikkerhed i fremtiden.

På trods af den stigende udbredelse og forbundenhed af mobile enheder som smartphones og tavle-pc'er har vi valgt ikke at behandle dem særskilt. Det på trods af, at de i stigende grad vil blive udsat for angreb, og således udgør en stigende trussel mod borgenes og organisationernes sikkerhed. Ud over at bidrage til større diversitet mener vi nemlig ikke, at de smarte mobile enheder adskiller sig fra computere, hvorfor sikkerheden bør behandles på lige fod med disse.

It-kriminalitet har skabt en online undergrundsøkonomi, hvor kriminelle og terrorister kan købe alt fra kreditkortinformationer og *malware* over adgang til *botnet* til *DDoS*-angreb og meget mere. Hovedparten af angrebene i 2010 var fokuseret på tyveri af data. 52% foregik via web[36]. Vores færdsel på nettet er altså ikke uden risiko. Det er derfor af vital betydning, at vi kan stå sammen, da ingen organisation eller myndighed alene kan beskytte danskerne.

I samarbejdets ånd har vi også i år inviteret en række eksterne aktører til i denne rapport at bidrage med deres perspektiv på it-sikkerheden i Danmark. Vi lægger i dette afsnit ud med Lars Højberg fra TDC, som fortæller om året, der gik set fra en internetudbyders perspektiv.

Herefter beskriver vi, hvordan og hvorfor de webapplikationer, vi alle bruger og besøger, kan være et problem for vores alles sikkerhed. Men hvorfor er det sådan, og hvad kan vi gøre ved det? Sårbare legale web-applikationer er stadig

34 Europol, 2011; *"Cybercrime presents a major challenge for law enforcement"*.

35 Eurostat, 2010; "*Information and communication technologies in the EU27s"*.

36 Websense.com, 2010; *"2010 threat report"*.

en væsentlig kilde til spredning af *malware*, hvad enten vi hoster dem selv, har placeret dem på et hotel eller de ligger i skyen.

Netop brugen af skyen giver i disse år grå hår i hovedet på mangen en it-chef. Der synes ikke at være nogen tvivl om, at *cloud computing* giver en række fordele med hensyn til skalerbarhed og fleksibilitet, men hvordan er det med sikkerheden? Vi forsøger at beskrive de problemstillinger og udfordringer, der forbinder sig til at benytte services placeret i skyen. En række faktorer gør nemlig, at tjenester placeret i skyen i dag adskiller sig fra tjenester hostet hos en traditionel serviceleverandør.

Vi beskriver herefter den *malware*, de it-kriminelle forsøger at liste ind på vores computere, og kigger på, hvordan den har udviklet sig gennem 2010. Hvor spredningen for kun få år tilbage var et mål i sig selv, har målet i dag ændret sig,- og dermed de tekniske virkemidler, som bruges.

Teknik er dog ikke alt. De it-kriminelle har overtaget forretningsverdens sprogbrug, hvor markedspenetrering og -andele går hånd i hånd med målinger af en *malware*-kampagnes succes. I denne verden handler det om at skabe maksimal profit. Forståelse af den menneskelige psyke er et væsentligt aspekt i det at ramme "kunderne". Vi forsøger at beskrive, hvordan it-kriminalitetens virkemidler har forandret sig med det mål at nå bag vores tekniske forsvarsværker. Det er lykkedes i en grad, så sikkerhedssoftwaren i dag ikke kan følge med. Kun 19% af al ny *malware* fanges af antivirusprodukterne[37].

It-kriminalitet er i dag blevet en industri, hvor de værktøjer der løbende udvikles og bruges, er til salg på undergrundsmarkeder. *Trojanske heste* som fx Zeus bliver solgt til kriminelle organisationer og benyttes herefter til et utal af forskellige angreb. Blandt dem der har taget brugen af disse værktøjer til sig, er efterretningstjenester, terrororganisationer og rabiate meningsfællesskaber. Under overskriften cyberwarefare og -terrorisme beskriver vi, hvordan denne udvikling har udmøntet sig i 2010. Det er en udvikling, hvor Muhammed-krisens *defacements* af danske hjemmesider ligner drengestreger.

Heldigvis har vi herhjemme såvel som i udlandet ikke ligget på den lade side. Der har i løbet af året været flere tiltag, der havde til formål at styrke værnet mod it-kriminalitet. Året bød således på lukningen af flere store *botnet*. Herhjemme blev statens forsvar styrket med den nyoprettede *GovCERT*, der i 2010 blev operativ.

Vi slutter afsnittet som vi startede med at lade nogle andre komme til orde. Vi har først valgt at lade Steen Petersen fra DTU fortælle om universitetets perspektiv på it-sikkerhed. Herefter har vi givet ordet til den nye dreng i klassen. På vegne af den nu operative *GovCERT* fortæller Thomas Kristmar om, hvordan de i *GovCERT* oplevede 2010 og de udfordringer vi står over for.

4.1. 2010 set fra en internetudbyder

Af Lars Højberg, teknisk sikkerhedschef, TDC
Der introduceres stadig flere forretningskritiske tjenester baseret på internettet, og både private, offentlige og erhvervskunder bliver mere afhængige af deres internetadgang. Derfor er kundernes tillid til nettet altafgørende. Som

37 Net-security.org, 2010; *"AV vendors detect on average 19% of malware attacks".*

internetudbyder er vi i TDC selvfølgelig fokuseret på at beskytte vores kunder og vores infrastruktur mod trusselsbilledet, som bliver mere og mere komplekst og med et niveau, der er konstant stigende.

Botnets påvirkning af trusselsbilledet på internettet er fortsat enormt. Det mærker vi også i vores infrastruktur i form af fx *spam* eller *DDoS*-angreb, som stammer fra pc'er inficeret med *botnet*-programmer.

Ud fra en sikkerhedsvinkel er de mest kritiske *spam*-mails dem, som kan udsætte modtageren for en sikkerhedsmæssig risiko. Det kan fx være mails, som enten indeholder skadelige programkode som vedhæftet fil, eller som indeholder et link til en webside med skadelig kode. I 2004 forudsagde Bill Gates, at *spam*-problemet var udryddet i løbet af et par år. Det er ikke just gået den vej, tværtimod. I 2010 har TDCs netbaserede *spam*filter til privatkunder filtreret 3,8 milliarder indgående mails fra. Det svarer til 10,4 millioner *spam*-mails om dagen eller 7 *spam*-mails pr. mailboks pr. dag.

I efteråret 2010 har TDCs filter for indgående mails oplevet det laveste *spam*-niveau siden McColo-lukningen i november 2008. Det skyldes sandsynligvis, at der i løbet af efteråret har været nogle markante begivenheder, som fx lukningen af *spam*-organisationen Spamit.com og *botnettet* Bredolab, samt arrestationen af medlemmer af Zeus-ringen. Belært af lukningen af McColo vil vi dog sandsynligvis se en "normalisering" af *spam*-mængden i løbet af de næste måneder.

Phishing er i løbet af 2010 blevet en større trussel mod de danske internetbrugere. Det skyldes, at langt flere af de *phishing*-mails, som havner i danskernes mailbokse, nu er udformet på velformuleret dansk og derfor fremstår mere troværdige. Vi har i år set dansksprogede *phishing*-mails, der bl.a. har forsøgt at franarre brugernavn/mailadresse/password fra webmail-kunder hos TDC og andre danske internetudbydere. Derudover har bl.a. PBS (nu Nets) været udsat for *phishing*-forsøg, hvor et antal danskere er blevet franarret deres kreditkortoplysninger.

Værdien af at lokke mailkonto-oplysninger ud af webmail-kunder synes måske ikke oplagt. Adgang til webmail-konti er nu ganske attraktivt for de it-kriminelle, da de på den måde kan "snylte" på webmail-tjenesternes normalt gode omdømme på nettet. *Spam*-mails har generelt en større sandsynlighed for at nå frem til de ønskede modtagere, når de sendes fra webmail-konti. Misbrug af denne slags kaldes for reputation hijacking.

Det er ikke kun gennem *phishing*, at de it-kriminelle forsøger at få adgang til TDCs og andre udbyderes webmail-konti. De fleste webmail-udbydere beskytter sig ved hjælp af *CAPTCHA* mod automatisk oprettelse af webmail-konti. Men i flere afrikanske lande sidder der folk, som mod betaling manuelt opretter webmail-konti.

Også *DDoS*-angreb bliver en større og større trussel mod både virksomheder, organisationer og nationalstaters infrastruktur. Den megen presseomtale af både *DDoS*-angrebene mod WikiLeaks og WikiLeaks' sympatisørers angreb mod fx PayPal, Visa og Mastercard gør, at det er et begreb og en trusselsform, som rigtig mange danskere efterhånden kender til, og som mange virksomheder er nødt til at forholde sig aktivt til. I TDCs netværk ser vi dagligt flere *DDoS*-angreb. Heldigvis er langt de fleste fortsat "tilfældige" og ustrukturerede.

I 2010 har vi i kampen mod *botnet* gjort nogle tekniske tiltag som fx at blokere

for mailtrafik på port 25 fra dynamiske IP-adresser i vores net. Herved har vi umuliggjort, at pc'er med dynamiske IP-adresser i TDCs net, der er inficeret med *botnet*-programmer, kan sende *spam* ud på nettet uden om vores mailservere.

Internettrusler i bred forstand kan dog ikke bekæmpes af internetudbyderne hver for sig. Vi er nødt til at samarbejde i kampen mod de it-kriminelle. TDC deltager i en række nationale og internationale samarbejdsfora som et led i vores indsats mod internettrusler. På den nationale front deltager vi bl.a. i ISP-Sikkerhedsforum, hvor en stribe af de danske internetudbydere er medlemmer, og hvor DK-CERT og *GovCERT* deltager som observatører. Et af dette forums vigtigste indsatsområder er som operationelt beredskab, der træder i aktion, når der er trusler på nettet, som kræver en tværgående aktion. I 2010 har dette beredskab igen været i aktion og vist sit værd. Vi er i øjeblikket ved at finde ud af, hvordan vi i fællesskab kan skærpe vores indsats i kampen mod *botnet*.

Kunderne kan selvfølgelig også gøre meget for at beskytte sig selv mod at få deres pc'er inficeret og misbrugt. Vores bidrag i den sammenhæng er at skabe opmærksomhed omkring sikkerhedsemner, der er relevante for slutbrugerne. Således har vi i 2010 igen deltaget i netsikker nu! kampagnen. Kampagnen havde fokus på temaerne: "Tænk!", "Blokér!" og "Opdatér". Vores indsats var sammen med finansverdenen (Finansrådet, Danske Bank og Nordea), Microsoft og DK•CERT koncentreret om temaet "Opdater" og sitet opdaterdinpc.dk. Også på siden sikkerhed.tdc.dk har brugerne mulighed for løbende at blive opdateret om de seneste trusler.

4.2. De farlige webapplikationer

Også i 2010 var webapplikationer en væsentlig kilde til spredning af *malware*. Som tidligere år besad den meste *malware* ikke evnen til selv at sprede sig, og drive-by-angreb fra kompromitterede sårbare legale websider var den foretrukne metode til spredning af fx *trojanske heste*.

Fra 2009 til 2010 identificerede virksomheden Websense en stigning i inficerede websites på 111%. 80% af de inficerede sites var legale websites, der var blevet kompromitteret. Det meste *malware* var placeret i USA og kommunikerede for 53,7% vedkommende med computere, der tilsvarende var placeret i USA[38]. Sikkerhedsfirmaet Dasient registrerede fra tredje kvartal 2009 til tredje kvartal 2010 en fordobling af websites, der var inficeret med skadelig kode. I tredje kvartal 2010 var over 1,2 millioner web-sites således inficeret med kode, der forsøger at inficere pc'er, der besøgte webstedet. Sandsynligheden for at et inficeret websted igen blev ramt af *malware* var 40%[39].

Ved *scanning* af netværk hos DK•CERTs kunder var webapplikationer, der lyttede på TCP-port 80 eller 443, de mest sårbare. Over 75% af alle konstaterede *CVE-nummererede sårbarheder* blev konstateret på disse porte. Ud over de *sårbarheder*, som kan konstateres med et *CVE-nummer* vil der ofte i tillæg hertil være *sårbarheder* i den specifikke webapplikation, der fx muliggør *SQL-injection*, *cross-site scripting* eller tilsvarende. Disse registreres ikke med et *CVE-*

38 Websense.com, 2010; *"2010 threat report"*.

39 Dasient.com, 2010; *"Web-based malware infections double since last year"*.

40 Csis.dk, 2010; *"Netbank tyv leveret via Midtjyllands avis hjemmeside"*.

41 Version2.dk, 2010; *"Advarsel: Hotmail spreder malware"*.

Midtjyllands Avis spredte netbank-spion

I perioden fra den 24. 25. november 2010 blev bannerreklamerne på mja.dk udnyttet til at sprede en avanceret netbank- og informationstyv, som specifikt angribeb danske netbanker. Det skadelige script, der via *SQL-injection* blev indsat i avisens bannerreklamer, tvang de besøgende over på sites med skadelig kode. Herfra blev det forsøgt at udnytte sårbarheder i bl.a. Adobe Flash, Adobe Acrobat/Reader, Java JRE og Microsoft Internet Explorer. Avisens ca. 15.000 daglige besøgende var således i potentiel fare for at få opsnappet informationer om netbanklogin og andre følsomme oplysninger.

CSIS Security Group A/S[40]

Hotmail-banner spredte malware

Microsoft-tjenesten Live.com, der benyttes af Hotmail, præsenterede i starten af december 2010 brugerne for *malware*-inficerede bannere. Hvis en bruger klikkede på banneret, blev han blevet ledt over på en side, der ved hjælp af sårbarheder i Java JRE og Adobe Reader forsøgte at installere *malware* på brugerens pc.

Version2.dk[41]

nummer. Selvfølgelig er det et billede på at webapplikationer er de hyppigst eksponerede applikationer, men også på at mange organisationer ikke har indarbejdet procedurer, der sikrer at *sårbarheder* rettes. Således efterlades mange webapplikationer med *sårbarheder*, der gør det muligt at benytte dem til spredning af *malware*.

SQL-injection og *cross-site scripting*, der bl.a. udnyttes til datatyveri, eksponering af links til *malware* samt egentlig systemkompromittering er de hyppigst udnyttede typer *websårbarheder*. Efter kompromittering af webapplikationen vil den ikke selv hoste *malware*, men blot med indlejrede scripts, henvise til *malware*, som ofte er hostet i *botnet*.

De typer af websites, der primært udnyttes til spredning af *malware* er hhv. pornografiske sites, blogs og bulletin boards, personlige hjemmesider og gambling sites. Der er dog sket en ændring. 50% af de personlige hjemmesider havde i starten af 2009 mindst et link til skadelig kode, mens det i starten af 2010 var kun cirka 10%. Hvor personlige hjemmesider tidligere blev ramt som det bløde mål, kan noget tyde på, at den manglende trafik på disse sider har gjort, at de ikke er attraktive til spredning af *malware*. Derimod er der sket en stigning i links til skadelig kode på henholdsvis pornografiske sites og blogs og bulletin boards[42]. Hvor de første har mange besøgende, vil de sidste tit være nemme mål, da det jo netop er meningen at brugerne interagerer og selv lægger data på sitet.

Det er således ikke kun de websites, hvor man kan forvente *malware*, der deltager i spredningen. Ofte ønsker de kriminelle at lukrere på et kendt domænes mange besøgende eller de besøgendes tillid til sites. Således kan også større mediesites eller andre sider med mange besøgende opleve at blive mål for angreb, hvis ikke de sørger for at afklare og fjerne *sårbarheder*. Således har også de sociale netværkssteder i 2010 været under angreb. Fx blev der i løbet af året konstateret *sårbarheder* på både Facebook og Twitter, der gav uvedkommende adgang til brugernavne og passwords eller til at skrive på andre brugeres væg.

Man kan argumentere for, at sårbare webapplikationer i en kontekst af *malware*-spredning kun er et problem, fordi de besøgende ikke opdaterer deres browser og de komponenter, som er knyttet til den. Det argument er kun til dels rigtigt. Den bruger, der oplever at få sin pc forsøgt inficeret med *malware* fra et givent site, vil have forbehold mod at besøge sitet igen. Ud over et vist tab af omdømme i den forbindelse risikerer sitet at blive blokeret af *malware* filtre og søgemaskiner. Herved risikeres et ikke uvæsentligt tab af omdømme og/eller omsætning.

Generelt mener vi, at der herhjemme bør være større fokus på sikring af webapplikationer for på den måde at beskytte borgene mod *malware*. Bevares, vi vil stadig blive ramt, selv om det skulle lykkes at sikre de danske hjemmesider. Det vil dog gøre det langt vanskeligere at målrette et angreb mod danskerne, hvis *malware* ikke længere spredes fra dansksprogede websider. I et marked hvor opgaven med at varetage it-sikkerhed bliver stadig mere kompleks, hostingselskaberne konkurrerer på prisen på bekostning af sikkerhed og service, og brugen af potentielt sårbare tredjeparts komponentereksploderer, tror vi, at løsningen skal findes gennem samarbejde og dialog. Vi mener, at det bør være muligt blandt ISP'erne, hostingselskaberne og sikkerhedsbranchen at indarbejde en løsning, der dels sikrer et minimum af sikkerhed på webapplikationerne og dels sikrer, at inficerede webapplikationer bliver isoleret, renset og sikret, inden de igen sættes på nettet.

42 IBM, 2010; *"X-Force 2010 mid-year trend and risk report"*.

4.3. Skyhøj sikkerhed eller ej?

Cloud computing var et af de mest brugte udtryk i 2010. Mange fokuserede på muligheden for fleksibel levering af it-tjenester, hvor man kun betaler for, hvad man bruger. Men med *cloud* følger der også nye overvejelser om sikkerhedsaspektet. Som konsulentfirmaet Deloitte udtrykker det:

"Cloud computing may, in many scenarios, be a more efficient way to deliver and manage it services. But in order to reap the full benefits, organizations must find ways to address a number of important security and privacy challenges."[43]

Cloud giver mulighed for at købe sig adgang til datakraft i form af store driftscentre. En af fordelene er elasticiteten: Når et websted pludselig får mange nye brugere, skruer man bare op for kapaciteten. Men den store datakraft kan også misbruges. Det så vi et eksempel på i april, hvor en række IP-telefonisystemer blev udsat for et bombardement af datapakker. Angrebet var et forsøg på at gætte sig til brugernavne og password, så angriberne kunne misbruge systemerne til at ringe gratis. Datapakkerne kom fra IP-adresser tilhørende Amazons Web Service tjeneste EC2 (Elastic Compute Cloud)[44]. Angriberne har sandsynligvis hacket sig ind på EC2-kunders konti og udnyttet dem til angrebene. I dette tilfælde var det *cloud*-servernes regnekraft og båndbredde, der blev misbrugt. Men *cloud* har også andre sikkerhedsmæssige udfordringer. Det gælder fx beskyttelsen af fortrolige oplysninger. På et system baseret på SaaS (*Software as a Service*) deles flere kunder om den samme software. Her er det vigtigt, at data kan isoleres, så konkurrenter ikke kan se hinandens kundedata.

Også fra et CERT-perspektiv er der udfordringer i *cloud*. Hvis man ser et angreb komme fra en IP-adresse tilhørende en *cloud*-udbyder, kan det være en udfordring at efterforske, hvilken af dennes kunder der står bag. For at gøre noget ved denne og andre problemstillinger tog organisationen Cloud Security Alliance i slutningen af året initiativ til CloudCERT[45]. Det er et samarbejde, som skal forsøge at løse nogle af de problemer, som *cloud computing* giver for CERT-funktioner. Blandt målene er, at udbydere af *cloud*-tjenester skal have en CERT-funktion til at håndtere sikkerhedshændelser. Den første statusrapport fra CloudCERT ventes klar i midten af februar.

Til at holde styr på sikkerhedshændelser i skyen lancerede organisationen Open Security Foundation i april webstedet Cloutage[46]. Her kan man følge med i, hvilke *cloud*-udbydere der har oplevet problemer med sikkerhed og tilgængelighed. I 2010 blev der registreret 322 sikkerhedshændelser. 261 af dem var af typen, hvor en tjeneste i en periode var utilgængelig. 18 hændelser handlede om hacking.

Brugen af *cloud computing* byder på en række udfordringer, man som organisation bliver nødt til at være sig bevidst. Særligt forhold omkring behandlingen af data i forhold til gældende lovgivninger beskrives af ENISA, som et forhold man skal tage højde for[47], men også de kontraktlige forhold kan medføre aspekter, der adskiller sig fra traditionelle leverandøraftaler.

---

43 Deloitte, 2010; *"2010 TMT global security study – key findings"*.

44 DK•CERT, 2010; *"Angreb på IP-telefoni fra Amazon EC2"*.

45 Cloud Security Alliance; *"CloudCERT"*.

46 Open Security Foundation, 2010; *"Cloutage"*.

47 ENISA, 2009; *"Cloud computing: Benefits, risks and recommendations for information security"*.

Da data i skyen ofte er placeret i et andet land, kan det være et problem at sikre sig, at de bliver behandlet korrekt i forhold til gældende lovgivning, da det er ejerens og ikke *cloud*-udbyderens ansvar at overholde lovgivningen. Fx kræver EU's datalovgiving, at følsomme data ikke må forlade Europa. Herhjemme rummer persondataloven en række krav til behandling af personhenførbare data, som her skal tænkes meget bredt. Fx er e-mail og IP-adresser beskyttede. Således stiller Datatilsynet krav om at personhenførbare data skal opbevares krypteret i et "sikkert land", eller af en organisation som er godkendt som en "safe harbor". Det stiller krav til at man ved hvor og hvordan data behandles, hvilket ikke altid er specificeret i kontrakten for brug af *cloud* services.

Yderligere kan der opstå problemer, hvis myndighederne i det land, hvor data hostes, kan kræve adgang til data uden dataejerens tilladelse eller vidende. For en dansk organisation kan det være i direkte konflikt med persondataloven, gældende standarder eller organisationens egen it-sikkerhedspolitik. Generelt gælder det om nærlæse de kontraktlige vilkår og sikre sig, at krav til fx gældende lovgivning overholdes.

Brugen af *cloud computing* byder derudover på en række kontraktlige faldgruber med hensyn til sikkerhed, som på mange måder ikke adskiller sig fra almindelig outsourcing. Oftest vil kunden være nødsaget til at forholde sig til en standardkontrakt, der i højere grad fraskriver udbyderen ansvar og fokuserer på fakturering af kunden. Ifølge Jesper Langemark fra advokatfirmaet Bender von Haller Dragsted skal man stille krav til sin leverandør. Man skal blandt andet sikre sig, at services og data er tilgængelige, hvilke formater data skal være tilgængelige i og hvor hurtigt de kan fremskaffes[51].

Derudover kan der opstå problemer i forhold til standarder og certificeringer, som udbyderen ikke overholder, ikke kan give garanti for at overholde og/eller ikke giver mulighed for at kontrollere overholdelsen af. Generelt kan outsourcing af it-services give udfordringer i forhold til organisationens *compliance*-initiativer, og brug af *cloud*-services kan vise sig ikke at være kompatibel med fx organisationens egen it-sikkerhedspolitik.

I december holdt IT-sikkerhedskomiteen en konference om *cloud computing* og sikkerhed. I forbindelse med konferencen udgav komiteen to publikationer: "*Sikkerhed i cloud computing*"[52] og "*Sikker cloud computing for forretningsansvarlige*"[53]. De gennemgår, hvordan man i *cloud*-sammenhæng kan sikre tilgængelighed, integritet, fortrolighed og privatlivets fred.

På konferencen udtalte videnskabsminister Charlotte Sahl-Madsen, at hun er klar til at se på, om der er brug for ændring af lovgivningen i forbindelse med anvendelsen af *cloud computing* i det offentlige. Men hun ville afvente Datarådets afgørelse i Odense-sagen før eventuelle ændringer. Sagen regnes for principiel.

Langt de fleste sikkerhedsproblemer med *cloud computing* var i 2010 relateret

48 Datatilsynet, 2010; *"Udtalelse i forbindelse med anmeldelse af Google Apps - online kontorpakke med kalender og dokumenthåndtering".*

49 Version2.dk, 2010; *"Datatilsynet forbyder Google Apps i kommuner".*

50 Version2.dk, 2010; *"Nu venter afgørelsen: Odense er klar til Google-gyser i Datarådet".*

51 Version2.dk, 2009; *"Sådan undgår du jura-faldgruberne i cloud computing".*

52 It-sikkerhedskomiteen, 2010; *"Sikkerhed i cloud computing".*

53 It-sikkerhedskomiteen; *"Sikker cloud computing for forretningsansvarlige".*

Google Apps i Odense kommune

Et væsentligt spørgsmål ved cloud computing er beskyttelsen af fortrolige og personfølsomme data. Det blev Odense Kommune opmærksom på, da kommunen besluttede at bruge cloud-tjenesten Google Apps til at holde styr på elevplaner. I en udtalelse i juni skrev Datatilsynet til kommunen, at tilsynet ikke kunne tiltræde, at planen gik i luften den 1. august som planlagt[48]. Årsagen var blandt andet, at login foregik med brugernavn og adgangskode, ikke med digital signatur[49].

Datatilsynet stillede kommunen 14 spørgsmål. Dem besvarede Odense Kommune med hjælp fra It- og Telestyrelsen i oktober. I november stillede Datatilsynet 14 nye, uddybende spørgsmål til kommunen. De blev besvaret, og sagen behandles nu i Datarådet[50].

til tilgængelighed: Systemer var nede, så kunderne ikke kunne bruge dem. Det skete for udbydere som Skype, Amazon, Rackspace og flere andre. Samlet set kom der i 2010 ikke en enkelt stor sikkerhedshændelse knyttet til en *cloud*-tjeneste. Sikkerhedsverdenen er blevet opmærksom på udfordringerne i *cloud* – og de it-kriminelle er utvivlsomt også i gang med at undersøge, hvordan de kan udnytte *cloud*. Vi vil utvivlsomt høre mere om *cloud* i 2011, også fra et sikkerhedsperspektiv.

4.4. Æblet eller ormen, nye malware-trusler

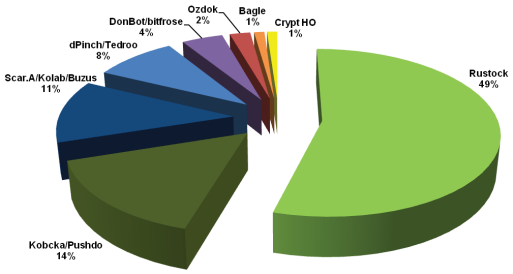
Botnet har i 2010 levet en relativt stille tilværelse. Ikke at de ikke eksisterer eller ikke er et problem, for det er de. *Botnet* er blevet en integreret del af den organiserede internetkriminalitet, som bagmændene ingen interesse har i bliver opdaget eller blokeret. Inficering med *botnet*-programmer er stadig en nærværende trussel, som i 2010 stod for udsendelse af 77% af al *spam*[54]. Herhjemme var op mod 100.000 danske computere ifølge Peter Kruse fra sikkerhedsvirksomheden CSIS Security Group A/S inficeret med *botnet*-programmer i 2009[55]. Dette tal formodes ikke at være mindre i 2010.

Ud over en række anholdelser har *botnet* ikke været så synlige i medierne, hvorfor vi i år har valgt ikke at behandle dem separat. Det mest aktive *botnet* var i 2010 Rustock, der udsendte over 44 milliarder *spam*-mails om dagen fra over en million pc'er[54]. Dette *botnet* stod for næsten halvdelen af den *botnet*-aktivitet, som blev registreret af BitDefenderi første halvår af 2010 (Figur 12).

En græsk gud var et af årets mest omtalte emner inden for it-kriminalitet. Navnet er Zeus, men programmet er også kendt som Zbot. It-kriminelle bruger det til at stjæle fortrolige oplysninger fra pc-brugere. Informationerne der fx kan give adgang til ofrenes netbankkonti. I 2010 kom version 2.0 af Zeus, der hurtigt blev populær i den digitale undergrund. Den nye version var sværere at opdage end forgængerne og indførte stærkere kryptering af kommunikationen i *botnettet*[56].

Omkring den 1. oktober gennemførtes i Storbritannien, USA og Ukraine en operation mod Zeus. Mere end 100 personer blev arresteret i det som blev kaldt operation Trident Breach. De var mistænkt for at have brugt *botnet*tet til at stjæle penge fra netbankkonti og misbruge kreditkort. Dette førte muligvis til, at Zeus trak sig tilbage efter nogle år i rampelyset. Et andet stykke skadelig software ved navn SpyEye har siden 2009 udfordret Zeus. Når SpyEye inficerer en pc, sletter den Zeus, hvis den finder konkurrenten på pc'en. Nogle uger efter operation Trident Breach offentliggjorde manden bag Zeus, at han trak sig tilbage, og at Zeus-koden ville blive overdraget til SpyEyes bagmand. Denne fusion ser dog endnu ikke ud til at have fundet sted[56].

Ifølge sikkerhedsfirmaet Trend Micro udsender it-kriminelle hvert sekund 3,5 nye skadelige programmer. Langt hovedparten er små variationer af kendte programmer, som udsendes for at gøre det sværere for antivirusprogrammer at genkende dem. Samtidig bliver truslerne stadig mere sofistikerede. Det så vi i 2010 med avancerede trusler som *Stuxnet* og Aurora-angrebet på Google og andre virksomheder.



Figur 12. Botnet aktivitet i første halvår af 2010[57].

54 MessageLabs Intelligence, 2010; *"MessageLabs intelligence: 2010 annual security report"*.

55 Computerworld.dk, 2009; *"Skal danske internetudbydere bekæmpe botnet?"*.

56 Trend Micro, 2010; *"2010 in review: New and better ways of stealing information"*.

57 Bitdefender.com, 2010; *"H1 2010 E-threat landscape report"*.

Ud over kryptering og *fast-flux*-egenskaber kan de fleste *botnet*-programmer og *trojanske heste* i dag opdatere sig selv. Derudover gøres der udbredt brug af forplumring af kode og avancerede algoritmer til bl.a. opdatering af domænelister. Over en bred kam kan man sige, at *malware* ikke står tilbage i forhold til legal software mede hensyn til funktionalitet og avancerede features. Således er der sket en sammensmeltning af metoder, der gør det vanskeligere entydigt at kategorisere *malware*.

Ovenstående tegner et billede af en stadig stigende mængde *malware*, som udsendes bl.a. med det formål at gøre det vanskeligere at opdage og afværge konsekvensen af. For at ramme under sikkerhedsorganisationernes radarer benyttes *malware* i dag til mindre, men til gengæld mere målrettede angreb end tidligere. Som en konsekvens af det udvikles der i dag også *malware* til platforme, som på grund af markedsandele ikke tidligere var attraktive. Tilsammen har det medført, af at kun 19% af de nye *malware*-angreb opdages af antivirus-softwaren[58].

Selvom andelen af *malware* på Apples Mac OS er i undertal i forhold til den *malware*, der eksisterer til Windows, er der ingen tvivl om, at den er i vækst. Det at man kan ramme over flere platforme, gør Mac'en attraktiv for nogle, mens de stigende markedsandele gør den attraktiv for andre. Tidligere tiders mantra om, at der ikke eksisterede *malware* til Mac og platformen derfor var mere sikker, holder ikke vand i dag og har sandsynligvis aldrig gjort det. Der har altid været *sårbarheder* på Mac, de er blot ikke blevet forsøgt udnyttet i samme grad, som de bliver nu.

Både i antal og diversitet er der en stigning i *malware* til Mac OS. Fx har en variant af *ormen* Koobface forsøgt at inficere Macintosh-computere via en Java-applet, været spredt på sociale netværkssteder. Flere applikationer kan afvikles på tværs af Mac og Windows med samme scripting-API. Det gør dem attraktive for angreb, der rammer begge platforme. Nogle *DDoS-botnet* er i stand til at styre store angreb på tværs af platforme. *DDoS*-angreb hvor både Macintosh- og Windows-computere deltog, er i 2010 konstateret af fx virksomheden Damballa[59].

Det formodes. at *malware* til andre systemer og platforme som fx Linux, Android og lignende er i vækst. Fx vil mobiltelefonen være et interessant mål, hvis der herigennem kan skaffes adgang til lokale netværk, mailkonti eller man kan sende overtakserede SMS'er. I den forbindelse tror vi ikke, at de styresystemer, der er placeret på andre netopkoblede enheder som spilkonsoller, eller fjernsyn går fri. Fælleds for dem er jo, at de giver potentiel adgang til det lokale net, men derudover også til en række internetbaserede betalingstjenester.

Særligt web 2.0-tjenester som fx sociale netværkssteder har fået de kriminelles opmærksomhed og er blevet et væsentligt medie for spredning af *malware*. Denne tendens tror vi desværre ikke stopper her. Vi venter, at fremtiden byder på ny *malware*, der enten spreder sig via sociale netværkssteder eller blot benytter dem som medie for indsamling af mere eller mindre personlige oplysninger, spredning af *spam*, misinformation eller lignende. Et oplagt mål vil her være at misbruge *sårbarheder* i de tredjepartsapplikationer som udvikles til de sociale netværkssteder.

58 Net-security.org, 2010; *"AV vendors detect on average 19% of malware attacks"*.

59 Damballa.com, 2010; *"DDoSing the night away on Mac"*.

60 DK•CERT, 2010; *"DK•CERT Trendrapport: It-sikkerhed i tredje kvartal"*.

Macintosh-trojansk hest på dansk universitet

I september 2010 blev en bærbar Macintosh-computer på et dansk universitet ramt af en *trojansk hest*. Den inficerede computer svarede på DHCP-forespørgelser fra det lokale net, hvor den udleverede sin egen IP-adresse som henholdsvis gateway og navneserver. Derved fungerede den som proxy for de maskiner, der benyttede den som DHCP-server. Det ville således fx være muligt at opsnappe brugernavne og passwords eller lade maskinen indgå som *Man in the Middle*.

Heldigvis udleverede den inficerede computer IP-adresser i et netsegment, der ikke var gyldigt på det lokale net. At computeren var bærbar og sandsynligvis var blevet inficeret et andet sted medførte således, at hændelsen blev opdaget og afværget[60].

I første halvdel af året oplevede virksomheden BitDefender en stigning i mængden af *ransomware*, der fx tager brugerens data som gidsel og kræver udbetaling af en løsesum. Meget *ransomware* var målrettet brugere af P2P-netværk, hvor man truede med retssager på grund af distribution af kopibeskyttet materiale[61]. Andre metoder som fx kryptering af brugernes data er også hyppigt anvendt.

4.5. De syv dødssynder - nye mål nye midler

Et forandret trusselslandskab har medført, at kun de færreste i dag forstår den trussel de prøver at beskytte sig mod. Fx er det en udbredt misforståelse, at det er tilstrækkeligt med et antivirus-program. Kun ca. 9% af den voksne befolkning føler sig ifølge antivirus-producenten Norton trygge, når de er online. Kun 3% mener, at de ikke bliver ofre for it-kriminalitet. 51% vil dog ikke ændre deres online adfærd, selv hvis de bliver udsat for it-kriminalitet[62].

Angreb er i dag mere målrettede, rammer over flere fronter og benytter sig af nye metoder og tricks. Fx er den menneskelige faktor i stigende grad blevet et svagt led i it-sikkerhedskæden. Løbende har den teknologiske udvikling givet os mulighed for at minimere de risici, der var knyttet til teknologien selv. Derimod er det vanskeligt at beskytte sig mod den menneskelige faktor. Blandt andet derfor er der sket et skifte, hvor målet for it-kriminalitet ikke længere er borgernes og organisationernes it-installationer, men deres data.

Man kan sige, at angrebsvektorerne er blevet udvidet fra de "syv dødssynder" til også at omfatte medmenneskelighed, medlidenhed og hjælpsomhed samt vores trang til at realisere os selv og interagere socialt. Tidligere straffede it-kriminaliteten de dovne og hovmodige, som ikke mente, de havde behov for et antivirus-program, firewall, backup eller lignende, eller blot ikke gad implementere det. De griske, grådige og misundelige blev straffet af *spam* og *phishing*, hvor man i bedste fald modtog virkningsløse Viagra-piller og i værste fald blev franarret penge. Imens ledte jagten på russiske kvinder og pornografi de utugtige i armene på *malware*-inficerede hjemmesider eller hjemmesider, hvor abonnementet kostede langt mere, end man troede og i nogle tilfælde var uopsigeligt. Kun de vrede syntes at være gået fri. De it-kriminelle har således også i 2010 tilpasset deres metoder til internettets dynamiske og sociale karakter.

Jordskælvskatastrofen, der den 12. januar 2010 ramte Haiti, medførte både herhjemme og i udlandet forsøg på at udnytte katastrofen til egen økonomisk vinding. Flere steder oplevede man herhjemme falske indsamlere, der udgav sig for at komme fra Dansk Røde Kors, Red Barnet og lignende organisationer. Også på internettet florerede de falske indsamlinger, bakket op af mailkampagner, der opfordrede til at støtte redningsarbejdet i Haiti.

Flere danske internetbrugere modtog i november 2010 som millioner af e-mail adresser verden over en mail fra den "russiske kvinde", Elena. Kvinden, der bor i en ikke angivet russisk provins, var ramt af en række ulykker, som oven i den økonomiske krise og inflation medførte, at hun og hendes familie ikke længere havde råd til opvarmning af hjemmet. I mailen, der ikke lagde skjul på, at den var oversat ved hjælp af Google Translate, opfordrer hun derfor til, om nogen vil sende

61 Bitdefender.com, 2010; *"H1 2010 E-threat landscape report"*.

62 Norton.com, 2010; *"Norton cybercrime report: The human impact"*.

hende en ovn, eller rettere pengene til en ovn[63]. Mailen var dog svindel og spillede på samme måde som falske indsamlinger ved naturkatastrofer på vores villighed til at hjælpe. Varianter af svindlen har været kendt siden 1988[64].

Tilsvarende oplevede nogle at modtage mails fra bekendte, der var ude at rejse, og som havde mistet deres ejendele. I mailen, som var sendt fra en mailadresse, der lignede den bekendtes, blev man opfordret til at overføre penge via Western Union eller tilsvarende, som ville blive tilbagebetalt ved hjemkomsten. Problemet var blot her, at den rejsende ikke havde problemer og var uvidende om mailen. Viden om at han var ude at rejse og hvem han var venner med, var sandsynligvis skaffet via en social netværkstjeneste eller efter at adgangen til hans mailboks var blevet afluret på en internetcafe. Herefter var der via internationale kontakter blevet fabrikeret en mail med den rejsendes eget sprog og sprogbrug. Det fik i årets løb flere til at gå i fælden og overføre penge til de kriminelle bagmænd.

Også de metoder, der benyttes til hvidvaskning af penge, har forandret sig. I takt med et stigende fokus på pengeoverførelser. Stjålne kreditkortinformationer bliver brugt til køb af vare på nettet. Det har skabt et behov for *muldyr* til at videresende de købte vare. *Muldyr*ene rekrutteres i stigende grad via jobannoncer, der udsendes via *spam*. I enkelte tilfælde er det lykkedes at infiltrere legale jobformidlere. Dette medførte i 4. kvartal af 2010, at der i medierne herhjemme var fokus på denne type kurerjob.

Hvor mange af os for kun få år siden havde en overskuelig vennekreds som vi følte et tillidsbånd til, er vennekredsen i dag vokset. Vores virtuelle venner og bekendtskaber på de sociale netværkssteder udgøres i dag for størstedelens vedkommende af mennesker, som vi kun har et sporadisk forhold til og/eller aldrig har mødt. Alligevel er tilliden til disse "nye venner" langt større end tilliden til tilfældige fremmede vi møder på gaden. Det på trods af, at vi reelt ikke ved, om de er dem, de giver sig ud for at være. Således accepteres venneanmodninger fra vores venners venner uden at blinke, og vi klikker på links og installerer applikationer på baggrund af henvendelse fra disse "nye venner".

I juli rundede tjenesten Facebook 500 millioner brugere. Så mange brugere gør tjenesten til et oplagt mål for svindlere. Året har da også bragt en stribe eksempler på misbrug af Facebook. De falder typisk inden for tre kategorier: *Likejacking*, survey scams og skadelige applikationer.

Likejacking er en ny type trussel, der er direkte forbundet til en facilitet på Facebook[65]. Den går ud på at få det til at se ud som om, en bruger "synes godt om" en bestemt webside. Bagmændene har interesse i at lokke mange til den pågældende webside, der fx kan indeholde skadelig software eller et spørgeskema (se nedenfor). Angrebet anvender en metode, der er kendt som *clickjacking*. Det består i, at en webside kidnapper et klik, som brugeren har afgivet, og bruger det til noget andet. Ved *likejacking* følger brugeren et link fra Facebook til et andet websted. Her klikker brugeren på en knap for at komme videre. Men klikket går i virkeligheden til en skjult knap, der instruerer brugerens Facebookprofil om, at vedkommende "synes godt om" websiden. På den måde kan brugerens venner blive lokket til at besøge samme webside.

En anden udbredt form for svindel er de såkaldte survey scams, der har til formål

63 JydskeVestkysten, 2010; *"Spammail: Elena trygler millioner om brændeovn"*.

64 Joewein.net; *"Begging spam from Russia"*.

65 Sophos.com, 2010; *"Facebook Worm – Likejacking"*.

Emne: Beskaeftigelsen for de studerende i din by

A EU retail company has opend a new COURIER position in your area, you can work on both part- and full-time schedule; everyone, including students and senior is welcome to apply. You can easily combine this job with your regular full time work as it demands from just 4 hours weekly. Your payment will consist of a fixed marked rate salary plus quarter bonuses.

You will be in charge of collecting parcels on employer's behalf at post offices and distributing them as instructed. All delivery-related issues are covered by the employer.

To apply, you should:
- be a citizen of Denmark aged eighteen and above
- be able to comtribute from 4 hours weekly
- be PC familiar, have access to Interntet, phone, printer

In order to apply and for additional information please contact us at work@XXXX.com

E-mail modtaget af DK•CERT, november 2010

at lokke brugere til at udfylde spørgeskemaer på nettet. Bagmændene får penge, hver gang en bruger besvarer et af skemaerne. De fleste af disse svindelnumre forsøger at lokke ofrene til med sensationelle overskrifter. I 2010 så vi blandt andet disse eksempler på lokkemad: "OMG! Look what happens when identical TWINS meet on Chat Roulette!" og "OMG!!!! Girl Caught by Dad While Making Video on Facebook"[66].

Svindlen med spørgeskemaer er ofte kombineret med *likejacking* og den tredje tendens: Skadelige applikationer. Det er Facebook-applikationer, som lokker med spændende funktionalitet. Vi har blandt andet set en applikation, der hævdede at udvide Facebook med en "Kan ikke lide-knap" og en anden, der lovede at kunne afsløre, hvem der har set på brugerens profil. Ingen af påstandene var sande. Formålet med dem var at lokke brugeren til at give en applikation adgang til at skrive på brugerens væg, sende mails eller på andre måder kontrollere data på brugerens Facebook-konto. Hvis det lykkedes, brugte applikationen sine nyvundne rettigheder til at skrive reklamer for sig selv på brugerens væg, så andre også kunne lokkes til at bruge den.

I starten af september var der to *sårbarheder*, som gav uvedkommende adgang til at skrive på andre brugeres vægge. Den første lå i Facebooks system til upload af fotos, mens den anden lå i den del, der administrerer applikationer. Begge sikkerhedshuller, er siden blevet lukket. Også beskedtjenesten Twitter har i årets løb haft sikkerhedsproblemer. I januar fandt en sikkerhedsforsker en *sårbarhed*, der kunne give uvedkommende adgang til brugernavne og passwords[67]. *Sårbarheden* menes ikke at have været udnyttet i praksis.

I september blev et hul i Twitter derimod udnyttet aktivt[68]. *Sårbarheden* gjorde det muligt for en angriber at afvikle kommandoer, hvis offeret førte sin mus hen over et link. Der blev skrevet en *orm*, som automatisk fik brugerne til at videresende en besked fra *ormen*. Twitter lukkede hullet efter nogle timer.

Hvor nogle trusler som fx Nigerianer mailen er af mere traditionel karakter, forstærkes en række tekniske trusler ved kendskabet til den menneskelige psyke, og vores lyst til at interagere i en social sammenhæng. I dette billede udnyttes vores søgen mod fælles referencer, hvad enten det er at læse om de samme kendisser eller benytte de samme applikationer, som den gruppe vi relaterer os til. De "syv dødssynder" står ikke længere alene som mulige angrebsvektorer. *Social engineering* er blevet et væsentligt middel til at udnytte vores nysgerrighed og den sociale kontekst hvori vi agerer.

4.6. Cyberwarfare og -terrorisme

Inden for industrispionage, efterretningsvirksomhed og tab af data har 2010 været et særdeles aktivt år. Særligt tre hændelser skabte røre i og uden for sikkerhedsverdenen. Angrebet på Google og andre, *Stuxnet* og WikiLeaks-affæren.

Året startede med den overraskende meddelelse fra Google, at virksomheden i december 2009 havde opdaget et særdeles omfattende angreb på dets infrastruktur fra computere i Kina. Mindst 20 andre store virksomheder viste sig

66 Sophos.com, 2010; *"Girl's sexy Facebook video is disguise for survey scam"*.

67 Techjaws.com, 2010; *"Twitter vulnerability discovered"*.

68 Twitter.com, 2010; *"All about the 'onMouseOver' incident"*.

også at være ramt. Angrebet der blev kendt under navnet Aurora, så ud til at have til formål at få adgang til Gmail-konti for kinesiske menneskerettighedsaktivister. Angrebet anvendte blandt andet en hidtil ukendt *sårbarhed* i Internet Explorer til at få adgang til ofrenes pc'er.

Som følge af angrebet tog Google firmaets politik i forhold til Kina op til revision og holdt op med at tilbyde censurerede søgeresultater til brugere i Kina[70]. I stedet blev brugerne henvist til Googles server i Hongkong. I juli indgik Google en ny aftale med den kinesiske regering og holdt op med automatisk at viderestille kinesiske brugere til Hongkong-serveren.

Også et andet højt profileret angreb anvendte hidtil ukendte *sårbarheder*. Det var *ormen Stuxnet*, der blev opdaget i juli og spredte sig ved blandt andet at udnytte en *sårbarhed* i Windows' behandling af genvejsfiler. Microsoft lukkede hullet med en ekstraordinær rettelse den 2. august. *Stuxnet* var dog også interessant af andre grunde. Det ser nemlig ud til, at den er sat i verden med det bestemte formål at finde og inficere en bestemt type industrikontrolsystemer fra Siemens. Efterforskningen har vist, at den er programmeret til at ændre på indstillingerne for en særlig type computerkontrolleret motor, der ofte bruges i centrifuger til behandling af blandt andet uran. En teori går derfor på, at formålet var at sabotere det iranske atomprogram. Irans præsident, Mahmoud Ahmadinejad, erkendte i slutningen af november, at *ormen* havde givet problemer for nogle af landets uran-centrifuger[71].

Organisationen WikiLeaks stiller websider til rådighed for folk, der ønsker at lække fortrolige dokumenter. WikiLeaks var flere gange i løbet af 2010 i medierne. Første gang var i april med offentliggørelsen af en video, der viste amerikanske soldater, som i 2007 dræbte to journalister fra Reuters i Irak[72]. Videoen menes at stamme fra en ansat i militæret, der også forsynede WikiLeaks med 260.000 hemmeligstemplede diplomatiske efterretninger fra den amerikanske udenrigstjeneste, der blev offentliggjort i slutningen af november.

Inden da havde WikiLeaks vakt opsigt med offentliggørelsen i juli af 92.000 hemmeligstemplede militære dokumenter om krigen i Afghanistan. Kilden til Afghanistan-dokumenterne er ikke kendt. Derimod er den tidligere ansatte i militæret anholdt i sagen om de diplomatiske efterretninger[73]. I kraft af sin stilling havde han adgang til store mængder hemmeligstemplet materiale, som han menes at have smuglet ud.

WikiLeaks' afsløringer førte til flere tiltag mod organisationen. Blandt andet nægtede nogle betalingsformidlere at betjene organisationen, hvilket førte til DDoS-angreb mod dem, der ikke ville samarbejde med WikiLeaks. Disse angreb kom blandt andet fra en gruppe, der kalder sig Anonymous[74]. Set fra en it-sikkerhedsvinkel handler WikiLeaks-sagen om flere elementer. Et af dem er beskyttelse af fortrolige data mod misbrug fra interne kilder. Det kaldes i fagsproget for DLP (*data leak prevention*). Et andet element er *DDoS*-angreb, og hvordan man beskytter sig mod dem.

69 Clarke, Richard A., 2010; *"Cyber war"*.

70 Wired.com, 2010; *"Google to stop censoring search results in China after hack attack"*.

71 Atlantic.com, 2010; *"Ahmadinejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges"*.

72 Wired.com, 2010; *"Whistleblower report: Leaked video shows U.S. 'Coverup'"*.

73 MotherJones.com, 2010; *"Alleged WikiLeaks video leaker arrested"*.

74 Metro.co.uk, 2010; *"MasterCard website taken down by pro-WikiLeaks anonymous hackers"*.

Cyberwarfare og -terrorisme

Cyberwarfare defineres som af Richard A. Clarke som:

"Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption". [69]

Definitionen bør dog tænkes videre og inkludere fx forsvar, informationsindsamling og spionage.

I denne kontekst vil vi opfatte cyberterrorisme som angreb foretaget af andre grupperinger end selvstændige stater med det formål at udstille eller destabilisere infrastrukturer og tjenester. Målet kan her være nationer såvel som organisationer.

Midlerne er i begge tilfælde alt fra *DDoS*-angreb over *malware* til egentlig hacking.

Mens ovenstående angreb fra et isoleret dansk synspunkt kan synes ligegyldige eller i værste fald som et bump på vejen, er de med til at tegne et billede af en ændret dagsorden med hensyn til brugen af it. Ikke blot nationalstater har oprustet og er klar til indsamling af information og angreb ved brug af it. Også mere eller mindre løse grupperinger er klar til at gøre deres særstandpunkter gældende ved brug af it. Det gælder, hvad enten sagen er retten til informationernes frie bevægelighed, eller hvad man i udvidet grad kunne kalde offentlighed i den globale forvaltning, generel uenighed om særstandpunkter, dyrevelfærd og meget andet. Alt sammen er muliggjort af værktøjer udviklet af organiserede it-kriminelle grupperinger, der mod betaling stiller deres services til rådighed.

Endnu har der ikke været dokumenterede angreb forårsaget af den virkelige verdens terrorister, der i løbet af 2010 flere gange herhjemme skabte overskrifter. Omtalen skyldes især anholdelser og mislykkede terror-angreb. Tidligere angreb på it-infrastrukturen i Estland, Georgien, Litauen og Burma har vist, at sådanne angreb kan være særdeles effektive og planlægges og udføres med langt mindre omkostninger og risici end traditionel terrorisme.

Konsulentvirksomheden Gartners vice-præsident Brian Gammage mener, at det blot er et spørgsmål om tid, før et større land bliver ramt af angreb. Han forudser, at et G20-lands kritiske infrastruktur inden 2015 vil blive lammet af cyber-terrorisme. I en artikel på Computer Weekly[75] opfordrer han således til, at virksomhedsledelsen laver fremadrettet planlægning, der blandt andet tager højde for angreb, der kan afbryde virksomhedsdriften. Tilsvarende mener han, at regeringerne bør gå mere effektivt ind i forberedelsen på at koordinere og besvare angreb på deres infrastruktur.

Truslen om it-kriminalitet og cyber-warfare udført af nationer, mere eller mindre organiserede professionelle og terrorister har i stigende grad gjort it-sikkerhed til et emne, der tages alvorligt på såvel nationalt som internationalt plan. Herhjemme er den nyoprettede *GovCERT*-funktion samt den mindre omtalte MilCERT et udtryk for dette. De nye trusler har dog også skabt en erkendelse af et behov for samarbejde på tværs af nationaliteter, sektorer, brancher og organisationer.

4.7. It-sikkerheden i 2010

Opgaven med at varetage organisationernes sikkerhed er gennem de seneste år blevet stadig mere kompleks. Fx har introduktionen af smartphones og tavle-pc'er introduceret nye platforme, som organisationerne skal risikovurdere og supportere. Samtidig stiller medarbejderne krav om at kunne benytte en række online services som fx sociale netværkstjenester, der også introducerer nye risici.

Når organisationerne tillige outsourcer og putter tjenester i skyen, er det med til at gøre trusselsbilledet mere diffust, end det tidligere har været.

En undersøgelse udført af Deloitte viser, at teknologi-, medie- og

Demokratiet under angreb

Op til Burmas første "demokratiske" valg den 7. november 2010 blev landets internet lammet af et *DDoS*-angreb. Angrebet startede den 25. oktober og afbrød internetforbindelse til resten af verden. Borgerne var herved afskåret fra udenlandske informationer, der kunne påvirke resultatet af valget. Heller ikke omverden kunne få informationer om valget i Burma, hvor udenlandske observatører og journalister er forment adgang[76].

Angrebet, der var større end de tilsvarende angreb på Estland og Georgien i 2007, bestod af flere forskellige typer DoS angreb, fra botnet computere i det meste af verden. Ingen har endnu taget ansvaret for angrebet. I betragtning af nedenstående advarsel fra regeringen er det dog ikke utænkeligt at landets militærjunta selv stod bag[77].

"Whoever uses computers, Internet, copiers and fax machines for the purpose of sending information to foreign media shall be punished by a maximum of 14 years imprisonment."[78]

75 Computerweekly.com, 2010; *"A G20 country will be hit by major cyber attack by 2015, Garter predicts"*.

76 Bbc.co.uk, 2010; *"Burma hit by massive net attack ahead of election"*.

77 Spectrum.ieee.org, 2010; *"Massive distributed denial-of-service cyberattack on Burma"*.

78 Irrawaddy.org, 2010; *"Regime reacts indifferently to cyber attack"*.

telekommunikations virksomheder i dag opfatter it-sikkerhed som et emne af strategisk betydning og ikke længere kun et emne med relevans for it-driften. Populært sagt kan man sige, at det er en forudsætning for at organisationerne varetager it-sikkerhed under strukturer af *god selskabsledelse*. It-sikkerhed er blevet en integreret del af det at lave forretning og betragtes gennem hele værdikæden. 44% af de adspurgte virksomheder svarede således, at de havde identificeret og vurderet deres forretningspartneres kompetencer og kontrolforanstaltninger med hensyn til it-sikkerhed. Mens 30% havde fuld tillid til it-sikkerheden hos deres forretningspartnere, havde kun 22% dog aktivt testet den[79].

Med forventningen om økonomisk vækst er udgifterne til it-sikkerhed ifølge Deloittes undersøgelse steget moderat i 2010. Det er dog tvivlsomt, om man er tilbage på niveauet inden den finansielle krise. 57% af virksomhederne mener, at man i bedste fald kun lige er up to date med de aktuelle trusler. 46% mener, at utilstrækkelige budgetter er den største barriere for organisationernes it-sikkerhed[79].

2010 blev året hvor en række finansielle institutioner herhjemme med PBS (nu Nets) i spidsen som værn mod *spam* og *phishing* implementerede *SPF (Sender Policy Framework)* på deres mailserver. De organisationer der tilsvarende har implementeret *SPF*, blokerer herefter mails afsendt fra mailservere, der i *SPF*-recorden ikke er angivet som autoritative for det pågældende domæne. Det gør det vanskeligere at udsende mails fra adresser under pbs.dk, da disse mange steder blokeres og aldrig når modtagerne, medmindre de rendt faktisk er udsendt af PBS.

I februar 2010 besluttede den danske regering, at alle statslige institutioner skulle overgå til den internationale sikkerhedsstandard *ISO 27001*. Det sker som led i regeringens handlingsplan for afbureaukratisering og vedligeholdelse af det offentliges brug af åbne standarder. I forhold til *DS 484* er ISO-standarden mere fleksibel og appellerer både til større og mindre organisationer. Hvorvidt skiftet skal ske nu eller først med næste revision af *ISO 27001*, er op til de enkelte myndigheder.

2010 blev også året, hvor flere centrale beslutninger med hensyn til danskernes it-sikkerhed udmøntede sig i konkrete tiltag. 1. juli gik en fælles dansk login-løsning til netbanker og offentlige hjemmesider i luften. *NemID* er en brugervenlig afløser for den digitale signatur, der aldrig rigtigt er slået igennem hos borgerne. *NemID* vil i forhold til de etablerede løsninger give forøget sikkerhed for både brugerne og bankerne. Også i forhold til de øvrige tjenester, der forventes at bruge *NemID*, vil løsningen tilbyde bedre beskyttelse mod misbrug af private oplysninger og data.

Efter en del kritik offentliggjorde IT- og Telestyrelsen på et informationsmøde den 8. marts 2010, at den danske *GovCERT*, også skal have informations- og varslingsaktiviteter rettet mod kommuner, regioner og visse kritiske sektorer. Ud over at alle offentlige institutioner nu kan benytte *GovCERT*, vil det således være muligt for telesektoren, elforsyningssektoren og finanssektoren at benytte tjenesten. Desuden gennemfører *GovCERT* i samarbejde med DK•CERT en varslings- og informationsindsats rettet mod borgere samt små og mellemstore virksomheder i et såkaldt nationalt CERT-samarbejde. Med etableringen af deres hjemmeside og offentliggørelse af den første situationsrapport[80] i slutningen af

79 Deloitte, 2010; *"2010 TMT global security survey – key findings"*.

80 Govcert.dk, 2010; *"Situationsbillede af sikkerhedstilstanden på den danske del af internettet Q4 2010"*.

december 2010 blev *GovCERT* en aktiv del af det danske it-sikkerhedsberedskab.

DK•CERT har flere gange tidligere påpeget, at it-kriminalitet er et fællesnationalt anliggende, som vi mener ISP'erne bør indgå aktivt i bekæmpelsen af. Den nyoprettede nationale *GovCERT*-funktion vil være et oplagt sted at placere ansvaret for at organisere og koordinere indsatsen.

Ifølge Dansk Industri var dette dog ikke vidtrækkende nok. Den 8. september fortalte organisationen i pressen, at man nu anså it-kriminalitet for så stort et problem, at den danske stat burde gå til angreb på de it-kriminelle. Særligt bekæmpelsen af *botnet* blev anset for et fællesnationalt anliggende. Dansk Industri foreslår en strategi, hvor man dels blokerer adgangen til inficerede sites, og dels hjælper brugerne, som er blevet inficeret. Dansk Industri foreslår, at der udpeges en offentlig myndighed som IT & Telestyrelsen, som i samarbejde med ISP'erne skal varetage opgaven[81].

I november søsatte EU-kommissionen en række nye tiltag mod it-kriminalitet. De skal blandt andet føre til bedre internationalt samarbejde i bekæmpelsen af it-kriminalitet. Inden 2012 skal alle EU-lande have en velfungerende CERT (Computer Emergency Response Team), og CERT'erne skal samarbejde på tværs af landegrænser. Til det formål oprettes et fælles center til koordinering af indsatsen i EU. Til at hjælpe med etableringen af centeret har Europol udarbejdet en trusselsvurdering af internet-kriminalitet, IOCTA (Threat Assessment on Internet Facilitated Organised Crime)[82]. Den venter, at EU-borgere og -organisationer vil blive udsat for flere angreb. Der vil også komme angreb fra egne af verden, som i dag har begrænset adgang til internettet.

Europol finder det afgørende, at myndighederne samarbejder med den private sektor. Det gælder såvel deling af information og bevismateriale som udvikling af tekniske hjælpemidler i kampen mod it-kriminaliteten. Og der er brug for en central koordinering af dataindsamling, analyse og uddannelse.

Globalt set bød 2010 på flere indgreb mod de store etablerede *botnet*. Først i begyndelsen af året, hvor *botnettet* Lethic blev lammet ved, at sikkerhedsfolk fra flere internetudbydere gik sammen om at sætte *botnettets* centrale kontrolservere ud af drift. Freden varede dog kun en måned. 11. februar blev Lethic vakt til live igen[83].

Den 22. februar fik Microsoft nedlagt fogedforbud mod en række domænenavne, som anvendes af *botnettet* Waledac. Ved at gå rettens vej gjorde firmaet det på den måde sværere for bagmændene at kommunikere med pc'erne i *botnettet*. Der har dog været uenighed om, hvor effektiv metoden er, når det ikke er de enkelte pc'er, der er inficeret med *botnet*-programmer, som bliver renset. Derfor var det en god nyhed, da Microsoft i oktober tog Zeus/Zbot med i Værktøj til fjernelse af skadelig software (MSRT). Efter en uge havde værktøjet renset næsten 275.000 pc'er for Zeus[83].

Også tre formodede bagmænd bag *botnettet* Mariposa blev i 2010 arresteret. Det skete i februar, men *botnettet* blev lukket ned allerede den 23. december 2009. Det menes at have inficeret 12,7 millioner computere i over 190 lande. På *botnettets* servere fandt politiet personlige data om 800.000 personer, herunder deres

81 Dr.dk, 2010; *"DI: Staten bør bekæmpe it-kriminelle"*.

82 DK•CERT, 2010; *"EU etablerer center mod it-kriminalitet"*.

83 Computerworld.dk, 2010; *"DK•CERT: 2010 stod i botnettets tegn"*.

netbanklogin og passwords til e-mail[84].

Botnettet Zeus vakte også i 2010 myndighedernes opmærksomhed. Omkring den 1. oktober blev operationen Trident Breach således gennemført i Storbritannien, USA og Ukraine. Mere end 100 personer blev arresteret. De mistænkes for at have brugt Zeus til at stjæle penge fra netbankkonti og misbruge kreditkort.

Endelig blev en mand, der menes at stå bag *botnettet* Bredolab anholdt i oktober i et samarbejde mellem hollandsk og armensk politi. Også dette *botnet* blev sat ud af drift[85]. Ligesom i de to øvrige sager har man sat ind mod de formodede bagmænd, og altså ikke kun mod underverdenens små fisk som fx de såkaldte *muldyr*.

4.8. It-chefens perspektiv på sikkerhed

Af Steen Pedersen, it-sikkerhedsansvarlig, DTU
Bestræbelserne på at opnå en samlet struktureret håndtering af begrebet informationssikkerhed på DTU startede i 2004 med brevet fra Ministeriet for Videnskab, Teknologi og Udvikling til alle statslige institutioner om at der nu skulle følges en fælles offentlig standard for informationssikkerhed, *DS 484*. Dette gav på DTU, gennem et betydeligt antal møder, anledning til etablering af dels en IT-sikkerhedsorganisation:

- IT-sikkerhedsforum, hvor alle institutter deltager med en ledelsesrepræsentant.
- IT-sikkerhed-teknik, hvor alle institutter deltager med en it-faglig person.

Samt til den første udgave af et sæt styrende dokumenter:

- Overordnet Informationssikkerhedspolitik – DTU 2006.
- Overordnede retningsliner for it-sikkerhed.
- Fælles regler – DTU 2007.

Politikken er godkendt af DTUs direktion, og de resterende dokumenter godkendes af IT-sikkerhedsforum.

Samtidig med denne mere formelle del blev der gennemført en konkret risikoanalyse for hver enkelt enhed, og der blev udarbejdet skabeloner for mere end 60 fælles procedurer og forretningsgange.

Alt i alt har indsatsen på næsten alle områder vist sig at være noget mere omfattende end antaget, og det har derfor taget længere tid at komme igennem de mange procedurer og dermed alle dele af standarden.

På DTU har vi i 2010 dels haft fokus på at afslutte den første gennemgang af de sidste punkter i standarden, der omfatter opstilling og afprøvning af beredskabsplaner, og dels er vi startet forfra på et nyt gennemløb af og hermed en justering og tilpasning af de styrende dokumenter. Der er gennemført en ny

84 Theregister.co.uk, 2010; *"Monster botnet held 800,000 people's details"*.

85 Computerworld.com, 2010; *"Dutch team up with Armenia for Bredolab botnet take down"*.

risikovurdering for alle enheder, og den overordnede informationssikkerhedspolitik er justeret og godkendt i direktionen her i efteråret. Denne gennemgang vil føre en del justeringer med sig, idet DTU dels har været igennem en fusionsproces, og dels har gennemført en øget koordinering og centralisering af væsentlige dele af IT infrastrukturen.

De konkrete hændelser der har fyldt mest i 2010, har været de stadig mere sofistikerede *phishing*-forsøg, der kulminerede den 4. oktober med en mail til en tilsyneladende udvalgt skare af brugere på DTU, der indeholdt originale grafiske elementer fra DTUs single-sign-on. Der blev brugt nogen tid på først at udskifte grafikfilerne, så det klart fremstod, at der var noget galt, på at aktivere it-sikkerhedsorganisationen til at informere om hændelsen, og på at følge op på de ganske få svar, der havde været på angrebet, idet sproget/stavning heldigvis ikke var på højde med layout og form.

Efter at have deltaget i it-sikkerhedsarbejdet i de seneste 5-6 år, er jeg efterhånden helt overbevist om, at den mere strukturerede, planlægnings- og tidskrævende tilgang til håndtering af informationssikkerheden ikke er et fænomen der går i sig selv igen. Det går ikke over. Det er blevet til faste møder i kalenderen, og det har også vist sig at disse krav om en mere formaliseret tilgang til beskrivelser af it-drift ud fra et it-sikkerhedsmæssigt udgangspunkt på mange måder spiller rigtig fint sammen med andre værktøjer og metoder til professionalisering af en it-organisation, fx ITIL (Information Technology Infrastructure Library).

Ud over tilpasning af dokumenter og procedurer så de kan holde trit med udviklingen i organisationen, er der mange andre grunde til, at dette område konstant bringer sig selv i fokus. Den teknologiske udvikling bringer en lind strøm af nye "gadgets", der er fikse og smarte til at håndtere/tilgå informationer på helt nye måder, som ingen havde tænkt var mulige, og som med stor sikkerhed ikke er beskrevet tilstrækkeligt i den gældende informationssikkerhedspolitik.

Informationssikkerhedsarbejdet er kommet for at blive, og det er ved at finde sit naturlige leje i organisationen. Resultaterne fra penetreringstesten fra Forskningsnet-CERT og den årlige "eksamen", IT-revisionen i forbindelse med den finansielle revision, bliver stadig mere omfattende og krævende, og så skal vi for resten også skifte fra DS til ISO,- man kommer ikke til at kede sig.

4.9. GovCERT – den nye dreng i klassen

Af Thomas Kristmar, GovCERT
Regeringen besluttede i maj 2009 at etablere en dansk *GovCERT* under IT- og Telestyrelsen i Videnskabsministeriet. Efter etableringsfasen har *GovCERT* i efteråret 2010 været i pilotdrift og er nu fuldt funktionsdygtig.

GovCERT dækker som udgangspunkt statslige myndigheder. Derudover vil regioner, kommuner og visse private virksomheder der beskæftiger sig med kritisk infrastruktur, kunne indgå i et samarbejde med *GovCERT*.

Et af de produkter, som *GovCERT* leverer, er et situationsbillede for, hvad man kan kalde "den danske del af internettet". Gennem analyse af hændelser på de forbindelser, som en række danske offentlige institutioner har til internettet, sammenholdt med informationer fra andre kilder både fra indland og udland, skabes et afbalanceret og verificerbart situationsbillede.

Den væsentligste trend i *GovCERT*'s situationsbillede fra 4. kvartal 2010 er, at effektiviteten af antivirus er faldende. Selv opdaterede antivirusprogrammer kan relativt let omgås, som situationen er i dag. Den traditionelle kombination af beskyttelsesforanstaltninger, såsom antivirus, firewalls og regelmæssige opdateringer, kan ikke i sig selv garantere, at angreb afvises.

Det betyder, at offentlige og private virksomheder bør overveje, om beskyttelsen af net forbundet til internettet opfylder organisationens behov. I første omgang bør it-sikkerhedsansvarlige stille to spørgsmål til forretningen: Hvad er konsekvensen, hvis en pc på det interne net overtages og benyttes til at trække dokumenter, mails og regneark ud af organisationen? Og hvor stor en risiko vil forretningen leve med?

For de fleste organisationer er situationen nok den, at for hovedparten af informationen vil det være "ærgerligt", men ikke kritisk. Meget information kan jo være offentliggjort i forvejen eller forældet.

Men for mindre dele af informationer vil læk være kritisk. Det kan dreje sig om følsomme personoplysninger eller andre typer fortrolige dokumenter. Det oplagte spørgsmål er: Hvorfor lagres disse informationer med samme beskyttelse som ikke-kritisk information?

Inden man køber sig fattig i *Data Leakage Prevention* produkter, er det nærliggende at overveje, om man som organisation kan opfylde beskyttelsesbehovet for sikring af kritisk information ved at klassificere informationen, altså at markere informationen som særlig beskyttelsesværdig og holde den væk fra arkiver, hvor alle i organisationen har adgang.

Uanset valg af løsning bør det overvejes, om ikke 2011 er året, hvor organisationen implementerer informationsklassifikation og tilpasser beskyttelsen af information efter informationens følsomhed. "One-size-fits all" tilgangen til beskyttelse af information er ikke længere effektiv.

5. Et kig ind i fremtiden

En ting er hvordan det ser ud lige nu, en anden er, hvilke trusler vi i fremtiden vil blive nødt til at forholde os til. Vi vil her forsøge at give vores bud på, hvordan it-kriminaliteten vil udvikle sig i de kommende år, og hvilke heraf afledte udfordringer vi kommer til at stå over for. En ting er sikkert, det bliver ikke lettere.

Gennem de seneste år er de transnationale organiserede grupperinger, der i dag udfører de større angreb, vi ser på danskernes it-sikkerhed, blevet stadig klogere og dygtigere. I dag arbejder de forskellige grupperinger sammen og deler værktøjer og data. Mindre dele af større *botnet* sælges eller udlejes ifølge virksomheden BitDefender på projektbasis, hvorefter andre it-kriminelle benytter dem til deres egne forehavender som fx udsendelse af *spam*, dataindsamling, *DDoS*-angreb eller lignende[86]. Gennem hele forsyningskæden er der sket en specialisering, således at succesraten for de meget målrettede angreb, vi gennem de seneste år har set, er stadig stigende. Desværre vil det nok altid være således, at vi der forsøger at beskytte danskernes it-aktiver, vil halse efter den udvikling, vi ser initieret af de it-kriminelle.

Heldigvis har vi ikke ligget på den lade side. It-branchen, de danske organisationer og vi, der forsøger at skabe forøget sikkerhed er også blevet klogere. En række nye tiltag både herhjemme og i udlandet giver forøget håb. Tilsvarende giver øget dialog forhåbning om mere samarbejde. På sigt tror vi også at lovgivningen bliver tilpasset de trusler vi oplever. Alt i alt mener vi, at vi i fremtiden bliver bedre i stand til at reagere på truslen fra it-kriminalitet.

I dette afsnit forsøger vi at konkretisere de it-kriminelles større opfindsomhed, målrettethed og specialisering i nogle overordnede scenarier for fremtiden. Efterfølgende beskriver vi de udfordringer, det vil medføre, når vi som borgere, organisationer og samfund vil beskytte vores aktiver mod it-kriminalitet. Endelig lader vi Henning Mortensen fra Dansk Industri ITEK beskrive organisationens visioner for, hvordan vi herhjemme kan bekæmpe truslen fra *botnet*, som globalt set er et væsentligt problem.

5.1. It-kriminalitetens udvikling

Indførelsen af *NemID* gør det ikke længere muligt at aflure og senere udnytte adgangen til danskernes bankkonti. Vi har dog tidligere set målrettede angreb på de danske netbanker, hvor *trojanske heste* placerede sig som man-in-the-middle og derved overtog en aktuel session mod netbanken. Sådanne angreb vil vi se flere af i fremtiden. Den *trojanske hest*, der blot passivt aflurer kontoinformationer, har dog langt fra udspillet sin rolle. Det er blot adgangen til andre tjenester end netbank, som er interessante. Fx gemmer mange netbutikker, betalingssider og onlinespil brugernes kreditkortinformationer. Adgang til en konto på Apples musiktjeneste iTunes gør det fx muligt at hente musik, uden selv at skulle have kreditkortet frem. Vi tror, at bankernes øgede fokus på sikkerhed vil flytte aktiviteten mod sådanne tjenester. Derudover er kreditkortinformationer selvfølgelig stadig attraktive ligesom adgangen til Gmail, Facebook osv. Alle informationer har i dag en værdi.

86 Bitdefender.com, 2010; *"H1 2010 E-threat landscape report"*.

Det primære motiv for spredningen af *malware* vil fortsat være at skaffe sig adgang til borgernes eller organisationernes fortrolige data. Vi tror derfor at *trojanske heste* og *botnet*-programmer også i fremtiden vil være de hyppigst distribuerede *malware*-typer. Ud over sårbare legale webapplikationer og P2P-netværk vil spredningsmediet i stigende grad være tredjepartsapplikationer på sociale netværkstjenester, smartphones og tavle-pc'er. Det gælder både applikationer, som er udviklet til formålet og spredes via de almindelige kanaler, Android Market og Apple App Store, og sårbare legale applikationer. Brugerens tillid til mobilmediet og de sociale netværkssteder spiller en væsentlig rolle i forsøget på at kompromittere brugerens sikkerhed, data og identitet.

Vi så ikke i 2010 væsentlige angreb, der var målrettet mod Windows 7. Mange organisationer har i dag implementeret denne nye platform, og flere vil komme til. Med større udbredelse kan den ligesom den nye HTM 5-standard blive et attraktivt mål for de it-kriminelle, der vil finde nye måder at udnytte den på. Vi vil se *sårbarheder* i både Windows7, HTM 5 og måden standarden implementeres på i browserne, som vil blive udnyttet strategisk i forhold til fx Microsofts fastlagte opdateringsdage. Det kan medføre udviklingen af nye *trojanske heste*, *botnet*-programmer, *orme* eller andet utøj.

Stuxnet satte i 2010 nye standarder for, hvor målrettet og avanceret *malware* kan blive. I dag er koden ude, og andre kan genbruge den eller blot benytte den som inspiration for deres egne projekter. Vi tror at udviklingen fortsætter med mere målrettet og avanceret *malware* til følge.

Ud over *spam*, *phishing* og *malware*-distribution tror vi, at højt specialiserede *botnet* vil blive benyttet til *DDoS*-angreb, som dem vi sidst på året så rettet mod de organisationer, der ikke længere ønskede at samarbejde med WikiLeaks. Disse angreb viste tilgængeligheden af metoder og teknologi, som kan gøre det attraktivt for andre. Vi tror derfor, at også andre typer af organisationer kan blive mål for sådanne angreb. Enten efter foregående afpresning, som vi tidligere har set mod online casinoer, eller fordi man er uenig med den måde de tænker eller agerer på.

Aurora-angrebet mod bl.a. Google peger på en anden tendens, vi kommer til at mere til: Angreb målrettet enkeltpersoner eller organisationer. *Social engineering* bliver et stigende element af internetkriminaliteten. Det kan være i form af e-mails, der angiver at komme fra personer, som modtageren har tillid til, og som indeholder information, kun den rette afsender burde kende. Ved at bruge informationsstjælende programmer som fx Zeus og SpyEye kan bagmændene skaffe sig oplysninger, der gør deres henvendelser mere troværdige. Vi har derfor en forventning om, at vi kommer til at se flere, mere målrettede og udspekulerede måder at manipulere borgerne på for at få dem til at købe varer, de ikke har brug for, hente og installere *malware*, selv aflevere fortrolige oplysninger og lignende. Angreb vil ikke krydse nationale og sproglige barrierer, og *malware* placeret på danske webapplikationer vil være målrettet indsamling af data fra danskere.

Undergrunden samler kræfterne. Den forestående fusion af Zeus og SpyEye er kun et eksempel på, at de kriminelle går sammen og bliver mere professionelle. I flere år har vi kendt til, at organiserede bander uden for hackermiljøet er blevet en del af den digitale undergrund. Vi har en forventning om at den kriminelle undergrund i stigende grad vil forsøge at holde deres aktiviteter skjult. Det betyder mindre, men til gengæld mere målrettede angreb, men også udbredt brug af kryptering, forplumring af kode, avancerede algoritmer til kodegenerering og -opdatering samt hosting i *botnet*, der benytter sig af *fast flux*-teknologi. Flere

unikke mutationer af samme kode betyder, at antivirus-producenter og lignende skal opdatere og vedligeholde stadig flere *malware*-signaturer. Alt i alt medfører det, at kun en mindre andel af ny *malware* kan opdages og bekæmpes med stigende succesrate som resultat.

Udviklingen har vist, at der i dag er et undergrundsmarked for alle typer informationer. Den kriminelle undergrund har specialiseret sig gennem hele forsyningskæden, således at nogle leverer værktøjerne, andre bruger dem til at skaffe informationer, som andre igen misbruger. Denne tendens vil sandsynligvis fortsætte. Allerede i dag kan man købe sig til *DDoS* as a service, og mon ikke også man kan forestille sig, at *malware* på lignende vis udbydes som en service? Ved en sådan forretningsmodel vil de der udvikler og udbyder *malware*, ikke have samme indtjeningspotentiale, til gengæld er risikoen minimal.

Flere forbrydelser vil tage udgangspunkt i sociale netværk. Brugerne af tjenester som Facebook har en tillid til hinanden, som de kriminelle kan misbruge. Det vil typisk være i form af svindel, hvor en bruger fx narres til at sende penge til en nødstedt ven – hvis konto senere viser sig at være hacket. Vi tror også, at de sociale netværkstjenester vil give anledning til flere hændelser vedrørende brud på ophavsretten og privatlivets fred, samt være en væsentlig kilde til identitetstyverier og spredning af *malware*. En kilde til dette kan meget vel være sårbare legitime tredjepartsapplikationer, der deles og benyttes på disse netværk.

Den traditionelle pc er ikke længere den eneste type apparat på internettet. Stadig flere anvender mobiltelefoner og andre lignende enheder. De vil også være i forbrydernes søgelys i jagten på nye metoder til at svindle og stjæle. I fremtiden må vi derfor vente skadelig software og svindelforsøg, der spredes via smartphones, tavle-pc'er, net-opkoblede fjernsyn og andet udstyr. Allerede i 2010 så vi eksempler på *malware* til smartphones, der havde til formål at sende overtakserede SMS'er. Det kommer vi nok til at se mere til ligesom *spam* og *malware* spredt fra mobiltelefoner til sociale netværkssteder. Har man i dag adgang til en smartphone, er der jo ofte også adgang til mailkonti og sociale netværkssteder via applikationer, der lagrer brugernes login-data.

Det er vigtigt at gøre sig klart, at de it-kriminelle altid vil være foran, da de ofte i forvejen kan planlægge angreb, der er tilpasset aktuelle begivenheder. It-kriminalitet vil derfor vedblive at være en god forretning. Da vi ikke på forhånd kan sige hvor og hvordan den rammer, vil vores bedste værn være årvågenhed. I dette perspektiv er det væsentligt, at vi formår at samarbejde og kommunikere de risici og trusler, vi oplever lige nu og her, således at vi kan imødegå dem.

5.2. Fremtidige udfordringer

Malware udgør i dag den største trussel mod it-sikkerheden hos både borgerne, organisationerne og i samfundet. *Malware*-producenterne sender en lind strøm af stadig mere avanceret *malware* efter os, som fx antivirus-producenterne har stadig vanskeligere ved at opdage og bekæmpe. Danmarks engagement i fx Afghanistan har gjort koordinerede *botnet* angreb mod vores infrastruktur til en nærværende trussel, ligesom borgernes og organisationernes data er i potentiel fare, blot vi surfer på nettet. At bekæmpe denne trussel er en væsentlig udfordring for de kommende år, som vi mener ikke kan løses af borgerne eller organisationerne alene. Hvordan vi som samfund kan dæmme op for denne trussel allerede på ISP'ernes netværk uden at krænke borgernes privatliv, står stadig til diskussion.

Oprettelsen af den nationale *GovCERT*-funktion kan dog være et skridt i retning af fælles koordinering af indsatsen.

Ud over implementering af traditionelle værktøjer til filtrering af *virus*, *spam*, *malware* og lignende har de større organisationer en udfordring i at opdage og afværge de stadig mere målrettede og avancerede angreb. De tider hvor *malware* hovedsageligt kommunikerede via IRC kanaler på dedikerede høje porte er ovre. Hvad der i logfilen kan ligne en legal trafikstrøm, kan således i dag ligeså godt være et forsøg på en kriminel handling. I dag har bl.a. stigende lagerkapacitet og øget maskinkraft muliggjort værktøjer til realtidsanalyse af data fra mange kilder, således at det er muligt at genkende mønstre, der tidligere ville være overset. I kombination med fx IPS (Intrusion Prevention Systemer) på netværket giver det mulighed for at afværge igangværende hændelser, efterforske tidligere og igangværende hændelser samt i forhold til revisionen at kunne påvise, hvilke hændelser organisationen er udsat for.

Data er den nye form for global møntfod. 64% af it-sikkerhedsadministratorerne i en global undersøgelse foretaget af Checkpoint frygter, at væksten af mobile medarbejdere vil medføre tab af virksomhedskritiske data[87]. Alle typer af data har sin pris, og også 2010 bød på historier om fortrolige data, der i udlandet blev enten lækket til pressen eller stjålet med misbrug for øje. Ifølge EU's statistikkontor Eurostat er dette dog hovedsagelig et udenlandsk problem, da ingen danske organisationer i en undersøgelse angav, at de i 2009 havde fået offentliggjort fortrolige data[88]. Der er dog ingen garanti for, at det i fremtiden også vil være sådan.

"In many cases, data loss is about good employees making bad mistakes."[89]

Mens det er de eksterne trusler der får størst opmærksomhed, er de interne trusler med stigende brug af mobile enheder, trådløse netværk og sociale medier større end nogensinde. Størstedelen af de datatab vi hidtil har set, skyldes da også fejl begået af medarbejderne. Hvad enten fejlen var, at en medarbejder glemte ukrypterede data på en bærbar pc, sendte dem til en forkert e-mail-adresse, eller med fuldt overlæg lækkede dem på WikiLeaks, er tab af data en udfordring, vi bliver nødt til at forholde os til. Prisen for tab af data kan nemlig være langt større end værdien af de tabte data. Således tror vi, at kryptering og systemer til *Data Leak Prevention* (*DLP*) vil vinde større indpas, også i de mindre organisationer. De største udfordringer bliver her at definere de centrale politikker, der er grundlaget for overvågning og beskyttelse af data i *DLP*-installationen.

Særligt i forhold til mobile platforme kan det være vanskeligt at sikre sig mod kompromittering og tab af data, da det her er vanskeligere at kontrollere, hvilke applikationer brugerne henter og benytter, samt hvorvidt styresystem og applikationer bliver opdateret. Fx viste en statistik fra applikationsudvikleren Bump, at 89,7% af brugerne af Bump til iPhone anvender den nyeste version af styresystemet, iOS 4. 10,3% anvender version 3. Derimod er det kun 0,4% af Android-brugerne, der er på den nyeste version af dette operativsystem[90].

87 Version2.dk, 2010; *" 7 gode råd: Sådan får du styr på mobilsikkerheden".*

88 Eurostat, 2010; *"Information and communication technologies in the EU27s".*

89 Websense.com, 2010; *"2010 threat report".*

90 T3.dk, 2011; *"IDevice-brugere opdaterer flittigst deres iOS"; www.t3.dk/idevice-brugere-opdaterer-flittigst-deres-ios.*

Mens det er naturligt at begrænse medarbejderne på deres arbejdsstationer, vil det være vanskeligt at overbevise brugerne om det fornuftige i, at de ikke selv må eller kan installere applikationer på deres smartphone eller tavle-pc. På mange områder er det jo netop styrken ved disse enheder, der bl.a. er skabt til afvikling af mindre spil. Den centrale kontrol med de mobile enheder, som vi kender fra de traditionelle pc'er, udfordres således af de mobile platformes nye muligheder og brugernes krav om at udnytte dem.

Styresystemerne Android fra Google og iOS til Apples iPhone har hver sin sikkerhedsmodel. Applikationer til iPhone kan kun hentes fra Apples App Store. Programmerne her skal tjekkes af Apple, før de kan hentes. Dermed har brugerne en vis grad af sikkerhed for, at der ikke skjuler sig ubehagelige overraskelser i applikationerne. Googles Android har også en central markedsplads, Android Market. Men her er der ingen kontrol med indholdet. Der er da også set adskillige skadelige programmer på Android Market. Til gengæld har brugeren en større frihed til at vælge, hvad der skal installeres på telefonen. Men med den frihed følger ansvaret for selv at tjekke, at sikkerheden er i orden[91].

At håndtere denne forskellighed kan være en udfordring, hvis organisationen ønsker at benytte sig af begge platforme. Under alle omstændigheder gælder det om at risikovurdere de enheder, der benyttes, og sørge for at der udfærdiges politikker på området. Fx bør man som minimum sikrer sig at, der implementeres procedure der sikre, at adgangen til de mobile enheder er beskyttet med login, samt at data er krypteret. Derudover bør man overveje, om følsomme data overhovedet skal kunne overføres til de mobile enheder, eller om de kan gøres tilgængelige på anden vis.

Også brugen af sociale netværkstjenester udgør en udfordring for organisationerne, hvad enten de bruges som del af organisationens kommunikation eller ej. Politikker om hvem der fx til pressen må udtale sig om hvad, hvornår og hvorfor er almindeligt accepteret, mens tilsvarende ikke eksisterer for brugen af de sociale netværkstjenester. Ofte omhandler politikkerne kun, om man må benytte dem til private formål i arbejdstiden. Facebooksagen med en nu tidligere kommunikationsmedarbejder i Venstre viser dog, at det kan være vanskeligt at adskille individet fra den organisation, man er ansat i. Mange organisationer har i dag ikke taget stilling til medarbejdernes brug af fx Twitter og Facebook, hvad enten det er i arbejdstiden eller derhjemme. Ud over at disse medier benyttes til spredning af *spam* og *malware*, kan informationer der eksponeres her, også ofte benyttes til at skaffe sig viden om organisationen og dens medarbejdere, der kan bruges ved *social engineering*.

Cloud computing er ikke længere blot en teoretisk mulighed. Det er muligt at køre sine applikationer fra skyen, hvad enten der er tale om kontor- eller webapplikationer, og mange organisationer benytter i dag *cloud* services. Tilsvarende er det muligt at placere hele systemer eller infrastrukturer hos en *cloud*-udbyder. Brugen af *cloud computing* byder dog på en række udfordringer, man bør være sig bevidst. Særligt behandlingen af data kan i forhold til lovgivningen være et problem, som det ifølge ENISA kan være nødvendigt at tage højde for[92]. Derudover kan der selvfølgelig være forhold, der gør, at brugen af *cloud computing* er i direkte modstrid med organisationens egen it-sikkerhedspolitik eller de standarder, som organisationen følger.

91 DK•CERT, 2010; *"Vil du være fri eller sikker?"*.

92 ENISA, 2009; *"Cloud computing: Benefits, risks and recommendations for information security"*.

Vi tror, at *cloud computing* vil være med til at sætte organisationernes leverandør- og samarbejdsrelationer i fokus. Generelt bør man være opmærksom på de kontrakter, der indgås med organisationens leverandører. Det handler om at stille krav til de ydelser, man ønsker, og så indgå i dialog og samarbejde om opfyldelsen af dem. Det kan selvfølgelig være vanskeligt, hvis leverandøren er placeret i fx USA, har 1.000 gange flere medarbejdere og betragter jeres ordre som økonomisk til at overse. Dette er desværre stadig virkeligheden for mange *cloud*-udbydere.

Selv om mange organisationer i dag benytter de samme platforme og systemer, implementeres, tilpasses og benyttes de ofte forskelligt som resultat af organisationernes forretningsprocesser. Når man tilsvarende har forskellige krav til fx fortrolighed og medarbejdernes ageren, betyder det, at der ikke er nogen fælles løsning, der dækker alles behov. Denne tanke ligger jo også i, at det er udformningen af it-sikkerhedspolitikken, der er standardiseret, og ikke indholdet. Der er vel ingen, der kan forestille sig, at man uden at ændre andet end organisationens specifikke navne og betegnelser blot kopierede indholdet fra en anden organisation. Vi mener derfor, at der ligger en udfordring i at bruge ressourcerne på de punkter, hvor organisationens krav er unikke, mens man bør styrke samarbejdet omkring de mere generelle løsninger. At dyrke forskellen og styrke samarbejdet bør således være midlet til at få mest mulig sikkerhed for pengene.

Ifølge en international undersøgelse havde 54% af organisationerne på tværs af brancher igangsat *awareness*-aktiviteter for deres ansatte[93]. Herhjemme formodes dette tal at være mindre, særligt i de mindre organisationer. *Awareness* aktiviteter og uddannelse af medarbejderne bør dog prioriteres højt og indgå som et centralt anliggende for organisationen. I dette perspektiv kan rammerne for *god selskabsledelse* tjene som middel til at synliggøre it-sikkerhed som et centralt anliggende for organisationen. Inddrag medarbejderne i processen med at sikre organisationens it-aktiver, det er trods alt dem, som ved, hvordan de benyttes.

Danske organisationer og borgere er i dag under angreb fra mange sider. Netop borgerne, der sjældent har hverken tilstrækkelig viden eller ressourcer, indgår som en væsentlig del af problemet. Større forbundenhed og sammensmeltning mellem arbejdsliv og fritid betyder, at kompromittering af sikkerheden ét sted kan have indflydelse på sikkerheden et helt andet sted. Der ligger således en væsentlig udfordring i at tænke it-sikkerhed i helheder, der både inddrager borgerne, organisationerne og samfundet. Organisationerne har her en central rolle, da deres ansatte også optræder som privatpersoner og samfundsborgere. Pointen er her, at medarbejderne tager deres viden om risici og trusler med sig, når de agerer derhjemme eller i det offentlige rum. Risikoen for at organisationens sikkerhed kompromitteres på grund af manglende sikkerhed på enheder som står uden for organisationens rækkevidde minimeres, hvis medarbejderen har grundlæggende viden og forståelse for hvordan de agerer sikkert.

Udviklingen udfordrer de dogmer, hvorunder vi hidtil har tænkt it-sikkerhed. Vi mener at man herhjemme bør tænke fornyelse i helheder, hvor der stilles krav til både borgerne, organisationerne og den måde, vi organiserer beskyttelsen på. Vi mener, at tiden kalder på mere samarbejde. Ikke kun om hvordan vi beskytter mod den aktuelle it-kriminalitet, men også hvordan vi gør det i fremtiden uden at krænke borgernes privatliv. Hvorfor, hvordan og hvem der har ansvaret, står endnu til debat.

93 Deloitte, 2010; *"2010 TMT global security survey – key findings"*.

5.3. Fremtidens botnet-bekæmpelse i Danmark

Af Henning Mortensen, chefkonsulent, DI ITEK
Botnet er blandt de væsentligste trusler mod informationssamfundet, og der er derfor behov for at samle kræfterne om at bekæmpe dette onde. Det er ifølge Dansk Industri nødvendigt med en national strategi, som satser på mange forskellige løsninger, fordi ingen enkeltstående løsning alene kan dæmme op for problemet.

Når *botnet* er så vanskelige at bekæmpe, skyldes det, at de kriminelle bagmænd har store økonomiske incitamenter til at lave teknisk avancerede løsninger, der gør det svært at opspore dem. Ved at sprede skadelig kode kan bagmændene få kontrol over et utal af computere, som kan fjernstyres. Disse computere kan lejes ud til fx at udsende *spam*, få webservere til at gå ned (*DDoS*-angreb) og afpresning. *Botnet*-programmer kan også bruges til at skaffe sig adgang til personlige informationer fra den computer, der er inficeret. Typisk kan man indsamle logins til forskellige services, fx en World of Warcraft-konto, eller få opsnappet et kreditkortnummer og udløbsdato. Disse informationer kan sælges. Der er altså betydelige økonomiske incitamenter for bagmændene til at udvikle avancerede *botnet*-programmer. Samtidig er bagmændene svære at bekæmpe. Dels fordi det er teknisk svært at identificere dem. Dels fordi problemet er internationalt og typisk kræver et godt samarbejde mellem politienheder i mange forskellige lande med hver deres lovgivning. Bagmændene bag har altså en relativt lille risiko for at blive fanget.

Botnet kan også bruges til at angribe infrastruktur i forbindelse med politisk aktivisme. Dette er set fx ved angrebet på Estland i 2007 og angrebene på VISA og Mastercard i forbindelse med deres blokering af frivillige bidrag til WikiLeaks i slutningen af 2010. Også Danmark har været ramt, idet blandt andet Jyllands-Postens hjemmeside blev angrebet i forbindelse med den såkaldte tegningesag, der ledte til Muhammed krisen.

For at imødegå truslerne fra *botnet* er det nødvendigt at iværksætte korrigerende tiltag. Udgangspunktet er at undgå, at en computer overhovedet inficeres med *botnet*-programmer. Først og fremmest kan man tage de sædvanlige initiativer, som kan dæmme op for mange sikkerhedstrusler. Man bør således sikre sig, at alle programmer er opdateret, installere en sikkerhedspakke, som blokerer skadeligt indhold, og som skanner lagermedier med videre. Endelig bør man udvise en fornuftig adfærd og lade være med at installere programmer, man ikke kender til, klikke på links i *spam*, osv.

Botnet er imidlertid typisk teknisk ganske snilde, og man kan sagtens blive smittet, selv om man udviser en fornuftig adfærd, opdaterer programmer og installerer sikkerhedspakker. Derfor er der behov for flere initiativer. DI ITEK har anbefalet, at der laves en national strategi på området. En sådan strategi bør adressere:

- **Myndighedsgodkendt frivillig DNS-filtrering:** Fra internetudbydernes side kan man blokere adresser på internettet, som myndighederne har valideret indgår i et *botnet*s infrastruktur.
- **Bevidsthed hos ejere af hjemmesider:** De der ejer og driver websider, bør sikre sig, at deres servere er opdaterede, at der jævnligt skannes for skadelig kode på serverne, og at servernes trafikmønster, som er logget, gennemgås.

DI ITEK

DI (Dansk Industri) er erhvervslivets organisation for 10.000 medlemsvirksomheder. DI arbejder målrettet for at påvirke politiske beslutninger, der har indflydelse på virksomheders muligheder for at skabe vækst og arbejdspladser.

DI ITEK er et tværgående branchefællesskab i DI, der varetager DI's interesser på det it- og telepolitiske område. DI ITEK agerer både politisk og fagligt og varetager branchens interesser over for regering, Folketing og offentlige myndigheder og over for DI's øvrige medlemmer.

- **Reduktion af spredning gennem e-mails:** Man kan sikre sig, at afsendere af e-mails skal verificere sig over for internetudbydernes mailservere. Generelt bør internetudbyderne styrke deres internationale samarbejde.
- **Walled garden:** Brugerne på nettet, som vurderes at været smittet af et *botnet*-program, kan placeres i et afgrænset netværk og der få hjælp til at komme af med den skadelige kode.
- **Supplerende tiltag:** Trafik kan analyseres for at se, om der er mønstre, der indikerer *botnet*-aktivitet, man kan arbejde med serviceudbyderes "ry og rygte", fælles opdateringsservice for al software og endelig en forbedring af politimyndighedernes internationale samarbejdsmuligheder.

Man kan også forestille sig, at den nationale strategi består af andre elementer. Imidlertid er det helt centralt at holde sig for øje, at man fortsat skal respektere privatlivets fred hos de potentielle ofre for *botnet*-programmer. Derfor vil der også være en grænse for, i hvilket omfang man kan gribe ind på en privat computer. Denne grænse er og skal fortsat være reguleret ved lov.

Som nævnt er der store økonomiske incitamenter for de kriminelle bagmænd til at udvikle *botnet*. Vi må derfor også forvente, at de med tiden vil forsøge at omgå de initiativer, som er skitseret i det, der bør være en national strategi. Særligt er der en forventning om, at de adresser på nettet, som er en central del af *botnettets* infrastruktur, vil benytte sig af *fast flux*-teknologi og dynamisk rykke rundt. Det kalder på, at vi hele tiden skal være parate med nye korrigerende initiativer. Derfor bør der iværksættes forskningsprojekter, som vurderer de langsigtede udviklingstendenser og kommer med forslag til fremtidens løsninger.

6. Opsamling

Kigger vi tilbage på året der er gået, kan vi konstatere at flere af sidste års forudsigelser for 2010 ikke er gået i opfyldelse, eller ikke er gået i opfyldelse endnu. Heldigvis for det. Mens det således kun er nogle af vores forudsigelser for 2010, der figurerer på listen over de faktiske tendenser, vi har kunnet se, har vi til gengæld oplevet angreb, som vi ikke var i stand til at forudsige. Sådan vil det nok også gå med vores forudsigelser for 2011.

Mens vi i de tidligere afsnit har beskrevet enkeltstående begivenheder og data, samler vi her op og beskriver de væsentlige overordnede tendenser, som vi har kunnet se i 2010. Flere af disse tendenser er ikke nye og fælles for dem er, at de også vil præge den fremtidige udvikling med hensyn til it-kriminalitet og -sikkerhed. It-kriminalitet er nemlig stadig en god forretning for organiserede transnationale grupperinger, der opererer stort set uden lovgivningens bevågenhed fra lande i Afrika, Asien og den tidligere sovjetblok.

Fra et overordnet perspektiv kan man sige, at der ikke er meget nyt på bedding. De it-kriminelle bliver stadig mere professionelle og målrettede. Hvad vi så forrige år, var også, hvad vi så i 2010 og er sikkert også hvad vi kommer til at se de kommende år, dog bredt ud over flere platforme og teknologier. Således tror vi, at den større diversitet i platforme, hvor fx også smartphones og tavle-pc'er er mål for angreb, medfører, at flere angreb vil flyve under sikkerhedsteknologiernes radarer. Denne tendens forstærkes ved mindre angreb, som i større grad er målrettet ofret, bl.a. ved en stigende brug af *social engineering*. I fremtiden forestiller vi os, at de data vi selv lægger ud på fx sociale netværkssider, bliver benyttet til at nå bag vores mentale forsvarsværker.

I det hele taget tror vi, at sociale netværkssider vil blive et stadig vigtigere medie for indsamling af data og spredning af *malware*. De fleste af os har på fx Facebook opbygget en anselig vennekreds, hvoraf det kun er de færreste, vi kender. Vi tror, at denne falske tillid vil blive (mis)brugt til fx at målrette *spam*, sprede *malware* og lignende. Det kan jo være svært at modstå en anmodning om at besøge en hjemmeside eller prøve en sjov applikation, når nu den kommer fra en ven. Dette så vi allerede i 2010.

Tilsvarende har vi en forventning om at udbredelsen af HTML 5, vil give anledning til nye angreb. I takt med udbredelsen af iPhones og iPad, der ikke understøtter Flash, er brugen af HTML 5 til visning af videoer på nettet steget eksplosivt i 2010. Det giver grobund for angreb, da man her kan nå bredt ud på tværs af platforme.

Efter et par års tale skred flere organisationer i 2010 til handling og begyndte at bruge *cloud computing*. Selvom teknologien kan give en række drifts- og sikkerhedsmæssige fordele, byder den også på en række udfordringer for danske organisationer. Særligt i forhold til lovgivningsmæssige og kontraktlige anliggender. Vi så i 2010 de første tilfælde, hvor *cloud* services blev brugt i kriminelt øjemed. Det venter vi vil stige, ligesom vi kommer til at se målrettede angreb på tjenester placeret i skyen og de datacentre, der driver skyen, i takt med udbredelse af teknologien.

Det er alt i alt ikke vores forventning, at der i fremtiden anmeldes flere hændelser om it-sikkerhed til DK•CERT, snarere tværtimod. Derimod tror vi, at de hændelser, hvor DK•CERT bidrager med analyse, efterforskning og rådgivning, vil stige i antal,

kompleksitet og tidsforbrug. Nedenfor har vi samlet de væsentligste tendenser for både 2010 og fremtiden, som vi har kunne identificere gennem rapportens tilblivelse. Det er vores håb, at du kan benytte dem som inspiration, således at vi i fællesskab kan være med til at sikre de danske it-aktiver.

6.1. Tendenser fra året der gik

2010 bød på større opfindsomhed fra de it-kriminelles side. Over en bred kam var tendensen som i tidligere år, at angrebene var mere udspekulerede, målrettede og avancerede. Angrebsvektorerne blev udvidet og omfatter med stigende brug af *social engineering* også tidligere perifere platforme som Mac OS, Android og lignende. Systemkompromittering og -misbrug er ikke længere forbeholdt Windows-brugere, men rammer på tværs af systemer og platforme, og beskyttelsesteknologierne har vanskeligere i at følge med.

At *spam* og *phishing* i stigende grad udfærdiges på modtagerens eget sprog og med brug af oplysninger som modtageren kan relatere sig til, virker i dag næsten banalt at skrive, men tegner et billede af større målrettethed og professionalisme. Et billede som også tegnes af *Stuxnet*, der er det hidtidige højdepunkt for, hvor målrettet og avanceret *malware* kan være. *Ormen* ramte industrielle kontrolsystemer og var, mener nogle, målrettet indsamling af oplysninger fra eller sabotage af det iranske atomprogram.

Det var ikke kun legale organisationer, der fattede interesse for *cloud computing*. Skyens store båndbredde og regnekraft gjorde den interessant til formål af mindre lødighed. Således var der i året der gik både angreb på og fra services placeret i skyen. Desuden opstod der en række services, der havde til formål at knække krypteringsalgoritmer, passwords og lignende.

Også i 2010 var sårbare legale webapplikationer en væsentligste kilde til spredning af *malware*. Vi så flere eksempler, hvor fx *cross-site scripting*- og SQL injection-*sårbarheder* blev udnyttet til at sprede *malware* til websidernes besøgende. Rangen som den væsentligste kilde til spredning af *malware* udfordres dog af sociale netværkssteder.

I nedenstående uprioriterede liste kan du se de tendenser inden for it-kriminalitet vi mener var de mest fremtrædende i 2010:

1. **Færre angreb målrettet de danske netbanker**. I 2010 oplevede de danske banker et fald i misbrug af kundernes netbank konti, og vi så ingen større angreb målrettet disse. Indførelsen af *NemID* kan kun for sidste halvdel af 2010 tilskrives en del af æren for dette.
2. **Stigende udnyttelse af sårbarheder ved læsning af PDF dokumenter**. PDF-dokumenter var en væsentlig kilde til spredning af *malware* ved udnyttelse af *sårbarheder* i Adobes PDF læser. Også andre populære tredjepartsfilformater som Flash og QuickTime-film var under angreb.
3. **Cross platform Malware**. Der har tidligere været *malware* målrettet fx Mac OS. 2010 bød dog på det endelige gennembrud for *malware* målrettet flere platforme. Fx kom der sidst på året en variant af Koobface til Mac OS, og Mac computere indgik i *botnet* og deltog i *DDos*-angreb på lige fod med Windows computere.

4. **Malware til mobile platforme**. Som det bløde mål der ofte ikke er beskyttet af antivirusprogrammer, blev mobile platforme mål for *malware*. Vi har tidligere set *malware* målrettet iPhone, men i 2010 kom også Android-baserede telefoner med på listen.
5. **Malware på sociale medier**. Sociale netværkssteder som fx Facebook blev i stigende grad benyttet til spredning af links til *malware*, *spam* og *phishing*, eller til spredning af *malware* gennem sårbare applikationer.
6. **Ransomware tager data som gidsel**. *Malware* krypterede brugernes data eller fandt kopibeskyttet materiale på brugernes pc. Mod udbetaling af en løsesum kunne man herefter få dekrypteret sine data eller slippe for sagsanlæg. *Ransomware* indgik som nyt begreb i ordbogen og spredte sig hovedsagelig via P2P-netværk.
7. **Mere målrettet og avanceret malware**. Med *Stuxnet* i spidsen udgjorde 2010 et højdepunkt for, hvor avanceret og målrettet *malware* kan være. Forplumring af kode, flere lag af kryptering og avancerede algoritmer til download og opdatering er reglen snarere end undtagelsen, hvorfor genkendelsesraten er faldende hos de store antivirusproducenter.
8. **Angreb fra skyen**. Med fx *DDoS as a service* har internetkriminelle overtaget principper og terminologi fra *cloud computing*. Året bød også på brug af *cloud computing* til at knække krypteringsalgoritmer, *brute-force* angreb og lignende.
9. **Datalækage i system**. WikiLeaks bød på nye muligheder for offentliggørelse af fortrolige data, der ikke længere behøver at blive glemt, tabt eller stjålet. Tjenesten leverede en mulighed for alle dem, der mente, at hemmeligstemplede dokumenter havde offentlighedens interesse, uden man selv skulle stå til ansvar for offentliggørelsen.
10. **Brugernes egne data brugt til social engineering**. Data fra brugernes pc, sociale netværkskonti eller andre online tjenester blev benyttet til at målrette og øge troværdigheden af onlinesvindel.

6.2. Fremtidige trends

Sommerens verdensmesterskaber i fodbold endte ikke med de massive angreb, som vi sidste år forudså. Umiddelbart kan dette tolkes som godt nyt for os, der arbejder med it-sikkerhed. Vi tror dog, at det snarere er et tegn på, at de it-kriminelle er blevet mere målrettede og i dag planlægger og udfører angreb nationalt. Det vil sige angreb, som er målrettet indsamling og misbrug af kreditkortinformationer, *NemID*-forbindelser, persondata, virksomhedsinformationer, infrastrukturer og lignende i netop det land, som er under angreb. Vi tror, at det vil ske med brug af *malware*, som er designet til at ryge under sikkerhedsbranchens radarer, og som spredes både via legale hjemmesider og hjemmesider, der er oprettet til formålet. Ved at udnytte aktuelle emner og begivenheder placeres de skadelige hjemmesider højt i søgemaskinernes resultater for udvalgte søgninger. *Spam* og *phishing* vil indgår som en naturlig del af det samlede angreb.

På ryggen af den økonomiske krise har organisationerne øget udgifterne til it-sikkerhed moderat. Spørgsmålet er blot om det er tilstrækkeligt og om vi bruger pengene rigtigt. I en tid hvor individet er det primære mål for stadig mere avanceret *malware*, der i stadig mindre omfang opdages af sikkerhedssoftwaren, er spørgsmålet, hvorvidt de store centrale systemer giver tilstrækkelig værdi for pengene. I DK•CERT tror vi på, at samarbejde er en væsentlig del af løsningen. Vi mener, at vi nationalt såvel som internationalt bør samarbejde om at detektere,

informere og blokere aktuelle angreb allerede i internetudbydernes netværk. Det kræver imidlertid en diskussion af, om og hvordan det kan gøres inden for den eksisterende lovgivning og uden at krænke borgerens privatliv. For nogle af os vil fremtiden således blive præget af de samarbejder, som herhjemme er godt på vej. Forhåbentlig til gavn for hele landets it-sikkerhed.

At spå om fremtiden er altid svært. Nedenfor giver vi alligevel vores bud på de øvrige tendenser, vi vil se i fremtiden. Ikke alle vil blive realiseret i 2011, men på sigt tror vi, at vi kan kigge tilbage på listen og nikke genkendende.

1. **Den menneskelige faktor**. *Social engineering* bliver i stigende grad midlet, der lokker os til at sænke paraderne. Hvad enten målet er at lokke os ind på specifikke hjemmesider, besvare eller klikke på links i mails, åbne vedhæftede dokumenter eller installere applikationer på vores smartphone, bliver det udført stadig mere udspekuleret. Viden om ikke nødvendigvis individet men så den gruppering vi tilhører, bruges til at målrette angreb og skaffe sig adgang til vores data og penge.
2. **Diversitet i platforme giver nye muligheder**. De seneste år har vi oplevet en vækst i operativsystemer og programmer til fx smartphones, tavle-pc'er, spilkonsoller og anden forbrugerelektronik, som er forbundet til internettet. Vi vil se målrettede angreb mod systemer, som på grund af deres udbredelse ikke tidligere ville være interessante.
3. **Blandede angreb over flere platforme og medier**. Vi tror, at fremtiden byder på massive angreb fra *malware* til flere platforme, hvor spredningsmediet er såvel sociale netværkssider som sårbare legale hjemmesider og hjemmesider oprettet til formålet, der alle promoveres via brug af søgemaskineoptimering og *spam*.
4. **(Mis)brug af skyen**. Regnekraft og båndbredde gør brugen af *cloud computing* attraktiv, også for de it-kriminelle. Derfor vil vi se flere angreb på *cloud* services, som kan misbruges til videre angreb, eller hvorfra der kan opsnappes følsomme data. Derudover vil vi se angreb fra *cloud* services, som er købt på legal vis og fx benyttes til at bryde krypteringsalgoritmer, brute force-angreb og lignende.
5. **Angreb på mobile platforme**. Mobile enheder som smartphones og tavle-pc'er udgør et blødt mål, da de ofte ikke er krypteret eller beskyttet af firewall, antivirussoftware og lignende. De bliver i stigende grad mål for *malware*, der har til formål at opsamle informationer fra enheden selv eller de tjenester og netværk, de kobles op mod.
6. **Angreb fra cyberterrorister**. Terrororganisationer og rabiate grupperinger benytter i dag internettet til bl.a. rekruttering. Springet til også at benytte internettet til finansiering og/eller egentlig cyberterrorisme er ikke lang. Fremtiden byder på økonomisk betinget it-kriminalitet, spionage, *DDoS*-angreb og lignende, der er målrettet organisationer eller nationer, som opfattes som fjenden. Alt sammen ved brug af de organiserede it-kriminelles strukturer, værktøjer og metoder.
7. **Malware på sociale netværkssteder**. Stigende integration med andre tjenester og mere end 500 millioner tillidsfulde brugere gør Facebook til et attraktivt mål for it-kriminelle. Mængden af *spam*, *malware* og *phishing*, som spredes over Facebook og de øvrige populære sociale netværkstjenester vil stige markant i de kommende år.

8. **Nye tab af fortrolige og personfølsomme data**. Lagring, behandling og transport af flere data, samt større integration mellem stadig mere komplekse systemer, øger risikoen for at fortrolige data eksponeres via organisationernes applikationer eller på anden vis lækkes som følge af menneskelige fejl. I tillæg hertil kommer data, der bevidst lækkes til pressen eller tjenester som WikiLeaks. Fremtiden byder på en stigning i hændelser vedrørende tab af fortrolige eller følsomme data.
9. **Målrettede angreb på HTM 5**. Udbredelsen af HTM 5 særligt til distribution af video gør standarden til et attraktivt medie for it-kriminelle. Fx det fælles scripting-API vil blive udnyttet til at ramme flere browsere og platforme.
10. **Signeret malware**. For at overkomme forhindringer som signering og hvidlistning af kode vil *malware*-skribenterne have behov for godkendte softwarecertifikater. Det skaber et marked for malwar, der enten stjæler eller bruger dem. Vi vil se *malware*, der er blevet signeret med stjålne certifikater, ligesom *spam* og *phishing* tilsvarende vil blive signeret for at øge troværdigheden og slippe gennem vores mentale og tekniske filtre.

7. Anbefalinger

"Det er vigtigt, at vi alle agerer sikkert på nettet for at reducere risikoen for it-kriminalitet."[94]
Charlotte Sahl-Madsen, Videnskabsminister.

Selvom teknologien og vores brug af teknologien er under hastig forandring, er mål og medie for it-kriminalitet stadig de samme som sidste år. Mens de tekniske trusler har forandret sig, er målet stadig vores private data, som forsøges tilvejebragt via *sårbarheder* i teknologien og/eller de mennesker, der benytter teknologien. Det betyder, at de steder vi kan sætte ind for at beskytte vores it-aktiver, grundlæggende er de samme som tidligere. På trods af dette er der i nedenstående anbefalinger variationer i forhold tidligere år.

I forhold til vores anbefalinger rettet mod borgerne betyder det, at vi i år har valgt at benytte os af de samme råd, som publiceres via opdaterdinpc.dk[95], der er oprettet i forbindelse med netsikker nu! kampagnen. Dem har vi suppleret med vores egne anbefalinger og som noget nyt medtaget smartphones og tavle-pc'er. Derudover har vores fokus på blandt andet *cloud computing* samt årets begivenheder som helhed været med til at præge vores anbefalinger rettet mod henholdsvis organisationernes it-ansvarlige og beslutningstagerne.

Det er vores håb, at du vil lade anbefalingerne danne baggrund for refleksion over, hvordan du kan bidrage til at skabe forøget it-sikkerhed. Vi håber, at vi herved kan bidrage til en diskussion om, hvordan vi i fællesskab kan skabe trygge rammer for danskernes digitale færden. Vi mener, at både lovgiverne, organisationerne og den enkelte borger bør tage et medansvar for denne proces,- gerne i samarbejde.

7.2. Anbefalinger til borgerne

Der er over en bred kam enighed om, hvordan vi beskytter borgernes it-installationer mod angreb, hvad enten det er som privatpersoner eller ansatte i en organisation. Vi har derfor valgt at benytte de samme fem råd, som publiceres på opdaterdinpc.dk[95], hvor rådene suppleres yderligere. Rådene dækker bredt, hvordan du beskytter din pc og er nedenfor suppleret med vores egne anbefalinger, hvor mange er gengangere fra sidste år.

Beskyt din pc:

1. Beskyt din pc mod ondsindede programmer. Brug firewall og antivirus.
2. Hold dine programmer opdateret. Brug automatisk opdatering, hvor det er muligt.
3. Slå krypteringen til på dit trådløse netværk. Brug som minimum WPA2-kryptering.
4. Indstil sikkerhedsniveauet i din browser.
5. Installer kun programmer du har brug for. *Sårbarheder* i ubrugte programmer udgør også en risiko.

94 IT- og Telestyrelsen, 2010; *"Netsikker nu magasinet 2010"*.

95 Opdaterdinpc.tdc.dk, 2010; "*Gode råd*".

Mobiltelefoner er i dag reelt små computere, hvorpå der kan installeres programmer, surfes på nettet, mailes og bruges netbank. Som sådan adskiller sikkerheden på smartphones og tavle-pc'er sig ikke fra sikkerheden på en almindelig pc. Alligevel er der et par råd, du i tillæg bør overveje, som mere knytter sig til, at disse enheder medbringes og kan glemmes eller stjæles overalt.

Beskyt din smartphone og tavle-pc:

6. Brug passwordbeskyttelse på din mobil telefon eller tavle-pc.
7. Overvej om du bør kryptere dine data.

Selvom dine systemer er opdaterede og sikre, er der stadig mulighed for ubehagelige overraskelser. En væsentlig årsag til kompromittering er installationer og services, der bruger standardbrugernavn og -password, eller brugernavne og passwords, der er nemme at gætte. Husk på, at brugernavne og passwords er personlige.

Brug sikre passwords:

8. Brug ikke standardbrugernavne og –passwords. Lav altid dine egne.
9. Brug passwords, der er vanskelige at gætte. Minimum otte tegn indeholdende både store og små bogstaver, tal og specialtegn.
10. Brug forskellige adgangskoder til forskellige tjenester. Brug evt. en elektronisk kodehusker.

Spam, *virus* og *phishing* udgør hovedparten af de mails, som sendes og modtages. Det er derfor vigtigt at vide, hvordan du beskytter dig, og hvad du skal gøre, når der alligevel er en mail med et (lidt for) godt tilbud, en lotterigevist eller tilsvarende, der slipper igennem. Fælles for denne type mails er nemlig, at de udgør en potentiel risiko.

Brug mail med omtanke:

11. Brug et filter til filtrering af *spam*.
12. Lad være med at udlevere personlige (konto)oplysninger på baggrund af en mail.
13. Undlad at svare eller klikke på links og vedlagte filer, hvis du er i tvivl om mailens lødighed. Slet i stedet mailen.

Vi bliver alle eksponeret for *malware* via inficerede sårbare legale websider. Den hyppigste metode til inficering af brugeren er gennem *sårbarheder* i browseren eller de programmer og plugins, der er knyttet til denne. Typisk opdateres tredjepartsprogrammer som medieafspilleren, Flash-playeren eller PDF-læseren ikke ved automatisk opdatering af pc'en, og de kan derfor udgøre en risiko for vores sikkerhed på nettet.

Sikker surf på nettet:

14. Opdater også tredjepartsprogrammer. Brug evt. programmerne PSI fra Secunia[96] eller Heimdal fra CSIS[97].
15. Brug browserens indbyggede *phishing*- og antispyware filter mm, eller installer selv.

96 Secunia.com; *"Download - Secunia Personal Software Inspector (PSI)"*.

97 Csis.dk, 2010; *"Heimdal"*.

16. Overvej om du som standard vil tillade afvikling af scripts i browser og PDF-dokumenter.

Også sociale netværkssteder bliver i stigende grad (mis)brugt til blandt andet spredning af *malware*. Ud over risikoen for at få misbrugt din egen konto kan du også modtage beskeder fra dine venner med links til inficerede applikationer eller hjemmesider. Følg nedenstående få anbefalinger til brug af sociale netværkstjenester, og suppler evt. med DK•CERT og KOMFOs vejledning til sikker brug af Facebook[98].

Brug af sociale netværkstjenester:

17. Brug tredjepartsapplikationer med omtanke. De kan have andre "funktioner" end dem, du umiddelbart ser.
18. Vær opmærksom på, hvilke informationer fra din profil du giver applikationer og brugere adgang til.
19. Beskyt dine private oplysninger på tjenester via privatlivsindstillinger/privacy settings.
20. Vær opmærksom på, hvem der kan have interesse i det indhold, du lægger på din profil. Fx kan en historie om, at du nu tager på ferie, sammen med billeder fra dit hjem være attraktivt for indbrudstyve.

De data du selv lægger på nettet, kan misbruges eller bruges i en sammenhæng, som du ikke selv havde forestillet dig. Det gælder også de data du afgiver, når melder dig til en online tjeneste, downloader et program, sender en jobansøgning eller lignende. Ud over at persondata selvfølgelig er personlige og skal forblive det, gælder det også billederne fra den seneste fest, debatindlæg med mere. Data der lægges på nettet, vil være tilgængelige selv om du sletter dem, og vil på et tidspunkt blive læst af dem, som du ikke ønskede skulle læse dem.

Beskyt privatlivets fred på nettet:

21. Læg kun oplysninger om dig selv på internettet, som alle til enhver tid må bruge.
22. Spørg, inden du lægger billeder og oplysninger ud om andre.
23. Vær kritisk, når du modtager forespørgsler og invitationer på nettet.
24. Læs aftalevilkår for tjenester, så du ved, hvad du går ind til.

Generelt gælder det, at man bør bruge sin sunde fornuft og tænke sig om, også med hensyn til brugen af it. Selvom man har beskyttet sig med eksempelvis anti-*virus*-program, firewall og et antispywareprogram, gælder det om at forholde sig kritisk til mediet og den information, det indeholder.

7.2. Anbefalinger til it-ansvarlige

Organisationernes it-ansvarlige varetager den praktiske del af it-sikkerheden på de systemer, hvor udvikling og drift endnu ikke er blevet outsourcet. Således er det de it-ansvarlige, der som minimum har et medansvar for, at organisationens systemer er i en sådan forfatning, at tilgængelighed, integritet og fortrolighed opretholdes. Retningslinjerne for denne proces beskrives i organisationens it-sikkerhedspolitik, som løbende bør være under revision, således at fx udbredelsen og brug af

98 DK•CERT & KOMFO, 2010; *"Styr dit privatliv på Facebook"*.

smartphones og "nye" emner som *cloud computing* inddrages.

Selvom de konkrete tekniske trusler løbende ændrer sig, er de måder, hvorpå organisationerne implementerer og organiserer it-sikkerhed, grundlæggende de samme som tidligere. Som for borgerne vil mange af vores anbefalinger til organisationernes it-ansvarlige derfor også være de samme som sidste år. Grundlæggende handler det om at holde sin sikkerhedspolitik opdateret på baggrund af aktuelle risikovurderinger og handle på baggrund af dette.

En væsentlig del af de it-ansvarliges ansvarsområde omhandler at holde de ansattes computere i en sådan forfatning, at de kan varetage deres job. Som en del af it-sikkerhedspolitikken bør der derfor implementeres procedurer, der sikrer, at medarbejdernes computere er opdaterede og sikret mod angreb.

De ansattes pc'er:

1. Hold brugernes pc'er opdaterede. Implementer procedurer til at sikre, at der benyttes automatisk opdatering.
2. Implementer procedurer der sikrer, at brugerne benytter firewall og opdateret antivirusprogram.
3. Giv kun brugerne mulighed for at definere stærke passwords lokalt såvel som på organisationens forretningssystemer.
4. Hold løbende organisationens ansatte opdateret med it-sikkerhedsproblematikker, der er relevante for netop dem.

Med brugen af mobile enheder er der introduceret en række nye platforme og medier, som skal interagere med organisationernes eksisterende miljøer. Grundlæggende bør sikkerheden på mobile enheder som mobiltelefoner og tavle-pc'er ikke opfattes anderledes end på de stationære pc'er. Den største trussel udgøres af enhedernes mobilitet. Fx udgør mangelfuld sikkerhed på en stationær pc ikke samme risiko, da de oftest er beskyttet bag organisationens sikkerhedssystemer, altid kobles på samme netværk og kun sjældent glemmes, tabes eller stjæles.

Mobilsikkerhed:

5. Udarbejd retningslinjer i organisationens it-sikkerhedspolitik og informer om hvordan mobile enheder bør bruges.
6. Brug en central løsning for automatisk kryptering af data på medarbejdernes bærbare computere og andre mobile enheder og lagringsmedier.
7. Sørg for at beskytte netværket mod risici fra mobile enheder og lagringsmedier. Overvej hvilke enheder der forsøges koblet på netværket i morgen og hvordan de kan kompromittere organisationens sikkerhed.

Ikke kun brugerne, deres arbejdsstationer og mobile enheder udgør en risiko for organisationens sikkerhed. Også organisationens forretningssystemer kan være sårbare og bør holdes opdaterede sikre mod angreb.

Organisationens forretningssystemer:

8. Luk for services, der ikke er nødvendige på det enkelte system.
9. Minimer adgangen til det nødvendige ved at begrænse adgang fra netsegmenter, services og brugerkonti, der ikke skal benytte den pågældende service.

10. Hold organisationens forretningssystemer opdaterede. Abonner eksempelvis på varsling af *sårbarheder*, og/eller brug automatisk softwareinspektion.
11. Sørg for, at brugersendte data valideres inden eksekvering og/eller lagring på organisationens webapplikationer.
12. Benyt *scanninger* efter *sårbarheder* og målrettede *scanninger* af webapplikationer til periodisk kontrol.

Tab af fortrolige data sker oftest som følge af menneskelige fejl. Gør derfor organisationens data tilgængelig på en sikker måde. Hvis ikke du gør det, vil medarbejderne, når de skal benytte data uden for arbejdspladsen, sende dem til deres egen Gmail-konto, overføre dem til Dropbox eller noget helt tredje. Fælles for disse "løsninger" er, at de tages i brug uden tanke på sikkerheden og uden at organisationen har indflydelse på, hvor data er og hvordan de bliver behandlet. Fortrolighed af data vedrører nemlig ikke kun organisationen selv. Hvis fx kunder, leverandører og samarbejdspartnere skal bevare tilliden til organisationen, skal fortrolige data vedblive at være fortrolige. Tænk derfor dataadgang og kryptering ind i alle scenarier for brug af it.

Fortrolighed af data:

13. Overvej, hvem der skal have adgang til hvilke data hvorfra og hvordan, og begræns adgangen til det nødvendige.
14. Brug evt. *Data Leak Prevention*-systemer for at sikre, at regler og procedurer overholdes.
15. Krypter forretningskritiske data både i skyen, på serveren, i transaktionen og ved anden transport på fx bærbare computere, smartphones og andre mobile enheder.

Organisationens leverandører udgør en væsentlig del af sikkerheden, hvad enten der er tale om hard- og softwareleverancer, hosting eller outsourcing. Generelt bør man undersøge markedet og stille krav til sine leverandører, således at organisationsspecifikke krav til drift og sikkerhed indføres i kontrakterne.

Samarbejdsrelationer og leverandører:

16. Benyt aktivt organisationens risikovurderinger ved udfærdigelse af kravspecifikationer og lignende.
17. Gør det klart, om leverandøren kan sikre opretholdelse af jeres krav til fx sikkerhed.
18. Tænk worst-case scenarier ind i kontrakten, og specificer ansvar herefter.
19. Sørg for at få den nødvendige information og uddannelse.

Vi har i år valgt at videregive nogle af de råd, som den nyoprettede *GovCERT*-funktion har offentliggjort i deres situationsrapport for 4. kvartal 2010[99]. Vi har valgt at gøre rådene mere almene, end de er tænkt i rapporten, hvor de er rettet mod myndighederne.

Anbefalinger fra GovCERT:

1. Det anbefales, at organisationerne proaktivt blokerer for kommunikation til IP-adresser relateret til bl.a. TDSS, Zeus, Spy-Eye og Koobface.

99 Govcert.dk, 2010; *"Situationsbillede af sikkerhedstilstanden på den danske del af internettet Q4 2010"*.

2. Det anbefales, at organisationerne verificerer egne logs og sikrer, at tidssynkroniseringen er korrekt i alle logs. Det er vigtigt, at der logges tilstrækkelig information, så kommunikation kan spores tilbage til klienten, selv om kommunikationen NAT'es flere gange undervejs.

7.3. Anbefalinger til beslutningstagere

Herhjemme er en række brancher reguleret af lovgivningen og/eller branchen selv. På internettet har denne regulering primært haft fokus på beskyttelse af privatlivets fred. Øvrige forhold vedrørende borgernes og organisationernes sikkerhed har været overladt til den øvrige lovgivning, der ikke tager højde for internetkriminalitetens grænseoverskridende væsen. Således mener vi, at der i debatten om it-teknologien som motor for udbredelse af informationssamfundet mangler nogle aspekter om, hvordan vi på nationalt plan kan sikre de danske it-aktiver. I modsætning til fx den finansielle sektor og telebranchen har internetudbyderne kun i meget lille grad haft incitament og mulighed for at opdage og afværge misbrug og svindel. I tråd med DI ITEK mener vi, at der bør laves en national strategi på området, der sikrer borgere og organisationer mod *malware*.

Spredning af malware:

1. Lav en national strategi der adresserer bekæmpelse af *botnet*.
2. Giv internetudbydere og hostingvirksomheder incitamenter til aktivt at bidrage med opretholdelse af kundernes sikkerhed.
3. Giv internetudbydere og hostingvirksomheder incitamenter til at samarbejde om detektering, varsling, afværgelse og rapportering af it-kriminalitet internt såvel som til relevante myndigheder.
4. Indføres tvungen brug af *SPF* (Sender Policy Framework) for alle danske domæner. Det vil mindske både mængden og troværdigheden af *spam*- og *phishing*-mails.

Spredning af *malware* og systemkompromittering har i dag primært tyveri af data som formål. I modsætning til fx i USA kan ens personlige data herhjemme blive stjålet fra en usikker netbutik, uden at den har pligt til at informere en herom. Vi mener, kunden har ret til at få besked, således at denne i tide kan tage sine forholdsregler.

Informationspligt ved datatyveri:

5. Dansk lovgivning bør omfatte pligt til at informere organisationernes kunder ved kompromittering af systemer eller data, der vedrører kunden.

Med introduktion og brug af *cloud computing* er outsourcing af it-drift blevet aktuelt som aldrig før. Grundlæggende handler outsourcing om at lade nogle, der er specialiseret i det, tage sig af driften. Så kan man fokusere indsatsen andre steder i forretningen. Grundet leverandørens fokus på netop driften burde det samlet set give billigere og mere stabil drift. I virkeligheden handler det også om to organisationer, der skal arbejde sammen og have fælles forventninger til samarbejdet. Også i de tilfælde hvor virkeligheden ikke er, som man forventede.

Kunde- og leverandørrelationer:

6. Indfør klare politikker vedrørende outsourcing af forretningskritiske systemer og data.
7. Læs kontrakten igennem, og sørg for at leverandøren overholder organisationens krav til sikkerhed, også når det går galt.
8. Hav sikkerhed for, at I har adgang til organisationens data, også i specielle situationer som tvister, konkurs eller lignende.

Cloud computing er i 2010 blevet en attraktiv mulighed, som flere organisationer benytter sig af. Ud over forretningsmæssige aspekter som fleksibilitet og skalerbarhed introducerer brugen af *cloud computing* en række udfordringer. Særligt forhold vedrørende overholdelse af persondataloven bør man sikre sig er specificeret tilstrækkeligt i kontrakten med *cloud*-udbyderen. Derudover bør man gøre op med sig selv, hvor meget man evt. vil gå på kompromis med egne politikker og standarder.

Cloud computing med omtanke:

9. Tag stilling og lav politikker for, hvilke *cloud* services organisationen og dens medarbejderne må bruge, samt hvordan og til hvad de må bruge dem.
10. Læs kontrakterne igennem. Man bør særligt sikre sig, at kontrakten overholder gældende lovgivning og egne sikkerhedspolitikker.
11. Hvilke standarder overholder *cloud* udbyderen? Gør det klart om der fx er en revisionsrapport, der dokumenterer *compliance* til *ISO 27001* eller lignende og vurder, om det er tilstrækkeligt.

Forskellige organisationer bruger i dag it-mediet forskelligt og accepterer i forskellig grad at medarbejderne benytter organisationens udstyr og installationer til mere eller mindre private forehavender. Fx indgår brugen af sociale netværkstjenester nogle steder som en accepteret og integreret del af forretningen, mens det andre steder ikke accepteres. I tillæg hertil betyder mangfoldigheden af systemer og forskellige krav til sikkerhed, at alle har forskellige behov. Der er ikke i dag nogen standardløsninger, der passer til alle. I vores optik er det nødvendigt at man accepterer det og i stedet dyrker forskelligheden, men til gengæld styrker samarbejdet og lader det indgå i it-strategien.

Sikkerhedspolitik i et perspektiv om god selskabsledelse:

12. Beskriv hvorledes I fremadrettet ønsker, at teknologien bruges, og hvilke krav I her stiller til medarbejderne.
13. Tag aktivt stilling til medarbejdernes brug af organisationens it-installationer. Synliggør politikker, der specificerer regler for brug af organisationens installationer og indfør procedurer, der implementerer reglerne.
14. Lad it-sikkerhed indgå på lige fod med forretningens krav til teknologien.
15. Lad samarbejde indgå i strategien som et middel til at skabe løsninger, der er tilpasset organisationens krav til it-sikkerhed.
16. Lad organisationens risikostyringsaktiviteter være en naturlig og synlig del af det at drive forretning.
17. Sørg for at kommunikere muligheder og begrænsninger såvel som rettigheder og pligter til medarbejderne.

En væsentlig udfordring er at implementere it-sikkerhed således, at organisationens ansatte til stadighed er bevidste om *sårbarheder*, trusler og risici, hvad enten de agerer som ansatte eller privatpersoner. Hvor strukturer af *god selskabsledelse* tjener som middel til at synliggøre værdien af risikovurdering, handler *awareness* om at opbygge en sikkerhedskultur, hvor uddannelse og træning er centrale aspekter

"Education is critical. People need to know what they should be defending against."[100]

På mange områder adskiller it-sikkerhed sig ikke fra andre af de områder, vi som samfund og organisationer tager forholdsregler mod. I fællesskab kan vi afværge de fleste trusler, når vi besidder den fornødne viden og påtager os ansvar. I modsat fald kan forglemmelser og uansvarlighed få katastrofale følger.

Prioriter uddannelse:

18. Viden og erfaring er et grundlæggende fundament for at kunne varetage it-sikkerhedsarbejdet. Prioriter derfor uddannelse og styrk aktiviteter til videndeling og *awareness*.

Det er sjældent nok at beskytte sig. Hvis eller når det alligevel går galt, er det for at begrænse skaderne også nødvendigt at vide, hvem der gør hvad, hvorfor og hvordan. Mange organisationer har i dag et ledelsesmæssigt beredskab, der sikrer, at kommunikation er konsistent og i tråd med organisationens værdier, når der opstår kriser. Ofte er der også procedurer, der inden for strukturer af *god selskabsledelse* sikrer, at der bliver taget handling. I it-sammenhæng er der dog langt fra altid implementeret strukturer og procedurer, der beskriver det tekniske beredskab længere nede i geledderne. En klar beredskabsplan er en væsentlig del af organisationens risikostyring, der i sidste ende kan spare mange penge.

Vær beredt:

19. Sørg for, at der udfærdiges fyldestgørende beredskabsplaner for kritiske forretningsaktiver, der klart specificerer, hvem der skal foretage sig hvad hvornår og hvorfor.

100 Websense.com, 2010; *"2010 threat report"*.

8. Ordliste

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

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 udsendelse 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, fra forud definerede lister.

CAPTCHA: Completely Automated Public Turing-test to tell Computers and Humans Apart er et antihacker- og digitaliseringssystem. CAPTCHA fungerer ved at brugeren tilkendegiver at være et menneske, ved at gengive tekst fra et billede hvor teksten forvredet.

Clickjacking: Angreb, hvor besøgendes klik på en hjemmeside udnyttes til at aktivere indhold, som denne ikke er klar over eller ikke kan se. Herved risikerer brugeren fx at klikke på indhold eller aktivere funktioner på en anden webside uden at vide det. Clickjacking kan således benyttes til informationsindsamling fra fx brugeren sociale netværksprofiler, spredning af malware og egentlig systemkompromittering.

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).

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. Fx DS 484, ISO 27001 eller lignende.

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

Cross-site scripting (XSS): En metode, hvor adressen på et sårbart website udnyttes til at vise yderlig information eller afvikle programmer. Der er forskellige former for cross-site scripting, som gør det muligt at udføre komplekse angreb. Metoden kan fx 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* og svagheder og 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.

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 er 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.

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).

Drive-by-download: Malware-infektion ved besøg på en inficeret hjemmeside. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til, og infektionen foregår uden dennes vidende.

DS 484: Dansk standard for it-sikkerhed.

Fast flux: Fast flux dækker over teknologi, der hurtigt og løbende skifter den netværks- eller IP-adresse, der er tilknyttet et givent domæne. Bruges fx til phishing-sider for at forhindre, at de bliver sporet og lukket ned. Teknologien så dagens lys i 2007, blandt andet i forbindelse med Storm-ormen.

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.

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: Government Computer Emergency Response Team er en enhed oprettet i under it-sikkerhedskontoret hos IT- & Telestyrelsen. Enheden skal være fuldt operationsdygtig fra 2011. Den 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 it-sikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler. GovCERT dækker hele staten, men ikke internetbaserede hændelser generelt i samfundet, som eksempelvis nedbrud i netbanker mv.

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

Infrastructure as a Service (IaaS): Virtuelle maskiner og anden abstraheret hardware. IaaS giver mulighed for at køre styresystemer på virtuelle maskiner, som havde man nogle rigtige computere. Man kan kontrollere sine instanser via et service-API.

ISO/IEC 27001: 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 og ISO 27006, en række standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder.

Likejacking: Likejacking er en variant af clickjacking, hvor det kaprede klik på Facebook bruges til at angive, at brugeren "synes godt om" en bestemt webside.

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

Man in the Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes viden, videresendes gennem en "mand i midten", 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.

Muldyr: Person, der stiller sin bankkonto til rådighed for overførsel af penge fra kompromitterede netbankonti. Muldyret rekrutteres ved hjælp af falske jobtilbud og videreoverfører pengene ad andre kanaler end bankens, mod et en procentsats af det overførte beløb. Muldyrsaktivitet er herhjemme ulovlig og kan straffes efter straffelovens hæleribestemmelse.

NemID: NemID er en fælles dansk login-løsning til netbanker og offentlige hjemmesider, som blev taget i drift i 1. juli 2010. NemID bliver drevet af firmaet DanID og kan benyttes fra en hvilken som helst computer uden foregående installation af software. NemID kræver et certifikat til den offentlige digitale signatur og består af en personlig adgangskode og et nøglekort, hvor hver kode kun bruges én gang.

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 eller kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

Platform as a Service (PaaS): En cloud-baseret tjeneste, hvor man abonnerer på en virtuel platform (styresystem og middleware), der drives af cloud-udbyderen.

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

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*.

Software as a Service (SaaS): Cloud-baseret tjenester, der tilbyder online brug af programmer efter behov. Det kan være online programmer som tekstbehandling, regneark eller CRM-services. Eksempler på SaaS er Google Docs, Hotmail og lignende.

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. Ormen der indeholder en *trojansk hest*, angriber herefter industrielle Siemens WinCC SCADA-systemer. Flere mener, at den er udviklet med statssupport og -finansiering. Fx mener nogle, at ormen er målrettet sabotage af det iranske atomprogram.

Spam: Uopfordrede massedistribuerede reklamemails med henblik på salg af produkter eller services.

SPF, Sender Policy Framework: En udvidelse til SMTP-protokollen, som muliggør filtrering af e-mails baseret på den afsendende mailservers IP-adresse og den benyttede e-mailadresse. Ved registeringen af et domæne angives en SPF record, der fortæller, hvilke(n) mailservere der må benytte dette. Benyttes SPF af den modtagne mailserver, foretager den et opslag på afsenderdomænets SPF-record, og hhv. afviser eller godkender mailen på baggrund af dette.

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 fx 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: Kortlæggelse af kendte sårbarheder knyttet til services på et systems åbne porte. Benyttes ofte efter foregående portscanning.

Trojansk hest: Er 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 *virus*, botter og lignende. Trojanske heste identificeres ofte af antivirus- og antispyware-programmer.

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 nu også gøre det. Virus spredes i oftest som mail vedlagt en trojansk hest, der indeholder virussen selv.

Websårbarheder: En sårbarhed på en webapplikation, eller et tilknyttet system, som kan udnyttes gennem webapplikationen.

9. Figuroversigt

10. Referencer

AdaptiveMobile.com, 2010; "*Cyber criminals target Smartphones as malware increases by a third in 2010, reveals AdaptiveMobile*"; www.adaptivemobile.com/press-centre/press-releases/cyber-criminals-target-smartphones-as-*malware*-increases-by-a-third-in-2010

Atlantic.com, 2010; "*Ahmadinejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges*"; www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/

Bbc.co.uk, 2010; "*Burma hit by massive net attack ahead of election*"; www.bbc.co.uk/news/technology-11693214

Bitdefender.com, 2010; "*H1 2010 E-threat landscape report*"; download.bitdefender.com/resources/files/Main/file/H1_2010_E-Threats_Landscape_Report.PDF

Clarke, Richard A., 2010; "*Cyber War*"; HarperCollins

Cloud Security Alliance; "*CloudCERT*"; www.cloudsecurityalliance.org/cloudcert.html

Computerweekly.com, 2010; "*A G20 country will be hit by major cyber attack by 2015, Garter predicts*"; www.computerweekly.com/Articles/2010/11/30/244251/Gartner-predicts-cyber-attack-will-seriously-damage-G20-economy-by.htm

Computerworld.dk, 2010; "*DK-CERT: 2010 stod i botnettets tegn*"; www.computerworld.dk/art/113015/dk-cert-2010-stod-i-botnettets-tegn?a=block&i=205&pos=1

Computerworld.com, 2010; "*Dutch team up with Armenia for Bredolab botnet take down*"; www.computerworld.com/s/article/9193080/Dutch_team_up_with_Armenia_for_Bredolab_botnet_take_down

Csis.dk, 2010; "*Heimdal*"; www.csis.dk/da/private/heimdal/

Csis.dk, 2010; "*Netbank tyv leveret via Midtjyllands avis hjemmeside*"; www.csis.dk/da/csis/news/3076

Damballa.com, 2010; "*DDoSing the night away on Mac*"; blog.damballa.com/?p=1068

Danmarks Statistik, 2010; "*Den offentlige sektors brug af it 2009*"; www.dst.dk/upload/den_offentlige_sektors_brug_af_it_2009.PDF

Dasient.com, 2010; "*Continued growth in web-based malware attacks*"; blog.dasient.com/2010/09/continued-growth-in-web-based-*malware*_9357.html

Dasient.com, 2010; "*Web-based malware infections double since last year*"; http://blog.dasient.com/2010/11/normal.html

Datatilsynet, 2010; "*Udtalelse i forbindelse med anmeldelse af Google Apps - online kontorpakke med kalender og dokumenthåndtering*"; www.datatilsynet.dk/

afgoerelser/afgoerelsen/artikel/udtalelse-i-forbindelse-med-anmeldelse-af-google-apps-online-kontorpakke-med-kalender-og-dokument/

Deloitte, 2010; "*2010 TMT global security survey – key findings*"; www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/2010_TMT_Global_Security_study.PDF

DK•CERT, 2010; "*Angreb på IP-telefoni fra Amazon EC2*"; www.cert.dk/nyheder/nyheder.shtml?10-04-21-11-33-00

DK•CERT, 2010; "*EU etablerer center mod it-kriminalitet*"; www.cert.dk/nyheder/nyheder.shtml?10-11-25-10-23-23

DK•CERT, 2010; "*DK•CERT Trendrapport: It-sikkerhed i tredje kvartal*"; www.cert.dk/trendrapport2010/Trendrapport_Q3_2010.PDF

DK•CERT & KOMFO, 2010; "*Styr dit privatliv på Facebook*"; www.cert.dk/vejled/facebook_guiden_komfo&dkcert.PDF

DK•CERT, 2010; "*Vil du være fri eller sikker?*"; www.cert.dk/artikler/artikler/CW24092010.shtml

ENISA, 2009; "*Cloud computing: Benefits, risks and recommendations for information security*"; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Europol, 2011; "*Cybercrime presents a major challenge for law enforcement*"; www.europol.europa.eu/index.asp?page=news&news=pr110103.htm

Eurostat, 2010; "*Information and communication technologies in the EU27s*"; europa.eu/rapid/pressReleasesAction.do?reference=STAT/10/187&format=HTML&aged=0&language=EN&guiLanguage=en

Finansrådet; "*Netbankindbrud - statistik*"; www.finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx

F-secure.com, 2010; "*F-Secure Security Lab - Virus World Map*"; www.f-secure.com/en_EMEA/security/worldmap/

Gartner, 2010; "*Gartner identifies the top 10 strategic technologies for 2011*"; www.gartner.com/it/page.jsp?id=1454221

Govcert.nl, 2010; "*2010 national cyber crime and digital safety trend report*"; www.govcert.nl/download.html?f=169

Govcert.dk, 2010; "*Situationsbillede af sikkerhedstilstanden på den danske del af internettet Q4 2010*"; www.govcert.dk/resources/6

Havard.edu, 2009; "*The economics of online crime*"; people.seas.harvard.edu/~tmoore/jep09.PDF

IBM, 2010; "*X-Force 2010 mid-year trend and risk report*"; www-935.ibm.com/services/us/iss/xforce/trendreports/

Interpol, 2010; "*1st INTERPOL information security conference*"; www.interpol.int/Public/ICPO/speeches/2010/SGinformationSecurityConf20100915.PDF

Irrawaddy.org, 2010; "*Regime reacts indifferently to cyber attack*"; www.irrawaddy.org/article.php?art_id=19967

IT- og Telestyrelsen, 2010; "*Netsikker nu magasinet 2010*"; borger.itst.dk/sikkerhed/bag-om-netsikker-nu/netsikker-nu-2010-magasinet/resolveuid/22b9ea7c9e169ee4897833bcbe923578

It-sikkerhedskomiteen; "*Sikker cloud computing for forretningsansvarlige*"; www.itst.dk/sikkerhed/fora/it-sikkerhedskomiteen/copy_of_it-sikkerhedskomiteen/Sikker%20cloud%20computing%20for%20forretningsansvarlige

It-sikkerhedskomiteen, 2010; "*Sikkerhed i cloud computing*"; www.itst.dk/sikkerhed/fora/it-sikkerhedskomiteen/copy_of_it-sikkerhedskomiteen/Sikkerhed%20i%20cloud%20computing.%20It-sikkerhedskomiteen.PDF

Joewein.net; "*Begging spam from Russia*"; joewein.net/spam/spam-elena-needs-woodburning-oven.htm

JydskeVestkysten, 2010; "*Spammail: Elena trygler millioner om brændeovn*"; www.jv.dk/artikel/991383:Business--Spammail--Elena-trygler-millioner-om-braendeovn

Kaspersky, 2010; "*First SMS Trojan for Android*"; www.securelist.com/en/blog/2254/First_SMS_Trojan_for_Android

Messagelabs.com, 2010; "*MessageLabs Intelligence*"; http://www.messagelabs.com/intelligence.aspx

Messagelabs.com, 2010; "*MessageLabs intelligence september 2010*"; www.messagelabs.com/mlireport/MLI_2010_09_September_FINAL_EN.PDF

MessageLabs Intelligence, 2010; "*MessageLabs intelligence: 2010 annual security report*"; www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.PDF

Metro.co.uk, 2010; "*MasterCard website taken down by pro-WikiLeaks anonymous hackers*"; www.metro.co.uk/tech/849792-mastercard-website-taken-down-by-anonymous-hackers

MotherJones.com, 2010; "*Alleged WikiLeaks video leaker arrested*"; motherjones.com/mojo/2010/06/wikileaks-iraq-video-leaker-arrest

Net-security.org, 2010; "*AV vendors detect on average 19% of malware attacks*"; www.net-security.org/*malware*_news.php?id=1419

Norton.com, 2010; "*Norton cybercrime report: The human impact*"; us.norton.com/content/en/us/home_homeoffice/media/PDF/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.PDF

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

Nvd.nist.gov; "*National Vulnerability Database version 2.2*";nvd.nist.gov/

Open Security Foundation, 2010; "*Cloutage*"; http://cloutage.org/

Opdaterdinpc.tdc.dk, 2010; "*Gode råd*"; opdaterdinpc.tdc.dk/publish.php?dogtag=tdc_ms_opdater_raad

Pc-library.com; "*TCP & UDP Port 3072 Information*"; www.pc-library.com/ports/tcp-udp-port/3072/

RSA, 2009; "*RSA online fraud report, august 2009*"; www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0809.PDF

Sans.org, 2009; "*The top cyber security risks*"; www.sans.org/top-cyber-security-risks/#trends

Secunia.com; "*Download - Secunia Personal Software Inspector (PSI)*"; secunia.com/vulnerability_scanning/personal/

Shadowserver.org, 2010; "*Scan charts*"; www.shadowserver.org/wiki/pmwiki.php/Stats/ScanCharts

Sophos.com, 2010; "*Facebook Worm – Likejacking*"; nakedsecurity.sophos.com/2010/05/31/facebook-likejacking-worm/

Sophos.com, 2010; "*Girl's sexy Facebook video is disguise for survey scam*"; nakedsecurity.sophos.com/2010/10/29/girls-sexy-facebook-video-is-disguise-for-survey-scam/

Spectrum.ieee.org, 2010; "*Massive Distributed Denial-of-Service Cyberattack on Burma*"; spectrum.ieee.org/riskfactor/telecom/internet/massive-distributed-denialofservice-cyberattack-on-burma

T3.dk, 2011; "*IDevice-brugere opdaterer flittigst deres iOS*"; www.t3.dk/idevice-brugere-opdaterer-flittigst-deres-ios

Techjaws.com, 2010; "*Twitter vulnerability discovered*"; www.techjaws.com/twitter-vulnerability-discovered/

Theregister.co.uk, 2010; "*Monster botnet held 800,000 people's details*"; www.theregister.co.uk/2010/03/04/mariposa_police_hunt_more_botherders/

Trend Micro, 2010; "*2010 in review: New and better ways of stealing information*"; blog.trendmicro.com/2010-in-review-new-and-better-ways-of-stealing-information/

Twitter.com, 2010; "*All about the 'onMouseOver' incident*"; blog.twitter.com/2010/09/all-about-onmouseover-incident.html

Veracode.com, 2010; "*State of software security report*"; volume 2; www.veracode.com/reports/index.html

Version2.dk, 2010; "*7 gode råd: Sådan får du styr på mobilsikkerheden*"; www.version2.dk/artikel/17272-7-gode-raad-saadan-faar-du-styr-paa-mobilsikkerheden

Version2.dk, 2010; "*Datatilsynet forbyder Google Apps i kommuner*"; www.version2.dk/artikel/15352-datatilsynet-forbyder-google-apps-i-kommuner

Version2.dk, 2010; "*Advarsel: Hotmail spreder malware*"; www.version2.dk/artikel/17257-advarsel-hotmail-spreder-*malware*

Version2.dk, 2010; "*Nu venter afgørelsen: Odense er klar til Google-gyser i Datarådet*"; www.version2.dk/artikel/17035-nu-venter-afgoerelsen-odense-er-klar-til-google-gyser-i-dataraadet

Version2.dk, 2010; "*Viruskrig på to fronter: Mærsk også ramt af genvejsvirus på kontrolsystemer*"; www.version2.dk/artikel/15663-viruskrig-paa-to-fronter-maersk-ogsaa-ramt-af-genvejsvirus-paa-kontrolsystemer

Websense.com, 2010; "*2010 threat report*"; www.websense.com/content/threat-report-2010-introduction.aspx

Wired.com, 2010; "*Google to stop censoring search results in China after hack attack*"; www.wired.com/threatlevel/2010/01/google-censorship-china/

Wired.com, 2010; "*Whistleblower report: Leaked video shows U.S. 'Coverup'*"; www.wired.com/dangerroom/2010/04/whistleblower-report-leaked-video-shows-us-coverup/

Kontakt:

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

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