DK•CERT

Trendrapport 2008

It-kriminalitet og sikkerhed i året der gik

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Christina Brunvoll Nielsen, Rasmus Lund-Hansen og Jens Borup Pedersen, DK•CERT

Grafisk arbejde: Kirsten Hougaard, UNI•C

Foto: colourbox.com

Tryk: Rosendahls-Fihl Jensen A/S

DK•CERT

Det er DK•CERTs mission at skabe øget fokus på it-sikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden, der sætter DK•CERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende problemer.

DK•CERT bygger på en vision om at skabe samfundsmæssig værdi gennem offentliggørelse af viden om it-sikkerhed, skabt gennem samarbejde med såvel den offentlige og private sektor, forsknings- og undervisningsverdenen samt internationale samarbejdspartnere. Vi har en vision om at benytte vores viden 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 organisation under Undervisningsministeriet.

DK•CERT var blandt pionererne, der først i 90'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.

Forord

Velkommen til DK•CERTs Trendrapport 2008. Her forsøger vi at give læseren et indblik i problemet internetkriminalitet. Vi mener nemlig, at et problem kun kan løses ved, at man åbent og transparent at informerer og diskuterer problemets art og størrelse. At internetkriminalitet i 2008 var et problem, der kostede både danske organisationer og skatteborgere mange penge, kan du læse mere om på de følgende sider.

Fra statistikker og tørre tal har vi samlet op på det forgangne års nyheder og tendenser inden for it- kriminalitet og sikkerhed. Vi håber derved at kunne bidrage til en minimering af problemet. Det er derfor vores håb, at du som læser får større indsigt og efterfølgende kan bidrage mere kvalificeret til, hvordan vi som borgere og organisationer bedst muligt kan sikre vores digitale aktiver. På samme vis er det vores håb, at de løsningsforslag vi stiller i rapporten, vil blive diskuteret og taget til overvejelse af relevante beslutningstagere.

Vi ser forøget bevidsthed og viden som et vigtigt skridt på vejen mod bedre it-sikkerhed. Vi mener, at denne opgave bør løses inden for strukturer af *god selskabsledelse*, hvad enten der er tale om en privat organisation eller organisationen Danmark. Kun ved i fællesskab at tage ansvar kan vi løse problemet internetkriminalitet, der i 2008 var blevet en stor forretning, som vi alle kan risikere at blive kunder i.

Vi præsenterer i rapporten data, som primært dækker de netværk, DK•CERT overvåger. Derudover må der formodes at eksistere et mørketal af aktiviteter, der aldrig opdages, anmeldes eller informeres om. På trods af dette mener vi, at rapporten giver et godt billede af situationen på hele den danske del af internettet i 2008.

I forbindelse med rapportens tilblivelse vil vi gerne takke de parter, der har bidraget med inspiration og data.

Vi ønsker dig fortsat god fornøjelse med læsningen.

Med venlig hilsen
Shehzad Ahmad, DK•CERT

Om *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[1]. *God selskabsledelse* handler om, hvordan ejere i samspil med bestyrelse og direktion sikrer en god ledelse af organisationen[2]. Begrebet dækker ikke en absolut størrelse, men snarere en synliggørelse af strukturer og retningslinjer, der skal sikre en hensigtsmæssig rolle- og ansvarsfordeling i forbindelse med kontrol og styring af organisationen. Et i denne sammenhæng ikke uvæsentligt element af god selskabsledelse omhandler risikostyring og revision.

De problematikker, der medførte *corporate governance* diskussionen, førte i 2002 til vedtagelse af *Sarbanes-Oxley* Act of 2002 (SOX) i USA.

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[3]. Vi vil i denne rapport udelukkende bruge betegnelsen *god selskabsledelse*.

1 København Fondsbørs' komité for god selskabsledelse, 2005; "*Rapport om god selskabsledelse i Danmark 2005*".
2 Foreningen af statsautoriserede revisorer, 2004; "God selskabsledelse i mindre og mellemstore virksomheder".
3 Dansk it's fagråd for it governance og management, 2006; "IT Governance-anbefalinger".

Indholdsfortegnelse

1.	**Resume**		6
2.	**Indledning**		7
3.	**2008 - året i tal**		9
	3.1.	Det sårbare net	10
	3.1.	Spam, malware og phishing	12
	3.2.	Portscanninger	15
4.	**Tingenes tilstand i 2008**		16
	4.1.	Botnet status	17
	4.2.	Identitetstyveri	19
	4.3.	Cyber warfare og industrispionage	21
	4.4.	Fra sikkerhedsfronten	23
5.	**Hvad fremtiden bringer**		25
	5.1.	It-kriminalitet	25
	5.2.	Fremtidens udfordringer	27
6.	**Opsamling**		30
	6.1.	Trends og tendenser i 2008	31
	6.2.	Fremtidige trends	31
7.	**Anbefalinger**		33
	7.1.	Anbefalinger til borgerne	33
	7.2.	Anbefalinger til it-ansvarlige	35
	7.3.	Anbefalinger til beslutningstagere	36
8.	**Ordliste**		39
9.	**Figurer og tabeller**		42
	9.1.	Figuroversigt	42
	9.2.	Tabeloversigt	42
10.	**Referencer**		43

1. Resume

It-sikkerhed er ledelsens ansvar, og bør varetages på forretningens præmisser med fokus på synliggørelse af organisationens risikostyringsaktiviteter.

DK•CERT har i 2008 behandlet færre anmeldelser om it-sikkerhedshændelser. De hændelser, hvor DK•CERT har bidraget med analyse, efterforskning og rådgivning er steget i antal. Det sker på bekostning af anmeldelser om portscanninger, der er faldet væsentligt i antal. Årsagen til dette er, at *malware* i 2008 i stigende omfang blev spredt til sårbare legale hjemmesider via webforespørgsler, der ikke blev opdaget og anmeldt til DK•CERT. Der var således ingen orme- eller virusepidemier af samme dimensioner, som vi tidligere har set.

2008 viste en større variation og målretning af angreb, der primært var initieret gennem brugen af flere og mere specialiserede botnet. Sårbare legale webapplikationer og -sider var den væsentligste kilde til spredning af *malware*. En væsentlig årsag til dette er, at organisationerne ikke opdaterer deres sårbare systemer og sikrer deres webapplikationer mod angreb. *Malware* bliver i stigende omfang benyttet i forbindelse med spamudsendelse og identitetstyveri.

Der er i rapporten identificeret en række tendenser for både 2008 og fremtiden. F.eks. kan Mac- og Linux-brugere også blive mål for *malware*, der i stigende grad inficerer computere gennem browserplugins, *widgets* og tredjepartsapplikationer på f.eks. sociale netværkssider. Sidstnævnte kan desuden blive mål for indsamling af informationer, der kan benyttes til målretning af identitetstyverier.

Sikring, eksponering og adgangen til data bør være et fokusområde for organisationerne. Et aspekt af dette er de brugersendte data, der behandles og fortolkes af organisationernes webapplikationer, som i 2008 har været en væsentlig kilde til spredning af *malware*. Det anbefales, at organisationer skaber en platform for inputvalidering af data, inden eksponering for organisationens kunder, samarbejdspartnere og lignende. Generelt bør der sættes større fokus på samarbejdsrelationer, og hvad der kan forventes/risikeres ved disse.

I 2008 lykkedes det en række ISP'er i udlandet at blokere aktiviteten på en række større botnet. Andre botnet fulgte i kølvandet, og på sigt kan dette medføre design af botnet, der er vanskeligere at spore og blokere. Episoden har dog vist at det er muligt at gribe ind, og DK•CERT opfordrer til større nationalt samarbejde og kommunikation omkring it-sikkerhed. Således anbefales det, at der sættes fokus på detektering og afværgelse af botnetrelateret trafik allerede i ISP'ernes netværk.

2. Indledning

Internetkriminalitet er et stigende problem, der ikke forventes at blive mindre i de kommende år, heller ikke for danske organisationer og borgere. Således svarede 67 procent af de adspurgte i en undersøgelse foretaget i december 2008 af DK•CERT, at deres organisation i løbet af de seneste 12 måneder havde været udsat for en sikkerhedshændelse.

At vi som følge af den finansielle krise i den vestlige verden er blevet mere sårbare for internetkriminalitet understreger blot denne problematik. Som resultat af økonomisk usikkerhed søger flere på nettet efter de bedste tilbud, jobs og lignende og risikerer herved at ryge i kløerne på kriminelle bander. Således beskrev Version2 den 11. december, hvordan stadig flere rekrutteres til at hvidvaske penge ved hjælp af falske jobannoncer[4]. Vi mener derfor at it-kriminalitet ikke har tilstrækkelig prioritet hos lovgiverne i den vestlige verden. Dette på trods af et potentiale til sætte vores økonomi og samfund i stå.

Danske organisationer oplever en stigning i de udgifter der benyttes til investeringer i it. I 2006 var de samlede estimerede udgifter ifølge Danmarks Statistik steget til 37,4 milliarder danske kroner for organisationer med mere end ti ansatte, eller ca. 35.000 kr. pr. ansat[5]. I takt med at værdien af organisationers digitale aktiver er steget, er de udgifter der bruges på it-sikkerhed tilsvarende steget. En verdensomspændende undersøgelse foretaget af PricewaterhouseCoopers viste, at 15 procent af organisationers it-budget i 2007 blev brugt på it-sikkerhed[6]. Omsat til danske forhold betyder det, at danske organisationer i 2008 brugte mere end 6 milliarder kroner på it-sikkerhed.

Grænserne mellem it-sikkerhed hos den enkelte borger og i organisationer er med et stigende antal mobile enheder, hjemmearbejdspladser og andre netopkoblede enheder, blevet mere flydende. Kompromittering af borgenes digitale enheder kan medføre kompromittering af tilgængelighed, integritet og fortrolighed i den organisation, hvor borgeren er ansat og vice versa.

Målet med denne rapport er at sætte fokus på it-sikkerhed ved at skitsere de udfordringer, vi som borgere, organisationer og beslutningstagere står overfor, når det drejer sig om beskyttelse af vores digitale aktiver. Kun sådan kan vi indgå i åbne dialoger om, hvordan vi bedst muligt modgår disse udfordringer.

4 Version2, 2008; "*Krisen får flere til at bide på jobannoncer for it-strømænd*".
5 Danmarks Statistik, 2008; "Serviceerhverv 2008:17 statistiske efterretninger".
6 PricewaterhouseCoopers, 2008; "*The 5th annual global state of information security, the end of innocence*".

I rapporten indgår resultater fra en spørgeskemaundersøgelse foretaget i december 2008 af DK•CERT. Respondenterne var DK•CERTs kunder og i alt besvarede 76 spørgeskemaet. Disse data bør ikke betragtes som repræsentative, men de giver dog indikation af, hvordan it-kriminalitet og sikkerhed opleves i danske organisationer.

I rapportens første afsnit præsenteres data, der beskriver udviklingen med hensyn til it-kriminalitet på den danske del af internettet. Herefter går vi i rapportens andet afsnit bag om tallene og giver en status på nogle tendenser fra 2008. I rapportens tredje afsnit forsøger vi at fremskrive udviklingen og give et bud på de udfordringer, vi i fremtiden kan stå overfor. Endelig samler vil vi i de to sidste afsnit op på rapportens konklusioner og forsøger at give nogle brugbare anbefalinger til såvel den enkelte borger, organisationernes it-ansvarlige som beslutningstagerne.

På trods af de til tider skræmmende perspektiver håber vi, at du som læser vil have fornøjelse af rapportens indhold og efterfølgende kan bruge den indsigt i it-kriminalitet og sikkerhed som du præsenteres for.

God læselyst.

3. 2008 - året i tal

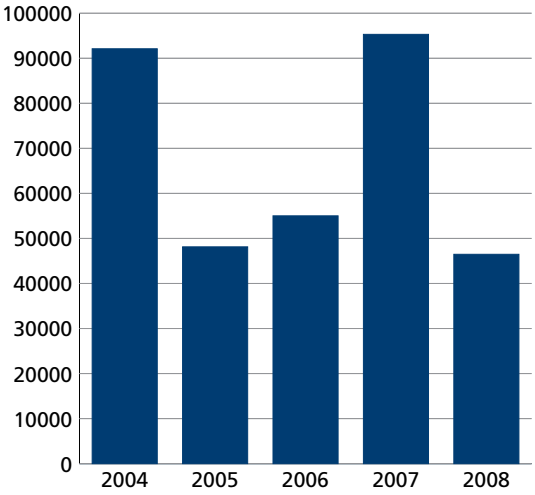
2. november 2008 markerede 20-årsdagen for Morris-ormen, som var den første internetorm. Ormen udnyttede sårbare UNIX-systemer. Det estimeres, at ca. 10 procent af internettet blev udsat for *denial of service-angreb* i den forbindelse. Ingen var på det tidspunkt forberedt på et sådant angreb. Spørgsmålet er, hvad der er sket siden da, og hvad vi som netværks- og sikkerhedsfolk i dag kan registrere og forebygge.

I dette afsnit præsenteres du for data, som beskriver den udvikling vi som borgere og organisationer i Danmark står overfor, når det handler om it-sikkerhed. Data er primært opsamlet fra de netværk som DK•CERT overvåger, men også tredjepart samt internettets åbne kilder har bidraget.

Der blev i 2008 anmeldt i alt 46.481 sikkerhedshændelser til DK•CERT, hvilket er et fald på ca. 51 procent i forhold til 2007, se Figur 1. En del af dette fald kan tilskrives, at der i 2008 ikke var nogle alvorlige ormeudbrud eller virusepidemier. Endvidere er nogle automatiserede anmeldelser om portscanninger bortfaldet. På trods af dette er det vores vurdering, at internettet ikke er blevet mere sikkert i 2008, men at der er tale om en ændring i it-kriminaliteten, således at den enten ikke blev opdaget og/eller blev anmeldt til DK•CERT. F.eks. har legale værktøjer som Google overtaget portscanningens rolle inden en kompromitering med f.eks. *SQL-injection*. Det har medført at hændelsen først blev anmeldt til DK•CERT når skaden var sket. Tilsvarende anmeldte borgere, der blev inficeret med *malware* via legale websites ikke hændelsen til DK•CERT, enten fordi de ikke opdagede det eller fordi hændelsen blev afværget af browserfiltre, antivirus eller antispyware programmer.

Mens antallet af anmeldte portscanninger er faldet, har der i 2008 været flere sager om websites hvorpå der var placeret trojanske heste eller phishing-sider, download af kopibeskyttet materiale samt hackede computere, se Tabel 1. Sagstypen *andet* dækker over en række sager, hvor DK•CERT modtog oplysninger om brugernavne og passwords til hackede FTP-servere på den danske del af internettet, der er opfanget på udenlandske botnetservere.

I det følgende fokuserer vi på tre emner, der repræsenterer forskellige aspekter af emnet it-sikkerhed. Først beskrives årets nye offentliggørelser af CVE-nummererede sårbarheder i kendte it-systemer samt konstatering af sårbarheder på den danske del af internettet. Herefter beskrives data vedrørende *malware*, spam, phishing og lignende. Afsnittet afrundes med data om portscanninger mod danske IP-adresser.



Figur 1. Sikkerhedshændelser anmeldt til DK•CERT i 2008.

Type	Antal
Portscanninger	44.666
Piratkopiering	580
Andet	488
Phishing/trojanske heste	332
Hacking	331

Tabel 1. Hændelsestyper anmeldt til DK•CERT i 2008.

3.1. Det sårbare net

Tjenesten *Common Vulnerability and Exposures* (CVE) samler og katalogiserer kendte sårbarheder i it-systemer. Hver sårbarhed udstyres med et CVE-nummer.

Mens antallet af offentliggjorte CVE-nummererede sårbarheder tidligere har været konstant stigende, er der siden 2006 sket et fald, se Figur 2. Således blev der i 2008 offentliggjort 5.496 nye sårbarheder mod 6.462 i 2007. Det kunne derfor menes, at internettet var blevet mere sikkert, hvilket nok en sandhed med modifikationer. Applikationsspecifikke sårbarheder, der udnyttes ved f.eks. *SQL-injections* eller *cross-site scripting*, offentliggøres kun sjældent med et CVE-nummer. Således skyldtes kun 5 procent af årets *malware*-infektioner, ifølge Trend Micro, CVE-nummererede programsårbarheder[7]. Dertil skal lægges at langt fra alle sårbarheder rettes med det samme.

De væsentligste begivenheder med hensyn til sårbarheder i 2008 var da sikkerhedsforskeren Dan Kaminsky i juli offentliggjorde en sårbarhed i DNS, samt Microsofts udsendelse af en ekstraordinær sikkerhedsrettelse til Windows' *Remote Procedure Call*-tjeneste (RPC) udsendt i oktober 2008.

Sårbarheden i DNS blev vurderet at være udbredt på mange af internettets DNS-servere og kunne medføre *cache poisoning* af en kompromitteret DNS-server. Et eventuelt angreb kunne således forårsage, at brugere af en kompromitteret DNS-server intetanende blev omdirigeret fra legitime websider til ondsindede websider styret af angriberen.

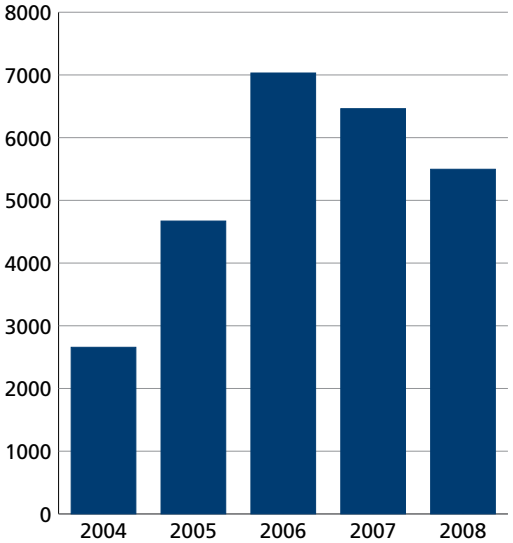
Microsoft valgte i oktober, efter at have konstateret målrettede angreb mod en alvorlig sårbarhed i Windows' RPC-tjeneste, at udsende en ekstraordinær sikkerhedsrettelse. Sårbarheden, der er alvorligst under Windows 2000, Windows XP og Windows Server 2003, kan medføre at en angriber får fuld kontrol over den sårbare pc.

Derudover markerede offentliggørelsen af sårbarheder i Adobe Flash og PDF-formattet sig blandt de mest omtalte og udnyttede. Særligt for disse var, at de kunne udnyttes på tværs af platforme, således at også f.eks. Mac- og Linux-brugerne i 2008 var i farezonen. Som med en sårbarhed i Microsoft Internet Explorer offentliggjort i december 2008, fandtes der tilgængelige programmer der udnyttede sårbarhederne, inden producenten frigav rettelser.

CVE-nummererede sårbarheder offentliggjort i 2008 blev i gennemsnit vurderet at være mere alvorlige end året før. *Base score* i Tabel 2 er et udtryk for hvor let en sårbarhed er at udnytte, samt dens potentielle udnyttelsesgrad[8]. Det dækker over, at sårbarheder offentliggjort i 2008 havde potentiale til at forvolde større skade (*impact*), mens de var lige så lette at udnytte som i 2007 (*exploitability*). I gennemsnit havde nye sårbarheder offentliggjort i 2008 en *base score* på 6,7, som risikovurderes til middel.

7 Computerworld.com, 2008; "*Vulnerabilities play only a minor role in malware spread, says researcher*".

8 Forum of Incident Response and Security Teams, FIRST; "Common vulnerability scoring system".



Figur 2. Offentliggjorte CVE-nummererede sårbarheder pr. år, DK•CERT.

År	Base score	Exploitability	Impact
2005	5,8	8,4	5,0
2006	6,0	8,4	5,4
2007	6,6	8,6	6,1
2008	6,7	8,6	6,2

Tabel 2. CVSS scores (0 – 10) for sårbarheder offentliggjort i 2008, DK•CERT.

Listen over CVE-nummererede sårbarheder offentliggjort i 2008 domineres af applikationer, der anvender HTTP-protokollen. Det vil sige webbrowsere og –servere samt programmer, der benyttes i forbindelse hermed, se Tabel 3. Mozilla-browseren Firefox var det system, hvori der blev konstateret flest nye sårbarheder efterfulgt af Apples operativsystem Mac OS X. Hvorvidt disse produkter er mere usikre at benytte end deres alternativer, kan dog ikke udledes, da dette afhænger af faktorer som f.eks.:

- Alvorligheden af de fundne sårbarheder.
- Tilgængeligheden af *exploits*.
- De sårbare systemers udbredelse.

En årsag til de mange sårbarheder i Mac OS X er måden, hvorpå de registreres. Flere sårbarheder i systemer, der knytter sig til Mac OS X, registreres således som sårbarheder i Mac OS X, og ikke som sårbarheder i f.eks. Adobe Flash Player.

Mens Mac- og Linux-brugerne tidligere har været forskånet for *malware*, er sårbarheder, der også rammer disse systemer, siden slutningen af 2007 gentagne gange blevet forsøgt udnyttet. Med stigende udbredelse af Linux og Mac OS X, og en måske falsk tryghedsfølelse hos brugerne, kan det forventes, at der i fremtiden vil være flere sårbarheder der forsøges udnyttet på disse platforme.

DK•CERT foretager årligt sårbarhedsscanninger på ca. 60.000 forskellige IP-adresser på den danske del af internettet. I 2008 viste disse scanninger, at ca. 2 procent af de scannede IP-adresser var tilgængelige fra internettet. De øvrige adresser må formodes ikke at være i brug eller være beskyttet bag firewall. Mere end halvdelen af de tilgængelige IP-adresser var sårbare for angreb, og på dem blev der i gennemsnit konstateret fire CVE-nummererede sårbarheder. På scanningstidspunktet var mere end 50 procent af disse sårbarheder offentliggjort mere end et år tidligere. Det indikerer, at mange organisationer ikke har en fast procedure for registrering, test og opdatering af sårbare systemer, hvorfor sårbarheder først rettes sent. En tendens, der den 4. december blev underbygget af sårbarhedsanalysefirmaet Qualys Inc[9].

I alt blev der ved sårbarhedsscanninger konstateret sårbarheder på 47 forskellige porte og/eller protokoller. Flest sårbarheder blev konstateret i forbindelse med webapplikationer (TCP port 80 og 443), se Tabel 4. Applikationsspecifikke sårbarheder forårsaget af f.eks. mangelfuld inputvalidering på webapplikationer fremgår ikke af statistikken, da de kun sjældent offentliggøres med et CVE-nummer. Netop disse sårbarheder, der f.eks. muliggør *SQL-injection* og *cross-site scripting*, var blandt de mest udnyttede i 2008.

Produkt	Sårbarheder i 2008
Mozilla Firefox	91
Apple Mac OS X	89
Apple Mac OS X server	79
Linux kerne	75
Mozilla SeaMonkey	68
Microsoft Internet Explorer	66
Microsoft Office	53
Sun Solaris	51
Mozilla Thunderbird	51
Sun JRE	51
Sun JDK	50
Apple Safari	37
Apple Quicktime	35

Tabel 3. Produkter med flest offentliggjorte sårbarheder i 2008, DK•CERT.

Port		procent
80 (http)	tcp	49,1
443 (https)	tcp	20,9
	icmp	9,3
88 (kerberos)	tcp	3,6
22 (ssh)	tcp	2,0
161(snmp)	udp	0,9
3389 (ms wbt server)	tcp	0,5
79 (finger)	tcp	0,5
53 (dns)	udp	0,5
1080 (socks)	tcp	0,5

Tabel 4. Fordeling af fundne sårbarheder på port og protokol, DK•CERT.

9 Computerworld.com, 2008; "*Windows users indifferent to Microsoft patch alarm, says researcher*".

Ved sårbarhedsscanninger konstaterede DK•CERT flest CVE-nummererede sårbarheder risikovurderet højt og middel, og kun cirka halvt så mange vurderet til at udgøre en lav risiko, se Figur 3.

3.2. Spam, malware og phishing

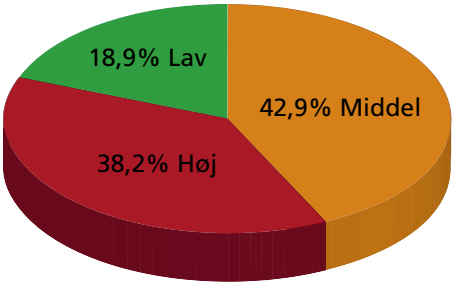
Spam defineres som uopfordrede massedistribuerede reklamemails med henblik på salg af produkter eller services. Herhjemme varetages anmeldelser af spam afsendt fra danske computere med henvisning til markedsføringsloven af forbrugerombudsmanden[10]. DK•CERT behandler kun anmeldelser om spam, der vedrører de netværk, DK•CERT overvåger. Vi har således ingen repræsentative data vedrørende anmeldelser om spam i Danmark.

Distinktionen mellem de enkelte typer af massedistribuerede mails kan være vanskelig, for hvordan kategoriseres f.eks. en mail, der indeholder uønsket reklame, og som samtidig indeholder links til skadelige websider og måske har vedlagt en trojansk hest? Og hvornår er noget en serviceydelse? Er f.eks. et "jobtilbud som muldyr" en serviceydelse?

I 2008 var 81,2 procent af alle afsendte mails ifølge MessageLabs Intelligence spam[11]. Det er et fald i forhold til 2007, hvor andelen var 84,6 procent. Sophos vurderede, at op til 97 procent af alle forretningsmails i perioder var spam[12]. Der har dog været stor spredning i mængden af afsendt spam. Det skyldes sandsynligvis, at et par større botnet midlertidig blev sat ud af spillet. I 2008 blev ca. 90 procent af al spam distribueret gennem botnet[13], der benyttede almindelige brugeres inficerede computere[14].

Året startede med et lille fald i forhold til 2007, hvilket formentlig skyldes, at aktiviteten fra spambotnettet Storm har været aftagende siden efteråret 2007. Andre botnet overtog dog Storms rolle, og mængden af afsendt spam var stigende indtil midt på efteråret 2008.

I november 2008 lykkedes det at lukke internetforbindelsen til en række webhostingfirmaer, som stod for en stor del af verdens spam. Heriblandt var hostingfirmaet McColo i USA, hvis maskiner stod for koordinering af op til 75 procent af verdens spam[15]. Dette medførte i en periode sidst på året, et markant fald i spamafsendelser, se Figur 4.



Figur 3. Risikovurdering af sårbarheder fundet ved sårbarhedscanning, DK•CERT.

Figur 4. Spammails anmeldt til Spamcop pr. sekund i 2008[16].

10 Forbrug.dk; "*Klag over spam*".
11 MessageLabs Intelligence, 2008; "*2008 Annual security report*".
12 Sophos, 2008; "*Security threat report: 2009*".
13 MessageLabs Intelligence, 2008; "*2008 Annual security report*".
14 Sophos, 2008; "*Security threat report: 2009*".
15 Washingtonpost.com, 2008; "*Major source of online scams and spams knocked offline*".
16 Spamcop.net, 2009; "*Total spam report volume, one year*".

Mens 2008 med hensyn til spam har været et turbulent år, har der ikke i 2008 været registreret alvorlige orme eller virusepidemier. Dette er en fortsættelse af tendensen fra 2007. I 2008 blev *malware* hovedsageligt spredt via inficerede websider, som brugeren havde tillid til, og gennem inficerede spammails. *Malware* indeholdt således ikke længere mekanismer til at sprede sig selv. Andelen af inficerede mails er steget i forhold til 2007, se Figur 5, og i slutningen af 2008 var andelen af inficerede mails cirka fem gange større end i starten af året[17]. Trojanske heste var i 2008 den mest almindelige type *malware*, der blev spredt pr. mail, se Figur 6.

Scareware var i 2008 et stigende problem. I gennemsnit identificerede Sophos fem nye *scareware* websites pr. dag[20]. *Scareware* er programmer, der forsøger at skræmme brugeren til at punge ud ved at udgive sig for at være et antivirusprogram. Programmet påstår at have fundet en farlig virus på brugerens computer, som kun kan fjernes ved at betale for at "opgradere" til den fulde version af programmet.

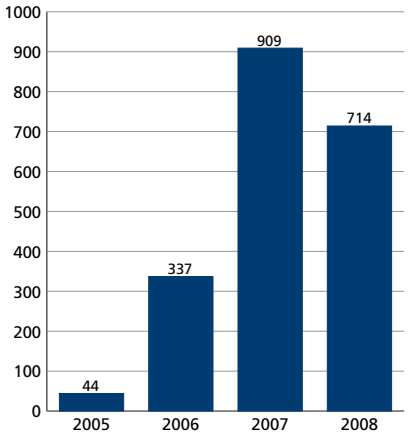
2008 har været præget af stigende flere hændelser, hvor *malware* har inficeret sårbare websites. DK•CERTs undersøgelse i december 2008 viste således, at knap 52 procent af de adspurgte organisationer havde været inficeret med botnetprogrammer, vira eller orme i løbet af de seneste 12 måneder. I tillæg hertil svarede 22 procent, at deres organisation havde været udsat for en sikkerhedshændelse i forbindelse med deres offentlige website.

I årets løb har der været flere eksempler på brug af *SQL-injections* til at inficere sårbare websites med *exploit*-kode , se Figur 7. Ifølge Joe Stewart[21] var Asprox det første botnet, som udnyttede *SQL-injections*. Sidst på året spredte Download-AZN sig via *SQL-injections*, efter at en Microsoft 0-day-sårbarhed blev kendt.

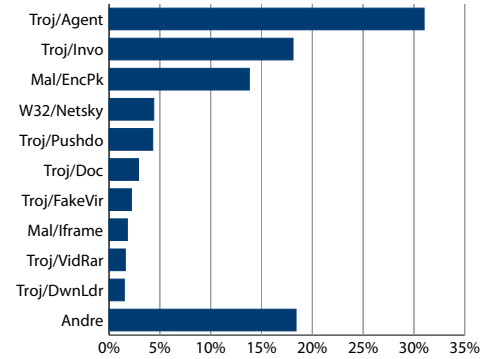
Trojaneren Asprox blev i første omgang kendt som et spambotnet, der udsendte phishing-mails. I foråret ændrede Asprox karakter og begyndte at foretage angreb via *SQL-injections* på sårbare websider. Asprox var i foråret og sommeren 2008 omdiskuteret i Danmark, da flere danske websider blev inficeret med Asprox. Botnettet brugte Google til at søge efter asp-sider som det angreb ved at indsætte et Iframe tag, som efterfølgende inficerede besøgende via en skadelig JavaScript-fil placeret på et andet domæne[22], typisk placeret i Kina. Scriptet udnyttede en række sårbare applikationer knyttet til webbrowseren.

I december 2008 blev der offentliggjort en 0-day-sårbarhed i Microsoft Internet Explorer på samme dag, som Microsoft udsendte sine opdateringer for december måned. Samme dag blev der udsendt et *exploit*, som udnyttede sårbarheden til at inficere sårbare webapplikationer. *Exploit*et installerede trojaneren Downloader-AZN. Ugen efter registrerede Microsoft en stigning på over 50 procent inficerede websteder. Udbredelsen af *exploitet* skete primært via kinesiske og taiwanske pornografiske websteder.

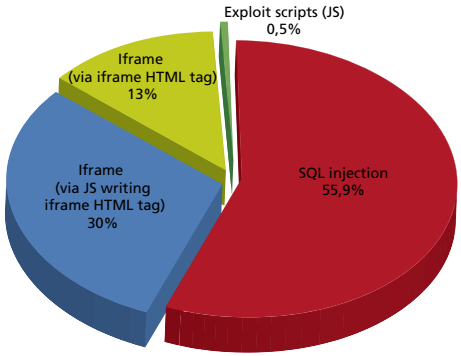
17 Sophos, 2008; "*Security threat report: 2009*".
18 Sophos, 2008; "*Security threat report: 2009*".
19 Sophos, 2008; "*Security threat report: 2009*".
20 Sophos, 2008; "*Security threat report: 2009*".
21 Darkreading.com, 2008; "*Bots use SQL injection tool in new web attack*".
22 Secureworks.com, 2008; "*Danmec/Asprox SQL injection attack tool analysis*".



Figur 5. Antal afsendte mails per inficeret mail[18].



Figur 6. Top 10 mail-baseret malware i 2008[19].



Figur 7. Inficeringstyper af webhostet malware på danske sites i 2008. Kilde Sophos.

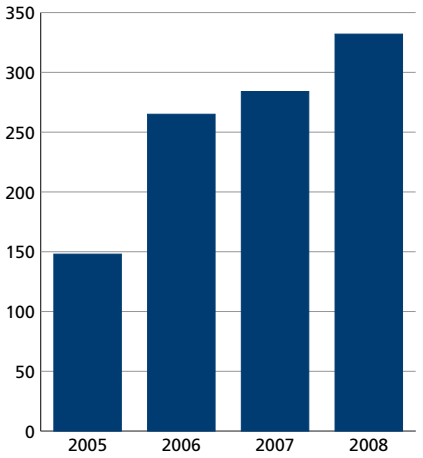
I 2008 blev der registreret flere angreb via trojanere og orme mod brugere af sociale netværkstjenester. Ormen Koobface angreb brugere af flere sociale netværk, bl.a. MySpace og Facebook. Den installerede en bagdør i de inficerede computere, som forbandt sig til botnet[23].

DK•CERT har i 2008 registreret en stigning på 17 procent i antallet af anmeldelser vedrørende danske websider inficeret med trojanske heste eller phishing-sider i forhold til 2007, se Figur 8. Tallene viser, at *malware* i højere grad også spredes via websites i Danmark, og phishing-websites er blevet mere udbredt. Det afspejler en global tendens for 2008.

Stigningen i phishing-sider på danske webservere er i sig selv en kedelig udvikling, men de dårlige nyheder stopper ikke her. Ser man på tal fra det tyske sikkerhedsfirma Clean MX, der indsamler og monitorerer oplysninger om phishing- og *malware*-sider i realtid, står det klart, at de danske webhosting-udbydere er langsomme til at reagere og lukke phishing-sites på deres servere. Median-levetiden for et phishing-site på danske servere er over 16 dage[24]. Det vil altså sige, at halvdelen af alle phishing-sider i Danmark når at være aktive over 16 dage, inden de lukkes. Lidt bedre står det til med hensyn til virus og anden *malware* – her er median-livetiden "kun" seks dage[25].

Det er især de små til mellemstore webhoteller, henvendt til private og mindre virksomheder, der er lang tid om at reagere. Men tendensen er ikke begrænset til dem. DK•CERT er således bekendt med et phishing-site placeret på en privat computer opkoblet via ADSL til en større dansk internetudbyder, der nåede at være oppe i 38 dage trods gentagne henvendelser til udbyderenen

En undersøgelse foretaget af DK•CERT viser at cirka 10 procent i deres organisation havde oplevet phishing-angreb indenfor det seneste år, hvor deres egen organisation stod som afsender. Således blev DK•CERT i starten af oktober opmærksom på, at flere danske universiteter oplevede målrettede phishing-forsøg mod deres brugere. Ansatte og studerende ved universiteterne fik tilsendt e-mails, der udgav sig for at være fra de pågældendes it-afdelinger: Teksten bad brugerne om at udlevere login og password til deres webmail-kontoer. Phishing-forsøget lykkedes i flere tilfælde, hvorefter kontoerne blev misbrugt til at udsende spam og Nigeria-mails. Ovenstående eksempel betegner en generel tendens for 2008, hvor it-kriminaliteten i stigende grad blev målrettet det enkelte offer.



Figur 8: Websites med trojanere og phishing-sider anmeldt til DK•CERT.

Målrettet phishing mod danske universiteter

"I e-mails, der udgiver sig for at være fra det pågældende universitets it-afdeling, forsøger angriberne at få universitetets brugere til at udlevere deres brugernavn og kodeord til universitetets webmail. Lykkes phishing-forsøget, vil kontoerne efterfølgende blive misbrugt til at udsende spam.

Phishing-mailene er blevet gradvist mere raffinerede i løbet af ugen. I starten var de kun på engelsk, men er nu set både på dansk og engelsk – ganske som man kan forvente af officielle mails i et universitetsmiljø."

DK•CERT, 2/10 2008[26]

23 Marshal.com, 2008; "*Social networking malware*".
24 http://support.clean-mx.de/clean-mx/phishing.php?country=dk&response=alive 15. Jan 2009
25 http://support.clean-mx.de/clean-mx/viruses.php?country=dk&response=alive 15. Jan 2009
26 DK•CERT, 2008; "*Målrettet phishing mod danske universiteter*".

3.2. Portscanninger

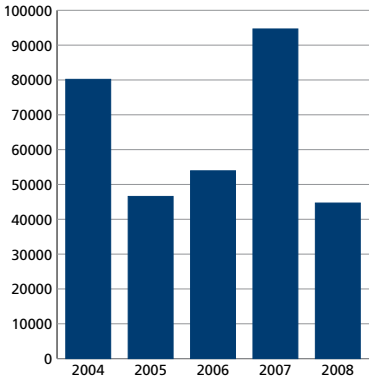
Antallet af anmeldte portscanninger behandlet af DK•CERT er i 2008 faldet til 44666, hvilket er på niveau med 2005, se Figur 9. En forklaring er delvist fraværet af nogle automatiserede kundeanmeldelser i 2008, men selv korrigeret for disse anmeldelser er der sket et drastisk fald. Samme tendens gør sig gældende internationalt. F.eks. modtog Internet Storm Center i 2008 kun 3,6 milliarder records mod 5,5 milliarder i 2007[27]. Også antallet af portscanninger registreret af Shadowserver.org er faldet gennem det sidste halvandet år[28]. At det er en tendens, der synes at fortsætte, illustreres ved, at antallet af portscanninger anmeldt til DK CERT var størst i årets første halvdel, se figur Figur 10.

Årsagen skal findes i, at udnyttelse af kendte sårbarheder via internettet i 2008 ikke længere var den primære angrebsmetode. Hvor de traditionelle portscanninger er lette at opdage og afværge, benyttes der i stigende grad angrebsmetoder, som enten ikke registreres eller ikke registreres som portscanninger.

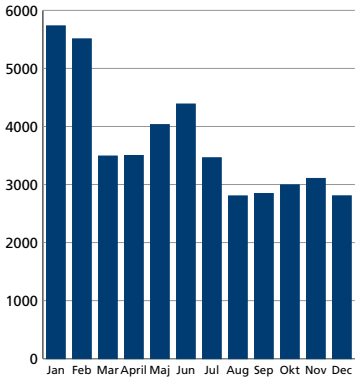
ICMP Ping på hele netsegmenter var i 2008 den hyppigste årsag til anmeldelser om portscanning til DK•CERT, se Figur 11. Scanninger mod NetBios, TCP port 137 og 139, der benyttes af Windows, udgjorde den største andel af de systemspecifikke scanninger. Også Microsofts SQL Server, port 1433 og 1434, var blandt de hyppigt scannede applikationer i 2008, kun overgået af scanninger mod port 1027, der blandt andet benyttes af Windows RPC tjeneste. Anmeldelser om scanning mod SSH (Secure Shell) på port 22 dækker i denne sammenhæng delvist over *brute-force* angreb, hvor der forsøges at logge på tjenesten ved at "gætte" brugernavn og kodeord.

Når TCP port 80 og 443, der benyttes til almindelig webtrafik, ikke er med på listen, skyldes det, at mange angreb på disse porte ikke opdages eller registreres som forsøg på kompromittering. Automatiserede forespørgsler ved hjælp af Google registreres f.eks. ikke som angreb, og et forsøg på *SQL-injection* er som sådan en legitim henvendelse, hvor det er værdien af de parametre, der forespørges med, der afgør, om der er tale om et angreb. Et eksempel på dette var årets udbrud af ormen der gav anledning til infektioner med Asprox, der ved *SQL-injection* lagde links til skadelige javascript-filer på sårbare websites. DK•CERT modtog i denne forbindelse ingen anmeldelser om scanninger med forsøg på *SQL-injection*, men udelukkende om websites, der var blevet ramt.

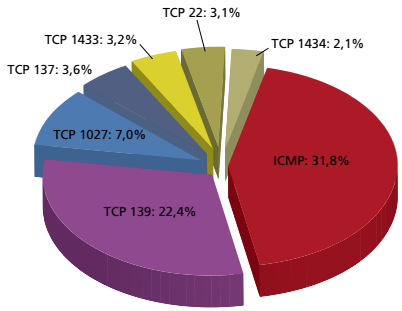
De fleste scanninger anmeldt til DK•CERT i 2008 blev foretaget fra IP-adresser i Asien, mens Danmark var nummer 18, se Tabel 5. På førstepladsen var USA, hvorfra 19 procent af alle anmeldte scanninger stammede. Danmarks relativt lave placering på listen er udtryk for, at 2008 var et år uden de store udbrud af orme, da mange af disse tidligere har scannet i eget netsegment eller segmenter der ligger tæt på det. Når USA, Kina, Sydkorea og Tyskland tillige figurerer på Sophos' liste over lande med flest websteder med *malware*[29], indikerer det at portscanninger primært udføres af inficerede maskiner.



Figur 9. Portscanninger anmeldt til DK•CERT siden 2004.



Figur 10. Månedlige portscanninger anmeldt til DK•CERT i 2008.



Figur 11. Hyppigst scannede portnumre i 2008, DK•CERT.

27 Internet storm center, 2009; "*Submission summary for last 1,000 days*".
28 Shadowserver.org, 2009; "*Scan charts*".
29 Sophos, 2008; "*Security threat report: 2009*".

4. Tingenes tilstand i 2008

Hvad skete der på it-sikkerhedsfronten i 2008? I dette afsnit gør vi status over nogle overskrifter for 2008. Vi dykker ned i tallene og fokuserer på overordnede sammenhænge, som vi mener repræsenterer en tendens, som det kan blive nødvendigt at tage højde for.

Selv om måske ikke alt ved første øjekast synes nyt, er det med danske briller ikke set tidligere. Som eksempel kan nævnes phishingangreb målrettet danske organisationers ansatte og danskproget rekruttering af muldyr til hvidvaskning af penge, som typisk er tjent ved phishing. Begge disse eksempler har eksisteret siden slutningen af 2007, men har taget til i 2008. Således svarede ca. 10 procent af de adspurgte i en undersøgelse foretaget af DK•CERT, at de i 2008 havde oplevet phishingangreb, hvor deres organisation var angivet som afsender. Til sammenligning var svaret i en tilsvarende amerikansk undersøgelse 27 procent[30].

Websites er nu hovedkilden til brugerinfektion med *malware*. Antivirusproducenten Sophos[31] angiver, at de hver 4,5 sekund opdagede en ny inficeret webside i 2008. 22 procent af de adspurgte i DK•CERT s undersøgelse svarede, at deres organisations offentlige websted havde været udsat for en sikkerhedshændelse. Således var den mest markante tendens i 2008, både herhjemme og i udlandet, en stigning i forsøg på *SQL-injections* af legale websider og heraf følgende *malware*-inficering af websitets besøgende.

Som i de seneste år var der i 2008 ingen alvorligere ormeangreb eller virusepidemier. Kendetegnende for de orme og virus angreb der var, er at de fleste var relateret til spredning af og brug af botnet. Brugen af botnet var et centralt element i den it-kriminalitet, som blev begået i 2008. Vi indleder derfor afsnittet med at gøre status på botnet, deres midler og metoder samt afledte effekter i 2008. Botnet er f.eks. et væsentligt element ved kriminalitetsformen identitetstyveri, som er et stigende problem, der beskrives i det følgende afsnit

Mens vi ikke i 2008 herhjemme er blevet ramt af den politisk betingede internetkriminalitet, var et par episoder fra udlandet i 2008 i mediernes søgelys. Vores forventning er, at vi ligesom med industrispionage vil se mere af dette i fremtiden. Også her spiller brugen af botnet en aktiv rolle, og vi har valgt at benytte det kommende afsnit til at gøre status på cyberwarfare og industrispionage.

Afslutningsvis gøres der status over nogle overordnede tendenser i organisationernes måde at opfatte og varetage it-sikkerhed på. Mens nogle af disse tendenser er naturligt afledt af en ændring i it-kriminalitetens væsen, er andre organisatorisk betinget eller opstået som følge af den teknologiske udvikling i it-sikkerhedsbranchen. Fælles må det dog formodes at disse tendenser vil pege fremad og præge organisationernes måde at varetage it-sikkerheden på i årene der kommer.

1	USA	19,0%
2	Kina	16,8%
3	Sydorea	9,0%
4	Japan	5,0%
5	Tyskland	3,7%
18	Danmark	1,0%

Tabel 5. Anmeldte lande ved portscanning mod danske IP-adresser, DK•CERT.

Danske jobsites spredte virus efter kinesisk hackerangreb

I slutningen af november 2008 blev en række danske jobwebsider hos organisationen Matchwork.com inficeret med *malware* efter vedholdende kinesiske hackerangreb. Angrebet betød at besøgende blev bedt om at installere en ActiveX-komponent, der angiveligt var fra Microsoft. Ved installationen blev der installeret en trojansk hest på pc'en.

Den administrerende direktør for Matchwork.com, Torben Dyhr, fortalte til Version2[32], at man konstant var udsat for angreb fra især kinesiske hackere, men at det var første gang, det var lykkedes dem at bryde igennem. Det var en menneskelig fejl, der var årsag til at angrebet lykkedes, og efter lukning af hullet blev der ikke konstateret datatab eller behov for genskabelse af data.

30 Computer Security Institute, 2008; "*2008 CSI computer crime & security survey*".
31 Sophos, 2008; "*Security threat report: 2009*".
32 Version2, 2008; "*Danske jobsites spredte virus efter kinesisk hackerangreb*".

4.1. Botnet status

Brugen af botnet er i dag en integreret del af den organiserede internetkriminalitet, hvad enten det drejer sig om *distrueret denial of service*-angreb, phishing eller anden indsamling og handel med data fra brugernes og organisationernes computere. På verdensplan er antallet af henholdsvis aktive botnet-pc'er[33] og *command and control servere*[34] til styring af botnet steget gennem 2008. Også Danmark er repræsenteret med både botnet-pc'er[35] og de centrale servere til styring af botnet[36].

Håndteringen af botnet-pc'er var i en amerikansk undersøgelse den hændelsestype, der i 2008 gav anledning til de næststørste økonomiske tab, kun overgået af økonomisk svindel[37]. 20 procent af respondenterne svarede, at de havde haft botnet-aktivitet på organisationens eget netværk. En spørgeskemaundersøgelse foretaget af DK•CERT viste, at 52 procent af de adspurgte danske organisationer havde været inficeret med botnetprogrammer og/eller virus i det forgangne år. Organisationernes korrigerende handlinger herpå var oftest at lukke de benyttede sikkerhedshuller i organisationernes netværkssystemer og installere opdateringer til eksisterende software. Undersøgelsen viste desuden, at 25 procent af de adspurgtes organisationer havde været ofre for *denial of service*-angreb.

DK•CERTs Trendrapport 2007 havde på grund af botnettets omfang fokus på Storm. Da Storm i midten af 2007 var størst, blev botnettet estimeret til at omfatte mellem en halv til 1 million kompromitterede computere i decentrale netværk og være ansvarlig for 20 procent af al verdens spam[38]. Udover spam blev Storm brugt til at udføre phishing og distribuerede *denial of service*-angreb. Storm benyttede sig af *social engineering*-metoder til at få ofret til at klikke på links i spammails eller på inficerede hjemmesider, hvorefter botnetprogrammet blev installeret.

I september 2007 aftog aktiviteten på Storm, og mængden af spam på verdensplan faldt støt. En årsag var, at Microsoft udsendte en opdatering, som indeholdte deres *malicious removal tool*, der efterfølgende har renset over 280.000 kompromitterede Windows-systemer[39]. En stor del af de inficerede systemer var Windows XP uden Service Pack 2 , se Figur 12. Igen i midten af september 2008 aftog aktiviteten på Storm, og der er ikke siden detekteret hverken spammails, *denial of service*-angreb eller *double fast flux*-aktivitet fra dette botnet[40].

Figur 12: Daglige spam-mængder afsendt fra Storm i 2008[41].

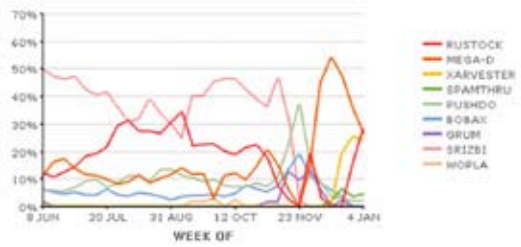
33 Shadowserver.org, 2009; "*Bot count yearly*".
34 Shadowserver.org, 2009; "*Botnet charts*".
35 Shadowserver.org, 2009; "*Botnet maps*".
36 Shadowserver.org, 2009; "*Drone maps*".
37 Computer Security Institute, 2008; "*2008 CSI computer crime & security survey*".
38 Theregister.co.uk, 2008; "*Storm botnet blows itself out*".
39 Marshal.com, 2008; "*Goodbye Storm?*".
40 Sudosecure.net, 2008; "*Storm Worm - Go away, we're not home*".
41 Marshal.com, 2008; "*Goodbye Storm?*".

Der har været flere bud på, hvad Storms inaktivitet skyldes. Det menes, at vi ikke har set det sidste til Storm[42]. Botnettet er under stadig udvikling og er i dag blevet opdelt i mindre segmenter, som er målrettet til udførelse af forskellig former for it-kriminalitet. Der synes dog at være et segment tilbage af Storm, som ikke foretager sig andet end i det skjulte at inficere nye computere. Joe Stewart fra SecureWorks mener, at segmenteringen af Storm kan være foretaget med henblik på videresalg af enkelte mindre segmenter[43]. Blandt mulige årsager til Storm inaktivitet nævnes blandt andet, at Joe Stewart på en Black Hat-konference offentliggjorde botnettets krypteringsmekanismer og *double fast flux* arkitektur, at bagmændene holder lav profil på grund af botnettets mediebevågenhed, eller at de blot holder ferie for udbyttet fra Storms tidligere succes[44].

Lukning af internetforbindelsen til webhostingfirmaet McColo i San José i november 2008 medførte et drastisk fald i mængden af spam. Efter anklager i Washington Post om at organisationens serverplads blev benyttet til styring af botnets, valgte firmaets to internetudbydere, Global Crossing og Hurricane Electric, at lukke McColos internetforbindelser. McColo havde inden da hostet centrale botnet-servere, som koordinerede udsendelsen af mellem 50 og 75 procent af verdens spam[45]. Det lykkedes efterfølgende McColo at få en midlertidig internetforbindelse via TeliaSonera, hvorigennem der blev overført data til servere i Estland og Rusland. Botnettene Srizbi og Rustock overlevede således begge lukningen af McColo[46]. Sikkerhedsfirmaet FireEye registrerede, at computere inficeret med den trojanske hest Rustock blev opdateret til at kontakte en ny server, og den globale spammængde begyndte herefter langsomt at stige igen[47].

I slutningen af november 2008 lukkede den estiske ISP Starline Web Services for internetadgangen til Srizbis centrale servere til styring af botnettet. Herefter har der ikke været spamaktivitet fra botnettet, der på sit højeste bestod af mere end 450.000 inficerede computere[48]. En række andre botnet har dog herefter været aktive. I slutningen af 2008 stod f.eks. botnettet Mega-D for en stor del af spamaktiviteten, mens andre kendte spambotnets ser ud til at være inaktive. Også botnettet Rustock, der oprindelig blev ramt af afbrydelsen af internetforbindelsen til McColo, har genvundet fordums styrke, se Figur 13.

Årelange kampagner om hvordan vi som brugere skal sikre os med antivirus-programmer, ikke have tiltro til links i e-mails og lignende, har givet it-kriminaliteten et nyt fokus. Mens botnet tidligere har spredt sig gennem orme og vira, har tendensen i 2008 været, at spredningen sker via inficering af sårbare legale websites, og efterfølgende brugerinficering gennem browseren eller hertil knyttede applikationer. I stigende grad installeres trojanere og botnetprogrammer på sårbare websteder ved hjælp af blandt andet *SQL-injection*, og efterfølgende inficeres de besøgende via sårbarheder i browseren. Den stigende kompromittering med botnetprogrammer fra websteder brugerne har tillid til, illustrerer vigtigheden af



Figur 13: Spam-mængder fra forskellige botnets i 2008[49]

42 Sudosecure.net, 2008; "*Storm worm - Go away, we're not home*".
43 Espn.com.com, 2008; "*Anatomy of a botnet*".
44 Darkreading.com, 2008; "*Storm may finally be over*".
45 Washingtonpost.com, 2008; "*Major source of online scams and spams knocked offline*".
46 News.dk, 2008; "*Spam-botnet vækket til live igen*".
47 Slashdot.org, 2008; "*McColo briefly returns, hands off botnet control*".
48 Arstechnica.com, 2008; "*Estonian ISP plays whack-a-botnet, has Srizbi on the run*".
49 Marshal.com, 2009; "*Spam statistics*".

at holde sine systemer opdateret med de seneste softwarerettelser.

Selvom botnetaktivitet stadig er det altoverskyggende problem, har vi i 2008 set, at målrettede indsatser midlertidig kan medføre, at bagmændene mister kontrollen med store dele af deres botnet. Hermed er den hellige grav dog ikke velforvaret. Bagmændene udvikler løbende deres metoder og teknikker, hvorfor indsatsen tilsvarende løbende bør fornyes[50] og i højere grad koordineres, nationalt såvel som internationalt.

4.2. Identitetstyveri

Identitetstyveri består i, at kriminelle giver sig ud for at være dem, de bedrager. En udbredt metode er at misbruge andres kreditkort til overførsel af penge eller køb af varer på nettet. I begge tilfælde ender regningen hos indehaveren af betalingskortet.

Phishing som middel til identitetstyveri er blevet en selvstændig industri. Ifølge en rapport fra Symantec satte it-kriminelle i perioden juli 2007 til juni 2008 varer til salg på internettet for en værdi af næsten 1,5 milliarder kroner[51]. Langt størstedelen af varerne var enten resultatet af phishing eller informationer, der kunne benyttes til at udfører phishing.

Som med manuel afluring af pinkoder og efterfølgende kreditkorttyveri samt lignende mere analoge processer, handler det også på internettet om at skaffe sig adgang til ofrenes kreditkort. Som en del af forsyningskæden indgår brugen af botnet-inficerede computere til distribution af phishingmails samt hackede webservere, hvorpå der kan placeres falske hjemmesider.

I starten af august 2008 blev 11 personer tiltalt i den hidtil største sag om identitetstyveri på internationalt plan. I den såkaldte TJX-sag fra USA blev 11 personer tiltalt for at have hacket sig ind på ni større amerikanske og canadiske butikskæder[52]. Ved at udnytte huller i butikkernes trådløse netværk fik de adgang til oplysninger om mindst 40 millioner kreditkort. Sagen illustrerer, at identitetstyveri er en grænseoverskridende forbrydelse. Tre af de tiltalte stammer fra USA, en fra Estland, tre fra Ukraine, to fra Kina og en fra Hviderusland. Efterfølgende forsikrede pressechef i PBS Søren Winge, at tilsvarende hændelser ikke kan foregå i Danmark, da vi er længere fremme med hensyn til de krav, som stilles til opbevaring og transaktion af kreditkortinformationer.

Kreditkortinformationer, loginoplysninger med mere skaffes ofte ved, at man udgiver sig for nogen, som ofret har tillid til, hvorved ofret narres til selv at afgive disse informationer. Således spiller forarbejde og psykologiske mekanismer i dag en større rolle i det, som kaldes *social engineering*. Gennem de seneste år er "fiskerne" blevet bedre til at benytte almindelige marketingprincipper. I stedet for blot at masseudsende mails fra "en stor bank" eller lignende, målrettes informa-

50 Darkreading.com, 2008; "*Storm may finally be over*".
51 Symantec, 2008; "*Symantec report on the underground economy july 07–June 08*".
52 Department of Justice, 2008; "*Retail hacking ring charged for stealing and distributing credit and debit card numbers from major U.S. retailers*".

tionen den enkelte gruppe af modtagere. Således modtog ansatte på flere danske universiteter i 2008 mails, der angiveligt var sendt fra it-administrationen, som bad dem verificere deres brugernavn og kodeord til universitets netværk.

I kølvandet på identitetstyveri følger et behov for lokale muldyr til hvidvask af penge. Muldyret er det sidste led i fødekæden og rekrutteres gennem falske jobannoncer, mails med tilbud om hjælp til overførsel af penge og lignende. Mens bagmændene oftest går fri, fanger usædvanlige pengeoverførsler herhjemme ofte bankernes og politiets øjne. I 2008 blev rekrutteringen af muldyr i stigende grad tilpasset det danske marked. Jobannoncer på danske jobsites og i dansksprogede mails forsøgte at lokke danskerne til at stille deres bankkonto til rådighed.

Statsadvokatens hvidvaskningssekretariat har i 2007 modtaget i alt 1349 underretninger om mulig hvidvask af penge, i forhold til 876 i 2006. Sekretariatets forventning til 2008 var, at denne udvikling, der hovedsageligt skyldes et skærpet fokus på hvidvaskning, ville fortsætte. Af de 1349 indberetninger var under 100 om transaktioner, hvor der var mistanke om hæleri på baggrund af it-kriminalitet. Resultater af efterforskningen viste i et vist omfang, at kriminaliteten blev styret fra Østeuropa[53].

Mens underretninger på baggrund af mistanke om phishing i løbet af 2007 var faldende, er det vores forventning, at vi vil se en stigning, som fortsætter de kommende år. Et stigende antal identitetstyverier medfører et øget behov for muldyr og set i lyset af den finansielle krise, kan det frygtes at stadig flere vil lade sig friste af tilbuddet om "nemme penge".

Udover phishing udført af internationale kriminelle bander har der været eksempler på, at personfølsomme data er tilvejebragt på anden vis. En dansk pc-bruger, Jesper Madsen, fortalte således til en konkurrence afviklet af årets Netsikker Nu-kampagne, hvordan han blev offer for identitetstyveri på World of Warcraft[55]. "*Min konto var blevet tømt for alt, hvad der var noget værd (hvilket var ikke så lidt). En af mine karakterer stod med en rose i hånden, og et brev lå i inventory, hvor der stod 'Better luck next time"*. Han mener, at hackeren har fået adgang til hans pc, fordi han hverken brugte firewall eller antivirus på det pågældende tidspunkt.
Ofte får forbryderne adgang til personfølsomme data ved at hacke sig ind på de systemer, hvor de ligger. Men i marts blev en amerikansk mand dømt for at have misbrugt oplysninger, han fandt ved at søge på fildelingstjenester af peer-to-peer-typen (P2P)[56]. Han brugte programmerne Limewire og Soulseek til at finde oplysninger, som han udnyttede til at oprette kreditkort i ofrenes navne. Kortene benyttede han så til at købe varer med for godt 400.000 kroner.

I sommeren 2008 oplevede brevkasseredaktør Suzanne Bjerrehuus en anden form for identitetstyveri. Nogen oprettede på Facebook en profil i hendes navn og førte sig frem, som om vedkommende var hende. I en klumme fortæller hun, at det med hjælp fra politiet lykkedes at få slettet den falske profil, men at det derudover ikke

53 Statsadvokaten for særlig økonomisk kriminalitet. Hvidvasksekretariatet, 2008; "*Årsberetning 2007*".
54 Netsikker Nu, 2008; "*Netsikker Nu magasinet*".
55 It-borger.dk, 2008; "*Computer hack havde store konsekvenser*".
56 Comon.dk, 2008; "*Fængslet for identitetstyveri via P2P*".

Muldyr blev dømt

"I januar 2008 blev en 26-årig dansker ved Vestre Landsret idømt et halvt års fængsel eller 150 timers samfundstjeneste. Han havde modtaget 315.000 kroner fra hackede netbankkonti i danske banker. Her var pengene sendt videre til en konto i Dubai. Landsretten mente, at fremgangsmåden lugtede så meget af svindel, at den tiltalte burde have indset, at der var tale om ulovligheder."

Netsikker Nu, 2008[54]

var muligt at få vedkommende dømt for noget.[57]

Identitetstyveri er et problem i vækst. De fleste phishing-angreb benytter sig af botnetteknologi til spredning af phishing-mails, upload af falske hjemmesider og lignende. Kun ved at bruge vores sunde fornuft kan vi som borgere undgå at ryge i phishingfælden. Der er dog andre steder, vi kan gribe ind. På samme måde som det er muligt at opdage finansielle transaktioner udført af muldyr, er det muligt at opdage og afværge botnetaktivitet på internetudbydernes netværk. Det synes straks vanskeligere, fra et isoleret dansk synspunkt at afskære spredningen af botnetprogrammer og falske hjemmesider, da de kan være placeret over hele kloden. Generelt bør der være større fokus på sikring af danske websites, hvad enten de tilhører hr. og fru Jensen eller en kommerciel organisation.

4.3. Cyber warfare og industrispionage

Den politisk motiverede it-kriminalitet ramte igen i 2008 mediernes søgelys, da webstedet NoOnProp8.com midt i den amerikanske valgkamp blev lagt ned af et *denial of service*-angreb[58]. Således blev sidste års rapports fokus på den politisk motiverede it-kriminalitet aktuel. Det var dog ikke det eneste tilfælde. Således blev flere hjemmesider, fora og communities, der arbejdede for demokrati i Burma, i løbet af sommeren ramt af *denial of service*-angreb. Disse formodes at være udført på foranledning af regeringen i Burma[59].

I forbindelse med konflikten mellem Georgien og Rusland i august 2008 var det ikke kun politiske og militære midler, der blev taget i brug[60]. Et storstilet angreb, angiveligt udført af russiske hackere med forbindelse til det berygtede *Russian Business Network*, lammede store dele af den georgiske it-infrastruktur. Hvorvidt angrebet var koordineret fra regeringsside eller blev foretaget spontant af grupper, der støttede den russiske side, står hen i det uvisse.

Med NATO's og EU's hovedkvarter placeret i Bruxelles blev der ifølge McAfee[62] i maj fremsat beskyldninger om internetangreb mod Belgien. Denne gang Skulle Kinesere stå bag.

Stadig flere værdifulde oplysninger opbevares i digital form. Det kan være kundedatabaser, regnskabsdata eller planer for nye produkter. Da organisationerne samtidig via internet bliver mere forbundet med omverdenen, øges risikoen for at miste fortrolige data ad denne vej.

Russian Business Network (RBN)

Russian Business Network er en organisation, som for en høj pris bl.a. tilbyder internetadgang og *bullet-proof hosting* websteder med børnepornografi, phishing, botnetaktivitet og lignende. Derudover er organisationen med base i Skt. Petersburg mistænkt for at stå bag botnettet Storm. Den er engageret i alle former for it-kriminalitet, heriblandt distribution af spam og malware[61]. Organisationer, som forsøger at modvirke netværket, er set blive ramt af *denial of service*.

Russian Business Network har ikke i 2008 været synlige og aktive.

57 Ekstrabladet, 2008; "*Bjerrehuus: Falske profiler er helt lovlige!*".
58 Version2, 2008; "*Cyberangreb optrapper bitter valgkamp*".
59 McAfee, 2008; "*McAffee virtual criminology report*".
60 Version2, 2008; "*Hackere invaderer georgiske websteder*".
61 Wikipedia,org; "*Russian Busines Network*".
62 McAfee, 2008; "*McAffee virtual criminology report*".

Selv om der ikke herhjemme i medierne har været alvorlige sager om industrispionage, beskriver PET i årsberetningen for 2006-2007 en stigende interesse rettet mod uretmæssig indsamling af information vedrørende f.eks. forskning og teknologi[64]. Også DK•CERT har været i forbindelse med organisationer, der mistede data, som kunne benyttes af organisationens konkurrenter. I et tilfælde fik en gæst i organisationen lejlighed til at være alene med en filserver i ca. fem minutter. I den periode koblede han sit digitalkamera til serveren via USB og overførte en mængde værdifulde data. I en anden sag fik en direktør stjålet sin bærbare pc fra bagsædet i en bil. Senere lancerede en konkurrerende organisation et produkt og et roadmap, der meget lignede det, hans organisation arbejdede med.[65]

Ovenstående illustrerer et behov for at beskytte mobile enheder. Hvis data på den bærbare pc havde været beskyttet med kryptering, kunne uvedkommende ikke have læst dem. Og hvis serveren var indstillet til kun at give adgang til godkendte USB-enheder, havde digitalkameraet ikke fået lov til at læse data på den.

At også mere traditionelle hackerangreb forekommer, er følgende et eksempel på. Autoreservedelsfirmaet FTZ anmeldte i december 2007 sin konkurrent Carl Christensen A/S til Rigspolitiets afdeling for it-kriminalitet. Firmaet havde mistanke om, at konkurrenten havde hacket sig ind på FTZ's servere og hentet oplysninger om kunder, priser og rabatter.
"*Det ser ud til, at vi har mistet kunder som en følge af den uberettigede it-indtrængen. Vi kan konstatere, at en række af de kunder, der har været opslag på i systemet, og hvor man kan se vores rabatstruktur, efterfølgende har fået et godt tilbud*" sagde direktør i FTZ, Michael Juul Hansen, til Fyens Stiftstidende.[66]

Det nuværende danske engagement i Irak og Afghanistan giver ikke umiddelbart grund til at frygte koordinerede it-angreb mod den danske infrastruktur. Politisk yderliggående grupperinger har med angrebet på NoOnProp8.com vist, at de er i stand til at samle den fornødne ekspertise og kapital til at benytte internettets muligheder til at ramme anderledes agerende organisationer. Vores vurdering er derfor, at der er større risiko for, at danske organisationer hvis produkter eller budskaber ikke stemmer overens med yderliggående politiske grupperingers, bliver udsat for sporadiske angreb.

Fyringer som følge af den økonomiske krise giver anledning til at frygte, at utilfredse medarbejdere forsøger at øge deres markedsværdi hos konkurrerende organisationer ved hjælp af fortrolige produkt- eller kundedata. Allerede i dag udgør organisationernes egne ansatte, ifølge en undersøgelse foretaget af DK•CERT, en lige så stor trussel i forhold til uautoriseret adgang til organisationsdata som eksterne. Denne balance frygtes at forrykke sig de kommende år.

Cyberangreb optrapper bitter valgkamp

"Torsdag blev webstedet NoOnProp8.com ramt af et distribueret *denial of service*-angreb, oplyser organisationen bag webstedet.

Proposition 8 er et lovforslag fremsat af den religiøse højrefløj, som vil forbyde ægteskaber mellem homoseksuelle i delstaten Californien.

Forslaget får især økonomisk støtte fra medlemmer af mormonkirken uden for Californien. Mens præsidentkampagnerne har en begrænsning for personlige donationer på 2.300dollars, så har de lokale forslag ikke det samme loft.

Ifølge No On 8 talsmand Geoff Kors skete der ingen indbrud i it-systemerne i forbindelse med angrebet mod serverne torsdag, men organisationen var ude af stand til at modtage indbetalinger, mens angrebet stod på"

Version2, 31/10 2008[63]

63 Version2, 2008; "*Cyberangreb optrapper bitter valgkamp*".
64 Politiets Efterretningstjeneste PET, 2008; "*Årsberetning 2006-2007*".
65 Version2, 2008; "*Dansk it-industrispionage tager til*".
66 Business.dk, 2008; "*Reservedelsgigant anmelder konkurrent for it-indbrud*".

4.4. Fra sikkerhedsfronten

Siden årtusindeskiftet er der gradvist sket et skifte i, hvorledes vi i organisationerne opfatter og varetager it-sikkerhed. Fra at være en driftsteknisk nødvendighed opfattes it-sikkerhed i stigende grad som en integreret del af det at drive forretning. Det afspejles i en verdensomspændende undersøgelse foretaget af PricewaterhouseCoopers, hvor 57 procent af de adspurgte organisationer i 2007 havde en sikkerhedsstrategi, mod 37 procent tre år tidligere[67].

Der er sandsynligvis ikke nogen entydig forklaring på denne udvikling. Undersøgelser i både Danmark og udlandet har dog vist, at implementering af formelle it-sikkerhedspolitikker og indførelsen af *Sarbanes-Oxley* loven, *SOX*, har skærpet ledelsens interesse for it-sikkerhed og flyttet fokus fra teknologi til *god selskabsledelse*. I en undersøgelse foretaget af DK•CERT i december 2008 svarede hovedparten af de adspurgte, at indførelsen af *DS 484* havde øget it-sikkerheden i deres organisation og til dels flyttet fokus mod *god selskabsledelse*. Populært sagt kan man sige, at med stigende fokus på risikovurdering har revisorerne indtaget serverrummet og gjort it-sikkerhed spiselig for ledelsen.

Nedenstående faktorer kan være medvirkende årsager til, at it-sikkerhed i stigende grad opfattes i et forretningsperspektiv snarer end i et it-perspektiv:

- Ændrede lovkrav sætter fokus på risikostyring.
- Stadig mere flydende systemgrænser og stigende kompleksitet af organisationens processer og systemer har nødvendiggjort formelle strukturer omkring it-sikkerhed.
- Generel fokus på *god selskabsledelse* har skabt stigende krav til implementering af formelle og synlige it-sikkerhedspolitikker.
- Implementering af strukturer for *entreprise arkitektur*, der blandt andet indbefatter it-sikkerhed.
- Stigende globalisering og professionalisering, også hos de it-kriminelle.

Med stigende involvering fra ledelsen følger et forretningsmæssigt syn på it-sikkerhed samt organisatorisk lettere implementering af forandringsprocesser. Netop ledelsesinvolvering[68] og forandringsledelse[69] betegnes af det europæiske it-sikkerhedsagentur, ENISA, som en nødvendig tilgang til udbredelse af it-sikkerhedspolitikken i hele organisationen, i form af implementering af succesfulde *awareness*-programmer. Når lige mange udefrakommende og organisationens egne medarbejdere i 2008 havde opnået uautoriseret adgang til organisationens digitale aktiver, kan en udfordring blive, på den ene side at vise tillid til organisationens medarbejdere og på den anden side begrænse og kontrollere dem. En udfordring der kun til dels finder sin løsning ved gennemsigtighed omkring organisationens it-sikkerhedsprocesser og vellykkede *awareness*-kampagner.

Med forretningen i centrum for it-sikkerheden har fokus tilsvarende flyttet sig fra tilgængelighed og integritet til i højere grad også at inkludere fortrolighed af data. Som en naturlig følge af dette har systemer til kryptering og *Data Leak*

67 PricewaterhouseCoopers, 2008; "The 5th annual global state of information security, the end of innocence".
68 ENISA, 2008; "Obtaining support and funding from senior management".
69 ENISA, 2006; "A users' guide: How to raise information security awareness".

Prevention, DLP, i 2008 vundet indpas i de danske organisationer. Det er yderligere styrket ved organisationernes behov for mobilitet, der har skabt et marked for kryptering, overvågning og fjernstyring af mobile enheder. Man kan sige, at når chefens bærbare computer, mobiltelefon med videre stjæles, og der efterfølgende opstår usikkerhed om hvilke data der var på dem, skabes der incitamenter til at undgå tilsvarende hændelser. It-sikkerhed er blevet nærværende og forståelig for ledelsen, der har implementeret systemer til at undgå tilsvarende fremtidige hændelser.

Perimeteren er i 2008 ikke længere det eneste eller vigtigste værn mod it-kriminalitet. Organisationen og dens systemer og ansatte, er i dag under angreb fra mange kanter. It-sikkerhed varetages både på perimeteren, centralt på organisationens servere og på de enkelte klienter. Den væsentligste udfordring kan blive også at implementere it-sikkerhed i hovedet på de brugere, der benytter organisationens ressourcer. *Awareness* var derfor i 2008 et centralt element af it-sikkerhed. Den væsentligste forskel var, at man i takt med implementeringen af standardiserede it-sikkerhedspolitikker, og brugerne som målet for it-kriminalitet, tog begrebet til sig i organisationerne og udviklede kampagner og materiale, der havde til formål at øge viden og håndtering af it-sikkerhed blandt de ansatte.

Når brugerne i højere grad inficerer sig selv med *malware*, har de mønstre, der tidligere har været benyttet til opdage angreb ændret sig. F.eks. kan det i firewall-loggen eller på IDS'et være stort set umuligt at opdage en inficeret computer, der selv kobler sig til en anden maskine på internettet for at modtage instrukser. Derfor benyttes der som supplement til disse i stigende grad systemer, der kan sammenkæde logs fra flere kilder. Således kan en hændelse fra f.eks. event-logs sammen med data fra f.eks. applikations- og firewall-loggen gøre det muligt hurtigere at detektere og afværge nye angreb og yderligere systemkompromittering. Intelligensen, eller evnen til i realtid at genkende nye mønstre fra stadig flere kilder, må for disse systemer formodes i de kommende år at stige.

En række tendenser muliggjort af såvel teknologiske fremskridt som organisatoriske forandringer, vil i de kommende år give os potentiale til at øge den enkelte organisations it-sikkerhed. Spørgsmålet er blot, om ikke også den it-kriminalitet vi forsøger at beskytte os mod vil forandre sig tilsvarende. Og hvad med den borger eller organisation, der ikke har muligheden for at implementere de seneste landvindinger? Vil de blive ofre for en it-kriminalitet, der i stigende grad målrettes de markeder hvor succesraten er størst?

Data Leak Prevention (DLP)

DLP defineres som systemer, der identificerer, overvåger og beskytter data, på grundlag af centralt definerede politikker[70].

DLP håndterer data, der er gemt, i bevægelse eller i brug, mod uautoriseret brug og tab af fortrolige data. Beskyttelsen sker ved dybdegående analyse af data og et centralt styret management framework[71]. DLP kan ske på den enkelte brugers system eller styres centralt via netværkssystemer. DLP er således også med til at beskytte organisationer mod *social engineering* og intern misbrug af data.

70 Securosis.com; "*Understanding and Selecting a Data Loss Prevention Solution*".
71 Wikipedia "*Data loss prevention products*".

5. Hvad fremtiden bringer

Skuer vi et år tilbage i tiden, ville kun de færreste af os have kunnet forudset den udvikling inden for it-kriminalitet og -sikkerhed, som vi har oplevet i 2008. Nedenstående fremskrivninger af eksisterende tendenser og forudsigelser af nye trends skal derfor ikke tages som en absolut sandhed. Vi tror dog at den stigende organisering, professionalisering og opfindsomhed hos de it-kriminelle vil fortsætte også i de næste år, med stigende udfordringer for os der arbejder med it-sikkerhed til følge. It-kriminalitet er en god forretning, og med stigende mængde og værdi af aktiver der gøres tilgængelige digitalt, er der ingen grund til at tro, at denne udvikling vil stoppe.

De tendenser, der har været gældende i 2008 vil fortsætte i de kommende år. Således vil f.eks. brugen af sociale netværkstjenester fortsat stige, også på arbejdspladserne. Selvom vi i dag ikke har oplevet alvorligere it-sikkerhedsmæssige problemer med brugen af dem, vil sociale netværkstjenester blive et emne, som man i de kommende år kan blive nødt til at tage stilling til i organisationerne.

Nedenfor identificeres nogle tendenser inden for it-kriminalitet, som vi mener kan gøre sig gældende i de kommende år. Herefter beskrives nogle afledte udfordringer, vi som borgere, organisationer og samfund kan komme til at stå over for.

5.1. It-kriminalitet

It-kriminalitet er en god forretning, og der er ingen grund til at formode, at udviklingen inden for dette felt vil stoppe i de kommende år. Bagmændene vil fortsætte med at målrette deres aktiviteter derhen, hvor succesraten og udbyttet er størst og risikoen mindst. Således kan vi i fremtiden forvente en større variation i typen af angreb. Belært af erfaringerne i 2008 vil man i højere grad forsøge at skjule sine aktiviteter og gøre dem mindre sårbare for ekstern indgriben. Som følge af dette kan vi forvente færre, men til gengæld mere målrettede og succesfulde angreb på danske borgere og organisationer.

De it-kriminelle bagmænd har til alle tider forsøgt at sløre deres spor. I 2008 var det hovedsageligt de små fisk, der blev fanget ved almindelige mekanismer til opdagelse af hvidvaskning af penge. Denne tendens er med udvikling og brug af botnet blevet en integreret del af it-kriminaliteten. Fremtidige botnets vil kommunikere over flere kanaler gennem flere lag og med brug af stadig stærkere kryptering. Vi vil samlet set se en voksende aktivitet, fra flere mindre og mere specialiserede botnets.

De hurtigtspredende orme og vira har for de organiserede kriminelle grupper udspillet deres rolle. Således bliver trojanske heste og botnet-programmer også i fremtiden de hyppigst distribuerede typer *malware*. De vil fortsat sprede sig via sårbare webapplikationer, men også gennem *widgets* og applikationer benyttet på sociale netværkssider, som i flere tilfælde er blevet kritiseret for deres manglende sikkerhed.

Motivet for spredningen af *malware* vil fortsat være adgang til borgernes eller organisationernes bankkonti, hvad enten der er tale om identitetstyveri, trusler om offentliggørelse af personlige data eller *denial of service*-angreb. Midlerne kan dog være anderledes. Vi mener således, at vi i fremtiden kan opleve *malware*, der i højere grad har til formål at indsamle personlige data fra brugernes egen computer, sociale netværkssider og andre steder, til målretning af f.eks. spam og phishing-kampagner.

Identitetstyveri har vist sig som en effektiv måde at lave "forretning" på, som vi tror vil være i vækst. I DK•CERT forventer vi således en stigning i antallet af phishing-mails og -websites, der vil være stadig mere målrettede, avancerede og troværdige. Erfaringerne har vist, at det kan betale sig at målrette phishingen til mindre grupper og formulere teksten, så den sprogligt kan forveksles med originale websider og e-mails. Disse forventninger baseres blandt andet på opdelingen af botnet i små forretningsnetværk målrettet til f.eks. spam, phishing og salg af følsomme data.

Som middel til inficering af brugernes computere har *click-jacking* været omdiskuteret i årets løb[72], efter at Robert Hansen og Jeremiah Grossman aflyste den del af deres præsentation på OWASP sikkerhedskonference d. 24. september, der omhandlede *proof of concept*-kode til *click-jacking*-angreb i Adobe Flash. Der har siden været diskussioner om omfanget af sårbarheden samt hvordan *click-jacking* kan udnyttes og hvor nemt.

Bruce Schneier definerer *click-jacking* således:
"*Clickjacking lets hackers and scammers hide malicious stuff under the cover of the content on a legitimate site. You know what happens when a carjacker takes a car? Well, clickjacking is like that, except that the click is the car.*"[73]

Click-jacking kan udnyttes til at få en bruger til at klikke på skjult indhold i en brugergrænseflade. Det betyder, at brugeren kan risikere at klikke på indhold fra en anden webside eller aktivere funktioner i et system, som f.eks. at give angriberen adgang til at aktivere og se indholdet af et webkamera. Robert Hansen har på sin blog udsendt 12 forskellige angrebsmetoder, hvoraf der kun er fundet en løsning til 2[74]. Ifølge Hansen og Grossmans er *click-jacking* kun muligt på grund af den fundamentale måde, hvorpå browsere fungerer[75]. Forskerne understreger dog, at det ikke er den værste sårbarhed nogensinde. *Click-jacking* er en omstændelig måde at udnytte en brugers system på, og f.eks. *cross-site scripting* og bufferoverløb giver i højere grad adgang til information i sårbare systemer[76]. Hvorvidt *click-jacking* bliver en anvendt angrebsmetode, kan der foreløbig kun gættes på.

Click-jacking er kun ét muligt scenarie for, hvorledes spredningen af *malware* vil blive mere kompleks. Fælles er dog, at den primære kilde til spredning, stadig vil være sårbare webapplikationer, som brugerne har tillid til. Således forventer vi en stigning i forsøg på misbrug af sårbare webapplikationer ved brug af *SQL injection*, *cross-site scripting* og lignende angrebsmetoder, der i stigende grad målrettes det

72 Sectheory.com, 2008; "*Clickjacking*".
73 Schneier.com, 2008; "*Schneier on security*".
74 Ha.ckers.org, 2008; "*Clickjacking details*".
75 Video.google.com, 2008; "*New zero-day browser exploits – clickJacking*".
76 Video.google.com, 2008; "*New zero-day browser exploits – clickJacking*".

enkelte site.

Ligesom som PET[77] har vi en forventning om at industrispionage vil være et emne som organisationerne i stigende grad bliver nødt til at tage højde for. Vi tror dog ikke at vi via medierne, eller hos DK•CERT, vil opleve flere tilfælde, da mistanken om lækage af fortrolige data oftest holdes internt eller kun deles med politiet, af hensyn til organisationens omdømme.

5.2. Fremtidens udfordringer

Botnet-aktivitet er involveret i store dele af den organiserede it-kriminalitet og er en stigende udfordring for både organisationer og borgere. Med stadig mere specialiserede og avancerede botnet, bliver de vanskeligere at opdage og stoppe. Vi så i 2008, at lukningen af webhosting-firmaer verden over medførte en periodisk reduktion af udsendt spam.

Mens det på borgernes og organisationernes netværk kan være vanskeligt at detektere og stoppe botnetaktivitet, har ISP'erne mulighed for at analysere netværkstrafik og identificere mønstre, som viser botnet-trafik og placeringen af ulovlige *command and control*-servere. Med en sådan viden vil det være muligt at få stoppet uhensigtsmæssig netværkstrafik og blokere adgangen til botnettenes centrale *command and control*-servere, hvad enten disse er placeret i Danmark eller i udlandet. Derfor er det nødvendigt, at ISP'erne deltager og samarbejder, hvis vi skal komme it-kriminaliteten til livs.

I en australsk undersøgelse[78] af hjemmebrugernes adfærd i forhold til it-sikkerhed mente 92 procent, at deres ISP burde informere dem, hvis ISP'en modtog information, der indikerede, at kundens computer var inficeret. En praksis der ifølge DK•CERTs erfaringer herhjemme langt fra er tilfældet. Information er nøglen til sikring af it-systemer, hvad enten disse er placeret hos den enkelte borger eller i virksomhederne. ISP'erne har et medansvar. Udfordringen bliver at koordinere et effektivt samarbejde omkring opdagelse, blokering og varsling af aktiviteter, der kan føre til misbrug af danskernes ressourcer.

Når legale applikationer er under pres som midlet til at ramme den enkelte borger, bliver det i stigende grad en udfordring at kontrollere validiteten af de data, der eksponeres via organisationens website, selv om disse ikke umiddelbart krænker lovgivningen. I 2008 var hyppigt brugte metoder således inficerede bannerannoncer, falske dating- og job profiler samt parametre, som ved brug af *SQL injection* indsatte henvisninger til *malware* i databasen, der senere blev eksponeret for andre brugere. Mens f.eks. brugen af inputvalidering på de enkelte applikationer kan dæmme op for sidstnævnte, er det vanskeligere at kontrollere validiteten af f.eks. en datingprofil eller jobannonce. En endnu større udfordring kan være at skulle stille spørgsmålstegn ved indhold leveret af kunder og leverandører, med hvem der ellers udvises gensidig tillid.

77 Politiets Efterretningstjeneste PET, 2008; "*Årsberetning 2006-2007*".
78 AusCert, 2008; "*Home users computer security survey 2008*".

Et andet aspekt af webteknologiens udvikling er den stigende brug af webservices, widgets og dashboards - ressourcer, der deles mellem flere uafhængige websites. Det har skabt mindre gennemsigtighed for brugeren. Hvad enten de benyttes i brugerens eget miljø eller via websider denne besøger, er det ofte vanskeligt at gennemskue, hvor koden kommer fra og hvem der leverer indholdet. Som vi tidligere har set med inficerede bannerannoncer eksponeret på legale websider, kan populære widgets, dashboards og lignende blive fremtidige midler til spredning af malware og derved blive en potentiel udfordring for de danske organisationer.

I denne sammenhæng spiller sociale netværkstjenester, der i større udstrækninger anvendes i både private og arbejdsmæssige sammenhænge, en væsentlig rolle. Vi tror således, at der i fremtiden vil være flere eksempler på, at brugere bliver offer for it-kriminalitet via sådanne tjenester. Chefkonsulent i DK•CERT Shehzad Ahmad udtalte følgende til Computerworld[79]:
"*Vi modtager flere og flere rapporter om forsøg på misbrug på sociale tjenester. Den slags tjenester er særligt udsatte, fordi brugerne oplever en - ofte falsk - tryghedsfølelse, når de befinder sig på deres private side på det sociale netværk. Derfor klikker mange brugere helt ukritisk på alle de links, som de modtager.*"

De sociale netværkstjenester benytter sig i stigende grad af tredjepartsapplikationer, der kan blive et potentielt problem for de organisationer, der tillader brugen af sociale netværkstjenester. Disse applikationer kan have skjulte hensigter og forsøge at få brugeren til at klikke på links, som inficerer computeren med *malware*.

På de sociale netværkstjenester lurer også faren for *social engineering*. De oplysninger som fortælleglade borgere lægger op om deres privat- og arbejdsliv, kan udover til målretning af spam- og phishing-kampagner, også benyttes til at indlede en korrespondance, som har til formål at få adgang til følsomme data. Hvad enten kontakten er privat eller arbejdsrelateret, er der ingen garanti for validiteten af den profil, der kommunikeres med.

Organisationerne bliver nødt til at tage stilling til om brugen af sociale netværkstjenester blot er en tidsrøver eller udgør en potentiel sikkerhedsrisiko. Emnet bør diskuteres og inkluderes i it-sikkerhedspolitikken. Den enkelte organisation må vurdere risikoen ved brug af disse tjenester, og hvordan brugen af dem evt. skal begrænses.

Hvor der tidligere blev talt om *pervasive computing*, eller it i alting, er virkeligheden, at der i stigende grad er netværk i alting. Således er mediacenteret, spillekonsollen og tv'et allerede i dag koblet på samme netværk som hjemmearbejdspladsen og mobiltelefonen. Herved åbnes for en stigning i mængden af sårbare applikationer, der kan give utilsigtet adgang til borgerens applikationer og data. Konsekvensen kan på sigt være alt fra en stigning i kompromitteringer af organisationer via hjemmearbejdspladser, identitetstyverier, afpresninger med truslen om offentliggørelse af private data eller indbrud efter at tyverialarmen forinden er blevet afbrudt via internettet. Det er i sidste ende kun teknologien og fantasien der sætter grænsen. Det kan således blive en udfordring at håndtere den stigende kompleksitet af interagerende systemer der nu også har sneget sig ind i borgernes hjem. Hvordan kan borgeren rette sårbarheder i systemer, som denne ikke har

79 Computerworld.dk, 2009; "*Bør din virksomhed spærre for Facebook og Twitter?*".

forstand på og måske end ikke kender eksistensen af?

Mens Danmark ikke synes som et naturligt mål for cyberwarfare, har Muhammed-krisen vist at dette kan ændre sig. I så fald vil det sandsynligvis ikke være vores infrastruktur, der står på spil, men snarere ministerier, internationalt agerende danske organisationer samt tilfældige ubeskyttede websites. Med den stigende mængde og værdi af data, der lagres digitalt, skabes der tilsvarende et marked for denne type af informationer, hvorfor truslen om industrispionage er mere nærliggende. Det understreges også af Politiets Efterretningstjeneste i deres seneste årsrapport[80]. Med stigende internationalisering, også hos de organiserede kriminelle, bliver markedet for disse data i stigende grad internationalt. Herved følger en stigende efterspørgsel og deraf afledt stigende pris på fortrolig organisationsdata.

En undersøgelse foretaget af DK•CERT viser, at det i 2008 ligeså ofte var interne som eksterne, der skaffede sig uautoriseret adgang til organisationernes systemer og data. Den økonomiske krise kan medføre fyringer og utilfredse medarbejdere, der kan have interesse i tyveri af data eller elektronisk hærværk. F.eks. kan. fyrede medarbejdere forsøge at øge deres markedsværdi hos en konkurrerende organisation, ved at medbringe fortrolige produkt- eller kundedata. Det kan således blive en udfordring også at beskytte adgangen til organisationens systemer og data mod organisationens egne medarbejdere. Det intensiverer en række dilemmaer mellem på den ene side at vise tillid til organisationens ansatte og på den anden side at begrænse og kontrollere dem.

Efter skandalen i IT Factory i starten af december 2008 vil der fra lovgivernes side være en naturlig fokus på bestyrelsens og revisionens rolle i organisationsdriften. En række organisationsskandaler i 2001 medførte indførelsen af *Sarbanes-Oxley* loven, *SOX*, i USA, som skærpede kravene til primært risikostyring og revision af organisationerne. På samme vis kan man forestille sig, at der herhjemme vil komme skærpede lovkrav til disse områder, der begge kan få relevans for varetagelsen af it-sikkerheden. Hvorvidt en eventuel revideret dansk lovgivning vil være mere udførlig end den i 2008 indførte *euroSOX* er endnu for tidligt at gætte på. En ændring af de retningslinjer der skal følges, vil dog altid være en udfordring, om ikke andet på det organisatoriske plan.

80 Politiets Efterretningstjeneste PET, 2008; *"Årsberetning 2006-2007"*.

6. Opsamling

Selv om det lykkedes en række ISP'er i udlandet midlertidigt at reducere aktiviteten fra enkelte botnet, var botnet et væsentligt element af den organiserede it-kriminalitet i 2008. Spredningen af botnet-programmer foregik primært via sårbare browsere og webapplikationer, som brugerne havde tillid til. Som resultat kunne vi i DK•CERT konstatere et fald i såvel anmeldelser om portscanninger såvel som aktivitet fra orme og vira i forhold til tidligere år. En væsentlig tendens for 2008 var således en vækst i aktiviteter, der knytter sig til brugen af botnets. Særligt identitetstyveri, bl.a. som resultat af målrettede phishing-angreb, har været i vækst.

Mens vi i Danmark ikke oplevede den politisk motiverede it-kriminalitet i 2008, var der i udlandet flere tilfælde af cyberwarfare. Muhammed-krisen har tidligere vist at dette pludseligt kan ændre sig, og i 2008 viste politiske grupperinger, at de var i stand til at mobilisere den fornødne kompetence og/eller kapital. Danske organisationer, der ytrer sig i modstrid med rabiate politiske grupperinger kan derfor blive et fremtidigt mål for angreb.

Som resultat af globalisering er markedet og dermed prisen for fortrolige produkt- og kundedata vokset. Mens industrispionage kun i sjældne tilfælde når offentlighedens lys, spår PET, at danske virksomheder i stigende grad kan blive mål for indsamling af fortrolige data[81]. Vi mener dog, at den største risiko kommer fra organisationens egne medarbejdere, der som resultat af den finansielle krise bliver sagt op.

Siden årtusindeskiftet er it-sikkerhed i stigende grad blevet varetaget som en organisatorisk snarere end en it-teknisk disciplin. Man har i organisationerne fået øjnene op for de forretningsmæssige risici ved brugen af it, hvorfor begreber som risikostyring og revision i høj grad også vedrører driften af organisationens it-systemer. Som en følge af de tekniske muligheder og globale tendenser er organisationens perimeterbeskyttelse i stigende grad flyttet ud på klienterne. Organisationerne har fået større fokus på tab af data og implementeret tekniske løsninger til at imødegå dette.

Det er vores forventning, at der i fremtiden ikke bliver anmeldt flere it-sikkerhedshændelser til DK•CERT, snarere færre. Derimod vil de hændelser, hvor DK•CERT bidrager med analyse, efterforskning og rådgivning, stige i antal, kompleksitet og tidsforbrug. Vi tror, at politiet og den finansielle sektor vil opleve en stigning i henvendelser primært vedrørende misbrug af kreditkortinformationer og andre former for identitetstyveri eller trusler om offentliggørelse af fortrolige eller personlige data.

Nedenfor samles der op på nogle af de tendenser, der er identificeret tidligere i rapporten. Det vil på nettet være muligt at finde lignende lister over trends i 2008 og forudsigelser om kommende tendenser, der afviger fra vores. Afvigelserne bør ikke ses som udtryk for, at den ene liste er mere rigtig end den anden, men snarere som et udtryk for forskel i synsvinklen, der lægges på udfærdigelsen af listen. Vi

81 Politiets Efterretningstjeneste PET, 2008; *"Årsberetning 2006-2007"*.

håber derfor, at du også kan bruge vores lister som inspiration til at skabe mere sikre it-systemer.

6.1. Trends og tendenser i 2008

Der er i de foregående afsnit blevet beskrevet og identificeret flere tendenser, der i 2008 gjorde sig gældende for den it-kriminalitet, som vi kunne observere. Vi har nedenfor beskrevet de trends, som vi mener, var de væsentligste i 2008.

- En stadig større variation og opfindsomhed i typen af angreb.
- Botnet blev mere specialiserede og effektive i udførelsen af stadig mere målrettede angreb.
- *Malware* blev i 2008 blev spredt som resultat af botnet-aktivitet, primært via sårbare hjemmesider og spammails.
- Man forsøgte at ramme borgerne via sårbare tredjeparts webapplikationer, som brugerne ellers havde tillid til. *SQL injection*, *cross-site scripting* og andre sårbarheder i webapplikationer blev udnyttet som middel til dette.
- Mere avanceret og målrettet udnyttelse af ofte flere sårbare browserkomponenter som f.eks. Flash, PDF og QuickTime, der kan udnyttes på tværs af platforme.
- Orme og vira har haft mindre betydning for spredningen af *malware*.

I 2008 så flere nye angrebsmetoder dagens lys, og generelt har de organiserede it-kriminelle udvist en stadig større opfindsomhed.

Orme og vira har tidligere været den primære kilde til spredning af *malware*, og i flere tilfælde har selve spredningen været formålet. Dette har nu ændret sig markant. Som resultat af dette har vi konstateret et markant fald i antallet af portscanninger, der var den traditionelle internetorms primære spredningsmekaniske. I stedet foregik spredningen af *malware* via webapplikationer, der havde sårbarheder som følge af mangelfuld programmering. En primær kilde til inficering med *malware* og udbredelse af botnet-programmer var i 2008 udnyttelse af sårbarheder i browseren eller plugins til denne.

6.2. Fremtidige trends

I takt med at borgere og organisationer får flere og bedre muligheder for at beskytte sig, tror vi at kreativiteten tilsvarende vil stige hos dem, der forsøger at skabe sig adgang til vores computere og data.

Sociale netværkssider som f.eks. Facebook og Myspace oplevede i 2008 en kraftig vækst i antallet af brugere, som vi tror ikke vil aftage. Mængden af personlige oplysninger gjort tilgængelig af borgerne selv vil således stige. Disse tjenester vil derfor blive endnu mere attraktive for it-kriminelle. Som selvstændige applikationer på brugernes computere, har widgets og lignende teknologier ofte adgang til det underliggende operativsystem. Da sikkerheden ved brug af disse ofte er mangelfuld, udgør *widgets* samt applikationer der benyttes på f.eks. sociale net-

værkssider en trussel for inficering med *malware*.

Apple- og Linux-brugerne har gennem en årrække vænnet sig til, at det ikke var nødvendigt med beskyttelse mod *malware*. I takt med stigende udbredelse af Apples produkter bliver disse brugere et interessant marked for udbredelsen af *malware*.

Hvad vi fremover vil opleve er selvfølgelig vanskeligt at spå om. Nedenfor giver vi nogle bud på de overordnede tendenser, vi mener, bliver aktuelle i den kommende tid.

- Også de kommende år vil byde på en stigning i variationen af angrebsmetoder der benyttes.
- Botnet-aktiviteten vil stige.
- Fremtidige botnets vil være mere sofistikerede. Botnets bliver segmenteret i mindre enheder og bliver dermed mindre synlige, samt designet således, at de er mindre sårbare over for ISP'ernes interventioner.
- Antallet af identitetstyverier vil stige og blive mere målrettet det enkelte offer. Blandt midlerne til dette kan være avancerede botnet-programmer, som samler informationer fra brugerens maskine, sociale netværkssider med mere, der benyttes til målretning af angreb mod det enkelte offer.
- Mængden af automatiserede angreb mod webservere med brug af f.eks. *SQL injection* og *cross-site scripting* vil stige i tiden der kommer.
- En stigning i spredning af *malware* via *widgets*, dashboards, applikationer der benyttets på sociale netværkssider og lignende
- Sociale netværk bliver et effektivt middel til indsamling af informationer, der bruges ved målretning af spam og phishing.
- Mac- og Linux-brugerne vil i stigende grad være mål for fremtidens *malware*.
- Mængden af angreb udført af nuværende såvel som tidligere medarbejdere vil stige.
- Beskyttelse mod tab af data vil få stigende prioritet i de kommende år.

Den økonomiske krise vil medføre medarbejdere, der er usikre over deres jobsituation eller måske helt mister jobbet. Det vil skabe grobund for utilfredshed, som vi tror i enkelte tilfælde bliver rettet mod den organisation, hvor medarbejderen er eller var ansat.

Et stigende antal mobile databærende enheder og truslen om industrispionage vil skærpe fokus på de forretningsmæssige konsekvenser af datatab. Organisationer, der rammes på enten troværdigheden eller indtjeningen som følge af tab af fortrolige data, vil i økonomiske nedgangstider mærke dette ekstra hårdt.

7. Anbefalinger

Borgernes tryghed og sikkerhed hænger i dag uløseligt sammen med sikkerheden i organisationerne og øvrige dele af samfundet. Det er derfor væsentligt, at vi alle bidrager til at sikre vores digitale aktiver og husker på, at kæden ikke er stærkere end det svageste led.

Vi mener, at it-sikkerhed bør flyttes op i værdikæden som et element af en strategi for risikostyring. En rejse man i organisationerne er begyndt på, men som den enkelte borger og lovgivningen kun står på dørtrinet af.

I nærværende afsnit forsøger vi på baggrund af rapportens øvrige indhold at give nogle anbefalinger til henholdsvis den enkelte borger, organisationernes it-ansvarlige og relevante beslutningstagere. Det er vores håb, at disse anbefalinger vil blive diskuteret og taget til overvejelse, for kun gennem refleksion og åben diskussion kan vi i fællesskab finde en løsning på problemet internet-kriminalitet.

7.1. Anbefalinger til borgerne

En undersøgelse af australske computerbrugere[82] viste, at 11 procent aldrig opdaterede deres operativ system og 8 procent aldrig opdaterede deres antivirussoftware i hjemmet. Foruroligende tal, da netop disse faktorer udgør en væsentlig risiko for at computeren bliver kompromitteret. DK•CERTs anbefalinger er derfor:

1. Sørg for at holde dine systemer opdateret – brug de indbyggede opdateringsfunktioner.
2. Brug altid opdateret antivirus og personlig firewall.

Samme undersøgelse viste, at 30 procent af brugerne klikkede på links i spammails. I denne sammenhæng kan der gives nedenstående generelle anbefalinger:

3. Brug browserens indbyggede phishing-filter, antispywarefiltre med mere, og overvej om du vil tillade, at browseren skal afvikle scripts.
4. Vær opmærksom på om du vil forvente at modtage mails fra denne afsender eller med denne titel, inden du åbner selve mailen.
5. Check om URL-adressen på et link svarer til teksten på linket eller en anden URL du kunne forvente. Det gøres ved at holde musen over linket uden at klikke, og kigge på adressen nederst i browserens statuslinje. Er linktesten f.eks. http://www.minbank.dk/login.asp og den tilhørende URL peger på *http://www.skole123.dk/images/0012/minbank/login*, kan det tyde på at der er noget galt, da domænet *minbank.dk* ikke umiddelbart har nogen forbindelse til domænet *skole123.dk*. Meget lange URLer bør generelt give anledning til mistænksomhed.
6. Slet mailen uden at åbne vedhæftede filer eller klikke på links, hvis du er i tvivl.

82 AusCert, 2008; "*Home users computer security survey 2008*".

Selvom dine systemer er opdateret, og du opfører dig fornuftigt i forhold til mails og surfing på internettet, er der stadig mulighed for ubehagelige overraskelser. En væsentlig årsag til kompromitteringer er installationer med standard brugernavn og password, eller brugernavne og password, der er nemme at gætte. Du bør derfor:

7. Ikke benytte standard brugernavne og passwords i dine installationer og tjenester. Det gælder, hvad enten der er tale om dit trådløse access point, din adgang til webmail, sociale netværkssider eller lignende.
8. Brug stærke passwords, der er vanskelige at gætte. Et stærkt password er på minimum otte teng og indeholder både store og små bogstaver, tal og specialtegn.
9. Brug forskellige adgangskoder til forskellige tjenester. Du kan evt. benytte en elektronisk adgangskodehusker på computeren.

En undersøgelse foretaget i Storkøbenhavn af netværksproducenten D-link i januar 2008 viste, at 20 procent af de trådløse netværk var usikre[83]. Således har fremmede ikke blot mulighed for at misbruge forbindelsen, men også lettere adgang til computere og lignende, der befinder sig på det trådløse netværk. Du bør derfor sørge for at:

10. Bruge adgangskontrol og kryptering på dit trådløse netværk. Find yderligere hjælp i Forbrugerstyrelsens vejledning[84] eller hos producenten af dit trådløse udstyr.

I 2008 har der været stor fokus på brugen af sociale netværkstjenester, og hvordan brugere kan sikre sig imod misbrug af deres profiloplysninger[85]. De sociale netværkstjenester bliver i stigende grad udnyttet af it-kriminelle, der udnytter følsomme oplysninger og inficere brugernes computere. Du bør overveje følgende:

11. Kan den information, du har lagt ud på din profil misbruges af uvedkommende? Er det nødvendigt at din adresse, dit cpr-nummer, telefonnummer med videre er angivet?
12. Brug tredjeparts-applikationer med omtanke, de kan være ude efter at fiske dit brugernavn og adgangskode eller være inficeret med virus, orme eller installere en trojansk bagdør i dit system[86]. Vær opmærksom på, hvilke informationer fra din profil du giver applikationen adgang til.
13. Være opmærksom på, hvilke billeder du lægger ud på din profil. Både fordi du i flere sociale netværkstjenester afgiver rettighederne til tjenesten, som herefter må bruge billederne i andre sammenhænge. Endvidere fordi indholdet i billederne kan afsløre mere end du måske ønsker at vise: Billeder fra din stue med dit nye fladskærmsfjernsyn eller dyre malerier. Sådanne billeder er formodentlige attraktive for kriminelle.

83 D-link, 2008; "*20 procent af trådløse netværk er usikre*".
84 Forbrugerstyrelsen, 2007; "*Hvordan sikrer du dit trådløse netværk?*".
85 Datatilsynet, 2008; "*Anbefalinger til beskyttelse af privatlivets fred i sociale netværkstjenester*".
86 Computerworld.dk, 2009; "*Bør din virksomhed spærre for Facebook og Twitter*".

IT-borger skriver at: "*20 procent af alle arbejdsgivere søger informationer om potentielle medarbejdere på nettet, og hvem ønsker, at den fremtidige chef får adgang til billeder af dig fra en fest for ti år siden?*"[87]. Du bør derfor:

14. Overveje hvilke situationsbilleder og information du lægger ud på din profil. Er dette nogle billeder som du senere ønsker skal ses af din kommende arbejdsgiver eller din familie?
15. Være bevidst om, hvilke personfølsomme informationer, der gøres tilgængelige hvor og for hvem. Overvej om disse informationer eventuelt nu eller i fremtiden vil kunne misbruges.
16. Være opmærksom på rettigheder og ejerskab af ting du publicerer på nettet.

Generelt gælder, at man bør bruge sin sunde fornuft og tænke sig om, også med hensyn til brugen af it.

7.2. Anbefalinger til it-ansvarlige

Det er de it-ansvarliges pligt at sikre, at brugernes systemer er i en sådan forfatning, at de på bedst mulige vis er i stand til at varetage deres forretningsmæssige virke. Organisationens interne regler og procedurer, bør derfor understøtte, at brugernes computere holdes opdaterede og sikre. Vores anbefaling er derfor:

1. At det sikres, at brugerne benytter de indbyggede opdateringsmekanismer, browserfiltre med mere, samt at der benyttes et opdateret antivirus- og evt. antispyware produkt.
2. At brugerne kun gives mulighed for at definere stærke passwords.
3. At brugerne løbende holdes opdateret med it-sikkerhedsproblematikker, der er relevante for netop dem.

På samme vis som brugernes systemer bør holdes opdaterede og sikre, bør man selvfølgelig også sikre adgangen til organisationens forretningssystemer. Du bør derfor:

4. Sikre at organisationens forretningssystemer holdes opdateret. Abonner eksempelvis på en sårbarhedsvarslingtjeneste, og brug sårbarhedsscanninger som periodisk kontrol.
5. Overveje hvilke services, der er nødvendige på det enkelte system, og luk for dem, som ikke er nødvendige.
6. Minimere adgangen til det nødvendige ved at lukke adgangen for brugere og services der ikke skal være adgang til.

Troværdighed er for enhver organisation et væsentligt element af det at passe forretningen. Hvis ikke kunder, samarbejdspartnere eller andre har tillid til organisationen vil de om muligt vælge alternativer. Gennem de seneste år har en tendens været, at man forsøger at kompromitterer den enkelte borgers sikkerhed ved fra hjemmesider denne ellers har tillid til at inficerer deres computere med malware. En tendens der kun er muliggjort, fordi der ikke har været etableret tilstrækkelig inputvalidering på de kompromitterede hjemmesider. Vi anbefaler at:

87 It-borger.dk, 2007; "*Beskyttelse af dit privatliv*".

7. Der bør etableres en samlet platform for validering af brugersendte data på alle organisationens webapplikationer, inden disse eksekveres.
8. Der periodisk testes for mulig udnyttelse af *SQL injection*, *cross-site scripting* og lignende på organisationens webapplikationer.

På samme vis bør kunder og øvrige samarbejdspartnere kunne have tillid til, at fortrolige data vedrørende dem forbliver fortrolige. Vores anbefalinger er at:

9. Man i organisationerne overvejer, hvem der har adgang til hvilke data hvorfra og hvordan. Alt sammen en del af en fornuftig it-sikkerhedspolitik. Brug evt. DLP-systemer (*Data Leak Prevention*) for sikre, at regler og procedurer overholdes.
10. Man krypterer forretningskritiske data både på serveren, i transaktionen og ved anden transport på f.eks. bærbare computere og andre mobile enheder.

Dine leverandører udgør en væsentlig del af organisationens sikkerhed. Vi mener derfor at du skal stille krav til dine leverandører, hvad enten de er eksterne eller interne. Vi anbefaler at man:

11. Aktivt benytter organisationens risikovurderinger ved udfærdigelse af kravspecifikationer og lignende.
12. Spørger ind til, og gør sig bevidst om, hvilke ydelser der er inkluderet og hvilke som ikke er inkluderet. Er det f.eks. en selvfølge, at netudbyderen, hosting-organisationen eller lignende videresender abuse-forespørgsler, og med hvilken hastighed forventes dette foretaget? Er der inkluderet nogen form for overvågning i ydelsen og så videre?
13. Sørger for at få den nødvendige information og uddannelse.

7.3. Anbefalinger til beslutningstagere

Vi mener, at *god selskabsledelse* indbefatter at varetage sine kunders tarv. I dag er det desværre således, at en ISP, teleudbyder eller hosting-organisation intet økonomisk incitament har til at rådgive sine kunder om kompromittering af kundens it-sikkerhed. Tværtimod vil en sådan rådgivning ofte være forbundet med ekstra udgifter. Vi mener derfor at:

1. Der som i andre dele af det danske samfund bør tilbydes et incitament til, at disse organisationer yder den fornødne service, således at yderligere uhensigtsmæssig og/eller kriminel aktivitet fra kundens installationer kan undgås. Hvorvidt det skal være i form af smiley-ordninger, midlertidig domæne-suspension, strafferetslige sanktioner eller lignende, bør være et spørgsmål for de relevante beslutningstagere.

I forlængelse af ovenstående mener vi at:

2. Danske organisationer bør, ligesom i USA, have pligt til at informere deres kunder om art, omfang og konsekvens af en eventuel kompromittering af egne systemer, der vedrører kunden, eller data der vedrørende denne.

Undersøgelser har påvist, at formelle it-sikkerhedspolitikker skærper ledelsens fokus på it-sikkerhed og flytter fokus fra teknologi til *god selskabsledelse*. Vi mener, at en periodisk ekstern revision af organisationens it-sikkerhedspolitik ikke blot vil styrke politikkens indhold og gøre den lettere at implementere, men også vil sætte yderligere ledelsesfokus på it-sikkerhed. Vi anbefaler derfor at:

3. Der bør stilles krav om periodisk ekstern revision af it-sikkerhedspolitikken hos kunder og leverandører, med hvem organisationerne deler data.

Mens en række brancher herhjemme er reguleret af enten lovgivningen og/eller branchen selv, har det ligget i internettets natur, at det er ureguleret. Internettet som middel til udbredelse af informationssamfundet har præget debatten, hvor skeptikerne primært har haft fokus på beskyttelse af borgenes privatliv. I modsætning til f.eks. den finansielle sektor og telebranchen har ISP'erne ikke haft økonomiske incitamenter til at opdage og afværge misbrug og svindel, hvorfor internettet i dag udgør et middel til udbredelse af kriminel aktivitet, der kun vanskeligt lader sig opdage og begrænse. Således føres de fleste sager om økonomisk betinget kriminalitet på internettet til en dom på baggrund af opdagelse af finansielle transaktioner, snarere end opdagelse af forbrydelsen mens den stod på. Vi mener derfor at:

4. Der bør etableres en lovgivningsmæssig ramme, der forpligter ISP'erne til at samarbejde om detektering, varsling, afværgelse og rapportering af it-kriminalitet internt såvel som til myndighederne. Kun ved en fælles national indsat, har vi mulighed for at beskytte danske borgere og organisationer mod en stadig mere professionel, organiseret og international kriminalitetsform.

Ved at overlade it-sikkerheden til teknologien og "eksperterne" i it-afdelingen har man frataget brugerne deres ansvar. Gennem de seneste år har awareness-kampagner vundet indpas, også i danske organisationer. Vi mener, at hvis de skal have en egentlig effekt hos den enkelte bruger, bør der fokuseres på synliggørelse af it-sikkerhedens forretningsmæssige konsekvenser. En synlighed der også af den hollandske stats-CERT, betegnes som et nøglekoncept for varetagelsen af it-sikkerhed[88]. For at skærpe fokus på forretningen kan der i flere organisationer løbende følges med i organisationens forretningsmæssige og finansielle nøgletal på organisationens interne netværk. DK•CERTs anbefaling er at:

5. Der i organisationerne skabes en platform for synliggørelse af organisationernes risikostyrings- og it-sikkerhedsaktiviteter samt deres forretningsmæssige betydning. F.eks. i form af dashboards på organisationens intranet, hvor brugerne kan orientere sig om f.eks. antal og typer af sikkerhedshændelse, de løbende udgifter forbundet hermed, organisationens faste udgifter til it-sikkerhed osv..

Medarbejdere bruger i højere grad sociale netværkstjenester i arbejdstiden, hvilket medfører flere trusler mod organisationen[89]. DK•CERT anbefaler derfor at organisationen stiller sig selv følgende spørgsmål:

88 Govcert.nl, 2008; "*Trend report /2008. insight into cyber crime: Trends & figures*".
89 Computerworld.dk, 2009; "*Bør din virksomhed spærre for Facebook og Twitter*".

6. Organisationen bør gøre sig klart, hvilke it-sikkerhedstrusler brugen af sociale netværkstjenester kan medføre for organisationen. Er organisationen beskyttet imod den mulighed, der er for, at medarbejderens pc bliver inficeret med skadelig kode? Er medarbejdere gjort opmærksom på de trusler, brugen af sociale netværk kan medføre? Ved de f.eks., at mange tredjeparts-applikationer forsøger at lokke følsomme informationer ud af brugerne og inficerer deres computere skadelig kode?
7. Organisationen bør gøre sig klart, hvilke informationer den tillader medarbejderne at dele via sociale netværkstjenester. Er det for eksempel tilladt at kommunikere forretning via en medarbejders private profil?
8. Organisationen bør overveje, om det skal være tilladt at anvende sociale netværkstjenester i arbejdstiden, eller om der skal lukkes for tilgangen til tjenesterne, f.eks. ved oprettelse af adgangspolitikker eller via webfiltrering.

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 en bot og indgår i botnettet. Angriberen udnytter gerne sine robotter til udsendelse at foretage koordinerede *denial of service*-angreb eller udsende spam- og phishing-mails

Bullet-proof hosting: En service uden restriktioner på det som hostes. Udbydes af ISP'er og hostingvirksomheder, der lægger net og maskiner til alt fra børnepornografi, phishing-sider, botnetaktivitet og lignende. Organisationer, der tilbyder *bullet-prof hosting* samarbejder ikke med myndighederne og reagerer ikke på klager over det som hostes. De fleste organisationer, der tilbyder *bullet-prof hosting* er placeret i Rusland, Kina samt Syd- og Nord Amerika.

Cache poisoning: En metode til at lægge falske oplysninger i en DNS-servers cache. Dette sker ved udnyttelse af sikkerhedshuller i den pågældende DNS-server. Når brugere besøger en webside via en kompromitteret DNS-server, vil de få vist en forfalsket side i stedet for den rigtige.

Cross-site scripting: 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 f.eks. 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.

Denial of service: 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 ekstremt mange forespørgsler. Disse angreb udføres ofte fra flere computere samtidigt, og kaldes i de tilfælde for distributed *denial of service*.

DS 484: Dansk standard for it-sikkerhed.

Exploit: Et program eller kodestump, der udnytter en sårbarhed. Et *exploit* benyttes til at skaffe uautoriseret adgang til sårbare it-systemer. *Exploits* til kendte sårbarheder kan ofte findes på internettet.

Fast flux: *Fast flux* dækker over teknologi, der hurtigt og løbende skifter den netværks- eller IP-adresse, der er tilknyttet et givent domæne. Bruges f.eks. 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.

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

Muldyr: Person, der stiller sin bankkonto til rådighed for overførsel af penge. 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.

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.

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

Scareware: *Malware*, som udgiver sig for eksempelvis at være et antivirus-program. Programmet forsøger at franarre brugeren penge ved at påstå at have fundet en virus på brugerens computer. Den påståede virus kan ifølge programmet kun fjernes ved at betale for at "opgradere" til den fulde version af programmet.

Social Engineering: Manipulation, der har til formål at få folk til at bidrage med informationer eller at udfører handlinger, som f.eks. at klikke på links, svare på mails eller installere *malware*.

SOX, euroSOX: *Sarbanes-Oxley* Act of 2002, *SOX*, blev indført I USA 30. juli 2002, som resultatet af en række erhvervsskandaler. Loven skærpede kravene til processer vedrørende regnskabsføring, revision og risikostyring af børsnoterede virksomheder samt synliggørelsen af disse processer. Den europæiske pendant *euroSOX* blev, med en række tilføjelser til EU-parlamentets selskabsdirektiv, en realitet med virkning fra den 1. juni 2008. *EuroSOX* pålægger europæisk børsnoterede virksomheder, blandt andet at beskrive og offentliggøre kodeks for *god selskabsledelse*, elementer for risikostyring samt interne kontrolforanstaltninger.

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 f.eks. 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.

Widget: Et selvstændigt grænsefladeelement der tillader interaktion med brugeren. *Widgets* benyttes f.eks. til opbygning af webapplikationer, eller som desktop widgets i brugerens styresystem. *Desktop widgets* benyttes til præsentation af ofte brugte informationer som ur, kalender, lommeregner mm.

9. Figurer og tabeller

9.1. Figuroversigt

Figur 1. Sikkerhedshændelse anmeldt til DK•CERT i 2008 9
Figur 2. Offentliggjorte CVE-nummererede sårbarheder pr. år, DK•CERT 10
Figur 3. Risikovurdering af sårbarheder fundet ved sårbarhedscanning, DK•CERT 12
Figur 4. Spammails anmeldt til Spamcop pr. sekund i 2008 12
Figur 5. Antal afsendte mails per inficeret mail 12
Figur 6. Top 10 mail-baseret malware i 2008 13
Figur 7. Inficeringstyper af webhostet malware på danske sites i 2008 13
Figur 8: Websites med trojanere og phishing-sider anmeldt til DK•CERT 14
Figur 9. Portscanninger anmeldt til DK•CERT siden 2004 15
Figur 10. Månedlige portscanninger anmeldt til DK•CERT i 2008 15
Figur 11. Hyppigst scannede portnumre i 2008, DK•CERT 15
Figur 12: Daglig spammaængde afsendt fra Storm i 2008 18
Figur 13: Spam-mængder fra forskellige botnets i 2008 18

9.2. Tabeloversigt

Tabel 1. Hændelsestyper anmeldt til DK•CERT i 2008 9
Tabel 2. CVSS scores (0 – 10) for sårbarheder offentliggjort i 2008, DK•CERT 10
Tabel 3. Produkter med flest offentliggjorte sårbarheder i 2008, DK•CERT 11
Tabel 4. Fordeling af fundne sårbarheder på port og protokol, DK•CERT 11
Tabel 5. Anmeldte lande ved portscanning mod danske IP-adresser, DK•CERT 16

10. Referencer

AusCert, 2008; "*Home users computer security survey 2008*"; http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf

Arstechnica.com, 2008; "*Estonian ISP plays whack-a-botnet, has Srizbi on the run*"; http://arstechnica.com/news.ars/post/20081201-estonian-isp-plays-whack-a-botnet-has-srizbi-on-the-run.html

Business.dk, 2008; "*Reservedelsgigant anmelder konkurrent for it-indbrud*"; http://www.business.dk/article/20080109/industri/80109029/

Comon.dk, 2008; "*Fængslet for identitetstyveri via P2P*"; http://www.comon.dk/news/faengslet.for.identitetstyveri.via.p2p_35272.html

Computer Security Institute, 2008; "*2008 CSI computer crime & security survey*"; http://www.gocsi.com/forms/csi_survey.jhtml

Computerworld.com, 2008; "*Vulnerabilities play only a minor role in malware spread, says researcher*"; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122901

Computerworld.com, 2008; "*Windows users indifferent to Microsoft patch alarm, says researcher*"; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122599

Computerworld.dk, 2009; "*Bør din virksomhed spærre for Facebook og Twitter?*"; http://www.computerworld.dk/art/49586/boer-din-virksomhed-spaerre-for-facebook-og-twitter?page=1

Danmarks Statistik, 2008; "*Serviceerhverv 2008:17 statistiske efterretninger*"; http://www.dst.dk/upload/serv200817_19100.pdf

Dansk it's fagråd for it governance og management, 2006; "*IT Governance-anbefalinger*"; http://www.dansk-it.dk/upload/dansk_it_-_it_governance-anbefalinger.pdf

Darkreading.com, 2008; "*Bots use SQL injection tool in new web attack*"; http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=211201082

Darkreading.com, 2008; "*Storm may finally be over*"; http://www.darkreading.com/security/showArticle.jhtml?articleID=211201266

Datatilsynet, 2008; "*Anbefalinger til beskyttelse af privatlivets fred i sociale netværkstjenester*"; http://www.datatilsynet.dk/erhverv/internettet/anbefalinger-til-beskyttelse-af-privatlivets-fred-i-sociale-netvaerkstjenester/

Department of Justice, 2008; "*Retail hacking ring charged for stealing and distributing credit and debit card numbers from major U.S. retailers*"; http://www.usdoj.gov/opa/pr/2008/August/08-ag-689.html

DK•CERT, 2008; "*Målrettet phishing mod danske universiteter*"; https://www.cert.dk/nyheder/nyheder.shtml?08-10-02-11-50-00

D-link, 2008; "*20 procent af trådløse netværk er usikre*"; http://www.dlink.dk/?go=jN7uAYLx/oIJaWVSD7YZU93ygJVYLelXSNvhLPG3yV3oVY52g6ltbNlwaaRp7T0sHD2onGQTo48EBc7n2aLnJ0gSuenc

Ekstrabladet, 2008; "*Bjerrehuus: Falske profiler er helt lovlige!*"; http://ekstrabladet.dk/nationen/article1057528.ece

ENISA, 2006; "*A users' guide: How to raise information security awareness*"; http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf

ENISA, 2008; "*Obtaining support and funding from senior management*"; http://enisa.europa.eu/doc/pdf/deliverables/obtaining_support_and_funding_from_senior_management.pdf

Espn.com.com, 2008; "*Anatomy of a botnet*"; http://espn.com.com/defense-in-depth/?keyword=Joe+Stewart

Forbrug.dk; "*Klag over spam*"; http://www.forbrug.dk/forbrugerombudsmanden/hvadgaelder/mfl/godskik/saerlige-omraader/internet/net-tjek-dk/spam/

Forbrugerstyrelsen, 2007; "*Hvordan sikrer du dit trådløse netværk?*"; http://www.forbrug.dk/raad/rbdigitalt/internetforbindelser/internetforbindelse/netvaerk/sikring/

Foreningen af statsautoriserede revisorer, 2004; "*God selskabsledelse i mindre og mellemstore organisationer*"; http://www.fsr.dk/41256B0500435720/no/01001816/$File/God%20selskabsledelse.pdf

Forum of Incident Response and Security Teams, FIRST; "*Common Vulnerability Scoring System*"; http://www.first.org/cvss/

Govcert.nl, 2008; "*Trend report /2008. Insight into cyber crime: Trends & figures*"; http://www.govcert.nl/download.html?f=115

Ha.ckers.org, 2008; "*Clickjacking details*"; http://ha.ckers.org/blog/20081007/clickjacking-details/

Internet storm center, 2009; "*Submission summary for last 1,000 days*"; http://isc.sans.org/submissions_ascii.html

IT-borger.dk, 2007; "*Beskyttelse af dit privatliv*"; http://www.it-borger.dk/sikkerhed/netsikker-nu/beskytditprivatliv

It-borger.dk, 2008; "*Computer hack havde store konsekvenser*". http://www.it-borger.dk/sikkerhed/netsikker-nu/konkurrence/nyeste-konkurrencer/computer-hack-havde-store-konsekvenser.

Københavns fondsbørs' komité for god selskabsledelse, 2005; "*Rapport om god selskabsledelse i Danmark 2005*"; http://www.cbs.dk/content/download/42805/627905/file/N%C3%B8rby%20udvalgets%20rapport%20om%20god%20selskabsledelse%20i%20Danmark%202005.pdf

Marshal.com, 2008; "*Goodbye Storm?*"; http://www.marshal.com/trace/traceitem.asp?article=786

Marshal.com, 2008; "*Social networking malware*"; http://www.marshal.com/trace/traceitem.asp?article=839

Marshal.com, 2009 (08/01 2009); "*Spam statistics*"; http://www.marshal.com/TRACE/spam_statistics.asp

McAfee, 2008; "*McAffee virtual criminology report*"; http://www.mcafee.com/us/local_content/reports/mcafee_vcr_08.pdf

MessageLabs Intelligence, 2008; "*2008 annual security report*"; http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf

Netsikker Nu, 2008; "*Netsikker Nu magasinet*"; http://www.it-borger.dk/sikkerhed/netsikker-nu/kampagneproduktioner/kampagneproduktioner/resolveuid/2eb51e4539247ba6d1245a07bb60dc8d

News.dk, 2008; "*Spam-botnet vækket til live igen*"; http://newz.dk/spam-botnet-vaekket-til-live-igen

Politiets Efterretningstjeneste PET, 2008; "*Årsberetning 2006-2007*"; http://www.pet.dk/upload/pet_%C3%A5rsberetning_2006_2007.pdf

PricewaterhouseCoopers, 2008; "*The 5th annual global state of information security, the end of innocence*"; http://www.pwc.com/extweb/pwcpublications.nsf/docid/F7D6BB0908EB5BE180257395002FE254/$file/pwc_stateofInfSecurity07.pdf

Schneier.com, 2008; "*Schneier on security*"; http://www.schneier.com/blog/archives/2008/10/clickjacking.html

Sectheory.com, 2008; "*Clickjacking*"; http://www.sectheory.com/clickjacking.htm

Securosis.com; "*Understanding and Selecting a Data Loss Prevention Solution*"; http://securosis.com/publications/DLP-Whitepaper.pdf

Secureworks.com, 2008; "*Danmec/Asprox SQL injection attack tool analysis*"; http://www.secureworks.com/research/threats/danmecasprox/

Shadowserver.org, 2009 (12/01 2009); "*Bot count yearly*"; http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCountYearly

Shadowserver.org, 2009 (12/01 2009); "*Botnet charts*"; http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetCharts

Shadowserver.org, 2009 (12/01 2009); "*Botnet maps*"; http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotnetMaps

Shadowserver.org, 2009 (12/01 2009); "*Drone maps*"; http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.DroneMaps

Shadowserver.org, 2009 (12/01 2009); "*Scan charts*"; http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.ScanCharts

Sophos, 2008; "*Security threat report: 2009*"; http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

Spamcop.net, 2009 (14/01 2009); "*Total spam report volume, one year*"; http://www.spamcop.net/spamgraph.shtml?spamyear

Statsadvokaten for særlig økonomisk kriminalitet. Hvidvasksekretariatet, 2008; "*Årsberetning 2007*"; http://www.rigsadvokaten.dk/media/dokumenter/Arsberetning_2007_SOK.pdf

Sudosecure.net, 2008; "*Storm worm - go away, we're not home*"; http://www.sudosecure.net/archives/264

Theregister.co.uk, 2008; "*Storm botnet blows itself out*"; http://www.theregister.co.uk/2008/10/14/storm_worm_botnet_rip/

Slashdot.org, 2008; "*McColo briefly returns, hands off botnet control*"; http://it.slashdot.org/article.pl?sid=08/11/18/219204&from=rss

Symantec, 2008; "*Symantec report on the underground economy July 07–June 08*"; http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

Version2, 2008; "*Cyberangreb optrapper bitter valgkamp*"; http://www.version2.dk/artikel/8920

Version2, 2008; "*Dansk it-industrispionage tager til*"; http://www.version2.dk/artikel/7037-dansk-itindustrispionage-tager-til

Version2, 2008; "*Danske jobsites spredte virus efter kinesisk hackerangreb*"; http://www.version2.dk/artikel/9165-danske-jobsites-spredte-virus-efter-kinesisk-hackerangreb

Version2, 2008; "*Hackere invaderer georgiske websteder*"; http://www.version2.dk/artikel/8116-hackere-invaderer-georgiske-websteder

Version2, 2008; "*Krisen får flere til at bide på jobannoncer for it-stråmænd*"; http://www.version2.dk/artikel/9336-krisen-faar-flere-til-at-bide-paa-jobannoncer-for-it-straamaend

Video.google.com, 2008; "*New zero-day browser exploits – clickJacking*"; http://video.google.com/videoplay?docid=-5747622209791380934&hl=en

Washingtonpost.com, 2008; "*Major source of online scams and spams knocked offline*"; http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

Wikipedia.org; "*Data loss prevention products*"; http://en.wikipedia.org/wiki/Data_Loss_Prevention

Wikipedia,org; "*Russian Busines Network*"; http://en.wikipedia.org/wiki/Russian_Business_Network

Kontakt:

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

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