DK•CERT

Trendrapport 2009

It-kriminalitet og sikkerhed i året der gik

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

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

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

DK•CERT

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

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

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

DK•CERT, det danske Computer Emergency Response Team, blev oprettet i 1991 som en afdeling af UNI•C, Danmarks it-center for uddannelse og forskning, der er en styrelse under Undervisningsministeriet.

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

Forord

Velkommen til DK•CERTs Trendrapport 2009. Formålet med rapporten er at give et dækkende billede af it-sikkerheden i Danmark, som den så ud i 2009. Ligesom i tidligere års rapporter handler en del af rapporten om it-kriminalitet, men vi kommer også ind på andre elementer af betydning for sikkerheden. Det er jo sådan at vi skal kende truslen, før vi kan beskytte os.

It-kriminalitet er under konstant udvikling. Ingen, hverken borgere eller organisationer, kan se sig ude af skudlinjen, da de, der forsøger at misbruge vores systemer og data, ikke diskriminerer. Således kræver opretholdelse af it-sikkerhed en fælles indsats, der hovedsageligt handler om viden og ansvar, mere end om isolerede tekniske løsninger. Som på mange andre områder i samfundet kan en vaklende brik i it-sikkerhedens univers tage flere brikker med sig i faldet.

Trendrapport 2009 bygger på data, som primært dækker de netværk, DK•CERT overvåger. Derudover trækker vi på offentligt tilgængelige data fra andre danske og internationale kilder. Endelig har nogle af vores samarbejdspartnere som noget nyt bidraget med afsnit om deres særlige ekspertiseområder.

Efter en gennemgang af it-sikkerheden anno 2009 giver vi vores bud på, hvad fremtiden vil bringe. Det vil sige et kvalificeret bud på de trusler, vi i fremtiden kommer til at stå overfor samt de udfordringer det vil bringe i forhold til varetagelse af sikkerheden. Endelig giver vi nogle forslag til, hvad henholdsvis borgerne, de it-ansvarlige og beslutningstagerne bør gøre for at øge it-sikkerheden i Danmark.

I forbindelse med rapportens tilblivelse vil vi gerne takke de parter, der har bidraget med inspiration, tekst og data. Særligt ønsker vi at takke Peter Kruse fra CSIS Security Group A/S, Thomas Kristensen fra Secunia, Lars Neupart fra Neupart A/S og Anette Høyrup fra Forbrugerrådet for deres bidrag til rapporten. Sidst men ikke mindst vil jeg gerne takke Jens Borup Pedersen (DK•CERT) for det store stykke arbejde han har ydet for rapportens tilblivelse.

Vi ønsker dig fortsat god fornøjelse med læsningen.

Med venlig hilsen

Shehzad Ahmad, DK•CERT

Indholdsfortegnelse

1. Resume

Starten af 2009 var præget af *Conficker*-ormens hærgen og et målrettet angreb på de danske netbanker. Således åbnede året med to tendenser, der peger henholdsvis tilbage og fremad i tiden. Hvor de større globale pandemier hører fortiden til, vil vi i fremtiden se langt mere avanceret og målrettet *malware*, og også tidligere "sikre" eller oversete platforme vil være i skudlinjen.

DK•CERT har i 2009 behandlet 37.535 anmeldelser om it-sikkerhedshændelser, hvilket er et forventet fald i forhold til året før. Hvor antallet af anmeldelser om scanninger efter åbne eller usikre systemer er faldet, er antallet af hændelser, hvor DK•CERT har bidraget med analyse, efterforskning og rådgivning steget. Således oplevede vi en vækst i sager om fx hacking og websider inficeret med *trojanske heste* og *phishing*-sider.

Hvor vi i 2009 oplevede et fald i antallet af *phishing*–mails, var *trojanske heste*, der ikke selv har evnen til at sprede sig, det fortrukne middel til at skaffe sig adgang til brugernes personlige oplysninger. Der var en eksplosiv vækst i ny målrettet og specialiseret *malware*, som overgik mængden af legitim software. Det mærkede vi indirekte følgerne af som et af de lande i verden, der modtog mest *spam*, udsendt gennem store, verdensomspændende *botnet*.

Sårbare legale webapplikationer var i 2009 den væsentligste kilde til spredning af *malware*, hvad enten der var tale om *botnet*-programmer eller målrettede *trojanske heste* som dem, der blev brugt i angrebet på de danske netbanker. En væsentlig årsag er, at sårbare systemer og applikationer ikke i tilstrækkelig grad sikres og opdateres, hverken hos borgerne, i organisationerne, eller de virksomheder der hoster deres applikationer.

Blandt de øvrige emner der i år har fået fokus, er sociale netværkstjenester og mobile platforme. 2009 bragte dog også andre emner i vores bevidsthed. Således har problematikker vedrørende samarbejds- og leverandørrelationer fået fokus i rapporten, særligt i forbindelse med emner som *cloud computing*, risikostyring og *compliance*. Det afspejler sig i de anbefalinger, der sidst i rapporten gives til henholdsvis borgeren, organisationernes it-ansvarlige og beslutningstagerne.

Vi har i rapporten identificeret nogle tendenser for 2009 og fremtiden. Den generelle tendens har været, at de organiserede it-kriminelle grupperinger specialiserer og målretter deres aktiviteter, så at ingen længere kan sige sig uden for farezonen. Således bliver sammenfatningen af vores anbefalinger da også, at man skal sørge for at holde sine systemer opdaterede og sikre, og bevæge sig med omtanke på nettet. Derudover opfordrer DK•CERT til samarbejde og kommunikation om blandt andet detektering, varsling og afværgelse af *malware*-relateret aktivitet. Det skal dog ske under hensyntagen til privatlivets fred og være underbygget af lovgivningen.

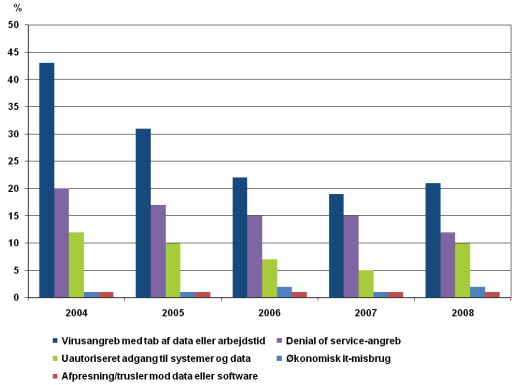
2. Indledning

It-sikkerhed handler grundlæggende om at implementere de nødvendige tekniske og organisatoriske løsninger i forhold til den aktuelle konfiguration af data, teknologi, processer og mennesker. Mens det fra et forretningsperspektiv er en overskuelig opgave at beskrive, hvad der skal beskyttes, er det straks vanskeligere at definere spørgsmålene om, hvad der skal beskyttes imod og hvordan. It-sikkerhed er nemlig ikke et spørgsmål om teknologi alene, men i lige så høj grad et menneskeligt eller kulturelt anliggende, der bør gennemsyre alle individer i organisationen og samfundet. Vi vil her forsøge at åbne læserens perspektiv på, hvilke trusler vi nu og i fremtiden bør være opmærksomme på og hvorfor, og overlade spørgsmålene om hvordan til litteraturen og den øvrige it-sikkerhedsbranche.

Vi er i dag afhængige af digitale strukturer og tjenester. Selvom den økonomiske krise i 2009 har stillet investeringer i bero, er der i dag bundet anseelige beløb til udvikling, drift, vedligeholdelse og sikring af de danske organisationers it-aktiver. Forventningen hos cirka halvdelen af de offentlige myndigheder var i 2008, at udgifterne til it i 2009 ville stige[1]. Når halvdelen af dem tilsvarende havde en forventning om stigende udgifter til it-sikkerhed i 2009, tager vi det som udtryk for, at værdien af de it-aktiver vi prøver at beskytte, er stigende, ligesom både mængden og følsomheden af de data, som transmitteres, lagres og behandles. En international undersøgelse blandt teknologi-, medie- og telekommunikationsvirksomheder foretaget af Deloitte viste dog, at 32% i de foregående 12 måneder under den finansielle krise havde reduceret budgettet til it-sikkerhed. Således allokerede 55 % af de responderende organisationer mindre end 6% af deres it-budget til sikkerhed[2].

At den økonomisk betingede it-kriminalitet er et stigende problem, har både vi og andre gennem de seneste år proklameret gentagne gange. Således er værktøjer til aktivitetsovervågning og –analyse af Gartner blevet identificeret som den syvende væsentligste strategiske it-teknologi i 2010[4]. It-sikkerhed er, fra en plads i mørket, kommet i det fine selskab med teknologier som *cloud computing* og *business intelligence*. Placeringen er dog også et udtryk for et flerfacetteret trusselsbillede, hvor det ikke længere er nok kun at beskytte perimeteren og den enkelte it-ressource. Mens der i perioden 2004-2008 har været et konstant eller faldende antal registrerede sikkerhedshændelser hos de danske myndigheder (Figur 1), er fx mængden og troværdigheden af *phishing*-mails rettet mod danskerne i 2009 steget.

It-kriminaliteten bliver stadig mere professionel og kompleks. Sammenhængen mellem årsag og virkning bliver derved vanskeligere at gennemskue. Således opdages og registreres it-kriminalitet begået mod borgeren kun sjældent som it-kriminalitet. I offentligheden er det ofte virkningen snarere end årsagen der mentalt kategoriseres. For eksempel betragtes et uautoriseret træk på netbankkontoen som økonomisk kriminalitet, selv om årsagen er et digitalt indbrud i en netbutik,



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

1 Danmarks Statistik, 2009; "*Den offentlige sektors brug af it 2008 – Årspublikation*".

2 Deloitte, 2009; "*2009 TMT global security survey*".

3 Danmarks Statistik, 2009; "*Den offentlige sektors brug af it 2008 – Årspublikation*".

4 Gartner, 2009; "*Gartner identifies the top 10 strategic technologies for 2010*".

inficering med et *botnet*-program eller besvarelse af en *phishing*-mail.

Det er denne rapports formål at sætte spot på nogle af de trusler, vi som borgere, organisationer og samfund står overfor. Kun med viden og kommunikation kan vi implementere de rigtige løsninger og modgå truslen om misbrug af vores digitale aktiver. Det er derfor vores håb, at du som læser vil bruge de perspektiver, du præsenteres for, til at reflektere over hvilke tekniske og organisatoriske løsninger der hos dig er nødvendige og rigtige nu og i fremtiden. Problemets omfang taget i betragtning mener vi nemlig ikke, at der er tilstrækkelig fokus på, hvordan vi kan beskytte danske borgere og organisationer mod it-kriminalitet. Regeringsbeslutningen fra maj 2009 om oprettelse af en national GovCERT er et skridt i den rigtige retning. Hvorvidt dens ressourcer, kompetencer og beføjelser er tilstrækkelige, må tiden dog vise.

Rapportens konklusioner er primært opstået på baggrund af data udtrukket fra DK•CERTs egne systemer, der dækker hændelser på de netværk, som DK•CERT overvåger. Hvor de skullet suppleres, har tredjepart aktivt bidraget med relevante data vedrørende den danske del af internettet. Derudover er data fra internettets åbne kilder benyttet til at perspektiverer de belyste problemstillinger samt at skitsere problemstillingens internationale karakter.

Rapportens første del beskriver med tal 2009 på den danske del af internettet, som vi oplevede det i DK•CERT. I rapportens andet afsnit samler vi op på nogle af de tendenser inden for it-kriminalitet og -sikkerhed, som har præget året der gik. Herefter lader vi tendenserne pege fremad, og forsøger at beskrive de udfordringer, vi som borgere, organisationer og samfund i de kommende år kan stå overfor. Til slut samler vi op på rapportens konklusioner og giver nogle brugbare anbefalinger til henholdsvis borgeren, organisationernes it-ansvarlige og beslutningstagerne.

God læselyst.

Om GovCERT

"GovCERT er en forkortelse for 'Government Computer Emergency Response Team'. GovCERT'en vil dække hele staten, men ikke internetbaserede hændelser generelt i samfundet, som eksempelvis nedbrud i netbanker mv.

En GovCERT skal sikre, at der i staten er overblik over trusler og sårbarheder i produkter, tjenester, net og systemer. På den baggrund skal tjenesten foretage en løbende vurdering af it-sikkerheden samt varsle myndigheder om it-sikkerhedsmæssige hændelser og trusler."

Ministeriet for videnskab teknologi og udvikling[5]

5 Ministeriet for videnskab teknologi og udvikling, 2009; "*Sander: Styrket dansk bekæmpelse af internettrusler*".

3. 2009 - året i tal

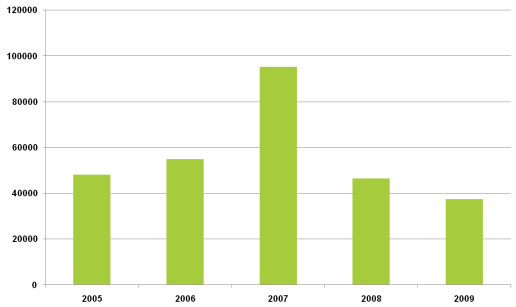
Du vil i dette afsnit blive præsenteret for data der beskriver året 2009 fra vores perspektiv i DK•CERT. Det vil sige data, der primært fortæller en historie om it-sikkerheden på de netværk, som vi overvåger. Til supplering, generalisering og perspektivering er der benyttet data leveret af tredjepart samt internettets åbne kilder. Vi mener derfor, at afsnittet giver en generel it-sikkerhedsstatus for hele den danske del af internettet.

Som forventet oplevede vi i 2009 et fald i antallet af sikkerhedshændelser anmeldt til DK•CERT. Således endte året med i alt 37.535 anmeldelser, hvilket er et fald på 19% i forhold til 46.481 anmeldelser i 2008 (Figur 2). Over året har antallet af anmeldelser været næsten konstant, svingende mellem 2.900 i maj og 3.400 i oktober. Denne udvikling, der hovedsageligt skyldes mere målrettede angreb, forudsagde vi sidste år. Den største årsag er et fald i anmeldelser af scanninger, som er faldet til 33.761 eller 24% i forhold til 2008. Derimod er mængden af sager vedrørende piratkopiering, hacking og *phishing*- og *trojaner*-inficerede websites steget markant (Figur 3). Det er derfor vores vurdering, at der ikke er blevet mindre it-kriminalitet, blot er den blevet mere målrettet og kompleks.

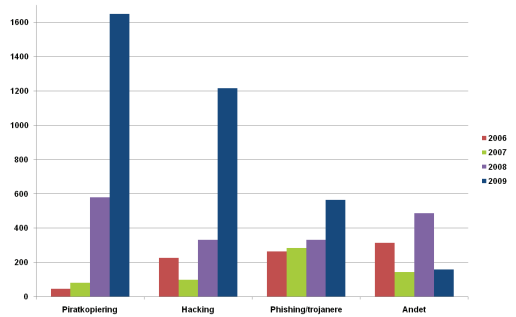
I 2009 var antallet af offentliggjorte nye *CVE-nummererede sårbarheder* 5.734. Mere interessant er det, at mere end 50% af dem vedrørte webapplikationer, da netop disse i stor udstrækning udnyttes af it-kriminelle. I 2009 var sårbare legale webapplikationer således den væsentligste kilde til spredning af *malware* i form af fx *botnet*-programmer og *trojanske heste*. Håndteringen af dette er et stigende problem for både organisationernes og borgernes sikkerhed.

Både de mailbaserede og netværksbaserede orme og vira er på retur. *Conficker*, der i starten af året spredte sig med stor hast, er dog undtagelsen, der bekræfter reglen. Tilsvarende er antallet af *phishing*-mails globalt set faldet i forhold til 2008, mens den samlede mængde *spam* igen er på niveau med tiden inden lukningen af den tvivlsomme hostingvirksomhed McColo i november 2008.

Vi har i dette afsnit lagt fokus på tre emner, der i et sikkerhedsperspektiv peger henholdsvis tilbage og fremad. Der indledes med data vedrørende årets offentliggjorte *sårbarheder*, som vi nu og i fremtiden vil se udnyttet. Vi har i år også fokuseret på *sårbarheder* i webapplikationer, som der opdages flere af, og som i stigende grad misbruges. Afsnittet aktualiseres med statistik over de *sårbarheder*, som vi via *sårbarhedsscanninger* har konstateret på den danske del af internettet. Herefter beskrives data, der vedrører de scanninger, der i årets løb er blevet anmeldt til DK•CERT. Tallene sammenlignes med tidligere år, og vi forsøger at give en forklaring på udviklingen. Afsnittet afrundes med data vedrørende det *malware*, som i årets løb har floreret på internettet.



Figur 2. Sikkerhedshændelser anmeldt til DK•CERT.



Figur 3. Væsentligste hændelsestyper anmeldt til DK•CERT.

Malware

"Malware er en sammentrækning af de engelske ord malicious software (på dansk: 'ondsindet programkode'). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på[6]."

Malware kan opdeles i en række kategorier, som fx vira, orme, trojanske heste, keyloggere, spyware, adware,scareware, botnet-programmer og lignende.

6 Wikipedia.org, 2009; "*Malware*".

3.1 Sårbarheder, ikke kun på nettet

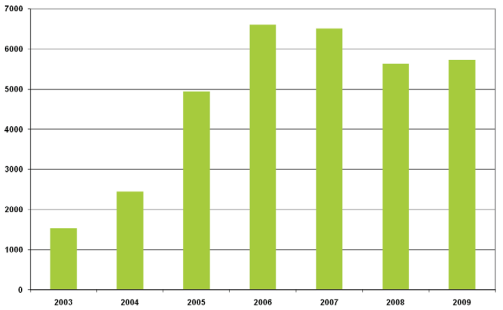
DK•CERT benytter bl.a. den amerikanske tjeneste NVD[7] (*National Vulnerability Database*), der samler og katalogiserer *CVE-nummererede sårbarheder* (*Common Vulnerability and Exposures*) i standard it-systemer. NVD offentliggjorde i 2009 i alt 5.734 nye *CVE-nummererede sårbarheder*.

Således var antallet af offentliggjorte *CVE-nummererede sårbarheder* i standard-programmer i 2009 på samme niveau som året før (Figur 4). Dette på trods af, at der til stadighed er et stigende antal programmer i et stigende antal forskellige versioner på markedet. En årsag kan være, at de der finder *sårbarheder* med udnyttelse for øje, har koncentreret indsatsen på områder, hvor *sårbarhederne* ofte ikke opdateres og/eller er vanskelige at rette. Mens operativsystemer og applikationer, der knytter sig direkte til disse, i dag ofte opdateres automatisk, skal brugeren som regel selv opdatere plugins i browseren, tredjepartsprogrammer mm. Tilsvarende kan det være vanskeligt selv at rette fejl i websider, der er oprettet i et CMS, da der typisk vil være mange steder, fejlen skal rettes.

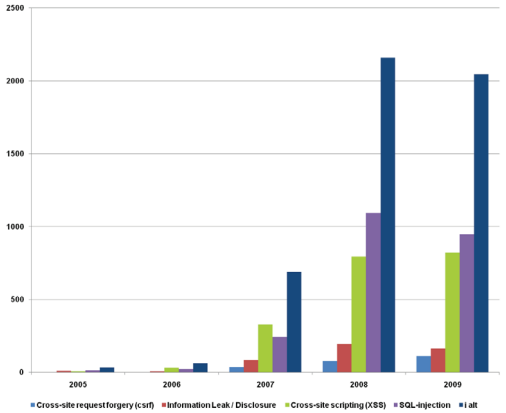
Den generelle tendens har gennem de seneste år været, at der findes stadig flere sårbarheder i applikationer, der kører oven på operativsystemet . Hvor det tidligere var sårbarheder i operativsystemet, der var i overtal, findes der nu flest applikationssårbarheder[9]. Mens antallet af offentliggjorte *CVE-nummererede* sårbarheder gennem de seneste år er faldet, er der således blevet offentliggjort flere *CVE-nummererede sårbarheder*, der knytter sig specifikt til webapplikationer. Mængden af sårbarheder af typerne *SQL injection*, *cross-site scripting*, *cross-site request forgery* og *information leak*, der hovedsageligt relaterer sig til webapplikationer, er steget markant i løbet af de seneste år (Figur 5), og udgør nu godt halvdelen af alle offentliggjorte *CVE-nummererede sårbarheder*. I tillæg hertil kommer *sårbarheder* i den specifikke webapplikation, der ikke offentliggøres med et *CVE-nummer*.

Listen over de programmer hvortil der blev offentliggjort flest *CVE-nummererede sårbarheder* domineres af operativsystemer fra de fleste større leverandører (Figur 6). Derudover er internetbrowsere fra både Microsoft, Apple og Mozilla repræsenteret, mens Mozilla Seamonkey og Adobe Acrobat er at finde på en hhv. 14. og 15. plads. Mozilla-browseren Firefox var det enkelt system, hvori der blev konstateret flest nye *sårbarheder* efterfulgt af Microsofts Windows Server 2003. Hvorvidt disse produkter således er mere usikre at benytte end deres alternativer, kan dog ikke udledes, da dette afhænger af faktorer som fx:

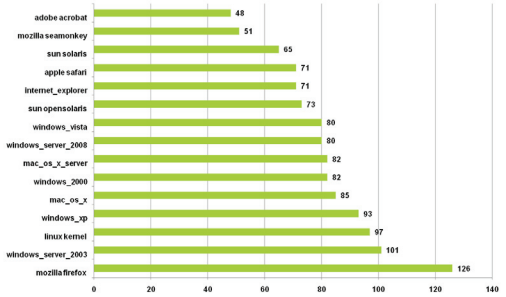
- Alvorligheden af de fundne *sårbarheder*.
- Tilgængeligheden af *exploits*.
- De sårbare systemers udbredelse.



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



Figur 5. Offentliggjorte CVE-nummerede websårbarheder pr. år.



Figur 6. CVE-nummererede sårbarheder offentliggjort i 2009 fordelt på produkter.

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

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

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

En årsag til de mange *sårbarheder* i Mac OS X er blandt andet måden, hvorpå disse registreres. Flere *sårbarheder* i applikationer, der knytter sig til Mac OS X, registreres som sårbarheder i Mac OS X, og ikke som sårbarheder i f.eks. Quicktime. Tilsvarende kan gøre sig gældende med andre systemer. Også placeringen af Linux-kernen på en tredjeplads kan diskuteres. Samme sårbarhed kan reelt godt optræde i flere versioner af Linux-kernen, der findes i flere versioner end fx Windows XP.

DK•CERT foretog i 2009 sårbarhedsscanning på mere end 50.000 forskellige IP-adresser på den danske del af internettet. Heraf svarede 1.719 eller cirka 3,4%. De øvrige IP-adresser må formodes ikke at være i brug eller være beskyttet bag en firewall. Af de svarende systemer havde 67% i gennemsnit 4 *CVE-nummererede sårbarheder*. På scanningstidspunktet var flere end 50% af de konstaterede *sårbarheder* blevet offentliggjort mere end et år tidligere.

Ved efterfølgende scanning af de sårbare systemer var cirka en tredjedel af de sårbare systemer stadig sårbare, og en tredjedel af *sårbarhederne* ikke rettet. Når *sårbarheder* således først rettes relativt sent, hvis de rettes, tyder det på, at mange organisationer ikke har en egentlig procedure for patch-management. Flere organisationer kan således have problemer med at overholde egen it-sikkerhedspolitik samt gældende standarder som fx *DS 484* og lignende.

Der blev ved scanningerne konstateret *sårbarheder* på 66 forskellige porte og/eller protokoller. Flest *sårbarheder* blev der konstateret på TCP port 80 og 443, der benyttes af webapplikationer (Figur 7). Applikationsspecifikke *sårbarheder* forårsaget af fx mangelfuld inputvalidering på webapplikationer fremgår ikke af statistikken, da de kun sjældent offentliggøres med et *CVE-nummer*. Netop disse *sårbarheder*, der fx muliggør *SQL injection* og *cross-site scripting*, var blandt de mest udnyttede i 2009.

Den væsentligste tendens med hensyn til programsårbarheder var i 2009, at de blev udnyttet hurtigere. Ofte også før de blev offentliggjort, eller der blev udgivet en rettelse til dem. Fx blev *sårbarheder* i Adobe Acrobat og Adobe Reader flere gange i løbet af året set udnyttet, inden der blev offentliggjort information om de udnyttede *sårbarheder*. Senest i december blev der fundet *exploits*, der udnyttede en ikke tidligere offentliggjort *sårbarhed* (CVE-2009-4324). *Sårbarheden* muliggjorde ved hjælp JavaScript i PDF-dokumenter, at en angriber potentielt kunne tage kontrol over det ramte system, der både kunne være Windows, Mac og UNIX[10].

At det var i forbrugerprogrammer, der i 2009 blev fundet *sårbarheder* i, er en anden af årets tendenser. Således blev der også konstateret kritiske *sårbarheder* i andre af Adobes programmer, som fx Flash Player og Shockwave, der ofte fungerer som plugin i browseren. Adobes programmer toppede i 2009 listen over de mest sårbare forbrugerprogrammer, men også andre software producenter måtte udgive rettelser til deres produkter[11]. Fx måtte Apple i 2009 udgive rettelser til kritiske *sårbarheder* i QuickTime (CVE-2009-0007, CVE-2009-0003 og CVE-2009-0957), der tilsvarende fungerer på flere platforme, og ofte også som plugin i

10 Adobe.com, 2009; "*Security advisory for Adobe Reader and Acrobat*".

11 Net-security.org, 2009; "*Top vulnerable applications in 2009*".

Sårbarheder - skal du bekymre dig om det?

Den typiske pc bruger 50-80 forskellige programmer fra mere end 20 forskellige producenter. 30-50 af de programmer der er installeret på pc'en, er ikke produceret af Microsoft, som derfor ikke laver automatiske opdateringer til dem. Således har ca. 70% af brugerne mere end 5 usikre programmer på deres pc. Selvom man ikke bruger et program, kan en sårbarhed i det ofte udnyttes igennem browseren eller ved, at der åbnes en uskyldigt udseende vedhæftet fil. Det er her, det helt store problem ligger.

Det er ikke underligt at de færreste bruger tid på at besøge producenternes hjemmesider for at kontrollere, om de har udgivet opdateringer. Dels ved mange ikke, hvor vigtigt det er, og dels er det tidskrævende manuelt at holde øje med så mange program- og producentsider. Det har de kriminelle desværre regnet ud. Derfor har de fokuseret på at udnytte sårbarheder i programmer, der ikke kommer fra Microsoft. Man kan derfor ikke nøjes med at bruge de automatiske opdateringer fra Microsoft. Antivirusprogrammet er desværre heller ikke til meget nytte. Det er nemlig de færreste antivirusprogrammer, der fanger udnyttelsen af sårbarheder. Faktisk er der ikke nogen anti-virus programmer, der fanger mere end 33%.

Der er dog ikke nogen grund til at bekymre sig alt for meget over, da disse opdateringer er gratis. Der findes også et værktøj, som automatisk kan scanne pc'en og give direkte adgang til at hente opdateringer fra producenterne - dette værktøj er også gratis og hedder Secunia Personal Software Inspector: secunia.com/vulnerability_scanning/personal

Thomas Kristensen, Secunia

browseren[12].

Mens fokus i dette afsnit har været på programsårbarheder, repræsenterer softwarefejl kun en ud af tre måder, sikkerhedshuller opstår på. De øvrige muligheder, som ofte overses, er svage konfigurationer og mennesker, der ifølge Joshua Corman fra IBM er langt mere farlige end softwarefejl[13]. Således spiller faktorer som naivitet, uvidenhed, grådighed og glemsomhed en afgørende rolle ved flere af de kriminalitetsformer, der i 2009 gav anledning til tab hos borgerne og organisationerne. Fx følte kun 28% af respondenterne i en international undersøgelse af Deloitte sig sikre i forhold til interne trusler, mod 51% i 2008[14].

Sårbarhederne er blevet flere og vanskeligere at finde og vurdere, da de består af flere interagerende både tekniske og menneskelige lag. Samtidig bliver det vanskeligere at forudse sandsynligheden for, at en *sårbarhed* udnyttes. Hvordan kan vi fx vurdere sandsynligheden for, at der skabes uautoriseret adgang til et it-system, ved at en bruger besvarer en *phishing*-mail, der skaber adgang til brugerens mailkonto, og derigennem skaffer adgang til et andet system, hvortil brugeren har fået tilsendt kontooplysninger pr. mail? Med stigende forventning om at den ansatte altid er forbundet til arbejdet via hjemmearbejdspladser og et stigende antal netopkoblede mobile enheder, stiger antallet af *sårbarheder* i et samlet system, hvis grænser bliver stadig mere flydende.

3.2. Scanninger

Der er ikke overraskende sket et fald i anmeldelser om systemscanninger til DK•CERT i 2009 (Figur 8). Antallet har henover året været stort set konstant og var på næsten samme niveau som de sidste måneder af 2008 (Figur 9). Den væsentligste årsag er, at it-kriminaliteten har flyttet sig til områder, hvor succesraten er større, og at 2009, bortset fra *Conficker*, har været fri for større udbrud af netbaserede orme, der tidligere har forsaget mange anmeldelser. Samme tendens med konstant eller svagt faldende mængde anmeldte scanninger gør sig også gældende internationalt. Også antallet af scanninger registreret af Shadowserver.org har været konstant eller svagt faldende gennem de sidste to år[15] med større og mindre udsving hen over perioden.

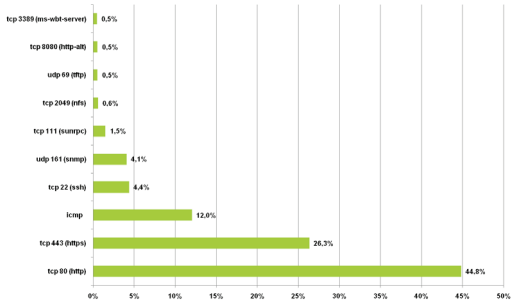
Der blev i 2009 til DK•CERT anmeldt scanninger mod i alt 152 forskellige porte og protokoller fra i alt 19.364 forskellige IP-adresser. I næsten en tredjedel af anmeldelserne indgik ICMP ping af store netsegmenter enten alene eller i kombination med andre porte (Figur 10). Ping er som sådan legal trafik og bør isoleret set ikke give anledning til større postyr. Når det i disse tilfælde alligevel har givet anledning til, at det blev anmeldt til DK•CERT, skyldes det mængden af trafik snare end arten. Derudover blev der igen i 2009 anmeldt flere scanninger mod Windows-systemer på TCP-port 139 og 445. Også Microsoft SQL Server var under angreb på TCP-port 1433.

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

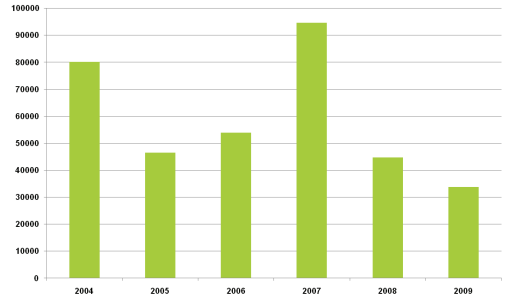
13 Cio.com, 2009; "*8 dirty secrets of the IT security industry*".

14 Deloitte, 2009; "*2009 TMT global security survey*".

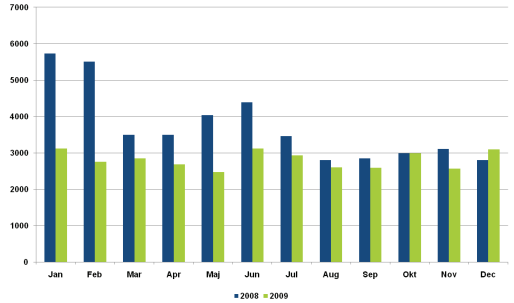
15 Shadowserver.org, 2009; "*Scan charts*".



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



Figur 8. Scanninger anmeldt til DK•CERT siden 2004.



Figur 9. Månedligt antal scanninger anmeldt til DK•CERT.

Mest opsigtsvækkende var scanninger mod henholdsvis TCP-portene 1024 og 1027. Port 1024 benyttes blandt andet af et legalt program til fjernstyring af en pc, mens der har været *trojanske heste*, der lyttede på port 1027. Blandt andet den trojanske hest ICQ-killer benytter port 1027. Derudover blev Telnet på TCP-port 23 hyppigere scannet end SSH på port 22, der nu er på en 10. plads. Anmeldte *portscanninger* på disse porte formodes delvist at dække over *brute-force* angreb, hvor der forsøges at logge på tjenesten ved at "gætte" kombinationer af brugernavn og kodeord.

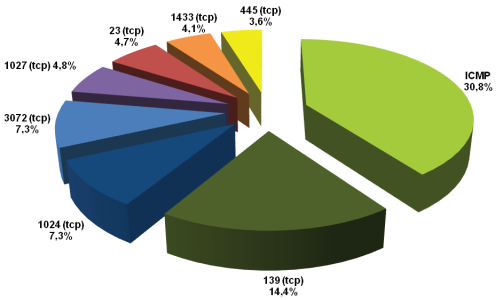
Scanninger mod HTTP og HTTPS på henholdsvis TCP-port 80 og 443 var heller ikke i 2009 blandt de hyppigst anmeldte, da de ofte ikke opdages eller registreres som forsøg på kompromittering. Således omhandlede kun henholdsvis 3,0% og 0,1% af anmeldelserne scanninger mod disse porte. For at undersøge om en webserver er sårbar, behøves kun ganske få opslag på Google, og hverken mængden eller typen af disse forespørgsler giver normalt anledning til mistænksomhed. Ligeledes vil en efterfølgende kompromittering med fx *SQL injection* tilsvarende opfattes som en legitim henvendelse, der i loggen ikke giver anledning til fejlmeddelelser eller andet, der normalt kan vække mistænksomhed. Ved denne type angreb er det værdien af de parametre, der forespørges med, der afgør, om der er tale om et angreb, og ikke forespørgslen i sig selv.

Hovedparten af de scanninger, som i 2009 blev anmeldt til DK•CERT, blev foretaget fra IP-adresser tilhørende asiatiske ISP'er (Figur 11). USA var dog igen det enkeltland, hvorfra flest scanninger havde sit udspring, mens Danmark med 1,4% af alle anmeldelser endte på en 18. plads.

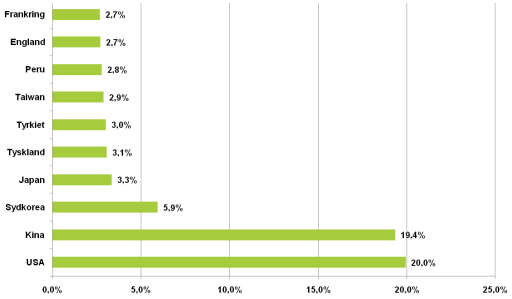
Mål og midler for scanninger har flyttet sig. Hvor man tidligere ved scanning af store netsegmenter blindt søgte maskiner, der havde den seneste sårbare applikation, afsøges der i stigende grad målrettet *sårbarheder* i specifikke webapplikationer og applikationer, der umiddelbart kan tilgås. Webapplikationerne kan findes via fx Google, og kompromittering kan ske, uden at det i firewall- eller applikationsloggen giver anledning til uregelmæssigheder.

3.3. Malware og andet utøj

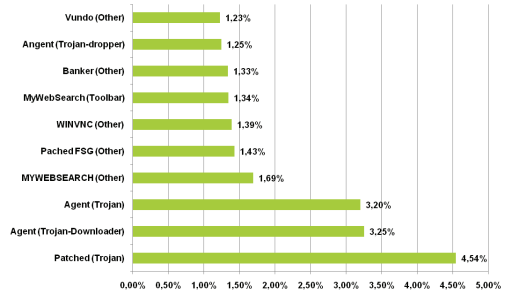
2009 bød på en fortsættelse af nogle af de tendenser, der gennem de seneste år har kunnet observeres. Bortset fra udbruddet af *Conficker* i starten af året blev der i 2009 ikke observeret væsentlige udbrud af netværksbaserede *orme*. Også de mailbaserede vira har været på retur. Det gennemsnitlige virusniveau faldt til en e-mail-inficeringsgrad på 0,35% mod 0,70% i 2008[16], således at kun 1 ud af 286 afsendte e-mails i 2009 indeholdt *virus*. Derimod er der i 2009 sket en stigning i antal og inficeringer med *trojanske heste*, som da også var bland de hyppigst fjernede *malware* typer i Danmark i 2009 (Figur 12). Således var den i Danmark hyppigst fjernede *malware* ifølge F-secure trojaneren Patched, der også er kendt under navnet *Patcher*. *Patcher* var et væsentligt element i et målrettet angreb mod de danske netbanker (se senere).



Figur 10. Hyppigst scannede portnumre i 2009, DK•CERT.



Figur 11. Scannende IP-adressers landetilhørsforhold.



Figur 12. Hyppigste danske malware infektioner identificeret af F-secure i 2009[17].

16 MessageLabs Intelligence, 2009; "*MessageLabs Intelligence: 2009 Annual Security Report*".

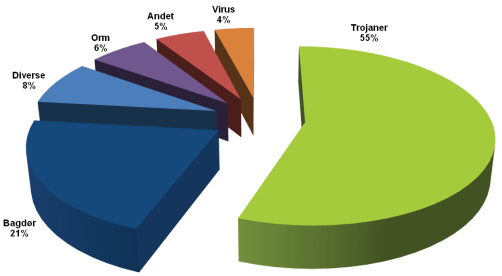
17 F-secure.com, 2009; "*F-Secure Security Lab - Virus World Map*".

2009 blev året, hvor nye *malware*-varianter oversteg mængden af legitim software[18], og også i udlandet udgjorde *malware* et stigende problem. Antallet af organisationer, der i en amerikansk undersøgelse oplevede *malware*-inficerede computere på eget netværk, steg således i 2009 til 64%[19]. Da *botnet*-programmer indgik som et separat punkt i undersøgelsen, må den væsentligste del af stigningen skyldes *trojanske heste*, men også den mailbaserede orm *Conficker* (eller *Downadup*) kan have haft en finger med i spillet. Netop udviklingen af *trojanske heste* havde i 2009 vind i sejlene. Således var 55% al ny *malware* i første kvartal af kategorien *trojanske heste*, mod kun 46% i 2008 (Figur 13). Denne tendens formodes at fortsætte, således at langt størstedelen af al ny *malware* ikke længere besidder evnen til selv at sprede sig. I Figur 13 dækker kategorien *diverse* over en række uønskede programmer som fx dialere, adware, hackerværktøjer mm., mens kategorien *andet* dækker over uklassificerede skadelige programmer.

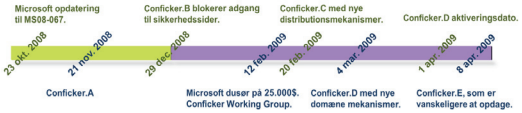
Netop *Conficker*, der dukkede op i oktober 2008, var en af årets mest omtalte. Den estimeres globalt at have inficeret mere end 6 millioner computere[21]. Den første version udnyttede et hidtil ukendt sikkerhedshul i Windows. Efter et par dage udsendte Microsoft en ekstraordinær sikkerhedsrettelse, der lukkede hullet. Lige før nytår kom den anden udgave af *Conficker*, der desuden spredte sig ved at kopiere sig over på USB-nøgler og andre flytbare medier. Her udnyttede den AutoRun-funktionen i Windows, så den kørte automatisk, når mediet blev sat i en pc.

Conficker udviklede sig i 2009 med yderligere tre varianter (Figur 14). Den første, *Conficker*.C, viste sig i februar, og i marts kom ormens fjerde version. Sikkerhedsfirmaerne har forskellige estimater af, hvor mange pc'er der var inficeret med en variant af *Conficker*, men der er enighed om, at det var millioner af computere[22]. Derfor har det undret eksperterne, at *Conficker* øjensynligt ikke gjorde andet end at sprede sig. I lang tid var der ingen bud på, hvad bagmændene ville opnå ved at sprede deres orm. I version C og dens efterfølger var der indbygget en funktion, som vakte opmærksomhed. Alle pc'er, der var inficerede med ormen, var programmeret til at opdatere sig med ny software den 1. april 2009. Det fik nogle til at vente et ragnarok, hvor millioner af inficerede pc'er på samme tid ville indlede et koordineret angreb.

Katastrofen udeblev. Pc'erne prøvede at opdatere sig den 1. april, men bagmændene lagde ikke ny kode ud til dem. Det skete først en uge senere, hvor der dukkede en ny udgave op. Og her fik vi måske første gang en forklaring på, hvad der var årsagen til, at ormen overhovedet er udviklet. Den nye udgave installerede et falsk antivirusprogram ved navn SpywareProtect2009[24]. Måske indgik *Conficker* på denne måde i den stadigt stigende strøm af *scareware* og virkningsløse falske sikkerhedsprogrammer, der ofte også besidder andre skjulte



Figur 13. Fordeling af ny malware i første kvartal 2009[20].



Figur 14. Tidslinje for Confickers udvikling i 2008 og 2009[23].

18 MessageLabs Intelligence, 2009; "*MessageLabs Intelligence: 2009 Annual Security Report*".

19 Computer Security Institute, 2009; "*2009 CSI computer crime & security survey*".

20 IBM, 2009; "*X-Force 2009 mid-year trend and risk report*".

21 MessageLabs Intelligence, 2009; "*MessageLabs Intelligence: 2009 Annual Security Report*".

22 Computerworld.dk, 2009; "*Conficker har gnavet sig ind i syv millioner pc'er*".

23 Govcert.nl, 2009; "*Trend report 2009. Insight into cyber crime: Trends & figures*".

24 DK•CERT, 2009; "*Conficker installerer falsk antivirus*".

"funktioner" og hensigter. I så fald var *Conficker* simpelthen udviklet med det formål at tjene penge på brugere, der narres til at købe et unødvendigt og virkningsløst antivirusprogram efter forudgående "detektion" af en eller flere farlige filer.

I februar udlovede Microsoft en dusør på 250.000 dollar for oplysninger, der kunne føre til domfældelse over bagmændene[25]. De menes at befinde sig i Ukraine, men ingen er endnu blevet anholdt, og der er ikke set nye varianter af *Conficker* siden april måned 2009.

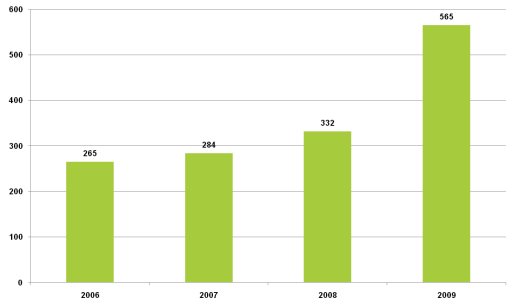
Som en konsekvens af *Conficker* har Microsoft ændret måden, hvorpå AutoRun fungerer. Ændringen betyder, at der fra Windows 7 kun vises de indbyggede muligheder i Windows for, hvad man kan gøre med en USB-nøgle, der sættes i pc'en. Et skadeligt program kan ikke længere vise en tekst som fx "Vis filer på disken" som forklaring på en kommando, der reelt kører et program.

I slutningen af 2008 og starten af 2009 oplevede vi i Danmark et angreb på netbankerne, som i sin målrettethed og professionalisme ikke tidligere er set. Midlet var en *trojansk hest*, som brugerne downloadede fra kompromitterede legale websites. *Trojanske heste* målrettet netbanker har overtaget markedet for indsamling af kreditkortinformationer. Således var der i 2009 sket en markant stigning i anmeldelser til DK•CERT vedrørende *malware*-inficerede websites (Figur 15). De fleste skyldtes *trojanske heste*.

Blandt nettets øvrige nye trusler i 2009 var den *trojanske hest* Opachki, der første gang blev opdaget den 22. september[26]. Trojaneren spredtes ved *drive-by-download* fra inficerede hjemmesider og benyttede sig af avancerede mekanismer til at holde sig skjult på det inficerede system. Den væsentligste nyhed var dog et skift i den bagvedliggende forretningsmodel. Bagmændene tjente penge ved at snyde websteder, der anvender såkaldt affiliate-baseret annoncering. Opachki omdirigerer links og søgeresultater til søgesider med reklamefinansiering. Hvis offeret efterfølgende klikker på et af søgeresultaterne, får bagmanden en lille gevinst i form af betaling fra partneren. Som en ekstra feature fjerner Opachki evt. tidligere infektioner med en anden *trojansk hest* Zeus. Årsagen til dette er ukendt[27].

Sikkerhedsdivisionen under det amerikanske it-firma EMC, RSA, opdagede i 2009, at kriminelle var begyndt at bruge Instant Messaging (IM, chat) til hurtigere levering af data høstet på computere inficeret med en *trojansk hest*[28]. Ved at indbygge Jabber IM-moduler i versioner af den *trojanske hest* Zeus var det herved muligt i realtid at opsamle data høstet på de inficerede computere. Netop hastigheden hvormed fx kreditkortinformationer kan leveres, har betydning for, hvor stor en del af de indsamlede informationer der stadig er valide, når de skal (mis)bruges.

Cirka 80% af de domæner, der i 2009 blev blokeret for at hoste *malware*, var



Figur 15: Websites med trojanere og phishing-sider anmeldt til DK•CERT.

25 Microsoft.com, 2009; "*Microsoft Collaborates With Industry to Disrupt Conficker Worm*".

26 Symantec.com, 2009; "*Trojan.Opachki*".

27 Secureworks.com, 2009; "*Opachki Link Hijacker Trojan Analysis*".

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

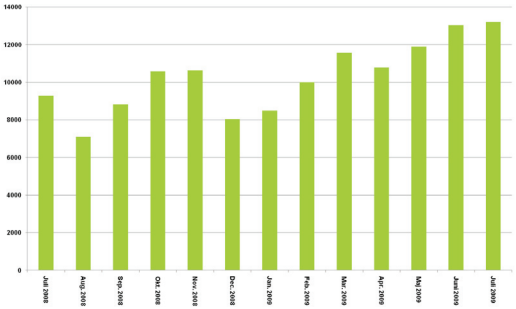
kompromitterede legale websites[29]. Det illustrerer behovet for at sætte fokus på webapplikationernes sikkerhed. Særligt set i lyset af, at it-analyse virksomheden Gartner allerede i 2008 slog fast, at:

"*Malware distribution methods have shifted from traditional viruses, mass mailers and network worms to Web-hosted attacks*[30]."

Ovenstående illustreres tillige ved, at mængden af *phishing*-mails i første halvdel af 2009 ifølge IBM var på 0,1% af al udsendt *spam*, eller ca. en femtedel i forhold til 2008[31]. Omvendt beskriver RSA en stigning i stigning i antallet af hostede *phishing*-sider på cirka 42% i perioden juli 2008 til juli 2009 (Figur 16). Tilsammen giver det et billede af flere målrettede angreb af mindre varighed og intensitet. En tendens vi også har set i DK•CERT.

Hvor *phishing*-sider tidligere blev hostet på kompromitterede legale websites, hostes 61% af alle *phishing*-sider i dag i *botnet*, der ifølge RSA benytter fast-flux teknologi[33]. Herved opnås, at *phishing*-sidens levetid mangedobles[34]. Levetiden er afgørende for mængden af data høstet via udsendte mails, hvor svarprocenten i forvejen må formodes at være lille. Et andet middel til at øge succesraten for *phishing*-mails har været at udsende færre, men til gengæld mere målrettede og troværdige mails. Fx modtog flere danske internetbrugere i september mails, der øjensynlig var afsendt af PBS og Banske Bank. De opfordrede modtageren til at oprette en *MasterCard SecureCode* eller *Verified by Visa*-kode til brug ved handel på nettet. Mailen var udført på fejlfrit dansk, og timingen var god. Mange var ved handel på nettet i løbet af 2009 blevet opfordret til at oprette disse koder netop som en sikkerhedsforanstaltning mod misbrug. Efterfølgende fortalte sikkerhedschef Poul Otto Schousboe fra Danske Bank, at man nu ville indføre *Sender Policy Framework (SPF)*. Det skal forhindre uautoriseret afsendelse af mails fra adresser under Danske Banks domæner[35].

Botnet er i dag den væsentligste kilde til *spam*. 75% af al *spam* blev i 2009 udsendt via kun fem forskellige *botnet*[36]. Tidligere infiltration har vist, at kun 28 af 350 millioner udsendte farmaceutiske *spam*-mails førte til et salg[37]. I perioden januar til juni 2009 skete der ifølge sikkerhedsorganisationen M86 Security globalt set en stigning i mængden af *spam* på 60%. Mængden af *spam* var i sommeren 2009 igen oppe på det "normale", eller ca. 151 milliarder afsendte *spam*mails om dagen[38]. Således var 84% af alle e-mails på verdensplan i november 2009 *spam*, mens andelen i Danmark, som toppede listen, var oppe på næsten 95%[39]. Siden juli 2009



Figur 16. Stigning i phishing-angreb i perioden juli 2008 - juli 2009[32].

29 MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*".

30 Gartner, 2008, "*Why malware filtering is necessary in the web gateway*".

31 IBM, 2009; "*X-Force 2009 mid-year trend and risk report*".

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

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

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

35 Computerworld.dk, 2009; "*Sådan vil Danske Bank beskytte dig mod phishing*".

36 M86security.com, 2009; "*Marshal8e6 security threats: Email and web threats*".

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

38 MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*".

39 MessageLabs Intelligence, 2009; "*Messagelabs intelligence november 2009*".

er mængden af *spam* ifølge Spamcop.net dog igen aftaget[40].

Anmeldelser vedrørende *spam* afsendt fra danske computere varetages herhjemme af forbrugerombudsmanden[41]. DK•CERT behandler kun anmeldelser om *spam*, som vedrører de netværk, DK•CERT overvåger. Vi har således ingen repræsentative data vedrørende *spam* i Danmark.

40 Spamcop.net, 2009; "*Total spam report volume, one year*".

41 Forbrugerombudsmanden; "*Klag over spam*".

4. Tingenes tilstand i 2009

Vi vil her forsøge at gøre status på it-sikkerhedsåret 2009 og sætte overskrift på nogle af de emner, som vi mener, var væsentlige. Med udgangspunkt i forrige afsnit fokuserer vi på overordnede sammenhænge og enkelte begivenheder, der tegner en tendens, der peger fremad. Afsnittet giver således med udgangspunkt i 2009 en pejling på de udfordringer, vi i fremtiden kan står overfor, når det handler om at beskytte vores it-aktiver.

Identitetstyveri var som i 2008 mål for en stor del af it-kriminaliteten. Midlerne var tilsvarende de samme, omend de er blevet mere komplekse og målrettede. For at øge andelen af besvarelser målretter bagmændene informationen til den enkelte gruppe af modtagere i stedet for blot at masseudsende mails fra "en stor bank" eller lignende. I denne proces spiller forarbejde og psykologiske mekanismer en væsentlig rolle i det, som kaldes *social engineering*. Således var flere af de *phishing*-kampagner vi så i 2009 udført på fejlfrit dansk.

Phishing er dog ikke den eneste måde at skaffe sig adgang til brugernes bankkonti på. *Trojanske heste* installeret fra kompromitterede legale websider er et andet yndet middel, som gennem de seneste år har vundet større indpas. Vi indleder afsnittet med at lade Peter Kruse fra CSIS Security Group A/S fortælle om et målrettet angreb mod danskerne, som det udspillede sig i 2009. Angrebet blev blandt andet muliggjort af sårbare legale webapplikationer, der er det andet emne vi beskriver.

Identitetstyveri har afledt et behov for *muldyr* til hvidvaskning 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 2009 blev rekrutteringen af muldyr i stigende grad tilpasset det danske marked. Jobannoncer på danske jobsites og i dansksprogede mails forsøgte således at lokke danskerne til at stille deres bankkonti til rådighed.

I alt var der i 2009 færre indbrud på danske netbank-kontoer, der til gengæld gav anledning til større tab[42]. Det er dog ikke kun borgernes bank- og kreditkortinformationer, der står for skud. Alle typer af personlige eller virksomhedsspecifikke oplysninger har med videresalg for øje interesse og er til salg på nettet. Således er der ifølge Trend Micro et marked for alt fra kreditkortinformationer til kontooplysninger fra fx Gmail, Twitter og iTunes[43]. Som en væsentlig del af forsyningskæden for *identitetstyveri* indgår brugen af sårbare webservere til distribution af *malware* samt *botnet*-inficerede computere til distribution af *phishing*-mails. Netop *botnet* er det tredje emne, der tages op i dette afsnit.

Hverken industrispionage eller den politisk motiverede it-kriminalitet ramte i 2009 mediernes overskrifter herhjemme. Stormen efter *Muhammed-krisen* er øjensynligt klinget af. Alligevel er antallet af *defacements* mod danske

42 Version2.dk, 2009; "*Netbanktyve bliver dygtigere og får større udbytte hos danskerne*".

43 Trendmicro.com, 2009; "*Priset för ditt kreditkort på svarta marknaden*".

Identitetstyveri

Identitetstyveri betegner brugen af personlige informationer til misbrug af en andens identitet. Mest udbredt er misbrug af kreditkortinformationer til overførsel af penge eller køb af varer på nettet. Derudover kan informationer, der benyttes, fx være personnumre samt adgangsoplysninger til offentlige myndigheder, mailkonti, internetbutikker, sociale netværkssider, onlinespil og lignende.

Identitetstyveri modsvares i den juridiske terminologi af dokumentfalsk og bedrageri.

hjemmesider ifølge Zone-h.org steget. Det var i 2009 højere end i 2006, som var året for *Muhammed-krisen*. Fx proklamerede en arabisk hackergruppe i oktober krig mod danske websites og havde i første omgang held til at *deface* 52 mindre websites, alle placeret på danske webhoteller[44]. Mens vi ikke forventer i fremtiden at modtage informationer vedrørende industrispionage, vurderer vi alvorligheden og forudsigeligheden af de politiske *defacements* til at være relativ lille. Hverken industrispionage eller den politisk motiverede it-kriminalitet vil derfor i år blive behandlet særskilt.

En amerikansk undersøgelse viste i 2009, at der var sket en stigning i mængden af organisationer, der blev udsat for *denial-of-service*-angreb[45]. Hvorvidt angrebet på Danske Spil i august 2009 var et forsøg på tyveri af kreditkortinformationer, afpresning, skulle skabe fordele for en konkurrerende spiludbyder, var politisk motiveret eller havde en helt femte årsag, er i offentligheden endnu uvist.

I 2009 synes smartphones at være blevet allemandseje. Mens de tidligere har været forbeholdt erhvervslivet, skulle man i 2009 ikke dreje hovedet mange gange før man fik øje på en, der med sin smartphone var i gang med at tweete, opdatere sin Facebook-profil eller lignende. Godt hjulpet på vej af teleselskabernes dataabonnementer ramte særligt Apples iPhone markedsandele, der ikke tidligere herhjemme er set for en enkelt telefonmodel. Både smartphones med iPhone i spidsen og de sociale netværkstjenester blev i stigende grad i 2009 målet for it-kriminalitet, og er derfor afsnittets følgende emner.

Vi afrunder med at gøre status på nogle overordnede temaer, der var med til at præge 2009 med hensyn til den måde, man i organisationerne opfatter og varetager it-sikkerhed på. Nogle af disse temaer er fremkommet som følge af den teknologiske udvikling, mens andre er betinget af ændret lovgivning eller behovet for tilpasningen af organisatoriske processer, således at de kan modsvare forandringer i it-kriminalitetens væsen. Fælles må det dog formodes, at disse tendenser peger fremad og vil præge organisationernes måde at varetage it-sikkerheden på i årene, der kommer.
Afslutningsvis beskriver Lars Neupart, Neupart A/S, it-sikkerhed fra et perspektiv af *Governance, Risk- og Compliance management (GSR)*.

4.1. Målrettede angreb mod Danmark

Af Peter Kruse, CSIS Security Group A/S.
Vi har nu begge ben godt inde i 2010 og nye trusler tegner sig i horisonten. 2010 bliver et år, hvor informationstyve vil skabe flere overskrifter i medierne. Det peger alt i retning af. 2009 blev startskuddet for en ny målrettet kampagne fra russiske it-kriminelle, som vil trække dybe spor ind i det nye år.

I 2009 blev informationstyven kendt som *Patcher* eller *Multibanker* en synlig og accepteret trussel mod danske organisationer og borgere. *Patcher*, der i dag findes

Danske Spil ramt af DDoS-angreb

Danske Spil blev lørdag den 15. august udsat for et systematisk DDoS angreb
med flere end 10 millioner logon-forsøg. Angrebet afskar store dele af weekenden spillelystne danskere fra at spille lotto, tips, oddset og lignende, og kostede virksomheden flere millioner kroner.

Angrebet, der kom fra mange og skiftende IP-adresser i blandt andet Østeuropa og Saudi arabien, gjorde det ifølge it-direktør i danske spil Jørgen Falsvig umuligt at blokere de angribende IP-adresser. Først søndag morgen kunne der åbnes for adgange til sitet, dog hovedsageligt fra IP-adresser i Danmark. Årsagen til angrebet havde Jørgen Falsvig den 17. august ingen idé om[46].

44 Version2.dk, 2009; "*Islamist-hackere til angreb mod Danmark: 52 sites skamferet med død og Allah*".

45 Computer Security Institute, 2009; "*2009 CSI computer crime & security survey*".

46 Version2.dk, 2009; "*Danske Spil ramt af DDoS-angreb*".

i flere end 100 forskellige varianter, var side om side med *Conficker* den største enkeltstående trussel i 2009, i form af inficerede danske maskiner. Da *Patcher* var på sit højeste infektionsniveau i starten af 2009 var flere end 10.000 maskiner herhjemme på samme tid ramt af denne skadelige og avancerede informationstyv, som er designet til at gennemføre indbrud i danske netbanker. På trods af generel høj sikkerhed i danske netbanker er *Patcher* designet, så den kan omgå sikkerhedsforanstaltningerne og udføre uautoriserede transaktioner fra inficerede maskiner.

De første *Patcher*-inficerede maskiner blev konstateret i september måned 2008. Med en antivirus detektion under gennemsnitlig 5% baseret på 42 forskellige produkter kunne den trives uden brugerens viden og i stilhed gøre klar til at høste sensitive data fra de mange tusinde inficerede maskiner.

Patcher blev plantet ved såkaldte *client-side drive-by*-angreb. Det vil sige angreb, hvor en tilsyneladende uskadelig hjemmeside tilbyder scripts, som misbruger *sårbarheder* i browseren og populære tredjepartprodukter som fx Adobe Reader, Adobe Flash eller Microsoft Office. Flere af de programmer som misbruges, er typisk at finde på en præinstalleret pc købt i en hvilken som helst butik. Som ansvarlig bruger bør man derfor altid kontrollere, om der anvendes seneste version af f.eks. Adobe Reader/Acrobat, Adobe Flash, Sun Java JRE og Quicktime.

Patcher er et *userland kernel rootkit*, som patcher (heraf navnet) centrale Windows-komponenter (kernel32.dll, powrprof.dll og wininet.dll) og gør systemgendannelse af filerne umulig efter infektion og genstart af maskinen. Det betyder, at den eneste måde at gennemføre en sikker rensning af en inficeret maskine er ved at geninstallere Microsoft Windows. *Patcher* angriber udelukkende Windows og kan ikke inficere MacOSX eller Linux-distributioner. Den yderst raffinerede kode er designet til at angribe udvalgte mål og vil automatisk og uden yderligere advarsel eller synlige symptomer på infektion for slutbrugeren downloade og køre supplerende komponenter på den kompromitterede maskine.

De supplerende komponenter består bl.a. af et Browser Helper Object (BHO), som ved hjælp af Internet Explorer foretager *Man in the Browser*-funktioner. Indsamlede data gemmes lokalt og transporteres derefter løbende til en server i bandens infrastruktur. Serveren gennemfører forskellige valideringschecks, hvorefter data sendes fra videre mod en MySQL-understøttet backend-server, der bruges som lagerplads for mange gigabyte høstede data. Serverne kommunikerer igennem en restriktionspolitik på IP-niveau. *Patcher* indsamler automatisk brugernavne og passwords gemt på det inficerede system, som bruges til at logge på forskellige webservices, VPN, Citrix eller Terminal Services. Der er således tale om en informationstyv med flere komplekse supplerende funktioner.

Patcher-banden arbejder med stor sandsynlighed fra Rusland og køber sig til trafik og *pay per install*-services. De udfører ikke selv infektionen, men betaler tredjepart for det beskidte arbejde og tjener mange penge på deres målrettede angreb. De udvælger specifikt et geografisk område som mål for deres operationer. De første operationer, som er sporet tilbage til denne bande, var isoleret til Holland. I dag er bandens primære mål Danmark og Grækenland. De køber sig services hos *bullet proof hosting*-virksomheder, som hoster tvivlsomme aktiviteter uden at stille spørgsmål. Disse bullet proof hosting-virksomheder spænder fra asiatiske udbydere

Gratis Patcher-værktøj fra CSIS

Det anbefales, at man scanner sin pc for den skadelige kode. På vegne af Finansrådet har CSIS udviklet et gratis værktøj, som hurtigt kan bruges til at afgøre, om en maskine er inficeret. I modsætning til diverse antivirus programmer kan dette værktøj detektere samtlige varianter af **Patcher**:
www.csis.dk/dk/media/Detector.zip
www.csis.dk/dk/media/Detector.exe

Værktøjet kræver, at man har Microsoft .Net Framework 2 installeret på systemet. Er der problemer med at køre programmet, kan Microsoft .Net Framework (dotnetfx.exe) hentes gratis hos Microsoft:
www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5

til off-shore virksomheder registreret med falske oplysninger.

Banden står selv for rekruttering af *muldyr*, som flytter penge fra bankkontoen over i anonyme betalingsoverførselssystemer som f.eks. Western Union og MoneyGram. Når *muldyret* har accepteret "jobtilbuddet", som bl.a. i 2009 blev opslået på Jobnet.dk og efterfølgende spammet ud til vilkårlige modtagere i Danmark, overføres der penge til dennes konto. Pengene skal efterfølgende hæves og via fx posthuset sendes ud af landet. Muldyret vil med denne operation stå med 20 procent af det samlede udbytte. Det er dog en kort glæde for den naive og letsindige dansker, idet alle digitale spor af de ulovligt overførte penge vil føre politiet direkte hen til *muldyret*, som så står tilbage med et forklaringsproblem.

4.2. De sårbare webapplikationer

Sårbarheder i legale webapplikationer, hvad enten der er tale om standardapplikationer eller egenudviklede webapplikationer, udgør i dag en væsentlig trussel mod internettets brugere. Sårbare webapplikationer var således i 2009 den væsentligste kilde til infektion med *malware*. De blev derudover bl.a. defacet og misbrugt til hosting af *phishing*-sider.

Det meste nye *malware* i 2009 havde ikke evnen til at sprede sig selv. *Drive-by-angreb* fra kompromitterede sårbare legale websider var den foretrukne metode til at snige fx *trojanske heste* ind på brugerens computere. En simpel søgning på Google kan således medføre, at man uforvarende eksponeres for *malware* fra en applikation, man ellers havde tillid til. I august 2009 indeholdt 0,8% af Googles søgeresultater en eller flere skadelige URL'er[47], hvilket er mere end en fordobling i løbet af de foregående 2,5 år. Andelen har dog i perioder været oppe på 1,6%[48]. I samme måned registrerede og blokerede Google ca. 330.000 inficerede (legale) websites, eller dobbelt så mange som et år tidligere[49]. Også hos antivirusproducenten Sophos har man oplevet en stigning af *malware*-inficerede websider. Virksomheden opdagede i første halvår af 2009 23.500 nye inficerede websider om dagen[50].
I de fleste tilfælde var de webapplikationer, der i første halvår af 2009 blev udnyttet til distribution af *malware*, webapplikationer som den besøgende ellers ville have tillid til[51]. Således stod personlige hjemmesider og kommunikationsservices, der tillader brugere at uploade indhold, for næsten halvdelen af de websites, som indeholdt mindst et link til skadeligt indhold.. Mens de personlige hjemmesider ofte er placeret på webhoteller, kan sidstnævnte services benyttes på tjenester hostet hvor som helst. Næstmest inficeret var søgemaskiner, webkataloger og portaler, der i mange tilfælde lader brugeren indtaste data, som benyttes af applikationen. Først herefter kom sider med pornografisk indhold. Øvrige typer sider som online aviser og magasiner, e-handelssider mm., stod tilsammen for kun godt 20%.

47 Google.com, 2009; "*Malware statistics update*".

48 Google.com, 2008; "*All your iFrame are point to us*".

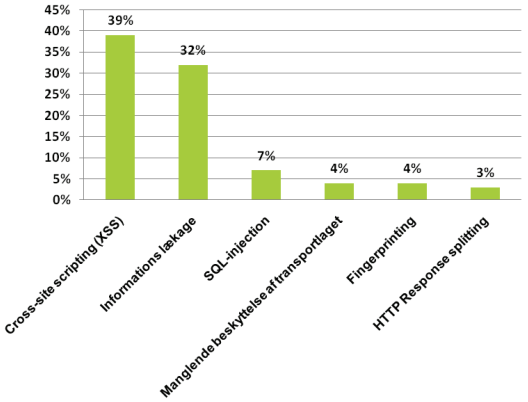
49 Google.com, 2009; "*Malware statistics update*".

50 Sophos.com, 2009; "*Security threat report: July 2009 update*".

51 IBM, 2009; "*X-Force 2009 mid-year trend and risk report*".

Webapplikationer er generelt et område, der bør have større fokus, da de i stigende grad er et delmål for it-kriminalitet. Problemet understreges ved antallet af tilgængelige sårbare webapplikationer. Således foretog DK•CERT i 2009 *sårbarhedsscanning* mod 802 forskellige webapplikationer på TCP port 80. På 456 af disse, eller mere end halvdelen, kunne der konstateres en eller flere *CVE-nummererede sårbarheder*. I alt blev der konstateret 2.557 *CVE-nummererede sårbarheder*, hvilket svarer til 5,6 pr. sårbar webapplikation. Langt størstedelen af de konstaterede *sårbarheder* blev vurderet at udgøre en medium til høj risiko for det scannede system. Således blev 709 *sårbarheder* risikovurderet højt, 1.698 middel mens kun 150 blev risikovurderet lavt.

I tillæg til de *CVE-nummererede sårbarheder*, der findes i selve webserveren, det benyttede CGI, CMS-systemet og lignende, er der ofte *sårbarheder* i den specifikke webapplikation. Ifølge WASC (*Web Applikation Security Consortium*) kunne der således på 49% af webapplikationerne, som i 2008 blev scannet af organisationerne i konsortiet, konstateres ikke *CVE-nummererede sårbarheder* vurderet til at udgøre en høj risiko. Mere end 13% af webapplikationerne kunne kompromitteres automatisk[52]. Der er ingen grund til at tro, at dette billede i 2009 havde ændret sig. Særligt *sårbarheder*, der muliggjorde *cross-site scripting*, udgjorde et væsentligt problem (Figur 17).



Figur 17. Websårbarheder konstateret ved scanning af 12.186 webapplikationer i 2008[53].

De hyppigst udnyttede sårbarhedstyper er *SQL injection* og *cross-site scripting*, der bl.a. udnyttes til datatyveri, eksponering af links til *malware* samt egentlig systemkompromittering.
En stor del af de kompromitterede webapplikationer hoster ikke selv *malware*, men henviser med indlejrede scripts til *malware*, som ofte er hostet i *botnet* og herfra eksponeres for applikationens brugere. Sikkerheden på organisationens webapplikationer er ikke kun et anliggende for organisationen selv, men i lige så høj grad for organisationens samarbejdspartnere, leverandører, kunder og andre besøgende på organisationens webapplikation. Hvis ikke organisationen formår at holde sine webapplikationer sikre, risikerer de alle, at blive inficeret med *malware*, med efterfølgende manglende tillid og troværdighed til følge.

For at afværge spredningen af *botnet*-programmer, *trojanske heste* og anden *malware* mener vi, at der bør være større fokus på sikring af danske websites, hvad enten de tilhører hr. og fru Jensen eller en kommerciel organisation. Særligt hostingvirksomheder mener vi bør tage et større ansvar for, at deres kunders sikkerhed og troværdighed ikke kompromitteres. Også ISP'erne bør tage et medansvar og blokere adgangen til de URL'er, som hoster *malware*. Men det er en vanskelig opgave, da meget af det hostes i *botnet*, der i vid udstrækning benytter *fast-flux-teknologi*.

52 Webappsec.org, 2009; "*Web application security statistics 2008*".

53 Webappsec.org, 2009; "*Web application security statistics 2008*".

4.3. Botnet, en Storm i et glas vand?

Efter at det i 2008 lykkedes at stække flere af de større *botnet*, har de levet en relativt stille tilværelse. Intet tyder dog på at *botnet* er blevet mindre, hverken i antal eller størrelse. Tværtimod synes en række nye *botnet* at have taget over, og brugen af *botnet* indgik også i 2009 som en central del af den organiserede it-kriminalitet. Det understreges også af, at der er sket en lille stigning i organisationer, der i en amerikansk undersøgelse måtte håndtere *botnet*-programmer på eget netværk. Således svarede 23% i 2009 mod 20% året før, at de havde oplevet computere inficeret med *botnet*-programmer i organisationens eget netværk[54].

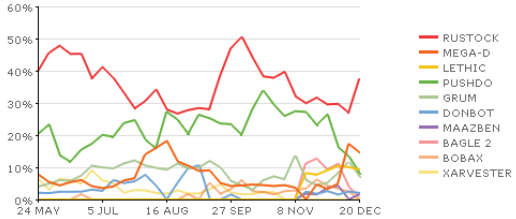
I tomrummet efter *Storm* samt efter lukningen af webhostingfirmaet McColo i november 2008 har en række nye *botnet* taget over. De er hovedsageligt involveret i udsendelse af *spam* og indsamling af data til brug ved *identitetstyveri*. Disse *botnet* har ifølge M86 Security[55] lært af lektien fra McColo. Således har de væsentligste *spam-botnet* i dag udviklet sofistikerede mekanismer, der gør dem mindre sårbare for lignende fremtidige interventioner.

Mest diskuteret var *botnet*tet Waledac, der siden sin fremkomst sidst i 2008 af mange blev spået til at være *Storms* afløser. Waledac indsamler informationer fra inficerede systemer og benyttes til distribution af *spam*. Ud over kryptering og *fast-flux*-egenskaber har de enkelte *botnet*-programmer egenskaben at kunne opdatere sig selv[56].

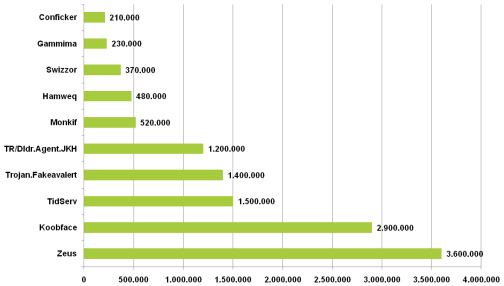
Botnet var i 2009 ansvarlige for afsendelse af op mod 90% af al *spam* på verdensplan[58]. Waledac har dog på dette punkt ikke været det mest aktive. Blandt de mest aktive *spam-botnet* var flere gengangere fra 2008 (Figur 18). Ingen af dem er dog blandt de største med hensyn til antallet af inficerede computere, der toppes af *botnet*, som benyttes til at høste data.

I juli 2009 bestod Zeus/Zbot, som ifølge sikkerhedsfirmaet Damballa er det største, af ca. 3,6 millioner inficerede computere i USA alene (Figur 19). Det kan dog diskuteres, om der i alle tilfælde i Figur 19 er tale om *botnet*-programmer eller *trojanske heste*, og hvorvidt fx Zeus er ét *botnet* eller flere mindre *botnet*, der blot benytter samme teknologi. Andre sikkerhedsleverandører, fx Messagelabs[59], nævner andre *botnet* og tal, men tendenserne er de samme.

Kun cirka 5% af de inficerede computere er del af de store *botnet*. De resterende computere er med i mindre *botnet*, der ofte er målrettet den enkelte organisation. Således er op til 9% af alle virksomhedscomputere ifølge sikkerhedsvirksomheden Damballa del af mindre og ukendte *botnet*, der målrettet indsamler data fra



Figur 18: Spam fra forskellige botnet i 2009, i forhold til den samlede mængde spam[57].



Figur 19. Botnet-størrelse baseret på inficerede computere i USA, juli 2009[60].

54 Computer Security Institute, 2009; "*2009 CSI computer crime & security survey*".

55 M86security.com, 2009; "*Marshal8e6 security threats: Email and web threats*".

56 M86security.com, 2009; "*Waledac*".

57 M86security.com, 2009; "*Tracking spam botnets*".

58 MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*".

59 MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*".

60 Damballa.com, 2009; "*America's 10 most wanted botnets*".

den inficerede organisation med videresalg for øje[61]. I Danmark må dette tal dog formodes at være mindre. Dels på grund af de i forhold til USA mindre organisationer, og dels på grund af den sproglige barriere for udenlandske kriminelle. Tilsammen gør det både mængden og anvendeligheden af data fra danske organisationer mindre.

Den væsentligste kilde til spredning af *botnet*-programmer var som med megen anden *malware* i 2009, inficering af sårbare legale websites. Brugernes computere inficeres i stigende grad ved scripts, der udnytter *sårbarheder* i browseren eller dens plugins. Disse scripts er placeret på legale websites inficeret ved hjælp af *SQL injection* eller *cross-site scripting*-angreb.

Botnet er i dag en integreret del af den organiserede it-kriminalitet. Vi har tidligere set, at en målrettet indsats kan medføre, at bagmændene mister kontrollen med store dele af deres *botnet*. Bagmændene udvikler løbende deres metoder og teknikker, hvorfor indsatsen tilsvarende løbende bør fornyes og i højere grad koordineres, nationalt såvel som internationalt. I denne sammenhæng mener vi, at ISP'erne bør spille en central rolle.

Op mod 100.000 danske computere indgår ifølge Peter Kruse fra sikkerhedsvirksomheden CSIS Security Group A/S i de verdensomspændende *botnet*[62]. Han mener, ligesom vi gav udtryk for i sidste års rapport, at ISP'erne med deres centrale placering bør indgå i bekæmpelsen af *botnet*. På samme vis som det er muligt at opdage finansielle transaktioner udført af *muldyr*, er det muligt at opdage og afværge *botnet*-aktivitet på internetudbydernes netværk. Vi mener, at man som i Sverige[63] i det mindste bør tage en diskussion om, hvorvidt ISP'erne herhjemme skal pålægges et ansvar for at bidrage til detektion og afværgelse af *botnet*-relateret trafik. Som det er i dag, er der hverken økonomiske eller lovmæssige incitamenter til dette.

4.4. Sociale netværkstjenester og privatlivets fred

I takt med at sociale netværk som Facebook, MySpace og Twitter er blevet populære, er de samtidig blevet mål for de it-kriminelles handlinger. Flere sociale netværkstjenester åbnede i 2009 deres API'er med en forventet stigning i antallet af tredjepartsapplikationer som følge. De fleste af disse hostes på domæner uden for den sociale netværkstjenestes egen struktur, og enkelte var designet til at generere online reklame, indsamle brugerprofiler og lignende[64].

I en undersøgelse foretaget af Deloitte svarede henholdsvis 83% og 80% af respondenterne, at man i deres organisation opfattede *sårbarheder* i web 2.0-teknologier og *social engineering* som trusler mod organisationens sikkerhed[65]. Brugen af web 2.0-teknologi er udbredt på de sociale netværkstjenester, hvor *social*

61 Darkreading.com, 2009; "*Up to 9 percent of machines in an enterprise are bot-infected*".

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

63 Version2.dk, 2009; "*Svenske myndigheder vil lukke internetadgangen for inficerede computere*".

64 MessageLabs Intelligence, 2009; "*MessageLabs Intelligence: 2009 Annual Security Report*".

65 Deloitte, 2009; "*2009 TMT global security survey*".

engineering er en udbredt angrebsvektor. Når brugeren modtager en beskeder fra sine venner i netværket, vil denne have større tilbøjelighed til at klikke på links eller aktivere applikationer og lignende, som kan vise sig at indeholde skadelig kode. Særligt i kombination med sårbare tredjepartsprogrammer på de besøgendes computer kan sociale netværkstjenester udgøre en trussel. Eksempelvis benytter Facebook sig af tredjepartsprogrammer som fx Quicktime, Flash og Windows Media Player, som brugerne kun sjældent opdaterer[66].

Der blev i 2009 registreret flere angreb med fx *trojanske heste* og *orme*, der udnytter netværkene til at inficere brugernes pc'er, angreb på personers privatliv og fortrolige oplysninger. Fx fik kendisser som Britney Spears, Miley Cyrus og P Diddy alle kompromitteret adgangen til en social netværkstjeneste i 2009. Vores forventning er, at også sårbare legitime tredjepartsapplikationer på sociale netværkstjenester i fremtiden vil være mål for angreb, der har til mål at kompromittere brugerne, deres data og/eller privatliv.

Inden for skadelige programmer på sociale netværk gjorde især ormen *Koobface* sig bemærket. Dens navn er dannet af bogstaverne i Facebook, men den angriber også brugere af MySpace, Hi5, Bebo, Friendster og Twitter. Når den har inficeret en pc, sender den beskeder via de sociale netværk, som pc'ens ejer er medlem af. Beskederne sendes til personens venner på tjenesten. Emnefeltet kan fx hedde "*My home video* :)" eller "*Hey! You are on news!*" I beskeden er der et link, som ofte angives at være til en opdatering af Adobe Flash Player. Linket fører til en fil, og hvis modtageren kører filen, bliver *Koobface* installeret på pc'en, hvorfra den kan sprede sig videre via modtagerens egne venner.

Koobface blev opdaget i december 2008. Der kom en ny version i marts 2009[67], hvorefter spredningen for alvor tog fart. I juli udsendte Twitter advarsel om, at flere af tjenestens brugere var ramt af *Koobface*, der udsendte "tweets" i deres navn[68].

En anden type angreb går ud på at udnytte kendte menneskers profiler. Der har været flere eksempler på, at kendtes navne optrådte på Facebook-profiler, som de ikke selv havde oprettet. Det er sket for blandt andre brevkasseredaktør Suzanne Bjerrehuus, Muhammed-tegneren Kurt Westergaard og den tidligere jægersoldat B.S. Christiansen.

Sociale netværk kan også misbruges til at sprede private og fortrolige oplysninger om andre. I februar blev en 28-årig mand idømt 20 dages ubetinget fængsel ved retten i Hjørring. Han havde lagt en video på sin Facebook-profil, hvor han havde sex med en tidligere kæreste. Foruden fængselsdommen skulle han betale 10.000 kroner i erstatning til ekskæresten. Godt 100 af mandens Facebook-venner havde haft mulighed for at se videoen[69].

Brugen af sociale netværkstjenester udgør en risiko for misbrug af data, informationer, og systemer, man både som borger og organisation bør gøre sig

66 Politiken.dk, 2009; "*Facebook er en legeplads for hackere*".

67 Us-cert.gov, 2009; "*Malicious Code Targeting Social Networking Site Users*".

68 Twitter.com, 2009; "*Koobface malware attack*".

69 It-borger.dk, 2009; "*Første dansker dømt for at uploade forbudte billeder på Facebook*".

bevidst. Herhjemme findes der en række vejledninger, der hjælper borgeren med at beskytte sit privatliv ved brug af sociale netværkstjenester. Fx findes der en generel vejledning[70] på it-borger.dk, og DK•CERT har i samarbejde med rådgivningsvirksomheden KOMFO udarbejdet en vejledning specifikt til Facebook[71].

Derimod synes der i de danske organisationer ikke at være konsensus om, hvorledes man håndterer de ansattes brug af sociale netværkstjenester i arbejdstiden, eller hvilke risici det udgør. Tilsvarende findes der da heller ikke fyldestgørende vejledninger rettet mod organisationerne.

4.5. Smartphones med mere

Ved indgangen til 2009 havde 11 procent af voksne amerikanske mobiltelefonbrugere en form for smartphone. Da året var omme, var tallet 17%[72]. Tallet dækker over en række forskellige platforme: Apples iPhone, diverse producenter med Windows Mobile, Androide, PalmOS, WebOS, Symbian eller varianter af Linux.

Den stigende udbredelse af smartphones betyder, at de it-kriminelle også er interesserede i denne nye platform. Året bragte flere eksempler på det, især når det gælder Apples iPhone. Således dukkede den første *orm*, der angriber iPhone, op i efteråret 2009. Samtidig var der flere sager om beskyttelse af private oplysninger på den populære smartphone.

Nogle af de mere avancerede brugere af iPhone udfører et såkaldt jailbreak. Det betyder, at de kører et program, der fjerner nogle af de begrænsninger, som Apple har lagt ind i telefonens styresystem. Dermed er det fx muligt at installere software, som ikke er leveret via Apples online butik for iPhone-applikationer, App Store.

I starten af november angreb en hollandsk hacker iPhones på et mobilnet ved at scanne efter TCP-port 22, der bruges af tjenesten secure shell (SSH). IPhone bruger et standardpassword for root-kontoen, som mange ofte glemmer at ændre, efter de har jailbreaket den. Det udnyttede hackeren til at installere en bagdør. Hans program viste en besked om, at offeret skulle betale fem euro for at slippe af med bagdøren[73].

Nogle dage senere blev iPhone-brugere i Australien overraskede, da der dukkede et billede af popsangeren Rick Astley op på deres telefoner. De var blevet ofre for den første iPhone-orm[74]. Ormen, der fik navnet Ikee, virkede kun på telefoner, der havde været udsat for jailbreak. Endvidere skulle telefonerne køre SSH uden ændret standardpassword. Alle disse forbehold gør, at kun en lille andel af iPhones

70 It-borger.dk, 2009; "*5 gode råd om Privatlivets fred på nettet*".

71 DK•CERT & KOMFO, 2009; "*Styr dit privatliv på Facebook*".

72 Blogs.forrester.com, 2009: "*2009: Year Of The Smartphone — Kinda*".

73 Arstechnica.com, 2009; "*Dutch hacker holds jailbroken iPhones hostage for €5*".

74 Theregister.co.uk, 2009; "*World's first iPhone worm Rickrolls angry fanbois*".

er i fare for at blive ramt. Det antages, at mellem seks og otte procent af alle iPhones har været gennem jailbreak.

Siden er yderligere et par *orme* dukket op. Phone/Privacy.A udnytter standardpasswordet til at komme ind på telefonen. Programmet kan give en hacker adgang til alle data på telefonen[75]. Endelig er der Duh/Ikee.B, som indgår i et *botnet*. Den stjæler data, som den sender til en server i Litauen[76]. Denne *orm* ændrer også standardpasswordet for root-kontoen, så brugeren får sværere ved at fjerne den. Generelt kan vi forvente i fremtiden at se mere *malware* rettet mod de mobile platforme. Problemet er, at når mobilen også bruges til blandt andet at gå på nettet og læse mail, åbnes der for en række nye angrebsvinkler. Samtidig med stigende udbredelse, kan det gøre mobile platforme til et attraktivt medie for it-kriminelle.

Foruden angreb på telefonens sikkerhed bragte året også eksempler på, at virksomheder udnyttede data om iPhone-brugerne på en måde, de var utilfredse med. Flere af de applikationer som man kan købe til iPhone, indsamler data om brugerne. Fx beskrev bloggeren Yobie Benjamin i august, hvordan spillet Vampires Live fra firmaet Storm8 ikke nøjes med at lade spillerne suge blod fra hinanden. Spillet suger også hver enkelt spillers telefonnummer op og sender det til firmaets webserver. Det samme gælder for firmaets øvrige spil til iPhone[77]. I november førte det til et sagsanlæg mod Storm8 i USA[78]. Firmaet anklages for at have overtrådt flere love ved at indsamle telefonnumrene uden at oplyse det, og uden at have brug for dem.

I oktober blev det svejtsiske firma ID Mobiles applikation MogoRoad fjernet fra Apples iPhone App Store. Det skete, efter at en blogger havde anklaget applikationen for at indsamle data om brugerne. De blev så ringet op af sælgere fra firmaet bag MogoRoad. ID Mobile skriver i et svar, at det ganske rigtigt indsamler telefonnumre, men kun for brugere på svejtsiske telenet, hvor det kan gøres lovligt. Dataene hentes ikke fra iPhonen, men fra telenettet. Applikationen er nu igen tilgængelig i App Store[79].

Eksemplerne understreger, at der er et stigende behov for at beskytte mobile enheder. Flere organisationer er blevet opmærksomme på, at de risikerer at miste fortrolige data, hvis en medarbejders smartphone bliver stjålet eller tabt. De seneste år har givet os flere eksempler på dette. Derfor er der brug for teknologier til at sikre data på enhederne, gerne med mulighed for at slette dem, når det bliver nødvendigt, selvom man ikke har fysisk adgang til enheden. Tilsvarende gælder selvfølgelig for andre typer af mobile enheder som fx laptops, netbooks, memory sticks med mere, der benyttes til lagring af data. Organisationen bør som minimum sikre, at data der transporteres uden for organisationens net, er sikret med kryptering.

Også andre typer computere, der adskiller sig fra de traditionelle pc'er, er udsat for

75 Intego.com, 2009; "*Hacker Tool Copies Personal Info from iPhones*".

76 Sophos.com, 2009; "*Another iPhone worm - and this time it's malicious*".

77 Sfgate.com, 2009; "*Apple privacy score - Snow Leopard - 10, iPhone – 0*".

78 Theregister.co.uk, 2009; "*Backdoor in top iPhone games stole user data, suit claims*".

79 Mogo.ch, 2009; "*Press Release: «mogoRoad iPhone removed from the Apple Store»*".

angreb. I 2009 så vi nogle eksempler på angreb på spilkonsoller. De er nu koblet på internettet, og dermed er de blevet særligt interessante for angriberne.

En anden type ny enhed er det mediecenter, der står under fjernsynet. Mange tænker nok ikke over, at det ofte er en computer med fuld internetadgang, og som derfor er i lige så stor fare for at blive angrebet som pc'en på kontoret. Det giver nye udfordringer for sikkerheden: Hvordan sikrer man fx, at mediecenteret er udstyret med de seneste fejlrettelser og opdateringer? Samme udfordring byder fx spilkonsollen på. Hvorvidt angreb mod forbrugerelektronik i hjemmet bliver attraktivt, synes at være bestemt af udbredelsen af platforme og tjenester.

4.6. It-sikkerhed i 2009

I Sverige var der i starten af året debat om ISP'ernes roller og bemyndigelser i forhold til *malware*-inficering af deres kunders computere. I marts 2009 indstillede Post- og Telestyrelsen således til, at ISP'erne uden kundens samtykke skulle have bemyndigelse til at begrænse eller helt lukke internetadgangen, hvis kundens pc indgik i et *botnet*[80]. Både i Holland og Australien er der indført tilsvarende ordninger, mens vi herhjemme stadig mangler koordinerede initiativer til begrænsning af udbredelse og konsekvenser af *malware*.

2009 var året hvor der herhjemme blev taget beslutning om at etablere en såkaldt GovCERT funktion, der skal sikre overblik over trusler og *sårbarheder* i produkter, tjenester, net og systemer i staten. GovCERT'en etableres i IT- og Telestyrelsen, der i forvejen varetager beredskabet for den mest kritiske teleinfrastruktur. Den forventes fuldt udbygget i løbet af i år. Selvom vi mener, at denne beslutning burde være taget langt tidligere, kan det kun være i samfundets tjeneste, at der oprettes en central enhed til varsling om it-sikkerhedsmæssige hændelser og trusler. Vi mener dog, at beslutningen er for begrænset i sit omfang og lader kommunerne, det private erhvervsliv og borgerne i stikken. Sikkerhed bør i vores øjne varetages ud fra en helhedsbetragtning og vi håber derfor, at den danske GovCERT vil indgå i samarbejder med tilsvarende private og offentlige organisationer, it-sikkerhedsbranchen, ISP'erne og lignende. Kun ved en fælles indsats kan vi påvirke it-sikkerheden i hele det danske samfund.

2009 blev også året hvor, *cloud computing* i medierne fik sit gennembrud, og teknologien nåede en førsteplads på Gartners liste over de vigtigste teknologier for 2010[83]. Alle talte om mulighederne med *cloud computing*, og ethvert nyhedsbrev med respekt for sig selv indeholdt historier om, at nu havde nogen lagt noget ud i skyen. Ud over perifere indslag, som at skyen også kunne give regnekraft til *brute-force*-angreb, blev sikkerhedsaspekter forbundet med brug af *cloud computing* næsten ikke diskuteret. At placere sine services i skyen giver ud over de forretningsmæssige fordele en række udfordringer af sikkerhedsmæssig karakter.

Cloud computing

Cloud computing er en måde at udbyde services med et højt niveau af abstraktion af ressourcer, der ofte er baseret på virtualisering. Skyen giver mulighed for service on demand, som betyder, at man får adgang til ressourcer efter behov. Har man et lille behov, bruger man få ressourcer, og hvis behovet stiger, kan man få adgang til flere ressourcer. Skalerbarhed og pris vil ofte være de væsentligste argumenter for at lade sine services outsource til skyen. Overordnet findes der tre forskellige typer af cloud-services:

Software as a Service (SaaS). Online brug af programmer efter behov, evt. med SOA-baseret funktionalitet. Det kan være online programmer som tekstbehandling, regneark og CRM-services.

Platform as a Service (PaaS). Det svarer til, at cloud-udbyderen kører styresystemet for en, og man kører applikationer i skyen, som styres ved hjælp af et API.

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

ENISA[81] og Wikipedia[82]

80 Version2.dk, 2009; "*Svenske myndigheder vil lukke internetadgangen for inficerede computere*".

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

82 Wikipedia.org, 2009; "*Cloud computing*".

83 Gartner, 2009; "*Gartner identifies the top 10 strategic technologies for 2010*".

Udbyderen vil ofte være specialiseret og kan opnå stordriftsfordele på bl.a. sikkerhed og kan i kraft af behov for standardisering tilbyde et højt minimumsniveau af sikkerhed[84]. Det betyder, at udbyderen kan tilbyde standardiserede sikkerhedsservices som en del af ydelsen til de kunder, som ikke selv har tilstrækkelig viden og/eller erfaring med it-sikkerhed. Således kan udbyderen fx tilbyde gennemtestede *patch management*-løsninger på virtuelle "standard-maskiner", som på forhånd er opdateret og sikrede. Derudover vil tilgængeligheden af services ikke blive berørt af fx bevissikring efter en sikkerhedshændelse, da man i skyen blot kan trække et virtuelt billede ned, mens servicen stadig kører.

Brugen af *cloud computing* rækker dog ikke ind i himlen. Hemmeligheden er nemlig, at hvis ikke den tjeneste man vælger at placere i skyen er sikker, kan den kompromitteres på samme vis, som hvis man havde valgt at hoste den selv. Derfor bød 2009 selvfølgelig også på tilfælde af hændelser, der havde rod i services, der var placeret i en sky. Fx blev en *command & control* server i et Zeus-*botnet* i december opdaget i en sky drevet af Amazon[85]. De sikkerhedsmæssige problemstillinger der knytter sig til *cloud-computing* synes fra et overordnet perspektiv således ikke forskellige fra al anden outsourcing.

Herhjemme oplevede bankerne stramninger i lovgivningen vedrørende deres brug af outsourcing[86]. Således blev der med virkning fra 1. oktober 2009 indført en ny lov om finansielle virksomheder, der blandt andet medfører kontroller af outsourcing-partneren og krav til udformning af kontrakten. Loven er indført for at specificere ansvar i forbindelse outsoucing af it-opgaver. DK•CERT har både tidligere og i 2009 oplevet, at netop manglende specificering af roller og ansvar ved outsourcing vanskeliggjorde udredningen af en sikkerhedshændelse. Det er vores indtryk, at kontrakterne fokuserer på normaldriften og kun i ringe grad beskriver det unormale, hvad enten der er tale om driftsforstyrrelser eller egentlige sikkerhedshændelser. Når vi tilsvarende kan konstatere, at det er muligt at kompromittere legale websider placeret på webhoteller, samt at hostingvirksomheder og ISP'er kun på ad-hoc basis adviserer deres kunder om brud på kundens it-sikkerhed, bekræfter det yderligere vores antagelse. Når det i samarbejdsrelationen ikke er specificeret, hvem der har ansvar for hvad og hvornår i situationer, der rækker ud over den normale drift, vil der være risiko for, at man som organisation ikke kan efterleve egen it-sikkerhedspolitik, gældende standarder og lovgivning. Emner som kontraktstyring og *compliance* var fra vores synsvinkel væsentlige punkter for varetagelse af it-sikkerheden i 2009, som begge rækker ud i fremtiden og fra et it-sikkerhedssynspunkt bør indgå i organisationernes varetagelse af *god selskabsledelse*.

Den 22. oktober 2009 frigav Microsoft Windows 7 som afløseren for Windows Vista. Windows 7 byder på en række funktioner, der i forhold til tidligere versioner af Windows giver mulighed for forbedret sikkerhed. I sin standardopsætning er Windows 7 dog mindre sikker end Windows Vista. En samlet implementering af Windows 7 er endnu ikke begyndt i organisationerne, men kan så småt forventes at begynde i 2010, hvor vi forventer at se de første målrettede angreb mod

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

85 DK•CERT, 2009; "*Farlige julekort kom fra Amazons cloud*"

86 Version2.dk, 2009; "*Bankernes it får outsourcing-håndjern på*".

Cookies – hvad med forbrugernes rettigheder?

Når du surfer på nettet, har du reklame- og markedsføringsvirksomheder i hælene. Via såkaldte tredjeparts-cookies, som blandt andet bruges til at skrue målrettede reklamer sammen, overvåges forbrugerens adfærd. Forbrugerrådet har ikke noget imod cookie-teknologi eller brugen af målrettede reklamer. Det er måden, det anvendes på, der har fanget Forbrugerrådets interesse.

Hellere relevant, tilpasset reklame frem for alverdens slam, vil mange mene, og man kan jo blot ignorere reklamen. Men cookie-teknologien kan også begrænse forbrugerens muligheder på nettet og herhjemme har vi set eksempler på, at det ikke kun er ens bevægelsesmønstre, der registreres og bruges. Indimellem er der også videregivet personlige oplysninger til reklamebureauerne.

Forbrugerrådet spurgte i september 2009 sit forbrugerpanel om deres viden og holdning til cookies. Et overvejende flertal vil gerne spørges, inden deres adfærd på hjemmesider registreres, og knap halvdelen mener, at det bør forbydes at bruge målrettede reklamer, som er baseret på forbrugernes adfærd. Persondata- og telelovgivningen indeholder ingen specifikke regler, men nogle generelle regler om oplysningspligt. Vi mener, at forbrugeren skal have mere indflydelse på, hvordan egne oplysninger benyttes. Udfordringen er at sikre balance mellem retten til et privatliv og et fortsat smidigt internet. EU's telepakke er netop blevet revideret, uden at det dog har medført bedre beskyttelse for forbrugeren. Men blot det at få reglerne frem vil være et fremskridt, da cookie-teknologien kun er i sin vorden og perspektiverne allerede skræmmende. Se mere om *cookies* på: www.fbr.dk/cookie

Anette Høyrup, Forbrugerrådet

operativsystemet.

Både borgerne, organisationer og myndigheder publicerer og lagrer stadig flere oplysninger om både sig selv og hinanden. Når data samkøres og bruges aktivt, lurer en stigende fare for krænkelse af borgerens privatliv, hvorfor også 2009 bød på diskussioner om beskyttelse af privatlivets fred. En diskussion der for alvor tog til i styrke efter indførelse af terrorlovgivningens logningsbekendtgørelser i 2007. I 2009 drejede debatten sig dog i højere grad om organisationernes brug af borgeroplysninger end om myndighedernes. Fx blev brugen af tredjeparts *cookies* taget op til debat af Forbrugerrådet[87].

Mens den teknologiske udvikling løbende giver os mulighed for at minimere risici, der knytter sig til teknologien selv, er det vanskeligere at beskytte sig mod den menneskelige faktor. Netop individet, enten som privatperson eller som medarbejder i en organisation, er i stigende grad det svage led i sikkerhedskæden. I takt med at de it-kriminelle er blevet dygtigere og mere opfindsomme, har de rettet indsatsen mod borgeren, hvor risikoen er mindst og gevinsten er størst. For organisationerne har det betydet et fokusskifte væk fra centrale tekniske løsninger til beskyttelse af perimeteren mod implementering af centralt styrede decentrale løsninger. Enterpriseversioner af fx antivirus og kryptering, logkonsolidering og *DLP* er eksempler på dette.

4.7. It-sikkerhed i et compliance-perspektiv

Af Lars Neupart, Neupart A/S.
It-branchen vælter sig i forkortelser, og nogle af dem glemmer vi hurtigere end andre. Blandt de mere sejlivede tror jeg er GRC, som vi så mere til i Danmark i 2009. GRC betyder *Governance, Risk-* , og *Compliance management*, hvor it-delen omfatter:

- *Governance*: It-ledelse, it-sikkerhedsledelse, tilpasning af it og it-sikkerhed til forretningsmål, ISMS, sikkerhedspolitikker, beredskabsplaner, forankring, awareness-kampagner med mere.
- *Risk Management*: Hvor stor er organisationens "risikoappetit". Hvordan afhænger forretningen af it, og hvad gør ondt på forretningen (konsekvensvurdering, "BIA"). Og hvor sandsynligt er det, at det sker? Hvordan håndterer organisationen disse risici?
- *Compliance Management*: Identifikation og aktiviteter, der sikrer efterlevelse (helt eller delvist) af kravsæt eller anbefalinger, typisk i form af lovgivning, kundekrav eller standarder for et område eller en branche.

Jeg vurderer GRC-begrebet som overlevelsesdygtigt, fordi langt de fleste, hvis ikke alle, organisationer har brug for de tre begreber hver for sig.

Betalingskortstandarden PCI DSS (Payment Card Industri – Data Security Standard) er endnu ikke slået rigtigt igennem i Danmark. Standarden er primært blevet opfattet som henvendt til den finansielle sektor, men er måske reelt vigtigere for detail-branchen. Ganske vist kan man kontraktmæssigt forpligte sine it-

87 Forbrugerrådet, 2009; "*Cookies på nettet*".

leverandører til at efterleve betalingskortkravene, og i nogen udstrækning nøjes med elektroniske erklæringer om dette. Man kan dog som bekendt ikke helt eliminere sit eget ansvar med en leverandøraftale.

Leverandøraftaler er også en vigtig ingrediens i forbindelse med et i 2009 meget omtalt fænomen, *cloud computing*. Skeptikere siger, at *cloud computing* kan være en modsætning til *compliance*, i hvert fald compliance til love og standarder. Sikkerheden i skyen afhænger af typen af sky, og der er masser af udfordringer. Der er også en særdeles tiltalende økonomi i *cloud computing*, hvorfor mange personer og organisationer aktivt arbejder på at løse sikkerhedsproblemer og *compliance*-udfordringer forbundet med skyen. I 2009 så vi således vejledninger fra blandt andet Cloud Security Alliance (cloudsecurityalliance.org) og Enisa[88], så der er håb forude.

Beredskabsplanlægning er en anden voksende tendens, som vi så i 2009. Blandt de mest fremstormende britiske standarder er BS25999, som beskriver et "Business Continuity Management System". Således er det nu muligt at få certificeret sin beredskabsstyring. Det var briterne der opfandt forløberne til ISO 2700x og dermed DS484, så vi kan have en forventning om en tilsvarende positiv effekt på beredskabsplanlægning og -styring i danske organisationer.

Apropos DS484 blev 2009 året, hvor flere begyndte at stille fornuftige spørgsmål til omfanget af DS484-efterlevelse. I staten har flere institutioner oplevet DS484-efterlevelse som bureaukratisk, hvilket ikke er underligt. Der kræves meget før man kan påberåbe sig efterlevelse, i modsætning til ISO 2700x-familien, der er mere fleksibel og fokuserer mere på processer og ledelse. I sidste ende er det dog *et governance* spørgsmål, hvor stringent DS484-efterlevelse indføres i praksis. Det bliver spændende at se, om det nye år bringer beslutning om, hvorvidt DS484 skal opdateres som en selvstændig dansk standard. Den ISO-standard, der var grundlaget for DS484, er i mellemtiden blevet til en serie af standarder med foreløbig fem dokumenter, og der er allerede flere opdateringer på vej. Så en beslutning er nødvendig.

Lovgivningsmæssigt er det stadig de gamle travere som persondataloven, bogføringsloven og markedsføringsloven, hvor *compliance*-begrebet har mest it-relevans i Danmark. Det er således værd at bemærke, at EU i 2009 i højere grad begyndte at tale om "Data Breach Notification". Det betyder, at virksomheder, der sjusker med sikkerheden omkring borgeres informationer, kan blive forpligtet til at informere de personer, hvis data de har mistet. Jeg er imod regler for reglernes skyld, men dårlig informationssikkerhed bør ikke være gratis. Derfor kan lovgivning på dette område være en sund drivkraft for, at flere organisationer tænker sig ekstra godt om og beskytter deres egne og deres kunders informationer ordentligt. Effekten vil utvivlsomt være bedre informationssikkerhed.

88 ENISA, 2009; "*Cloud computing risk assessment*".

5. Et kig i krystalkuglen

Conficker tog os i starten af 2009 med bukserne nede. Hvem kunne have forudsagt, at vi i 2009 ville blive ramt af et så alvorligt internationalt ormeangreb? Ja, vi havde i hvert fald ikke. Men sådan er det vel med forudsigelser. Dette afsnits forudsigelser af kommende trends skal derfor læses som et kvalificeret bud på, hvad vi kommer til at opleve, og ikke som den absolutte sandhed om it-kriminalitetens udvikling.

Siden *Conficker* slog til har vi ikke været ramt af alvorligere udbrud af hverken orme eller vira, hvilket er en tendens, vi tror fortsætter i de kommende år. Derimod oplevede vi i 2009 andre begivenheder, vi mener i større grad peger fremad og vil være med til at tegne den fremtid, vi er på vej ind i. Fx blev danskernes netbankkonti angrebet fra flere kanter på måder, der virkede langt mere overbevisende og professionelle, end vi tidligere har oplevet.

Vi tror, at bankernes stigende fokus på sikkerhed kan flytte it-kriminaliteten til områder, hvor gevinsten er lettere at hente og med mindre risiko, på samme vis som pengeløse banker, farvepatroner og forsinkelser på større kontantudbetalinger har flyttet røverierne fra bankerne til de mindre beskyttede posthuse. Et andet scenarie er selvfølgelig, at vi kan komme til at se færre, men til gengæld mere professionelle, målrettede og økonomisk givtige angreb, som de indbrud vi i 2009 oplevede mod værdihåndteringscentraler. Måske var *DDoS*-angrebet på Danske Spil i august måned en forsmag på dette.

Under alle omstændigheder tror vi, at vi kommer til at opleve større målrettethed og opfindsomhed hos de it-kriminelle, som i stigende grad organiserer sig i stadig mere professionelle internationale netværk. Således kan man fra en overordnet betragtning sige, at der er tale om *business as usual*. Det vi oplevede i 2009, vil også være det, vi i fremtiden vil opleve, blot mere målrettet og professionelt udført.

Nedenfor har vi forsøgt at konkretisere dette i nogle overordnede scenarier for fremtiden, som vi tror vil præge billedet de kommende år. Efterfølgende beskriver vi de udfordringer, det vil medføre, når vi som borgere, organisationer og samfund vil beskytte vores aktiver mod it-kriminalitet.

5.1. It-kriminalitetens fortsatte udvikling

It-kriminalitet var også i 2009 er en god forretning. Vores forventning er derfor, at bagmændene i de kommende år vil forsøge at udvide deres aktiviteter for at optimere succesraten og udbyttet samt minimere risikoen for at blive fanget. Det betyder ikke større medieeksponering af enkelte angreb og trusler, snarere tværtimod. Vi forventer nemlig, at de angreb der kommer, bliver mere målrettede og udspekulerede, som vi også så det i 2009. Således kan vi i fremtiden forvente en større variation i typen af angreb, der i stigende grad forsøges skjult for offentligheden. Som følge af dette forventer vi, at fremtiden byder på en fortsættelse af udviklingen fra sidste år med færre, men til gengæld mere

Informationstyveri anno 2010

Vi er trådt ind i et nyt årti og samtidig en ny æra i kampen mod it-kriminalitet. Vi kæmper mod flere organiserede bander end nogensinde før, som binder maskiner ind i store *botnet*, der kan misbruges til forskellige formål. Denne kamp vil trække dybe spor ind i det nye år og det nye årti.

Antallet af malware er siden 2008 nærmest eksploderet. Vi ser en markant stigning i mængden af malware, som indeholder funktionalitet til dataindsamling. Der er mange penge i informationstyveri. De indsamlede data, som bl.a. også stammer fra store børsnoterede selskaber, kan potentielt indeholder regnskaber, strategier og intellectual property, der indlysende nok kan skade danske organisationers konkurrenceevne og troværdighed i hænderne på de forkerte mennesker.

I takt med at malware-skribenterne er blevet flere og bedre, tyder udsigten til det nye år på, at de traditionelle it-sikkerhedsteknologier som f.eks. antivirus vil blive blandt de store tabere i kampen mod skadelig kode. For at bremse denne udvikling er det bindende nødvendigt, at der tænkes "ud af boksen", og der iværksættes initiativer, der kan afbøje angreb mod borgerne og organisationer i Danmark.

Peter Kruse, CSIS Security Group A/S

målrettede og succesfulde angreb på danske borgere og organisationer.

Det primære motiv for spredningen af *malware* forbliver adgang til borgernes eller organisationernes fortrolige data, hvad enten der er tale om *identitetstyveri*, trusler om offentliggørelse af personlige data eller *denial of service*-angreb.

Trojanske heste og *botnet*-programmer bliver også i fremtiden de hyppigst distribuerede typer *malware*, som ud over sårbare webapplikationer i stigende grad også vil sprede sig gennem *widgets* og applikationer benyttet på sociale netværkstjenester, der er blevet kritiseret for deres manglende sikkerhed. Således forventer vi, at tredjepartsapplikationer på sociale netværkstjenester i stigende grad bliver benyttet i angrebet på borgeren. Både applikationer der er designet til formålet, og kompromitterede sårbare legale tredjeparts applikationer, vil blive benyttet til at ramme brugerne af disse tjenester. Brugerens tillid til mediet og de beskeder, der modtages fra venner og lignende, spiller en væsentlig rolle i forsøget på at kompromittere brugerens sikkerhed, data og identitet.

Vi tror stadig, at netbankerne vil have *malware*-udviklernes fokus. I takt med at netbankerne implementerer sikkerhedsmæssige modforholdsregler, tror vi dog, at dette fokus kan flytte sig til større lokale webshops, der ikke i samme grad som bankerne har implementeret it-sikkerhed som del af deres forretningsmodel. Således forventer vi i fremtiden at se *trojanske heste* målrettet indsamling af kontooplysninger fra fx store online butikker, der sælger letomsættelig forbrugerelektronik og lignende.

Også de mobile platforme kan blive målet for *malware*. Med udbredelsen af smartphones, der bl.a. bruges til at gå på nettet, vil en oplagt forretningsmodel være *malware*, der sender overtakserede SMS'er, MMS'er og lignende. Vi tror, at vi på denne måde vil opleve en genopstandelse af 90'ernes dialerprogrammer, der var udviklet til at ringe op via modem til overtakserede telefonnumre.

Udbredelsen af tjenester til netopkoblet forbrugerelektronik kan på sigt udgøre en trussel mod borgeren og organisationerne. Mediecenteret, spillekonsollen, radioen, tv'et og tilsvarende forbrugerelektronik kobles i stigende grad på samme netværk som hjemmearbejdspladsen og mobiltelefonen. I modsætning til computeren har sikkerheden på disse i dag hverken brugerens eller producentens bevågenhed. Det åbner for en stigning i mængden af applikationer, der kan blive målet for *malware*, som giver adgang til borgerens og organisationernes applikationer og data. Vi tror, at udbredelsen af tjenester der benyttes af denne type apparater i hjemmet, vil skabe et nyt marked for *malware*-inficering, hvis konsekvenser kan være alt fra en stigning i tyverier af fortrolige organisationsdata til *identitetstyveri*er, afpresninger med truslen om offentliggørelse af private data eller indbrud, efter at tyverialarmen forinden er blevet afbrudt via internettet. Er det fx muligt at inficere tv'ets indbyggede medieafspiller via en sårbar annoncetjeneste, kan der være fri adgang til ikke blot data på medieafspilleren, men også til det lokale net og de enheder, der er koblet til dette. I sidste ende er det kun teknologien og fantasien, der sætter grænsen.

Ved at narre brugeren, kan angriberen overkomme de teknologiske barrierer for sine ugerninger. *Social engineering* var også i 2009 en væsentlig angrebsvektor. Vi forventer, at fremtiden vil byde på flere, mere målrettede og

udspekulerede måder at manipulere borgerne på for at få dem til at købe varer, de ikke har brug for, hente og installere *malware* og selv aflevere fortrolige oplysninger og lignende. *Scareware* og en stigende mængde virkningsløse sikkerhedsprogrammer er et eksempel på dette, der sandsynligvis også vil præge fremtiden. Forretningsmodellen er den enkle, at narre folk til fx at købe et bestemt antivirusprodukt. Ofte har en hjemmeside anbefalet produktet, efter foregående at have "detekteret" en eller flere farlige filer på brugerens pc. De benyttede hjemmesider kan både være lavet til formålet, eller være inficerede sårbare legale webapplikationer.

En begivenhed som sommerens verdensmesterskaber i fodbold tror vi vil blive benyttet til at udnytte borgernes interesse for begivenheden. I forhåbningen om billige fodboldbilletter og -rejser vil nogle have paraderne sænket og blive fristet af tilbud, som man ellers ville mene var for gode til at være sande. Fx vil vi se en række falske online butikker, der sælger alt fra fodboldrejser til -billetter, -trøjer og lignende. Flere af disse vil være placeret højt i søgemaskinernes søgeresultater som resultat af søgemaskineoptimering, og vil tillige blive annonceret via *spam*. Samtidig kan det forventes, at online medier, der beskæftiger sig med begivenheden, vil blive udsat for massive angreb, der har til formål at inficere de besøgende med *malware* målrettet det enkelte medies besøgende. Fx vil *malware* placeret på danske webapplikationer fortrinsvis være målrettet indsamling af data fra danskere.

De it-kriminelle vil i stadig større grad forsøge at holde deres aktiviteter og intentioner skjult. Det vil betyde kortere tid mellem geografisk afgrænsede distributioner af *malware*, der i stigende grad besidder evnen til at mutere. *Malware*-kode krypteres i flere lag og hostes i *botnet*, der benytter sig af *fast flux*-teknologi. Derudover vil brug af tjenester til linkforkortelse (fx www.tinyurl.com) blive benyttet til at skjule den endelige destination. Som Kaspersky Lab tror vi, at selskaber der leverer *bullet-proof hosting* af f.eks. et *botnet*s centrale servere, vil forsøge at blive deres egen ISP[89]. Har organisationen bag først fået adgang til deres egne IP-segmenter i fx Asien, Østeuropa, Caribien eller andre mindre regulerede områder af verden, kan det være vanskeligt at fratage dem adresserne igen. Tidligere har organisationen *Russian Business Network* fungeret som egen ISP, indtil det i maj 2008 lykkedes at trække deres IP-segmenter tilbage. *Russian Business Network* levede blandt andet af levering af *bullet-proof hosting* og var under mistanke for at stå bag botnettet Storm.

Ud over *spam*, *phishing* og *malware*-distribution, tror vi at enkelte *botnet* vil blive benyttet til *denial of service*-angreb, som det vi i august så udført mod Danske Spil. Tidligere har disse angreb været udført efter foregående afpresning, primært mod online kasinoer og spillevirksomheder på nettet. Vi forventer, at også andre typer af virksomheder som større webbutikker og bannerannoncedistributører, der lever af online aktivitet, kan komme i skudlinjen, da de i mindre grad har paraderne oppe og derfor udgør bløde mål.

Stadig flere værdifulde oplysninger opbevares i dag på digital form. Da organisationerne i stigende grad forbindes elektronisk til omverdenen, øges risikoen for ad denne vej at miste fortrolige data. Således tror vi, som PET i deres

89 Threatpost.com, 2009; "*Attackers Buying Own Data Centers for Botnets, Spam*".

seneste årsberetning for 2006-2007[90], at industrispionage er et forhold, som viden- og teknologitunge organisationer bliver tvunget til at forholde sig til. Særligt i lyset af den globale finansielle krise kan der være organisationer, der vil forsøge at skyde genvej til konkurrencemæssige fordele for simpelthen at sikre overlevelse. Vi har dog ingen forventning om, at vi i DK•CERT vil modtage anmeldelser, der specifikt vedrører mistanke om industrispionage, ligesom vi ikke tror at, sådanne historier vil ramme medierne.

5.2. Fremtidens udfordringer

Fra 2010 træder den omdiskuterede multimedieskat i kraft. Den kan medføre, at mange fravælger arbejdsgiverbetalte "goder" som mobiltelefon, bærbar computer, internetadgang mm., hvis ikke der på anden vis kompenseres fra arbejdsgiveren. Da både medarbejder og arbejdsgiver stadig har en interesse i de muligheder, netop disse enheder giver, frygter vi, at det i stedet vil være medarbejderens egen pc, der opkobles til arbejdspladsen og benyttes. Herved introduceres organisationerne for en række risici, som den kun har ringe mulighed for at tage højde for, da borgerens egen pc står uden for arbejdsgiverens øvrige sikkerhed.

Organisationerne, deres systemer og ansatte er i dag under angreb fra mange kanter, hvor kompromittering af sikkerheden ét sted kan have indflydelse på sikkerheden et helt andet sted. Tidligere tiders centrale perimeterbeskyttelse er ikke længere tilstrækkelig, da perimeteren i dag i ligeså høj grad består af forbundne individer i samspil med mange interagerende teknologier. Med stigende kompleksitet i de indbyrdes interaktioner, der kan have betydning for sikkerheden, er det vanskeligere fra centralt hold at overskue og risikovurdere organisationens *sårbarheder*. Den væsentligste udfordring kan derfor blive også at implementere it-sikkerhed som et kulturelt aspekt, således at organisationens ansatte til stadighed er bevidste om *sårbarheder*, trusler og risici, hvad enten de agerer som ansatte eller privatpersoner. I dette perspektiv tjener *god selskabsledelse* som middel til at synliggøre risikovurdering som et centralt anliggende for organisationen, som også de ansatte bør deltage i. Således handler *awareness* i højere grad om at opbygge en sikkerhedskultur end blot om information. For at opretholde tilgængelighed, integritet og fortrolighed mener vi, at man som organisation skal være i stand til at lede it-sikkerhed som en fortsat forandringsproces. Det synspunkt er også tidligere fremført af ENISA[91].

Stigende forbundenhed og mere komplekse mønstre for it-kriminalitet har skabt et behov for mere avancerede analyseværktøjer. Hvad der i logfilen kan ligne en legal trafikstrøm, kan i det store perspektiv være en del af en utilsigtet eller kriminel handling. Som Gartner[92] tror vi derfor, at en udfordring de kommende år bliver at forstå og implementere værktøjer, der i realtid kan analysere data fra mange kilder og genkende mønstre, der tidligere ville være overset. Kravet til indførelse af sådanne værktøjer er i lige høj grad et spørgsmål om at kunne afværge igangværende hændelser, efterforske tidligere og igangværende hændelser samt

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

91 ENISA, 2006; "*A users' guide: How to raise information security awareness*".

92 Gartner, 2009; "*Gartner identifies the top 10 strategic technologies for 2010*".

i forhold til revisionen at kunne påvise, hvilke hændelser organisationen er udsat for, og hvad der gøres for at afværge disse og fremtidige hændelser.

En relateret udfordring bliver implementering af procedurer, der sikrer mod tab af data, også når de er i bevægelse eller uden for virksomheden. Fx tror vi, at kryptering af data samt systemer til *Data Leak Prevention (DLP)* vil vinde stadig større indpas, også i de mindre organisationer. De største udfordringer bliver at definere de centrale politikker, der er grundlaget for overvågning og beskyttelse af data i *DLP*-installationen.

Når organisationerne for alvor begynder at adoptere skyen som en almindelig del af it-driften, skabes der samtidig et attraktivt mål for it-kriminalitet. Hvornår og hvordan det vil udmønte sig, er i dag for tidligt at spå om. Brugen af *cloud computing* byder dog på en række andre udfordringer, man som organisation bliver nødt til at være sig bevidst.

Da udbyderen af skyen ofte er store organisationer med behov for standardiserede ydelser, kan de tilbyde sikkerhed billigere, end de fleste organisationer selv kan. Det er ganske simpelt forholdsmæssigt mindre ressourcekrævende for en stor virksomhed at fokusere på sikkerhed. Men netop udbyderens organisatoriske størrelse, behov for standardisering af egne ressourcer og geografiske placering kan i forhold til danske organisationer også give udfordringer. Særligt i forhold til de kontraktlige forhold medfører brug af teknologien nogle aspekter, der adskiller sig fra traditionelle leverandøraftaler, som det kan være nødvendigt at forholde sig til. Ud over specificering af ydelsens pris, indeholder brugen af *cloud computing* ifølge Jesper Langemark fra advokatfirmaet Bender von Haller Dragsted en række kontraktlige faldgruber med hensyn til sikkerhed[93].

Når man som dansk organisation vælger at få hostet sine computere eller services hos en dansk hostingpartner, vil ydelsens indhold blive specificeret i en kontrakt på baggrund af forhandlinger. Ud over pris beskriver kontrakten, hvilke øvrige ydelser i form af fx driftsstabilitet, overvågning og sikkerhed, der følger med. Og den specificerer, hvem der i tilfælde af uregelmæssigheder har ansvar for at gøre hvad, hvornår og hvorfor. Omvendt vil det ofte forholde sig, når en organisation vælger at placere sine services i skyen. Oftest vil kunden være nødsaget til at forholde sig til en standardkontrakt, der i højere grad fraskriver udbyderen ansvar og fokuserer på fakturering af kunden.

Derudover kan behandlingen af data i forhold til gældende lovgivninger være et element, som det ifølge ENISA[94] kan være nødvendigt at tage højde for. Da data i skyen ofte er placeret i et andet land, kan det være et problem at sikre sig, at de bliver behandlet korrekt i forhold til gældende lovgivning, da det er ejerens og ikke *cloud*-udbyderens ansvar at overholde lovgivningen. Fx kræver EU's datalovgiving, at følsomme data ikke må forlade Europa. Yderligere kan der opstå problemer, hvis myndighederne i det land, hvor data hostes, kan kræve adgang til data uden at få lov af dataejerne, og endda måske uden deres vidende. For en dansk organisation kan det være i direkte konflikt med fx persondataloven, gældende standarder eller organisationens egen it-sikkerhedspolitik.

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

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

At *cloud computing* som teknologi ikke er moden, betyder indtil videre, at der hverken er *best practices* eller standarder. Som kunde risikerer man derfor at blive låst fast hos en bestemt udbyder, da data, ifølge ENISA[95], ikke nødvendigvis kan konverteres til andre udbydere eller en traditionel fysisk infrastruktur. Derudover kan der opstå problemer i forhold til overholdelse af standarder og certificeringer, som udbyderen ikke overholder, ikke kan give garanti for at overholde og/eller ikke giver mulighed for at kontrollere overholdelsen af. Således kan organisationens sikkerhedspolitik vise sig ikke at være kompatibel med brug af *cloud*-services.

Yderligere gælder for skyen en række forhold, der tillige gør sig gældende ved al anden outsourcing af it-ydelser. Man har fx ikke samme kontrol med data, der er placeret ude i byen, hvilket i forbindelse med fx sletning kan give problemer, hvis ikke det kontraktlig er specificeret. Hvis data reelt ikke slettes, men blot skjules for brugeren, kan det være i uoverensstemmelse med lovgivningen og/eller organisationens egen sikkerhedspolitik. Generelt gælder, at det bliver vanskeligere at risikovurdere egne systemer og data, hvis ikke leverandøren åbent kommunikerer sine egne risikoprofiler og -vurdering til kunden, hvilket ikke altid er praksis.

Problematikker omkring outsourcing af it-drift var i 2009 et emne med relevans for varetagelse af organisationernes it-sikkerhed. I en international undersøgelse foretaget af Deloitte svarede 49%, at de ikke eller kun i mindre grad havde tillid til outsourcing-leverandørernes it-sikkerhedspraksis, der for 19% vedkommende udelukkende var baseret på aftaler om fortrolighed[96]. 56% af de respondenter, der havde oplevet brud på it-sikkerheden, hvor kilden var ekstern, svarede, at hændelsen udsprang fra en leverandør.

Vi tror, at der i fremtiden vil komme større fokus på organisationernes digitale samarbejdsrelationer. I kølvandet på nye lovkrav til outsourcing i finanssektoren kan det formodes, at også det øvrige danske erhvervsliv vil have større fokus på outsourcing og de problematikker, der kan knytte sig til det. Når uheldet er ude, kan outsourcing give anledning til mangelfuld udredning af hændelsen og/eller tvister, hvis det ikke i kontrakter og SLA'er er klart defineret, hvem der har ansvar for hvad, hvordan og hvornår. Gør det på forhånd klart, hvilke interesser leverandøren har i fx en fuld udredning af en it-sikkerhedshændelse, datatab som følge af hardwarenedbrud og lignende. Generelt kan outsourcing af it-services give udfordringer i forhold til organisationens *compliance*-initiativer.

Vi tror, at udbredelsen af Windows 7 i det kommende år kommer til at byde på en række nye udfordringer både for den enkelte borger, der har købt en ny pc med styresystemet, og for organisationerne. Med større udbredelse af systemet bliver det et attraktivt mål for de it-kriminelle. De vil opdage nye *sårbarheder*, som de vil udnytte hurtigere og strategisk i forhold til Microsofts fastlagte opdateringsdage. Det kan medføre fremkomsten af nye *trojanere*, *orme* og vira, der udnytter huller i systemet. Derudover bliver det for organisationerne en udfordring at implementere Windows 7 i det eksisterende driftsmiljø og i den eksisterende sikkerhedsmodel.

Usikre webhoteller er ansvarlige for spredning af meget *malware*. Det kan være

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

96 Deloitte, 2009; "*2009 TMT global security survey*".

en udfordring at dæmme op for denne udvikling, da hostingselskaberne i forhold til borgeren og mindre organisationer hovedsageligt konkurrerer på prisen. Mens webbutikker er underlagt reguleringer i forhold til persondataloven og kortudbyderne, er dette marked ureguleret og for de fleste uigennemsigtigt. Det er vanskeligt at sammenligne, hvad man egentlig får for pengene, og kunden vil ofte indgå som en del af problemstillingen. Spørgsmålet er, om en ændring af lovgivningen kan være en del af løsningen på problemet.

Netop borgeren, der sjældent har hverken tilstrækkelig viden eller ressourcer, indgår som en væsentlig del af problemet kriminalitet. Spørgsmålet er, hvordan vi på samme tid beskytter borgeren og beskytter mod yderligere kompromittering fra borgeren uden at det krænker dennes privatliv. Når vi som privatpersoner benytter egne installationer i arbejdsmæssig henseende, eller benytter organisationens installationer i private anliggender, risikerer vi at krænke sikkerheden i den organisation, vi er ansat i. Et aspekt af dette er de sociale netværkstjenester, som i vid udstrækning også benyttes fra arbejdspladserne. Denne sammensmeltning af arbejde og privatliv vil blive en stigende udfordring for organisationerne, som de bliver nødt til at tage stilling til og efterfølgende inkludere i organisationens it-sikkerhedspolitik. Hvordan det konkret gøres, må afhænge af den enkelte organisations risikovurderinger og temperament.

Alt i alt byder fremtiden på en række udfordringer, som stiller nye krav til både borgerne, organisationerne og den måde, vi organiserer samfundet på. Selvfølgelig er førsteprioriteten i dette perspektiv, at vi beskytter mod den aktuelle it-kriminalitet, men hvordan vi gør det og hvem der har ansvaret, står endnu til debat. Vi mener, at vi bedst løser denne opgave i fællesskab. De danske organisationer og i særdeleshed it- og telebranchen bør tage ansvar for borgerens sikkerhed på nettet. Det kræver selvfølgelig en lovgivning, der faciliterer, at man kan overvåge og hurtigt afværge igangværende angreb uden at gå på køb med opretholdelse af privatlivets fred.

6. Opsamling

Vi har i de foregående afsnit beskrevet flere begivenheder og tendenser, der i 2009 gjorde sig gældende for den it-kriminalitet som vi kunne observere. I dette afsnit samler vi op og beskriver de trends, vi mener, var de væsentligste i det forgangne år, og som vi tror vil komme til at præge fremtiden.

It-kriminalitet er en god forretning for organiserede kriminelle grupperinger, som særligt fra lande i Afrika, Asien og den tidligere sovjetblok kan operere stort set uden lovgivningens bevågenhed. Mens man i den vestlige verden løbende har tilpasset lovgivningen til udbredelsen og brugen af elektroniske medier, er tilsvarende aktiviteter i disse områder af verden vanskeliggjort af en eksplosiv vækst i internetopkoblinger, der ikke modsvares af en tilsvarende nationaløkonomisk fremgang. Når man samtidig kæmper med kulturelle og sociale problemer samt opbygning af infrastrukturer og sundhedsvæsen, giver det et miljø, hvor organiserede kriminelle bander kan operere uden for lovens rækkevidde.

De kriminelle grupperinger er de seneste år blevet mere professionelle i både deres mål og midler, hvilket blandt andet afspejles ved angrebet mod de danske netbanker i 2009. Vi tror desværre, at denne udvikling fortsætter, således at vi som borgere og organisationer udsættes for mere målrettede og sofistikerede angreb tilpasset fx geografi og aktuelle begivenheder. I samspil med udvidet brug af metoder til at skjule lyssky aktiviteter betyder det, at vi i sikkerhedsbranchen vil få stadig sværere ved at opdage, analysere og afværge aktuelle angreb.

Sårbare legale webservere er i dag en central del af forsyningskæden for spredning af *malware*. I forhold til tidligere er det i stigende grad *sårbarheder* i tredjepartsprogrammer på de besøgendes klient, der forsøges udnyttet, hvor det tidligere var sårbarheder i browseren. Denne tendens tror vi kommer til at forsætte. Vi tror også, at tendensen med større variation i *malware* vil fortsætte, således at den er målrettet distributionsmetode, platforme og geografi. Således spår vi sager om fx målrettet misbrug af danske profiler på sociale netværkstjenester ved udnyttelse af *sårbarheder* på mobile platforme.

Botnet-programmer var blandt de typer *malware*, der bl.a. blev spredt via *drive-by download* fra legale webapplikationer. Efter lukningen af hostingvirksomheden McColo i 2008 er mængden af computere, der indgår i *botnet*, igen steget ligesom mængden af *spam* der udsendes via dem. De *botnet*, der har rejst sig fra asken af McColo, har i dag lært af lektien og benytter metoder til at undgå tilsvarende interventioner. Derudover har vi oplevet en opdeling i få meget store *spam-botnet*, og mange små, mere målrettede og specialiserede *botnet*, der bl.a. benyttes til hosting af *phishing*-sider, *trojanske heste* og lignende.

Tilsvarende har vi en forventning om, at 2010 vil byde på målrettede angreb mod Windows 7. I takt med udbredelsen vil der dukke *sårbarheder* op, som vil blive forsøgt udnyttet. Som tendensen har været, vil nogle af disse *sårbarheder* på angrebstidspunktet endnu ikke være offentliggjort og/eller der vil ikke være kommet rettelser til dem.

Cloud computing fik i 2009 sit store gennembrud, og selvom teknologien kan give en række drifts- og sikkerhedsmæssige fordele, byder også på en række udfordringer for danske organisationer. Særligt i forhold til lovgivningsmæssige og kontraktlige anliggender byder teknologien på en række udfordringer, som kan adskille sig fra anden outsourcing af it-services. Derudover kan fremtiden byde på målrettede angreb på tjenester placeret i skyen og de datacentre, der driver skyen, i takt med udbredelse af teknologien.

Det er alt i alt ikke vores forventning, at der i fremtiden anmeldes flere hændelser om it-sikkerhed til DK•CERT, snarere tværtimod. Derimod tror vi, at de hændelser, hvor DK•CERT bidrager med analyse, efterforskning og rådgivning, vil stige i antal, kompleksitet og tidsforbrug. Omvendt venter vi, at både politiet og den finansielle sektor vil opleve en stigning i henvendelser, der primært handler om misbrug af kreditkortinformationer og andre former for *identitetstyveri* samt henvendelser vedrørende krænkelse af privatlivets fred.

Der er i rapporten identificeret en række tendenser for både 2009 og fremtiden. Vi har nedenfor samlet dem, vi finder væsentligst. Det vil selvfølgelig være muligt at finde tilsvarende lister, som afviger fra vores. Dette skal primært tages som udtryk for forskelle i synsvinklen, der lægges ved udfærdigelsen af den enkelte liste. Det er vores håb, at du kan bruge vores lister som inspiration, således at vi i fællesskab kan være med til at sikre de danske it-aktiver.

6.1. Trends og tendenser i 2009

2009 var præget af en stadig større variation og opfindsomhed i typen af angreb, der samtidig blev mere målrettet og professionelt udført. Således oplevede vi *trojanske heste* målrettet danske banker, samt *spam-*, *phishing-* og *muldyr*skampagner udført på fejlfrit dansk og timet efter de omkringliggende begivenheder.

Også i 2009 så flere nye angrebsmetoder dagens lys. Generelt udviste de organiserede it-kriminelle en stadig større opfindsomhed. Således oplevede vi flere målrettede angreb på danske organisationer og borgere. Angreb, hvor man havde gjort sit forarbejde, og fx sproglige barrierer ikke var nogen hindring. Indsamling af data og information var med misbrug eller videresalg for øje målet for it-kriminaliteten, og det var ikke længere kun kreditkortinformationer, der havde interesse. Også virksomhedsdata og private oplysninger samt kontoinformationer til sociale netværkstjenester, webmail og lignende havde værdi for de kriminelle grupperinger.

Webapplikationer var også i 2009 den væsentligste kilde til spredning af *malware*. Således så vi en stigning i udnyttelsen af *cross-site scripting-* og *SQL injection-sårbarheder* på legale webservere, der generelt bør have større fokus. Som følge af en eksplosiv vækst i brug og udbredelse af sociale netværkstjenester og Apples iPhone blev disse i 2009 et yndet mål for spredning af *malware* og indsamling af informationer. Systemkompromittering og -misbrug var således ikke længere forbeholdt Windows-brugere, men ramte på tværs af systemer og platforme.

Nedenstående uprioriterede liste var i vores øjne de væsentligste tendenser for 2009, når det drejer sig om it-kriminalitet:

1. Danmark var et attraktivt marked for it-kriminalitet, og angrebene blev i stigende grad målrettet de danske borgere og organisationer.
2. Sårbare legale websider, som brugerne ellers har tillid til, var den væsentligste kilde til distribution af *malware*.
3. Antallet af ny *malware* eksploderede. Flere varianter besad evnen at opdatere sig selv.
4. Stigende udnyttelse af *sårbarheder* i tredjepartsbrowserkomponenter som fx Flash, Adobe Reader og QuickTime.
5. Flere *sårbarheder* blev udnyttet, inden de blev offentliggjort, eller inden der kom rettelser.
6. Sammensmeltning eller overlap af begreber som *orme*, *trojanske heste*, *botnet*-programmer med mere, der i mange tilfælde besidder samme egenskaber.
7. Opdeling i få, meget store *botnet* og mange små, men til gengæld meget specialiserede og målrettede *botnet*.
8. *Phishing*-sider blev i stigende grad hostet i *botnet* med *fast-flux* egenskaber, hvor levetiden er længere.
9. *Malware* målrettet sociale netværkstjenester og applikationer på disse.
10. Udbredelsen af Apples iPhone medførte målrettede angreb på de brugere, som havde fjernet de medfødte begrænsninger i telefonen.

6.2. Fremtidige trends

Mens 2009 har været præget af den internationale finanskrise, er Gartners forventning til 2010, at udgifterne til it igen vil stige, dog ikke til samme niveau som i 2008[97]. Inden den finansielle krise var udgifterne til it-sikkerhed i danske såvel som udenlandske organisationer stigende i takt med de generelle udgifter til it. Spørgsmålet er, om denne sammenhæng nødvendigvis er en naturlov. Særligt set i forhold til, at man i en amerikansk undersøgelse gennem de seneste tre år har haft faldende økonomiske tab på grund af brud på it-sikkerheden[98].

Vi tror, at finanskrisen giver anledning til, at organisationerne i deres iver efter at reducere omkostningerne i højere grad vil kigge indad på egne erkendte erfaringer og behov i stedet for at lade sig påvirke af medier, producenter, forhandlere og konsulenter. Spørgsmålet er jo, hvorvidt disse eksterne parter uden skelen til egen forretning formår at tegner et korrekt billede af organisationernes aktuelle behov. En sådan "sund skepsis" kan medføre, at man i netværk og branchefællesskaber opstiller *best practices* for organisationernes implementering af it-sikkerhed, som i sidste ende resulterer, i at danske organisationer får mere sikkerhed for færre penge.

Sommerens verdensmesterskaber i fodbold, som løber af stablen i Sydafrika, bliver en begivenhed, der vil vække begejstring hos andre end fodboldentusiaster.

97 Gartner, 2009; "*Gartner saysit spending to rebound in 2010 with 3.3 percent growth after worst year ever in 2009*".

98 Computer Security Institute, 2009; "*2009 CSI computer crime & security survey*".

Vi forudser, at de it-kriminelle vil benytte begivenheden til at inficere webapplikationer, der sælger rejser og billetter til kampene, publicerer resultater, nyheder og lignende. Tilsvarende tror vi, at vi kommer til at opleve *spam*-kampagner med falske fodboldbilletter og -rejser samt *phishing*-kampagner der fortæller modtageren, at denne har vundet en rejse til fodbold-VM.

Med stadig flere trusler, der angriber os fra stadig flere kanter, bliver det traditionelle antivirus software i fremtiden utilstrækkeligt, og vi må kigge andre steder hen for at beskytte de danske borgere og organisationer. Særligt de mobile platforme, men også stigende brug af sociale netværkstjenester åbner for nye trusler, der kan ramme både borgeren og organisationerne.

Udbredelsen af tjenester til netopkoblet forbrugerelektronik kan betyder at der eksponeres nye *sårbarheder*, der kan udnyttes i fx mediacenteret, spillekonsollen, radioen, tv'et og lignende. Vi forventer angreb, der har til formål at kompromittere forbrugerelektronik i hjemmet, som i modsætning til computeren hverken har brugerens eller producentens bevågenhed med hensyn til sikkerhed. Herved åbnes adgangen til det lokale net og potentielt brugerens øvrige tjenester og data.
Mens det kan synes relativt enkelt at fremhæve de væsentligste tendenser i det forgangne år, er det straks vanskeligere at spå om fremtiden. I nedenstående uprioriterede liste forsøger vi alligevel at give vores bud på, hvad der fra et it-sikkerheds perspektiv, vil præge fremtiden:

1. Den menneskelige faktor bliver det svageste led. *Social engineering* bliver en primær angrebsvektor til at modgå tekniske modforholdsregler.
2. I forbindelse med sommerens fodbold-VM i Sydafrika vil vi i 2010 opleve målrettede angreb, der relaterer sig til begivenheden.
3. Stigende udnyttelse af *sårbarheder* i tredjepartsapplikationer på sociale netværkstjenester, på samme vis som vi nu oplever udnyttelse af *sårbarheder* i browserplugins og tredjepartsprogrammer.
4. Stigende forurening af resultater fra søgemaskiner. Søgemaskineoptimering leder brugerne til websider med skadeligt indhold.
5. Tjenester til forkortelser af URL'er (fx www.tinyurl.com) benyttes ved spredning af *spam* og *malware* til at skjule destinationen på links.
6. *Malware* til tidligere "perifere" netopkoblede platforme som fx Mac OS, Linux, iPhone, Android, Playstation med flere.
7. Dialere til smartphones, der sender overtakserede SMS'er og MMS'er.
8. Målrettede angreb på Windows 7.
9. Målrettede angreb til opsamling af kreditkortinformationer mm. fra fx spilkonsoller og lignende netopkoblet forbrugerelektronik.
10. Målrettede angreb på skyen, datacentret som hoster skyen og/eller tjenester placeret i skyen.

7. Anbefalinger

Med baggrund i rapportens øvrige indhold giver vi nedenfor en række anbefalinger til, hvorledes vi som borgere, it-ansvarlige og beslutningstagere kan skabe forøget it-sikkerhed. Selv om meget er hørt før, er det vores håb, at disse anbefalinger vil danne grobund for den refleksion og omtanke, som kan være med til, at vi som borgere i Danmark kan føle os trygge i vores digitale færden, hvad enten det er i hjemmet eller på arbejdspladsen. Vi mener, at både lovgiverne, organisationerne og den enkelte borger skal tage medansvar for denne proces, og håber derfor, at vi kan være med til at skabe de nødvendige diskussioner.

Som en følge af, at it-kriminaliteten synes at udvikle sig med evolution snarere end revolution, er de tekniske og organisatoriske løsninger, der er nødvendige for at opretholde it-sikkerheden, grundlæggende de samme som sidste år. Når der i nedenstående anbefalinger alligevel er afvigelser i forhold til sidste år, skyldes det bl.a., at vi i dette års rapport har valgt at sætte fokus på de sociale netværkstjenester. Vi tror nemlig, at de sociale netværkstjenester i fremtiden vil give anledning til flere hændelser vedrørende brud på ophavsretten og privatlivets fred, samt være en væsentlig kilde til *identitetstyverier* og spredning af *malware*.

7.1. Anbefalinger til borgerne

Når det gælder beskyttelse af den enkelte borger, hvad enten det er som privatperson eller medarbejder i en organisation, er der grundlæggende enighed om de forholdsregler, man bør tage. Vi har derfor i år valgt at videregive de samme "10 gode råd"[99], som bl.a. blev benyttet i kampagnen Netsikker nu, der løb af stablen i uge 40. På it-borger.dk kan du finde uddybninger af de enkelte råd. Vi har efterfølgende valgt at supplere rådene med vores egne anbefalinger til, hvordan du som borger opnår mest mulig sikkerhed.

Opdater din pc:
1. Hold programmerne på din pc opdateret og brug automatisk opdatering.
2. Hold dit antivirusprogram ved lige og brug firewall.
3. Husk at sikre dit trådløse netværk.
4. Pas på med at klikke på links i mails fra ukendte afsendere.
5. Installér kun programmer, du har behov for.

Beskyt privatlivets fred på nettet:
6. Læg kun oplysninger om dig selv på internettet, som alle og enhver må bruge.
7. Spørg, inden du lægger billeder og oplysninger ud om andre. Det gælder også børn.
8. Vær kritisk, når du modtager forespørgsler og invitationer på nettet.
9. Læs aftalevilkår for tjenester, så du ved, hvad du går ind til.
10. Beskyt dine private oplysninger på tjenester via privatlivsindstillinger/privacy settings.

Ovenstående anbefalinger om beskyttelse af privatlivets fred kan suppleres med

99 It-borger.dk, 2009; "*10 gode råd*".

Datatilsynets generelle anbefalinger til brug af sociale netværkstjenester[100] og DK•CERT og KOMFOs vejledning til sikker brug af Facebook[101].

Mange af os modtager dagligt mails fra folk, vi ikke kender eller ikke forventer at få den type mails fra. Fra tid til anden modtager vi også mails, der indeholder "gode tilbud", mails fra vores bank eller lignende, der beder os indtaste personlige oplysninger, eller blot "sjove" mails der vækker vores interesse eller nysgerrighed. Fælles for disse er, at de udgør en potentiel risiko.

Brug mail med omtanke:

11. Brug et *spam*filter.
12. Lad være med at udlevere private (konto)oplysninger på baggrund af en mail.
13. Undlad at klikke på links eller åbne vedlagte filer, hvis du er i tvivl om mailens lødighed.
14. Check om URL-adressen på et link stemmer med, hvad du forventer, inden du klikker (hold musen over linket uden at klikke, og kig på adressen nederst i browserens statuslinje).
15. Slet mailen, hvis du er i tvivl.

Sårbarheder i browseren og de programmer og plugins, der er knyttet til den, udgør en stigende risiko. Typisk opdateres tredjepartsprogrammer som medieafspilleren, Flash-playeren eller PDF-læseren ikke ved automatisk opdatering af pc'en. Da det ofte er *sårbarheder* i disse, der udnyttes, udgør de selvfølgelig også en risiko.

Sikker surf på nettet:

16. Opdater også tredjepartsprogrammer. Brug evt. programmet PSI fra Secunia[102].
17. Brug browserens indbyggede *phishing*-filter, antispywarefiltre mm, eller installer selv.
18. Overvej om du vil tillade afvikling af scripts i browseren som standard.

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 standardbrugernavn og -password, eller brugernavne og passwords, der er nemme at gætte.

Brug sikre passwords:

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

Sociale netværkssteder opleves i stigende grad som middel til spredning af *malware*. Ud over risikoen for at få misbrugt din egen konto kan du også modtage beskeder fra dine venner med links til inficerede applikationer eller hjemmesider.

---

100 Datatilsynet, 2008; "*Anbefalinger til beskyttelse af privatlivets fred i sociale netværkstjenester*".

101 DK•CERT & KOMFO, 2009; "*Styr dit privatliv på Facebook*".

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

Ud over Datatilsynets anbefalinger vedrørende beskyttelse af privatlivets fred[103] bør du derfor være opmærksom på nedenstående.

Sikker brug af sociale netværkstjenester:
22. Brug tredjepartsapplikationer med omtanke. De kan have andre "funktioner" end dem, du umiddelbart ser.
23. Vær opmærksom på, hvilke informationer fra din profil du giver applikationen adgang til.
24. Vær opmærksom på, hvem der kan have interesse i det indhold, du lægger på din profil. Fx kan en historie om, at du nu tager på ferie, sammen med billeder fra dit hjem være attraktivt for indbrudstyve.

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

7.2. Anbefalinger til it-ansvarlige

I organisationerne varetages den praktiske del af it-sikkerheden af de it-ansvarlige, der således har medansvar for, at organisationens systemer er i en sådan forfatning, at tilgængelighed, integritet og fortrolighed kan opretholdes. Retningslinjerne for denne proces bør være beskrevet i organisationens it-sikkerhedspolitik, der benyttes ved udfærdigelse og implementering af konkrete procedurer.

Det er den it-ansvarliges ansvar at holde de ansattes computere i en sådan forfatning, at de kan varetage deres job. Det betyder, at der bør implementeres procedurer, der sikre, at alle arbejdsstationer skal holdes opdaterede og sikre.

De ansattes pc'er:
1. Hold programmerne på brugernes pc'er opdateret og sørg for, at der benyttes automatisk opdatering.
2. Sørg for, at brugerne benytter opdateret antivirusprogram og bruger firewall.
3. Giv kun brugerne mulighed for at definere stærke passwords lokalt såvel som på organisationens forretningssystemer.
4. Hold løbende organisationens ansatte opdateret med it-sikkerhedsproblematikker, der er relevante for netop dem.

Det er selvfølgelig ikke kun brugernes lokale arbejdsstationer, der skal holdes sikre. Også organisationens forretningssystemer bør holdes sikre og opdaterede.

Organisationens forretningssystemer:
5. Luk for alle services, der ikke er nødvendige på det enkelte system.
6. Minimer adgangen til det nødvendige ved at begrænse adgang fra netsegmenter, services og brugerkonti, der ikke skal benytte den pågældende service.
7. Hold organisationens forretningssystemer opdaterede. Abonner eksempelvis på en sårbarhedsvarslingtjeneste, og/eller brug automatisk softwareinspektion.

103 Datatilsynet, 2008; "*Anbefalinger til beskyttelse af privatlivets fred i sociale netværkstjenester*".

8. Benyt *sårbarhedsscanninger* til periodisk kontrol.

Forventningen til organisationens evne til at gøre troværdige informationer tilgængelige samt tilliden til integritet og troværdighed af data er et væsentligt element af det at passe forretningen. Hvis ikke den basale tillid til organisationen er til stede, vil investorer, kunder og samarbejdspartnere vælge alternativer. Organisationernes primære digitale kommunikationskanal, webapplikationerne, er i stigende grad under pres. Vores anbefaling er derfor, at der sættes særligt fokus på disse.

Organisationens webapplikationer:

9. Sørg for, at brugersendte data valideres inden eksekvering og/eller lagring på organisationens webapplikationer.
10. Benyt periodiske webapplikationsscanninger som kontrol, og sørg for at rette evt. *sårbarheder*.

Fortrolighed vedrører ikke kun ens egne forretningskritiske data. Hvis kunder, leverandører og øvrige samarbejdspartnere skal bevare tilliden til organisationen, er det kritisk, at fortrolige data bliver ved at være fortrolige. Tænk derfor dataadgang og kryptering ind i alle scenarier for brug af it.

Fortrolighed af data:

11. Overvej, hvem der skal have adgang til hvilke data hvorfra og hvordan, og begræns adgangen til det nødvendige.
12. Brug evt. *DLP*-systemer (*Data Leak Prevention*) for sikre, at regler og procedurer overholdes.
13. Krypter forretningskritiske data både på serveren, i transaktionen og ved anden transport på fx bærbare computere, smartphones og andre mobile enheder.
14. Tænk sikkerhed i skyen. Krypter forretningskritiske data i skyen og brug en implementering, hvor dekrypteringsnøgler ikke bliver liggende på maskiner i skyen.

Leverandørerne udgør en væsentlig del af organisationens sikkerhed, hvad enten der er tale om hard- og softwareleverancer, hosting eller outsourcing. Leverandørrelationer handler derfor ikke kun om drift, men i ligeså høj grad om specificering af, hvem der har ansvar for hvad, hvornår og hvorfor. Man bør undersøge markedet og stille krav til sine leverandører, således at organisationsspecifikke krav til drift og sikkerhed bliver indført i kontrakten.

Samarbejdsrelationer og leverandører:

15. Benyt aktivt organisationens risikovurderinger ved udfærdigelse af kravspecifikationer og lignende.
16. Undersøg markedet og spørg ind til, hvilke ydelser der kan inkluderes og hvilke som ikke kan.
17. Gør det klart, om leverandøren kan sikre opretholdelse af jeres krav
18. Tænk worst-case scenarier ind i kontrakten, og specificer ansvar herefter.
19. Sørg for at få den nødvendige information og uddannelse.

Generelt gælder det, at du bør stille krav til udfærdigelse af organisationens it-sikkerhedspolitik og bruge den. Er den konsistent og fyldestgørende, vil de

fleste retningslinjer kunne findes her. Når it-sikkerhedspolitikken efterfølgende benyttes aktivt, forankres den i organisationen, og det bliver lettere internt at sikre ressourcemæssig opbakning til tiltag, der sikrer overholdelse af den.

7.3. Anbefalinger til beslutningstagere

Mens en række brancher herhjemme er reguleret af enten lovgivningen og/eller branchen selv, har det ligget i internettets natur, at det er ureguleret. Fokus på debatten om internettet som middel til udbredelse af informationssamfundet har primært været præget af organisationernes muligheder på den ene side og beskyttelsen af privatlivets fred på den anden. I modsætning til fx den finansielle sektor og telebranchen har ISP'erne kun i meget lille grad haft incitament og mulighed for 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.

Man kan diskutere, hvorvidt en ISP, teleudbyder eller hostingvirksomhed, der informeres om kompromittering af en kundes installationer og herefter undlader at handle, i juridisk forstand er medvidende om evt. yderligere kriminalitet. I dag er det desværre sådan, at der intet incitament er til at oplyse eller rådgive kunden om kompromittering af dennes systemer. Tværtimod vil en sådan rådgivning ofte være forbundet med ekstra udgifter, hvorfor vi ofte oplever at henvende os forgæves.

En stor del af de websider, der spreder *malware*, er sårbare legale websider placeret på webhoteller. På samme vis som vi mener, man bør tage et aktivt ansvar for at informere og rådgive om kompromittering af kundens systemer, mener vi også, at hostingvirksomheder bør tage ansvar for at begrænse spredningen af *malware* fra danske websites. På andre områder i samfundet sikres kunden gennem garantimærkninger implementeret i branchefællesskaber som fx rejsegarantiordningen eller e-handelsmærket.

Spredning af malware:

1. Opret en lovgivningsmæssig ramme, der muliggør og forpligter ISP'erne til at samarbejde om detektering, varsling, afværgelse og rapportering af it-kriminalitet internt såvel som til relevante myndigheder.
2. Opret et fælles garantimærke eller tilsvarende ordninger for hostingvirksomheder, der bl.a. garanterer kunden et minimum af sikkerhed på de underliggende platforme, samt basale rettigheder i forbindelse med betaling, opkøb, konkurs mm.
3. Tilbyd lovgivningsmæssige incitamenter til, at ISP'er, teleudbydere og hostingvirksomheder informerer og rådgiver deres kunder om kompromittering af deres systemer, således at yderligere uhensigtsmæssig og/eller kriminel aktivitet undgås.

I dag er den eneste beskyttelse mod uønskede mails de filtre, som er i mailklienten, i de gratis webmail, eller som borgerne og organisationerne selv sætter op. Med kortere, mere intensive og målrettede kampagner er de hverken nu eller i fremtiden tilstrækkelige.

Spredning af spam- og phishing-mails:

4. Vi mener, at der for alle danske domæner bør indføres tvungen brug af *SPF* (*Sender Policy Framework*). Der vil mindske både mængden og troværdigheden af *spam*- og *phishing*-mails.

Systemkompromittering har i dag primært datatyveri som formål. I Danmark kan ens personlige data blive stjålet fra fx en usikker netbutik, uden at den har pligt til at informere en herom. Vi mener, kunden har ret til at få besked, således at denne i tide kan tage sine forholdsregler.

Informationspligt ved datatyveri:

5. Dansk lovgivning bør, som i fx USA, omfatte pligt til at informere organisationernes kunder ved kompromittering af egne systemer eller data, der vedrøre kunden.

De seneste år har særligt i udlandet vist flere eksempler på fortrolige data, der glemmes, tabes eller stjæles under transport uden for organisationen. I tillæg hertil kommer eksempler, hvor organisationen ved en fejl selv har offentliggjort fortrolige kunde- og/eller virksomhedsspecifikke data på grund af menneskelige og/eller tekniske fejl.

Tab af fortrolige data:

6. Lad it-sikkerhed indgå i strukturer af *god selskabsledelse*.
7. Etabler en kultur, hvor synliggørelse af organisationens risikostyringsaktiviteter er en naturlig del af det at drive forretning.
8. Lad medarbejderne tage aktivt medansvar for risikostyring.

Mens finanssektoren har fået strammet lovgivningen vedrørende outsourcing af it-driften, er det vores erfaring, at mange samarbejdsaftaler i det øvrige erhvervsliv etableres ud fra standardkontrakter, der specificerer rammerne for normalsituationen. I tilfælde af kompromittering af outsourcede systemer kan det give anledning til usikkerheder om ansvar og pligter, da det ikke er beskrevet. Det vil ofte forværre hændelsen og forholdet til aftalepartneren.

Kunde- og leverandørrelationer:

9. Indfør klare politikker vedrørende outsorcing af forretningskritiske systemer.
10. Brug organisationens risikostyring og tænk worst case scenarier ind i kontrakten.
11. Tænk *compliance* ved outsourcing. Outsorcingspartnerens risikovurdering og -styring har også betydning.
12. Vær sikker på, at juraen er klar og på din side, når det går galt.

Brugen af *cloud computing* er gennem 2009 blevet en attraktiv mulighed for mange organisationer. Ud over forretningsmæssige aspekter som fleksibilitet og skalerbarhed introducerer *cloud computing* fra et it-sikkerhedsmæssigt synspunkt både en række fordele og mulige trusler, der kan adskille sig fradem, man ser ved anden outsourcing. En væsentlig del af problemstillingerne omkring *cloud computing* vedrører kontraktlige forhold, som fra et overordnet synspunkt ikke adskiller sig fra anden outsourcing, men også forskelle i lovgivning og myndighedernes rettigheder kan have betydning, da skyen ofte er placeret i et andet land.

Cloud computing med omtanke:

13. Tænk geografisk placering og lovgivning ind i dine overvejelser om at placere services i skyen. Vær opmærksom på, at det ikke er alt, der fra et lovgivningsperspektiv kan placeres i skyen.

Arbejdsmarkedet oplever i disse år en stigende sammensmeltning af arbejdsliv og privatliv. Ikke blot er flere af organisationens it-aktiver flytbare og/eller placeret uden for organisationens fysiske rammer, vi medbringer også organisationens data og informationer. Det forventes, at vi hjemmefra kan besvare mails og lige kigge på den seneste markedsføringsplan inden vi møder i morgen. Derudover benytter vi også arbejdspladsens installationer til at læse sportsresultater, handle på nettet, opdatere vores Facebookprofil og meget andet. Det introducerer en række risici for organisationerne, som det er meget vanskeligt at forudsige og tage hånd om.

Sammensmeltning af privat- og arbejdsliv:

14. Tag aktivt stilling til brugen af fx sociale netværkstjenester på arbejdspladsens installationer og hvilke arbejdsrelaterede informationer medarbejderne må dele.
15. Indfør og synliggør politikker, der specificerer regler for brug af organisationens installationer. Sørg for, at der indføres procedurer der implementerer reglerne.
16. Tag aktivt stilling til brug af private it-ressourcer uden for organisationens it-sikkerhedspolitik i arbejdsrelaterede sammenhænge.
17. Indfør og synliggør politikker, der specificerer regler for brug af medarbejdernes egne it-ressourcer. Sørg for at der indføres procedurer, der implementerer reglerne.
18. Accepter, at medarbejderen ikke kan eller må benytte sine egne it-ressourcer, eller tilbyd alternativer.

Det er ofte ikke nok at beskytte sig, det er også nødvendigt at vide, hvem der skal gøre hvad, når det alligevel går galt. I kommunikationsmæssige sammenhænge har mange organisationer i dag et kriseberedskab på ledelsesniveau, mens det i it-sammenhænge ofte halter med det tekniske beredskab længere nede i geledderne. En klar beredskabsplan er dog en væsentlig del af organisationens risikostyring, der i sidste ende kan spare organisationen for mange penge. Fx vil en e-handelsapplikation, der er unødvendigt nede, give anledning til mistet salg og troværdighed hos kunderne, mens nedbrud i andre brancher yderligere kan medføre reduceret produktion og/eller erstatningskrav fra kunder og samarbejdspartnere.

Vær beredt:

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

På mange områder adskiller it-sikkerhed sig ikke fra andre af de områder, vi som samfund og organisationer tager forholdsregler mod. Ofte handler det om, at når vi besidder den fornødne viden og påtager os ansvar, kan vi i fællesskab afværge de fleste trusler. I modsat fald kan forglemmelser og uansvarlighed få katastrofale følger. En usikker dominobrik kan få de øvrige til at vælte.

8. Ordliste

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

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

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

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, *botnet*-aktivitet 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.

Cloud computing: Services distribueret i en sky af primært virtuelle ressourcer. Skyen giver mulighed at man får adgang til ressourcer efter behov. Skalerbarhed og pris vil ofte være de væsentligste argumenter for at lade sine services outsource til skyen. Overordnet skelnes mellem 3 forskellige typer af cloud-services: *Software as a Service (SaaS)*, *Platform as a Service (PaaS)* og *Infrastructure as a Service (IaaS)*.

Compliance: Overensstemmelse eller efterlevelse af gældende regler. I it-sikkerheds sammenhæng beskriver *compliance* organisationernes evne til, at efterleve krav til informationssikkerhed efter gældende lovkrav eller godkendte standarder. Fx *DS 484*.

Conficker: Orm der dukkede op i oktober 2008. Den første version udnyttede ukendt sikkerhedshul i Windows. Lige før nytår kom anden udgave af *Conficker*, der desuden spredte sig kopiering til USB-nøgler og andre flytbare medier og udnyttede Windows AutoRun-funktion. *Conficker* udviklede sig med yderligere tre varianter i 2009. Der er ikke set nye varianter af *Conficker* siden april 2009.

Cookie: En cookie er en slags datapakke, der blandt andet indsamler oplysninger om forbrugerens gøren og laden på nettet. Cookies findes overalt på nettet og er med til at gøre det lettere at navigere på forskellige hjemmesider. Det er fx en cookie, der sørger for, at ens mailadresse allerede står i adressefeltet, så man kun behøver at skrive sit password, når man skal tjekke mails.

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

Cross-site scripting (XSS): En metode, hvor adressen på et sårbart website udnyttes til at vise yderlig information eller afvikle programmer. Der er forskellige former for *cross-site scripting*, som gør det muligt at udføre komplekse angreb. Metoden kan fx anvendes til *phishing*, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website som en bruger har tillid til, til at få adgang til fortrolig information.

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

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

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

Denial of service: 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*.

Drive-by-download: *Malware*-infection ved besøg på en inficeret hjemmeside. Den inficerede hjemmeside vil ofte være en sårbar legal side, som brugeren har tillid til, og infectionen forgår uden dennes viden.

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 fx til *phishing*-sider for at forhindre at de bliver sporet og lukket ned. Teknologien så dagens lys i 2007, blandt andet i forbindelse med Storm-ormen.

God selskabsledelse: Corporate governance, på dansk *god selskabsledelse*, opstod som følge af en række erhvervsskandaler i England og USA og bredte sig op gennem 1990'erne til resten af Europa . *God selskabsledelse* skal sikre en

hensigtsmæssig rolle- og ansvarsfordeling i forbindelse med kontrol og styring af organisationen. Et væsentligt element af *god selskabsledelse* omhandler risikostyring og revision. It governance er en integreret del af *corporate governance*, der har til formål at sikre strategisk udnyttelse af brugen af it, således at it både understøtter organisationens effektivitet og medvirker til at udvikle organisationen.

Identitetstyveri: *Identitetstyveri* betegner brugen af personlige informationer til misbrug af en andens identitet, fx kreditkortinformationer. Personlige informationer indsamles og misbruges ved phishing, hacking eller infektion med *trojanske heste*.

Koobface: Orm opdaget i december 2008, der angriber via sociale netværkstjenester som Facebook, MySpace, Hi5, Bebo, Friendster og Twitter. Ormens navn er dannet af bogstaverne i Facebook. *Koobface* sender beskeder til venner på sociale netværksider, fra en inficerede pc, med et link til en skadelig fil. Marts 2009 kom der en ny version og i Juli 2009 udsendte Twitter en advarsel om, at flere af tjenestens brugere var ramt af *Koobface*.

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

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

Man in the Middle: En angrebsform, hvor kommunikationen mellem to parter uden parternes viden, relæs gennem en "mand i midten", der aktivt kan kontrollere kommunikationen. I praksis kan et *Man in the Middle* angreb fx foregå ved en ændring af DNS registrering, enten på DNS-serveren eller ved ændring af hosts filen.

Muhammed-krisen: Diplomatisk krise i 2006 mellem Danmark og flere arabiske lande. Krisen blev afstedkommet af, at daværende statsminister Anders Fogh Rasmussen ikke på Danmarks vegne ville undskylde publiceringen af tolv satiriske tegninger af profeten Muhammed. Tegningerne blev første gang 30. september 2005 bragt i Jyllands-Posten, som illustrationer til en artikel om selvcensur og ytringsfrihed. Tegningerne medførte voldsomme reaktioner fra muslimer i både Danmark og de islamiske lande, hvor omfattende demonstrationer fandt sted. Krisen medførte bl.a. en omfattende arabisk handelsboykot af danske varer, hjemkaldelse af ambassadører og afbrænding af de danske ambassader i Damaskus og Beirut

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.

Patcher: Den *trojanske hest*, w32.patcher findes i mere end 100 forskellige udgaver og med flere forskellige navne. *Patcher* er en avanceret informationstyv, der udelukkende angriber Microsoft Windows, hvor den "opdaterer" centrale Windows komponenter, heraf navnet. Patcher installeres ved *drive-by download* fra webapplikationer og udnytter sårbare versioner af Adobe Reader, Adobe Flash, Sun Java JRE og Quicktime på klient maskinen.

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 *portscanninge*r. 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 fx 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.

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

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

SQL injection: Et angreb der ændrer i indholdet på en webside ved at sende kommandoer til den bagvedliggende SQL-database gennem usikre input-felter på websiden, som fx søgefelter eller kommentarfelter, eller gennem usikre parametre i websidens URL'er.

Storm: *Spam-botnet*, opdaget i januar 2007, der formodes at være kontrolleret fra Rusland. *Botnettet* spredte sig ved hjælp af inficerede e-mails, og i midten af 2007, estimeret til at have mellem 250.000 og 1million inficerede Windows systemer. Lokationen af de centrale *command & control servere*, blev skjult ved hjælp af *fast flux*. I september 2008 aftog aktiviteten fra *Storm*, der ikke længere er blandt de aktive *botnet*.

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 fx 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. Figuroversigt

10. Referencer

Adobe.com, 2009; "*Security advisory for Adobe Reader and Acrobat*"; www.adobe.com/support/security/advisories/apsa09-07.html

Arstechnica.com, 2009; "*Dutch hacker holds jailbroken iPhones hostage for €5*"; arstechnica.com/apple/news/2009/11/dutch-hacker-holds-jailbroken-iphones-hostage-for-5.ars

Blogs.forrester.com, 2009; "*2009: Year Of The Smartphone — Kinda*"; blogs.forrester.com/consumer_product_strategy/2010/01/2009-year-of-the-smartphone-kinda.html

Cio.com, 2009; "*8 Dirty secrets of the IT security industry*"; www.cio.com/article/499829/8_Dirty_Secrets_of_the_IT_Security_Industry

Computer Security Institute, 2009; "*2009 CSI computer crime & security survey*"; www.gocsi.com/forms/csi_survey.jhtml

Computerworld.dk, 2009; "*Conficker har gnavet sig ind i syv millioner pc'er*"; www.computerworld.dk/art/53699

Computerworld.dk, 2009; "*Skal danske internetudbydere bekæmpe botnet?*"; www.computerworld.dk/art/53059/skal-danske-internetudbydere-bekaempe-botnet

Computerworld.dk, 2009; "*Sådan vil Danske Bank beskytte dig mod phishing*"; www.computerworld.dk/art/53257/saadan-vil-danske-bank-beskytte-dig-mod-phishing?a=related&i=54135&bottom

Damballa.com, 2009; "*America's 10 most wanted botnets*"; www.damballa.com/downloads/news/ITN_CIO_2.pdf

Danmarks Statistik, 2009; "*Den offentlige sektors brug af it*"; www.dst.dk/Statistik/ags/IT/Myndigheder.aspx

Danmarks Statistik, 2009; "*Den offentlige sektors brug af it 2008 – Årspublikation*"; www.dst.dk/upload/den_off._sektors_brug_af_it_2008.pdf

Darkreading.com, 2009; "*Up to 9 percent of machines in an enterprise are bot-infected*"; www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=220200118

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

Deloitte, 2009; "*2009 TMT global security survey*"; www.deloitte.com/assets/Dcom-Norway/Local%20Assets/Documents/tmt_securitysurvey2009.pdf

DK•CERT, 2009; "*Conficker installerer falsk antivirus*"; www.cert.dk/nyheder/nyheder.shtml?09-04-14-15-24-00

DK•CERT, 2009; "*Farlige julekort kom fra Amazons cloud*"; www.cert.dk/nyheder/nyheder.shtml?09-12-11-11-35-38

DK•CERT & KOMFO, 2009; "*Styr dit privatliv på Facebook*"; www.cert.dk/pdf/Facebook_Guiden-juli%202009.pdf

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

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

ENISA, 2009; "*Cloud computing risk assessment*"; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

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

Forbrugerrådet, 2009; "*Cookies på nettet*"; www.forbrugerraadet.dk/nyheder-alle/angrebet-af-fjendtlige-smaakager/?ref=2820

F-secure.com, 2009; "*F-Secure Security Lab - Virus World Map*"; www.f-secure.com/en_EMEA/security/worldmap/

Gartner, 2009; "*Gartner identifies the top 10 strategic technologies for 2010*"; www.gartner.com/it/page.jsp?id=1210613

Gartner, 2009; "*Gartner saysit spending to rebound in 2010 with 3.3 percent growth after worst year ever in 2009*"; www.gartner.com/it/page.jsp?id=1209913

Gartner, 2008, "*Why malware filtering Is necessary in the web gateway*"; www.gartner.com/DisplayDocument?doc_cd=158459

Google.com, 2008; "*All your iFrame are point to us*"; googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html

Google.com, 2009; "*Malware statistics update*"; googleonlinesecurity.blogspot.com/2009/08/malware-statistics-update.html

Govcert.nl, 2009; "*Trend report 2009. Insight into cyber crime: Trends & figures*"; www.govcert.nl/download.html?f=152

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

IBM, 2009; "*X-Force 2009 mid-year trend and risk report*"; www-935.ibm.com/services/us/iss/xforce/trendreports/

Intego.com, 2009; "*Hacker Tool Copies Personal Info from iPhones*"; blog.intego.com/2009/11/11/intego-security-memo-hacker-tool-copies-personal-info-from-iphones/

It-borger.dk, 2009; "*5 gode råd om Privatlivets fred på nettet*"; www.it-borger.dk/sikkerhed/netsikker-nu/folg-disse-10-rad-og-bliv-sikker-pa-nettet/5-gode-rad-om-privatlivets-fred-pa-nettet

It-borger.dk, 2009; "*10 gode råd*"; www.it-borger.dk/sikkerhed/netsikker-nu/folg-disse-10-rad-og-bliv-sikker-pa-nettet

It-borger.dk, 2009; "*Første dansker dømt for at uploade forbudte billeder på Facebook*"; www.it-borger.dk/lov-og-ret/nyheder/forste-dansker-domt-for-at-uploade-forbudte-billeder-pa-facebook/

M86security.com, 2009; "*Marshal8e6 security threats: Email and web threats*"; www.m86security.com/newsimages/trace/Marshal8e6_TRACE_Report_July_2009.pdf

M86security.com, 2009; "*Tracking spam botnets*"; www.m86security.com/labs/bot_statistics.asp

M86security.com, 2009; "*Waledac*"; www.m86security.com/trace/i/Waledac,spambot.918~.asp

Microsoft.com, 2009; "*Microsoft Collaborates With Industry to Disrupt Conficker Worm*"; www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.mspx

Ministeriet for videnskab teknologi og udvikling, 2009; "*Sander: Styrket dansk bekæmpelse af internettrusler*" vtu.dk/nyheder/pressemeddelelser/2009/styrket-dansk-bekaempelse-af-internettrusler/

MessageLabs Intelligence, 2009; "*MessageLabs Intelligence: 2009 Annual Security Report*"; www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf

MessageLabs Intelligence, 2009; "*Messagelabs intelligence november 2009*"; www.messagelabs.com/mlireport/November_2009_MessageLabs_Intelligence_Report_FINAL_EN.pdf

MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*"; www.messagelabs.com/mlireport/MLI_2009.09_Sept_SHSFINAL_EN.pdf

Mogo.ch, 2009; "*Press release: «mogoroad iPhone removed from the Apple Store»*"; www.mogo.ch/presse/ID_MOBILE_COMMUNICATE_MOGOROAD_EN.pdf

Net-security.org, 2009; "*Top vulnerable applications in 2009*"; www.net-security.org/secworld.php?id=8628

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

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

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

Politiken.dk, 2009; "*Facebook er en legeplads for hackere*"; politiken.dk/kultur/article561914.ece

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

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

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

Secureworks.com, 2009; "*Opachki Link Hijacker Trojan Analysis*"; www.secureworks.com/research/threats/opachki/

Sfgate.com, 2009; "*Apple privacy score - Snow Leopard - 10, iPhone – 0*"; www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?blogid=150&entry_id=46236

Shadowserver.org, 2009; "*Scan charts*"; www.shadowserver.org/wiki/pmwiki.php/Stats/ScanCharts

Sophos.com, 2009; "*Another iPhone worm - and this time it's malicious*"; www.sophos.com/blogs/chetw/g/2009/11/21/malicious-iphone-worm-loose/

Sophos.com, 2009; "*Security threat report: July 2009 update*"; www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf

Spamcop.net, 2009; "*Total spam report volume, one year*"; www.spamcop.net/spamgraph.shtml?spamyear

Symantec.com, 2009; "*Trojan.Opachki*"; www.symantec.com/security_response/writeup.jsp?docid=2009-092213-3317-99&tabid=2

Theregister.co.uk, 2009; "*Backdoor in top iPhone games stole user data, suit claims*"; www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/

Theregister.co.uk, 2009; "*World's first iPhone worm Rickrolls angry fanbois*"; www.theregister.co.uk/2009/11/08/iphone_worm_rickrolls_users/

Threatpost.com, 2009; "*Attackers Buying Own Data Centers for Botnets, Spam*"; threatpost.com/en_us/blogs/attackers-buying-own-data-centers-botnets-spam-122109

Trendmicro.com, 2009; "*Priset för ditt kreditkort på svarta marknaden*"; emea.trendmicro.com/emea/about/news/pr/se/article/20091214150539.html

Twitter.com, 2009; "*Koobface malware attack*"; status.twitter.com/post/138789881/koobface-malware-attack

Us-cert.gov, 2009; "*Malicious Code Targeting Social Networking Site Users*"; www.us-cert.gov/current/archive/2009/03/04/archive.html#malicious_code_targeting_social_networking

Version2.dk, 2009; "*Bankernes it får outsourcing-håndjern på*"; www.version2.dk/artikel/12203-bankernes-it--faar-outsourcing-haandjern-paa?highlight=outsourcing

Version2.dk, 2009; "*Danske Spil ramt af DDoS-angreb*"; www.version2.dk/artikel/11801-danske-spil-ramt-af-ddos-angreb

Version2.dk, 2009; "*Islamist-hackere til angreb mod Danmark: 52 sites skamferet med død og Allah*"; www.version2.dk/artikel/12374-islamist-hackere-til-angreb-mod-danmark-52-sites-skamferet-med-doed-og-allah

Version2.dk, 2009; "*Netbanktyve bliver dygtigere og får større udbytte hos danskerne*"; www.version2.dk/artikel/12365-netbanktyve-bliver-dygtigere-og-faar-stoerre-udbytte-hos-danskerne

Version2.dk, 2009; "*Svenske myndigheder vil lukke internetadgangen for inficerede computere*"; www.version2.dk/artikel/10265-svenske-myndigheder-vil-lukke-internetadgangen-for-inficerede-computere

Version2.dk, 2009; "*Sådan undgår du jura-faldgruberne i cloud computing*"; www.version2.dk/artikel/12317-saadan-undgaar-du-jura-faldgruberne-i-cloud-computing

Webappsec.org, 2009; "*Web application security statistics 2008*"; projects.webappsec.org/Web-Application-Security-Statistics

Wikipedia.org, 2009; "*Cloud computing*"; en.wikipedia.org/wiki/Cloud_computing

Wikipedia.org, 2009; "*Malware*"; da.wikipedia.org/wiki/Malware

Kontakt:

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

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