DK•CERT

Trendrapport 2007

– it-sikkerhed nu og i fremtiden

UNI•C

Redaktion: Shehzad Ahmad, DK•CERT

Grafisk arbejde: Kirsten Hougaard

Fotos: PhotoDisc®

Tryk: Fihl Jensen Grafisk Produktion A/S

DK•CERT

Trendrapport 2007

– it-sikkerhed nu og i fremtiden

UNI•C

Resume

Velkommen til DK•CERT Trendrapport 2007! Fremover vil DK•CERT udsende en sådan Trendrapport hvert år. Formålet er at samle op på tendenser på it-sikkerhedsområdet i det forgangne år. Til det formål har vi gennemgået alle de anmeldelser, som DK•CERT har modtaget i 2007. Den viden suppleres med informationer fra vores internationale samarbejdspartnere og fra internettet i øvrigt.

Mængden af sikkerhedshændelser på den danske del af internettet er stigende. DK•CERT behandlede i 2007 over 90.000 anmeldelser. Året før var tallet godt 55.000. Samtidig fortsætter tendensen til, at en voksende andel af hændelserne skyldes berigelseskriminalitet. Hvor mange sikkerhedshændelser for fem år siden kunne karakteriseres som drengestreger, der udforskede nettets tekniske muligheder, er drivkraften i dag ønsket om at få penge fra ofrene. Det kan ske ved at narre dem til at afsløre fortrolige oplysninger såsom kreditkortnumre via phishing eller gennem afpresning med trusler om ude-af-drift-angreb. Blandt årets trends var botnets, som kriminelle udlejer til udsendelse af spam eller andre lyssky formål. Vi så også mange eksempler på udnyttelse af sårbarheder i udbredte applikationer og i web-systemer. Mængden af uønskede mails er nu så stor, at nogle organisationer filtrerer 90 procent af alle indkommende mails fra.

Rapporten bygger primært på informationer fra de tre netværk, DK•CERT overvåger: Forskningsnettet, Sektornettet og UNI•Cs eget netværk. Men vi mener, at den også giver et dækkende billede af sikkerhedssituationen på den øvrige danske del af internettet i 2007. God fornøjelse med læsningen!

Med venlig hilsen Shehzad Ahmad, leder af DK•CERT

Hvad er DK•CERT

DK•CERT er en organisation under UNI•C, Danmarks IT-Center for Uddannelse og Forskning, som er en landsdækkende virksomhed under Undervisningsministeriet. UNI•C oprettede DK•CERT i 1991 i forbindelse med en af Danmarks første hackersager. Inspirationen kom fra det amerikanske CERT (Computer Emergency Response Team), som blev oprettet i 1988.

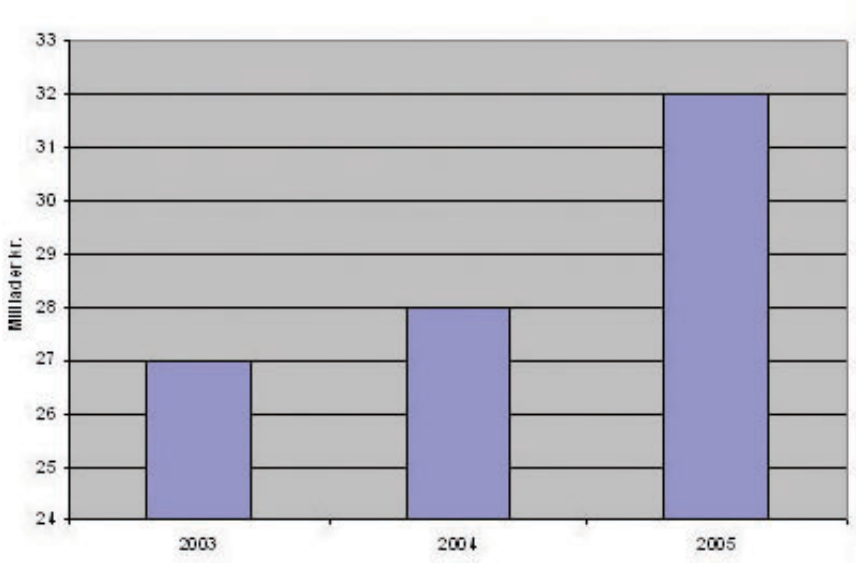
DK•CERT har til formål at følge sikkerheden på internettet og advare om potentielle it-sikkerhedsproblemer. For at kunne gøre det indsamler vi viden fra både åbne kilder og andre CERT-lignende organisationer. Samarbejdet med dem foregår i organisationen Forum of Incident Response and Security Teams (FIRST).

DK•CERT tager imod anmeldelser af sikkerhedshændelser på internettet, både udefra og fra de tre netværk, vi overvåger: Forskningsnettet, Sektornettet og UNI•Cs eget netværk.

Indholdsfortegnelse

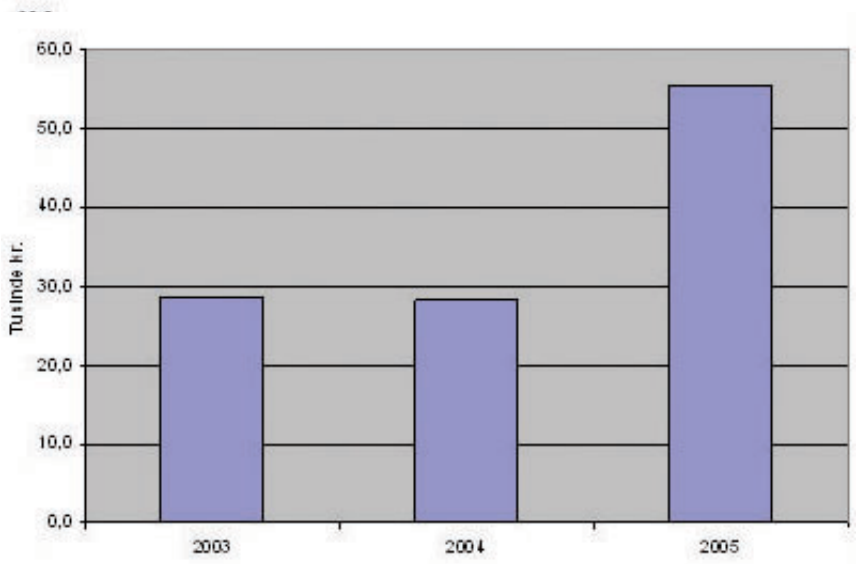
Indledning

Siden årtusindeskiftet er det danske samfunds udgifter til it steget. Dermed er også værdien af it-aktiver, der skal beskyttes, øget. Ifølge Danmarks Statistik lå danske organisationers it-udgifter i 2003 på 27 milliarder kroner, hvor de i 2005 var vokset til 32 milliarder kroner (se Figur 1). Tallet er utvivlsomt endnu højere i dag.



Figur 1. Danske organisationers it-udgifter ifølge Danmarks Statistik.[1]

Det fremgår ikke af tallene, hvor mange penge organisationerne bruger på at beskytte deres it-mæssige aktiver. Men it fylder stadig mere i både arbejdsliv og fritid. Det fremgår også af, at der nu bruges flere ressourcer på it per ansat end før i tiden (Figur 2).



Figur 2. Danske organisationers it-udgifter pr. fuldtidsansat ifølge Danmarks Statistik.[2]

1 www.dst.dk
2 www.dst.dk

Der er altså en stor mængde it-systemer, der skal beskyttes. DK•CERT har siden organisationens start specialiseret sig i sikkerhed i forhold til internettet. Efterhånden som internettet er blevet en naturlig del af danskernes hverdag, er mængden af vores aktiviteter øget. Denne rapport giver et billede af sikkerhedssituationen på den danske del af internettet i 2007.

Rapporten er opdelt i tre hovedafsnit. Det første ser på trends inden for it-kriminalitet i 2007, mens det næste ser på fremtiden inden for it-kriminalitet. Det sidste afsnit handler om it-sikkerhed nu og i fremtiden.

It-sikkerhed handler om at sikre tre elementer ved et it-system: Tilgængelighed, integritet og fortrolighed. Tilgængelighed handler om, at systemet skal virke og kunne bruges. Integritet handler om, at man skal kunne stole på de data, der ligger i det. Fortrolighed handler om at beskytte, hvem der har adgang til hvilke data og systemer.

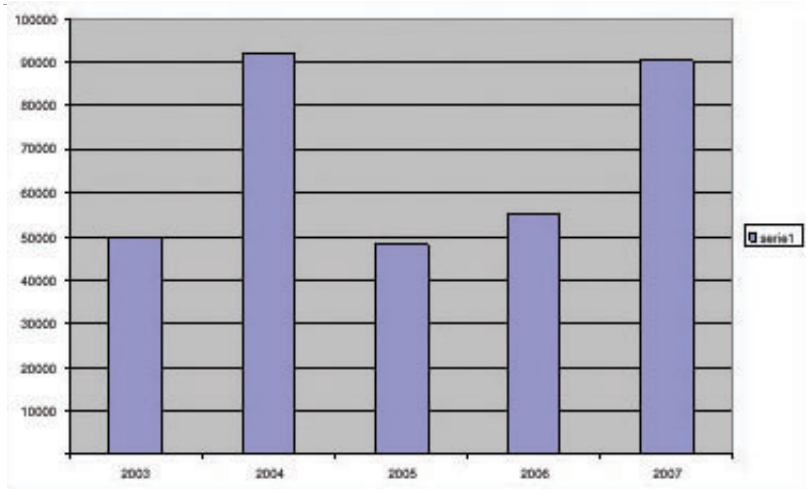
Hvor it-sikkerhed er et bredt emne, er it-kriminalitet smallere. Et system kan således godt have et sikkerhedsproblem, uden at det er kriminelt. Megen it-kriminalitet handler om, at kriminelle udnytter sikkerhedsproblemer til at begå forbrydelser.

Målgruppen for denne rapport er alle, der er interesserede i it-sikkerhed. Vi har bestræbt os på at forklare de tekniske emner, så de er forståelige for ikke-teknikere. Dermed giver rapporten folk uden for sikkerhedsverdenen et indblik i de sikkerhedsmæssige udfordringer, som danske organisationer dagligt møder på internettet.

It-kriminalitet – trends 2007

DK•CERT har i 2007 oplevet en vækst i antallet af anmeldelser af it-sikkerhedshændelser, se Figur 3, og niveauet er nu på højde med 2004, hvor Microsoft udgav Service Pack 2 til Windows XP. Service Pack 2 lukkede en række sårbarheder i Windows XP og udbredte brugen af personlige firewalls, hvilket sandsynligvis har været medvirkende årsag til et fald i registrerede it-sikkerhedshændelser. F.eks. har der siden 2005 ikke været større ormeangreb eller virusepidemier rettet mod operativsystemet Windows[3]. Det formodes at den efterfølgende faldende succesrate og større mulighed for opdagelse, har medført, at kun de mest kyndige og ihærdige har fortsat deres aktiviteter. Dette har været medvirkende årsag til ændrede motiver og mønstre for it-kriminalitet.

3 http://www.sans.org/top20/



Figur 3. It-sikkerhedshændelser anmeldt til DK•CERT.

Hvor formålet med udbredelse af orme og virus tidligere har været spredningen i sig selv, synes formålet i dag at være målrettet specifikke kriminelle aktiviteter. Derfor har virusprogrammøren ingen interesse i hurtig spredning og dermed opdagelse. Således havde de væsentligste nye orme og virus i 3. kvartal af 2007, jævnfør viruslist.com[4], alle som formål at placere trojanske heste eller "botter" for at stjæle brugerdata fra den inficerede maskine. Størst opmærksomhed fik Storm Worm, som siden januar 2007 har spredt sig via e-mail. Den menes at have samlet mere end 6 millioner computere i botnettet Storm[5].

Generelt er mængden af uønskede mails i 2007 steget. Flere steder filtreres over 90 procent af alle mails fra.

Omsætningen inden for it-kriminalitet skønnes i dag at være på mere end 105 milliarder dollars[6]. I 2007 var de it-kriminelle både professionelle og organiserede. Grænserne mellem it-kriminalitet og traditionel organiseret kriminalitet er flydende, og it er i stigende grad blevet et middel til at udføre traditionel kriminalitet i form af svindel, tyveri og afpresning. Når motivet har ændret sig til økonomisk vinding, er det ikke længere blot organisationernes it-systemer, der er i fare for at blive ramt, men i lige så høj grad borgerne og deres pengepunge. Et skift i motiverne for it-kriminalitet medførte, at vi i 2007 oplevede mere målrettede angreb mod den enkelte borger. Som udtryk for dette ses et stigende antal phishing-sider og trojanske heste placeret på danske websteder. De havde alle til formål at indsamle brugerdata fra den besøgende.

Stigende professionalisering har medført større opfindsomhed og stigende kompleksitet i it-kriminalitetens væsen. Det går lige fra produktion og distribution af kopiprodukter over "markedsføring" via mailkampagner til ulovligt høstede e-mail-adresser til hvidvaskning af penge. De kriminelles værktøjskasse er blevet mere avanceret og involverer blandt andet brugen af botnets, falske hjemmesider og falske trådløse hotspots. Med stigende professionalisering er udnyttelse af sårbarheder, hvortil der endnu ikke er udgivet rettelser (zero-day attacks), blevet et problem. I 2007 blev der blandt andet udgivet exploits (angrebsprogrammer) til sårbarheder inden udgivelse af programrettelse[7] i følgende applikationer:

4 http://www.viruslist.com/en/analysis?pubid=204791973
5 http://www.enisa.europa.eu/pages/02_01_press_2007_11_27_botnets.html
6 http://www.computerworld.com.au/index.php/id;1164052503;pp;2
7 http://www.sans.org/top20/

- Microsoft Word
- Windows Graphics Rendering Engine (ANI)
- Windows DNS Server
- Adobe Acrobat Reader plug-in
- RealPlayer
- QuickTime

Alt er i dag til salg på nettet. Handel med e-mail-adresser, kreditkortnumre, virusgeneratorer og udlejning af botnets er i dag en særskilt industri. For eksempel har segmenteringen af botnettet Storm givet anledning til spekulationer om, at formålet med dette botnet var at tjene penge på at udleje dele af det til spam udsendelse eller DDOS- angreb (Distributed Denial of Service) med mere[8].

Botnets

2007 har på mange måder stået i botnettets tegn. Botnets er i dag en central del af mange former for it-kriminalitet. De største trusler mod private brugere er alle direkte relateret til botnets.

Botnets anvendes til kriminelle handlinger på internettet såsom udsendelse af spam, tyveri af fortrolige oplysninger og DDOS- angreb. Det er der set flere eksempler på i løbet af 2007. Formålet med at benytte bots til at udføre kriminelle handlinger er at skjule, hvorfra kriminaliteten bliver udført, og at kunne benytte flere computere til at udføre angreb. Det er ikke svært at finde et botnet på internettet: Placer blot en pc uden opdateringer på internettet og undersøg, hvad der sker med den.

Storm-botnettets bagmænd er mistænkt for at stå for udlejning af mindre botnets til spammere. Spammere kan dermed udsende spam fra inficerede computere i det lejede botnet uden ejernes viden. I sidste halvår af 2007 begyndte Storm at kryptere peer-to-peer-trafik. Dermed vil inficerede computere kun være i stand til at kommunikere med andre computere, som bruger samme krypteringsnøgle[9]. Sikkerhedseksperten Joe Stewart påpeger dog, at netop den krypterede trafik vil gøre det nemmere at identificere trafikken imellem inficerede computere og "peer-to-peer"-servere.

I 2007 blev botnets også brugt til at stjæle fortrolige oplysninger fra brugere ved at benytte phishing-teknikker og udnytte sårbarheder i brugeres computersystemer. For eksempel blev en række brugerprofiler på MySpace inficeret med botnet-kode, der førte en bruger til en forfalsket MySpace login-side. Her blev brugeren narret til at indtaste sit brugernavn og adgangskode, fordi websiden til forveksling lignede den originale login-side på MySpace[10]. Bagmændene kunne herefter udnytte de indsamlede brugernavne og adgangskoder til at tilgå brugeres fortrolige informationer. Ud over at stjæle brugernavne og adgangskoder forsøgte bagmændene også at udnytte kendte sikkerhedshuller til at installere skadelige programmer på brugernes computersystemer.

8 http://www.computerworld.com.au/index.php/id;1164052503
9 http://www.secureworks.com/research/blog/index.php/2007/10/15/the-changing-storm/
10 http://googleonlinesecurity.blogspot.com/2007/06/thwarting-large-scale-phishing-attack.html

Sådan virker et botnet

Et botnet er et netværk af pc'er. På hver pc er der installeret et program, en "bot", som en bagmand kan fjernstyre uden ejerens vidende. Begrebet botnet kommer fra ordene "robot" og "netværk." De overtagne computere i et botnet kaldes derfor botter eller bots.

Bagmændene benytter botnets til at udføre kriminelle handlinger, såsom at stjæle følsomme oplysninger, udsende spam eller udføre massive angreb mod en udvalgt destination. Bagmanden kan tjene penge på at udføre kriminelle handlinger eller udleje bots til andre kriminelle.

En computer bliver optaget i et botnet, hvis der bliver installeret en bot på computersystemet. Det gør det muligt at fjernstyre computeren. Denne bot bliver installeret via sårbarheder i computerens system, som bottens skadelige kode udnytter. Mange bots åbner en bagdør i systemet. Bots kan herefter sprede sig selv via bagdørene i de inficerede systemer til andre sårbare systemer på samme måde.

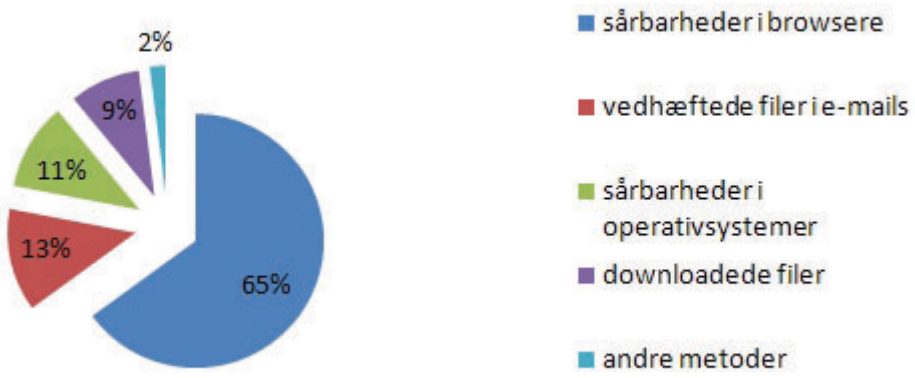
Nogle bots kommunikerer via centrale servere, som fungerer som såkaldte Command and Control (C&C)-servere for et helt botnet. Kommunikationen forsøges så vidt muligt holdt skjult for eksempel ved at benytte HTTP- og HTTPS-protokollerne til servere, fordi disse protokoller typisk tillades igennem firewallen. Bagmanden styrer de centrale servere. Det er nærmest umuligt at finde frem til placeringen af de centrale kommunikationsservere, som kontrollerer botnets, fordi de skjules bag en DNS-teknik, der kaldes fast flux. Det er et konstant ændrende netværk af kompromitterede computere, der fungerer som proxyservere. Det betyder, at det ikke som tidligere er muligt at finde frem til en bagmand igennem landets CERT'er og internetudbydere, når man kender til den centrale server, fordi den konstant ændres.

I udviklingen af botnets ses også brugen af distribuerede kommunikationsservere. Det betyder, at man ikke kan deaktivere et botnet blot ved at fjerne den centrale server, fordi andre servere har samme funktion via "peer-to-peer"-netværk. Sikkerhedsekspert Bruce Schneier[11] betegner brugen af "peer-to-peer"-netværk som et problem, fordi netværksovervågning ikke kan afsløre forbindelser til distribuerede servere, da de er spredt over flere serverforbindelser, i modsætning til hvis bots kun forbandt sig til én central server.

Udbredelse via sårbare applikationer

Den væsentligste metode til spredning af botnet-programmer er ifølge sikkerhedsfirmaet S21sec sårbarheder i browseren (se figur 4). 65 procent af de pc'er, der bliver inficeret af botnet-programmer, rammes på denne måde. Den næstmest almindelige spredningsmetode er e-mails med vedhæftede filer med 13 procent, mens sårbarheder i styresystemet muliggjorde 11 procent. Downloadede filer står for 9 procent af infektionerne.

11 http://www.schneier.com/crypto-gram-0710.html



Figur 4: Botnet inficeringsmetoder ifølge sikkerhedsfirmaet S21sec[12].

Udbredelse gennem browseren kan ske via sårbarheder i selve browseren og dens plug-ins eller gennem applikationer, som åbnes i browseren. Et af de seneste eksempler på en sådan sårbarhed blev fundet i november måned i Apple QuickTime, som er en applikation til at afspille mediefiler med. Applikationen kan åbnes via browsere i Microsoft Windows og Mac OS X. En angriber kan udnytte sårbarheden til at afvikle skadelig programkode på en brugers computer, hvis brugeren åbner en speciallavet QuickTime-fil. Dermed risikerer brugeren at få sin computer inficeret med botnet-programmer. Den populære medieafspiller iTunes er også sårbar over for denne sårbarhed, da den anvender QuickTime.

Udbredelse via banner injection
Botnet-programmer kan også spredes via bannerannoncer. Banner injection sker ved at forfalske originale bannerreklamer og indsætte skadelig programkode, for eksempel en trojansk hest, i den forfalskede reklame. Det skadelige program kan afvikles på en brugers computer blot ved, at brugeren besøger en webside, som indeholder den forfalskede bannerreklame. Det skyldes, at det skadelige program udnytter sårbarheder i pc'ens browser. Når programmet har inficeret brugerens computersystem, kontakter det inficerede system en C&C-server, hvorfra bagmænd kan kontrollere alle inficerede systemer og sørge for at opdatere de skadelige programmer.

Udbredelse af Storm-botnettet via e-mails
Storm-botnettet er kendt for at sprede sig via spam-mails, som for eksempel indeholder links til websider, der udnytter sårbarheder i operativsystemer og installerede applikationer. I slutningen af 2007 blev der udsendt e-mails med julehilsnerne: "Your Secret Santa," "Santa Said, HO HO HO," "Warm Up this Christmas" og "Mrs. Clause Is Out Tonight!" Disse e-mails indeholdt billeder og et link til en webside med billeder af letpåklædte nissepiger. Hvis man klikkede på billederne eller "Download for free"-knappen, blev der installeret en variant af Storm-ormen via websiden. Metoden er ofte blevet benyttet til at sprede Storm-ormen, hvilket var med til at gøre den til det mest udbredte botnet i 2007[13].

12 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf
13 http://www.theregister.co.uk/2007/12/27/storm_worm_seasonal_attacks/

De mange inficeringsmetoder viser vigtigheden af, at man holder sine computersystemer sikre og opdaterer operativsystemer og alle applikationer med seneste rettelser.

Botnet-kode bliver automatisk opdateret
Storm var det mest omtalte botnet i 2007. Men Storm er ikke kun en orm, men fungerer som en trojansk hest og et botnet på en gang [14]. Selvom Storm er det mest udbredte botnet, spreder den skadelige programkode sig langsomt på sårbare Windows-systemer. Det interessante ved Storm og lignende botnet er, at botnet-programmet på de inficerede systemer bliver opdateret via botnettets C&C-servere (Command and Control), som er "peer-to-peer"-servere. Opdateringen af programmet gør det nemt at skjule udbredelsen af Storm, fordi antivirusprogrammer, IDS-systemer og lignende har sværere ved at identificere det skadelige program. Når botnettet kommunikerer via ofte brugte protokoller, er det svært for systemadministratorer at lukke for kommunikationskanalen.

Sårbare webapplikationer

Udnyttelse af sårbare webapplikationer er et problem, der er taget til i omfang gennem 2007. Tendensen er muliggjort af offentliggørelsen af flere sårbarheder, som har været nemme at udnytte. Endvidere har brugen af webplatformen været ideel til at ramme den almindelige bruger, der besøger de udnyttede websites. Det gælder, hvad enten formålet har været at placere skadelige programmer i den besøgendes browser eller narre oplysninger ud af offeret.

Hver dag rapporteres der sårbarheder i både kommercielle og open source webapplikationer som for eksempel Content Management Systemer (CMS), Wikier, portaler og diskussionsfora, der benyttes af både store og små organisationer. Over 10 procent af alle angreb anmeldt til DK•CERT i 2007 var rettet mod webapplikationer.

At sårbare webapplikationer er et problem, understreges yderligere af, at DK•CERT ved sårbarhedsscanning fandt cirka en tredjedel af alle sårbarheder på kundernes webapplikationer. Dertil kommer sårbare FTP-servere samt brugerkonti med standardbrugernavne og/eller svage passwords, der også kan give anledning til upload af filer eller indsættelse af skadelige programmer i de eksisterende filer.

Alle udviklingsplatforme (PHP, .Net, J2EE, Ruby on Rails med flere) og alle webapplikationer er potentielt i risikozonen. De mest udnyttede sårbarheder på webapplikationer er ifølge SANS[15]:

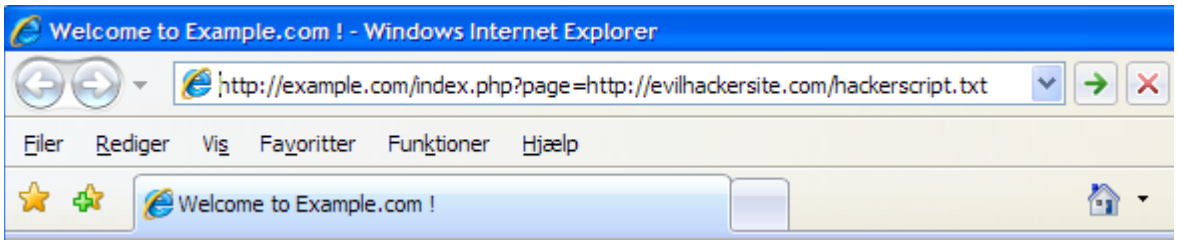
- PHP remote include: Ved brug af "allow_url_fopen", der som standard er aktiveret i PHP, tillades, at applikationen kan benytte ressourcer på internettet. Når brugernes input bruges til at angive filnavne, der skal inkluderes i applikationen, giver dette mulighed for at afvikle og installere programmer.

14 http://www.schneier.com/crypto-gram-0710.html
15 http://www.sans.org/top20/

- SQL injection: Uhensigtsmæssig programmering af webapplikationer giver mulighed for, at besøgende kan sende SQL-kommandoer til applikationen, så databasen udfører dem. Det giver risiko for såvel eksponering af data, der ikke var tilsigtet, som oprettelse og ændring af poster i databasen. I værste tilfælde fører det til kompromittering databaseserveren.

- Cross-Site Scripting (XSS): En sårbarhed, der muliggør, at besøgende kan indsætte HTML- eller client-side script-kode på den side, de besøger, som efterfølgende ses af andre besøgende. Denne type angreb benyttes blandt andet ved defacement (web-graffiti) og phishingangreb, men også til installation af skadelige programmer i brugerens browser.

Flere af årets publicerede sårbarheder i for eksempel PHP er meget lette at udnytte, eksempelvis blot ved at angive en URL til skadelige programmer som parameter i webadressen (Figur 5). Dette giver anledning til, at danske websites bliver defacet eller uforvarende kommer til at hoste phishing-sider, trojanske heste eller anden skadelig kode.



Figur 5. Eksempel på udnyttelse af php sårbarhed, allow_url_fopen aktiveret

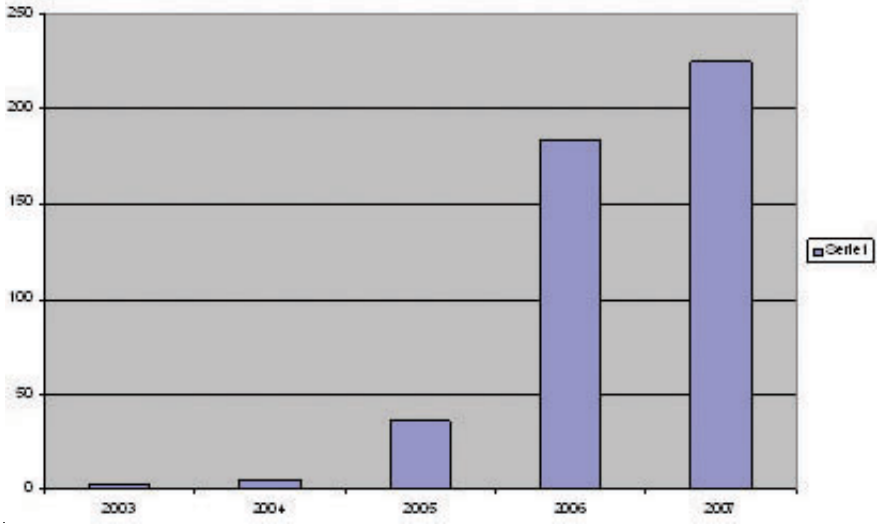
Udnyttelse af sårbare webapplikationer
Et angreb på en webapplikation har sjældent til formål at kompromittere de bagvedliggende data. Hackerens formål er i stedet at indsætte skadelige programmer eller scripts og derved sprede skadelig software til de brugere, der besøger webstedet. Den sårbare webapplikation er altså ikke et mål i sig selv, men et middel til at ramme det endelige mål, den enkelte bruger.

Mediebureauer, der leverer bannerreklamer, er blevet et populært mål for hackere. Da bannerreklamer typisk udsendes til flere forskellige websites fra én central server, kan en hacker ramme meget bredt, hvis han formår at få adgang til et mediebureaus servere. Herfra kan han koble skadelige programmer eller scripts på bannerreklamer, der ellers burde være helt legitime.

I Danmark har vi set eksempler på, at læsere af websider er blevet inficeret med skadelig software via bannerreklamer. Blandt andet spredte Ekstra Bladets hjemmeside i december måned skadelige programmer gennem bannerreklamer på siden. Senere i december var TV2's hjemmeside offer for banner injection, idet siden spredte en trojansk hest, der udgav sig for at være et antispyware-værktøj. Også Børsen har haft bannerreklamer, som installerede skadelige programmer på en besøgendes computer. Herhjemme har vi først sidst på året for alvor oplevet indsættelse af skadelig software via bannerreklamer på populære websider[16], men metoden har været velkendt internationalt gennem længere tid.

16 http://www.csis.dk/dk/nyheder/nyheder.asp?tekstID=655&side=1

Banner injection er et alvorligt problem, da det kan ramme brugeren gennem websteder, han ellers har tillid til.



Figur 6. Anmeldelser til DK•CERT om phishing-sider og trojanere placeret på danske websites.

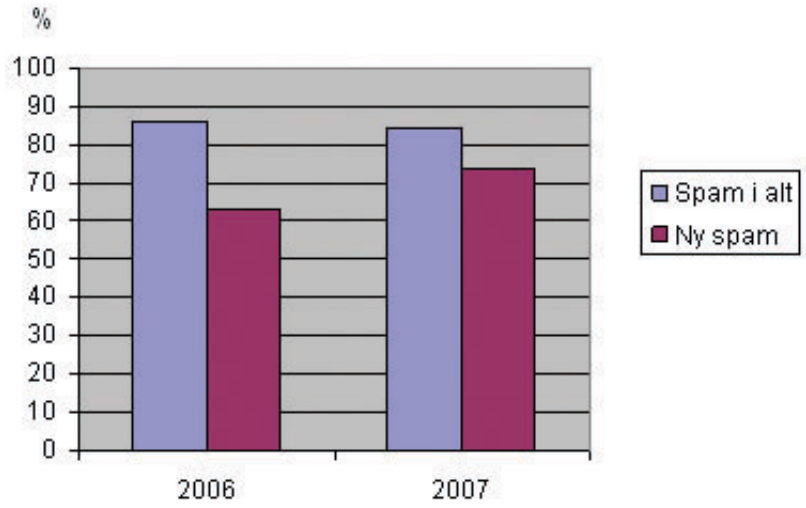
Derudover har DK•CERT i 2007 observeret en markant stigning i antallet af phishing-sites på danske servere (figur 6)

Ekstra Bladet – en case om banner injection

Midt i december blev Ekstra Bladets webside, eb.dk, udnyttet til at sprede skadelige programmer til sidens læsere. Koden blev spredt gennem en af de bannerreklamer, der blev vist på siden. Ved at udnytte sårbarheder i webbrowseren installerede programmet en række programmer på brugerens computer, heriblandt en kendt datatyv, der forsøger at aflure login og kodeord til netbanker.

Når først programmerne var installeret, kontaktede de en C&C-server i Kina for at hente opdateringer og ledsagerkomponenter. Desuden installeredes et rootkit.

Spam, virus og phishing-mails



Figur 7. Mængden af spam på verdensplan faldt en smule fra 2006 til 2007, men en større andel var ny, hidtil ukendt spam. Tallene angiver spam i procent af alle mails. Messagelabs Intelligence: 2007 Annual Security Report[17].

Junkmails

Junkmails er den fælles betegnelse for spam-, virus- og phishing-mails. Vi benytter os her af den fælles betegnelse for de tre typer mails, da den samme fremgangsmåde bliver benyttet til at sprede disse mails, og da formålet i langt de fleste situationer er det samme.

Spam: Defineres af forbrugerombudsmanden som uønskede reklame-mails, som sendes via e-mail. Det er forbudt i markedsføringslovens paragraf 6. Man kan klage over spam til forbrugerombudsmanden. Lovgivningsmæssigt skelner man altså mellem spam og andre uønskede e-mails, selvom fremgangsmåden for masseudsendelse af spam er den samme som for virus- og phishing-mails.

Virus-mails: Er e-mails som indeholder skadelige programmer, der bliver afviklet på modtagerens computer med eller uden brugerinteraktion. Virussen kan være indeholdt i selve e-mailen eller ligge som en vedhæftet fil eller et link til et websted.

Phishing-mails: Forsøger at lokke fortrolige oplysninger ud af modtageren. Det kan være brugernavne og adgangskoder til websteder eller kontonumre til modtagerens bankkonti. Typisk indeholder phishing-mails links til forfalskede websteder, som modtageren opfordres til at klikke på. Figur 6 viser stigningen i modtagne anmeldelser på phishing-websites.

17 http://www.messagelabs.com/mlireport/MLI_2007_Annual_Security_Report.pdf

I slutningen af 2007 blev flere brugere af det danske websted Jobindex.dk udsat for spammails. I en e-mail fik de tilbuddet om at tjene ekstra penge ved at modtage en økonomisk gevinst fra afsenderne af e-mailen og sende pengene videre til en bankkonto i udlandet[18]. Tilbuddet drejede sig om ulovlig hvidvaskning af penge, som ifølge Kaare Danielsen fra Jobindex.dk formentlig var tjent ved at bryde ind i folks netbanker. Folk, der tager imod den slags tilbud, kaldes for muldyr.

Denne metode til at lokke folk til at sende penge til kriminelle er blevet mere udbredt igennem flere år. Det startede med de såkaldte nigerianske tiggerbreve, hvor modtageren skal hjælpe afsenderen med at få en stor pengesum ud af et afrikansk land mod løfte om del i udbyttet. I de seneste år har denne trend udviklet sig. For eksempel oplever flere brugere at modtage e-mails, hvor de skal følge links til websites, hvor de skal indtaste fortrolige oplysninger, de såkaldte phishing-mails. Phishing-mails benytter sig af samme teknikker som spammails til at skjule den oprindelige afsender.

Junkmail har udviklet sig gennem tiden fra at indeholde reklamer for diverse medicinalprodukter og pornografi med mere til at være en metode til at sprede virus og trojanske heste, samt lokke fortrolige oplysninger ud af læserne og sprede falske oplysninger. Lovgivningsmæssigt er der forskel på spam, virusmails og phishing, men efterhånden ses en mere flydende overgang mellem definitionerne, fordi de samme teknikker benyttes til at udsende e-mailene. Modtagerne skelner derfor ikke imellem disse former for uønskede e-mails.

En udvikling i 2007 er, at junkmails indeholdt skadelige programmer i form af links til websteder, hvor brugere bliver inficeret med de skadelige programmer, når de klikker på linket. For eksempel spredtes botnettet Storm via spam, som indeholdt links til forfalskede websider med skadelige programmer, ligesom phishing-mails indeholder links til forfalskede websteder, som også er sat op via botnets[19].

I 2007 var der flere eksempler på, at svindlere forsøgte kunstigt at pumpe aktiekurser op ved at udsende informationer via mail om bestemte aktier, de såkaldte 'pump-and-dump'-mails. Der er set flere eksempler på, at aktier er steget i værdi, efter at spammere har udsendt junkmails med informationer om de pågældende aktier.[20] [21] Sikkerhedseksperten Joe Stewart påpeger, at 'pump and dump'-mails også bliver udsendt fra botnettet Storm.

Spammere ændrer hele tiden på junkmails indhold for at omgå spam- og gateway-filtre. I 2007 har vi set spammere bruge billedfiler, PDF-dokumenter og Excel-filer til at udsende junkmails. Metoderne og indholdet ændrer sig hele tiden for at sikre, at junkmails når modtagernes indbakker

18 http://www.version2.dk/artikel/5496
19 http://www.usatoday.com/tech/news/computersecurity/wormsviruses/2007-08-02-storm-spam_N.htm
20 http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043242&pageNumber=2
21 http://www.securityfocus.com/brief/414

Trusler mod infrastrukturer

Angreb mod infrastruktur – forstået som angreb, der har til formål at forhindre kommunikation, frem for at stjæle data eller give angriberen ulovlig adgang til systemer – udgør fortsat en trussel. Det er meget vanskeligt at gardere sig mod Distributed Denial of Service (DDoS)-angreb, medmindre ens organisation i forvejen håndterer meget store mængder trafik.

Der er tidligere set flere eksempler på, at DDoS-angreb udføres som led i forsøg på afpresning. De har typisk været rettet mod online casioner og bookmakere og andre organisationer, der i høj grad er afhængige af internettet til at drive deres forretning.

Angreb på DNS-rodservere

Den 6. februar 2007 blev flere af DNS-rodserverne, der udgør internettets fundament, udsat for et storstilet DDoS-angreb. Angrebet var fordelt på to bølger på henholdsvis to en halv og fem timer. Det var det største af sin art siden et lignende angreb i 2002. Dengang lykkedes det angriberne at sætte ni af de i alt 13 rodservere ud af drift.

Angrebet i 2007 var rettet mod seks af de 13 rodservere. Alle seks servere forblev dog operationelle, mens angrebet stod på, og kun to af serverne blev alvorligt påvirket af angrebet. Når angrebet ikke havde større konsekvenser, skyldes det de sikkerhedsforanstaltninger, der blev iværksat efter angrebet i 2002. Siden da har flere af rodserverne været fysisk fordelt over flere hundrede maskiner og lokaliteter, i stedet for at ligge på én fysisk lokalitet. Teknologien, der gør det muligt, kaldes Anycast. Den er medvirkende til at gøre rodserverne langt mindre sårbare over for DDoS-angreb. De to servere, der var hårdest påvirket af angrebet i 2007, er endnu ikke omfattet af Anycast-systemet.

Angreb på Letland

I april og maj 2007 var Letland offer for et større DDoS-angreb fra russiske hackere. Angrebet var en hævnaktion, efter de estiske myndigheder flyttede et sovjetisk (og dermed russisk) krigsmonument fra centrum af hovedstaden Tallinn til udkanten af byen. Computere fordelt på botnet spredt over det meste af verden deltog i angrebet.

Det lykkedes for angriberne at lukke for adgangen til en række estiske netaviser og netbanker samt hjemmesider for flere ministerier og private firmaer. Desuden blev flere hjemmesider, heriblandt siden for regeringspartiet Reformierakond, udsat for webgraffiti.[22] [23] [24]

22 http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
23 http://news.bbc.co.uk/1/hi/world/europe/6665195.stm
24 http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/

Angreb på CSIS
I slutningen af august blev det danske it-sikkerhedsfirma CSIS udsat for et omfattende DDoS-angreb. CSIS havde forinden været i færd med at optrevle botnettet Storm og var tilsyneladende blevet opdaget af botnettets bagmænd.

Storm-bagmændene indledte herefter et angreb på CSIS, enten som hævn eller i et forsøg på at stoppe efterforskningen. Angrebet involverede flere tusinde computere fra Storm-botnettet. Det formåede totalt at lukke internetforbindelsen hos CSIS' efterforskningsafdeling[25]

It-kriminalitet – fremtidige trends

De kommende år vil sandsynligvis bringe mere af det, vi har set i 2007, blot med mere komplekse og udspekulerede måder at udnytte potentielle ofres frygt og grådighed på. Vi vil se kortere og mere målrettede angreb, hurtigere opdateringer og mutering af skadelige programmer, samt flere forsøg på at sløre sine angreb. En stigning i den økonomisk motiverede it-kriminalitet vil derudover skabe et stigende behov for hvidvaskning af penge, og det kan forventes, at rekrutteringen af "muldyr" intensiveres og bliver mere målrettet og udspekuleret.

Med voksende professionalisme vil de organiserede it-kriminelle i stigende grad benytte forretningslivets metoder. Business Intelligence-løsninger vil blive brugt til at målrette "markedsføringen" af spam- og phishing-kampagner. Der vil sandsynligvis blive oprettet komplekse globale selskabsstrukturer, hvorigennem penge tjent ved it-kriminalitet kan vaskes hvide.

Botnet bliver stadig mere udbredte og brugt til eksempelvis spamafsendelse, DoS-angreb og lignende. Hvor afpresning med truslen om, at organisationens servere eller internetforbindelse ville blive sat ud af drift, tidligere har været forbeholdt online kasinoer og bookmakere, kan man forestille sig, at også almindelige internetbutikker og større organisationer vil blive ramt af dette fænomen.

Derudover vil de kommende år sandsynligvis byde på flere angreb mod og med mobile enheder. For eksempel kan nye virus have til formål at indsamle kontaktoplysninger fra telefonen på samme måde som de traditionelle mailbaserede orme. De kan også gå efter forretningsdata eller lignende. Når flere data lagres i organisationerne, får de større værdi for organisationen og kan blive mål for it-kriminalitet. Data kan sælges eller benyttes til afpresning med trussel om offentliggørelse. Et middel til dette kan blandt andet være mobile enheder, der i dag kan indeholde store mængder data.

25 http://www.version2.dk/artikel/3766?rss

Datatyveri fra private kan give anledning til identitetstyveri, hvor varer og tjenesteydelser bestilles i andres navn og med andres betalings- og kreditkort. En afart af dette er tyveri af virtuelle genstande i for eksempel online rollespil, der efterfølgende sælges på online auktioner. Persondata bliver til stadighed eksponeret på internettet og vil i stigende grad give anledning til denne type kriminalitet.

I en verden med stadig større fragmentering af samfundsgrupper og meninger, kan den politisk eller religiøst motiverede kriminalitet blive et problem på nettet, hvis de "rigtige" grupperinger formår at skaffe kompetencer eller økonomi til deres forehavender.

Målrettet tyveri af data

Hvor gamle dages typiske virus- og ormeangreb var rettet mod alle, der kunne rammes, ses nu en tendens til mere målrettede angreb. Det gælder især inden for phishing-svindel, hvor såkaldt "spear phishing" er dukket op. Det går ud på, at svindlerne tilpasser deres mails til den enkelte modtager. De skriver således modtagerens navn, stilling og firmanavn i mailen. Formålet er at få mailen til at virke mere troværdig, så brugeren ikke mistænker afsenderen for at have lumske bagtanker. Fænomenet er kendt i udlandet, men vi har ikke set danske eksempler på det.

En tilsvarende tendens gælder inden for skadelige programmer. Her har der internationalt været nogle få eksempler på, at svindlere har udnyttet sårbarheder i Office-pakken i målrettede angreb. De udsendte mails med vedhæftede dokumenter, der var udformet, så de så legitime ud. Formålet var her at få modtageren til at åbne det vedhæftede dokument, som så udnyttede en sårbarhed til at afvikle programkode på vedkommendes pc.

En anden form for målrettet tyveri af data kan være bevidste forsøg på at stjæle bærbare pc'er, som man ved indeholder værdifulde oplysninger. Der kendes ikke til sager, hvor tyvene med vilje har gået efter bestemte personers computere. De typiske sager med stjålne pc'er er af typen, hvor ejeren har glemt pc'en i en bil, hvorefter en tyv har brudt ind og stjålet den uden at vide, hvem ejeren var.

Identitetstyveri

Identitetstyveri består i, at en svindler giver sig ud for at være en anden. Det kan bruges til at bestille varer i offerets navn. Som regel indebærer identitetstyveri, at svindleren skaffer sig kendskab til fortrolige oplysninger om offeret: Cpr-nummer, bankkontooplysninger, kreditkortnummer og lignende. Svindleren kan få fat i informationerne via phishing eller ved at hacke sig ind på it-systemer, hvor de opbevares. Endelig kan oplysningerne også komme i hænderne på uvedkommende, hvis backupbånd forsvinder under transport eller en bærbar pc bliver stjålet.

Vi venter en stigning i antallet af identitetstyverier de kommende år. Det skyldes, at stadig mere af vores identitet er tilgængelig online. Dermed bliver det også lettere for uvedkommende at få fat i personfølsomme oplysninger.

En anden trend, der er beslægtet med identitetstyveri, er tyveri af virtuel ejendom. Det kan fx gå ud over ejendele, som folk har købt eller tilkæmpet sig i et online rollespil. I 2007 så vi et mindre eksempel på det, da en superbrugers konto på webstedet Netstationen blev hacket. Bagmanden udnyttede kontoens privilegier til at få adgang til andres dele af Netstationen. Flere brugere hævder, at de har fået stjålet ejendele fra deres virtuelle "lejligheder" i systemet.

Identitetstyveri – en case

I oktober blev en 24-årig dansk studerende offer for identitetstyveri, da det lykkedes udenlandske hackere at få adgang til hans personlige oplysninger, såsom navn, adresse og dankortinformationer. De blev brugt til at oprette og betale et domæne og webhotel hos en dansk udbyder. Herefter brugte hackeren domænet til at hoste en phishing-side, der udgav sig for at være fra PayPal.

Dette er det første kendte eksempel i Danmark på, at identitetstyve opretter et domæne i et offers navn.

Hacktivisme

Oven på "Muhammedkrisen" i 2006 fulgte en række religiøst motiverede defacements (webgraffiti) af danske websider (Figur 8). De fleste af disse angreb ramte mindre organisationers og privates hjemmesider på dårligt beskyttede webhoteller og var fra et samfundsperspektiv forholdsvis uskyldige. Angrebene var efter al sandsynlighed, ligesom urolighederne i Mellemøsten, der opstod som følge af Jyllands Postens tegninger, hverken organiserede eller koordinerede.

Figur 8. Eksempel på Muhammed-defacement (webgraffiti).

Det synes gennem de seneste år at være blevet lettere at opnå tilslutning og finansiel opbakning til en aktuel "sag", hvad enten det drejer sig om dyrevelfærd, global opvarmning eller naturkatastrofer, både herhjemme og i udlandet Det må derfor også forventes, at de mere yderliggående synspunkter, hvad enten de er religiøst, etisk eller politisk betinget, globalt set kan finde opbakning, og bruge internettet som medie for deres aktioner. For eksempel var angrebet mod den lettiske infrastruktur i april og maj 2007 betinget af politiske motiver.

Rabiate dyreværnsaktivister, abortmodstandere, menneskerettighedsforkæmpere, miljøforkæmpere med flere har tidligere globalt set udvist adfærd i strid med gældende lovgivning. For eksempel har amerikanske abortmodstandere flere gange slået læger ihjel, som udførte aborter. Herhjemme har vi set "befrielsesaktioner" på danske minkfarme.

Hvis ovenstående grupperinger kan finde økonomi og/eller kompetence, er det ikke utænkeligt, at de religiøst og politisk motiverede angreb flytter på nettet, hvor det er muligt at ramme organisationer globalt, der ikke følger gruppens etiske kodeks. Det kunne for eksempel være storstillede DDOS-angreb på danske hospitaler, der udfører aborter, danske pelsvirksomheder samt organisationer, der måske uforvarende benytter børnearbejdere eller benytter ikke-FSC-certificeret træ i produktionen af deres produkter.

Finansiering af politisk aktivisme gennem it-kriminalitet

På samme vis som den organiserede kriminalitet er flyttet på nettet, er det tænkeligt, at en større del af finansieringen af ulovlig politisk aktivitet i fremtiden flytter på nettet. På nettet kan de politisk motiverede kriminelle agere internationalt med mindre risiko for at blive opdaget og fanget end ved de "traditionelle" bankrøverier, som eksempelvis Blekingegadebanden benyttede sig af. At straffen i flere lande er væsentlig mindre for it-kriminalitet end for bankrøverier, er blot endnu et incitament for at gøre finansieringen af oprørs- og terrorbevægelsers aktiviteter elektroniske.

Det forventes ikke, at den politisk motiverede berigelseskriminalitet vil fremgå særskilt af statistikkerne, da mål og midler vil være de samme som ved den aktivitet, vi ser i dag. Eneste forskel vil være, hvordan pengene i sidste ende benyttes.

It-sikkerhed nu og i fremtiden

It-sikkerhed har altid handlet om at beskytte sine systemer i forhold til grænsefladerne mod omverdenen. I de senere år har organisationerne som følge af den af teknologiske, organisatoriske og lovmæssige udvikling fået flere og mere komplekse grænseflader. Nedenfor skitseres problemstillinger i forhold til de grænseflader, der i dag kan identificeres:

- Grænsefladen mellem organisationen og privatlivet. I dag medbringer ansatte, besøgende og konsulenter i organisationerne databærende medier i form af mobiltelefoner, USB-nøgler, musikafspillere med mere. Nogle af disse medier kan tilgå organisationens netværk, hvad enten det er kablet eller trådløst. Heri ligger ikke blot en risiko for kompromittering af organisationens fortrolighed ved mangelfuld kontrol med, hvilke medier der kan tilgå hvilke ressourcer hvordan, men også risikoen for distribution af skadelige programmer til organisationens systemer. Læs mere i det følgende afsnit.
- Et andet aspekt af de flydende grænser mellem organisationen og privatlivet er hjemmearbejdspladser med adgang til organisationens systemer. De fleste af dem benyttes, ud over arbejde, også til spil, web surfing, download af musik mm. Hvis den ansatte finder det bekvemt at opsætte et trådløst netværk i hjemmet, vil han/hun gøre det uden hensyntagen

til organisationens politik på området. Organisationen kan således blive sårbar for angreb fra en kompromitteret hjemmearbejdsplads, hvad enten det er som følge af mangelfuld konfiguration, uhensigtsmæssig brug eller et ikke sikret trådløst netværk.

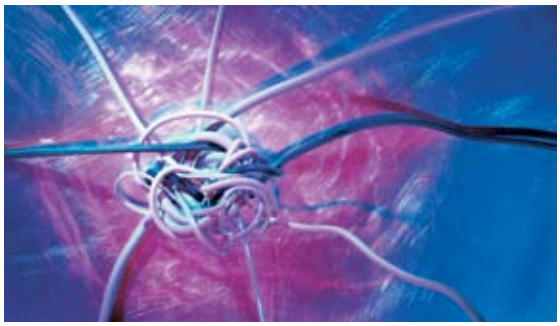
- Grænseflader til lovgivningen. I takt med at organisationerne transporterer og lagrer stadig flere data elektronisk, er Datatilsynets bekendtgørelser blevet aktuelle for flere. I tillæg hertil kommer indførelse af nye love. Flere organisationer har i dag grænseflader mod eksisterende og kommende lovgivning, som de bliver nødt til at tage stilling til.

- Grænseflader mellem organisationer. Som følge af fokusering på de elementer i værdikæden, som tilfører værdi, er brugen af eksterne konsulenter og outsourcing af it-aktiver blevet almindeligt. Heri åbnes for mulige brud på organisationens fortrolighed, hvis ikke det klart defineres, hvilke ressourcer konsulenten skal have adgang til, hvordan han må benytte dem og hvornår. Den samme problemstilling kompliceres yderligere, når ansatte i den organisation, som driften af it-systemerne er outsourcet til, for at kunne udføre deres arbejde, har hel eller delvis adgang til organisationens data.

- Grænseflader mellem it-systemer. Siden årtusindskiftet har blandt andet brugen af web-services muliggjort integration af it-systemer både internt og på tværs af organisationerne. En serviceorienteret it-arkitektur er blevet reglen snarere end undtagelsen, og kunders og leverandørers it-systemer kommunikerer gennem hele forsyningskæder. Herved åbnes der potentielt for, at kompromitterede eller fejlbehæftede it-systemer i én organisation kan få afgørende betydning for tilgængeligheden eller fortroligheden af data i en anden organisations it-systemer.

Nogle af ovenstående problematikker kræver organisatoriske og/eller kontraktlige tiltag, mens andre kræver tiltag af mere teknisk karakter. Fælles er dog, at man i organisationerne er nødt til at være sig problemstillingerne bevidst og udstikke retningslinier for, om og hvorledes de skal håndteres.

På teknologisiden vil vi opleve flere integrerede produkter. Filtrering af skadelige programmer og anden ondsindet trafik vil i højere grad foregå både centralt på klient- og serverniveau og decentralt på firewallniveau. Derudover vil vi opleve intelligent overvågning af uregelmæssigheder på såvel klienter som netværk, som det eksempelvis kendes fra telefonselskabers, bankers og kreditkortselskabers løsninger til opdagelse af svindel.



Sikring af og mod mobile enheder

En mobil enhed kan være en bærbar pc, musikafspiller, mobiltelefon eller USB-nøgle. Fælles for dem er, at de jævnligt befinder sig uden for organisationens trygge mure: De følger med, når deres ejer er på kundebesøg, på rejser, eller blot tager noget arbejde med hjem. Derfor bliver de udsat for påvirkninger, som pc'erne inde bag organisationens firewall aldrig oplever. Selve det faktum, at de er mobile, stiller særlige sikkerhedskrav til dem.

En konsekvens af mobiliteten er, at de mobile enheder er i større fare for at blive stjålet. En mobiltelefon kan blive listet op af en jakkelomme eller taske, og en bærbar pc kan blive stjålet fra bagsædet i en parkeret bil. Hvis det sker, indebærer det flere sikkerhedsproblemer. Fortrolige data på enheden kan komme i de forkerte hænder. Og enheden giver måske mulighed for at koble sig op på firmaets netværk, hvis ejeren har gemt de adgangskoder, han skal bruge til at logge ind.

Mobile enheder, som ikke tilhører organisationen, kan udgøre en sikkerhedstrussel. En gæst kan medbringe en bærbar pc og i et ubemærket øjeblik slutte den til et netværksstik i væggen. Selvom gæsten ikke har ondt i sinde, kan han uafvidende volde skade, hvis hans pc er inficeret med virus.

En anden mobil sikkerhedsrisiko ligger i trådløse netværk. Hvis en udsendt medarbejder kobler sin bærbare til et trådløst netværk på et hotel eller en cafe, kan kommunikationen aflyttes. Det kan man beskytte sig mod ved kun at koble sig op mod netværk, der er beskyttet med kryptering.

Men der er stadig den risiko, at en angriber sætter en basestation op, der giver sig ud for at tilhøre det lokale trådløse netværk, for eksempel ved at bruge et netværksnavn, der lyder tilforladeligt. Så hjælper det ikke noget, at kommunikationen er krypteret, når al kommunikation går gennem hackerens computer.

Det er let at udveksle data ved hjælp af små USB-nøgler. Det indebærer en risiko for, at fortrolige data, der er omfattet af organisationens sikkerhedspolitik, kopieres over på ubeskyttede enheder.

En anden risiko ved USB-nøglerne er, at man aldrig ved, hvor de har været før. Hvis en USB-nøgle har været gennem en virus-inficeret pc, kan den være inficeret. Så risikerer efterfølgende brugere også at blive inficeret.

Virus og andre skadelige programmer har foreløbig primært været rettet mod traditionelle computere. Men der er de senere år også dukket viruslignende programmer op, som inficerer mobiltelefoner. Langt de

fleste af dem kræver dog aktiv medvirken fra ejeren: Man skal sige ja tak til at modtage en fil, før man bliver inficeret. I november 2005 kendte antivirusfirmaet F-Secure til 83 virus rettet mod mobiltelefoner med Symbian-styresystem og to til Windows Mobile[26]. Ingen af dem har fået nogen større udbredelse.

26 http://www.techworld.com/security/features/index.cfm?featureid=1926&pagtype=samecatsamechan "Busting the botnet-herders, an interview with virus expert, Mikko Hyppönen," Computerworld US, November 2005

Der er altså flere sikkerhedsproblemer, som dukker op, når it bliver mobil. En teknologi, der kan være med til at løse sikkerhedsproblemerne, er kryptering. Hvis man krypterer data på en mobil enhed, vil uvedkommende ikke kunne få adgang til dem, hvis de ikke kan gætte koden til krypteringssystemet.

Der findes også særlige løsninger til sikring af mobile enheder. De gør det for eksempel muligt at slette indholdet på en enhed, hvis den bliver stjålet.

Stadig mere it-udstyr bliver mobilt. Derfor er det vigtigt, at organisationers og organisationers it-sikkerhedspolitik dækker mobile enheder. Den kan for eksempel indeholde regler om, hvilke typer data det er tilladt at kopiere til mobile enheder, og hvordan de skal beskyttes. Der kan også være krav til, hvordan kommunikation udefra må foregå, for eksempel om medarbejderne må anvende offentligt tilgængelige trådløse netværk. Endelig skal der være regler for brugen af udstyr udefra på organisationens eller organisationens interne netværk, for eksempel når konsulenter medbringer bærbare pc'er.

Endvidere er der behov for tekniske løsninger, der gør det muligt at kontrollere, at it-sikkerhedspolitikken overholdes – også på dette område

Lovgivningens krav til it-sikkerhed

Lovgivningen er i stigende grad noget, som organisationerne bliver nødt til at være bevidste om og forholde sig til i implementeringen af deres it-sikkerhedsforanstaltninger.

Den 1. juli 2000 afløste "Lov om behandling af personoplysninger" tidligere lovgivning om registrering af persondata. Loven dækker områder som indsamling, opbevaring og behandling af personoplysninger. Den har relevans for alle offentlige såvel som private organisationer, der behandler oplysninger om danske borgere. Tilsvarende har anden lovgivning, eksempelvis terrorlovens logningsbekendtgørelse, der trådte i kraft den 15. september 2007, pålagt danske organisationer at følge regler, der har direkte relevans for it-driften og dermed sikkerheden. Senest er det som følge af folketingsbeslutning B 103 om anvendelse af åbne standarder i det offentlige blevet pålagt statslige organisationer pr. 1. januar 2008 at oprette en sikkerhedspolitik, der skal følge standarden DS 484[27].

Lovgivningen påvirker således ikke blot, hvordan vi opbevarer data og hvilke, men har i nogle tilfælde også direkte indflydelse på de interne procedurer og foranstaltninger, der skal sikre, at det overholdes og kan dokumenteres.

Efter en række amerikanske regnskabsskandaler i 2001 blev Sarbanes-Oxley-loven (SOX) den 30. juli 2002 vedtaget. Loven blev gennemført for at genoprette offentlighedens tillid til den regnskabsmæssige rapporteringsproces. Den medførte skærpede krav til børsnoterede amerikanske selskabers måde at udføre revision på. SOX har for danske organisationer betydet at de, selvom de ikke selv er dækket af loven, har kunnet blive pålagt at følge den af deres amerikanske kunder eller leverandører.

27 http://www.itst.dk/it-sikkerhed/ds-484

Med EU-parlamentets vedtagelse af tilføjelser til EU's 4., 7. og 8. selskabsdirektiv, også kendt som Eurosox, skal EU-landene senest i juni 2008 implementere national lovgivning. Det betyder at organisationerne skal vise gennemsigtighed og åbenhed om finansielle transaktioner og implementere interne kontrolsystemer i henhold til god selskabsledelse (corporate governance)[28]. I modsætning til den amerikanske lovgivning er Eurosox baseret mere på principper end på regler, hvorfor forventningerne ifølge The Eurosox Institute[29] er, at omkostningerne ved at være i overensstemmelse med Eurosox bliver mindre, end de amerikanske organisationer har erfaret med SOX.

Eurosox pålægger selskaber registreret på de europæiske børser at offentliggøre deres risikostyringsaktiviteter i årsrapporten. Den skal indeholde et særskilt kapitel om ledelsens ansvar, herunder[30]:

- Beskrivelse af grundelementer for risikostyringen.
- Beskrivelse af interne kontrolforanstaltninger.
- Undtagelser relateret til nationale regler.
- Beskrivelse af organisationens kodeks for god selskabsledelse.

Synliggørelse af risikoanalyse og -styringsaktiviteter må forventes på sigt at få positive konsekvenser for organisationernes udfærdigelse og efterlevelse af it-sikkerhedspolitikker. Det vil føre til et højere it-sikkerhedsniveau. Indførelsen af Eurosox vil således skærpe ledelsens interesse for it-sikkerhed og flytte fokus fra teknologi til god selskabsledelse, som tilfældet ifølge en amerikansk undersøgelse[31] har været efter indførelsen af SOX.

Afledt af både lovmæssige og forretningsmæssige krav til it-driften er it governance blevet et begreb, som flere og flere organisationer forholder sig til. Hvordan sikres, at organisationen til hver en tid kan dokumentere, at den overholder loven samt leverandørens eller kundens krav til gældende standarder? Med erfaring fra corporate governance-bølgen, som siden årtusindskiftet er skyllet gennem de større organisationer, synes it governance at være svaret.

Awareness om organisationens it-sikkerhedspolitik

I dag har mange organisationer implementeret it-sikkerhedspolitikker, og det er ikke længere et problem for organisationer at få udformet it-sikkerhedspolitikken. Der findes flere danske organisationer, som tilbyder tilpassede it-sikkerhedspolitikker til organisationen.

Problemet består i at få implementeret it-sikkerhedspolitikken i organisationen og få videreformidlet politikken til medarbejderne og sikre overholdelse af den. Organisationens it-sikkerhedspolitik er ikke korrekt implementeret i organisationen, før disse parametre er udført. Det er således en vigtig udfordring for organisationen at nå fra teori til praksis. Det betyder, at alle niveauer i organisationen har et ansvar for at få implementeret it-sikkerhedspolitikken helt ned til slutbruger-niveau. Awareness til slutbrugere er vigtig, da disse i stigende grad bliver ofre for it-kriminalitet og ofte er ansvarlige for at håndtere fortrolige data. En

28 http://www.dansk-it.dk/netvaerk/4_typer_netvaerk/kompetence_netvaerk/eurosox_compliance.aspx
29 http://www.eurosox.dk/
30 http://www.grccontrollers.com/files/Overreach.doc
31 [CSI/FBI, 2007] 2007 CSI/FBI Computer Crime & Security survey

amerikansk undersøgelse[32] viser, at 71 procent af de adspurgte amerikanske organisationer mener, at awareness-træning om organisationens it-sikkerhedspolitikker har høj prioritet. Det viser, at der eksisterer en viden hos organisationer om behovet for at oplyse deres medarbejdere. Det synes derfor som et naturligt næste skridt, at organisationen underviser dens medarbejdere i it-sikkerhedspolitikken og lærer dem at være kritiske over for behandling af data og i omgangen med it-systemer. Der findes allerede tilrettelagte undervisningsforløb, som informerer brugere om implementeringer af it-sikkerhedspolitikker i organisationer. Det vil være en god indsats for organisationen at lade dens brugere følge sådanne kurser for at opnå en sikring af, at brugerne er bekendte med, hvordan de skal overholde it-sikkerhedspolitikken.

I 2007 er der set flere eksempler på ansatte, som sløser med personfølsomme informationer ved enten at sende oplysninger ukrypteret eller lægge følsomme oplysninger på organisationens websted, så det er nemt for uvedkommende at tilgå denne information. Hvis organisationer sørger for at have restriktive politikker om personfølsomme data og kommunikere til deres medarbejdere, hvordan de skal behandle sådanne data, vil de have mulighed for at kunne påvirke medarbejderes håndtering af data. Organisationen har i sidste ende over for lovgivningen ansvaret for at sikre data.

Bekæmpelse af botnets

Der kan i fremtiden forventes en videre udvikling af de metoder, som botnets benytter til at sprede sig. Flere applikationer ud over browsere vil blive benyttet til at inficere brugeres computere med bots. Dette ses allerede via Instant Messaging (IM) netværk (chat), hvor orme spreder sig via links eller vedhæftede filer i f.eks. MSN Messenger. De vigtigste midler til bekæmpelse af botnets er overvågning af spredningsmetoderne og at få udbredt forståelsen for, hvordan botnets udbredes.

For at bekæmpe udbredelsen af botnets skal almindelige internetbrugere oplyses om risikoen for, at deres computere kan blive optaget i botnets, hvis systemet ikke er opdateret med de seneste programrettelser. Sker det ikke, vil udbredelsen af botnets ikke kunne forhindres[33]. Internetbrugere har behov for vejledning i, hvad de skal være opmærksomme på, og hvordan de skal reagere, hvis deres computer bliver inficeret med botnet-kode. Flere undersøgelser viser, at brugere ikke mener, at udefrakommende indtrængen på deres computere er et stort problem, men at spyware, virus og orme mv. er en større trussel, som for det meste kan bekæmpes med antispyware- og antivirusprogrammer. Men ikke alle virusser og spyware-programmer fanges af filtrene[34]. Det er derfor vigtigt at lave oplysningskampagner, som når ud til disse brugere. Kampagnerne skal beskrive, at der lurer større trusler på internettet.

Ligeledes er der set en tendens sidst på året til, at danskere efterlyses til at hvidvaske penge. Sådanne forespørgsler udsendes via junkmails. Det sker typisk ved at sende pengene fra Danmark til et andet land. Det er vigtigt at oplyse internetbrugere om, at det er ulovligt, og de kan risikere at blive bedraget ligesom ved phishing.

32 [CSI/FBI, 2007] 2007 CSI/FBI Computer Crime & Security survey
33 http://www.microsoft.com/protect/computer/viruses/zombies.mspx
34 http://www.commtouch.com/site/ResearchLab/virusLab/recent_activity.asp

Opsamling

Hændelserne i 2007 viser, at angrebene på it-sikkerheden kommer over en bred front. Derfor er det vigtigt at forberede sig på mange forskellige typer angreb. Den hellige gral er ikke velforvaret, selvom man har antivirus og firewall – skønt begge dele bestemt er nødvendige. DK•CERT anbefaler, at man prioriterer indsatsen på disse områder:

- Opdatering og beskyttelse af servere og centrale systemer.
- Opdatering og beskyttelse af brugernes pc'er.
- Opdatering og beskyttelse af systemer der kan nås fra internettet, herunder især web-applikationer og databaser.
- Beskyttelse af og mod mobilt udstyr (mobiltelefoner, bærbare pc'er, USB-nøgler, medieafspillere og lignende).
- Kryptering af forretningskritiske data og kontrol med adgang hertil.
- Løbende kontrol og overvågning af de tekniske beskyttelsesforanstaltninger, for eksempel ved scanninger og penetrationstest.
- Implementering og udbredelse af it-sikkerhedspolitiken i hele organisationen.
- Løbende revision af it-sikkerhedspolitiken og risikostyringsaktiviteterne angivet heri.
- Uddannelse og information om it-sikkerhed til brugerne.

Ordliste

applikation: Et eller flere programmer, der løser en opgave for computerens brugere.

botnet: 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 indgår i botnettet. Angriberen udnytter gerne sine robotter til at foretage koordinerede ude-af-drift-angreb eller udsende spam.

denial of service, DoS, DDoS, ude-af-drift: Et denial of service-angreb er et angreb, der har til formål at blokere for adgang til et givent system, for eksempel en webside. Et distributed denial of service (DDoS)-angreb udføres ved, at flere computere (ofte flere tusinder) bombarderer en webside med forespørgsler eller data i en mængde så stor, at serveren bag websiden ikke kan følge med og går ned.

DS 484: Dansk standard for it-sikkerhed.

FTP-server: Server til overførsel af filer, eksempelvis til upload af websider. FTP-serverprogrammet kører som regel på TCP-port 21.

kryptering: En metode til at kode information ved hjælp af en nøgle. Kun med den rigtige nøgle kan man afkode informationen og dermed læse den. Kryptering bruges til at sikre fortroligheden af informationer, der sendes over usikre netværk (såsom internettet).

organisation: En virksomhed, offentlig myndighed, forening eller anden sammenslutning.

orm: Et program, der spreder sig i netværk ved at udnytte sårbarheder i dets computere. I TCP/IP-verdenen sker det typisk ved, at ormeprogrammet kontakter den port, som det sårbare program lytter på.

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

system: En kombination af computerudstyr og programmer, der til sammen udfører en eller flere opgaver for brugerne.

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.

virus: Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres virusen, og den inficerer andre programfiler.

zero-day exploit: et angrebsprogram, der udnytter en sårbarhed, som hidtil har været ukendt, og som der derfor ikke findes rettelser til.

zero-day angreb: et angreb, der udnytter en sårbarhed, som hidtil har været ukendt, og som der derfor ikke findes rettelser til.

Kontakt:

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

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