Handelshögskolan
VID GÖTEBORGS UNIVERSITET
Institutionen för informatik

2005-06-13

Malware-relaterade kostnader för offentlig sektor

Abstrakt:

Malware är mjukvara som beter sig på ett för användaren oönskat sätt. Virus, trojaner och maskar kan orsaka stora skador i organisationer som är beroende av datorer och fungerande datakommunikation. Den offentliga sektorn är sårbar beroende på konceptet med öppenhet och en 24-timmarsmyndighet som ständigt ska vara tillgänglig för medborgarna. Uppsatsens syfte var att undersöka vilka kostnaderna är för att skydda offentlig sektor mot malware och hur viktigt det är att den skyddas. Undersökningen byggdes på litteraturstudier samt statistik från Sveriges IT-incidentcentrum, Statskontoret och Statistiska Centralbyrån. Slutsatsen som drogs är att kostnaderna är avsevärda. Kostnaderna kan delas in i fyra kategorier: tekniska skydd, utbildning, förändrade rutiner och ökad belastning på myndigheter. Skyddet är viktigt eftersom den offentliga sektorn är sårbar och fyller viktiga samhällsfunktioner.

Nyckelord: offentlig sektor, malware, virus, trojaner

Författare: Robert Karlsson
Handledare: Mathias Klang
Examensarbete I, 10 poäng

Innehållsförteckning

Inledning

Alla organisationer och individer som använder sig av datorer riskerar att drabbas av virus eller andra former av illasinnad kod. Är datorerna dessutom uppkopplade mot Internet ökar risken att drabbas. Vad kostar det för den offentliga sektorn att skydda sig mot dessa angrepp och hur dyrt kan det bli om man misslyckas?

Malware

Malware är den gängse termen för programvara som, med eller utan avsikt, orsakar skada på datorutrustning, nätverk eller data. Uttrycket kommer från engelskans **mal**icious soft**ware**, det vill säga ondsint eller skadlig mjukvara. Malware finns av många olika typer med olika egenskaper och ursprung. Följande kategorier brukar räknas som malware:

- Virus, maskar och trojaner
- Spyware och Adware
- Bakdörrar i applikationer och operativsystem
- Oavsiktliga fel i applikationer och operativsystem

Malware är alltså ett brett begrepp som kan sägas innefatta all mjukvara som på ett eller annat sätt kan vara skadlig för system, ägande organisation eller användare.

Hur skadar malware?

Malware kan skada en organisation på tre huvudsakliga sätt:

- Förlust (radering) av information
- Stöld/spridning av känslig information
- Minskad tillgänglighet till datorsystem

Olika organisationer drabbas olika hårt av de tre skadekategorierna. En organisation som handhar konfidentiella uppgifter drabbas t.ex. hårdare av informationsläckor än en organisation som har till uppgift att sprida information. Om skadan består i minskad tillgänglighet eller total utestängning från systemet är det istället den informationsspridande organisationen som drabbas hårdare. Alltså måste organisationens skydd mot malware anpassas efter funktion och behov.

Hur skyddar man sig?

Det är svårt eller kanske till och med omöjligt att upprätthålla ett totalt skydd mot malware. Malware kan komma in i systemet över nätverksanslutningar, på flyttbara media eller till och med direkt genom tangentbordet från en illasinnad användare. Det senaste alternativet är kanske lite långsökt och om personalen är en så påtaglig säkerhetsrisk kan man nog räkna med större problem än malware i organisationen. Man måste alltså bestämma sig för hur långt man ska gå i sin kamp mot den illasinnade mjukvaran och vad man är beredd att offra för att uppnå den säkerhetsnivå man eftersträvar.
Naturligtvis kan man använda sig av tekniska hjälpmedel som virusscanners, brandväggar och begränsningar av normalanvändarens rättigheter på systemet, men kompromisser måste göras för att bibehålla systemets användbarhet. Målsättningen blir därför att åstadkomma ett godtagbart skydd, ett skydd som täcker så många risker som möjligt utan att kosta för mycket i pengar, resurser eller användbarhet. De tekniska delarna av skyddet bör kompletteras med utbildning av användarna och tydliga policys och rutiner angående användning av systemet.

Som komplement till skyddet mot malware måste dessutom beredskap finnas för återställande av systemet för de fall när malware tar sig förbi skyddet eller andra hot slår ut datorerna.

Kostnader

Kostnaderna kan delas upp i två huvudkategorier, dels de kostnader som uppstår när den illasinnade koden tar sig in i systemet och orsakar skador, dels vad de skyddsåtgärder man vidtar kostar.

Vad kostar skadorna?

Kostnader för skadorna som malware kan åstadkomma:

- Återställande av system
- Återskapande av förlorad information
- Förlorad arbetstid när systemet är nere
- Återuppbyggnad av förtroende för organisationen

Att återställa ett kraschat system kan innebära en liten kostnad jämfört med värdet på förlorad information, förlorad arbetstid eller minskat förtroende efter en attack mot organisationens tillgänglighet.

Vad kostar det att skydda sig?

Kostnader för att upprätthålla ett godtagbart skydd:

- Virusskydd
- Backup-system och -rutiner
- Utbildning i säkert användande av datorer

Virusskydd medför licenskostnader och underhåll. Backup-system kostar pengar och resurser. Att utbilda användare i hur de ska använda sina datorer på ett säkert sätt kostar tid och pengar. Dessutom finns det ingen garanti för att tekniken håller måttet eller att användarna gör som de blir lärda.

Offentlig sektor

Till den offentliga sektorn räknas all produktion av varor och tjänster som bedrivs av stat, landsting och kommuner och till största delen finansieras med skatter. Den offentliga sektorn i Sverige är stor jämfört med andra länder. Ca 35% (1 345 972 st.) av landets förvärvsarbetande är anställda inom offentlig sektor (SCB, 2005c). Kostnaderna för den offentliga sektorn är bland de högsta i världen sett i relation till BNP.
För den offentliga sektorn gäller andra förhållanden än för den privata. Öppenhet, tillgänglighet och andra lönsamhetskrav är de största skillnaderna.

Offentlighet

Inom den offentliga sektorn finns regler som ska följas angående öppenhet och tillgänglighet för allmänheten. Dessa regler kan göra det svårare att skydda organisationerna mot malware. Öppenheten kan ha den positiva effekten att organisationerna kan söka extern hjälp och anmäla eventuella brott utan att tyglas av den försiktighet som råder inom den privata sektorn där man ogärna erkänner svagheter i sina systems säkerhet.

Kostnader

Alla offentliga verksamheter har krav på sig att hålla sin budget i balans, det vill säga hålla utgifterna på en nivå som inte överstiger inkomsterna. Det innebär att om kostnaderna för att skydda organisationen mot malware ökar, måste man dra ner på andra utgifter inom organisationen. Eftersom offentliga organisationer finansieras till största delen med skattemedel kan kostnader relaterade till malware i slutändan annars innebära ett ökat tryck på skattebetalarna.
Offentliga organisationer köper varor och tjänster, t.ex. antivirusprogram och IT-expertis, från privata och offentliga leverantörer (NOU, 2002). All sådan upphandling styrs av lagen om offentlig upphandling – LOU. Grundläggande i LOU är att upphandlingar ska ske på ett affärsmässigt och rättvist sätt så att de lämpligaste leverantörerna kan väljas utan att orättvisa hänsyn tas till tidigare kontakter eller geografisk närhet.

Kostnader för skador

Offentliga organisationer hanterar ofta känsliga uppgifter som kan orsaka svårberäknade kostnader om de läcker ut eller förstörs så att de måste återskapas. Exempel är patientjournaler och andra personuppgifter. Om medicinskt viktiga uppgifter förstörs eller korrumperas kan kostnaderna till och med innefatta människoliv!

Avgränsningar

För att hålla arbetets omfång inom rimliga gränser och koncentrera min arbetsinsats har jag valt att inte behandla följande typer av malware:

- Oavsiktliga fel i applikationer och operativsystem som får negativa konsekvenser
- Avsiktliga, dolda fel i applikationer och operativsystem (bakdörrar)
- Adware
- Spyware

Min avsikt med uppsatsen är inte att ta fram exakta summor i kronor och ören, utan snarare att ge en bild av problemets natur och storlek. Jag vill veta om malware är ett stort problem och hur förhållandet mellan kostnaderna för skyddet mot malware relativt de skador man riskerar .

Frågeställning

Den offentliga sektorn utsätts, som alla andra organisationer och individer som använder datorer, för ständiga risker för skada åsamkad av malware.
Vilka är kostnaderna för att skydda offentlig sektor mot malware och hur viktigt är det att den skyddas?

Teori

Här ges en introduktion till vad malware är, hur det fungerar och varför det kan vara ett problem för den offentliga sektorn.

Malware – illasinnad kod

Det engelska uttrycket malware täcker in alla program som är konstruerade med avsikt att på något sätt skada.
Malware brukar delas upp i kategorier efter programvarans egenskaper. Tre av de vanligaste kategorierna är virus, trojaner och maskar. Var och en av dessa kategorier diskuteras nedan. Notera att det råder viss oenighet om definitionerna och vilka företeelser som ska räknas till vilken kategori. Extremfallet är att i stort sett all kod med av användaren oönskad funktionalitet sägs vara virus, medan andra definitioner är oeniga om det ska krävas ont uppsåt för att koden ska sägas vara illasinnad eller om det är kodens effekt som är avgörande. Gemensamt för virus, trojaner och maskar är att de, även om de inte har någon direkt skadlig effekt, kan anses stjäla resurser som nätverkskapacitet, processorcykler och minne, eftersom de ofta transporteras och / eller exekveras utan systemets ägares tillstånd.

Virus

Virus är kod som infekterar ett värdprogram och lever i ett parasiterande förhållande med det infekterade programmet. Virus kan dessutom infektera sektorer på hårddisken, t.ex. bootsektorn som datorn startar upp ifrån (Symantec, 2004). Kännetecknande för virus är att de sprider sig genom att infektera andra program med kopior av den illasinnade koden. Virus kan alltså sprida sig på egen hand. Den biologiska hänvisningen i beteckningen virus kommer från virusets förmåga att föröka sig på ett sätt som påminner om levande organismer.
När det infekterade programmet exekveras kan viruskoden ta kontrollen och utföra helt andra instruktioner än vad programmet i vanliga fall gör, t.ex. radera slumpmässigt valda filer eller kopiera sig själv till andra programfiler (Haynes, 1992). Ett virus förmåga att sprida sig kan hindras av dess egen förmåga till förstörelse, därför är det vanligt att virusprogrammeraren lägger in funktioner som fördröjer eller minskar omfånget av skadan.
Man diskuterar också möjligheten till godartade virus som skulle kunna sprida sig mellan datorer och t.ex. installera nya säkerhetspatchar eller laga skador orsakade av andra virus.

Trojaner

Trojaner eller trojanska hästar är namngivna efter den trähäst som användes för att smyga in fientliga soldater i Troja. Hästen lämnades som en gåva utanför staden och togs in som en trofé innanför stadsmurarna. På natten smög sig soldaterna ut och anföll staden inifrån.
En trojansk häst är alltså ett program som ser lockande och ofarligt ut, men när du har installerat det innanför dina försvarsmurar kan det bete sig på ett annat sätt än vad du förväntar dig. Trojanen kan t.ex. öppna säkerhetshål mot Internet eller på annat sätt skada din dator eller information som finns lagrat på den (Haynes, 1992).
En trojan saknar förmåga att sprida sig själv och är därför beroende av godtrogna användare som sprider den mot bättre vetande. Den förekommer ofta i form av ett litet skämtprogram eller som en trevlig skärmsläckare som sprids mellan godtrogna datoranvändare (Symantec, 2004). Trojanen kan också spridas med hjälp av en mask som bär den med sig.

Maskar

En mask är ett program som sprider sig över nätverk på egen hand. Den kryper från dator till dator, ofta utan att användaren behöver hjälpa till eller ens förstå att något har hänt. Masken är i sig ofta ganska ofarlig, men den kan ha virus eller andra skadliga program som last

(payload). Skillnaden mellan en mask och ett virus är främst att masken är ett fristående program som skapar kopior av sig själv medan viruset existerar som ett bihang på ett program och därifrån smittar andra programfiler (Haynes, 1992). Masken kan sprida sig via e-post eller genom att utnyttja någon svaghet i det angripna systemet. En mask som i stor omfattning sprids över ett nätverk kan ta så stora nätverksresurser i anspråk att åtkomsten för legitima program och användare begränsas eller helt hindras.

Syftet med malware

I motsats mot vad många tror är inte längre virusprogrammering något som görs som ett skämt eller experiment av en uttråkad datakunnig yngling. Enligt Krisberedskapsmyndigheten (2005a) sprids 90% av all skadlig kod på Internet med kriminella syften, resterande 10% sprids av så kallade script kiddies. Script kiddies är IT-säkerhetsbranschens föga smickrande namn på individer med små kunskaper som orsakar stor skada med hjälp av de färdiga virusskapande program som finns att ladda ner från Internet.
Enligt Krisberedskapsmyndigheten (2005b) finns det tecken på att organiserade brottslingar börjat intressera sig för informationsteknik och de möjligheter till vinning som den erbjuder.

Skador

Harley, Slade & Gattiker (2001) delar upp skadorna som malware kan åstadkomma i primär och sekundär skada.
Primär skada är den skada som blir resultatet om inget görs för att hindra viruset (eller någon annan form av malware) från att exekvera och utföra de avsedda, skadliga instruktionerna. Det vill säga den skada som avsetts med programmet. Exempel på primär skada är t.ex. förlust av data, minskad tillgänglighet eller kränkt integritet.
Sekundär skada är de negativa effekter som den illasinnade koden kan medföra förutom den direkta, primära skadan, exempelvis resultatet av panikåtgärder som formatering av hårddiskar som blivit infekterade av virus. Andra former av sekundär skada är den sociala risken att bli utpekad som syndabock för vidarespridning av malware, negativa effekter i affärssammanhang (man kan anses inkompetent eller farlig att ha att göra med) och tidsåtgång för scanning, felsökning och återställning av system.
Enligt Haynes (1992) kan illasinnad kod åstadkomma temporära eller permanenta förluster av data, minskad tillgänglighet till data och applikationer lagrade lokalt eller på via nätverk och förlorad kontroll över känsliga eller hemliga uppgifter.

Skada på mjukvara

Mjukvara som skadas kan räknas till de primära skadorna när exekverbara filer blir infekterade med virus eller skadade av andra former av malware, men även sekundära skador är möjliga.
Ett virus som infekterat en programfil går alltid att ta bort, men det är inte säkert att arbetsinsatsen är ekonomiskt försvarbar eller att systemets funktionalitet blir helt återställd. Oftast är det lättare att ersätta det infekterade objektet än att försöka ta bort viruset från det (Harley, Slade & Gattiker, 2001). I allmänhet innebär skador på mjukvara inte att man på nytt måste köpa in programmen, oftast har man möjlighet att göra en ominstallation från backuper eller det media som mjukvaran från början blev levererad på. Trots det kan skadad mjukvara orsaka kostnader eftersom ominstallationen tar värdefull tid. Dessutom kan skadad mjukvara i sin tur orsaka skador eller förändringar på datafiler så att filernas trovärdighet kan ifrågasättas och verifikation krävs.
Så kallade hoaxes, dvs. falska virusvarningar som cirkulerar på nätet, kan lura användare att ta bort viktiga systemfiler eller att på andra sätt skada datorns operativsystem eller applikationer.

Förlorad kontroll över information

Malware kan vara utformade på så sätt att organisationens kontroll över information minskar. Trojaner kan samla lokalt lagrad information och skicka den till destinationer utanför det lokala nätverket, så att känslig eller hemlig information sprids på ett oönskat sätt. I samband med detta kan kostnader uppstå på grund av förlorad hemlig information och kostnader som uppstår när systemets säkerhet ska återställas.
Kostnaderna kan dessutom öka om man räknar in förlorad goodwill och eventuella missnöjda kunder / samarbetspartners som i fortsättningen inte vill riskera sin egen säkerhet genom att vara beroende av en osäker organisation. Risken för förlust av förtroende kan vara en anledning till att företag ofta väljer att inte polisanmäla malware-angrepp, utan istället tystar ner incidenter. Offentliga organisationer har tack vare offentlighetsprincipen inte så många hemligheter att vara rädda om och kan därmed fritt anmäla dataintrång och malware-angrepp.

Skada på information

Information kan skadas på flera sätt. Dels kan informationen gå helt förlorad så att den måste återskapas från noll. Eller så kan informationen korrumperas så att man inte vet säkert vilken information som är tillförlitlig och vilken som är felaktig. Det senare fallet kan vara minst lika skadligt som om informationen försvinner helt, eftersom man måste gå igenom all data för att verifiera dess integritet.

Förlorad tillgång till systemet

Om malware får en organisations hela nätverk att sluta fungera leder det till stora kostnader. Mikalsen & Borgesen (2002) beräknar att genomsnittskostnaden för ett företag med 100 datorer i ett nätverk blir över 100kkr / timme om datornätet är helt oanvändbart. Man säger till och med att de flesta företag riskerar konkurs om datorsystemet är nere i mer än en vecka. Naturligtvis varierar kostnaderna kraftigt mellan olika sorters organisationer i olika branscher, men man kan ändå säga säkert att skador som leder till att hela nätverket blir tillfälligt oanvändbart alltid är kostsamma. När tillfällig otillgänglighet är så dyrt kan man lätt förstå att total förlust av data är att betrakta som katastrof för nästan alla organisationer. Förlorad data kan ta lång tid att återställa, vara dyr att köpa in eller vara helt omöjlig att återskapa.
För offentliga organisationer ser läget annorlunda ut eftersom de oftast inte riskerar konkurs, men myndigheter som tillhandahåller samhällsviktig information och tjänster som är viktiga för allmänheten måste naturligtvis vara tillgängliga.

Skada på hårdvara

Endast i undantagsfall kan malware skada hårdvara. Anledningen till detta är att de normala mjukvaruinstruktioner som alla program (även malware) byggs upp av är utformade på ett sådant sätt att datorns hårdvara inte kan ta skada av dem. Det finns helt enkelt inget vettigt motiv till att implementera instruktioner som kan skada hårdvaran. Undantagen utgörs av de fall där malware kan orsaka extremt slitage av komponenter genom att utföra en i sig oskadlig instruktion onormalt ofta eller under en lång tid.
Virus som angriper datorns BIOS-chip är inte att betrakta som skada på hårdvara eftersom det inte är chipet, utan informationen på det som skadas. Alltså är det att betrakta som skada på information eller mjukvara.

Tekniska motmedel

För att minska riskerna att angripas av malware och minimera skadorna vid ett lyckat angrepp har ett flertal tekniska motmedel tagits fram. Det finns inget helt säkert sätt att skydda sig, men om man använder en kombination av tekniska hjälpmedel, utbildning och förhållningsregler kan man få ner riskerna till en minimal nivå. Vad man eftersträvar är en

proaktiv strategi, dvs. man vill agera innan malware har angripit systemet och göra det mer ogästvänligt för ovälkommen kod. I realiteten blir man dock oftast tvungen att agera reaktivt, dvs. reagera på de angrepp som redan sker (Harley, Slade & Gattiker, 2001).

Antivirusprogram

Antivirusprogram finns av olika typer men de flesta inkluderar en scanner som söker efter kända hot på användarens begäran. Som komplement finns ofta ”change-detection” och ”activity monitor”.

Scanner

En KVS, Known Virus Scanner, är ett program som söker igenom hårddisken efter kända hot (Harley, Slade & Gattiker, 2001). En virusscanner har begränsade möjligheter att hitta illasinnad kod som inte finns med i de mönsterfiler den har tillgång till. Det är därför viktigt att se till att scannern alltid har de senaste mönsterfilerna installerade. En virusscanner placerad på en gateway eller brandvägg kan gå igenom alla nya filer som förs in i systemet, men det är ändå nödvändigt att med jämna mellanrum söka igenom hela filsystemet efter hot som inte upptäcktes då de tog sig in på hårddisken.
Inköpskostnaden för antivirusprogram för en stor organisation kan variera från 0 – 500kr / klient inklusive uppdateringar för ett år framåt (Dustin, 2005). Ytterligare kostnader tillkommer för installation och hantering av programmen. Ofta erbjuder säkerhetsföretagen programpaket med diverse program som ska förbättra säkerheten på organisationens datorsystem.

Checksummor

En annan metod för att upptäcka virus på ett datorsystem är att förse alla filer (eller bara körbara applikationer) med checksummor beräknade på filstorlek eller -struktur, så att man direkt kan se om en fil har ändrats (Harley, Slade & Gattiker, 2001). Om ett virus infekterar en fil kommer filens storlek och eller innehåll förändras så att den beräknade checksumman inte stämmer med den man tidigare beräknat. Viktigt när man använder sig av checksummor är att systemet är rent när man första gången beräknar checksummorna. Checksummor kan implementeras i ett antivirusprogram så att man endast behöver scanna igenom filer som förändrats sen senaste scanningen.

Heuristik

Heuristik eller tumregler är användbara om man vill kontrollera systemet i realtid. Metoden kallas av antivirusbranschen activity monitor, eftersom man övervakar alla aktiviteter på systemet (Harley, Slade & Gattiker, 2001). Man kan konfigurera sitt skydd så att det reagerar och varnar eller avbryter operationen om det upptäcker misstänkt aktivitet. Heuristik kan aldrig bli 100% korrekt eftersom operationer som i en del fall är skadliga i andra fall är precis vad användaren önskar, t.ex. radering av filer eller formatering av hårddiskar. Positiva felidentifikationer är önskade operationer som tolkas som oönskade, negativa felidentifikationer är oönskade operationer (malware) som inte upptäcks. Malware skiljer sig egentligen inte från vanliga program på andra sätt än att de utför operationer som användaren inte anser önskvärda. Det är svårt att i olika situationer veta vad användaren anser vara önskvärt. En operation som vid ett tillfälle är önskad kan i ett annat sammanhang vara förödande, det är detta sammanhang som de heuristiska reglerna ska uppfatta.
Heuristik kan ingå som en komponent i ett antivirusprogram som komplement till scanning och checksummor. Att kontrollera varje instruktion som utförs i realtid resulterar i en viss prestandaförlust eftersom datorns processor belastas utöver sina ordinarie uppgifter. Prestandaförlusten blir knappast märkbar på dagens överdimensionerade kontorsdatorer, men

om man redan utan den heuristiska kontrollen lider av bristande beräkningsresurser kan förlusten bli betydande.

Hårdvarubaserade antivirussystem

Försök har gjorts med hårdvarubaserade antivirussystem. En metod är att implementera skydd mot boot-sector-virus i datorns BIOS-chip. Eftersom virusutvecklingen har rört sig bort från boot-sector-virus är den inte längre så intressant. En annan metod är att installera hårdvara som scannar all nätverkstrafik in och ut ifrån datorn och filtrerar bort alla hot efter jämförelser mot en aktuell databas. Metoden har prövats men invändningar har gjorts angående prestandaförluster och kostnader jämfört med mjukvarubaserade ”activity monitor”-system (Harley, Slade & Gattiker, 2001).

Brandvägg

En brandvägg kan ge ett visst skydd mot maskar och kan dessutom se till att trojaner och andra hot inte kan kommunicera ut på Internet och sprida privata eller konfidentiella uppgifter utan användarens vetskap. Cheswick, Bellovin & Rubin (2003) jämför en Internetansluten dator utan brandvägg med nakenbad: det ger en extra frihetskänsla, men kan också innebära risker. De rekommenderar bara att man prövar detta på extremt säkra klientdatorer om man vet vad man gör. Brandväggar finns både som skydd för ett helt nätverk och som mjukvara som skyddar en enskild dator. Priserna för fristående brandväggar varierar mycket beroende på kapacitet och funktioner. Personliga brandväggar finns från 0 – några hundra kronor per klient (Dustin, 2005).
Kostnaderna för brandväggar kan inte helt räknas till malware-relaterade kostnader eftersom deras syfte ofta inte bara är att skydda mot malware utan att skydda organisationen mot intrång och att hindra kommunikation på otillåtna protokoll.

Backup

Ett fungerande backup-system kan innebära skillnaden mellan ett tillfälligt avbrott i arbetet och total förlust av data. Backuper är viktiga inte bara i malware-sammanhang utan även när dataförluster orsakas av användarfel, sabotage eller andra orsaker. Hela kostnaden för ett backup-system kan därför inte räknas som malware-relaterad.
Haynes (1992) kallar säkerhetskopian för det slutliga skyddet, det vill säga det skydd som finns kvar när allt annat har misslyckats.
Viktiga frågor gällande backup är bland annat: hur ofta och vad ska säkerhetskopieras, hur länge och var ska det sparas, vem ska göra det och när på dygnet. Frågorna besvaras i följande citat: ”A backup-strategy should be devised so backups are made *often enough* and *thoroughly enough* to make sure the company is still *productive* if computer errors occur.” (Mikalsen & Borgesen, 2002). Naturligtvis måste arbete läggas på att reda ut hur ofta och utförligt som är tillräckligt och vad som egentligen menas med att företaget fortfarande är produktivt. Krav och förhållanden varierar mellan olika organisationer. För offentliga organisationer kan det vara helt oacceptabelt att överhuvudtaget förlora någon information. Då får man anpassa sig därefter och använda sig av ett överdimensionerat backup-system.
Kostnaden för backup-system varierar kraftigt beroende på organisationens krav och datamängd. Olika tekniska lösningar, t.ex. cd-brännare, dat-stationer och lagringslösningar för nätverk är anpassade för olika behov. En lösning som lagrar några hundra gigabyte kostar på Dustin (2005) mellan från ca 20 000 kr och uppåt.

Uppdateringar och patchar

Efterhand som svagheter och säkerhetsrisker upptäcks i operativsystem, applikationer och andra komponenter är det viktigt att man håller sig uppdaterad med patchar och säkerhets-

fixar. Traditionellt har patchar varit gratis som en service från företaget som tillverkat mjukvaran, men Microsoft har övervägt att börja ta betalt för liknande tjänster (CNN, 2004). Risken finns att om ett stort företag som Microsoft tar betalt för att leverera säkerhets-fixar så kan andra ta efter.

Övriga åtgärder

Malware kan inte stoppas enbart med tekniska medel. Utan samarbetande, välvillig och utbildad personal blir de tekniska hjälpmedlen meningslösa. För att alla ska veta vad som är rätt och vad som är fel krävs en tydlig policy gällande användandet av datorer.

Allmänna förhållningsregler

Alla organisationer behöver en säkerhetspolicy. Policyn ska vara en samling regler som beskriver vad som är ett acceptabelt beteende på organisationens datorer (Cheswick, Bellowin & Rubin, 2003). Policyns innehåll bör vara noga genomtänkt och ta både affärsmässiga och säkerhetsmässiga hänsyn och bör dessutom vara flexibelt ifall omvärlden förändras. Cheswick, Bellowin & Rubin föreslår att policyn ska baseras på följande tre frågor:

1. Vilka resurser är det du försöker skydda?
2. Vem är intresserad av att attackera dig?
3. Hur mycket säkerhet har du råd med?

Fråga 1 är starkt beroende av vilken organisation policyn gäller. Ofta är information en organisations största tillgång, andra viktiga resurser kan vara nätverkstillgång eller identitet. Fråga 2 är mindre intressant i malware-sammanhang eftersom hotets skapare ofta inte har en viss organisation som mål för sin attack. Man kan däremot vända på frågan och fråga vem som är målet för angreppet. Ett hot som drabbar hundratusentals användare av en populär e-post-klient går att avvärja genom att använda en annan klient.
Gällande fråga 3 uppges kostnaderna för höjd säkerhet förutom direkta kostnader som inköp av mjuk- och hårdvara och ökade administrationskostnader även innefatta minskad bekvämlighet, produktivitet och moral.

Utbildning

”Safe Hex” är en benämning på de grundläggande saker alla som använder datorer bör tänka på (Harley, Slade & Gattiker 2001). Alla inom organisationen bör få utbildning på hur man beter sig med datorer för att inte utsätta sig för onödiga risker. Hur långt man går för att skydda sig beror på riskerna i den miljö man befinner sig i och vikten av det system och de uppgifter man arbetar med. Kostnaderna för utbildning varierar efter individernas tidigare kunskaper och den nivå man vill uppnå, men i samtliga fall kan man räkna med minskad produktivitet under den tid utbildningen pågår. Eventuellt kan också det säkra sättet att använda en dator skilja sig från det effektiva eller bekväma sättet, då uppstår lätt en konflikt mellan olika intressen inom organisationen. Risken finns att det blir säkerheten som får stryka på foten under kraven på hög effektivitet. Utbildning är avgörande för att personalen ska förstå varför säkerhetspolicyn ser ut som den gör och varför de ska följa direktiven även när de hindrar produktivitet eller bekvämlighet.

Säkrare mjukvara

Microsoft har fått ta emot mycket kritik för säkerhetsbrister i sina operativsystem och kritiker anser att deras säkerhetstänkande brister. Harley, Slade & Gattiker (2001) påpekar att problemet delvis beror på att risken att någon utvecklar malware för ett visst system ökar i proportion med antalet användare av systemet. Microsofts operativsystem och

kontorsapplikationer är marknadsledande och har miljoner användare. Därmed blir de stora måltavlor för skapare av malware. Ett annat problem med Microsofts produkter är att de fram tills de senaste versionerna ofta har varit grundkonfigurerade för maximal användbarhet och minimal säkerhet. Standarden har varit att funktioner är aktiverade tills användaren avaktiverar dem istället för den säkrare inställningen att alla tjänster är avstängda tills användaren aktiverar dem.
Ett alternativ om man vill ha total kontroll över sitt system är att själv utveckla den mjukvara man använder. Öppen källkod ger goda möjligheter att kontrollera och eventuellt modifiera operativsystem och programvara om man är beredd att spendera den tid och kompetens som krävs.
Oavsett varifrån mjukvaran kommer går den inte att anse som säker om inte användaren, eller systemansvarig, vet tillräckligt om den för att konfigurera den på ett säkert sätt.

Det säkra systemet

Trusted computing base – TCB är ett begrepp som används i amerikanska försvarsdepartementets berömda ”The Orange Book” (Brand, 1985). TCB innebär att man har en pålitlig, säker bas att stå på när man skapar applikationer, det vill säga ett säkert operativsystem. Olika nivåer av säkerhet för mjukvara definierades och skulle kunna garantera hela systemets totala säkerhet. Det amerikanska försvarsdepartementet ville ha en bas som var matematiskt bevisad säker, något som är mycket svårt att åstadkomma. Kostnaderna för att utveckla ett helt säkert system skulle bli mycket höga och användbarheten troligtvis bli lidande.
Dokumentet är nu föråldrat och inaktuellt, men idén är i grunden ändå intressant.

Säkerhet och användbarhet

Säkerhet kan komma till ett pris i form av att användbarheten minskar. Hur radikala säkerhetsåtgärder man använder kan vara beroende av vilka faror man ser och hur mycket man litar på sin omgivning. Eftersom Internet inte är att betrakta som säkert kan man till exempel begränsa tillgängligheten så att endast de i en organisation som behöver tillgång får det. Det är kanske inte nödvändigt för kassapersonal eller maskinoperatörer att kunna surfa på Internet? Om säkerheten blir för hård kan anställda reagera med olydnad. T.ex. kan de koppla in ett eget modem och på så sätt få obehindrad tillgång till Internet (Cheswick, Bellovin & Rubin, 2003).

Katastrofplan

Haynes (1992) rekommenderar att alla företag, oavsett storlek, ska ha en katastrofplan inspirerad av jordskalvet i San Fransisco 1989. Stora databeronde företag som t.ex. Borland International var då tvungna att prioritera vilka resurser som var viktigast att rädda på den korta tid man hade på sig. Borland var ett av de företag som drabbades hårdast men ändå återhämtade de sig snabbt eftersom de hade en väl genomtänkt katastrofplan, inklusive databackup lagrad på annan ort. Katastrofplanen är lika användbar vid ett omfattande malware-angrepp som vid t.ex. en brand eller naturkatastrof.

Speciellt för offentlig sektor

För den offentliga sektorn kan malware-problemet vara svårare att hantera på grund av den öppenhet som krävs från offentliga organisationer. De kan till exempel ha krav på sig att ta emot all e-post som skickas till dem, då försvinner möjligheten att filtrera bort e-post som andra organisationer hade betraktat som alltför riskfyllda att ta emot.

Krav

Eftersom offentliga organisationer är viktiga för samhällets funktion och finansierade med allmänna medel ställs särskilda krav på dem gällande tillgänglighet, öppenhet och anpassade lönsamhetskrav.

Tillgänglighet

Många offentliga organisationers verksamhet syftar till att erbjuda medborgare tjänster eller information. Exempel på sådana organisationer är försäkringskassan och i viss mån skatteverket. Med tillgång till modern informationsteknologi är det rimligt att kräva en mycket god tillgänglighet till information och självservice.
I regeringens proposition (2001/02:158) skriver Person och von Sydow att samtliga statliga myndigheter bör analysera risker och sårbarheter för att stärka förmågan att fungera även i krissituationer. Det innebär att även IT-säkerheten måste skärpas. Samhällsviktiga system ska inte kunna slås ut av riktade eller slumpmässiga malware-attacker.

24-timmarsmyndigheten

24-timmarsmyndigheten är regeringens vision för hur framtidens myndigheter ska vara tillgängliga 24 timmar om dygnet (24-timmarsmyndigheten, 2005). Offentliga organisationer ska kunna erbjuda nya, utvecklade och förbättrade tjänster. E-tjänster ska i förlängningen innebära billigare och bättre offentlig service och en starkare demokrati. Med så höga mål är det givetvis viktigt att tjänsterna är säkra och tillförlitligheten är hög. Som medborgare ska man alltid kunna få information och utföra självservicetjänster över Internet med bibehållen integritet och skydd av sekretessbelagda uppgifter.
24-timmarsmyndigheten har satt upp riktlinjer, standarder, normer och regelverk som ska hjälpa myndigheterna att utveckla dessa nya, säkra och pålitliga tjänster.

Offentliga handlingar

Offentlighetsprincipen innebär att offentliga handlingar är tillgängliga för allmänheten (Riksdagen, 2005). Allmänna handlingar är information som tillkommit eller förvaras hos en offentlig organisation. Allmänna handlingar kan beläggas med sekretess, om inte är de att betrakta som offentliga. Principen har anor från sjuttonhundratalet och har som syfte att ge insyn och möjlighet att kontrollera hur politiker och tjänstemän på offentliga organisationer sköter sitt jobb. Med hjälp av informationsteknologi kan offentliga handlingar göras mer lättåtkomliga för allmänheten t.ex. via Internet.
Även kommunikation, som t.ex. e-post, mellan privatpersoner eller företag och offentliga organisationer är offentliga handlingar som ska lagras och registreras. Undantag är reklam, handlingar av ringa betydelse, pressklipp, cirkulär, kopior av andra handlingar, statistiska meddelanden och anonyma handlingar (Broms, 1998).
Eftersom även inkommande e-post kan vara offentliga handlingar som måste arkiveras (Broms, 1998) kan myndigheter och andra offentliga organisationer inte välja att filtrera bort all e-post som misstänks innehålla malware. Det blir därför betydligt svårare att skydda sig mot malware som använder sig av den spridningsvägen. Man kan däremot välja att filtrera bort misstänkt e-post som hör till undantagen ovan, t.ex. spam och anonyma e-postmeddelanden. Enligt Statskontorets (2005d) vägledning för myndigheternas spamhantering är det juridiskt och tekniskt riktigt att filtrera bort e-post som innehåller felaktiga uppgifter angående avsändare, mottagare och innehåll. På så sätt kan man bli mer tillgänglig för legitim e-post och samtidigt skydda sig mot en stor andel av de malware-bärande e-postmeddelandena.

Lönsamhetskrav

Enligt kommunallagen ska kommuner och landsting årligen upprätta en budget som är i balans, det vill säga med utgifter som inte överstiger intäkterna (Finansdepartementet, 1991). Det kan, precis som för privata organisationer, vara svårt att motivera stora utgifter för malware-skydd om man inte har klart för sig vilka riskerna är.

Ansvariga myndigheter

Det övergripande ansvaret för Sveriges IT-säkerhet ligger hos krisberedskapsmyndigheten. Post och Telestyrelsen har, genom sitt centrum för IT-incidentrapportering - SITIC, ansvar för informationsutbyte om IT-incidenter, informationsspridning om nya risker, rådgivning om skyddande åtgärder och sammanställning av statistik (SITIC, 2002).

Krisberedskapsmyndigheten

Krisberedskapsmyndigheten har till uppgift att samordna utvecklingen av krisberedskap i samhället. Myndigheten ska analysera vilka hot som finns mot samhället i fredstid och redovisa hur säkerheten kan förstärkas samt vad det kan kosta (Krisberedskapsmyndigheten, 2005b). De hot som analyseras kan vara allt från naturkatastrofer till terroristdåd eller tekniska problem.

Post och Telestyrelsen

Post och Telestyrelsen är ansvarig myndighet för post och elektronisk kommunikation. Till elektronisk kommunikation räknas förutom tv och radio även datoriserad kommunikation som t.ex. e-post.
Enligt Näringsdepartementet (1997) ska Post och Telestyrelsen främja tillgången till säkra och effektiva elektroniska kommunikationer samt stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation.

SITIC

Sveriges IT-incidentcentrum ska fungera som en spridare av information angående IT-incidenter, nya risker och förebyggande åtgärder (Post och Telestyrelsen, 2002). Centret ska systematiskt bevaka och samla information om nya problem på IT-säkerhetsområdet och sprida informationen till samhällets organisationer. För att bli effektivare och eftersom Internet är internationellt samarbetar SITIC med organisationer i andra länder. EGC är ett samarbete mellan europeiska, nationella IT-säkerhetsorganisationer (CITIC, 2005). EGC eftersträvar att på ett mer effektivt sätt hantera IT-säkerhetsincidenter, utbyta teknologi och information samt stödja skapandet av IT-incidentcenter i andra länder. I EGC ingår i nuläget organisationer från Frankrike, Tyskland, Finland, Nederländerna, Sverige och Storbritannien. CITIC medverkar även i det nordiska samarbetsforumet NCF.

Metod

Metodavsnittet beskriver hur arbetet har utförts och på vilket sätt information har inhämtats.

Vetenskaplig metod

För ett akademiskt arbete finns det två huvudsakliga inriktningar att välja mellan – induktiv eller deduktiv. Den induktiva inriktningen innebär att man utgår från data och kommer fram till en teori. Deduktivt arbete går ut på att man sätter upp en teori som man sedan försöker bevisa är sann.
Uppsatsens frågeställning (*Vilka är kostnaderna för att skydda offentlig sektor mot malware och hur viktigt är det att den skyddas?*) är av den karaktären att det induktiva arbetssättet ligger närmast till hands. Men samtidigt bör man komma ihåg att tidigare erfarenheter och förutfattade meningar hos författaren påverkar arbetet åt det deduktiva hållet (om man tror sig veta vad undersökningen kommer utvisa kan den lätt bli en självuppfyllande profetia). Författarens grundläggande inställning är dock att undersökningen ska följa den induktiva linjen.

Arbetsmetod

Uppsatsen följer en arbetsgång som inleds med en frågeställning framtagen av författaren och omformad efter diskussion med kursansvarig och handledare. Steg två innehåller insamling och analys av intressant litteratur. Det insamlade resultatet kompletteras med statistik och tolkas innan slutsatsen kan dras.

Insamlingsmetod

Litteraturstudier har valts eftersom det är en metod som, på ett effektivt sätt, kan ge stora mängder kvalitativ information. Till litteraturstudierna har specifik litteratur om malware kompletterats med allmänna IT-säkerhetsböcker. Propositioner och lagar gällande offentlig sektor har genomsökts efter relevanta fakta. Dessutom har ett antal faktakällor på Internet kunnat bidra med för arbetet intressant information.
I det här arbetet har litteraturstudierna kompletterats med inhämtning av information från de myndigheter som är ansvariga för att elektronisk kommunikation fungerar på ett säkert och effektivt sätt.

Genomförande

Försök till inhämtning av direkt information från ett antal kommuner avbröts på grund av bristande intresse från de tillfrågade IT-cheferna. Av de förfrågningar som skickades ut till IT-ansvariga och IT-säkerhetsansvariga på tio kommuner runt om i landet har endast svar inkommit från en. Utfallet förvånar, då frågan borde vara av intresse för de ansvariga. Inget svar kan så klart också betraktas som ett svar. Tolkningen kan vara att problemet inte anses intressant, att kunskap saknas eller att man helt enkelt inte har tid att avvara. Då bland annat Krisberedskapsmyndigheten nyligen genomfört en stor undersökning med liknande frågor kanske man är trött på undersökningar och enkäter. Med svar från endast en kommun är undersökningens värde tveksamt. Svaren från den enda svarande kommunen (Trollhättan) är därför inte med i arbetet. Istället används statistik från Statistiska Centralbyrån och Svenska IT-incidentcentrets kvartalsrapporter för att komplettera det sekundära materialet. Då SITIC:s statistik är inhämtad från ett trettiotal myndigheter är det att betrakta som ett kvantitativt omfattande material.

Resultat

Här redovisas insamlat material från svenska myndigheter och organisationer.

Uppgifter från Statskontoret och SCB

Statskontoret och Statistiska Centralbyrån har ett stort utbud av material som är intressant för det här arbetet. Det insamlade resultatet är sammanställt från sex undersökningar som Statskontoret genomfört samt statistik publicerad på SCB:s webbplats.

Offentlig sektors webbinnehåll

Innehållet på offentlig sektor webbplatser går att placera i tre kategorier: information, e-tjänster och e-demokrati (Statskontoret 2004b).

Myndighetsinformation

En stor del av den offentliga sektorns webbmaterial består av information om myndigheter, deras verksamhet och hur man kan kontakta dem. Innehållet kan vara av stor vikt både för privata medborgare och för företag. Det kan t.ex. handla om rättigheter, skyldigheter eller möjligheter till ekonomiska bidrag. Enligt statskontorets undersökning (Statskontoret 2004b) är denna del av materialet omfattande och välstrukturerat.

E-tjänster

E-tjänster erbjuder möjligheter för medborgare att registrera sig, göra anmälningar eller ansökningar med stöd av webbplatserna. Tjänsterna kan förenkla och snabba upp ärendehantering eftersom informationen ögonblickligen överförs till myndigheten istället för att sändas med post. Tjänsterna kan också minska kostnaderna för offentlig sektor genom minskat pappersarbete. (Statskontoret 2004b) tar upp kategorierna blankettservice, on-line-ansökan, personlig service, följa ett ärende, avancerade interaktiva tjänster och personligt utformade sidor. Tabell 1 visar i vilken grad de olika tjänsterna är implementerade.

Blankettservice	On-lineansökan	Personliga tjänster	Följa ett ärende	Avancerade interaktiva tjänster	Personligt utformade sidor
100%	41%	34%	8%	53%	9%

Tabell 1 (Statskontoret)

Blankettservice finns på alla de undersökta myndigheternas webbplatser. De mer avancerade tjänsterna förekommer i mer varierande omfattning. Resultaten redovisar endast om tjänsten finns på myndigheten, inte i vilken omfattning varje myndighet har implementerat den. 100% på blankettservice innebär t.ex. att samtliga myndigheter har någon form av blankettservice, inte att samtliga blanketter finns on-line.

E-demokrati

Med E-demokrati menas att medborgarna får ta del av offentlig sektors beslut och beslutsunderlag samt får möjlighet att direkt påverka eller lämna synpunkter via webbplatsen (Statskontoret 2004b). Enligt statskontorets undersökning är e-demokratin dåligt utbyggd, endast arkiven är tillgängliga i någon större omfattning. Skadlig kods påverkan på e-demokrati är därför inte något stort problem i nuläget.

Offentlig sektors hantering av malware

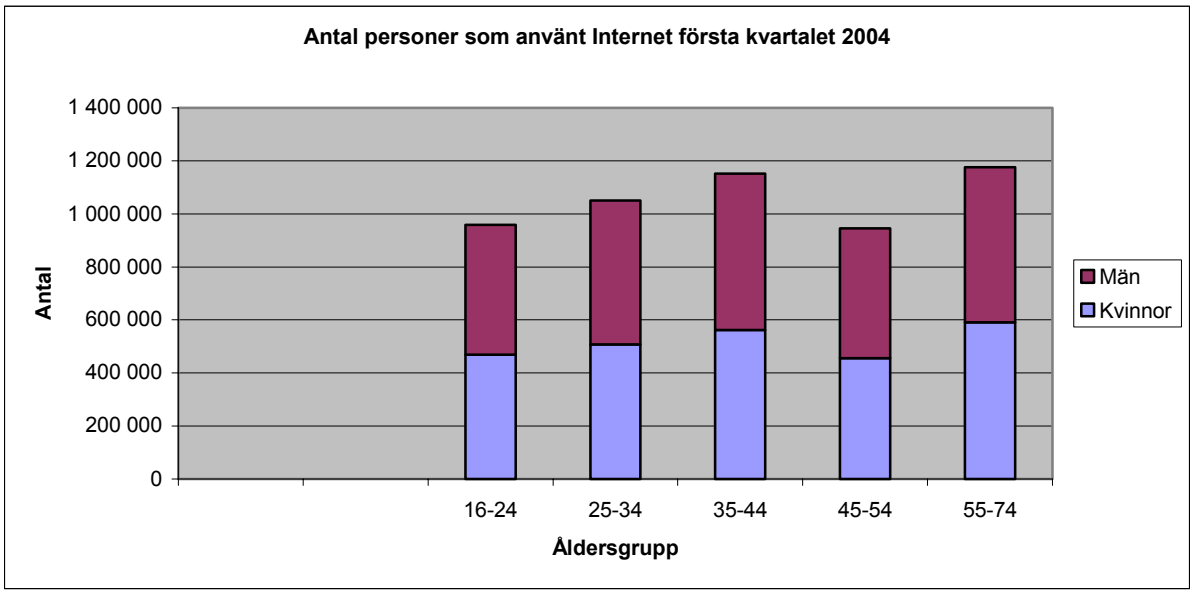
Statskontoret (2005) jämför virus i e-post med brevbomber. Även om det kan finnas ett meddelande i brevbomben kan man inte kräva att den mottagande myndigheten tar emot paketet och öppnar det. Samma sak med e-post, om man misstänker att meddelandet innehåller skadlig kod kan man filtrera bort det utan att bry sig om innehållet.
AMS får enligt (Statskontoret, 2004c) varje vecka in 350 000 e-postmeddelanden av dessa innehåller drygt 15 000 malware. Det innebär att ca 4% av den inkommande e-posten är potentiellt skadlig. Från andra organisationer uppges i samma artikel att från 4% upp till 30% av den inkommande e-posten innehåller skadlig kod.

Internetanvändning i Sverige

Då en stor del av den offentliga sektorns IT-satsningar går ut på att ge privatpersoner och företag bättre tillgång till myndigheter och annan offentlig verksamhet är det av intresse att gå igenom hur stor del av landets medborgare och organisationer som har tillgång till Internet och kan använda tjänsterna.

Privatpersoners tillgång till Internet

Enligt statistiska centralbyrån använde över 5,2 miljoner svenskar i åldern mellan 16 och 74 år Internet under det första kvartalet 2004.

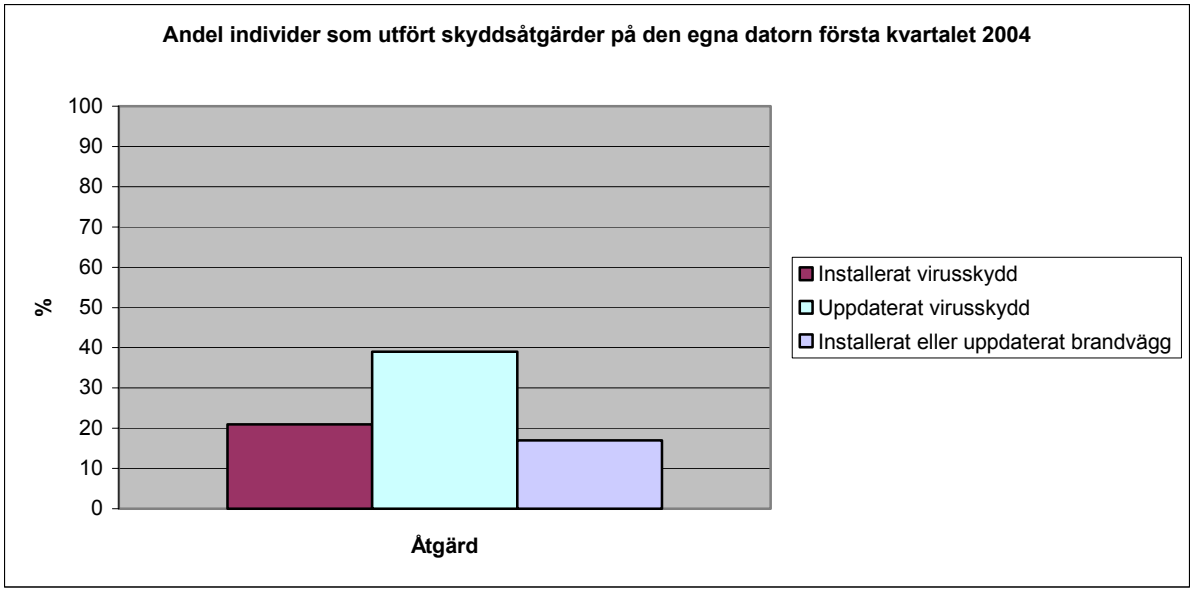


Figur 1 (SCB)

Åldersgrupperna i det statistiska materialet som ligger till grund för diagrammet i figur 1 är valda av SCB, men passar uppsatsens syften bra, då det är i dessa åldrar man kan tänka sig att behovet av kontakter med offentlig sektor är störst. Andelen Internetanvändare varierar beroende på åldersgrupp och kön, men totalt kan man se att antalet motsvarar 82% av befolkningen i de undersökta åldersgrupperna.

Privatpersoners säkerhetsåtgärder

Om privatpersoner ska använda sina datorer till att utnyttja de tjänster som offentlig sektor erbjuder är det viktigt att deras datorer är säkra. Malware på de privata datorerna kan sprida känslig information, störa kommunikationen eller spridas till servrar på de offentliga organisationerna.

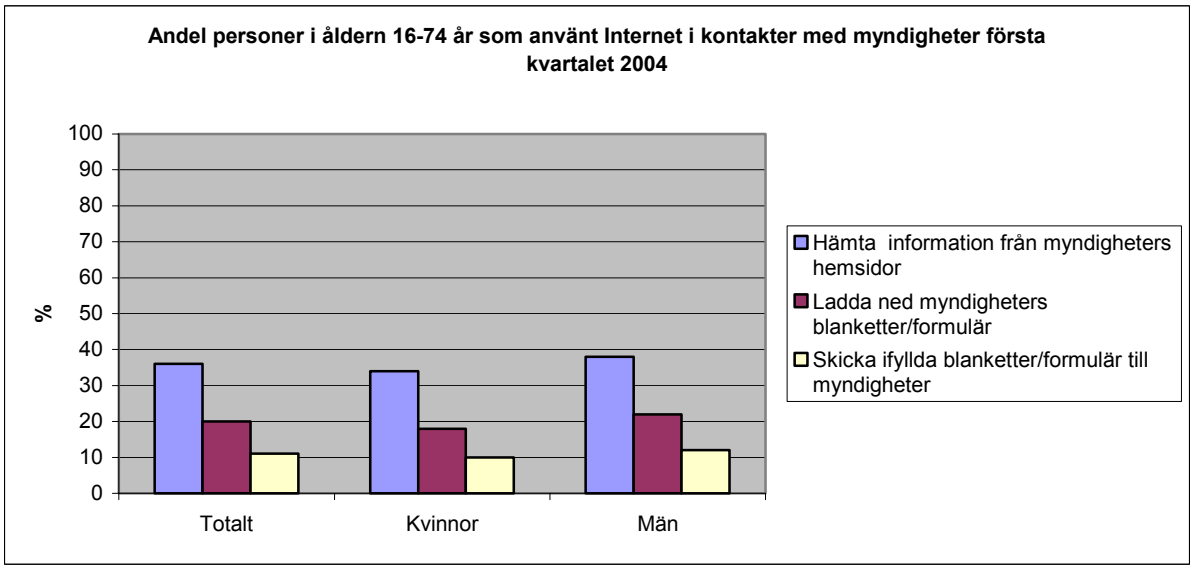


Figur 2 (SCB)

Från diagrammet i figur 2 framgår det tydligt att privatpersoners datorer inte är att betrakta som säkra! Att inte ens 40% av de tillfrågade har uppdaterat sitt virusskydd under det kvartal som undersökningen gällde innebär att risken är stor att mer än 60% av allmänhetens datorer är infekterade med malware. Om inte privatpersoners datorer är säkra måste e-tjänster och annat som offentlig sektor erbjuder vara desto mer säkert för att om möjligt täcka upp de privata datorernas brister.

Privatpersoners användande av offentlig sektors webbtjänster

Privatpersoner kan använda offentlig sektors webbplatser för att hämta information, ladda ner blanketter eller formulär som sedan skickas in med post, eller för att direkt på webbplatsen fylla i formulär och blanketter som elektroniskt förmedlas till myndigheten.



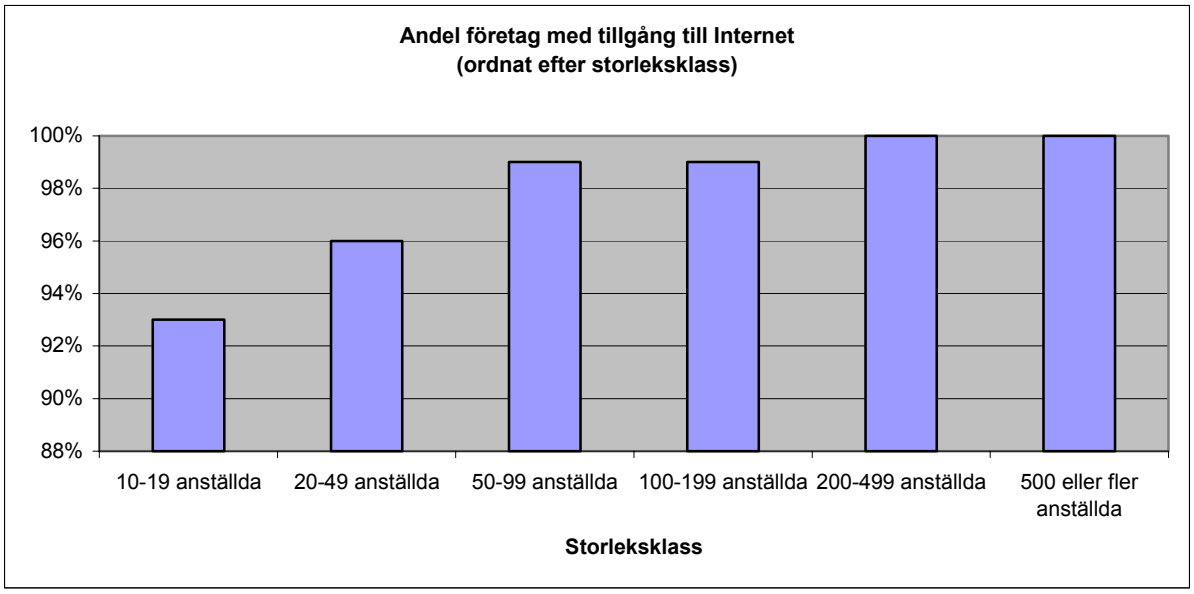
Figur 3 (SCB)

SCB:s statistik i figur 3 visar att det är informationshämtning som är vanligast med ca 35% av de tillfrågade grupperna. Nerladdning av blanketter kommer på andra plats med 20% och den direkta, elektroniska hanteringen kommer nätt och jämt över 10%. Genomgående är det

vanligare att män använder tjänsterna, vilket troligtvis hänger samman med att män använder sig av Internet i högre grad.

Företags tillgång till Internet

Statistiska centralbyråns statistik visar att oavsett storlek eller bransch har så gott som alla företag tillgång till Internet. Bland de stora företagen ligger siffran på 100%, på de mindre sjunker den ner mot 93%.

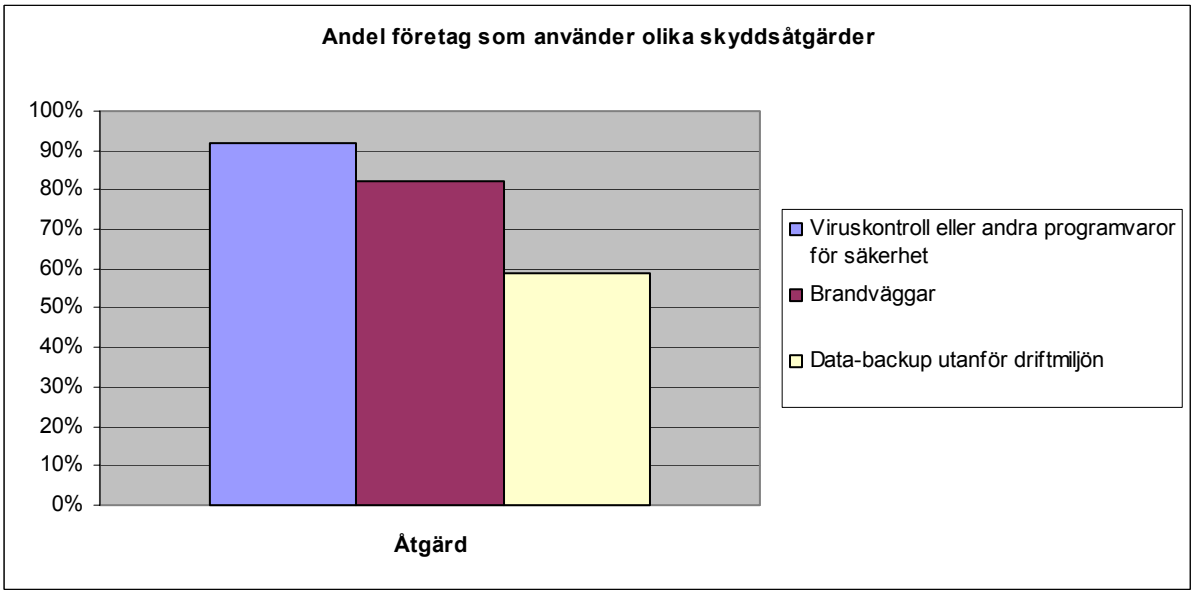


Figur 4 (SCB)

Av ovanstående statistik kan man se att så gott som alla företag har en anslutning till Internet som de skulle kunna använda till kontakter med den offentliga sektorn.

Företagens säkerhetsåtgärder

Hos landets företag ser säkerhetstänkandet bra ut.

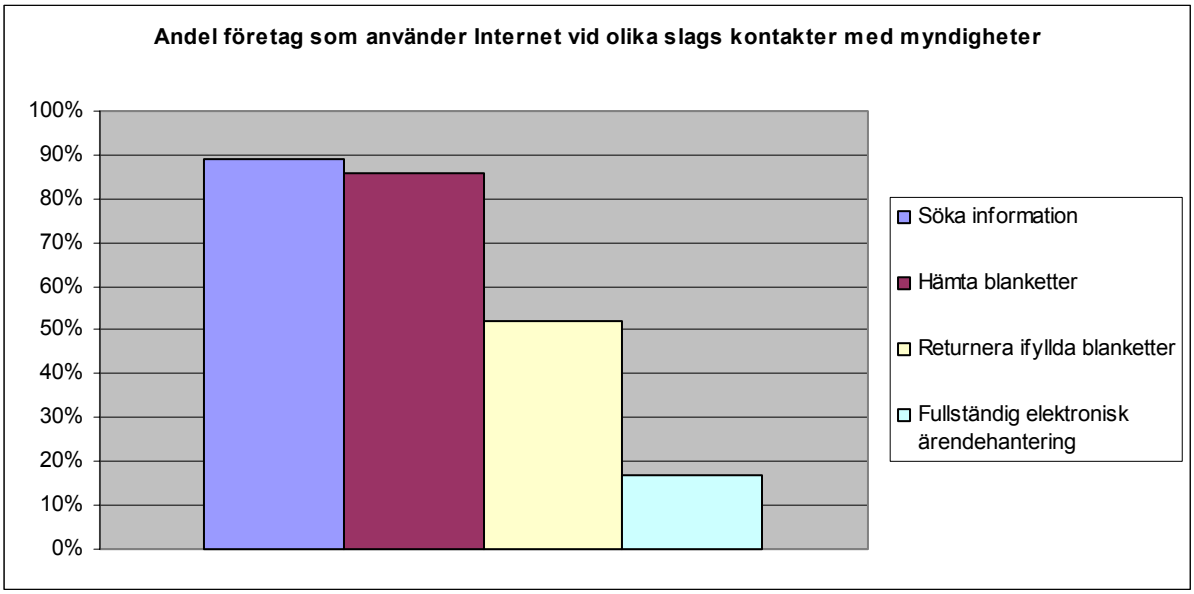


Figur 5 (SCB)

Figur 5 visar att över 90% av företagen använder sig av antivirusprogram. Mer än 80% av företagen har brandväggar och fler än hälften har backupsystem utanför driftmiljön.

Företags användande av offentlig sektors webbtjänster

Diagrammet i figur 6 visar hur företag använder Internet i sina kontakter med svenska myndigheter. Uppemot 90% av företagen använder sig av den offentliga sektorns webbplatser för att söka information.



Figur 6 (SCB)

Hämtning av blanketter är också mycket vanligt. Returnering av ifyllda blanketter hamnar på en tredje plats med drygt 50% och fullständig elektronisk ärendehantering kommer upp i drygt 15%. Alla dessa tjänster kan vara kostnadsbesparande och effektivitetsökande för båda parter.

Information från Krisberedskapsmyndigheten

Tabell 2 är hämtad från Krisberedskapsmyndighetens studie ”Beredskap mot skadlig kod” (Krisberedskapsmyndigheten, 2005c). Tabellen visar hur viktiga ett antal utvalda IT-säkerhetsansvariga anser att olika säkerhetsåtgärder är och hur bra deras organisation implementerar åtgärden. Skillnaden mellan viktighet och säkerhetsnivå i tabellen visar ett mått på organisationens sårbarhet. En viktig åtgärd som inte är implementerad på ett godtagbart sätt innebär en sårbarhet. Från tabellen kan man utläsa att områdena som kräver mest förbättring gäller kunskap och följande av rutiner.

IT-säkerhetsrelaterade faktorer	Viktighet	Säkerhetsnivå	Skillnad
Optimalt brandväggsskydd	9,7	9,0	-0,7
Kontinuerligt uppdaterade antivirusprogram	9,6	8,7	-0,9
Back-up system	9,5	8,4	-1,1
Säker strömförsörjningsmiljö	9,5	8,5	-1,0
Att de som är insatta i IT-frågor följer alla rutiner & processer	9,3	6,9	-2,4
Specialistkompetens när det gäller IT/informationssäkerhet	9,2	7,7	-1,5
Kompetensbredd; att ett tillräckligt antal personer är insatta i säkerhetsfrågor	9,2	6,9	-2,3
VLAN	9,1	8,3	-0,8
Kontinuerlig uppdatering av övriga system/ tilltäppande av sårbarhet	9,1	7,3	-1,8
Optimal konfigurering av säkerhet	9,1	7,2	-1,9
Generell medvetenhet hos de anställda på området IT/informationssäkerhet	8,9	6,4	-2,5
Övrig redundans/övriga reservsystem som kan användas vid behov	8,8	7,4	-1,4

Tabell 2 (KBM)

Krisberedskapsmyndighetens studie presenterar även resultat i tre kategorier som är intressanta för mitt arbete:

Svagheter i IT-säkerheten

Den största svagheten i IT-säkerheten är de människor som använder tekniken. Antingen saknar användarna relevant kunskap i hur man använder sig av IT på ett säkert sätt, eller så har man kunskap och rutiner som man väljer att inte följa. IT-säkerhetsansvariga har också svårt att få igenom förbättringar av säkerheten i de fall där säkerhetskraven kolliderar med effektivitet eller användbarhet. Större ekonomiska resurser är därför inte den avgörande faktorn för säkerheten. Snarare är det kunskap och ändrade attityder som krävs

Inträffade incidenter

Undersökningen visar att allvarliga malware-incidenter har förekommit med omfattande effekter inom organisationerna. Skadorna har varit kostsamma att åtgärda men har inte fortplantats till system som hanterar viktiga samhällsfunktioner.

Organisationernas behov

IT-systemen anses vara mycket viktiga för de tillfrågade myndigheternas funktion. I framtiden tros beroendet av fungerande IT-system öka, i och med utbyggnaden av 24-timmarsmyndigheten. Den ökade öppenheten från myndigheter och andra offentliga organisationer sägs öka sårbarheten. Samtidigt tror man att skadlig kod kommer bli ett än mer aggressiv och därmed innebära ett allt större problem. Mer resurser behövs för att uppnå de högre säkerhetsnivåer som kommer krävas.

Statistik från Svenska viruslistan

Svenska viruslistan är en webbplats som samlar in och redovisar statistik över malware-angrepp mot svenska organisationer (Svenska viruslistan, 2005). År 2004 rapporterades det in 666 olika instanser av illasinnad kod, varav 637 stycken var nya för året. Malware utvecklas alltså och nya versioner kommer ständigt ut. Säkerhetslösningar är därför en slags färskvara som ständigt måste hållas uppdaterade. Av de inrapporterade hoten är ca en tredjedel trojaner som kan användas till att ta kontroll över den drabbade datorn eller till att stjäla information.

Regeringen

Följande citat från propositionen (2001/02:158) visar att de vill se ett delat ansvar mellan stat och systemägare:

> Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att uppnå detta mål bör liksom övrig krishantering i samhället utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. Principiellt gäller att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande. En viktig roll för staten är därför att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilda systemägaren. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänstens arbete förstärkas. (Person, von Sydow, 2002)

I promemorian ”Angrepp mot informationssystem” (Ds 2005:5) behandlas behovet av förändringar för att svensk lag ska överrensstämma med EU:s rambeslut. Bland annat föreslås ett utökande av begreppet dataintrång till att gälla vissa typer av malware som hindrar åtkomst till system. Man hänvisar bland annat till riskerna inom industri, sjukvård och myndigheter:

> Det finns en risk för att också t.ex. industrin, sjukvården eller myndigheter utsätts för allvarliga tillgänglighetsattacker över öppna nät eller mer avancerade intrång och attacker i systemen. Även andra kan utsättas för angrepp. Angreppen kan orsaka betydande kostnader och ekonomiska förluster eller annars få allvarliga konsekvenser. De riskerar också att göra informationssystemen dyrare och därmed mindre tillgängliga för envar. Förtroendet för tekniken, t.ex. elektroniska tjänster som 24-timmarsmyndigheter, kan också skadas. (Ds 2005:5)

Arbete pågår alltså med att skapa ett säkrare IT-klimat i Sverige och inom EU.

Statistik från SITIC

Svenska IT-incidentcentret ger varje kvartal ut statistik över skadlig kod stoppad i filtrering hos ett trettiotal så kallade bevakningsmyndigheter som samarbetar med centret för att samla in information. Diagrammen nedan är sammanställda från SITIC:s kvartalsrapporter k1-2004 till k1-2005 och visar antalet stoppade bilagor med skadlig kod. Enligt SITIC själva är underlaget begränsat och uppgifterna endast att betrakta som indikativa.

Om bevakningsmyndigheterna

Bevakningsmyndigheterna är myndigheter som har ett särskilt ansvar för krishantering i fredstid och under höjd beredskap (Försvarsdepartementet, 2002). Myndigheterna är uppdelade i fyra typkategorier: T1 – T4 och återfinns i bilaga 1.

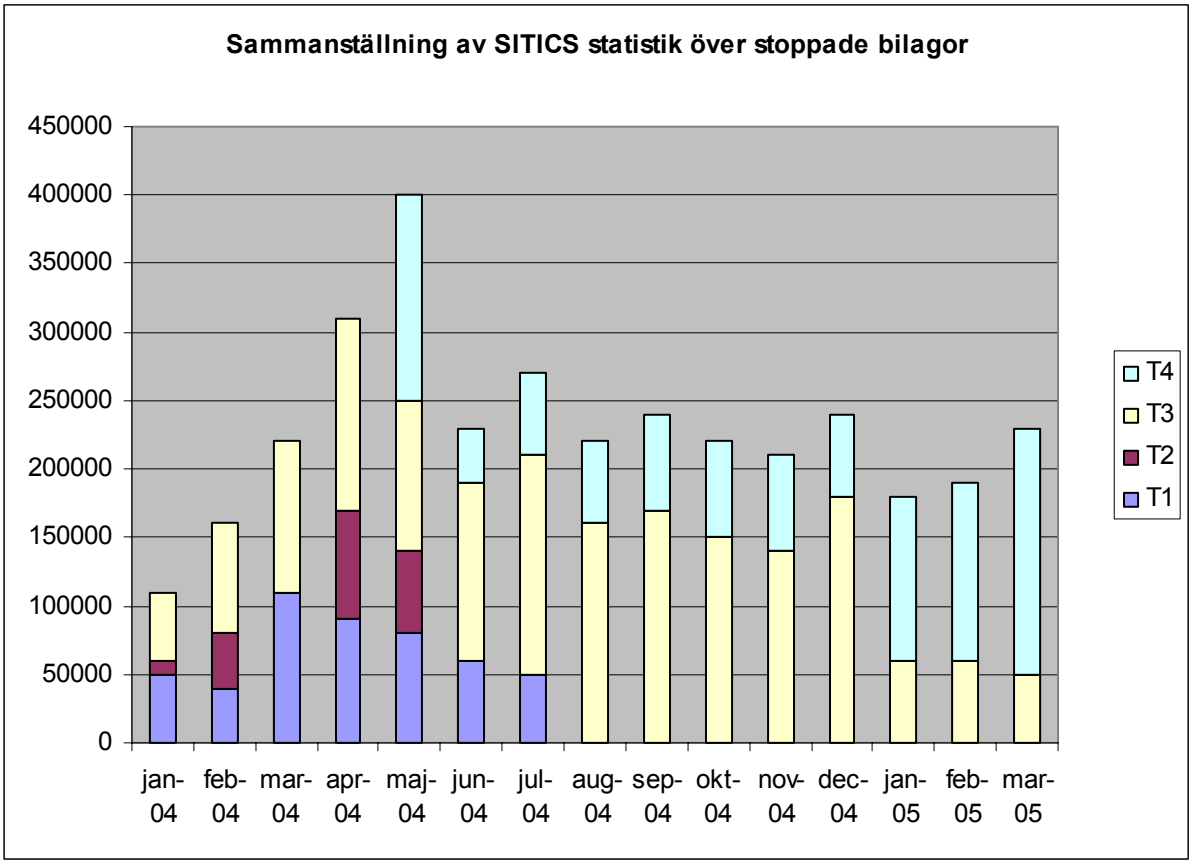
Om filtreringen

En virusscanner fungerar bara om den känner igen ett inkommande virus mot en signatur i sin databas. Därför är det avgörande att databasen är uppdaterad. Enligt en artikel i Mikrodatorn (Arnold, 2005) har de vanligaste antivirusprogrammen reaktionstider på mellan 16 och 4 timmar. I bästa fall har man alltså ett fungerande skydd fyra timmar efter att ett hot har

upptäckts och ett motmedel arbetats fram. Rimligtvis hinner en del malware komma in på bevakningsmyndigheternas datorer innan skyddet hunnit uppdateras. Dessa hot måste tas om hand vid senare tillfälle när programmen hunnit uppdateras så att de känner igen och kan oskadliggöra hotet. För att inte system eller information lagrad på datorerna ska ta skada krävs att systemet är byggt på ett robust sätt eller att man använder sig av metoder som t.ex. heuristik för att hitta okända hot.

Om den skadliga koden

Den skadliga koden som stoppas av myndigheternas filter kan vara av varierande grad skadlig. Det är tillverkarna av antivirusprogram som avgör vad som stoppas. Olika filterregler på olika myndigheter kan ge missvisande statistik.



Figur 7 (SITIC)

Tolkning av statistiken

Under det dryga året som statistiken omfattar har det sammanlagda antalet malware-angrepp på de olika typerna av myndigheter varierat mellan noll och 400 000 angrepp per månad. De inblandade myndigheterna rapporterar tusentals, ibland hundratusentals, blockerade malware-bilagor per månad. Då det endast rör sig om ett trettiotal myndigheter ser man att varje myndighet varje månad stoppar ett stort antal malware-angrepp.
Alla myndighetstyper rapporterar inte i varje kvartalsrapport och enligt SITIC använder de rapporterande myndigheterna inte alltid en enhetlig bakomliggande terminologi. Därför är statistiken mer att betrakta som en indikator på att stora mängder malware stoppas, inte hur stora mängder eller hur antalet stoppade bilagor varierar med tiden.

Diskussion

Här tolkas resultatets betydelse och de konsekvenser som det får för den offentliga sektorn och för samhället i stort.

Tolkning av resultatet

Att malware är ett omfattande och kostsamt problem framgår från resultatet i föregående kapitel. Nedan gås omfattningen och kostnaderna igenom och analyseras med hjälp av den fakta som togs upp i teoriavdelningen.

Malware-problemets omfattning

SITIC:s statistik visar att landets myndigheter ständigt attackeras med malware. Genomsnittet för 2004 hamnar på över 200 000 angrepp per månad. Svenska viruslistan visar att hoten är många och att ständigt nya former av malware dyker upp. För att vara säker krävs dels att man ständigt uppdaterar de tekniska skyddsåtgärderna, dels att man håller sin kunskap färsk och anpassar sina rutiner efter de nya hoten. Offentlig sektor har över en miljon anställda och uppskattningsvis flera hundra tusen datorer som alla måste skyddas. Att skydda en dator är en sak, men att skydda organisationer med hundratals eller tusentals datorer som alla har varsin användare är en annan sak. Det räcker inte med att se till att de senaste tekniska skydden finns installerade på samtliga datorer, man måste också säkerställa att alla användare har den nödvändiga kunskapen och följer de rutiner som finns. På den tekniska sidan är det främst antivirusprogrammens databaser med kända hot som behöver hållas aktuella, men även brandväggar och andra hjälpmedel kan behöva uppdateras. Mjukvara och framför allt operativsystem behöver få de senaste uppgraderingarna installerade så fort en ny sårbarhet upptäcks. På personalsidan är det inte rimligt att ständigt utbilda användarna på det senaste inom IT-säkerhetsområdet, men de måste ha grundläggande kunskaper så att de förstår varför rutiner och policys måste följas. IT-personal måste ha mer djupgående säkerhetskunskaper och kontinuerligt förnya sina kunskaper för att kunna hålla organisationen säker. Förståelse och kunskap krävs också från ledningen så att de inser att förändringar som drabbar produktivitet eller användbarhet ibland är nödvändiga för att hålla systemen säkra.
Enligt Krisberedskapsmyndighetens undersökning anser tillfrågade IT-tekniker att den mänskliga faktorn är den svagaste länken i IT-säkerheten. Det är också den faktorn som är svårast att kontrollera och som ligger längs ifrån de säkerhetsansvarigas vanliga arbetsuppgifter och kompetens.

Skyddsåtgärdernas kostnad

Kostnaden för att skydda en dator med antivirusprogram och personlig brandvägg hamnar enligt mitt teoriavsnitt på ungefär 600 kr. Till detta kommer kostnaden för backupsystem som kan variera stort, men om vi antar att man behöver en backup på några hundra gigabyte till 100 klientdatorer hamnar kostnaden per dator på några hundra kronor per dator. För att komplettera organisationens säkerhet krävs dessutom en yttre brandvägg. Kostnaden för de tekniska skydden hamnar totalt kring 1000 kr per dator.
De tekniska skyddsåtgärderna är dock inte hela kostnaden. Den svaga länken är användarna och den kunskap som de behöver för att kunna hantera datorer på ett säkert sätt. Att utbilda personal kostar pengar och dessutom förloras tid då de kunde ha arbetat produktivt. Den säkerhetsansvariga IT-personalens utbildning är mer omfattande och tidskrävande, men gäller färre anställda och drabbar inte produktiviteten på samma sätt.
Ytterligare en svårbedömd kostnad kan härledas till den minskning av effektiviteten som ökad säkerhet ofta innebär. De tekniska skydden är ofta inte till hinder för effektivitet eller

produktivitet, men när man utformar rutiner och policys kan man ibland behöva välja mellan säkerhet och användbarhet.
Myndigheter som Post och Telestyrelsen, Försvarets Radioanstalt, Försvarets Materielverk, Polisen och Krisberedskapsmyndigheten får på grund av malware-problemet en ökad arbetsbelastning som antingen får ersättas med ökade resurser från skattemedel eller med minskade insatser på andra områden. Att ett nationellt IT-incidentcenter inrättats är enkom för att hantera malware och andra IT-säkerhetsrisker är ett klart exempel på en malware-relaterad kostnad i stor skala.

Skador

Kostnaderna för att återställa en stor organisations datorsystem är omfattande, så en god beredskap kan löna sig även om det kostar tid och andra resurser att upprätthålla den. Förlust av data som t.ex. personregister eller forskningsresultat kan vara förödande för en organisation. Myndigheter och kommuner handhar ofta databaser med känsliga uppgifter som till exempel personuppgifter och journaler. Okontrollerad spridning av sådana uppgifter kan orsaka stora skador både för individer och för myndigheten som ansvarar för informationen. Om filerna skadas eller raderas kan det också komma att kosta mycket för organisationen som måste återställa dem eller samla in informationen på nytt.
Om en organisations nätverk går ner kan hela organisationen lamslås och eventuella webbplatser eller e-tjänster blir svåra att upprätthålla och kontrollera. Man kan dessutom räkna med att kostnaderna för uteblivet arbete blir höga

Konsekvenser

Skadorna som malware kan orsaka och kostnaderna som det enligt ovanstående stycken för med sig har konsekvenser för individer, organisationer och för hela samhället.

För enskilda individer

Alla som använder datorer uppkopplade mot Internet, eller på annat sätt i kontakt med omvärlden, påverkas av malware. En person som använder sin hemdator till underhållning och rekreation drabbas naturligtvis inte på samma sätt som en organisation om datorns tjänster under en tid blir otillgängliga, men skador orsakade av malware måste ändå åtgärdas innan datorn kan användas normalt igen. Många individer är beroende av fungerade hemdator och Internetanslutning för att utföra bankaffärer och kommunicera med myndigheter och bekanta. I takt med att mängden tillgängliga tjänster ökar, ökar också individernas beroende av fungerande teknik.
24-timmarsmyndigheten innebär att enskilda medborgare själva ska kunna inhämta information och utföra vissa tjänster via Internet. Om malware har infekterat användarens dator kan det bli omöjligt att komma åt informationen eller utföra tjänsten. I värsta fall kan malware på användarens dator stjäla information eller påverka utförandet av tjänsten på ett sätt som skadar användaren ekonomiskt. Man kan t.ex. tänka sig en trojan som infekterar webbläsaren och stör kommunikationen mellan klient och server när användaren lämnar sin deklaration via Internet, så att felaktiga uppgifter lämnas in. Liknande scenarion kan tänkas där det istället är användaren av en Internetbanktjänst som drabbas. Följderna skulle kunna bli katastrofala.
Rädslan för angrepp och skador på mjukvara och information kan påverka individens beteende och öka hennes utgifter genom inköp av tekniska skydd som antivirusprogram och brandväggar. Individens ökade kostnader och risker kan få datoranvändare att bli mer restriktiva i hur de använder Internet.
På individnivå finns det mycket att göra för att öka informationssäkerheten och på så sätt göra system och organisationer mindre mottagliga för malware-angrepp. En okunnig eller slarvig

individ kan orsaka stora skador genom att medvetet eller omedvetet sprida malware. I förlängningen kan samhället besparas stora kostnader om datoranvändare får en skyldighet att bete sig på ett säkert sätt och hålla sin dator i ett säkert skick. En parallell kan dras till de skyldigheter som trafikanter har att skaffa sig den rätta behörigheten för sitt fordon och att hålla det i ett trafikdugligt skick. Kanske kan ett liknande system bli aktuellt för datorer som ansluts till allmänna nätverk? Frågan är om det är var och ens ansvar eller om samhället ska se till att alla har den kunskap som behövs för att minimera risker och kostnader i samband med malware-angrepp. Ett system med obligatoriska datorkörkort och årliga kontroller av hård- och mjukvara skulle troligtvis bli alltför kostsamt för samhället, men om kostnaderna för malware blir tillräckligt höga kan det bli ett möjligt handlingsalternativ. Kanske blir IT-säkerhet i framtiden ett obligatoriskt ämne i grundskolan.

För offentliga organisationer

Riskerna kan få offentliga organisationer att bli mer slutna och övervaka sina anställdas datorvanor på ett sätt som kan kännas kränkande för den enskilda individen. Både användare av e-tjänster och anställda kan komma att övervakas och kontrolleras hårdare än nu. Ökad säkerhet innebär ofta ökade kostnader och minskad produktivitet. Ökade kostnader för övervakning och skydd mot malware går inte att ta ut som ökade intäkter i organisationen. Kostnader relaterade till skydd mot malware bör behandlas som priset man får betala om man vill vara tillgänglig och kunna bedriva sin verksamhet. Om medborgarna inte vill använda 24-timmarsmyndighetens tjänster eftersom de inte anses säkra innebär det stora kostnader för de myndigheter och organisationer som genomfört förändringarna för att öka flexibiliteten för användarna och minska sina kostnader genom utökad självservice. Det är rimligt att anta att det i slutändan blir skattebetalarna som får stå för notan när kostnaderna för IT-säkerheten öka.

Konsekvenser för samhället

Även för samhället i stort kan malware utgöra ett stort problem. Enligt en rapport från en underavdelning till det amerikanska Homeland Security (Thornberry, 2004) kan den ökade tillgången till vad de kallar ”automated tools for mailicious actions” utgöra ett hot mot USA:s säkerhet. Sabotage eller spionage, utfört med malware kan påverka hela den amerikanska ekonomin. Det samma gäller rimligtvis också den svenska ekonomin som är minst lika känslig som den amerikanska. Även i Sverige har man på regeringsnivå insett att man måste vidta åtgärder för att minska IT-samhällets sårbarhet:

> Alla statliga myndigheter bör i syfte att stärka krishanteringsförmågan analysera om det finns sådan sårbarhet eller sådana risker inom myndighetens ansvarsområde som mycket allvarligt kan nedsätta förmågan hos verksamheten inom området (Person, von Sydow, 2002)

Det moderna samhället är beroende av ett säkert informationsflöde. Utan fungerande informationsteknik lamslås både vårt civila samhälle och vår förmåga att klara av en höjd beredskap. Enligt Krisberedskapsmyndigheten (2005b) kan förlust av information på grund av underrättelseoperationer allvarligt skada Sveriges nationella säkerhet. Det kan även leda till betydande ekonomiska förluster både för staten och för svenska företag. Krisberedskapsmyndigheten har huvudansvaret för att minska landets sårbarhet för IT-säkerhetsrisker och har till sitt stöd SITIC, Försvarets Radioanstalt och Försvarets Materielverk. SITIC samarbetar även på internationellt plan med motsvarande myndigheter i Norden och i Europa. Nödvändigheten av dessa myndigheter och kostnaderna som de innebär kan självklart inte enbart skyllas på malware-problemet, men informationssäkerheten och det hot mot den som malware innebär är ett av de problem som de har att tampas med.

Även polisen får en ökad arbetsbelastning när malware-problemet växer. Svensk polis rekommenderar att man anmäler alla IT-brott till sin lokala polisstation som, om de inte har egen kompetens på området, skickar ärendet vidare till specialiserade avdelningar. De rekommenderar också att företag och organisationer kontaktar dem redan innan IT-brott har begåtts för att skapa kontakter och få information och råd om hur man bör bete sig för att förhindra brott och hur man ska bete sig om man blir utsatt. Enligt IT-brottsroteln kan spridning av malware rubriceras som skadegörelse om spridningen är avsiktlig och orsakar skada i de angripna systemen (Polisen, 2005). Läget är dock oklart eftersom prejudikat saknas. På senare tid har organiserade brottslingar har börjat intressera sig för informationsteknologi och de brott som man kan begå med dess hjälp. På sikt kan man tänka sig att kopplingar till tyngre brottslighet kan få polisen att visa ett större engagemang för området. Efterhand som problemet växer kommer man tvingas lägga allt större resurser på utbildning och införskaffande av material och kompetens på IT-området.
Individers rädsla för malware och den ökade försiktighet som rädslan leder till kan bli ett bakslag för den pågående utvecklingen mot ett 24-timmarssamhälle. Samhällets ansvar bör därför vara att följa utvecklingen av malware och skydd och sprida information om hur man bäst skyddar sig, både som individ och som organisation. Det är viktigt att samhället tar detta ansvar för att skydda medborgare och organisationer (offentliga och privata) från det hot som malware utgör. Regeringen visar i sin proposition (2001/02:158) om samhällets säkerhet och beredskap att de faktiskt tar IT-säkerheten på allvar.

Slutsats

Hela tiden kommer nya varianter av virus, trojaner och maskar ut på Internet. Över 600 nya hot upptäcktes på svenska datorer 2004. Till Svenska IT-incidentcentret, som samarbetar med ett trettiotal svenska myndigheter, inrapporterades under det gångna året genomsnittligen över 200 000 incidenter i månaden.
Malware kan skada eller stjäla känslig information, förstöra applikationer och operativsystem eller minska systems tillgänglighet. Vad som är mest skadligt beror på den drabbade organisationens verksamhet och vilka skyddsåtgärder man vidtagit. I en del fall är det viktigaste att ingen information läcker ut, för andra organisationer är tillgänglighet dygnet runt viktigare.
Tekniska medel för att skydda en dator mot malware kan kosta omkring tusen kronor. För en organisation med tusentals datorer kan det bli en avsevärd kostnad. När en hel organisation ska säkras krävs dessutom kunskap och säkerhetsrutiner som följs av alla användare. Utbildning är tidskrävande och nya rutiner kan påverka effektiviteten negativt, konflikter kan därför uppstå mellan säkerhet och produktivitet.
Krisberedskapsmyndigheten, Svenska IT-incidentcentret, Post och Telestyrelsen, Försvarets Materielverk och Försvarets Radioanstalt arbetar alla för att skydda organisationer och individer i Sverige mot malware. SITIC har som enda syfte att övervaka IT-incidenter i Sverige och sprida information om hur man kan skydda sig. Polisens IT-brottsrotel har hand om lag och rätt i sammanhanget.
Kostnaderna för att skydda offentlig sektor mot malware kan ses som summan av följande fyra kostnadsgrupper:

1. Tekniska skyddsåtgärder
2. Utbildning av användare och IT-personal
3. Rutiner och förhållningssätt som eventuellt kan drabba effektiviteten
4. Ökad belastning på befintliga myndigheter samt behov av ett IT-incidentcenter

Den offentliga sektorn handhar känsliga uppgifter som kan skada individer eller samhälle om de kommer i fel händer eller skadas av malware. Förutom de direkta skadorna kan också allmänhetens förtroende för offentliga organisationer skadas. Tjänsterna som landets myndigheter i och med 24-timmarsmyndigheten ska erbjuda kan endast vara tillgängliga om IT-systemen fungerar. Om systemen blir onåbara eller opålitliga blir satsningen på en 24-timmarsmyndighet bortkastad. Kontakter med den offentliga sektorn måste då även i fortsättningen ske på traditionellt vis.

Referenser

Arne Arnold, Koppla greppet om datorns säkerhet, Mikrodatorn 6-05, 2005

William R Cheswick, Steven M Bellovin & Aviel D Rubin, Firewalls and Internet Security second edition, Addison-Wesley, 2003

David Harley, Robert Slade & Urs E Gattiker, Viruses Revealed, Osborne, 2001

Colin Haynes, Virushandboken, Almquist & Wiksell, 1992

Kevin Mitnick & William Simon, Bedrägerihandboken, Pagina Förlags AB, 2002

SCB, Kortperiodisk sysselsättningsstatistik - 1:a kvartalet 2005, SCB, 2005

Mac Thornberry et. al., Cybersecurity for the Homeland, Subcomittee on Cybersecurity, Science, and Research & Development of the U.S. House of Representatives Select Committee of Homeland Security, 2004

Internet

Susanna Broms, 1998: Elektronisk post m.m., Kungl. Biblioteket / BIBSAM (2005-04-10), http://www.kb.se/bibsam/upphovsr/e-postpm.htm

Sheila L. Brand, 1985: DoD trusted computer system evaluation criteria, DoD Computer Security Centre (2004-11-10), http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

CNN, 2004: Microsoft may charge extra for security software, CNN (2004-11-10), http://www.cnn.com/2004/TECH/internet/12/16/microsoft.spyware.ap/index.html

Susanne Ekroth, 2005: 24-timmarsmyndigheten (2005-04-10), http://www.24-timmarsmyndigheten.se/

Finansdepartementet, 1991: Kommunallag 1991:900, Finansdepartementet (2005-04-10), http://www.notisum.se/rnp/sls/lag/19910900.HTM

Försvarsdepartementet, 2002: Förordning 2002:472 om åtgärder för fredstida krishantering och höjd beredskap, Försvarsdepartementet (2004-11-10), http://www.notisum.se/rnp/sls/lag/20020472.htm

Krisberedskapsmyndigheten, 2005a: Samhällets informationssäkerhet - Lägesbedömning 2005, Krisberedskapsmyndigheten (2005-04-10), http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utredningar%20och%20remissvar/Utredningar-uppdrag/lagesbedomn_infosak_%202005.pdf

Krisberedskapsmyndigheten, 2005b: En utvecklad krisberedskap – KBM:s underlag inför 2005 års proposition om krisberedskap, Krisberedskapsmyndigheten (2005-04-10),

http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utredningar%20och%20remissvar/Utredningar-uppdrag/en_utv_krisberedskap_ruben-2005.pdf

Krisberedskapsmyndigheten, 2005c: Beredskap mot skadlig kod, Krisberedskapsmyndigheten (2005-05-12),
http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationsserier/Temaserie/skadligkod_2005-1.pdf

NOU, 2002: Kort om lagen om offentlig upphandling, Nämnden för offentlig upphandling (2004-11-10),
http://www.nou.se/pdf/broschyr.pdf

Näringsdepartementet, 1997: Förordning 1997:401 med instruktion för Post- och telestyrelsen, Näringsdepartementet (2004-11-10),
http://rixlex.riksdagen.se/htbin/thw?%24%7BOOHTML%7D=SFST_DOK&%24%7BSNHTML%7D=SFSR_ERR&%24%7BBASE%7D=SFST&BET=1997%3A401&%24%7BTRIPSHOW%7D=format%3DTHW

Göran Person & Björn von Sydow, 2001: Regeringens proposition 2001/02:158 Samhällets säkerhet och beredskap, Försvarsdepartementet (2004-11-10),
http://www.sitic.se/dokument/Regeringens_proposition_200102_158.pdf

Polisen, 2005: IT-brott, Polisen (2005-03-09),
http://www.polisen.se/inter/nodeid=30903&pageversion=1.html

Post och Telestyrelsen, 2002: Faktablad Sveriges IT-incidentcentrum – SITIC, Post och Telestyrelsen (2004-11-10),
http://www.pts.se/Archive/Documents/SE/Faktablad-sitic.pdf

Riksdagen, 2005: Parlamentarisk ordbok, Sveriges Riksdag (2005-03-09),
http://www.riksdagen.se/ordbok/

SITIC, 2005: Sveriges IT-incidentcentrum, SITIC (2005-04-10),
http://www.sitic.se/om_sitic/

Statistiska Centralbyrån, 2005a: IT i företag, Statistiska Centralbyrån (2005-05-12),
http://www.scb.se/templates/Product____15308.asp

Statistiska Centralbyrån, 2005b: IT bland individer, Statistiska Centralbyrån (2005-05-12),
http://www.scb.se/templates/Product____15266.asp

Statistiska Centralbyrån, 2005c: Kortperiodisk sysselsättningsstatistik 1:a kvartalet 2005, Statistiska Centralbyrån (2005-05-12),
http://www.scb.se/templates/Product____7820.asp

Statskontoret, 2004a: Den offentliga förvaltningen i e-samhället, Statskontoret (2005-04-10),
http://www.statskontoret.se/upload/Publikationer/2004/200427.pdf

Statskontoret, 2004b: E-tjänster på myndigheternas webbplatser, Statskontoret (2005-04-10),
http://www.statskontoret.se/upload/Publikationer/2004/200407.pdf

Statskontoret, 2004c: Öppna system nr 3-4, Statskontoret (2005-04-10), http://www.statskontoret.se/upload/Publikationer/os/0403-4.pdf

Statskontoret, 2005d: Myndigheternas spamhantering - en vägledning kring rättsliga frågor, Statskontoret (2005-05-12), http://www.statskontoret.se/upload/Publikationer/2005/200505.pdf

Svenska viruslistan, 2005: Virusläget i Sverige, Svenska Viruslistan (2005-04-10), http://www.svenskaviruslistan.se/

Symantec, 2005: Security response - glossary, Symantec (2005-03-09), http://securityresponse.symantec.com/avcenter/refa.html#worm

Bilaga 1

Förteckning över bevakningsmyndigheter

Samverkans-områden	Myndigheter med särskilda uppgifter inom samverkansområdena	Myndighet med ansvar enligt 4 §	Myndighet med ansvar enligt 8 §
Teknisk infrastruktur	Affärsverket svenska kraftnät	x	x
	Elsäkerhetsverket	x	x
	Krisberedskaps-myndigheten	x	x
	Livsmedelsverket	x	x
	Post- och telestyrelsen	x	x
	Statens energi-myndighet	x	x
	Statens kärnkraft-inspektion	x	x
Transporter	Banverket	x	x
/Upphör att gälla U:2005-01-01/			
	Luftfartsverket	x	x
/Träder i kraft I:2005-01-01/			
	Luftfartsstyrelsen	x	x
	Sjöfartsverket	x	x
	Vägverket	x	x
Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen	Kustbevakningen	x	x
	Livsmedelsverket	x	x
	Rikspolisstyrelsen	x	x
	Smittskyddsinstitutet	x	x
	Socialstyrelsen	x	x
	Statens jordbruks-verk	x	x
	Statens kärnkraft-inspektion	x	x
	Statens räddnings-verk	x	x
	Statens strål-skyddsinstitut	x	x
	Statens veterinär-medicinska anstalt	x	x
	Tullverket	x	x
Ekonomisk säkerhet	Arbetsmarknads-styrelsen		x
	Ekonomistyrnings-verket	x	x
	Finansinspektionen	x	x
/Upphör att gälla U:2005-01-01/			
	Riksförsäkrings-verket	x	x
/Träder i kraft I:2005-01-01/			
	Försäkringskassan	x	x
	Riksgäldskontoret	x	x
	Skatteverket	x	x
	Statens energi-myndighet	x	x
	Statens jordbruks-verk	x	x
	Tullverket	x	x

	Verket för närings-livsutveckling	x	x
Områdesvis samordning, samverkan och information	Ekonomistyrnings-verket	x	x
	Krisberedskaps-myndigheten	x	x
	Lantmäteriverket	x	x
	Länsstyrelserna	x	x
	Skatteverket	x	x
	Statistiska central-byrån	x	x
	Styrelsen för psykologiskt försvar		
Skydd, undsättning och vård	Kustbevakningen	x	x
	Luftfartsverket	x	x
	Migrationsverket	x	x
	Rikspolisstyrelsen	x	x
	Sjöfartsverket	x	x
	Socialstyrelsen	x	x
	Statens räddningsverk	x	x
	Statens strål-skyddsinstitut	x	x
	Tullverket	x	x