Hotbilden i Sverige

En undersökning av den digitala hotbilden mot ett medelstort svenskt företag

Maria Carlsson
2010-06-07
Abstract

Internet and information technology today has a rather obvious role in the activities of companies and organizations. All cash transactions within and between companies is digitized, communication within the company is done via e-mail, sales and marketing is done largely with marketing and ads on the Internet. This has resulted in economic benefits for companies and organizations, and facilitated the work for them. However, this has also led to new threats have emerged. Companies and organizations is well aware that there are numerous threats that comes with using the Internet and Information Technologies but exactly what those threats are for a mid-sized company in Sweden is not clarified anywhere. New reports made annually by various companies and government agencies around the world but no one puts a medium-sized Swedish business in focus. In this study several reports, made by different companies and government agencies are compared and compiled, too try too make an overview over the threats against a mid-sized company in Sweden. Together with interviews done with key people in the field of IT-security this study identifies the threats, draws conclusions of how to prevent them and also try to take a look into the future to see what threats a mid-sized company or organization can expect in just a matter of years. In the study we notice how all of the IT threats are increasing and that the digital crime are becoming more organized, that some of the key protections for a company is staff training and standard technical solutions such as antivirus software and firewalls. In the future operating systems will no longer be the target for intrusion, but instead web application be the major vulnerabilities. This essay is written in Swedish.

Keywords: IT-security, IT-threats, Information Technology
Sammanfattning


Nyckelord: IT-säkerhet, IT-hot, Informationsteknik
6.2 Empiri .................................................................................................................. 58
6.3 Studiens kunskapsbidrag ..................................................................................... 59
6.4 Förslag på fortsatt forskning ............................................................................. 59
7 Litteratutförteckning .......................................................................................... 60
  7.1 Tidskrifter ......................................................................................................... 60
  7.1.1 Elektroniska artiklar ..................................................................................... 61
  7.2 Elektroniska källor ........................................................................................... 61
  7.3 Intervjuer .......................................................................................................... 62
8 Bilagor ..................................................................................................................... 63
  8.1 Intervjufrågor .................................................................................................... 63
1 Inledning

Syftet med detta kapitel är att ge läsaren en inledande förståelse för de faktorer som ligger till grunden för studien samt en inblick i problemområdet.

1.1 Problembeskrivning och frågeställning

Internet och informationstekniker har idag en ganska självklar roll inom verksamheter hos företag och organisationer. All pengatransaktion inom och emellan företag digitaliseras, kommunikationen inom företaget sker via e-post, försäljning och marknadsföring görs till stor del med informationsteknik på Internet. Detta har medfört ekonomiska vinster för organisationer och företag samt underlättat arbetet för dem. Dock har detta även medfört att nya hot har dykt upp. Den 18 februari rapporterade The Wall Street Journal i artikeln ”Broad new hacking attack detected” (Gorman, 2010) om datahackare i Europa och Kina som lyckats bryta sig in i datorer hos närmare 2,500 företag inom en period av 18 månader. I mer än 100 av dessa fall lyckades datahackarna få tillgång till företagets servrar som lagrade stora mängder av data, som företagets filer, databaser och e-post. Enligt SOPHOS rapport ”Security threat report: July 2009 Update” består 89,7% av all jobbe-post av SPAM. (Sophos, 2009) I april 2010 skickade antivirusprogramtillverkarna McAfees ut en uppdatering till deras viruskydd som såg en viktig systemfil på de datorer som använde Windows XP med Service Pack 3 som skadlig och satte denna fil i karantän. Detta innebar att de datorer som utsattes för detta inte kunde starta. Enligt tekniker på University of Michigan drabbades 800 000 datorer globalt och i Sverige slogs bland annat 5 000 av datorerna i Göteborgs kommun ut. 27 systembolag runt om i landet tvungna att stänga för att uppdateringen slagit ut deras kassasystem. (Lindström, 2010)

Idag vet de flesta företag och organisationer om att informationstekniker och Internet medför ett nytt hot men exakt vad hotet är och hur påtagligt det är finns det ingen samlad rapport som kan visa för en verksamhet i Sverige. Nya rapporter upprättas årligen av olika bolag och myndigheter men ingen sätter en medelstor svensk verksamhet i fokus. Detta leder oss till studiens huvudfråga:

Hur ser hotbilden ut för ett medelstort företag i Sverige idag?

I denna uppsats ska jag undersöka rapporter som har upprättats hos olika myndigheter och företag för att försöka få en överblick över hotbilden i Sverige. Med hjälp av statistik genom åren och trender som vuxit fram med nya tekniker vill jag även besvara frågan:

Hur ser framtidens hotbild ut?

Om trenderna fortsätter som de gjort de senaste åren, hur kommer då hotbilden att se ut hos verksamheterna inom bara några år?

Dessutom skall denna studie också ha som uppgift att med hjälp av rapporterna samt intervjuerna med säkerhetsspecialister hos olika organisationer försöka ta fram hur en organisation lättast kan skydda sig mot de hot som studien inringat.
1.2 **Syftet med uppsatsen**

Genom att sammanställa olika IT-säkerhetsrapporter, intervjuer med nyckelpersoner inom ämnet IT-säkerhet och bevakning av media skall denna uppsats ge en överblick över den digitala hotbilden mot ett medelstort företag i Sverige. Studien har dessutom som uppgift att förklara hur företaget lättast kan skydda sig mot de identifierade hoten samt försöka analysera trender för att ge en blick hur framtidens hotbild kommer att se ut.

1.3 **Avgränsning**


1.4 **Centrala begrepp**

<table>
<thead>
<tr>
<th>Ord</th>
<th>Beskrivning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT- Säkerhet</strong></td>
<td>En del i begreppet informationssäkerhet men som endast berör Informations Teknologiska säkerheten.</td>
</tr>
<tr>
<td><strong>Hot</strong></td>
<td>Möjlig oönskad händelse med negativa konsekvenser för verksamheten.</td>
</tr>
<tr>
<td><strong>Hotbild</strong></td>
<td>Hot som bedöms förekomma mot en viss verksamhet från en viss källa.</td>
</tr>
<tr>
<td><strong>Medelstort Företag</strong></td>
<td>Ett medelstort företag har färre än 250 anställda. Företaget ska ha en årlig omsättning som understiger 40 miljoner euro eller ha en balansomslutning som understiger 27 miljoner euro (Rekommendation 96/280/EG).</td>
</tr>
</tbody>
</table>

1.5 **Disposition**

**Inledning**
I detta kapitel beskrivs syftet med denna studie samt själva problembakgrunden och frågeställningen. Detta för att ge läsaren en inblick i vad studien kommer att handla om.

**Metod**
I detta kapitel beskrivs vilka metoder som används vid insamlingen av data till denna studie. Kapitlet ska visa läsaren vilken grund som utredningen står på.

**Teori**
I detta kapitel beskrivs de myndigheter och företag som upprättat de olika rapporterna. Läsaren får även en kort beskrivning av de olika hot som kommer att tas upp i resultatet av utredningen.
Resultat av utredning
I detta kapitel presenteras resultatet av studiens utredning. Här sammanställs de olika rapporterna, intervjuerna samt artiklarna.

Avslutande del
Syftet med detta kapitel är att koppla den teoretiska delen i studien med resultatet av utredningen. Samt att presentera svaret på studiens huvudfrågor Hur ser hotbilden ut för ett medelstort företag i Sverige idag?, Hur ska ett företag skydda sig? samt Hur ser framtiden ut?
2 Metod

Syftet med detta kapitel är att ge inblick i de tillvägagångssätt som tillämpas i studien och skapa en förståelse för de perspektiv som ligger till grund för studiens analys och utvärdering.

2.1 Forskningsstrategi


En komparativ studie innebär att man som författare av en uppsats jämför olika objekt i avseende att analysera de skillnader som finns. Objekten skall vara så pass lika att det är meningsfullt att jämföra dem men det skall finnas tillräckligt många skillnader att det finns ett värde att analysera dem (Denk, 2002). Då jag valt att jämföra och analysera rapporter som alla beskriver incidenter och hot på Internet i världen kommer jag att göra en komparativ studie över dessa.

2.2 Vetenskapssyn

Hermeneutiken handlar om att tolka och förstå hur andra människor upplever sin situation. Då syftet med min uppsats är att skapa en bild av de digitala hot som ett företag präglas utav ska jag samla in mina data med hjälp av kvalitativa metoder kommer jag använda mig av ett hermeneutiskt förhållningssätt i min studie (Lundahl & Skärvad, 1982,1999)

2.3 Insamlingsmetoder

Nedan följer en beskrivning av de insamlingsmetoder som används i denna studie. Samt argument till varför just dessa valts.
2.3.1 Litteraturstudie

Genom att studera begrepp samt företagsbeskrivningar ämnar jag ge en bättre förståelse för huruvida rapporterna jag sammanställer upprättats. För begreppen har jag källkritiskt bedömt och jämfört litteratur för att hitta lämpliga referenser.

2.3.2 Empirisk undersökning

I denna studie har jag valt att arbeta utifrån några specifika punkter för att lättare kunna belysa just likheter och olikheter hos rapporterna. Jag kommer hela tiden ha ett medelstort svenskt företag i åtanke då jag samlar presenterar mitt data.

Denna studie skall även använda artiklar från diverse nyhetskanaler för att kunna få en mer uppdaterad bild över IT-säkerheten och hoten som upplevs både på nationell skala men även på ett globalt plan då olika risker och hot är gränsöverskridande över Internet. Artiklarna väljs ut efter resultatet utav rapporterna skrivits, just för att komplettera rapporterna med mer uppdaterade siffror och dessutom få siffror som berör Sverige.

Rapporterna och artiklarna kommer att kompletteras med semistrukturerade intervjuer där en djupare inblick skall ges för den digitala hotbilden som finns just i Sverige. Intervjuerna på hos säkerhetsexperterna på MSB och Sitic gjordes på plats medan intervjuerna med säkerhetsexperterna på Symantec och TeliaSonera CERT gjordes över telefon på grund av reslängd och tidsbrist. Alla intervjuer utom en spelades in, då valde jag ändå att anteckna flitigt under hela intervjun för att lättare kunna ställa följdfrågor under intervjuens gång. Intervjun hos Sitic gjordes utan inspelnings på respondentens begäran, då förlitade jag mig helt på mina anteckningar för att sammanställa intervjun.

2.3.3 Urvalsmetod

För att kunna få en överblick över IT-hoten använder jag mig av rapporter som upprättats och publicerats av olika myndigheter och företag s. Rapporterna beskriver bland annat hur företag ser på informationssäkerhet, hur IT-relaterade brott begås och sammanställer olika sorts statistik som berör IT-hot. Valet av rapporter gjordes genom att dela in dem i vilka organisationer som har upprättat rapporterna. De delas in i företag som erbjuder tjänster, företag som erbjuder produkter och myndigheter. Detta för att försöka täcka alla vinklar i detta ämne då denna studie ämnar få just en generell överblick.

För att säkra kvalitén och för att studien skall resultera i en förstående kunskap har jag valt att använda mig av intervjuer som insamlingsteknik. Jag kommer att jobba utifrån en kvalitativstrategi och genomför kvalitativa semistrukturerade intervjuer med fyra säkerhetsspecialister vid olika företag och myndigheter. Dessa valdes utifrån deras mångåriga erfarenhet inom området. För att få en spridd bild från dessa intervjuer har de utförts både av säkerhetsspecialister på myndigheter och privata företag.
2.3.4 Argumentation för urval

Rapporterna som upprättats hos olika företag kan mycket väl spegla den bild som dessa företag vill att de ska spegla. Då flera av företagen säljer IT-säkerhetslösningar och olika sorters program är det möjligt att de väljer att ta upp de siffror som ställer sina egna produkter i ett bättre ljus samt försöker påvisa hur deras produkter är av stor vikt. Därför har jag valt att ställa rapporterna mot varandra och belysa deras likheter och olikheter dels för att få en överblick men även för att kunna få en sådan riktig bild av verkligheten som möjligt. Jag har dessutom valt dessa rapporter att de kommer dels från företag som erbjuder tjänster inom IT-säkerhet, företag som säljer faktiska säkerhetsprodukter och en myndighet. Detta för att få en sådan bred vy som möjligt samt för att undvika en vinklad bild i slutsatsen av denna studie.

Artiklarna har valts för att komplettera de siffror som presenteras i rapporterna och de tidningar som artiklarna valts från är välkända svenska och utländska tidsskrifter. Dessa tidsskrifter användes för att de anses som trovärdiga källor.

Intervjuerna genomfördes med personer som har mångårig kunskap och erfarenhet inom området teknik och informationssäkerhet. Flera av dem har dessutom fått nationellt erkännande för deras kunskap inom IT-säkerhet.

2.3.5 Genomförande

De punkter som kommer att belysas i studien är elakartad kod, digitala angripare, nya trender, ny teknik, den mänskliga faktorn och hur en organisation ska skydda sig. Det är även dessa punkter jag använde då jag strukturerade upp de intervjuerna som utfördes.
3 Teori

Detta kapitel skall ge läsaren förståelse över de begrepp som kommer att användas under denna studie. Samt en överblick över de företag och myndigheter som upprättat de rapporter som skall presenteras.

3.1 Tjänsteföretag


3.1.1 Verizon business


3.1.2 Trustwave

Trustwave är ett privatägt företag som är verksam på ett globalt plan med kontor i 6 världsdeler och huvudkontor ibland annat Europa och Amerika. De arbetar med säkerhetslösningar åt organisationer för att säkra data och säkra lösningar inom betalkortsbranchen. De sköter säkerheten åt mer än 15,000 organisationer världen över. (Trustwave, 2010)

3.2 Produktföretag

Nedan tas fyra företag upp som erbjuder olika produkter inom området IT och IT-säkerhet. Organisationerna kommer att beskrivas samt dess verksamhet. Dessutom förklaras hur deras rapportera upprättats.

3.2.1 Symantec


3.2.2 Sophos

Sophos är ett privatägt företag som utvecklar antivirusprogram och andra lösningar för att skydda privatpersoners och företags datorer och servrar. Har 100 miljoner användare av deras produkter i mer än 150 olika länder (SOPHOS, 2010).


3.2.3 IBM

IBM, International Business Machines, är ett globalt IT-företag som grundades 1911. Företaget har idag 386 558 anställda varav ca 4000 i Sverige. IBM utvecklar, säljer och marknadsför sorters produkter, både hårdvara och mjukvara. Dessutom erbjuder de en rad olika tjänster till marknaden. De hjälper bland annat till att skapa säkra åtkomst för till exempel användarhantering och förhindra olovlig åtkomst av data. IBM arbetar även mycket med forskning och utveckling av nya produkter och programvaror. På grund av deras höga investering i just denna avdelning av IBM har de fått fler patent i USA än något annat företag, 17e året på raken. (IBM, 2010)

3.2.4 Trend Micro

Trend Micro är ett privatägt företag som grundades 1988 i USA men har idag sitt huvudkontor i Tokyo, Japan. Företaget har idag 4239 anställda och har kontor i mer än 30 länder. Företaget erbjuder ett flertal olika produkter för att skydda ditt nätverk och din dator, bland annat antivirusprogram, spamskydd och brandväggar. Produkterna erbjuds till såväl som privatpersoner, medelstora företag och stora företag. (Trendmicro, 2010)


3.3 Myndighet

I denna studie tas även en myndighet upp. Dess organisation och verksamhet kommer att beskrivas nedan samt hur deras rapport upprättats.

3.3.1 MSB


MSB:s rapport från 2009 ska försöka få en helhetssyn på samhällets informationssäkerhet, då syftar de till ett svenskt samhälle. Lägesbedömningen bygger på information från öppna källor, ett flertal fördjupningsstudier, djupintervjuer med aktörer inom såväl offentlig som privat sektor samt enkätundersökningar riktad till privat sektor. (MSB, 2009)

3.4 Digitala Hot

I detta kapitel skall jag förklara de digitala hot som kommer att tas upp i de rapporter och intervjuer jag presenterar denna studie.

3.4.1 Malware
Samlingsnamnet för ondsint programvara är malware, traditionellt delar man sedan in denna programvara i olika sorter datorvirus. Idag är det dock svårt att dela in dessa i specifika sorter då de mer eller mindre liknar varandra på många olika sätt. Indelningen är dock kvar och används men många av dessa ondsinta programvaror placeras ofta in i fler än en kategori. (Gralla, 2007)

**Virus**

Ett virus är en programvara som infekterar ett redan existerande program i en dator. När själva vårdprogrammet åt viruset körs exekveras viruset och den utför de skadliga aktiviteterna. Många virus gör inte annat än försöker kopiera över sig själv till andra program på datorn. Dock finns det även virus som åstadkommer större skador genom att förstöra eller korrumpera data eller förstöra stora delar av operativsystemet. (Gralla, 2007)

**Trojansk häst**

Namnet kommer från den grekiska legenden om hur grekerna intog Troja genom att gömma sig i en stor trähäst som de lurade trojanerna att de lämnat som en gåva. Denna legend har nu blivit en synonym för en gåva som bär på en dold förbannelse. Det är på detta sätt denna typ av datorvirus agerar. En trojansk häst kan komma till ett datorsystem dold som ett program som användaren vill ha installerat på sitt system, till exempel ett spel. När programvaran väl är installerat på datorn utför den trojanska hästen aktiviteter som kan vara skadliga för datorn. (Gralla, 2007)

**Maskar**

Denna form av malware skiljer sig från virus på det sättet att de har möjligheten att kopiera sig själv och skicka sig vidare till andra datorer. De skapar alltså exakta kopior av sig själva då de infekterat en dator och använder sedan kommunikation med andra datorer för att kunna vidarebefordra sin kopia. (Sophos, 2009)


**Backdoor**

En backdoor, eller bakdörr, är en odokumenterad funktion i ett program som an utnyttjas för att kringgå normala kontroller vid programmets användning. Detta betyder att man alltså kan kringgå säkerhetsskyddet i programmet. Denna funktion kan vara medvetet inlagt av skaparen av programmet för att underlätta testning. (SIS/TK 456, 2007)

En sådan bakdörr kan även skapas med hjälp av en trojansk häst, då kallas det för en bakdörrtrojan. Denna fungerar som en vanlig trojan som infekterar datorn genom att låtsas vara ett legitmit program. När trojanen väl är installerad skapas alltså en så kallad bakdörr till

---

1 Ett e-postprogram skapat av Microsoft (Gralla, 2007)
användarens dator och den person som skapat trojanen har möjlighet att ta kontroll över användarens dator. (Sophos, 2009)

Spyware
Spyware är mjukvara om tillåter marknadsförare och hackare att komma åt känslig information som finns lagrad på användarens dator utan användarens tillåtelse. Mjukvaran kan installeras på datorn genom att användaren klickar på en länk som beskriver att denna mjukvara är viktig för att användarens dator ska fungera. Det kan även vara så att mjukvaran laddas ner och installeras utan användarens vetskap med en så kallad Drive-by download2. En form av spyware är så kallad ”Keylogging” som samlar de tryck som görs på ett tangentbord och lagrar det för att någon senare kan gå igenom filen och se exakt vad en användare skrivit. (Sophos, 2009)

3.4.2 Hacking

Hacking, eller ”att hacka” definieras som ”otillåten användning av data system eller att kringgå säkerhetsmekanismerna i ett datasystem” enligt ”Definitioner och förekomster” skrevet av säkerhetshuset. Detta utförs av en så kallad hackare som definieras av SIS Handbok, 2007, som ”en person som vinnlägger sig om att behärska alla detaljer om hur man påverkar och styr IT-system”.

Att utföra en hacker- attack kan göras på flera olika vis en del av tillvägagångssätten innebär att ”hackaren” helt enkelt försöker gissa sig till ett lösenord för att få åtkomst till ett system eller webbtjänst. Jag listar nedan några av de tillvägagångssätten som kommer att tas upp i min empiri.

SQL-Injection
Dessa attacker innebär att en angripare för in egna elakartade SQL3- kommandon i till exempel användares indatafält och koden exekveras sedan av som riktiga SQL- kommandon. På detta sätt kan man som angripare hämta data från databaser tabeller som han egentligen inte skall ha tillgång till. Ett annat vanligt sätt att utföra SQL- injections som inte är lika direkt är att föra in elakartad kod i strängar som är menad för lagring i tabeller eller som metadata. När de lagrade strängarna konkateras med andra, riktiga, SQL-kommandon exekveras den elakartade koden. (Microsoft, 2010)

Cross-Site Scripting (XSS)
Cross-Site Scripting är en typ av datorsäkerhetssårbarhet som kan hittas i webbapplikationer och som tillåter angripare att föra in elakartade skript till en användares webbrowser. Det är alltså användaren som är det tänkta offret och angriparen använder sårbarheten i en webbapplikation som ett medel för attacken. (Whitehat Security, 2006)

---

2 Drive-by download; då en användare besöker en webbsida och infekteras med malware utan användarens vetskap. (Sophos, 2009)
3 Structured Query Language är ett språk designad för att skapa databaser, lägga till nya rader och manipulera data i databaser. (Taylor, 2010)
**Botnät**
Ett botnät är ett nätverk av infekterade datorer som på avstånd kan kontrolleras av en hackare. När en dator är en del i ett sådant nätverk kan den fjärrstyras över Internet och kan då användas i hackarens attacker helt utan användarens vetskap. (Sophos, 2009)

**DoS och DDoS**

DDoS står för ”Distributed Denial Of Service” och är en attack som använder flera datorer för att utföra samma sorts attacker som med DoS. Dessa attacker utförs ofta med datorer vars användare inte är medveten om att de utför denna attack. Vanligtvis har dessa datorer infekterats med en trojan som skapat en så kallad bakdörr och därmed tar kontroll över dessa datorer för att utföra attacken. Dessa nätverk av infekterade datorer är så kallade botnät. (Sophos, 2009)

**Infekterad Dokument**
Infekterade PDF filer är ett vanligt PDF dokument som en angripare utnyttjat dess inbäddade skript eller makro för att sprida elakartat material. När en användare öppnar den infekterade filen kan utomstående få kontrollen över datorn genom en så kallad bakdörr. (Sophos, 2009)

**3.4.3 SPAM**

SPAM är oönskad kommersiell e-post. Alltså den elektroniska motsvarigheten till skräppost eller reklam som kommer till din vanliga brevlåda. (Sophos, 2009)

SPAM kan komma i flera former och föra med sig andra digitala hot. Till exempel:

- **Phishing** – Innebär att man använder sig av påhittade företag eller personer och genom webbsidor och e-post försöker lura besökaren av webbsidan eller mottagaren av e-posten till att ge ut personlig information. (Sophos, 2009)
- **E-post malware** – Malware som distribueras via e-post (Sophos, 2009)
- **Spoofing** – Innebär att sändaren av e-post är förfalskad i syfte att lura mottagaren att e-posten kommer från en betrodd och säker källa. (Sophos, 2009)

---

4 Resultat av utredning

Detta kapitel består av resultatet av studien. Den är uppdelad i tre delar. Först presenteras rapporternas resultat. Efter det presenteras artiklarna som belyser samma ämne och sist presenteras fyra intervjuer.

4.1 Rapporter

Rapporternas resultat kommer att presenteras i sex rubriker där varje rapport sammanställer sina siffror och slutsatser till respektive rubrik.

4.1.1 Malware

Verizon

Enligt Verizons rapport från 2009 är malware det andra vanligaste formen av hot mot ett företag. (Verizon business, 2009)


Symantec

Enligt Symantecs rapport angående trenderna under år 2008 bestod de 50 vanligaste formerna av malware till 68% av trojaner. Genomgående för hela denna rapport är just att det hela tiden är en generell ökning för all sorts attacker, skadlig kod och fientlig programvara. (Symantec, 2009)

Botnät som utnyttjas på distans för att utför attacker utan användarens vetskap ökade också under perioden som Symantec dokumenterade i rapporten från 2009. Medelvärdet för aktiva botinfekterade datorer under året 2008 var 75 158 stycken. Detta är en ökning med 31% från året innan. (Symantec, 2009)

**Sophos**

Sophos skriver i sin halvårsrapport från juli 2009 att de tar emot 40 000 unika missnänsamma filer varje dag, vilket är 28 filer varje minut, 24 timmar om dygnet. De skriver även att en självständig testagentur vid rapportens tillfälle kunde räkna att det fanns upp till 22,5 miljoner unika malware. Detta är nästan en dubblering från året innan i juni då Sophos rapporterade att det fanns 12,3 miljoner unika malware. (Sophos, 2009)

Enligt samma rapport bestod 89,7 % av all jobb e-post hos företagen i världen av spam. Dessutom upptäckts det ungefär 6 500 nya spam-relaterade webbsidor varje dag, denna siffra är nästan en fördubbling från samma period är 2008. (Sophos, 2009)

**Trustwave**

Enligt Trustwaves rapport så utnyttjade hackare malware för att kunna samla data från en organisation i 54 % av de fallen av intrång i organisationen. De valde att infektera datorerna med olika sorters virus vars enda syfte var att lagra data, då till störst del genom att hämta data direkt från RAM5- minnet eller direkt från tangentbordet. (Trustwave - SpiderLabs, 2010)

**IBM**

När det gäller malware anser IBM:s säkerhetsrapport om år 2009 att fler och fler antivirusleverantörer slutat använda specifika namn för nya former av malware. Istället används samlingsnamn som inte förklarar vad denna form av malware gör. Vad en leverantör kallar för ett virus kallar nästa för en trojan och därför säger det inte användaren mycket när IBM rapporterar att 86 % av alla malware är trojaner. Det IBM visar i sin rapport är att av alla malware är gruppen trojaner störst med 86 % och efter det kommer virus som består av 45 %. Bara de två blir tillsammans mer än 100 % men detta menar IBM är ett resultat av att antivirusleverantörerna benämner samma malware med två eller flera olika namn. (X-Force, 2010)

---

5 Random Access Memory, en lagringsenhet i datorn där användaren kan få åtkomst till datan i vilken ordning som helst (Brookshear, 2007)

Phishing-attacker fortsätter att gå upp och ner enligt IBM:s siffror. Volymen tycks dock hålla sig till mellan 0,1 % - 1 % av volymen av spam. IBM rapporterar också att det fortfarande är den finansiella sektorn som är mest utsatt för denna form av attacker. (X-Force, 2010)

**MSB**


Enligt MSB är det svårt att få exakta siffror på hur många datorer det finns som är kopplade till ett botnät världen över. Vissa lägger fram siffror om att det finns cirka 12 miljoner datorer som är anslutna till ett botnät och att det varje dag ansluter i genomsnitt 280 000 stycken nya datorer till nätverken. I Sverige beräknar MSB på att det finns cirka 27 000 stycken datorer som är anslutna i ett botnät. (MSB, 2009)

### 4.1.2 Hackare

**Verizon**

I Verizons rapport drar de slutsatsen att de flesta angrepp som idag sker mot företag till störst del kommer utifrån företagets gränser. Där 74 % av alla intrång mot organisationer kommer från en extern källa. Dock rapporterar Verizon att de interna attackerna/intrången är mycket skadligare för verksamheten. (Verizon business, 2009)

För femte året på raken leder hacking över vilka typer av attacker som är vanligast över Internet. Inom hacking är det just när angriparen får tag på anställdas lösenord eller på annat sätt kommit in på deras konton som är det vanligaste, till exempel att de anställda delar på lösenord eller att lösenorden är för korta och lätta att gissa sig till. Näst vanligast är SQL-injections. (Verizon business, 2009)

De intrång som dokumenteras i Verizons rapport beror till störst del på säkerhetsbrister hos och emellan en tredjepart till verksamheten. Rapporten menar att detta beror på att organisationen inte sköter säkerheten på samma sätt när det gäller verksamhetens interna system som det som används mot leverantörer och kunder. (Verizon business, 2009)

Verizon rapporterar även att numera använder inte hackare plattformen på datorn för att göra intrång i nätverk och datorer utan den största delen av intrång görs istället med hjälp av applikationerna på datorn. I ungefär fyra av tio hacker-relaterade intrång fick en angripare obehörig åtkomst till offret via olika typer av fjärråtkomstprogram och administration program. På nästan samma antal intrång som Verizon dokumenterat kommer olovlig åtkomst via webbapplikationer. Sist på listan av hurupvida en angripare gått tillväga för åtkomst till användaren och nätverket är själva plattformen, eller operativsystemet. (Verizon business, 2009)
Symantec
Mer än någonsin tidigare motiveras hackare av pengar. Att på något sätt lura en användare för finansiell vinning. Symantec rapporterar även att under år 2008 var 78 % av de hot som berörde konfidentiell information, stöld av användardata. Av dessa användes ”keystroke-logging” som medel för stölden i 76 % av fallen. När en angripare väl fått tag på finansiell information eller personliga detaljer, som namn adresser och statliga identifieringsnummer, säljs denna information på det som Symantec kallar för den ”ekonomiska underjorden”. Vilket är olika sorters forum på webben och realtidschattprogram där informations säljs, köps och byts i kriminella syften. (Symantec, 2009)


I Sverige är 1 av 618,8 av all e-post som skickas ett spam, detta kan jämföras med Kina där 1 av 196,9 av all e-post som skickas ett spam. På det hela taget har spam på internet ökat radikalt enligt Symantec, de rapporterar en ökning av spam från 119,6 miljarder skickade SPAM till 349,6 miljarder från 2007 till 2008. Symantecs rapport visar att det är just finansiella sektorn som utsätts för phishing attacker, denna sektor fick 76 % av den totala phishing- attackerna som Symantec dokumenterade. (Symantec, 2009)

Sophos
I Sophos halvårsrapport från juli 2009 beskriver de att en av anledningarna till att webben är populär bland angripare, hackare, är att sidor som användare litar på kan äventyras och användas för att infektera ett stort antal användare. Detta syns tydligt när det gäller SQL-injections. Denna typ av attack sker när en användares indata inte filteras korrekt och därför exekverar elakartad kod som utför instruktioner i databasen som ej skall utföras. Hackare fortsätter förutom SQL-injections att använda sig av länkar som de lägger ut i forum och bloggar som användaren klickar på och kommer vidare till en ny sida som är värd för malware. (Sophos, 2009)

Trustwave

Trend Micro

6 Som till exempel personnummer i Sverige eller Social Security Number i Amerika
**MSB**
Enligt MSB:s rapport är risken för stora angrepp av Internetvirus med bred bas förbi. Denna sorts angrepp skedde då hackaren bara ville ha uppmärksamhet och göra ett namn åt sig själv. Den nya generationen säkerhetshot som sprids idag består av skadliga angrepp ledda av cyberbrottslingar som är riktade mot specifika företag för personlig eller finansiell vinning. (MSB, 2009)

**4.1.3 Mänskliga faktorn**

**Verizon**
Enligt Verizons rapport var just den mänskliga faktorn, eller missbruk av användaren, som var det tredje vanligaste medlet för dataintrång. Där användarens tillgång till eller sina privilegier i systemet som missbrukats vilket orsakat sårbarheter i systemet. Till störst del sker denna sortsintrång ovetande och inte menat som ett försök till intrång men detta beteende är också ofta det som leder till att olika sorts malware introduceras till systemet och nätverket. (Verizon business, 2009)

**Sophos**
Sophos skriver i sin rapport att anställda börjat dela med sig för mycket information på Internet, inte bara sociala nätverk, och 63 % av de tillfrågade systemadministratörerna oroar sig över vad det är för information som de anställda egentligen lämnar ut. I rapporten tas ett extremt exempel upp, i juni 2009 då personlig information åt en kommande chef i MI6 exponerades till hela Facebooks nätverk när hans fru valde att låta hela hennes profil visas för hennes nätverk ”London”. (Sophos, 2009)

**4.1.4 Ny teknik**

**Sophos**
I Sophos halvårsrapport från juli 2009 beskriver de hur organisationer mer och mer bekymrad över elakartade attacker som har sitt ursprung från Sociala nätverk\(^7\), såväl som att användaren lämnar ut privat eller företagsinformation över Internet. (Sophos, 2009)

I rapporten skriver även Sophos att så kallade ”SmartPhones\(^8\)” mer och mer börjat användas på arbetsplatser. Även om ”SmartPhones” ännu inte varit målet för en stor signifikant attack är det fakta att en ”SmartPhone” både är en dator och en mobiltelefon som kan utgöra en riskfaktor. Dels på grund av att det är lättare att klicka på en illvillig länk om telefonen använder sig av pekplatta, det blir lättare för användaren att trycka av misstag, och dessutom kan det vara svårt att utläsa om den länken är illvillig på grund av den lilla skärmen. (Sophos, 2009)

\(^7\) Så som Facebook, Twitter, MySpace och LinkedIn (Sophos, 2009)

\(^8\) På svenska kallas denna teknik för ”pekskärmsmobil” och är ett slags mellanting mellan handdator och mobiltelefon (Sophos, 2009)
**Trend Micro**

I rapporten från Trend Micro tar de upp att de sociala nätverken börjar mer och mer bli ett bekymmer för verksamheten då detta är målet för flera cyberbrottslingar. Till exempel var facebook med sina 300 miljoner användare det tänkta målet för KOOBFACE⁹- botnätet. (Trend Micro, 2009)

Trend Micro menar att ”cloud computing”¹⁰ kommer att slå hårt inom de kommande åren på grund av den hårda ekonomin som driver företagen att hitta billigare alternativ. Denna nya teknik kommer att medföra många förmåner men utbildning och ökad medvetenhet om de medföljande riskerna behövs också. Det finns flera risker med denna tjänst, till exempel kan en angripare försöka med enkla medel att angripa själva anslutningen till molnet så att användaren inte får tillgång till sina tjänster. (Trend Micro, 2009)

**MSB**

Mobila enheter, som USB-minnen, MP3-spelare, mobiltelefoner och bärbara hårdiskar hanterar idag en stor mängd information och dessutom erbjuder de funktioner som tidigare enbart kunde erbjudas av datorer. Ökad användning av dessa produkter medför nya överväganden när det gäller säkerhet. Dessa tekniker är lätt att ta med och därför lätt att tappa bort och om dessa hårdiskar då saknar kryptering av informationen kan detta leda till allvarliga problem för verksamheten. Även yttre hot kan förekomma med dessa tekniker. MSB skriver att till exempel mobiltelefoner kommer att utsättas för SMS-spam, virus och botnätattacker.

---

⁹ KOOBFACE var det första malware som lyckades och fortsatt att köra förökningsmaterial via sociala nätverk och är ett anagram av facebook- (Trend Micro, 2009)

¹⁰ Grundtanken med datormoln är att delar av ett nätverks resurser, eller till och med hela nätverket, kan flyttas ut på nätet och hanteras av ett annat företag (Söderlind, 2010)
4.1.5 Nya trender

**Verizon**
Verizon såg en enorm ökning av identifieringstypsstölder under 2008, detta innefattar stölder av lösenord och dylikt som används för att identifiera sig på olika tjänster på Internet. (Verizon business, 2009)

Figur 2: Förändringen av antalet skräddarsydda Malware använda vid dataintrång
Källa: (Verizon business, 2009, s. 22)

En annan trend som Verizon rapporterar om är hur olika typer av malware mer och mer börjar bli skräddarsydda för det offer eller organisation som är menad att motta till exempel masken eller trojanen. Under 2008 var 59 % av de intrång gjorda med malware gjorda med specialanpassade malwareprodukter. Detta kan sättas i jämförelse med året innan då samma sorts intrång låg på 24 %. (Verizon business, 2009)

**Symantec**
Fler och fler webbaserade attacker, hackare försöker attackera användarna istället för datorer. Under år 2008 var 63 % av de sårbarheter som upptäcktes och dokumenterades sådana som påverkade webbapplikationer. Detta är en ökning från 2007 då dessa var 59 %. Attackerna utnyttjar trafiken som går igenom HTTP\(^\text{11}\) och HTTPS\(^\text{12}\) protokoll då det är omöjligt att blockera denna trafik för att legitima organisationer är beroende av denna i deras dagliga arbete. Symantechs rapport menar att om en organisation skulle försöka filtrera denna trafik skulle all deras trafikgenomströmning sakta ner signifikant och detta skulle alltså skada deras verksamhet. En annan anledning till att denna form av attack blir allt mer attraktiv är det överflöd av dynamiska sidor som använder webbaserade applikationer, som forum, bloggar och webbshoppar. Dessa webbsidor används för att sprida skadlig kod och elakartad programvara för att webbapplikations sårbarheter sätter dem i större risk. (Symantec, 2009)

\(^{11}\) Hypertext transfer protocol, är ett kommunikationsprotokoll används för att överföra webbsidor över Internet (Gralla, 2007)

\(^{12}\) Hypertext transfer protocol secure, är ett protokoll för krypterad transport av data via HTTP- protokollet. (Gralla, 2007)

**Sophos**

**IBM**

---

13 Googles egna webbrowser som är gratis. Kommer med applikationer i basen, så som textredigerare, mail, kalender. (Google, 2010)
**MSB**

Nya tendenser som MSB rapporterar om är hur Internet går mot en mer användarstyrd miljö med hög interaktivitet, webb 2.0, och innefattar till exempel sociala nätverk. Dessa tjänster används både privat och inom näringslivet vilket gör att gränsen mellan arbete och privatliv suddas ut. Detta kan medföra säkerhetsrisken i och med att sårbarheterna i dessa tjänster kan utnyttjas för att få tillgång till organisationers interna nät. (MSB, 2009)

### 4.1.6 Skydda organisationen

**Verizon business**

I Verizons rapport från 2009 kunde de se att 87 % av alla intrång kunde ha undvikits med billiga och enkla medel. De mest rekommenderade skydden är:

- Kontrollera att säkerhetspolicys efterföljs.
- Se till att hela verksamheten är skyddad, inte bara delar av den.
- Utbilda anställda om risk och informationshantering. (Verizon business, 2009)

**Symantec**

Symantec menar att det finns flera sätt att sydda sig mot elakartade aktiviteter över Internet. Organisationer bör övervaka alla datorer som är sammankopplade i nätverk efter skadlig aktivitet, inkluderande botnätaktivitet och potentiella säkerhetsintrång, och göra klart att en infekterad dator tas bort från nätverket och rensas så snart som möjligt efter upptäckt. (Symantec, 2009)

Organisationer bör också använda antivirusprogram och brandvägg som kontinuerligt och regelbundet skall uppdateras. Administratörer på företaget skall även förvissa sig om att alla datorer, bärbara datorer och servrar är konstant uppdaterade. (Symantec, 2009)

Symantec rekommenderar även att organisationer och företag gör filtrering av både den ingående och den utgående nätverksstrafiken för att försäkra sig om att elakartade aktiviteter och otillåten kommunikation inte pågår på nätverket. Just filtrering av utgående nätverksstrafik är effektivt för att lindra DoS attacker. (Symantec, 2009)

Andra punkter som tas upp som viktiga för hur en organisation skyddar sig är till exempel, stäng av och ta bort applikationer som inte behövs, genomdriv en effektiv lösenordspolicy och utbilda personal till att inte öppna bifogade filer i inkommande e-post så länge filen inte förväntas eller kommer från en säker källa. (Symantec, 2009)

**Sophos**

För att skydda sig mot Web 2.0, sociala nätverk, attackerar Sophos att företagen inte ska blockera dessa tjänster då de anställda bara kommer försöka hitta andra sätt att komma åt dem. Detta kan då leda till andra säkerhetsbrister som är svåra att förutse. Istället menar Sophos att företaget ska utbilda personalen om de risker som kommer med sociala nätverk och Internet, samt att tillåta sociala nätverk över lunchtimmen bara och dessutom kontrollera vad det är för information som de anställda delar med sig av över Internet. (Sophos, 2009)
Sophos lägger även stor vikt på att företagen måste kryptera information, bärbara datorer och avtagbara lagringsanordningar för att förhindra dataläckage. Dessutom skall användaren av dessa hårdvaror och information kontrolleras att de hanterar dem på ett korrekt sätt. Så att de inte glöms på olämpliga ställen eller skickas på ett olämpligt sätt. (Sophos, 2009)

**Trustwave**


**IBM**

IBM anser att för att skydda sig är det bäst att enbart använda antivirusprogram- återförsäljare som har ett bra och välkänt rykte samt att alltid hålla antivirusprogrammet uppdaterat. (X-Force, 2010)

**Trend Micro**

Trend Micro anser att företag skall använda effektiva lösningar för att skydda sin verksamhet. Om företaget använder "cloud computing" bör de välja en lösning som har en säkerhetslösning just för molnet. (Trend Micro, 2009)

För att skydda sig mot förlorat förtroende från kunder genom olika sorters phishing anser Trend Micro att företagen bör köpa upp alla domäner som liknar deras varumärke. På detta sätt kan företaget själva ha kontroll över hur sin profil marknadsför överb Internet. (Trend Micro, 2009)

Dessutom anser Trend Micro att företaget bör införa effektiva IT-användningsriktlinjer för att förebygga sårbarheter. (Trend Micro, 2009)
### 4.2 Sammanfattning av rapporter

Sammanfattningen redovisas i två tabeller för att få en överblick av de skillnader och likheter som presenterade i rapporterna. Tabellerna utgår ifrån de rubriker som tagits upp i kapitel 4.1.

<table>
<thead>
<tr>
<th></th>
<th>Malware</th>
<th>Hackare</th>
<th>Mänskliga Faktorn</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verizon</strong></td>
<td>Vanligaste formen av hot mot ett företag</td>
<td>Hacking leder listan över vanligaste attacken över Internet</td>
<td>Tredje vanligaste medlet för intrång</td>
</tr>
<tr>
<td></td>
<td>Numera är malwares funktion övervägande spionage</td>
<td>Använder hacking för att ”ta sig in genom dörren”</td>
<td>Missbruk av privilegier i systemet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>74% av alla attacker kommer externt</td>
<td>Missbruk av användaruppgifter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intrång görs via applikationer</td>
<td></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>Vanligaste formen av hot mot ett företag</td>
<td>Använder hacking för att ”ta sig genom dörren”</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>68% är trojaner</td>
<td>Finansiella sektorn är målet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finansiella sektorn utsatt för phishing</td>
<td>Vid stöld av data användes keystroke logging som medel i 76% av fallen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ökning av infekterade datorer i botnät med 31%</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOPHOS</strong></td>
<td>40 000 misstänksamma filer varje dag</td>
<td>Använder SQL-Injections</td>
<td>Anställda delar med sig för mycket av känslig information i sociala nätverk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Använder Sociala Nätverk</td>
<td></td>
</tr>
<tr>
<td><strong>Trustwave</strong></td>
<td>1 54% av fallen använder hackare malware för att samla data</td>
<td>Utnyttjar existerande kanaler</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>86% av alla malware är trojaner</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>46% av alla malware är virus</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>22 miljoner prover av nya malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
<td>N/A</td>
<td>Phishing är ett betydande hot för företaget</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>MSB</strong></td>
<td>Varamann e-post inom en verksamhet är spam</td>
<td>Cyberbrottslingar som vill tjäna pengar</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>27 000 datorer anslutna till botnät i Sverige</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ny teknik</td>
<td>Nya Trender</td>
<td>Skydda Organisationen</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Verizon</strong></td>
<td>N/A</td>
<td>Enorm ökning i identifieringsstölder Kontrollera att säkerhetspolicys efterföljs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware blir mer och mer skräddarsydda Hela verksamheten skall vara skyddad</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Utbilda anställda</td>
<td></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>N/A</td>
<td>Mer sårbarheter i webbapplikationer Övervaka organisationens nätverk efter skadlig aktivitet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alla digitala hot ökar Ta bort och rensa infekterad dator</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus och brandvägg Filtra ingående och utgående trafik</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stäng av onödiga applikationer och onödig aktivitet</td>
<td></td>
</tr>
<tr>
<td><strong>Sophos</strong></td>
<td>Sociala nätverk leder till nya risker Spam börjar skickas över tjänster som MSN Utbilda anställda i riskerna med Internet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iPhone och andra ”Smartphones” utgör hot mot verksamheten Webbe-posttjänster är inte längre attraktiva medel för spammare Kontrollera vad för information som delas över nätverk. Kryptera information</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trustwave</strong></td>
<td>N/A</td>
<td>N/A Se över exakt vilka tillgångar organisationen har Bevaka och gör policy över relation med tredjepart</td>
<td></td>
</tr>
<tr>
<td><strong>IBM</strong></td>
<td>N/A</td>
<td>Inte längre OS som är problemet, numera är det applikationer Antivirus och andra säkerhetslösningar hos välkända leverantörer HåLLA säkerhetslösningarna uppdaterade</td>
<td></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
<td>Sociala Nätverk blir målet för allt fler cyberbrottsslingar N/A Specialanpassad säkerhetslösning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>”Cloud computing”, med enkla medel kan själva anslutningen till molnet slås ut Företag bör köpa upp domän med liknande namn</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MSB</strong></td>
<td>Mobila enheter är ett hot, dels p.g.a. ockuperad data men också yttre hot Webb 2.0 medför nya hot. Som sociala nätverk N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.3 Artiklar

Likt föregående avsnitt delas resultaten av artiklarna in i sex rubriker. Under varje rubrik presenteras artiklar som belyser respektive ämne.

4.3.1 Malware

Trojaner
I ett nummer av tidningen TechWorld från april 2009 rapporterar journalisten Joel Brandell att under det föregångna kvartalet bestod 71 % av all skadlig kod av trojaner och att det dessutom under denna period skapats omkring 5 miljoner nya varianter av skadlig kod vilket är ett rekord. Dagligen rapporteras det 50 000 nya fall av skadlig kod. (Brandell, 2009)

Spam

4.3.2 Hackare

Infekterad pdf

SQL-Injections
SQL-injections har alltid varit en mardröm för IT administratörer för att de har varit svårt att skydda sig mot. Hackare använde dessutom detta medel för att få tillgång till företags nätverk i 60 % av de betydande intrång som granskades av 7Safe, en ledande datorsäkerhet konsultfirma i London. Dessutom rapporterar samma konsultbolag att 80 % av alla intrång kom från attacker utifrån verksamheten och att 73 % av dessa klassades som ososfisterade intrång. Inte heller var det förvånande när det framkom siffror om att 86 % av attackerna skedde genom webbapplikationer. (Barret, 2010)

Stöld av data
I Computer Sweden kunde vi läsa att under 2008 drabbades 110 miljoner människor av förluster av känslig data. Första halvåret av 2009 var redan uppe i samma siffra. Till störst avseende är den känsliga dataen finansiell information. Denna enorma ökning tros bero på att fler använder IT-baserade tjänster för att till exempel uträta sina finansiella ärenden. (Wallenström, 2009)
4.3.3 Mänskliga faktorn

Trots ansträngningar från IT-avdelningen står det att anställda forstår att koppla bort eller ta bort krypteringslösningar på sina laptops och därmed möjliggöra att hemlig företagsinformation hamnar i fel händer om datorn stjäls. Till exempel kopplar cirka 60 % av företagsledarna i USA bort krypteringen. I Sverige beskriver 71 % av IT-personalen rapporterar att någon i deras organisation blivit bestulen på en laptop och 49 % rapporterar att detta har lett till dataintrång.

5 % av företagsledare i Sverige skriver ner sina lösenord på post-it lappar och 13 % delar med sig av sina lösenord till andra. (securityuser.com, 2010)

![Figur 4: Undersökning i PC för Alla](image)

Källa: (Appel, 2010, s. 45)

Enligt en undersökning i PC för alla slår var två av tre svenskar med sina lösenord. I undersökningen tillfrågades över 5000 datoranvändare angående deras lösenordshantering. På frågan hur ofta de byter sitt lösenord svarar 65,1 % att de byter sitt lösenord mer sällan än en gång per år. Dessutom svarar 76 % att de använder samma lösenord på flera ställen. (Appel, 2010)

4.3.4 Ny Teknik

*Mini-PC*

Nya tekniker leder till nya hotbilder som företag bör vara uppmärksam på. Enligt en artikel i Computerworld berättar journalisten John Edward om hur Mini-PC\(^\text{14}\) eller Ultraportables, som de benämns i artikeln, kan leda till allvarliga säkerhetsbrister i och med att dess processorer oftast halkat efter en generation eller två. Detta innebär att dessa datorer får kompromissa när det gäller mjukvaruprogrammen och använda äldre och mindre versioner av operativsystem som inte har samma säkerhetsfunktioner som de nyare operativsystemen med högre kapacitet. Mini-PC:s låga kapacitet innebär också att den har mindre möjlighet att använda extra

\(^{14}\) Till exempel de nya små bärbara datorerna som Asus Eee PC, Acer Aspire One och HP 2133 är så små och lätt; de har i regel en skärm på 7–10 tum och väger runt 1 kg. (Språkrådet, 2009)
säkerhetsfunktioner som kryptering och antimalwareverktyg, John Edward menar att detta innebär att dessa datorer används med liten eller ingen säkerhet. (Edward, 2008)

Cloud Computing
I en artikel i Computer Sweden pratar Per Brand, forskare på Swedish institute of computer science, om att det ännu inte är dags att lita på molntekniken. ”cloud computing” är idag attraktivt för många företag på grund av det låga priset men Per Brand menar att den ännu inte är mogen för användning. Det är inte bara det legala problemet med denna teknik som han anser är problemet, då man som företag egentligen inte vet vart i världen sin data kommer att placeras, utan att stora moln kan i fremtiden bli attraktiva måltavlor för hackare. Detta är något som företag och organisationer måste ha i åtanke innan de väljer en sådan tjänst. (Hellström, 2010)

Sociala Nätverk
I en artikel av PC för alla listar de olika faror som finns med Facebook. 2,9 miljonerna av de 350 miljoner medlemmarna på Facebook är idag svensk och IT-säkerhetsföretaget McAfee menar att facebook kommer att bli ett av de favoritverktygen för Internetbrottslingar. Till exempel varnar de för de olika applikationerna som finns på det sociala nätverket. Som IT-skurk kan de lura användarna att tro att det är en vanlig applikation men egentligen används den för att infektera användarens dator med skadlig kod. En annan fara med Facebook är att angripare kan kapa kontot, genom att på något sätt få fram lösenordet till kontot, på detta sätt kan angriparen lura dennes kontakter på pengar eller känsliga uppgifter. (Engström, 2010)


Mobiltelefoner

4.3.5 Nya Trender

I Computer Sweden kunde vi läsa i april 2010 om hur webbläsaren håller på att ta över rollen som operativsystem. Fler och fler applikationer körs numera i webbläsaren, i rask takt har vi börjat gå bort ifrån att en websida egentligen är en websida. Allt mer funktioner byggs in i sidorna vilket innebär att de blir mer complexa och att mer kod körs direkt i webbläsaren.
Detta är smidigt för både användaren och tjänsteleverantören då de får en snabb och välfungerande applikation utan att behöva installera något på sin dator utan kan köra det direkt i webbläsaren. Detta gör det dock enklare även för angriparen då det uppstår en rad säkerhetsrisiker när allt mer kod körs direkt i webbläsaren och säkerhetsprogrammen halkar efter. Jonas Renold som är säkerhetskonsult på Bitsec menar också att det inte finns något bra skydd mot sådana här attacker och sårbartigheter. (Stadigs, 2010)

4.3.6 Skydda organisationen

För att undvika skräppost skall man som individ och företag vara noga med antivirusprogram samt inte öppna e-post som kommer från okända avsändare. (Dalén & Hoppe, 2010)

I en artikel i TechWorld beskriver journalisten Tomas Gilså hur man som användare skall skydda sig mot trojaner. Det viktigaste är att hålla operativsystem, webbläsare och insticksprogram uppdaterade. Dessutom skall antalet program som har kontakt med Internet vara så få som möjligt. Ett antivirusprogram skadar inte, dock tar det inte bort risken att bli smittad helt utan ny skadlig kod skapas dagligen och antivirusprogrammen skyddar endast mot de redan kända malware. (Gilså, 2010)

4.4 Intervju 1

Den första intervjun genomfördes över telefon och respondenten är Per Hellqvist (Hellqvist, 2010) som arbetar som säkerhetsspecialist på Symantec.

4.4.1 Bakgrund

Per Hellqvist har arbetat med Informationsteknologisk- och Informationssystem-säkerhet sedan mitten på 90-talet. Pers huvudfokus har legat på malware men också ny teknik och nya trender inom säkerhet.


Per utsågs även till ”Årets Säkerhetsprofil” på Säkerhetsgalan 2010.

4.4.2 Resultat av intervju

De mest påtagliga hot
Det som är vanligast att man som angripare av ett företag försöker komma åt är inloggningssuppgifter och kreditkortsuppgifter. Det kan även vara så att angriparen försöker komma åt företagskänsliginformation för att använda denna information i någon form av
utpressning för att få pengar. Därför är det väldigt viktigt för ett företag att se över hur hanteringen av deras information görs.

**Trender**

En annan ny trend uppkom i januari 2004, då dök det upp trojaner som var specialskrivna för att stjäla information. Dessa trojaner och virus har alltid funnits men då i mycket mindre utsträckning. Plötsligt var ca 90 % av alla virus och trojaner specialskrivna för att stjäla information.

**Interna eller Externa**
Om de flesta attacker sker internt eller externt menar Per beror helt på vilka rapporter han läser. Interna attacker kan ske av tre olika typer av ”problempersoner”. Den snälla användaren som bara begär ett missstag, till exempel räkar han radera filer eller skickar ut känslig information till en hel e-postlista istället för en person. Den elake ”insidern” som av en eller annan anledning måste byta arbetsuppgifter och för att höja sitt värde på den nya arbetsplatsen bestämmer sig för att ta med företagskänslig information till den nya arbetsställen. Sist menar Per är den rena hackern som på något sätt gjort intrång i företagets nätverk och därifrån kan utföra attacker inifrån själva företaget.

Det finns olika tekniska lösningar för att ta hand om alla tre områden men det enklaste är antagligen att hålla i utbildningar för att de fel som begås av misstag kan hållas på så låg nivå som möjligt. Genom utbildning kan man få användaren att förstå vad han får och inte får göra för att undvika onödiga misstag. Om dessa misstag är under kontroll kan man som säkerhetsansvarig fokusera på övriga problemområden. Per anser att hackers har företag skyddat sig emot i så många år att de vet vad de ska göra, även fast det finns mycket jobb kvar har de ändå en sorts grundläggande kontroll på hur man skyddar sig.

**Arbetsplatsen**
I fall de flesta digitala hoten mot ett företag sker på eller utanför själva arbetsplatsen är svårt att definiera menar Per. Dels blir det skillnad på hur själva hotbilden ser ut hos företaget och

\(^{15}\) Ett virus som sprids via dokument, till exempel ett Word-dokument

**Ny teknik**


**Cloud Computing**


Samma problem blir det om företaget som levererar denna tjänst går i konkurs eller blir uppköpta. Kunden måste då veta vad som egentligen händer med de applikationer och den
information som finns i molnet. Kommer de bara att hamna på soptippen? Hur tas dessa data hand om?

Den andra saken man som kund till molntjänsten bör tänka på är hur är informationen skyddad. Sköter de det med till exempel nyckelhantering eller dylikt.

Det tredje med molntjänster som kanske är mest intressant är att fler och fler funktioner samlas i din webbläsare så webbläsarsäkerheten är ytterst viktig just nu. ”Elakingarna” har sen flera år tillbaka fått ökat intresse i särbarheterna i just webbläsarna samt insticksprogrammen till webbläsaren. Detta är en sådan enkel väg in i din dator. Till exempel kan jag skicka en länk via e-post som du klickar på och har personen som klickar på länken sårbarheter i en av webbläsarens insticksprogram kan man som angripare infektera datorn med trojaner mycket lättare. Ju fler applikationer som används i webbläsaren ju mer intressant blir det för ”elakingarna” att försöka komma in den vägen. Under många år har detta varit väldigt högt tryck mot tillverkare av webbläsare men nu tycker jag att tillverkarna måste tänka till ytterligare ett par snäpp så att de verkligen ser till att de släpper produkter med väldigt lite säkerhetshål.

**Skydda företaget**


Då det är just informationen som är det viktiga för företaget menar också Per att backupar är väldigt viktigt för ett företag. Ifall något händer ska det vara snabbt och enkelt som möjligt att återställa allting. Så att verksamheten kan fortsätta. Ifall attackerna gör datorerna obrukbara av en eller annan anledning ska det bara vara att springa på Elgiganten och köpa nya datorer sedan ladda backupen och verksamheten är igång igen.

Ett talesätt som Per använder är att en välhanterad dator är en säker dator. Detta innebär att det är viktigt att ha någon form av systemhanteringsverktyg i sin ”säkerhetsverktygsläda” så att det går snabbt och enkelt att uppdatera sin dator samt stänga av processer som ej används.

---

16 Den plattform som används, till exempel smartphone, stationär dator eller bärbar dator.
4.5 Intervju 2

Denna intervju genomfördes på MSB, Myndigheten för samhällskydd och beredskap, och respondenten var Svante Nygren (Nygren, 2010) som arbetar som säkerhetsspecialist på avdelningen för utvärdering och lärande.

4.5.1 Bakgrund


Svante brukar börja sin dag med att skanna igenom olika sorters media för att få en bild av avbrott i teknik eller dylikt. Han menar att det knappast är så att det är här man får reda på alla incidenter som förekommer men det är en bra början och ger en överblick över vad som händer i landet. Där samlar han inte bara info angående datainbrott eller hackerattacker utan även elavbrott eller driftavbrott i teknik.

4.5.2 Resultat av intervju

De mest påtagliga hot

Svante har skapat en tabell där han listat och graderat de olika slags attacker som finns i nivåer, efter hur det utförs:

- **Nivå 1:** Denna nivå avser till exempel blockering av webbsidor och klotter. Som att förändra ett företags logga på dess webbsida.
- **Nivå 2:** Omriktning av trafik och manipulering av information och data. Denna attack kan leda till mycket allvarligare konsekvenser. Till exempel om information angående vilket datum som vi i Sverige senast skall lämna in sin deklaration ändras på skatteverkets hemsida till ett senare, felaktigt datum.
- **Nivå 3:** Angrepp mot kritisk infrastruktur. Detta är snarare det man som angripare uppnår istället för sättet han gör de på. Det kan till exempel vara att slå ut elnätet, vattenledningarna eller kollektivtrafiken.

När det kommer till de mest påtagliga hoten rent allmänt så menar Svante att det egentligen inte är den organiserade hackerattackerarna som är de värsta. Det kan vara det som medför störst konsekvenser men inte de som är mest påtagliga. Han menar att det är komplexiteten och att företagen arbetar i för homogena miljöer som utgör större hot, till exempel nu när McAfee:s nya uppdatering av deras antivirusprogram raderade en systemfil för att programmet trodde filen var ett virus vilket gjorde att datorerna inte kunde starta. Det största problemet här var att företag och kommuner och län hade gemensamt skydd. Alltså samma antivirusprogram och detta gjorde att hela organisationer slogs ut.

Hackare är något spektakulärt som kan medföra stora konsekvenser men som ändå inte drabbar större delen av de svenska företag som finns.
Malware & Botnät
Svante förklarar att botnät alltid kommer att vara en plåga för alla användare av Internet men då de flesta botnät befinner sig i andra länder så är det lättare för oss i Sverige att filtrera bort den oönskade trafik som botnät kommer att medföra. Den senaste stora botnätattacken var 2007 när DNS servrar attackerades och hackarna lyckades slå ut två utav de 13 rotservrar som finns i världen.


Spam

DoS & DDoS

Mänskliga faktorn
Svante menar att de mest allvarliga hoten mot verksamheten är de som egentligen kan sammanfattas som mänskliga fel. Som exempel berättar Svante om en temepratursensor som glömde en bort att kontrolleras vilket ledde till att när serverhallarna överhettades så var det BIOS som varnade för det. Då denna varning då kommer från datorn och inte i hallen så var det närmare 75 grader inne i hallarna och alla servrar riskerade att förstöras helt.

Ett annat exempel är då e-post man som anställd skickat iväg uppgifter som är sekretessskyddade och dessutom räkta skicka ut det till en hel e-postlista istället för en enskild person. Svante nämner även McAfee:s snedsteg i mitten av April 2010 då de skickade ut en uppdatering av deras antivirusprogram. Där programmet började tro att en av datorns 17

---

17 De servrar som bland annat delegerar toppdomänen på Internet, t ex .net ,com eller .se
18 (Basic Input/Output System) Det mest grundläggande programmet i din dator som körs när datorn startar
systemfiler var ett virus och raderade den. Detta gjorde att de som hade detta antivirusprogram installerat inte längre kunde starta upp sin dator.

Ett annat fel som är relaterat till den mänskliga faktorn är att datorer som upptäcks vara infekterade med virus ändå inte rensas. Då de på vissa företag inte har rutin för det eller inte har med i organisationen det som berör informationssäkerhet och IT-säkerhet.

Ny teknik


Sociala medier anser Svante inte egentligen medför någon större risk än den. I varje fall inte i Sverige där nästan inga fall av attacker denna väg har rapporteras. Detta är snarare ett problem på individnivå. Han menar att det eventuella hot de kan se här är om personen som får sitt sociala nätverk kapat använder samma lösenord till alla sina olika tjänster på webben och till sina tjänster på arbetsplatsen. Så att den som angriper en användares sociala nätverk på detta sätt kan få tillgång till en arbetsplats system och nätverk.

Organiserad digital brottslighet

Vid frågan om den organiserade brottsligheten på nätet så svarade Svante att detta är något som är numera är mer påtagligt för den finansiella världen. Kreditkortsföretag kan till exempel idag alltid räkna med denna sorts attacker men att det är en risk de räknar med för att kunna tjäna pengar.

Och denna sortens attack kan även användas vid företagssionage men detta är inte heller kanske det vanligaste de stöter på. Svante anser ändå att det största hotet för företag och organisationer är just driftavbrott och att det är dessa som är vanligast.

Mest utsatta sektorn

När frågan om vilken sektor som Svante trodde var mest utsatt så svarade han med en annan fråga: ”Varför är du kriminell?”. Han menar att motivet alltid är pengar och därför är det den finansiella sektorn som är mest utsatt för hot. Där angriparen kan få tag i något av värde eller kan på något sätt omvandla det denne får tag på till något av värde.

4.6 Intervju 3

Den tredje intervjun genomfördes hos Sitic, Sveriges IT-incident centrum, där respondenten är Stefan B. Grinneby (Grinneby B, 2010) som är ansvarig för enheten.

4.6.1 Bakgrund

Stefan tog sin examen 1990 vid Uppsala universitet och det är en master of science i datavetenskap. Stefan har arbetat inom IT i 23 år, under denna tid har han arbetat med allt från programmering till sälj och projektledning. Sedan 2007 har Stefan arbetat som avdelningschef på avdelningen Sitic hos Post och Telestyrelsen. Sitic är Sveriges CSIRT (Computer Security Incident Response Team) och de arbetar med att förhindra, eller åtminstone snabbt mildra, effekterna av IT-incidenter på Internet.

4.6.2 Resultat av intervju

De mest påtagliga hot
Stefan berättar att det finns tre olika hot som är mest påtaglig för verksamheten hos ett medelstort företag:

- Förlorad kontroll och tillgång till verksamhetens data.
- Personer inom verksamheten som inte använder företagets produkter på ”rätt” sätt.
- Företaget används som en komponent i att komma åt större företag. Till exempel att man som angripare utnyttjar säkerhetsbrister hos företaget för att utföra större organiserade attacker.

De allvarligaste hoten kommer alltid inifrån ett företag, där personer som till exempel är anställda vid företaget medvetet försöker att skada verksamheten på ett eller annat sätt.

Nya Trender
Stefan anser inte att det förkommit så många nya trender på senaste tiden, för några år sedan så skedde dock en förändring i hur hackaren arbetar. Stefan menar att först så fanns det hackare för att skapa sig ett namn, det var nyt och häftigt att vara hackare. Numera är
hackaren snarare någon som finns för att tjäna pengar. Detta är dock inte helt nytt fenomen utan den förändringen skedde för ett antal år sedan.

En ny trend som uppkommit nu på senare tid är snarare att idag så kan en person som är relativt oerfaren inom teknik få tag i verktyg som kan hjälpa denne att ta kontroll över verksamheter. De nya digitala hoten kan alltså komma från personer som inte har nästan någon kännedom inom teknik men ändå bryta sig in hos verksamheter med stor IT-säkerhetskännedom.

**Nya tekniker**

”Cloud computing” anser Stefan idag att det enbart finns risker med, det enda som tycks vara relativt bra med denna nya teknik är den minskade kostnaden för företagen men att detta enbart kan locka företag att inhandla tjänsten utan att ens tänka på de risker som detta medför. Han säger att idag så finns det inga ordentliga säkerhetslösningar alls till denna nya teknik. I varje fall inga som är beprövade och testade till att fungera.


Sociala medier anser Stefan egentligen inte vara ett stort problem utan bara en ny kanal för hot som redan funnits. Sociala medier kommer dock antagligen att spela stor roll då angriparen försöker att skapa en form av förtroende med användaren som angriparen senare kan utnyttja till sin egen winning. Då det blir svårare och svårare att försöka tränga sig in rent tekniskt hos ett företag, tack vare mer sofistikerade antivirusprogram, brandväggar och mer fokus på själva IT- och informationssäkerheten, så kan detta bli ett större hot.

**Den mest utsatta sektorn**

Den mest utsatta sektorn kommer alltid att vara bank och finans menar Stefan. Där pengarna finns kommer det alltid att finnas skurkar som vill åt dem.


**Spam**

Spam är något företag måste se upp med även om detta kan anses som en obetydlig plåga. Ur en säkerhetssynpunkt skall man alltså inte strunta i att spam inkommer till företaget utan enligt bästa möjliga mån filtrera bort den då detta är det vanligaste hotet. Han säger att det är
så vanligt med spam just för att det faktiskt finns personer som tjänar pengar på detta och det kan vi inte skjuta under stolen med.

**Skydda verksamheten**

När det handlar om att skydda sitt företag och sin verksamhet måste man titta till vilka behov detta företag egentligen har. Till exempel så bör företaget se över om dess anställdes egentligen har behov av en webbrowser. Det som är dåligt med en brandvägg och ett antivirusprogram enbart ”blacklistar”, alltså helt enkelt inte tillåter viss trafik in och ut från företaget, och att detta inte är bra då det är lätt hänt att missa att inte tillåta en viss trafik. Stefan anser att man istället skall ”whitelist”, det vill säga att bestämma specifikt vilken trafik som är tillåten och hålla all annan trafik ute. På detta sätt så missas inte viss farlig trafik på grund av slarv och nya hot är lättare att hålla ute.

Dock så bör det hållas i åtanke att antivirusprogram skyddar ungefär mot 70 % av de vanliga malware som finns och kanske 0 % av de farligaste som kan användas mot ett företag.

Utbildning av personal är egentligen inte ett effektivt sätt att skydda företaget mot attacker. Han anser att detta inte skulle göra någon verklig skillnad. Då ett företags problem oftast är just att de inte använder en programvara på rätt sätt för att de inte läser instruktionerna så blir det detsamma när man försöker utbilda personal att göra rätt. De gör ändå fel.

**Varför denna hotbild?**

Stefan förklarar att han anser att denna stora hotbild fortfarande finns mot verksamheten samt anledningen till att den är påtaglig och konsekvenserna kan bli så hög är för att det är svårt för ett företag som inte har ett stort säkerhetsintresse att bry sig. Det är svårt att ponera i den exakta sannolikheten och därför inte förstå värdet i att skydda sig. Detta i kombination med otillräcklig kunskap i hur man som företag kan skydda sig gör att konsekvenserna av dessa attacker blir mycket större än vad de kan bli med små medel.

**4.7 Intervju 4**

Denna intervju genomfördes över telefon och respondenten var Torsten Enquist som arbetar som projektledare på TeliaSonera CERT CC. (Enquist, 2010)

**4.7.1 Bakgrund**

Torsten arbetar på en enhet hos TeliaSonera som heter TeliaSonera CERT som är en incidentorganisation som jobbar som ett samordnande organ med specialkompetens när det gäller IT-säkerhet. Dess arbete är att analysera och utvärdera de digitala hot som finns.

Torsten har arbetat 12 år på TeliaSonera CERT och har bakgrund som programmerare men har under hela sitt arbetsliv, sedan 1997, arbetat med just IT-säkerhetsfrågor.
4.7.2 Resultat av intervju

*De mest påtagliga hot*

Torsten förklarar att det finns de traditionella hoten mot verksamheter som är till exempel virus och phishing men de trendar han nu ser för företagen är just ”cloud computing” och ”outsourcing” och dessa medför helt nya hotbilder som bör utvärderas närmare av företagen. Torsten ser dock att den främsta hotbilden idag är olika former av malware och att dessa bara blir mer och mer sofistikerade. Olika former av malware är oftast svåra att särskilja så kan han inte säga exakt vilken som är mest förekommende men det är ändå trojaner som är de farligaste. Då trojanerna har inbyggda funktionaliteter som ”keylogge”, fjärranslutning och bakdörrar.

När det gäller attackerna så är det pengar som driver dem i en eller annan form. Numera är det inte längre någon som gör detta enbart för att de har ett brinnande teknikintresse. Antingen försöker angriparen få tag på information som angriparen kan sälja vidare och på så sätt tjäna pengar eller så försöker han få direkt tillgång till, till exempel, kredittkortsinformation.

Spionage kan även det vara en motivation för angrepp. Torsten anser att svenska företag har vanligtvis en liten väl blåögda inför detta hot. De flesta företagen inte tror att någon vill ha deras information och att detta tänk kan göra dem sårbara för dessa attacker.

*Organiserad digital brottslighet*

Enligt Torsten så är de angrepp som sker mot företag är mer eller mindre organiserad. Han menar dock inte den traditionella bilden av organiserad brottslighet, som till exempel maffian, utan snarare något som kallas för ”Networked Crime”. Detta innebär att det finns mindre specialiserade grupper som säljer tjänster emellan varandra. Det är alltså en grupp som specialiserar sig på att tillverka en viss typ av trojaner som en annan grupp köper för de har information om en viss typ av säkerhetsbrist hos ett företag och på så sätt blir det snarare som en kedja av brottslighet och inte den traditionella sortens organiserad brottslighet.

*Nya Trender*

De trenden som Torsten kan se när det gäller de digitala hoten är att all malware blir mer och mer sofistikerad och att man som företag inte egentligen kan förlika sig enbart på vanliga antivirusprogram. En trend som inte har förändrats men som heller inte är avtagande är att dessa former av digitala hot inte blir färre, utan hela tiden ökar. Torsten menar att de olika typerna av hot går i vågor, ibland så kommer en våg av phishing och nya virus men att de hela tiden avtar och byts ut mot något nytt, men att de som samling alltid ökar.

Alla sorters hot går lite hand i hand, som phishing e-post som länkar vidare till en hemsida där en infekterad programvara laddas ner till datorn. På så sätt så går spam, phishing och malware hand i hand och alltså svårt att urskilja exakt vilken sort attack som man själv blivit utsatt för. En annan förändring är att numera utnyttjas inte längre brister i operativsystemen särskilt mycket utan nu är det snarare brister i applikationer som används och utnyttjas vid attacker. Där målet är att använda dessa brister och installera vad än angriparen vill på datorn utan att upptäckas. Här menar Torsten att man som företag måste vara restriktiv med vad som får och inte får laddas ner på verksamhetens datorer.
**Mänsklig faktor**


Smartphones eller annan bärbar utrustning med nätverksanslutning medför alltid risker. Dock ser Torsten dessa risker som desamma som för en vanlig bärbar dator enda skillnaden är då att den utrustning som är bärbar och har nätverksanslutning bara blir fler och fler och detta leder då till att det blir fler och fler datorer som man som angripare kan attackera. Samt att det kan vara lätt att glömma att uppdatera all sin utrustning vilket kan leda till sårbarheter.

På individplan leder dessa SmartPhones dock till nya hot då de har ett inbyggt simkort vilket gör att om en telefon blir infekterad med ett virus så kan kanske detta virus användas för att skicka tusentals sms till en betaltjänst och på så sätt tjänar angriparen pengar.

Sociala medier är något som man som företag kan försöka stoppa men som antagligen inte går. Det som är det största hotet med detta är mängden av information som flödar mellan personer över nätverket och att man som arbetsgivare inte har kontroll över vad som spreds. Som till exempel intern information som inte får läckas utåt. Detta är något som en arbetsgivare måste tänka över och se över för att få bättre kontroll över menar Torsten.

**Arbetsplatsen**


**Skydda verksamheten**

För att skydda sitt företag bäst anser Torsten att man ska använda en kombination av utbildning, antivirus, brandväggar och restriktioner när det gäller nyttjandet av nätet. Företagen bör även se över de arbetsuppgifter som en anställd har för att kanske tänka på vad som egentligen är nödvändigt för denne att inneha på sin dator. Till exempel i ett kundtjänstyrke kanske det inte är nödvändigt med en tjock klient med stor användarfrihet utan här kanske det är bättre att använda en tunn klient med visst antal applikationer och restriktioner på användning av den. Medan en IT-tekniker behöver större frihet i sin miljö annars kan det leda till irritation och att denne inte kan utföra sina uppgifter korrekt.
## 4.8 Sammanfattning av intervjuer

Sammanfattningen av artiklarna visas nedan i en tabell där jag sammanfattar i punktform vad varje respondent sa angående rubrikerna som är listade.

<table>
<thead>
<tr>
<th></th>
<th>Intervju 1 (Symantec)</th>
<th>Intervju 2 (MSB)</th>
<th>Intervju 3 (Sitic)</th>
<th>Intervju 4 (TeliaSoneraCERT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>De mest påtagliga hot</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angripare som försöker komma åt inloggningssuppgifter</td>
<td>Komplexiteten i systemen</td>
<td>Förlorad kontroll av data</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>Försöker få tag i företagskänslig-information</td>
<td>För homogena miljöer</td>
<td>Personer använder inte produkter ”rätt”</td>
<td>Trojaner är de farligaste</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Nya trender</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004 blev det mer organiserad brottslighet, för pengar</td>
<td>Mer organiserad brottslighet</td>
<td>Angripare försöker numera tjäna pengar</td>
<td>Malware blir allt mer sofistikerad</td>
<td></td>
</tr>
<tr>
<td>Började sälja trojaner eller information om säkerhetshåll</td>
<td>Angriper finansiella sektorn</td>
<td>Relativt oerfarna inom teknik kan numera angripa företag digitalt</td>
<td>Digitala hot blir allt fler</td>
<td></td>
</tr>
<tr>
<td>Specialskrivna trojaner som stjäl information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webbläsare, större intresse för angripare</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mänsklig faktor</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Allvarligaste konsekvensen</td>
<td>Människor har svårt att greppa vikten i informations och IT-säkerhet</td>
<td>Människor kommer alltid att fela</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ny teknik</td>
<td>Intervju 1 (Symantec)</td>
<td>Intervju 2 (MSB)</td>
<td>Intervju 3 (Sicit)</td>
<td>Intervju 4 (TeliaSoneraCERT)</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Hur är informationen skyddad i molnet?</td>
<td>&quot;Cloud computing&quot;, driftsäkerhet</td>
<td>&quot;Cloud computing&quot;</td>
<td>&quot;Cloud computing&quot; finns det enbart risker med</td>
<td>&quot;SmartPhones&quot;</td>
</tr>
<tr>
<td>Sociala medier inte någon större risk</td>
<td></td>
<td></td>
<td>Sociala Medier</td>
<td></td>
</tr>
<tr>
<td>Skydda verksamheten</td>
<td>Håll informationen säker</td>
<td>N/A</td>
<td>Vilka behov har organisationen?</td>
<td>Utbildning, antivirus, brandväggar och restriktioner</td>
</tr>
<tr>
<td>Säkerhetslösningar från samma leverantör</td>
<td></td>
<td></td>
<td>Whitelista istället för blacklista</td>
<td>Måste se till vilka applikationer som egentligen behövs</td>
</tr>
<tr>
<td>Backup!</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utbildning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5 Avslutande del

Detta kapitel skall ge läsaren en avslutande diskussion som belyser de likheter och olikheter som funnits i studiens resultat. Sist visas en sammanfattnings där studiens huvudfråga besvaras samt de två underfrågor som presenterades i första kapitlet, Inledning.

5.1 Diskussion

I denna del av delen av uppsatsen skall jag diskutera kring rubrikerna malware, hacking, mänsklig faktor, ny teknik, nya trender och hur företaget kan skyddas utifrån mitt resultat i det tidigare kapiteln.

5.1.1 Malware


Malware & Hackare

En person som gör intrång på ett nätverk åt en verksamhet använder inte sällan just malware för att sedan kunna samla och stjälja data. Därför så går hacking och malware hand i hand och är inte alltid lätt att särskilja på. Till exempel en trojan som är programmerad att öppna en bakdörr i ett system för framtida intrång. Även om just malware är den vanligaste formen av hot mot ett företag så går konsekvensen upp avsevärt om den utförs i kombination med hacking. Större delen av malware idag är dessutom designad i syfte att spionera och stjäla information. Detta påvisar även tesen att malware används i samarbete med hacking.

Malwares uppgifter

Spam


5.1.2 Hackare/ Angripare

Tillvägagångssätt


Några av andra tillvägagångssätt som vi kunnat läsa om i resultatet är bland annat infekterade PDF:er som lätt kan användas för att få tillgång till en verksamhets nätverk. Dessutom kan denna form av attack bli närmare omöjlig att spåra om angriparen använder ett oskyddat trådlöst nätverk för att skicka den infekterade PDF:en.

Mål

5.1.3 Mänsklig Faktor


Sårbarheter hos verksamheten kan även bero på ren lathet, att organisationen känner till säkerhetsbrister men helt enkelt inte gör något åt detta av en eller annan anledning. Till exempel infekterade datorer som inte rensas.

5.1.4 Ny Teknik

Många av de nya kommande teknikerna leder till att företagen måste försöka ligga steget före när det gäller det nya hotbilderna och snabbt ta upp dem på agendan. Ett flertal nya tekniker har tagits upp i denna studie men det som rapporter och respondenter varit rörande överrens om är att sociala nätverk, ”smartphones” och, speciellt, cloud computing är tre nya tekniker som företag måste beakta då de ser över sin säkerhet.

Sociala nätverk


SmartPhones


Mängden av applikationer som dyker upp till denna sortens mobiltelefon är dessutom stor och snabbt växande. Som vi har kunnat läsa i rapporten är just applikationer en stor sårbarhet och därför ett mål för hackare. Därför kommer antagligen dessa mobiltelefoner att utnyttjas för dataintrång mer och mer i framtiden ju fler applikationer som finns att tillgå.
Cloud computing


5.1.5 Nya Trender

Hackare/angripare


Organiserad brottslighet

Pengar har varit motivet för intrång nu i många år och kan antagligen inte räknas som en ny trend. De åren då hackaren var en ung tjej eller kille som bara ville testa sina tekniska förmågor och bli världskändis över Internet är sedan länge förbi. Det som dock påvisats i denna studie är att det börjat bli mer av en organiserad brottslighet över Internet, något Torsten Engquist på TeliaSonera CERT kallade för ”Networked Crime”. Där det finns en marknad att köpa och beställa olika sorters malware för att utnyttja säkerhetsbrister hos företag. Vilket innebär att man som relativt tekniskt okunnig ändå kan utföra allvarliga dataintrång his organisationer. Detta anser jag påvisats i och med att malware blir mer och mer skräddarsydda för specifika uppgifter och att det på ett snabbare och mer effektivt sätt kommer ut på marknaden. Enligt Symantec beror detta på att det är mer lönsamt numa att tillverka malware. Det visar att det finns en marknad för att sälja malware samt att någon
måste sitta med informationen angående säkerhetsbristerna och göra beställningen av den skräddarsydda trojanen.

5.1.6 Skydda Företaget


För ett medelstort företag i Sverige är säkerhetslösningar som är av den billigare sorten samt lätt att underhålla som kan vara mer betydande. Därför är alternativet, som flera av rapporterna och respondenterna i intervjuerna var överens om, att använda antivirusprogram och brandvägg det mest grundläggande för säkerheten inom organisationen. Då måste detta självklart underhållas och uppdateras för att detta skall anses som ett reellt skydd. Denna studie har belyst just att det växande antalet malware, i form av virus, trojaner och maskar, är enormt. Vilket innebär att om inte säkerhetslösningar och andra system knutna till verksamheten uppdateras regelbundet gör skydden näst intill ingen skillnad från att inte ha något skydd alls.
5.2 **Slutsats**

I detta kapitel skall jag besvara frågorna som presenterades i inledningen av denna studie.

5.2.1 **Hur ser hotbilden ut för ett medelstort företag i Sverige idag?**

Hotbilden skiljer sig självklart beroende på vad för verksamhet företaget bedriver. Dock då denna studie ämnar ge en generell överblick har jag valt att försöka illustrera de existerande hoten i en bild som gjorts efter studiens resultat och diskussion.

Bilden är en illustration av en organisation, där kärnan är de hot som finns inom väggarna av organisationen. Det ljusare fältet skall visa relationen med kunder, leverantörer och även de anställda då de ej vistas på arbetsplatsen. De yttersta delarna är de yttre hoten som finns mot organisationen.

<table>
<thead>
<tr>
<th>Hot</th>
<th>Sannolikhet</th>
<th>Konsekvens</th>
<th>Förklaring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slarv</td>
<td>HÖG</td>
<td>MEDEL</td>
<td>Den mänskliga faktorn med slarv eller misstag kommer alltid att finnas på arbetsplatsen. Därför graderas denna med hög sannolikhet. Däremot är konsekvensen olika. Ibland gör det ingen skillnad och ibland, som med McAfee och antivirusuppdateringen, kan det förstöra för hela verksamheten.</td>
</tr>
<tr>
<td>Felaktig hantering av resurs</td>
<td>MEDEL</td>
<td>LÅG</td>
<td>Att nyttja resurserna hos organisationen felaktigt kan leda till problem för organisationen. Väldigt sällan har detta stora konsekvenser men händer ändå alltför ofta.</td>
</tr>
<tr>
<td>Datastöld</td>
<td>LÅG</td>
<td>HÖG</td>
<td>Detta är ett hot inifrån organisationen. Att en anställd skulle stjäla data har väldigt låg sannolikhet men konsekvenserna kan vara stora för organisationen.</td>
</tr>
<tr>
<td>Lösenordslarv</td>
<td>HÖG</td>
<td>HÖG</td>
<td>Som det påvisats i denna uppsats resultat är sannolikheten för att någon form av lösenordsslav inträffar väldig hög. Detta kan dessutom leda till allvarliga konsekvenser för en verksamhet då detta lätt kan ge tillgång till systemet och nätverket för utomstående.</td>
</tr>
<tr>
<td>Stöld av datalagringsenhet</td>
<td>LÅG</td>
<td>HÖG</td>
<td>Idag då datalagringenheter blir mer portabla och dessutom finns i till exempel våra mobiltelefoner är det större sannolikhet att detta kan hända idag. Dock är sannolikheten för detta fortfarande relativt låg men konsekvenserna för att en datalagringenhet med okrypterad data skulle falla i fel händer är väldigt hög för en verksamhet.</td>
</tr>
<tr>
<td>Driftavbrott</td>
<td>MEDEL</td>
<td>MEDEL</td>
<td>Driftavbrott i form av till exempel avgrävda kablar eller förlorad trasig maskinvara är en relativt vanlig företeelse och kommer antagligen att drabba de flesta verksamheter vid ett eller annat tillfälle. Konsekvenserna är dock medelstora då de oftast är lätt att åtgärda men kan skada verksamheten om avbrottet varar en längre tid.</td>
</tr>
<tr>
<td></td>
<td>Spam</td>
<td>Phishing</td>
<td>Hacking</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Hög</td>
<td>Låg</td>
<td>Hög</td>
</tr>
</tbody>
</table>

**Spam**

Enligt Sophos undersökningar då var närmare 90 % av all e-post inom en verksamhet spam, därför är sannolikheten för detta hög. Konsekvenserna för verksamheten är dock relativt låg då de flesta spam egentligen bara gör mot verksamheten är att att tid från de anställda då de måste radera dem.

**Phishing**


**Hacking**


**Maskar**

Mängden malware ökar årligen och det ser inte ut att avta där för är sannolikheten för att ett företag kommer att råka ut för detta väldigt högt. Maskars syfte är dock egentligen bara att kopiera sig själv och skicka sig vidare vilket gör att konsekvenserna är relativt låg.

**Trojaner**

Mängden malware ökar årligen och det ser inte ut att avta där för är sannolikheten för att ett företag kommer att råka ut för detta väldigt högt, då trojaner dels är den största andelen av malware och dessutom oftast har till uppgift att lagra och skicka data över Internet är har detta hot högre konsekvens än andra malware.

**Virus**

Mängden malware ökar årligen och det ser inte ut att avta där för är sannolikheten för att ett företag kommer att råka ut för detta väldigt högt. Enligt rapporterna är de flesta virus är mer eller mindre harmlösa i jämförelse med trojaner.
Figur 6: Konsekvens- och Sannolikhetsmatris

Denna matris är baserad på konsekvens och sannolikhetstabellen ovanför. Ingen av de hot som identifierats i denna uppsats hamnade i det gröna fältet, låg sannolikhet och låg konsekvens. Detta beror på att ingen av hoten är obetydande för en verksamhet. Speciellt om organisationen inte vidtagit några säkerhetsåtgärder. Det som också går att utläsa av matrisen är att slarv och lösenordslarv är i det röda fältet. Dessa två hot är dessutom svårast att undvika, det finns inget filter för mänskliga fel och slarv. Även om rapporterna inte tog upp många nämnbare siffror i just den mänskliga faktorn nämnde nästan varje rapport samt respondent i intervjuerna det hot som kan leda till de allvarligaste konsekvenserna. De hot som kommer utifrån en verksamhet hamnade nästan ingen av dem i det röda fältet, detta beror på att medelstora företag i Sverige generellt inte utpekades som mål för riktade attacker.
5.2.2 Hur kan ett företag skydda sig?

Det finns en otrolig mängd alternativ för ett företag att skydda sig. Utifrån mitt resultat och diskussion har jag gjort en kort lista med förklaringar.

<table>
<thead>
<tr>
<th>#</th>
<th>Säkerhetslösning</th>
<th>Förklaring</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Antivirus och Brandägg</td>
<td>Grundläggande skydd för datorn och nätverket, viktigt att tänka på vilken leverantör som används.</td>
</tr>
<tr>
<td>2</td>
<td>Utbilda Anställda</td>
<td>Även om fel kan uppstå oavsett hur mycket utbildning som ges kan denna punkt inte hoppas över då konsekvenserna för ett internt dataintrång, medvetet eller omedvetet, ofta är mycket allvarligare än de externa.</td>
</tr>
<tr>
<td>4</td>
<td>Säkerhetspolicy</td>
<td>En säkerhetspolicy är alltid bra att luta sig tillbaka på om frågor uppstår. Det som dock är viktigt med den är att den efterföljs. Därför är det viktigt att vidta åtgärder för att detta görs.</td>
</tr>
<tr>
<td>5</td>
<td>Skydda information</td>
<td>Genom till exempel kryptering av hårddiskar. Dock för att kunna skydda den information som företaget besitter måste även företaget veta VAD för information de faktiskt besitter.</td>
</tr>
</tbody>
</table>

5.2.3 Hur ser framtiden ut?

Att ponera om framtiden kan tänkas bli ett svårt arbete och denna slutsats kan mycket väl se helt annorlunda ut inom bara ett par veckor då det mesta inom Internet och IT kan förändras över en natt. Dock drar jag några slutsatser utifrån studiens resultat och diskussion.

- De sociala nätverken kommer att växa sig större med fler användare och därför bli ett mer attraktivt mål för nätbedragare och andra cyberbrottlingar.
- Den generella samlingen malware kommer att fortsätta att växa.
- ”Cloud computing” kommer att användas av allt fler organisationer och därmed likt sociala nätverk bli mer attraktivt för cyberbrottlingar.
- Operativ System kommer knappt att användas alls som medel för dataintrång.
- Spam kommer fortsätta att öka.
- Malwares primära uppgifter kommer att vara att samla och skicka data över Internet.
- Det kommer inte längre vara möjligt att dela in malware i olika klasser.
6 Metodutvärdering

I detta kapitel skall studien försöka utvärdera metoderna som är använda vid studien samt ge förslag till fortsatt studie.

6.1 Teori

Genom ett medvetet val av relevant litteratur har jag skapat mer av en begreppslista i min teori då jag förklarat de olika digitala hoten som nämns i denna studies empiri.

Jag valde medvetet att låta företagens egna organisationsbeskrivningar finnas med i teorin då min uppgift med studien inte var att kritiskt granska de olika företagen och myndigheterna som upprättat rapporterna utan snarare ge läsaren en förståelse vilka som upprättat rapporterna och hur de samlat sin data.

6.2 Empiri

Vid genomförande av den emiriska studien har min kvalitativa metod varit ett stöd för att få svar på studiens forskningsfrågor. Jag upplever att det var relevant att genomföra personliga intervjuer för att få en djupare uppfattning av nyckelpersoner som dagligen arbetar med dessa frågor och på så sätt mer tillförlitligt bidrag till studiens empiriska del.

Positiva aspekter

Mängden rapporter som jag utvärderade och bedömde att vara underlag för denna studie var mycket omfattande och jag gjorde tidigt ett val vilka punkter som jag ville belysa under arbetets gång. Detta gör att valet av rapporter är väl grundat och dessutom ger en bred vy då dessa rapporter kommer från ett flertal organisationer med olika bakgrund, verksamheter och de har dessutom olika insamlingstekniker till de olika rapporterna.


Negativa aspekter

Som jag tidigare diskuterade så var mängden av rapporter omfattande, jag bedömer att jag gjort ett lämpligt urval och spridd information men detta har ändå medfört att jag varit tvungen att välja bort information som kan ha bedömts av andra som relevant information för studien.
6.3 Studiens kunskapsbidrag

Resultatet för denna studie skall kunna användas av företag för att ge en överblick över de hot de själva utsätts för och väcka frågor hos organisationen som kan hjälpa dem att förbättra skyddet hos organisationen.

6.4 Förslag på fortsatt forskning

Denna studie skall kunna bidra till fortsatt forskning inom området genom att ställa denna studie mot ett medelstort företag för att analysera hur den verkliga hotbilden upplevs. Denna studie baseras på rapporter från organisationer som sammanställts för att ge en generell överblick av hotbilden. Det som vore intressant för framtida forskning är alltså att se om detta stämmer hos ett verkligt, medelstort företag i Sverige.
7 Litteraturförteckning


Symantec. (den 24 04 2010). Symantec Corporate Fact Sheet. USA.


7.1 Tidsskrifter

Dalén, K., & Hoppe, K. (den 2 Januari 2010). Expert varnar för rekordstor spamattack. *DN s. 54*.


Danielsson, L. (den 11 November 2009). ...och bedrägerierna ökar i sociala medier. Computer Sweden, s 33.


7.1.1 Elektroniska artiklar


7.2 Elektroniska källor


7.3 **Intervjuer**
Grinneby B. S. (den 05 Maj 2010). Säkerhetsspecialist. (M. Carlsson, Intervjuare)
Hellqvist, P. (den 03 Maj 2010). Säkerhetsspecialist. (M. Carlsson, Intervjuare)
Engquist, T. (den 06 Maj 2010). Projektledare (M.Carlsson, Intervjuare)
8 Bilagor

8.1 Intervjufrågor

- Berätta om dig själv och ditt jobb.
  - Vad är dina arbetsuppgifter?
  - Hur länge har du jobbat inom branschen?
  - Hur länge har du jobbat på denna arbetsplats?

- Vilket/vilka hot anser du vara mest påtaglig?

- Vem är angriparen?

- Vad har du märkt för trender när det gäller digitala hot?

- Hur tror du all den nya teknik som kommer nu påverkar de hot som finns?

- Är det på arbetsplatsen de flesta hoten finns för företaget?

- Hur skall ett företag skydda sig?