Beredskap mot skadlig kod

EN KARTLÄGGNING AV IT- OCH INFORMATIONSSÄKERHETEN
INOM STÖRRE MYNDIGHETER OCH STATLIGA BOLAG
I SVERIGE MED FÖRDJUPAD ANALYS AV SKADLIG KOD

KBM:S TEMASERIE | 2005:1

KRISBEREDSKAPS
MYNDIGHETEN

KBM:S TEMASERIE | 2005:1

Beredskap mot skadlig kod

EN KARTLÄGGNING AV IT- OCH INFORMATIONSSÄKERHETEN INOM STÖRRE MYNDIGHETER OCH STATLIGA BOLAG I SVERIGE MED FÖRDJUPAD ANALYS AV SKADLIG KOD

Titel: Beredskap mot skadlig kod – en kartläggning av IT- och informationssäkerheten inom större myndigheter och statliga bolag i Sverige med fördjupad analys av skadlig kod
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Photo Disc
Upplaga: 1 500 ex

ISSN: 1652-2915
ISBN: 91-85053-72-4
KBM:s dnr: 0797/2004
Författare: Opticom International Research
Grafisk form: AB Typoform
Tryck: Edita, Västerås 2005

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning.
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

KBM:s temaserie 2005:1

Innehåll

Förord

En viktig uppgift för Krisberedskapsmyndigheten (KBM) i dess strävan att samordna arbetet kring samhällets beredskap inför allvarliga kriser, är att samla in information om IT- och informationssäkerhet i det offentliga Sverige och ta del av olika resonemang som förs kring dessa frågor. Påverkan av samhällsviktiga IT-system har de senaste åren utvecklats till ett allvarligt hot mot olika funktioner i samhället. I syfte att öka kunskapen om hur skadlig kod sprids samt hur systemägare har utvecklat arbetet med att skydda sig mot skadlig kod har KBM initierat denna studie.

Det främsta syftet med studien är att kartlägga utformningen av, och rutiner kring, IT- och informationssäkerheten hos ett antal större myndigheter och statliga bolag i Sverige. Utöver detta är målet med studien att få svar på följande frågor:

- Vilken betydelse har IT-systemen för de undersökta organisationerna och vilka externa krav ställs på dem?
- Hur ser organisationernas IT- och informationssäkerhet ut generellt och i krissituationer?
- Hur är beredskapen vad det gäller skyddet mot skadlig kod och hur har organisationerna eventuellt blivit drabbade?
  - Vilken påverkan har skadlig kod haft på samhällsviktig infrastruktur?
  - Vilka kaskadeffekter har detta haft?
  - Skulle samhällsviktig infrastruktur ha kunnat skyddats bättre?
  - Vad kan göras för att förbättra skyddet utifrån dagens förutsättningar?
- Hur står sig IT- och informationssäkerheten i svenska myndigheter och statliga bolag jämfört med privata företag?

Staffan Karlsson
Chef informationssäkerhets- och analysenheten
Krisberedskapsmyndigheten

Presentation av författarna

Under hösten 2004 har Opticom International Research, på uppdrag av Krisberedskapsmyndigheten, gjort en studie om IT- och informationssäkerhet och beredskap mot skadlig kod hos ett antal större myndigheter och statliga bolag i Sverige.

Opticom International Research är ett konsultföretag som är specialiserat på internationella marknadsanalyser och rådgivning. Sedan starten 1987 har Opticom genomfört över 500 uppdrag i fler än 70 länder. Opticom omfattar fyra affärsområden, alla riktade till behoven av olika kundgrupper och marknader. Utöver IT & Telecom-divisionen finns divisioner inriktade på företag inom pappersindustrin, läkemedelsindustrin samt en division vars kunder finns inom övriga näringslivssektorer och den offentliga sektorn. Som en global leverantör av marknadsanalystjänster kan Opticom erbjuda ett övergripande strategisk synsätt i kombination med ett mikroperspektiv där varje marknad och varje målgrupp analyseras.

Sammanfattning

Övergripande slutsatser

Under hösten 2004 har Opticom International Research utfört en studie om IT- och informationssäkerhet och beredskap mot skadlig kod inom stora offentliga organisationer i Sverige. Studien har gjorts på uppdrag av Krisberedskapsmyndigheten (KBM). Utgångspunkten för studien har varit att kartlägga utformningen av, och rutinerna kring, IT- och informationssäkerheten på ett antal större myndigheter och statliga bolag i Sverige, med en fördjupad analys av beredskapen mot skadlig kod. För att få en djupare förståelse av alla aspekter som är av intresse på detta område har Opticom valt att göra besöksintervjuer med 22 respondenter i fjorton olika organisationer, samtliga med viktiga samhällsfunktioner. Utöver dessa besöksintervjuer har en mindre tilläggsstudie gjorts per telefon bland 10 företag inom det svenska näringslivet, med syfte att se hur resultatet för myndigheter och statliga bolag står sig i förhållande till IT- och informationssäkerhetsnivån på privata företag.

Opticoms övergripande slutsats är att IT- och informationssäkerheten inom myndigheter och statliga bolag har höjts betydligt under de senaste tre-fyra åren. I många fall är det intrång med skadlig kod i den egna organisationen som ligger till grund för en större satsning på IT-säkerhet. Denna grupp av myndigheter och statliga bolag skulle kunna betecknas som *reaktiva drabbade*. För ett antal andra organisationer är det snarare incidenter som andra aktörer råkat ut för som har satt igång den här processen. Här skulle man kunna tala om *reaktiva icke-drabbade*. Bara ytterst få aktörer tänker långsiktigt inom alla de av Opticom undersökta områdena och visar sig därmed vara *pro-aktiva icke-drabbade*.

Det finns två viktiga *interna* skäl till varför det generella beteendet är reaktivt snarare än pro-aktivt:

1. Brist på medvetande om att det finns sårbarheter i IT-miljön och/eller brist på kunskap om hur man ökar skyddet gör att man behåller vissa rutiner eller tekniska lösningar som inte är optimala ur IT-säkerhetssynpunkt.

2. I organisationer där en del av nyckelpersonerna är medvetna om sårbarheter kan det ändå vara svårt att få till stånd en förändring p.g.a. svårigheter att förankra en högre säkerhetsnivå högre upp i organisationen. Anledningen är ofta inte pengar utan att den tilltänkta lösningen i för hög grad påverkar systemens funktionalitet.

Det finns också exempel på myndigheter och statliga bolag där både IT-chefer och ledningen är helt med på att förbättra eller bibehålla de nuvarande skyddsnivåerna, men där man känner att vissa *externa förutsättningar* gör det svårt att uppnå alla mål:

1. En del organisationer upplever att det finns en spänning mellan den offentliga förvaltningsmodellen och försöken att optimera IT-säkerheten. Den yttrar sig framför allt i situationer där krav på (ökad) öppenhet, t.ex. i samband med hantering av inkommande handlingar i elektroniskt format eller 24-timmarsmyndighetssatsningen, innebär en ökad exponering mot källor av skadlig kod. I vilken utsträckning detta beror på ett verkligt problem eller informationsbrist är svårt att avgöra, men det är viktigt att uppmärksamma dessa signaler.
2. Det är inte ovanligt att organisationer känner sig som leverantörens fångar. De är för små för att själva kräva en viss standard eller ett större utbud av lösningar. En gemensam kravställare från statens sida (t.ex. mot leverantörer av IP-telefoni) skulle underlätta för många aktörer.

Den upprustning som gjorts under de senaste åren är i första hand av teknisk karaktär, med fokus på brandväggslösningar, virusskydd, nya patchningsrutiner och ibland en mer robust strömförsörjning. Nästa steg har varit att se över mjuka faktorer som förbättrade administrativa rutiner, ökad medvetenhet och kompetensutbildning. Den erfarenhet som många respondenter har är dock att det fortfarande finns för många exempel som visar att de anställda saknar kunskap samt att de som är insatta kanske inte följer de regler och rutiner som finns. Att förbättra IT-miljön med hjälp av tekniska lösningar är mycket viktigt, men det finns en gräns där det inte längre är meningsfullt att investera i hård- och mjukvara om inte den interna medvetenheten och disciplinen också förbättras.

Givetvis är bilden mycket varierande och det finns exempel på organisationer som lyckats bra i sina försök att öka medvetenheten om IT-säkerhet, förbättra kommunikationsrutinerna och ständigt uppdatera dokumentationen. De flesta organisationer har dessvärre inte kommit så långt. Det som däremot är positivt är att intervjupersonerna ofta själva vet att säkerhetsnivån inte är tillräckligt bra och att detta innebär sårbarhet i skyddet av IT-systemet och information.

De incidenter med intrång av skadlig kod som respondenterna har velat diskutera med Opticom har i vissa fall

varit allvarliga, men skadorna har begränsats till att gälla de administrativa stödfunktionerna. I och med att kärnverksamheten inte påverkats nämnvärt har det inte funnits många exempel på externa kaskadeffekter. I de fall där avbrotten var märkbara utanför organisationen har effekterna varit ganska kortvariga och av lokal karaktär. Internt har skadorna dock varit större, både i förlorad produktion och i en kraftigt ökad arbetsbelastning för IT-personalen. De typer av skadlig kod som oftast nämndes bland de drabbade organisationerna var Loveletter, Nimda, Sasser och Blaster. Bara ett fåtal organisationer har sluppit incidenter helt och hållet.

Den främsta skillnaden mellan statliga organisationer och privata företag är att kraven på IT- och informationssäkerhet inom näringslivet generellt är något lägre än på den offentliga sidan. Visserligen är de kommersiella intressena inom näringslivet mycket stora, men ett stort avbrott skulle i många fall inte ha lika stor påverkan på den interna verksamheten eller på samhällskritisk infrastruktur. Mot bakgrund av att IT-säkerhetsnivån inom de företag som ingår i denna studie ändå bedöms vara lika hög som säkerhetsnivån för myndigheter och statliga bolag kan man dra slutsatsen att privata företag ligger närmare den för dem optimala IT- och informationssäkerhetsnivån än statliga organisationer.

Ett annat konstaterande är att privata företag i större utsträckning än statliga organisationer verkar ha varit pro-aktiva i sina satsningar på förbättrad IT-säkerhet. En majoritet av företagen har visserligen blivit drabbade av incidenter i samband med intrång av skadlig kod, men konsekvenserna har varit förhållandevis lindriga och intrången har inte nödvändigtvis varit den viktigaste anledningen att skynda på eller påbörja förbättringsarbetet. En gemensam nämnare för aktörer inom den privata och den statliga sidan är att det är samma aspekter som främst bekymrar IT-ansvariga, t.ex. den generella medvetenheten i organisationen, hur IT-regler och -rutiner följs och kompetensbredden på området IT-säkerhet. Det finns dock ett påtagligt större fokus inom näringslivet på möjligheten att behöriga kan utgöra ett hot mot IT-säkerheten om de inte längre är lojala mot organisationen.

Rekommendationer

Utifrån det som kommit fram i undersökningen rekommenderar Opticom följande för att förbättra skyddet av samhällsviktig infrastruktur:

1. Verka för mer central styrning!

Det som myndigheter och statliga bolag enligt dem själva skulle vara mest behjälpta av är mer central styrning och tydligare krav uppifrån. Myndigheter i Sverige är i regel mycket självständiga, vilket har en del fördelar. En nackdel är däremot att de är som öar i ett stort hav och att man är tvungen att själv uppfinna hjulet i många avseenden. Många uppfattar att de får alldeles för lite hjälp på vissa områden och att det finns en brist på tydliga direktiv. Ett stort antal respondenter efterlyser därför:

1. Tydligare regler och direktiv uppifrån.
2. En gemensam kravställare mot leverantörer av viktiga IT-lösningar från statens sida.
3. En kanalisering av information av gemensamt intresse för myndigheter och statliga bolag för att främja ett ökat erfarenhetsutbyte.

Att befrämja och stimulera spontan informationsutväxling mellan myndigheter skulle kunna förstärka dessa synergieffekter.

2. Låt en myndighet bli rösten utåt för alla myndigheter som verkar för att befrämja IT-säkerheten!

En vanlig kommentar som kommit fram i undersökningen är att myndigheter och statliga bolag anser att det finns för många instanser som har en egen roll i den gemensamma strävan från staten att höja IT-säkerheten och skydda viktig nationell infrastruktur. Det som efterlyses är färre kontaktytor och helst att *en myndighet* agerar som röst utåt på alla områden som är kopplade till IT- och informationssäkerhet. Utöver ett mer enhetligt sätt att kommunicera bör denna myndighet även ha en samordnande funktion och kanalisera informationsutbyte mellan de berörda instanserna.

3. Kanalisera information om incidenter!

Bara ett fåtal organisationer är helt pro-aktiva i sin satsning på förbättrad IT- och informationssäkerhet och det blir lätt så att man känner en falsk trygghet om man inte har drabbats av skadlig kod under en lång period. Det krävs dock stor kunskap och fantasi om vad som skulle kunna hända och på vilket sätt för att ständigt kunna vara proaktiv. Det vore bra om nyckelpersoner i alla dessa organisationer får omedelbar information om lyckade intrång av skadlig kod i Sverige och utomlands samt en inblick i vilka brister i säkerheten som har gett – eller kan ha gett – upphov till dessa incidenter. Denna

information kan ses som en rullande checklista vars främsta syfte är att hjälpa myndigheter och statliga bolag att kalibrera IT- och informationssäkerheten mot bakgrund av de senaste verkliga händelserna.

4. Utbilda IT- och informationssäkerhetsansvariga i pedagogisk framställning!

Bland en del av nyckelpersonerna i denna studie finns ett uttalat behov av att få hjälp med att 1. Öka medvetenheten bland de anställda och 2. Sälja in IT-säkerhetsrelaterade budskap på ledningsnivå. KBM bör överväga att antingen själva erbjuda seminarier och utbildningsmaterial eller aktivt förmedla kontakter till externa organisationer som erbjuder dessa tjänster.

Frågor som bör tas upp är bl.a.:

- Hur kommunicerar man med ledningen för att förankra IT-beslut som befrämjar IT-säkerheten?
- Hur ska IT-säkerhetsrelaterade utbildningar vara utformade för att budskapet ska nå ut på ett så effektivt sätt som möjligt. Vilka alternativ finns. Vilka är för- och nackdelarna med Intranät jämfört med tryckt material och CD-ROM-skivor?
- Hur ska IT-säkerhetsrelaterade regler/rekommendationer kommuniceras?

5. Kommunicera ut de viktigaste slutsatserna av denna studie till samtliga myndigheter och statliga bolag!

Både i det frågeformulär som användes för besöksintervjuerna och de resultat som presenteras i denna rapport finns många små och stora väckarklockor. Flera respondenter har själva gjort noteringar under intervjun och KBM skulle kunna uppmuntra till en fortsatt satsning på förbättrad IT- och informationssäkerhet genom att distribuera ut resultatet, till de intervjuade organisationerna såväl som till andra myndigheter och bolag. Förutom att innehållet i sig är mycket intressant för alla berörda, förmedlas också budskapet att KBM är måna om att lyssna på aktörerna och använda deras erfarenheter och åsikter i det fortsatta arbetet med att förbättra IT- och informationssäkerheten inom den nationella infrastrukturen.

6. Överväg att införa en obligatorisk standard för IT/informationshantering på myndigheter och statliga bolag!

Det finns nästan lika många rutiner kring IT- och informationshantering som det finns organisationer. Visserligen går det att få tillgång till bra rekommendationer och riktlinjer om hur man kan bygga ett gediget skydd mot digitala hot, men i de flesta fall är det den interna medvetenheten och kompetensen som bestämmer hur IT-säkerheten ser ut. En standard för all IT- och

informationshantering, till exempel liknade ISO 17799, skulle förmodligen innebära en signifikant höjning av IT-säkerheten.

7. Fundera på en kvantitativ uppföljningsstudie med kortare intervjuer bland ett större antal myndigheter, statliga bolag och privata företag!

Studien som denna rapport grundar sig på har varit mycket djuplodande och till stor del kvalitativ i sitt upplägg. Som en konsekvens av detta har urvalet av myndigheter och statliga bolag varit förhållandevis litet. En del intressanta frågor går därför inte att besvara, t.ex. om det finns ett samband mellan organisationsstorlek och IT- och informationsnivå eller om regional tillhörighet, typ av verksamhet, åldersstruktur m.m. har någon inverkan. De mycket omfattande resultat som framkommit i denna undersökning kan tjäna som underlag för att ta fram en uppföljningsstudie med färre och mer fokuserade frågor till ett avsevärt större urval. Detta för att fastställa vilka slutsatser som är allmängiltiga för hela den svenska myndighetsvärlden och alla statliga bolag samt ge kvantitativt underlag för prioritering och planering av angelägna insatser.

Stockholm, februari 2005

Maarten Sengers
Opticom International Research

Studiens resultat i punktform

Följande 20 punkter sammanfattar studiens viktigaste iakttagelser.

1. Ett välfungerande IT-system är extremt viktigt för dagens myndigheter och statliga bolag, och blir ännu viktigare under de närmaste fem åren.
2. Få respondenter är helt nöjda med hur deras nuvarande IT-system fungerar; bland de övriga varierar nöjdheten med systemet starkt. Många pekar på strukturella problem med IT-miljön för det relativt låga betyget.
3. De främsta styrkorna i de IT-system som utvärderats är: IT-säkerhet, att systemen uppfyller de ställda kraven och att IT-systemen kan hanteras i egen regi. De främsta svagheterna är att systemen i vissa fall är decentraliserade, omoderna och heterogena.
4. En majoritet av respondenterna i studien anser att det finns instanser som ställer krav på systemens funktionalitet (ofta Staten) samt att det finns instanser som är beroende av systemens funktionalitet. Däremot tycker bara en tredjedel att det finns instanser som ställer krav på IT-systemens säkerhet.
5. Outsourcing av IT-tjänster förekommer bland ungefär hälften av de intervjuade organisationerna. Det handlar i dessa fall främst om administrativa stödfunktioner och inte om affärskritiska funktioner. De flesta respondenter känner sig trygga med den IT-säkerhet som deras partners kan garantera, men vissa andra uppger att de inte har lika bra koll.
6. Microsoft Windows är utan undantag det operativsystem som används för administrativa funktioner, ofta i kombination med Unix, Solaris, Linux och/eller stordatorsystem för mer komplexa funktioner som tillhör kärnverksamheten.
7. IP-telefoni tros kunna leda till stora kostnadsbesparingar och många förväntar sig ett ökat tryck att titta på IP-telefoni som alternativ för dagens fasta telefoni. Många är dock medvetna om säkerhetsriskerna och tveksamma är framför allt respondenter som har en IT-säkerhetsbakgrund.
8. Även om mer resurser skulle underlätta vissa delar av IT-säkerhetsarbetet verkar pengar inte vara den största begränsande faktorn i de flesta organisationerna när det gäller att (ytterligare) höja systemskyddet.
9. Den mänskliga faktorn betraktas av en majoritet av respondenterna som den svagaste länken när det gäller att bygga bra IT-säkerhet. Detta yttrar sig både i att de anställda saknar kunskap och därigenom omedvetet äventyrar IT-säkerheten samt att de som är väl insatta kanske inte följer regler och rutiner.

10. Två av tre respondenter säger att det finns en särskild säkerhetsavdelning inom deras organisation och nästan samtliga uppger att det finns en särskild IT-säkerhetsansvarig.

11. Medvetenheten kring IT- och informationssäkerhet sprids framförallt via olika typer av utbildningar, tryckt informationsmaterial och Intranät. Trots dessa insatser är den genomsnittliga medvetenheten kring IT- och informationssäkerhet i de olika organisationerna förhållandevis låg.

12. Kompetensnivån hos de intervjuade organisationerna anses generellt vara bra, men bygger mycket på att olika personer kompletterar varandra.

13. Förutom en höjning av viss teknisk kompetens vill respondenterna främst få hjälp med kommunikation av IT-säkerhetsrelaterade budskap och bättre kunskap om nya produkter/tjänster på området IT-säkerhet.

14. Intern kommunikation är av mycket stor betydelse för hur myndigheter och statliga bolag hanterar kriser. Rutinerna skiljer sig dock mycket åt mellan de olika organisationerna. De myndigheter och organisationer som verkar ha lyckats bäst har representanter från IT-avdelningen och personer som jobbar med kärnverksamheten (speciellt från ledningen) som träffas med viss regelbundenhet i ett forum för att tala om IT-säkerhet och funktionalitet.

15. Skadlig kod anses bli ett större hot i framtiden (främst p.g.a. mer aggressiva typer av skadlig kod som sprider sig snabbare) och många tror att detta kommer att kräva en större satsning på IT-säkerhet inom organisationen.

16. De två enskilt största hindren för en förbättring av IT-säkerhetsnivån är 1. Brist på medvetenhet om att det finns sårbarheter i IT-miljön eller brist på kunskap om hur man ökar skyddet och 2. att det är svårt för IT-säkerhetsansvariga att sälja in och förankra beslut om bättre skydd hos ledningen.

17. De incidenter med intrång av skadlig kod som respondenterna har velat diskutera med Opticom har i vissa fall varit allvarliga, men skadorna har generellt varit begränsade till administrativa stödfunktioner. I och med att kärnverksamheten inte påverkats nämnvärt har det inte funnits många exempel på samhällspåverkan i form av externa kaskadeffekter.

18. I många organisationer har de interna kaskadeffekterna av incidenter med intrång av skadlig kod varit omfattande, både i förlorad produktion och extra timmar för IT-personalen.

19. Två tredjedelar av de intervjupersoner som representerar myndigheter anser att skadlig kod påverkar myndigheternas 24-timmarssatsning. Eftersom mer öppenhet tycks öka sårbarheten innebär denna satsning att det kommer att krävas mer övervakning, högre skyddsnivåer och ändrade rutiner.

20. Respondenterna efterlyser mer central styrning i form av ett större samlat grepp från myndigheterna på området IT-säkerhet och en bättre samordning mellan de ansvariga nämnderna och myndigheterna.

Rapportens disposition

Sammanfattning
Presenterar övergripande slutsatser och rekommendationer samt resultaten i punktform.

Kapitel 1
Förklarar studiens bakgrund, syfte, metod, centrala begrepp samt rapportens resultatredovisning och disposition.

Kapitel 2
Redovisar undersökning av IT-systemens betydelse för och behovstillfredsställelse inom de undersökta organisationerna och vilka externa krav som ställs på dem.

Kapitel 3
Redogör för hur organisationernas IT- och informationssäkerhet ser ut i vardags- och krissituationer.

Kapitel 4
Beskriver hur beredskapen att stå emot skadlig kod ser ut i dagsläget och hur organisationerna eventuellt har blivit drabbade av skadlig kod.

Appendix
Visar det frågeformulär som tjänade som underlag vid genomförandet av de personliga djupintervjuerna.

Inledning

Bakgrund

Under hösten 2004 har Opticom International Research gjort en studie om IT- och informationssäkerhet och beredskap mot skadlig kod hos ett antal större myndigheter och statliga bolag i Sverige. Studien har gjorts på uppdrag av Krisberedskapsmyndigheten (KBM). Samtliga undersökta organisationer har som gemensam nämnare att de spelar en viktig roll i den nationella IT-infrastrukturen. Förutsättningarna för deras verksamhet, som i många fall är reglerade i de officiella uppdrag som de har fått från Staten, innebär att det ställs mycket höga krav på dem när det gäller att garantera en säker och välfungerande informationshantering.

För att få en uppfattning om hur IT- och informationssäkerhetsnivån bland myndigheter och statliga bolag står sig i förhållande till nivån på privata företag har en mindre tilläggsstudie gjorts bland 10 företag inom det svenska näringslivet. I resultatredovisningen (kapitel 2-4) hittas resultatet av denna jämförelse i särskilda rutor.

Syfte

En viktig uppgift för KBM i dess strävan att samordna arbetet kring samhällets beredskap inför allvarliga kriser är att samla in information om IT- och informationssäkerhet i det offentliga Sverige och ta del av de olika resonemang som förs kring dessa frågor. Den studie som presenteras i denna rapport ger KBM tillgång till primär data som samlats in och analyserats av en objektiv tredje part.

Det främsta syftet med studien är att kartlägga utformningen av, och rutiner kring, IT- och informationssäkerheten hos ett antal större myndigheter och statliga bolag i Sverige. Utöver detta huvudsyfte är målet med undersökningen att få svar på följande frågor:

- Vad är IT-systemens betydelse för och behovstillfredsställelse inom de undersökta organisationerna och vilka externa krav ställs på dem?
- Hur ser organisationernas IT- och informationssäkerhet ut generellt och i krissituationer?

- Hur är beredskapen vad det gäller att stå emot skadlig kod och hur har organisationerna eventuellt blivit drabbade av skadlig kod?
  - Vilken påverkan har skadlig kod haft på samhällsviktig infrastruktur?
  - Vilka kaskadeffekter har detta haft?
  - Skulle samhällsviktig infrastruktur ha kunnat skyddas bättre?
  - Vad kan utifrån dagens förutsättningar göras för att förbättra skyddet?
- Hur står sig IT- och informationssäkerheten i svenska myndigheter och statliga bolag jämfört med företag inom det svenska näringslivet?

Metod

För att få en heltäckande bild av IT- och informationssäkerheten inom större myndigheter och statliga bolag har Opticom valt att göra besöksintervjuer med 22 respondenter på fjorton olika organisationer med viktiga samhällsfunktioner. Hellre än att göra många korta intervjuer inom ett större urval av organisationer har bedömningen gjorts att längre och mer djuplodande intervjuer med ett mindre antal personer skulle ge de bästa förutsättningarna för att svara på frågorna ovan. Den stora fördelen med metodiken besöksintervjuer är att den ger en bättre förståelse för respondenternas uppfattning, inställning, attityd och värdering kring de ämnen som tas upp.

Urvalet av myndigheter och statliga bolag gjordes av Krisberedskapsmyndigheten i samråd med Opticom. Från en lista bestående av sex centrala myndigheter, fyra statliga bolag, två större landsting och tre större kommuner kontaktades samtliga organisationer förutom en (en kommun), vilket i samtliga fall ledde till att åtminstone en intervju kunde göras. Svarsfrekvensen i denna undersökning har därför varit mycket hög. Ingen organisation eller person har tackat nej till att delta i studien. I ett fall var det inte möjligt att etablera kontakt med den person som var mest lämpad att besvara frågorna och i tre fall har Opticom valt att enbart göra en intervju per organisation eftersom respondenten visade sig både ha en förankring i den administrativa ledningen och i den operationella IT eller IT-säkerhetssfären.

I möjligaste mån gjordes två intervjuer per organisation, en med en person i ledande administrativ befattning och en med en person som har mer operativt ansvar för IT och IT-säkerhet. Genom att välja detta upplägg uppstår möjligheten att belysa frågorna från två olika perspektiv för att åskådliggöra om det finns några signifikanta skillnader mellan olika typer av befattningshavare när det gäller deras åsikter kring frågor om IT- och informationssäkerhet. Det bör noteras att gränsen mellan dessa två målgrupper inte är knivskarp. Samtliga personer på IT- eller IT-säkerhetssidan

jobbar operationellt med dessa frågor, men inom gruppen av ledande befattningar finns både personer med en administrativ funktion (som i detta fall inkluderar styrande ansvar för IT-relaterade frågor) och personer med ett IT-ansvar eller IT-säkerhetsansvar som är med i ledningsgruppen eller har en tydlig anknytning till den.

Totalt gjordes tolv intervjuer med IT-chef eller IT-säkerhetschefer och tio med personer i en ledande administrativ befattning. Målet har varit att göra intervjuer med de högst ansvariga personerna på båda sidor. När det gäller den operationella IT eller IT-säkerhetssidan har Opticom utan några problem kunnat boka intervjuer med de högst ansvariga, medan frågan ofta har delegerats ner ett eller två steg på den administrativa sidan, t.ex. från generaldirektör till överdirektör eller säkerhetschef. Intervjuerna tog i genomsnitt 1,5 timmar.

Tilläggsintervjuerna bland privatföretagen gjordes per telefon. Tjugo nyckelfrågor, som tidigare hade ställts till de statliga organisationerna, valdes ut för att underlätta en jämförelse och samtidigt korta ner intervjutiden. Företagen valdes ut av Opticom inför intervjuprocessen och de viktigaste två kriterierna var att det skulle handla om förhållandevis stora företag från olika branscher. I det här fallet handlar det om tre industriföretag, tre företag inom papper och pappersmassa, två läkemedelsföretag, en bank och ett annat serviceföretag. Samtliga tio respondenter hade någon form av operationellt IT- eller IT-säkerhetsansvar. Intervjuerna tog mellan 20 och 30 minuter.

Fördelning av intervjuer per målgrupp och ansvarsområde

Målgrupp	Ledande adminstrativ befattning	Operativ IT- eller IT-säkerhet	Totalt
Central myndighet	5	5	10
Statligt bolag	2	3	5
Länsstyrelse	1	2	3
Kommun	2	2	4
Totalt statliga organisationer	10	12	22
Privata företag	–	10	10
Totalt	10	22	32

Samtliga organisationer, både myndigheter, statliga bolag och privata företag, garanterades total anonymitet.

Centrala begrepp

I denna rapport används i stor utsträckning begreppet IT- och informationssäkerhet, som innefattar både IT-säkerhet och informationssäkerhet. Krisberedskapsmyndigheten definierar dessa termer som följer:

Informationssäkerhet innebär säkerhet vid hantering av information avseende:

1. Tillgänglighet (möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid).
2. Informationskvalitet (att information inte avsiktligt eller oavsiktligt förändras eller förstörs).
3. Sekretess (att information inte får göras tillgänglig eller avslöjas för obehöriga).
4. Spårbarhet (att en verksamhet och tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer).

IT-säkerhet innefattar de delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring denna.

En annan term som används frekvent är skadlig kod:

Skadlig kod definieras som program som sprider sig själva och som tränger in i system via olika kanaler. De viktigaste är e-post, Internet-sidor och smittade informationsbärare såsom disketter och USB-minnen. Skadlig kod kan ta sig olika former som t.ex. virus, maskar, trojaner och hybrider.

Resultatredovisning

De myndigheter och statliga bolag som har varit med i denna undersökning skiljer sig åt avsevärt när det gäller verksamhetsinriktning och uppdrag. En viktig konsekvens av detta är att det också finns stora skillnader när det gäller frågan i vilken mån kärnverksamheten i sig själv är IT-baserad eller om den snarare stöds av (administrativa) IT-system. Oavsett frågan om det handlar om centrala myndigheter, lokala myndigheter eller statliga bolag kan organisationerna delas upp i tre huvudgrupper:

1. Myndigheter och statliga bolag som behöver avancerade IT-system för att kunna sköta sina uppgifter som t.ex. flygtrafikledning, radiokommunikation eller brottsbekämpning. Ett avbrott för dessa organisationer skulle direkt innebära stora kaskadeffekter i samhället.

2. Organisationer vars kärnverksamhet inte är IT-baserad i lika stor utsträckning som hos ovanstående myndigheter och organisationer, men som behöver omfattande administrativa IT-system som *stödjer* verksamheten. Detta gäller t.ex. i hög grad för myndigheter som är ansvariga för stora finansiella transaktioner. Administrativa IT-system har ersatt mycket av den manuella hanteringen som fanns förr i tiden.
3. Lokala myndigheter såsom landsting eller kommuner, vars IT-system är till för att stödja olika typer av verksamhet som har mer lokal karaktär. Effekterna av störningarna kan vara besvärliga för de drabbade men är samtidigt mer diffusa och svårare att mäta på samhällsnivå.

På grund av dessa skillnader mellan organisationerna vad det gäller samhällsfunktion, verksamhetsområde och framför allt vilken typ av beroende de har av IT-systemen ligger fokus först och främst på allmänna erfarenheter och åsikter som respondenterna har när det gäller att upprätthålla en bra och säker IT-miljö, snarare än att exakt följa målgruppsgränserna. Hur svaren exakt skiljer sig åt mellan och inom de olika målgrupperna är inte lika relevant med tanke på de skillnader i verksamhet som finns från början och att de jobbar under helt olika förutsättningar.

Slutligen är det viktigt för läsaren att observera att många av de intervjuade organisationerna har visat sig ha haft stora problem med IT-säkerheten under de senaste fem åren, ofta i samband med intrång av skadlig kod. I många fall baseras respondenternas bedömningar av dagens säkerhetsnivåer därför på ett förbättringsarbete som ofta har pågått i flera år och där i många fall grundläggande delar av IT-infrastrukturen har förbättrats avsevärt.

Organisationens IT-rutiner

Vikten av ett väl fungerande IT-system för verksamheten

I detta första resultatkapitel presenteras en analys av IT-system och rutiner som finns inom de undersökta organisationerna samt de krav som ställs på dem av externa instanser.

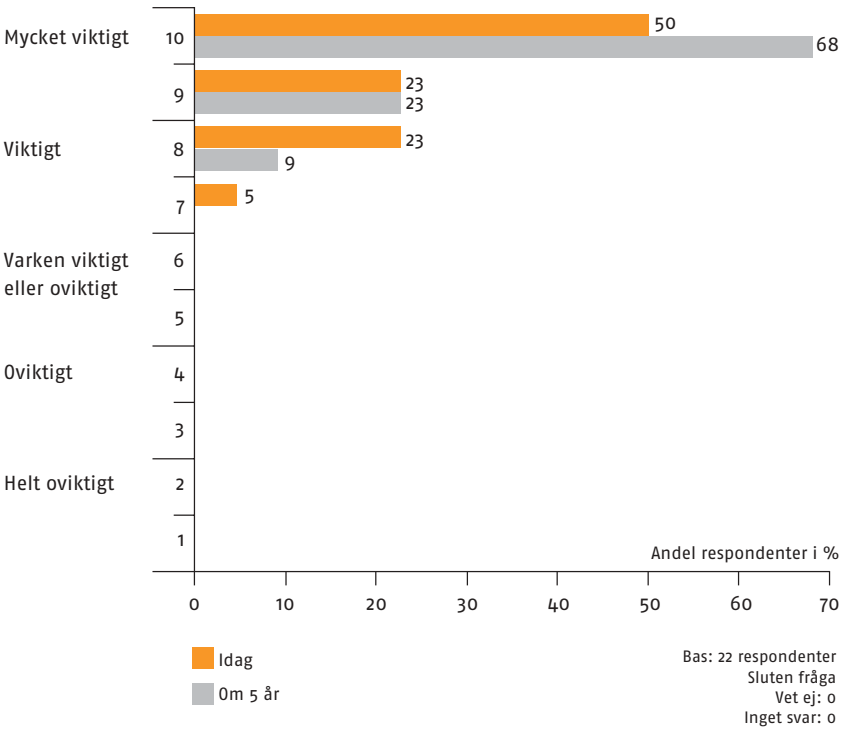
Inom samtliga myndigheter och statliga bolag anses ett väl fungerande IT-system vara av mycket stor vikt för organisationens verksamhet. Oberoende av frågan om kärnverksamheten i sig är helt IT-baserad eller om den 'enbart' stöds av IT-system, är samtliga respondenter eniga om att det skulle innebära allvarliga konsekvenser om systemen inte fungerar som de ska. Alla myndigheter och bolag som har varit med i undersökningen anser att IT-systemet kommer att vara åtminstone lika viktigt om fem år som idag, och i vissa fall till och med viktigare. Nästan samtliga respondenter som säger att vikten kommer att ligga kvar på samma nivå säger att den redan idag ligger på 9 eller 10 på skalan 1–10. Systemen kan visserligen komma att moderniseras och bli fler eller färre, men vikten av IT-systemet för kärnverksamheten kommer inte att förändras.

De sju respondenter som anser att betydelsen kommer att öka under de närmaste fem åren hänvisar först och främst till effektivitetsskäl. En del av de administrativa funktioner som stödjer kärnverksamheten har fortfarande inte helt datoriserats. Datoriseringen kommer att intensifieras eller fullbordas under de närmaste åren. I ett statligt bolag pågår ett teknikskifte inom själva kärnverksamheten genom att analog teknologi ersätts av digital teknologi, vilket ökar beroendet av IT-baserade lösningar. Slutligen tros IT-systemen bli ännu viktigare i en av kommunerna p.g.a. ambitionen att öka tillgängligheten och kontakten med medborgarna.

Om man tittar på hur väl organisationernas nuvarande IT-system fungerar är svaren mycket mer varierande, med betyg mellan 5 och 10 (skala 1–10). Av de tjugo respondenter som kan svara på denna fråga finns enbart tre som är helt nöjda med hur IT-systemen lever upp till de förväntningar som man har avseende funktionalitet, IT-säkerhet och ibland också ekonomi och användar-

Bild 1. Respondenternas bedömning av vikten av IT-systemen idag och om fem år

På en skala från 1–10, hur viktigt är ett välfungerande IT-system för organisationens verksamhet idag och hur viktigt kommer IT-systemet att vara om 5 år?



vänlighet. Dessa tre personer är alla IT- eller IT-säkerhetsansvariga.

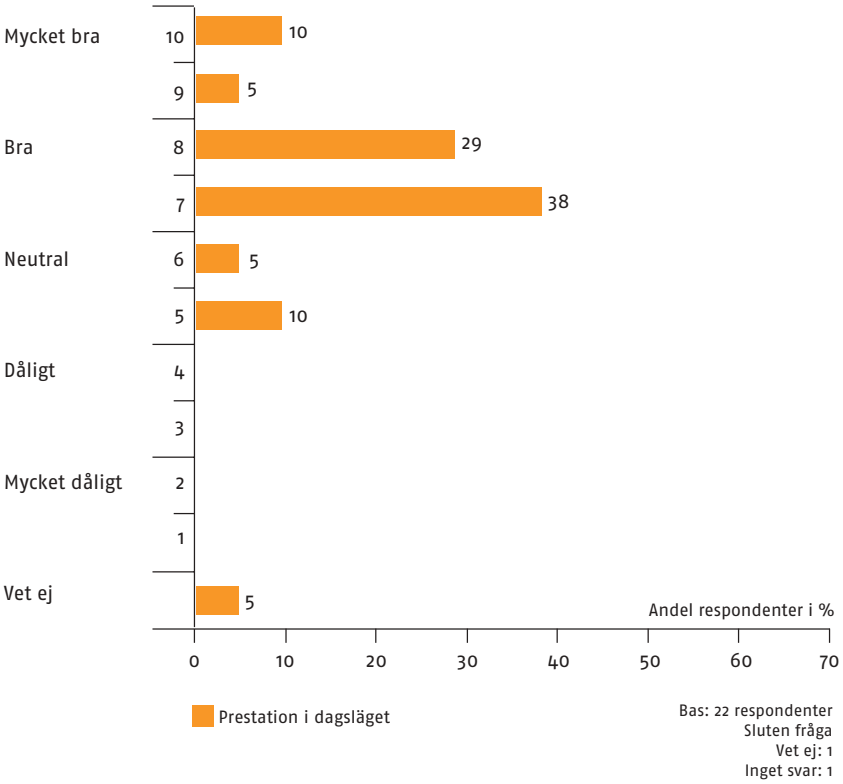
I största allmänhet är de respondenter som innehar en ledande befattning och de som främst jobbar med IT ganska eniga om vilka delar i IT-systemet som skulle kunna förbättras, men i några fall verkar personer i ledande befattningar ha något större fokus på funktionalitet och IT-ansvariga på IT-säkerhet.

Överlag anser IT-ansvariga i större utsträckning än personer i ledande administrativa befattningar att systemen fungerar bra och att det som de får ut ur systemen kommer ganska nära de krav som ställs på dem (d.v.s. de krav som ska tillgodoses för att verksamheten ska kunna bedrivas på bäst möjliga sätt). En annan trend är att det är de mest affärskritiska systemen som i regel fungerar bäst och de mer perifera delarna av det administrativa IT-systemet som drabbas i första hand vid incidenter.

Att prestationsbetygen inte till fullo ligger på samma nivå som viktighetsbetygen beror inte på att respondenter

Bild 2. Respondenternas bedömning av hur väl IT-systemen i deras organisation fungerar i dagens läge på en skala från 1–10

På en skala från 1–10, hur väl anser du att ert nuvarande IT-system fungerar?



anser att det skulle saknas funktionalitet i systemet. Bara någon enstaka respondent tycker att det behövs nya system eller applikationer. Inte heller IT-säkerhet nämns spontant som ett förbättringsområde. Något som däremot ses som ett större problem är att det egentligen finns för många olika typer av IT-system inom organisationen. IT-miljön är i dessa fall väldigt heterogen och blir därmed svårhanterbar. Det är inte ovanligt att vissa system dessutom har många år på nacken och skulle kunna förenklas och moderniseras väsentligt. Detta gäller både organisationer med riktigt gamla IT-system samt bolag som nyligen fusionerats och ska bygga upp ett gemensamt IT-system.

Att funktionalitet och IT-säkerhet inte är det första som oroar respondenterna när de svarar på frågan om hur väl IT-systemen fungerar bekräftas när respondenterna ombeds ange de främsta svagheterna. Det är mest strukturella hinder som gör det svårt att få IT-systemet att fungera på ett tillfredsställande sätt. Exempel på detta är decentraliserade system p.g.a. geografisk spridning eller organisationens utformning, system som av olika anledningar är svåra att anpassa till dagens krav och måste bytas ut helt, system som är omoderna och bygger på ett gammalt arv samt en för stor heterogenitet i IT-miljön.

Trots de bekymmer som uppenbarligen finns i en del organisationer är bilden som respondenterna i huvudsak målar upp att systemen står sig bra. Bland de styrkor som nämnts finns IT-säkerhet påfallande ofta med (mer än

JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

1. Vikten av IT-systemet idag och om fem år samt nöjdheten med IT-systemet i dagsläget

Privatföretag skiljer sig inte nämnvärt från myndigheter och statliga bolag när det gäller hur viktigt IT-systemet är för organisationens kärnverksamhet idag och om fem år. Däremot är representanterna för de privata företagen överlag något mer nöjda med hur deras nuvarande IT-system fungerar än deras kollegor från den offentliga sidan. Detta kan delvis bero på att enbart personer med operativt IT-ansvar har intervjuats inom näringslivet, men även om man räknar bort denna effekt anses IT-systemen fungera något bättre i privata företag.

Precis som på myndigheter och i statliga bolag finns det bara någon enstaka respondent inom näringslivet som spontant anser att det i dagsläget saknas funktionalitet eller IT-säkerhet i systemet. Det största problemet är även här att IT-systemet upplevs vara för decentraliserat och att det är svårt att förändra och modernisera systemet.

Jämförelsebild 1. Vikten av IT-systemet idag och om fem år samt nöjdheten med IT-systemet i dagsläget

Målgrupp	Viktighet idag	Viktighet om 5 år	Nöjdhet med det nuvarande IT-systemet	Skillnad mellan viktighet idag och nöjdhet idag
Statliga organisationer	9,2	9,6	7,1	-2,1
Privata företag	9,3	9,6	7,5	-1,8

vart fjärde svar). Att IT-systemen kan skötas i egen regi, bra driftsäkerhet och bra kompetens & tekniska resurser i organisationen är andra svar som har nämnts av flera respondenter.

Bild 3. IT-systemens främsta styrkor och svagheter enligt respondenterna

Vilka anser du är de största styrkorna och svagheterna i ert IT-system som det ser ut idag?

Styrkor (37)	Antal svar
1. IT-säkerhet*	10
2. Generellt bra system som uppfyller kraven	5
3. IT-system i egen regi	4
4. Driftsäkerhet	3
5. Kompetens/tekniska resurser i organisationen	3
6. Geografisk täckning/ bra kommunikationsförmåga	2
7. Standardiserat system	2
8. Erfarenhet/lång tradition	1
9. Bra rutiner/arbetssätt/strategi	1
10. Ekonomi/kostnadseffektivt	1
11. Inga klara styrkor	1
11. *Övrigt*	4

*** IT-säkerhet: styrkor (10 svar)**

1. Ligger långt framme med IT-säkerhet (generellt)	3
2. Robust system	2
3. Reservkapacitet i systemet	1
4. Bra patch-struktur	1
5. Installerade IDS-er	1
6. Anti-virusprogram överallt	1
7. Hårt sektionerat IT-system	1

Svagheter (29)	Antal svar
1. Decentraliserat system (geografiskt eller genom organisationens utformning)	5
2. (Delvis) omoderna system	4
3. Oflexibilitet (svårt att anpassa/ uppdatera systemen)	4
4. För stor mångfald/heterogenitet i IT-miljön	4
5. IT-säkerhet*	3
6. Brist på användarvänlighet	1
7. Ofärdigt system	1
8. Svagheter i det fysiska skyddet	1
9. Inga klara svagheter	1
10. *Övrigt*	5

*** IT-säkerhet: svagheter (3 svar)**

1. Sårbarheter (generellt)	1
2. Svårt att förmedla IT-åtgärder	1
3. Förbättringar krävs i skyddet mot skadlig kod	1

Bas: 22 respondenter
Öppen fråga
Summa svar: 37 styrkor/29 svagheter
Vet ej: 0
Inget svar: 2

Externa krav på IT-systemets funktionalitet och säkerhet

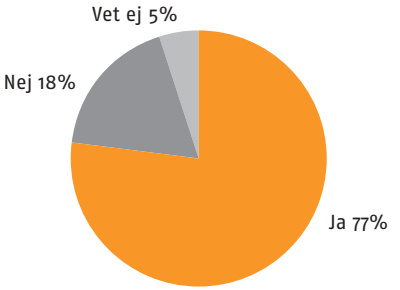
En stor majoritet av respondenterna anser att det finns instanser[1] som ställer externa krav på IT-systemets *funktionalitet*, men ett statligt bolag och två kommunala myndigheter uppger sig inte ha några externa krav. Nästan hälften av respondenterna i den första gruppen nämner staten som den instans som direkt (t.ex. via regleringsoch författningsbrev) eller indirekt (via andra statliga myndigheter som Skatteverket, Datainspektionen och Post & Telestyrelsen) ställer krav på IT-systemets funktionalitet.

Så gott som samtliga respondenter säger att det finns instanser som är beroende av IT-systemets funktionalitet. Det finns ett brett spektrum av intressenter som är beroende av att IT-systemet fungerar som det ska: myndigheter, olika kundgrupper, privatpersoner, anställda, leverantörer och samhället i sin helhet. Ett exempel är de s.k. VMA-sändningar (Viktigt Meddelande till Allmänheten) som under alla omständigheter måste kunna nå ut. Även ett antal internationella instanser nämns, främst de som är involverade i regleringen av den internationella lufttrafiken och brottsbekämpande samarbetsorgan.

En fråga som är mycket svårare att besvara än de två föregående är den om det finns externa instanser som ställer

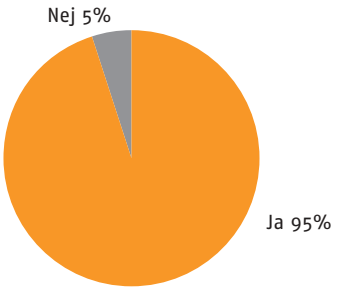
Bild 4 och 5. Andel respondenter (i %) som anser att det finns externa instanser som 1. ställer formella krav på IT-systemets funktionalitet och 2. som är beroende av IT-systemets funktionalitet

Finns det instanser utanför er organisation som ställer formella krav på IT-systemets funktionalitet?



Bas: 22 respondenter
Sluten fråga
Vet ej: 1
Inget svar: 0

Finns det instanser utanför er organisation som är beroende av IT-systemets funktionalitet?



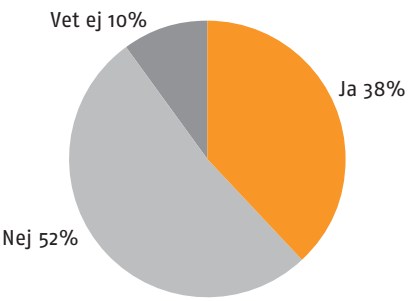
Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 0

1. Instanser definieras under intervjun som: Alla möjliga intressenter som aktören har kontakt med, t.ex. regeringen, (andra) myndigheter, kunder, ägare m.m.

krav på IT-systemets *säkerhetsnivå.* Hälften anser att så inte är fallet medan en av tio inte vet. Totalt åtta personer svarar ”ja”, och enbart fem av dem kan specificera vilka instanser som ställer krav: 1. Krisberedskapsmyndigheten (2); 2. Staten (1), SÄPO (1), EU/ICAO (1). Överlag känner sig många osäkra när de besvarar den här frågan. Ett gängse resonemang är att det visserligen finns krav på verksamheten i sin helhet, medan det inte verkar finnas liknande krav på själva IT-säkerheten.

Bild 6. Respondenternas bild av styrkor och svagheter som kännetecknar de IT-system som finns inom de intervjuade myndigheterna och statliga bolagen

Finns det instanser utanför er organisation som ställer formella krav på IT-systemets säkerhetsnivå?



Bas: 22 respondenter
Sluten fråga
Vet ej: 2
Inget svar: 1

Ansvarsfördelning kring IT-relaterade frågor

I och med att de fjorton myndigheter och bolag som är med i den här studien skiljer sig så mycket åt när det gäller verksamhetsområde, geografisk täckning och antal intressenter är det inte meningsfullt att analysera ansvarsfördelningen kring IT-relaterade frågor på aggregerad nivå. Även inom de olika målgrupperna kan skillnaderna vara betydande, men här finns ändå ett antal mönster som kommer fram och som är värda att nämnas:

Funktionalitet

Hos centrala myndigheter är det mest systemägarna/systemförvaltarna som har det huvudsakliga ansvaret för funktionaliteten och som ofta är beställare. IT-enheten, IT-chefen/IT-säkerhetschefen och driftchefen kan vara med på ett hörn men de har inte det främsta ansvaret.

På statliga bolag, länsstyrelser och kommuner är ansvaret för funktionaliteten i högre grad inbakat i IT-avdelningens uppdrag.

IT-säkerhet

Ansvarsfördelningen på området IT- och informationssäkerhet är mer enhetligt mellan de olika målgrupperna. In många fall är det personer på säkerhetsavdelningen eller de som jobbar med IT-säkerhet som i första hand ansvarar för dessa frågor. De tar både egna initiativ och rekommenderar IT-säkerhets-

lösningar till beställarsidan, om det finns en sådan. Inom vissa centrala myndigheter finns en klar förankring av IT-säkerhetsfrågor inom verksamhetsledningen medan kopplingen är mer indirekt i andra myndigheter.

Investeringar/budgetfrågor

Rutinerna i samband med IT-relaterade investeringar/budgetfrågor varierar något från en organisation till en annan och kan till och med skilja sig inom organisationerna beroende på om det handlar om investeringar i ny funktionalitet eller i förbättrad IT-säkerhet. Det är både systemägare, IT- eller IT-säkerhetsansvariga, verksamhetsledningen eller driftsorganisationen som kan vara mest pådrivande i processen, och i vissa fall finns det speciellt beredskapsgrupper där personer från olika avdelningar är med för att garantera att den här processen kan fortskrida smärtfritt.

Kommunikation om IT-frågor generellt

I de flesta organisationer finns klara rutiner för hur IT-frågor ska kommuniceras, både från en funktionalitets- och säkerhetssynpunkt och vid incidenter. Det är inte ovanligt att rollfördelningen mellan de olika enheterna, avdelningarna och nyckelpersonerna beskrivs på ett detaljerat sätt i verksamhetsdokumentationen. Kommunikationen kan ta olika former. Det är vanligt med regelbundna möten mellan nyckelpersoner samt olika typer av forum, ofta med en strategisk inriktning. I många fall är intranätet det främsta sättet att sprida information av mer allmän karaktär. Avvikelser från det normala rapporteras till de ansvariga och vid incidenter intensifieras kontakterna.

Antalet statliga bolag som är med i undersökningen är givetvis inte tillräckligt stort för att dra generella slutsatser för hela landet, men av det begränsade urvalet framgår att rutinerna verkar vara något mindre utvecklade där än på de flesta myndigheter. I ett av de statliga bolagen gör organisationens utformning att IT-systemet är väldigt decentraliserat och det är de olika enheterna som i hög grad sköter sina egna IT-frågor. Vid behov kan IT-avdelningen och säkerhetsavdelningen kontakta varandra, men det sker inte rutinmässigt. Först vid incidenter finns det mer stringenta rutiner och ett större engagemang från t.ex. ledningsfunktioner.

Outsourcing av IT-verksamhet

Outsourcing av IT-funktioner förekommer inom alla målgrupper, men mest inom gruppen ”centrala myndigheter”. Man påpekar dock att det inte handlar om affärskritiska tjänster utan främst om olika typer av drift- och underhållstjänster, stöd- och hjälpdeskfunktioner och andra administrativa funktioner. De organisationer som inte outsourcar anger olika skäl till detta. Det vanligaste är att det finns interna lösningar som anses vara bättre eller billigare, och för två av de intervjuade statliga bolagen

gäller att deras verksamhet varken kan eller får läggas på entreprenad p.g.a. deras samhällsfunktion.

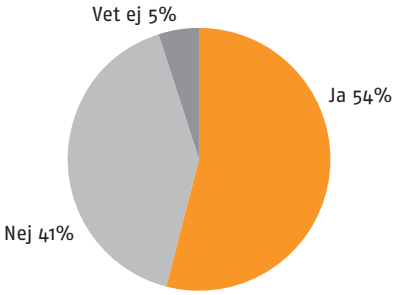
En närmare analys av de organisationer som outsourcar IT-funktioner visar att det är besvärligt för de flesta respondenter att uppskatta vilken andel av den totala IT-verksamheten det rör sig om, men av svaren framgår att det mestadels handlar om mindre uppdrag, upp till högst fem procent. Det finns dock ett antal undantag, och i en av kommunerna lägger man hela 95 procent av alla IT-funktioner på entreprenad. Här ingår även nätverket och serverdrift. Det enda som denna organisation har kvar internt är en IT-säkerhetsfunktion.

Det är intressant att se att sju av de tolv respondenter som anger att outsourcing förekommer känner en stor eller mycket stor trygghet att deras IT-partner(s) kan uppnå samma IT-säkerhetsnivå som de själva (betyg 8–10 på en skala från 1–10). De fem övriga kan däremot inte svara på frågan för att de inte kan eller inte vill. Detta kan bero på att respondenterna känner sig osäkra eftersom det handlar om förhållandevis enkla funktioner som de inte har så mycket att göra med, men det finns också respondenter som medger att det verkar variera mycket mellan parterna och att de inte kollar upp IT-säkerhetsdetaljer lika frekvent som de borde göra.

Det vanligaste sättet att ställa krav på externa parter är genom att utforma avtalen enligt de krav som ställs på den interna verksamheten. I några fall görs dock en extra bearbetning av avtalen och då ställs mer specifika krav på dessa leverantörer. I många fall ingår det inte i standardrutinerna att ställa krav på att de externa leverantörerna själva ska ha en kontinuitetsplan. En tredjedel av respondenterna gör det, ytterligare en tredjedel säger att de inte gör det och de resterande personerna kan inte svara på frågan.

Bild 7. Outsourcing av IT-funktioner till instanser utanför den egna organisationen

Outsourcar ni delar av er IT-verksamhet till instanser utanför organisationen?



Bas: 22 respondenter
Sluten fråga
Vet ej: 1
Inget svar: 0

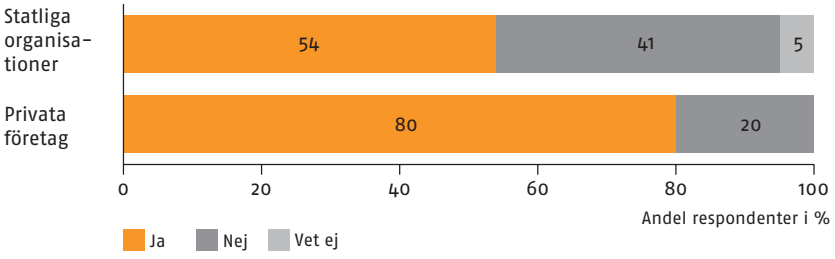
2. Outsourcing

Inom det privata näringslivet finns större utrymme att outsourca centrala IT-funktioner än i statliga organisationer. De privata företag som intervjuats är varken med i totalförsvaret eller på något annat sätt begränsade av ett uppdrag från en instans utanför organisationen, vilket gör att outsourcing är vanligare inom näringslivet (se bilden nedan). En annan skillnad är att externa IT-partners i något högre grad tar hand om affärskritiska tjänster inom det svenska näringslivet än på den offentliga sidan.

Myndigheter och statliga bolag som outsourcar IT-tjänster känner sig generellt något säkrare än privata företag på att deras IT-partner(s) kan uppnå åtminstone samma IT- och informationssäkerhetsnivå som de själva hade gjort om de hade behållit de outsourcade tjänsterna (8,9 för statliga organisationer mot 8,1 för privata företag på en skala från 1–10). Det bör dock noteras att urvalet av privata företag är litet och att betyget i det här fallet dras ner av ett företag som ligger signifikant under snittet.

Jämförelsebild 2. Outsourcing av IT-verksamhet

Outsourcing till instanser utanför organisationen:



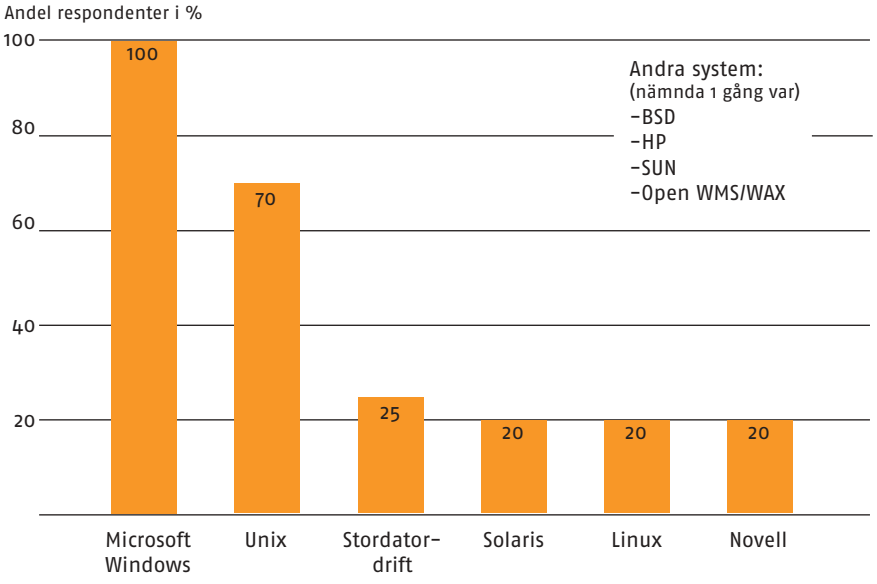
Organisationens val av operativsystem

Gemensamt för myndigheter och bolag i denna studie är ett antal grundläggande administrativa stödfunktioner och där Microsoft Windows utan undantag är förstahandsvalet. Microsoft Windows utbredda standard, funktionalitet, användarvänlighet och det faktum att det finns så många bra applikationer är starka argument för organisationer att välja denna lösning för klientbaserade funktioner.

Frågan i vilken mån andra operativsystem behövs för att sköta organisationens IT-verksamhet beror till stor del på kärnverksamhetens karaktär och de specifika krav som ställs på utformningen av IT-lösningarna. Den generel-

Bild 8. Andel av respondenter som väljer ett visst operativsystem

Kring vilket/vilka operativsystem har ni byggt er IT-verksamhet?



Bas: 22 respondenter
Öppen fråga
Vet ej: 0
Inget svar: 2

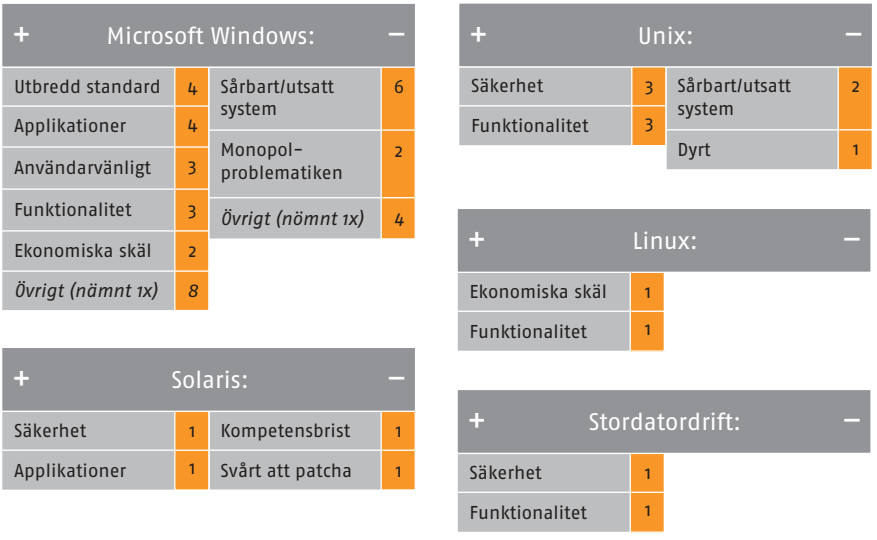
la bilden är att antalet olika system och plattformar blir fler om kärnverksamheten är av mer teknisk karaktär. Det vanligaste är att antalet operativsystem är mellan ett och fyra, men i ett statligt bolag fanns det upp till sju system. Förutom Microsoft Windows är Unix, Solaris, Linux och olika typer av stordatordrift vanliga.

Så gott som samtliga respondenter betraktar funktionalitet som det tyngsta argumentet för att välja ett visst operativsystem, antingen som det enskilt viktigaste skälet eller i kombination med säkerhet och/eller ekonomi. Bara i ett fall anser en respondent att säkerheten är överordnad funktionalitet och i ytterligare ett fall bedöms ekonomin som viktigast. En analys av respondenternas resonemang vid val av operativsystem visar också att säkerhet och ekonomi, som alltså ofta kommer på andra eller tredje plats, väger ungefär lika tungt på en övergripande nivå. Gemensamt för samtliga organisationer i undersökningen är dock att de alltid försöker väga in alla tre kriterier i beslutet.

Bilden på nästa sida visar de främsta för- och nackdelarna med de fem system som väljs mest.

Bild 9. För och nackdelar av de mest valda operativsystemen

Vilka är de viktigaste för- och nackdelarna med de operativsystem ni har mest erfarenhet av?



Bas: 22 respondenter
Öppen fråga
Vet ej: 0
Inget svar: 2

IP-telefoni

IP-telefoni är just nu ett mycket aktuellt ämne inom telekommunikationsvärlden och många företag och organisationer gör för närvarande en granskning av IP-telefonins möjligheter för att se om det kan vara intressant att ta klivet från vanlig telefoni till IT-telefoni. En klar majoritet av respondenterna (16 av 22) känner sig tillräckligt insatta i ämnet för att kunna svara på frågorna.

En generell kartläggning av vad respondenterna anser är de främsta för- och nackdelarna med IP-telefoni visar klart att det finns en tro på att stora kostnadsbesparingar väntar efter införandet av den tekniken, men att säkerhetsriskerna är ett stort problem.

Av de respondenter som är med i den här studien säger fem personer, som alla representerar en kommun eller ett landsting, att det redan idag finns IP-telefoni på de myndigheter som de representerar. Ytterligare åtta respondenter, som representerar tre centrala myndigheter, två statliga bolag och den andra av två kommuner, tror att IP telefoni kommer att vara ett faktum om fem år.

Bild 10. För och nackdelar med IP-telefoni

Hur ser ni generellt på IP-telefoni? Vilka är de främsta för- och nackdelarna?

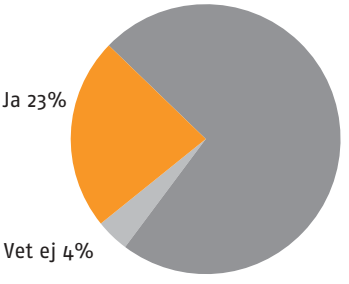
Fördelar (20)	Antal svar
1. Kostnadseffektivt	10
2. Optimering av nätet/ olika typer av synergieffekter	4
3. Användarvänligt – flyttbara telefoner	1
4. Öppnar upp för nya tjänster	1
5. Kvalitetsökning	1
6. *Vet ej*	*3*

Nackdelar (19)	Antal svar
1. Säkerhetsrisker (generellt)	11
2. Säkerhetsrisker (strömförsörjning)	2
3. Obeprövat/omoget	2
4. Krävs ombyggnad av nätverket	1
5. Klarar inte av "Universal Services Obligations"	1
6. *Vet ej*	*2*

Bas: 22 respondenter
Öppen fråga
Summa svar: 20 fördelar/19 nackdelar
Vet ej: 3/2
Inget svar: 6/6

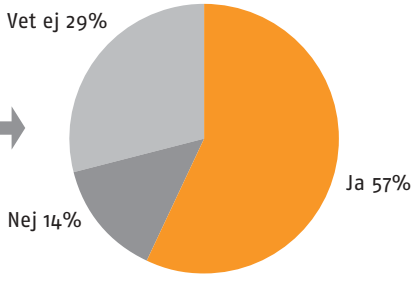
Bild 11. Användning av IP-telefoni idag och om fem år

Har ni IP-telefoni idag?



Bas: 22 respondenter
Sluten fråga
Vet ej: 1
Inget svar: 0

Om nej, tror du att ni kommer att ha IP-telefoni om fem år?



Bas: 16 respondenter
Sluten fråga
Vet ej: 4
Inget svar: 2

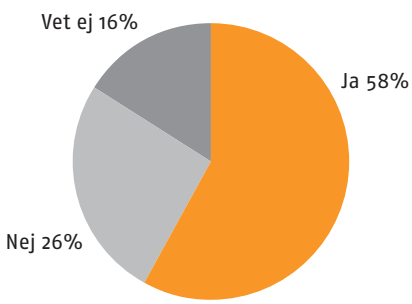
Ny teknik innebär ofta sårbarhet, och det är ett klart bekymmer för respondenterna. Funderingar kring ökad sårbarhet finns både bland dem som tror att de kommer att ha IP-telefoni inom fem år (sex av sju respondenter), de som inte tror att IP-telefoni kommer att bli aktuell under den här perioden (fyra av fyra respondenter) och till och med någon enstaka respondent som redan har erfarenhet av IP-telefoni idag.

Resonemanget från de personer som inte ser ökad sårbarhet som ett problem lutar sig främst mot bedömningen att den går att bygga bort och att det trots allt finns möjligheter att skapa redundans. Ett antal respondenter påpekar också att vanlig telefoni har andra nackdelar och att det är förhållandevis lätt att avlyssna mobiltelefoni och koppartrådsteknik idag. För dem handlar det inte om den ovan diskuterade sårbarheten utan en sårbarhet av ett annat slag, mer förbunden med hot om terrorism, spionage etc.

Många av de respondenter som däremot känner en osäkerhet inför IP-telefoni beskriver ett antal olösta problem som ökar sårbarheten. Mest bekymrad är man för hur strömförsörjningen kan garanteras och att vissa specifika IT-relaterade sårbarhetsproblem också kan drabba telefonin. I och med att det finns så stora frågetecken blir införandet av IP-telefoni också en komplex ekonomisk fråga, eftersom de kostnadsbesparingar som går att uppnå måste vägas mot de investeringar som behövs för att göra om nätverket och bygga in redundans. Frågan är om alla nödvändiga investeringar kommer att göras. Det

Bild 12. Antal respondenter (i %) som anser att IP-telefoni ökar sårbarheten för organisationen

Anser du att IP-telefoni innebär/skulle innebära ökad sårbarhet för er verksamhet?



Bas: 22 respondenter
Sluten fråga
Vet ej: 3
Inget svar: 3

framgår i intervjuerna att IP-telefoni är ett ämne som diskuteras intensivt och mellan raderna kan man läsa att en del respondenter är rädda för att det blir för stort fokus på kostnadsbesparingar och för lite på säkerhetsfrågor.

Ingen av personerna i organisationer som redan har IP-telefoni idag kan svara ”ja” på frågan om det finns en plan om all IT-telefonin skulle bli utslagen. Tre av dem kan säga att det inte finns någon plan, en är osäker och en väljer att stå över frågan.

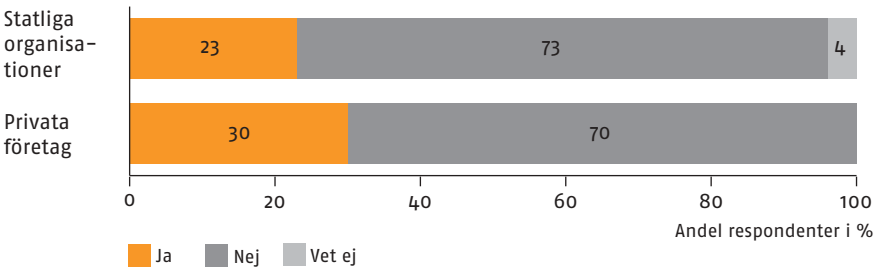
I dagens läge är det allra vanligaste att IT och telefoni ligger på samma avdelning. Det finns bara en central myndighet och ett statligt bolag där IT och telefoni fortfarande är uppdelade, men i båda fall diskuteras en omstrukturering och en mer enhällig datastruktur.

3. Användning av IP-telefoni

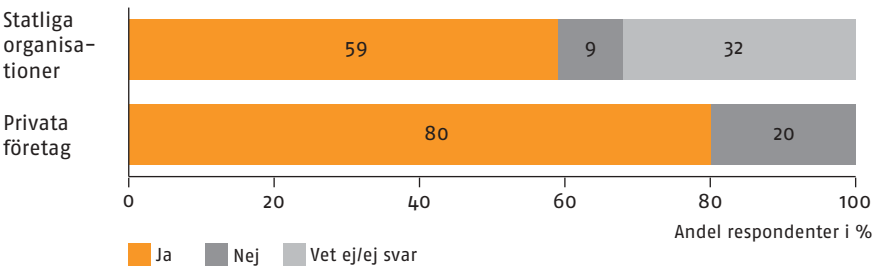
I dagsläget finns det förhållandevis få skillnader mellan statliga organisationer och privata företag när det gäller användning av IP-telefoni. Bilderna nedan visar att ungefär två av tio respondenter på myndigheter/statliga bolag och tre av tio näringslivsrespondenter uppger att IP-telefoni redan nu är ett faktum i deras organisation. Många av dem som inte har IP-telefoni idag tror dessutom att tekniken kommer att införas under de närmaste fem åren. Om man räknar ihop dessa siffror (användningen idag och förväntad användning om fem år) kommer IP-telefoni inom en nära framtid att vara vanligare än traditionell telefoni både inom det offentliga Sverige och i näringslivet. Införandet av IP-telefoni kommer dock att gå snabbare i privata företag, vilket till stor del beror på att det finns en mer utbredd känsla inom näringslivet att det går att lösa säkerhetsproblem som är förknippade med IP-telefoni och att riskerna inte är så stora att de kan äventyra kärnverksamheten. (se även nästa sida)

Jämförelsebild 3. Användning av IP-telefoni idag och om fem år

IP telefoni idag:



IP telefoni om fem år: ***(inklusive de respondenter som säger att IP-telefoni redan finns idag)***



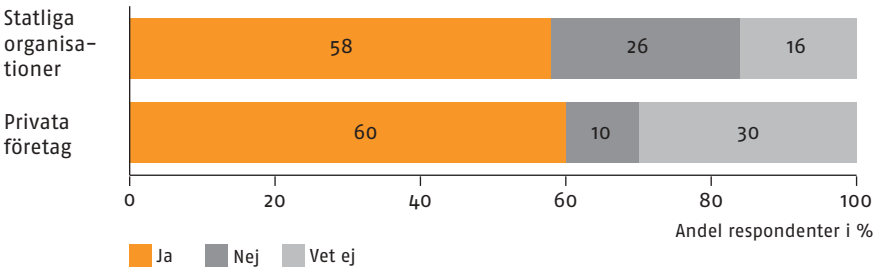
JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

4. Sårbarheter i samband med användning av IP-telefoni

Precis som inom offentliga organisationer finns det en medvetenhet bland IT- och IT-säkerhetsansvariga inom näringslivet att IP-telefoni med dagens förutsättningar kan innebära ökad sårbarhet. Som bilden nedan visar är förhållandet mellan dem som tror på ökad sårbarhet och de som inte gör det till och med större i privata företag. En viktig skillnad är dock att säkerhetsmarginalerna inom många myndigheter och statliga bolag behöver vara större än inom privata företag. Tekniska lösningar som finns idag eller som man tror kommer att finnas inom några år kan därför vara tillfredsställande för representanter inom näringslivet medan de inte räcker till för att skydda vissa typer av offentlig och samhällskritisk verksamhet.

Jämförelsebild 4. Användning av IP-telefoni idag och om fem år

Möjligheten att sårbarheten ökar vid införandet av IP-telefoni:



IT-säkerhet generellt och i krissituationer

Bedömning av organisationens säkerhetsnivå idag

Efter den detaljerade kartläggningen av den allmänna IT-miljön som presenterades i förra kapitlet redogörs i detta tredje kapitel nu mer specifikt för hur själva IT-säkerhetsarbetet ser ut hos de myndigheter och statliga bolag som deltar i studien. För att få en bra, övergripande bild av IT-säkerhetsläget började denna del av intervjuerna med en mycket detaljerad fråga kring tolv IT-säkerhetsrelaterade faktorer. Respondenterna ombads först att ange hur viktiga de tycker att dessa faktorer är på en skala från 1–10 och sedan hur väl deras organisation presterar på dessa punkter, m.a.o. hur god säkerhetsnivån är. De fick ta ställning till faktorer inom följande fyra områden:

I. Skydd/åtgärder mot intrång av skadlig kod

1. Optimalt brandväggsskydd
2. Kontinuerligt uppdaterade anti-virus program
3. Kontinuerlig uppdatering av övriga system/tilltäppande av sårbarheter
4. VLAN
5. Optimal konfigurering av säkerhet i nätverket (generellt)

II. Back-up

6. Back-up system
7. Övrig redundans/reservkapacitet i systemet som kan användas vid behov

III. Fysiska skydd mot strömbortfall

8. Säker strömförsörjningsmiljö: UPS (Unbreakable Power System), kylning, vatten m.m.

IV. Kompetens/medvetenhet om IT- och informationssäkerhet

9. Specialistkompetens när det gäller IT-och informationssäkerhet
10. Kompetensbredd: att ett tillräckligt antal personer är insatta i säkerhetsfrågor
11. Att de som är insatta i IT-frågor följer alla rutiner och processer

12. Generell medvetenhet av de anställda på området IT- och informationssäkerhet

Tabellen på nästa sida och det tillhörande diagrammet visar att många respondenter anser att de största säkerhetsriskerna idag inte ligger på tekniksidan utan på den mjuka sidan, d.v.s. den *mänskliga faktorn*. De tre faktorer som förknippas mest med säkerhetsrisker tillhör alla tre den fjärde av de ovanstående grupperna: kompetens & medvetenhet om IT-och informationssäkerhet.

Om man tittar på den aggregerade säkerhetsnivån för varje faktor (d.v.s. genomsnittet för samtliga 22 respondenter) i förhållande till faktorns aggregerade viktighet framgår klart att myndigheter och statliga bolag känner mest oro när det gäller *generell medvetenhet hos de anställda på området IT- och informationssäkerhet*, tätt följt av att *de som är insatta i IT-frågor inte följer alla rutiner och processer* och att *kompetensbredden är för smal och att inte ett tillräckligt antal personer är insatta i säkerhetsfrågor.* Bilden är något bättre när det gäller *specialistkompetens på området IT-säkerhet*, trots att det finns problem även där.

De områden där säkerhetsnivån anses vara bra är av mer teknisk karaktär. De senaste årens många intrång eller försök till intrång av skadlig kod har gjort att skyddet har förbättrats väsentligt. I dagsläget känner sig de flesta myndigheter och bolag trygga när det gäller *optimalt brandväggsskydd, kontinuerligt uppdaterade anti-virus program* och, för dem som har det, *VLAN*. Även när det gäller strömförsörjningsmiljön är den generella bilden att det finns ett bra fysiskt skydd mot strömbortfall, motsvarande den acceptabla för upprätthållandet av en god IT-säkerhetsnivå.

Det är viktigt att observera att det trots allt finns ett antal teknikrelaterade aspekter där det finns en del övrigt att önska sig, t.ex. optimal konfigurering av säkerhet, kontinuerlig uppdatering av övriga system/tilltäppande av sårbarheter och redundanslösning, såsom reservsystem.

I vilken mån respondenternas bedömning av kvaliteten på deras skydd mot skadlig kod är grundat på ett gediget strategiskt IT-säkerhetsarbete eller enbart på det faktum att de inte har drabbats så hårt tidigare är svårt att besvara. I vissa kommentarer kopplas t.ex. nöjdheten med olika delar av virusskyddet till uteblivna incidenter, vilket kan tyda på en falsk trygghet.

Den viktiga slutsatsen att IT-säkerhetsrisker i hög grad är kopplade till brist på kompetens, disciplin eller medvetenhet illustreras tydligt i ett citat från en säkerhetschef:

”Det är extremt viktigt att man har en bra säkerhetskultur som når ut till användarna, men den behöver inte vara djup. De stora bristerna ligger inte i tekniska lösningar eller spetskompetens utan i att rutiner inte följs. Jag har jobbat i den här branschen sedan början av 70-talet och mycket beror på användarnas medvetenhet och rutiner. Du kan ställa

Bild 13. IT-relaterade faktorer ordnade efter viktighet (aggregerat resultat för samtliga 22 respondenter)

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

stor sårbarhet

ansenlig sårbarhet

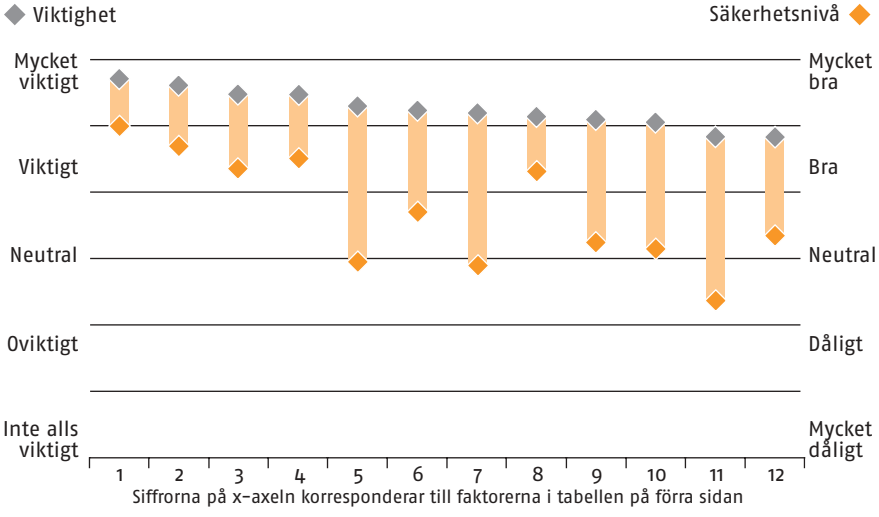
liten sårbarhet

Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: viktighet: 1 / säkerhetsnivå: 3

upp hur många brandväggar som helst men om rutinerna inte följs fungerar det ändå inte." (Ledande befattning, central myndighet)

Förutom att uttala sig om ovanstående tolv faktorer ger respondenterna också en mer generell och sammanfattande bedömning av IT-säkerheten, både när det gäller viktighet och den säkerhetsnivå som uppnås inom respektive organisationer. En jämförelse mellan de viktigaste målgrupperna visar att IT-säkerheten ligger mellan 9 och 10 på skalan 1-10. Högst krav på IT-säkerhet finns inom centrala myndigheter och centrala bolag. Den faktiska säkerhetsnivån ligger mellan två och tre poäng under viktighetsbedömingarna, med undantag av länsstyrelserna. Det bör observeras att det låga antalet intervjuer gör att det egentligen inte finns en statistiskt signifikant grund för en sådan jämförelse, men det är ändå intressant att se vilka mönster och samband som finns inom detta lilla urval.

Bild 14. Visuell redovisning av säkerhetsnivå i relation till viktighet (aggregerat resultat för samtliga 22 respondenter)



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: viktighet: 1 / säkerhetsnivå: 3

Bild 15. Viktighet av IT/informationssäkerhet generellt i förhållande till den faktiska säkerhetsnivån som uppnås (redovisning per målgrupp och totalt)

Målgrupp	Viktighet	Säkerhets-nivå	Skillnad
Central myndighet	9,8	7,5	-2,3
Statligt bolag	9,5	7,0	-2,5
Länsstyrelse	9,0	7,7	-1,3
Kommun	9,3	6,7	-2,7
Totalt	9,5	7,3	-2,2

Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: viktighet: 1 / säkerhetsnivå: 3

---

5. IT-säkerhet inom det svenska näringslivet jämfört med myndigheter och statliga bolag

Trots att det finns stora likheter mellan statliga organisationer och privatföretag i deras syn på vad som krävs för att uppnå en fullgod IT-säkerhetsnivå känner respondenterna i båda målgrupper sig olika nöjda med den IT-säkerhet som faktiskt uppnås. Bilden nedan visar tydligt att skillnaden mellan säkerhetsnivån för varje faktor och det betyg som uttrycker dess viktighet i många fall är betydligt större för myndigheter och statliga bolag än för privata företag. Anledningen är inte att själva säkerhetsnivån är så mycket högre inom näringslivet, även om det finns en liten skillnad till de privata företagens favör. I själva verket är det så att de statliga organisationernas verksamhet generellt sett är av en sådan karaktär att kraven på IT/informationssäkerhet är högre än i näringslivet och därmed även vikten av nedanstående IT-säkerhetsrelaterade faktorer. Så även om IT-säkerheten i absoluta termer inte är sämre i offentliga organisationer är den ändå inte tillräckligt bra för att möta de höga kraven.

Med undantag av VLAN, som i många privata företag inte betraktas som ett viktigt verktyg för att befrämja IT-säkerheten, bekräftas den bild som kom fram i analysen av de statliga organisationerna att det är inom de 'mjuka faktorerna (kompetens, rutiner, medvetenhet) det finns mest potential för förbättring. Det som efterlyses i första hand inom det privata näringslivet är *bättre generell medvetenhet hos de anställda på området IT-säkerhet* och *att de som är insatta i IT-frågor inte följer alla rutiner och processer*. På området kompetens är det främst *bredden på IT-säkerhetsrelaterad kompetens* som inte är optimal. Däremot anses *specialistkompetensen* inom näringslivet vara förhållandevis hög. Ett bättre

back-up system eller i alla fall bättre rutiner kring hanteringen av det är den enda tekniska faktorn där den faktiska säkerhetsnivån ligger lite längre ifrån det genomsnittliga viktighetsbetyget.

Jämförelsebild 5. IT-säkerhetsnivå i förhållande till viktighet inom statliga organisationer och privata företag

IT-säkerhetsrelaterade faktorer: (siffran inom parentes hänvisar till grupp)	Statliga organisationer			Privata företag		
	Viktighet	Säkerhetsnivå	Skillnad	Viktighet	Säkerhetsnivå	Skillnad
1. Optimalt brandväggsskydd (I)	9,7	9,0	-0,7	9,4	8,6	-0,8
2. Kontinuerligt uppdaterade antivirusprogram (I)	9,6	8,7	-0,9	9,2	8,7	-0,5
3. Back-up system (II)	9,5	8,4	-1,1	10	8,8	-1,2
4. Säker strömförsörjningsmiljö (III)	9,5	8,5	-1,0	9,5	8,8	-0,7
5. Att de som är insatta i IT-frågor följer alla rutiner & processer (VI)	9,3	6,9	-2,4	9,1	7,8	-1,3
6. Specialistkompetens när det gäller IT/informationssäkerhet (VI)	9,2	7,7	-1,5	8,9	8,3	-0,6
7. Kompetensbredd; att ett tillräckligt antal personer är insatta i säkerhetsfrågor (VI)	9,2	6,9	-2,3	8,7	7,5	-1,2
8. VLAN (I)	9,1	8,3	-0,8	6,6	7,0	+0,4
9. Kontinuerlig uppdatering av övriga system/tilltäppande av sårbarhet (I)	9,1	7,3	-1,8	8,5	7,5	-1,0
10. Optimal konfigurering av säkerhet (I)	9,1	7,2	-1,9	8,4	7,7	-0,7
11. Generell medvetenhet hos de anställda på området IT/informationssäkerhet (VI)	8,9	6,4	-2,5	8,1	6,6	-1,5
12. Övrig redundans/övriga reservsystem som kan användas vid behov (II)	8,8	7,4	-1,4	7,9	7,1	-0,8

stor sårbarhet

ansenlig sårbarhet

liten sårbarhet

Säkerhet och IT-säkerhet inom organisationen

Det är relativt vanligt att myndigheter och statliga bolag har en särskild säkerhetsavdelning. I två av de centrala myndigheterna, ett landsting och en kommun är organisationen dock uppbyggd på ett annat sätt. Inom dessa organisationer finns också personer som arbetar med säkerhet, men inte i en självständig operativ enhet.

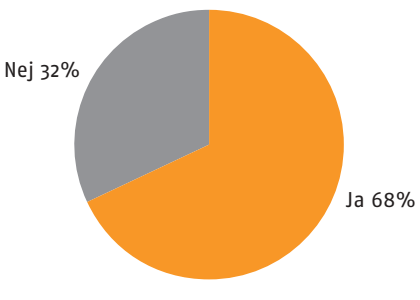
Med undantag av en central myndighet finns inom alla organisationer åtminstone en och ibland flera IT-säkerhetsansvariga. Inom den myndighet där båda två respondenter svarar nekande på denna fråga finns visserligen en IT-säkerhetschef (som också är med i undersökningen) men formellt är denna person inte ansvarig för säkerhet utan styr upp säkerheten. De olika avdelningscheferna har själva ansvaret.

Antalet personer som arbetar med IT-säkerhet varierar starkt; olika respondenter hanterar olika definitioner av IT-säkerhetsarbete och vem som kan tänkas vara involverade i det. Beroende på organisationens storlek och struktur samt verksamhetens inriktning kan det röra sig om allt från några enstaka nyckelpersoner till tiotals eller till och med hundratals personer som delvis har IT-säkerhet på sitt bord.

I många fall är IT- och informationssäkerhet och fysisk säkerhet integrerade. Inom de organisationer där detta inte är fallet finns det vanligtvis regelbundna kontakter mellan de båda avdelningarna. Flera av de respondenter som säger att fysisk och IT-säkerhet

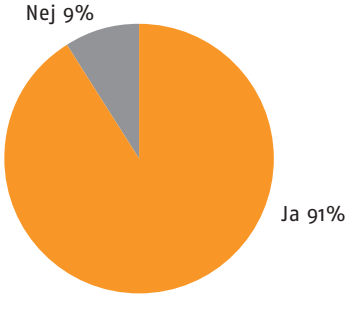
Bild 16. Organisationens utformning med hänseende till säkerhet och IT-säkerhet

Har ni en specifik säkerhetsavdelning?



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 0

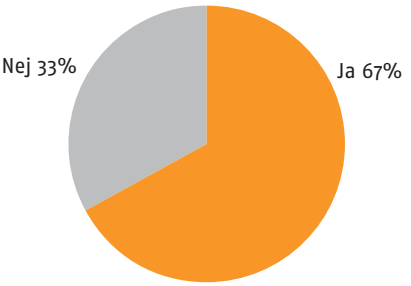
Har ni en IT-säkerhetsansvarig?



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 0

Bild 17. Organisationens utformning med hänseende till säkerhet och IT-säkerhet

Är fysisk- och IT/informationssäkerhet integrerade?



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 1

inte är integrerade påpekar att de delar av det fysiska skyddet som är direkt relaterade till IT kan ligga på IT-säkerhetssidan, medan alla andra aspekter av det fysiska skyddet tas hand om av en speciell avdelning. En respondent anser att båda funktioner ska vara integrerade i en avdelning och att han har lagt fram ett förslag om detta, men inte fått gehör för det.

Generell medvetenhet kring IT-säkerhet i organisationen

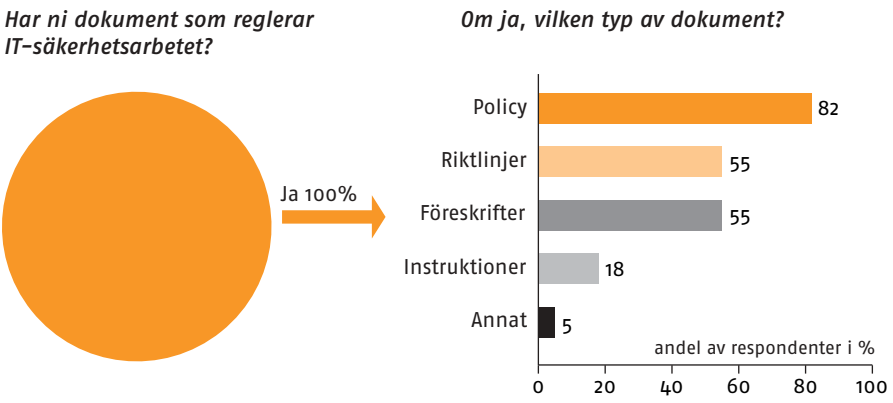
Fokuserar man på den icke-tekniska sidan av IT-säkerhet inom myndigheter och statliga bolag finns ett antal faktorer som starkt påverkar medvetenheten kring IT-säkerheten och det faktiska beteendet som detta leder till. En av dessa faktorer är kvaliteten och utformningen av dokumentation samt hur lätt det är att få tillgång till relevant information, både för IT-ansvariga och vanliga anställda. En annan faktor är i vilken mån en organisation aktivt sprider medvetenhet kring dessa frågor genom att t.ex. satsa på utbildning och olika typer av kompetensutveckling. Även här är det viktigt att både titta på investeringar i ökad *spetskompetens* och i en bredare och mer generell baskompetens för samtliga anställda.

En underliggande fråga som påverkar den totala insatsen på området IT- och informationssäkerhet är givetvis vilka ekonomiska medel som är avsatta för det totala IT-och informationssäkerhetsarbetet och hur dessa fördelas mellan exempelvis tekniska skyddsåtgärder mot skadlig kod, förbättringen av strömförsörjningsmiljön och investeringar i mjuka faktorer såsom ökad medvetenhet, ökad kompetens och bättre rutiner. Just denna fråga är dock mycket svår att besvara för de allra flesta, i vissa fall för att de inte delar upp budgeten på det här viset och även p.g.a. att det är svårt att dra en exakt gräns för när det gäller var IT-säkerhetsarbete slutar och vanliga IT-rutiner, som t.ex. driftservice, börjar. De som kan göra en uppskattning tror generellt att det ligger mellan 1–5 % av den totala IT-budgeten.

Dokumentation

Dokumentation som reglerar IT-säkerhetsarbetet finns inom varje deltagande organisation, främst som policydoku-

Bild 18. Dokument som reglerar IT-säkerhet



ment, men även som föreskrifter och riktlinjer. (se bild 18 på nästa sida). Ett antal respondenter nämner också instruktioner i form av säkerhetshandböcker. Av vikt i sammanhanget är hur ofta och enligt vilka rutiner dessa dokument uppdateras. Ungefär varannan respondent anser att det i det stora hela finns bra, fasta rutiner inom deras organisation när det gäller uppdatering av IT-säkerhetsdokument. Detta kan vara inom olika typer att rullande scheman eller fasta avstämningsmoment som man har kommit överens om internt. Två av de centrala myndigheterna jobbar med en informationssäkerhetsstandard enligt ISO 17799.

Bland de resterande respondenterna finns en större osäkerhet och en vanlig kommentar är att dokumenten uppdateras först när det finns ett uppenbart behov. I dessa fall finns dock inga fasta rutiner för att se över dokumenten och att hålla dem helt uppdaterade. Två personer (på landstings- och kommunnivå) hänvisar till KBM och säger att ett arbete pågår för att strukturera upp IT-säkerhetsarbetet enligt rekommendationerna i BITS.

Aktiva åtgärder för att befrämja säkerhetsmedvetande kring IT

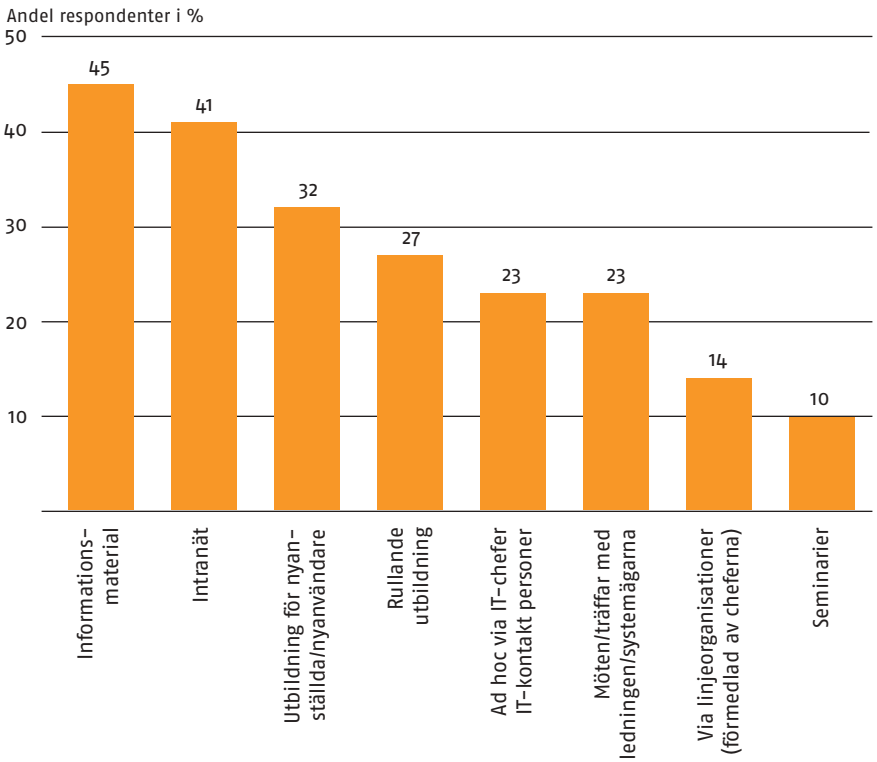
Medvetenheten kring IT- och informationssäkerhet kan ökas på en mängd olika sätt. Samtliga organisationer i studien är mer eller mindre aktiva när det gäller att nå ut till de anställda, men exakt vilka informationskanaler som används och med vilken frekvens skiljer sig åt väldigt mycket. För vissa myndigheter och statliga bolag är det givet att dokument som reglerar IT-säkerhetsarbete

görs tillgängligt till samtliga anställda i en förenklad form, t.ex. som informationshäfte. För andra kan det däremot vara en medveten policy att inte ”frysa” IT-säkerhetsrekommendationer på papper och i stället satsa på Intranät där uppdateringar kan göras direkt.

Överlag kan man säga att det finns lika många idéer om hur man ska nå ut till personalen som det finns organisationer, och förmodligen även fler eftersom nyckelpersoner inom samma organisation inte alltid har samma åsikter. Respondenterna nämner i många fall

Bild 19. Viktigaste informationskanaler som används för att öka medveten kring IT-säkerhet

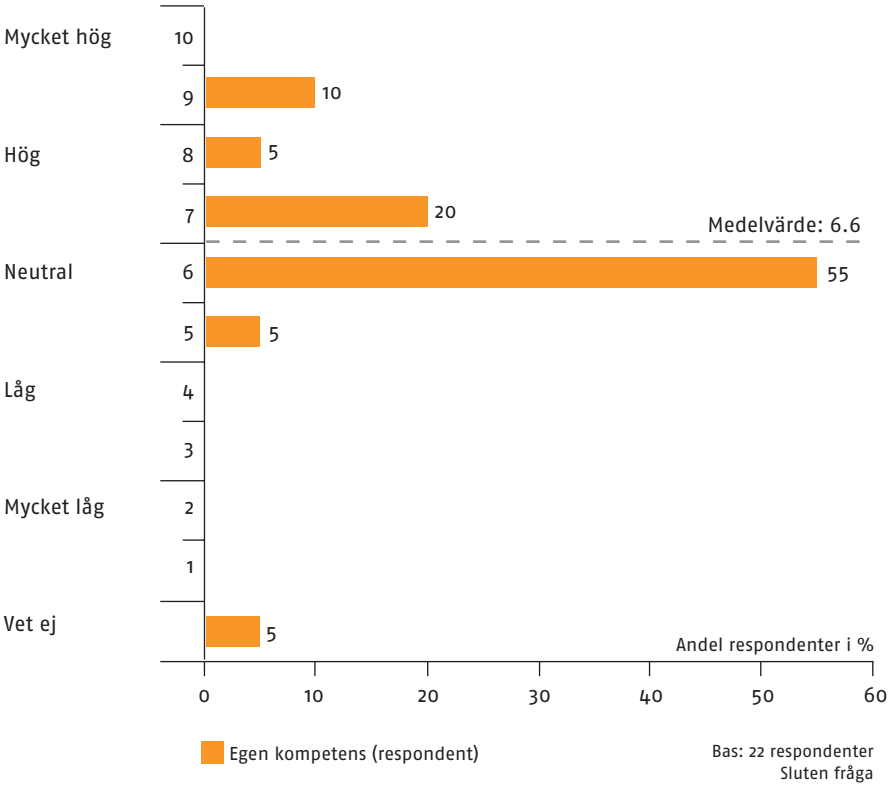
Hur sprids medvetenheten kring IT/informationssäkerhet i organisationen?



Bas: 22 respondenter
Öppen fråga
Vet ej: 0
Inget svar: 0

Bild 20. Respondenternas nöjdhet med den generella IT-medvetenheten kring IT/informationssäkerhet

På en skala från 1–10, hur nöjd är du med den generella medvetenheten kring IT/informationssäkerhet i organisationen som helhet?



Bas: 22 respondenter
Sluten fråga
Vet ej: 1
Inget svar: 2

en kombination av informationsinsatser som tillsammans ska få medvetenheten att bli tillräckligt bra. På en aggregerad nivå är dokument som t.ex. informationshäften och säkerhetshandböcker viktigast (nämnt av 45 % av respondenterna), följt av intranätet (41 %). I hälften av dessa myndigheter och statliga bolag (sju av fjorton) satsas det antingen på utbildningar till nyanställda/nyanvändare (32 % av respondenterna) eller rullande utbildningar (27 %). Andra sätt att sprida information är ad hoc insatser av IT-chefer eller andra kontaktpersoner från IT-avdelningen, möten med ledningen eller system-

ägarna, muntliga eller skriftliga uppdateringar via cheferna i linjeorganisationen och via seminarier.

Trots de vidtagna åtgärderna inom samtliga organisationer är många respondenter inte nöjda med den generella medvetenheten kring IT- och informationssäkerhet. På en skala från 1-10 är det genomsnittliga betyget bara 6,6, vilket tyder på att det finns en stor förbättringspotential. Kommentarerna visar att missnöjet både kan bero på att fler insatser behövs och att de som görs inte överallt har förväntad effekt.

Det är viktigt att notera att medvetenheten kan skilja sig mycket mellan de olika avdelningarna beroende på hur organisationen är uppbyggd och hur heterogen organisationen är. Inom vissa myndigheter och bolag kan det finnas helt olika yrkeskategorier som t.ex. IT-experter med ansvar för kärnverksamheten, tekniker som rör sig i landet och administrativ personal som tar hand om löner, fakturering etc. Att effektivt nå ut till alla dessa personer förutsätter att kommunikationen anpassas efter arbetssituation och förkunskaper.

Även inom organisationer med en mer homogen sammansättning finns skillnader mellan olika avdelningar eller personalkategorier. Ett vanligt problem är att det finns två ”arketyper” som brukar ställa till det när det gäller IT-säkerheten. Först finns det ett antal ’vanliga anställda’ som vet väldigt lite om IT-säkerhet eftersom de inte har fått eller tagit till sig den information som finns att tillgå. Deras agerande leder ofta till små incidenter som visserligen tar tid och energi i anspråk från IT-avdelningen, men som ändå inte gör så mycket skada att det leder till produktionsbortfall. De personer som verkligen kan hålla IT-säkerhetscheferna vakna om nätterna är personer som är insatta och som har tillgång till stora delar av systemet, antingen för att de är IT-tekniker eller för att de spelar en viktig roll inom kärnverksamheten. Övertro på sig själv och på systemet kan leda till ödesdigra felbedömningar.

Kompetens hos dem som är involverade i IT-säkerhetsarbetet

Förutom den generella medvetenheten kring IT-säkerhet påverkas den totala säkerhetsbilden också av den kompetens och de rutiner som finns bland dem som är direkt IT-ansvariga, antingen operativt eller på ledningsnivå. De personer som intervjuats inom ramen av den här studien är nästan utan undantag nyckelpersoner som tillhör denna kategori och det är intressant att se hur de själva ser på sin kompetens på området. Innan man gör det är det dock viktigt att notera att kompetens är ett begrepp som man kan tolka på olika sätt. Som vissa personer påpekar finns det många system inom IT-miljön som de inte kan i detalj, men de har däremot den övergripande kunskap om IT-säkerhet som behövs för att kunna föreslå åtgärder som höjer säkerheten för organisationen. Andra går ännu ett steg längre och säger att deras funktion

framför allt kräver att de har en ingående förståelse för organisationens kärnverksamhet och att de ska ha beställarkompetens för att kunna omge sig med personer som kan föreslå konkreta anpassningar och uppdateringar inom IT-miljön.

De kompetensbetyg som respondenterna ger sig själva bör därför främst betraktas som ett uttryck för hur väl de är rustade för att kunna göra ett bra jobb som beslutfattare eller operativt ansvarig inom området IT-säkerhet, snarare än ett absolut mått på deras IT-

Bild 21. Bedömningar av respondenternas egen kompetens och den kompetens som deras kollegor har som är aktiva inom området IT-säkerhet

På en skala från 1–10, hur bedömer du din egen kompetens på området IT/informationssäkerhet och hur bedömer du den genomsnittliga kompetensen hos övriga personer som är involverade i detta arbete?

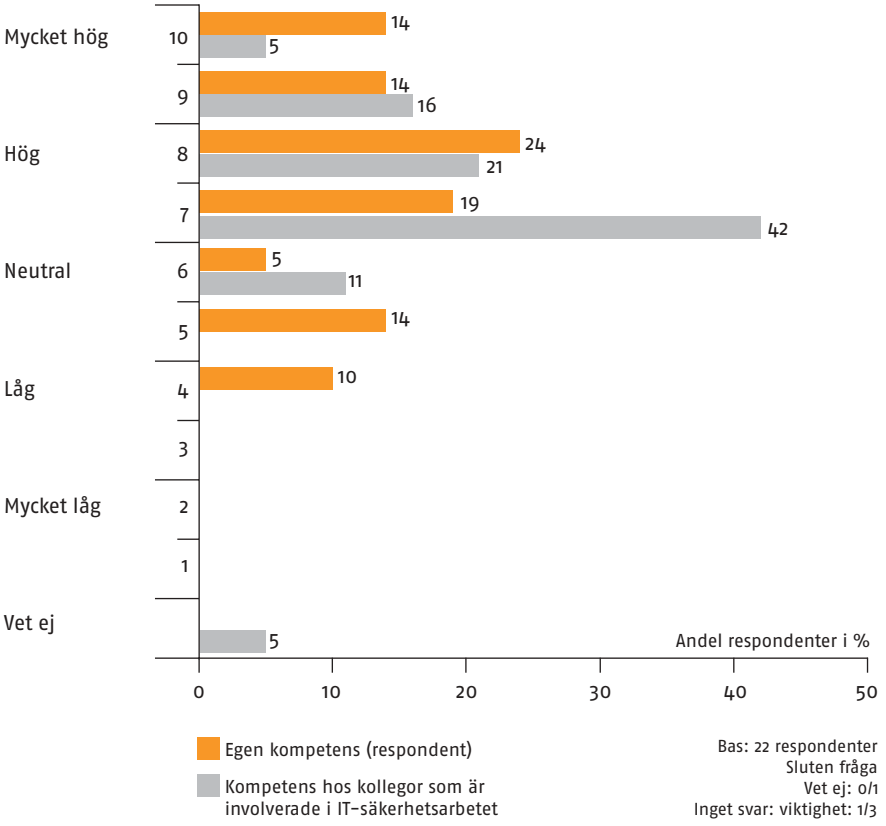


Bild 22. Behov av kompetenshöjning

På vilket/vilka områden skulle du önska dig att du själv och organisationen* får bättre kunskap?

Andel respondenter i %

Kompetenshöjande åtgärder som respondenterna efterlyser:	Egen kompetens:	Kollegornas kompetens:
1. Bättre *teknisk* kunskap om IT-lösningar (olika områden)	33	5
2. Ökad kunskap om hur man kommunicerar/förmedlar IT-säkerhet i organisationen	19	–
3. Ökad kunskap om (nya) produkter/tjänster på området IT-säkerhet	19	5
4. Generell kunskapsökning inom IT/IT-säkerhet (ospecificerat)	14	11
5. Inget konkret behov	14	5
6. Ökad kunskap om interna system och deras kopplingar	10	16
7. Bättre omvärldsanalys av eller kunskap om externa hot/ skadlig kod	10	11
8. Ökad kunskap om fysiska hot	5	5
9. Visa bättre förståelse för regler/följa rutiner på ett bättre sätt	–	21
10. Visa bättre förståelse för konsekvenser av justeringar i IT-miljön för kärnverksamheten	–	16
11. Bredda befintlig kompetens till fler personer	–	11
12. Övriga svar	5	5

* Den del av organisationen som jobbar med IT-säkerhetsfrågor

Bas: 22 respondenter
Öppen fråga
Vet ej: 1/0
Inget svar: 1/3

relaterade kunskaper. När respondenterna bedömer kunskapen hos andra personer som på något sätt är involverade i arbetet med IT- och informationssäkerhet inom är det däremot bara den sistnämnda dimensionen som gäller. Denna skillnad i perspektiv kan vara en av anledningarna till varför kompetensen hos de kollegor som jobbar med IT-säkerhet bedöms vara mer homogen än den egna kompetensen. Genomsnittet för kompetensbetygen i båda grupper är däremot relativt lika: 7,3 för respondenternas egen kompetens och 7,6 för kollegor som är verksamma inom området IT-säkerhet.

Genom att studera de existerande kompetensbehoven inom respektive organisation går det att få en djupare förståelse för hur ovanstående siffror bör tolkas. Om man börjar med att titta på det som respondenterna anser om den egna kompetensen framgår av tabellen på förra sidan (bild 22) att en ökad teknisk kunskap om befintliga och nya IT-lösningar är mest eftertraktad. Den övergripande och sammanlänkade kompetens som de flesta respondenterna har i dagsläget räcker visserligen långt för att kunna strukturera upp IT-säkerhetsarbetet, men i många fall är det teknikernas specifika kunskaper som krävs för att göra planerna konkreta.

Två andra typer av kompetens som efterlyses är att vara mer uppdaterad när det gäller utvecklingen av nya produkter och tjänster som befrämjar IT-säkerhet, samt ett förbättrat sätt att kommunicera frågan i organisationen. Den sistnämnda punkten är särskilt viktig eftersom kommentarer om icke-optimal kommunikation även nämns på andra håll i intervjuerna. Kommunikation om IT-säkerhet kan rikta sig både mot ledningen (för att sälja in och förankra nödvändiga förändringar), mot IT-personalen (för att instruera de som har ett operativt ansvar) och mot vanliga anställda (för att öka medvetenheten). I alla dessa fall är det väldigt viktigt med bra pedagogik i framställningen för att kunna nå ut med budskapet. Även om en del av ansvaret givetvis ligger på mottagarna finns det i alla fall bland en del respondenter en medvetenhet om att det bör finnas möjligheter att förbättra kommunikationen. Följande två citat illustrerar detta behov:

”Jag har en bakgrund från tekniken och en förmåga att se sammanhang. Jag har gått kurs som VM-Data driver och följer utvecklingen, men man kan ju alltid behöva mer. Det som gör det hela svårt är att jag har en så blandad roll. Det jag skulle behöva mer av är praktisk erfarenhet av att sälja in budskap, ha aktiviteter tillsammans med personalen, t ex. göra riskanalyser under lite enklare former.” (IT, landsting)

”En av de viktigaste saker som jag skulle vilja lära mig är att följa upp och ställa krav på personalen att de gör det de ska göra. Det är ingen idé att jag sätter mig in i alla våra olika system. De viktigaste är att jag har den övergripande kunskap som krävs för att se till att de som är ansvariga för alla dessa system gör sitt jobb.” (IT, statligt bolag)

Det är signifikativt att de två viktigaste kompetenshöjande åtgärderna som respondenterna föreslår för andra inom organisationen som jobbar med IT eller IT-säkerhetsarbete är att de först och främst blir bättre på att lära sig reglerna och följa rutinerna samt att de visar mer förståelse för konsekvenserna av justeringar i IT-miljön för kärnverksamheten. Även detta är delvis är en kommunikationsfråga och understryker ännu en gång vikten av de mjuka faktorerna inom IT-säkerhetsarbetet.

Bättre omvärldsanalys i samband med externa hot, som t.ex. riskerna för intrång av skadlig kod, nämns också som ett område där den egna kompetensen och IT-kollegornas kompetens skulle kunna höjas, men de allra flesta anser att de är väl insatta när det gäller skadlig kod.

JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

6. Kompetensbehov inom näringslivet på området IT/informationssäkerhet

Den genomsnittliga kompetensen hos samtliga personer som är insatta i IT-frågor skiljer sig inte nämnvärt åt mellan privatföretag och statliga organisationer och ligger i båda fall nära 7,5 på en skala från 1–10. Dessa siffror bör dock tolkas mot bakgrunden att kraven på specialistkompetens och kompetensbredd generellt är något högre hos statliga organisationer än hos privatföretag, vilket medför att behovet av kompetenshöjande åtgärder också är större.

Tittar man mer exakt på vilken kompetenshöjning som främst efterlyses av respondenterna inom privatföretag framgår att hårda faktorer såsom *bättre kunskap om IT-lösningar* och *ökad kunskap om (nya) produkter/tjänster på området IT-säkerhet* nämns något oftare än mjuka faktorer, men på det stora hela korresponderar bilden av näringslivet väl med den av de statliga organisationerna.

Kommunikation kring IT-säkerhet generellt och vid incidenter

Som framgick i kapitel 2 har de flesta organisationer klara rutiner om hur IT-frågor ska kommuniceras, både i vardagssituationer och vid incidenter. Det finns dock undantag. Speciellt när det gäller incidenthantering medger ett antal respondenter på kommun- och landstingsnivå att det finns få fasta rutiner (se bild 24 längst ner på sidan). Generellt kan man säga att de centrala myndigheterna har de mest väldefinierade kommunikationsrutinerna.

Bilden på nästa sida visar hur kommunikationen ser ut i vardagssituationer, d.v.s. när det inte är relevant med incident- eller krishantering. Det är intressant att konstatera att personer i ledande befattningar och personer med operativt IT-ansvar eller IT-säkerhetsansvar inom samma organisation ibland ser lite olika på vilken som är den vanligaste kanalerna för att kommunicera IT-/informationssäkerhet.

Bild 23. Viktigaste kommunikationskanaler när det gäller IT/informationssäkerhet i allmänhet

Till IT-personal:
Hur kommunicerar ni med ledningsgruppen när det gäller IT/informationssäkerhet i allmänhet?

Till personer i ledande befattningar:
Hur kommunicerar ni med era IT-ansvariga när det gäller IT/informationssäkerhet i allmänhet?

Viktigaste kommunikationskanal:	Antal svar Operativt IT/IT-säkerhetsansvar (12)	Antal svar Ledande befattningar (10)
1. Gemensam IT- och ledningsgrupps representation i IT-råd/IT-forum	4	3
2. Inga fasta rutiner: möten mellan IT-avdelningen och ledningsgruppen vid behov	3	4
3. Direkt representation av IT-/IT-säkerhetschefer i ledningsgruppen	2	2
4. Fasta kommunikationsrutiner via IT-samordningsgruppen	1	1
5. Rapportering direkt till VD:n (regelbundna avstämningar)	1	–
6. Regelbunden kommunikation med ledningen via en driftsorganisation	1	–

Bas: 22 respondenter (12 personer med operativt IT/IT-säkerhetsansvar / 10 personer i ledande befattningar)
Öppen fråga
Vet ej: 0/0
Inget svar: viktighet: 0/0

Bild 24. Viktigaste kommunikationskanaler vid incidenter

Bara till IT-personal:
Hur kommunicerar ni med ledningsgruppen när det gäller incidenter?

Kommunikationssätt vid incidenter:	Antal svar Operativt IT/IT-säkerhetsansvar (12)	Antal svar Kontinuerlig kommunikation (ja/nej)
1. Formering av operativ incidentgrupp och kontinuerlig kontakt med ledningen/VD:n	6	Ja
2. Inga fasta rutiner: ad hoc kommunikation mellan IT/IT-säkerhet och ledningen	4	Nej
3. Krisledningsgrupp med representation från ledningen och IT	2	Ja

Bas: Samtliga 12 respondenter med operativt IT/IT-säkerhetsansvar
Öppen fråga
Vet ej: 0
Inget svar: 0

Beredskap mot intrång av skadlig kod

Skadlig kod

I förra kapitlet analyserades ett stort antal aspekter kopplade till IT- och informationssäkerhet i de organisationer som intervjuats av Opticom. I detta tredje kapitel fördjupas analysen genom att titta närmare på en av dessa aspekter: skadlig kod. Skadlig kod definieras som program som sprider sig själva och som tränger in i system via olika kanaler. De viktigaste kanalerna är e-post, Internet-sidor och smittade informationsbärare såsom disketter och USB-sticks. Skadlig kod kan ta olika former, t.ex. virus, maskar, trojaner och hybrider. Det som kommer att tas upp i detta kapitel är respondenternas allmänna syn på skadlig kod, kvaliteten på organisationernas befintliga skydd mot skadlig kod, hypotetiska och verkliga intrång av skadlig kod och kaskadeffekter som kan uppträda som följd av incidenter med skadlig kod.

Utvecklingen av skadlig kod idag och i framtiden

En stor majoritet av respondenterna ser skadlig kod som ett stort hot och det finns en påtaglig oro för att det blir större i framtiden. Respondenterna är framför allt bekymrade över att vi kommer att se aggressivare former, att nya typer kommer att sprida sig ännu snabbare än idag och att skadlig kod i högre grad kommer att användas för att bedriva industrispionage och sabotera verksamhet. En annan intressant kommentar är att de egenskaper som kännetecknar traditionella typer av skadlig kod (virus, maskar, trojaner) kommer att blandas med andra typer av skadlig kod som ofta betecknas som SPAM (t.ex. spyware eller adware).

Ett antal respondenter väljer att gå in på konsekvenserna av skadlig kod snarare än att beskriva utvecklingen i sig själv och pekar exempelvis på att ökningen av skadlig kod begränsar myndigheternas möjligheter att vara öppna och tillgängliga i framtiden.

Bild 25. Respondenternas syn på utvecklingen av skadlig kod idag och i framtiden

Hur ser du på utvecklingen av skadlig kod idag och i framtiden?

Andel respondenter i %

Viktigaste åsikter om utvecklingen av skadlig kod idag och i framtiden	Samtliga
1. Växande problem – mer aggressiva former av skadlig kod (ospecificerat)	36
2. Oro för snabbare spridning samt ändrat spridningsmönster	18
3. Ökad användning av skadlig kod (t.ex. skräddarsydda trojaner) i samband med industrispionage/terrorhot	9
4. Påverkar hur öppna och tillgängliga vi kan vara i framtiden	9
5. Ökad fara av webbaserad kod	5
6. Farligare former av spyware för att lura åt sig uppgifter ("fishing")	5
7. Blandning av traditionell skadlig kod och SPAM	5
8. Kommer att tvinga fram vidare fysisk separation av känsliga system med minskad efffektivitet som följd	5
9. Kommer att kräva nya former av skydd	5
10. Potentiellt farlig vid dålig hantering – ofarlig så länge den sover	5
11. Inget stort problem p.g.a. ökad medvetenhet	5

Oro – fokus på skadlig kod i sig
Oro – fokus på konsekvenserna
Ingen stor oro

Bas: 22 respondenter
Öppen fråga
Vet ej: 0
Inget svar: 1

Två respondenter är mindre oroliga och anser att ökad medvetenhet och klok hantering av skadlig kod minskar farorna.

Organisationernas skydd mot skadlig kod

Optimalt skydd mot skadlig kod kräver en helhetssyn och en lång rad åtgärder på många olika områden. I en fråga där respondenterna får nämna de största enskilda faktorer som måste tillgodoses för att bygga upp ett effektivt skydd mot intrång av skadlig kod är fördelningen mellan svar som avser teknik och svar som avser människans agerande nästa helt jämn. Detta resultat bekräftar bilden från förra kapitlet att faktorer som bra och välkonfigurerade brandväggar, ett optimalt virusskydd och en bra patchhantering visserligen är extremt viktiga, men att IT-säkerheten i allmänhet och skydd mot skadlig kod i synnerhet inte kan garanteras utan att organisationen har medvetna användare,

Bild 26. De största enskilda faktorer som kan skydda mot intrång av skadlig kod enligt respondenterna

Vilka tror du är de största enskilda faktorer som skulle kunna skydda myndigheter/ organisationer mot intrång av skadlig kod?

Andel respondenter i %

De största ensklida faktorer som skyddar mot skadlig kod:	Samtliga respondenter
1. Bra medvetenhet hos användarna	43
2. Välskött brandvägg	43
3. Bra och frekvent uppdaterat virusskydd	38
4. Bra rutiner & regler för IT & driftpersonal	19
5. Patchning	19
6. Sektionering av nätverket	10
7. Bra spetskompetens	10
8. Intrångs-IDS:er	10
9. *Övriga svar relaterade till människan*	*29*
10. *Övriga svar relaterade till tekniken*	*5*

Relaterat till människan (kompetens/rutiner/medvetenhet)

Teknikrelaterat

Bas: 22 respondenter
Öppen fråga
Summa svar: 48
Vet ej: 1
Inget svar: 0

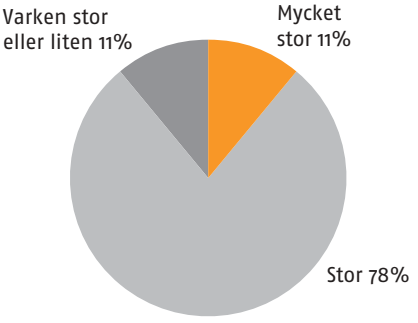
klara regler och rutiner för alla jobbar med IT och bra kompetens, både i djupet och i bredden.

Trots att det finns en del möjligheter till förbättring när det gäller medvetenhet, rutiner och kompetens, känner sig de allra flesta respondenter ganska trygga vad det gäller kapaciteten att stå emot skadlig kod. I det stora hela finns två huvudsakliga sätt att resonera. Antingen har den aktuella organisationen drabbats relativt hårt av intrång av skadlig kod de senaste åren och gjort en stor satsning för att få skyddet att hamna på en acceptabel nivå, eller så har organisationen klarat sig förhållandevis bra och ser detta som ett tecken att man har en bra kapacitet att stå emot dessa angrepp. Samtidigt förklarar många respondenter att de inte kan svara ”mycket stor kapacitet”, p.g.a. de brister i medvetenhet eller rutiner som ändå finns kvar. Fyra respondenter väljer att inte svara på frågan.

Den oroande utveckling kring skadlig kod som respondenterna förutspår leder till att en klar majoritet av dem (70 %) förväntar sig att det kommer att krävas en större satsning på IT-säkerhet om fem år jämfört med idag. Endast var tionde respondent tror att det räcker med en lika stor satsning som idag. De som inte känner sig säkra på vad som ska hända säger att mycket beror på den faktiska utvecklingen av skadlig kod och leverantörernas förmåga att leverera säkrare produkter, samt att interna förbättringar och förenklingar av IT-miljön kan väga upp ökade kostnader på annat håll.

Bild 27. Respondenternas bedömning av organisationens kapacitet att stå emot skadlig kod

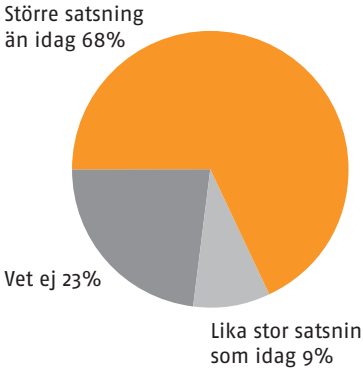
I vilken utsträckning skulle du säga att ni har kapacitet att stå emot skadlig kod?



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 4

Bild 28. Utecklingen av skadlig kod: konsekvenser för framtida satsningar på IT-säkerhet

Kommer det att krävas en större satsning på IT-säkerhet om 5 år jämförrt med idag eller räcker det med en lika stor eller t.o.m. mindre insats?



Bas: 22 respondenter
Sluten fråga
Vet ej: 5
Inget svar: 0

7. Utvecklingen av skadlig kod och konsekvenserna för organisationen

Det råder stor enighet bland representanter för statliga organisationer och privatföretag om att skadlig kod är ett växande problem och att det kommer att krävas en större satsning på IT-säkerhet om fem år för att även fortsättningsvis kunna stå emot den. Av de personer som svarat på frågan om utvecklingen av skadlig kod anser åtta av tio respondenter inom det privata näringslivet och nio av tio inom den offentliga sektorn att problemen kommer att bli större, mest på grund av att nya eller mer aggressiva former av skadlig kod som sprider sig snabbare tros vara på väg.

I bilden nedan har de största enskilda faktorer som skyddar mot skadlig kod rangordnats på nytt utefter hur många procent av respondenterna som har nämnt dem sammanlagt i båda undersökningarna. Den mest påfallande skillnaden mellan de båda målgrupperna är att det inom näringslivet finns ett större fokus på vikten av lojala medarbetare. Resonemanget är att ett bra skydd mot skadlig kod som kommer utifrån inte räcker för att uppnå total säkerhet. Även om det bland de av Opticom intervjuade företagen bara handlar om mindre incidenter finns det en rädsla för just denna typ av sabotage, eftersom det är mycket svårt att värja sig mot det. I statliga organisationer är det än så länge mer omedvetna handlingar av vanliga anställda som ställer till problem, en faktor som hamnar mer i bakgrunden hos näringslivsrepresentanterna.

Jämförelsebild 6. De främsta enskilda faktorer som skulle kunna skydda organisationer mot intrång av skadlig kod

Vilka tror du är de största enskilda faktorer som skulle kunna skydda myndigheter/ organisationer mot intrång av skadlig kod?

Andel av respondenter i %

De största ensklida faktorer som skyddar mot skadlig kod:	Statliga org.	Privata företag
1. Välskött brandvägg	43	30
2. Bra och frekvent uppdaterat virusskydd	38	30
3. Bra medvetenhet hos användarna	43	10
4. Bra rutiner & regler för IT & driftpersonal	19	20
5. Lojala medarbetare	–	30
6. Bra spetskompetens	10	10
7. Övervakningsverktyg & kunskap om dessa	10	10
8. Patchning	19	–
9. Sektionering av nätverket	10	–
10. Bättre kunskap om infrastruktur/nätverk	–	10
11. *Övriga svar relaterade till människan*	*29*	*10*
12. *Övriga svar relaterade till tekniken*	*5*	*20*

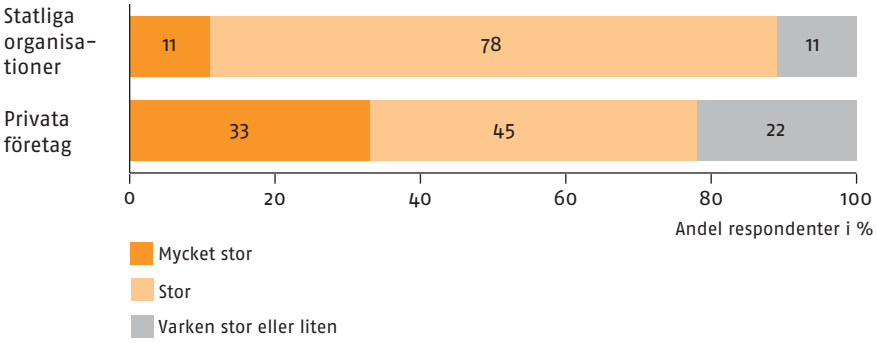
Relaterat till människan (kompetens/rutiner/medvetenhet)

Teknikrelaterat

Bas: 22 respondenter
Öppen fråga
Summa svar: 48
Vet ej: 1
Inget svar: 0

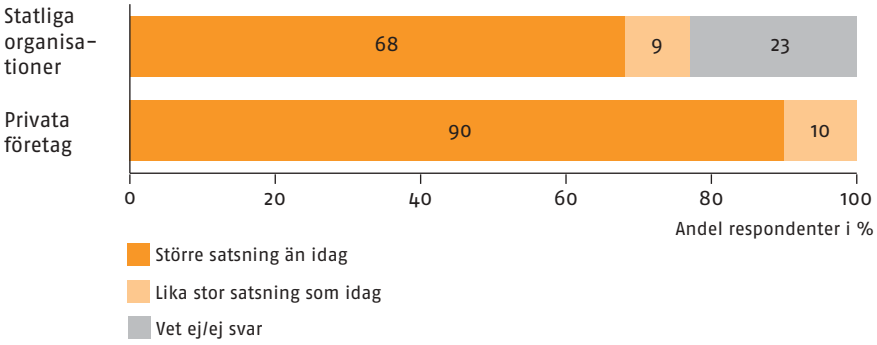
Om man jämför de olika organisationernas kapacitet att stå emot intrång av skadlig kod är "stor" det vanligaste svaret i båda grupperna. Bland de privata företagen anser var tredje respondent att det handlar om mycket stor kapacitet (en av tio bland respondenterna i gruppen myndigheter och statliga bolag), medan var femte anser att kapaciteten varken är stor eller liten (återigen mot en av tio i de statliga organisationerna). Det bör dock noteras att svaret på denna fråga inte bara baseras på den faktiska säkerhetsnivå som har uppnåtts i de olika organisationerna utan för vissa respondenter även på en bedömning av hur sannolikt det är att en ny variant av skadlig kod kan dyka upp som inte kan fångas in med det nuvarande systemet.

Jämförelsebild 7. Kapacitet att stå emot skadlig kod i statliga organisationer och privata företag



Sju av tio respondenter i statliga organisationer och nio av tio respondenter inom näringslivet tror att det kommer att krävas en större satsning på IT-säkerhet än idag. I båda grupperna tycker var tionde person att det räcker med en lika stor satsning som idag.

Jämförelsebild 8. Behovet av framtida satsningar på skadlig kod jämfört med dagens satsningar



Hypotetiska intrång av skadlig kod

Som kommer att framgå senare i det här kapitlet har en stor majoritet av myndigheterna och bolagen i den här studien på något sätt drabbats av intrång av skadlig kod. Eftersom det handlar om ett antal olika typer av intrång är det svårt att jämföra organisationerna när det gäller hur de skulle agera om de skulle bli konfronterade med exakt samma typ av intrång. För att ändå få en uppfattning om hur cheferna för IT respektive IT-säkerhet tänker i dessa situationer har de ombetts att ange hur de skulle reagera om ”Loveletter” och ”Blaster” hade varit helt okända och skulle drabba dem idag. För båda typer av skadlig kod besvarades följande tre frågor:

1. Var skulle problemet dyka upp/komma till ytan först? (**Upptäckt**)
2. Hur skulle ni karlägga/analysera problemet? (**Bedömning**)
3. vilka åtgärder skulle ni vidta för att begränsa skadan/skydda systemet? (**Åtgärd**)

Även om så gott som samtliga respondenter har ingående kunskaper om Loveletter och Blaster väljer många att prata om intrång i mer generella termer, så att vissa *specifika skillnader i hanteringen av dessa två typer av skadlig kod* inte kommer fram lika klart i alla svar. En gemensam nämnare för många IT-chefer eller IT-säkerhetschefer är att de har många funderingar kring belastning på nätverket, vilket är ett vanligt bekymmer ju större nätverket är. Problem med nätverksbelastning nämns framför allt i samband med Loveletter-liknande intrång.

Blaster drabbar i första hand klienten (arbetsstationen), och påverkar därigenom personalens arbete. I de fall där organisationen har drabbats av Blaster verkar servrarna ofta ha klarat sig, vilket gör att de mer ”livsviktiga” funktionerna som t.ex. extern kommunikation har kunnat fortsätta ganska ostört.

Det som de flesta respondenter i första hand strävar efter är att åtgärda de problem som kan uppstå med båda typer av skadlig kod så snabbt som möjligt medan systemet kan hållas i drift. Om detta inte går är nästa steg att man stänger av delar systemet. De flesta organisationer har system som på något sätt är sektionerade, vilket gör det förhållandevis lätt att stänga av olika delar av det. Många verkar också ha en färdig incidentrutin som strukturerar upp krishanteringsarbetet oberoende av vilken typ av incident det gäller. Detta beror troligtvis på att man på ett tidigt stadium inte riktigt vet vad det är för fel och omfattningen av det.

En närmare granskning av existerande rutiner kring virushanteringen visar att många respondenter förlitar sig på externa leverantörer och inte verkar ha någon riktigt djup egen kompetens inom detta område. En fråga som man kan ställa sig är om det finns risk för överbelastning hos de få leverantörer som finns (website, telefonväxlar) om ett massivt virus angriper och hela Sverige drabbas.

Verkliga intrång av skadlig kod

En stor majoritet av respondenterna uppger att den myndighet eller det bolag som de representerar har drabbats av skadlig kod. Bara i ett fall, en central myndighet, hävdar båda respondenter att det inte har funnits några intrång av skadlig kod utifrån, men även där har man kunnat konstatera olika försök. I två andra organisationer, en kommun och annan central myndighet, har respondenterna olika åsikter om huruvida det har uppstått en situation som kan beskrivas som intrång av skadlig kod. Orsaken till att respondenter ibland bedömer samma typ av händelser på olika sätt är att vissa först vill tala om intrång om det leder till påtagliga skador i systemet medan andra lägger ribban lägre.

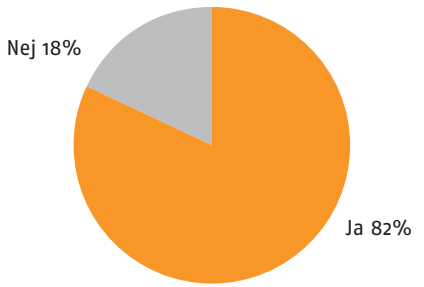
De typer av skadlig kod som har ställt till problem inom de intervjuade organisationerna under de senaste fyra åren är främst Loveletter (6), Nimda (3), Sasser (3), Blaster (3), Code Red (2) och Korgo T (1). Utöver dessa kan det ha funnits ett antal andra exempel på skadlig kod bland de incidenter som respondenterna inte har velat eller kunnat specificera (7), alla under 2003 och 2004.

Det är slående att se att så få organisationer har sluppit undan intrång av skadlig kod och att till och med de som säger att de inte haft problem ändå råkat ut för små incidenter. Alla nämnda virusangrepp verkar ha skett på 2000-talet. Detta kan bero på att tidigare angrepp glömts bort, men förmodligen är det en konsekvens av att virusmängden har ökat så mycket under innevarande decennium och att vissa av dessa har haft extremt stor penetration. Samtliga nämnda typer av skadlig kod drabbar i första hand Windows-klienter, och samtliga myndigheter och statliga bolag har Microsoft Windows som operativsystem, antingen bara för ekonomiska stödfunktioner eller för hela verksamheten.

Det framgår tydligt av respondenternas beskrivningar av de incidenter som de har drabbats av att långt ifrån alla virus som kommit in i systemet kommer via själva nätet och Internet-uppkopplingen. Det är inte ovanligt att anställda har CD, disketter eller bärbara datorer med sig. De största sårbarheterna

Bild 29. Verkliga intrång av skadlig kod

Har ni någon gång blivit drabbad av skadlig kod?



Bas: 22 respondenter
Sluten fråga
Vet ej: 0
Inget svar: 0

i systemen verkar därmed vara de externa komponenterna i systemet. Detta gäller givetvis inte de specifika mailvirus som framför allt kommer in via nätverket/Internet. Utöver de problem som nämnts med klassiska exempel på skadlig kod verkar även SPAM vara ett ökande problem. För att hantera SPAM på ett bra sätt i framtiden behövs externa leverantörer som filtrerar dessa mail på ett intelligent sätt.

Ett gemensamt problem med virus är att Internet och de interna näten får tung belastning och slutar fungera. Detta gör att både intern och extern kommunikation bryts, även om det ofta inte finns ett virus i den egna organisationen. Hur stora skadorna var efter de olika angreppen skiljer sig mycket beroende på kärnverksamhetens inriktning, tidpunkt för intrånget, spridningshastighet och givetvis incidenthanteringsrutiner. Alla incidenter innebär åtminstone en omprioritering av IT-personalens uppgifter och ett visst produktionsbortfall av dem som inte kan jobba som vanligt. I mer allvarliga fall kan det röra sig om mycket övertid för IT-personalen och ett massivt produktionsbortfall, vilket innebär stora problem.

Om man i efterhand tittar på alla de incidenter som ägt rum de senaste åren kan man konstatera att de flesta exempel på lyckade intrång av skadlig kod verkar ha haft en mellan- till hög grad av allvar, men tack vare snabba åtgärder har de flesta klarat sig relativt bra. Att systemet står still i tre- fyra timmar (vilket verkar vara en vanlig tidslängd) är visserligen allvarligt men inte katastrofalt. Många organisationer klarar upp till ett dygn, i alla fall så länge det inte är de livsviktiga systemen som går ner. Detta har i de flesta fall inte hänt och både servrar och stordatorsystem har klarat sig.

En erfarenhet som många IT-chefer och IT-säkerhetschefer delar är att de efter allvarliga incidenter har fått gehör hos ledningen för vissa säkerhetsbefrämjande åtgärder som tidigare inte har godkänts, mestadels beroende på att det skulle innebära för stora begränsningar in funktionalitet. På så sätt kan man säga att många incidenter har fungerat som en väckarklocka. Under själva krishanteringen följdes i många fall de rutiner som fanns eller så gjordes det marginella förändringar under resans gång. Många som drabbats har i efterhand förstärkt sina rutiner för incidenthantering och investerat i utrustning för att öka säkerheten i framtiden. Bilden på nästa sida visar de viktigaste förändringarna.

En av de vanligaste åtgärderna som vidtas efter incidenter med skadlig kod är att se över rutiner kring virusskydd, exempelvis genom en frekventare uppdatering av virusdefinitioner. Paradoxalt nog ställer denna rutin i sig stora krav på nätverket och det blir mycket trafik när det kommer nya definitioner som ska laddas ner. Om den tidigare frekvensen var en uppdatering per dag eller en uppdatering per tolv eller sex timmar innebär det en stor omställning

Bild 30. Långsiktiga förändringar i IT-systemen/rutiner/ansvarsfördelningen med anledning av incidenter med intrång av skadlig kod

Har ni gjort någon långsiktig förändring i systemet/rutinerna/ansvarsfördelningen?

Förändringar i rutiner (16)	Antal svar
1. Bättre rutiner/ökad medvetenhet generellt	4
2. Förbättrad kommunikations-/informationsplan	4
3. Förbättrade krishanteringsrutiner	2
4. Nya checklistor	2
5. Strängare regler om vilka filer som får komma in via mailfunktionen	1
6. Åtskillnad användarindentiteter/titta över behörigheter	1
7. Nya ansvarsfördelning driftorganisation-IT-avd.	1
8. Bättre omvärldsbevakning	1

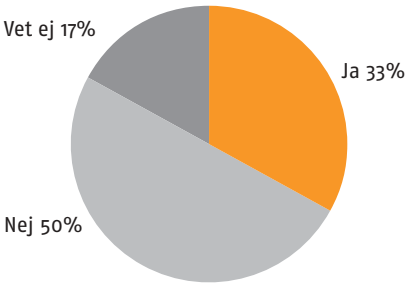
Förändringar på tekniksidan (16)	Antal svar
1. Bättre rutiner kring virusbevakning/mer frekvent uppdatering	5
2. Bättre patch-hantering	5
3. Generell översyn av säkerhetsorganisationen/täppa till sårbarheter	2
4. Bättre brandväggslösningar	1
5. Bättre virusskydd	1
6. Höjning av säkerhetsnivån i dotterbolag till den standard som gäller för moderbolaget	1
7. Uppdatering av bärbara datorer (brandvägg och virusskydd)	1

Förändringar i organisationen	Antal svar
1. Förändringar i ledningsorganisationen	1
2. IT-ansvarig inom CEO-funktion	1
3. Översyn av säkerhetsorganisationen	1

Bas: 22 respondenter
Öppen fråga
Summa svar: 35
Vet ej: 2
Inget svar: 2

Bild 31. Behov av extern hjälp för att hantera incidenter som inträffat

Till dem som har blivit drabbade: Har ni fått eller köpt hjälp för att hantera incidenter som inträffat?



Bas: 18 respondenter
Sluten fråga
Vet ej: 3
Inte relevant eller inget svar: 1

att börja uppdatera varannan eller t.o.m. varje timme, vilket det finns exempel på i denna studie. I sådana fall går det inte längre att välja tidpunkter då det inte finns mycket annan trafik på nätet. Paradoxen består därför i att man måste acceptera en tillfällig hård belastning av nätet för att slippa en ännu hårdare och okontrollerad belastning som följt av intrång av skadlig kod.

En tredjedel av respondenterna anger att de har fått eller köpt extern hjälp (utöver de tjänster och produkter som de normalt köper) för att hantera incidenter som inträffat. Det handlar t.ex. om FRA, leverantörer av virusdefinitioner eller IT-konsultföretag med ett mer allmänt verksamhetsområde.

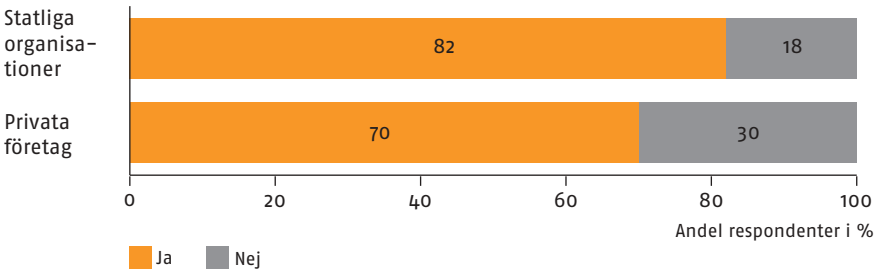
JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

8. Exempel på intrång av skadlig kod

Som bilden nedan visar uppger en klar majoritet av respondenterna i både statliga organisationer och privata företag att det har funnits exempel på intrång av skadlig kod under de senaste åren. Däremot är uppgifterna om de intrång som har ägt rum inom näringslivet är inte lika specifika som de uppgifter som kommit fram under intervjuerna med myndigheter och statliga bolag. Exempel på skadlig kod som har nämnts i näringslivsintervjuerna Loveletter, Blaster och Sasser.

Enbart i ett fall har ett företag fått eller köpt hjälp för att hantera incidenter som inträffat. En av anledningarna kan vara att incidenterna i nästan samtliga fall bedömdes vara lindriga.

Jämförelsebild 9. Andel respondenter som säger att deras organisation har drabbats av intrång av skadlig kod



Kaskadeffekter

Även om vissa organisationer har råkat ut för förhållandevis allvarliga intrång av skadlig kod har kärnverksamheten inte påverkats så mycket att det har lett till påtagliga externa kaskadeffekter[2]. I några fall var det däremot mycket nära och ren tur (tack vare tidpunkten då intrånget ägde rum) att det inte blev någon påverkan på samhällsviktig infrastruktur. Frågan är dock vad som händer om en central del eller hela systemet verkligen skulle vara nere hos dessa myndigheter och statliga bolag och på så sätt påverka kärnverksamheten. Många av organisationerna har en sådan central roll i samhället att ett avbrott skulle kunna ha ödesdigra konsekvenser.

2. Kaskadeffekter: När ett avbrott i en infrastruktur förorsakar avbrott i en eller flera andra infrastrukturer (internt eller externt).

Externa kaskadeffekter

Exakt vad kaskadeffekterna skulle bestå i beror väldigt mycket på kärnverksamhetens inriktning och kan egentligen bara analyseras på aggregerad nivå, men det är intressant att se var i tiden respondenterna bedömer att situationen kan betecknas som allvarligt med tanke på deras uppdrag. I vissa fall (lufttrafik och radiokommunikation) skulle kaskadeffekterna vara omedelbara, medan det kan dröja upp till en vecka innan effekterna blir påtagliga för dem som är beroende av organisationer som jobbar med handläggning av ärenden och tar hand om stora finansiella transaktioner.

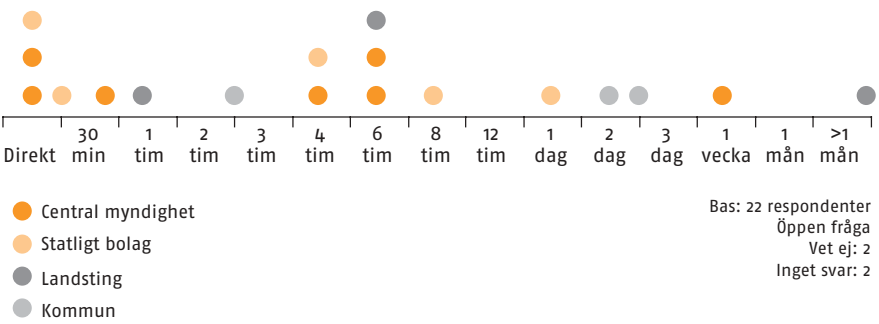
En IT-säkerhetsansvarig uttrycker det så här:

”[Vid ett kortare avbrott] *måste man internt prioritera ärenden, vissa ärenden kan man ta en månad senare. Visst blir folk sura men det är inget avgörande. Har det däremot stått helt still i en vecka så tar det månader innan man är ifatt igen eftersom det läggs på hög. Man skulle behöva kräva övertidsarbete under en ganska lång tid.”* (IT, central myndighet)

En gemensam nämnare för myndigheter när det gäller externa kaskadeffekter är att de får svårare att leva upp till offentlighetsprincipen, eftersom det i nästan alltid blir svårare att nå dem. Det verkar för övrigt finnas ett svagt samband mellan typ av myndighet (central eller lokal) och respondenternas bedömning av hur lång tid avbrottet kan vara innan samhällsviktig infrastruktur påverkas. Den kritiska tidsgränsen ligger generellt lite längre fram i tiden för lokala myndigheter (se bild 32 nedan). Svaren är dock inte homogena och ibland gör personer som representerar samma typ av organisation

Bild 32. Tidpunkt där avbrottets längd kan betecknas som allvarligt med tanke på effekterna

Var på denna tidsskala bedömer du att situationen kan betecknas som allvarlig med tanke på ert uppdrag?



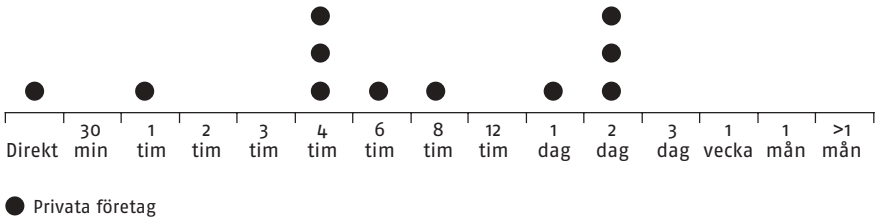
Bas: 22 respondenter
Öppen fråga
Vet ej: 2
Inget svar: 2

JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

9. Kritiska tidsgränser vid större avbrott

Inom det privata näringslivet verkar tidsmarginalerna vara något större än hos myndigheter och statliga bolag om hela eller delar av systemet skulle vara nere, men även här finns exempel på organisationer som anser att situationen kan betecknas som allvarlig redan inom en timme (t.ex. banker). För de övriga är det vanligast att ha beredskap för att klara avbrott antingen under en halv dag eller under två dagar, beroende på verksamheten. Pappers- och pappersmassaföretag tillhör de organisationer som har förhållandevis små marginaler (högst fyra timmar) medan industriföretag generellt klarar sig i upp till två dagar.

Jämförelsebild 10. Tidpunkt där avbrottets längd kan betecknas som allvarligt för privata företag



(t.ex. landsting) vitt skilda bedömningar av när smärtgränsen är nådd och på vilka sätt problemen yttrar sig.

Frågan om när avbrottet kan betecknas som allvarligt uppfattas som svår av många respondenter eftersom det beror på så många variabler (tidpunkt, omfattning), men de flesta kommer ändå fram till en tidsgräns där de tror att ett större avbrott har externa kaskadeffekter på ett eller annat sätt. Ett fåtal respondenter anser dock att man inte kan göra en realistisk uppskattning och väljer att avstå från att besvara frågan.

Interna kaskadeffekter:

Interna kaskadeffekter följer ett mer enhetligt mönster. Många angrepp har bara varit kännbara internt och då händer nästan alltid följande:

1. IT-personalen måste prioritera bort sina vanliga uppgifter och ägna all tid åt att ta bort den skadliga koden och fixa de maskiner eller delar av systemet som blivit påverkade. Är avbrottet av mer allvarlig karaktär så innebär detta inte bara att de vanliga uppgifterna får vänta utan

också att personer måste jobba övertid och står under en extrem press. Incidenthanteringsrutiner (om de finns) ersätter de vanliga rutinerna för IT- och IT-säkerhetspersonalen och (delar av) ledningsgruppen.

2. Beroende på typ av intrång försvinner nästan alltid en del funktionalitet för en stor grupp vanliga anställda. Om bara e-postkommunikationen faller bort finns de vanligtvis alternativa sätt att jobba men om delar av systemet eller hela systemet måste stängas av innebär detta per automatik produktionsbortfall för alla som drabbas.
3. Om avbrottet leder till externa kaskadeffekter innebär det även att det interna trycket ökar eftersom folk kommer att ringa in utifrån och höra av sig på olika sätt. Det kan vara kunder, leverantörer, samarbetspartners och andra intressenter. I så fall kan det även bli tal om mediebevakning. I vissa fall betyder interna avbrott automatiskt externa kaskadeffekter om de skulle vara längre än några minuter, t.ex. om landstingets patientadministrationssystems skulle vara nere. Det skulle direkt innebära problem på mottagningar och kunna leda till förseningar för patienter ett antal veckor framöver.
4. Många organisationer måste antingen hitta nya arbetssätt eller skicka hem personalen, framför allt om det rör sig om administrativ verksamhet som lätt kan utföras manuellt. Det måste finnas en prioritetsordning av de uppgifter som fortfarande kan utföras och en plan för hur man kan komma ikapp efter avbrottet. De myndigheter och statliga bolag som har en kärnverksamhet som i sig är baserad på IT- och kommunikationslösningar har mycket redundans i systemet, speciellt om de är del av totalförsvaret.

Speciellt för statliga bolag:

5. Eftersom de statliga bolagen helt eller delvis bedriver kommersiell verksamhet, kan de förmodligen inte ta in order och ta in nya affärer under den tid som avbrottet varar.

De ekonomiska effekterna av stora avbrott är svåra att uppskatta, framför allt vad gäller externa kaskadeffekter. Internt finns det däremot ofta tidigare exempel på vad mindre intrång av skadlig kod hade för konsekvenser och det finns ingen som tvekar om att ett stort avbrott skulle kunna ha enorma ekonomiska konsekvenser.

JÄMFÖRELSE MELLAN STATLIGA ORGANISATIONER OCH PRIVATA FÖRETAG

10. Kaskadeffekter och interna konsekvenser av intrång av skadlig kod

De intrång av skadlig kod som de tio privatföretagen i Opticoms urval har drabbats av under de senaste åren har haft förhållandevis små kaskadeffekter internt och obefintliga kaskadeffekter externt enligt respondenterna. Samtliga respondenter som representerar drabbade företag talar om att det visserligen har inneburit en viss mån av merarbete för IT-personalen men att produktionsbortfallet i organisationerna har varit ytterst begränsat.

En klar skillnad mellan statliga organisationer och privatföretagen är att incidenter med skadlig kod inte i lika stor utsträckning har satt igång ett förändringsarbete i den sistnämnda gruppen. Ett antal respondenter uppger att de förändringar i systemet, rutinerna eller ansvarsfördelningen som har gjorts redan var planerade, vilket ger intrycket av en mer pro-aktiv attityd inom näringslivet.

De företag som *har* vidtagit extra åtgärder efter incidenter med skadlig kod har precis som myndigheter och statliga bolag lagt mest krut på att se över rutiner kring virusskydd och i vissa fall även de system som används. Bättre patch-hantering, förbättrade krishanteringsrutiner och generella organisationsförändringar är andra faktorer som nämnts.

Övriga frågor

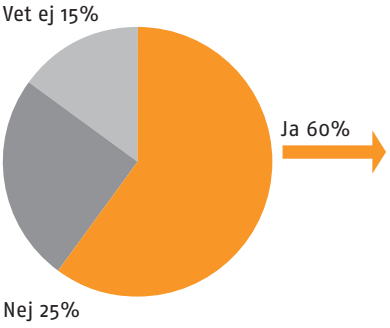
Att jobba med externa nyckelkonsulter är ofta ett kostnadseffektivt sätt att knyta till sig viktig spetskompetens, men det kan också innebära en fara i och med att dessa personer ofta jobbar för flera uppdragsgivare samtidigt och inte kan fokusera på en kund i krissituationer. Av de tjugo personer som kan uttala sig om detta uppger drygt hälften att de ibland eller ofta anlitar externa nyckelresurser som samtidigt jobbar för flera uppdragsgivare. Bara två av dem är helt säkra på att dessa externa nyckelpersoner skulle prioritera just dem (se bild 33 på nästa sida), ytterligare två är ganska säkra och fyra känner sig mer osäkra. För några av dessa är frågan en väckarklocka. Av de övriga fyra kan två inte svara på frågan och två väljer att inte besvara den.

En liknande fråga kan ställas när det gäller storleken på den interna krisberedskapsgruppen, som ska leda IT-arbetet i krissituationer. Trots vissa frågetecken kring kompetensbredd och kompetensdjup tror tre av fyra respondenter att den grupp som skulle formeras är tillräckligt stor, även om en nyckelperson i gruppen skulle falla bort. (se bild 34 på nästa sida).

En fråga som bara ställdes till myndigheter var hur mycket skadlig kod påverkar 24-timmarmyndighetssatsningen. Av sjutton svarande respondenter anser fem att det inte finns några begränsningar, medan sju personer tycker att tanken visserligen är bra men

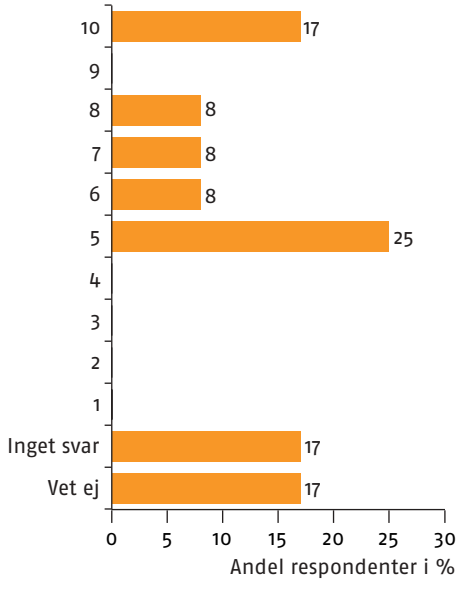
Bild 33. Externa nyckelkonsulter i organisationen och säkerheten att dessa personer skulle prioritera respondentens organisation i krissituationer

Har ni externa IT-konsulter som är nyckelresurser hos er och samtidigt jobbar för flera uppdragsgivare?



Bas: 22 respondenter
Sluten fråga
Vet ej: 3
Inget svar: 2

På en skala från 1–10, hur säkra är ni på att dessa personer skulle prioritera er om ett angrepp med skadlig kod skulle drabba många myndigheter samtidigt?



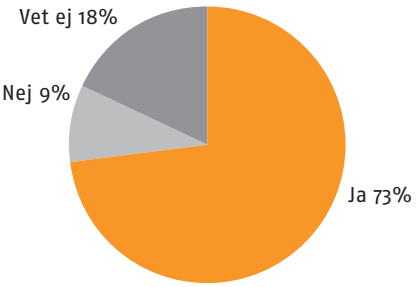
Bas: 12 respondenter
Sluten fråga
Vet ej: 2
Inget svar: 2

att det innebär en extra påfrestning för organisationen i och med att mer övervakning krävs och rutiner måste läggas om. En IT-chef går så långt att han tycker att 24-timmarmyndighetssatsningen bör begränsas i och med att riskerna är för stora

Undersökningens sista fråga om vilken hjälp från samhället de olika myndigheterna och bolagen skulle vara betjänta av i deras strävan att optimera IT-miljon (både när det gäller funktionalitet och IT-säkerhet) resulterar i ett antal önskemål som delvis återspeglar en mer generell känsla som finns inom myndighets-Sverige. Det som många framför allt efterlyser är en mer centraliserad styrning från staten på området IT- ochinformationssäkerhet (se bild 35). Detta inkluderar bland annat att staten kommer med klarare regler och direktiv samt agerar i större utsträckning än

Bild 34. Storlek på den grupp av personer som ska leda IT-arbetet i krissituationer

Anser du att den grupp av personer som ska leda IT-arbetet i krissituationer (t.ex. om en stor del av systemet skulle vara nere p.g.a. skadlig kod) är tillräcklig stor?



Bas: 22 respondenter
Sluten fråga
Vet ej: 4
Inget svar: 0

idag som kravställare mot olika typer av leverantörer (som t.ex. Internet- och IP-telefonileverantörer).

En typ av kommentar som hänger starkt ihop med denna åsikt är att alla myndigheter som har tilldelats en roll vad gäller säkerhet generellt och i synnerhet IT- och informationssäkerhet ska (KBM, FRA, FMV, PTS och Statskontoret m.m.) ska ha en klarare rollfördelning och jobba mer utifrån ett övergripande perspektiv, helst med färre kontaktytor. Att KBM spelar en viktig roll är för övrigt inte något som ifrågasätts. En del respondenter säger spontant att de skulle vilja se att KBM fortsätter satsa på det sätt de gör idag, d.v.s. att samordna arbetet kring samhällets beredskap inför allvarliga kriser, i det här fallet med fokus på IT-säkerhet.

Bild 35. Storlek på den grupp av personer som ska leda IT-arbetet i krissituationer

Hur mycket påverkar skadlig kod 24-timmarsmyndighetssatsningen?

Antal svar

Påverkan av skadlig kod på myndigheternas 24-timmarssatsning:	Samtliga respondenter
1. Nej, ingen påverkan	5
2. Ja, kräver mer övervakning/högre skyddsnivå	3
3. Ja, större risker	3
4. Ja, dyrare eftersom rutiner måste läggas om	1
5. Stort problem – begränsar satsningen	1
6. Annat	1

Bas: 17 respondenter
Öppen fråga
Vet ej: 2
Inget svar: 0

Bland de övriga svaren finns önskemål om åtgärder inom utbildningsväsendet och mer aktiv forskning för att på sikt kunna garantera en bas av kompetent personal. Att se över vissa lagar (t.ex. om tillämpningen av offentlighetsprincipen) är också en viktig punkt för vissa. Under intervjuernas gång har spänningen mellan förvaltningsmodellen och IT-säkerheten kommit på tal ett antal gånger, ofta som en parantes till andra frågor, och det är viktigt att titta närmare på den punkten.

Bild 36. Hjälp från samhället som skulle underlätta en mer optimal IT- och Informationssäkerhet hos myndigheter och statliga bolag

Vilken hjälp av samhället (t.ex. ändrade regler, resurser, ökad kompetens) behöver ni för att åstadkomma en optimal IT-miljö?

Andel respondenter i %

Önskemål:	Samtliga resp.
1. Mer central styrning i frågan om IT-säkerhet på nationell nivå (t.ex. behov av en gemensam kravställare mot Internet eller IP-telefonileverantörer / tydligare regler & direktiv / tydligare roller)	55
2. Mer samarbete mellan myndigheter i Sverige (mer erfarenhetsutbyte på området IT/informationssäkerhet/mer standardiserat sätt att tänka)	23
3. Fortsatta satsningar på de saker som KBM arbetar med (IT-säkerhetsarbete/robusta system/enklare manualer)	18
4. Mer samverkan mellan nämnder och myndigheter med ansvar för IT-säkerhet i Sverige (t.ex. KBM, FRA, FMV, PTS och Statskontoret); bättre övergripande perspektiv	14
5. Aktiv forskning på högskolor/rekryteringsbas av kompetent personal, specialister, rådgivare	14
6. Lagändringar (brister i regler kring offentlighetsprincipen och reglerna om inkommen handling gör att man behöver exponera sig i onödan)	9

Hjälp från Staten

Egna initiativ

Bas: 22 respondenter
Öppen fråga
Vet ej: 1
Inget svar: 0

Appendix: frågeformulär besöksintervjuer

KRISBEREDSKAPSMYNDIGHETEN: STUDIE SKADLIG KOD

Bakgrundsinformation:

Myndighet / statligt bolag:
……
Adress:
……
Telefon nummer:
……
Namn på respondent:
……
Titel:
……
E-post adress:
……

Målgrupp: 1 ☐ Centrala myndigheter 2 ☐ Länsstyrelse 3 ☐ Lokala myndigheter

Ansvarsområde respondent: 1 ☐ Ledande administrativ befattning 2 ☐ Operationellt IT-ansvar
Funktion: ……
Geografiskt område: 1 ☐ Stockholm 2 ☐ Utanför Stockholm
Operativsystem: 1 ☐ Microsoft 2 ☐ Linux 3 ☐ Unix 4 ☐ Solaris ☐ Annat: ……
☐ Annat: ……
Det totala antalet anställda: ……
Kan bli citerad: 1 ☐ Ja 0 ☐ Nej
Kvalitetssäkring: 1 ☐ Ja 0 ☐ Nej Datum: …… Signatur: ……

I. Generell verksamhetsbeskrivning

Opticom gör en liten förstudie av varje myndighet/statligt bolag och sammanfattar deras uppdrag enligt det som står på myndighetens/bolagets hemsida. Intervjun börjar med en kort genomgång.

1. Tycker du att denna sammanfattning beskriver ert uppdrag/er verksamhet på ett tillfredsställande sätt?
   1 ☐ Ja 2 ☐ Nej

Om nej:

2. Vilka tillägg skulle du vilja göra?

II. Organisationens IT-rutiner

3. På en skala från 1-10, hur viktigt är ett väl fungerande IT-system för organisationens verksamhet idag och hur viktigt kommer IT-systemet att vara om 5 år?

   Idag: _____ Om 5 år: _____ (1 är helt oviktigt och 10 mycket viktigt)

Om det finns en skillnad mellan dessa siffror (3):

4. Varför blir ett välfungerade IT-system viktigare/mindre viktigt?

---

5. På en skala från 1-10, hur väl anser du att ert nuvarande IT-system fungerar?

   _____ (1 är inte bra alls och 10 är mycket bra)

---

6. Vilka anser du är de största styrkorna och svagheterna i ert IT-system som det ser ut idag?

Styrkor:	Svagheter:

7. Finns det instanser utanför er organisation som ställer formella krav på IT-systemets funktionalitet?
   1 □ Ja 2 □ Nej

Om ja (7):

8. Vilken/vilka?

---

9. Finns det instanser utanför er organisation som är beroende av IT-systemets *funktionalitet*?
   1 □ Ja 2 □ Nej

Om ja (9):

10. Vilken/vilka?

---

11. Finns det instanser utanför er organisation som ställer formella krav på IT-systemets *säkerhetsnivå* ?
   1 □ Ja 2 □ Nej

Om ja (11):

12. Vilken/vilka?

---

13. Vilka personer inom organisationen* jobbar med/bär ansvar för följande saker?
(1 = viktigast, 2 = näst viktigast m.m.)

	Titlar: (* = detta kan även inkludera externa konsulter)		
Ansvarsområde:	**1**	**2**	**3**
Vilka personer har ansvar för IT-systemets funktionalitet?			
Vilka personer har ansvar för IT-systemets säkerhet/ informationssäkerhet?			
Vilka personer är involverade när det gäller IT-relaterade investeringar/ budgetfrågor?			

14. Hur kommunicerar ni IT-frågor generellt? Finns det några fasta rutiner?

---

15. Outsourcar ni delar av er IT-verksamhet till instanser utanför organisationen?
1 □ Ja 2 □ Nej

Om ja (15):
16. Vilka funktioner?

Om ja (15):
17. Vilken andel av den totala IT-verksamheten (i %) handlar det om?

_____

18. Vilka krav ställer ni på dem som sköter dessa funktioner när det gäller IT/informationssäkerhet?

---

19. På en skala från 1 till 10, i vilken mån känner ni er trygga att er IT-partner/era IT-partners kan uppnå åtminstone samma IT- och informationssäkerhetsnivå som ni själva om ni hade behållit de outsourcade tjänsterna?

_____ (1 = ingen trygghet alls; 10 = fullständig trygghet)

20. Ställer ni krav på att de ska ha en kontinuitetsplan?
1 □ Ja 2 □ Nej

---

21. Kring vilket/vilka operativsystem har ni byggt er IT-verksamhet?
1 □ Microsoft 2 □ Linux 3 □ Unix 4 □ Solaris □ Annat: _____
□ Annat: _____

22. Om man antar att funktionalitet (egenskaper), ekonomiska skäl och säkerhetsskäl ligger till grund för valet av operativsystem, hur tungt väger då dessa tre skäl i ert val?

1.

2.

3.

---

23. Vilka är de viktigaste för- och nackdelarna med detta/dessa system?

---

24. Hur ser ni på Internet-baserad telefoni (s.k. IP-telefoni)? Vilka är för och nackdelarna?

Fördelar:	**Nackdelar:**

25. Har ni IP-telefoni idag?
    1 □ Ja 2 □ Nej

Om nej (25):

26. Tror du att ni kommer att ha IP-telefoni om 5 år?
    1 □ Ja 2 □ Nej

Om inte svaret har kommit fram i fråga 24:

27. Anser du att IP-telefoni innebär/skulle innebära ökad sårbarhet för er verksamhet?
    1 □ Ja 2 □ Nej

28. Varför/varför inte?

---

29. Vilken är ansvarsfördelningen i organisationen när det gäller IT och telefoni?

Om organisationen har IP-telefoni idag:

30. Har ni en plan om all Internet-baserad kommunikation blir utslagen?
    1 □ Ja 2 □ Nej

Om ja (30):

31. Hur ser den ut?

III. IT-säkerhet generellt och i krissituationer

32. Vi kommer nu att gå igenom ett antal faktorer som kan vara viktiga för att garantera bra IT/informationssäkerhet inom myndigheter och organisationer. Jag skulle vilja be dig att ange hur viktig du tycker att varje faktor är för dig på en skala från 1-10 där 1 är "inte alls viktigt" och 10 "mycket viktigt". Sen skulle jag vilja att du anger vilken säkerhetsnivå du anser att ni har på en skala från 1-10, där 1 = "inte bra alls" och 10 = "mycket bra".

GAP-ANALYS IT/INFORMATIONSSÄKERHET	Viktighet	Säkerhetsnivå
Skydd/åtgärder mot intrång av skadlig kod		
1) Optimalt brandväggsskydd		
2) Kontinuerligt uppdaterade anti-virus program		
3) Kontinuerlig uppdatering av övriga system/tilltäppande av sårbarheter		
4) VLAN		
5) Optimal konfigurering av säkerhet i nätverket (generellt)		
Back-up		
6) Back-up system		
7) Övrig redundans/reservkapacitet i systemet som kan användas vid behov		
Fysiska skydd mot strömbortfall		
8) Säker strömförsörjningsmiljö: UPS (Unbreakable Power System), kylning, vatten m.m.		
Kompetens/medvetenhet om IT- och informationssäkerhet		
9) Specialistkompetens när det gäller IT- och informationssäkerhet		
10) Kompetensbredd: att ett tillräckligt antal personer är insatta i säkerhetsfrågor		
11) Att de som är insatta i IT-frågor följer alla rutiner och processer		
12) Generell medvetenhet av de anställda på området IT- och informationssäkerhet		
Övergripande bedömning IT/informationssäkerhet		
13) IT/INFORMATIONSSÄKERHET GENERELLT		

Kommentarer om siffran för viktighet > siffran säkerhetsnivå:

33. Har ni en specifik säkerhetsavdelning?
    1 □ Ja 2 □ Nej

34. Har ni en IT-säkerhetsansvarig?
    1 □ Ja 2 □ Nej

35. Hur många personer arbetar med IT-säkerhet i er organisation?

    _____

36. Är fysisk- och informationssäkerhet integrerade?
    1 □ Ja 2 □ Nej

Om nej (36):

37. Varför inte?

---

38. Har ni dokument som reglerar IT-säkerhetsarbetet?
    1 □ Ja 2 □ Nej

Om ja (38)

39. Vilken typ av dokument?
    1 □ Policy 2 □ Föreskrifter 3 □ Riktlinjer □ Annan: _____

Om ja (38):

40. Hur uppdaterar ni dokumentet/dokumenten? Vilka rutiner finns det?

---

41. Hur stora ekonomiska resurser har ni avsatta för IT/informationssäkerhetsarbete? (i % av er totala budget för IT-verksamheten)

---

42. Hur sprids medvetenheten kring IT- och informationssäkerhet i organisationen?

---

43. På en skala från 1-10, hur nöjd är du med den generella medvetenheten kring IT/informationssäkerhet i organisationen som helhet?
    1 □ Ja 2 □ Nej

44. Skiljer det sig mellan olika avdelningar/personalkategorier?
    1 □ Ja 2 □ Nej

Om ja (44):

45. Varför skiljer det sig?

---

46. Har ni en kontinuerlig/rullande personalutbildning när det gäller IT- och informationssäkerhetsfrågor?
    1 □ Ja 2 □ Nej

47. Hur ser du på din egen kompetens på området IT- och informationssäkerhet om du använder en skala från 1-10 där 1 är mycket dålig och 10 är mycket bra?

    _____

48. På vilket/vilka områden skulle du önska dig bättre kunskap?

---

49. Om du tänker på alla andra personer som på något sätt är involverade i arbetet med IT/informationssäkerhet inom organisationen, hur bedömer du den genomsnittliga kompetens som dessa personer har på en skala från 1-10 där 1 är mycket dålig och 10 är mycket bra?

    _____

50. På vilka områden skulle du önska dig att organisationen får bättre kunskap?

BARA TILL IT-PERSONAL (fråga 51-54):

51. Hur kommunicerar ni med ledningsgruppen när det gäller IT- och informationssäkerhet i allmänhet?

---

52. Hur kommunicerar ni med ledningsgruppen när det gäller incidenter?

---

53. Sker detta kontinuerligt?
    1 □ Ja 2 □ Nej

54. Vilka tror du är de enskilt största faktorerna som skulle kunna skydda myndigheter/organisationer mot intrång av skadlig kod?

BARA TILL LEDANDE ADMINISTRATIV PERSONAL (fråga 55-57):

55. Hur kommunicerar ni med era IT-ansvariga när det gäller IT- och informationssäkerhet?

---

56. Sker detta kontinuerligt?
    1 □ Ja 2 □ Nej

57. Vilka tror du är de enskilt största faktorerna som skulle kunna skydda myndigheter/statliga bolag mot intrång av skadlig kod?

IV. Skadlig kod

58. Hur ser du på utvecklingen kring skadlig kod idag och i framtiden?

---

59. Kommer det att krävas en större satsning på IT-säkerhet om 5 år jämfört med idag eller räcker det med en lika stor eller t.o.m. mindre insats?

    1 □ Större satsning än idag 2 □ Lika stor satsning som idag 3 □ Mindre stor satsning än idag

---

60. I vilken utsträckning skulle du säga att ni har kapacitet att stå emot skadlig kod.
    1 □ Mycket stor
    2 □ Stor
    3 □ Varken stor eller lite
    4 □ Liten
    5 □ Mycket liten

BARA TILL IT-PERSONAL (fråga 61):

61. De senaste åren har vi sett ett flertal exempel på medvetna angrepp med skadlig kod. Kända exempel är bl.a. ”Loveletter” och ”Blaster”. Om dessa två fortfarande hade varit helt okända och skulle drabba er idag:
    1. Var skulle problemet dyka upp/komma till ytan först? (Upptäckt)
    2. Hur skulle ni kartlägga/analysera problemet? (Bedömning)
    3. Vilka åtgärder skulle ni vidtaga för att begränsa skadan/skydda systemet? (Åtgärd)

A] Upptäckt?

Loveletter: Ω **Blaster:**

B] Bedömning?

Loveletter: Ω **Blaster:**

C] Åtgärd?

Loveletter: Ω **Blaster:**

---

62. Har ni någon gång blivit drabbade av skadlig kod?
    1 □ Ja 2 □ Nej

Om ja (62)

63. När? Vid vilka tillfällen?

    År: _____ _____
    År: _____ _____
    År: _____ _____

Om ja (62)

64. Kan du beskriva angreppet/angreppen närmare?

_____

Om ja (62)

65. Hur har angreppet/angreppen drabbat er och vad gjorde ni åt det/dem?

Skada:	**Åtgärder:**

Om ja (62)

66. Har ni gjort någon förändring i systemet/rutinerna/ansvarsfördelningen, ad hoc och/eller långsiktigt?

Ad hoc:	**Långsiktigt:**

Om ja (62)

67. Har ni fått eller köpt hjälp för att hantera incidenter som inträffat?
    1 □ Ja 2 □ Nej

68. Om en del av systemet eller hela systemet skulle gå ner idag, vilka kaskadeffekter skulle detta ha 1. internt (inom er egen organisation) och 2. externt (andra aktörer) ifall avbrottet skulle vara

Tidsåtgång:	**Interna kaskadeffekter**	**Externa kaskadeffekter**
5 min.		
30 min.		
1 timme		
4 timmar		
1 dag		
2 dagar		
4 dagar		
1 vecka		
2 veckor		
4 veckor		

69. Var på denna tidsskala bedömer du att situationen kan betecknas som allvarligt med tanke på ert uppdrag?

_____

70. Vad skulle de ekonomiska konsekvenserna vara vid avbrott med den här längden?

Tidsåtgång:	**Ekonomiska konsekvenser**
5 min.	
30 min.	
1 timme	
4 timmar	
1 dag	
2 dagar	
4 dagar	
1 vecka	
2 veckor	
4 veckor	

71. Har ni externa IT-konsulter som är nyckelresurser hos er och samtidigt jobbar för flera uppdragsgivare?
1 □ Ja 2 □ Nej

72. På en skala från 1-10, hur säkra är ni på att dessa personer skulle prioritera er om ett angrepp med skadlig kod skulle drabba många myndigheter och företag samtidigt?

_____

73. Anser du att den grupp av personer som ska leda IT-arbetet i krissituationer (t.ex. om en stor del av systemet skulle vara nere p.g.a. skadlig kod) är tillräcklig stor?
1 □ Ja 2 □ Nej

74. Hur skulle ni klara av IT-arbetet om en nyckelperson i gruppen faller bort?

Bara till myndigheter:

75. Hur mycket påverkar skadlig kod 24-timmarsmyndighetssatsningen?
Innebär risken för skadlig kod begränsningar på er 24-timmarssatsning?

---

76. Rent generellt, vad kännetecknar bra IT- och informationssäkerhet i en organisation?

---

77. Hur tycker ni att er IT-miljö bör se ut om 5 år?

---

78. Vilken hjälp från samhället (t.ex. ändrade regler, resurser, ökad kompetens) behöver ni för att nå dit?

Opticom International Research © 2004
Private and confidential

Grev Turegatan 30, 114 38 Stockholm
Tel: +46-8-50 30 90 00 Fax: +46-8-50 30 90 01
e-mail: info@opticom.se www.opticom.se

KBM:S TEMASERIE

2005:1 Beredskap mot skadlig kod
En kartläggning av IT- och informationssäkerheten inom större myndigheter och statliga bolag i Sverige med fördjupad analys av skadlig kod

2004:6 Hot- och riskrapport 2004
Gränsöverskridande sårbarheter

2004:5 "We're a peaceful nation"
Krigsretorik efter 11 september

2004:4 Ministermordet
En studie om myndigheternas kommunikation vid attentatet mot Anna Lindh

2004:3 Säkerhet och beredskap i Europeiska unionen

2004:2 Stereotyper i vardagen
Bilder av "de främmande"

2004:1 Krisjournalistik eller journalistik i kris?
En forskningsöversikt om medier, risker och kriser

2003:6 Demokratin och mordet på Anna Lindh

2003:5 IT och sårbarhet
Kritiska beroendeförhållanden i den nationella IT-infrastrukturen

2003:4 Från osäker källa
Bevakningen av Irakkriget i svenska medier

2003:3 Krisberedskap i omvärlden
Samordningsstrukturer i fem länder

2003:2 Irakkrigets andra dag
En jämförelse mellan SVT och tidningspressen den 21 mars 2003

2003:1 Bagdad-Bob, menige Jessica Lynch och Cirkus Saddam
Irakkriget iscensatt i svenska medier

SPECIAL FEATURE

2004:5 "We're a peaceful nation"
War Rhetoric after September 11

Beredskap mot skadlig kod

EN KARTLÄGGNING AV IT- OCH INFORMATIONSSÄKERHETEN INOM STÖRRE MYNDIGHETER OCH STATLIGA BOLAG I SVERIGE MED FÖRDJUPAD ANALYS AV SKADLIG KOD

Under hösten 2004 har Opticom International Research gjort en studie om IT- och informationssäkerhet och beredskap mot skadlig kod hos ett antal större myndigheter och statliga bolag i Sverige. Studien har gjorts på uppdrag av Krisberedskapsmyndigheten. Samtliga undersökta organisationer har som gemensam nämnare att de spelar en viktig roll i den nationella IT-infrastrukturen. Förutsättningarna för deras verksamhet innebär att det ställs höga krav på dem när det gäller att garantera en säker och väl fungerande informationshantering.

RAPPORTENS DISPOSITION

Sammanfattning. Presenterar övergripande slutsatser och rekommendationer samt resultaten i punktform.

Kapitel 1. Förklarar studiens bakgrund, syfte, metod, centrala begrepp samt rapportens resultatredovisning & disposition.

Kapitel 2. Redovisar undersökning av IT-systemens betydelse för och behovstillfredsställelse inom de undersökta organisationerna och vilka externa krav som ställs på dem.

Kapitel 3. Redogör för hur organisationernas IT- och informationssäkerhet ser ut i vardags- och krissituationer.

Kapitel 4. Beskriver hur beredskapen att stå emot skadlig kod ser ut i dagsläget och hur organisationerna eventuellt har blivit drabbade av skadlig kod.

Appendix. Visar det frågeformulär som tjänade som underlag vid genomförandet av de personliga djupintervjuerna.

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se

ISSN 1652-2915
ISBN 91-85053-72-4