



POST & TELESTYRELSEN

PROMEMORIA

DATUM

5 juli 2005

VÅR REFERENS

05-9152/59

HANDLÄGGARE, AVDELNING/ENHET, TELEFON, E-POST

Peter Wallström
SITIC
08-678 57 27
peter.wallstrom@pts.se

Mörkertalsundersökningen 2005

Svenska organisationer om IT-säkerhetsincidenter

POSTADRESS Box 5398, 102 49 Stockholm

BESÖKSADRESS Birger Jarlsgatan 16

TELEFON 08-678 55 00

FAX 08-678 55 05

E-POST pts@pts.se

WEBBADRESS www.pts.se

Innehållsförteckning

1	Bakgrund.....	3
2	Metod och genomförande.....	3
2.1	Målgrupper och urval.....	3
2.2	Fältarbete	4
2.3	Frågeformulär.....	4
2.4	Vägning.....	4
3	Urvalsprofil och säkerhetsorganisation.....	5
3.1	Andel organisationer som är verksamma inom privat- respektive offentlig sektor.....	5
3.2	Andel organisationer som bedriver IT-säkerhetsarbetet i egen regi.....	5
3.3	Andel organisationer som har hela eller delar av IT-säkerhetsarbetet outsourcad och som får återrapportering på allt som berör allvarigare IT-säkerhetsincidenter.....	6
3.4	Delsammanfattning	6
4	Omfattning av IT-säkerhetsincidenter och internrapportering.....	7
4.1	Andel organisationer som <i>någon gång</i> har varit med om någon av de fyra typerna av IT-säkerhetsincidenter	7
4.2	Andel organisationer som <i>under de senaste 12 månaderna</i> har varit med om någon av de fyra typerna av IT-säkerhetsincidenter	8
4.3	Andel organisationer som internrapporterar denna typ av IT-säkerhetsincidenter omedelbart vid varje enskilt tillfälle.....	8
4.4	Andel organisationer som har dokumenterade rutiner för hur denna typ av IT-säkerhetsincidenter rapporteras internt.....	9
4.5	Delsammanfattning	10
5	Rapportering av IT-säkerhetsincidenter till polisen	11
5.1	Benägenhet att polisanmäla IT-säkerhetsincidenter.....	11
5.2	Andel organisationer som har dokumenterade rutiner för när IT-säkerhetsincidenter ska polisanmälas.....	12
5.3	Andel organisationer som har haft IT-säkerhetsincident under de senaste 12 månaderna och som har polisanmält incidenten	12
5.4	Orsaker till att organisationer inte väljer att polisanmäla IT-säkerhetsincidenter.....	13
5.5	Delsammanfattning	13
6	Rapportering av IT-säkerhetsincidenter till Sitic	14
6.1	Kännedom om Sitic.....	14
6.2	Benägenhet att rapportera IT-säkerhetsincidenter till Sitic.....	14
6.3	Andel organisationer som känner till Sitic och som har dokumenterade rutiner för när IT-säkerhetsincidenter ska rapporteras till Sitic.....	15
6.4	Andel organisationer som har haft någon av de fyra IT-säkerhetsincidenterna under de senaste 12 månaderna och som har rapporterat denna till Sitic	16
6.5	Orsaker till att organisationer inte väljer att rapportera IT-säkerhetsincidenter till Sitic	16
6.6	Delsammanfattning	17
7	Sammanfattning.....	18
7.1	Säkerhetsorganisering.....	18
7.2	Omfattning av IT-säkerhetsincidenter och internrapportering.....	18
7.3	Rapportering av IT-säkerhetsincidenter till polisen	19
7.4	Rapportering av IT-säkerhetsincidenter till Sitic	19
7.5	Reflektioner kring Sitics verksamhet.....	19

1 Bakgrund

Sveriges IT-incidentcentrum, Sitic, ska stödja samhället i arbetet med skydd mot IT-incidenter. Sitic har fyra uppgifter:

1. att tillhandahålla ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer,
2. att sprida information i samhället om nya problem som kan störa IT-system,
3. att lämna information och råd om förebyggande åtgärder samt
4. att sammanställa och ge ut statistik som underlag för kontinuerliga förbättringar i det förebyggande arbetet.

Mörkertalsundersökningen genomförs som ett led i Sitics uppgifter 1 och 4.

Undersökningen syftar till att bl.a. få aktuell information om omfattningen av antalet incidenter som inträffar inom samhällets organisationer, i vilken grad incidenter kommer till organisationens säkerhetsansvariges kännedom, i vilken grad incidenter polisanmäls och/eller rapporteras till Sitic och bakomliggande orsaker till benägenheten att polisanmäla och/eller rapportera till Sitic.

Undersökningens hypotes är att mörkertal kan spåras i underrapportering inom fyra områden: rutiner för outsourcing, rutiner för internrapportering, rutiner för externrapportering samt faktisk rapportering/anmälan.

Föreliggande promemoria syftar till att ge läsaren en snabb och dagsaktuell överblick över de basresultat som tidigt kan redovisas ur undersökningen.

Sitic kommer att korsrelatera undersökningsresultaten för att exempelvis beräkna och jämföra av undersökningsresultaten förväntad rapportering av IT-incidenter till Sitic med faktisk rapportering. Undersökningsresultaten kommer också att jämföras med liknande svenska undersökningar och internationella motsvarande mörkertalsundersökningar.

Undersökningen genomförs i samverkan med Rikskriminalpolisen och fältarbetet har utförts av Temo.

2 Metod och genomförande

2.1 Målgrupper och urval

Målgrupp för undersökningen har varit företag och organisationer, privata som offentliga, med 50 anställda eller fler. Ett slumpmässigt urval har köpts in från PAR. Urvalet har stratifierats på företag/organisationer med 50-199 anställda, respektive 200 anställda eller fler.

Genomgående i denna promemoria kallas företag/organisationer med 50-199 anställda för medelstora organisationer, och företag/organisationer med 200 anställda eller fler för stora organisationer.

2.2 Fältarbete

Datinsamlingen har skett genom en telefonundersökning utförd av Temo, som bedömde att det är den metod som skulle ge högst svarsfrekvens. Innan telefonundersökningen påbörjades skickades ett aviseringsbrev ut per post till ett bruttourval omfattande 2 000 organisationer, i vilket syftet med undersökningen beskrevs närmare. Aviseringsbrevet var undertecknat av PTS generaldirektör och chefen för Rikskriminalpolisen. Brevet ställdes till ”säkerhetschef eller säkerhetsansvarig i IT-frågor”. Temo har sedan vid själva telefonkontakten i organisationens telefonväxlar sökt efter säkerhetschef eller säkerhetsansvarig i IT-frågor.

Flera av de organisationer som fick aviseringsbrevet har meddelat Sitic och Temo vem i deras organisation som ska svara på frågorna.

Totalt har 500 intervjuer genomförts med svenska organisationer vilka fördelades på 250 intervjuer med medelstora respektive 250 intervjuer med stora organisationer. Svarsfrekvensen för undersökningen är 68 %. 738 telefonsamtal resulterade i 500 telefonintervjuer. Detta är, med Temos erfarenhet, en bra svarsfrekvens med tanke på den målgrupp som intervjuats. Temo har i andra telefonundersökningar med denna målgrupp erfarit betydligt lägre svarsfrekvenser. Sannolikt har det utskickade aviseringsbrevet haft betydelse för svarsfrekvensen.

Fältarbetet har bedrivits mellan 050504 och 050523.

2.3 Frågeformulär

Frågeformuläret har utarbetats i samråd mellan Sitic, Rikskriminalpolisen och Temo. Då undersökningsmetoden var telefonintervjuer fick frågeformuläret begränsas till en intervjutid på ca sju minuter vilket medger ett frågeformulär med ca 20 frågor.

2.4 Vägning

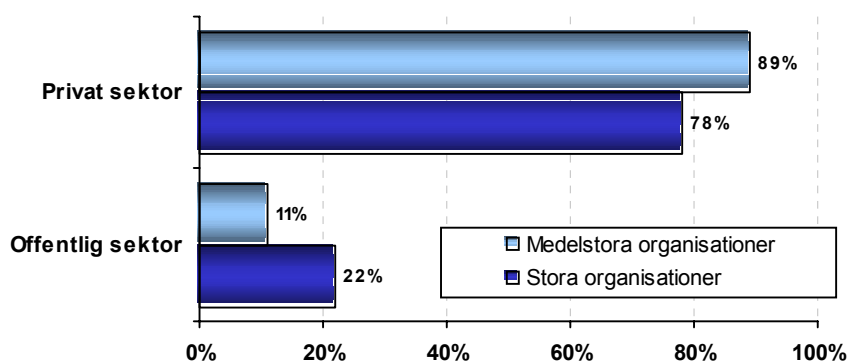
Undersökningsresultaten har viktats motsvarande de populationer som medelstora respektive stora organisationer har i Sverige. Det betyder att resultaten har viktats så att medelstora respektive stora organisationer får den inverkan på totalresultatet de ska ha i förhållande till sin andel av samtliga organisationer enligt viktal från PAR. Medelstora organisationer har i resultaten viktats till 73% (4 680 av 6 409 organisationer) och stora organisationer har viktats till 27% (1 729 av 6 409 organisationer).

3 Urvalsprofil och säkerhetsorganisation

3.1 Andel organisationer som är verksamma inom privat- respektive offentlig sektor

Till den privata sektorn inräknas företag och icke-statliga organisationer, till offentlig sektor inräknas verksamheter inom stat, kommun och landsting.

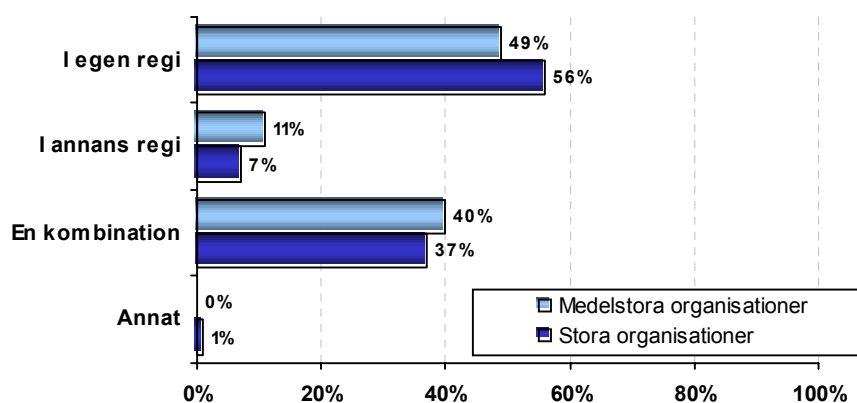
Fråga: *Arbetar du inom privat eller offentlig sektor?*



Drygt åtta av tio organisationer är verksamma inom den privata sektorn.

3.2 Andel organisationer som bedriver IT-säkerhetsarbetet i egen regi

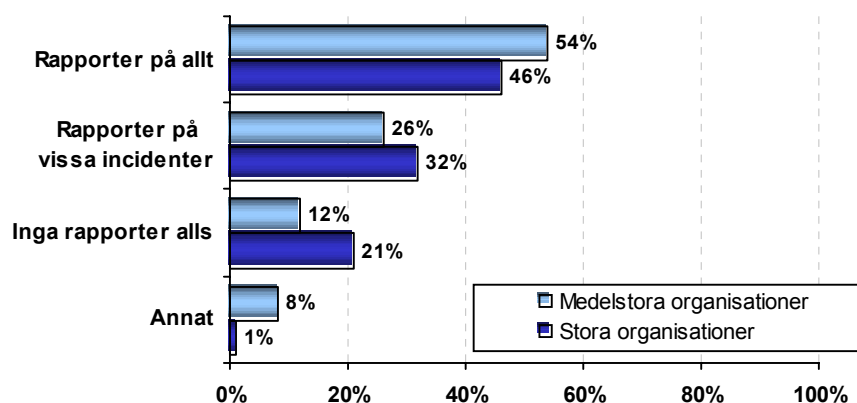
Fråga: *Hur är IT-säkerhetsarbetet organiserat i din organisation? Är det...*



Hälften av organisationerna bedriver IT-säkerhetsarbetet i egen regi. En av tio organisationer har hela IT-säkerhetsarbetet outsourcad. Organisationer verksamma inom den offentliga sektorn bedriver i högre grad IT-säkerhetsarbetet i egen regi. Att bedriva IT-säkerhetsarbetet som en kombination av egen regi och annans regi görs i högre grad av privata företag.

3.3 Andel organisationer som har hela eller delar av IT-säkerhetsarbetet outsourcad och som får återrapportering på allt som berör allvarligare IT-säkerhetsincidenter

Fråga: Får ni någon återrapportering av allvarligare IT-säkerhetsincidenter från det företag ni anlitar tjänster av? Får ni...



Hälften av organisationerna som har hela eller delar av IT-säkerhetsarbetet outsourcad uppger att de från det anlitate företaget får återrapportering på allt som berör allvarligare IT-säkerhetsincidenter. En av tio organisationer uppger att de inte får några rapporter alls från det anlitate företaget.

3.4 Delsammanfattning

- Drygt åtta av tio organisationer är verksamma inom den inom den privata sektorn.
- Hälften av organisationerna bedriver IT-säkerhetsarbetet helt i egen regi.
- Organisationer inom offentlig sektor bedriver i högre grad än organisationer inom privat sektor IT-säkerhetsarbetet i egen regi.
- Att bedriva IT-säkerhetsarbetet som en kombination av egen regi och annans regi görs i högre grad av privata företag.
- En av tio organisationer har hela IT-säkerhetsarbetet outsourcad.
- Hälften av organisationerna som har hela eller delar av IT-säkerhetsarbetet outsourcad får återrapportering på allt som berör allvarligare IT-säkerhetsincidenter.
- En av tio organisationer uppger att de inte får några rapporter alls.

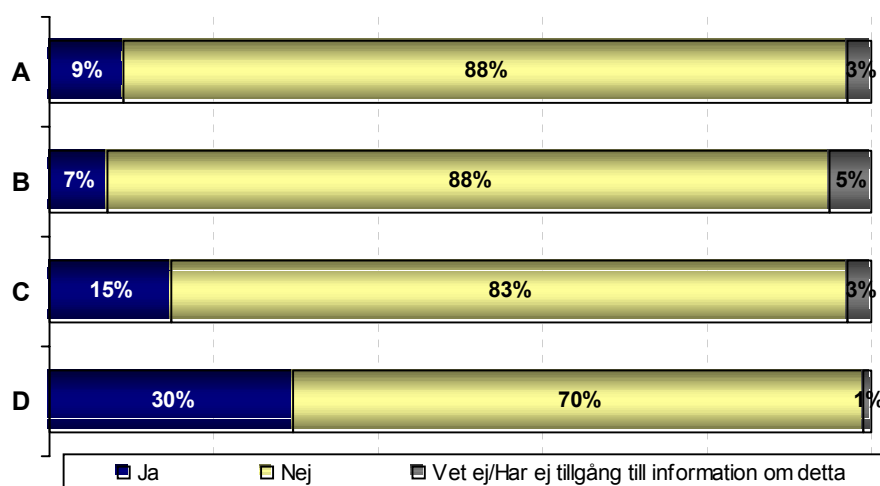
4 Omfattning av IT-säkerhetsincidenter och internrapportering

4.1 Andel organisationer som *någon gång* har varit med om någon av de fyra typerna av IT-säkerhetsincidenter

Respondenterna fick uppläst beskrivningen av följande typincidenter och tillfrågades om de någon gång hade varit med om någon av dessa.

- A. "IT-säkerhetsincident som har medfört att information eller systemkomponent blivit åtkomlig för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, att någon "hackat" sig in i systemen."
- B. "IT-säkerhetsincident som har inneburit en utförlig kartläggning av era system. Det handlar alltså om att obehörig letat efter sårbara punkter på ett sätt som skiljer sig från det vardagliga mönstret."
- C. "IT-säkerhetsincident som har medfört att system eller delar av system blev otillgängliga, så kallad DOS-angrepp eller Denial of Service. Det kan alltså handla om att system/nätverk blivit överbelastat på grund av ett DOS-angrepp."
- D. "IT-säkerhetsincident som har inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Det kan alltså handla om virus, maskar, trojaner m.m."

Fråga: Har din organisation varit med om IT-säkerhetsincidenter av typen...

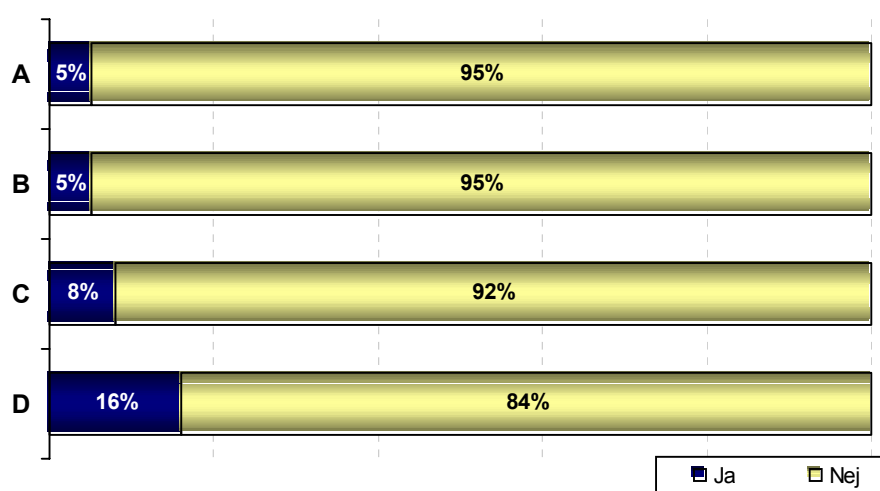


227 organisationer har *någon gång* haft någon av de fyra typerna av IT-säkerhetsincidenter, vilket motsvarar 45% av samtliga organisationer. Organisationer verksamma inom offentlig sektor har i högre grad varit utsatta för dataintrång. Två av tio offentliga organisationer (21%) har någon gång blivit utsatt för

dataintrång. För privata företag är andelen 7%. I övrigt finns inga skillnader i utsatthet mellan medelstora eller stora organisationer, eller mellan offentliga respektive privata företag.

4.2 Andel organisationer som *under de senaste 12 månaderna* har varit med om någon av de fyra typerna av IT-säkerhetsincidenter

Fråga: Har din organisation varit utsatt för någon av de 4 typerna av IT-säkerhetsincidenter under de senaste 12 månaderna?



141 organisationer har varit utsatta för någon av de fyra typerna av IT-säkerhetsincidenter *under de senaste 12 månaderna* vilket motsvarar 28% av samtliga organisationer. 428 typincidenter inträffade under perioden fördelade enligt:

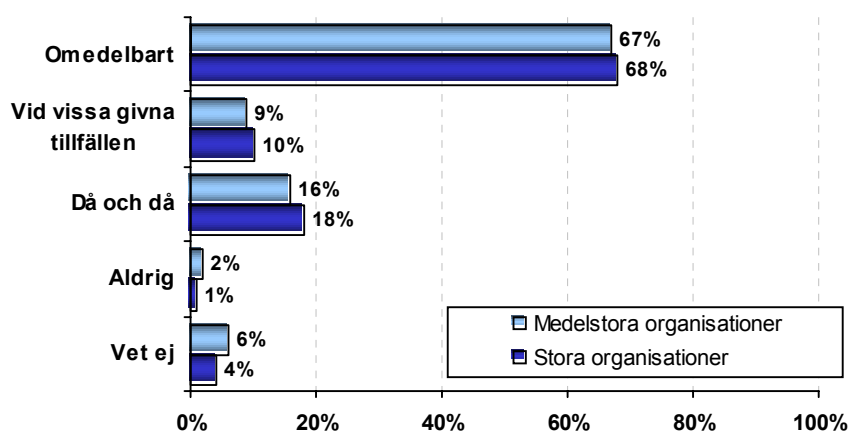
- dataintrång: 78 incidenter vid 26 organisationer,
- utförlig kartläggning av system: 88 incidenter vid 24 organisationer,
- DOS-angrepp: 115 incidenter vid 40 organisationer,
- allvarligt utbrott av skadlig kod: 147 incidenter vid 78 organisationer.

4.3 Andel organisationer som internrapporterar denna typ av IT-säkerhetsincidenter omedelbart vid varje enskilt tillfälle

Respondenterna är tillfrågade om man inom organisationen rapporterar dessa typer av IT-säkerhetsincidenter

- omedelbart vid varje tillfälle,
- vid vissa givna tillfällen, exempelvis genom att samla upp och redovisa regelbundet,
- då och då, exempelvis vid extraordinära händelser.

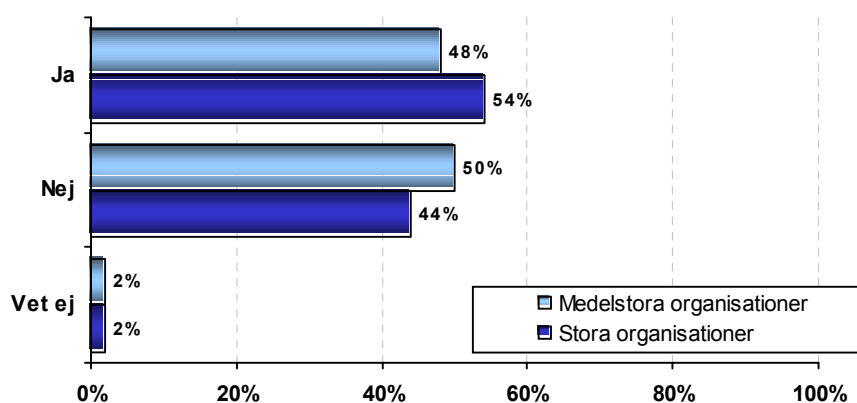
Fråga: På vilket sätt rapporteras denna typ av IT-säkerhetsincidenter till säkerhetsansvarig inom organisationen? Är det...



Två av tre organisationer internrapporterar denna typ av IT-säkerhetsincidenter omedelbart vid varje enskilt tillfälle.

4.4 Andel organisationer som har dokumenterade rutiner för hur denna typ av IT-säkerhetsincidenter rapporteras internt

Fråga: Har din organisation dokumenterade rutiner/policies för hur denna typ av IT-säkerhetsincidenter ska komma till säkerhetsansvarigs kännedom?



Hälften av organisationerna uppger att de har dokumenterade rutiner/policies för hur dessa typer av IT-säkerhetsincidenter ska rapporteras internt. En av tre organisationer som har hela IT-säkerhetsarbetet outsourcad har sådana dokumenterade rutiner/policies.

4.5 Delsammanfattning

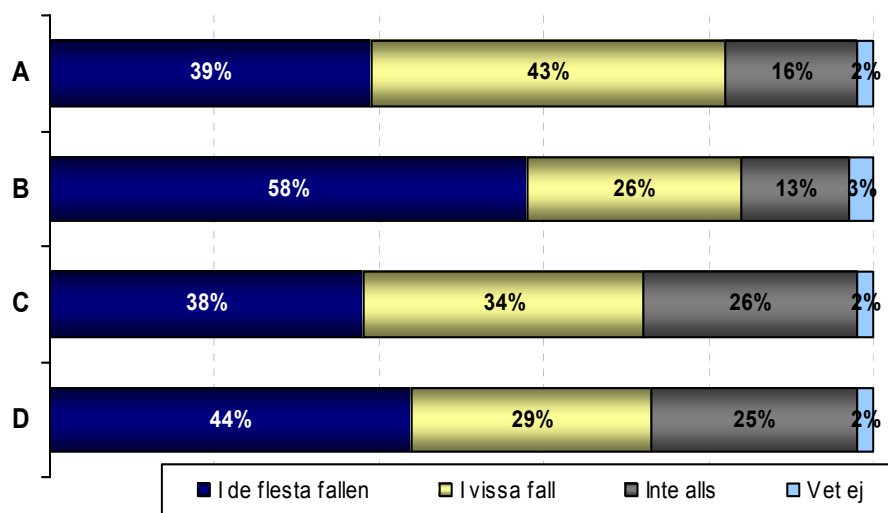
- 227 organisationer har *någon gång* haft någon av de fyra typerna av IT-säkerhetsincidenter, vilket motsvarar 45% av samtliga organisationer.
- Organisationer verksamma inom offentlig sektor har i högre grad varit utsatta för dataintrång. Två av tio offentliga organisationer (21%) har någon gång blivit utsatt för dataintrång. För privata företag är andelen 7%.
- 428 typincidenter har inträffat *under de senaste 12 månaderna* fördelat över 141 organisationer, vilket motsvarar 28% av samtliga organisationer.
- Två av tre organisationer internrapporterar denna typ av IT-säkerhetsincidenter omedelbart vid varje enskilt tillfälle.
- Hälften av organisationerna uppger att de har dokumenterade rutiner/policies för hur denna typ av IT-säkerhetsincidenter ska rapporteras internt.
- En av tre organisationer som har hela IT-säkerhetsarbetet outsourcad har sådana dokumenterade rutiner/policies.

5 Rapportering av IT-säkerhetsincidenter till polisen

5.1 Benägenhet att polisanmäla IT-säkerhetsincidenter

Fråga: För var och en av de fyra typerna av IT-säkerhetsincidenter så undrar jag om ni skulle polisanmäla sådana incidenter, i de flesta fallen, i vissa fall eller inte alls...

- A. ”IT-säkerhetsincident som har medfört att information eller systemkomponent blivit åtkomlig för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, att någon ’hackat’ sig in i systemen.”
- B. ”IT-säkerhetsincident som har inneburit en utförlig kartläggning av era system. Det handlar alltså om att obehörig letat efter sårbara punkter på ett sätt som skiljer sig från det vardagliga mönstret.”
- C. ”IT-säkerhetsincident som har medfört att system eller delar av system blev otillgängliga, så kallad DOS-angrepp eller Denial of Service. Det kan alltså handla om att system/nätverk blivit överbelastat på grund av ett DOS-angrepp.”
- D. ”IT-säkerhetsincident som har inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Det kan alltså handla om virus, maskar, trojaner m.m.”

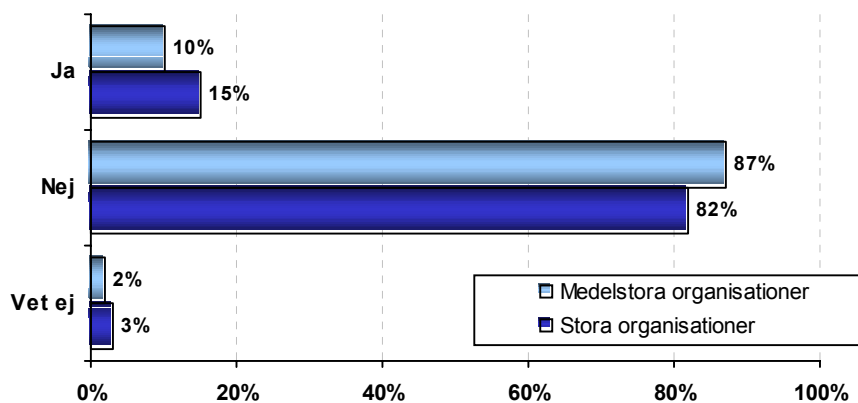


Sex av tio organisationer uppger att de i de flesta fall skulle polisanmäla utförliga kartläggningar av sina system. Fyra av tio organisationer skulle i de flesta fall polisanmäla dataintrång, DOS-angrepp och allvarligare utbrott av skadlig kod.

Den typ av IT-säkerhetsincidenter man är mindre benägen att polisanmäla är DOS-angrepp och allvarligare utbrott av skadlig kod. Här uppger en av fyra organisationer att man inte alls skulle polisanmäla denna typ av incidenter.

5.2 Andel organisationer som har dokumenterade rutiner för när IT-säkerhetsincidenter ska polisanmälas

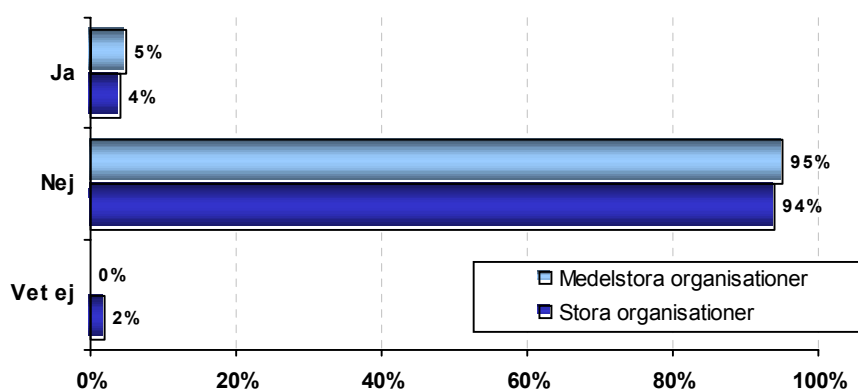
Fråga: Har din organisation dokumenterade rutiner/policies för när de typer av IT-säkerhetsincidenter vi frågat om ska polisanmälas?



Endast en av tio organisationer har dokumenterade rutiner/policies för när IT-säkerhetsincidenter ska polisanmälas.

5.3 Andel organisationer som har haft IT-säkerhetsincident under de senaste 12 månaderna och som har polisanmält incidenten

Fråga: Har ni polisanmält någon IT-säkerhetsincident under de senaste 12 månaderna?



Endast 4% av organisationer som haft någon av de fyra typerna av IT-säkerhetsincidenter uppger att de har polisanmält denna under de senaste 12 månaderna. Det finns inga signifikanta skillnader när det gäller anmälningsfrekvensen mellan medelstora och stora organisationer eller mellan organisationer i privat- eller offentlig sektor.

5.4 Orsaker till att organisationer inte väljer att polisanmäla IT-säkerhetsincidenter

Fråga: Vilka orsaker tror du att det kan finnas till att organisationer väljer att inte polisanmäla allvarligare IT-säkerhetsincidenter

Denna fråga ställdes utan att svarsalternativ upplästes. Intervjuaren fyllde i de fasta svarsalternativ som passade bäst in på organisationens svar.

De fem främsta orsakerna som organisationerna tror kan finnas till att organisationer väljer att inte polisanmäla incidenter är enligt följande.

- För att man tror att det kan ge negativ uppmärksamhet för organisationen (37%)
- För att man inte tror att polisen har resurser att klara upp saken (12%)
- För att de inte tror att det är möjligt att finna gärningsmannen (11%)
- För att incidenterna är obetydliga/ej tillräckligt allvarliga (9%)
- Dålig kunskap om att man kan/bör polisanmäla/tänker ej på det (8%)

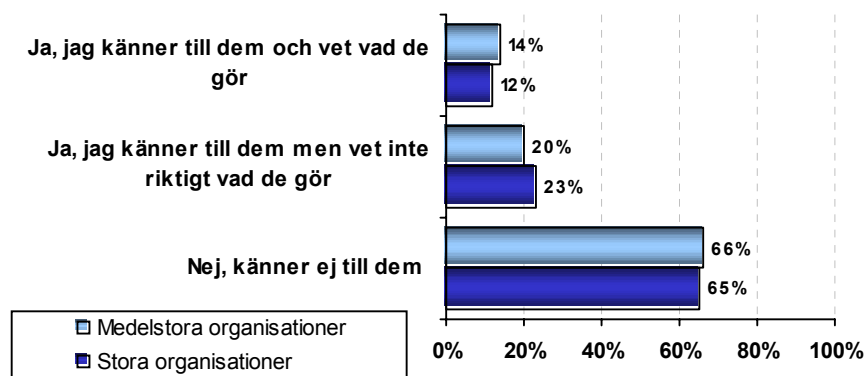
5.5 Delsammanfattning

- Sex av tio organisationer uppger att de i de flesta fall skulle polisanmäla utförliga kartläggningar av sina system.
- Fyra av tio organisationer skulle i de flesta fall polisanmäla dataintrång, DOS-angrepp och allvarligare utbrott av skadlig kod.
- Den typ av IT-säkerhetsincidenter man är mindre benägen att polisanmäla är DOS-angrepp och allvarligare utbrott av skadlig kod.
- Endast en av tio organisationer har dokumenterade rutiner/policies för när IT-säkerhetsincidenter ska polisanmälas.
- Endast 4% av organisationer som haft någon av de fyra typerna av IT-säkerhetsincidenter uppger att de har polisanmält denna under de senaste 12 månaderna.
- 37% av organisationerna nämner att det kan ge negativ uppmärksamhet kring organisationen som orsak till att organisationer inte polisanmäler allvarligare IT-säkerhetsincidenter. Resultatet kan också utläsas som att sex av tio inte ser att orsaken till att organisationer inte polisanmäler är att det kan ge negativ uppmärksamhet för organisationen.

6 Rapportering av IT-säkerhetsincidenter till Sitic

6.1 Kännedom om Sitic

Fråga: Känner du till Sveriges IT-incidentcentrum, Sitic?

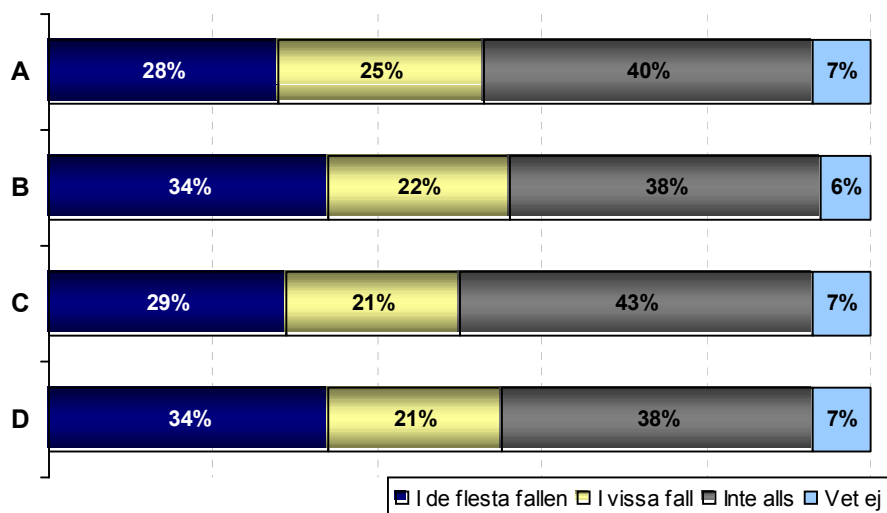


Två av tre organisationer uppger att de inte känner till Sitic. Offentliga organisationer samt organisationer som bedriver IT-säkerhetsarbetet i egen regi känner i högre grad till Sitic och vet vad de gör.

6.2 Benägenhet att rapportera IT-säkerhetsincidenter till Sitic

Fråga: Sitic är en myndighet som bl.a. har till uppgift att stödja samhällets organisationer i arbetet med att skydda sig mot IT-säkerhetsincidenter, och sammanställer och ger ut statistik inom området. Jag kommer nu att läsa upp samma 4 IT-säkerhetsincidenter som tidigare. För var och en av dem så undrar jag om ni skulle rapportera sådana incidenter till Sitic i de flesta fallen, i vissa fall eller inte alls

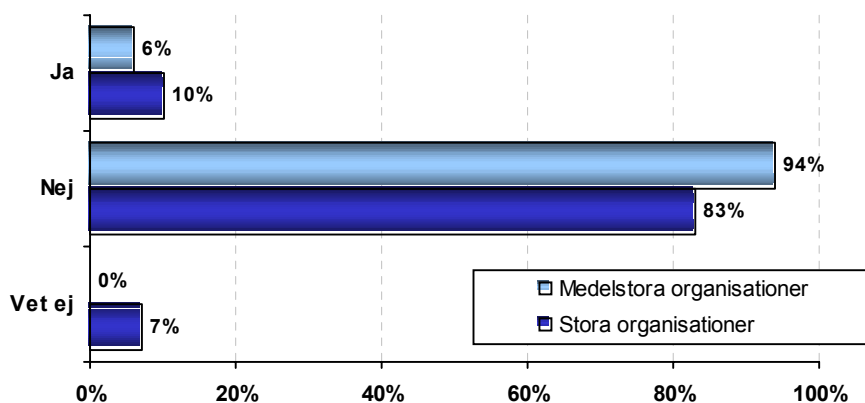
- ”IT-säkerhetsincident som har medfört att information eller systemkomponent blivit åtkomlig för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, att någon ’hackat’ sig in i systemen.”
- ”IT-säkerhetsincident som har inneburit en utförlig kartläggning av era system. Det handlar alltså om att obehörig letat efter sårbara punkter på ett sätt som skiljer sig från det vardagliga mönstret.”
- ”IT-säkerhetsincident som har medfört att system eller delar av system blev otillgängliga, så kallad DOS-angrepp eller Denial of Service. Det kan alltså handla om att system/nätverk blivit överbelastat på grund av ett DOS-angrepp.”
- ”IT-säkerhetsincident som har inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Det kan alltså handla om virus, maskar, trojaner m.m.”



Tre av tio organisationer uppger att de i de flesta fallen skulle rapportera någon av IT-säkerhetsincidenterna till Sitic. Det finns inga signifikanta skillnader mellan medelstora och stora organisationer eller mellan organisationer i privat- eller offentlig sektor vad gäller benägenheten att rapportera till Sitic.

6.3 Andel organisationer som känner till Sitic och som har dokumenterade rutiner för när IT-säkerhetsincidenter ska rapporteras till Sitic

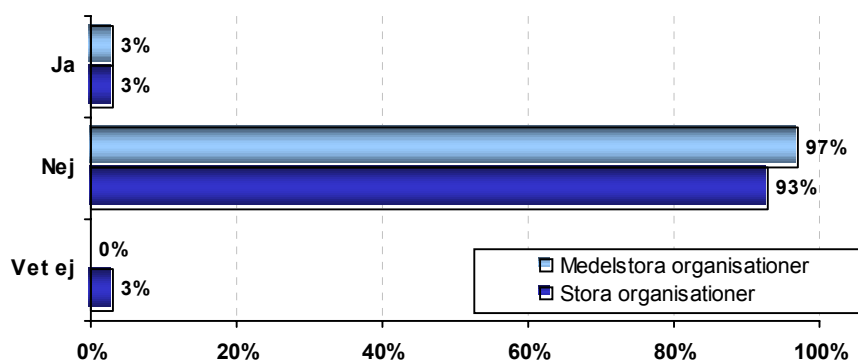
Fråga: Har din organisation dokumenterade rutiner/policies för när en incident ska rapporteras till Sitic?



7% av de organisationer som känner till Sitic har dokumenterade rutiner/policies för när en IT-säkerhetsincident ska rapporteras till Sitic.

6.4 Andel organisationer som har haft någon av de fyra IT-säkerhetsincidenterna under de senaste 12 månaderna och som har rapporterat denna till Sitic

Fråga: Har din organisation rapporterat någon IT-säkerhetsincident som ni haft under de senaste 12 månaderna till Sitic?



Endast 3% av de organisationer som känner till Sitic har rapporterat någon av de fyra IT-säkerhetsincidenterna de haft under de senaste 12 månaderna till Sitic.

6.5 Orsaker till att organisationer inte väljer att rapportera IT-säkerhetsincidenter till Sitic

Fråga: Vilka orsaker tror du att det kan finnas till att organisationer väljer att inte rapportera allvarigare IT-säkerhetsincidenter till Sitic?

Denna fråga ställdes utan att svarsalternativ upplästes. Intervjuaren fyllde i de fasta svarsalternativ som passade bäst in på organisationens svar.

De fyra främsta orsakerna som organisationerna tror kan finnas till att organisationer väljer att inte rapportera till Sitic är enligt följande.

- För att man inte känner till Sitic (53%)
- För att man tror att det kan ge negativ uppmärksamhet för organisationen (24%)
- För att man inte har någonting att vinna på det (7%)
- För att rapporteringen är för krånglig/resurskrävande/tar för mycket tid (5%)

Organisationer verksamma inom offentlig sektor uppger i högre grad än företag inom privat sektor att incidenterna är obetydliga/ej tillräckligt allvarliga som orsak till att organisationer inte rapporterar till Sitic.

I övrigt finns det inga signifikanta skillnader mellan medelstora och stora organisationer eller mellan organisationer i privat- eller offentlig sektor när det gäller vad man uppger som orsak till att organisationer inte rapporterar allvarigare IT-säkerhetsincidenter till Sitic.

6.6 Delsammanfattning

- Två av tre organisationer uppger att de inte känner till Sitic.
- Offentliga organisationer samt organisationer som bedriver IT-säkerhetsarbetet i egen regi känner i högre grad till Sitic och vet vad de gör.
- Tre av tio organisationer uppger att de i de flesta fallen skulle rapportera någon av IT-säkerhetsincidenterna till Sitic.
- 7% av de organisationer som känner till Sitic har dokumenterade rutiner/policies för när en IT-säkerhetsincident ska rapporteras till Sitic.
- Endast 3% av de organisationer som känner till Sitic har rapporterat någon av IT-säkerhetsincidenterna de haft under de senaste 12 månaderna till Sitic.
- Fem av tio organisationer uppger att främsta orsaken till att organisationer väljer att inte rapportera till Sitic är för att man inte känner till Sitic (53%).
- Organisationer verksamma inom offentlig sektor uppger i högre grad än företag inom privat sektor att incidenterna är obetydliga/ej tillräckligt allvarliga som orsak till att man inte rapporterar till Sitic.

7 Sammanfattning

7.1 Säkerhetsorganisering

Drygt åtta av tio organisationer i undersökningen är verksamma inom den privata sektorn och av dem bedriver hälften av organisationerna IT-säkerhetsarbetet helt i egen regi. Organisationer inom offentlig sektor bedriver i högre grad än de inom privat sektor IT-säkerhetsarbetet i egen regi. Att bedriva IT-säkerhetsarbetet som en kombination av egen regi och annans regi görs i högre grad av privata företag. En av tio organisationer har hela IT-säkerhetsarbetet outsourcad.

Hälften av organisationerna som har hela eller delar av IT-säkerhetsarbetet outsourcad får återrapportering på allt som berör allvarligare IT-säkerhetsincidenter. En av tio organisationer uppger att de inte får några rapporter alls.

7.2 Omfattning av IT-säkerhetsincidenter och internrapportering

Omfattningen av följande fyra typer av IT-säkerhetsincidenter har efterfrågats:

- dataintrång,
- utförlig kartläggning av system,
- DOS-angrepp,
- allvarligt utbrott av skadlig kod.

227 organisationer har *någon gång* haft någon av de fyra typerna av IT-säkerhetsincidenter, vilket motsvarar 45% av samtliga organisationer. Organisationer verksamma inom offentlig sektor har i högre grad varit utsatta för dataintrång. Två av tio offentliga organisationer (21%) har någon gång blivit utsatt för dataintrång. För privata företag är andelen 7%.

141 organisationer har varit utsatta för någon av de fyra typerna av IT-säkerhetsincidenter *under de senaste 12 månaderna* vilket motsvarar 28% av samtliga organisationer. 428 typincidenter inträffade under denna period fördelade enligt:

- dataintrång: 78 incidenter vid 26 organisationer,
- utförlig kartläggning av system: 88 incidenter vid 24 organisationer,
- DOS-angrepp: 115 incidenter vid 40 organisationer,
- allvarligt utbrott av skadlig kod: 147 incidenter vid 78 organisationer.

Två av tre organisationer internrapporterar allvarligare IT-säkerhetsincidenter omedelbart vid varje enskilt tillfälle. Hälften av organisationerna uppger att de har dokumenterade rutiner/policies för hur denna typ av IT-säkerhetsincidenter ska rapporteras internt. En av tre organisationer som har hela IT-säkerhetsarbetet outsourcad har sådana dokumenterade rutiner/policies.

7.3 Rapportering av IT-säkerhetsincidenter till polisen

Sex av tio organisationer uppger att de i de flesta fall skulle polisanmäla utförliga kartläggningar av sina system. Fyra av tio organisationer skulle i de flesta fall polisanmäla dataintrång, DOS-angrepp och allvarigare utbrott av skadlig kod. Den typ av IT-säkerhetsincidenter man är mindre benägen att polisanmäla är DOS-angrepp och allvarigare utbrott av skadlig kod.

Endast en av tio organisationer har dokumenterade rutiner/policies för när IT-säkerhetsincidenter ska polisanmälas.

Endast 4% av organisationer som haft någon av de fyra typerna av IT-säkerhetsincidenter uppger att de har polisanmält denna under de senaste 12 månaderna.

En av tre organisationer nämner att det kan ge negativ uppmärksamhet kring organisationen som orsak till att organisationer inte polisanmäler allvarigare IT-säkerhetsincidenter. Resultatet kan också utläsas som att sex av tio inte ser att orsaken till att organisationer inte polisanmäler är att det kan ge negativ uppmärksamhet för organisationen.

7.4 Rapportering av IT-säkerhetsincidenter till Sitic

Två av tre organisationer uppger att de inte känner till Sitic. Offentliga organisationer samt organisationer som bedriver IT-säkerhetsarbetet i egen regi känner i högre grad till Sitic och vet vad de gör.

Tre av tio organisationer uppger att de i de flesta fallen skulle rapportera någon av IT-säkerhetsincidenterna till Sitic. 7% av de organisationer som känner till Sitic har dokumenterade rutiner/policies för när en IT-säkerhetsincident ska rapporteras till Sitic.

Endast 3% av de organisationer som känner till Sitic har rapporterat någon av IT-säkerhetsincidenterna de haft under de senaste 12 månaderna till Sitic.

Fem av tio organisationer uppger att främsta orsaken till att organisationer väljer att inte rapportera till Sitic är för att man inte känner till Sitic (53%). Organisationer verksamma inom offentlig sektor uppger i högre grad än företag inom privat sektor att incidenterna är obetydliga/ej tillräckligt allvarliga som orsak till att man inte rapporterar till Sitic.

7.5 Reflektioner kring Sitics verksamhet

Ett av Sitics uppdrag är att tillhandahålla ett system för informationsutbyte om IT-incidenter mellan samhällets organisationer. Sitic kan aktivt bidra till att försöka minska mörkertalen inom de områden där underrapportering kan antas ske. Informationsåtgärder och förebyggande rådgivning vad gäller bra rutiner för outsourcing och bra rutiner för intern rapportering kan möjliggöra ett lägre mörkertal.

Det faktum att två av tre organisationer inte känner till Sitic ligger i linje med Sitics egna uppskattningar av hur känd verksamheten är. Detta förhållande anges också vara den främsta orsaken till att organisationer inte rapporterar till Sitic. En annan orsak till att organisationer inte rapporterar till Sitic är att man tror att det kan ge negativ uppmärksamhet för organisationen.

Sitic behöver, och har planerat, att utöka sina informationsåtgärder i syfte att medvetandegöra verksamheten för fler än de intressenter som Sitic har idag.

Informationsåtgärderna ska intensifieras vad gäller Sitics möjligheter att sekretessbelägga incidentrapporter enligt Sekretesslagen. Den förändring av Sekretesslagen som trädde i kraft 1 juli 2004 medför att Sitic kan sekretessbelägga samtliga uppgifter som behandlar informationssäkerhet. Dessa sekretessuppgifter är också enligt Sekretesslagen undantagna den s.k. meddelarfriheten. Sitic kan således sekretessbelägga samtliga incidentrapporter och avsändaridentiteter på organisationer som rapporterar.

En tredje orsak till att organisationer inte rapporterar till Sitic uppges vara att rapporteringen är för krånglig/resurskrävande/tar för mycket tid. I Sitics planerade informationsåtgärder bör det automatiserade webbrapporteringsverktyget som finns på Sitics hemsida särskilt belysas.

Det är tillfredsställande att endast en av 500 organisationer anser att orsaken till att organisationer inte rapporterar till Sitic är att verksamheten är lokaliserad till PTS.

Den största utmaningen för Sitic torde dock vara att tydliggöra incitamenten för att rapportera. Huvudbudskapet i Sitics informationsåtgärder bör vara de incitament som finns för organisationer att rapportera till Sitic:

- varje enskild rapport ökar möjligheterna att generera relevant statistik och hotbilsrapportering - beslutsunderlag,
- det går att uppnå kostnadsreduktioner genom samarbete,
- inrapportering kommer andra tillgodo (man kan vara först med att upptäcka en ny företeelse),
- Sitic kan eventuellt associera en inkommen rapport med en eller flera andra (se mönster i hot och angrepp),
- Sitic kan förfoga över ännu inte allmänt känd information som kan ha betydelse,
- Sitic kan, i särskilda fall, bidra med spetskompetens, egen såväl som samarbetspartners, i arbetet med analys av händelsen.