Datakriminalitet i Norge
De mørke tallene

Line Sunnarvik Andersson

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2007

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Sammendrag

Bruken av Internett har ført til en globalisering av datakriminalitet. I økende grad er det ressurssterke organiserte miljøer som står bak de alvorligste sakene. Dagens teknologi gjør det mulig å gjennomføre avansert datakriminalitet uten at det nødvendigvis kan spores tilbake til de ansvarlige.

I denne rapporten har vi satt søkelyset på omfanget av datakriminalitet som norske virksomheter utsettes for og hva som kan gjøres for å få flere virksomheter til å anmelde datakriminalitet. Dette har vi gjort ved å gjennomføre en spørreundersøkelse blant medlemmer av IT-SikkerhetsForum (ISF), ved å benytte datagrunnlaget fra Mørketallsundersøkelsen for 2006 og ved å gjennomføre intervjuer med virksomheter som har anmeldt datakriminalitet. Videre har vi intervjuet en representant fra Kripos og fått innspill fra en tidligere datakriminell.

Ved analyser av datagrunnlaget fra Mørketalsundersøkelsen 2006 har vi funnet en del rapporteringer i forbindelse med datakriminelle hendelser, som vi mener er usikre eller direkte feil. Vi anser at enkelte virksomheter kan ha misforstått spørsmålsstillingen, at det kan være feilrapporteringer eller at det kan ha skjedd feil ved den manuelle registreringen av dataene fra spørreskjemaene. Når vi i våre analyser utelukket disse rapporteringene fant vi at antall vellykkede og oppdagede hendelser var 48,9 % lavere enn det som ble presentert i Mørketallsundersøkelsen 2006. Noe som følgelig påvirket våre estimater for mørketall.

Ett av rapportens bidrag er å beskrive hvorfor norske virksomheter ikke anmelder datakriminelle hendelser. I den forbindelse har vi sett at den vesentligste årsaken, basert på våre dataanalyser, er at virksomhetene mente at sakene var ubetydelig. Vi antar at dette kan henge sammen med det faktum at den hendelseskategorien som oppnådde flest rapporteringer var "infeksjon av virus/orm/trojaner". Det fremkommer av våre intervjuer at virksomhetene ikke hadde anmeldt alle hendelser de har vært utsatt for. Noen av virksomheter opplyste at det er usikkert hvorvidt de vil gjennomføre en anmeldelsesprosess neste gang de blir utsatt for visse typer datakriminalitet. De hadde erfart at dette hadde vært meget ressurskrevende, ikke minst i forhold til bevissikring. Dessuten ble sakene henlagt. Videre har våre intervjuer vist at dersom det ønskes at flere virksomheter skal anmelde datakriminalitet bør de få informasjon om hvordan de skal håndtere datakriminelle hendelser.

I denne rapporten har vi også vurdert hvorvidt medlemmer av ISF har et større fokus på informasjonssikkerhet enn virksomhetene som deltok i Mørketallsundersøkelsen. Våre resultater viser at ISFs medlemmer i større grad har implementert tekniske og formelle sikringstiltak enn virksomheter som deltok i Mørketallsundersøkelsen. Videre har de i større grad rapportert og anmeldt datakriminelle hendelser.

Rapporten bidrar til slutt med veiledninger for håndtering av datakriminelle hendelser og for sikring av elektroniske bevis.

Abstract

The use of internet has enabled a globalisation of computer crime and the crimes are increasingly being committed by resourceful organized criminal syndicates. With today's technology it is feasible to commit a computer crime without being detected and prosecuted.

In this report we have focused on the extent of computer crime committed against Norwegian companies and on which actions that can be performed to change the companies' unwillingness to report computer crime to the police authorities. Our work is based on a survey among members of IT-SikkerhetsForum (ISF), the dataset from Mørketallsundersøkelsen 2006 and interviews with companies which have reported computer crime. Furthermore we have interviewed a representative from Kripos and have received a contribution from a former computer criminal.

When we analysed and interpreted the dataset from Mørketallsundersøkelsen 2006 we discovered that some of the numbers reported by the companies in regards to computer criminal incidents were suspiciously high. We deemed that some of the companies could have misinterpreted the questions, hence given too high numbers, or that mistakes had been made when the data from the questionnaires were manually registered. In our analyses we have disregarded these data and considered them to be statistical outliers, thus our calculation of the total number of computer criminal incidents given by the respondents of Mørketallsundersøkelsen 2006 is 48,9 % lower than previously reported. Accordingly, our estimate of computer crime committed against Norwegian companies is in all considerably lower.

One of this report's contributions is to describe why Norwegian companies fail to report computer crime to the police authorities. Our analyses show that the most common reason is because the companies did not consider the incident to be serious enough. We have made an assumption that this is due to the fact that infection by virus/worm/trojans is the incident that most companies have experienced. Furthermore, throughout our interviews we learned that the companies had not chosen to report all incidents, and that some are unsure of whether they will report a computer crime the next time they are affected. They have experienced that the process of handling and reporting a computer crime is resource-demanding, and that the cases they reported were dropped. Most of our interviewees called for guidelines on how to handle computer crime.

In this report we have also compared the dataset from the ISF-survey with the dataset from Mørketallsundersøkelsen 2006. Our analyses disclose that ISF-members to a greater degree have implemented technical and formal safety measures, and that they experience more computer crime and that more of these crimes have been reported.

This report includes a guideline on handling a computer crime incident and a guideline for the collection of electronic evidence.

Forord

Nå settes punktum for 2 år med intense og utfordrende studier. Etter å ha jobbet i 20 år med IT og informasjonssikkerhet var det en utfordring å skulle sette seg på skolebenken igjen. Men, en ting er i hvert fall sikkert, jeg har ikke angret et sekund på at jeg sa opp jobben jeg hadde og gikk over til en tilværelse som fulltidsstudent. Forhåpentligvis får jeg nå oppfylt et av mine store ønsker – å få en mastergrad i informasjonssikkerhet.

I forbindelse med arbeidet med denne oppgaven er det mange som jeg vil takke. Først og fremst en takk til min interne veileder Frode Volden, ved Høgskolen i Gjøvik, som tålmodig loset meg gjennom uttallige dataanalyser og var et viktig korrektiv i forhold til arbeidet med denne oppgaven. Jeg vil også takke min eksterne veileder og oppdragsgiver Tore Larsen Orderløkken, NorSIS, for god bistand og for at du lot meg definere oppgaven slik at den ble *min*.

Av andre som bør takkes er representantene for de virksomhetene jeg intervjuet i forbindelse med oppgaven, og som var villige til å bidra med sine erfaringer og med nyttige innspill.

Videre vil jeg takke IT-SikkerhetsForum for at jeg fikk gjennomføre en spørreundersøkelse blant deres medlemmer og for at jeg har blitt invitert til høstens konferanse for å presentere min oppgave.

En stor takk går også til representanter fra Kripos sin Datakrimavdeling. Jeg ser ikke bort fra at jeg til tider satt deres tålmodighet på prøve med alle mine spørsmål og ønsker.

Takk til mine medstudenter – heltid og deltid. Jeg har satt stor pris på den tiden vi har hatt sammen.

Avslutningsvis vil jeg rett min største takk til Rune Ask. Du har vært min viktigste støttespiller gjennom hele studiet og har hele tiden har sagt: "Dette klarer du!"

Tusen takk!

Line Sunnarvik Andersson
Oslo, 30.6.2007

Innholdsfortegnelse

Figurer

Tabeller

1. Innledning

"The list of electronic crimes is as unlimited as the imaginations of those who use technology in harmful and dangerous ways."

Markow & Breithaupt [1]

Internett vokser raskere enn noe annet kommunikasjonssystem i historien. Mange virksomheter har innsett at det å være tilgjenglig via Internett er vesentlig for en videre suksess for virksomheten, men ikke alle tenker over at det å knytte virksomhetens interne nettverk og informasjonssystemer til Internett gjør dem sårbare for angrep fra datakriminelle [2].

Trusler i den digitale verden er ofte et speilbilde av trusler i den fysiske verden. Trusler som underslag, bankran, tyveri, svindel, vandalisme, utpressing osv. finnes i begge verdener. Selv om truslene er de samme, kan konsekvensene bli mye større i den digitale verden. Dette er fordi metodene som benyttes fører til at det er vanskeligere å spore, pågripe og domfelle gjerningsmennene. I den digitale verden kan angrepene automatiseres. Internett benyttes til å publisere angrepsverktøy og metoder, noe som fører til at det i mindre grad er behov for å ha tung kompetanse for å gjennomføre IT-baserte angrep. Dessuten er ikke Internett et fysisk område som kan kontrolleres – det finnes ingen landegrenser. Følgelig kan man sitte i et land og angripe en server på den andre siden av jordkloden [2].

1.1 Tema

Norske virksomheter, i likhet med utenlandske, vil med stor sannsynlighet, i all overskuelig fremtid, bli utsatt for datakriminelle hendelser. Det finnes for mange dyktige datakriminelle, for mange sårbarheter i nettverksløsninger, operativsystemer, applikasjoner etc., for lavt fokus på informasjonssikkerhet i virksomhetene og for stort potensial for økonomisk vinning for de kriminelle til at vi kan unngå dette. Det som kan endres er blant annet holdningen til det å anmelde datakriminalitet slik at man i større grad kan få straffet de som begår disse handlingene.

I denne oppgaven søker vi å beskrive omfanget av datakriminalitet som norske virksomheter utsettes for. Vi vil presentere erfaringer fra virksomheter som har anmeldt datakriminalitet. Videre vil vi vurdere om medlemskap i et sikkerhetsforum medfører at virksomheter har en mer bevisst holdning til datakriminalitet og informasjonssikkerhet enn de som ikke tilhører et slikt forum. Vi vil også søke å beskrive hva som kan gjøres for å få flere virksomheter til å anmelde datakriminalitet.

1.2 Nøkkelord

Informasjonssikkerhet, sikringstiltak, kontroll, rapportering, sikkerhetsledelse, data-kriminalitet, datainnbrudd, datatyveri, DoS-angrep, Copyright, infeksjon, hacking, orm, trojaner, virus, lovgivning, spørreundersøkelse, mørketall.

1.3 Problemstilling

Datakrimutvalget i Næringslivets sikkerhetsråd (NSR) offentliggjorde i september 2006 den 5. Mørketallsundersøkelsen. Undersøkelsen er basert på et spørreskjema som ble sendt ut til 2.000 norske virksomheter innen offentlig og privat sektor. Det var 749 virksomheter som besvarte undersøkelsen. Formålet med undersøkelsen var "*å kartlegge omfanget av datakriminalitet og andre uønskede IT-hendelser som norske virksomheter utsettes for. Offentlig statistikk forteller lite om disse forholdene, og det råder en generell oppfatning om at datakriminalitet og uønskede hendelser i liten grad anmeldes eller rapporteres til myndighetene*." [3].

Denne oppgaven har tatt utgangspunkt i det faktum at vi i 2006 fortsatt har behov for en mørketallsundersøkelse – det vil si at det fortsatt er en del norske virksomheter som ikke anmelder datakriminalitet de utsettes for.

Mørketallsundersøkelsen 2006 [3] ble gjennomført i april 2006. I forbindelse med spørsmål om datakriminelle hendelser (kartlegging av sikkerhetsbrudd) ble virksomhetene spurt om hendelser de hadde vært utsatt for i de siste 12 månedene. Vi har for enkelhetsskyld definert denne 12-månedersperioden som året 2005.

I Mørketallsundersøkelsen 2006 [3] estimeres det at det i 2005 ble begått ca. 3.900 vellykkede datainnbrudd som ble oppdaget. Statistikken for 2005 viser at bare 61 datainnbrudd ble anmeldt til politiet. Videre estimeres det i rapporten at det har vært ca. 8.900 tilfeller av misbruk av IT-ressurser. Bare 11 slike forhold ble anmeldt til politiet.

Hvorfor er ikke norske virksomheter i større grad villige til å anmelde datakriminalitet? Mørketallsundersøkelsen 2006 [3] viste at hovedårsaken var at virksomhetene mente at saken var ubetydelig. Dernest at det ikke ville være mulig å finne gjerningsmannen og at angrepet ikke var spesielt rettet mot virksomheten. Det var 8 svaralternativer som kunne benyttes og disse er redegjort for i kapittel 5.2. Det vil imidlertid være naturlig for oss å stille spørsmål om det er andre bakenforliggende årsaker enn de som ble benyttet i [3].

En utfordring vi har sett gjennom mangeårig arbeid med informasjonssikkerhet er at en del virksomheter som har dokumenterte planer for kontinuitet og krisehåndtering ikke har inkludert håndtering av datakriminelle hendelser i disse planene. Følgelig er de helt uforberedte når de utsettes for sin første hendelse, og det faktum kan også medføre en motvillighet eller reservasjon i forhold til å anmelde hendelsen, da det kan avsløre mangler og svakheter i virksomheten.

1.4 Motivasjon og begrunnelse

> *"Samfunnet blir i stadig større grad avhengig av IT, og trusselbildet endrer seg over tid. Vi ser en markert økning i identitetstyverier, og kompromitterte klienter og servere både hjemme og i virksomheter utnyttes av kriminelle. Det er i større grad organisert kriminalitet med økonomiske motiver som står bak." [3]*

Vår motivasjon for denne oppgaven var å bidra til å få flere virksomheter til å anmelde datakriminalitet.

Gjennom en spørreundersøkelse, bruk av datagrunnlaget fra Mørketallsundersøkelsen 2006 og intervjuer ønsker vi å belyse hvor omfattende datakriminalitet er og årsakene til at mange avstår fra å anmelde hendelsen.

I tillegg ønsker vi å se om det å være medlem av et sikkerhetsforum fører til at virksomheter i større grad implementerer formelle og tekniske sikringstiltak og om det fører til en mer bevisst holdning til datakriminalitet og anmeldelse.

Videre ønsker vi å vurdere hvilke mulige tiltak som kan iverksettes for å få flere virksomheter til å anmelde datakriminelle hendelser. Vi vet av erfaring at mange virksomheter er usikre på hva de skal gjøre dersom de utsettes for datakriminalitet. Med utgangspunkt i dette har vi sett at det kan være behov for en veiledning i forhold til anmeldelse av datakriminalitet. Vi har også sett et behov for en veiledning i hvordan virksomheter skal forholde seg dersom de har mistanke om at en hendelse har skjedd – eksempelvis i forhold til sikring av elektroniske bevis. Dette ble bekreftet gjennom våre intervjuer.

Oppgaven er skrevet på oppdrag fra Norsk Senter for Informasjonssikring (NorSIS). NorSIS jobber for å bedre informasjonssikkerheten og redusere sårbarheten for informasjons- og kommunikasjonsteknologi i samfunnet generelt. Deres målgruppe er primært små og mellomstore virksomheter i privat og offentlig sektor, herunder kommunene. NorSIS jobber for å bevisstgjøre om trusler, å opplyse om sikringstiltak og å påvirke til gode holdninger gjennom forebyggende aktiviteter [4].

1.5 Forskningsspørsmål

De forskningsspørsmålene det i denne oppgaven søkes svar på, er følgende:

1. Hvor stort er omfanget av datakriminalitet i Norge?
2. Hvorfor anmelder ikke flere virksomheter datakriminalitet?
3. Hva skjer dersom datakriminalitet anmeldes?
4. Hva kan gjøres for å få flere til å anmelde datakriminalitet?
5. Håndteres informasjonssikkerhet forskjellig blant ISF-medlemmer og Mørketallsundersøkelsens respondenter?

Spørsmål 1 søkes besvart gjennom statistisk behandling av resultatene fra spørreundersøkelsen som ble foretatt blant ISF-medlemmer og resultatene fra Mørketallsundersøkelsen 2006.

Spørsmål 2 søkes besvart gjennom statistisk behandling av resultatene fra spørreundersøkelsene, i tillegg til resultater fra intervjuer.

Spørsmål 3 søkes besvart ved hjelp av intervjuene vi har gjennomført.

Spørsmål 4 skal besvares ved hjelp av intervjuene vi har gjennomført i tillegg til at vi har sett på hvordan dette er forsøkt løst i andre land.

Spørsmål 5 skal besvares gjennom sammenligning av resultatene fra ISF-undersøkelsen og Mørketallsundersøkelsen.

1.6 Avgrensning

Denne oppgaven har ikke som mål å gjennomføre en spørreundersøkelse i samme omfang som Mørketallsundersøkelsen 2006 [3].

Det har ikke vært oppgavens å mål gjennomføre en analyse av utviklingen av mørketallene i forhold til tidligere års rapporteringer.

Det har heller ikke vært oppgavens intensjon å presentere en diskusjon av effekten av dagens lovverk og straffebud for datakriminelle saker. Vi har heller ikke valgt å diskutere de nylig foreslåtte lovtiltak mot datakriminalitet.

2. Relatert arbeid

"Computer security is a kind of game between two parties, the designer of a secure system, and a potential attacker."

Jajodia and Miller [5]

I dette kapitlet presenterer vi innledningsvis en redegjørelse for lovgiving knyttet til datakriminalitet – nåværende straffebud og forslag til nye straffebud. Deretter presenterer vi resultater fra undersøkelser om informasjonssikkerhet og datakriminalitet i andre land og sammenligner disse med tilsvarende resultater fra Norge. Så presenterer vi hva politimyndigheter i andre land gjør for å få virksomheter til å anmelde datakriminalitet og hva som er gjort av arbeid i forhold til veiledninger for håndtering av datakriminelle hendelser. Dernest ser vi litt på utviklingen innen datakriminalitet og hvilke trender som er fremtredende. Til slutt i kapitlet presenterer vi en oppsummering av kapitlet.

Det vil i dette kapitlet bli presentert informasjon som vi fikk i intervju med en representant fra Kripos og denne informasjonen er merket som "[Kripos]".

2.1 Datakriminalitet og lovgivning

I dette kapitlet presenterer vi i korthet nåværende lovgivning for datakriminalitet og forslag til nye straffebud i ny straffelov. Vi har som nevnt i kapittel 1.6 Avgrensning, valgt å ikke diskutere forslag til nye straffebud, men velger å presentere dem fordi vi mener at dette er et positivt signal om at lovgivende myndigheter begynner å ta datakriminalitet på alvor.

Gjennom arbeidet med denne oppgaven, har vi fra Kripos fått tilsendt noen av dommene som har vært avsagt i sammenheng med datakriminelle forhold i de senere årene. I Appendiks C vises en oppsummering av disse dommene. Av dommene fremgår det at det ofte er flere straffebud som er gjenstand for en dom. Videre kan vi til en viss grad konkludere at det økonomiske tapet som er påført fornærmede er innvirkende på straffen. Det er dog ikke nevnt økonomisk tap i alle dommene som vi har sett på.

Vi har forsøkt å få tak i statistikk over domfellelser knyttet til datakriminelle forhold for 2004-2006, men har ikke lykkes med dette.

2.1.1 Nåværende lovgivning

I dag er det Straffeloven, "Almindelig borgerlig Straffelov" [6], som regulerer datakriminelle forhold. I politiets straffesaksregister, STRASAK, benyttes følgende paragrafer [3] i Straffeloven:

§ 145, 2. ledd Inntrenging i og avlytting av dataanlegg/-system (datainnbrudd)
§ 151b Rettsstridig forføyning datasystem (ulovlig bruk - stort omfang)
§ 261 Ødeleggelse av dataavhengige samfunnsviktige installasjoner (sabotasje)

§ 270, 1. ledd nr 2 Forandring, manipulering datasystem (databedrageri)
§ 294 Misbruk datalagret forretningshemmeligheter (industrispionasje)
§ 291 Skadeverk på datalagringsmedier
§ 292 Grovt skadeverk på datalagringsmedier
§ 317 Heleri datainformasjon
§ 391, 2. ledd Uaktsomt grovt skadeverk på datalagringsmedier
§ 393 Rettsstridig forføyning datasystem (ulovlig bruk - mindre omfang)
§ 405a Innsyn i datalagret forretningshemmelighet (industrispionasje)

I Appendiks C redegjør vi for hvordan vi har kategorisert disse straffebestemmelser i forhold til datakriminelle hendelser (forhold) vi har omhandlet i denne oppgaven.

I januar 2002 ble Datakrimutvalget opprettet ved kongelig resolusjon. Utvalget skulle utrede "Lovtiltak mot datakriminalitet". Utvalget har avgitt 2 delutredninger. Den første utredningen omhandlet "*de endringer som var nødvendige å foreta i norsk rett for å ratifisere Europarådets konvensjon av 8. november 2001 (datakrimkonvensjonen 185 ETS)* [7]. Konvensjonen omhandler bekjempelse av kriminalitet knyttet til informasjons- og kommunikasjonsteknologi. Denne konvensjonen er gjennomført i norsk rett og trådte i krav med virkning for Norge per 01.10.2006. Justis- og politidepartementet fulgte opp utredningen i Odelstingsproposisjon nr. 40 (2004-2005) *"om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon*. Dette resulterte i endringslov 08.04.2005 nr. 16 som trådte i kraft umiddelbart.

2.1.2 Fremtidig lovgivning

Straffeloven er stadig gjenstand for endringer for å reflektere nye typer av kriminalitet som begås, og dette har også vært gjeldende for datakriminalitet. Datakrimutvalget sier i sin andre utredning at dagens regler om datakriminalitet er uttilstrekkelige og at det er behov for presiseringer og nykriminalisering [8]. Uttilstrekkeligheten i forhold til dagens regler har eksempelvis medført at kodingen av datakriminelle hendelser i STRASAK ikke alltid har vært korrekt. Dette er spesielt gjeldende for politidistriktene [Kripos]. I tillegg vil vi som legfolk våge påstanden om at det heller ikke kan være så enkelt for alle virksomheter å finne ut av de forskjellige straffebudene.

I Storbritannia anslås at 1 av 4 politidistrikter ikke kan generere oversikt over datakriminalitet (anmeldte saker). Dette henger sammen med at lovgivningen ikke er tilstrekkelig og at datakriminalitet ikke kodes separat, noe som gjør det vanskelig for myndigheter og politiet å kunne vise reelle statistikker over datakriminalitet [9].

Datakrimutvalgets andre utredning [8] ble oversendt Justis- og politidepartementet den 12. februar 2007 og deretter sendt ut på høring med høringsfrist satt til 25. mai 2007. I henhold til utvalgets mandat skulle de utrede hvilke endringer som burde gjøres i straffelovgivningen og utforme forslag som kunne tas inn i en spesiell del av en ny straffelov. Videre i mandatet står det at *"Utvalget bes særskilt om å vurdere*

- *om bestemmelsene om lovens stedlige virkeområde i den nye straffelovens alminnelige del gir hensiktsmessige avgrensninger når det gjelder ulovlig materiale på internett, jf. Ot.prp. nr. 90 (2003-2004) side 167 flg., og eventuelt foreslå særregler,*
- *om data og datasystemer har et tilstrekkelig strafferettslig vern etter dagens regler, og eventuelt hvordan vernet bør forbedres,*

- *om den gjeldende straffeloven i tilstrekkelig omfang og tilstrekkelig strengt straffer handlinger som begås ved misbruk av data og datasystemer, og*
- *hvilke lovendringer som er nødvendige for at Norge skal kunne ratifisere tilleggsprotokollen 28. januar 2003 til Europarådskonvensjonen om IKT-kriminalitet (om kriminalisering av rasistiske og fremmedfiendtlige handlinger begått i et datasystem) [...]*
- *om å utrede og foreslå straffeprosessuelle regler om dataavlesing, jf. Ot.prp. nr. 60 (2004-2005) side 141-142 med videre henvisninger.*
- *i tillegg til hensynet til samfunnsbeskyttelse vurdere rettssikkerhetsmessige aspekter og hensynet til personvern og ytringsfrihet. Ved drøftelsen av enkeltspørsmål skal utvalget gjøre rede for hvordan disse hensynene berøres og for hvordan disse hensynene bør veies mot hverandre."*

Videre hadde utvalget et ønske å kartlegge lovgivningen i andre land for å oppnå harmonisering av straffelovgivningen, men tiden de hadde til disposisjon tillot ikke dette. Mye av datakriminaliteten som foregår, skjer på tvers av nasjonale grenser, så en harmonisering av straffelovgivningen kan ha betydelig innvirkning på effektiviteten i forhold til internasjonal samarbeid. I delutredning 2 skriver de at det ligger betydelig utfordringer i straffeforfølging på tvers av landegrensene og at det ofte er vanskelig å identifisere forbrytere. Dersom man klarer å identifisere dem kan de befinne seg i land hvor de ikke kan straffeforfølges eller som ikke vil utlevere vedkommende til et annet land [8]. I 2004 foretok Nasjonal Sikkerhetsmyndighet (NSM) en analyse av 205 koordinerte angrep (et angrep representerte opptil flere hendelser) mot norske virksomheter. Det viste seg at bare 4,4 % kom fra Norge [10]. Dette illustrerer hvor vesentlig internasjonalt samarbeid er for oppklaring av datakriminelle saker.

I Kapittel 11 i delutredning II presenteres utvalgets lovforslag [8]:

- *Straffebud som rammer elektronisk kartlegging av sårbarheter på et datasystem (§ 2).*
- *Straffebud som rammer ulovlig anbringelse av utstyr eller dataprogram på eller i tilknytning til et datasystem eller elektronisk kommunikasjonsnett (§ 3).*
- *Straffebud som rammer ulovlig tilgang til hele eller del av et datasystem (§ 4).*
- *Straffebud som rammer tyveri av informasjon og data (§§ 5 og 6).*
- *Straffebud som rammer uberettiget endring, ødeleggelse, sletting eller skjuling av andres data (§ 7).*
- *Straffebud som rammer uberettiget bruk av andres datasystem eller elektroniske kommunikasjonsnett (§ 8).*
- *Straffebud om etterfølgende befatning med ulovlig tilegnet data og informasjon (§ 9).*
- *Straffebud som rammer uberettiget befatning med passord, adgangskode, krypteringsnøkkel eller lignende som kan gi tilgang til data, databasert informasjon eller datasystem (§ 10).*
- *Straffebud som rammer befatning med dataprogram eller utstyr som er særlig egnet til å begå straffbare handlinger (flertallsforslag i § 11).*
- *Straffebud som rammer rettsstridig befatning med selvspredende dataprogram, eller initiert spredning av slikt program (§ 12).*
- *Straffebud som rammer handlinger som vesentlig hindrer eller er egnet til vesentlig å hindre driften av et datasystem eller elektronisk kommunikasjonsnett (§ 13).*
- *Straffebud som rammer ulovlig masseutsendelse av elektroniske meldinger (spam) til mottakere som ikke har samtykket (§ 14).*

- *Straffebud som rammer identitetstyveri eller uberettiget bruk av uriktig identitet ved elektronisk kommunikasjon (§ 15).*
- *Straffebud som rammer den som med forsett om vinning uberettiget disponerer en konto som tilhører en annen, ved å gi opplysninger til et datasystem og derved volder tap eller fare for tap for noen (kontomisbruk - § 16).*

Utvalget har også foreslått endringer i ny straffelov, markedsføringsloven og åndsverkloven.

2.2 Informasjonssikkerhet – en modningsprosess

Informasjonssikkerhet og informasjonssikring er en modningsprosess for mange virksomheter. På mange måter kan dette sammenlignes med Trygg Trafikks mangeårige kampanje for bedre sikring i bil. Går man 40 år tilbake i historien var det sjelden bruk av bilbelter, og bruk av barneseter var et ukjent fenomen. Nå er dette påbudt og sikkerhet i biler er blitt et konkurransefortrinn.

En internasjonal spørreundersøkelse utført av Ernst & Young i 2006 [11] slår fast at virksomhetenes ledelse er i en modningsprosess. De setter i økende grad informasjonssikkerhet på dagsorden og kravet om etterlevelse av lover og forskrifter er en vesentlig bidragsyter til dette. Videre slår de fast at virksomheter i de senere årene har gjort betydelige investeringer i forhold til informasjonssikkerhet. Dette er representert ved at virksomheter ansetter flere medarbeidere innen informasjonssikkerhetsområdet, det utarbeides og implementeres formelle policyer/retningslinjer og det investeres i tekniske sikringstiltak som eksempelvis tilgangskontroll, IDS og antivirusløsninger.

I en undersøkelse foretatt blant britiske virksomheter [12] konstateres det at 3 av 4 respondenter mener at informasjonssikkerhet har høy eller veldig høy prioritet blant ledelse og styre. I løpet av de siste 6 årene har antallet virksomheter som har en formell informasjonssikkerhetspolicy blitt tredoblet. I gjennomsnitt brukes 4-5 % av IT-budsjettet på informasjonssikring [12].

2.3 Tekniske sikringstiltak – Norge vs andre land

Det er positive signaler at virksomheter i større grad tar informasjonssikkerhet på alvor, men utfordringene er store og økende. Blant annet oppdages det stadig nye sårbarheter i nettverksløsninger, operativsystemer, applikasjoner etc. Her representert ved CERTs statistikk over sårbarheter per 1. kvartal 2007 [13]:

Year	2000	2001	2002	2003	2004	2005	2006	Q1, 2007
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	8,064	2,176

Tabell 1: CERTs statistikk over sårbarheter per 1. kvartal 2007

Av disse antas det at følgende antall er kritiske sårbarheter:

Year	2000	2001	2002	2003	2004	2005	2006	Q1,2007
Vulnerability Notes	47	326	375	255	341	285	422	150

Tabell 2: CERTs statistikk over kritiske sårbarheter per 1. kvartal 2007

Dette medfører at ikke bare oppdages det flere sårbarheter, men at disse også i økende grad er kritiske. Dette er selvfølgelig også informasjon som er kjent for de som ønsker å utføre datakriminelle handlinger. I følge Symantec [14] blir 25 % av programmer for å utnytte sårbarheter (sikkerhetshull) publisert på Internett mindre enn 24 timer etter at sårbarhetene er gjort kjent. Ytterligere 31 % av programmer for å utnytte sårbarheter publiseres innen de 6 neste dager etter at det er blitt kjent.

I perioden 1992-95 gjennomførte U.S. Departement of Defense's Defense Information Systems Agency (DISA) 38.000 angrep mot departementets IT-systemer for å teste sikkerheten [15]. Av disse angrepene var 65 % vellykkede angrep (de resterende ble blokkert av brannmurer). Hele 96 % av de vellykkede angrepene ble ikke oppdaget. Av de resterende 4 % som ble oppdaget ble kun 27 % rapportert.

Videre estimerte DISA at de kunne ha vært utsatt for 250.000 uoppdagede dataangrep i 1995 og at antallet angrep bare ville øke [16]. Dette er i seg selv svært urovekkende opplysninger spesielt med tanke på at dette var i den spede begynnelse av Internett. I 2002 estimerte FBI's National Computer Crime Squad at mellom 85 og 97 prosent av alle datainnbrudd ikke oppdages [17].

Vi har gjennom arbeidet med denne oppgaven funnet undersøkelser fra andre land vedrørende implementerte sikringstiltak og vi har valgt å sammenligne med disse undersøkelsene med Mørketallsundersøkelsen 2006 [3]. Undersøkelsene viser at nesten alle virksomhetene i Norge [3], Australia [18] og USA [19] har implementert brannmurløsninger som ett av sikringstiltakene. Når det gjelder systemer for å detektere innbrudd (IDS) har amerikanske virksomheter [19] implementert slike i en mye større grad enn norske virksomheter [3] – 69 % mot 15,9 %. Hele 43 % av amerikanske virksomheter [19] har implementert IPS-løsninger (Intrusion Prevention System) – dette spørsmålet ble verken stilt i den norske eller den australske undersøkelsen.

Tabell 3 viser oversikt over sikringstiltak som er gjennomført, blant de norske [3], australske (AusCert) [18] og amerikanske virksomhetene (CSI/FBI) [19]:

	MU	AusCert	CSI/FBI
Virtuelt privat nettverk (VPN)	47,3 %	86,0 %	
Filter mot uønsket e-post (Spamfilter)	76,9 %	90,0 %	
Innbruddsdetekteringssystem (IDS)	15,9 %	44,0 %	69,0 %
Digital signatur	5,9 %	47,0 %	36,0 %
Brannmur for nettverket	89,6 %	98,0 %	98,0 %
Biometrisk autentisering (f.eks. fingeravtrykk)	2,5 %	5,0 %	20,0 %
Antivirusprogramvare	92,5 %	98,0 %	97,0 %

Tabell 3: Tekniske sikringstiltak – Norge vs andre land

2.4 Datakriminalitet anmeldes ikke – Norge vs andre land

I dette kapitlet presenterer vi en sammenligning mellom Mørketallsundersøkelsen 2006 [3] og tilsvarende undersøkelser fra Sverige [20], Australia [18] og USA [19] vedrørende årsaker til at datakriminalitet ikke anmeldes.

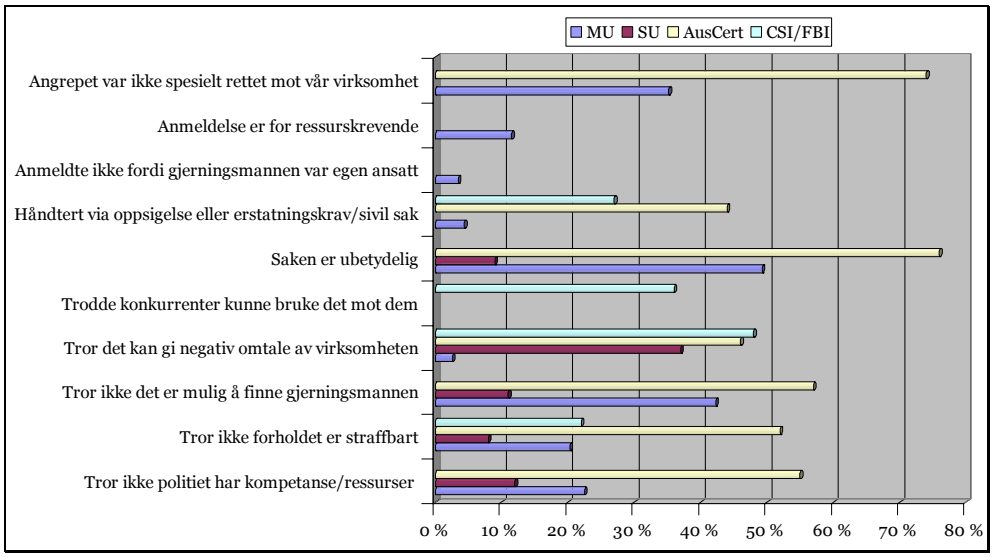
I den svenske mørketallsundersøkelsen for 2005 [20] har man stilt spørsmål om virksomhetene ville anmelde datakriminelle hendelser. Der viser det seg at 39 % har svart at de i de fleste tilfellene ville anmelde datainnbrudd. Videre har 58 % har svart at de i de fleste tilfellene ville anmeldt kartlegging av sårbarheter i IT-systemene. 38 % ville i de fleste tilfellene anmelde DoS-angrep og 44 % ville i de fleste tilfellene ha anmeldt infeksjon av virus/orm/trojaner. Dette kan virke litt motstridende mot de faktiske forholdene, siden bare 5 % av middelsstore virksomheter har svart at de har anmeldt datakriminalitet og bare 4 % av de store virksomhetene har gjort det samme. I tilsvarende undersøkelser gjort blant australske virksomheter i 2006 [18] viser det seg at 22 % valgte å anmelde datakriminalitet.

I Mørketallsundersøkelsen 2006 [3] oppgir 49 % av virksomhetene at hovedårsaken til at de ikke anmelder datakriminalitet er at saken var ubetydelig. Det tilsvarende tallene fra 2003 [21] og 2001 [22] var henholdsvis 35 % og 15 %. I 2006 og 2003 var dette hovedårsaken til at virksomhetene ikke anmeldte, mens den i 2001 kom på andreplass etter "vet ikke" som hadde hele 23 %. I Sverige [20] oppgir bare 9 % at saken var ubetydelig, mens i den australske undersøkelsen [18] oppgir hele 73 % at hendelsen ikke var alvorlig nok.

En undersøkelse i Storbritannia [12] anser at tap av omdømme kan ha større økonomiske konsekvenser enn de direkte økonomiske tapene virksomhetene kan få som følge av at de har vært utsatt for en datakriminell hendelse. Dersom det er en kjent virksomhet som har vært utsatt for datakriminalitet, er det også større sannsynlighet for at mediene vil være interessert i å omtale saken. Det er følgelig interessant at frykt for tap av omdømme ikke spiller noen vesentlig rolle i Norge [3], da bare 2,6 % oppgir dette som årsak til at de ikke anmeldte. Både i Sverige [20] og USA [19] er dette oppgitt som den viktigste årsaken til at virksomhetene ikke anmeldte, med henholdsvis 37 % og 48 %. I Australia [18] var fare for tap av omdømme årsaken til at 46 % ikke ville anmelde.

Det er også verdt å merke seg at 52 % av de australske virksomhetene [18] ikke trodde at forholdet var straffbart, mens bare 8 % av de svenske virksomhetene [20] svarte det samme. De norske og amerikanske virksomheter hadde tilnærmet oppfatning i forhold til dette spørsmålet med henholdsvis 20,3 % [3] og 22,0 % [19].

I Figur 1 vises årsakene til at virksomhetene i Norge (MU) [3], Sverige (SU) [20], Australia (AusCert) [18] og USA (CSI/FBI) [19] ikke valgte å anmelde, og som det fremgår av tabellen er ikke de samme årsakskategoriene benyttet i alle undersøkelsene:



Figur 1: Årsaker til at datakriminalitet ikke anmeldes – Norge vs andre land

2.5 Datakriminalitet – informasjon og anmeldelse

I en del land har politimyndighetene tatt i bruk Internett for å få flere til å anmelde eller rapportere datakriminalitet. Noen har lagt ut webbaserte skjemaer for formålet. Andre har lagt ut utfyllende informasjon om datakriminalitet og informasjon om hvem som skal kontaktes dersom man ønsker å anmelde en hendelse. I noen tilfeller er det også lagt ut veiledninger i forhold til hvordan virksomhetene kan sikre elektroniske bevis.

Et godt eksempel vi fant, gjennom vårt arbeid med denne oppgaven, var websidene hos Florida Departement of Law Enforcement. På sin hovedside har de lagt ut en lenke til Florida Computer Crime Center og informasjon om datakriminalitet, i tillegg til et skjema som kan fylles ut for å rapportere [23].

På hovedsiden til Metropolitan Police i Storbritannia finnes lenker til anmeldelse av hendelser. Der er det lenket videre til deres Computer Crime Unit [24] hvor det finnes informasjon om anmeldelse av datakriminalitet (diverse kategorier) i tillegg til en lenke til UNIRAS (Unified Incident Reporting & Alert Scheme), UK Government's computer emergency response team hvor virksomhetene også kan rapportere hendelser [25].

Det amerikanske justisdepartementet (Departement of Justice) har en egen side med opplysninger om hvem som kan kontaktes dersom man har vært utsatt for data-kriminelle handlinger – henholdsvis FBI, U.S. Secret Service eller IC3 (Internet Crime Complaint Center) [26].

Kripos har på sine websider et lite avsnitt om Datakrimavdelingen og dens funksjon, men det finnes ingen utfyllende informasjon om datakriminalitet eller henstilling om å anmelde. Følgelig finnes det ei heller informasjon om hvem som det bør anmeldes til. [27]

I flere land er det etablert såkalte CERT (Computer Emergency Response Team). Disse har også i varierende grad lagt ut informasjon og skjemaer for direkterapportering av datakriminalitet. Gjennom våre undersøkelser har vi funnet at australske AusCert er av de CERT-ene som har gjort mest på dette området. På deres websider er det detaljert informasjon om datakriminalitet, i tillegg til et elektronisk skjema for å rapportere hendelser [28]. Sveriges CERT – Sitics har også websider med utfyllende informasjon om rapportering av hendelser og et elektronisk skjema for rapportering [29]. Tilsvarende finnes også i USA på Internet Crime Complaint Center (IC3) sine websider [30].

I Norge har NorCert på sine websider oppgitt en e-postadresse for rapportering av hendelser og lagt ut informasjon om hva de har ansvar for [31].

2.6 Håndtering av datakriminelle hendelser

Vi har funnet at det i noen land er gjort en del arbeid fra politimyndighetenes side for å opplyse om hvordan man skal håndtere datakriminelle hendelser. Noen har også valgt å legge ut veiledninger på Internett om håndtering av datakriminelle hendelser og hvordan elektroniske bevis bør sikres. Eksempelvis har US Secret Service lagt ut guiden "Best Practices for Seizing Electronic Evidence" [32]. I Storbritannia har National Hi-Tech Crime Unit (NHTCU) og Association of Chief Police Officers laget en veiledning for sikring av elektroniske bevis, "Good Practice Guide for Computer based Electronic Evidence", som ligger tilgjengelig på Internett [33]. Ministry of Managed Services i kanadiske British Columbia har lagt ut en presentasjon om hvordan elektroniske bevis skal innsamles og håndteres [34]. Disse veiledningene er i første rekke ment for polititjenestemenn, men informasjonen som er presentert er også relevant dersom en virksomhet selv ønsker å sikre elektroniske bevis.

Det britiske Centre for the Protection of National Infrastructure (CPNI), har laget en veiledning for hvordan man kan være foreberedt på etterforskning av en datakriminell hendelse. Den gir et rammeverk for hva som bør være dokumentert, implementert og testet i forbindelse med håndtering av en etterforskning. I stor grad kan veiledning sammenlignes med rammeverk som ofte lages ved utvikling av kontinuitets- og kriseplaner. Veiledningens konsept er at man skal være forberedt og vite hva som skal gjøres dersom noe hender [35].

Det er også en rekke andre organisasjoner som har laget veiledninger for sikring av elektroniske bevis, eksempelvis Australske AusCert [36], Dansk IT [37] og TechRepublic [38].

Detaljeringsgraden i de forskjellige veiledningene er varierende, men det er oftest det samme konseptet som går igjen. Vesentlig for all etterforskning av datakriminalitet er at det finnes bevis å sikre. Virksomhetene må ha aktivisert logging av aktiviteter på servere, nettverkskomponenter, brannmurer, IDS-er etc. Disse loggene må sikres slik at de ikke overskrives (dersom de går fulle) og ikke kan manipuleres. Noen av veiledningene går også inn på fysisk sikring av utstyr og lokaler.

2.7 Datakriminalitet – senere års utvikling

"Folk som tidligere angrep datasystemer gjorde det for moro skyld, men nå er trenden snudd på hodet. Det er de som er interessert i økonomisk vinning som står bak truslene."

Christophe Birkeland, avdelingsdirektør i NorCERT [39]

"Trendene viser at datakriminaliteten blir mer organisert og internasjonal, og at det foreligger tydeligere vinningsmotiv. ... Det er vanskelig å bekjempe og etterforske datakriminalitet over landegrenser fordi det er enklere å anonymisere seg."

Kripos årsrapport for 2006 [40]

Datakriminalitet er i ferd med å bli god forretning og benyttes i økende grad av organiserte miljøer. Det anslås at de største miljøene har tilhørighet i Russland, tidligere Øst-Europa og Brasil, men det er også en del syndikater som har etablert seg i Asia. Det er så mye penger å tjene på datakriminalitet at det også finnes IT-sikkerhetseksperter som mener at terrorister bruker dette til å finansiere sine aksjoner og organisasjoner. Ingen av disse ekspertene er villige til stå frem med fullt navn av frykt for egen sikkerhet, og det er dessuten en del uenighet om hvorvidt dette er korrekt [41]. I følge det britiske National Infrastructure Security Coordination Centre (NISCC) er sannsynligheten for at terrorister benytter datakriminalitet for å angripe nasjonal infrastruktur lav sammenlignet med risiko for bombeangrep, men de påpeker at trusselen kan endre seg [9]. I 2004 ble sentrale servere til det nederlandske regjeringsapparatet utsatt for datainnbrudd og DoS-angrep (tjenestenektangrep). Dette anses for å være det første kjente politisk motiverte dataangrepet [42].

Organiserte kriminelle miljøer i økende grad tar i bruk bot-nettverk. Bot er en forkortelse av robot og er "kaprede" maskiner som er infisert med virus/trojanere. Bot-nettverk benyttes til å spre ondsinnet kode (virus, orm og trojanere), spam (uønsket reklame) og i økende grad til å gjennomføre DoS-baserte utpressingsforsøk (DoS – Denial of Service – tjenestenektangrep) [43]. Under en paneldiskusjon om Internetts fremtid ved World Economic Forum i Davos uttalte Vint Cerf, en av grunnleggerne av Internett, at av 600 millioner maskiner som i dag er koblet til Internett kan mellom 100 og 150 millioner være en del av forskjellige bot-nettverk [44]. Dette estimatet er det en del diskusjoner om og en del sikkerhetseksperter hevder at tallet er for høyt [41]. Symantec observerte i perioden juli-desember 2006 et gjennomsnitt på 63.912 bot-infiserte maskiner per dag. I samme periode observerte de 6.049.594 unike bot-infiserte maskiner – en økning på 29 % fra perioden januar-juni 2006 [43].

Personer som tidligere lagde ormer og virus, tjener nå store summer på å lage kode til bot-nettverk. Det hevdes at det er stort marked for kjøp og salg av verktøy og kode som kan benyttes til å stjele informasjon, sende spam og å jamme nettverk (redusere tilgjengeligheten til IT-systemene). I 2006 ble det verifisert at et bot-nettverk besto av 20 millioner maskiner [45].

I 2006 ble 3 russere arrestert for pengeutpressing av virksomheter som drev med Internett-basert gambling. De var en del av et miljø på 16 kriminelle som benyttet bot-nettverk til stoppe nettverkstrafikken til virksomhetene. I følge bevisene som ble fremlagt i retten "tjente" de $3,9 millioner på utpressingen. I russiske medier ble det estimert at det totale økonomiske tapet for virksomhetene hadde vært $79 millioner. De 3 russerne ble dømt til 8 års fengsel [41].

I 2005 ble mer enn 50 brasilianere arrestert for å ha tilegnet seg $33 millioner ved å bruke trojanere til å stjele nettbankpassord. I en annen sak ble 100 brasilianere arrestert for å ha tilegnet seg tilgang til 10.000 brasilianske bankkontoer. I følge en brasiliansk IT-ekspert arresteres bare 4 til 5 prosent av de som står bak slike datakriminelle handlinger i Brasil [41].

I noen tilfeller er datakriminalitet benyttet som hevn. I 2006 følte en russisk spammer, PharmaMaster, at "virksomheten" hans var truet av Blue Security, en virksomhet som drev med antispam. Han angrep og tok ned Blue Securitys websted. Firmaet la ut informasjon om angrepet på en blogside som ble drevet av TypePad, eid av Six Apart Ltd. PharmaMaster leide da en "bot herder" (bestyrer av et bot-nettverk) til å gjennomføre et DoS-angrep som tok ned alle Six Aparts blogger, inklusive de som ble drevet av TypePad. Blue Security kapitulerte til slutt og la ned virksomheten. PharmaMaster betalte bot-bestyreren $1 million for å gjennomføre angrepet, og dette beløpet er ikke så stort med tanke på at han tjente $3 millioner på spam hver måned. I følge sikkerhetseksperter var angrepet så alvorlig at bare de aller største av verdens virksomheter kunne ha stått imot [41].

I Norge har en rekke nettbankkunder, tilhørende forskjellige banker, vært utsatt for nettbanksvindel. Svindlerne benyttet mellommenn som de hadde rekruttert gjennom en webside, til å opprette kontoer. Fremgangsmåten for svindelen var å infisere kundenes pc-er med trojanere slik at det når kunden logget seg på nettbanken ble det overført penger til mellommennenes kontoer. Når det var blitt overført penger til disse kontoene tok mellommennene ut pengene og sendte de videre slik at de tilslutt havnet hos bakmennene for angrepet [46,47,48].

I Kredittilsynets Risiko- og sårbarhetsanalyse (ROS) 2006 slås det fast at "*det ikke er tvil om at det vil komme nye angrep av organisert kriminalitet og at noen vil lykkes*" [49]. De konstaterer også at organisert datakriminalitet mot finansnæringen er økende. Kundenes egne pc-er anses for å være det svakeste leddet. Et utsagn i ROS-analysen som vi finner noe spesielt er: "*Det er viktig å ligge foran de kriminelle med tiltak.*" [49] Historien har til nå vist at de datakriminelle hele tiden har ligget et hakk foran de som jobber for å beskytte informasjonssystemene. Ikke minst illustreres dette gjennom at det til stadighet oppdages nye og kritiske sårbarheter i operativsystemer, nettverksløsninger og applikasjoner, og at det raskt publiseres informasjon om hvordan disse sårbarhetene kan utnyttes. Dette er spesielt en utfordring for store virksomheter, fordi de ofte har store og komplekse IT-løsninger. Følgelig kan ikke patcher (oppdateringer) installeres umiddelbart når de foreligger, men det må gjennomføre rigorøs testing for å sikre at applikasjonene fungerer tilfredsstillende etter patchingen.

2.8 Oppsummering

De nåværende straffebudene for datakriminalitet er uttilstrekkelige og dette kan medføre at eksempelvis statistikker over anmeldte saker blir ukorrekte som en følge av feilkoding i STRASAK. Videre kan det være vanskelig for virksomheter å finne ut av hvilke hendelser som anses for å være straffbare og som følgelig bør anmeldes. Vi stiller oss positive til den nye lovgivningen som er foreslått i Datakrimutvalgets 2. delutredning [8]. Det er likevel beklagelig at det ikke i større grad har vært mulig å harmonisere lov-

givningen med andre lands lovgivning, slik at den kan reflektere at mange av de datakriminelle handlingene begås av gjerningsmenn som befinner seg i andre land.

Krav til etterlevelse av lover og forskrifter fører til at virksomheter i større grad gjør investeringer for å bedre informasjonssikkerheten. Når vi sammenligner Norge med land som USA og Australia ser vi at norske virksomheter i mindre grad har implementert sikringstiltak enn det som er tilfelle for virksomheter i disse landene.

I forbindelse med årsaker til at virksomheter ikke anmelder datakriminalitet har vi sett at det er en del forskjeller mellom Norge og de landene vi har sammenlignet med. Dette gjelder ikke minst i forhold til tap av omdømme, hvor norske virksomheter i liten grad frykter dette, mens det er en vesentlig faktor i de andre landene.

Politimyndigheter i enkelte andre land er langt mer aktive enn Kripos i forhold til å få virksomheter til å anmelde. Dette er gjort gjennom å bruke Internett for å informere om datakriminalitet, gi mulighet til å anmelde, informasjon om hvem som kan kontaktes og veiledninger for å håndtere en hendelse.

Avslutningsvis har vi sett at det er en oppadgående trend at datakriminalitet begås av organiserte miljøer og at årsaken til dette er ganske enkel - det er mye penger å tjene.

3. Metodevalg

3.1 Forskningsstrategi

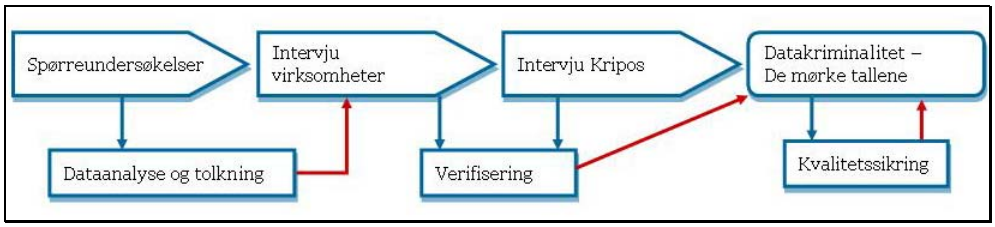
Metodevalget for gjennomføring av denne oppgaven har vært en kombinasjon av kvantitativ og kvalitativ metode – "mixed study" [50]. Ved å gjennomføre en spørreundersøkelse og å benytte dataene fra Mørketallsundersøkelsen 2006 [3] har vi fått et bredt datagrunnlag for blant annet å analysere typer av hendelser som norske virksomheter har vært utsatt for. Videre har vi kunnet analysere årsaker til at de ikke velger å anmelde datakriminalitet og mer generelt, norske virksomheters forhold til informasjonssikkerhet.

Hovedkilden for den kvantitative delen av forskningen har vært datagrunnlaget fra Mørketallsundersøkelsen 2006 (dette datagrunnlaget vil heretter bli omtalt som MU) og datagrunnlaget fra en undersøkelse foretatt blant ISFs medlemmer – IT-SikkerhetsForum (dette datagrunnlaget vil heretter bli omtalt som ISF-U). ISF-U hadde 31 respondenter mot MUs 749. Følgelige har vi ansett ISF-U for være en referanseundersøkelse og ikke en like fullverdig undersøkelse som MU.

Basert på teorier og synspunkter vi har dannet oss ut fra analyser av datagrunnlaget, har vi gjennomført intervjuer med virksomheter som har anmeldt datakriminalitet – kvalitativ metode. Med utgangspunkt i resultatene fra disse intervjuene gjennomførte vi et intervju med Kripos. I tillegg har vi lykkes i å få noen innspill fra en person som tidligere har vært datakriminell.

Dette har i stor grad vært en sekvensiell studie – det vil si at den kvantitative delen ble gjennomført før den kvalitative ble påbegynt.

Prosessen frem til rapportens skriftlige resultat er beskrevet i Figur 2.



Figur 2: Prosessen

3.2 Definisjoner

3.2.1 Datakriminalitet

Begrepet datakriminalitet har ingen entydig juridisk definisjon, men beskriver en modus – en måte – å begå datakriminalitet på [3].

I straffeloverådets utredning om datakriminalitet fra 1985 [51] ble datakriminalitet definert som følger:

> *"Datakriminalitet skulle etter dette være straffbare handlinger hvor utnyttelsen av datateknologi har vært vesentlig for overtredelsen og som fører til at en eller flere straffebestemmelser overtredes"*

I Datakrimutvalgets utredning om Lovtiltak mot datakriminalitet [8] står det som følger:

> *"Begrepet "datakriminalitet": Etter en alminnelig forståelse omfatter uttrykket «datakriminalitet» både kriminalitet som er rettet mot data og datasystemer, og kriminalitet hvor datautstyr benyttes som verktøy for å begå handlingen. Utvalget har ikke sett behov for å gi uttrykket «datakriminalitet» en rettslig definisjon. Mandatet sett under ett oppfattes som et oppdrag om å gi regler om kriminalitet som har sammenheng med bruk og utnyttelse av datateknologi (IKT). Begrepet datakriminalitet er hensiktsmessig for å indikere hva lovforslaget gjelder."*

En kan også benytte en mer snever definisjon:

> *"Straffbare handlinger der en datamaskin er objekt for den straffbare handlingen"* [3]

Det er denne definisjonen som er benyttet i politiets straffesaksregister, STRASAK.

3.2.2 Mørketall

Vi velger her å benytte den samme definisjonen som det er gjort i Mørketallsundersøkelsen 2006 [3]:

> *"antall hendelser som virksomhetene kjenner til men ikke anmelder"*

3.2.3 Kategorisering av straffebestemmelser og hendelsestyper

Vi har i denne oppgaven benyttet samme kategorisering av straffebestemmelser og hendelsestyper som i Mørketallsundersøkelsen 2006 [3]. Dette er det redegjort for i Appendiks D: Kategorisering av straffebestemmelser og hendelsestyper.

Vi vil påpeke at det ikke finnes sammenlignbare data fra anmeldelsesstatistikken når det gjelder følgende type uønskede hendelser; "Trusler om å angripe IT-systemer (utpressing)" og "Tyveri av IT-utstyr (PC, Server, PDA etc.)". Dessuten kommer "Tyveri av IT-utstyr" inn under kategorien vinningskriminalitet og er følgelig heller ikke presentert i Kripos sine statistikker over anmeldte datakriminelle saker [Kripos].

3.3 Litteratur

I arbeidet med oppgaven ble det benyttet databaser som ScienceDirect, Academic Search Elite, ISI Web of Science, Springer Link etc. for søk etter relevant litteratur. Det er verdt å bemerke at det var ved søk ved hjelp ulike søkemotorer på Internett vi i størst grad fant litteratur som var relevant for denne oppgaven. Dette gjelder spesielt undersøkelser, tilsvarende Mørketallsundersøkelsen 2006 [3], som er gjennomført i andre land.

3.4 Spørreundersøkelsen

Spørreundersøkelsen fortatt blant ISF-medlemmer er som nevnt tidligere ment å være en relevant referanseundersøkelse i forhold til MU. ISF-U og MU var samlet ment å gi svar på forskningsspørsmål i tillegg til at resultatene fra disse undersøkelsen skulle gi bidrag til intervjuene vi gjennomførte.

3.4.1 Utvalget

Vi gjennomførte en spørreundersøkelse blant deltakerne på ISFs høstkonferanse i september 2006. Ved å gjennomføre en undersøkelse blant ISFs medlemmer gjorde vi et bevisst bekvemmelighetsutvalg. Bakgrunnen for dette utvalget er at ISF "*... har som overordnet målsetning å være landets ledende organisasjon og samlende fagmiljø innenfor fagområdet IT-sikkerhet, og derigjennom være en sentral aktør for å bedre IT-sikkerheten både innen medlemsvirksomhetene og det norske samfunn generelt*" [52].

Vi har antatt at ISFs medlemmer kan ha en større bevissthet i forhold til informasjonssikkerhet og datakriminalitet enn de fleste virksomhetene som besvarte MU. Følgelig har det vært av interesse å søke svar på om dette reflekteres i besvarelsene av undersøkelsene.

3.4.2 Spørreskjemaet

Spørsmålene i spørreskjemaet (Appendiks A) var basert på skjemaet som ble brukt for MU. Med det menes at vi ikke valgte å benytte alle spørsmålene som var stilt i MU. I tillegg valgte vi å omstrukturere noen av spørsmålene. Det ble stilt noen generelle spørsmål om virksomheten for å kunne ha uavhengige variabler til den statistiske analysen. Spørreskjemaet ble kvalitetssikret av ekstern veileder og av andre eksterne ressurspersoner innen informasjonssikkerhet.

Til sammen ble det stilt 18 spørsmål og disse var gruppert etter følgende kategorier:

1. Generelt om virksomheten
2. Informasjonssystemene i virksomheten
3. Sårbarhet og organisatoriske sikringstiltak
4. Tekniske sikringstiltak
5. Hendelser

3.4.3 Distribusjon

Spørreskjemaet ble delt ut til alle deltakerne ved ISFs høstkonferanse i 2006. I tillegg ble det oppfordret av ISFs leder om at deltakerne skulle besvare skjemaet. Etter konferansen ble også skjemaet lagt ut på ISFs hjemmesider på Internett og det ble sendt ut en e-post fra leder med oppfordring om å delta. Vi fikk inn 26 skjemaer fra konferansen og 5 valgte å besvare elektronisk.

3.4.4 Tolking av data og statistiske undersøkelser

Vi er bevisst at et flertall av virksomhetene som har besvart ISF-U er store virksomheter med mange ansatte. I våre analyser har vi tatt hensyn til dette blant annet ved å

kjøre Univariat variansanalyse for å korrigere for virksomhetenes størrelse. Vi har også, der det har vært egnet, kjørt analyser av dataene fra de største virksomhetene i MU og ISF-U.

Til behandling og analyse av datagrunnlaget (MU og ISF-U) benyttet vi SPSS 15.0 [53,54]. Under dette arbeidet identifiserte vi behovet for å lage en del nye variabler for å kunne få svar på en del av våre spørsmål. For krysstabeller har vi anvendt Pearsons kjikvadrattest for signifikansberegning. Dessuten har vi benyttet T-tester og variansanlyser (Anova) for sammenligning av andre variabler.

Ved statistiske beregninger av signifikansnivå (Pearsons kjikvadrattest – p-verdi) ble p=0,05 valgt som signifikant og et signifikansnivå på mindre en 0,01 som meget signifikant.

Et lite utvalg fra dataanalysene er presentert i Appendiks E.

3.4.5 Bearbeiding av datagrunnlaget fra MU

Vi valgte å ta hensyn til uteliggere [53] i forhold til datagrunnlaget fra MU, spesielt i forhold til rapportering av antall hendelser. Med bakgrunn i vår erfaring fra arbeid med informasjonssikkerhet anså vi at noen av virksomhetene kunne ha misforstått spørsmålsstillingen og overrapportert eller at det kan ha vært begått feil ved manuell registrering av dataene. I forbindelse med de resultatene hvor vi har tatt hensyn til uteliggere, er dette kommentert og det er argumentert for beslutningen.

Vi gjør oppmerksom på at det ikke ble tatt hensyn til uteliggere i Mørketallsundersøkelsen 2006 [3] og følgelig har vi kommet frem til litt andre resultater i våre analyser og tolkninger, blant annet i forhold til estimater for mørketall.

3.5 Intervjuer

Vi gjennomførte intervjuer med 8 virksomheter som har anmeldt datakriminalitet. Dette ble gjort for å få en innsikt i hvilke erfaringer de hadde gjort knyttet til hendelsen(e) de var utsatt for, og for å få informasjon om prosessen fra de oppdaget hendelsen, anmeldte den og til saken var avsluttet. Videre intervjuet vi 2 ressurser som har erfaring fra å bistå virksomheter med etterforskning av hendelser, så som sikring av elektroniske spor og dokumentasjon av hendelsesforløpet. Det ble også gjennomført intervju med en representant fra Datakrimavdelingen i Kripos for å få deres innspill i forhold til datakriminalitet i Norge.

Intervjuene ble foretatt som en åpen dialog basert på spørsmål som var sendt ut på forhånd. Intervjuene ble tatt opp på mp3-spiller og i etterkant ble det skrevet en oppsummering som ble sendt til det enkelte intervjuobjektet for verifisering. Verifiseringen ble gjennomført som en del av kvalitetssikring av oppgaven og for å sikre at oppsummeringen var korrekt og at intervjuobjektene følte at deres behov for konfidensialitet ble ivaretatt.

Ved gjennomføring av disse intervjuene har vi fått innblikk i erfaringer både fra de som har anmeldt datakriminalitet og de som skal etterforske anmeldelser (Kripos). Når vi startet arbeidet med denne oppgaven hadde vi også et ønske om å få innspill fra

personer som har utført datakriminelle handlinger. Vi har lykkes med å få innspill fra en person med datakriminell fortid. I denne forbindelsen vil vi påpeke at vi har vært veldig klare og tydelige på følgende: vi ønsket ikke å være i direkte kontakt med vedkommende eller å bli gjort kjent med vedkommendes identitet. Ei heller ønsket vi å få informasjon som omhandlet navngitte virksomheter.

3.6 Kvalitet

I forbindelse med forskningsdesign og metode er det vesentlig at krav til pålitelighet og gyldighet ivaretas, og at egen forskerrolle diskuteres. [55,56] Dette redegjøres det for i det følgende.

Vi har tidligere i oppgaven opplyst om at spørsmålene vi benyttet i vår spørreundersøkelse (ISF-U) var basert på spørsmål stilt i MU. Under vårt arbeid med utformingen av spørreskjemaet identifiserte vi at det var behov for noen korrigeringer blant annet i forhold til bruk av terminologi. Dette ble gjort for å sikre at spørsmålene skulle bli så tydelige som mulig og for å forhindre misforståelser. Vi kvalitetssikret også spørreskjemaet før det ble levert ut. Derfor mener vi at spørreskjemaet er utformet slik at det er mulig å reprodusere resultatene og at data fra undersøkelsen i stor grad er gyldige.

Det å benytte en kvalitativ tilnærming til et tema kan medføre at resultatene blir preget av subjektive meninger [50]. Et annet forhold var at de fleste av de som ble intervjuet er i vår kontaktkrets og således personer vi kjenner. Det kan dessuten være vanskelig å vurdere i hvor stor grad resultatene har blitt påvirket av personlige vurderinger. Det har vært svært vesentlig for oss at oppgaven gir et mest mulig korrekt bilde, særlig med henblikk på den kvalitative delen. Derfor har vi sørget for at resultatene fra intervjuene har blitt verifisert av intervjukandidatene. I tillegg til å benytte intern og ekstern veileder har vi også benyttet andre eksterne ressurser innen informasjonssikkerhetsmiljøet for å sikre at konklusjoner blir så korrekte og objektive som mulig.

Vi er også inneforstått med at vi under dataanalysene og tolkningen av disse til en viss grad har lagt til grunn den erfaring og kunnskap vi har opparbeidet oss gjennom flere år med arbeid innen informasjonssikkerhet. Følgelig har det vært en utfordring å begrense subjektive vurderinger i diskusjonene rundt resultatene fra dataanalysene. Dette kan medføre at andre ville ha presentert resultatene litt annerledes dersom de hadde gjennomført tolkningen av dataanalysen. Derfor har vi, der det er gjeldende, meddelt det dersom våre resonnementer med en viss sannsynlighet er basert på subjektive meninger.

3.7 Etiske og juridiske hensyn

Resultatene fra spørreundersøkelsene er anonymisert og vil således ikke medføre brudd på konfidensialitet. Når det gjelder resultatene fra intervjuene har disse også blitt anonymisert og intervjuobjektene har fått anledning til å verifisere resultatene fra intervjuet og at krav til konfidensialitet har blitt overholdt.

Alle grunnlagsdata knyttet til virksomheter og personer vil bli slettet etter at oppgaven er ferdigstilt.

Innspill fra personen med datakriminell bakgrunn ble innhentet uten at vedkommendes identitet ble avslørt. Vi ba ikke om, eller aksepterte å få, informasjon om faktiske datakriminelle handlinger vedkommende hadde utført. Vedkommende er for enkelhetsskyld omtalt som NN videre i oppgaven.

I forbindelse med intervjuene ble det undertegnet taushetserklæringer hos de virksomheter som ønsket dette.

Da det har vært svært vesentlig å sikre virksomhetenes behov for konfidensialitet har vi naturligvis ikke nevnt dem ved navn. Ei heller har vi valgt å referere til dem med nummer eller bokstav. Dette fordi det kan være en sannsynlighet for at det er mulig å identifisere virksomheter gjennom å se hvem som har gitt hvilke opplysninger. Man kan se en "rød tråd".

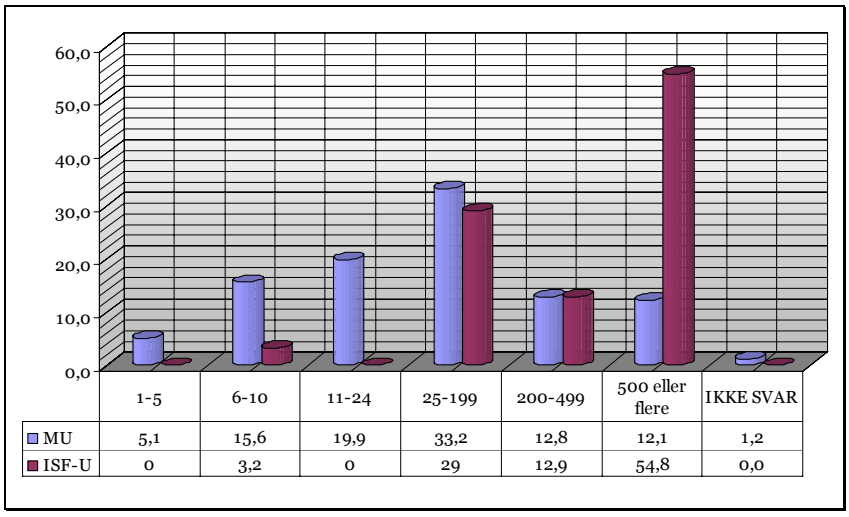
4. Datagrunnlag

Vår spørreundersøkelse resulterte i 31 besvarelser. De innkomne dataene fra ISF-U ble kategorisert og omkodet for at vi skulle kunne benytte dem i en sammenligning med dataene fra MU. Videre fant vi det nødvendig å lage en del nye variabler både for dataene fra ISF-U og MU slik at det i større grad ville være mulig å sammenligne resultatene. Noen av spørsmålene fra undersøkelsen danner et grunnlag for å karakterisere virksomhetene som har deltatt og de presenteres i dette kapitlet. I kapitel 5 diskuteres resultatene fra undersøkelsene.

4.1 Besvarelse av spørreundersøkelsen

Vårt spørreskjema ble delt ut på ISFs høstkonferanse 2006. Det var 70 medlemsbedrifter som deltok på konferansen. 31 av 70 virksomheter besvarte skjemaet, noe som gir en svarprosent på 44,3. Spørreskjemaet for MU var sendt ut til 2000 virksomheter. Av disse hadde 400 5-9 ansatte, 800 10-99 ansatte og 800 mer enn 100 ansatte. Av de 2000 var det 749 virksomheter som besvarte spørreskjemaet [3]. Følgelig var det en svarprosent på 37,5.

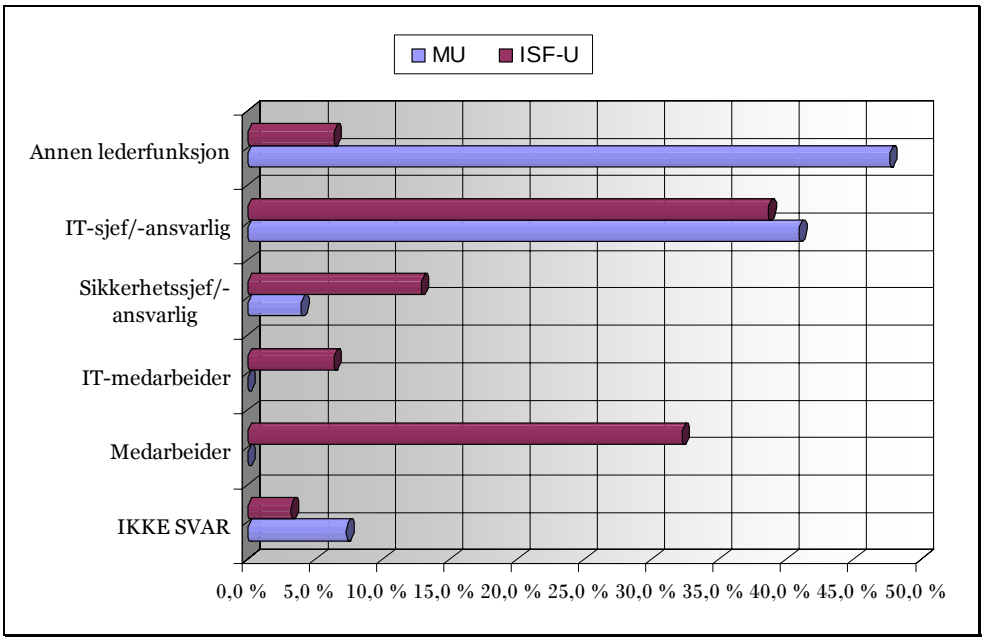
I Figur 3 vises virksomhetene fordelt på antall ansatte både for MU og for ISF-U. Det ble benyttet samme inndeling for begge undersøkelsene: 1-5, 6-10, 11-24. 25-199, 200-499 og 500 eller flere. Figuren viser at det for ISF-U er en klar overvekt av store virksomheter som har besvart spørreskjemaet. Statistisk analyse med kjikvadrat viser en meget signifikant forskjell ($p < 0,01$) mellom størrelsen på virksomhetene som deltok i henholdsvis MU og ISF-U. Dette lar seg forklare med at blant ISFs medlemsmasse, på 164 virksomheter, er de aller fleste virksomhetene å anse for å være store. I diskusjoner av resultatene, kapittel 5, vil eventuelle konsekvenser av denne forskjellen bli tatt opp.



	1-5	6-10	11-24	25-199	200-499	500 eller flere	IKKE SVAR
MU	5,1	15,6	19,9	33,2	12,8	12,1	1,2
ISF-U	0	3,2	0	29	12,9	54,8	0,0

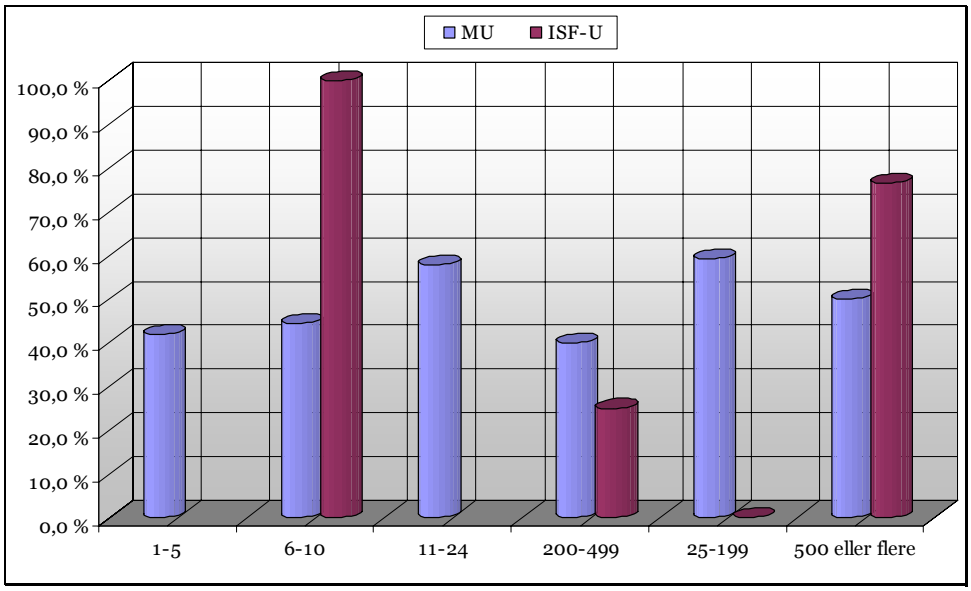
Figur 3: Antall ansatte – ISF-U og MU

I spørreundersøkelsene ble respondentene spurt om hvilken stilling/funksjon de hadde i virksomheten. Vi valgte i ISF-U å benytte litt andre kategorier enn i MU og har derfor omkodet dataene som en følge av dette. Videre vil det for MUs del være 2 kategorier som er blanke av den grunn at de ikke var med i MU. Dette medfører at vi ikke kan presentere en statistikk der det direkte kan trekkes slutninger om fordeling av respondentenes stilling/funksjon. Vi mener allikevel at denne fordelingen er relevant. Kategorien "Annen lederfunksjon" består for MUav kategoriene: Daglig leder og Økonomiansvarlig. For ISF-U består "Annen lederfunksjon" av: Daglig leder og Annen lederfunksjon. Figur 4 viser er det en klar forskjell mellom MU og ISF når det gjelder antallet for "Annen lederfunksjon", MU 47,7 % og ISF-U 6,5%.



Figur 4: Virksomheter fordelt på stilling/funksjon

I begge undersøkelsene ble det stilt spørsmål om hvorvidt virksomhetene selv var ansvarlige for IT-driften eller om de hadde valgt å tjenesteutsette (outsource) hele eller deler av den. 52,2 av MUs virksomheter har valgt å tjenesteutsette hele eller deler av IT-driften, og 48,4 % av ISF-Us virksomheter har gjort det samme. Analysen vår viser at det i stor grad er de større virksomhetene som velger å tjenesteutsette IT-driften. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$) både for MU og ISF-U. Videre viser analysen vår at blant ISF-Us virksomheter hadde 76,5 % av de aller største virksomhetene (500 eller flere ansatte) valgt å tjenesteutsette IT-driften. Det tilsvarende tallet for MU var 50,0 %. I Figur 5 presenterer vi resultatene for prosentandel virksomheter som har valgt å tjenesteutsette IT-driften fordelt på antall ansatte i virksomheten.



Figur 5: Virksomheter som har outsourcet fordelt på antall ansatte

5. Diskusjon av resultater

"De større bedriftene er selvfølgelig flinkere enn de små til å ivareta informasjonssikkerheten, men også her syndes det en del. Spesielt i FOU miljøer samt på direktørnivå. Det er verd å merke seg at selv om små virksomheter "glemmer" å prioritere informasjonssikkerhet, betyr ikke det at de ikke responderer med full tyngde dersom noe skulle skje, noe som dessverre ikke blir utført i like stor grad hos de større organisasjonene."

NN

I dette kapitlet vil vi diskutere resultatene fra spørreundersøkelsene, MU og ISF-U, og intervjuer med virksomheter som har anmeldt datakriminalitet.

I første del av kapitlet diskuterer vi omfanget av datakriminalitet i Norge. Dette gjøres ved at det først redegjøres for våre beregninger av det totale omfanget av datakriminalitet i forhold til MU og deretter estimater for mørketall. Så vil vi presentere mer detaljerte resultater fra våre analyser av dataene fra MU og ISF-U i forhold til datakriminelle hendelser. Deretter presenterer vi resultater for hvorfor virksomheter ikke anmelder datakriminalitet og så hva som skjer dersom de anmelder. Videre drøfter vi hva som kan gjøres for å få flere virksomheter til å anmelde. Dernest presenterer vi en diskusjon av resultatene fra sammenligning av MU og ISF-U i forhold til implementerte sikringstiltak, kontroll og oppfølging. Til slutt i kapitlet presenterer vi et sammendrag.

5.1 Hvor stort er omfanget av datakriminalitet i Norge?

5.1.1 Hendelser og anmeldelser

Ved analyse av dataene fra MU har vi funnet at det kan være en del rapporteringer som vi anser at må være noe usikre. Noen virksomheter er registrert med tallet 99 for antall hendelser. Tallet 99 er for en del andre variabler benyttet som koding av "Vet ikke"-svar. Vi har derfor valgt å ta hensyn til uteliggere i forhold til disse variablene. I tillegg er det i forbindelse med rapportering av antall hendelser, for noen kategorier, oppgitt tall som vi anser for å være unormalt høye basert på virksomhetens størrelse og hendelsestype. Følgelig har vi også tatt hensyn til uteliggere for disse rapporteringene. Dette er kommentert i mer detalj i kapittel 5.1.3.

Under vår dataanalyse fant vi også at det var en del virksomheter som var registrert med at de hadde anmeldt hendelser, som de ikke hadde rapportert å ha blitt utsatt for. Vi har derfor valgt å utelate disse rapporteringene i våre analyser.

På bakgrunn av det ovennevnte har vi derfor identifisert et behov for å prøve å presentere et bilde av totaltallene fra MU som vi anser kan være mer korrekt. I Tabell 4 representerer kolonnen "Vår analyse av MU" totaltall for antall rapporterte hendelser og anmeldte hendelser. I denne kolonnen har vi bare valgt å trekke fra de virksomhetene som har rapportert 99 hendelser innen de respektive kategoriene.

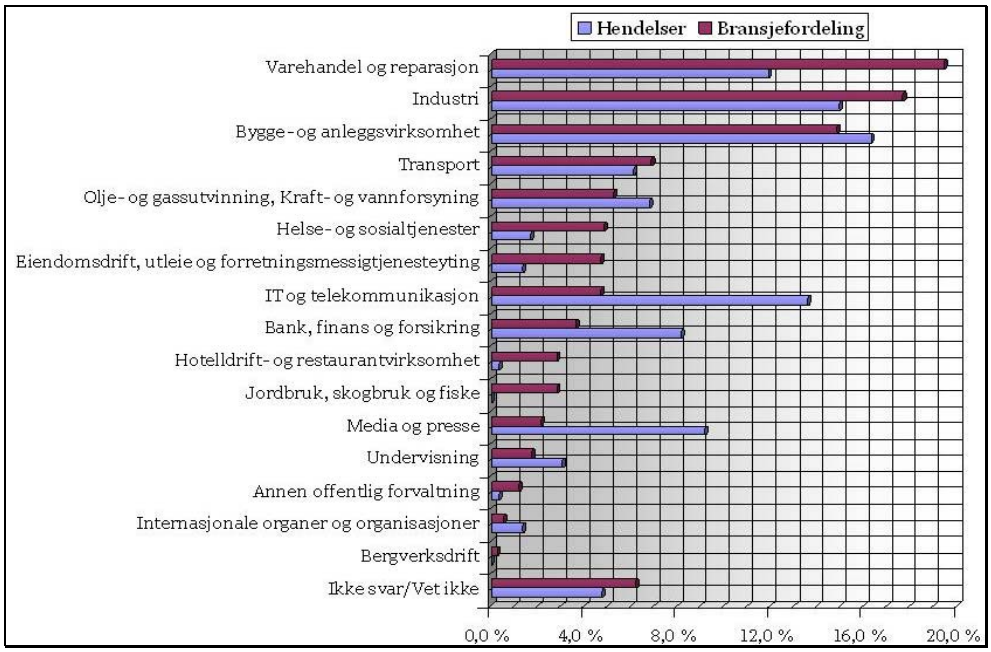
Kolonnen "Mørketallsrapporten" presenterer de tallene som ble oppgitt for Mørketallsundersøkelsen 2006 [3]. I den siste kolonnen "Potensielle tall", som også er vår analyse, har vi valgt å trekke fra andre store tall som ikke virker logisk i forhold til den gitte virksomhets størrelse og bransje. I tillegg har vi valgt å trekke ut tall fra virksomheter som har oppgitt å ha anmeldt en hendelse de ikke er registrert med å ha vært utsatt for.

Gitt de forutsetningene vi nå har presentert viser våre analyser og tolkninger ("Potensielle tall") at det i MU ble rapportert 1.125 hendelser fordelt på 10 kategorier, mot 2.079 som ble presentert i Mørketallsundersøkelsen [3]. Dette innebærer at våre totaltall er 48,9 % lavere enn i [3]. Av disse hendelsene viser våre analyser at 268 ble meldt til Kripos/politiet. Dette medfører at 23,8 % av hendelsene ble anmeldt. Det tilsvarende for tallene oppgitt i Mørketallsundersøkelsen 2006 [3] er 13,8 %. Den hendelseskategorien som utpeker seg i forhold til "villighet" til å anmelde er tyveri av IT-utstyr. I følge våre "Potensielle tall" har hele 72,2 % av IT-tyveriene blitt anmeldt.

	Vår analyse av MU		Mørketallsrapporten		Potensielle tall	
	Hendelser	Anmeldt	Hendelser	Anmeldt	Hendelser	Anmeldt
Datainnbrudd (hacking)	28	3	226	3	28	3
Datatyveri	7	7	7	7	7	3
Uautorisert endring/sletting av data	88	2	88	2	68	1
Misbruk av IT-ressurser	94	7	94	7	94	7
Spredning av ulovlig/ opphavsrettsling materiale	13	0	13	0	13	0
Angrep på tilgjengelighet (DoS)	50	1	149	1	50	0
Virus/orm/trojaner-infeksjon	722	1	1118	1	511	1
Trusler om å angripe IT-systemer	33	3	33	9	3	2
Bedrageri ved misbruk av kredittkort over Internett	31	22	31	22	31	20
Tyveri av IT-utstyr (PC, server, PDA etc.)	320	234	320	234	320	231
Totalt	1.386	280	2.079	286	1.125	268

Tabell 4: Oversikt over antall hendelser per kategori – nye analyser

I Figur 6 presenterer vi prosentandel hendelser fordelt på prosentandel bransjer. Den viser at bransjer som "Media og presse", "IT og telekommunikasjon" og "Bank, finans og forsikring" i mye større grad utsettes for datakriminelle hendelser sett i forhold til andelen de utgjør blant bransjer i MU.



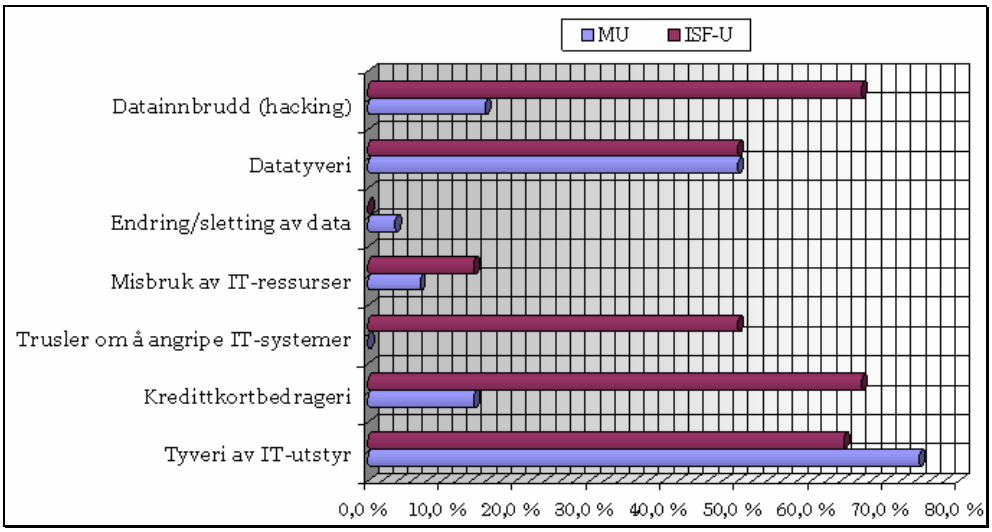
Figur 6: Hendelser fordelt på bransjer

I Tabell 5 viser vi antall virksomheter som har oppgitt at de har hatt en eller flere hendelser og antallet virksomheter som har valgt å anmelde – fordelt på hendelseskategorier. I tillegg viser vi antall virksomheter i ISF-U som har hatt hendelser og antall som har anmeldt. Det går frem av Tabell 3 at ISF-Us virksomheter i større grad enn MUs har valgt å anmelde. Av ISF-Us respondenter var det 53,8 % av de som hadde vært utsatt for en eller flere datakriminelle hendelser som hadde anmeldt disse, for MU er tallet 25,8 %. Igjen vises det at det er anmeldelse av tyveri av IT-utstyr som er mest fremtredende – 64,3 % av ISF-U-virksomhetene hadde anmeldt 1 eller flere tyverier og tallet for MU-virksomheter var 72,5 %.

	ISF		MU	
	Rapportert	Anmeldt	Rapportert	Anmeldt
Datainnbrudd (hacking)	3	1	19	3
Datatyveri – uautorisert lesing/ kopiering av data	2	1	6	3
Endring/sletting av data (uautorisert)	3	0	27	1
Misbruk av IT-ressurser (PC/nett/server)	7	1	43	3
Spredning av ulovlig/opphavsrettslig beskyttet materiale	2	0	8	0
Angrep på tilgjengelighet (DoS-angrep)	0	0	23	0
Virus/orm/trojanerinfeksjon (virkelige infeksjoner)	7	0	188	1
Trusler om å angripe IT-systemer	2	0	3	0
Bedrageri ved misbruk av kredittkort over internett	3	2	7	1
Tyveri av IT-utstyr (PC, server, PDA etc.)	14	9	153	111
Totalt	26	14	477	123

Tabell 5: Oversikt over antall virksomheter som har rapportert og anmeldt hendelser

Figur 7 viser prosentandelen virksomheter som har anmeldt hendelser de har vært utsatt for. Vi har valgt å utelate kategoriene "Spredning av ulovlig/opphavsrettsling materiale" og "Angrep på tilgjengelighet (DoS)" fordi det ikke var rapportert anmeldelser. Dessuten har vi utelatt kategorien "Virus/orm/trojanerinfeksjon" fordi det bare var 1 virksomhet av 188 som hadde rapportert at de hadde anmeldt. Våre resultater viser at ISF-Us virksomheter i større grad har anmeldt 1 eller flere hendelser i de respektive kategoriene enn MUs. Dette er spesielt tydelig for kategoriene "Datainnbrudd", "Trusler om å angripe IT-systemer" og "Bedrageri av misbruk av kredittkort over Internett". I kapittel 5.1.3 Hendelser vil disse resultatene bli presentert i mer detalj.



Figur 7: Prosentandel virksomheter som har anmeldt hendelser

"... som alle vet kan ikke en brannmur stoppe den menneskelige trangen til å snakke og ta kopier av ting. Brannvegger er nytteløst når alt man trenger å gjøre er å rappe en laptop."

NN

Tyveri av IT-utstyr omfattes ikke av Kripos sin statistikk for datakriminalitet fordi dette anses for å være vinningsforbrytelser. Figur 7 viser at det som hyppigst anmeldes er nettopp tyveri av IT-utstyr. Dette går også frem av våre intervjuer med virksomheter som har anmeldt datakriminalitet (kapittel 5.3). Det som også fremgikk av disse intervjuene var at virksomhetene i liten grad hadde dokumenterte retningslinjer for å vurdere om interesse for datainnholdet på eksempelvis frastjålne bærbare pc-er kan være årsaken til at pc-ene var blitt stjålet. Følgelig om var de ikke bevisst på om det var en ren vinningsforbrytelse eller om tyvene ønsket å få tak i data/informasjon.

Statistikk over anmeldte lovbrudd [Kripos], etter Kripos sin definisjon av datakriminalitet [Appendiks D], for helår 2002-2006 viser at det fra 2005 til 2006 har vært en økning på 40,2 % i forhold til antall anmeldte saker. I Tabell 6 ser vi at det er en økning for alle kategoriene. I forbindelse med statistikken opplyses det fra Kripos at det er kjent at det kan være tilfeller hvor anmeldte saker ikke er gitt korrekt kode når de etterforskes av politidistriktene.

Kategori	2002	2003	2004	2005	2006	Δ 05-06
Datainnbrudd	70	58	60	61	76	24,6 %
Dataskadeverk og –bedrageri:	16	101	96	129	152	17,8 %
Misbruk av dataressurser:	60	12	20	11	17	54,5 %
Tyveri av datainformasjon	8	19	14	29	76	162,1 %
Spredning av ulovlig/opphavs-rettslig beskyttet materiale	8	14	5	4	7	75,0 %
Totalt for alle kategorier	162	204	195	234	328	40,2 %

Tabell 6: Anmeldte lovbrudd – datakriminalitet – 2002-2006

5.1.2 Estimat av mørketall innen datakriminalitet

"Ble du noen gang mistenkt for å ha utført datakriminelle handlinger?: Nei, da hadde jeg nok ikke jobbet der jeg gjør i dag. ;-)"

NN

"Det er vanskelig å uttrykke den delen av kriminalitetsutviklingen som har sammenheng med teknologiutviklingen i form av troverdig statistikk. Dette har flere årsaker. For det første foreligger et registreringsproblem. Antall anmeldelser av straffbare forhold rettet mot datasystemer og infrastruktur er trolig svært lite i forhold til det antall kriminelle handlinger som faktisk begås. Dette kan skyldes at tilfeller av datakriminalitet ikke blir oppdaget, at de ikke blir gjenkjent som datakriminalitet eller at man av ulike årsaker ikke ønsker å anmelde forholdene."

NOU 2007: 2 – Lovtiltak mot datakriminalitet [8]

Det å estimere mørketall for datakriminalitet kan anses for å være en relativt risikabel affære. Noen vil sikkert si at det kan sammenlignes med å legge hodet på hoggestabben. Det er en rekke usikkerhetsfaktorer som spiller inn og følgelig må det tas høyde for at dette bare er estimater og ikke eksakte og vitenskaplig beviselige tall.

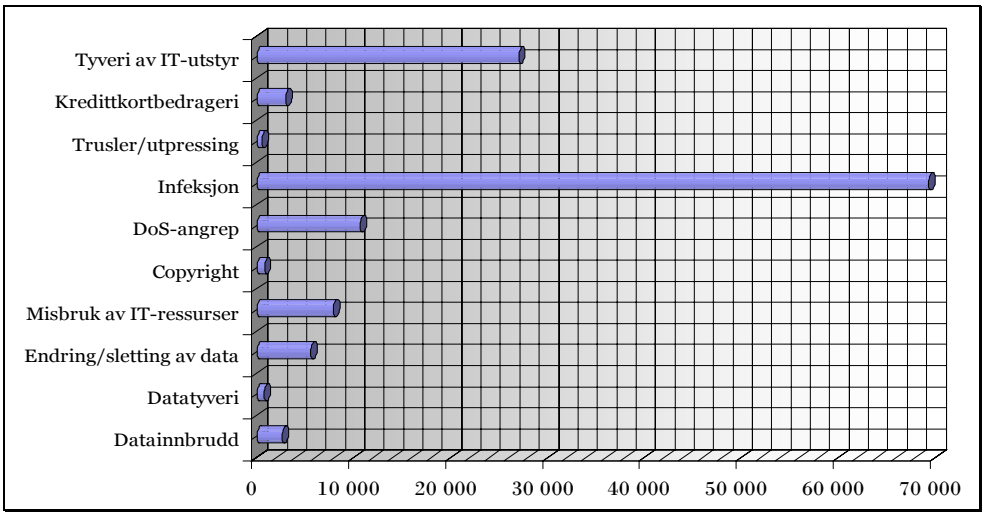
Ved beregning av estimater for potensielle mørketall har det blitt tatt utgangspunkt i antall rapporterte hendelser i Mørketallsundersøkelsen 2006 [3]. Det innebærer altså at estimatene er basert på antall kjente hendelser. Således vil de reelle tallene, de virkelig mørke tallene, for en del av hendelseskategoriene være mye høyere uten at vi kan ha en konkret og beviselig konklusjon om dette. Dette er spesielt gjeldende for kategorier som "datainnbrudd", "datatyveri", "misbruk av IT-systemer" og "spredning av ulovlig/opphavsrettslig beskyttet materiale".

I Mørketallsundersøkelsen 2006 [3] benyttet de SSBs statistikk for næringsstrukturen i Norge – med antall virksomheter fordelt på antall – for å estimere hvor mange virksomheter som hadde vært utsatt for datainnbrudd og misbruk av IT-systemer. Tallet for antall virksomheter som var medregnet var 175.440. Det ble estimert at norske virksomheter hadde vært utsatt for 3.900 datainnbrudd i perioden undersøkelsen omhandlet. Estimatet for antall virksomheter som hadde vært utsatt for misbruk av IT-systemer var 8.900. Når Mørketallsundersøkelsen 2003 [21] ble presentert oppga de at mørketall for datainnbrudd var 5.200. Dette ble kommentert av eksperter som mente at tallet var altfor lavt. En hevdet at 10.400 datainnbrudd var nærmere sannheten [57].

Basert på datagrunnlaget fra MU (hvor vi har tatt hensyn til uteliggere) og SSBs statistikk for næringsstrukturen i Norge per 01.04.2007 [58], har vi estimert antall datakriminelle hendelser som norske virksomheter var utsatt for i 2005. Utregningen av estimatet er gjort på følgende måte:

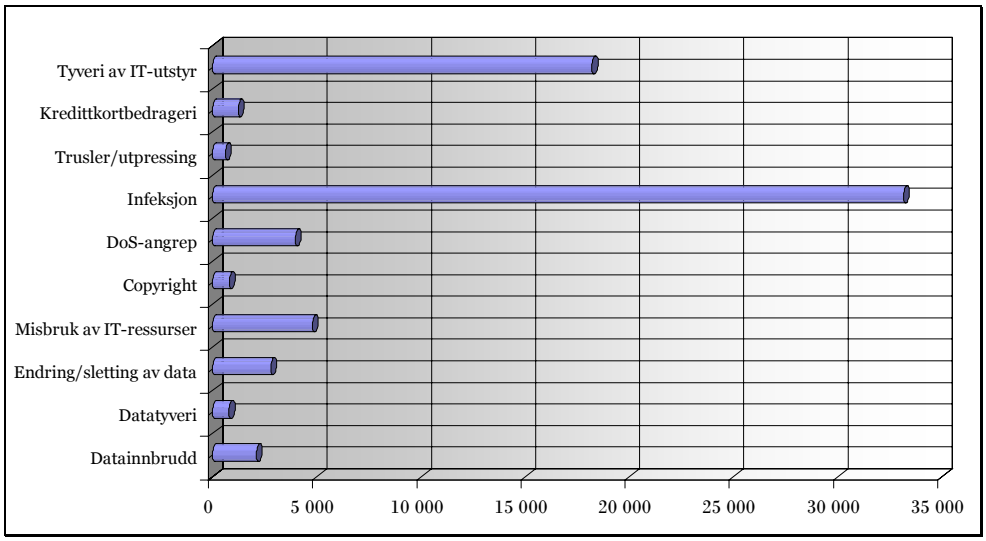
1. Ved å bruke datagrunnlaget fra MU og summere antall hendelser fordelt på virksomhetens størrelse (antall ansatte) beregnet vi prosentandelen av hendelser fordelt på virksomhetenes størrelse. Da kategoriene for virksomhetens størrelse var noe ulik for MU og SSBs statistikk [58] måtte vi foreta noen tilpasninger.
2. Deretter benyttet vi denne prosentberegningen i forhold til SSBs statistikk [58] og antall virksomheter fordelt på virksomhetenes størrelse, og beregnet det potensielle antall vellykkede og oppdagede datakriminelle hendelser som norske virksomheter kan ha vært utsatt for i 2005.

Antall virksomheter, med ansatte, var i følge SSBs statistikk per 01.04.2007 179.988 [58]. Vårt estimat for det total antall datakriminelle hendelser, som norske virksomheter ble utsatt for i 2005, er 128.307. Dersom vi trekker fra tallene for kategorien "Tyveri av IT-utstyr" er estimatet 101.254 datakriminelle hendelser. Videre estimerer vi at det har vært ca. 2.600 tilfeller av vellykkede, oppdagede datainnbrudd og ca. 7.900 tilfeller av misbruk av IT-systemer som er oppdaget. Figur 8 viser hvordan antall hendelser er fordelt på kategorier. Fordi vi tok hensyn til uteliggere er naturligvis våre estimater lavere enn det som er presentert i Mørketallsundersøkelsen 2006 [3].



Figur 8: Estimat antall hendelser per hendelseskategori - mørketall

Videre har vi estimert at 68.375 virksomheter ble utsatt for datakriminalitet i 2005. Hvis vi trekker fra kategorien "Tyveri av IT-utstyr" er antallet 50.176. I Figur 9 vises antall virksomheter som har hatt hendelser fordelt på hendelseskategorier.



Figur 9: Estimat antall virksomheter som har hatt hendelser per hendelseskategori

5.1.3 Hendelser

> *"Mørketallsundersøkelsen for 2006 viser en reduksjon av antallet datainnbrudd. Dette kan f.eks skyldes at flere angrep kommer via trojanere og at virksomheter i liten grad har mulighet til å identifisere at et trojanerangrep kan være et innbruddsangrep. Kripos sin etterforskning viser at det er mange alvorlige trojanerangrep hvor det hentes ut informasjon som brukes i annen type kriminalitet. Dette er en av grunnene til at spørsmål om virus-trojaner ikke ble droppet fra Mørketallsundersøkelsen 2006."*
>
> Kripos

Ved analyse og profilering av 205 koordinerte angrep (et angrep representerte flere hendelser) detektert av NSM (Nasjonal Sikkerhetsmyndighet) i 2004 fant de at angrep som krever planlegging, så som datainnbrudd, i større grad kom fra industrialiserte land enn land med dårlig IKT-infrastruktur. De så også at ormangrep, som ikke krever særlig planlegging, i stor grad kom fra land med dårlig IKT-infrastruktur. Videre viste det seg at 41,5 % av angrepene var det hendelser knyttet til datainnbrudd og 9,8 % til DoS-angrep. I hele 92,7 % av angrepene ble det gjort skanning som et ledd av angrepet. [10].

I presentasjonen av resultater for hendelser har vi valgt å ha hovedfokus på antall virksomheter som har hatt hendelser og ha et mindre fokus på hvor mange hendelser de har hatt. Dette på grunn av usikkerheten i forhold til enkelte av de rapporterte tallene (uteliggerne). Vi gjør oppmerksom på at vi ikke har utelatt virksomheter som har rapportert uforholdsmessig høye tall, da vi antar at det kan være korrekt at de har vært utsatt for hendelser. Våre resultater viser at størrelsen til ISF-Us virksomheter kan ha betydning for noen av resultatene og dette er det redegjort for.

En sammenstilling av antall virksomheter som har opplevd hendelser fordelt på om de har tjenesteutsatt IT-driften (outsourcet) eller ikke, viser at det i liten grad er signifikante forskjeller for de ulike hendelseskategoriene. De eneste kategoriene hvor funnene våre viser seg å være signifikante ($p < 0,5$) er "Misbruk av IT-ressurser", "Angrep på tilgjengelighet" og "Trusler om å angripe IT-systemer". Resultatene for disse kategoriene viser at de som ikke har outsourcet i større grad utstettes for slike hendelser. I vår videre presentasjon av resultater har vi valgt å ikke differensiere i forhold til hvorvidt virksomhetene har outsourcet eller ikke.

A. Datainnbrudd (hacking)

MU viser at 2,5 % (19/749) av respondentene har opplevd datainnbrudd. Tilsvarende tall for ISF-U viser at det er flere virksomheter som har opplevd datainnbrudd – 9,7 % (3/31). Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene ikke er signifikante. Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter her påvirker resultatene.

I ITAKTs undersøkelse for 2006 [59] rapporterte 8 % av virksomhetene at de hadde vært utsatt for datainnbrudd. Dette ligger nærmere svarprosenten i ISF-U enn i MU.

Ved gjennomgang av datagrunnlaget fra MU fant vi at 2 virksomheter hadde oppgitt at de hadde hatt 99 datainnbrudd. For øvrig viser analysen at de som har hatt nest mest antall hendelser har hatt 4. Virksomhetene som hadde hatt 99 datainnbrudd har 25-199 ansatte. Bare den ene virksomheten har benyttet ekstern ekspertise og dette er gjort i 11 av tilfellene. Ingen av virksomhetene har valgt å anmelde. Tallene for disse 2 virksomhetene ble håndtert som uteliggere.

Av de 19 MU-virksomhetene som opplevde datainnbrudd var det bare 3 som valgte å anmelde. Mens tilsvarende for ISF-U viser at 2 av 3 valgte å anmelde. Kjikvadrattesten viser en nesten tilfredsstillende signifikans - $p = 0,051$.

B. Datatyveri – uautorisert lesing/kopiering av data

MU viser at 0,8 % (6/749) av virksomhetene har rapportert at de har opplevd datatyveri. Igjen viser tallene for ISF-U at prosentandelen virksomheter som har rapportert dette er høyere – 6,5 % (2/31). En av ISF-U-virksomhetene hadde opplevd 11-20 tilfeller av datatyveri. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene fortsatt er meget signifikante ($p < 0,01$). Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter ikke påvirker disse resultatene.

1 av ISF-U-virksomheten valgte å anmelde. Dataanalyse av MU viser at 7 virksomheter har valgt å anmelde. Når dataene undersøkes videre viser det seg at bare 3 av de virksomhetene som har anmeldt faktisk har rapportert å ha opplevd datatyveri, mens 4 virksomheter har anmeldt uten at de har rapportert at de har opplevd datatyveri. Vi har her valgt å se bort fra kjikvadrattesten.

C. Endring/sletting av data (uautorisert)

3,6 % av MUs respondenter hadde opplevd denne typen hendelser (27/749) og 2 av dem rapportert mellom 11-20 hendelser. Blant ISF-Us respondenter hadde 9,7 % av respondentene opplevd dette (3/31), hvorav 1 hadde opplevd mellom 6-10 hendelser. Statistisk analyse med kjikvadrat viser at resultatet ikke er signifikant ($p > 0,05$).

Ingen ISF-U-virksomheter valgte å anmelde. Blant MUs virksomheter var det 2 som valgte å anmelde. Den ene av disse virksomhetene var ikke registrert med at de hadde vært utsatt for endring/sletting av data.

D. Misbruk av IT-ressurser (PC/nett/server)

5,8 % av MUs virksomheter har erfart misbruk av IT-ressurser (43/749). Tilsvarende tall for ISF-U er markant høyere – 22,6 % (7/31). Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene ikke er signifikante. Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter her påvirker resultatene.

Til sammenligning var svarprosenten i ITAKT-undersøkelsen 7 % [59]. Her viser prosentandelen et større samsvar med den for MU.

Det var 3 MU-virksomheter og 1 ISF-U virksomhet som anmeldte. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$).

E. Spredning av ulovlig/opphavsrettslig beskyttet materiale (Copyright)

1,0 % (8/749) av MUs virksomheter rapporterte brudd på copyright, mens 6,5 % (2/31) av ISF-U-virksomhet rapporterte det samme. Av ISF-U virksomhetene rapporterte én mellom 11 og 20 brudd på copyright-reglene. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene ikke er signifikante. Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter her påvirker resultatene.

Ingen av virksomhetene i MU eller ISF-U valgte å anmelde forholdene.

F. Angrep på tilgjengelighet (DoS-angrep)

Det var 23 MU-virksomheter som rapporterte at de hadde vært utsatt for DoS-angrep (3,0 %). Ingen av ISF-Us virksomheter rapporterte dette. En MU-virksomhet rapporterte 99 DoS-angrep. Denne virksomheten hadde flere enn 500 ansatte, men vi anser likevel at dette kan være en feilrapportering og behandlet dette som en utligger.

I følge ITAKTs undersøkelse var det 5 % av virksomhetene som hadde oppdaget DoS-angrep [53].

Bare 1 av MUs respondenter som hadde anmeldt DoS-angrep, men denne virksomheten hadde ikke rapportert at de hadde vært utsatt for et slikt angrep.

G. Virus/orm/trojanerinfeksjon (virkelige infeksjoner)

188 MU-respondenter rapportert at de hadde vært utsatt for infeksjon av virus/orm/trojaner (25,1 %). Blant ISF-U var det 7 som hadde vært utsatt for tilsvarende (22,6 %). Statistisk analyse med kjikvadrat viser at resultatet ikke er signifikant ($p > 0,05$).

I Tabell 7 vises en oversikt over rapporteringer vi har utelatt i våre beregninger og den viser antall infeksjoner fordelt på MU-virksomhetenes størrelse. Vi har her valgt å presentere antallet virksomheter som har rapportert 30 infeksjoner eller flere. Når vi tok hensyn til uteliggere satt vi en grense ved 20 infeksjoner, selv om dette tallet også kan virke litt for høyt. Det er uansett litt påfallende at så mange som 7 MU-virksomheter rapporterte å ha hatt 30 eller flere virkelige infeksjoner og at hele 4 virksomheter hadde opplevde 99 infeksjoner. I MUs spørreskjema står det tydelig at de skal "*Spesifiser antall hendelser ikke hvor mange servere/klienter som ble infisert*" [60]. Når vi sammenstiller antall rapporterte infeksjoner med antall ansatte i de respektive virksomhetene kan det være en enda større grunn til å stille spørsmål om dette kan være rapportert korrekt. Kan en virksomhet med mellom 1-5 ansatte ha vært utsatt for 50 virkelige infeksjoner? Vi tror ikke det.

		Antall virksomheter som har rapportert mange virus/orm/trojanerinfeksjon (virkelige infeksjoner)		
Antall rapporterte infeksjoner		30	50	99
Hvor mange ansatte er det i virksomheten?	1-5	0	1	0
	6-10	0	1	0
	11-24	0	0	1
	25-199	0	0	3
	200-499	1	0	0
Total		1	2	4

Tabell 7: Antall infeksjoner fordelt på virksomhetenes størrelse

Et tilfelle av infeksjon er anmeldt av en MU-virksomhet – ingen av ISF-U-virksomhetene har anmeldt. Statistisk analyse med kjikvadrat viser at resultatet ikke er signifikant ($p = 0,870$).

H. Trusler om å angripe IT-systemer (utpressing)

0,4 % (3/749) av MUs respondenter hadde vært utsatt for utpressing. Tilsvarende tall for ISF-U er igjen høyere – 6,5 % (2/31). Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene ikke er signifikante. Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter her påvirker resultatene.

Den ene av ISF-U-virksomhetene valgte å anmelde trusselen. 1 av MU-virksomhetene har rapporter at de har vært utsatt for 30 tilfeller av utpressing. Dette er en virksomhet med mellom 6 og 10 ansatte. Vi anså denne rapporteringen for å være en uteligger.

Ved analyse av MU viser det seg at det er registrert at 3 virksomheter som ikke har vært utsatt for utpressing har anmeldt, mens de som ble utsatt for utpressing ikke valgte å anmelde. Det er her mye som tyder på at det er fortatt en feil når dataene ble registrert. Vi har her valgt å se bort fra kjikvadrat-testen.

I. Bedrageri ved misbruk av kredittkort over internett

Blant MUs virksomheter har 1,5 % (7/749) rapportert å ha vært utsatt for kredittkortbedrageri over Internett. Tilsvarende tall for ISF-U var også her høyere – 9,7 % (3/31). Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene fortsatt er meget signifikante ($p < 0,01$). Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter ikke påvirker disse resultatene.

En av MU-virksomhetene rapporterte 20 kredittkortbedrageri og alle ble anmeldt. I tillegg er det registrert 2 anmeldelser på en virksomhet som ikke har blitt utsatt for kredittkortbedrageri. 2 av ISF-U-virksomhetene valgte å anmelde. Vi har her valgt å se bort fra kjikvadrattesten.

J. Tyveri av IT-utstyr (PC, server, PDA etc.)

20,4 % (153/749) av MU-virksomhetene rapporterer å ha vært utsatt for tyveri av IT-utstyr, mot 45,2 % (14/31) av ISF-U-virksomhetene. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Når vi ser på resultatene for virksomheter med 200 ansatte eller flere viser kjikvadrattesten at resultatene ikke er signifikante. Følgelig kan vi konkludere at størrelsen på ISF-Us virksomheter her påvirker resultatene.

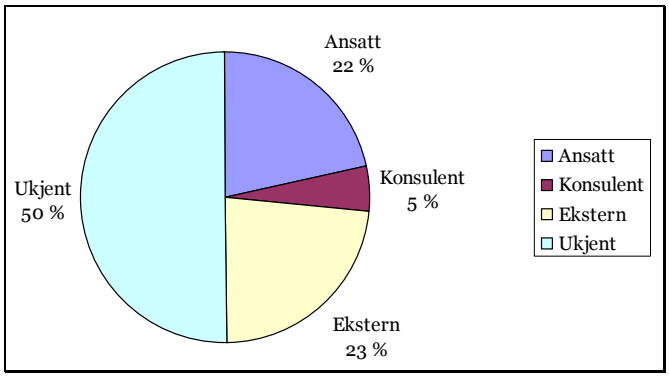
40 % av ITAKTs respondenter [59] hadde vært utsatt for tyveri av IT-utstyr og som vi ser er dette en prosentandel som korresponderer mer med resultatene fra ISF-U.

MU viser at 74,5 % (114/749) av de virksomhetene som ble utsatt for tyveri av IT-utstyr har anmeldt dette. 3 av MU-virksomhetene som rapporterte å ha anmeldt har ikke rapportert at de har blitt utsatt for IT-tyveri. 68,3 % (9/31) av ISF-U-virksomhetene valgte å anmelde. Statistisk analyse med kjikvadrat viser at resultatet ikke er signifikant ($p > 0,05$).

5.1.4 Gjerningsmenn

Vi fant det interessant å forsøke å gi et bilde hva hvem gjerningsmennene er i forbindelse med hendelsene som har blitt rapportert. Spørreskjemaet som ble benyttet i MU ga oss ikke den muligheten – hendelser og gjerningsmenn lot seg ikke krysskoble.

Når vi benytter datagrunnlaget fra MU og ISF-U kan vi presentere et relativt generelt bilde over forhold mellom de ulike kategoriene gjerningsmenn. Det stadfester til en viss grad det nokså kjente "20-80"-forholdet, her representert ved at 22 % av de som tår bak en hendelse er ansatte. Figur 10 viser fordeling av gjerningsmenn på kategorier.



Figur 10: Gjerningsmenn fordelt på kategorier

I CIO & PWCs undersøkelse fra 2005 svarte 63 % av virksomhetene at datakriminelle (hackere) sto bak datainnbruddene. 33 % svarte at ansatte gjorde, 20 % var tidligere ansatte, 11 % kunder og 25 % var ukjent [61].

Ved utformingen av ISF-U-spørreskjemaet forsøkte vi å få til en kobling mellom gjerningsmenn og hendelseskategoriene. Svakheten ved resultatene er at vi ikke kan få en direkte kobling mellom gjerningsmenn og hver enkelt hendelse virksomhetene har vært utsatt for. Det vi kan presentere er en oversikt som viser hvordan gjerningsmenn fordeler seg generelt på de enkelte hendelseskategoriene. En del av virksomhetene krysset av for flere gjerningsmenn i forhold til de forskjellige hendelseskategoriene og disse fremkommer under kolonnen "En kombinasjon" hvor numrene representerer de forutgående kolonnene – eksempelvis 1 = Ansatt. Tabell 8 viser at et flertall av gjerningsmennene er ukjent og da spesielt i kategorier som datainnbrudd, infeksjoner og tyveri. Mens ansatte har en mer fremtredende rolle i forhold til datatyveri, endring/sletting av data og misbruk av IT-ressurser.

	Gjerningsmenn						
	1 Ansatt	2 Konsulent	3 Ekstern	4 Ukjent	En kombinasjon		
					1,2	1,2,3	3,4
Datainnbrudd (hacking)			1	2			
Datatyveri – uautorisert lesing/kopiering av data	2						
Endring/sletting av data	2				1		
Misbruk av IT-ressurser	4				2	1	
Spredning av ulovlig/opp-havsrettslig beskyttet materiale	1					1	
Angrep på tilgjengelighet (DoS-angrep)							
Virus/orm/trojanerinfeksjon	1		1	4		1	
Trusler om å angripe IT-systemer (utpressing)			1	1			
Bedrageri ved misbruk av kredittkort over internett				1		1	
Tyveri av IT-utstyr			4	7			2
Totalt	10	0	7	15	3	4	2

Tabell 8: Gjerningsmenn fordelt på hendelseskategorier

5.2 Hvorfor anmelder ikke flere virksomheter datakriminalitet?

"Norske virksomheter anmelder ikke datakriminalitet fordi de ikke vet at de er tatt før det har gått for lang tid (1–6 måneder)."

"I en periode hadde jeg kontroll på 150.000 mailadresser hos 4 forskjellige ISP`r, hadde også admin tilgang på nesten alle komponentene deres (radius ol). I den perioden kunne jeg ta ned flere ISP`r i løpet av et par minutter. De fikk vite det når det ikke var spennende lenger."

NN

"I noen tilfeller kontaktes Kripos av virksomheter som utsettes for/har vært utsatt for datakriminalitet og man starter en etterforskning uten en anmeldelse. I ettertid kan det vise seg at virksomheten endrer oppfatning og velger å ikke anmelde saken. Dette oppleves som frustrerende for politiet, spesielt med tanke på at man da har lagt beslag på deres begrensede ressurser. Kripos kan selv begjære påtale for straffbare forhold som er undergitt offentlig påtale, men det blir gjort forholdsvis sjelden."

Kripos

Gjennom våre intervjuer har det kommet frem at flere av våre virksomheter hadde dokumentert og implementert policy og retningslinjer for informasjonssikkerhet før de ble utsatt for datakriminelle hendelser, men at de ikke hadde prosedyrer for håndtering av disse hendelsene. Når de så ble utsatt for hendelsene var det for de fleste av dem en stor usikkerhet knyttet til hvordan de skulle håndtere hendelsen. De var usikre på om virksomheten selv måtte sikre elektroniske bevis og i så fall hvordan dette skulle gjøres. Dessuten visste de ikke hvilke bevis som ville være vesentlige. Videre var de usikre på hvem de skulle anmelde til, Kripos (eller tidligere datakrimavdelingen i Økokrim) eller nærmeste politikammer. Mange hadde kontakter innen informasjons-sikkerhetsmiljøet og hadde hørt at politiets ressurser og kompetanse var begrenset, og at selv om det fantes kompetanse i Kripos (Økokrim) så var ressursene få. Noen av virksomhetene hadde ingen erfaring med den rent formelle delen av å anmelde en sak (hendelse) og visste heller ikke hvem i virksomheten som hadde myndighet til å gjøre dette.

Så for de fleste av våre virksomheter ble prosessen i forhold til anmeldelse av den første datakriminelle saken en relativt tung prosess, med en bratt læringskurve. Basert på dette er vi derfor av den formening at dette også kan være tilfelle for mange andre virksomheter som utsettes for datakriminelle hendelser, og at denne kombinasjonen av usikkerhetsmomenter kan føre til at en del virksomheter heller velger å unnlate å anmelde datakriminelle hendelser.

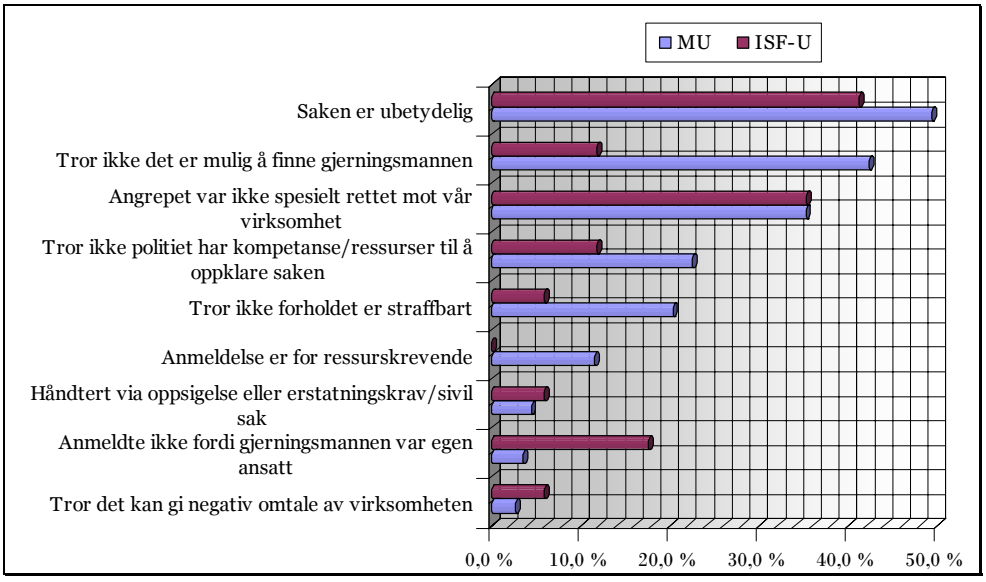
Videre har enkelte av virksomhetene påpekt at det er en økonomisk belastning ved etterforskning av datakriminelle hendelser, dersom virksomheten selv må besørge den. Virksomheter som har vært utsatt for en datakriminell hendelse, og velger å anmelde denne, kan potensielt dra på seg kostnader på mellom 200'-400' i forbindelse med etterforskningsbistand dersom de selv ikke har personale som kan etterforske hendelsen og må benytte ekstern ekspertise. Det er ingen garanti for at sakene vil ende opp i rettsapparatet selv om det finnes tilstrekkelige bevis og dokumentasjon. For virksomheter som har vært igjennom slike erfaringer kan konsekvensen være at de ikke ønsker å anmelde dersom de utsettes for en ny hendelse.

Spørsmålsstillingen i MU, og følgelig også i ISF-U, gir oss beklageligvis ikke muligheten til å se sammenhengen mellom type hendelse og årsak til at virksomheter ikke anmelder. Noe som vi anser at ville ha vært meget interessant og relevant når vi skal diskutere årsaker til at datakriminalitet ikke anmeldes.

Våre resultater fra spørreundersøkelsen viser at hovedårsaken til at MUs og ISF-Us respondenter ikke anmeldte datakriminalitet var at de mente at saken var for ubetydelig – henholdsvis 49,3 % og 41,2 %. Med tanke på at infeksjon av virus/orm/trojaner var den største kategorien av hendelser kan vi kanskje anta at det er en sammenheng mellom denne kategorien og årsaken til at virksomheter mente at saken var ubetydelig. Hele 42,2 % av MUs respondenter mente at det ikke ville være mulig å finne gjerningsmannen, mens det blant ISF-Us respondenter var 11,8 % som var av samme oppfatning. Statisk analyse med kjikvadrat viser at resultatet er signifikant ($p < 0,05$).

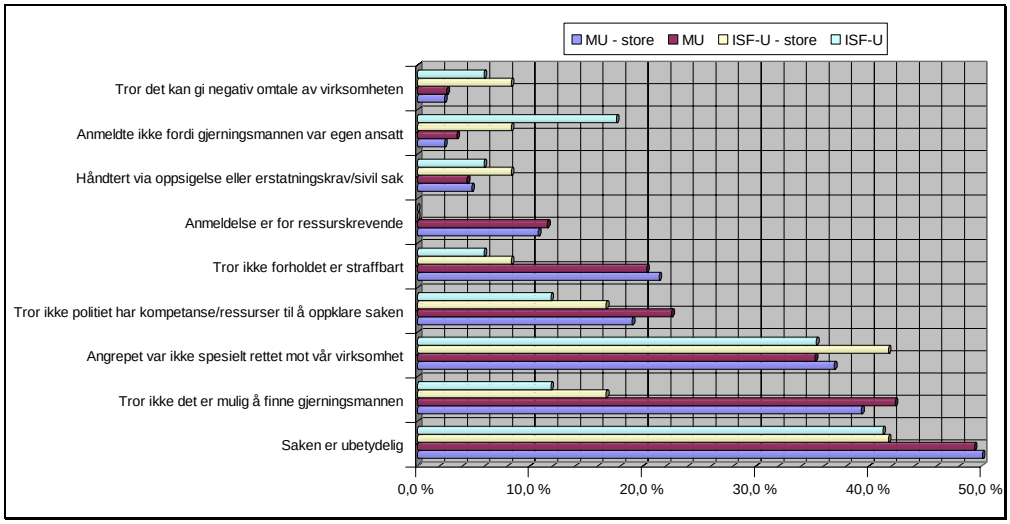
I forhold til virksomheter som ikke valgte å anmelde fordi "gjerningsmannen var en egen ansatt" fikk vi et meget signifikant resultat ($p < 0,01$). 17,6 % av ISF-Us respondenter svarte dette, mens 3,5 % av MUs ga samme svar. Ut fra dette skulle vi kanskje anta at flere av ISF-Us respondenter hadde valgt å håndtere hendelsen via oppsigelse eller erstatningskrav/sivil sak, men resultatene viser at det ikke er statistisk signifikans i forhold til dette og at 5,9 % i ISF-U og 4,4 % i MU valgte denne løsningen.

I Figur 11 vises oversikt over årsaker til at virksomhetene ikke anmeldte datakriminelle hendelser. For de øvrige kategoriene var det ingen signifikante resultater, men det bør bemerkes at ingen i ISF-U mente at anmeldelse var for ressurskrevende. Hele 20,3 % av MUs respondenter trodde at forholdet ikke var straffbart, noe som kanskje kan reflektere at gjeldende straffebud for datakriminalitet kan være litt vanskelig å tolke for virksomhetene. For ISF-U var det tilsvarende tallet 5,9 %.



Figur 11: Årsaker til at virksomheter ikke anmeldte datakriminelle hendelser

Vi har også valgt å se på om virksomhetens størrelse har noen innvirkning på årsaken til at de ikke velger å anmelde. I Figur 12 representer "MU – store" og "ISF-U – store" virksomheter med 200 ansatte eller flere. MU og ISF-U representerer hele datagrunnlaget. Vi ser at forskjellene mellom store MU-virksomheter og det total grunnlaget for MU ikke er særlig betydelig, mens det for ISF-U viser litt større variasjoner for enkelte av kategoriene. Eksempelvis svarte 8,3 % av de store ISF-U-virksomhetene at de ikke anmeldte fordi gjerningsmannen var egen ansatt, mens det tilsvarende tallet for hele ISF-U-grunnlaget er 17,6 %.



Figur 12: Årsaker til at virksomheter ikke anmeldte datakriminelle hendelser – store virksomheter skilt ut

5.3 Hva skjer dersom datakriminalitet anmeldes?

Resultatene fra våre intervjuer viser at 33 saker ble anmeldt til politiet/Kripos. Av disse ble 29 henlagt av ulike årsaker og i forhold til 2 saker vet ikke de respektive virksomhetene hva utfallet har blitt, men antar at sakene er henlagt. I forhold til den siste saken antas det at den fortsatt er under etterforskning. I en av de 33 sakene har det blitt domfellelse og denne saken omhandlet tyveri av IT-utstyr. De fleste av virksomhetene har opplevd en rekke tyverier av IT-utstyr og anmelder konsekvent alle tilfeller.

En virksomhet har vært utsatt for en rekke DoS-angrep, men har valgt å bruke ressursene på bedre sikring fremfor egen etterforskning og anmeldelse. Likeledes har en virksomhet som har opplevd en rekke tilfeller av spredning av ulovlig/opphavsrettslig materiale valgt å håndtere hendelsene som personalsaker i stedet for å anmelde. De aller fleste har rapportert at de har erfart infeksjon av virus/orm/trojaner, men bare en virksomhet har anmeldt. En virksomhet informerte at de har vært utsatt for en rekke forsøk på trojanerinfeksjoner, men anser ikke disse for å være direkte rettet mot virksomheten.

De aller fleste av sakene har vært tyveri av IT-utstyr og i forhold til dette har det vært mulig for virksomhetene å beregne økonomisk tap i forhold til hendelsene. I forbindelse med de øvrige sakene har ingen kunnet dokumentere hva det økonomisk tapet var.

Videre i dette kapitlet presenterer vi et utdrag av resultatene fra våre intervjuer. Det redegjøres for et utvalg av hendelser virksomhetene har vært utsatt for. Hendelsene er gruppert i henhold til de kategoriene som er brukt tidligere i oppgaven.

5.3.1 Datainnbrudd (hacking)

Hendelse 1:

Virksomheten ble i 2005 utsatt for et forsøk på datainnbrudd. Datainnbruddet var rettet mot virksomhetens nettsted. Innbruddforsøket ble oppdaget av deres tjenesteleverandør. Virksomheten ble varslet umiddelbart og trafikken fra "angriper" ble filtrert bort. Angrepet ble ikke ansett for å være særlig avansert. Det var et forsøk på å oppnå tilgang ved å benytte kjente sikkerhetshull. Angrepet skjedde via en annen norsk bedrift, som var kompromittert. Bedriften hvor angrepet kom fra, ble varslet. Virksomheten sporet angrepet så langt tilbake som mulig og det så tilsynelatende ut som om det kom fra Øst-Europa. Det var mye materiale/logger å gå gjennom og således en ressurskrevende operasjon. Utover dette anses det ikke for å ha medført noe økonomisk tap.

Virksomheten hadde i forkant av hendelsen ikke foretatt en prinsipiell og dokumentert avgjørelse av hvorvidt slike typer hendelser skulle anmeldes, men når saken ble presentert for ledelsen ble det umiddelbart besluttet å anmelde. Virksomheten hadde en dokumentert prosedyre for generell anmeldelse, men denne var ikke kjent for de personene som håndterte hendelsen. Anmeldelsen og bevismaterialet ble levert 2 dager etter at hendelsen hadde skjedd.

Virksomheten mottok bekreftelse av anmeldelsen fra politiet og ca. 2 måneder etter et brev om at saken var henlagt. Brevet ble i utgangspunktet sendt til en annen del av organisasjonen og det tok noe tid før de som hadde håndtert hendelsen ble varslet om utfallet av saken.

Hendelse 2:

Virksomheten ble utsatt for "aggressiv" skanning av nettet. Dette ble gjort gjennom bruk av en autorisert VPN-konto. Angrepet startet fra Russland og etter 10 min ble det startet skanning fra samme VPN-konto fra Tyskland (denne informasjonen ble hentet fra loggene). Angrepet ble oppdaget fordi loggene vokste raskere enn normalt, noe som ført til alarmer i HP Open View. Angrepet skjedde på formiddagen (ca. kl. 10) og ble oppdaget ganske raskt, men pga av den eksterne nettverksleverandøren ble ikke VPN-kontoen deaktivert før etter 4 timer. Det antas at angriperne i løpet av denne tiden fikk inngående kjennskap til virksomhetens nettverk. Virksomheten hadde ikke en egen konsolltilgang til nettet og loggene, følgelig var de avhengig av bistand fra leverandøren for å få hentet ut logger og informasjon om aksesspunkter. Det tok lang tid før leverandøren utleverte loggene. Når virksomheten fikk loggene viste de at det var ringt fra telefonnumre i Russland og Tyskland.

Basert på data fra loggene (fra leverandøren og egen IDS) ble det laget en oversikt over hendelsesforløpet med informasjon om hva som hadde skjedd, når og hvor angrepet kom fra. Virksomheten visste ikke med sikkerhet om angriperne hadde gjort noe galt. Alle systemer virket som normalt, men de hadde ingen visshet om hvorvidt angriperne hadde skaffet seg data eller aksess til mer enn nettet. (Ved en oppringt VPN-forbindelse gis det bare tilgang til en visst nivå.) Dagen etter angrepet ble CEO kontaktet og informert om angrepet så vel som mulige følgeskader (eksempelvis datatyveri). Det ble besluttet å anmelde forholdet.

Bevissikringen skjedde vet at alle logger ble brent på CD. Virksomheten hadde ikke dublerte servere, så speiling av disker var ikke mulig. Videre var det ikke mulig eller ønskelig å stenge noen systemer da dette kunne føre til direkte økonomiske tap. Virksomheten har ikke kjennskap til om bevissikringen som ble foretatt ville vært tilstrekkelig/tilfredsstillende i en eventuell rettssak.

Økokrim ble kontaktet via telefon og saken ble presentert. Den umiddelbare tilbakemelding virksomheten fikk var at saken nok ikke ville bli etterforsket på grunn av ressursmangel og sakens natur – at de ikke kunne påvise at skade hadde skjedd, at ikke systemene gikk ned, virksomhetskritiske data var ikke borte. Men, at de likevel burde anmelde.

På grunn av anbefalninger fra andre i sikkerhetsmiljøet valgte virksomheten å anmelde saken til Oslo politikammer (i stedet for Asker og Bærum). Anmeldelsen med bevismateriale ble overlevert Oslo Politikammer 3-4 dager etter angrepet. Etter en tid mottok virksomheten en anmeldelsesbekreftelse. Noen måneder etter fikk de beskjed om at saken var henlagt. Det antas at politiet bare vurderte saken uten å foreta noen videre etterforskning.

I 2005 var det et par tilfeller med misbruk av autoriserte VPN-kontoer. Kontoene tilhørte personer som satt på huset når det skjedde. Ved hjelp av nettverksleverandøren ble kontoene deaktivert, men også denne gangen tok det tid. På bakgrunn av erfaring fra den første hendelsen ble hendelsene i 2005 ikke anmeldt. Det ble skrevet en hendelsesrapport og gjort nødvendige tiltak. Hendelsen ble også inkludert i rutinemessig rapportering til ledelsen.

Hendelse 3:

I 2004 ble virksomheten utsatt for datainnbrudd. Det oppdaget at "fingerprint" ved ssh-innlogging til en e-postserver, med 50.000 brukere, var endret. Endringen medførte at virksomheten ikke kunne logge seg på serveren. Ved undersøkelser av andre servere på segmentet viste seg at det kun var den ene serveren som var kompromittert. Av den berørte serverens to disker var det en som var inntakt og denne ble fjernet for bevissikring. Den andre ble brukt til å bygge opp systemet igjen. Angrepet ble oppdaget av eksternt vedlikeholdspersonale og fra angrepet ble oppdaget til serveren ble tatt av nettet tok det 1 1/2 time.

Virksomheten kontaktet politiet og fikk beskjed om at politiet ikke hadde ressurser til å bistå i etterforskningen. Virksomheten ble rådet til å leie inn ekstern hjelp for bevissikring og dokumentasjon av angrepet. Ekstern ekspertise ble leid inn og bistod med bevissikring av logger og dokumentasjon av hendelsesforløpet. Intern etterforskning

viste at serverens Linux-kjerne var manipulert og de fleste systemfilene var erstattet med trojanere.

Man anser at det økonomiske tapet virksomheten led, som følge av hendelsen, i hovedsak var relatert til utgiftene knyttet til innleie av ekstern ekspertise. Virksomheten besluttet raskt at hendelsen skulle anmeldes, men prosessen i forhold til finne ut hvilken instans de skulle anmelde til tok relativt lang tid.

Anmeldelse av hendelsen ble levert Oslo Politidistrikt 18 dager etter hendelsen. Virksomheten fikk beskjed om at politiet hadde greid å spore angrepet utenlands – Tyskland. Etter 3 måneder mottok virksomheten beskjed fra politiet om at saken var henlagt fordi det ikke var "*fremkommet tilstrekkelig opplysninger til å identifisere gjerningsmannen*". Virksomheten hadde noe telefonisk kontakt med politiet før henleggelsen.

Hendelse 4:

I 1999 ble det ved rutinemessig monitorering av nettverket oppdaget unormal nettverkstrafikk i det interne nettet. Etter litt intern etterforskning klarte de å dokumentere hva som skjedde og hvilke maskiner som var involvert. Det viste seg at 2 ansatte hadde installert en bakdør (SubSeven) på deres overordnedes pc-er for å overvåke deres aktiviteter. Maskinene ble beslaglagt og analysert og forholdet anmeldt. Virksomheten hadde sikret bevis ved å speile diskene på pc-ene og kjøre etterforskning på de kopierte diskene. Alt bevismateriale – original disker, logger, dokumentasjon etc. – ble overlevert Økokrim. Virksomheten bistod også Økokrim i den videre etterforskningen. Gjerningsmennene ble avhørt av Økokrim og ga full tilståelse. Motiv for handlingen hadde vært spenning og nysgjerrighet. Av prinsipielle årsaker var Økokrim interessert i å forfølge saken. Dette var en type sak som ikke hadde vært prøvd for en rettsinstans tidligere. Rettsprøvelse av saken ble stoppet og årsaken til dette var at det ikke var mulig å dokumentere et økonomisk tap. Følgelig ble saken henlagt. Gjerningsmennene ble avskjediget.

5.3.2 Datatyveri – uautorisert lesing/kopiering av data

Hendelse 1:

I 2003 ble det oppdaget at en tidligere ansatt hadde tatt med seg deler av virksomhetens malverk når vedkommende sluttet. Vedkommende hadde startet eget konkurrerende firma og benyttet virksomhetens malverk ved utarbeidelse av tilbud. Dette ble oppdaget da virksomheten fikk et tilbud elektronisk og ved selvsyn kunne se en påfallende likhet med eget malverk. I tillegg viste egenskaper for dokumentet virksomheten som eier. Hendelsen var å anse som datatyveri og ble umiddelbart anmeldt. Selv om virksomheten ikke anså saken for å være alvorlig mente de at det prinsipielt sett var viktig å anmelde. Det ble benyttet intern juridisk bistand i forbindelse med anmeldelsen. Det er usikkert hva som har skjedd videre med saken.

Hendelse 2:

Virksomheten har vært utsatt for publisering av konfidensiell informasjon på Internett. Utenlandske server ble brukt til å publisere informasjonen og det ble brukte chatte-kanaler til å formidle linker til disse serverne. Virksomheten fant ut hvor serverne befant seg, men anså at det ikke ville la seg gjøre å få stoppet dem. Dessuten kunne materialet lett flyttes over til nye servere. Det var ikke mulig for virksomheten å finne ut hvem som hadde foretatt publiseringen. Det ble besluttet å ikke anmelde saken.

5.3.3 Endring/sletting av data (uautorisert)

Hendelse:

Virksomheten har vært utsatt for "defacing" (endring) av dens websider. Litt intern etterforskning viste at angrepet tilsynelatende kom fra Brasil. Det var bare forsider som var endret og det var tilsynelatende ikke gjort forsøk på ytterligere skade. Defacing skjedde i løpet av en helg og ble oppdaget før mandagen etter. Den skjedde noen måneder i forkant av et datainnbrudd og det ble etter datainnbruddet ikke vurdert om defacingen hadde vært en forløper til datainnbruddet. Virksomheten valgte ikke å anmelde hendelsen.

5.3.4 Misbruk av IT-ressurser (PC/nett/server)

Hendelser:

Virksomheten har hatt hendelser hvor ansatte har utnyttet jobb e-postsystemer til å sende mindre hyggelige/upassende e-post. Virksomheten skanner ikke e-poster for innhold og har derfor ikke vært oppmerksom på hendelsene før de har blitt kontaktet av politiet. I virksomhetens policy for informasjonssikkerhet er det dokumentert at misbruk av virksomhetens e-postsystemer vil kunne føre til personalsak. I forbindelse med enkelte hendelser, som har ført til straffesak, har virksomhetens dokumentasjon har vært en del av bevismaterialet. Dette gjelder spesielt e-post og logger.

5.3.5 Spredning av ulovlig/opphavsrettslig beskyttet materiale

Hendelse:

Virksomheten har ved flere anledninger hatt hendelser i forhold til ulovlig distribusjon av opphavsrettsmateriale – fildeling. I praksis sperres det ikke for slikt da det har liten hensikt, eksempelvis er det fildelingsprogrammer som benytter port 80. Virksomheten har løsninger som detekterer fildeling og dersom slike hendelser skjer blir dette håndtert som personalsak og anmeldes vanligvis ikke. Periodisk skannes server med henblikk på ressursbruk. Dersom det oppdages store mengder av video- og musikkfiler håndteres det også som en personalsak.

5.3.6 Angrep på tilgjengelighet (DoS-angrep)

Hendelse:

Virksomheten har vært utsatt for DoS-angrep mot infrastrukturen. Disse angrepene har ikke vært motivert av utpressing, men har ført til at virksomheten har vært uten utenlandsforbindelse i noen timer på grunn av angrepene. Virksomheten har bevisst valgt å bruke lite ressurser på å finne ut hvor DoS-angrepene kommer fra, men heller valgt å sette inn ressurser på å lage et godt forsvar mot angrepene. Blant annet har de valgt å stoppe eventuelle DoS-angrep i kantruterne. Dette krever mye manuelt arbeid, men anses for å være viktigere enn å etterforske selve angrepene. Virksomheten har ikke anmeldt DoS-angrep.

5.3.7 Virus/orm/trojanerinfeksjon (virkelige infeksjoner)

Hendelse 1:

Sommeren 2006 ble virksomheten varslet av et sikkerhetsfirma om at de hadde funnet en trojaner som var skrevet/rettet mot virksomheten. Saken ble anmeldt og etterforsket. Etterforskningen viste at angrepet var rettet fra utlandske ressurser og ble henlagt fordi oppklaring av saken ville bli for ressurskrevende for politiet. Virksomheten mottok beskjed om henleggelse 4 måneder etter anmeldelsen.

Virksomheten har i den senere tid hatt flere hendelser knyttet til trojanere og alle disse sakene er anmeldt av de enkelte juridiske enhetene som er en del av virksomheten.

Hendelse 2:

Virksomheten oppdaget i 2006 en trojaner på en intern pc. Denne trojaneren fanget opp og sendte brukernavn og passord til en adresse i Russland. Hendelsen ble fanget opp av IDS-løsningen og den eksterne leverandøren varslet virksomheten. Eier av brukerkontoen ble kontaktet og pc-en ble koblet av nettet og reinstallert. Brukeren fikk logget på fra en annen pc og endret passordet sitt. Senere på kvelden ble brukerkontoen automatisk stengt en periode som en følge av at det ble gjort gjentatte påloggingsforsøk fra uvedkommende med det gamle passordet. Saken ble ikke anmeldt da prosessen ble antatt for å være for ressurskrevende og fordi virksomheten ikke antok at det var noe økonomisk tap. I tillegg ble det også vurdert dit hen at siden angrepet tilsynelatende kom fra Russland, ville det være heller vanskelig å finne gjerningspersonen og å få vedkommende straffeforfulgt.

Hendelse 3:

Det har vært hendelser som virksomhetens kunder har vært utsatt for, som har ført til et så pass stort økonomisk tap at kunder har rettet krav til den/de som var ansvarlig for hendelsen. Eksempelvis benyttet en innleid konsulent hos en kunde MSN til å chatte med kontakter utenfor kundens interne nett. I tillegg til at dette var et brudd på kundens informasjonssikkerhetspolicy, medførte hendelsen at 300-400 klienter hos kunden ble infisert med virus. Følgende av denne saken var at konsulentfirmaet mottok en regning fra virksomheten på ca. 300.000 kroner for rensing av klientene hos kunden. Hendelsen ble ikke anmeldt av kunden.

5.3.8 Tyveri av IT-utstyr (PC, server, PDA etc.)

Hendelser 1:

Sommeren 2006 ble virksomheten utsatt for tyveri av bærbare pc-er, pda-er etc. Utstyret ble stjålet fra virksomhetens lokaler og ble derfor ansett for å være en meget alvorlig hendelse. Basert på tips fra ansatte ble en person anhold av sikkerhetsvakter. Personen hadde ikke tyvegodset på seg, men hadde ingen gyldig grunn for å oppholde seg i bygget. Politiet ble tilkalt og de brukte 2 dager på bevissikring og dokumentasjon av forholdet. Vedkommende ble dømt til ubetinget fengsel, men utstyret som ble stjålet kunne ikke oppspores og returneres til virksomheten. Det tok 5 måneder fra hendelse til domfellelse. Virksomheten antar at vedkommende også var siktet for andre forhold. Det økonomiske tapet ble beregnet til kr. 50.000.

Virksomheten har hatt 5 tyverier av IT-utstyr det siste året. Blant annet tyveri av bærbare pc-er fra bil. Alle sakene har blitt anmeldte og de fleste av dem henlagt relativt fort – ca. 1 måned etter anmeldelsen.

Hendelser 2:

Virksomheten holder til på flere lokasjoner og har blant annet lokaler i et hardt kriminelt belastet område. De vært utsatt for innbrudd og tyveri av bærbare pc-er. I et tilfelle tok gjerningsmennene seg inn via et vindu – med montert sikkerhetsglass – i underetasjen. En bærbar pc ble stjålet. Pc-en tilhørte en innleid konsulent. Det er usikkert hvorvidt pc-ens harddisk var kryptert. Virksomheten var opptatt av om hvorvidt pc-en inneholdt data som var virksomhetens, men de anser at tyveriet var en vinningsforbrytelse. Hendelsen ble anmeldt påfølgende dag og etter en tid fikk de beskjed om at politiet hadde henlagt saken.

Det har også vært tyveri av bærbar pc fra en annen lokasjon. Pc-en var ikke utstyrt med harddiskkryptering, men virksomheten anser ikke at den inneholdt konfidensielle data. Hendelsen ble anmeldt og henlagt.

Hittil i 2007 har virksomheten vært utsatt for 4 tyverier. Hvorav det siste rett etter påske. 18 maskiner og en projektor ble stjålet. Gjerningsmannen er kjent og forholdet anmeldt.

Hendelser 3:

Virksomheten holder til på flere lokasjoner. De har opplevd innbrudd og tyveri av bærbare pc-er etc. I et tilfelle ble pc-en til en sikkerhetsansvarlig stjålet. På den tiden var det en tyveribande som opererte i området og brøt seg inn og stjal IT-utstyr fra flere virksomheter. Følgelig anses det at tyveriene var vinningsforbrytelser og at det ikke var interesse for dataene på de bærbare pc-ene. Forholdet ble anmeldt og deretter henlagt av politiet.

5.3.9 Andre straffbare hendelser

Hendelse 1:

Virksomheten gjennomfører periodisk søk i surfeloggene for å avdekke om ansatte surfer på nettsteder som inneholder ulovlig materiale – både i henhold til straffeloven og i henhold til virksomhetens policy. I 2003 ble det ved gjennomgang av surfeloggene fattet mistanke om at en ansatt hadde surfet på barneporno. Ved nærmere granskning ble det verifisert at vedkommende hadde surfet på barneporno og at vedkommende hadde besøk mange nettsteder som inneholdt barneporno. En av virksomhetens direktører ble varslet om forholdet og det ble umiddelbart besluttet at forholdet måtte anmeldes.

Man tok en innledende kontakt med Økokrim fordi virksomheten hadde et behov for bistand i den videre håndteringen av saken. Det ble fremlagt utskrift fra loggene og Økokrims representant kunne bekrefte at dette var kjente barnepornosider. Virksomheten følte at de hadde en god dialog med Økokrim, men fordi Økokrim ikke hadde ressurser nok måtte virksomheten selv gjøre alt det grunnleggende etterforskningsarbeidet. De fikk generell informasjon fra Økokrim om hvordan de skulle anmelde.

Det gikk 2-3 uker fra forholdet ble oppdaget til anmeldelse ble levert. Økokrims oppsett for anmeldelse ble benyttet og virksomhetens egne advokater utferdiget anmeldelsen. Det var først ved utarbeidelse av anmeldelsen at det ble dokumentert en sammenheng mellom IP-adresse og vedkommendes navn.

Per i dag vet virksomheten fortsatt ikke hva som har skjedd videre med saken. De første par årene etter anmeldelse ringte de jevnlig for å forhøre seg, men så ble det besluttet at det beste var å legge saken bak seg.

Sakens natur førte til at den etterforskningen virksomheten selv måtte gjennomføre var en sterk belastning for ressursene som utførte den. Virksomheten påpeker at etterforskning av barnepornosaker er ikke noe som legfolk er trent i å håndtere. De føler også en stor usikkerhet knyttet til om de gjennomført en tilstrekkelig bevissikring og om dokumentasjonen var god nok.

5.4 Hva kan gjøres for å flere til å anmelde datakriminalitet?

Gjennom de siste årene har de fleste virksomheter forstått behovet av å ha dokumentert og implementert policy og retningslinjer for informasjonssikkerhet. En del, spesielt større virksomheter, har også sett nødvendigheten av å dokumentere og implementere planer for kontinuitet, herunder kriseplaner, katastrofeplaner osv. Dette skyldes til en viss grad at de er underlagt krav fra offentlige myndigheter. Eksempelvis så plikter virksomheter som omfattes av Kredittilsynets IKT-forskrift å ha oppdaterte kontinuitetsplaner [62] og virksomheter som behandler personopplysninger er av Datatilsynet pålagt å sikre tilgjenglighet til dataene [63].

Vi har gjennom vårt arbeid innen informasjonssikkerhet og vårt arbeid med denne oppgaven erfart at selv om en del virksomheter har implementert informasjonssikkerhetspolicy og -retningslinjer og kontinuitetsplaner, så er det et fåtall av dem som

i det hele tatt har vurdert å implementere prosedyrer for håndtering av datakriminelle hendelser. Skadeverk ved et alvorlig datainnbrudd eller DoS-angrep kan resultere i at en virksomhets informasjonssystemer blir utilgjengelige og da er det viktig at det på forhånd er dokumentert prosedyrer for hvordan slike hendelser skal håndteres.

I kapittel 5.3 beskrev vi at de fleste av våre virksomheter var helt utforberedt når de ble utsatt for den første datakriminelle hendelsen og følgelig førte det til at prosessen fra hendelsen ble oppdaget til anmeldelse ble levert var relativt tung og utfordrende. Flere av virksomhetene etterlyste informasjon om hvordan de skal håndtere datakriminalitet. De var videre usikre på om hvorvidt de egentlig var ansvarlig for å sikre elektroniske bevis eller om dette var en oppgave Kripos/politiet skulle håndtere. I tilfelle de var ansvarlige for å sikre bevis, ønsket de informasjon om hvordan dette burde gjøres for at bevisene skulle være tilstrekkelige i forbindelse med en eventuell rettssak.

Vi mener å kunne anta at dette er en virkelighet som rammer de aller fleste virksomheter når de utsettes for sin første datakriminelle hendelse. Derfor har vi valgt å utarbeide en veiledning for hvordan en datakriminell hendelse kan håndteres (Appendiks F). Veiledningen er utarbeidet etter rammeverk som ofte benyttes ved utarbeidelse av kriseplaner. Den inneholder informasjon om hva virksomheten bør ha gjort av forberedende arbeid. I tillegg er det utarbeidet vedlegg for:

- Hendelser, varsling og aktiviteter: Her spesifiseres forslag til hvem som intielt bør varsles ved forskjellige typer hendelser og hovedaktivitet som bør iverksettes.
- Hendelseslogg: For å dokumentere informasjon om hendelsen og alle aktiviteter som iverksettes, inklusive et skjema hvor det fylles ut om det er valgt å anmelde eller ikke.
- Interne og eksterne varslingslister: Navn på kontaktperson, telefonnummer etc.

Videre har vi utarbeidet en veiledning for sikring av elektroniske bevis (Appendiks G). Denne veiledningen er delt i 2. Del 1 omhandler logging og bevissikring av logger. Del 2 beskriver ytterligere bevissikring, eksempelvis av kompromitterte server. Vi har i denne delen valgt et detaljnivå som medfører at personer uten tilstrekkelig kompetanse innen området, ikke kan gjennomføre bevissikringen. Eksempelvis har vi ikke listet opp spesifikke verktøy/programmer som bør benyttes. Dette er et bevisst valg, fordi den bevissikringen som her omtales krever svært god kompetanse og erfaring ellers er det stor fare for at bevis kan bli ødelagt. Slik sett er denne delen av veiledningen mer en bevisstgjøring for hvor komplisert og omfattende dette arbeidet er, men kan også bidra til å hjelpe virksomheter som har ansatte med tilstrekkelig kompetanse.

Veiledningene er kvalitetssikret av NorSIS og ressurser ved datasikkerhetsmiljøet ved Oslo politidistrikt. Disse veiledningene skal distribueres av NorSIS til deres kontaktnettverk bestående av små og mellomstore virksomheter.

For øvrig er vårt inntrykk at vi i Norge har mye å lære av hvordan enkelte andre land har valgt å profilere deres enheter som arbeider med oppklaring av datakriminalitet, og at Internett aktivt bør benyttes som en informasjonskanal. Vi mener at det er et behov for at Kripos og politiet blir mer synlige for virksomhetene dersom de skal få flere til å anmelde datakriminalitet. Kripos har innsett dette og deltar på konferanser og seminarer, men de – og da mener vi spesifikt Datakrimavdelingen – bør også bli mer

synlige på Internett og Kripos sine websider slik vi har sett at noen av andre lands politimyndigheter er.

Videre er det også vesentlig at det i forbindelse med ny lovgivning i forhold til datakriminalitet aktivt jobbes for å informere virksomhetene slik at de større grad får en forståelse for hvilke handlinger som anses for å være straffbare. I MU rapporterte hele 20,3 % at de ikke trodde forholdet var straffbart. Dersom Kripos ikke har ressurser til eksempelvis å utarbeide informasjon til norske virksomheter, bør det være andre aktører, som ønsker å bidra til å bedre informasjonssikkerhet blant norske virksomheter, som kan ta denne utfordringen.

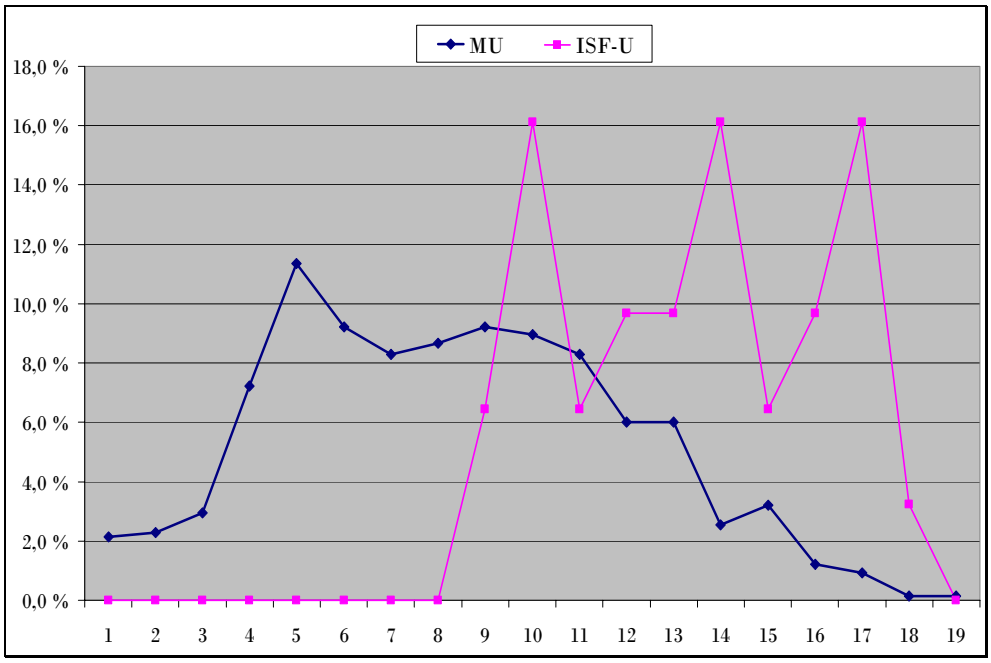
5.5 Håndteres informasjonssikkerhet forskjellig blant ISF-medlemmer og MUs respondenter?

> *"De 4-5 mest virkningsfulle sikringstiltakene for å unngå å bli hacket er antivirus, brannmur, sundt bondevett og opplæring av ansatte. IDS og IPS er tull, og spesielt dersom man lar andre enn sine egne overvåke trafikken, hvilken garanti har man for at konsulenten ikke sover, drikker, chatter med dama ol. Sistnevnte vet at foregår hos flere sikkerhetsleverandører som jeg har jobbet for."*
>
> NN

I dette kapitelet redegjør vi for hvorvidt det finnes forskjeller mellom MU og ISF bedrifter, med tanke på i hvilken grad tekniske og formelle tiltak er implementert i bedriftene, ved å sammenlikne de respektive undersøkelsene. Videre ser vi på om det er forskjeller mellom MUs og ISFs virksomheter når det gjelder kontroll og oppfølging, og tilslutt hvor hyppig det rapporteres og hvorvidt logger følges opp.

5.5.1 Tekniske sikringstiltak

I MU og ISF-U ble virksomhetene spurt om hvilke tekniske sikringstiltak de har implementert. I alt var det 19 potensielle sikringstiltak som det var mulig å krysse av for. I våre analyser har vi valgt å summere opp antall implementerte sikringstiltak per virksomhet. Det viser seg at det er en vesentlig forskjell mellom MU og ISF-U. I gjennomsnitt har ISF-Us respondenter implementert 13,42 sikringstiltak, men MUs respondenter har implementert 8,21. Statistisk analyse med kjikvadrat viser at resultatene er meget signifikante ($p < 0,01$). Det viser seg at 10 av MUs virksomheter har rapportert at de ikke har implementert noen tekniske sikringstiltak. Videre går det frem at ingen av ISF-Us virksomheter har implementert mindre enn 9 sikringstiltak, mens hele 52,1 % av MUs virksomheter har implementert 8 eller færre sikringstiltak. I Figur 13 presenteres antall sikringstiltak (X-aksen) og den prosentvise fordeling av virksomheter som har implementert dem (Y-aksen).



Figur 13: Antall tekniske sikringstiltak implementert av virksomhetene

I Tabell 9 viser vi oversikt over andel virksomheter som har implementert de forskjellige tekniske sikringstiltakene. Ved statistisk analyse av tekniske sikringstiltak viser at det seg at resultatene for 14 av 19 sikringstiltak er meget signifikante ($p < 0,01$). Bare i forbindelse med et av sikringstiltakene viser det seg at det var flere av MUs respondenter som hadde implementert tiltaket enn av ISF-Us. Dette er "Fysisk autentiseringsmekanismer" hvor tallene for MU var 14,4 % og tallene for ISF-U var 3,2 %. Forklaring til tabell: "++" = meget signifikant og "-" = ikke signifikant.

	MU	ISF-U	Signifikans
Virtuelt privat nettverk (VPN)	47,3 %	96,8 %	++
Ulike sikkerhetssoner i nettet	29,1 %	77,4 %	++
Personlige brannmurer	30,8 %	61,3 %	++
Kryptering av trådløse nettverk	30,3 %	64,5 %	++
Kryptering av bærbare media	11,5 %	48,4 %	++
Innbruddsdetekteringssystem (IDS)	15,9 %	48,4 %	++
Fysiske autentiserings mekanismer (f.eks. smartkort)	14,4 %	3,2 %	++
Duplisering av kritiske komponenter	25,9 %	87,1 %	++
Digital signatur	5,9 %	22,6 %	++
Avlåst datarom	49,5 %	96,8 %	++
Reservestrøm, UPS	64,6 %	93,5 %	++
Engangspassord	16,7 %	38,7 %	++
Filter mot uønsket web-trafikk	36,7 %	61,3 %	++
Spam-filter	76,9 %	96,8 %	++
Brannmur for nettverket	89,6 %	100,0 %	-
Personlig passord	92,3 %	100,0 %	-
Anti-virusprogramvare	92,5 %	100,0 %	-
Backup	88,5 %	96,8 %	-
Biometrisk autentisering (f.eks. fingeravtrykk)	2,5 %	3,2 %	-

Tabell 9: Oversikt over andel virksomheter fordelt på tekniske sikringstiltak

Vi kjørte en lineær regresjonsanalyse for å se på effekten av størrelse på bedrift og ISF-medlemsskap, som forklaring på varians i antall tiltak, og fant at den viktigste forklaringen var størrelse på virksomheten. Når vi korrigerte for bedriftsstørrelse viste det seg likevel at ISF-Us respondenter hadde implementert flere tiltak og at funnene er meget signifikante ($p < 0,01$).

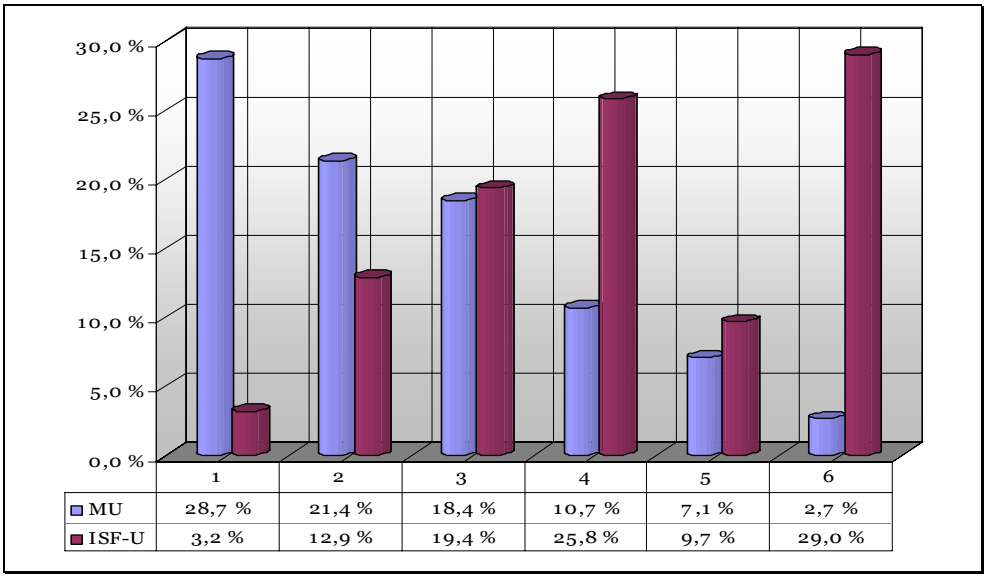
5.5.2 Formelle sikringstiltak

I MU og ISF-U er respondentene spurt om hvilke formelle sikringstiltak de har innført. Med formelle sikringstiltak mener vi dokumenterte og implementerte policyer/retningslinjer.

Følgende kategorier er listet opp:

- Virksomheten har utarbeidet retningslinjer for ansattes bruk av virksomhetens informasjonssystemer
- Ansatte må undertegne taushetserklæring
- Ansatte gis opplæring i sikker bruk av IT
- Virksomheten har utarbeidet planer for håndtering av de viktigste bruddene på informasjonssikkerheten
- Virksomheten gjennomfører systematiske katastrofe-/kriseøvelser knyttet til IT
- Virksomheten er i stand til å håndtere IT-sikkerhetsbrudd utenfor arbeidstiden

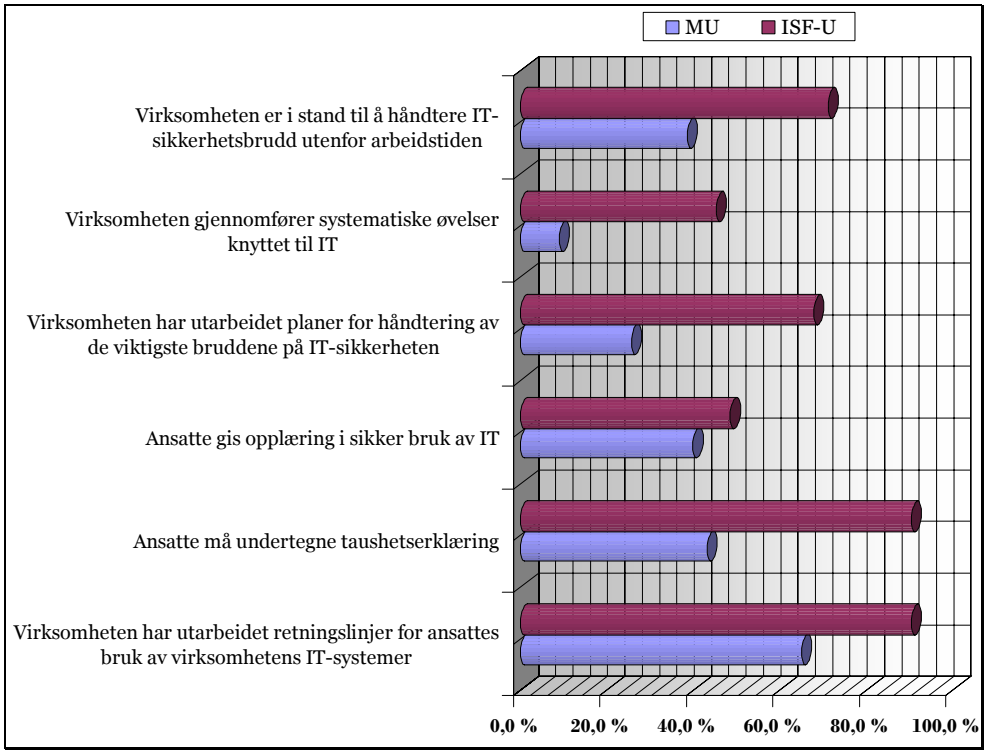
Vi har valgt å anse disse tiltakene for å være likeverdige. Videre oppsummerte vi antall tiltak per virksomhet - maksimalt antall tiltak var 6. Resultatene fra denne analysen viste at ISF-Us respondenter i større grad har implementert formelle sikringstiltak enn MUs og gjennomsnittet for antall tiltak var 4,1. Blant MUs respondenter var snittet på 2,2 implementerte tiltak. 83 av MUs respondenter har ikke rapportert at de har formelle sikringstiltak. Statistisk analyse med kjikvadrat viser at resultatet er meget signifikant ($p < 0,01$). Figur 14 viser oversikt over prosentandelen virksomheter som hadde implementert formelle sikringstiltak fordelt på antall innførte tiltak.



	1	2	3	4	5	6
MU	28,7 %	21,4 %	18,4 %	10,7 %	7,1 %	2,7 %
ISF-U	3,2 %	12,9 %	19,4 %	25,8 %	9,7 %	29,0 %

Figur 14: Antall formelle sikringstiltak implementert av virksomhetene

I Figur 15 presenteres en oversikt over prosentandelen virksomheter som har implementert tiltak fordelt på det enkelte tiltaket. Med unntak av et tiltak – "Ansatte gis opplæring i sikker bruk av IT" viser statistisk analyse med kjikvadrat at resultatene er meget signifikante ($p < 0,01$).



Figur 15: Virksomheter som har implementert formelle sikringstiltak

Vi har kjørt en Univariat variansanalyse hvor vi har korrigert for bedriftsstørrelse. Den viser at bedriftsstørrelse er den viktigste uavhengige variabelen. Når det korrigeres for den viser det seg likevel at ISF-Us respondenter har implementert flere tiltak og at funnene er meget signifikante ($p < 0,01$).

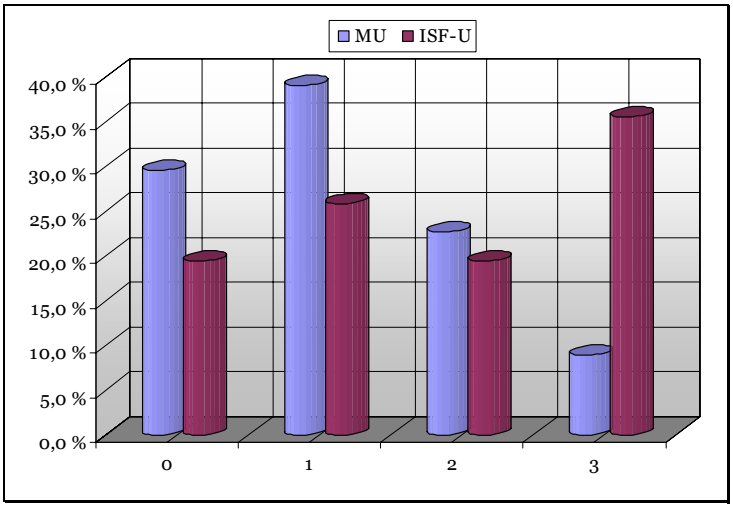
5.5.3 Kontroll og oppfølging

I spørreundersøkelsen ble det stilt spørsmål om hvilke tiltak som er innført i forbindelse med kontroll/revisjon og rapportering. Svaralternativene var:

- Intern revisjon/kontroll
- Ekstern revisjon/kontroll
- Rapportering til ledelse
- Liten eller ingen oppfølging (er ikke tatt med i resultatene)

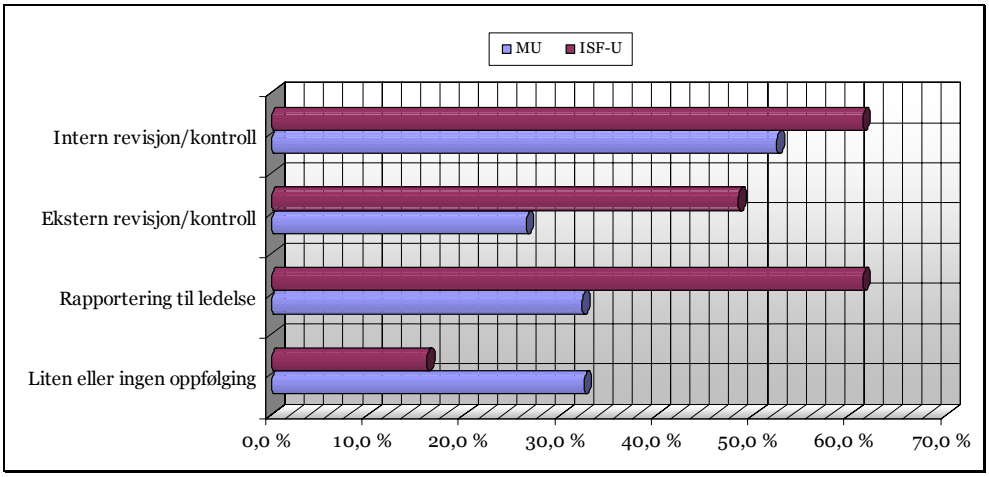
Vi valgte å se de første 3 alternativene som likeverdige og summerte opp antall tiltak per virksomhet. Gjennomsnittsverdien for MU var 1,1 og for ISF-U 1,7. ISF-U viser atter en gang bedre resultater og statistisk analyse med kjikvadrat viste at resultatet var meget signifikant ($p < 0,01$). 172 av MUs respondenter og 6 av ISF-Us har ikke besvart

dette spørsmålet. Figur 16 viser oversikt over antallet innførte tiltak for kontroll/revisjon og rapportering.



Figur 16: Antall implementert tiltak for kontroll/revisjon og rapportering

For kategoriene "Rapportering til ledelse" og "Ekstern revisjon/kontroll" viser statistisk analyse med kjikvadrat at resultatet er meget signifikant ($p < 0,01$). I Figur 17 presenteres oversikt over prosentandelen virksomheter som har implementert tiltak fordelt på det enkelte tiltaket.

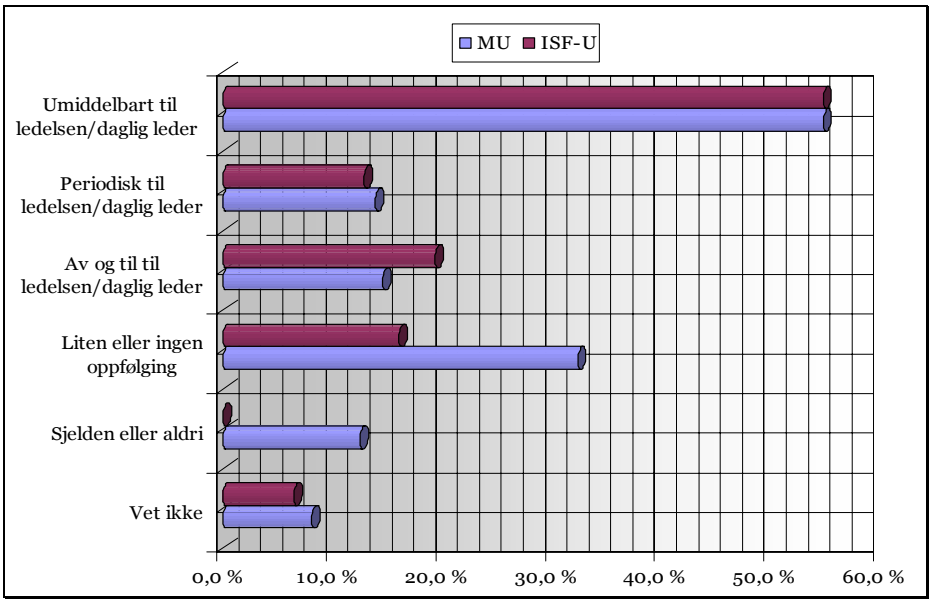


Figur 17: Virksomheter som har implementert tiltak for kontroll/revisjon og rapportering

Vi har kjørt en Univariat variansanalyse hvor vi har korrigert for bedriftsstørrelse. Den viser at bedriftsstørrelse er den viktigste uavhengige variabelen. Når det korrigeres for den viser det seg likevel at ISF-Us respondenter har implementert flere tiltak og at funnene er signifikante ($p < 0,05$).

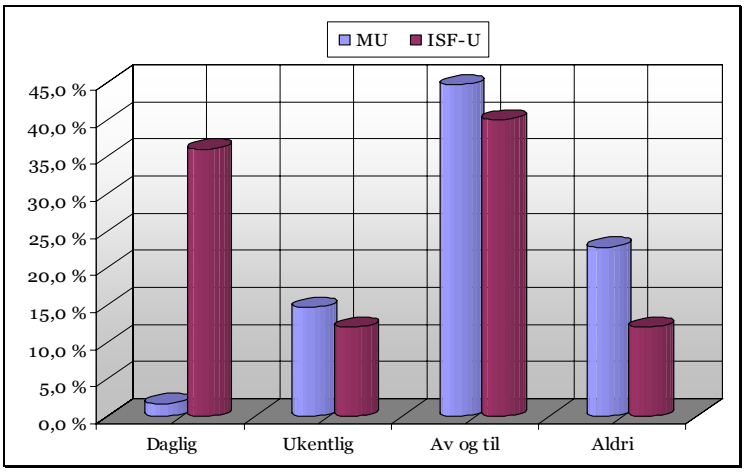
5.5.4 Rapportering og gjennomganger av logger

I forbindelse med spørsmål om hvor ofte det rapporteres til ledelsen har vi valgt å se bort fra statistiske analyser med kjikvadrat fordi noen av virksomhetene har krysset av for flere alternativer. Figur 18 viser imidlertid at det ikke er store forskjeller mellom ISF-U og MU. Et positivt signal er at så mange som 54,8 % (for både MU og ISF-U) rapporterer hendelser umiddelbart til ledelsen.



Figur 18: Hyppighet i forhold til rapportering til ledelsen

Våre analyser av gjennomgang av logger viser ved statistisk analyse med kjikvadrat at resultatene ikke er signifikante ($p > 0,05$). I Figur 19 viser vi hvor ofte virksomhetene gjennomgår logger. Den viser at 36,0 % av ISF-Us respondenter gjennomgår logger daglig, mens blant MUs er 17,7 % som gjør det. Ikke alle virksomhetene har besvart dette spørsmålet, henholdsvis 123 av MUs og 6 av ISF-Us.



Figur 19: Gjennomgang av logger

5.6 Oppsummering

Gjennom vår analyse av datagrunnlaget fra MU fant vi en del rapportering i forbindelse med datakriminelle hendelser som vi mente var usikre. Vi anså at dette kunne være feilrapportering basert på at enkelte virksomheter hadde misforstått spørsmålsstillingen eller at det kan ha skjedd feil ved den manuelle registreringen av dataene fra spørreskjemaene. Videre var det for enkelte hendelseskategorier uoverensstemmelse mellom anmeldte hendelser og rapporterte hendelser – virksomheter hadde anmeldt hendelser de ikke hadde vært utsatt for. Når vi i våre analyser valgte å håndtere disse rapporteringene som uteliggere kom vi frem til litt andre tall enn det som ble presentert i Mørketallsundersøkelsen 2006 [3]. Basert på dette fant vi at det hadde vært 1.125 hendelser, tilsvarende i [3] var 2.079, og at av disse hendelsene var 23,8 % anmeldt til Kripos/politiet, tilsvarende i [3] var 13,8 %. Videre viser våre estimater at det totale antallet vellykkede og oppdagede hendelser var 128.307, hvorav 2.600 er tilfeller av vellykkede, oppdagede datainnbrudd og 7.900 tilfeller av misbruk av IT-systemer som er oppdaget.

Ved analyse av MU og ISF-U i forhold til hendelser og anmeldelser fant vi at ISF-Us virksomheter i større grad hadde rapportert og anmeldt hendelser, og at resultatene var signifikante eller meget signifikante. Når vi tok hensyn til at ISF-U besto av besvarelser fra hovedsakelig store virksomheter viste det seg at noen av resultatene ikke kunne karakteriseres som signifikante. Videre var ikke mulig å se sammenheng mellom gjerningsmenn og hendelseskategoriene i MU, men et generelt bilde av MU og ISF-U viser at litt over 20 prosent er egne ansatte og litt over 50 % er ukjente.

Når det gjelder årsaker til at virksomheter ikke anmelder viser våre resultater, for både MU og ISF-U, at den vesentligste årsaken er at de mente at saken var ubetydelig. Dernest mente MUs respondenter at det ikke ville være mulig å finne gjerningsmannen, mens kategori nummer 2 for ISF-U var at angrepet ikke var spesielt rettet mot virksomhetene. 1 av 5 MU-respondenter trodde ikke at forholdet var straffbart, noe som vi antar henger sammen med at nåværende straffebud er uttilstrekkelige og litt vanskelige å tolke.

Det fremkommer i resultatene fra våre intervjuer med virksomheter som har anmeldt datakriminalitet, at noen av disse ikke har anmeldt alle hendelser de har vært utsatt for. Flere av hendelsene originerte fra angripere i andre land. Videre fremgikk det også at en del virksomheter selv hadde foretatt bevissikring fordi politiet/Kripos ikke hadde ressurser. Noen av virksomhetene har oppgitt at på grunn av erfaringer de har gjort i forbindelse med tidligere anmeldelser er det også usikkert hvorvidt de vil gjennomføre en anmeldelsesprosess neste gang de blir utsatt for visse typer datakriminalitet. Dette gjelder spesielt i forhold til hendelser som vil være ressurskrevende å anmelde og hvor virksomheten antar at de selv må stå for bevissikring.

Videre fremgikk det av våre resultater fra intervjuene at dersom vi skal få flere virksomheter til å anmelde datakriminalitet, bør de få informasjon om hvordan de skal håndtere datakriminelle hendelser. Vi har gjennom vårt arbeid med oppgaven sett at Kripos i forsvinnende liten grad har benyttet Internett for aktivt å informere om datakriminalitet og for å få opp anmeldelsesprosenten. Politimyndigheter i enkelte andre land har vært langt mer aktive og sågar lagt ut veiledninger på Internett for håndtering av datakriminelle handlinger.

Våre resultater viser at ISF-Us respondenter i mye større grad har implementert tekniske sikringstiltak enn MUs respondenter. Det samme resultatet ser vi også i forhold til implementering av formelle sikringstiltak. Når det gjelder kontroll og oppfølging av informasjonssikkerhet finner vi også signifikante forskjeller i ISF-Us favør, og disse resultatene mister ikke sin signifikans dersom vi tar hensyn til at ISF-Us respondenter i større grad enn MUs er store virksomheter. I forbindelse med hyppighet av rapportering til ledelse og gjennomgang av logger er det ikke statistisk signifikante forskjeller.

6. Kripos - Datakrimavdelingen

"Politiet har en forståelse av datakriminalitet, men mangler «the edge», de er litt for forskerrelaterte til å utgjøre noe trussel for den etablerte miljøene. Man må huske at medlemmene i disse miljøene er ifra 25-40 år."

NN

Kripos har en svært vesentlig rolle i forhold til bekjempelse og etterforskning av datakriminalitet. Vi har derfor valgt å presentere deres utfordringer og innspill i et eget kapittel. Det som presenteres her er basert på intervju med en representant for Seksjon for datakrimetterforskning i Kripos og det som er gjengitt er godkjent av denne representanten.

Avslutningsvis i kapittel 6.7 presenterer vi det inntrykket virksomhetene vi intervjuet har av Kripos. Disse tilbakemeldingene inkluderer også resultater fra intervjuer med ressurser som har bistått virksomheter i etterforskning av datakriminelle hendelser.

6.1 Innledning

Manglende ressurser er en av de største utfordringene for Kripos og politidistriktene i forhold til etterforsking og bekjempelse av datakriminalitet. I tillegg er kompetansen veldig varierende i de forskjellige politidistriktene. Det er forholdsvis liten koordinering mellom Kripos og politidistriktene i forhold til saker som er under etterforskning. Andre utfordringer de står overfor er at en del virksomheter venter forholdsvis lenge før de anmelder datakriminelle saker. Dette kan føre til at vesentlige elektroniske bevis har gått tap og at saken ikke kan etterforskes.

Det bekreftes av Kripos at de har svært mange etterforskningssaker hvor det er behov for internasjonalt samarbeid, og at det ofte er en rekke kompliserende faktorer som virker inn på etterforskningsarbeidet. Disse kan være at det er ulikt lovverk og prosessuelle bestemmelser, men også kompliserende faktorer som ulike tidssoner, språk og prioriteringer kan få konsekvenser for etterforskning av en sak.

6.2 Om organisasjonen

Datakrimavdeling har 35 ansatte og er den minste avdelingen i Kripos. Avdelingen består av:

- Seksjon for Datakrimetterforskning
- Seksjon for elektroniske spor
- Seksjon for nasjonal kommunikasjonskontroll
- Seksjon for IKT drift og systemutvikling

Seksjon for Datakrimetterforskning har 7 medarbeidere – en leder, 4 politietterforskere og 2 politiadvokater. I de øvrige seksjonene i Datakrimavdelingen er de fleste medarbeiderne ingeniører eller sivilingeniører.

Seksjon for Datakrimetterforskning ved Kripos skal etterforske datakriminalitet som er alvorlig og/eller organisert, teknisk krevende og krever spesiell kompetanse, har klare internasjonale forgreninger eller saker som er av prinsipiell karakter.

6.3 Etterforskning av datakrimsaker

Datakriminelle hendelser er som oftest et element i en større kriminell handling. Følgelig er ikke en hovedforhandling bare basert på elektroniske bevis, men det må også være annen informasjon som underbygger saken.

Sakene som etterforskes av Kripos krever ofte store ressurser og med dagens bemanning medfører det at de må prioritere hvilke saker som skal etterforskes. I større saker benyttes også ressurser fra andre deler av politiet, som Økokrim og andre avdelinger ved Kripos.

Det er politiet/Kripos som skal sikre bevis, men en forutsetning for at dette skal være gjennomførbart er selvfølgelig at de blir kontaktet så tidlig som mulig. Tar det for lang tid fra en hendelse til etterforskningen kan startes er det stor sannsynlighet for at eventuelle elektroniske spor er forringet – eksempelvis blir ofte logger overskrevet etter en tid eller når de når en viss størrelse.

Generelt er det 3 måter etterforskning av straffesaker starter på:

- Anmeldelser sendes direkte til Kripos
- Anmeldelser sendes til lokalt politidistrikt for så å bli videresendt til Kripos
- Får informasjon om mulig straffbart forhold og starter etterforskning før det foreligger en anmeldelse

De fleste sakene starter med at det blir innlevert en anmeldelse. For mange av disse sakene er det naturlig at det er sendt en skriftlig anmeldelse og at det ikke er behov for en umiddelbar aksjon. Utfordringen er imidlertid at de i disse sakene kan være avhengige av at virksomhetene har sikret bevis. Når en sak blir anmeldt skriftlig har det gjerne gått litt tid før virksomheten anmelder. I tillegg kan den initielle saksbehandling hos Kripos ta tid og det går raskt en uke før etterforskningen kan starte. Sannsynligheten for at de da finner elektroniske spor er vesentlig redusert. Avhengig av forholdets art kan bevissikringen som virksomhetene gjør være tilstrekkelig, men dersom de ikke foretar bevissikringen umiddelbart, når en hendelse oppdages, kan det være at elektroniske spor går tapt.

Ideelt sett bør en virksomhet som utsettes for datakriminalitet, og da i særdeleshet et datainnbrudd, kontakte politiet/Kripos umiddelbart. Da har de mulighet til raskt å få avklart hva slags type hendelse det dreier seg om og dersom det er behov kan de aksjonere umiddelbart. Dersom det er angrepsforsøk som pågår har de større mulighet til å spore hvor angrepet kommer fra og å sikre elektroniske bevis. Dette vil igjen kunne føre til at det er større sannsynlighet for at saken oppklares. I de store og alvorlige datakrimsakene starter oftest etterforskningen ved en direkte henvendelse til Kripos.

I 2005 etterforsket politiet 76 saker vedrørende datainnbrudd. Fra tidligere år har det vist seg at drøyt 1/3 av disse sakene blir oppklart. Totalt blir mer enn halvparten av de anmeldte datainnbruddene henlagt. Andelen som blir henlagt i politidistriktene er trolig større enn hos Kripos. Dette skyldes blant annet at Kripos, når de mottar en anmeldelse som de ikke kan håndtere pga ressursmangel eller annet, oversender sakene til det lokale politidistrikt.

Når Kripos tar saker til retten er det bare unntaksvis at de ikke ender med domfellelse. Dette har en sammenheng med at de i utgangspunktet har valgt å etterforske saker som det er stor sannsynlighet for at man kan oppklare og at man ikke velger å ta saker i retten med mindre man er rimelig sikre på at det ender med domfellelse. Dette har selvfølgelig en klar sammenheng med de begrensede ressursene Kripos har og nødvendigheten av klare prioriteringer.

6.4 Utfordringer

Det er viktig at virksomheter anmelder all datakriminalitet. Det er ikke alltid like lett for en enkelt virksomhet å avgjøre om et angrep rettet mot virksomheten eller om det er et stort alvorlig angrep som kan være rettet mot flere virksomheter. Det er Kripos/politiet som vil kunne se om dette er forhold som kan/bør sees i sammenheng.

Man ser i en del tilfeller at virksomheter bruker lang tid – en måned eller mer – før de leverer en anmeldelse og da er det ikke alltid realistisk å forvente at Kripos/politiet kan få utrette så mye i forhold til etterforskning og oppklaring av saken. Spesielt er dette gjeldende dersom virksomheten selv ikke har sørget for sikring av elektroniske bevis.

Kripos har liten oversikt over behandlingen av datakrimsaker som etterforskes i politidistriktene. Det kunne vært ønskelig å ha en bedre oversikt blant annet for lettere å kunne se eventuelle sammenhenger mellom sakene, men med de ressursene som er avsatt til etterforskning av datakriminalitet ved Kripos i dag, er dette ikke gjennomførbart.

Man ser at i enkelte saker at virksomheter som har blitt/blir angrepet velger å håndtere hendelsen ved å sørge for at serveren(e) som angriper tas ned, fremfor å anmelde forholdet til politiet slik de kan etterforske den og ha mulighet til å ta gjerningsmennene. Dette er en kortsiktig løsning av problemet og de færreste ser hvilke konsekvenser en slik aksjon kan få. Det som oppnås er at det signaliseres til de som står bak angrepet at man er oppmerksom på dem og at gjerningsmennene tar i bruk andre servere/nye metoder for å fortsette angrepet.

I så å si alle datakrimsaker er politiet avhengig av internasjonalt samarbeid. Dette er kompliserende fordi en må forholde seg ikke bare til ulike lovverk og prosessuelle bestemmelser, men også ulike tidssoner, språk og prioriteringer.

Kripos har for få ressurser, noe som fører til at dersom de får store og presserende saker så må alt annet legges til side. For etterforskningsenheten oppleves det som vanskelig at de eksempelvis må utsette til langt ut i 2007 å etterforske saker fra 2005. Følgelig må de holde antallet saker nede slik at de ikke blir hengende med for mange gamle saker over lang tid.

Det er en utfordring at politiet er stort og de som tar kontakt kan oppleve at de ved telefonisk henvendelse føler at de blir avvist. Når de tar kontakt med politidistriktene så er det lite sannsynlig at tjenestemennene de får kontakt med har kompetanse i forhold til datakrimsaker og det kan være at disse personene vil kvie seg for å ta i mot henvendelser. Dette kan igjen føre til at virksomheter velger å la være å anmelde datakriminalitet.

6.5 Kompetanse

De aller fleste politidistriktene har noen tjenestemenn med kompetanse innen IT og datakriminalitet, men det er alt for få. De unge tjenestemennene har generelt bedre forståelse for IT, men datakriminalitet representerer et lite mindretall av sakene som etterforskes. Enkelte politidistrikt kan være uten tjenestemenn som kan forstå hvor alvorlig en datakrimsak kan være, i andre er det 1 eller 2 og de vil bare unntaksvis være i stand til å etterforske sakene selv. De største politidistriktene som Oslo og kanskje Bergen, Trondheim og Rogaland, har kompetanse til å etterforske saker selv.

Videre bør nok sakens omfang være nokså begrenset hvis politidistriktene skal gjennomføre etterforskningen. Det er også stor sannsynlighet for at de vil trenge bistand fra Kripos. Om ikke fra etterforskningsenheten, så fra de enhetene som driver med elektroniske spor eller nettverk.

Alle politidistriktene er kjent med kompetansen til Kripos og datakrimavdelingen, og kan be om bistand dersom sakene er kompliserte. Manglende kompetanse i politidistriktene bør derfor ikke medføre at politidistriktene henlegger saker som er av vanskelig karakter.

6.6 Hva bør virksomhetene gjøre?

Virksomheter kan ringe Kripos dersom de trenger rådgivning i forhold til en hendelse – de vil da bli satt videre til etterforskningsenheten. Da kan Kripos ha muligheten til å fange opp alvorlige saker på et tidlig tidspunkt.

Det er viktig at virksomheten ved en anmeldelse begjærer påtale. Dersom de ikke gjør det vil saken bli registrert, men etterforskningen av den vil trolig ikke bli prioritert. Hvis virksomhetene bare ønsker å bidra til statistikken er dette likevel en mulighet.

Virksomhetene bør ta kontakt med Kripos når de skal sikre informasjon. Kripos ser i en del saker at ikke alle elektroniske spor som bør sikres er sikret. Dersom Kripos etterspør ytterligere informasjon hender det at den ikke finnes lenger. Det er ikke alltid mulig for Kripos å gi beskjed om hva som trengs. Dersom virksomheten ikke kan ta ned servere for å sikre spor, er det bare å håpe at tilstrekkelige elektroniske bevis kan sikres.

6.7 Om Kripos og politiets kompetanse og ressurser

Det følgende er en oppsummering av tilbakemeldinger vi fikk i våre intervjuer med virksomhetene og med ressurspersoner som har bistått virksomheter med etterforskning. Dette er erfaringer som virksomhetene har gjort seg som følge av å ha anmeldt datakriminalitet og reflekterer også at det er et samsvar mellom det som Kripos ser som sin utfordring og det som virksomhetene har erfart. Vi gjør oppmerksom på at vi ikke har gjort noe forsøk på å moderere eller endre innspillene vi fikk. Videre ønsker vi å påpeke at våre virksomheter i liten grad ga uttrykk for negativ kritikk av Kripos, men heller uttrykte at de har stor forståelse for at Kripos sine begrensede ressurser fører til at en del anmeldte saker blir henlagt.

Det er en kjent problematikk at politidistriktenes kompetanse når det gjelder etterforskning av datakrimsaker er svært varierende. I tillegg er det også svært varierende hvor mye ressurser politidistriktene kan sette inn i etterforskning av slike saker. Det er mange saker som ikke blir etterforsket. Videre er det flere saker som har blitt henlagt fordi det har blitt begått feil i etterforskningen.

Kripos tar i stor grad presedenssaker eller saker hvor det kan påvises betydelig økonomisk tap. De skal prinsipielt ta saker som er av vanskelig karakter og mer banebrytende art. Et problemet er at det er en økende grad av saker som ikke faller under disse kategoriene. Generelt sett henger de fleste politidistriktene etter i forhold til kompetanse og ressurser, med unntak av eksempelvis Oslo-politidistrikt. Det finnes også dyktige og kompetente ressurser i de andre distriktene, men de er ikke del av noen gruppering og således ikke en del av et team som har som hovedoppgave å jobbe med etterforskning av datakriminalitet. Dagens situasjon er at Kripos har ikke nok kapasitet til å bistå politidistriktene og at kompetansen ute ikke bygges opp i tilstrekkelig grad til å håndtere alle saker som anmeldes.

Politiets budsjett styres av antall saker – få saker = lite budsjett. I "vanlig" kriminalitet benyttes datakriminalitet i økende grad som middel for å begå en forbrytelse. Myndighetene må innse at datakriminalitet er et verktøy for å utføre store kriminelle handlinger. Politiet begynner i økende grad å se at datakriminalitet og elektroniske spor er en del av et større bilde. Det krever enorme ressurser for å se sammenhengen. Dagens fingeravtrykk er elektroniske spor.

I en del tilfeller har virksomheter, som har blitt utsatt for datakriminalitet, leid inn ekstern ekspertise for å sikre bevis og dokumentere hendelsen. I forbindelse med anmeldelse av forholdet har alle beviser og dokumentasjon blitt overlevert politiet. Således har politiets videre arbeid bare vært å verifisere materialet. Selv ved slike saker har virksomheter opplevd at politiet ikke har hatt ressurser til å videreføre arbeidet og sakene har blitt henlagt. Det er også gjort erfaring med at det har tatt lang tid for politiet å presiseres hvordan de ønsker at bevissikring utføres og dokumentasjon skal utarbeides. Dette fører igjen til en forlengelse av etterforskningen.

Tidsaspektet i en etterforskning er vesentlig og dersom det tar for lang tid før etterforskningen starter eller selve etterforskningen tar for lang tid kan det føre til at viktige bevis forspilles. Få ressurser og stor saksmengde er en vesentlig faktor i så henseende. Dessuten hender det også at det under en etterforskning skiftes ut saks-

behandlere og/eller jurister noe som igjen kan føre til at etterforskningen ikke blir en suksess.

I forbindelse med rettssaker er det en utfordring at aktoratet og dommere ikke har nok kompetanse når det gjelder datakriminalitet og generelt sett IT. Det har vært tilfeller hvor ekstern ekspertise under en rettssak har måttet instruere/korrigere aktoratet fordi de har vært i ferd med å utelate hovedbeviset.

Det er ikke er en stor utfordring å utføre datakriminalitet uten å bli oppdaget. Forutsetningen er at de vet hva de skal gjøre og hvordan, i tillegg til at de kan fjerne eventuelle elektroniske spor. De store og alvorlige hendelsene, så som industri-spionasje, blir sjelden oppdaget og følgelig ikke anmeldt. Dette er utført av personer med stor kompetanse og ressurser, ofte med tilknytning til organiserte miljøer. Mye av datakriminaliteten er ofte motivert av spenning og moro eller for eksempelvis å skaffe lagringsplass for piracy – musikk og filmer. Datakriminalitet som omfater piracy etc. kan være ressurskrevende etterforskningsmessig, men anses ikke som alvorlige saker.

7. Konklusjon

Omfanget av datakriminalitet

Under arbeidet med datagrunnlaget fra Mørketallsundersøkelsen 2006 (MU) fant vi en del rapporteringer som vi har ansett for ikke å være korrekte. Følgelig har vi sluttet andre konklusjoner med hensyn til omfanget av datakriminalitet i Norge og spesifikt gjelder dette mørketallene. Vi har kommet fram til at det sannsynlige antallet hendelser rapportert gjennom MU er 1.125, hvilket er nesten halvparten av det som ble presentert i rapporten for Mørketallsundersøkelsen 2006. Av disse 1.125 hendelsene ble bare 23,8 % anmeldt. På bakgrunn av dette har vi estimert at det totale antallet vellykkede og oppdagede hendelser var 128.307, hvorav ca. 2.600 er datainnbrudd og ca. 7.900 er av misbruk av IT-systemer.

Virksomheter anmelder ikke

Hovedårsaken til at datakriminalitet ikke anmeldes er at virksomhetene anser at saken er for ubetydelig. Dette er gjeldende både for undersøkelsen gjennomført blant medlemmer av IT-SikkerhetsForum (ISF-U) og MU. Dernest oppgir MUs virksomheter at det ikke ville være mulig å finne gjerningsmannen, mens ISF-Us virksomheter mente at angrepet ikke var rettet mot dem. I MU er denne årsaken på 3. plass, mens i ISF-U var det fordi gjerningsmannen var en ansatt. Vedgående virksomhetenes manglende tiltro til politiets kompetanse og ressurser, viser det seg at dette var en årsak for flere av MUs respondenter enn for ISF-U.

Gjennom våre intervjuer fant vi at virksomheter som hadde anmeldt datakriminalitet, uttrykte at de hadde erfart stor usikkerhet i forbindelse med krav til egen håndtering av hendelsen og følgelig anser vi at dette kan være en "unevnt" årsak til at virksomheter ikke anmelder.

Erfaringer med anmeldelse av datakriminalitet

Vi intervjuet 8 virksomheter som hadde anmeldt datakriminalitet. Til sammen hadde de anmeldt 33 saker og av disse er til nå 29 henlagt. Bare i én sak har det vært domfellelse. Enkelte virksomheter har uttalt at de vil vurdere å la være å anmelde datakriminelle hendelser i fremtiden dersom de anser at saken med stor sannsynlighet blir henlagt. Årsaken til dette er at prosessen knyttet til håndtering av en datakriminell hendelse kan være ganske omfattende og ressurskrevende, ikke minst i forhold til bevissikring og juridisk bistand.

Når virksomheter anmelder datakriminalitet og opplever at sakene stort sett blir henlagt, er dette erfaringer som de deler med sitt faglige nettverk. Dette kan også føre til at noen anbefaler at ikke bør anmeldes, fordi virksomhetens egen innsats ikke står i forhold resultatene i forhold til anmeldelsen.

Håndtering av informasjonssikkerhet – ISF-U vs MU

Basert på våre resultater kan vi konkludere med at ISF-Us respondenter i større grad enn MUs har implementert tekniske og formelle sikringstiltak. De samme funnene har vi også gjort i forhold til tiltak knyttet til kontroll/revisjon og rapportering. Flere av funnene har vist seg å være meget signifikante. Videre kan vi konkludere at virksomheter som er medlem av ISF i større grad har rapportert hendelser og at de også i større grad velger å anmelde disse hendelsene. Til tross for at flertallet av respondentene som deltok i ISF-U var store virksomheter, noe som ikke var tilfelle for MU, viste variansanalysene at resultatene i hovedsak var signifikante eller meget signifikante.

Få flere til å anmelde datakriminalitet

Vi mener at dersom vi skal få flere virksomheter til å anmelde må Kripos/politiet få flere ressurser, være mer synlige for virksomhetene og at dette kan gjøres ved å bruke Internett som informasjonskanal. I forbindelse med den nye lovgivningen som kommer i forhold til datakriminalitet er det vesentlig at det gjøres en innsats for å informere virksomhetene om konsekvensen den vil få. Videre anser vi at veiledningene vi har utarbeidet kan være viktige hjelpemidler for virksomheter som utsettes for datakriminalitet og at dette kan føre til at flere anmelder.

Sluttlærdom

Det er en stor utfordring at datakriminalitet er internasjonalt og at manglende harmonisering av lovverk og samarbeid landene i mellom ofte fører til at gjerningsmenn ikke kan straffefølges fordi de befinner seg i et annet land. På dette området har norske myndigheter en klar utfordring som de er nødt til å ta tak i, dersom datakriminelle saker i større grad skal oppklares og gjerningsmenn som tilsynelatende befinner seg i utlandet kan straffeforfølges.

I kriminalsaker er det politiet som har ansvar for å sikre bevis, og dette gjelder også i datakriminelle saker. Flere virksomheter har erfart at de ikke har fått bistand med bevissikring og har selv måttet utføre dette arbeidet. Kripos lider av ressursmangel og de fleste politidistrikter av en kombinasjon av mangel på ressurser og kompetanse. Det er ikke en langsiktig løsning for bekjempelse av datakriminalitet at norske virksomheter ikke anmelder. Manglende anmeldelser fører til at det ikke tilføres kompetanse og ressurser til Kripos og politiet.

Vårt råd til norske virksomheter er at de konsekvent anmelder og begjærer påtale når de utsettes for datakriminalitet. Dette bør gjøres uansett om virksomhetene selv ikke har kompetanse, ressurser eller ønske om selv å sørge for sikring av bevis. Det vil bidra til at anmeldelsesstatistikken går opp og at myndighetene blir nødt til å sørge for økte ressurser til politiet og Kripos og at behandling av datakriminelle saker effektiviseres.

Norske virksomheter viser stor modenhet i forhold til å ta i bruk ny teknologi. Påtrykk om ny funksjonalitet og ny løsninger skaper sikkerhetsmessige utfordringer. Når vi ser på norske virksomheters vilje til å ta i bruk sikringstiltak, viser det seg at de ikke har den samme modenheten og at vi på de fleste områder ligger dårligere an enn virksomheter i sammenlignbare land. Vi mener at dette henger sammen med en generell uvillighet til å bruke ressurser på sikringstiltak. Noe som igjen kan skyldes

manglende innsikt i dagens trusselbilde. Dersom norsk virksomheter skal fortsette å henge med i den teknologiske utviklingen er de også nødt til å ta inn over seg de sikkerhetsmessige utfordringene dette medfører. De må i størst mulig grad sørge for å implementere tekniske og formelle sikringstiltak som samsvarer med den teknologien de tar i bruk. De er i tillegg nødt til å iverksette prosedyrer for håndtering av datakriminelle hendelser, for er det noe vi er ganske sikre på så er det at mange har vært utsatt for datakriminalitet og kommer til å bli utsatt for det i fremtiden.

Avslutningsvis vil vi poengtere at Mørketallsundersøkelsen slik den ble gjennomført i 2006 har tydelige kvalitetsmessige svakheter, noe som medfører at vi stiller spørsmål med dens betydning i sin helhet. Før neste undersøkelse bør hele spørreskjemaet omarbeides, slik at misforståelser kan unngås og riktige konklusjoner kan trekkes i etterkant.

8. Videre arbeid

Denne oppgaven har hatt som mål å bidra til at flere norske virksomheter vil velge å anmelde datakriminalitet. Mørktall er et fenomen vi har hatt i mange år og det antas ikke at denne oppgaven vil kunne føre til at de forsvinner.

8.1 Fremtidige Mørketallsundersøkelser

Gjennom vårt arbeid med Mørketallsundersøkelsen for 2006 har vi erfart at det er rom for en del kvalitetsmessige forbedringer. Det har også vært et ønske fra vår oppdragsgiver, NorSIS som en av partene som har deltatt i arbeidet med Mørketallsundersøkelsen, at vi skulle foreta en vurdering av Mørketallsundersøkelsen og gi innspill til kvalitetsmessige forbedringer. Videre har det også fra Kripos sin side, som også deltok i arbeidet med Mørketallsundersøkelsen, blitt gitt innspill til utfordringene de ser i forhold til undersøkelsen og gjennomføringen av den.

Utfordringen med Mørketallsundersøkelsen er at det kan være vanskelig for mottakere å svare på alle spørsmålene. Spørreskjemaet ble sendt ut til 2.000 virksomheter i offentlig og privat sektor. Skjemaet ble ikke sendt direkte til kontaktpersoner, men var adressert til virksomheten. Slik spørreskjemaet ble distribuert er det uvisst om de som besvarte på vegne av sin virksomhet var de som hadde tilstrekkelig kompetanse og kunnskap til å gjøre dette – om skjemaene ble videresendt internt i virksomhetene til de rette personene. Det er derfor vanskelig å si hvor gode svarene som ble gitt fra de enkelte virksomhetene er. Videre er det også en usikkerhet knyttet til hva respondentene har tenkt når de har svart. Vi mener at det er vesentlig at det gjøres et større arbeid for å sørge for at skjemaene for neste Mørketallsundersøkelse kommer til de personene som kan besvare spørsmålene.

Videre mener vi at det er behov for å utføre intervjuer med de virksomhetene som svarer at de har vært utsatt for datakriminalitet. Dette for å sikre rapporteringene er så korrekte som mulig.

Vi anser også at det er behov for en revisjon av en del av spørsmålene slik at det sikres bruk av korrekt terminologi. Dessuten bør det også vurderes om spørsmålene kan omstruktureres slik at det i større grad er mulig å se sammenhengen mellom de enkelte variablene. Eksempelvis er det i Mørketallsundersøkelsen ikke mulig å koble hendelser mot gjerningsmenn. Ei heller hendelser som ikke anmeldes mot årsak til at de ikke anmeldes.

En annen utfordring vi har sett er at fordi rapporteringene registreres manuelt oppstår det mulighet for feilregistrering. Følgelig bør det vurdere om det i fremtiden skal ta i bruk elektroniske skjemaer på web.

8.2 Andre videreføringer

Vi ser at det kan være interessant å utvikle metrikker som kan brukes av virksomheter for å registrere datakriminelle hendelser og å for å få en bedre statstikk over disse hendelsene.

Videre er det som vi har påpekt tidligere i denne oppgaven vesentlig at det gjøres et arbeid for å gi norske virksomheter relevant informasjon ved innføring av nye/endrede straffebud for datakriminalitet. I så henseende vil det være interessant om vi i fremtiden kan se endringer i forhold til villighet til å anmelde datakriminelle handlinger.

Vi anser også at veiledningen vi utarbeidet for sikring av elektroniske bevis kan være gjenstand for et videre arbeid. Da spesielt i forhold til ytterligere detaljering av fremgangsmåten som er beskrevet i del 2. Forbeholdet vi tar i den forbindelsen er at dette må være en veiledning som må være beregnet på virksomheter med kompetanse innen området, og at veiledningen er godkjent av politiet. Hensikten med bevissikring er at bevisene skal holde i en eventuell rettssak, og dersom feil gjøres under dette arbeidet vil det få negative konsekvenser for utfallet av saken.

9. Referanser

[1] M. Merkow & J. Breithaupt: Information Security: Principles and Practices – 2006. ISBN: 0-13-154729-1

[2] Bruce Sneier: Secrets & Lies – 2000. ISBN: 0-471-45380-3

[3] Næringslivets Sikkerhetsråd: Mørktallsundersøkelsen 2006 (full rapport)

[4] Norsis: www.norsis.no besøkt 13.06.2007

[5] Sushi Jajodia and Jonathan Miller, (2003), "Editor's Preface," Journal of Computer Security. (2) 2/3, p. 85.

[6] LOV 1902-05-22 nr 10: Almindelig borgerlig Straffelov (Straffeloven) http://www.lovdata.no/all/hl-19020522-010.html – besøkt 13.06.2007

[7] NOU 2003: 27 "Lovtiltak mot datakriminalitet" (delutredning I) http://www.regjeringen.no/nb/dep/jd/dok/NOUer/2003/NOU-2003-27.html?id=382564 – besøkt 13.06.2007

[8] NOU 2007: 2 Lovtiltak mot datakriminalitet (delutredning II) http://www.regjeringen.no/nb/dep/jd/dok/NOUer/2006/NOU-2006-6.html?id=157408 – besøkt 13.06.2007

[9] Parliamentary Office of Science and Technology: Computer Crime (2006 Postnote # 271) http://www.parliament.uk/documents/upload/postpn271.pdf – besøkt 13.06.2007

[10] Maria Kjaerland – artikkel: Profiling Coordinated Cyber Incidents towards the Critical Infrastructure in Norway (27.04.2007) – tilsendt av forfatter

[11] Ernst & Young: Global Information Security Survey 2006 http://www.ey.com/Global/download.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf – besøkt 13.06.2007

[12] PricewaterhouseCoopers: DTI Information Security Breaches Survey 2006 http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16 – besøkt 13.06.2007

[13] CERT Statistics: http://www.cert.org/stats/ – besøkt 28.05.2007.

[14] Symantec: For your information # 1 – 2006 http://eval.veritas.com/mktginfo/downloads/fyi_no_1_2006.pdf – besøkt 29.05.2007

[15] FBI – Publications – Law Enforcement Bulletin – August 2001.
http://www.fbi.gov/publications/leb/2001/aug01leb.htm – besøkt 28.05.2007

[16] GAO – United States General Accouting Office: Information Security: Computer Attacks at Department of Defense Pose Increasing Risks
http://www.fas.org/irp/gao/aim96084.htm – besøkt 28.05.2007

[17] Will Spencer, Network System Architects, Inc.: Network Security Assessment (2000)
http://www.nsai.net/White_Paper-Network_Security_Assessment.pdf – besøkt 28.05.2007

[18] AusCert: Computer Crime & Security Survey 2006
http://www.auscert.org.au/images/ACCSS2006.pdf – besøkt 13.06.2007

[19] CSI/FBI: Computer Crime and Security Survey 2006
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf – besøkt 13.06.2007

[20] Post & Telestyrelsen: Mörketalsundersökningen 2005
http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf – besøkt 13.06.2007

[21] Næringslivets Sikkerhetsråd: Mørktallsundersøkelsen 2003

[22] Næringslivets Sikkerhetsråd: Mørktallsundersøkelsen 2001

[23] Florida Departement of Law Enforcement – Florida Computer Crime Center
http://www.fdle.state.fl.us/Fc3/report.html – besøkt 28.05.2007

[24] Metropolitan Police – Computer Crime Unit
http://www.met.police.uk/computercrime/index.htm – besøkt 28.05.2007

[25] UNIRAS – CPNI (Centre of Protection for National Infrastructure)
http://www.uniras.org.uk/ – besøkt 28.05.2007

[26] United States Department of Justice: Reporting Computer, Internet-Related, or Intellectual Property Crime
http://www.cybercrime.gov/reporting.htm – besøkt 29.05.2007

[27] Kripos web-side
http://www.politi.no/portal/page?_pageid=34,49028&_dad=portal&_schema=PORTAL&articles2_mode=about&articles2_articleId=24974&navigation3_mode=shortcuts1&navigation4_mode=shortcuts1&articles5_mode=aboutCategory_od&articles5_articleGroupName=Om%20distriktet%20Underkategori&navigation1_parentItemId=1897&navigation1_selectedItemId=1980&orgUnitId=1926&uicell=12497.JPG&navigation3_parentItemId=1980 – besøkt 29.05.2007

[28] AusCert: Report a computer security incident
http://www.auscert.org.au/render.html?it=3191 – besøkt 29.05.2007

[29] SITIC: Incidentrapportera
http://www.sitic.se/incidenter – besøkt 29.05.2007

[30] IC3: Welcome to IC3
http://www.ic3.gov/ – besøkt 29.05.2007

[31] NorCert: Hendelseshåndtering
http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Hendelseshandtering/http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Hendelseshandtering/
– besøkt 29.05.2007

[32] United States Secret Service: Best Practices for Seizing Electronic Evidence
http://www.secretservice.gov/electronic_evidence.shtml – besøkt 16.06.2007

[33] NHTCU (National Hi-Tech Crime Unit – Association of Chief Police Officers): Good Practice Guide for Computer based Electronic Evidence
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf – besøkt 29.05.2007

[34] British Columbia – Ministry of Managed Services: Electronic Evidence Gathering and Preservation
http://www.cio.gov.bc.ca/Security/presentations/Electronic_Evidence_Preservation_NN.pdf – besøkt 16.06.2007

[35] NISCC – National Infrastructure Security Co-ordination Center: An Introduction to Forensic Readiness Planning - 2005
http://www.cpni.gov.uk/docs/re-20050621-00503.pdf – besøkt 16.06.2007

[36] AusCert: Collecting Electronic Evidence After a System Compromise
http://www.auscert.org.au/render.html?it=2247 – besøkt 16.06.2007

[37] Danks IT: Quick Guide – Optimering af efterforskningsmulighederne ved datakriminalitet
http://www.dansk-it.dk/upload/quick_guide_endelig_lav.pdf – besøkt 16.06.2007

[38] TechRepublic: Computer crime evidence-preservation checklist (tilgang til dokumentet krever medlemskap i Tech Republic)
TechRepublic: 10 things you should know about computer crime evidence preservation (tilgang til dokumentet krever medlemskap i Tech Republic)

[39] Computerworld: Fra ødeleggende moro til vinningskriminalitet
http://www.idg.no/karriere/karrierenyheter/article16511.ece – besøkt 13.06.2007

[40] Kripos: Årsrapport 2005
http://www.politi.no/pls/idesk/docs/f2042663704/arsrapport2005.pdf
– besøkt 13.06.2007

[41] Bob Sullivan, msnbc: The Red Tape Chronicles: Who's behind criminal bot networks?
http://redtape.msnbc.com/2007/04/whos_behind_cri.html – besøkt 29.05.2007

[42] VG: Al-Qaida planlegger cyberangrep
http://www.vg.no/pub/vgart.hbs?artid=103947 – besøkt 13.06.2007

[43] Symantec Internet Security Threat Report: Trends for July-December 2006 http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf – besøkt 13.06.2007

[44] Tim Weber, BBC News Criminals 'may overwhelm the web' http://news.bbc.co.uk/2/hi/business/6298641.stm – besøkt 29.05.2007

[45] Jens Kristian Roland, Kripos: Etterforskning av botnet/trojanere (Medlemsmøte ISF 14.02.2007)

[46] Dagens Næringsliv (papirutgave): Svindelalarm i bankene (20/21. januar 2007)

[47] Dagens Næringsliv: Tappet 14.000 fra nettbank-konto (22.12.2006) http://www.dn.no/forsiden/politikkSamfunn/article963881.ece – besøkt 05.06.2007

[48] Dagens IT: Russisk mafia hacker Nordea (29.01.2007) http://www.dagensit.no/finans/article1001853.ece – besøkt 05.06.2007

[49] Kredittilsynet: Risiko- og sårbarhetsanalyse (ROS) 2006 http://www.kredittilsynet.no/archive/stab_pdf/01/03/26032043.pdf – besøkt 13.06.2007

[50] Paul D. Leedy & Jeanne Ellis Ormrod: Practical Research – Planning and Design, 8th edition, Pearson Merrill Prentice Hall (ISBN 0-13-124720-4)

[51] NOU 1985: 31 Datakriminalitet http://www.regjeringen.no/upload/kilde/odn/tmp/2002/0034/ddd/pdfv/154594-nou1985-31.pdf – besøkt 13.06.2007

[52] IT-SikkerhetsForums hjemmeside: www.isf.no – besøkt 05.06.2007

[53] Julia Pallant: SPSS Survival Manual, Open University Press (ISBN 0-335-21640-4)

[54] Asbjørn Johannessen: Introduksjon til SPSS, 3. utgave, Abstrakt forlag (ISBN 978-82-7935-223-5)

[55] Creswell JW. 2003. Research Design: Qualitative, quantitative, and mixed method approaches: SAGE Publications

[56] Booth WC, Colomb et al. The craft of research. Chicago: The University of Chicago Press (2003)

[57] Computerworld: Sikkerhetsfolk oppjusterer antall datainnbrudd http://www.idg.no/bransje/bransjenyheter/article27104.ece – besøkt 13.06.2007

[58] SSB: Bedrifter, etter ansattegrupper og næring. 1. april 2007 http://www.ssb.no/emner/10/01/bedrifter/tab-2007-04-13-01.html – besøkt 25.05.2007

[59] ITAKT: Elektroniske trusler (2006) www.itakt.no/1_trusler/Trusselvurdering_MMIrapport2006_itakt.doc – besøkt 13.06.2007

[60] Mørketallsundersøkelsen 2006: Spørreskjema

[61] CIO and PriceWaterHouseCoopers: The Global State of Information Security (2005)
http://www.pwc.com/extweb/ncsurvres.nsf/docid/15BD9CBE7490630085257 0760056939F/$file/SEPT15INFO_SURVEY_FINAL.pdf – besøkt 13.06.2007

[62] Kredittilsynet: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) Vedlegg til rundskriv nr. 17/2003
http://www.kredittilsynet.no/archive/stab_word/01/03/nr___016.doc
– besøkt 13.06.2007

[63] Datatilsynet: Sikkerhetsbestemmelsene i personopplysningsforskriften stiller konkrete krav til virksomhetene
http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/SV100_00.pdf
– besøkt 13.06.2007

Appendiks A: Spørreskjema IT-SikkerhetsForum

Informasjonssikkerhetsundersøkelse

i samarbeid med

Line Andersson, mastergradstudent, Informasjonssikkerhet, Høgskolen i Gjøvik

"I forbindelse med arbeidet med min masteroppgave, som i hovedsak fokuserer på informasjonssikkerhetsundersøkelser og sikkerhetshendelser, trenger jeg et bidrag fra dere. Jeg skal sammenligne resultatene fra denne undersøkelsen med Mørketallsundersøkelsen til Næringslivets sikkerhetsråd og diverse internasjonale undersøkelser. Jeg skal i tillegg se på politiets statistikker i forbindelse med anmeldte sikkerhetsbrudd. Da ISF er en organisasjon som består av sikkerhetsbevisste personer, er det svært interessant å bruke ISF-medlemmenes svar som en referanseramme i forhold til de andre undersøkelser. Jeg har valgt å benytte en del av spørsmålene fra Mørketallsundersøkelsen, uten vesentlige endringer. Når masteroppgaven er ferdig vil den selvfølgelig være tilgjengelig for de som er interesserte."

Jeg ville sette stor pris på om du kan besvare dette spørreskjemaet og levere det til konferansens sekretariat. Svarene dine vil bli behandlet konfidensielt og vil ikke kunne spores tilbake til deg eller din virksomhet.

Om virksomheten

1. Hvor mange ansatte er det i virksomheten?

- ☐ 1-5
- ☐ 6-10
- ☐ 11-24
- ☐ 25-199
- ☐ 200-499
- ☐ 500 eller flere

2. Hva er din funksjon i virksomheten

- ☐ Daglig leder
- ☐ Annen lederfunksjon
- ☐ Sikkerhetssjef/-ansvarlig
- ☐ IT-sjef/ansvarlig
- ☐ IT-medarbeider
- ☐ Sikkerhetsmedarbeider
- ☐ Medarbeider

Om informasjonssystemene i virksomheten

3. Hvordan bruker virksomheten Internett?
FLERE SVAR MULIG

- ☐ Hjemmeside
- ☐ Selger varer eller nettbaserte tjenester
- ☐ Kjøper varer eller nettbaserte tjenester
- ☐ Betaler regninger/fakturaer elektronisk
- ☐ IP-telefoni
- ☐ Instant messaging (MSN, AOL eller lignende)
- ☐ WAN-kommunikasjon mellom avdelingskontorer
- ☐ Ansatte har tilgang til virksomhetens interne systemer hjemmefra eller på reise

4. Har en eller flere av virksomhetens kunder, samarbeidspartnere eller andre tilgang til deler av virksomhetens informasjonssystemer utenfra?

☐ Ja ☐ Nei ☐ Vet ikke

5. Hvordan er IT-driften organisert i virksomheten?

☐ Som del av egen virksomhet med egne ansatte
☐ I andres regi ("outsourcing")
☐ En kombinasjon
☐ Vet ikke

Hvis virksomheten "outsourcer" eller kombinerer IT-driften; kryss av om følgende elementer er med i kontrakten med driftspartner:
FLERE SVAR MULIG

☐ Krav til tilgangskontroll til informasjon
☐ Krav til tekniske tiltak eller rutiner
☐ Krav til tilgjengelighet/oppetid
☐ Rett til innsyn i relevante sikringsrutiner og dokumentasjon
☐ Rett til måling av sikkerhetsnivå
☐ Kontraktsfestet et økonomisk ansvar ved misbruk fra driftspartners side
☐ Sanksjoner dersom krav ikke oppfylles
☐ Vet ikke

Sårbarhet og organisatoriske sikringstiltak

6. Hvor lang tid vil det ta før det skaper vesentlige problemer for virksomheten dersom de viktigste informasjonssystemene er ute av drift?
(Konsekvensene kan være tap av salg/inntekter/kunder/aktiva, økte kostnader/ekstraarbeid/ erstatningsansvar, redusert omdømme mv.)

☐ I løpet av 1 time
☐ I løpet av 1 dag
☐ I løpet av 2-3 dager
☐ I løpet av 4-7 dager
☐ I løpet av 1-4 uker
☐ Mer enn 1 måned
☐ Det ville ikke skape større problemer
☐ Vet ikke

7. Hvor ofte gjøres det vurdering av risiko og behov for sikringstiltak av eksisterende IT–løsninger?

☐ Løpende ☐ Sjeldent ☐ Vet ikke
☐ Av og til ☐ Aldri

8. Hvor ofte gjøres det vurdering av risiko og behov for sikringstiltak ved innføring av nye IT–løsninger eller endringer?

☐ Hver gang ☐ Sjeldent ☐ Vet ikke
☐ Av og til ☐ Aldri

9. Vennligst kryss av for om følgende tiltak er innført:
FLERE SVAR MULIG

☐ Virksomheten har utarbeidet retningslinjer for ansattes bruk av virksomhetens informasjonssystemer
☐ Ansatte må undertegne taushetserklæring
☐ Ansatte gis opplæring i sikker bruk av IT
☐ Virksomheten har utarbeidet planer for håndtering av de viktigste bruddene på informasjonssikkerheten
☐ Virksomheten gjennomfører systematiske katastrofe-/kriseøvelser knyttet til IT
☐ Virksomheten er i stand til å håndtere IT-sikkerhetsbrudd utenfor arbeidstiden
☐ Vet ikke

10. a. Dersom virksomheten har etablert retningslinjer for sikker drift av IT-infrastruktur, hvordan bli disse fulgt opp?
FLERE SVAR MULIG

- ☐ Intern revisjon/kontroll
- ☐ Ekstern revisjon/kontroll
- ☐ Rapportering til ledelse
- ☐ Liten eller ingen oppfølging
- ☐ Vet ikke

10. b. Dersom virksomheten har prosedyrer for å rapportere sikkerhetsbrudd internt, hvordan rapporteres disse?

- ☐ Umiddelbart til ledelsen/daglig leder (rapportering ved hvert enkelt brudd)
- ☐ Periodisk til ledelsen/daglig leder
- ☐ Av og til til ledelsen/daglig leder
- ☐ Sjelden eller aldri
- ☐ Vet ikke

Tekniske sikringstiltak

11. Hvilke tiltak brukes for å sikre virksomhetens informasjon og systemer/nettverk?
FLERE SVAR MULIG

- ☐ Personlig passord
- ☐ Engangspassord
- ☐ Fysiske autentiseringsmekanismer (f.eks. smartkort)
- ☐ Biometrisk autentisering (f.eks. fingeravtrykk)
- ☐ Sikkerhetskopiering (backup)
- ☐ Anti-virusprogramvare
- ☐ Spamfilter
- ☐ Brannmur for nettverket
- ☐ Personlige brannmurer
- ☐ Innbruddsdetekteringssystem (IDS)
- ☐ System for å forhindre innbrudd (IPS)
- ☐ Virtuelt privat nettverk (VPN)
- ☐ Ulike sikkerhetssoner i nettet
- ☐ Avlåst datarom
- ☐ Kryptering av bærbare media
- ☐ Kryptering av trådløse nettverk
- ☐ Duplisering av kritiske komponenter
- ☐ Reservestrøm, UPS
- ☐ Digital signatur
- ☐ Filtrering av uønsket webtrafikk
- ☐ Filtrering av e-postinnhold

12. Oppdatering av sikkerhetsprogramvare

Hvor ofte oppdaterer virksomheten:	Automatisk	Umiddelbart når oppdatering foreligger	Periodisk/ regelmessig	Tilfeldig/av og til	Aldri	Vet ikke	Ikke relevant
Antivirusprogramvare?							
Programvare for å beskytte mot spionvare (spyware)?							
Spamfilter?							
Sikkerhetsoppdatering av OS (f.eks. installering av "patcher")?							
Annen programvare (f.eks. brannvegger)?							

13. Oppfølging av informasjonssikringstiltak

Hvor ofte:	Årlig	Kvartalsvis	Månedlig	Aldri	Vet ikke
Gjennomgår virksomheten brannmursreglene?					
Gjennomgår virksomheten tilgangskontrollene?					
Skiftes administratorpassord?					

14. Hvor ofte gjennomgås logger for å følge opp informasjonssikkerheten i virksomheten?

- ☐ Daglig
- ☐ Ukentlig
- ☐ Av og til
- ☐ Aldri
- ☐ Logger ikke
- ☐ Vet ikke

Hendelser

Resten av spørsmålene i denne undersøkelsen besvares bare dersom virksomheten har hatt uønskede hendelser knyttet til informasjonssystemene i løpet av det siste året.

15. Kartlegging av sikkerhetsbrudd

Hendelser:	Antall 1-5	Antall 6-10	Antall 11-20	Anmeldt ja/nei	Gjerningsmann (sett kryss)			
					Ansatt	Konsulent	Ekstern	Ukjent
Datainnbrudd (hacking)								
Datatyveri (uautorisert kopiering av data)								
Uautorisert endring/sletting av data								
Misbruk av IT-ressurser (pc/nett/server)								
Spredning av ulovlig/opphavsrettslig beskyttet materiale								
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)								
Virusinfeksjon, spredning av orm eller trojaner i nettverket								
Trusler om å angripe informasjons-systemer (utpressing)								
Bedrageri ved misbruk av kredittkort over Internett								
Tyveri av IT-utstyr (pc, server, pda etc.)								

16. Dersom hendelsene ikke ble anmeldt til politiet – hva var de viktigste årsakene?

FLERE SVAR MULIG

- ☐ Trodde ikke forholdet var straffbart
- ☐ Trodde det kunne gi negativ omtale av virksomheten
- ☐ Trodde ikke det var mulig å finne gjerningsmannen
- ☐ Trodde ikke politiet hadde kompetanse eller ressurser til å oppklare saken
- ☐ Saken var ubetydelig
- ☐ Anmeldte ikke fordi gjerningsmannen var egen ansatt
- ☐ Ble håndtert via oppsigelse eller erstatningskrav/sivil sak
- ☐ Anmeldelse er for ressurskrevende
- ☐ Angrepet var ikke spesielt rettet mot vår virksomhet
- ☐ Vet ikke

17. Hva er gjort for å hindre tilsvarende hendelser? FLERE SVAR MULIG

- ☐ Investering i tekniske sikringstiltak
- ☐ Forbedring av informasjonssikkerhets-policy/-retningslinjer
- ☐ Flere personer/mer tid til sikkerhetsarbeid
- ☐ En total gjennomgang av sikringsnivå
- ☐ Ingen ting
- ☐ Vet ikke

18. Hvilke følger fikk de uønskede hendelsene? FLERE SVAR MULIG

- ☐ Ekstra arbeid
- ☐ Tap av inntekt
- ☐ Erstatningsansvar
- ☐ Tap av omdømme
- ☐ Ingen
- ☐ Vet ikke

Appendiks B: Spørsmål brukt ved intervjuene

- Hva slags type saker/hendelser dere har hatt?
- Hvor mange saker/hendelser har dere hatt?
- Hvordan ble de oppdaget? (Gjennom etablerte rutiner, logging, tilfeldigheter etc.)
- Hvordan sikret dere bevis?
- Har dere noe estimat for økonomiske tap som sakene/hendelsene har påført dere?
- Har dere dokumenterte retningslinjer for anmeldelse?
- Hvem anmelder?
- Hvor lang tid tok det fra hendelsene ble oppdaget til de ble anmeldt?
- Hvordan var prosessen fra anmeldelse til henleggelse/siktelse ble utferdiget?
- Hvilken bistand fikk dere fra politiet?
- Hvor mange saker har blitt henlagt?
- Hvor mange saker har ført til straffeforfølgelse?
- Dersom dere har vært utsatt for tyveri av IT-utstyr, har dere vurdert hvorvidt tyveriene kan ha vært utført for å stjele data/informasjon?

Når det gjelder hva som defineres som saker/hendelser har jeg, for enkelhets skyld, valgt å benyttet kategoriene som ble brukt i Mørketallsundersøkelsen:

- Datainnbrudd (hacking)
- Datatyveri (uautorisert kopiering av data)
- Uautorisert endring/sletting av data
- Misbruk av IT-ressurser (pc/nett/server)
- Spredning av ulovlig/opphavsrettslig beskyttet materiale
- Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)
- Virusinfeksjon, spredning av orm eller trojaner i nettverket
- Trusler om å angripe informasjonssystemer (utpressing)
- Bedrageri ved misbruk av kredittkort over Internett
- Tyveri av IT-utstyr (pc, server, pda etc.)

Appendiks C: Domsavsigelser datakriminelle forhold

I følgende saker er straffebud § 145, 2. ledd Inntrenging i og avlytting av dataanlegg/-system (datainnbrudd) benyttet:

Borgarting lagmannsrett – 2007-02-09
Straffeloven §145, straffeloven §258, straffeloven §60a. - To personer fra Makedonia ble dømt til fengsel i 2 år og 6 måneder for skimming av norske minibanker og medvirkning til etterfølgende uberettigede uttak på ca. 1 mill. kr fra kontoene til personer som hadde fått sine kort skimmet. Lagmannsretten fant at straffeloven §60a om organisert kriminell gruppe kom til anvendelse.

Frostating lagmannsrett – 2006-11-17
Straffeloven §145 annet ledd og §257 jf. §258. - 26 år gammel tysk statsborger dømt til fengsel i 2 år og 9 mndr for medvirkning til grovt tyveri ved hjelp av kopiering av bankkort - «skimming». Kopieringen ble gjennomført i Trondheim. Uttak fra en rekke konti skjedde for det vesentlige i Spania ved bruk av falske bankkort.

Kristiansand tingrett – 2005-04-14
«Skimming» av bankkort. Straffeloven §257 jf §258, §179, §183, §185, §186 og §145. - Tre rumenske menn dømt til fengsel i 11 måneder for grovt tyveri, forsøk på grovt tyveri samt dokumentfalsk. De hadde skimmet andres bankkort ved hjelp av en innretning (skimmer) og et videokamera montert på en minibank. De hadde overført opplysningene fra skimmeren til andre magnetbåndkort,

Norges Høyesterett – 2004-10-27
Endringer i lagrede data. Skadeverk. Straffelovens stedlige virkeområde. Lovanvendelse. - Saken gjaldt datakriminalitet hovedsakelig med virkning for datamaskiner som befant seg i utlandet, og reiste spørsmål om straffelovens stedlige virkeområde, jf straffeloven §12 første ledd nr 1. Høyesterett fant at norsk strafferett kom til anvendelse for overtredelse av straffeloven §145 annet ledd, samt §393.

Gulating lagmannsrett – 2004-05-11
Tidligere ustraffede menn, 20 og 23 år, var funnet skyldig i, fra Norge, å ha brutt seg inn i datamaskiner som i det vesentlige var i utlandet. Lagmannsretten fant at forholdet ble rammet av strl. §145 annet ledd da den straffbare handling måtte anses begått i Norge, jfr. strl. §12 nr. 1. Etter en konkret vurdering ble handlingen ikke ansett for å være skadeverk.

Norges Høyesterett – 2004-01-22
En mann hadde foretatt datainnbrudd og slettet abonnentdata hos en konkurrent, jf straffeloven §145 annet ledd, §291 og §393. Høyesterett kom til at skadepotensialet ikke gjorde at skadeverket kunne karakteriseres som grovt, jf straffeloven §292. På bakgrunn av behovet for å kunne stole på datasystemers konfidensialitet og pålitelighet ble straffen satt til 60 timers samfunnsstraff, kombinert med en bot på 10.000 kroner.

I følgende sak er straffebud § 405a Innsyn i datalagret forretningshemmelighet (industrispionasje) benyttet:

Høyesterett – Kjennelse – 2003-06-23
Kværnerdommen - Saken gjaldt spørsmål om brudd på straffeloven §405a. Høyesterett kom til at bestemmelsen ikke rammet den som tilfeldig kommer over bedriftshemmeligheter. Ettersom de to tiltalte hadde lagt til rette for at e-post skulle feilsendes til dem, ble imidlertid kunnskapen ansett skaffet til veie på en urimelig måte. Kjennelse: Lagmannsrettens dom med hovedforhandling oppheves for så vidt gjelder frifinnelsen av A og B for overtredelse av straffeloven §405a.

I den neste saken er straffebud § 275 (For utroskap straffes den som i hensikt å skaffe seg eller andre en uberettiget vinning eller å skade, forsømmer en annens anliggender som han styrer eller har tilsyn med, eller handler mot den annens tarv) benyttet. I våre legmannstolkninger ville vi sagt at dette dreier seg om datatyveri:

Borgarting lagmannsrett – 2006-06-21:
En IT-sikkerhetsarkitekt i en bank ble dømt for grov utroskap, jf straffeloven §275, jf §276, til syv måneders fengsel hvorav 120 dager ble gjort betinget. Han hadde i løpet av de siste fem dager før siste arbeidsdag i banken kopiert og sendt som e-post til sin private usikrede PC en stor mengde materiale, herunder kildekode, som samlet sett ga en oversikt som kunne gi hjelp til å planlegge og å utføre uvennlige handlinger mot banken. Dette var et sikkerhetsbrudd, som bl.a. kunne ha svekket bankens omdømme og tillit i markedet. Ved straffutmålingen ble det bl.a. annet lagt vekt på det betydelige skadepotensiale og på at tiltalte var dømt i tingretten for overtredelse av åndsverkloven for å ha kopiert en kildekode. Bankens kostnader med å avverge skade var uavklart, men ble vurdert til minst 200.000 hundre tusen kr. Tiltaltes utbytte ville neppe ha blitt betydelig, selv om han ikke var blitt oppdaget meget raskt.

Appendiks D: Kategorisering av straffe-bestemmelser og hendelsestyper

I politiets straffesaksregister, STRASAK, er datakriminalitet forhold som rammes av følgende straffebud [3] i Straffeloven [6]:

§ 145, 2. ledd Inntrenging i og avlytting av dataanlegg/-system (datainnbrudd)
§ 151b Rettsstridig forføyning datasystem (ulovlig bruk - stort omfang)
§ 261 Ødeleggelse av dataavhengige samfunnsviktige installasjoner (sabotasje)
§ 270, 1. ledd nr 2 Forandring, manipulering datasystem (databedrageri)
§ 294 Misbruk datalagret forretningshemmeligheter (industrispionasje)
§ 291 Skadeverk på datalagringsmedier
§ 292 Grovt skadeverk på datalagringsmedier
§ 317 Heleri datainformasjon
§ 391, 2. ledd Uaktsomt grovt skadeverk på datalagringsmedier
§ 393 Rettsstridig forføyning datasystem (ulovlig bruk - mindre omfang)
§ 405a Innsyn i datalagret forretningshemmelighet (industrispionasje)

Av hensynt til sammenlignbarhet har vi valgt å benytte samme kategoriseringen av hendelser som det er gjort i Mørketallsrapporten [3]:

A. Datainnbrudd (hacking)
B. Datatyveri (uautorisert lesing/kopiering av data)
C. Endring/sletting av data (uautorisert)
D. Misbruk av IT-ressurser (PC/Nett/Server)
E. Spredning av ulovlig/opphavsrettslig beskyttet materiale
F. Angrep på tilgjengelighet (DoS-angrep)
G. Virus/orm/trojaner infeksjon (virkelige infeksjoner)
H. Trusler om å angripe IT-systemer (utpressing)
I. Bedrageri ved misbruk av kredittkort over Internett
J. Tyveri av IT-utstyr (PO, server, PDA etc)

Følgelig har vi også benyttet den samme felleskategorisering av hendelser og straffebud som det ble benyttet i Mørketallsrapporten [3]:

Kategori 1 – Datainnbrudd:

0607	Inntrenging i dataanlegg/system (§ 145, 2. ledd)
A	Datainnbrudd (hacking)

Kategori 2 – Misbruk av dataressurser:

2352	Rettsstridig forføyning datasystem (ulovlig bruk - stort omfang) (§ 151b)
4204	Rettsstridig forføyning datasystem (ulovlig bruk - mindre omfang) (§ 393)
D	Misbruk av IT-ressurser (PC/nett/server)

Kategori 3 – Dataskadeverk og –bedrageri:

0716	Ødeleggelse dataavhengige samfunnsviktige installasjoner (§ 261)
2612	Forandring, manipulering datasystem (§ 270, 1. ledd nr 2)

2818	Skadeverk på datalagringsmedier (§ 291)
2819	Grovt skadeverk på datalagringsmedier (§ 292)
4103	Uaktsomt grovt skadeverk på datalagringsmedier (§ 391, 2. ledd)
C	Endring/sletting av data (uautorisert)
F	Angrep på tilgjengeligheten (DoS-angrep)
G	Virus/ormer/trojanerinfeksjon (virkelige infeksjoner)
I	Bedrageri ved misbruk av kredittkort over Internett

Kategori 4 – Tyveri av datainformasjon:

0615	Avlytting av dataanlegg/-system (§ 145, 2. ledd)
2817	Misbruk datalagret forretningshemmelighet (§ 294)
3307	Heleri datainformasjon (§ 317)
4306	Innsyn i datalagret forretningshemmelighet (§ 405a)
B	Datatyveri (uautorisert lesing/kopiering informasjon)
E	Spredning av ulovlig/opphavsrettslig beskyttet materiale

Det finnes ikke sammenlignbare data fra anmeldelsesstatistikken når det gjelder følgende type uønskede hendelser:

H: Trusler om å angripe IT-systemer (utpressing)
J:Tyveri av IT-utstyr (PC, Server, PDA etc)

Tyveri kommer inn under kategorien vinningskriminalitet og det er ikke mulig ut i fra anmeldelsesstatistikken å trekke ut spesifikt tyveri av IT-utstyr. [3]

Appendiks E: Analyser fra spørreundersøkelsen

I forbindelsen med denne oppgaven ble det kjørt en stor mengde med dataanalyser og derfor har vi bare valgt å presentere et utdrag av dem.

Hvor mange ansatte er det i virksomheten?

		Hvor mange ansatte er det i virksomheten?					
		1-5	6-10	11-24	25-199	200-499	500 eller flere
MU	Antall	38	117	149	249	96	91
	%	5,1%	15,8%	20,1%	33,6%	13,0%	12,3%
ISF-U	Antall	0	1	0	9	4	17
	%	,0%	3,2%	,0%	29,0%	12,9%	54,8%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	49,543(a)	5	,000

Hendelser

Datainnbrudd

		Datainnbrudd		Total
		0	1-5	
MU	Antall	730	19	749
	%	97,5%	2,5%	100,0%
ISF-U	Antall	28	3	31
	%	90,3%	9,7%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,538(b)	1	,019

Datatyveri

		Datatyveri			Total
		0	1-5	11-20	
MU	Antall	743	6	0	749
	%	99,2%	,8%	,0%	100,0%
ISF-U	Antall	29	1	1	31
	%	93,5%	3,2%	3,2%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26,208(a)	2	,000

Endring/sletting av data

		Endring/sletting av data				Total
		0	1-5	6-10	11-20	
MU	Antall	722	24	1	2	749
	%	96,4%	3,2%	,1%	,3%	100,0%
ISF-U	Antall	28	2	1	0	31
	%	90,3%	6,5%	3,2%	,0%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12,240(a)	3	,007

Misbruk av IT-ressurser

		Misbruk av IT-ressurser				Total
		0	1-5	6-10	11-20	
MU	Antall	706	41	2	0	749
	%	94,3%	5,5%	,3%	,0%	100,0%
ISF-U	Antall	24	2	1	4	31
	%	77,4%	6,5%	3,2%	12,9%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	104,374(a)	3	,000

Copyright

		Copyright			Total
		0	1-5	11-20	
MU	Antall	741	8	0	749
	%	98,9%	1,1%	,0%	100,0%
ISF-U	Antall	29	1	1	31
	%	93,5%	3,2%	3,2%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	25,450(a)	2	,000

DoS-angrep

		DoS-angrep			Total
		0	1-5	6-10	
MU	Antall	727	21	1	749
	%	97,1%	2,8%	,1%	100,0%
ISF-U	Antall	31	0	0	31
	%	100,0%	,0%	,0%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	,937(a)	2	,626

Virus/orm/trojaner-infeksjon (virkelige infeksjoner)

		Infeksjon				Total
		0	1-5	6-10	11-20	
MU	Antall	568	156	17	8	749
	%	75,8%	20,8%	2,3%	1,1%	100,0%
ISF-U	Antall	24	4	1	2	31
	%	77,4%	12,9%	3,2%	6,5%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7,768(a)	3	,051

Trusler/utpressing

		Trusler/utpressing			Total
		0	1-5	6-10	
MU	Antall	747	2	0	749
	%	99,7%	,3%	,0%	100,0%
ISF-U	Antall	29	1	1	31
	%	93,5%	3,2%	3,2%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	31,051(a)	2	,000

Kredittkortbedrageri

		Kredittkortbedrageri			Total
		0	1-5	11-20	
MU	Antall	742	6	1	749
	%	99,1%	,8%	,1%	100,0%
ISF-U	Antall	28	1	2	31
	%	90,3%	3,2%	6,5%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	33,076(a)	2	,000

Tyveri av utstyr

		Tyveri av utstyr				Total
		0	1-5	6-10	11-20	
MU	Antall	596	147	6	0	749
	%	79,6%	19,6%	,8%	,0%	100,0%
ISF-U	Antall	17	8	4	2	31
	%	54,8%	25,8%	12,9%	6,5%	100,0%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	85,219(a)	3	,000

Sum tekniske sikringstiltak

T-Test – Group Statistics

	N	Mean	Std. Deviation	Std. Error Mean
MU	749	8,21	3,744	,137
ISF-U	31	13,42	2,754	,495

Crosstabs

		Sum tekniske sikringstiltak											
		0	1	2	3	4	5	6	7	8	9	10	11
MU	Antall	10	16	17	22	54	85	69	62	65	69	67	62
	%	1,3	2,1	2,3	2,9	7,2	11,3	9,2	8,3	8,7	9,2	8,9	8,3
ISF-U	Antall	0	0	0	0	0	0	0	0	0	2	5	2
	%	0,0	0,0	0,0	0,0	0,0	0,0	,0%	0,0	0,0	6,5	16,1	6,5

		Sum tekniske sikringstiltak							
		12	13	14	15	16	17	18	19
MU	Antall	45	45	19	24	9	7	1	1
	%	6,0	6,0	2,5	3,2	1,2	0,9	0,1	0,1
ISF-U	Antall	3	3	5	2	3	5	1	0
	%	9,7	9,7	16,1	6,5	9,7	16,1	3,2	0,0

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	108,423(a)	19	,000

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
		Lower	Upper	Lower	Upper	Lower
Sum tekniske sikringstiltak	Equal variances assumed	3,897	,049	-7,660	778	,000
	Equal variances not assumed			-10,151	34,756	,000

Sum formelle sikringstiltak

T-Test – Group Statistics

	N	Mean	Std. Deviation	Std. Error Mean
MU	749	2,2083	1,53807	,05620
ISF-U	31	4,1290	1,52188	,27334

Crosstabs

		Sum av formelle sikringstiltak						
		0	1	2	3	4	5	6
MU	Antall	83	215	160	138	80	53	20
	%	11,1	28,7	21,4	18,4	10,7	7,1	2,7
ISF-U	Antall	0	1	4	6	8	3	9
	%	0,0	3,2	12,9	19,4	25,8	9,7	29,0

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	73,400(a)	6	,000

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
		Lower	Upper	Lower	Upper	Lower
Sum av formelle sikringstiltak	Equal variances assumed	,012	,914	-6,816	778	,000
	Equal variances not assumed			-6,883	32,588	,000

Revisjon/Rapportering oppsummert

T-Test – Group Statistics

	N	Mean	Std. Deviation	Std. Error Mean
MU	584	1,1096	,93069	,03851
ISF-U	31	1,7097	1,16027	,20839

Crosstabulation

		Revisjonstiltak/Rapportering			
		0	1	2	3
MU	Antall	172	228	132	52
	%	29,5%	39,0%	22,6%	8,9%
ISF-U	Antall	6	8	6	11
	%	19,4%	25,8%	19,4%	35,5%

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	22,821(a)	3	,000

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
		Lower	Upper	Lower	Upper	Lower
Revisjonstiltak/ Rapportering	Equal variances assumed	7,784	,005	-3,452	613	,001
	Equal variances not assumed			-2,832	32,082	,008

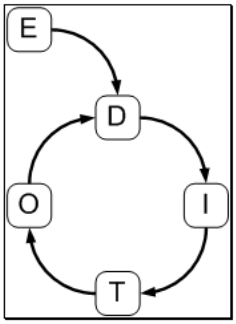
Appendiks F: Veiledninger for håndtering av datakriminelle hendelser

Veiledning for Håndtering av datakriminelle hendelser

Når en virksomhet utsettes for en datakriminell hendelse kan den, avhengig av omfang og alvorlighetsgrad, oppleves som en krise. For å håndtere en slik krise på en best mulig måte bør man ha utarbeidet en kriseplan.

En kriseplan for håndtering av datakriminell hendelser må være:

- **E**tablert — Prosessen med kriseplanlegging startet
- **D**okumentert: — Utarbeidet prosedyrer og retningslinjer som skal følges
- **I**mplementert: — Tilgjenglig for berørte parter og nødvendig opplæring gitt
- **T**estet regelmessig: — Eksempelvis skrivebordstesting og simulering av hendelser
- **O**ppdatert — I henhold til resultater fra tester, erfaringer fra tidligere hendelser og endringer i organisasjonen.



I forbindelse med håndtering av en datakriminell hendelse er det svært vesentlig at følgende er gjort på forhånd:

- Utarbeidet en retningslinje som beskriver i hvilke saker politiet skal kontaktes.
- Utpekt en koordinator, med stedfortreder, som skal ha det overordnede ansvaret for å håndtere hendelser.
- Identifisert kompetansepersonale – både internt og eksternt.
- Dersom virksomheten ikke selv har tilstrekkelig kompetanse til å håndtere hendelser, bør det inngås avtaler med eksterne ressurser.
- Sørget for at systemer og nettverk er godt dokumenterte og at dokumentasjonene er oppdatert.
- Aktivert logging på alle relevante enheter.
- Rutinemessig synkronisering av systemklokker på servere, nettverksenheter etc.
- Implementert rutiner for backup av servere og logger, og rutinemessig verifisering at backup kan leses.

En kriseplan for håndtering av datakriminelle hendelser bør omfatte:

- Interne og eksterne varslingslister. (Se vedlegg 3)
- Maler for å dokumentere hendelsen og håndtering av denne. (Se vedlegg 1 og 2)
- Dokumentert ansvarsfordeling – hvem skal gjøre hva?
  - Vurdering av hendelsen – hva har skjedd og hva må gjøres?
  - Varsle ledelsen i virksomheten
  - Varsle eksterne parter – eksempelvis driftsleverandører
  - Varsle politi (spesielt dersom angrepet fortsatt pågår)
  - Dokumentere hendelsen og alle aktiviteter
  - Rapportering til ledelsen underveis mens hendelsen håndteres
  - Håndtere juridiske aspekter i forbindelse med en eventuell anmeldelse
  - Ha kontakt med media, partnere og kunder?
- Dokumenterte prosedyrer for hvordan forskjellige typer hendelser skal håndteres
- Dokumentasjon for hvordan elektroniske bevis skal samles inn
- Dokumenterte prosedyrer for gjenoppretting av normal drift
- Prosedyrer for evaluering av håndtering av hendelsene

Outsourcing

Virksomheter som benytter driftsleverandører for hele eller deler av IT-driften bør sørge for at det er dokumentert i kontrakt med leverandør hvilket ansvar som påhviler denne i tilfelle virksomheten utsettes for en datakriminell hendelse.

Det bør spesifiseres krav i forbindelse med:

- Hva som skal logges, spesielt hvilke data.
- Hvor ofte logger skal gjennomgås.
- Hvor raskt leverandøren skal respondere og varsle dersom det oppstår en hendelse.
- Eventuelle plikter leverandøren har i forhold til sikring av elektroniske bevis.

Vedlegg 1: Datakriminelle hendelser, varsling og aktiviteter

Kommentar: Politiet er nevnt under varsling for de aller fleste kategorier. Erfaring viser at man bør kontakte Kripos, før man tar kontakt med lokalt politikammer, dersom man utsettes for straffbare sikkerhetshendelser av alvorlig karakter. Dette fordi Kripos har god kompetanse og kan gi vesentlig rådgivning dersom virksomheten selv må besørge sikring av elektroniske bevis.

Sikkerhetshendelse	Varsling	Aktivitet
Datainnbrudd (hacking) – pågår	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Datainnbrudd (hacking) har skjedd	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Angrep på tilgjengelighet (DoS-angrep) – pågår	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Angrep på tilgjengelighet (DoS-angrep) – har skjedd	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Barneporno – lagret på servere av eksterne	▪ Koordinator ▪ Politiet	▪ Anmod om at politiet foretar bevissikring ▪ Anmeld hendelsen.
Barneporno – surfing/lagring av egne ansatte	▪ Koordinator ▪ Politiet ▪ HR ▪ Vedkommendes overordnede	▪ Anmod om at politiet foretar bevissikring ▪ Anmeld hendelsen.
Datatyveri – uautorisert lesing/ kopiering av data – eksterne gjerningsmenn	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Datatyveri – uautorisert lesing/ kopiering av data – egne ansatte	▪ Koordinator ▪ HR ▪ Vedkommendes overordnede	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Endring/sletting av data (uautorisert) – eksterne	▪ Koordinator	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Endring/sletting av data (uautorisert) – egne ansatte	▪ Koordinator ▪ HR ▪ Vedkommendes overordnede	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Misbruk av IT-ressurser (PC/nett/server) – eksterne	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Misbruk av IT-ressurser (PC/nett/server) – egne ansatte	▪ Koordinator ▪ HR ▪ Vedkommendes overordnede	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Spredning av ulovlig/opphavsrettslig beskyttet materiale – eksterne	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Spredning av ulovlig/opphavsrettslig beskyttet materiale – egne ansatte	▪ Koordinator ▪ Politiet ▪ HR ▪ Vedkommendes overordnede	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Virus/orm/trojanerinfeksjon	▪ Koordinator ▪ Politiet	▪ Anmeldes dersom det er grunnlag for mistank om at angrepet er rettet mot virksomheten. Spesielt i forbindelse med trojaner-infeksjoner, da dette kan være en del av et datainnbrudd.
Trusler om å angripe IT-systemer	▪ Koordinator ▪ Politiet	
Bedrageri ved misbruk av kredittkort over internett	▪ Koordinator ▪ Politiet	▪ Foreta bevissikring dersom det ikke kan gis bistand fra politiet. ▪ Anmeld hendelsen.
Portskanning: Portskanning kan være et forutgående stadium for forsøk på datainnbrudd, men er per i dag ikke definert som en datakriminell handling. Portskanning sammenlignes ofte med at man går fra hus til hus og kjenner etter om ytterdøren er åpen. Så lenge man ikke går inn har man ikke begått et lovbrudd.	▪ Koordinator	▪ Anmeldes ikke. ▪ Ta en ekstra backup av logger. ▪ Dokumenter hendelsen. ▪ Vær oppmerksom.

Vedlegg 2: Hendelseslogg

Dato:		Hendelsestype:	
Klokkeslett:		Oppdaget av:	
Loggnummer:			
Hvilke systemer er berørt?			
Når ble hendelsen oppdaget?			
Hvordan ble hendelsen oppdaget?			

Følgende er informert om hendelsen:	Navn:	Funksjon:	Dato:	Klokkeslett:

Aktiviteter

Aktivitetsnr.:	Dato	Tid - start:	Tid - stopp:	Aktivitet:	Ansvarlig:	Kommentar:

Anmeldelse

Er hendelsen anmeldt?		
☐ Ja		☐ Nei
Dato for anmeldelse:		Hendelsen ble ikke anmeldt fordi:
Anmeldt til: (Politiet eller navn på politikammer)		

Vedlegg 3 – Varslingslister

Varslingsliste – Internt:

Navn	Enhet	Funksjon	Telefon Jobb	Telefon Mobil	Telefon Privat

Varslingsliste – Eksternt

Virksomhet	Navn	Funksjon	Telefon

Appendiks G: Veiledninger for sikring av elektroniske bevis

Veiledning for
Sikring av elektroniske bevis

Elektroniske bevis er avgjørende i forhold til håndtering av datakriminelle hendelser. Dette gjelder ikke bare i forhold til datainnbrudd, men også i økende grad i forhold til andre typer av datakriminalitet som begås mot virksomheter. Elektroniske bevis er også avgjørende i forhold til straffbare handlinger som begås av ansatte i virksomheten, eksempelvis i forbindelse med barnepornografi. Listen er over potensielle datakriminelle hendelser er lang og hver av disse hendelsestypene kan ende i en rettssak. Da er det vesentlig at man har elektroniske bevis som entydig kan dokumentere hendelsen.

Sikring av elektroniske bevis, når det har skjedd en datakriminell hendelse, skal i utgangspunktet foretas av politiet. I dag er dessverre situasjonen slik at det ikke finnes tilstrekkelig med ressurser innen politiet til å utføre disse oppgavene i forbindelse med all datakriminalitet som begås. Det anbefales at man umiddelbart tar direkte kontakt med Kripos i forbindelse med visse type saker – så som datainnbrudd, DoS-angrep og ikke minst dersom det oppdages at ansatte har surfet på/lagret barneporno på virksomhetens servere. Kripos har nødvendig kompetanse og kan gi råd om sikring av bevis og hvordan man skal håndtere datakriminelle hendelser.

I forbindelse med sikring av elektroniske bevis er følgende meget viktig:

Dersom virksomheten ikke har egne ressurser med tilstrekkelig kompetanse til å utføre denne oppgaven, må man benytte eksterne ressurser. Dette gjelder spesielt dersom man ikke kan få bistand fra politiet. Det er viktig at alle bevisene kan knyttes til hendelsen slik at de benyttes i en eventuell rettssak.

Viktige regler for elektroniske bevis dersom man vil anmelde:

- Bevisenes (dataenes) integritet må sikres.
- Bevissikringen må utføres av kompetent personale med egnede og anerkjente verktøy.
- Bevisene må kunne støtte opp om dokumentasjon av hendelsesforløpet.
- Bevisene må innhentes og analyseres ved hjelp av metoder som sikrer ekthet og pålitelighet.
- Bevisene må kunne presenteres på en slik måte at en jury kan forstå hendelsesforløpet.

Denne veiledningen har vi valgt å dele i to deler:

- Del 1 omfatter det som man må gjøre – bevissikring av logger
- Del 2 omfatter det som man bør gjøre – ytterligere bevissikring for å få komplette bevis.

Logger er vesentlig som første kilde, men man må gå til primær kilde, det som ligger på disken(e), for å kunne verifisere hva som er gjort.

Del 1: Bevissikring av logger

Hvorfor logge?

Man skal logge for å oppdage og forebygge sikkerhetshendelser og uautoriserte handlinger. Videre logger man for å etterleve lovkrav, virksomhetens informasjonssikkerhetspolicy og revisjonskrav. Ved at man logger kan man avdekke hvorvidt implementerte sikringstiltak fungerer tilfredsstillende. Videre får man oversikt over hva som skjer i systemer og nettverk. Det første tegnet på en uønsket hendelse er ofte endringer i systemer og nettverk, eksempelvis kan nettverkstrafikken øke drastisk. Loggfiler gir ikke alltid en full oversikt, men kan gi en indikasjon på at noe er under utvikling eller har skjedd.

Hva bør logges?

I forbindelse med logger tilknyttet nettverksenheter er ofte politiet interessert i at loggene inkluderer trafikk fra en periode før selve angrepet startet. Dette for å finne eventuelle spor som kan knyttes til kartlegging av systemet i forkant av selve hendelse, eksempelvis portskanning.

Alle brukeraktiviteter, avvik og sikkerhetshendelser bør logges. Man bør aktivere logger på følgende enheter:

1. Nettverksenheter:

- Rutere og svitsjer
- DHCP-servere
- Webservere
- Webcache
- Mailservere
- VPN
- Nettverkstrafikk (Netflow-logger)

2. Implementerte sikringstiltak:

- Brannmurer
- Antivirusløsninger
- IDS/IPS

3. Operativsystemer:

- Servere
- Arbeidsstasjoner (pc-er)
- Databaser

4. Applikasjoner:

- Egenutviklede applikasjoner
- Forretningsapplikasjoner
- Brukerapplikasjoner

I forbindelse med operativsystemer og applikasjoner bør man spesifikt logge følgende:

1. Autorisert tilgang:
    - bruker-id
    - dato og klokkeslett
    - typer av aktivitet
    - datafiler som er aksessert
    - programmer/hjelpeprogrammer som er brukt

2. Bruk av utvidede rettigheter, eksempelvis systemadministratorer:
   - bruker-id
   - dato og klokkeslett
   - aktiviteter
   - aksesserte datafiler
   - aksesserte programmer
   - oppstart og stopp av systemer
   - til- og frakobling av utstyr

   I tillegg bør det føres manuelle logger over aktiviteter som utføres av brukere med systemadministratorrettigheter eller andre spesielle rettigheter. Loggene bør omfatte:

   - Tidspunkt for aktiviteten
   - Identiteten til personen som utfører aktiviteten
   - Prosedyrer, verktøy og systemer som benyttes
   - Loggene bør regelmessig gjennomgås av en uavhengig part.

3. Forsøk på uautorisert tilgang
   - mislykkede påloggingsforsøk (bruker-id og tidspunkt)
   - forsøk på å åpne datafiler uten tilstrekkelig autorisasjon
   - forsøk på å endre/slette datafiler uten tilstrekkelig autorisasjon
   - brudd på tilgangsrettigheter og varsling i forbindelse med nettverksporter og brannmurer
   - alarmer fra proprietære innbruddsvarslingssystemer

Beskyttelse av logger

Det må tas backup av loggfilene daglig. Videre må loggfiler beskyttes mot manipulasjon og tekniske feil. Loggene bør skrives til en egen disk (egne disker) – helst på en egen server. Videre bør loggingsutstyr må beskyttes mot:

- Deaktivering av logging
- Enhver form for endringer av hva som skal logges
- Endring eller sletting av loggfilene
- Tekniske feil, eksempelvis overskrivninger fordi det ikke er avsatt tilstrekkelig med lagringsplass eller at logger ikke lagres fordi media er slitt ut

Utfordringer i forbindelse med håndtering av loggdata

En loggfil inneholder ofte store mengder med data og ikke alle dataene vil være relevante i forhold til å identifisere sikkerhetshendelser. Dersom man har mange loggfiler blir utfordringen desto større. For lettere å identifisere aktiviteter som er relevante i forbindelse med en sikkerhetshendelse er det derfor vesentlig at man kan konsolidere loggdata fra de forskjellige enhetene (server, IDS, brannmurer, rutere etc.). Dette kan gjøres gjennom å implementere verktøy/løsninger som automatisk kopierer bestemte typer data til en felles loggfil. Eventuelt også benyttet hjelpeprogrammer eller revisjonsverktøy for å utføre søking i loggfilene. For at loggingen skal ha en hensikt må loggfiler gjennomgås regelmessig og dette må gjøres av personer som har tilstrekkelig kompetanse til å tolk dataene. Videre må loggdata beskyttes ved overføring til eksempelvis analyseverktøy. Når det gjelder spørsmål om hvor lenge loggdata skal oppbevares så er dette, i forhold til visse typer data, regulert gjennom lover og forskrifter, eksempelvis IT-forskriften og Personopplysningsloven. I Tabell 1 vises forslag til håndtering av loggdata:

Tabell 1: Forslag til håndtering av loggdata

Kategori	Lite viktige systemer	Viktige systemer	Meget viktige systemer
Oppbevaring av loggdata	1 til 2 uker	1 til 3 måneder	3 til 12 måneder
Kopiering av loggdata til analyseverktøy	Innen intervallet 3 - 24 timer	Innen intervallet 15 til 60 minutter	Minst hvert 5. minutt
Loggdata bør analyseres	Minst ukentlig	Minst 1 gang i døgnet	Minst 6 ganger per dag
Integritetssjekking av loggfiler ved overføring til analyseverktøy	Valgfritt	Ja	Ja
Kryptering av loggfiler ved overføring til analyseverktøy	Valgfritt	Valgfritt	Ja
Backup av loggfiler	Daglig	Daglig	Daglig

Synkronisering av systemklokker

Riktig innstilling av systemklokker er viktig for å sikre loggenes nøyaktighet og dette er svært vesentlig i forbindelse med etterforskning av en sikkerhetshendelse. Unøyaktige systemklokker kan forhindre etterforskning og svekke bevisenes troverdighet. Dersom det er mulig å benytte sanntidsklokke i datamaskiner og/eller nettverksenheter bør denne stilles etter bestemt standard, eksempelvis Greenwich Mean Time (GMT). Man kan også benytte NTP (Network Time Protocol), som er en protokoll designet for å synkronisere klokker på alt IT-utstyr som er knyttet til et nettverk. NTP supporterer både Unix og Windows.
Dessuten bør man, uansett om man bruker sanntidsklokke, implementere prosedyrer for regelmessig å sjekke at systemklokkene er synkronisert.

Hva skal gjøres med loggfilene ved en sikkerhetshendelse?

- Ta en backup av loggfilene ved å kopiere bit-for-bit, med checksum av originaldisk(ene) og kopidisk(er). Det anbefales at det benyttes en maskinvarebeskytter – write blocker – slik at loggfilenes egenskaper (attributter) ikke endres.
- Ikke kjør analyse på de(n) originale disken(e), den (disse) må oppbevares på en sikker måte slik at politiet kan benytte disse dersom de skal kjøre egne analyser.
- Installer ny disk(er) for lagring av loggfiler.
- Ved analyse av kopidisken(e) må det benyttes en maskinvarebeskytter – write blocker – for å beskytte dataene på disken(e) som skal analyseres. Write blocker-en plasseres mellom disken som skal analyseres og maskinen som benyttes for analyse, og skrivebeskytter kopidiskene slik at man forhindrer at dataene endres (for eksempel dato og tid på enkelte filer) ved tilkobling til en analysemaskin.
- Ha ekstra disker tilgjenglig.

Del 2: Ytterligere bevissikring

Under forutsetning av at man enten har egen kompetanse på området eller benytter eksterne ressurser anbefales det at man foretar ytterligere bevissikring, eksempelvis servere som er angrepet/kompromittert, og ikke bare sikrer logger fra diverse enheter.

Den bevissikringen som vi i korthet redegjør for her forutsetter at man på forhånd har en dokumentert og testet metodikk for gjennomføringen. Dersom dette ikke er gjort er det stor fare for at man kan ødelegge viktige elektroniske bevis. I tillegg til at metodikken inneholder prosedyrer som skal følges må den også omfatte det man kaller "first responders toolkit", med andre ord verktøy som skal benyttes av den som gis ansvar for bevissikring.

"First responder toolkit"

Når man skal lage en "first responder toolkit" – verktøykasse – for sikring av elektroniske bevis må man på forhånd ha gjort følgende:

- Dokumentert prosedyrer for gjennomføring av bevissikringen.
- Dokumentert, og kontinuerlig oppdatert, hvilke operativsystemer som virksomhetens servere kjører.
- En maskinvarebeskytter – write blocker – for å beskytte dataene på disken(e) som skal analyseres.
- Velge hvilke verktøy som skal benyttes i forhold til hvilke operativsystemer som kjøres:
  - Verktøy for kopiering av "volatile" (temporære) data
  - Verktøy for kopiering av metadata
  - Verktøy for av bit-for-bit-kopiering
  - Verktøy for å generere sjekksummer (hash-verdier) og digitale signaturer for filer og andre data
  - Lag boot-bare cd-er/dvd-er med verktøyene som er valgt
- Sørge for at de som skal besørge den elektroniske bevissikringen har fått tilstrekkelig opplæring i forhold til de prosedyrer som må følges og de verktøyene som skal benyttes.

"First responder toolkit" bør bestå av:

- En bærbar pc installert med flere typer av operativsystemer og verktøy (programmer) for å hente ut elektroniske bevis. Disse verktøyene må være testet på forhånd slik at man vet at man kan hente ut de bevisene man trenger.
- Backup-utstyr
- Blanke media (disker, cd-er, dvd-er)
- Nettverksutstyr
- Kabler

Fremgangsmåte for bevissikring

1. Dokumenter kronologisk alle aktiviteter som utføres i forbindelse med bevissikringen.

2. Serveren må ikke slås av og det må ikke kjøres shutdown. Dersom man gjør det kan man miste temporære data som er lagret i minne (RAM) og som forsvinner dersom man tar strømmen til serveren eller kjører shutdown.

NB: Dersom man har mistanke om at foregår destruktive aktiviteter på serveren, så som aktiviteter rettet mot annet IT-utstyr som står på samme nettverkssegment eller at aktiviteter sletter bevis på serveren som er vesentlig for etterforskningen bør følgende gjøres:

   - Koble serveren fra nettverket.
   - Trekk ut strømstøpselet – kjør ikke shutdown for da kan man miste ytterligere bevis eventuelt kan angriper ha installert script/programmer som gjør ytterligere skade dersom man kjører shutdown.
   - Gjennomfør punkt 3 og gå til punkt 5.

3. Kobl til den bærbare pc-en, med eksterne harddisker, som skal benyttes for å sikre bevis til serveren. Pc-en må tilkobles via en maskinvarebeskytter – write blocker.
4. Kopiering og sikring av temporært minne. Gjennomfør aktiviteter for å sikre data som er lagret i minne (RAM) og gjør dette i henhold til dokumentert prosedyrer. Sikring av temporære filer og prosesser gjøres med uttestet og anerkjent programvare for deretter å bli skrevet til eksternt medium (minnepinne eller lignende).

   Data som bør kopieres er eksempelvis:

   - Registers and Cache
   - Routing Tables
   - Arp Cache
   - Process Table
   - Kernel Statistics and Modules
   - Main Memory
   - Temporary File Systems
   - Secondary Memory
   - Router Configuration
   - Network Topology

5. Trekk ut strømstøpselet og nettverkskabel, og start opp serveren ved hjelp av en boot-bar cd/dvd.

6. Kopier metadata ved hjelp av uttestede og anerkjent programvare.

7. Ta en bit-for-bit-kopi av hele serverens harddisk(er) ved hjelp av uttestede og anerkjent programvare og generer sjekksummer (hash-verdier) og digitale signaturer for filer og andre data.

8. Trekk ut serverens strømstøpsel og ta ut disken(e). Forsegl de og oppbevar de på en sikker måte.

9. Ta en backup av verktøyene som er benyttet i forbindelse med bevissikringen slik at det i etter tid kan redegjøres for hvordan arbeidet er utført.