Insider Threat

Jon Petter Syvertsen

Master's Thesis
Master of Science in Information Security
30 ECTS
Faculty of Computer Science and Media Technology
Gjøvik University College, 2007

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

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

Sammendrag

Denne masteroppgavens rapport retter søkelyset mot innsidetrusselen i Norge. Ved å se på nettopp dette, ønsker vi å kartlegge denne trusselen.

Vi ønsker også å finne ut om Norge er mer eller mindre utsatt for samme type angrep enn USA. For å kunne finne svarene på dette, så ble det laget en spørreundersøkelse som ble sendt ut til over 50 ulike bedrifter innenfor to sektorer. Av disse var det bare 7 stykker som valgte å besvare denne undersøkelsen. Dette førte til at

Som nevnt var oppgavens intensjon å kartlegge innsidetrusselen i Norge, samtidig som vi vil bevisstgjøre bedrifter om dette problemet. Ved å utføre en grundig litteraturstudie, så har vi fått et dypere innblikk i trusselen fra innsidere. Denne kunnskapen ville vi bruke for å danne et inntrykk av samme problemstilling i Norge. Dessverre lyktes vi ikke med dette. Ettersom flere bedrifter ikke ønsket å delta i undersøkelsen, så har vi ikke nok grunnlag til å kunne gi et godt bilde av denne type trussel i Norge.

Gjennom en spørreundersøkelse har vi skaffet informasjon om innsidetrusselen blant 7 norske bedrifter fra to ulike sektorer. Årsaken til denne lave deltagelsen er mange, men bedriftene er meget tilbakeholden med opplysninger som er så sensitive.

Rapporten tar for seg de viktigste funnene i undersøkelsen, hvor vi analyserer og sammenligner dataene med spørreundersøkelsen utført av CERT i 2006. Fra de dataene vi har analysert er det ikke noen svar som skiller seg veldig ut. Bedriftene gir et inntrykk av at angrep fra utsiden og innsiden er meget beskjedne. Av de angrepsforsøkene som bedriftene har vært utsatt for, så viser det seg at nesten ingen av dem er vellykkede.

De fleste angrepsforsøkene viser seg å komme fra utsiden. Det samme kan vi se fra undersøkelsen til CERT. Selv i de angrepene som har vært vellykkede har ikke bedriftene hatt noen kritiske tap i form av driftsstans eller store økonomiske tap. Noen bedrifter har opplevd tap av kunder på bakgrunn av hendelser på innsiden, men det kommer ikke frem i undersøkelsen hvor mye dette kostet bedriften økonomisk.

Abstract

This thesis takes a closer look into the insider threat problem in Norway. By reviewing this problem, we hope to be able to map this threat.

We wanted to find out weather the insider threat is a bigger problem in Norway then USA or vice versa. To find answers on the problem we made a survey. This survey was sent to over 50 unique companies within two different sectors. Only 7 companies chose to participate in this survey.

As mentioned, the goal for this report was to map the insider threat in Norway, at the same time we try to make companies aware of this kind of threat. By carrying out a thorough literature study, we have been able to get a deeper insight in the threat performed by insiders. This knowledge where used to create an impression of current problem in Norway. Unfortunately we were not able to do this. Since many companies did not want to participate in the survey, we do not have enough material to make an impression of this kind of threat here in Norway.

By performing a survey, we were able to get inside threat information from 7 Norwegian companies from to unique sectors. There are lots of reasons why so many chose not to participate, but most companies informed that they would not share this kind of sensitive information.

This report looks into the most important discovery in the survey, at the same time we analyse the data and compare this survey with the survey from CERT 2006. The data we have analysed, there is not much to report. We get the impression that security events carried out from the outside or inside is very low. Therefore have there been very few successfully security events.

Most security events seem to occur from outside the security perimeter. This is also noticeably in the survey from CERT. Even if the attacks have been successfully, the companies did not suffer any financial loss or system disruption. Some companies experienced loss of customers based on a security event. The survey does not give us any indication on how much the loss of customers cost.

Takk til

Min veileder Jose J. Gonzalez ved Universitetet i Agder, som har bidratt med uvurderlig støtte gjennom hele arbeidet med oppgaven. Han har vært tilgjengelig, vært til stor inspirasjon og hjelp i med kritiske spørsmål og konstruktive kommentarer.

Takk til NorSIS og Espen Torseth som har bidratt med lisens til programmet QuestBack, som ble brukt for å lage spørreundersøkelsen.

Takk til Odd Hauge for godt samarbeid og god støtte gjennom store deler av masterstudiet.

Til slutt vil jeg takke alle virksomheter som bidro med data til oppgavens resultater ved å delta i spørreundersøkelsen. Uten deres bidrag hadde resultatene uteblitt.

Tusen takk!

Lørenskog, 30.10.2007

_____

Jon Petter Syvertsen

Innholdsfortegnelse

1 Innledning

1.1 Tema

Mange organisasjoner bruker store summer på å sikre bedriften mot angrep som kommer uten i fra. Det mange ikke er klar over er at det skjer også ngrep skjer på innsiden av organisasjonen. Grunnen til at mange angrep skjer på innsiden av organisasjon er fordi personer har enkel og lovlig tilgang til utstyr, brukerkonto og nettverk. Ved at man har tilgang til slike ressurser, så er det lettere å tappe informasjon, eller skade systemet. Slike tap kan koste organisasjonen dyrt og skape dårlig publisitet om dette blir offentlig kjent. I en artikkel fra CERT blir det nevnt at denne type angrep er underrapportert på grunn av mangel på bevis og at organisasjonens er redd for sitt renommé [13].

I Norge er det gjort lite undersøkelser på lik linje med CERT, som viser omfanget av slike angrep mot ulike sektorer [11] [13]. I denne oppgaven vil vi lage en spørreundersøkelse mot 2 ulike sektorer for å danne et bilde av denne type trussel i Norge.

1.2 Problembeskrivelse

Innside trusler er en form for angrep som vil bli mer og mer utbredt. Ettersom man regner med at den er underrapportert, så kan vi anta at det også er et problem i Norge som vil øke med tiden.

Problemene med slike angrep er at de er vanskelig å forutse og beskytte seg mot. De blir utført av personer som har tilgang på lovlig vis, for eksempel brukerkonto, nettverk eller hjemmekontor. Fra diverse undersøkelser, så viser det seg at gjerningsmennene ikke skiller seg spesielt ut.

Forskjellige angrep har blitt utført av personer mellom 18-59 år, og hele 31 % var gift og hadde familie. Så lite som 27 % av de som har utført en kriminell handling fra innsiden hadde vært straffet fra før [11].

Et annet problem med en slik trussel er at den kan utføres enkelt av personer med mindre teknisk bakgrunn. I de fleste sammenhenger viste det seg at gjerningsmennene ikke kunne knyttes til noen historikk innenfor tekniske angrep eller ”hacking” [11]. Dermed er det ikke lett å kunne avsløre hvem som kan komme til å utføre et angrep fra innsiden.

Uansett hvem som utfører slike angrep, så kan det koste organisasjonen masse penger i form av direkte tap, eller gjenoppretting av skaden som er påført.

Ved å utføre en slik undersøkelse, så kan vi gjøre organisasjoner oppmerksomme på en slik type trussel i Norge.

I denne rapporten vil vi se på problemene forbundet med trusler på innsiden og hvor

mye dette koster organisasjoner per år.

1.3 Motivasjon og gevinst

Målet med å kartlegge en slik trussel i Norge er for å informere organisasjoner om problemene med trusler på innsiden. Ved å informere og kartlegge problemet i enkelte sektorer, så vil organisasjonene kunne lettere beskytte seg mot en slik trussel.

Tall fra blant annet USA viser at skader fra et slik angrep har kostet en enkelt organisasjon over $10.000.000 [13]. Slike summer rammer en organisasjon og med kunnskap om slike angrep, så er målet at man unngår slike tap.

Fordi vi vet så lite om denne formen for angrep og hvordan vi skal beskytte oss, så er denne undersøkelsen veldig relevant for alle bedrifter og offentlige sektorer.

1.4 Forskningsspørsmål

I denne oppgaven vil i prøve å kartlegge innside trusselen i Norge. Vi tok for oss 2 ulike sektorer for å få et bedre bilde av problemet, og en høyere svarprosent.

For å komme frem til en så god undersøkelse som mulig, så har vi stilt oss disse forskningsspørsmålene:

1. Hva slags undersøkelser har blitt utført tidligere i Norge og utlandet?
2. Hvor utbredt er ”insider threat” i Norge?
3. Hvilke sektorer er det mest hensiktsmessig å ta kontakt med i forbindelse med en slik undersøkelse?
4. Vil spørreundersøkelsen kunne hjelpe oss i arbeidet med å redusere slike trusler i Norge?
5. Hvordan er innsidetrusselen i Norge sammenlignet med tilsvarende undersøkelser fra CERT?

For å få en oversikt over hvordan innside trusselen er blant norske organisasjoner, vil vi bruke kvantitativ metode for å få tilgang til underlagsdata. Vi vil derfor utføre en spørreundersøkelse mot de aktuelle bedriftene. I spørreundersøkelsen vil vi legge vekt på å få svar på noen av forskningsspørsmålene.

- Hvor utbredt er ”insider threat” i Norge?
- Vil spørreundersøkelsen kunne hjelpe oss i arbeidet med å redusere slike trusler i Norge?
- Hvordan er innsidetrusselen i Norge sammenlignet med tilsvarende undersøkelser fra CERT?

Denne spørreundersøkelsen vil være basis for å kunne kartlegge problemet om innside trusselen blant norske sektorer.

2 Relatert arbeid

For å få en bedre innsikt i innsidetrussel problematikken, så vil vi først se på definisjonen av en innsider. Videre ser vi på relaterte undersøkelser, og hva disse har funnet ut av innsidetrusselen.

2.1 Definisjon på en innsider

Mange skriver om innsider problemer, men ikke alle har en klar definisjon på hva en innsider egentlig er. Ved å søke på ordet ”insider” i en engelsk ordbok på nettet http://dictionary.reference.com/ så finner vi denne definisjonen fra American Heritage Dictionary:

1. An accepted member of a group.
2. One who has special knowledge or access to confidential information.

Ved å se på denne definisjonen fra oppgavens problemstilling, så kan vi tolke en innsider på denne måten.

En innsider kan være en ansatt i en bedrift som har blitt akseptert av bedriften og er innenfor sikkerhetsperimeteren som bedriften har satt opp for å motvirke angrep og innsyn i sensitive data.

Innsidere i en bedrift har/eller kan skaffe seg informasjon som brukernavn og passord som gir dem lettere tilgang til systemene og sensitiv informasjon. Noe en fra utsiden ikke har samme mulighet til.

Den generelle definisjonen på en innsider fra American Heritage Dictionary er ikke så veldig ulik den vi finner i ulike artikler. Stort sett finner vi de samme definisjonene i de forskjellige artiklene, men vi velger å se på definisjonen av en innsider som i artikkelen ”The insider problem” av Matt Bishop [23].

1. Ondsinnede handlinger utført av personer som allerede er autorisert med tilgang til sensitiv informasjon og informasjonssystemer.
2. Noen med tilgang, fordel (privilegium), eller kunnskap om informasjonssystemet og tjenester.
3. Enhver person som betjener datasystemer fra innsiden av sikkerhetsperimeteren.

Nå som vi har sett litt på definisjonen av en innsider, så kan følgende scenarioer gi oss et bilde på hva en innsider er. Hvert av scenarioene under viser et eksempel på de definisjonene som er nevnt over [23].

1. En medarbeider ved en militærbase får vite at hun skal bli sagt opp. Dermed krypterer hun kritiske filer på systemet og tilbyr dekrypteringsnøkkelen mot en betaling på $10 000 og uten politianmeldelse. Arbeidsgiveren går med på tilbudet. Vedkommende har ikke ødelagt noe informasjon på systemet, bare forhindret tilgang til de kritiske systemfilene for en periode.
2. En systemadministrator ved en bank finner en overføring på $10 000 000 i systemet. Dette beløpet var overført fra konto 1011 til konto 6734. Vedkommende

ser at dette kontonummer er veldig likt en nær venn sitt kontonummer, som er 6834. Penge blir overført til vennens konto samtidig som deler av den originale loggfilen blir slettet, mens noe blir endret for skjule overføringen fra konto 6734 til 6834.

3. En vaktmester i et stort firma finner personnummer på en ansatt i søpla. Denne informasjonen blir brukt til å utføre identitetstyveri.

Som vi kan se av de ulike scenarioene over, så tilfredsstiller hver av dem hvert sitt punkt i definisjonen av en innsider.

2.2 Undersøkelser om innsidetrussel

Arbeid med innsidetrusselen i Norge virker noe begrenset ut i fra litteraturen vi kan finne om temaet. De fleste undersøkelser kommer fra utlandet, mye fra USA. CERT har sammen med U.S. Secret Service, gjennomført en omfattende undersøkelse i 2004, 2005 og 2006. Undersøkelsene fra 2004 og 2005 ble utført som en studie for å undersøke temaet innsidetrusselen i forskjellige sektorer.

CSI og FBI i San Francisco har siden 1995 utført undersøkelser om temaet datakriminalitet og sikkerhet. Disse undersøkelsene blir omtalt for å ha holdt på lengst når det gjelder å undersøke informasjonssikkerhet.

Andre relaterte undersøkelser er utført av både norske og utenlandske studenter. De er mer rettet mot forebyggende arbeid og bevisstgjøring av denne trusselen, og ikke en direkte undersøkelse av problemet.

2.3 Undersøkelser utført av CERT

Den første rapporten fra CERT er en studie om *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* fra 2004. Fokuset her er basert på hendelser innen bank og finanssektoren. Den andre rapporten *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* fra 2005, tar for seg undersøkelser fra 49 innsidehendelser på tvers av sektorer for kritisk infrastruktur. Her var primær målet til gjerningsmannen å sabotere deler av organisasjonen eller enkelt individer.

CERT ønsket med denne undersøkelsen å undersøke innsiderne på det mentale planet om hvorfor de utførte disse angrepene. I tillegg undersøkte de teknikkene som ble brukt for å utføre angrepene mot bedriftene.

2.3.1 Bank og finanssektoren

En av de første artiklene som tok for seg problematikken omkring innsidetrusselen kom i 2002 [14]. Denne tok i hovedsak for seg forståelsen og hvordan forutse angrep på innsiden.

Først to år senere kom det en mer omfattende rapport fra CERT og United States Secret Service. Denne tok for seg problematikken omkring innsidetrusselen i Bank og

Finans sektoren. Ved hjelp av spørreundersøkelser prøvde de å finne ut om det var noen sammenheng mellom gjerningsmennene, deres interesser, bakgrunn, forhold til organisasjonen etc.

Studien var ment på å analysere hendelsene fra en atferds- og teknisk perspektiv. Hendelsene som ble undersøkt i studiet var utført av personer på innsiden (nåværende og tidligere ansatte eller leverandører), som bevisst utførte eller missbrukte en autorisert tilgang på nettverket, systemet, eller data som berørte sikkerheten til organisasjonens datasystemer. Undersøkelsen tar for seg hendelser som har skjedd i perioden 1996-2002 [6] [7] [11].

Siden 2001 har U.S. Secret Service og CERT/CC utført flere forsøk for å identifisere, fastsette og håndtere potensielle trusler mot data og kritiske systemer. Samarbeidet representerer en forbedret sikkerhet og beskyttende praksis gjennom to elementer:

1. Finne måter å identifisere, fastsette og formidle truslene mot data og kritiske systemer som kan påvirke sikkerheten og true bedriften.
2. Finne måter å identifisere, fastsette og formidle individer som utgjør en trussel mot data og kritiske systemer.

Målet med undersøkelsen var å skaffe mer informasjon om selve innsidetrussel problemet. Informasjonen skulle hjelpe privat sektor, myndigheter og politi til en bedre forståelse, hvordan oppdage og forhindre skadelig innsideaktivitet. Studien består av flere elementer:

- En grundig analyse av hendelser som inntraff kritisk infrastruktur mellom 1996 og 2002.
- Gjennomgåelse av forekomster innen innsidetrusselen på tvers av kritisk infrastruktur over en 10 års periode.
- En undersøkelse basert på nylig opplevd innsideaktivitet av et utvalg på offentlig og privat sektor.

Rapporten fra CERT tar for seg 23 hendelser utført av 26 innsidere i bank og finanssektoren. Av de 23 hendelsene var 15 av dem svindel, 4 var tyveri av opphavsrett og 4 var sabotasje mot informasjonssystemer og nettverk.

2.3.2 Funn fra undersøkelsen i bank og finanssektoren

De fleste hendelsene som ble undersøkt i bank og finanssektoren var ikke spesielt tekniske eller komplekse. Typisk for disse hendelsene var utnyttelse av fortetningsinstrukser og policyer innad i organisasjonene. Disse svakhetene ble utnyttet fordi man i liten grad trengte tekniske ferdigheter for å utføre angrepene. Her er de viktigste funnene fra CERT oppsummert.

Funn 1:

- I 87% av tilfellene som ble undersøkt av CERT, viste det seg at innsiderne brukte enkle lovlige kommandoer for å utføre hendelsene. I få tilfeller (9%) ble det brukt et skript for å gjennomføre et angrepet. Det ble ikke funnet noen beviser på at

datamaskiner ble skannet for å avsløre sårbarheter før hendelsene inntraff.

- I 70% av tilfellene som ble studert utnyttet eller ble det gjort forsøk på å utnytte systematisk sårbarheter i programmer og/eller prosesser eller prosedyrer. I 61% av tilfellene ble sårbarheter knyttet til design av hardware, programmer eller nettverk utnyttet.
- I 78% av tilfellene var innsiderne autoriserte brukere med brukerkonto da hendelsen inntraff. I 43% av tilfellene brukte innsideren sitt egent brukernavn og passord for å utføre hendelsen.
- I 26% av tilfellene ble det enten brukt en annen brukerkonto, en ubeskyttet terminal uten beskyttet brukernavn eller "social engineering" (for eksempel, skaffe seg tilgang ved å manipulere en person eller personer som har muligheten til å gi tilgang til ulike personer).
- Kun 23% av innsiderne var ansatt i tekniske stillinger, hvor bare 17% hadde administrator/root tilgang på systemene.
- 39% av innsiderne hadde ikke kjennskap til organisasjonens sikkerhetstiltak.

De fleste hendelsene viste seg å være planlagt i god tid. I Noen tilfeller hadde andre personer kjennskap til innsiderens hensikt, planer og/eller aktiviteter.

Funn 2:

- I 81% av hendelsene, hadde innsideren planlagt sine gjerninger i forkant.
- I 85% av hendelsene, så hadde noen full eller delvis kjennskap til innsiderens hensikt, planer og/eller aktiviteter. Dette gjelder:
  - Personer som var involvert i hendelsen og/eller skulle dra nytte av innsideaktiviteten (74%)
  - Medarbeidere (22%)
  - Venner (13%)
  - Familiemedlemmer (9%)
- I 61% av tilfellene var det noen personer i innsiderens omgangskrets som kjente planene.
- I 31% av tilfellene var det en merkbar indikasjon på innsiderens planlagte hendelser.
- 65% tok ikke i betraktning muligheten for de negative konsekvensene etter et angrep.

De fleste gjerningsmennene hadde økonomisk motiv contra det å skade selskapet eller informasjonssystemet. Andre motiver var hevn, missnøye til ledelsen, kulturer eller policyer eller ønske om respekt.

- Funn 3:
- 81% av innsiderne hadde penger som motiv eller mål for hendelsen. Kun 27% hadde finansielle problemer når hendelsen inntraff.
- Andre årsaker til motivasjon var
  - Hevn (23%)
  - Missnøye til ledelsen, kulturer, eller policyer (15%)
  - Ønske om respekt (15%)

- 27% hadde med hensikt å sabotere driften til firmaet, data, eller bedriftens informasjonssystem/nettverk . Noen hadde også fått i oppdrag å stjele informasjon (19%).
- I 27% av hendelsene, så hadde innsiderne flere motiver for å utføre slike handlinger.

Av de gjerningsmennene som ble studert, så var det stor variasjon mellom de forskjellige innsiderne.

- Funn 4:
- Innsidernes alder varierte fra 18 til 59 år. 42% av dem var kvinner. 54% var single, mens 31% var gift.
- Få av innsiderne var kjent for å være vanskelige å lede (15%) eller upålitelig (4%).
- 19% av innsiderne ble oppfattet som misfornøyde av sine medarbeidere.

Som vi kan se fra disse funnene så er det ingen klare skiller på hvem som utførte angrepene mot bedriftene. Dette er en av grunnene til at det er vanskelig å beskytte seg mot innsidere.

Angrepene er også vanskelig å oppdage ettersom de kan være veldig enkle og blir utført av personer med lite teknisk bakgrunn. Likevel viser det seg at slike angrep kan gjøre stor skade på bedriften.

2.3.3 Sabotasje av datasystemer i sektorer med kritisk infrastruktur

Undersøkelsene fra denne rapporten viser at de fleste tilfellene av sabotasje på innsiden var utført av tidligere ansatte i tekniske stillinger.

Som et resultat av denne undersøkelsen, så kunne de finne elementer som førte til en slik handling. Noen nøkkelelementer:

- Årsaken til slike hendelser ble som oftest utløst på grunn av negativ opplevelse på arbeidsplassen.
- De fleste insidere utførte handlingene uten for mye oppmerksomhet på arbeidsplassen.
- Insiderne planla handlingene i forkant.
- Ved ansettelse fikk mange administrator rettigheter eller privilegert tilgang til systemet. Under halvparten av disse hadde autorisert tilgang da hendelsen inntraff.
- Det ble ikke brukt avanserte metoder for å utnytte sårbarhetene i prosesser, programmer og prosedyrer.
- Flertallet av insiderne skaffet seg ulovlig brukertilgang, lagde uautoriserte brukerkontoer eller brukte delte brukerkontoer for å utføre angrepene.
- ”Remote access” ble også mye brukt i slike angrep.
- De fleste ble avslørt på grunn av at det ble oppdaget avvik i informasjonssystemet eller at systemet ble utilgjengelig.
- Innside aktivitetene påførte organisasjonene finansielle tap, negativ innvirkning på driften og skadet organisasjonens renommé.

I denne rapporten ble det sett på ulike karakteristiske trekk ved innsiderne. De fant ut følgende:

- Nesten 60% av innsiderne var tidligere ansatte da hendelsen inntraff. Resten var ansatt da hendelsen fant sted.
- Av de innsiderne som hadde vært ansatt i bedriften, så ble nesten 50% av dem oppsagt av ulike årsaker.
- Blant innsiderne var nesten 80% heltidsansatt.
- Innsiderne besto av personer mellom 17-60 år.
- Hele 96% av innsiderne var menn.
- 30% hadde blitt straffet tidligere.

Det viste seg også at det var enkelte typer sektorer som skilte seg ut i forhold til de andre.

- 8% av hendelsene skjedde i bank- og finanssektoren.
- Hele 63% av hendelsene skjedde i informasjons- og telekommunikasjonssektoren.

Som vi ser av denne undersøkelsen, så har informasjons- og telekommunikasjonssektoren vært veldig attraktive mål for sabotasje av innsidere. Dette er en veldig god indikasjon på hvilken sektor som er interessant for undersøkelsen som ble sendt ut til norske bedrifter. Valg av sektorer er beskrevet mer i detalj i kapittel 3.3.1 Utvalget.

Funne fra denne undersøkelsen viser helt klare motiver til innsiderne.

- I 92% av tilfellene viste det seg at det var en enkelt eller en rekke hendelser på jobben som utløste handlingen.
- Hele 85% av innsiderne var plaget i forkant av hendelsen. I 92% av disse tilfellene var plagen jobbrelatert. Problemene var oftest rettet mot medarbeidere eller sjefen.
- 84% av episodene som inntraff var motivet å hevne seg. I over halvparten av tilfellene hadde innsideren mer enn et motiv for å utføre hendelsen.

Det som ble oppdaget i denne rapporten var at de fleste hendelsene var planlagt i god tid før hendelsen inntraff. Angrepet var også kjent blant noen av de ansatte, men det ble aldri rapportert. Mange av innsiderne uttrykte sin missnøye, og til tider kom det frem direkte hevnaksjoner. Adferden til innsiderne ble oftest lagt merke til av medarbeidere i form av lavere arbeidslyst, mye fravær og mye diskusjon med medarbeidere.

Videre viser analyser av hendelsene at over 60% av innsiderne hadde lagt planer for hvordan de skulle skade bedriften. I 42% av sakene var forberedelsene så åpenlyse før hendelsen, som å stjele backup-taper og lignende. Under 30% av tilfellene involverte en noe mer teknisk oppgave som testing av logiske bomber på nettverket, sabotere backup eller installere bakdører.

I en tredjedel av tilfellene hadde andre viten om de planene som innsideren skulle utføre. Oftest var det bare medarbeidere som visste om planen til innsideren, men i enkelte tilfeller visste også venner og familie om det.

Mye av problemene knyttet til sabotasje på infrastruktur kan ha en sammenheng med at over halvparten av innsiderne ble tildelt administratorrettigheter til systemet da de ble ansatt. Sårbarheter i programmer og prosedyrer ble utnyttet til fordel for å enklere kunne utføre angrepene på arbeidsplassen.

Andre metoder ble også brukt for å lettere kunne skjule sin identitet. Ofte ble brukerkontoene til medarbeiderne utnyttet, eller det ble opprettet uautoriserte brukerkonti som bakdører. Det hendte også at det ble brukt konti som var delt mellom flere brukere. Nå som innsiderne hadde opprettet konti som bakdører, så åpnet dette for angrep som kunne skje ved hjelp av fjerntilgang. Dermed kunne også fleste parten av angrepene skje uforstyrret og etter arbeidstid.

Enkelte brukerkonti var i tillegg fortsatt operative etter at innsideren hadde sagt opp sin stilling. Så bare 43% av innsiderne hadde lovlig tilgang til systemet/nettverket da hendelsen inntraff.

Selv med usofistikerte metoder, så viser det seg at innsiderne klarte å gjøre skade på informasjonssystemet.

Den mest vanlige metoden som ble brukt var å utnytte en brukerkonto til angrepet. I en tredel av tilfellene, så ble andre medarbeideres konti brukt for å utføre angrepet. Kun i en femtedel av tilfellene ble en uautorisert opprettet konto brukt. Over 90% av disse hendelsene ble heller ikke sett på som noen mistenkelig aktivitet.

Angrepene som ble utført mot bedriftene ble kun oppdaget da det var uregelmessighet i informasjonen på systemet eller om systemet ble utilgjengelig. System loggene var de mest effektive hjelpemidlene for å avsløre innsiderne. Hele 70% ble avslørt på denne måten.

Det er også tilfeller der innsiderne slettet eller modifisere loggene på systemet for å kunne skjule identiteten og aktiviteten.

De fleste angrepene var gjennomført ved å bruke utstyret til bedriften, og rundt halvparten av disse tilfellen var med maskiner som tilhørte andre medarbeidere. Innsamling av tekniske bevis viste seg å være meget effektivt for å avsløre identiteten og samle beviser mot innsiderne. Generelt ble 75% av innsiderne avslørt ved manuelle prosedyrer.

Angrep forårsaket av innsidere hadde stor betydning for bedriftens omdømme. I tillegg opplevde bedriftene store finansielle tap og negativ innvirkning på den dagelige driften. Data, systemer/netteverk og komponenter ble rammet av angrepene.

75% av bedriftene opplevde innvirkning på datasystemene etter et angrep. Problemene kunne vise seg å være utilgengelig nettverk eller servere. Ødeleggelse av kritisk informasjon som lagringsmedia, datasystemer, og opphavsbeskyttet programvare.

Innsiderne gikk som oftest inn for å sabotere informasjonssystemene, bedriftsoperasjoner eller dataene. Enkelte hadde også til hensikt å skade spesielle personer.

For å sammenligne disse to undersøkelsene, så kan vi si at innsiderne hadde ulike motiver for sine angrep. I den første rapporten ser vi at de ikke hadde som hensikt å skade bedriftens omdømme, men ble mer fristet av økonomisk vinning.

I den andre rapporten fra CERT er motivasjonen å skade bedriften, medarbeidere eller sjefen. Den utløsende faktor for hendelsene er ofte relatert til missnøye på arbeidsplassen.

2.4 Undersøkelser utført av CSI/FBI

CSI har sammen med FBI avdelingen i San Francisco utført en rekke undersøkelser i forbindelse med datasikkerhet. De undersøkelsene som vi har funnet til nå er fra 2003 og fram til 2006 [19][20][21][22].

Viktige elementer fra undersøkelsene:

2003 (året 2002):

- Antallet hendelser er fortsatt det samme som året før, til tross for at de finansielle tapene er mindre
- Tyveri av konfidensiell informasjon medførte de størst finansielle tapene
- DNS angrep er den nest største kostnaden ved datakriminalitet
- Drastisk nedgang i rapportering av tapt grunnet finansiell svindel
- Virus angrep og missbruk av intern nettverkstilgang var den mest omtalte formen for angrep og missbruk

2004 (året 2003):

- Nedgang i uautorisert bruk av datasystemer, som følge av nedgang i finansielle tap grunnet sikkerhetsbrist.
- Virus og DNS angrep utgjør nå det største finansielle tapet. Tyveri av konfidensiell informasjon ligger nå på en annen plass.
- Nedgang i antall rapporteringer i forbindelse med data inntrening. Grunnen til dette er frykten for negativ omtale.
- Over 80% utfører sikkerhetslogging.
- Stor andel av organisasjonene ser på opplæring og bevisstgjøring av sikkerhet som viktig, men de mener at det ikke blir brukt nok penger på området.

2005 (året 2004):

- Angrep fra virus er fortsatt årsaken til de største finansielle tapene. Uautorisert tilgang har hatt en betydelig økning i finansielle tap, og er derfor mer kostbart enn DNS angrep.
- Uautorisert bruk av datamaskiner har økt noe, til tross for at de finansielle tapene er redusert.
- Webside angrep har økt betydelig.
- Fortsatt nedgang i antall rapporteringer i forbindelse med data inntrening. Grunnen til dette er frykten for negativ omtale.
- Over 87% utfører sikkerhetslogging.

- Fortsatt stor andel av organisasjonene ser på opplæring og bevisstgjøring av sikkerhet som viktig, men de mener at det ikke blir brukt nok penger på området.

2006 (året 2005):

- Angrep fra virus er fortsatt årsaken til de største finansielle tapene. Uautorisert tilgang ligger er nest størst når det gjelder finansielle tap. Tap grunnet bærbare maskiner og tyveri av konfidensiell informasjon tar tredje og fjerde plassen. Disse fire kategoriene utgjør til sammen over 74% av det totale finansielle tapet.
- Uautorisert bruk av datamaskiner har hatt en liten nedgang dette året.
- Det totale finansielle tapet i forbindelse med sikkerhetsgjennomtrening har blitt vesentlig redusert dette året. En årsak til dette kan henge sammen med at veldig få ville oppgi sitt finansielle tap.
- En liten økning i antall rapporteringer i forbindelse med data inntrening. Fortsatt er frykten for negativ omtale hovedårsaken til de lave tallene.
- Over 80% utfører sikkerhetslogging.
- Fortsatt stor andel av organisasjonene ser på opplæring og bevisstgjøring av sikkerhet som viktig, men de mener at det ikke blir brukt nok penger på området.

Tabell 1 viser en oversikt over andelen av sikkerhetsbrudd som er utført fra innsiden og utsiden. Vi kan se av denne tabellen at angrep fra innsiden har hatt en jevn utvikling de siste årene. Det trenger ikke bare bety at angrepene fra innsiden øker, men at bedriftene blir flinkere til å avsløre slike angrep enn tidligere.

Sikkerhetsbrudd de siste 8 årene					
Antall hendelser i % pr svarende	1-5	6-10	>10	Vet ikke	Antall svarende
2006	48	15	9	28	341
2005	43	19	9	28	453
2004	47	20	12	22	280
2003	38	20	16	26	356
2002	42	20	15	23	321
2001	33	24	11	31	348
2000	33	23	13	31	392
1999	34	22	14	29	327
Antall hendelser i % er utført av en på utsiden?	1-5	6-10	>10	Vet ikke	Antall svarende
2005	47	10	8	35	453
2004	52	9	9	30	280
2003	46	10	13	31	356
2002	49	14	9	27	321
2001	41	14	7	39	348
2000	39	11	8	42	392
1999	43	8	9	39	327

Antall hendelser i % er utført av en på innsiden?	1-5	6-10	>10	Vet ikke	Antall svarende
2005	46	7	3	44	453
2004	52	6	8	34	280
2003	45	11	12	33	356
2002	42	13	9	35	321
2001	40	12	7	41	348
2000	38	16	9	37	392
1999	37	16	12	35	327

Tabell 1: Sikkerhetsbrudd de siste 8 årene.

2.5 Andre undersøkelser av e-kriminalitet

Siden 2004 har CERT og U.S. Secret Service gjort omfattende spørreundersøkelser om e-kriminalitet, som også omfatter innsidetrusselen. Hvert år gir de ut et sammendrag av undersøkelsen som gir et bilde om problemet er synkende eller økende.

Rapporten fra 2004 viser at e-kriminalitet i 2003 var et økende problem i forhold til året før. Av de som svarte på undersøkelsen, så opplevde hele 43% en økning i e-kriminalitet. Hele 70% kunne rapportere at de har hatt et eller flere tilfeller av e-kriminalitet. Undersøkelsen viser at hele 71% ble utsatt for et angrep på utsiden, mens 29% rapporterte om angrep fra innsiden. Nesten 30% vet ikke om angrep skjedde fra utsiden eller innsiden i organisasjonen [7].

Sammenlignet med undersøkelsen fra 2005 så er det en nedgang i ukjente angrep, fra 30% til 19%. Innsideangrep gikk ned fra 29% til 20%, mens angrep utenfra økte fra 71% til 80% [4].

Den siste undersøkelsen som er kommet fra CERT og U.S. Secret Service er fra 2006. Tallene her viser at innsidetrusselen er på vei oppover igjen i forhold til undersøkelsen i 2005. Hele 27% hadde et angrep utført fra innsiden, mens ”bare” 58% opplevde angrep utenfra. Hele 55% av de som hadde en sikkerhetshendelse, kunne rapportere at de hadde minst en innside hendelse [18].

2.6 Annen litteratur

Annen litteratur som er å finne i forbindelse med informasjonssikkerhet, er om det å skape holdninger og bevissthet blant de ansatte i bedrifter. Det er en vanlig oppfatning at menneskene og deres oppførsel faktisk betyr mer for informasjonssikkerheten enn alle mulige tekniske løsninger. Dette er velkjent også blant alle store norske bedrifter og organisasjoner. Derfor jobber de også veldig aktivt for å heve bevisstheten og forbedre oppførselen og holdningene blant sine ansatte. Mange gjør dette ved å arrangere spesielle sikkerhetskampanjer. Men vet de noe om effekten av dette arbeidet?

Fører kampanjene virkelig til bedre holdninger og bedret oppførsel når det gjelder informasjonssikkerhet?

Kan effekten av informasjonssikkerhetskampanjer, eller annet holdningsskapende

arbeid, måles?

Er det noen som måler effekten av det arbeidet de gjør eller håper og tror de bare at innsatsen deres har en positiv effekt på de ansattes oppførsel?

Det ble gjort en undersøkelse blant mange norske bedrifter for å finne svarene på disse spørsmålene. Sikkerhetsledere og andre personer som jobber med bevissthet og holdninger til informasjonssikkerhet har blitt intervjuet for å frembringe nødvendig informasjon. De har blitt stilt spørsmål om hvordan de jobber med å heve bevisstheten og forbedre holdningene blant sine ansatte samt hvordan de eventuelt måler nivået på bevisstheten [2] [12].

Mange sikkerhetseksperter mener at innsidetrusselen er den største trusselen mot diverse selskaper. Selv om antall angrep fra innsiden er lavere enn angrep fra utsiden, så er det en høyere andel vellykkede angrep. Samtidig så er skadeomfanget mye mer alvorlig og kostbart [24].

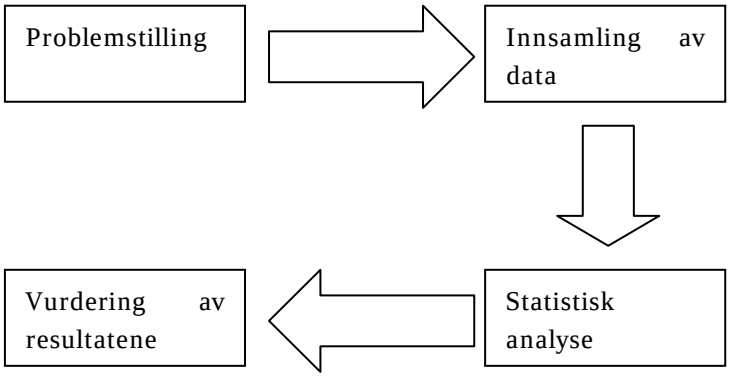
Denne type trusselen er også den vanskeligste å forholde seg til. Grunnen til dette er at en innsider har informasjon og muligheter som en fra utsiden ikke har [23].

3 Valg av metode

I arbeidet med denne oppgaven inngår plan for forskningsarbeidet, metoder for innsamling av data, statistisk analyse av dataene og vurdering av resultatene. Valget av forskningsmetode baseres på arbeidet som ble nedlagt i denne oppgavens forprosjekt. I valget av metode, var kvantitativ metode den som ble valgt. Dette med bakgrunn i at vi ønsker å besvare forskningsspørsmål for å danne oss et bilde av innsideproblematikken i Norge.

3.1 Forskningsstrategi

Planen for forskningsstrategien, kan illustreres av figuren nedenfor:



Figur 1: Plan for forskningsarbeid

Planen tar utgangspunkt i en gitt problemstilling. Med bakgrunn i denne er det gjennomført en innsamling av data. Innsamlingen foregikk både i form av et litteratursøk og en spørreundersøkelse. For å kunne besvare forskningsspørsmålene var en statistisk analyse av dataene fra spørreundersøkelsen nødvendig. Funn i den statistiske undersøkelsen, var sammen med relevant litteratur fra litteraturstudiet med på å besvare forskningsspørsmålene og vil kunne gi ny kunnskap i forhold til gitt problemstilling.

3.2 Litteratur

En viktig tilnærming til forskningstemaet er vurderingen av relevant litteratur. Litteraturen har spilt veldig viktig rolle for utformingen av spørreundersøkelsen. Letingen etter relevant informasjon ble gjort ved å bruke anerkjente databaser som blant annet CiteSeer og Springer Link. I tillegg ble ulike søkemotorer på Internett benyttet.

Undersøkelsen fra CERT har i denne oppgaven blitt brukt som mal for å få en

spørreundersøkelse så lik, og sammenlignbar som mulig. Fordelene med å bruke CERT sin undersøkelse enn de andre er at den har gjennom to detaljerte undersøkelser belyst problemene fra et mer adferd og teknisk perspektiv, som nevnt i tidligere kapittel.

Undersøkelsen i denne oppgaven er inspirert av undersøkelsene som har blitt utført av CERT og til dels CSI/FBI i USA. Fordelen med dette er at de har gjort samme undersøkelse gjennom mange år, og har derfor stor troverdighet blant myndigheter og bedrifter.

Litteraturstudiet viser også at det finnes en del undersøkelser om innside problematikken, men dessverre er flertallet av dem fra Amerika. Hadde det vært noen liknende undersøkelser fra Skandinavia eller Europa, så hadde det vært enklere å kunne sett resultatene i sammenheng med eventuelle naboland.

3.3 Spørreundersøkelsen

Spørreundersøkelsen er sammen med relevant litteratur den viktigste delen av datainnsamlingen. Systematisk og strukturert datainnsamling med kvantitative metoder muliggjør sammenligninger og statistiske beregninger, som kan gi et tverrsnitt av dagens situasjon blant virksomheter med fokus på informasjonssikkerhet. Resultater fra spørreundersøkelsen skal gi svar på hypoteser og forskningsspørsmål, og bidra til god praksis for måling av nivå for informasjonssikkerhet.

Spørreundersøkelsen vil sammen med en god litteraturstudie være den viktigste delen av en datainnsamling.

3.3.1 Utvalget

For å gjøre en så god undersøkelse som mulig, så bør vi velge ut et par sektorer som vi ønsker å undersøke. Ser vi på undersøkelsen fra CERT og U.S. Secret Service i 2006 er svarprosenten høyest fra sektorer som staten, informasjonsteknologi og telekommunikasjon, bankvesenet [18].

Her utgjør de til sammen over 50% av totalt 14 forskjellige infrastrukturer som valgte å svare på denne undersøkelsen. I en annen undersøkelse utført av CSI/FBI i 2006, så er tendensen nesten den samme. Her ser vi at staten, bankvesenet og informasjonsteknologi og telekommunikasjon til sammen utgjør litt over 45% [22].

Dataene fra disse undersøkelsene gir oss en god indikasjon på hvilke sektorer som er mest relevante å ta utgangspunkt i. Basert på omfanget av undersøkelsen vi skal utføre, så bør vi begrense oss til to sektorer.

I en mer omfattende studie som CERT og U.S. Secret Service utførte i 2005, viser at hele 63% av hendelsene fra 1996-2002 berørte informasjon og telekommunikasjon. Denne type sektor er veldig sårbar ovenfor innsidetrusler og vil være et veldig godt utgangspunkt for videre undersøkelser.

Motivene til innsiderne har også blitt undersøkt av CERT og U.S. Secret Service. De mest ”vanlige” motivene for disse hendelsene viste seg å være sabotasje og finansiell

gevinst. Sabotasje ble stort sett utført for å ta hevn, samtidig skade bedriftens renommé. Mens de som ble motivert av de finansielle gevinstene hadde ikke til hensikt å skade bedriftens renommé. Likevel førte resultatet av en sik hendelse til at bedriftens renommé ble betydelig svekket [11][13].

Slik tendensen er i USA, så kan vi ikke annet enn å anta at den også kan være slik i Norge. Ettersom det ikke er gjort en slik type undersøkelse i Norge, så vil vi undersøke disse to sektorene for å kunne sammenlikne dem med de undersøkelsene som er utført i USA. I denne oppgaven velger vi sektorene informasjon og telekommunikasjon og bank og finanssektoren.

Nå som vi har kommet frem til hvilke sektorer som er mest hensiktsmessig å undersøke i denne oppgaven, så kan vi se på hvilke bedrifter vi vil ha med i undersøkelsen. Hvilke bedrifter som er aktuelle er ikke lett å avgjøre, men de bør bli valgt ut i fra ulike faktorer. En faktor er sammenlikningsgrunnlag. Det er viktig at vi velger bedrifter fra samme type sektor, så de kan bli sammenlignet i oppgaven. En annen faktor er også størrelsen på de forskjellige bedriftene. I oppgaven vil vi prøve å få gjort undersøkelsen med bedrifter av ulike størrelser. Dette for å få en mer bredde i undersøkelsen. Ved å få for mange av en liten eller stor bedrift, så kan vi risikere å få et bilde av problemet som ikke er nær virkeligheten.

De ulike bedriftene i de forskjellige sektorene fant vi ved å bruke en tjeneste fra Proff (www.proff.no).

Proff er en tjeneste hvor man kan sjekke en bedrift mer grundig i forhold til soliditet, lønnsomhet og størrelse. Et verktøy som kom til stor nytte når vi skulle bedømme hvilke bedrifter vi ville undersøke.

3.3.2 Spørreskjemaet

I denne oppgaven har vi vurdert å dele opp spørreundersøkelsen i fire kategorier:

1. Om virksomheten
2. Om informasjonssystemene og sikringstiltak
3. Trusler og angrep mot virksomheten
4. Håndtering av hendelser og oppbevaring av logger

Det er totalt 24 spørsmål som sammen vil gi et bilde av hvordan innsidetrusselen er blant norske bedrifter. Spørsmålene er også lagt opp slik at de kan sammenlignes med noen av de undersøkelsene som er utført i USA.

I den første kategorien ønsker vi å få en liten oversikt over størrelsen på bedriften og hvem som besvarer undersøkelsen. For at vi lettere skal kunne sammenligne resultater, så er det en fordel å se andelen av små og store bedrifter. Dette kan også gi oss et innblikk i hvilke bedrifter som har mest problemer angående angrep fra innsiden eller utsiden, avhengig av størrelse.

Videre i den andre kategorien spør vi etter informasjon om datasystemene og sikringstiltak i bedriften. Her ønsker vi å få en oversikt over hvor mye penger

bedriftene bruker på sikkerhet i året, og hva slags sikkerhetsmekanismer de bruker for å beskytte seg mot ulike angrep.

Den tredje kategorien er den mest omfattende delen som er rettet mot trusler og angrep mot bedriftene. Spørsmålene her er laget for å kunne få et best mulig bilde av innsidetrusselen i Norge. De vil også bli brukt til sammenligning med det CERT og Secret Service U.S. har funnet ut i sine undersøkelser. Vi undersøker blant annet hvilke trusler som har vært de største mot bedriften de siste 10 årene; type angrep som har blitt utført; hvor mange angrepsforsøk de har hatt; og eventuelle finansielle tap og tap av renommé.

Grunnen til vi har valgt å samle informasjon for de siste 10 årene er for å øke sannsynligheten til at angrep kan ha skjedd mot de mindre bedriftene. Om vi hadde brukt de siste 5 årene, så er det ikke sikkert at de mindre bedriftene vi sender undersøkelsen til har hatt noen form for angrep.

Til slutt har vi en kategori som kort undersøker håndtering av hendelser og oppbevaring av logger. Her får vi et innblikk i bedriftens rutiner for rapportering av hendelser og hvordan disse blir behandlet videre. Hvor lenge de oppbevarer slike logginger kan være utslagsgivende for hvordan de foregående spørsmålene er besvart. Blir det for eksempel ikke arkivert informasjon om angrep, så kan det være at samme bedrift heller ikke svarer at de har hatt angrep eller hatt lignende tilfeller.

Spørsmålene som er brukt i spørreundersøkelsen er gjengitt som vedlegg til rapporten.

3.3.3 Utsendelsen

For å få en til en så anonym og effektiv utsendelse av spørreskjemaet som mulig, så brukte vi tjenesten QuestBack (QB). Dette er en tjeneste som er spesielt egnet for slike typer undersøkelser. QB sørger for at respondenten er anonym og resultatene blir lagret hos QB. Så ingen skal kunne hente ut noe informasjon om hvilke respondenter som har svart hva. Lisens til QB ble ordnet av Espen Torseth som jobber ved NorSiS.

Spørreskjemaet ble utsendt ved hjelp av e-post, med en link til spørreundersøkelsen. I samme epost ble det sendt ut et skriv om undersøkelsen og hva jeg ville oppnå. I tillegg ble det sendt med en fortrolighetsavtale som skulle sikre anonymiteten til respondentene fra mitt. Om noen ikke ønsket å besvare undersøkelsen på via nettet, så fikk de tilbud om at jeg kunne sende den pr. post. Når noen hadde sendt inn svar fra undersøkelsen, så ble jeg informert via epost fra QB.

Sikkerheten til QB

Når du som informant avgir dine besvarelser (trykker send), så blir dataene lagret i QuestBack sin database. Det vil kun være vi som utfører denne undersøkelsen, som vil ha tilgang til svarene via QuestBack sine tjenester. Svarene fra en respondent vil kun bli registrert med et nummer. Vi vil ikke ha tilgang til denne informasjonen, og vil derfor ikke kunne koble svarene til en e-postadresse eller annen informasjon som kan avsløre bedriftens identitet.

En referanse til respondentens e-postadresse (som utgjør respondentens identitet) vil bli lagret sammen med svarene i databasen. Denne referansen vil være nødvendig for å kunne sende ut invitasjoner og påminnelser. Kun teknisk personell fra QuestBack som vedlikeholder og kjører denne tjenesten kan lage en kobling mellom svarene og e-postadressene. Gjennom deres ansettelse, så er QuestBack sine ansatte forpliktet til å opptre profesjonelt og konfidensielt nivå.

QuestBack sin database lagret på servere som star i en brannsikkeromgivelse med begrenset tilgang. All kommunikasjon med databasen skjer via en kryptert forbindelse. Dette gjelder også for hvordan svarene til respondenten blir avgitt.

3.4 Gjennomgang og tolkning av data

Resultatene fra undersøkelsen skulle etter planen gi oss nok informasjon til å se etter mulige sammenhenger mellom variabler i datasettene. Dessverre var det ikke mange av bedriftene som besvarte denne undersøkelsen. Etter gjentatte forsøk på å få bedriftene til å gjennomføre undersøkelsen, så var tilbakemeldingene stort sett den samme. Enkelte hadde ikke tid til å svare på spørreundersøkelsen. Flere svarte at de ikke ønsket å besvare en undersøkelse som spurte etter sensitive opplysninger.

For å gjøre det beste ut av den lave svarprosenten, så valgte vi å trekke frem de viktigste funnene fra undersøkelsen. Disse funnene vil se i sammenheng med de undersøkelsene som har blitt utført av CERT i 2006. Gjennom å sammenligne disse dataene, så kan vi gjøre noen antagelser på hvordan innsidetrusselen er blant bedriftene i Norge.

3.5 Kvalitet

En generell svakhet ved spørreundersøkelser er faren for at spørsmålene og svaralternativene ikke er de riktige eller ikke relevante, og at dette ikke oppdages. Det er viktig at resultatet av spørreundersøkelsen gir et så korrekt bilde som mulig.

For å unngå at dette skulle skje har det vært god kommunikasjon med veileder gjennom utarbeidelsen av spørreskjemaet. I tillegg ble det sendt ut en fortrolighetsavtale som sikret respondenten at undersøkelsen var 100% anonym. Videre ble det også lovet at dataene fra undersøkelsen skulle behandles konfidensielt, og at bedriftene som besvarte undersøkelsen ville forbli anonyme i avhandlingen.

En spørreundersøkelse er en egenevaluering hvor respondenten i noen grad kan ønske å skjønnmale situasjonen. Det er lagt vekt på å forsikre deltakerne om konfidensiell behandling og anonymisering av data og resultater, slik at det ikke skal ligge til grunn motiver for å svare uærlig. Respondentene sto også fritt til å besvare spørreundersøkelsen. Dessverre viste det seg at mange av respondentene ikke ønsket å svare ettersom undersøkelsen inneholdt en del sensitive opplysninger. De stilte spørsmålstegn ved anonymiteten og bruken av informasjonen i etterkant. Årsaken til dette vil se nærmere på i rapporten.

På bakgrunn av det som er nevnt ovenfor anser vi resultantene i spørreundersøkelsen

som pålitelige. For å sikre påliteligheten var det viktig at vi sendte ut undersøkelsen til de som hadde nok kunnskap til å gjennomføre, uten for mye svar av typen “vet ikke.” I e-posten som ble sendt til de ulike bedriftene, ble det oppfordret at undersøkelsen ble besvart av personer innenfor IT-avdelingen i bedriftene.

4 Datagrunnlag

4.1 Besvarelsen av spørreundersøkelsen

Spørreundersøkelsen ble sendt til 50 forskjellige bedrifter av ulik størrelse. Disse bedriftene var fordelt mellom 2 sektorer. Den ene var bank- og finanssektoren, mens den andre var informasjons- og telekommunikasjonssektoren.

Blant disse respondentene, så valgte bare 7 stykker å besvare undersøkelsen. Etter gjentatte purringer på mail, så klarte vi ikke å få flere til å besvare undersøkelsen. Mange unnskyldte seg med at de ikke hadde tid, eller at de rett og slett ikke ønsket å besvare i frykt for missbruk av opplysningene.

I e-posten som ble sendt til samtlige bedrifter, så fulgte det med et skriv som beskrev sikkerheten med undersøkelsen og at vi garanterte 100% anonymitet. Likevel valgte over 25% av respondentene å ikke svare. De resterende som ikke svarte har vi ikke hørt noe fra.

Så de viktigste funnene fra denne undersøkelsen vil kun bli presentert i kapittel 6. Deretter vil vi si litt om funnene og se dem i sammenheng med dataene fra CERT. Gjennom denne sammenligningen kan vi gjøre noen antagelser på hvordan innsidetrusselen er i Norge, kontra USA.

4.2 Påliteligheten til resultatene

På bakgrunn av den lave svarprosenten, så må vi behandle tallene fra undersøkelsen meget kritisk. Ved å sammenligne ulike spørsmål fra undersøkelsen, så viser det seg at de noen av svarene ikke er spesielt roverdige. I tabell 2 under, så kan vi se et utdrag av to forskjellige spørsmål fra undersøkelsen. Den viser hvilke angrep som bedriften har blitt utsatt for de siste 10 årene, og hvor angrepet kom fra. Spørsmålet om angrepstypen passordsniffing, så svarer ingen at de har hatt denne typen angrep, mens 14,3% av deltagerne har hatt et slikt angrep. Slike funn svekker påliteligheten til undersøkelsen.

Hvilke av følgende angrepsforsøk har blitt begått mot deres bedrift de siste 10 årene? (flere svar er mulig)		Hvilke av disse angrepstypene har blitt begått mot deres bedrift fra utiden og/eller innsiden? (flere svar er mulig)		
Type angrep	Svarprosent	Utenfra	Innsiden	Vet ikke
Bedrageri (misbruk av kredittkort el.)	42,9 %	42,9 %	0,0 %	57,1 %
"Zombie-maskiner" på bedriftens nettverk	0,0 %	0,0 %	0,0 %	100,0 %
Passord sniffing	0,0 %	0,0 %	14,3 %	85,7 %
Utpressing	0,0 %	0,0 %	0,0 %	100,0 %

Tabell 2: Avvik i spørreundersøkelsen

Det kan være flere årsaker til dette avviket. I en spørreundersøkelse må man regne med at folk svarer feil, eller misforstår spørsmålene. Dette ville ha jevnet seg ut om vi hadde hatt flere svar. Slike feil ville derfor ikke ha hatt så stor betydning på resultatene.

5 Diskusjon av resultater

5.1 Innledning

Resultatene fra spørreundersøkelsen ble behandlet statistisk for å kunne besvare noen av forskningsspørsmålene. Det vi ønsker å finne svar på er følgende:

1. Hvor utbredt er ”insider threat” i Norge?
2. Vil spørreundersøkelsen kunne hjelpe oss i arbeidet med å redusere slike trusler i Norge?
3. Hvordan er innsidetrusselen i Norge sammenlignet med tilsvarende undersøkelser fra CERT?

Vi ønsket med denne undersøkelsen å kunne finne ut hvor utbredt innsidetrusselen er i Norge. Til det har vi fått for få svar til at vi kan trekke noen endelig konklusjon om temaet, men vi kan gjøre noen antagelser basert på svarene fra noen av spørsmålene.

De mest interessante funnene fra undersøkelsen vil bli presentert i dette kapittelet, samtidig som de vil bli sammenlignet med undersøkelsen ”2006 E-Crime Watch Survey - Complete Survey Results” fra CERT [18]. Vi velger å bruke data fra denne undersøkelsen, ettersom den er mest oppdatert i forhold til situasjonen i USA for øyeblikket.

Funnene fra spørreundersøkelsen håper vi til en viss grad kan gi oss et enkelt bilde av hvordan innsidetrusselen i Norge er.

5.2 Om virksomhetene

Spørreundersøkelsen ble sendt til bedrifter av ulik størrelse, med anbefaling at den ble besvart av ansatte innenfor IT. Årsaken til dette var at vi ønsket så pålitelige svar som mulig. Tabellen 3 viser andelen av størrelsene på de bedriftene som besvarte undersøkelsen.

Antall ansatte	Fordeling i prosent
1-5	28,6 %
5-20	0,0 %
20-50	14,3 %
50-100	14,3 %
100-250	14,3 %
250-500	14,3 %
500-1000	0,0 %
Over 1000	14,3 %

Tabell 3: Størrelsen på virksomhetene

I denne undersøkelsen har vi fått svar fra små og store bedrifter. Fordelen med dette er at vi vil få et noe mer korrekt bilde av innsidetrusselen i Norge. En overrepresentasjon av små eller store bedrifter kunne ha gitt oss et ”falskt” bilde av trusselen i Norge. Vi mener med dette at store bedrifter har større sannsynlighet for angrep enn de som er betydelig mindre. Grunnen til dette kan være ulike årsaker, men ved å angripe en større bedrift vil kunne gi en større økonomisk fortjeneste ved et angrep. I tillegg kan større bedrifter ha bedre utstyr for å kunne avsløre angrep fra innsiden enn det de mindre har.

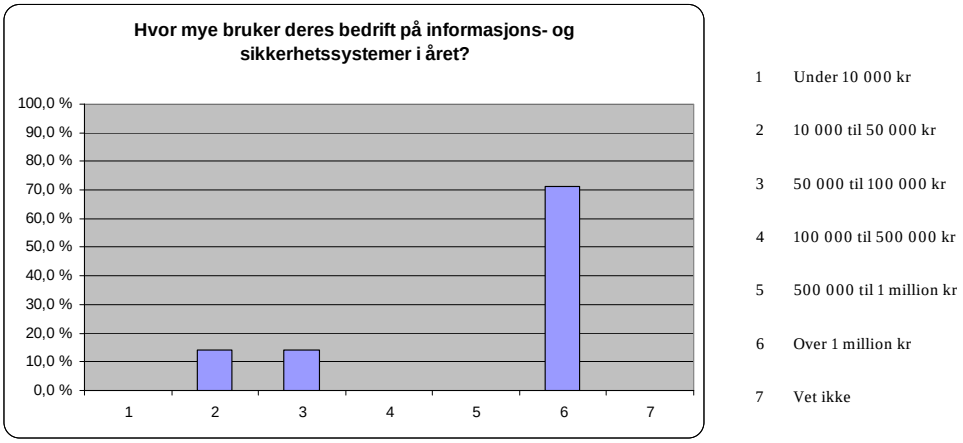
Når det gjelder påliteligheten til svarene som har kommet inn, så antar vi at respondentene vet hva de har svart på. Et av spørsmålene spurte om stillingen til respondenten, og hele 85,8 % hadde stilling som IT-sjef/ansvarlig eller Sikkerhetssjef/-ansvarlig. Bare 14,3 % av respondentene var daglig leder.

5.3 Om informasjonssystemene og sikringstiltak

For å kunne danne oss et bilde av hvordan sikkerheten er blant norske bedrifter, ønsket vi å vite hvor mye som blir brukt til sikringstiltak. I tillegg ville vi vite hva slags utstyr bedriftene bruker for å beskytte seg mot angrep.

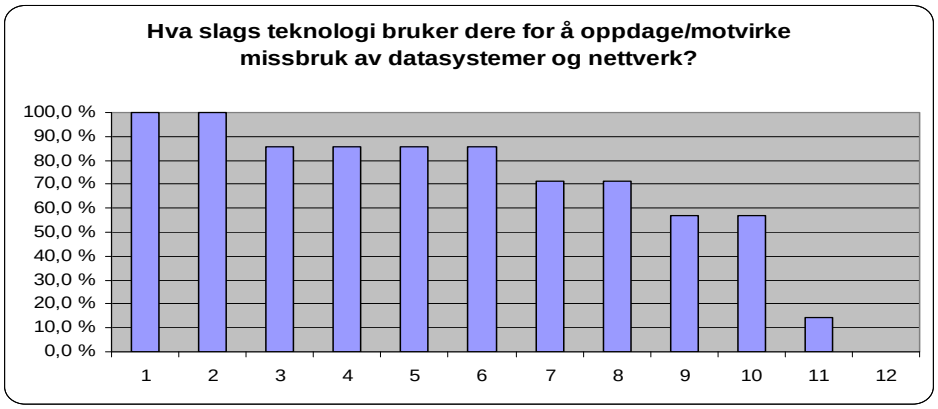
Figur 2 viser at sikkerheten står i fokus blant de bedriftene som svarte på undersøkelsen. Over 70 % svarte at de bruker så mye som over 1 million kroner på sikkerhet. Dette kan virke noe overraskende ettersom vi også har mindre bedrifter med i undersøkelsen. Undersøkelsen som CERT har utført viser at 1 av 4 bruker under $ 100 000 (ca 600 000 kroner) på sikkerhet. En forklaring på dette kan være at utstyr/programvare kan være billigere i USA enn i Norge. Så sammenlignet med USA, så er Norge flinkere til å investere i sikkerhetsutstyr. Dette kan også indikere at vi tar

sikkerhet på alvor.



Figur 2: Hvor mye brukes på sikkerhetssystemer i året.

Hva slags utstyr bruker bedriftene for å beskytte seg mot angrep? Ved å studere figur 3 kan vi tolke at alle bedriftene er meget opptatte av å beskytte seg mot angrep fra utsiden. Slike løsninger kan være en stor utgift for bedriftene, noe som gjenspeiles i figur 2.



1	Brannmurer	7	Innbruddsdeteksjonssystemer (IDS)
2	Antivirus	8	System for å forhindre innbrudd (IPS)
3	Antispionvare	9	Fysiske/biometriske autentifiseringsmekanismer
4	Rutiner for manuell/automatisk feilretting	10	Kryptert trådløst nett
5	Kryptering av sensitiv informasjon	11	Logge/overvåke tastetrykk av individuelle brukerkontoer
6	Rollebasert tilgangskontroll	12	Vet ikke

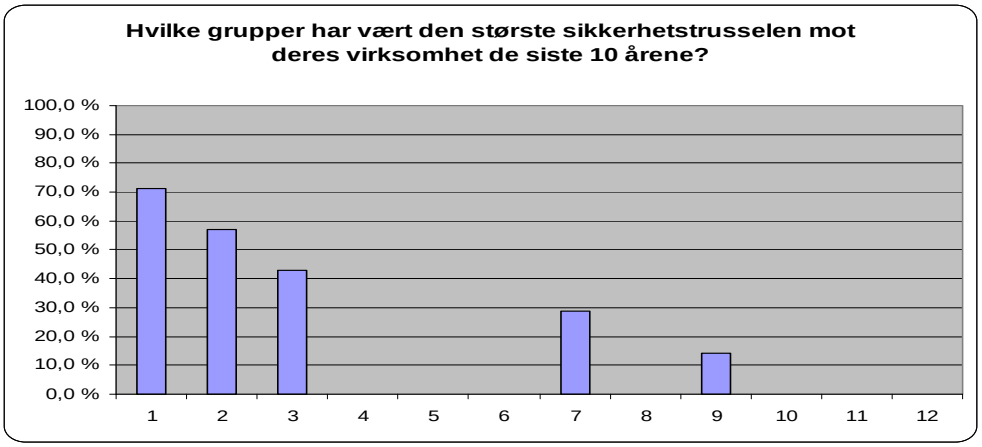
Figur 3: Sikkerhetsteknologi

Sammenligner vi funnene med de fra CERT, så ser vi valg av sikkerhetsutstyr er meget likt i USA og Norge. Fokuset er antivirus og brannmur, som gir en betryggende beskyttelse mot farer fra utsiden. Vi ser også at en stor andel er flinke til å kryptere sensitiv informasjon. Dette øker sikkerheten mot uautorisert innsyn i sensitiv informasjon.

Selv om bedriftene er flinke til å kryptere sensitiv informasjon, vil dette fungere mot innsyn når trusselen kommer fra innsiden? Brukere som er på innsiden vil antagelig kunne klare å lese slik informasjon, ettersom de allerede er ”sikkerhetsklarert.”

5.4 Trusler og angrep mot virksomheten

Bedriftene er bevisste på dette med sikkerhet, og viser at de bruker mye penger på utstyr. Men hvilke trusler er størst mot bedrifter i Norge? Av figur 4 kan vi se at det ikke overraskende nok er hackere som utgjør størst sikkerhetstrussel mot bedriftene. Noe som i midlertidig er meget interessant er at medarbeidere og tidligere medarbeidere utgjør en meget stor sikkerhetstrussel. De samme tilfellen finner vi i undersøkelsen fra CERT.

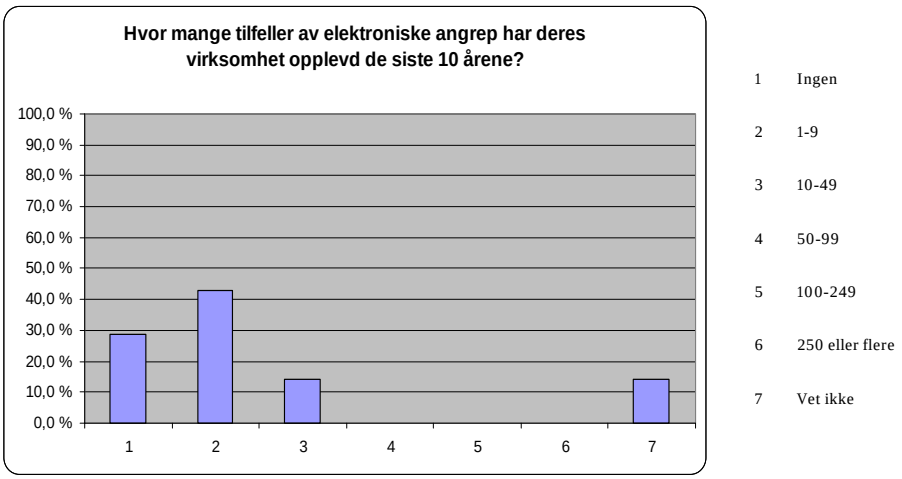


1	Hackere	7	Kunder
2	Medarbeidere	8	Leverandør / forretningspartnere
3	Tidligere medarbeidere	9	Konkurrenter
4	Informasjonsmeklere	10	Tidligere tjenesteleverandører / konsulenter / leverandør
5	Tjenesteleverandører / konsulenter / leverandør	11	Vet ikke
6	Terrorister	12	Annet, spesifiser her

Figur 4: Sikkerhetstrussel mot bedriftene

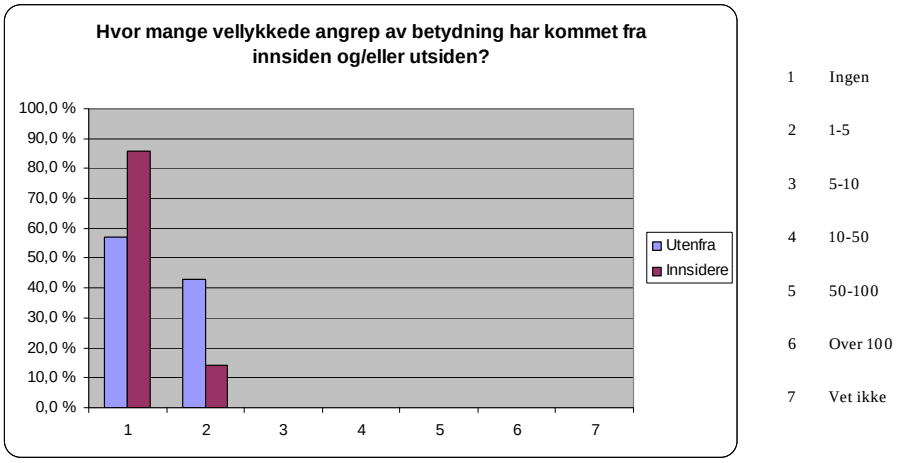
Bedriftene er bevisste på at medarbeidere utgjør en stor trussel mot bedriften. Noe av grunnen til dette er at medarbeidere har enkel tilgang til datasystemer, brukerkonti og passord.

Som vi kan se fra disse figurene 5 og 6, så er angrep fra innsiden ikke spesielt utbredt blant respondentene.



Figur 5: Angrep mot bedriftene

Av figur 5 kan vi se at bedriftene har vært utsatt for angrep, men bare et fåtall av disse angrepene har vært vellykkede, som vist i figur 6. En teori kan være at bedriftene har mer utstyr for å kunne beskytte seg mot, og oppdage angrep fra utsiden. Angrep fra innsiden kan være vanskeligere å oppdage og vil kanskje ikke gjenspeile virkeligheten i denne undersøkelsen.



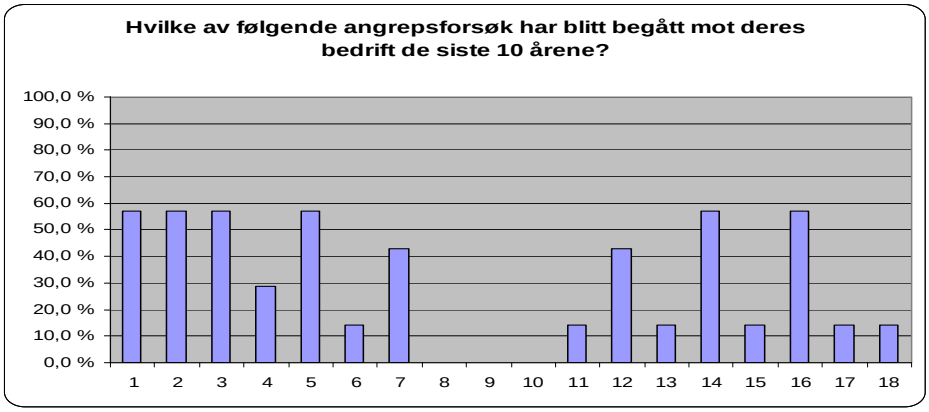
Figur 6: Vellykkede angrep

Undersøkelsen fra CERT viser at hele 43% av respondentene har vært utsatt for 1-9 angrep de siste 12 månedene. Hele 20% har vært utsatt for 10-49 angrep. Ut i fra dette

kan vi ikke annet enn å anta at antall angrep de siste 10 årene burde vært noe høyere enn det vi kan se av figur 5.

Videre kan vi se at angrep fra utsiden er høyere representert når det gjelder angrep. Samme tendens kan vi se fra USA. Her viser det seg at over 80% av angrepene er antatt å komme fra utsiden.

Figur 7 viser de vanligste angrepene som bedriftene stort sett er utsatt for. Her er det ingen store overraskelser at de fleste har vært utsatt for hacking, spionvare, ”phishing” og virus. Litt overraskende er det at så mange bedrifter har vært utsatt for tyveri av IT-utstyr. Tyveri av slike gjenstander kan være stor sikkerhetsrisiko dersom innholdet ikke er kryptert eller sikret. På nettsiden www.datainform.no kommer det frem at halvparten av bedriftene ikke har noen form for sikring på sitt bærbare IT-utstyr. Denne sårbarheten kan i verst tenkelig scenario eksponere sensitive opplysninger som absolutt ikke skal komme på avveie. Personopplysninger, forretningshemmeligheter, personalsaker, kundekontrakter eller strategidokumenter er eksempler på informasjon som ikke bør komme på avveie [43].



1	"Phishing"	10	Utpressing
2	Spionvare	11	Sabotasje på systemer, drift, informasjon, data
3	Ulovlig generering av søppelpost	12	Uautorisert tilgang til informasjon, systemer eller nettverk
4	Denial of Service (DoS) angrep	13	Tyveri av opphavsrettslig beskyttet materiale
5	Virus eller annen ondsinnet kode	14	Tyveri av IT-utstyr
6	Identitetstyveri	15	Uautorisert innsyn av privat eller sensitive informasjon
7	Bedrageri	16	Hacking
8	"Zombie-maskiner" på bedriftens nettverk	17	Vet ikke
9	Passord sniffing	18	Annet, spesifiser her

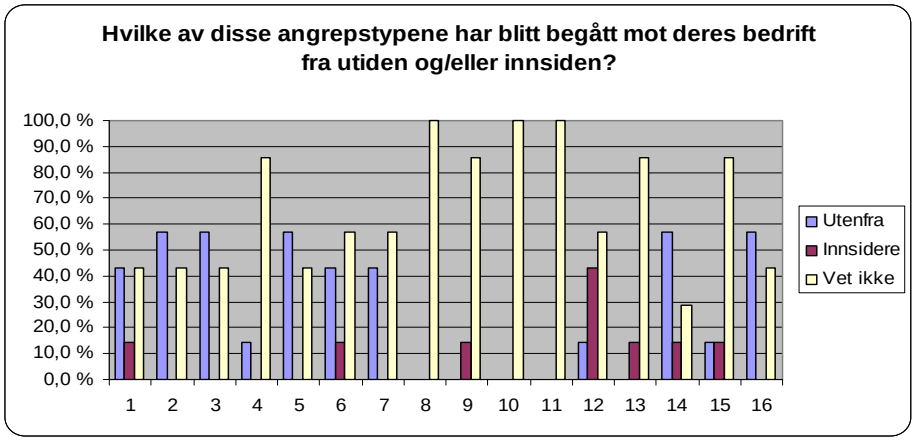
Figur 7: Angrepsforsøk mot bedriftene

Uautorisert innsyn av privat eller sensitive informasjon er også verdt å merke seg. Slik innsyn er vanskelig å beskytte seg mot ettersom mange kan ha tilgang til denne informasjonen og missbruke den.

Tolker vi tallene fra USA, så ser vi også her at hendelser av typen uautorisert tilgang til informasjon, systemer eller nettverk er meget utbredt. Hele 60% har svart at de er utsatt for slike hendelser.

Bedrageri er også en faktor som blir mer å mer utbredt. Den årlige undersøkelsen fra CSI/FBI i 2007 viser at "fraud" (bedrageri) er den største kilden til finansielle tap [37]. Vi har ikke undersøkt om hvor mye denne type trussel koster bedriftene, men vi kan ut i fra dette, tolke at denne trusselen vil øke i fremtiden. Vi ser også fra figur 7 at flere bedrifter er utsatt for bedrageri.

Når det gjelder andel av angrep som har blitt begått mot bedriftene, så viser figur 8 at det er personer fra utsiden som utgjør størst trussel. Det samme viser tallene fra undersøkelsen til CERT.

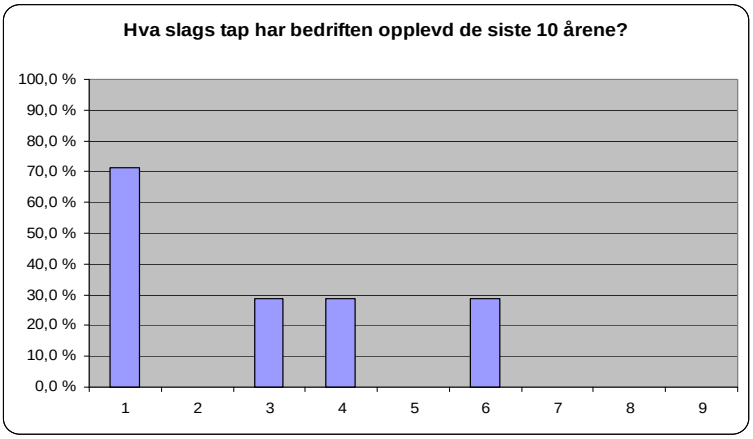


1	"Phishing"	9	Passord sniffing
2	Spionvare	10	Utpressing
3	Ulovlig generering av søppelpost	11	Sabotasje på systemer, drift, informasjon, data
4	Denial of Service (DoS) angrep	12	Uautorisert tilgang til informasjon, systemer eller nettverk
5	Virus eller annen ondsinnet kode	13	Tyveri av opphavsrettslig beskyttet materiale
6	Identitetstyveri	14	Tyveri av IT-utstyr
7	Bedrageri	15	Uautorisert innsyn av privat eller sensitive informasjon
8	"Zombie-maskiner" på bedriftens nettverk	16	Hacking

Figur 8: Hvem utførte de ulike angrepstypene mot bedriftene

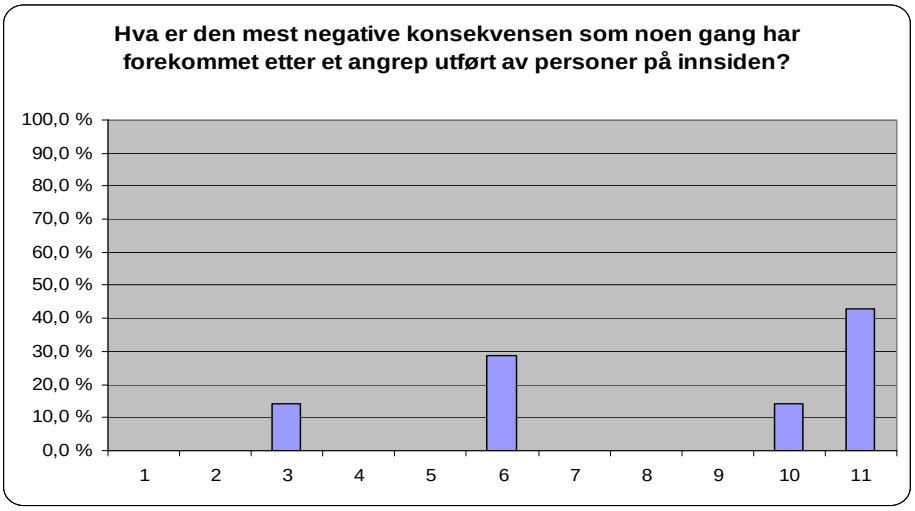
Vi kan fra figur 8 se at det er uautorisert tilgang til informasjon, system eller nettverk som utgjør den største trusselen til bedriftene.

De bedriftene som har besvart denne undersøkelsen har på ingen måte vært ekstremt utsatt for angrep fra innsiden eller utsiden. Likevel kan vi se at enkelte har opplevd tap av omdømme, grunnet angrep. Denne type tap kan koste bedrifter dyrt i det lengre løp, samtidig som den tapte tillitten tar mange år å få opparbeidet igjen. Av figur 10 kan vi se at resultatet av et angrep fra innsiden resulterte i tap av omdømme, og kunder.



1	Ubetydelige driftstap	6	Tap av omdømme
2	Kritiske driftstap	7	Ikke opplevd tap
3	Finansielle tap	8	Vet ikke
4	Ubetydelige finansielle tap	9	Annet, spesifiser her
5	Kritiske finansielle tap		

Figur 9: Tap bedriftene har hatt



1	Kritisk systemsammenbrudd i bedriften	7	Mistet bedriftssamarbeid
2	Kritisk systemsammenbrudd som påvirket kunder og bedriftspartnere	8	Tap av menneskeliv
3	Tap av bedriftens omdømme	9	Personskader
4	Tap av nåværende og/eller fremtidig inntekter	10	Ingen innvirkning
5	Kritisk systemsammenbrudd som påvirket større kritiske infrastruktursektorer	11	Vet ikke
6	Tap av kunder		

Figur 10: Konsekvens etter angrep fra innsiden

Ser vi på undersøkelsen fra CERT, så viser det seg at de har opplevd betydelige driftstap og finansielle tap etter et angrep. Angrep fra innsiden har resultert i kritisk systemsammenbrudd. Noen rapporterte også tap av omdømme.

6 Oppsummering og konklusjon

Oppgavens intensjon var å kartlegge innsidetrusselen i Norge, samtidig som vi vil bevisstgjøre bedrifter om dette problemet. Ved å utføre en grundig litteraturstudie, så har vi fått et dypere innblikk i trusselen fra innsidere. Denne kunnskapen ville vi bruke for å danne et inntrykk av samme problemstilling i Norge. Dessverre lyktes vi ikke med dette. Ettersom flere bedrifter ikke ønsket å delta i undersøkelsen, så har vi ikke nok grunnlag til å kunne gi et godt bilde av denne type trussel i Norge.

Gjennom en spørreundersøkelse har vi skaffet informasjon om innsidetrusselen blant 7 norske bedrifter fra to ulike sektorer. Årsaken til denne lave deltagelsen er mange, men bedriftene er meget tilbakeholden med opplysninger som er så sensitive.

Rapporten tar for seg de viktigste funnene i undersøkelsen, hvor vi analyserer og sammenligner dataene med spørreundersøkelsen utført av CERT i 2006. Fra de dataene vi har analysert er det ikke noen svar som skiller seg veldig ut. Bedriftene gir et inntrykk av at angrep fra utsiden og innsiden er meget beskjedne. Av de angrepsforsøkene som bedriftene har vært utsatt for, så viser det seg at nesten ingen av dem er vellykkede.

De fleste angrepsforsøkene viser seg å komme fra utsiden. Det samme kan vi se fra undersøkelsen til CERT. Selv i de angrepene som har vært vellykkede har ikke bedriftene hatt noen kritiske tap i form av driftsstans eller store økonomiske tap. Noen bedrifter har opplevd tap av kunder på bakgrunn av hendelser på innsiden, men det kommer ikke frem i undersøkelsen hvor mye dette kostet bedriften økonomisk.

6.1 Konklusjon

På bakgrunn av gjennomført analyse av dataene fra spørreundersøkelsen, kan vi ikke komme med noen endelig konklusjon på trusselbildet i Norge. Til det har vi fått alt for få svar. Av de svarene vi har fått og analysert, kan vi gjøre noen antagelser på hvordan denne trusselen er, og om bedriftene er bevisste på slike angrep.

Dataene fra undersøkelsen viser at angrep fra innsiden i Norge er meget lav. Vi tok utgangspunktet i angrep de siste 10 årene, likevel var det få angrep å merke seg. En av grunnene til dette kan være at slike angrep ikke har blitt oppdaget. Mange selskaper er mer opptatt av å beskytte seg mot angrepene som skjer på utsiden og dermed blir fokuset på det som skjer innenfor sikkerhetsperimeteren redusert. Selv om undersøkelsen viser at tilfellene av innsideangrep er lavere her enn i USA, så trenger ikke det bety at det ikke forekommer. Noe som i midlertidig viser seg å være veldig interessant, er andelen av uautorisert tilgang til informasjon, systemer eller netteverk. Her svarer over 40% at det har blitt forsøkt og begå en slik ulovlig handling. Slike hendelser er noe vi kan anta at skjer oftere enn det bedriftene også er klar over. Denne typen uønskede hendelser er vanskelig å beskytte seg mot.

Tallene fra undersøkelsen gir ingen klare indikasjoner på om mange bedriftene i Norge

er utsatt for angrep fra innsiden, men selv med så få svar har vi en liten indikasjon på at det forekommer.

7 Videre arbeid

Denne rapporten hadde som mål å bidra i arbeidet med å danne et bilde av problemene rundt innsidetrusselen i Norge. Etablering av en god praksis er imidlertid et meget ressurs og tidkrevende arbeid som krever praktisk erfaring og læring. Det vil derfor alltid være et generelt behov for å evaluere bruk av måling i virksomheter og forskning på området for å videreutvikle god praksis for måling av informasjonssikkerhetsnivå.

Denne oppgavens spørreundersøkelse har et ganske enkelt, men noe omfattende spørreskjema. Likevel så var svarprosenten meget lav. I et videre arbeid av denne problemstillingen bør man se mer på mulighetene for å kunne få flere svar. Noe vi erfarte med denne oppgaven var bedriftenes skepsis til å besvare en så sensitiv undersøkelse. For å få bedriftene til å besvare en undersøkelse som denne, må det bygges tillitt til den som utfører undersøkelsen. En måte som kan fungere er å lage en noe enklere spørreundersøkelse som tar få minutter å besvare. På denne måten kommer man i lettere kontakt med personen som skal besvare undersøkelsen. Om noen er interessert så kan de få muligheten til å svare på en noe mer komplisert undersøkelse. Denne vil bli mer omfattende i forhold til innsidetrussel problematikken i bedriften, noe som igjen stiller større krav til respondenten.

En annen metode kan være å ta direkte kontakt med bedriftene og gjøre et enkelt intervju med generelle spørsmål som berører problematikken. Er vedkommende interessert, så kan han få tilsendt en mer detaljert undersøkelse. På denne måten bygger man opp litt tillitt til respondenten og man kan formidle problemet mer direkte.

Skulle interessen i Norge være for liten, så kan man utvide undersøkelsen til å gjelde for Skandinavia. Er det noen land som skiller seg ut i forhold til de andre? Hva er årsaken til dette? Slike indikasjoner kan også være med på å styrke troverdigheten til en fremtidig undersøkelse.

Et annet interessant tema kunne være å undersøke de angrepene som skyldes ukjente årsaker. Vi kan fra ut i fra undersøkelsene til CERT og CSI/FBI se at mange angrep er uidentifiserte av bedriftene. Angrepene er oppdaget, men de kan ikke si om det kommer fra utsiden eller innsiden. Dette er en viktig del som bør undersøkes nærmere. Hvor stor del av de angrepene som bedriftene ikke vet stammer fra, kan være fra innsiden?

8 Referanser

[1] Allen, J.
Protecting Against Insider Threat
2006

[2] Hansen, A. & Hoffstad, A. L.
Att mäta informationssäkerhetsmedvetenhet
Institutionen för data- och systemvetenskap, Stockholms universitet/Kungliga Tekniska Högskolan, 2005

[3] Assante, M.; Boni, B. & Masters, D.
2005 E-CRIME WATCH™ SURVEY SHOWS E-CRIME FIGHTERS MAKING HEADWAY
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2005

[4] Assante, M.; Boni, B. & Masters, D.
2005 E-CrimeWatch™ Survey Summary of Findings
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2005, 1-58

[5] Assante, M.; Boni, B. & Masters, D.
2005 E-Crime Watch Survey – Survey Results
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2005, 1-19

[6] Assante, M.; Boni, B.; Masters, D.; Rose, B.; Treece, D. & Wellington, J.
2004 E-CRIME WATCHTM SURVEY SHOWS SIGNIFICANT INCREASE IN ELECTRONIC CRIMES
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2004, 1-20

[7] Assante, M.; Boni, B.; Masters, D.; Rose, B.; Treece, D. & Wellington, J.
2004 eCrime Watch Survey - Summary of Findings
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2004

[8] Cappelli, D. M.; Desai, A. G.; Moore, A. P.; Shimeall, T. J.; Weaver, E. A. & Willke, B. J.
Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage
Carnegie Mellon University

[9] Rich, E.; Martinez-Moyano, I. J.; Conrad, S.; Cappelli, D. M.; Moore, A. P.; Shimeall, T. J.; Andersen, D. F.; Gonzalez, J. J.; Ellison, R. J.; Lipson, H. F.; Mundie, D.; Sarriegui, J. M.; Sawicka, A.; Stewart, T. R.; Torres, J. M.; Weaver, E. A. & Wiik, J.
Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model
University at Albany, State University of New York, CERT, University at Albany, Sandia National Laboratories, Agder University College Norway, University of Navarra Spain, Worcester Polytechnic Institute, 2005

[10] MacGibbon, A.

Australian Computer Crime and Security Survey
Australian High Tech Crime Centre, 2004

[11] Randazzo, M. R.; Cappelli, D.; Keeney, M.; Moore, A. & Kowalski, E.
Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector
United States Secret Service, CERT® Coordination Center, 2004

[12] Mathisen, J.
Measuring Information Security Awareness
Høgskolen i Gjøvik, 2004

[13] Keeney, M.; Kowalski, E.; Cappelli, D.; Moore, A.; Shimeall, T. & Rogers, S.
Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors
United States Secret Service, CERT® Program, 2005,

[14] Schultz, E. E.
A framework for understanding and predicting insider attacks
University of California - Berkeley Lab, 2002

[15] Jahner, S. & Krcmar, H.
Beyond technical aspects of information security: Risk culture as a success factor for IT risk management
Socio-technical Dimensions in IS Security, 2005

[16] Nordby, Y. & Hansen, C. W.
Informasjonssikkerhet atferd, holdninger og kultur
NTNU, 2005

[17] Olsen, V.; Olsen, S. R. & Nystuen, K. O.
Samfunnets sårbarhet som følge av avhengighet til IT
Nærings- og handelsdepartementet, 2000

[18] Bragdon, B.
2006 E-Crime Watch Survey - Complete Survey Results
CSO magazine, CERT Coordination Center, U.S. Secret Service, 2006, 1-15

[19] Richardson, R.
2003 CSI/FBI Computer Crime and Security Survey
CSI/FBI, 2003

[20] Gordon, L. A.; Loeb, M. P.; Lucyshyn, W. & Richardson, R.
2004 CSI/FBI Computer Crime and Security Survey
CSI/FBI, 2004

[21] Gordon, L. A.; Loeb, M. P.; Lucyshyn, W. & Richardson, R.
2005 CSI/FBI Computer Crime and Security Survey
CSI/FBI, 2005

[22] Gordon, L. A.; Loeb, M. P.; Lucyshyn, W. & Richardson, R.
2006 CSI/FBI Computer Crime and Security Survey

CSI/FBI, 2006

[23] Bishop, M.
Hempelmann, C. F. & Raskin, V. *(ed.)*
New Security Paradigms Workshop 2005
The insider problem revisited
2005, 75-76

[24] Schwarting, I.
Hempelmann, C. F. & Raskin, V. (ed.)
New Security Paradigms Workshop 2005
Position paper
PANEL SESSION: The insider problem revisited, ACM Press, 2005, 79-81

[25] Andersen, D.; Cappelli, D. M.; Gonzalez, J. J.; Mojtahedzadeh, M.; Moore, A. P.; Rich, E.; Sarriegui, J. M.; Shimeall, T. J.; Stanton, J. M.; Weaver, E. A. & Zagonel, A.
Preliminary System Dynamics Maps of the Insider Cyber-threat Problem
University at Albany, Engineering Institute, Agder University College, Attune Group, Inc., CERT Coordination Center, Department of Information Technology Management, University of Navarra, Syracuse University Syracuse, Worcester Polytechnic Institute, University at Albany, 2004, 1-36

[26] Bragdon, B.
Over-Confidence Is Pervasive Amongst Security Professionals
U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Program and Microsoft Corp., 2007

[27] Hasan, R.; Myagmar, S.; Lee, A. J. & Yurcik, W.
Toward a Threat Model for Storage Systems
National Center for Supercomputing Applications, National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign, 2005

[28] Pramanik, S.; Sankaranarayanan, V. & Upadhyaya, S.
Security Policies to Mitigate Insider Threat in the Document Control Domain
Department of Computer Science and Engineering, University at Buffalo, 2004

[29] PricewaterhouseCoopers
DTI Information Security Breaches Survey 2006
Department of Trade and Industry, 2006

[30] PricewaterhouseCoopers
Information security breaches survey 2006 - Executive summary
Department of Trade and Industry, 2006

[31] PricewaterhouseCoopers
Information security breaches survey 2006 - Viruses and malicious software
Department of Trade and Industry, 2006

[32] PricewaterhouseCoopers

Information security breaches survey 2006 - Trustworthy networking
Department of Trade and Industry, 2006

[33] PricewaterhouseCoopers
Information security breaches survey 2006 - Identity and access management
Department of Trade and Industry, 2006

[34] PricewaterhouseCoopers
Information security breaches survey 2006 - e-mail and web usage
Department of Trade and Industry, 2006

[35] Randazzo, M. R.; Keeney, M.; Kowalski, E.; Cappelli, D. & Moore, A.
Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector
Carnegie Mellon University, 2005,

[36] Rich, E.
Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model
University at Albany, State University of New York, 2005

[37] Richardson, R.
2007 CSI Computer Crime And Security Survey
Computer Security Institute, 2007

[38] Rønning, K.; Christensen, C.; Sellæg, J.; Taraldset, B.; Willassen, S.; Gulbrandsen, H. P.; With, C. & Sunde, I. M.
NOU Lovtiltak mot datakriminalitet, Delutredning II
Departementenes servicesenter Informasjonsforvaltning, 2007

[39] Schultz, E. E.
A framework for understanding and predicting insider attacks
University of California - Berkeley Lab, 2002

[40] Schwarting, I.
Hempelmann, C. F. & Raskin, V. (ed.)
New Security Paradigms Workshop 2005
Position paper
PANEL SESSION: The insider problem revisited, ACM Press, 2005, 79-81

[41] Wood, B. J.
An Insider Threat Model For Adversary Simulation
SRI International, 2000

[42] Yu, Y. & Chiueh, T.
Display-Only File Server: A Solution against Information Theft Due to Insider Attack, 31-39

A Følgebrev

Følgebrevet som ble sendt sammen med spørreskjemaet i spørreundersøkelsen finnes som vedlegg på påfølgende side.

FORTROLIGHETSAVTALE

Mellom

.....

(Avsenderen)

og

.....

(Mottakeren)

er i dag inngått følgende avtale om de fortrolige opplysninger som Mottakeren har mottatt eller vil motta av Avsenderen, opplysninger som nedenfor er benevnt Informasjonen:

1. Informasjonen er avgitt i form av et elektronisk skjema på internett. Denne Informasjonen vil kun bli brukt til en undersøkelse i forbindelse med en masteroppgave om temaet Insider Threat.

2. Mottakeren plikter å behandle Informasjonen på en slik måte at den forblir utilgjengelig for uvedkommende og forøvrig slik at det heller ikke oppstår fare for at uvedkommende skal få kjennskap til den.

3. Mottakeren har ikke rett til å benytte Informasjonen på annen måte enn forutsatt i pkt. 1.

4. Mottakeren forplikter seg til ikke i større utstrekning enn hva som etter forutsetningene må ansees nødvendig eller forsvarlig, å overlate Informasjonen til noen han samarbeider med, har som sine ansatte eller liknende. Før Mottakeren i slike tilfeller overlater Informasjonen til andre, skal disse være instruert om opplysningenes fortrolighet og de skal være bundet av skriftlig fortrolighetsavtale.

5. Avsenderen har rett til når han måtte ønske det å få opplyst hvordan Mottakeren sikrer Informasjonen mot å bli tilgjengelig for andre.

6. Mottakeren har ikke rett til å kopiere det utleverte materialet hvis ikke følgende erklæring er godkjent av Avsenderen:

Ved å godkjenne denne avtalen, så gir Avsenderen Mottakeren adgang til å kopiere det utleverte materialet i den utstrekning dette er nødvendig for en hensiktsmessig behandling av det etter forutsetningene.

Hvis ikke annet er skriftlig avtalt, skal Mottakeren, når Avsender krever det, straks tilbakelevere det under pkt. 1 ovenfor utleverte materiale samt eventuelle kopier som

ikke blir tilintetgjort.

7. Denne avtale omfatter ikke:

a. Tekniske eller andre opplysninger som på det tidspunkt Avsenderen ga Informasjonen til Mottakeren, måtte ansees som allment kjent eller som senere blir allment kjent uten at Mottakeren er ansvarlig for dette.

b. Opplysninger om Informasjonen som på lovlig måte er kommet Mottakeren til kjennskap direkte eller indirekte gjennom andre enn Avsender.

8. Mottakeren er erstatningspliktig overfor Avsenderen for eventuelle tap ved brudd på denne avtale. Mottakerens erstatningsplikt gjelder også når bruddet på avtalen er forøvet av en tredjemann som har fått Informasjonen av Mottakeren.

§

Denne fortrolighetsavtale er utarbeidet i to eksemplarer, hvorav partene beholder hvert sitt.

....., den ..... 20..

(Mottakeren) (Avsenderen)

B Spørreundersøkelsen

Spørreundersøkelsen som ble benyttet i denne oppgaven på de neste sidene.

Del 1: Om virksomheten

1) Hvor mange ansatte er det i deres virksomhet (i Norge)?

Over 1000 ☐
500-1000 ☐
250-500 ☐
100-250 ☐
50-100 ☐
20-50 ☐
5-20 ☐
1-5 ☐

2) Hva er din stilling i bedriften?

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

Del 2: Om informasjonssystemene og sikringstiltak

3) Hvordan er informasjonssystemet organisert i deres virksomhet?

Som del av egen virksomhet med egne ansatte ☐
Ved hjelp av ”outsourcing” ☐

En kombinasjon ☐

Vet ikke ☐

4) Omtrent hvor mange personer jobber med virksomhetens informasjonssystem?

(Inkluder både ansatte og/eller innleid personale)

1-5 ☐

5-10 ☐

10-50 ☐

50-100 ☐

Over 100 ☐

Vet ikke ☐

5) Omtrent hvor mye bruker deres bedrift på informasjons- og sikkerhetssystemer i året? (Det inkluderer kjøp av programvare, oppgraderinger, tjenester etc.)

Over 1 million kr ☐

500 000 til 1 million kr ☐

100 000 til 500 000 kr ☐

50 000 til 100 000 kr ☐

10 000 til 50 000 kr ☐

Under 10 000 kr ☐

Vet ikke ☐

6) Har virksomheten noe utstyr for å motvirke angrepsforsøk?

Ja ☐

Nei ☐

Vet ikke ☐

7) Hva slags teknologi bruker dere for å oppdage/motvirke missbruk av datasystemer og nettverk? (flere svar er mulig)

Brannmurer	☐
Antivirus	☐
Antispionvare	☐
Rutiner for manuell/automatisk feilretting	☐
Kryptering av sensitiv informasjon	☐
Rollebasert tilgangskontroll	☐
Innbruddsdeteksjonssystemer (IDS)	☐
System for å forhindre innbrudd (IPS)	☐
Fysiske/biometriske autentifiseringsmekanismer (smartkort, fingeravtrykk el.)	☐
Kryptert trådløst nett	☐
Logge/overvåke tastetrykk av individuelle brukerkontoer	☐
Annet	(skrive felt)
Vet ikke/ikke sikker	☐

* Ordene er forklart under Ordforklaring

8) Overvåker dere om datasystemene og nettverk misbrukes av ansatte eller leverandører?

Ja, men bare systemene	☐
Ja, men bare nettverket	☐
Ja, både systemene og nettverket	☐
Nei	☐
Vet ikke/ikke sikker	☐

Del 3: Trusler og angrep mot virksomheten

9) Hvilke grupper har vært den største sikkerhetstrusselen mot deres virksomhet de

siste 10 årene?

Hackere	☐
Medarbeidere	☐
Tidligere medarbeidere	☐
Informasjonsmeklere	☐
Tjenesteleverandører/konsulenter/leverandør	☐
Terrorister	☐
Kunder	☐
Leverandør/forretningspartnere	☐
Konkurrenter	☐
Tidligere tjenesteleverandører/konsulenter/leverandør	☐
Annet	(skrive felt)
Vet ikke/ikke sikker	☐

10) Hvor mange tilfeller av elektroniske angrep har deres virksomhet opplevd de siste 10 årene?

Ingen	☐
1-9	☐
10-49	☐
50-99	☐
100-249	☐
250 eller flere	☐
Vet ikke	☐

11) Har det totale antallet angrep mot deres virksomhet økt, avtatt eller ikke hatt noen forandring i 2006 kontra tidligere år?

Økt	☐

Avtatt ☐

Ingen forandring ☐

Vet ikke ☐

12) Hvor mange vellykkede angrep av betydning har kommet fra innsiden og/eller utsiden?

	Utenfra	Innsidere
Ingen		
1-5		
5-10		
10-50		
50-100		
Over 100		
Vet ikke		

13) Av vellykkede angrep fra innsiden og/eller utsiden. Hvor ofte har angrep kategorisert som liten, moderat, stor og katastrofal skjedd?

Konsekvens: Hyppighet:	Liten	Moderat	Stor	Katastrofal
Aldri				
Nesten aldri				
Sjelden				
Ofte				
Svært ofte				

14) Omtrent hvor stor del av angrepene ble avslørt ved en tilfeldighet? (I forhold til angrep avslørt av systemer/policyer)

	Utenfra	Innsidere
Ingen		
Mindre enn 10%		
10-24%		
25-49%		
50-74%		
75-99%		
100%		
Vet ikke		

15) Hvilke av følgende angrepsforsøk har blitt begått mot deres bedrift de siste 10 årene? (flere svar er mulig)

"Phishing"	☐
Spionvare	☐
Ulovlig generering av søppelpost	☐
Denial of Service (DoS) angrep	☐
Virus eller annen ondsinnet kode	☐
Identitetstyveri	☐
Bedrageri (misbruk av kredittkort el.)	☐
"Zombie-maskiner" på bedriftens nettverk	☐
Passord sniffing	☐
Utpressing	☐
Sabotasje på systemer, drift, informasjon, data el.	☐
Uautorisert tilgang til informasjon, systemer eller nettverk	☐
Tyveri av opphavsrettslig beskyttet materiale	☐
Tyveri av IT-utstyr (pc, server, pda, mobiltelefon el.)	☐
Uautorisert innsyn av privat eller sensitive informasjon	☐
Hacking (datainnbrudd)	☐
Annet	(skrive felt)

Vet ikke/ikke sikker ☐

16) Hvilke av disse angrepstypene har blitt begått mot deres bedrift fra utiden og/eller innsiden?(flere svar er mulig)

	Utenfra	Innsider	Vet ikke
"Phishing"			
Spionvare			
Ulovlig generering av søppelpost			
Denial of Service (DoS) angrep			
Virus eller annen ondsinnet kode			
Identitetstyveri			
Bedrageri (misbruk av kredittkort el.)			
"Zombie-maskiner" på bedriftens nettverk			
Passord sniffing			
Utpressing			
Sabotasje på systemer, drift, informasjon, data el.			
Uautorisert tilgang til informasjon, systemer eller nettverk			
Tyveri av opphavsrettslig beskyttet materiale			
Tyveri av IT-utstyr (pc, server, pda, mobiltelefon el.)			
Uautorisert innsyn av privat eller sensitive informasjon			
Hacking (datainnbrudd)			
Annet			

17) Hvor stort var det totale verditapet dere opplevde i forbindelse med en enkelt hendelse av elektronisk kriminalitet eller systeminntrening?

1 million kr eller mer	☐
500 000 til 1 million kr	☐
100 000 til 500 000 kr	☐
50 000 til 100 000 kr	☐
10 000 til 50 000 kr	☐
Under 10 000 kr	☐
Vet ikke/ikke sikker	☐

18) Var denne hendelsen utført av en på innsiden eller utenfra?

Innsiden	☐
Utenfra	☐
Vet ikke	☐

19) Hva slags tap har bedriften opplevd de siste 10 årene?

(flere svar er mulig)

Ubetydelige driftstap	☐
Kritiske driftstap	☐
Finansielle tap	☐
Ubetydelige finansielle tap	☐
Kritiske finansielle tap	☐
Tap av omdømme	☐
Ikke opplevd tap	☐
Annet	(skrive felt)
Vet ikke/ikke sikker	☐

20) Hvilke av disse kildene antas å ha vært årsaken til innsideinntrengningen dere har opplevd de siste 10 årene? (flere svar er mulig)

Medarbeidere som ikke var engasjert i lederstilling da hendelsen inntraff ☐

Medarbeidere som var engasjert i lederstilling da hendelsen inntraff ☐

Leverandører/vikarer da hendelsen inntraff ☐

Tidligere medarbeidere som var ansatt i ikke-ledende stillinger ☐

Tidligere leverandører/vikarer ☐

Tidligere medarbeidere som tidligere var ansatt i ledende stillinger ☐

Vet ikke/ikke sikker ☐

21) Hva er den mest negative konsekvensen som noen gang har forekommet etter et angrep utført av personer på innsiden? (Mot nettverk, data eller systemer)

Kritisk systemsammenbrudd i bedriften ☐

Kritisk systemsammenbrudd som påvirket kunder og bedriftspartnere ☐

Tap av bedriftens omdømme ☐

Tap av nåværende og/eller fremtidig inntekter ☐

Kritisk systemsammenbrudd som påvirket større kritiske infrastruktursektorer ☐

Tap av kunder ☐

Mistet bedriftssamarbeid ☐

Tap av menneskeliv ☐

Personskader ☐

Ingen innvirkning ☐

Del 4: Håndtering hendelser og oppbevaring av logger

22) Har virksomheten en plan for håndtering og rapportering av elektronisk kriminalitet som er utført mot virksomheten?

Ja ☐

Nei, men planlegger å lage en plan de neste 12 månedene ☐

Nei, ingen planer om å gjennomføre en plan ennå ☐

Vet ikke ☐

23) Krever dere intern rapportering ved missbruk av maskiner som er brukt av ansatte eller leverandører?

Ja ☐

Nei ☐

Vet ikke/ikke sikker ☐

24) I hvor lang tid arkiverer dere informasjon/logginger om angrep på nettverk, data og systemer?

1 år eller mindre ☐

Fra 1 til 2 år ☐

Fra 2 til 5 år ☐

5 år eller lengre ☐

Vet ikke ☐

Arkiverer ikke ☐

25) Hvor ofte gjennomgår eller oppdaterer dere sikkerhetspolicyen?

Hver 6 måned ☐

Årlig ☐

Om nødvendig ☐

Har ikke sikkerhetspolicy ☐

Annet ☐

Vet ikke ☐

Ordforklaring

Phishing (Password Harvesting fishing) er å lure til seg fortrolig informasjon (f.eks.

passord) fra noen ved å gi seg ut for å være en troverdig kilde med behov for slik informasjon.

Spionvare er programvare som utfører visse oppgaver på datamaskinen, vanligvis uten ditt samtykke. Programvaren kan for eksempel vise annonser eller prøve å samle inn personlige opplysninger om deg.

DoS angrep hindrer normal tjeneste på f.eks en webserver ved å bombardere den med nettverkstrafikk.

Zombie-maskin kalles en PC som har fått installert fiendtlig kode som gjør at den kan fjernstyres av en hacker.

Definisjon konsekvens

Katastrofal: Uopprettelig økonomiske tap

Stor: Alvorlig økonomisk tap (inkludert tap av tid)

Alvorlig tap av renommé eller rykte

Moderat: Gjenopprettelig økonomisk tap (inkludert tap av tid)

Moderat tap av renommé eller rykte

Liten: Ubetydelige økonomiske tap (inkludert tap av tid)

Intet tap av renommé eller rykte

Definisjon hyppighet

Svært ofte: Hendelsen har forekommet flere ganger årlig

Ofte: Hendelsen har forekommet årlig

Sjelden:Hendelsen har forekommet ca hvert 5. år

Nesten aldri: Hendelsen har forekommet ca hvert 10. år