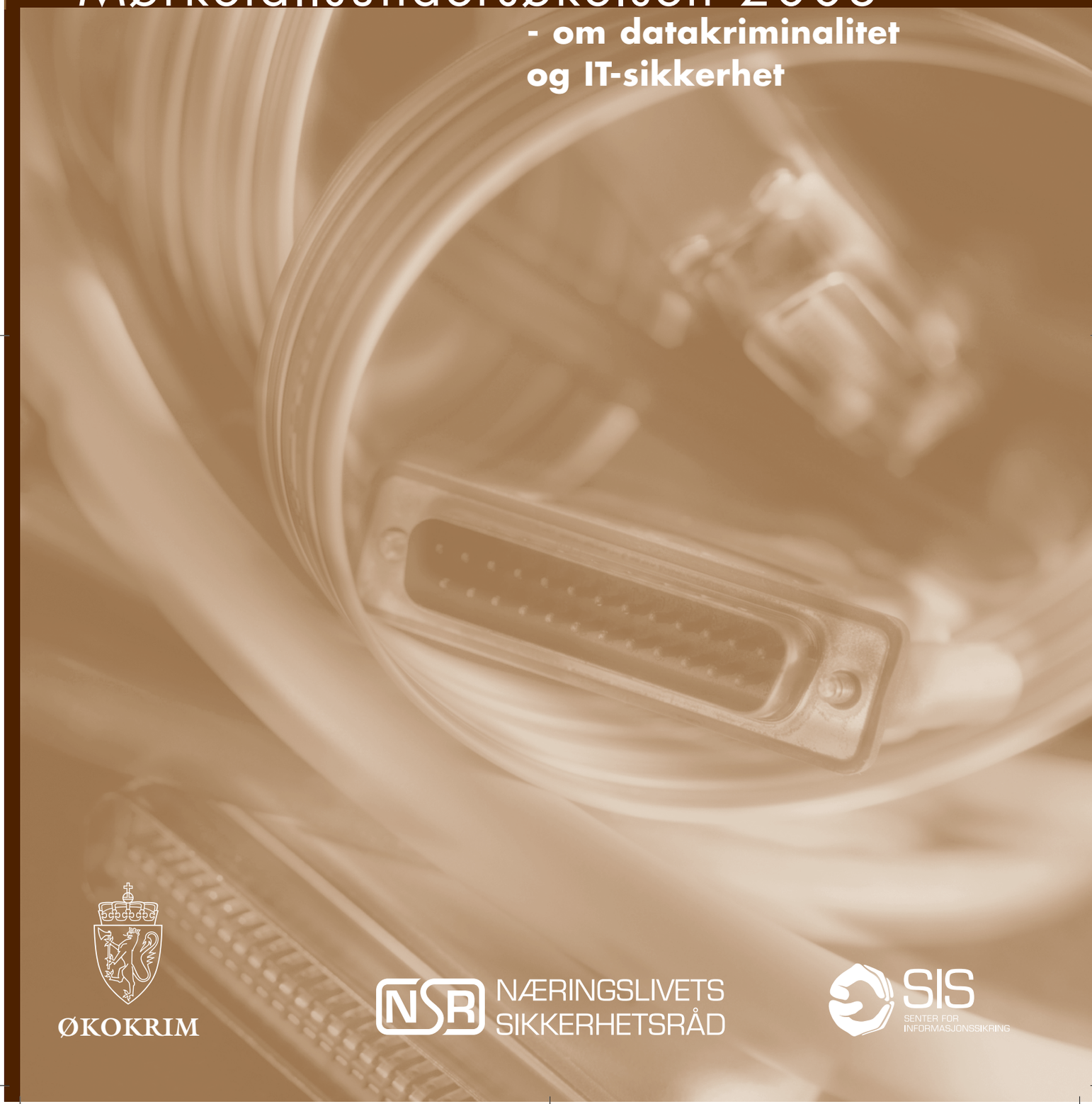
Mørketallsundersøkelsen 2003

- om datakriminalitet og IT-sikkerhet



ØKOKRIM

NÆRINGSLIVETS SIKKERHETSRÅD

SIS
SENTER FOR INFORMASJONSSIKRING

Innhold

Det samlede tapet til norske virksomheter kan anslås til 5 milliarder

Sammendrag

Mørketallsundersøkelsen 2003 omhandler både datakriminalitet og andre uønskede IT-hendelser.

Til tross for at 60 % av norske virksomheter ble rammet av slike hendelser i 2003 viser tall fra politiet at bare 187 tilfeller av datakriminalitet ble anmeldt.

I 2003 ble norske virksomheter utsatt for omtrent

- 5200 datainnbrudd
- 2,7 mill. forsøk på data-innbrudd
- 150 000 virusinfeksjoner
- 50 mill. forsøk på virusinfeksjon

Bare 50 av datainnbruddene ble anmeldt. Undersøkelsen viser at selv om virksomhetene kjenner til disse innbruddene velger de av ulike årsaker ikke å anmelde dem.

To av tre virksomheter vil få vesentlige problemer allerede etter én dag dersom de viktigste IT-systemene er ute av drift. Åtte av ti virksomheter har lagret verdifull informasjon elektronisk og ni av ti vil få vesentlige problemer hvis informasjonen er upålitelig eller gal.

Det står derfor i skarp kontrast at bare hver fjerde virksomhet som ble rammet, kunne anslå hvor mye de har tapt. 12 % har rutiner for å beregne slike tap.

Det samlete tapet for norske virksomheter kan anslås til 5 milliarder kroner. 70 % av virksomhetene får ekstra arbeid på grunn av uønskede hendelser.

Bare hver femte virksomhet som har vært utsatt for datakriminalitet, har greid å identifisere en gjerningsmann. For å få til det, må man vite hva som foregår i systemene. Selv om mange virksomheter logger aktivitet, går mindre enn halvparten systematisk gjennom loggene. De fleste mangler rutiner for rapportering dersom de skulle avdekke en uønsket hendelse.

Trådløse nettverk brukes av stadig flere, men mer enn 30 % unnlater å sikre disse dataene med kryptering.

Hver tredje virksomhet er trege med å oppdatere sin antivirus-programvare, og like mange slurver med sikkerhetsoppdatering av annen programvare.

Virksomheter i helse- og sosialsektoren har lagret store mengder personopplysninger, men halvparten av dem vet ikke om de har vært utsatt for datainnbrudd eller datatyveri. Sektoren bruker sikringsmekanismer som kryptering i langt mindre grad (13 %) enn andre sektorer. Til sammenligning bruker 40 % av virksomhetene innen bank- og finansnæringen kryptering.

Innenfor datakriminalitet er mørketallene store

Innledning

Offentlig statistikk forteller oss lite om omfanget av datakriminaliteten og de trusler som rettes mot IT-systemene. På alle kriminalitetsområder finnes mørketall, lovovertredelser som ikke anmeldes. Tidligere mørketallsundersøkelser har vist at disse er store når det gjelder datakriminalitet. Mange av hendelsene som skaper IT-problemer er forårsaket av ulykker og uhell. Selv ikke en fullstendig oversikt over datakriminaliteten, ville derfor gitt hele bildet av hvilke IT-trusler norske virksomheter står overfor.

Mørketallsundersøkelsen 2003 er gjennomført for å finne ut:

- Hvilke typer datakriminalitet forekommer og i hvilket omfang?
- Er noen bransjer mer utsatt enn andre?
- Hvilke følger får datakriminalitet?
- Hvor sårbare er norske virksomheter på IT-siden?
- Hvilke sikkerhetstiltak og -rutiner er satt i verk, og hvordan påvirker det omfanget av datakriminalitet?

Mørketallsundersøkelsen 2003 er en oppfølging av en forskningsrapport fra 1989 og tilsvarende undersøkelser fra 1993, 1997 og 2001. Denne gangen er undersøkelsen gjennomført som et samarbeid mellom av Næringslivets Sikkerhetsråd (NSR), ØKOKRIM og Senter for informasjonssikring (SIS). Innhentingen av data ble foretatt i januar 2004 av Markeds- og Mediainstituttet AS. Av 1300 utsendte kom det inn 722 skjemaer.

Analysen er utført av forsker Lillian Røstad og seniorforsker Øyvind Eilertsen fra SIS i samarbeid med NSRs Datakrimutvalg som i 2004 består av:

- Sikkerhets- og beredskapsdirektør Britt Amundsen Hoel, Norges Bank (leder)
- Politiinspektør Berit Børset Solstad, ØKOKRIM
- Daglig leder Ove Olsen, SIS
- IT sikringsleder Øyvind Davidsen, Statoil
- Seksjonssjef IS-sikkerhet Per Bjørkum, Norsk Hydro
- Seniorkonsulent Arne Tjemsland, Systemsikkerhet AS

Med **datakriminalitet** menes straffbare handlinger der data eller en datamaskin er objekt for den straffbare handlingen.

Med **sikkerhetsbrudd** menes hendelser som er forårsaket av at personell har brutt gjeldende sikkerhetsregelverk i virksomheten.

Med **uønskede hendelser** menes alle uønskede hendelser i en virksomhet, både uhell, ulykker og tilsiktede handlinger.

Seks av ti norske virksomheter ble rammet av datakriminalitet eller andre uønskede IT-hendelser i 2003

Datakriminalitet i norske virksomheter

60 % av norske virksomheter har vært utsatt for uønskede hendelser i 2003.

Undersøkelsen viser at virusinfeksjon, tyveri av IT-utstyr og misbruk av IT-ressurser er de mest vanlige former for uønskede hendelser i norske bedrifter.

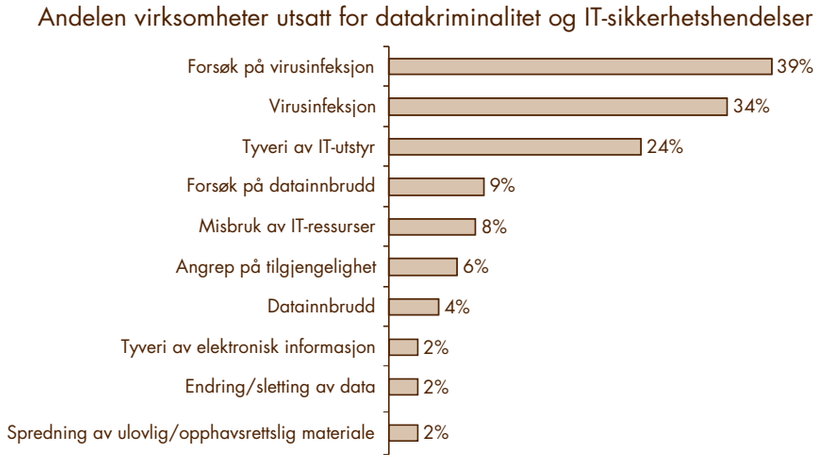
En av tre bedrifter oppgir at de har vært utsatt for virusinfeksjon i 2003, tilsvarende tall for 2001 var én av to. Dette tyder på økende bevissthet rundt virusbeskyttelse. Virusplagen har økt dramatisk i perioden.

Større virksomheter er naturlig nok mer utsatt for tyveri av IT-utstyr og misbruk av IT-ressursene enn mindre. 8% av virksomhetene har påvist misbruk av IT-ressurser. Relativt mange saker som omfatter misbruk av IT-ressurser har ført til disiplinære tiltak. I en fjerdedel av de totalt 408 rapporterte sakene ble gjerningsmannen identifisert. Seks personer er blitt anmeldt, fem er blitt oppsagt og 12 har fått en sivil sak mot seg.

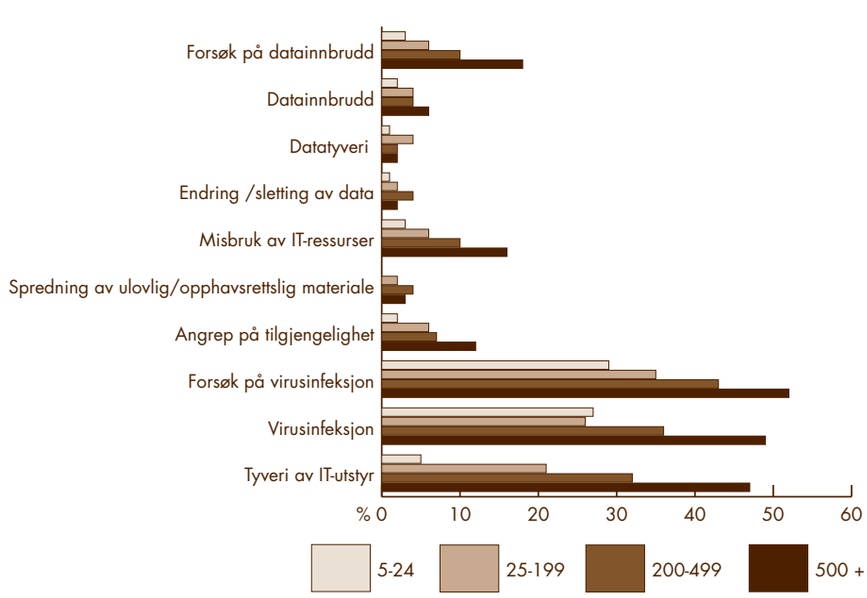
Omtrent 2 % av virksomhetene har vært utsatt for tyveri av datainformasjon i 2003. Dette er på samme nivå som i 2001. Det er tydelig at virksomhetene i økende grad er opptatt av hvilke skadevirkninger datatyveri kan ha. I 2001 ble bare to slike saker anmeldt, mens tilsvarende tall for 2003 var 23.

Undersøkelsen gir grunnlag for å beregne at 5200 norske virksomheter ble utsatt for datainnbrudd i 2003. Dette representerer en nedgang fra 2001 da tilsvarende tall var 7500. I samme periode har det vært en tilnærming mellom skaden av virusinfeksjoner og datainnbrudd på den måten at stadig flere virustyper søker å sende informasjon fra virksomheten ut på Internett. Det er derfor vanskelig å si om nedgangen i datainnbrudd er reell, eller om det her er snakk om en vridning i angrepsmåten.

Andelen virksomheter utsatt for datakriminalitet og IT-sikkerhetshendelser



Utsatt for datakriminalitet - antall ansatte



Mange følger ikke med på hva som skjer og har ingen planer for hvordan de skal håndtere en hendelse dersom de skulle snuble over en.

Hvem oppdager datakriminalitet?

For å bekjempe datakriminalitet, er det viktig å ha rutiner for overvåking og varsling av uønsket aktivitet. Til tross for at innbruddsdetekteringssystem (IDS) er et anerkjent verktøy for dette, bruker færre enn 20% av de store virksomhetene IDS. Bare 6% av mindre virksomheter gjør det. Undersøkelsen viser ingen merkbar utvikling på dette feltet siden 2001. Det er store forskjeller mellom bransjene. 50% av virksomhetene innen bank- og finansnæringen benytter IDS, mens bare 8% i helse- og sosialsektoren gjør det samme.

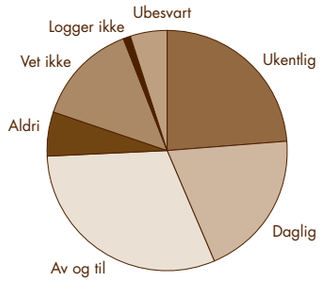
Mange virksomheter benytter verktøy som logger aktivitet, men bare 44% går systematisk gjennom loggene. Færre enn 27% av små virksomheter har daglig eller ukentlig gjennomgang, mens 63% av de store har det. Her er det ubetydelig forandring siden 2001.

Undersøkelsen bekrefter at hyppig gjennomgang av logger fører til at en oppdager flere uønskede hendelser.

Undersøkelsen viser at en større andel av virksomheter som har outsourcet IT, ikke vet om de har vært utsatt for uønskede hendelser enn de som selv står for IT-driften. Dette på tross av at de i større grad rapporterer at IDS brukes for å sikre deres systemer.
Det kan tyde på mangler i rapporteringskrav i outsourcingsavtalene.

Undersøkelsen viser at bransjene har ulik evne til å avdekke uønskede hendelser. Mens 20 % av virksomhetene innen bank- og finansnæringen oppgir at de ikke vet om de har vært utsatt for datainnbrudd eller datatyveri, svarer nesten 50 % innenfor helse- og sosialsektoren det samme. Virksomheter i helse- og sosialsektoren har gjennomgående mindre kunnskap om de uønskede hendelsene de har vært utsatt for enn virksomheter i andre bransjer. Med tanke på de sensitive opplysningene som behandles i denne sektoren, var det overraskende at bransjen ikke satser mer på å avdekke uønskede hendelser.

Rutinemessig gjennomgang av logger



Bare 20% av virksomhetene som rammes av datakrininalitet, har greid å identifisere en gjerningsmann

Finnes det rutiner for rapportering av hendelser?

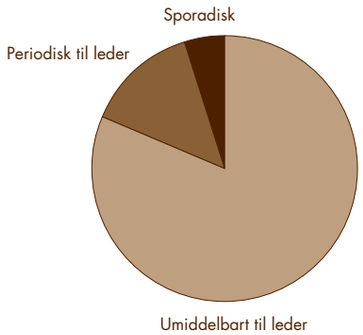
Det er skremmende å konstatere at mer enn halvparten av virksomhetene fremdeles mangler rutiner for rapportering av uønskede hendelser internt. I virksomheter som har slike rutiner rapporterer 83% umiddelbart til leder etter en uønsket endelse.

Bare 20% av de virksomhetene som har vært utsatt for datakriminalitet, har greid å identifisere minst én av gjerningsmennene. Det samme kom frem i 2001-undersøkelsen. Datainnbrudd, virus og tjenestenekting (DoS-angrep), kommer ofte utenfra, og det er vanskelig for virksomhetene selv å knytte dem til en gjerningsmann.

Vanligvis er det virksomhetens egne ansatte som står for datatyveri, uautorisert endring og sletting av data og misbruk av IT-ressurser.

I 66 tilfeller oppgir virksomhetene at egne ansatte er kilden til virusspredning. Vi tolker det slik at virus er blitt spredd internt i virksomheten fordi en av de ansatte ikke har fulgt rutinene for virusbeskyttelse.

Hvordan rapporteres bruddene?



IT-sikkerhet er alltid en kombinasjon av tekniske tiltak og gode rutiner og holdninger blant brukerne. Når rutinene svikter, kan ikke tekniske tiltak i seg selv avverge problemene.

Politiet mottok bare 187 anmeldelser av datakriminalitet i 2003

Håndtering av datakriminalitet

Tall fra ØKOKRIM viser at det i 2003 ble anmeldt totalt 187 tilfeller av datakriminalitet. Det er en liten nedgang fra 2001. Det var en vesentlig nedgang i antallet datainnbrudd, mens det var en betydelig økning i antallet tyveri av elektronisk informasjon. Dette er i tråd med funnene i Mørketallsundersøkelsen.

Mørketallsundersøkelsen 2003 viser at viljen til å anmelde straffbare forhold varierer sterkt med typen kriminalitet. 75% anmelder tyveri av datamaskiner, mens annen type datakriminalitet anmeldes unntaksvis. Det kan synes som om offentlige virksomheter i større grad anmelder misbruk av IT-ressurser enn private.

De grunnene som oftest trekkes frem som årsak til at forhold ikke anmeldes, er at saken er ubetydelig, at det er umulig å finne gjerningsmannen eller at politiet ikke har ressurser.

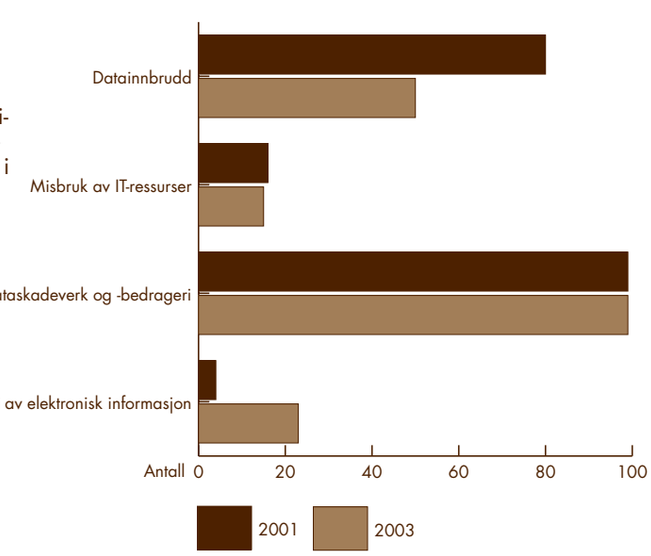
En rekke lover og forskrifter pålegger rapportering av sikkerhetsbrudd til eksterne instanser. Undersøkelsen viser at kun 16 % av virksomhetene har etablert rutiner for dette. Forholdene er betydelig bedre i offentlig sektor enn i privat.

Andelen hendelser som anmeldes

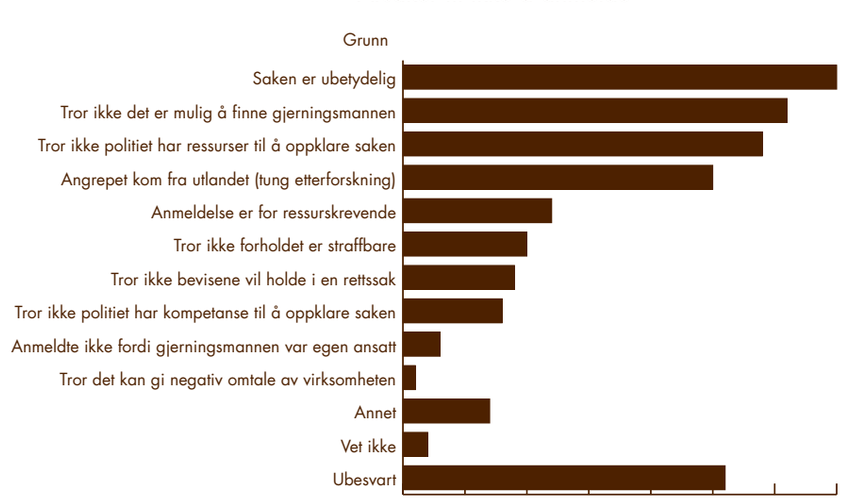
Type hendelse	Andel som anmeldes
Datainnbrudd	0,6 %
Datatyveri	0,9 %
Endring/sletting av data	0,0 %
Misbruk av IT-ressurser	2,7 %
Virusinfeksjon	0,0 %
Tyveri av IT-utstyr	76,3 %

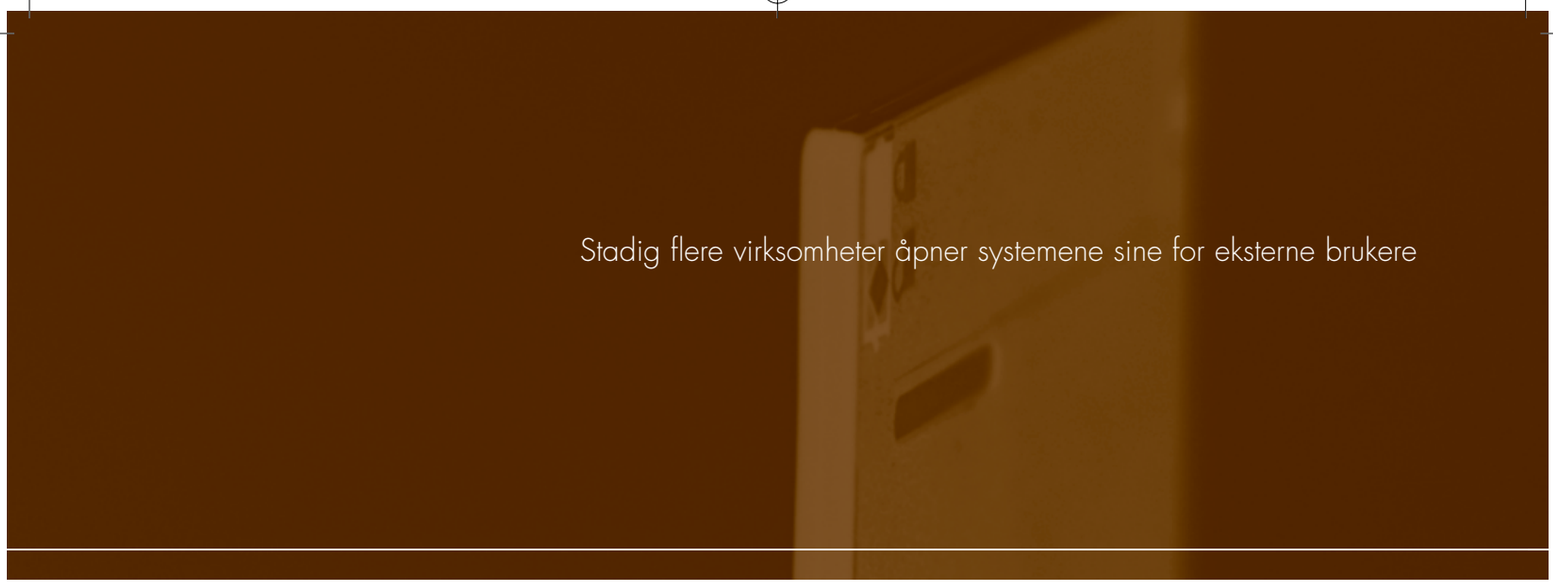
Kilde: ØKOKRIM

Antall anmeldelser av datakriminalitet (tall fra politiet)



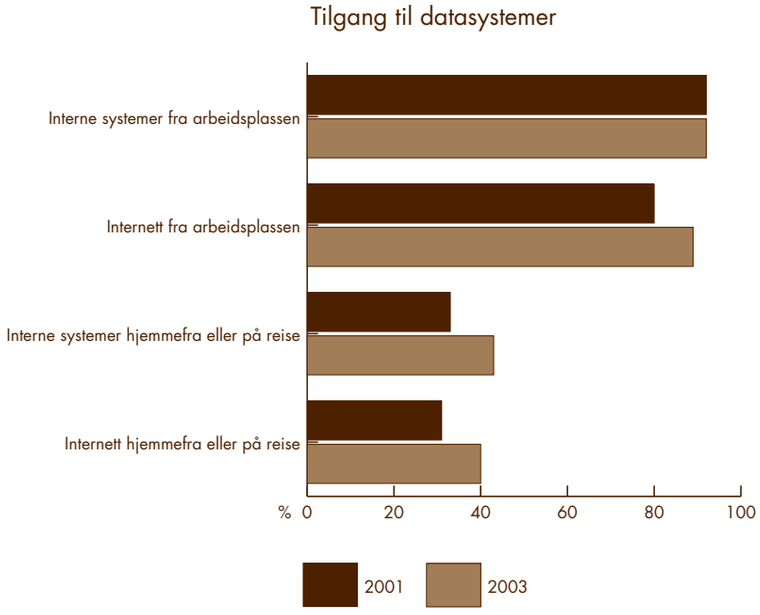
Årsaker til ikke å anmelde





Stadig flere virksomheter åpner systemene sine for eksterne brukere

Avhengighet av IT



Norske virksomheter er svært avhengig av IT, likevel er det varierende hvor godt de beskytter seg mot uønskede hendelser på dette området.

Alle virksomhetene i undersøkelsen benytter Internett, og nesten halvparten har åpnet sine systemer for kunder, samarbeidspartnere eller andre eksterne brukere. Bortimot halvparten gir ansatte tilgang til interne systemer hjemmefra. I 2001 var andelen en tredjedel. Det har dermed skjedd en markant økning fra 2001 til 2003. Det er imidlertid stor variasjon mellom bransjene. Over 80 % av virksomhetene i bank- og finansnæringen tillater hjemmearbeid opp mot interne IT-systemer, mens bare 17% i helse- og sosialsektoren gjør det samme.

Virksomhetene er sårbare for datakriminalitet på flere områder:

Konfidensialitet - Tyveri av verdifull eller sensitiv informasjon.

Integritet - Manipulering eller feilbehandling av informasjon slik at denne ikke lenger er til å stole på.

Tilgjengelighet - Sabotasje eller forstyrrelse av IT-systemer slik at disse ikke blir tilgjengelige for virksomheten.

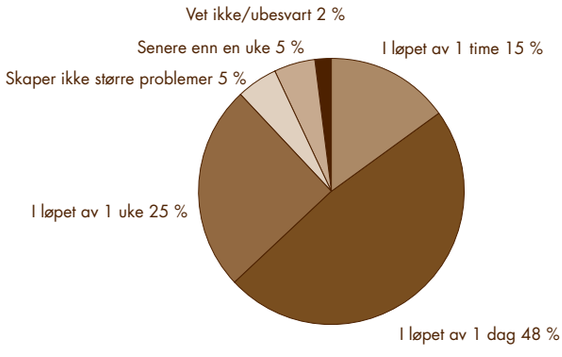
Åtte av ti virksomheter har verdifull informasjon lagret elektronisk. Ni av ti får store problemer dersom denne informasjonen er upålitelig.

80 % av virksomhetene har lagret verdifull eller sensitiv informasjon elektronisk. På tross av dette krypterer bare 14 % av virksomhetene informasjonen. I bank og finansnæringen bruker 40 % av virksomhetene kryptering, mens bare 13 % av virksomhetene i helse- og sosialsektoren gjør det samme. Begge disse bransjene er underlagt egne krav til informasjonssikring og har egne tilsyn.

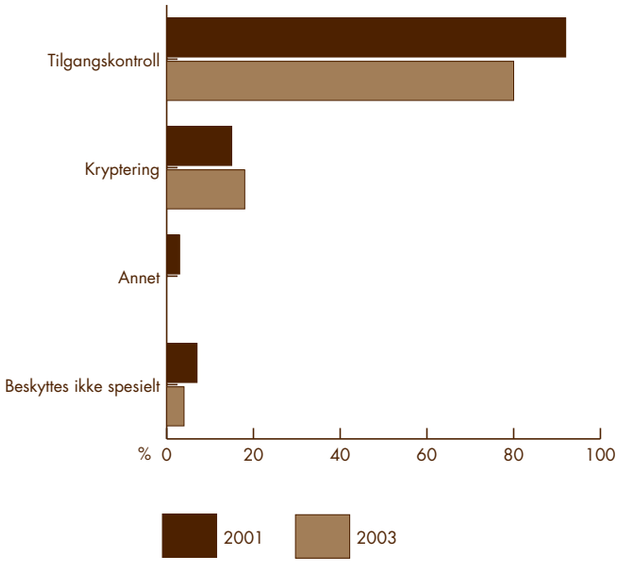
Elektronisk informasjon er viktig for styringen av virksomheten og sentral i beslutningsprosessene. Nesten 90 % oppgir at de vil få vesentlige problemer hvis informasjonen er upålitelig eller gal for eksempel på grunn av manipulering.

IT blir stadig mer integrert i forretningsprosessene. Mer enn to tredjedeler av virksomhetene vil få vesentlige problemer allerede etter én dag dersom de viktigste IT-systemene er ute av drift. Dette er en noe lavere andel enn ved forrige undersøkelse.

IT systemer ute av drift
- når fører dette til vesentlige problemer



Hvordan beskyttes bedriftssensitiv informasjon?



«Koste hve det koste vil ….»

Tap og skade

Følger av hendelser

Følge	2001	2003
Ekstra arbeid	65 %	69 %
Gjennomgang av sikkerheten i virksomheten	31 %	38 %
Tap av forretning	2 %	5 %
Tap av renommé	3 %	2 %
Ingen av disse	9 %	5 %
Annet		2 %
Vet ikke		1 %

Undersøkelsen viser at det er svært vanskelig å anslå tap knyttet til datakriminalitet og andre uønskede IT-hendelser. Bare 25% av virksomhetene var i stand til å anslå det direkte tapet og bare 6% det indirekte tapet knyttet til hendelsene. Dette er den samme situasjonen som for to år siden. Blant de som oppgav kostnadene var det gjennomsnittlige tapet på ca 200.000 kroner i direkte kostnader og 450.000 kroner i indirekte kostnader.

Av dem som rapporterte slike hendelser, var det bare 12% som oppga at de hadde rutiner for å estimere tapet. Dette avslører at kostnader ved sikkerhetshendelser fremdeles ikke er i fokus.

Det samlede direkte tapet for norske virksomheter er estimert til 1,3 milliarder kroner i 2003, og det samlede indirekte tapet til 4 milliarder kroner. Totalt utgjør det mer enn 5 milliarder kroner. Dette følger trenden en har sett i de tidligere undersøkelsene.

Av de virksomhetene som hadde hatt uønskede hendelser i 2003, rapporterte 70% at de hadde hatt ekstra arbeid i forbindelse med hendelsen. Nesten 40% rapporterte at de hadde satt i verk en gjennomgang av sikkerheten som følge av hendelsen. Snaut 5% mente at hendelsen hadde ført til tap av forretning, mens vel 2% var redd for at hendelsen hadde skadet virksomhetens omdømme.

Mange virksomheter bruker i dag store summer på IT-sikkerhet, men samtidig er det vanskelig å måle hvilken økonomisk nytte disse investeringene gir. Så lenge virksomhetene i liten grad beregner tapet ved IT-sikkerhetshendelser, mener Datakrininalitet at det vil være svært vanskelig å vurdere hvor vidt sikkerhetstiltakene er nyttige og hvilke som gir mest nytte.

Mange har de grunnleggende beskyttelsestiltakene på plass, men manglende vedlikehold svekker sikkerheten.

Beskyttelse mot datakriminalitet

Mørketallsundersøkelsen viser at passord, antivirusprogram og brannmur brukes i så å si alle norske virksomheter. To av tre oppgir at de har avlåste serverrom. Andre tilgangskontrollmekanismer enn passord brukes fremdeles sjelden, men hver tredje større virksomhet benytter engangspassord eller smartkort.

Hver tredje virksomhet har tatt i bruk trådløse nettverk, men undersøkelsen viser at mer enn 30 % av disse ikke sikrer dataene i nettet med kryptering. Dette innebærer at mange virksomheter gir omverden enkel tilgang til sine data. Likevel har det vært en dobling i utbredelsen av virtuelle private nett (VPN) som sikringsmekanisme fra 2001 til 2003. Sammen med økningen i bruk av engangspassord og smartkort indikerer dette økt mobilitet og bevissthet omkring sikkerhetstiltak. Det er Datakrimutvalgets oppfatning at det er viktig at det fokuseres på sikring av trådløse nett fremover.

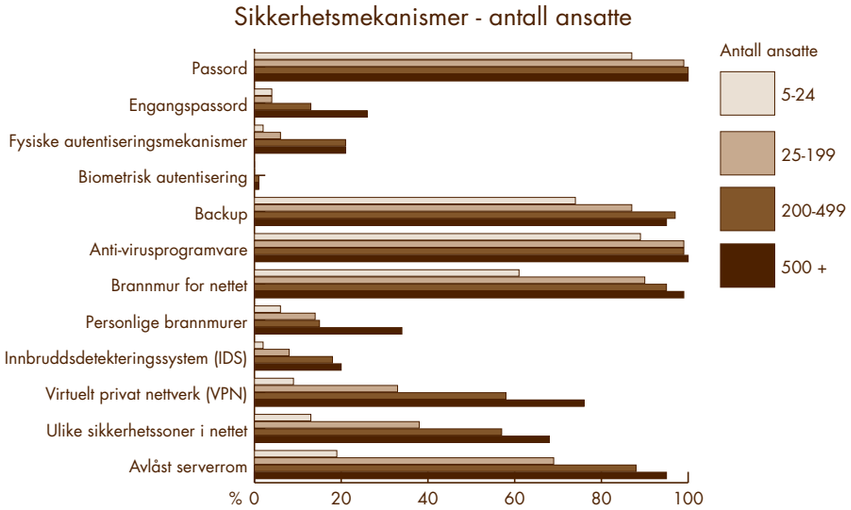
Brannmurer filtrerer trafikken mellom virksomheten og eksterne nettverk og kan derfor beskytte mot både datainnbrudd og virus. Det har vært en markant økning i bruken av brannmur fra 67 % i 2001 til 84 % i 2003. Likevel har ikke antallet rapporterte datainnbrudd gått ned. Bare 60 % av små virksomheter (5-24 ansatte) bruker brannmur. Datakrimutvalget mener at brannmur fremdeles er for lite utbredt som beskyttelsesmekanisme i små virksomheter.

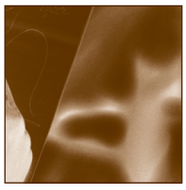
Kontinuerlig eller periodisk sikkerhetsoppdatering (patching) av programvare er viktig. Hver tredje virksomhet har likevel ikke som rutine å gi slike oppdateringer.

De aller fleste virksomhetene benytter programvare som beskytter mot virus. Likevel var det 150.000 «vellykkede» virusangrep i Norge i fjor. Selv om 90 % av virksomhetene rapporterer at de har rutiner for å oppdatere antivirusprogramvare, innbærer ikke disse rutinene umiddelbar oppdatering når nye virussignaturer foreligger for mer enn to tredjedeler.

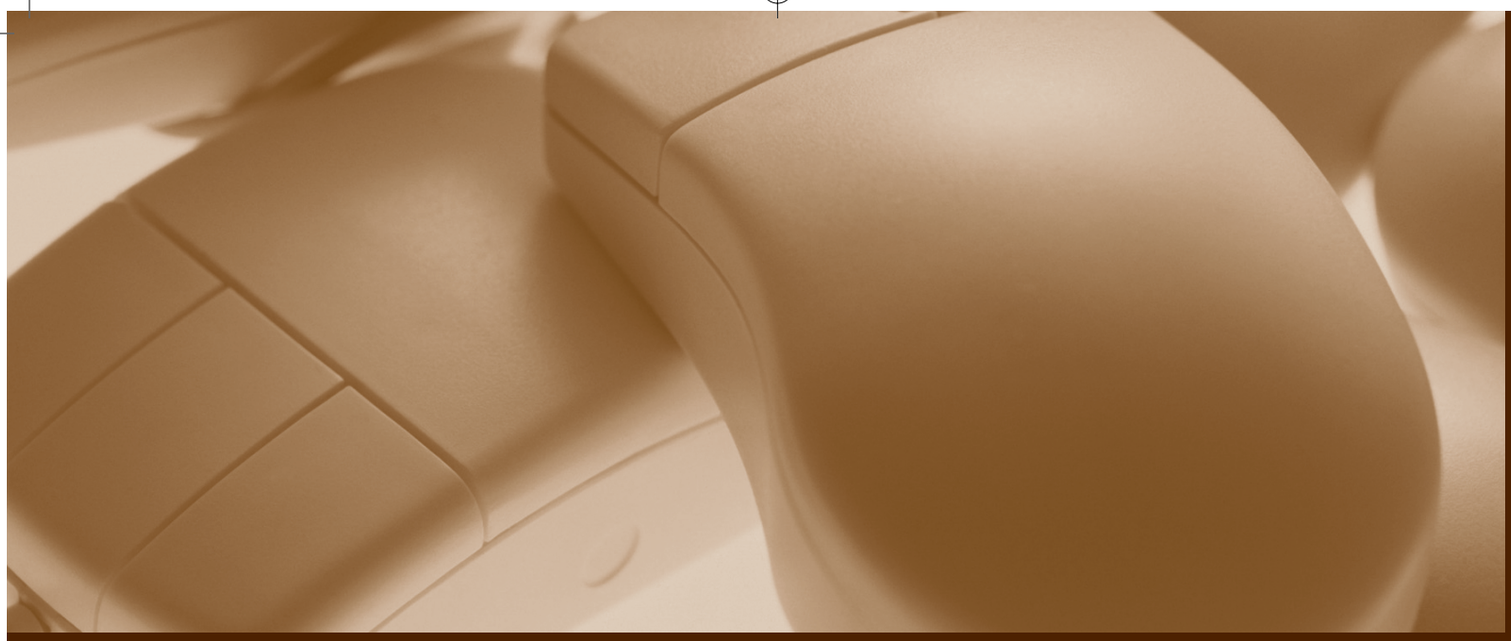
Datakrimutvalgets erfaring er at virksomheter som ikke jevnlig patcher sine systemer, er betydelig mer utsatt for datainnbrudd.

Sikkerhetsmekanismer - antall ansatte




Datakriminalitet i 2003



ØKOKRIM

Politiets datakrimsenter

Politiets datakrimsenter (PDS) ved ØKOKRIM er et nasjonalt polititjenesteorgan for å forebygge, etterforske og påtale datakriminalitet, og et kompetanseorgan for å utvikle nye kunnskaper om metoder og teknologi i kriminalitetsbekjempelsen. Senteret bistår politietaten i sikring og analyse av elektroniske spor, spesielt i større og komplekse saker. PDS bidrar også til trusselvurderinger, blant annet gjennom deltakelsen i arbeidet med Mørketallsundersøkelsene.
Se også www.okokrim.no

NSR NÆRINGSLIVETS SIKKERHETSRÅD

Næringslivets Sikkerhetsråd/Datakrimutvalget

Næringslivets Sikkerhetsråd (NSR) er næringslivets securityfaglige forum.
NSR er en selvstendig medlemsforening stiftet av Næringslivets Hovedorganisasjon, Finansnæringens Hovedorganisasjon, Handels- og Servicenæringens Hovedorganisasjon, Sparebankforeningen i Norge, Arbeidsgiverforeningen NAVO og Norges Rederiforbund/Den Norske Krigsforsikring for Skib.
NSR har oppnevnt spesialistutvalg, bl.a. Datakrimutvalget innen IT-kriminalitet. Det er Datakrimutvalget som har det faglige ansvaret for å gjennomføre mørketallsundersøkelsene.
Se også www.nsr-org.no

SIS SENTER FOR INFORMASJONSSIKRING

Senter for informasjonssikring

Senter for informasjonssikring (SIS) har ansvar for å koordinere aktiviteter knyttet til IKT-sikkerhet i Norge og arbeider med å kartlegge det totale trusselbildet mot IKT-systemer i det norske samfunnet.
SIS skal være en nasjonal informasjonskilde med hensyn til IKT-trusler og tilhørende tiltak. SIS vil i særlig grad prioritere tiltak rettet mot små og mellomstore bedrifter i Norge.
SIS deltar i mørketallsundersøkelsen fordi dette er en unik mulighet til å analysere utviklingen av datakriminalitet i Norge. Mørketallsundersøkelsen har gjennom mange år etablert seg som en uunnværlig kilde i arbeidet med informasjonssikring.
Se også www.norsis.no

Næringslivets Sikkerhetsråd ■ Essendrops gate 6, Postboks 5493 Maj, 0305 Oslo ■ Tlf.: 23088460 ■ E-post: nsr@nso.no ■ URL: www.nsr-org.no