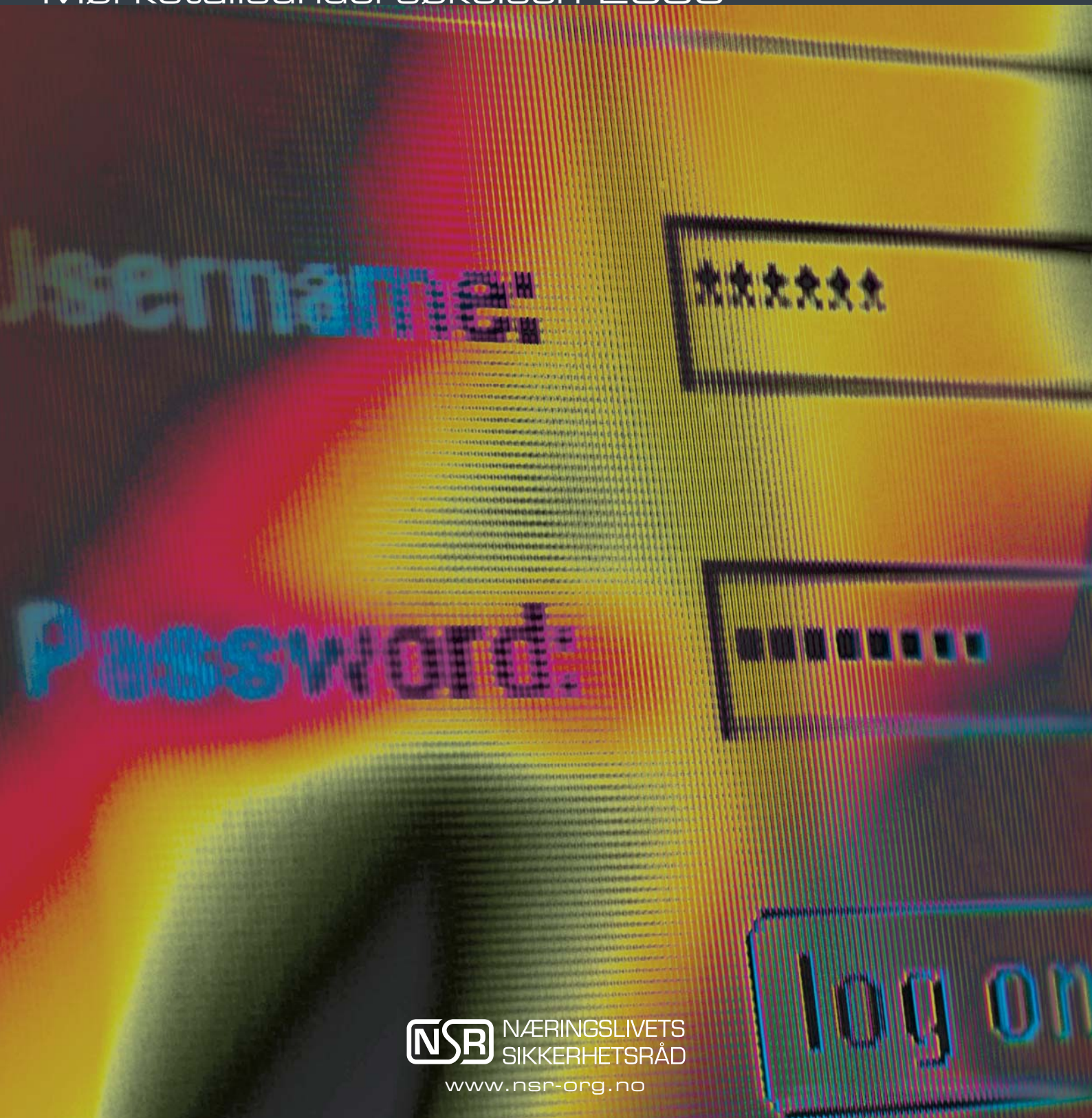
Mørketallsundersøkelsen 2006



NÆRINGSLIVETS SIKKERHETSRÅD

www.nsr-org.no

Innhold

Innledning

Dette er den 5. mørketallsrapporten som utarbeides av Datakrimutvalget (DKU) i NSR. Formålet med undersøkelsen er å belyse omfanget av datakriminalitet og andre uønskede IT-hendelser som norske virksomhet utsettes for. Offentlig statistikk forteller lite om disse forholdene, og det råder en generell oppfatning om at datakriminalitet og uønskede hendelser i liten grad anmeldes eller rapporteres til myndighetene.

Samfunnet blir i stadig større grad avhengig av IT, og trusselbildet endrer seg over tid. Vi ser en markert økning i identitetstyverier, og kompromitterte klienter og servere både hjemme og i virksomheter utnyttes av kriminelle. Det er i større grad organisert kriminalitet med økonomiske motiver som står bak. Årets undersøkelse er derfor utvidet ved at den inkluderer kartlegging av virksomhetenes bevissthet omkring informasjonssikring. Videre virksomhetens avhengighet av IT, hvilke sikringstiltak som er innført, hvorvidt IT drift er satt ut til eksterne kontraktører, og om virksomhetene anses som del av nasjonal kritisk infrastruktur.

Undersøkelsen ble gjennomført i mai 2006 ved at et postalt spørreskjema ble sendt ut til et representativt utvalg på 2000 norske virksomheter innen offentlig og privat sektor. Tidsrommet for kartleggingen var de foregående 12 måneder. I alt 749 svar ble mottatt. Forskjeller i offentlig og privat sektor er ikke belyst i rapporten slik som tidligere, da offentlig sektor denne gang kun utgjorde 5,7 % av respondentene.

Denne kortversjonen av rapporten inneholder et utvalg av resultatene som kan trekkes ut av undersøkelsen. Et avsnitt viser også hvordan Mørketallsundersøkelsen samsvarer med tilsvarende undersøkelser i andre land. Ytterligere informasjon om undersøkelsen vil være tilgjengelig på www.nsr-org.no.

Spørreundersøkelsen er gjennomført av Perduco AS og analysene er gjennomført av stipendiat Janne Hagen, Høgskolen på Gjøvik/UiO/FFI,i samarbeid med Datakrimutvalget som i 2006 består av:

- IT Sikringsleder Øyvind Davidsen, Statoil (leder)
- Direktør Kim Ellertsen, NSR
- Politiinspektør Berit Børset Solstad, KRIPOS
- Leder Tore Larsen Orderløkken, NorSIS
- Avdelingsdirektør Christophe Birkeland, NorCERT - NSM
- Ove Olsen, SINTEF
- Seniorkonsulent Arne Tjemsland, Secode Norge AS
- Jan Gusland, Komplett AS

Sammendrag

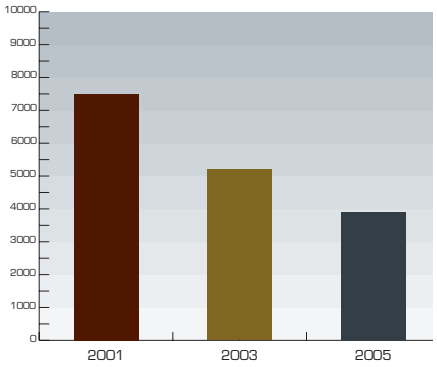
De rapporterte hendelsene domineres av virusangrep, tyveri av utstyr og misbruk av IT ressurser. I alle disse kategoriene er manglende bevissthet hos sluttbrukere avgjørende for at hendelsene skjer. Mens virksomhetene er godt rustet på viktige tekniske sikringstiltak har kun 40 % av virksomhetene gjennomført opplæring av ansatte i sikker bruk av IT.

I de tilfellene hvor gjerningsmann er identifisert er bortimot halvparten egne ansatte eller innleid personell. Det er utvalgets oppfatning at holdninger og bevisstgjøring av brukere er vel så viktig som teknisk sikringstiltak. Undersøkelsen viser for øvrig at kun 40 % av bedrifter med under 200 ansatte har krav til sikkerhet i avtaler med tjenesteleverandør ved utkontraktering av IT-drift.

Sett i lys av antall tyverier er det verdt å legge merke til at kun 11 % av virksomhetene krypterer bærbart utstyr.

Basert på opplysninger i undersøkelsen og SSBs statistikk over næringsstrukturen i Norge, er det estimert at norske virksomheter ble utsatt for nærmere 3900 datainnbrudd i perioden. Tallmaterialet viser at omtrent like mange virksomheter er utsatt for datainnbrudd, men at de opplever færre tilfeller. Resultatet står fremdeles i sterk kontrast til politiets statistikk som kun viser 61 anmeldelser i denne kategorien. Tilsvarende har vi estimert 8900 tilfeller av misbruk av IT-ressurser, der kun 11 anmeldelser er registrert.

Antall datainnbrudd



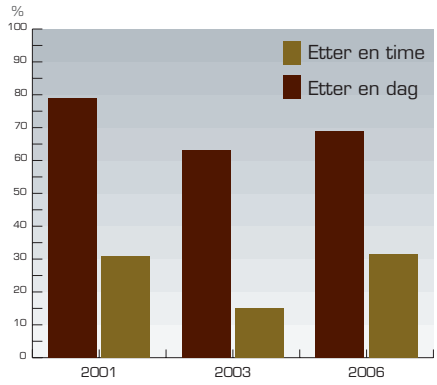
Konklusjonen er at mørketallene fremdeles er store når det gjelder datakriminalitet. Dette bekreftes også i internasjonale undersøkelser.

Om lag hver tredje virksomhet vet ikke om de har hatt uønskede hendelser. Dette i seg selv viser mangelfull fokus på sikring og sikringstiltak.

Tallene fra undersøkelsen gir et estimat på de totale kostnader knyttet til datakriminalitet for norske virksomheter til 1,8 mrd. kroner, noe som er betydelig lavere enn estimatene fra 2003. I denne perioden har det imidlertid vært en betydelig forandring i trusselbildet fra synlige trusler (virus angrep) til mindre åpenbare som for eksempel datatyveri og misbruk IT-ressurser.

Det har i de tre siste periodene vært en overraskende variasjon av virksomhetenes vurdering av egen sårbarhet (jfr. figur). Den siste økningen kan forklares med at økt bruk av internett tjenester i forretningsførselen har gjort virksomhetene mer sårbare selv for kortere driftsavbrudd.

Sårbarhet ved datainnbrudd



Datakrimutvalget mener at det er bekymringsfullt at virksomheter som anser seg selv til å være en del av kritisk infrastruktur, ikke hever seg vesentlig over andre virksomheter når det gjelder sikringsnivå.

Av 3900 datainnbrudd er kun 61 anmeldt

Hendelser

Undersøkelsen viser at 40 % av norske virksomheter ble utsatt for datakriminalitet eller andre uønskede IT-hendelser i løpet av en periode på 12 måneder. Tallet er lavere enn i 2003. Dette skyldes at undersøkelsen i 2003 også inkluderte forsøkshandlinger.

Datainnbrudd
Basert på resultatene i undersøkelsen og SSBs statistikk over næringsstrukturen i Norge, kan vi estimere at norske virksomheter ble utsatt for nærmere 3900 datainnbrudd i perioden. Dette er en fortsatt nedgang i det estimerte antallet sammenlignet med undersøkelsen i 2001 og 2003 hvor tallene var hhv. 7500 og 5200. Tallmaterialet viser at antall virksomheter som blir rammet er nokså konstant, men at antall hendelser reduseres. Resultatet står imidlertid fremdeles i sterk kontrast til politiets statistikk som kun viser 61 anmeldelser i denne kategorien.

Tilsvarende har vi estimert 8900 tilfeller av misbruk av IT-ressurser, men kun 11 anmeldelser.

Anmeldelser
Som ved tidligere undersøkelser viser Mørketallsundersøkelsen 2006 at viljen til å anmelde straffbare forhold varierer sterkt med typen kriminalitet.

Konklusjonen er at mørketallene fremdeles er store når det gjelder Datakriminalitet.

Prosentvis andel av virksomheter som er utsatt for ulike hendelser

Hendelser	2003	2006
Virus/ormer	34 %	36 %
Tyveri av IT utstyr	24 %	26 %
Misbruk av IT ressurser	8 %	9 %
Dos Angrep	6 %	5 %
Endring/sletting av data	2 %	5 %
Datainnbrudd	4 %	4 %
Spredning av ulovlig/beskyttet materiale	2 %	2 %
Datatyveri	2 %	1 %
Misbruk av kredittkort		1 %
Trusler om å angripe IT systemer		1 %

Hvor mye ble anmeldt

Type hendelse	Andel som ble anmeldt
Tyveri av IT-utstyr	73,1 %
Misbruk av IT-ressurser	7,4 %
Uautorisert endring/sletting av data	2,3 %
Datainnbrudd	1,3 %
Angrep på tilgjengelighet	0,7 %
Infeksjon av ondsinnet kode	0,1 %

For kategoriene Datatyveri, Spredning av ulovlig/ beskyttet opphavsrettslig materiale, trusler om å angripe IT-systemer og Bedrageri ved misbruk av kredittkort over internett er svarprosenten så lav at det ikke gir grunnlag for konklusjoner.

Virksomhetene er så sårbare på flere områder:

Konfiensialitet - Tyveri av verdifull eller sensitiv informasjon

Integritet - Manipulering eller feilbehandling av informasjon slik at den ikke er å stole på

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

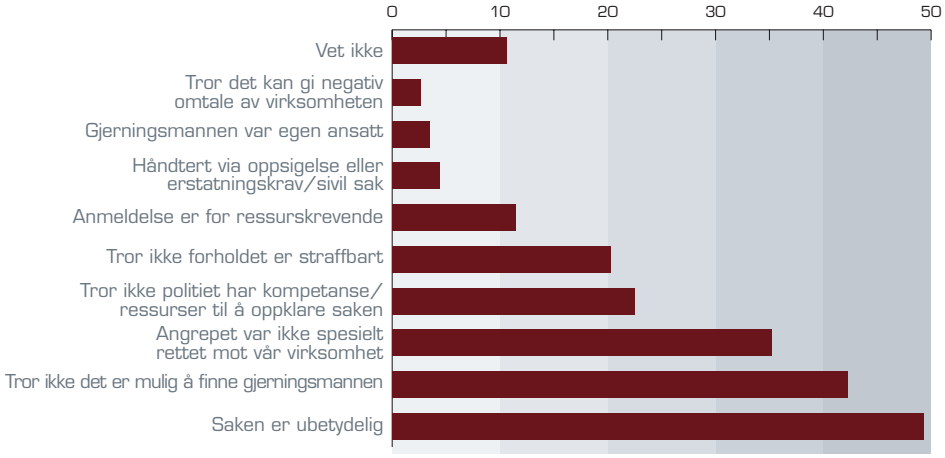
Årsaker til ikke å anmelde
Det som oftest oppgis som årsak til at forhold ikke anmeldes er at saken er ubetydelig. Videre unnlater mange å gjøre det fordi de ikke tror det vil være mulig å finne gjerningsmannen, eller at angrepet ikke var spesielt rettet mot virksomheten.

Hvem er gjerningsmannen?
I alt ble det rapportert inn 2079 hendelser. Av disse ble 401 gjerningsmenn identifisert, mao. hver fjerde hendelse identifisert.

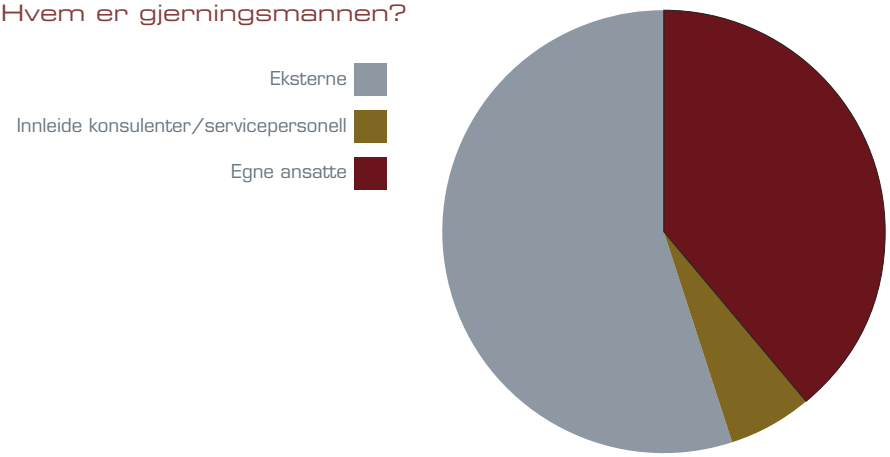
Datakrimutvalget mener en her ser to trender: Det oppdages mer, og en kan i større grad enn tidligere konkretisere hvor angrepet kommer fra, noe som er oppløftende i sikringsarbeidet. Tallene bekrefter også resultater fra andre undersøkelser som viser at trusselen fra egne ansatte øker i disse kategoriene.

Gjerningsmann blir identifisert i hver 4. hendelse

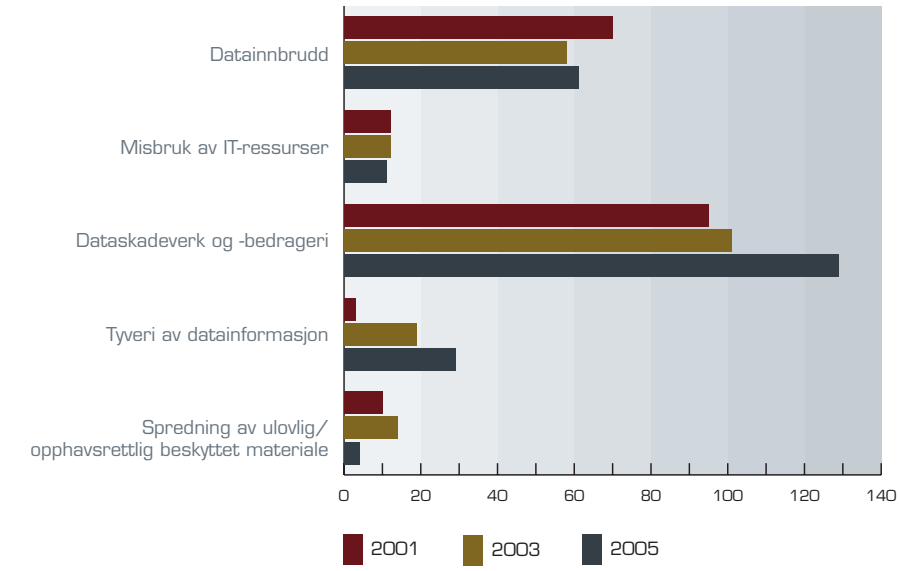
Årsaker til ikke å anmelde



Hvem er gjerningsmannen?



Antall anmeldelser av datakriminalitet (kilde: Kripos)



IT bruk – avhengighet

Norske virksomheter blir stadig mer avhengige av IT. Omtrent alle virksomhetene i undersøkelsen benytter seg av e-post, 4 av 5 har egne hjemmesider og tilsvarende andel betaler regninger/faktura elektronisk. I forhold til 2003 har elektroniske beatalinger eksplodert fra 1 til 80% og bruken av trådløse nett økt blant virksomhetene fra 30 % til 40 %.

Halvparten av virksomhetene gir kunder og eksterne samarbeidspartnere tilgang til sine systemer. Her har det bare vært en mindre økning i forhold til tidligere undersøkelser. Det har imidlertid vært en markert økning i å gi ansatte tilgang til virksomhetens systemer hjemmefra. I 2003 hadde 43 % av virksomhetene gitt ansatte tilgang til systemene, og nå er dette økt til 64 %.

Store bedrifter er raskere enn små bedrifter i å ta i bruk ny teknologi. Dette gjelder for alle teknologier. For eksempel er det bare 5 % av de minste bedriftene som bruker IP-telefoni, mens tilsvarende tall for de største er 27 %.

Ved driftsavbrudd blir 2 av 3 virksomheter hardt rammet allerede første dagen

Økning i bruk av IT

IT bruk (%andel av virksomhetene)	2003	2006
Epost	96	95,6
Hjemmeside	80	82,2
Elektronisk betaling	1	80,5
Ansatte har tilgang hjemmefra	43	64,1
Kunder/samarbeidspartnere har tilgang utenfra	46	49,3
Kjøp via internett	1	44,2
Trådløse nett (WLAN)	30	40,7
WAN mellom avd.kontor	Ingen data	39,1
Salg via Internett	9	25
Instant messenger	Ingen data	19,2
IP-telefoni	Ingen data	14,6

IT er blitt en viktig del av alle forretningsprosesser og avhengigheten synes å øke. En økende andel av virksomhetene (hver tredje bedrift) får vesentlige problemer allerede etter en times driftsavbrudd for de viktigste systemene. 2 av 3 virksomheter blir hardt rammet allerede første dagen.

Hvor fort får virksomhetene alvorlige problemer dersom systemene er utilgjengelige.

Tidsintervall	2003	2006
I løpet av 1 time	15	31,4
I løpet av 1 dag	48	37,4
I løpet av en uke	25	26,4
Mer enn en uke	5	2,8
Det ville ikke skape større problemer	5	1,4
Vet ikke	2	0,5

Beskyttelsestiltak

Tekniske beskyttelsestiltak
Mørketallsundersøkelsen 2006 bekrefter trender fra tidligere undersøkelser. Så å si alle har tatt i bruk passord og antivirusløsninger. Bruken av engangspassord øker, og vi noterer spesielt at bruken av fysiske autentiseringsmekanismer som smartkort i de største virksomhetene har doblet seg, selv om fortsatt svært få benytter seg av dette. Bruken av sikkerhetskopi er også allment utbredt, dette gjelder også små virksomheter som i større grad enn tidligere har tatt dette i bruk (fra ca 73 % i 2003 til 83 % i 2006).

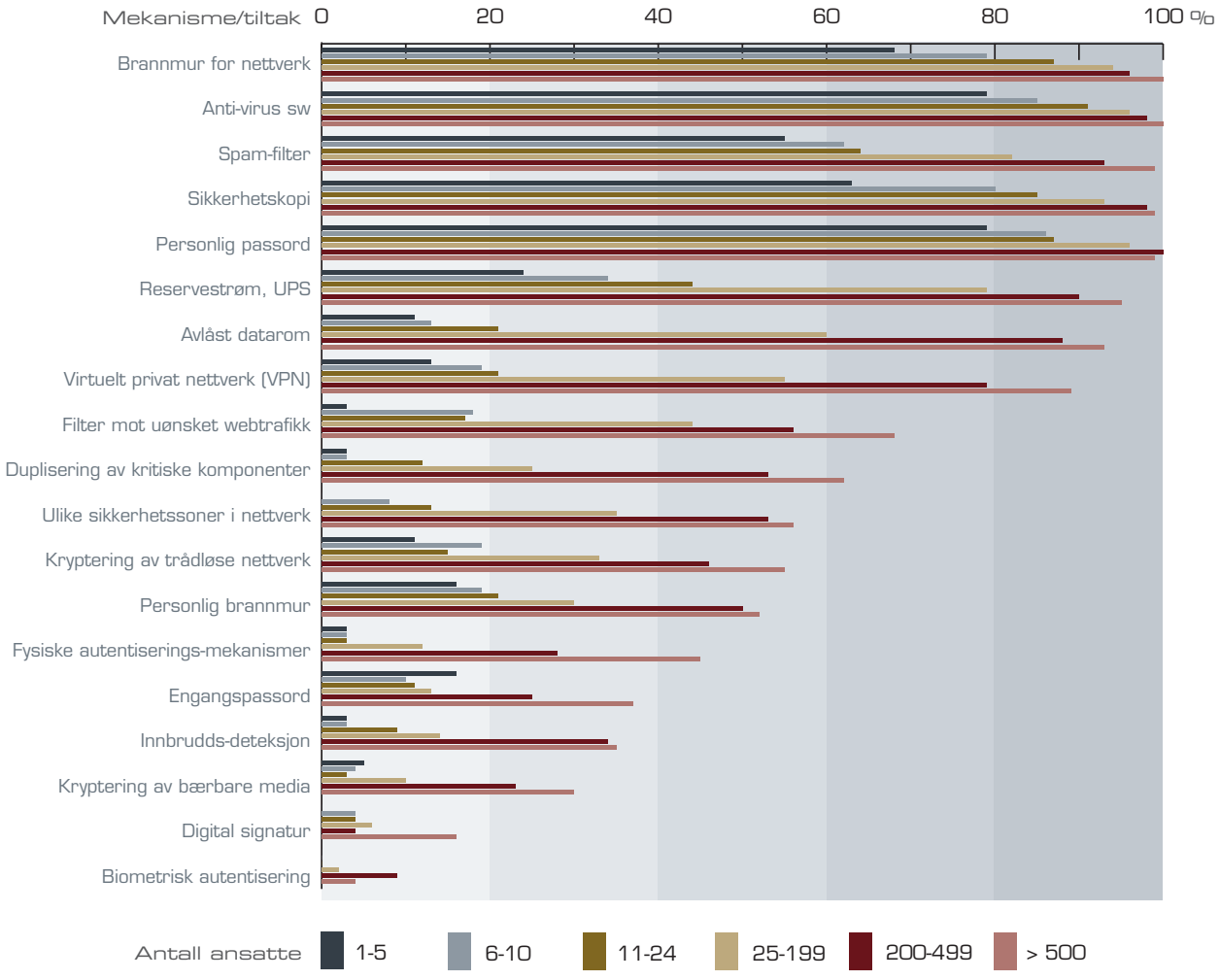
Det er verdt å merke seg at kun 11 % av virksomhetene har krypterte harddisker på bærbart utstyr, til tross for at tyveri av IT utstyr rammer hver 4. virksomhet. I 2003 påpekte Datakrimutvalget at brannmur var lite utbredt i små virksomheter. På 3 år har dette endret seg, og i dag har ca. 83 % av små virksomheter implementert brannmurer (mot ca 62 % i 2003). Datakrimutvalget påpeker samtidig behovet for vedlikehold av brannmur regelsett og gjennomgang av sikkerhetslogger. Undersøkelsen avdekker at kun 15 % av virksomhetene har prosedyrer for dette.

Bruken av sikringsteknologier som VPN og IDS øker, men det er først og fremst store virksomheter som implementerer slike sikringstiltak.

Når man ser på tekniske sikringsmekanismer er den største endringen i resultatene fra forrige undersøkelse økningen i bruken av personlige brannmurer fra ca 20 % til 31 %. Denne endringen må ses i sammenheng med utbredelsen av Microsoft Windows XP Service Pack 2, som automatisk installerer en personlig brannmur på datamaskinen.

Bruken av spam-filter er svært utbredt blant store virksomheter, mens kun 63 % av virksomheter med mindre enn 25 ansatte har tatt dette i bruk. Datakrimutvalget påpeker verdien av slike filtre, som bidrar til mer effektiv bruk av e-post og begrenser spredningen av ondsinnet kode.

Tekniske sikringstiltak – virksomhetens størrelse



Det er fortsatt et mindretall av virksomhetene som krypterer sine trådløse nettverk. Selv om informasjonen likevel kan være kryptert gjennom bruk av krypteringsprotokoller som SSL, vil ukrypterte trådløse nett øke risikoen for misbruk og datainnbrudd.

Mørketallsundersøkelsen avdekker videre at få virksomheter har duplisert kritiske komponenter i sine nettverk. Dette til tross for at duplisering av utsatte og kritiske komponenter ofte vil være en rimelig og effektiv forsikring mot avbrudd og stopp i tjenester og nettverk. Bruk av UPS og reservestrøm er utbredt blant store virksomheter, men nærmest fraværende i de små.

Vi merker oss at av de virksomhetene som har opplevd uønskede hendelser hadde 97 % anti-virusprogramvare, 86 % spam-filter og 94 % brannmur for nettverket. Dette understreker at tekniske tiltak alene ikke er nok beskyttelse i forhold til de trusler virksomhetene utsettes for.

Organisatoriske tiltak

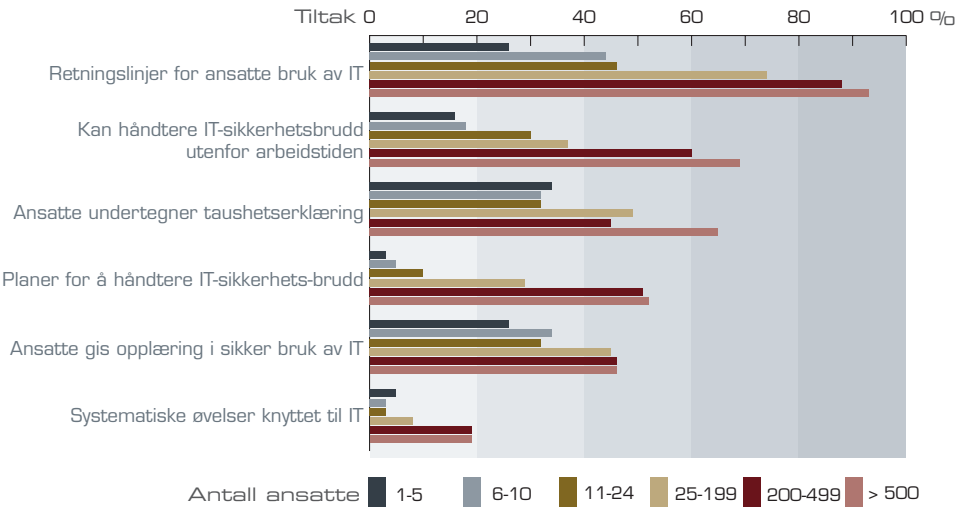
Generelt sett har bruk av organisatoriske tiltak ikke utviklet seg i tråd med virksomhetenes trusseleksponering. Blant store virksomheter har de fleste retningslinjer for ansattes bruk av IT, men bare hver fjerde blant de minste virksomhetene har det. Datakrimutvalget påpeker særlig mangelfull opplæring av ansatte i sikker bruk av IT og mangelfull forberedelse på håndtering av IT-sikkerhetsbrudd.

Risikovurdering

Risikovurdering er en forutsetning for å avdekke sårbarhet og iverksette sikringstiltak. I undersøkelsen svarer 83 % av virksomhetene at de løpende eller av og til gjør en vurdering av risiko og behov for sikringstiltak i eksisterende IT løsninger. 17 % gjør sjelden eller aldri en slik vurdering.

Når nye IT-løsninger innføres, svarer 88 % at de løpende eller av og til gjør vurdering av risiko og behov for sikringstiltak. 12 % gjør sjelden eller aldri slike vurderinger.

Organisatoriske sikringstiltak – virksomhetens størrelse



Informasjonssikring er ikke et produkt man kan kjøpe, men noe man må skape sammen i organisasjonen

Bevissthet

30 % av virksomhetene har svart at de ikke vet antallet hendelser, noe som kan tyde på at de har mangelfull håndtering av uønskede hendelser. Hele 64 % av virksomhetene har ikke hatt uønskede hendelser i de kategoriene undersøkelsen etterspør. Kun 11 % av virksomhetene har rutiner for å beregne økonomisk tap av slike hendelser.

Brukeropplæring

Hendelsene domineres av virus/orm angrep (36 %), tyveri av utstyr (26 %) og misbruk av IT ressurser (9 %). I alle disse tilfellene er manglende bevissthet hos sluttbrukere avgjørende for at hendelsene skjer: Privat internettbruk, åpne vedlegg i e-post fra ukjent/tvilsomt opphav, manglende sikring/innlåsing av bærbart utstyr, etc. Kun 40 % av bedriftene har imidlertid gjennomført opplæring av ansatte i sikker bruk av IT.

Sammenhenger

Forhold omkring virksomheters størrelse

Desto større virksomhetene er desto mer avhengige er de av IT.

2/3 av virksomheter med over 200 ansatte får vesentlige problemer ved driftstans i 1 dag. Hver fjerde får problem ved driftstans i en time. Større bedrifter har også tatt i bruk flere IT baserte tjenester. Et unntak her er faktura og elektroniske betalinger som er mest utbredt blant mellomstore bedrifter (11 - 24 ansatte 91 % og 25 -199 ansatte 81 %).

Desto større virksomhetene er desto høyere er sikringsnivået.

Dette er gjennomgående når det gjelder tekniske tiltak. Men selv i større virksomheter som er sterkt avhengige av IT er det mangelfulle beredskapstiltak. Kun halvparten av store virksomheter med flere enn 500 ansatte har planer for håndtering av brudd på IT-sikkerheten, og kun 2 av 10 virksomheter gjennomfører systematiske øvelser knyttet til IT.

Desto større virksomhetene er desto mer utsatt er de for datakriminalitet.

Dette gjelder både tyveri av ustyr, datainnbrudd, uautorisert endring av data, tjenestenekt-angrep, datatyveri og virus/ormer. Dette henger sammen med at risikoen øker med aktivitetsnivå og antall aktører (brukere). Videre antas det at større selskaper er mer profilerte og mer utsatt for økonomisk kriminalitet. Mindre virksomheter med lavere sikringsnivå vil ofte ikke være i stand til å avdekke hendelser og dermed antakelig være underrepresentert mht. identifiserte hendelser.

Ekstern tilgang til virksomhetens nett

Egne ansatte

Resultater fra undersøkelsen viser at de virksomheter som gir sine ansatte tilgang til systemene hjemmefra også er de som i størst grad benytter ulike sikringstiltak. De tilbyr også opplæring og har planer/systemer for håndtering av sikkerhetsbrudd i og utenom arbeidstiden.

Sikringstiltak i virksomheter som gir ansatte tilgang hjemmefra til interne IT-systemer

Sikringstiltak	Tilgang (%)	Ikke tilgang (%)
Ansatte gis opplæring i sikker bruk av IT	45	30,5
Planer for brudd på IT-sikkerheten	33,8	11,2
Håndterer IT-sikkerhetsbrudd utenom arbeidstid	49,2	19,3
Personlig passord	97,2	82,2
Brannmur for nettverket	97,5	75,5
IDS	22,1	4,8
Ulike sikkerhetssoner i nettet	39,6	10,4
Kryptering av bærbare media	15,2	4,8
VPN	66,7	12,6

Sikringstiltak i virksomheter som gir kunder, samarbeidspartnere tilgang til interne IT-systemer

Sikringstiltak	Tilgang (%)	Ikke tilgang (%)
Kontraktsfestet ansvar	30,2	14,2
Planer for håndtering av IT sikringsbrudd	35,2	16,9
Personlig passord	96,2	89,5
Brannmur for nettverket	97	83,6
IDS	20,8	11,5
Ulike sikkerhetssoner i nettet	42,9	16,4
Kryptering av bærbare media	14,5	8,6
VPN	66,4	29,5
Håndterer IT-sikkerhetsbrudd utenom arbeidstid	46,2	31,9

Selv i store organisasjoner mangler halvparten planer for å håndtere brudd på IT-sikkerheten

Kritisk infrastruktur
Begrepet kritisk infrastruktur har fått betydelig oppmerksomhet både nasjonalt og internasjonalt de siste årene. Dette har sammenheng med økende fokus på samfunnets sårbarhet og omfatter virksomheter hvis bortfall av deres tjenester vil få akutt og kritisk følge for store deler av samfunnet.

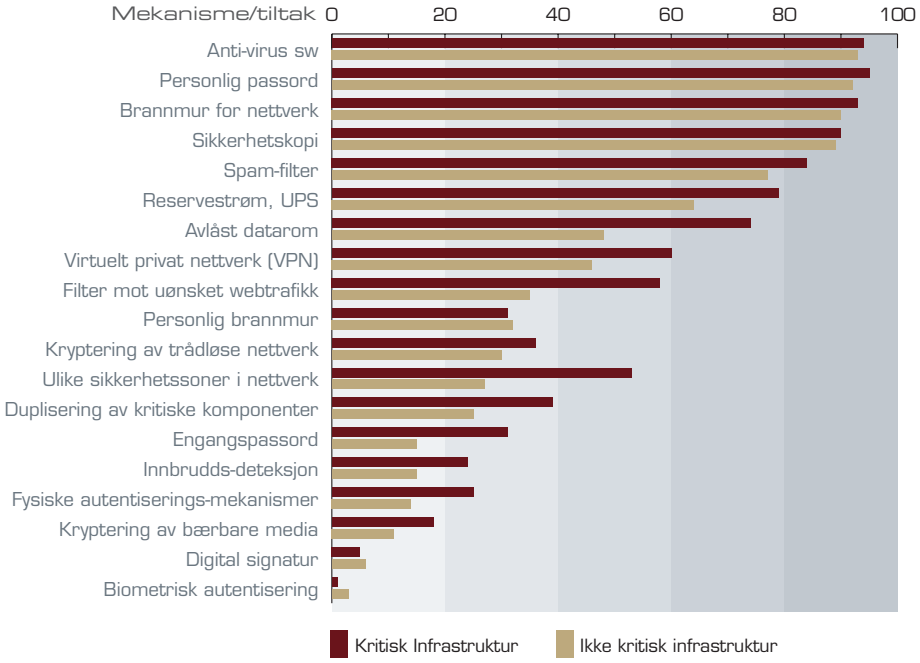
11 % av virksomhetene oppgir at de anser seg for å være en del av kritisk infrastruktur. Disse virksomhetene oppgir også en større sårbarhet ved at 40 % mener de får alvorlige problemer innen 1 time dersom viktige IT systemer er ute av drift. For øvrige virksomheter er denne andelen 30 %.

Ser vi på tiltak, er det på noen områder et fornuftig samsvar mellom sårbarheten og sikringsnivå. Dette gjelder både organisatoriske og tekniske tiltak. Men det avdekkes også flere overraskende forhold:

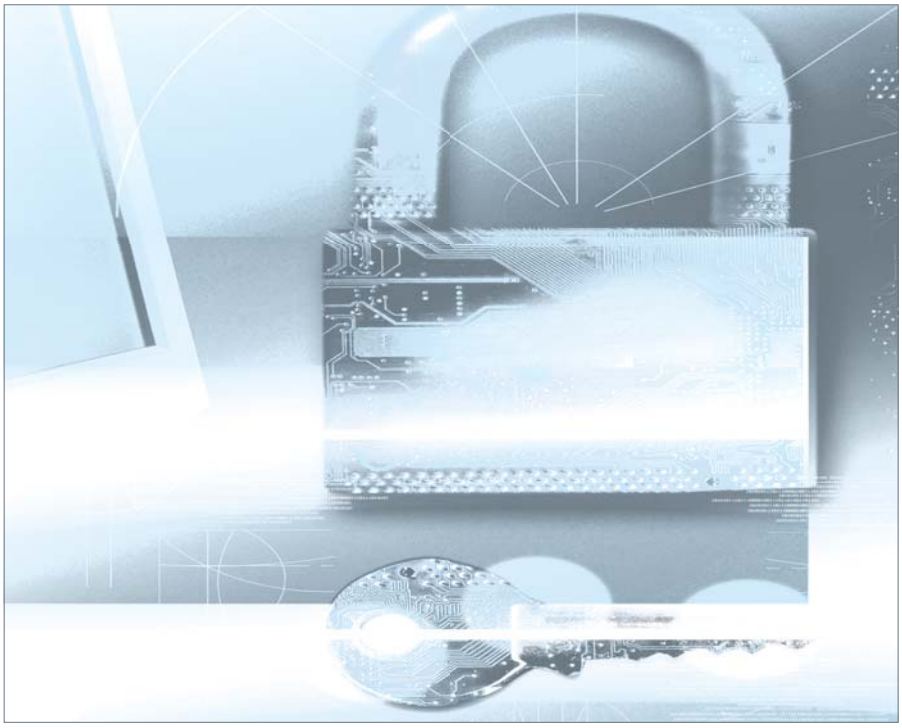
- Mer enn halvparten mangler opplæringsprogram i sikker bruk av IT
- 6 av 10 mangler planer for håndtering av brudd på IT-sikkerheten
- 8 av 10 gjennomfører ikke øvelser knyttet til IT (katastrofeøvelser)
- 4 av 10 er ikke i stand til å håndtere brudd på IT sikkerhet utenom arbeidstiden

Datakrimutvalget vil ellers påpeke at 6 % av små virksomheter (<25 ansatte) anser seg som del av nasjonal kritisk infrastruktur. Majoriteten av norske foretak har mindre enn 25 ansatte. Det tyder på at det er behov for at myndighetene klargjør begrepet kritisk infrastruktur, og i samsvar med dette pålegger relevante krav til IT sikring.

Sikringstiltak – kritisk infrastruktur



Det er bekymringsfullt at virksomheter som anser seg som en del av kritisk infrastruktur har så mangelfulle sikringstiltak.



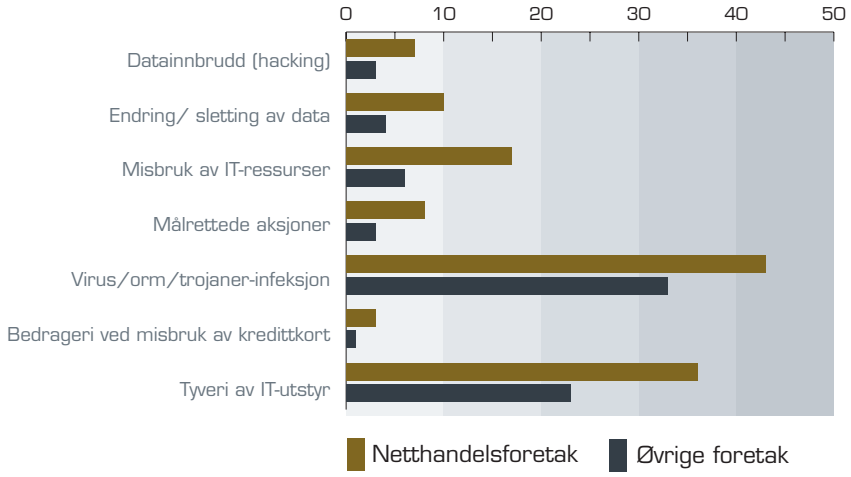
Netthandel

Stadig flere virksomheter benytter internett for salg av varer og nettbaserte tjenester. Andelen har økt fra 9 % ved forrige undersøkelse til 25 % ved denne undersøkelsen. Netthandelsvirksomhetene legger generelt sett mer vekt på sikringstiltak enn de andre. Dette er gjennomgående for alle typer sikringstiltak.

76 % av virksomhetene svarer at de vil få problemer i løpet av 1 dag dersom de viktigste IT-systemene er ute av drift. Til tross for dette svarer bare 52 % at de kan håndtere sikkerhetsbrudd utenfor arbeidstid. Det kan derfor stilles spørsmål om netthandelsvirksomhetene virkelig har tatt inn over seg at netthandel er en 24/7 tjeneste.

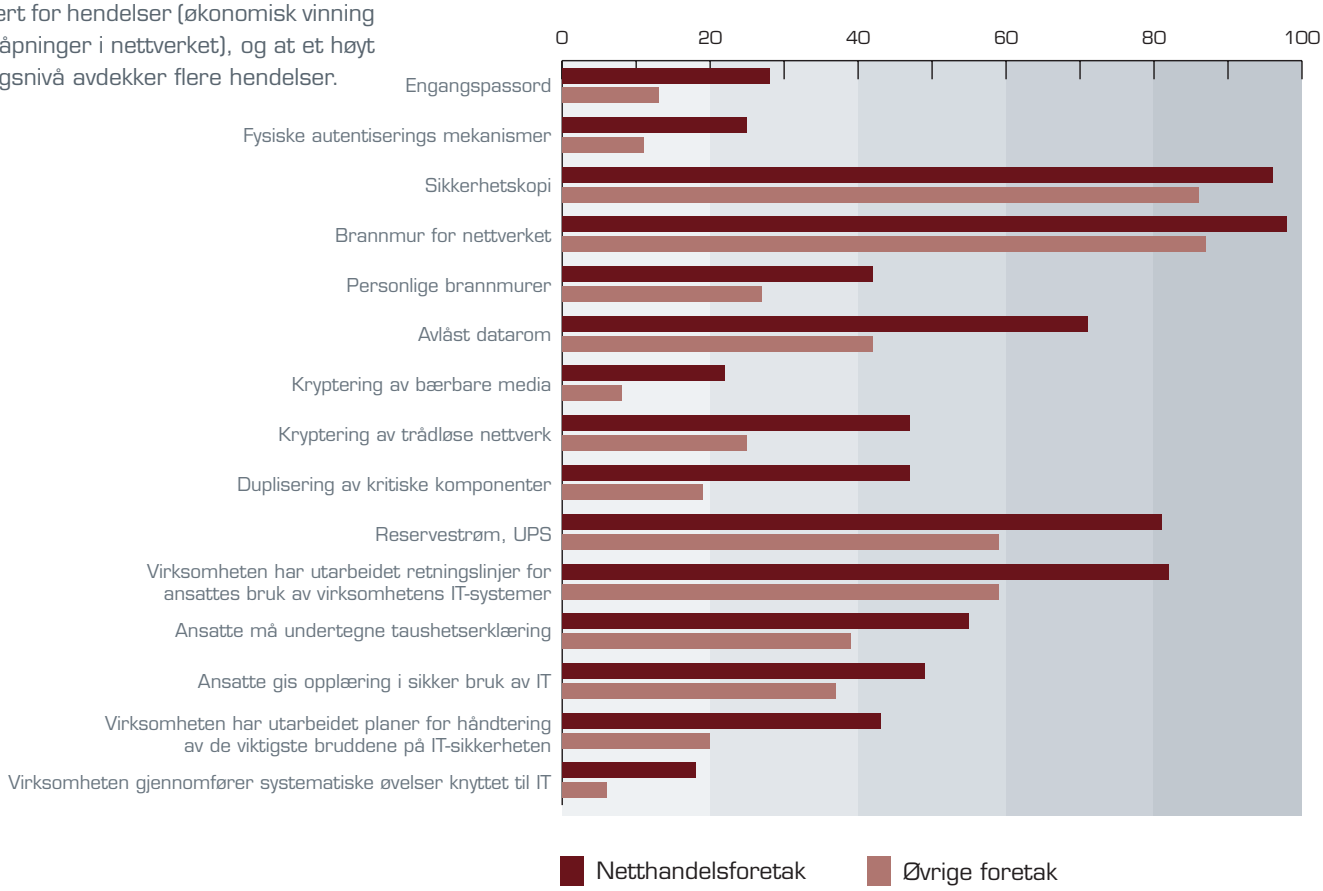
Mørketallsundersøkelsen viser at selv om netthandelsvirksomhetene har mer fokus på sikringstiltak har de likevel hatt flere hendelser. Forklaringen til dette kan være at virksomhetene er mer eksponert for hendelser (økonomisk vinning - har åpninger i nettverket), og at et høyt sikringsnivå avdekker flere hendelser.

Hendelser i netthandelsforetak



Det kan stilles spørsmål om netthandelsvirksomhetene virkelig har tatt innover seg at netthandel er en 24/7 tjeneste

Sikringstiltak i netthandelsforetak



Outsourcing
40-60 % av virksomhetene (avhengig av størrelse) har satt bort hele eller deler av IT-driften. Hvordan er sikkerheten ivaretatt i når man setter ut driften?

Sikringskrav i kontrakter
Når det gjelder krav til tekniske tiltak og rutiner, herunder tilgangskontroll, mangler snaut halvparten av virksomhetene med færre enn 200 ansatte slike krav i kontraktene. For virksomheter med over 200 ansatte mangler hver 5. virksomhet slike krav.

Hver tredje av virksomhetene med 25-199 ansatte mangler krav til tilgjengelighet/oppetid overfor driftspartner. For større virksomheter er det kun ca 10 % som mangler slike krav.

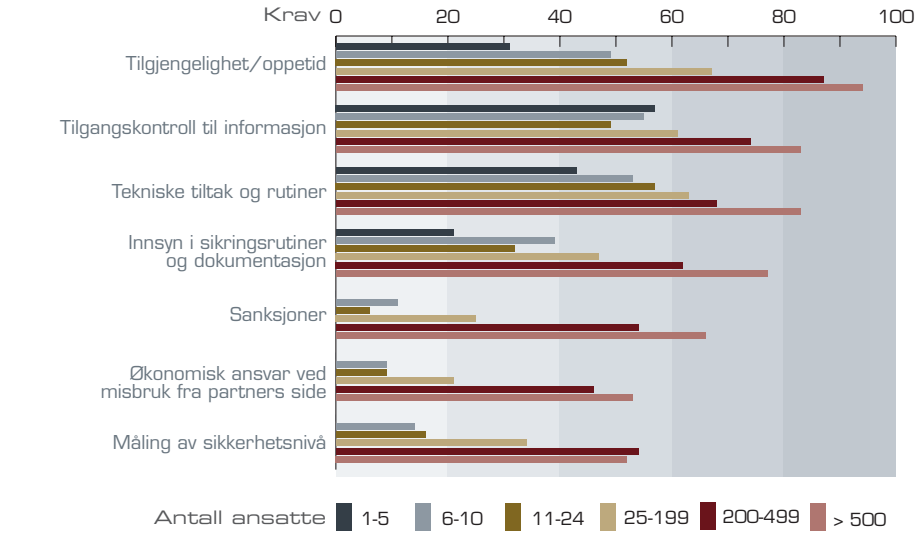
Når det gjelder kontroll av driftspartner mangler hver fjerde av større bedrifter (200+) krav til innsyn i driftpartners sikringsrutiner og dokumentasjon. Kun havparten har krav om måling av sikringsnivå.

Ca. halvparten av større bedrifter mangler rett å innføre sanksjoner eller har kontraktsfestet økonomisk ansvar fra driftspartner dersom misligheter skjer.

Sett i lys av hvor sårbare virksomhetene er, er det betenkelig at krav til sikkerhet ofte mangler i driftsavtalene. Datakrimutvalget ønsker å påpeke at outsourcing av IT-drift kan utgjøre en sikkerhetsrisiko når krav til sikring ikke spesifiseres i kontrakten.

De foretak som setter ut driften beskriver i undersøkelsen et sikringsnivå som ikke er signifikant høyere enn for virksomheter som drifter selv. Det er et tankekors at virksomheter som har IT-drift som kjernevirksomhet tilsynelatende ikke har et høyere sikringsnivå enn virksomheter forøvrig.

Sikringskrav i kontrakter



Sett i lys av hvor sårbare virksomhetene er, er det betenkelig at krav til sikkerhet ofte mangler i driftsavtalene.

Norge i forhold til andre land

I siste tiårsperiode har en rekke land gjennomført tilsvarende undersøkelser som Mørketallsundersøkelsen. De mest relevante er:
CSI/ FBI: Computer crime and security survey (2005)
FBI: 2005 Computer crime survey
DTI (England): Information security breaches survey 2006.
AUSCERT (Australia): Computer crime and security survey 2006.
SITIC: Mørketallsundersøkelse i Sverige 2005.

Hendelser
Det synes å være en trend i alle undersøkelsene at antallet virksomheter som har hatt sikkerhetshendelser reduseres. Videre at antallet hendelser hos den enkelte virksomhet øker. Detter står i kontrast til Mørketallsundersøkelsen som konkluderer med at i Norge er antall virksomheter som utsettes nokså konstant mens antall hendelser i det enkelte foretak er redusert.

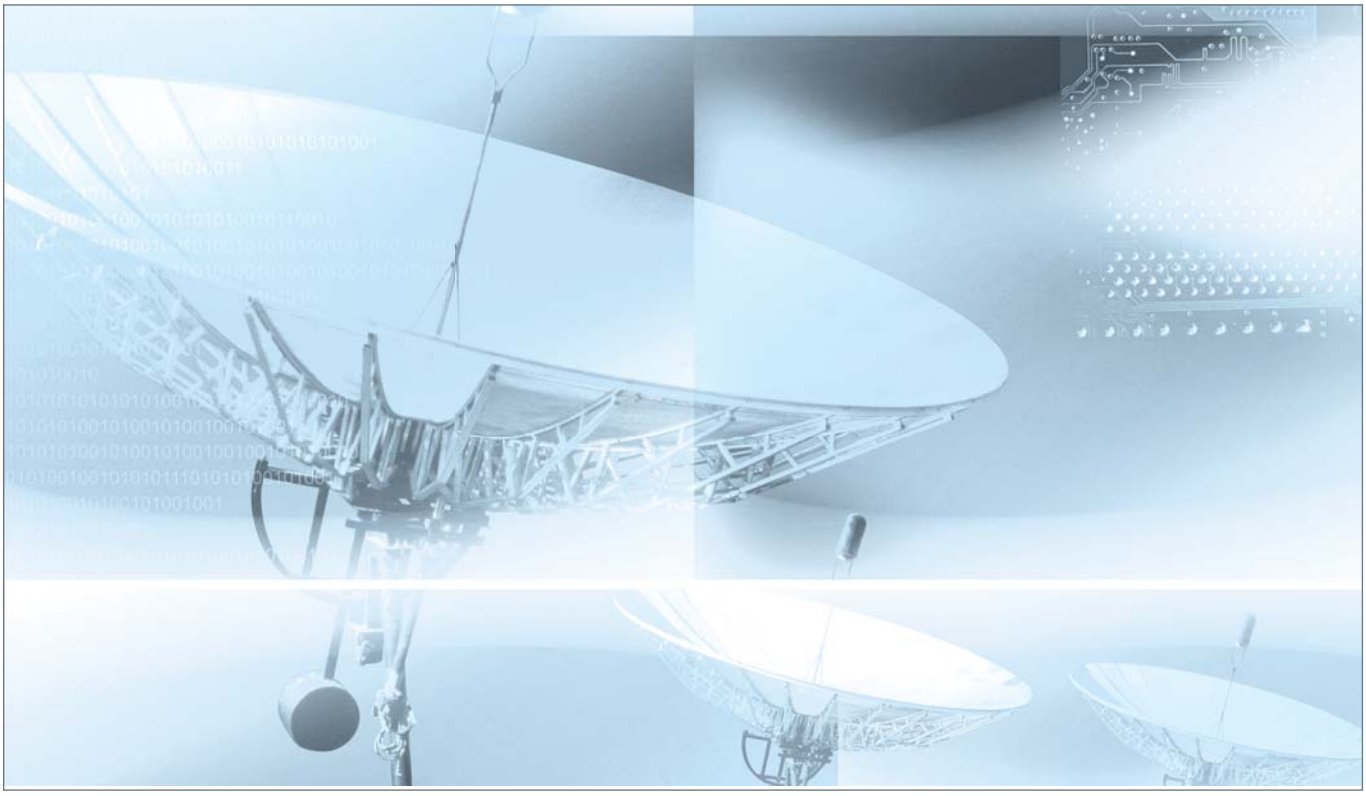
Internasjonale rapporter viser også en bevegelse i mønsteret av hvem som utøver hendelsene. For mindre virksomheter er det nå to tredjedeler som oppgir at utøver er ekstern. Store virksomheter har en mer lik fordeling intern/ ekstern.

Mørketallsundersøkelser har i alle år vist at det er veldig få virksomheter som anmelder sine sikkerhetshendelser. Det samme forholdet ser vi også i Sverige hvor kun 4 % av hendelsene er anmeldt. Også andre land melder om nedgang i andel anmeldelser.

Tiltak
Samtlige undersøkelser viser at tekniske sikringstiltak har hatt en positiv vekst og er for flere områder optimal i dag. Norge skiller seg negativt ut på noen områder. Spesielt synes det som bruk av VPN (virtuelt privat nettverk) og bruk av IDS (innbruddsdetekteringssystem) er dårligere enn i utlandet.

Kostnader
Utenlandske undersøkelser viser høyere kostnader pr. hendelse enn i Norge. I utlandet ser vi også at store virksomheter har større kostnader pr. hendelse enn mindre virksomheter. Det framgår ikke klart av undersøkelsene hva som inngår i kostnadsbegrepet.

Begrunnelse for ikke å anmelde
Gjennom undersøkelsene som er gjennomført i Norge er det en svært liten andel som oppgir at hensynet til dårlig omdømme for virksomheten er grunn til ikke å anmelde saken. I undersøkelser fra andre land blir dette oppgitt som årsak i over 50 % av tilfellene. Ja, selv i Sverige i 2005 var det i 37 % av tilfellene begrunnet med frykt for dårlig omdømme.



Mørketallsundersøkelsen for 2006 er utarbeidet med støtte fra Telenor og Fornyings- og administrasjonsdepartementet (FAD).

telenor

FORNYINGS- OG ADMINISTRASJONSDEPARTEMENTET

Næringslivets Sikkerhetsråd takker for støtte og engasjement.