Mørketallsundersøkelsen 2008
- IT-sikkerhet og datakriminalitet

NSR, STATOILHYDRO, NorSIS, KRIPOS, NSM, SINTEF, SECODE

NÆRINGSLIVETS SIKKERHETSRÅD

Innhold

1 Innledning

Dette er den 6. utgaven av mørketallsundersøkelsen utarbeidet av Datakrimutvalget i Næringslivets Sikkerhetsråd. Formålet med undersøkelsen er å belyse omfanget av datakriminalitet og andre uønskede IT-hendelser som norske virksomheter er utsatt for. Undersøkelsen omfatter også hvilke sikringstiltak norske virksomheter gjennomfører med tanke på å sikre sine IKT-systemer og sin informasjon.

Trusselbildet knyttet til informasjonssikkerhet er i stadig endring, og økonomisk motivert kriminalitet utgjør en økende andel av dette bildet. Norske virksomheter er stadig mer avhengig av IKT-systemer, og informasjon inngår i stadig større grad som en del av virksomhetenes verdier. Med dette som bakgrunn gir undersøkelsen et bilde av hvilke hendelser norske virksomheter er utsatt for samt hvilke sikringstiltak virksomhetene har iverksatt.

Undersøkelsen ble gjennomført i april 2008 og for første gang er undersøkelsen gjennomført elektronisk over Internet. Tidsrommet for kartleggingen var 2007. Et representativt utvalg på 5000 norske virksomheter innen offentlig og privat sektor har mottatt undersøkelsen, og 864 av disse besvarte den. Dette er en økning i antall respondenter på 15 % fra 2006. Mørketallsundersøkelsens svarprosent er den høyeste blant tilsvarende undersøkelser som Datakrimutvalget kjenner til.

Denne rapporten inneholder et utvalg av resultatene som kan trekkes ut av undersøkelsen. Ytterligere informasjon om undersøkelsen vil være tilgjengelig på www.nsr-org.no.

Spørreundersøkelsen er gjennomført av Perduco AS og analysen er gjennomført av Datakrimutvalget som i 2008 består av:

- Øyvind Davidsen, IT sikringsleder Statoil (Leder)
- Berit Børset Solstad, politiinspektør KRIPOS
- Tore Larsen Orderløkken, leder av NorSIS
- Christophe Birkeland, assisterende direktør (fg.) Nasjonal sikkerhetsmyndighet
- Arne Tjemsland, seniorkonsulent Secode Norge AS
- Astri Vik, IT sikkerhetssjef SINTEF
- Kim Ellertsen, direktør NSR

Sammendrag

Undersøkelsen viser at 1/3 av virksomhetene var utsatt for datakriminalitet i 2007. Av totalt 4.400 estimerte datainnbrudd er kun 57 anmeldt til politiet. Dette viser at vi fremdeles har store mørketall, og at det er en utfordring å få virksomhetene til å anmelde slike forhold. Undersøkelsen viser også at det er grunn til å tro at virksomhetene (særlig de mindre) ikke er klar over at de er utsatt for hendelser. Større virksomheter som har sikkerhetsansvarlig eller IT leder rapporterer flere hendelser, og har også gjennomført flere sikringstiltak, som ofte er en forutsetning for å oppdage hendelser. Datainnbrudd, trojanere samt misbruk av IT ressurser krever tiltak og kompetanse for å bli oppdaget.

Det som kjennetegner dagens informasjonssamfunn er at virksomhetenes informasjon ikke lenger bare ligger på sentrale servere, men er i stor grad kopiert til bærbare enheter og lagringsmedia.

Undersøkelsen slår fast at tyveri av datautstyr er den desidert vanligste formen for datakriminalitet, og at slike hendelser anmeldes mye oftere enn andre. Det er derfor bekymringsfullt at kun hver 5. virksomhet krypterer informasjonen på bærbare enheter. Krypteringsteknologi er tilgjengelig, men virksomhetene har ikke tatt denne risikoen inn over seg i tilstrekkelig grad.

Når det gjelder avhengighet og bruk at IKT vil 2 av 3 virksomheter få store problemer dersom sentrale IT-systemer er ute av drift i mer enn 1 dag. Vi ser at bruken av internett i forretningsvirksomheten øker og bruken av elektroniske betalingsløsninger har økt fra 1 % til 90 % de siste fire årene. Hver 3. virksomhet opplyser at de benytter Internett til salg av varer og tjenester. Disse virksomhetene opplever også flere hendelser enn andre. På den tekniske siden ser vi en sterk vekst i bruken av trådløse nettverk - WLAN, IP telefoni og lynmeldinger.

Et resultat av teknologiutviklingen er at grensene mellom arbeid og privatliv viskes ut, også i mindre virksomheter. Denne utviklingen er utfordrende for virksomhetenes IT-sikkerhet både når det gjelder retningslinjer for bruk, og sikring av mobilt datautstyr og nettverk. Vi ser at innføring av tekniske tiltak er økende, mens organisatoriske tiltak ikke har samme utvikling. Opplæring av brukere og beredskapstiltak er eksempler på områder som fortsatt har betydelig forbedringspotensial. Datakrimutvalget mener det er viktig at virksomhetene fortsatt har fokus på sikringsarbeidet, og i større grad også prioriterer organisatoriske tiltak.

Nytt i denne undersøkelsen er en kartlegging av virksomhetenes håndtering av personopplysninger. Det er verdt å merke seg at 4 av 5 virksomheter kjenner til personopplysningsloven, mens bare halvparten følger den. Vi er nå i en tid der ID-tyveri og misbruk av personopplysninger er sterkt økende. Datakrimutvalget mener derfor at det er et klart behov for økt aktivitet innen dette området både fra sentrale myndigheter og det private næringsliv.

Resultatet fra undersøkelsen bekrefter det vi har sett tidligere – at virksomheter i liten grad stiller krav til outsourcing partner.

Generelt sett varierer resultatene relativt lite mellom offentlig og privat sektor.

Undersøkelsen viser at sikringsnivået varierer mellom bransjene. Bransjene varehandel, hotell og restaurant synes å ha minst fokus på informasjonssikkerhet. Tallene viser at bransjer som undervisning, helse/sosial og personlig tjenesteyting har for liten fokus på sikkerhetskrav ved ekstern drift. Også når det gjelder krav til taushetserklæringer er det stor forskjell mellom de private (52 %) og de offentlige (76 %). Innen bransjen undervisning, helse/ sosial og personlig tjenesteyting er det 36 % som ikke krever at taushetserklæring undertegnes, noe som er alvorlig da disse håndterer store mengder personopplysninger.

På den positive siden viser undersøkelsen at innføringen av sikkerhetstiltak øker og forskjellen mellom store og små virksomheter avtar. Viktige sikringstiltak som bruk av passord, sikkerhetskopiering, antivirus og brannmur er nå på plass i så å si alle virksomheter. Det er også en klar trend at stadig flere virksomheter innfører ytterligere sikringstiltak. Selv med mange tiltak på plass viser undersøkelsen at antall rapporterte hendelser øker. Den økte bruken av IKT i virksomhetene kan være med på å forklare dette.

1/3 av virksomheter var utsatt for datakriminalitet i 2007.

2. Hendelser og mørketall

2.1 Hendelser

Undersøkelsen viser at 33 % av norske virksomheter ble utsatt for datakriminalitet i løpet av 2007. Den viser også at andelen av virksomheter som utsettes for ulike typer av datakriminalitet holder seg svært stabilt.

Hendelser – Prosentvis av antallet virksomheter	2003	2006	2008
Datainnbrudd (hacking)	4 %	4 %	3 %
Datatyveri (uautorisert lesing/ kopiering av informasjon)	2 %	1 %	2 %
Uautorisert endring/sletting av data	2 %	5 %	4 %
Misbruk av IT-ressurser	8 %	9 %	9 %
Spredning av ulovlig/opphavsrettlig beskyttet materiale	2 %	2 %	3 %
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten	6 %	5 %	4 %
Trusler om å angripe IT-systemer	-	1 %	0 %
Bedrageri ved misbruk av kredittkort over internett	-	1 %	2 %
Tyveri av IT-utstyr	24 %	26 %	24 %

2.2 Mørketall for datainnbrudd og misbruk av IT-ressurser

Mørketall for datakriminalitet er differansen mellom den anmeldte kriminaliteten som fremkommer i myndighetenes statistikker og den kriminaliteten som virksomhetene faktisk blir utsatt for. I undersøkelsen ble virksomhetene blant annet bedt om å oppgi antall hendelser de ble utsatt for av type «datainnbrudd» og «misbruk av IT-ressurser». Basert på opplysninger fra undersøkelsen og SSBs statistikk over næringsstrukturen i Norge har vi estimert at norske virksomheter totalt ble utsatt for nær 4.400 datainnbrudd i perioden. Dette er på samme nivå som i forrige undersøkelse. Til sammenligning har politiet i den samme perioden bare registrert 57 anmeldelser av datainnbrudd som er like lavt som ved forrige undersøkelse.

Tilsvarende har vi estimert nær 15.500 tilfeller av misbruk av IT-ressurser. Dette er en stor økning fra undersøkelsen i 2006, hvor tilsvarende tall var 8.900. I samme periode har politiet kun registrert 23 anmeldelser av slik kriminalitet.

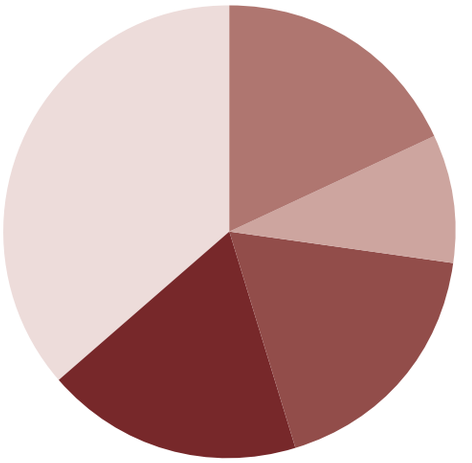
Årets undersøkelse bekrefter tidligere funn som viser at mørketallene innen datakriminalitet er store. Virksomhetenes vilje til å anmelde er liten, og totalt sett er bare 14 % av hendelsene anmeldt. Når det gjelder datainnbrudd som er en hendelse som kan medføre store problemer og tap for virksomhetene, anmeldes så lite som 0,4 % av tilfellene.

Tyveri av utstyr blir i større grad anmeldt, noe Datakrimutvalget mener kan skyldes krav fra forsikringsselskapene. For alle de andre kategoriene er anmeldelsesprosenten svært lav. For å forebygge IT-kriminalitet oppfordrer Datakrimutvalget virksomhetene til i større grad å anmelde hendelser.

2.3 Årsaker til ikke å anmelde

Den hyppigste årsaken til at et forhold ikke anmeldes, er at saken er ubetydelig eller at fornærmede anser det for å være umulig å finne gjerningsmannen. Det er så å si ingen som oppgir at de unnlater å anmelde forhold av frykt for at det kan skade omdømmet, noe som står i kontrast til resultatet i utenlandske undersøkelser.

Årsaker til ikke å anmelde

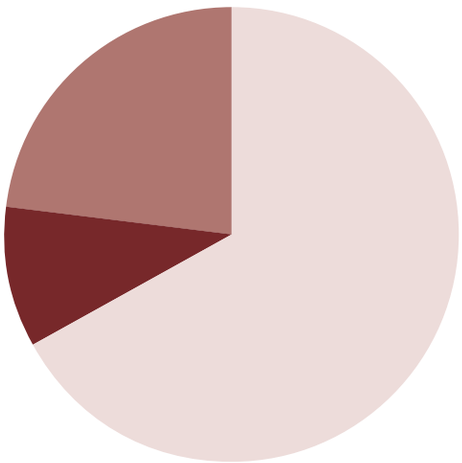


Annet	18%
Ikke spesielt rettet mot virksomheten	9%
Ikke straffbart	18%
Ikke mulig å finne gjerningsmannen	18%
Saken er ubetydelig	37%

2.4 Hvem er gjerningsmannen?

Virksomhetenes egne ansatte og personer de har leid inn blir i økende grad pekt ut til å stå bak datakriminaliteten. Det ble i undersøkelsen rapportert inn til sammen 2.958 hendelser. I disse var gjerningsmannen identifisert som en egen ansatt eller en person som var innleid i virksomheten i hele 1.751 tilfeller. Dette bekrefter tendensen en har sett i tidligere undersøkelser som viser at trusselen fra egne ansatte øker.

Antatt gjerningsmann



Egen ansatt	67%
Ekstern	23%
Innleid	10%

I 3 av 4 hendelser er gjerningsmannen en intern medarbeider.

3. Avhengighet av IT

3.1 Bruk av IT

Undersøkelsen viser at så godt som alle virksomheter har e-post og hjemmeside på Internett. Enkelte bruksområder har hatt en eksplosiv utvikling. Et eksempel er andelen av virksomheter som har tatt i bruk elektroniske betalingsløsninger som har økt fra 1 % til 90 % på 4 år. Anvendelse av informasjonsteknologi får på generelt grunnlag stadig større utbredelse, som f eks WAN , kjøp over Internett og tilgang til virksomhetens datasystemer hjemmefra. Hele 78 % av virksomheter gir nå ansatte mulighet for tilgang til IT-systemene hjemmefra. For de største virksomhetene gir 92 % slik tilgang.

Datakrimutvalget fremhever også at bruken av sanntidstjenester som IP-telefoni og lynmeldinger øker kraftig og medfører nye sikkerhetsutfordringer for virksomhetene. 3 av 10 virksomheter bruker nå IP-telefoni, noe som er en fordobling fra 2006. Bruken av lynmeldinger (Instant Messaging) benyttes av nærmere 1/3 av virksomhetene. I private virksomheter er lynmeldinger omtrent 50 % mer utbredt enn i det offentlige.

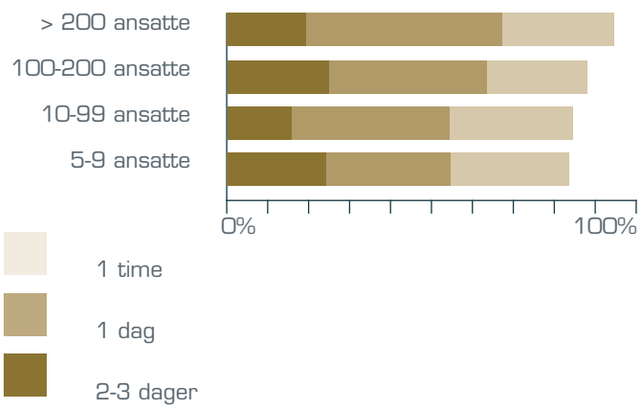
Også e-postløsninger for mobiltelefon har stor utbredelse, og 69 % av de store virksomhetene tilbyr nå e-post løsninger for mobiltelefon. Mobiltelefoner er ofte usikre og Datakrimutvalget mener dette er en sikkerhetsutfordring.

Teknologiutviklingen viser tydelig at grensene mellom arbeid og privatliv viskes ut. Dette gjelder nå også i stor grad for mindre bedrifter. Derfor mener Datakrimutvalget at arbeid med retningslinjer og sikring av mobilt utstyr og nettverk må prioriteres.

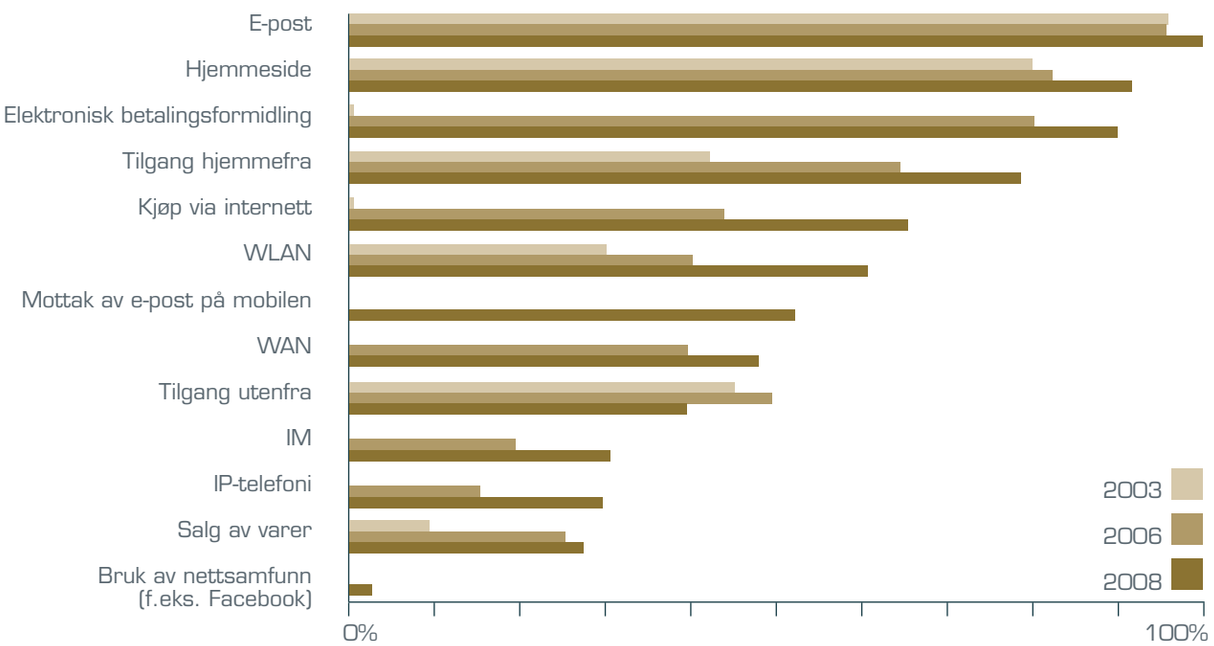
3.2 Avhengighet

Undersøkelsen viser videre at det vil få alvorlige konsekvenser for de fleste virksomheter om de viktigste IT-systemene er ute av drift i mer enn 1 dag. Datakrimutvalget er noe overrasket over at «kritisk nedetid» er vurdert nokså likt uavhengig av virksomhetenes størrelse.

Kritisk nedetid



Prosentvis av virksomheter som benytter IT-løsningene:



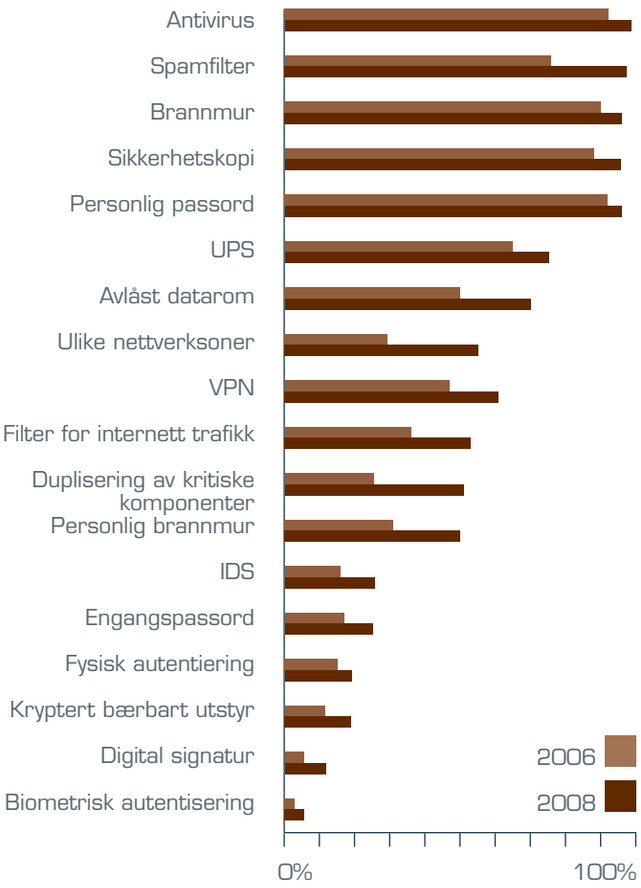
4. Beskyttelsestiltak

Undersøkelsen viser at tekniske tiltak er mer utbredt enn organisatoriske. Datakrimutvalget understreker at organisatoriske tiltak som retningslinjer, opplæring og intern kontroll er vesentlige forutsetninger for et godt sikkerhetsnivå.

4.1 Tekniske tiltak

Godt over 96 % av alle virksomheter har i 2008 gjennomført de viktige sikringstiltak som for to år siden stort sett kun var utbredt i store virksomheter. Det gjelder spesielt løsninger for sikkerhetskopiering, antivirus, spam-filter og brannmurer. En meget positiv trend viser at også små og mellomstore bedrifter har tatt inn over seg behovet for å sikre egne IT-systemer. Spesielt kan vi trekke frem utbredelsen av spam-filtrering, som nå er på 97 %. Det er også positivt at antall virksomheter som unnlater å ta sikkerhetskopi er redusert med hele 70 %.

Tekniske sikkerhetstiltak



Figuren viser en klar økning i utbredelsen av samtlige sikringstiltak de siste to årene. Vi registrerer likevel at det fortsatt er de store virksomhetene som implementerer flest sikringstiltak. For eksempel har over 90 % av virksomheter med mer enn 100 ansatte avlåste datarom, mens dette kun er gjennomført hos halvparten av virksomhetene med mindre enn 100 ansatte.

Samme trend registreres i forhold til bruk av inntrengningsdeteksjonssystemer (IDS) som har økt med over 60 % de siste to årene. Nå benytter 40% av de største virksomhetene teknologien, men bare 15 % av de små virksomhetene.

Datakrimutvalget vil også fremheve at selv om kryptering av bærbare media er nær doblet de siste to årene, er det fortsatt kun 19 % av virksomhetene som har tatt dette i bruk. Datakrimutvalget mener at dette må ses i sammenheng med antall hendelser som virksomhetene utsettes for, der tyveri av IT-utstyr er i en særstilling. Nær 1 av 4 virksomheter har vært utsatt for slike tyverier i 2007, og kryptering av bærbare media vil ved slike hendelser være et effektivt tiltak for å beskytte viktig informasjon og redusere konsekvensene ved tap.

Virksomhetene synes i stor grad å gjennomføre de samme tekniske sikringstiltak med få variasjoner mellom bransjene.

Vi merker oss spesielt at bare halvparten av bedriftene i bygg/anlegg og varehandel har avlåst datarom. Selv for undervisning og personlig tjenesteyting er svarprosenten kun 64 %. Her er det også en forskjell mellom privat og offentlig sektor. I privat sektor er det 64 % som låser inn servere, mens det i offentlig sektor er hele 82 %.

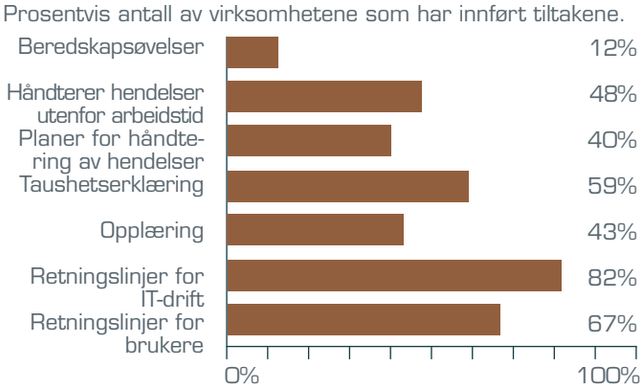
4.2 Organisatoriske tiltak

Kun 1 av 10 bedrifter gjennomfører beredskapsøvelser og under halvparten gjennomfører brukeropplæring. På den andre siden gjennomfører 3 av 4 virksomheter risikovurderinger av eksisterende IT-løsninger.

Datakrimutvalget erfarer at organisatoriske tiltak ikke har samme oppmerksomhet som de tekniske, men påpeker at slike tiltak kan være avgjørende for å unngå hendelser. Spesielt innen bevisstgjøring og opplæring av brukere er det mulighet for store forbedringer. Organisatoriske tiltak krever kompetanse, menneskelige og organisatoriske ressurser. Dette kan forklare at de største virksomhetene i større grad gjennomfører flere organisatoriske tiltak enn de mindre.

Organisatoriske tiltak

Prosentvis antall av virksomhetene som har innført tiltakene.



4.2.1 Retningslinjer

Totalt mangler 1 av 3 virksomheter retningslinjer for ansattes bruk av virksomhetens IT-løsninger. Blant de største virksomhetene har 9 av 10 dette på plass. For virksomheter med mindre enn 100 ansatte har under halvparten av bedriftene slike retningslinjer. Riktignok er dette en bedring fra 2006, da bare hver fjerde av de minste bedriftene hadde retningslinjer på plass, men Datakrimutvalget oppfatter dette fremdeles som et høyt tall tatt i betraktning de saker som har vært i media omkring personvern, uønsket bruk av IT systemer og innsyn i e-post. Undersøkelsen avdekker 15.500 tilfeller av misbruk av IT-ressurser. Datakrimutvalget oppfordrer virksomhetene til i større grad å prioritere utformingen av retningslinjer og oppfølgingen av disse.

I snitt mangler 4 av 10 virksomheter at de ansatte undertegner taushetserklæring. Her er det store forskjeller mellom virksomhetene, hvor 42 % av de minste undertegner taushetserklæring, mot 79 % av de største virksomhetene. Det er imidlertid en positiv økning fra i 2006, da nesten 6 av 10 virksomheter manglet taushetserklæring.

Bare halvparten av virksomhetene innen undervisning, helse og personlig tjenesteyting har noen form for oppfølging av interne retningslinjer. Datakrimutvalget mener dette er for lavt sett hen til mengden personopplysninger enkeltpersoner har tilgang til i denne bransjen.

Kun hver fjerde virksomhet krypterer informasjon på mobilt utstyr

Det kommer stadig nye utfordringer, og en av disse er bruken av nettsamfunn og hvordan disse innvirker på sikkerheten. Hele 8 av 10 virksomheter mangler retningslinjer for ansattes bruk av nettsamfunn.

4.2.2 Risikovurdering

Forståelse av hvilken risiko virksomheten er utsatt for er en viktig del av, og grunnlaget for sikringsarbeidet. Flere norske lover, forskrifter og instrukser stiller også krav til at risikovurderinger knyttet til informasjonssikkerhet skal gjennomføres.

Mørketallsundersøkelsen viser at 76 % av norske virksomheter gjennomfører risikoanalyser regelmessig eller løpende for eksisterende IT-løsninger. Ved innføring av nye IT-løsninger gjennomfører 90 % av virksomhetene risikovurdering. Tallene er på samme nivå som i 2006.

4.2.3 Brukeropplæring

Mange typer hendelser kan best forebygges av bevisste og kompetente medarbeidere. Det er imidlertid bare 43 % av virksomhetene som har gjennomført opplæring i sikker bruk av IT. Dette er omtrent som sist. Virksomheter med mange ansatte gjennomfører i større grad opplæring enn de med få ansatte, og offentlig sektor (48 %) har noe mer opplæring enn privat sektor (41 %). Aller dårligst står det til med opplæringen i bygg- og anleggsbransjen med 24 %.

4.2.4 Beredskap

Et viktig sikringstiltak for å redusere konsekvensene ved hendelser er beredskapsplaner og øvelser. Kun 1 av 10 virksomheter gjennomfører beredskapsøvelser. Også for gruppen med mellom 100 og 200 ansatte er det bare 1 av 10 som øver. Virksomheter med over 200 ansatte er noe bedre med 22 % og virksomheter som anser seg å være en del av kritisk infrastruktur er på 20 %. Datakrimutvalget mener slike øvelser bør inngå som en naturlig del av sikkerhetsarbeidet i virksomhetene.

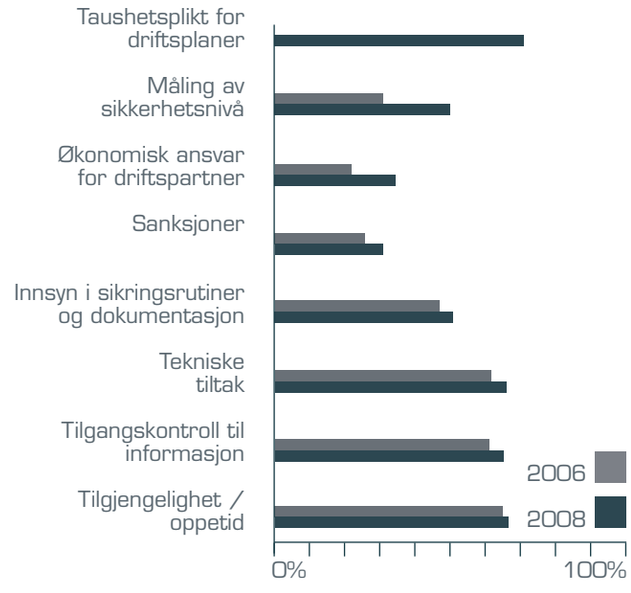
Når det gjelder bransjer, svarer bare 4 av 10 virksomheter i bygg/anlegg og varehandel at de dupliserer kritiske komponenter. Samtidig viser undersøkelsen at 70 % av virksomhetene i varehandelen får alvorlige konsekvenser dersom de viktigste datasystemene er nede inntil en dag. For bygg og anlegg er tilsvarende tall bare 40 % og for undervisning, helse og sosial 50 %. Datakrimutvalget mener dette tyder på at varehandel og til dels undervisning og personlig tjenesteyting ikke har gjennomført tilstrekkelig tiltak for å sikre seg mot driftsavbrudd.

5. Outsourcing

15 % av virksomhetene har satt bort hele IT-driften til en ekstern partner, og 37 % opplyser at de har en kombinasjon av intern og ekstern drift. Andelen som helt eller delvis har satt bort driften har økt noe fra sist undersøkelse.

Bevissthet om informasjonssikkerhet er viktig for alle virksomheter uansett om de drifter sine IT-systemer selv eller har satt dette bort til andre. Tallmaterialet fra undersøkelsen tyder på at virksomhetene som har satt bort IT-driften oppfatter sikkerhetsnivået som lavere enn de som drifter systemene sine selv. Datakrimutvalget mener dette kan skyldes manglende kjennskap til driftspartners sikringstiltak, eller manglende kompetanse eller kunnskap om hvilke krav som kan stilles overfor sin driftspartner.

Krav ved outsorcing
Prosentvis andel av virksomhetene som har stilt krav overfor leverandør av tjenester.



5.1 Sikringskrav i kontrakter

Generelt er det en klar trend at krav i kontrakter med driftspartner henger sammen med størrelsen på virksomheten. Virksomheter med flere enn 200 ansatte stiller flere krav enn de mindre. For virksomheter med mer enn 200 ansatte har for eksempel 85 % stilt krav om tekniske sikringstiltak i kontraktene i forhold til 47 % for de minste virksomhetene.

Det er langt færre som har kontraktsfestet rett til målinger av sikkerhetsnivå. Halvparten av virksomhetene med mer enn 200 ansatte har det mens for de minste virksomhetene har kun 14 % stilt dette kravet. Konsekvensen kan være at de som kjøper driftstjenester ikke får det sikkerhetsnivået som er kontraktsfestet, og heller ikke har rett eller mulighet til å sjekke hvilket nivå de får.

Nytt i årets undersøkelse er spørsmålet om det er stilt krav om taushetsplikt fra driftspartner. Totalt har 71 % av virksomhetene krav til taushetsplikt. For de største virksomhetene er tallet 90 % og bare 59 % for de minste.

Kun 40 % av de minste virksomhetene har krav om oppetid/ tilgjengelighet til tross for at 55 % av virksomhetene i denne kategorien svarer at det vil skape alvorlige problemer om viktige IT-systemer er ute av drift i en dag. Fortsatt er det mange virksomheter som ikke sikrer seg økonomiske rettigheter eller sanksjonsmuligheter ved sikringsbrudd eller manglende leveranse. Selv om kun en av tre virksomheter har stilt slike krav er dette noe bedre enn i 2006.

Datakrimutvalget mener fortsatt at virksomhetene som har overlatt forvaltningen til en ekstern partner i altfor liten grad har stilt krav til leverandøren og har lite kjennskap til sikkerhetsnivået (risikoen) hos denne.

5.2 Bransjebetraktninger

Bare halvpartene av virksomhetene i varehandel, hotell og restaurant som har satt ut driften til tredjepart har krav til tilgangskontroll, taushetserklæring, tekniske tiltak og oppetid. Tilsvarende tall for transport og offentlig administrasjon er vesentlig høyere.

Når det gjelder krav til innsyn i sikkerhetsrutiner, måling av sikkerhetsnivå og rett til økonomisk erstatning / sanksjoner ved alvorlige sikkerhetshendelser, har alle undersøkte bransjer lave tall, og spesielt utmerker undervisning, helse og personlig tjenesteyting seg negativt med svært lave tall. Tallene er ikke akseptable da disse bransjene ofte forvalter personopplysninger som kjøpsprofiler, kredittkortopplysninger og andre persondata. Datakrimutvalget er overrasket over at virksomhetene i varehandel, hotell og restaurant ikke stiller strengere krav til sin driftspartner.

For bransjen varehandel, hotell og restaurant har 65 % oppfølging av interne retningslinjer. Dette står i kontrast til hva denne bransjen svarer på krav stilt til outsourcingpartner hvor andelen som har stilt krav kun er på 23 % - 53 %, jfr tabell: "Krav til outsourcer". Dette kan tyde på at bedriftene innen varehandel har mer fokus på egne ansatte enn til tredjepart som drifter systemene. Samtidig innebærer driftstilgang vesentlig høyere tilgangsrettigheter enn det en typisk ansatt vil ha, som igjen utgjør et økt risikopotensial for eier av informasjonen.

Krav til outsourcer
Prosentvis fordeling på bransjer som har stilt krav til driftspartner.

Krav til outsourcer	Primær-næringer of industri	Bygg og anlegg	Varehandel, restaurant og hotell	Transport og tjenesteytende næringer	Offentlig administ-rasjon	Undervisning, helse og personlig tjenesteyting
Tilgangskontroll	69 %	62 %	51 %	80 %	70 %	55 %
Taushetserklæring	71 %	72 %	53 %	83 %	80 %	63 %
Tekniske tiltak	62 %	64 %	48 %	78 %	79 %	67 %
Oppetid	71 %	56 %	49 %	82 %	78 %	59 %
Innsyn i sikkerhetsrutiner og dokumentasjon	52 %	56 %	33 %	61 %	67 %	33 %
Rett til å måle sikkerhetsnivå	34 %	36 %	31 %	43 %	43 %	14 %
Rett til økonomisk erstatning i gitte tilfelle	29 %	31 %	23 %	48 %	42 %	29 %

Under halvparten av norske virk-somheter gir opplæring i sikker bruk av IT.

6. Personopplysninger

Undersøkelsen viser at 80 % kjenner kravene i personopplysningsloven, men kun 50 % etterlever kravene. Det er gjennomgående god kjennskap til personopplysningslovens krav til håndtering av personopplysninger, nærmere 80 % av alle virksomheter sier at de er kjent med disse kravene. I offentlig sektor er denne andelen hele 92 %. Av de virksomheter som sier de kjenner kravene er det imidlertid kun halvparten som oppfyller personopplysningslovens krav om oversikt over personopplysninger, rutiner og intern kontroll. Dette gjelder også for virksomheter over 200 ansatte. Offentlig sektor er noe bedre enn privat sektor når det gjelder å ha innført de lovpålagte krav.

I bransjen undervisning, helse og sosial vil det være virksomheter som i stor grad behandler sensitive personopplysninger. Halvparten av disse oppfyller ikke lovens krav, og hele 20 % av virksomhetene har ikke iverksatt noen av tiltakene som loven krever. Vi ser at kun 1 av 3 virksomheter innenfor helse / sosial og undervisning har planer for håndtering av de viktigste IT sikkerhetsbruddene. 45 % av virksomhetene i denne bransjen mangler rutiner for internkontroll av håndtering av personopplysninger. Datakrimutvalget mener det er oppsiktsvekkende at så mange virksomheter som behandler sensitive personopplysninger ikke følger lovpålagte krav til behandling av personopplysninger.

Videre har halvparten av virksomhetene i bransjen satt ut hele eller deler av IT driften til eksterne driftsleverandører. Kun en tredjedel av de virksomhetene som har satt ut IT driften har avtalefestet rett til innsyn i sikringsrutiner og dokumentasjon hos driftsleverandøren. Dette er et krav i personopplysningslovens forskrifter. Enkelte sikringskrav er det knapt noen av virksomhetene som har avtalt med IT-drifts leverandør. Det gjelder for eksempel rett til å måle sikkerhetsnivå hos partner og sanksjonere dersom sikringskrav ikke oppfylles.

Bransjen varehandel, hotell og restaurant utmerker seg med lavest kjennskap til kravene i personopplysningsloven, kun 66 % som sier de kjenner dem. Imidlertid har bare 38 % av bedriftene oversikt over de person¬opplysninger som behandles i virksomheten, og kun halvparten av bedriftene i denne bransjen har rutiner for behandling av opplysningene.

Sett i lys av at varehandel, hotell og restaurant ofte forvalter personlig informasjon er det verdt å merke seg at under halvparten oppfyller personopplysningslovens krav.

Undersøkelsen viser at 80 % kjenner kravene i personopplysningsloven, men kun 50 % etterlever kravene.

7. Netthandel

Hele 27 % av respondentene oppgir at de benytter internett for salg av varer og nettbaserte tjenester. Disse virksomhetene er mer avhengig av IT enn andre virksomheter, og 67 % av disse får alvorlige problemer dersom IT-systemene er nede i en dag. Gitt denne avhengigheten er kun 59 % i stand til å håndtere et sikringsbrudd utenfor arbeidstiden. Selv om dette er en klar forbedring fra forrige undersøkelse mener Datakrimutvalget andelen er for lav sett hen til avhengigheten til IT-systemene og at netthandel er en 24/7 virksomhet.

7.1 Tiltak

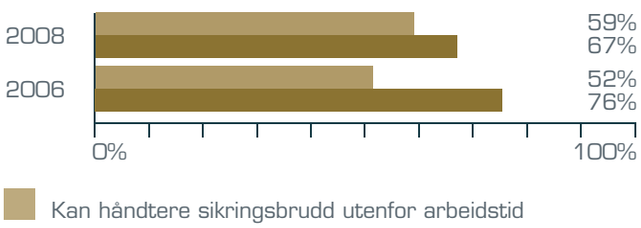
Virksomheter som selger varer og tjenester har et høyere sikringsnivå enn andre virksomheter. Disse virksomhetene skiller seg imidlertid ikke ut fra de andre med hensyn til kjennskap til og etterlevelse av personopplysningsloven. Dette er overraskende da slike virksomheter ofte behandler personopplysninger.

7.2 Hendelser

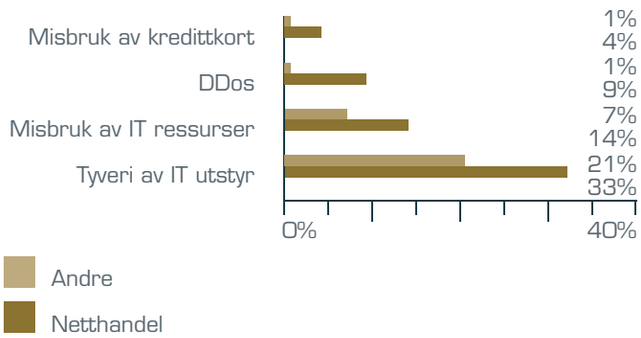
Netthandelsforetak har hatt flere hendelser med større konsekvenser enn andre virksomheter.

Slike foretak har derfor et større behov for sikring av IKT-systemene. Undersøkelsen viser også at disse virksomhetene er mer aktive enn andre for å styrke sikkerheten etter en hendelse, både når det gjelder investering i sikringstiltak og personellressurser til sikringsarbeid.

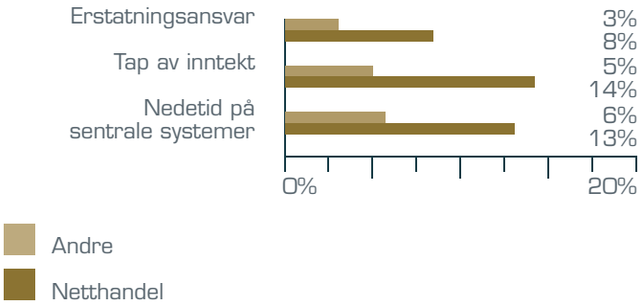
Håndtering av hendelse ift. kritikalitet



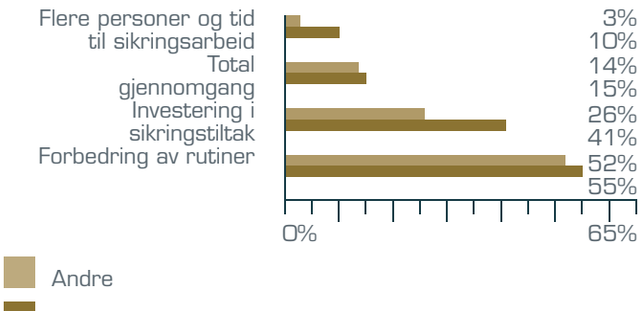
Hendelser



Følger av uønskede hendelser



Tiltak etter hendelser



Virksomhetene stiller i liten grad krav til driftspartnere. Kun 1 av 3 virksomheter har stilt krav til kompensasjon eller sanksjoner ovenfor driftspartner ved avbrudd.

8. Norge i forhold til andre land

Det er gjennomført lignende IT-sikkerhetsundersøkelser i andre land som det er relevant å sammenligne trender med. Datakrimutvalget har denne gang sett på:
CSI (USA) – Computer Crime and Security Survey 2007
BERR (UK) - Information security breaches survey 2008

8.1 Hendelser
Omtrent hver tredje norske virksomhet rapporterer at de har vært utsatt sikkerhetsrelaterte hendelser i årets undersøkelse. I utenlandske undersøkelser rapporterer omtrent halvparten om det samme. I likehet med vår undersøkelse konkluderer undersøkelsene fra utlandet også med at de største virksomhetene rapporterer oftere hendelser enn de mindre virksomhetene.

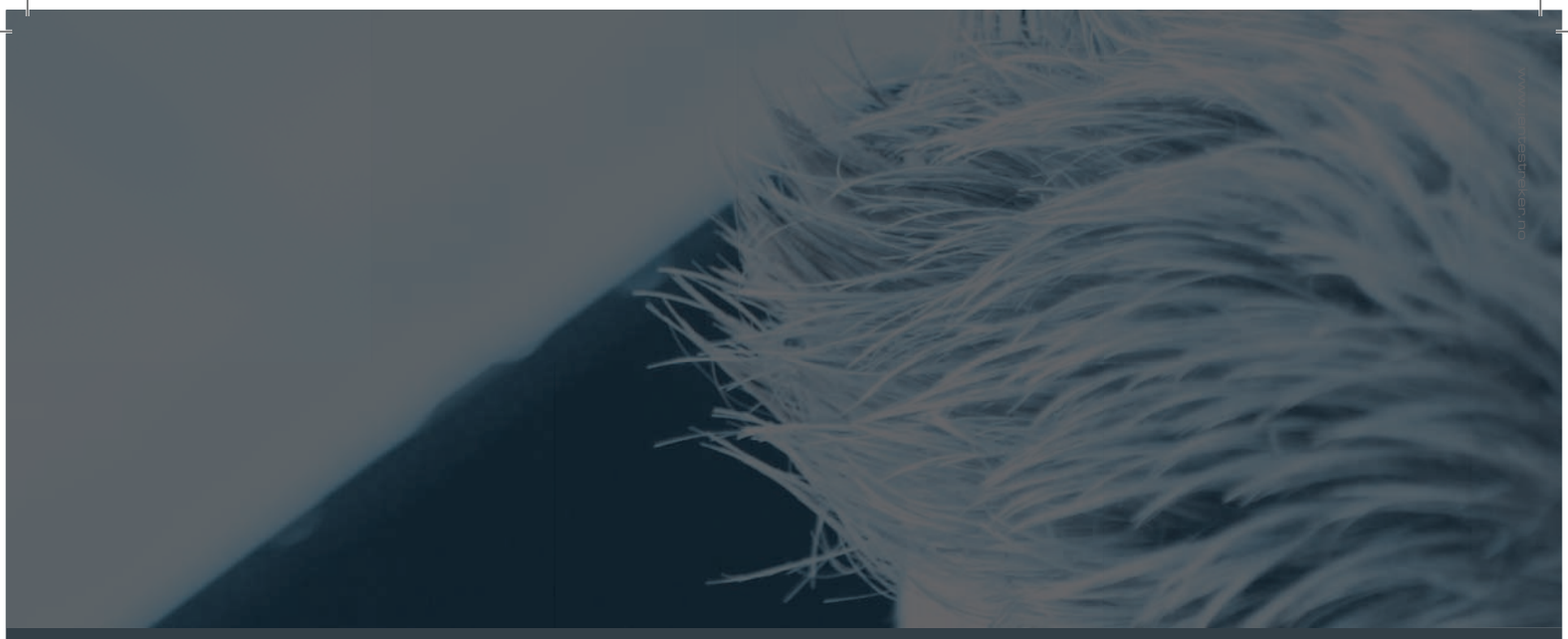
8.2 Antatt gjerningsmann / hvor kommer trusselen fra
Utenlandske undersøkelser viser også at det i større grad er interne gjerningsmenn som står hendelsene. Dette bekrefter våre observasjoner både i 2008 og 2006 som enda tydeligere viser at det er interne gjerningsmenn vi snakker om.

Information security breaches survey 2008: " … for the first time in its nine years history employees are now considered the single most likely cause of a security incident."

8.3 Begrunnelser for ikke å anmelde
Fra CSI undersøkelsen svarer 26 % at "negative publicity" er vektlagt når de ikke anmelder dette til politiet. Dette en markert forskjell fra det vi ser her hjemme Både denne og forrige mørketallsundersøkelse viser at norske virksomheter sjelden opplyser at grunnen til ikke å anmelde saker til politiet er frykt for negativt omdømme for egen virksomhet.

8.4 Sikringstiltak
Sammenliknet med CSI Survey 2007 har norske virksomheter i mindre grad enn de spurte i CSI undersøkelsen implementert sikringstiltak. Spesielt skiller bruken av inntreningninsdeteksjonssystemer (IDS) seg ut. Kun 19% av norske virksomheter har innført IDS (sammenlignet med 69% i CSI undersøkelsen).

Sett i lys av hvor sårbare virksomheter er, er det betenkelig at krav til sikkerhet ofte mangler i driftsavtale med leverandør.



Med støtte fra:

telenor

Microsoft

NSO
NÆRINGSLIVETS SIKKERHETSORGANISASJON

FORNYINGS- OG ADMINISTRASJONSDEPARTEMENTET

NHO
NÆRINGSLIVETS HOVEDORGANISASJON