2010

MØRKETALLSUNDERSØKELSEN 2010

INFORMASJONSSIKKERHET OG DATAKRIMINALITET

Næringslivets Sikkerhetsråd med deltagelse fra: Norsk Senter for Informasjonssikring, Kripos, Nasjonal sikkerhetsmyndighet, SINTEF, SECODE, Telenor, Det Norske Veritas, Forsvarets Forsknings institutt

NSR NÆRINGSLIVETS SIKKERHETSRÅD

1 INNHOLD

VEILEDNING FOR IT- OUTSOURCING

Spesielt rettet mot små og mellomstore bedrifter

De siste mørketallundersøkelser, inkludert denne, viser en økning i outsourcing av IT-tjenester. Undersøkelsen viser også at få virksomheter stiller tilstrekkelige krav til leverandør av slike tjenester.

Næringslivets Sikkerhetsråd (NSR) har derfor utarbeidet, og i samarbeid med NorSIS, utgitt en veiledning med sjekkliste for outsourcing av IT- tjenester. Veiledningen er à jour etter regler og forskrifter pr. juni 2010.

Veiledningen er skrevet av Astri Vik, SINTEF, som et medlem av NSRs datakrimutvalg. Datakrimutvalget har kvalitetssikret veiledningen. Høringssvar fra Datatilsynet, Nasjonal Sikkerhetsmyndighet, NorSIS og Finanstilsynet er innarbeidet i sjekklisten så langt det har vært praktisk mulig.

IT- outsourcing innebærer å sette ut en eller flere IT -funksjoner/ tjenester til eksterne leverandører. Det er viktig å ha orden og oversikt i eget hus og gjennomføre nødvendig planleggings- og forberedelsesarbeid som et ledd i en outsourcingsprosess. Vær oppmerksom på at outsourcing ikke endrer det ansvar ledelsen i virksomheten har for å følge lover og regler.

NSR mener at denne veilederen vil være til nytte, både for kunde, rådgiver og leverandør. Bruk av veilederen og sjekklisten vil bidra til en bedre felles forståelse av hva outsourcing innebærer og hvilke krav som bør med i en slik avtale.

Veileder med sjekkliste kan lastes ned fra NSRs og NorSIS hjemmeside.

KOLOFON:
Næringslivets Sikkerhetsråd
Hjemmeside: www.nsr-org.no
E-post: nsr@nsr-org.no
Facebook: www.facebook.com/Naeringslivets.Sikkerhetsraad

Næringslivets Sikkerhetsråds:
Mot kriminalitet – for næringsliv og samfunn

1 INNLEDNING

Næringslivets Sikkerhetsråd har som formål å forebygge kriminalitet i og mot næringslivet.

Et av virkemidlene vi bruker er å informere om de kriminelle trusler og trender vi ser i dag og forventer i fremtiden. Mørketallsundersøkelsen har en sentral plass i opplysnings- og informasjonsstrategien mot næringslivet og offentlige myndigheter.

Mørketallsundersøkelsen 2010 er den 7. undersøkelsen som foretas av Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget. Undersøkelsen er enestående i Norge og er et viktig bidrag til å kartlegge omfanget av datakriminalitet og IT-sikkerhetshendelser, samt bevissthet omkring informasjonssikring og omfanget av sikringstiltak i norske virksomheter. Alle svar er anonymisert slik at verken respondenter eller deres virksomheter har mulighet til å bli identifisert.

Spørreundersøkelsen er gjennomført elektronisk av Perduco AS i mai 2010. Tidsrommet for kartleggingen er 2009. Analysen er utført av Datakrimutvalget som i 2010 består av:

- Arne-Johan Helle, Telenor (leder)
- Arne Skeide, Det Norske Veritas
- Arne Tjemsland, Secode
- Astri Vik, SINTEF
- Christophe Birkeland, Nasjonal sikkerhetsmyndighet (NSM)
- Janne Hagen, Forsvarets Forskningsinstitutt (FFI)
- Johnny Mathisen, Telenor
- Thomas Stærk, KRIPOS
- Tore Larsen Orderløkken, Norsk senter for informasjonssikring (NorSIS)
- Erland Løkken, NSR.

I tillegg har Fornyings-, administrasjons- og kirkedepartementet (FAD) gitt innspill til undersøkelsen.

1.1 Kriterier og deltakerne i undersøkelsen

Populasjon: Norske virksomheter i privat og offentlig sektor med 5 ansatte eller flere (enkelte næringskoder er holdt utenfor; barnehager, barneparker, SFO, førskoler, kulturskoler, lønnet arbeid i private husholdninger, kinoer m. fl.), samt enkelte organisasjonsformer (borettslag, eierseksjonssameie, forening/lag/innretning, sokn/kirkelig fellesråd, stiftelse).

Utvalg: Det er trukket ut 6000 virksomheter til undersøkelsen. I bruttoutvalget er det 4500 private virksomheter og 1500 offentlige virksomheter. I undersøkelsen er små bedrifter med opp til 10 ansatte, mellomstore fra 10 til 100 ansatte og store bedrifter er bedrifter med mer enn 100 ansatte.

Svarprosent: 745 virksomheter har svart på undersøkelsen. Dette gir en svarrespons på 12,4 prosent.

2

HOVEDFUNN

Dette er hovedfunnene og hovedanbefalingene etter Mørketallundersøkelsen 2010.

I det etterfølgende ser vi på trender og utvikling siste år med fokus på utviklingen fra 2008 til 2010.

Resultatene fra undersøkelsen viser at sikkerheten er sviktende hos mange.

- Virksomhetene er mer avhengige av IT og har større mobilitet.
- 1/3 av virksomhetene er utsatt for datakriminalitet, ca. 1 % blir anmeldt til politiet.
- Opp mot halvparten av gjerningsmennene er egne ansatte eller innleide konsulenter.
- 56 % av virksomhetene outsourcer helt eller delvis IT-driften. Det stilles få krav til leverandørene.
- Stor tiltro til outsourcingsaktørenes håndtering av sikkerheten, men lav fokus på kontroll, oppfølging eller sanksjoner ved mangler.
- Det finnes ingen offentlig pålagte sikkerhetskrav til selskapene som tar på seg IT-driftsoppgavene for andre virksomheter. Det finnes krav til noen virksomheter innenfor enkelte bransjer, men ingen krav direkte til driftsleverandørene som f. eks. sertifiserer virksomhetene.
- Små og mellomstore bedrifter er underrepresentert når det gjelder å ta i bruk en rekke sikkerhetstiltak sammenlignet med store bedrifter. Dette er i samsvar med undersøkelsen fra 2008.
- Bare 1/3 har kontinuerlig opplæring av de ansatte og under halvparten har sikkerhetsopplæring av nyansatte. Et bekymringsfullt resultat, med tanke på at ca. halvparten av gjerningsmennene bak avdekkede hendelser er egne ansatte.
- Ingen forbedring når det gjelder sikringstiltak siden 2008
- Sikringstiltak igangsettes uten at nødvendige risikoanalyser er gjennomført. Virksomhetene prioriterer enklere teknologiske tiltak og ikke organisatoriske tiltak som f. eks. opplæring
- Manglende overvåking og gjennomgang av logger medfører manglende oversikt og rapportering av sikkerhetshendelser til ledelsen. Dette reduserer muligheten til å iverksette preventive sikkerhetstiltak.
- Informasjon spres i nye medier og kanaler. Bruken av nettsamfunn har syv-doblet seg siden 2008, mens under 1/3 har retningslinjer for bruk av nettsamfunn.
- Offentlige virksomheter har mer fokus på personopplysninger og har etablert formelle rutiner og kontroller.
- Virksomheter som driver forskning og utvikling er dobbelt så utsatt som andre virksomheter for å få frastjålet datautstyr, og de er 77% mer utsatt for datahendelser.

Hovedanbefalinger:

- Mer sikkerhetsfokus på mobile enheter
- Anmelde alle vesentlige sikkerhetshendelser
- Sertifiseringsordning for IT-driftsleverandører på sikkerhet
- Verdivurdering. Mer fokus på prosesser og rutiner i virksomheten for å ivareta og beskytte egne verdier.
- Kunnskapsformidlingen må fortsette med fokus på de små og mellomstore virksomhetene
- Kompetanse må økes. Obligatoriske IT sikkerhetskurs for virksomhetsledere.

Mørketallsundersøkelsen 2010 er den 7. undersøkelsen som foretas av Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget.

3

TRUSSELEN

En vurdering av Telenor Security Operation Center (TSOC).

Telenor Sikkerhetssenter (TSOC) har levert sikkerhetstjenester til bedriftsmarkedet i 10 år, og har fulgt en skremmende utvikling fra innsiden. Vi er alle kjent med at mennesker som jobber med IT-sikkerhet jobber mot kriminelle miljøer som er ute etter én ting: tjene penger. Bildet vi har av gutteromshackeren fra midten av forrige tiår ser vi sjelden i dag. Vi ser lite til de som forsøker å stjele ressursene våre, og det er i deres interesse at de forblir skjult.

Samtidig er mange norske virksomheter mindre på vakt. For få år siden var det utenkelig å ta lunsjpause når man visste at en datamaskin var kompromittert. For flere norske virksomheter er dette blitt en normalsituasjon og det kan gå flere dager før virksomheten får tatt en maskin av nett, selv om den står under kontroll av utenforstående.

Når vi ser på utviklingen av infeksjoner har vi hatt en økende utvikling. Til tross for at de fleste bruker betydelig mer penger på sikkerhetsutstyr, har TSOC aldri registrert flere infiserte maskiner hos norske virksomheter enn i 2010.

Sentraliserte data og alt er forbundet med alt

Generelt blir flere og flere systemer koblet sammen via Internett. Data blir stadig mer sentralisert og normalen er gjerne å gi alle ansatte tilgang til alt som standard. Minnepinner rommer mange gigabyte med data til tross for størrelsen. Den nye standarden for lading av mobiltelefoner er også USB-basert og vil føre til at mange etter hvert vil koble PC-en og mobilen sammen daglig, også på jobben. Konsekvensen av én utro tjener eller én kompromittert maskin kan være betydelige da store mengder data i en bedrift kan kopieres og flyttes ut i løpet av få sekunder.

Sosiale nettverk og tillit

Sosiale nettverk blir stadig mer utbredt og dette vet angriperne å benytte seg av. På Facebook er det stadig nye svindelforsøk som prøver å få brukeren til å gi fra seg login-data, høste brukerinformasjon og få brukerens maskin infisert av malware. Det mest kjente eksempelet er Koobface-ormen, som har spredd seg i stadig nye varianter i flere år på Facebook.

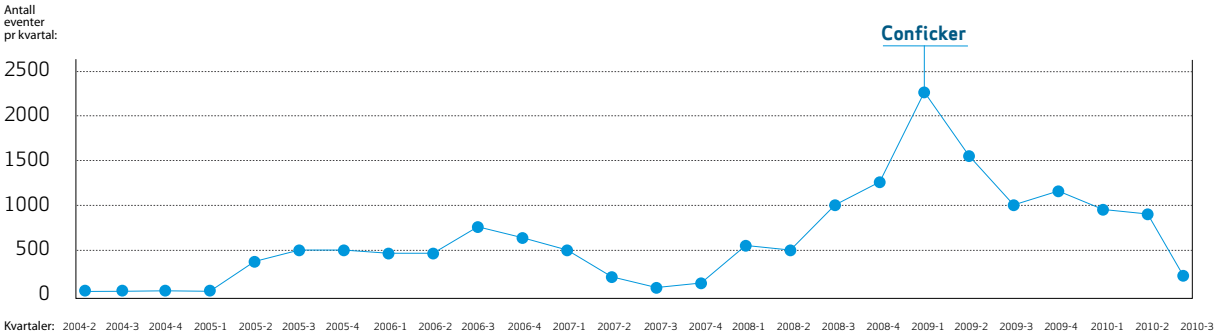
Nettsamfunnet Twitter har også fått utbredelse. På Twitter er en av de største truslene at meldinger bare kan ha opp til 140 tegn. Dette medfører at medlemmer ofte benytter seg av tjenester som forkorter linkene som blir sendt ut på denne tjenesten. Dette er bra for å spare plass, men det er umulig å vite til hvilken adresse en virkelig blir sendt ved å følge linken. Trikset med å forkorte nettadresser blir nå også benyttet i stadig større grad i vanlige spam e-poster.

Private data og jobbdata

De siste årene ser vi en økning i mobilitet blant brukerne. Mange skal ha tilgang til virksomhetnenes informasjon på reise og fra hjemmekontor. Fra et sikkerhetsperspektiv fører dette ofte til en sammenblanding av jobbdata og private data. Mobiltelefonen brukes til begge deler. Bærbare PC-er brukes til private aktiviteter også via bedriftens nettverk. Nettbrett er også en ny plattform for sammenblanding.

Antall svakheter øker fra år til år. Man skulle kanskje tro at antall alvorlige svakheter i systemer og programmer gikk ned etter hvert som folk lærte seg å lage programvare på en sikker måte og ble klar over problemene, men dette viser seg ikke å være tilfelle. Det oppdages stadig flere svakheter i et økende antall nye systemer. Også i helt nyutviklede systemer viser det seg ofte å være flere måter å omgå sikkerheten på.

Tabell 1: Alvorlige hendelser Telenor SOC (Siste kvartal er ufullstendig)



Det er derfor fremdeles viktig å sette fokus på en sikker utviklingsprosess der sikkerheten ikke blir nedprioritert til fordel for funksjonalitet og hurtig utvikling. Det er også viktig å benytte utviklingsmiljøer som oppfordrer til sikker koding og inneholder mye sikkerhet i bunnen.

Virkelige tall fra TSOC
Erfaringen fra TSOC viser at til enhver tid har halvparten av Norges største bedrifter minst én maskin som er kompromittert av eksterne angripere. Maskinen er ofte koblet opp i et såkalt botnett for fjernkontroll. Ofte vet eieren av denne datamaskinen ikke om dette selv.

Angriperne har til enhver tid de samme tilgangene i bedriftens nettverk som den ansatte har. Når de har et brohode inn i bedriften i form av en slik maskin, er det mye enklere å oppnå videre tilgang til andre interne maskiner og nettverk.

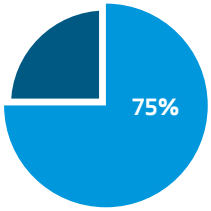
Det som foreløpig redder de fleste bedrifter er at de kompromitterte maskinene så langt ikke i stor grad brukes til tyveri av bedriftshemmeligheter og tømming av bedriftens bankkonti. I dag er det gjerne enklere ting som gjøres, som å spre spam-epost, vise reklame til brukeren og lure vedkommende til å betale penger for falsk sikkerhetsprogramvare. Dette vil endre seg i årene som kommer. I USA overfører allerede kriminelle årlig flere hundre millioner dollar ut fra bedrifters kontoer ved hjelp av bank-trojanere. Problemet er også stort for større banker i Europa.

Trusselbildet utvikler seg altså stadig og blir mer og mer alvorlig. Flere har tilgang til mer informasjon, skillet mellom bedriftens data og personlige data viskes ut og de kriminelle finner stadig på nye metoder for å kunne jobbe uforstyrret. De tradisjonelle forsvarsverkene som brannmur og anti-virus har nesten utspilt sin rolle og fungerer i dag som støybegrensning.

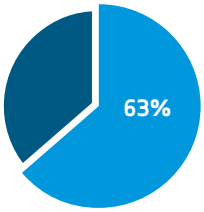
De gode nyhetene:
I 2009 var det 20 % av TSOC kunder som ikke hadde påviste infiserte maskiner. Blant disse var det flere som hadde mange ansatte, operativsystem og brukte internett aktivt. Derimot hadde disse kundene høy bevissthet, god sikkerhetspolicy og sterkt fokus på IT-sikkerhet.

Tabell 2: Statistikk pr 30.08.2010 over siste 100 dager hendelser mot et utvalg av Telenor kunder:

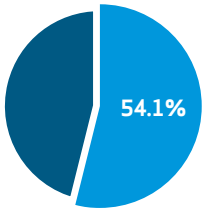
Andel av kundene med alvorlige hendelser:



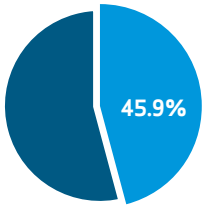
Andel av utplasserte sensorer med alvorlige hendelser:



Røde hendelser:
Hver hendelse representerer minst en kompromittert maskin hos kunden - 544 hendelser



Orange hendelser:
sannsynligvis kompromittert, eller "vil bli" kompromittert
461 hendelser



4 AVHENGIGHET OG BRUK AV IT

Når vi sammenligner sammensetningen av bedrifter som har svart i 2008 med 2010, så har det vært en reduksjon i antall store bedrifter, en svak økning i antall mellomstore, samt en svak reduksjon i antall små virksomheter.

For undersøkelsen og tolkningen av resultatene betyr dette at noe av den generelle økningen i bruk av sikkerhetstiltak vil kunne forklares ved en endring i bedriftssammensetningen fra 2008 til 2010.

4.1 Avhengighet til IT

I datainnsamlingen har vi samlet inn informasjon om hva Internett brukes til. Fra tidligere undersøkelser har virksomhetene bekreftet at alle har e-post og hjemmesider, dette er derfor ikke med i årets undersøkelse. Vi har fokus på mobilitet i bruken av ovennevnte områder.

Det blir viktigere for virksomhetene å være tilgjengelig, ha tilgang til Internett og forretningssystemer. Det er de største virksomhetene som er mest sårbare når systemene og applikasjonene ikke er tilgjengelige. Fra årets undersøkelse ser Datakrimutvalget en svak økning i kravet til tilgjengelighet for alle bransjer, uansett størrelse. Økningen er i midlertidig størst for store virksomheter.

Av deltakerne i undersøkelsen, er det bare 4 % som ikke får problemer i virksomheten når de opplever driftsstans lengre enn en dag. Det er små virksomheter som utgjør den største andelen i denne kategorien. Hele 56 % har nedetid på inntil en dag som følge av uønskede IT-hendelser i 2009. Dette er en økning sammenlignet med 2008. 44 % fikk nedetid på 2 dager eller mer som følge av uønskede IT-hendelser i 2009.

19 % rapporterer å ha en nedetid på 4 dager og mer (inntil 1 måned). Dette er en høy andel av de virksomheter som rapporterer å ha sikkerhetshendelser. Dette understreker behovet for gode prosesser og rutiner som er gjennomøvet for å redusere tiden det tar å komme tilbake til normal drift etter en sikkerhetshendelse.

4.2 Bruk av IT

Se tabell 3

Analyse av ulik bruk og teknologi:
Vi har i årets undersøkelse fokusert mer på mobilitet og bruk av Internett i forhold til sikkerhetsutfordringene.

Det er 64 % blant virksomhetene i undersøkelsen som har tilgang til e-post på mobilen. Dette er en økning på 18 % siden 2008. Blant de store virksomhetene er bruken av e-post på mobil hele 78 %. Forskjellene på e-post på mobil mellom privat sektor og offentlig virksomhet er markant med henholdsvis 72 % i privat og 44 % i offentlig virksomheter.

Når vi spør om retningslinjer og sikkerhetskrav til mobiltelefoner (Smartphone) blant de som har e-post på mobil, svarer bare 39 % at de har utarbeidet retningslinjer for bruk. Uten krav og retningslinjer er det grunn til å anta at sikkerheten på mobilbruk og e-post er en sikkerhetsrisiko for 61 % av virksomhetene.

Utviklingen viser at avhengigheten i daglig bruk av mobile enheter øker og krav til oppetid er større i alle sektorer enn for 2 år siden.

Det er også en markert økning i bruk av nettsamfunn, som Facebook, Twitter, etc. Økningen viser at nettsamfunn blir anvendt syv-ganger så mye som i 2008. Det betyr at 21 % av virksomhetene i dag benytter nettsamfunn i jobbsammenheng.

Dette gir nye sikkerhetsutfordringer når bare 30 % av virksomhetene som benytter nettsamfunnene har utarbeidet retningslinjer for de ansatte.

Det er også en økning på 18 % i bruk av trådløs kommunikasjon.

Anvendelse og avhengighetene av informasjonsteknologi er stadig større for alle virksomheter og vi blir sårbare når tilgjengeligheten uteblir. Endringene på øvrige spørsmål i undersøkelsen er små i forhold til 2008. Hele 80 % av virksomhetene gir ansatte mulighet for tilgang til IT-systemene på reise og hjemmefra.

På tiltakssiden er det bare 23 % som bekrefter å ha kryptering på bærbare medier. Det viser at virksomhetene er sårbare når 18 % i undersøkelsen svarer at de har mistet IT-utstyr.

Anbefalinger
Mobilitet og tilgang til virksomhetens informasjon krever økt sikkerhetsfokus blant brukerne og nye krav til sikker kommunikasjon i henhold til virksomhetens behov for sikring. Risikoanalyser og klassifisering bør gjennomføres for å skille på hva som kan kommuniseres åpent over Internett og hva som krever beskyttelse. Her listes noen viktige tiltak for å øke sikkerheten:

- Gjennomføre risikovurdering ved bruk av nye medier/applikasjoner
- Verdivurdere (Klassifisere) informasjonen i hht. beskyttelsesbehov.
- Utarbeide retningslinjer og brukeropplæring innenfor de områdene som virksomhetene benytter (for eksempel e-post på mobil og bruk av nettsamfunn).

5 OUTSOURCING AV IT-DRIFTEN

Undersøkelsen viser ingen store endringer i antallet som outsourcer IT-driften fra 2008 til 2010.

IT driftens organisering og bruk av IT
18 % av virksomhetene har satt bort hele IT-driften til en ekstern partner, og 38 % opplyser at de har en kombinasjon av intern og ekstern drift. Andelen som helt eller delvis har satt bort IT-driften er da 56 % og relativt stabil sammenlignet med 2008 der andelen som helt eller delvis satte bort IT driften var 52 %.

Se tabell 4

5.1 Krav til outsourcingspartner

Generelt er det en klar trend at krav i kontrakter med outsourcingspartner henger sammen med størrelsen på virksomheten. Store og mellomstore virksomheter stiller flere krav enn små virksomheter. I store virksomheter har for eksempel 77 % stilt krav om tekniske sikringstiltak i kontraktene i forhold til 43 % for de små virksomhetene.

Det er langt færre som har kontraktsfestet rett til målinger av sikkerhetsnivå. Halvparten av de store virksomhetene har kontraktsfestet dette, mens for de små virksomhetene har bare 17 % 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.

Bare 40 % av de små virksomhetene har krav om oppetid/tilgjengelighet til tross for at 50 % av virksomhetene i denne kategorien svarer at det vil skape alvorlige problemer om viktige IT-systemer er ute av drift i et døgn. Fortsatt er det mange virksomheter som ikke sikrer seg økonomiske rettigheter eller sanksjonsmuligheter ved sikringsbrudd eller manglende leveranse. Bare én av tre virksomheter har stilt krav om dette og andelen er synkende fra 2008 til 2010.

Negativ utvikling de to siste årene.
Det er en gjennomgående trend fra forrige undersøkelse til denne undersøkelsen at vi ser en stagnasjon i andelen som har stilt sikringskrav i kontrakter. Dette gjelder totalt og for ulike virksomhetsstørrelser og de fleste bransjer.
Spesielt gjelder dette sikringskravene:

- Krav til tilgangskontroller
- Rett til innsyn i sikkerhetsrutiner
- Rett til måling av sikkerhetsnivå

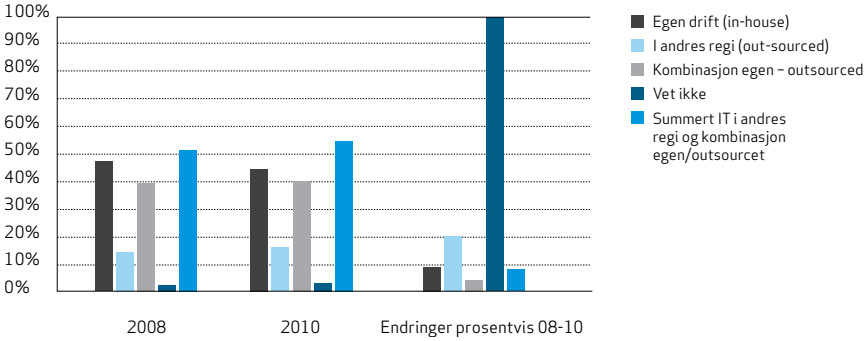
Det er overraskende at selv de store virksomhetene stort sett har stagnasjon eller tilbakegang fra 2008 til 2010 i andelen virksomheter som stiller sikringskrav i kontrakter. Spesielt urovekkende er det at andelen av de store virksomhetene som stiller krav om tilgangskontroll til informasjon er redusert fra 80 % til 65 %.

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 fokuset på informasjonssikkerhet ikke har økt i de siste to årene, men heller har hatt en svak tilbakegang når det gjelder krav til outsourcingsleverandør.

Tabell 3: Hvordan bruker virksomheten internett?

	2008	2010	Endringer prosentvis 08 -10
Selger varer og tjenester	27 %	25 %	- 7 %
Kjøper varer og tjenester	66 %	71 %	8 %
E-post på mobil	54 %	64 %	18 %
Instant messaging (MSN)	31 %	33 %	6 %
IP telefoni	29 %	33 %	14 %
WAN kommunikasjon	48 %	46 %	- 4 %
WI-FI trådløs kommunikasjon	61 %	72 %	18 %
Tilgang til arbeid hjemme/reise	78 %	80 %	3 %
Tilgang for kunder samarbeidsparter	39 %	35 %	- 10 %
Legger ut info. på nett (Facebook, Twitter)	3 %	22 %	633 %

Tabell 4: Hvordan er IT-driften organisert i virksomheten?



Bransjebetraktninger
For de fleste bransjer er utviklingen negativ eller uendret fra 2008 til 2010 når det gjelder sikringskrav som stilles til outsourcingspartner.

Det er likevel noen positive trekk ved utviklingen for noen bransjer.

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. Undervisning, helse og personlig tjenesteyting har likevel hatt en forbedring på noen områder fra 2008 til 2010. Det gjelder spesielt innenfor områdene rett til måling av sikkerhetsnivå, her er det en økning fra 14 % i 2008 til 30 % i 2010. Når det gjelder rett til innsyn i sikkerhetsrutiner og dokumentasjon er det en forbedring fra 33 % i 2008 til 44 % i 2010.

Andelen virksomheter innenfor denne næringen som stiller krav er likevel fortsatt altfor lav. Det er f. eks bare omlag halvparten av de som setter ut IT-driften i denne bransjen, som stiller krav om tilgangskontroll til informasjon til sin IT-driftspartner. Fordi denne bransjen ofte forvalter personopplysninger som kjøpsprofiler, kredittkortnummer og andre persondata, er det ikke godt nok at bare 50 % stiller krav om tilgangskontroll til informasjon.

For varehandel, hotell og restaurant har andelen som stiller krav til tekniske sikringstiltak økt fra 48 % i 2008 til 63 % i 2010, og andelen som stiller krav til tilgangskontroll har økt med 20 %. Dette er positivt. Også denne bransjen forvalter personopplysninger som kjøpsprofiler, kredittkortnumre og andre persondata og derfor er det ikke godt nok at bare 61 % stiller krav om tilgangskontroll til informasjon.

Av virksomheter som har svart at de anser seg selv som en del av nasjonal kritisk infrastruktur, har 55 % helt eller delvis outsourcet. Dette er samme nivå som i 2008. Av de virksomheter som oppfatter seg selv som kritisk infrastruktur er 80 % store virksomheter med mer enn 100 ansatte. Datakrimutvalget velger derfor å feste lit til virksomhetenes vurdering av sin egen betydning for nasjonal kritisk infrastruktur. Selv om dette ikke uten videre er sammenfallende med de virksomheter som omfattes av sikkerhetsloven med forskrifter , så gir dette en indikasjon på hvordan slike virksomheter oppfatter sin egen rolle i forhold til sikringskrav ved outsourcing. For slike virksomheter gjelder ofte særskilte lover og forskrifter som stiller mer omfattende krav til informasjonssikkerhet og sikringstiltak enn for øvrige virksomheter.

Som for virksomhetene generelt er det ingen økning i andelen som stiller krav til outsourcingspartner, det er derimot en svak tilbakegang. Når det gjelder krav til måling av sikkerhetsnivå, økonomisk ansvar ved sikringsbrudd og sanksjoner er resultatene svake, henholdsvis 48 %, 44 % og 42 % har dette. Dette gir en indikasjon om at virksomheter som vurderer seg selv som kritisk nasjonal infrastruktur ikke har tilstrekkelig fokus på sikringskrav i forbindelse med outsourcingskontrakter.

Dette er spesielt urovekkende på bakgrunn av at NSM i sin årsrapport sier at IKT-trussel og sårbarhetsbildet er betydelig forverret de to siste årene .

Datakrimutvalget mener fortsatt at virksomheter som har overlatt forvaltningen av IT til en ekstern partner i altfor liten grad har stilt krav til leverandøren og har lite kjennskap til sikkerhetsnivået (risikoen) hos denne. Med få unntak har det ikke vært noen forbedring siden 2008. Sett i lys av det økende trusselnivået fra Internettkriminalitet, kan dette representere en risiko for grunnsikkerheten i virksomhetene.
NSM har i sitt forslag til strategi for cybersikkerhet hevdet at grunnsikkerheten vedr IT må opp på et høyere nivå i virksomhetene som en helhet. Dette underbygges av de funn som her er gjort.

Anbefalinger:
Myndighetene bør stille sikringskrav gjennom forskrift for de virksomheter som skal drifte IT systemer på vegne av andre. Myndighetene bør også intensivere tilsyn og veiledningsmøter.

For de fleste bransjer er utviklingen negativ eller uendret fra 2008 til 2010 når det gjelder sikringskrav som stilles til outsourcingspartner.

Tabellen nedenfor over sikringskrav viser at fremgangen fra 2006 til 2008 er snudd, og har fått tilbakegang fra 2008 til 2010.

Tabell 5: Krav til outsourcing part?
Prosentvis av antallet virksomheter som har helt eller delvis outsourcet.

	2006	2008	2010	Endringer prosentvis 08 - 10
Krav til tilgangskontroll i kontrakt	62 %	66 %	57 %	-14 %
Krav til taushetsplikt	-	71 %	68 %	-4 %
Krav til tekniske sikkerhetstiltak	62,9 %	66 %	65 %	-2 %
Krav til tilgjengelighet/oppetid	65,8 %	67 %	65 %	-3 %
Rett til innsyn i sikkerhetsrutiner	47 %	51 %	47 %	-8 %
Rett til måling av sikkerhetsnivå	31 %	35 %	31 %	-11 %
Økonomisk ansvar ved sikkerhetsbrudd	23 %	34 %	31 %	-9 %
Andre sanksjoner dersom kravene ikke følges	26 %	32 %	27 %	-16 %
Vet ikke	-	18 %	14 %	-22 %
Ingen av ovennevnte krav er med	-	-	8 %	-

Tabell Krav til outsourcer – tall for 2008 i parentes

Tabell 6: Prosentvis fordeling på bransjer som har stilt krav til outsourcingspartner.

	Primærnæringer og industri	Bygg og anlegg	Varehandel, restaurant og hotell	Transport og tjenesteytende næringer	Offentlig administrasjon	Undervisning, helse og personlig tjenesteyting
Tilgangskontroll	56 % (69 %)	64 % (62 %)	61 % (51 %)	57 % (80 %)	61 % (70 %)	54 % (55 %)
Taushetserklæring	75 % (71 %)	69 % (72 %)	60 % (53 %)	71 % (83 %)	79 % (80 %)	63 % (63 %)
Tekniske sikrings tiltak	64 % (62 %)	69 % (64 %)	64 % (48 %)	65 % (78 %)	73 % (79 %)	61 % (67 %)
Tilgjengelighet/Oppetid	63 % (71 %)	64 % (56 %)	66 % (49 %)	74 % (82 %)	76 % (78 %)	54 % (59 %)
Innsyn i sikkerhetsrutiner og dokumentasjon	40 % (52 %)	44 % (56 %)	39 % (33 %)	56 % (61 %)	67 % (67 %)	44 % (33 %)
Rett til å måle sikkerhetsnivå	26 % (34 %)	28 % (36 %)	23 % (31 %)	39 % (43 %)	45 % (43 %)	30 % (14 %)
Rett til økonomisk erstatning i gitte tilfelle	30 % (29 %)	22 % (31 %)	31 % (23 %)	39 % (48 %)	42 % (42 %)	21 % (29 %)
Sanksjoner dersom krav ikke oppfylles	26 % (30 %)	19 % (28 %)	26 % (17 %)	34 % (50 %)	39 % (37 %)	22 % (18 %)

6 HENDELSER

Undersøkelsen viser at 30 % av norske virksomheter ble utsatt for datakriminalitet, og at denne andelen holder seg stabil i forhold til 2008.

Definisjonen av datakriminalitet vil ofte variere med hvilken sammenheng begrepet benyttes. Mørketallsundersøkelsen omfatter også hendelser som ikke nødvendigvis inngår i den etablerte definisjonen av datakriminalitet, men som likevel er relevante i forhold til datasikkerhet og informasjonssikkerhet. Eksempel på dette er tyveri av IT-utstyr, som tradisjonelt inngår i kategorien vinningskriminalitet.

6.1 Analyse av hendelser

Virksomheter utsettes for mange ulike typer hendelser som har ulike sikkerhetsaspekter.

Se tabell 7 og tabell 8

Undersøkelsen viser at tyveri av IT-utstyr har en nedgang sammenliknet med tidligere år. Ser man derimot på kriminalstatistikken viser denne en økning i vinningskriminaliteten for første gang siden 2002. Imidlertid skiller ikke kriminalstatistikken i denne sammenheng mellom privatpersoner og virksomheter som fornærmet, eller for den saks skyld om vinningskriminaliteten retter seg mot IT-utstyr.

Sammenholdt med tidligere undersøkelser ser man også en økning i antall virksomheter som utsettes for misbruk av IT-ressurser, samt en økning knyttet til spredning av ulovlig opphavsrettslig beskyttet materiale. For øvrig ser man en svak nedgang blant virksomheter som er utsatt for målrettede aksjoner som har til hensikt å redusere tilgjengeligheten.

Mørketall

Mørketall er differansen mellom den anmeldte kriminaliteten som fremkommer i politiets statistikk og den kriminaliteten som virksomhetene og privatpersoner faktisk blir utsatt for.

Politiets statistikk skiller ikke på om fornærmede er en virksomhet eller en privatperson. Tallene som er brukt her er totalt antall anmeldelser, og inneholder derfor også anmeldelser i kategoriensomerinngittavenfornærmet privatperson. Antallet anmeldelser fra virksomheter vil følgelig kunne antas å være enda lavere. I undersøkelsen er virksomhetene bedt om å gi et estimat for antall hendelser de har vært utsatt for, i kategorier som til en viss grad er sammenlignbare med statistikkgrupper i politiets statistikk.

Basert på opplysningene gitt i undersøkelsen, samt SSBs statistikk over næringsstrukturen i Norge, har Datakrimutvalget estimert det totale antallet i utvalgte grupper av hendelser undersøkelsen tar for seg. Flere forhold gjør det vanskelig å oppnå helt presise anslag for det faktiske antallet hendelser. Anslaget har imidlertid tatt hensyn til ekstremverdier der slike forekommer. Videre presiseres at virksomhetene selv har estimert antallet hendelser.

Datakrimutvalget har estimert at norske virksomheter ble utsatt for ca. 9800 datainnbrudd i 2009. Til sammenlikning har politiet bare registrert 88 anmeldelser for datainnbrudd for perioden.

Ser man på antallet tilfeller av uautorisert sletting og/eller endring av data, kan dette estimeres til ca. 1700 tilfeller hos norske virksomheter i 2009. Politiet mottok 87 anmeldelser for slike forhold i perioden.

Tabell 7: Virksomheter utsatt for hendelser

Type hendelse	2006	2008	2010
Datainnbrudd (hacking)	4 %	3 %	5 %
Tyveri av informasjon	1 %	2 %	2 %
Uautorisert endring/sletting av data	5 %	4 %	5 %
Misbruk av IT-ressurser (PC/nett/server)	9 %	9 %	11 %
Spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering)	2 %	3 %	5 %
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)	5 %	4 %	4 %
Trusler om å angripe IT-systemer (utpressing)	1 %	0 %	1 %
Bedrageri ved misbruk av kredittkort over Internett	1 %	2 %	1 %
Tyveri av IT-utstyr (PC, server, etc)	26 %	24 %	18 %
Tap av opplysninger underlagt personopplysningsloven			1 %

Tabell 8: Utvalgte hendelser etter kategori, samt antallet anmeldelser

Type hendelse	Estimat	Anmeldt
Datainnbrudd (hacking)	9900	88
Uautorisert endring/sletting av data	1800	87
Misbruk av IT-ressurser	9200	24
Målrettede aksjoner som har til hensikt å redusere tilgjengelighet	2700	19
Totalt	23500	218

Estimatene er basert på opplysningene fra undersøkelsen, samt SSBs statistikk over næringsstrukturen i Norge.

Videre kan antallet målrettede angrep som har til hensikt å redusere tilgjengelighet estimeres til ca. 2600 for 2009. Politiets statistikk inneholder ikke tall for denne typen hendelser spesielt, men den gruppen slike angrep inngår i viser bare 19 anmeldte forhold. Ingen av virksomhetene i undersøkelsen oppgir for øvrig at de har anmeldt denne typen forhold.

Virksomhetene i undersøkelsen rapporterer at misbruk av IT-ressurser er et utbredt problem. Totalt for norske virksomheter kan antallet slike tilfeller estimeres til ca. 9100 i 2009. Politiets statistikk for 2009 viser at totalt 24 slike tilfeller ble anmeldt.

Totalt for disse fire kategoriene hendelser blir antallet 23.500 i løpet av 2009. 218 anmeldelser er registrert hos politiet. Disse kategoriene av hendelser må sies å være representative for den datakriminaliteten norske virksomheter utsettes for.

Følgelig er det rimelig å anslå at under 1 % av datakriminaliteten mot norske virksomheter blir anmeldt til politiet.

Mørketallsundersøkelsen 2010 bekrefter med dette tidligere undersøkelser, som viser at mørketallene for datakriminalitet er svært store.

Når det gjelder tyveri av IT-utstyr, så anmeldes 70 % av denne kriminaliteten til politiet. Det er grunn til å tro at dette i stor grad skyldes at forsikringsselskapene setter som vilkår for erstatning, at forholdet anmeldes til politiet.

For Datakrimutvalget er det et paradoks at ingen av virksomhetene oppgir at målrettede angrep som hadde til hensikt å redusere tilgjengelighet ble anmeldt til politiet, mens de samtidig oppgir at 70 % av tyveriene av IT-utstyr blir anmeldt. Dette paradokset forsterkes ytterligere når det samtidig oppgis at nedetid blir stadig mer kritisk for virksomhetene.

Gjerningsmann

Virksomhetene anslår at gjerningsmannen i 42 % av tilfellene er en egen ansatt eller innleid personell. Om man utelater tyveri av IT-utstyr fra tallmaterialet står disse for 48 % av tilfellene. For noen typer hendelser ser man en stor overrepresentasjon av tilfeller der gjerningsmann oppgis å være egen ansatt eller innleid personell.

Dette er tyveri av informasjon, uautorisert endring eller sletting av data, samt spredning av ulovlig opphavsrettslig beskyttet materiale. Ingen oppgir at målrettede aksjoner som har til hensikt å redusere tilgjengeligheten, trusler om å angripe IT-systemer eller bedragerier ved misbruk av kredittkort over Internett er begått av egne ansatte eller innleid personell.

6.2 Anbefalinger og tiltak hendelser

Det er store mørketall for datakriminalitet. Undersøkelsen gir ingen klare indikasjoner på hva som er årsaken til at datakriminalitet ikke anmeldes. Imidlertid er årsaker som "Saken er ubetydelig", "Tror ikke det er mulig å finne en gjerningsmann" og "Tror ikke forholdet er straffbart" gjengangere. Manglende tiltro til politiets kompetanse er også en årsak som en del oppgir, men den er ikke av de mest fremtredende forklaringene.

Politiets statistikk er dårlig egnet til å omtale omfanget av datakriminalitet mot norske virksomheter, eller datakriminalitet i sin alminnelighet. Det finnes få andre målinger på omfanget av datakriminalitet i Norge enn Mørketallsundersøkelsen. Datakrimutvalget vil oppfordre virksomheter til å anmelde forhold av en viss alvorlighet til politiet, slik at politiets statistikk gir et mer realistisk bilde av den faktiske kriminaliteten på området.

Mørketallsundersøkelsen bekrefter at datakriminalitet er svært utbredt i Norge. Flere internasjonale undersøkelser har påvist en betydelig illegal økonomi knyttet til slik kriminalitet, samt at de økonomiske tapene knyttet til datakriminalitet er store.

Datakrimutvalget anbefaler derfor en betydelig styrking av politiets evne til å forebygge, etterforske og iretteføre denne formen for kriminalitet. Datakrimutvalget mener det er et fåtall politidistrikter i Norge som i dag har kompetanse eller ressurser til å etterforske denne formen for kriminalitet. Samtidig ser man at de spesialiserte miljøene som finnes, på langt nær er store nok til alene å kunne forebygge, etterforske og iretteføre den datakriminaliteten som faktisk forekommer i Norge.

Den teknologiske utviklingen på området krever robuste spesialiserte miljøer som kan være den kompetansemessige spydspissen i bekjempelsen av datakriminalitet. Disse bør styrkes. Samtidig krever omfanget av datakriminalitet en betydelig styrking av kompetansen i det enkelte politidistrikt, der hoveddelen av kriminaliteten i Norge tross alt etterforskes.

Mange gjerningsmenn for datakriminalitet er i følge undersøkelsen egne ansatte eller innleid personell. Datakrimutvalget understreker viktigheten av gode interne rutiner, og ikke minst oppfølging av disse. God og grundig bakgrunnssjekk ved ansettelser, outsourcing og innleie av personell bør etableres som en del av internkontrollen. Videre mener Datakrimutvalget at god kontinuerlig opplæring vil virke forebyggende med tanke på hendelser som begås av egne ansatte eller innleid personell, som en del av den interne sikkerhetskulturen i virksomheten.

6.3 Utgifter knyttet til sikkerhets-hendelser

Hele 28 % av alle virksomheter hadde utgifter opp til 50.000 som følge av IT-sikkerhetshendelser i 2009. Virksomhetens størrelse er en klar faktor når det gjelder tap. Små virksomheter har små tap, mens store virksomheter har store tap.

Analyse

Undersøkelsen viste at 25 % mente de ikke hadde noen direkte utgifter tilknyttet IT-sikkerhetshendelser i 2009. 28 % hadde opp til 50.000 i utgifter, mens 11 % hadde over 50.000.

Det er klare forskjeller tilknyttet utgifter når man sammenligner de ulike størrelsene på virksomhetene. Små virksomheter har i større grad små utgifter, mens store virksomheter har større utgifter. Når spurt om anslåtte kostnader tilknyttet IT-sikkerhetshendelser var trendene de samme.

6.4 Hva er gjort for å hindre tilsvarende hendelser?

Se tabell 9

Analyse

Det er ingen bemerkningsverdige trender eller vesentlige endringer fra 2008. Som tabellen viser er investering i tekniske sikringstiltak og forbedring av sikringsrutiner de mest brukte tiltakene for å forhindre tilsvarende hendelser. En dypere analyse i datagrunnlaget viser at de store virksomhetene er bedre enn små og mellomstore virksomheter på å investere i tekniske sikringstiltak.

Kun 5 % tildeler mer tid eller personer til sikringstiltak. Ser man dette opp mot at hele 67 % rapporterer at uønskede hendelser i 2009 medførte ekstra arbeid, viser dette at ekstra arbeid blir brukt til å løse problemet, mens man ikke tildeler ressurser til å håndtere løpende forbedringsarbeid.

Hele 16 % rapporterer at de velger å gjennomføre en total gjennomgang av sikringsnivået i virksomheten. Dette er forholdsvis høyt når en ser på virksomhetene i utvalget. Kun 11 % hadde tap på 50.000,- eller mer som følge av uønskede hendelser.

Det er ikke noen spesielle grupper som skiller seg ut. 16 % valgte å gjøre ingenting for å hindre tilsvarende hendelser. Dette er tilsynelatende et høyt tall, men sammenligner man med direkte og indirekte kostnader, svarte henholdsvis 25 % og 39 % at uønskede hendelser ikke fikk noen kostnader.
Sikringstiltakene de fleste velger å implementere etter å ha vært utsatt for en hendelse, er investering i tekniske sikringstiltak og forbedring av sikringsrutiner knyttet til uønskede hendelser. Store virksomheter er flinkere til å investere i tekniske sikringstiltak.

Få virksomheter tildeler mer ressurser til sikringsarbeid etter å ha vært utsatt for en uønsket hendelse.

Anbefalinger

Virksomhetene bør fokusere tiltakene knyttet til kontinuerlig forbedring hvor tekniske sikringstiltak (Teknologi) kombineres med forbedringer på rutiner (Prosesser) og mer tid til opplæring og holdninger til brukerne. (Organisasjon)

6.5 Hvilke følger hadde den/de uønskede hendelsen(e) for virksomheten i 2009?

Se tabell 10

Analyse

Uønskede hendelser medførte ekstra arbeid for 2/3 av virksomhetene i 2009. Derimot er det bare 14 % som rapporterer at de hadde nedetid og 13 % hadde tap av inntekt som følge av uønskede hendelser.

Tabell 9: Hva er gjort for å hindre tilsvarende hendelser?

Tiltak	2006	2008	2010	Endringer prosentvis 08-10
Investering i tekniske sikringstiltak	39 %	32 %	31 %	-3 %
Forbedring av sikringsrutiner	44 %	52 %	54 %	4 %
Flere personer og/eller mer tid til sikringsarbeid	4 %	6 %	5 %	-17 %
En total gjennomgang av sikringsnivå	14 %	14 %	16 %	14 %
Ingenting	22 %	17 %	16 %	-6 %
Annet	-	13 %	18 %	38 %
Vet ikke	5 %	3 %	4 %	33 %

Tabell 10: Hvilke følger hadde den/de uønskede hendelsen(e) for virksomheten i 2009?

Følger	2006	2008	2010	Endringer prosentvis 08-10
Ekstra arbeid	67 %	62 %	67 %	8 %
Nedetid på sentrale IT systemer	-	9 %	14 %	56 %
Tap av inntekt (enten direkte og/eller tapt salg/ omsetning	11 %	9 %	13 %	44 %
Erstatningsansvar	1 %	5 %	5 %	0 %
Tap av omdømme	1 %	5 %	7 %	40 %
Ingen følger	29 %	31 %	22 %	-29 %

Dette viser at de fleste virksomhetene (86 %), klarer seg godt og har lite nedetid. Bare 13 % av de som hadde uønskede hendelser opplevde større tap.

Dette er et relativt lite antall med tanke på alle trusler og sikkerhet-sutfordringer vi hører og leser om i pressen. Vi skal imidlertid være klar over at dette er at bildet er sammensatt, og det skjuler seg store tap for de store virksomhetene, mens relativt små tap kan ha store konsekvenser for små virksomheter.

En nærmere analyse av svarene avdekker videre at det er forskjell mellom ulike sektorer:

- Offentlig sektor hadde signifikant mer ekstraarbeid som følge av uønskede hendelser.
- Privat sektor rapporterte signifikant mer tap av inntekt.
- Varehandel, hotell- og restaurant-virksomhet, samt transport, kommunikasjon og tjenesteytende næringer rapporterte signifikant mer tap av inntekt i forhold til andre bransjer.

Følger som konsekvens av uønskede hendelser har generelt økt fra 2008. Det er også en drastisk reduksjon i antallet som sier at uønskede hendelser ikke hadde noen konsekvens.

Uønskede hendelser får stadig større konsekvenser for virksomheter. Hele 2/3 rapporterte at de fikk ekstra arbeid som følge av uønskede hendelser i 2009.

Anbefalinger
Virksomhetene bør fokusere tiltakene på kontinuerlig forbedring av tekniske sikringstiltak (Teknologi) kombinert med forbedringer på rutiner (Prosesser) og mer tid til opplæring og holdninger til brukerne. (Organisasjon).

Hele 35 % vet ikke eller rapporterer at utgifter ikke er aktuelt ved sikkerhets-hendelser. 29 % av de som definerer seg å være del av kritisk infrastruktur vet ikke hvor store utgiftene var.

Virksomhetene trenger bedre rutiner for:

- Logging av hendelser og rutiner for oppfølging.
- Hendelsesrapportering til ansvarlig

Hele 56 % har nedetid på inntil en dag som følge av uønskede IT-hendelser i 2009. Dette er en økning sammenlignet med 2008. 44 % fikk nedetid på 2 dager eller mer som følge av uønskede IT-hendelser i 2009.

7 FORSKNING OG UTVIKLING OG IMMATERIELLE RETTIGHETER

Undersøkelsen viser at FoU- og IPR-virksomheter er mer utsatt for datahendelser enn andre virksomheter.

7.1 Virksomheter med forskning og utvikling i immaterielle rettigheter.

20,7 % av virksomhetene svarer at de driver med forskning og utvikling (FoU), og 20,3 % svarer at de innehar immaterielle rettigheter (Intellectual Property Rights – IPR).

49 % av alle virksomheter med immaterielle rettigheter driver også med FoU. Det er således ikke de samme virksomhetene som har immaterielle rettigheter som driver FoU.

Se tabell 11 og tabell 12

Datahendelser
43,7 % av virksomhetene med immaterielle rettigheter har opplevd uønskede hendelser, mot 27,1 % for dem som ikke har immaterielle rettigheter (16,6 prosentpoeng).

46,1 % av virksomhetene som driver FoU har opplevd uønskede hendelser, mot 26,1 % av de virksomhetene som ikke driver FoU (20 prosentpoeng).

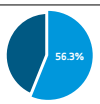
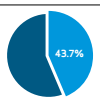
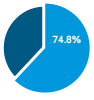
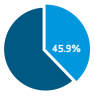
Dette er store forskjeller. Resultatene har derfor blitt kontroller mot flere mulige naturlige forklaringer:

- Størrelse på virksomheten. Større virksomheter kan være mer utsatt enn mindre virksomheter i kraft av antall databrukere og kjennskap til virksomheten.
- Egen it-sikkerhetsansvarlig. Virksom-heter med egen it-sikkerhetsansvarlig er mer kompetent til å oppdage hendelser enn dem uten it-sikkerhetsansvarlig.
- Drifter it-systemene selv. De virksomheter som drifter it-systemene selv er bedre i stand til å avdekke hendelser enn de som har outsourcet driften til ekstern partner.
- Verdivurdering, retningslinjer for bruk av nettsamfunn, opplæring i sikker bruk av IT, og retningslinjer for eksterne lagringsmedier. Virksomheter med retningslinjer og bevissthet knyttet til datasikkerhet har større sannsynlighet for å avdekke hendelser.
- Bransje: Noen bransjer er mer utsatt for datahendelser enn andre bransjer.

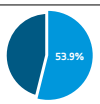
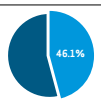
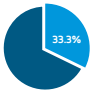
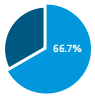
Kontrollert mot disse faktorene er det like fullt signifikante forskjeller. IPR-virksomheter og FoU-virksomheter skiller seg ikke fra andre virksomheter på noen av disse områdene, unntatt for it-sikkerhetsansvarlig. IPR/FoU-virksomheter har i noe større grad egen it-sikkerhetsansvarlig enn øvrige virksomheter, men det forklarer ikke det differansen.

Undersøkelsen viser derfor at FoU- og IPR-virksomheter er mer utsatt for datahendelser enn andre virksomheter. Det er derfor grunnlag for å anta at målrettet informasjonsinnhenting (informasjonsspionasje) foregår mot FoU- og IPR-virksomheter i større grad enn for virksomheter uten denne aktiviteten og rettigheter.

Tabell 11: Innehar virksomheten IPR?
Uønskede hendelser:

Innehar virksomheten IPR?	Har ikke opplevd uønskede hendelser	Har opplevd uønskede hendelser
JA		
NEI		
VET IKKE		

Tabell 12: Driver din virksomheten FoU?
Uønskede hendelser:

Driver din virksomheten FoU?	Har ikke opplevd uønskede hendelser	Har opplevd uønskede hendelser
JA		
NEI		
VET IKKE		

7.2 Datatyveri

Undersøkelsen viser at 30,5 % av FoU-virksomhetene har blitt frastjålet datautstyr, mot 15,3 % for dem som ikke driver FoU, og 28,5 % av IPR-virksomhetene har blitt frastjålet datautstyr mot 17,4 % for dem uten IPR. For undersøkelsens totalt er det 18,4 % som har fått frastjålet datautstyr.

Se tabell 13 og tabell 14

Kontrollert for de samme faktorer som under datahendelser, opprettholdes differansen mellom de virksomhetene som driver FoU og de som ikke driver FoU. Størrelse, it-sikkerhetsansvarlig, etc, forklarer ikke hvorfor FoU-virksomheter er mer utsatt for tyveri av datautstyr. Forklaringen må ligge i FoU-aktiviteten.

For virksomheter som innehar immaterielle rettigheter kan differansen muligens forklares ved størrelse på virksomhetene. Det er således ikke grunnlag i våre tall for å si at IPR-virksomheter er mer utsatt for tyveri av datautstyr på grunn av sine immaterielle rettigheter alene.

7.3 Tyveri av informasjon

2 % av virksomhetene oppgir at de har opplevd tyveri av informasjon. Det er utelukkende virksomheter i privat sektor som oppgir at de har hatt tyveri av informasjon. Antall respondenter er for lavt til at videre analyse er forsvarlig.

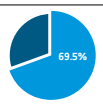
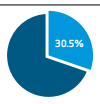
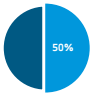
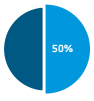
7.4 Oppsummering FoU og IPR

Virksomhetene som driver FoU er ca 77 % (20 prosentpoeng) mer utsatt for uønsket dataaktivitet (datahendelser) og har dobbelt så stor risiko (15,7 prosentpoeng) for å for å få frastjålet datautstyr som de som ikke driver FoU.

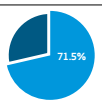
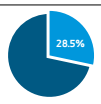
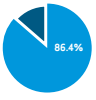
Virksomheter som innehar immaterielle rettigheter er ca 60 % (16 prosentpoeng) mer utsatt for uønsket dataaktivitet enn dem som ikke har immaterielle rettigheter. De er også mer utsatt for tyveri av datautstyr enn andre virksomheter, men dette kan muligens forklares ved andre faktorer.

Undersøkelsens andre deler viser at FoU- og IPR-virksomheter ikke er bedre til å sikre seg enn andre virksomheter i Norge. Dette er betenkelig.

Tabell 13: Innehar virksomheten IPR?
Tyveri av IT-utstyr:

Driver din virksomheten FoU?	Tyveri av IT-utstyr NEI	Tyveri av IT-utstyr JA
JA		
NEI		
VET IKKE		

Tabell 14: Driver din virksomheten FoU?
Tyveri av IT-utstyr:

Innehar virksomheten IPR?	Tyveri av IT-utstyr NEI	Tyveri av IT-utstyr JA
JA		
NEI		
VET IKKE		

8 TILTAK

Det er en klar sammenheng mellom bruk av sikkerhetstiltak og bedriftens størrelse. Små bedrifter er underrepresentert i forhold til å ta i bruk en rekke sikkerhetstiltak sammenlignet med store bedrifter. Denne tendensen er den samme i datamaterialet for 2010 som i 2008.

Utvalget har derfor valgt å kommentere kun de store endringene.

8.1 Organisatoriske tiltak - Analyse
Som nevnt innledningsvis er store bedrifter flinkere enn små til å ta i bruk en bredde av sikkerhetstiltak, men det er likevel ingen forskjell når det gjelder å ha pekt ut en IT-ansvarlig eller ikke. Vel halvparten av bedriftene har pekt ut en IT-ansvarlig. Datakrimutvalget mener at det er en svakhet at ikke alle bedriftene har pekt ut en IT-ansvarlig.

Formelle tiltak som planer og rutiner/ retningslinjer har større utbredelse enn tiltak som går på evnen å være forberedt dersom en krisesituasjon skulle oppstå. Mens hver fjerde bedrift har planer for å håndtere et brudd, er det bare én av ti bedrifter som faktisk gjennomfører systematiske øvelser, noe som er viktig for å teste og oppdatere kriseplanene. Omlag annenhver bedrift gir sine ansatte opplæring.

Virksomheter innen undervisning, helse/ sosial og personlig tjenesteyting er best på å ha tiltak rettet mot å øke ansattes bevissthet i forhold til informasjons-sikkerhet. Bygg og Anlegg er svakest på å innføre organisatoriske sikkerhetstiltak, mens 8 av 10 bedrifter innen helse/ sosial/personlig tjenesteyting har retningslinjer for ansattes bruk av virksomhetens IT-systemer, gjelder dette bare hver fjerde bedrift innen bygg og anlegg.

Se Tabell 15

Retningslinjer
Blant 70 % av bedriftene som har retningslinjer for ansattes bruk av IT, har ca. 40 % retningslinjer for bruk av eksterne lagringsmedier og mobiltelefon, mens ca. 30 % har retningslinjer for bruk av nettsamfunn. Retningslinjer for nettsamfunn har hatt en økning, opp fra 21 % i 2008. Offentlig administrasjon er dårligst på spesielle retningslinjer for nettsamfunn, kun 17 % av organisasjonene her har slike retningslinjer.

Se tabell 16

59 % av bedriftene har generelle retningslinjer for behandling av informasjon generelt, og 46 % har retningslinjer for omtale av virksomheten. Men bevisstheten rundt den mest verdifulle informasjonen er svært mangelfull. Dette vises ved at kun 20 % av bedriftene klassifiserer informasjon og gjør verdivurderinger. Kun hver tiende bedrift har retningslinjer for behandling av informasjon i forbindelse med forskning og utvikling og beskyttelse av immaterielle rettigheter. Industrien er best, her har 21 % av bedriftene retningslinjer for FoU prosjekter. Til sammenligning er det bare 2 % av bedriftene i bygg og anlegg og offentlig sektor som har retningslinjer for FoU-prosjekter.

Dette spørsmålet er nytt, og det er derfor ingen sammenligningsmuligheter med tidligere undersøkelser.

Se Tabell 17

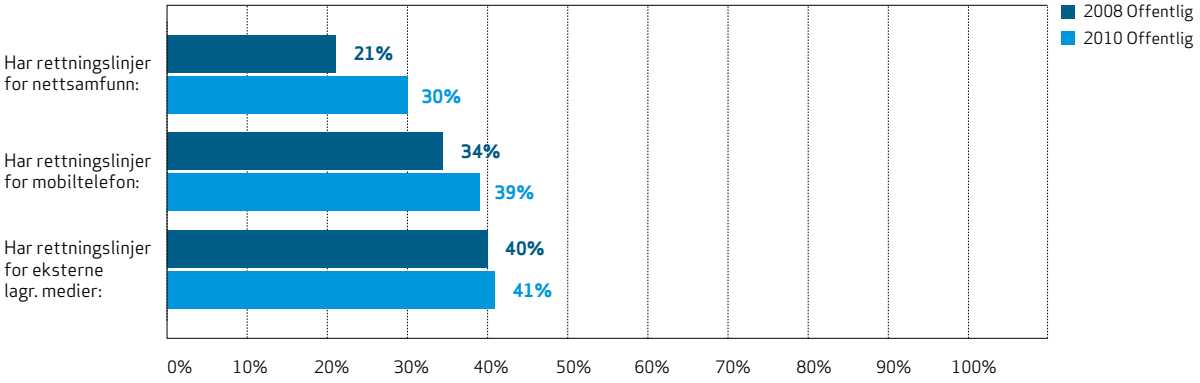
Oppfølging av retningslinjene
Retningslinjer har liten verdi om de ikke følges opp. De kan følges opp gjennom ulike tiltak, alene eller i kombinasjon. Hver tredje bedrift har rapportert at de ikke følger opp retningslinjene. Her er det ingen forskjeller mellom bransjene. 59 % av bedriftene følger opp retningslinjene gjennom interne kontroller, 39 % gjennom rapportering til ledelse og 24 % av bedriftene følger opp retningslinjene gjennom ekstern kontroll.

Se tabell 18

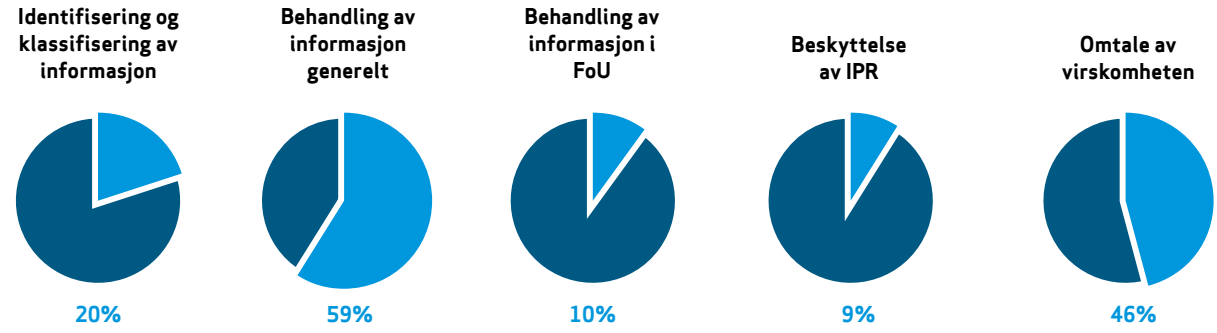
Tabell 15: Oversikt over organisatoriske tiltak – prosentandel ja-svar:

Virksomheten har følgende organisatoriske tiltak	2006	2008	2010
Retningslinjer for ansattes bruk av virksomhetens IT-systemer	65 %	67 %	71 %
Retningslinjer for sikker drift		82 %	77 %
Planer for håndtering av IT-sikkerhetsbrudd	26 %	40 %	40 %
Gjennomfører systematiske øvelser knyttet til IT-beredskap	9 %	12 %	11 %
Kan håndtere IT-sikkerhetsbrudd utenfor arbeidstiden	39 %	47 %	48 %
Har IT-sikkerhetsansvarlig			57 %
Ansatte undertegner taushetserklæring	43 %	59 %	66 %
Gir opplæring ved ansattelse	40 %	43 %	42 %
Gis regelmessig opplæring etter ansettelse			31 %
Må undertegne retningslinjer for IT-bruk			34 %
Verdivurdering, beskyttelse av FoU og immaterielle retningslinjer			

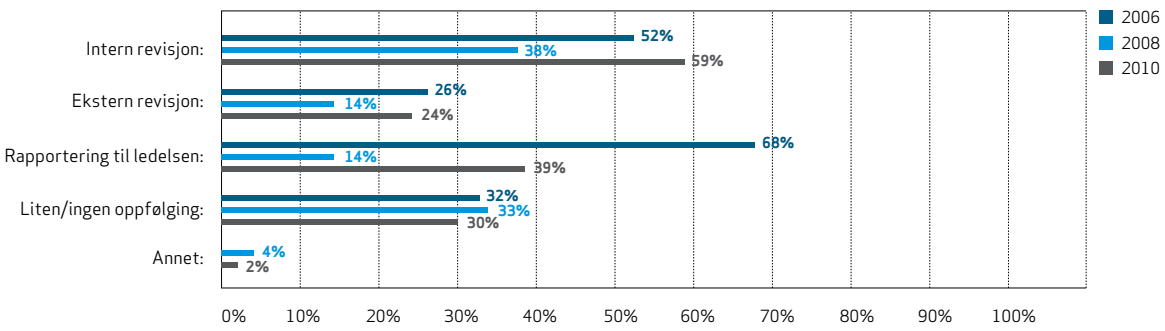
Tabell 16: Retningslinjer – prosendandel ja-svar :
(Verdivurdering, beskyttelse av FoU og immaterielle retningslinjer)



Tabell 17: Immaterielle rettigheter og forskning – prosentandel ja-svar:
Har virksomheten i 2010 utarbeidet retningslinjer i forhold til...



Tabell 18: Oppfølging av retningslinjene – andel ja-svar blant dem som har retningslinjer:



Virksomheter innen kritisk infrastruktur er best på organisatoriske tiltak

Virksomheter innen kritisk infrastruktur har i større grad enn andre virksomheter tatt i bruk ulike organisatoriske tiltak, for eksempel retningslinjer for ansattes bruk av IT (82 % mot 67 %), følger opp disse via intern kontroll (68 % mot 56 %) og ekstern kontroll (33 % mot 22 %) og gir sine nyansatte opplæring i informasjonssikkerhet (50 % mot 39 %). Det er ingen forskjell når det gjelder retningslinjer for sikker IT-drift (patching, oppdatering av programvare etc.) og evne til å håndtere IT-sikringsbrudd utenfor arbeidstiden, eiheller noen forskjell når det gjelder sikring av FoU og IPR.

Anbefalinger:

- Utarbeide retningslinjer for brukerne i de bransjer hvor dette ikke benyttet
- Opplæring og holdningsskapende arbeid
- Bedre oppfølging av retningslinjer for å sikre etterlevelse

8.2 Teknologi

Det er stort sett en økning i bruken av tekniske sikringstiltak i virksomhetene. Økningen er størst blant de mindre virksomhetene, mens det er de store virksomhetene som har implementert flest tiltak. Som eksempel kan nevnes oppdeling av nettet i ulike sikkerhetssoner.

8.2.1 Sikringstiltak

Andelen virksomheter som deler nettet i sikkerhetssoner er dobbelt så stor blant de største virksomhetene som blant de minste (79 % kontra 40 %). Det er fortsatt veldig få virksomheter som har tatt i bruk biometrisk autentisering, det vil si bruk av for eksempel fingeravtrykk.

Se tabell 19

Det er, naturlig nok vil nok mange si, de enkleste og rimeligste tiltakene som har den største økningen fra 2008. Eksempler på dette er bruken av filter mot uønsket web-trafikk og bruken av personlig brannmur. Disse to tiltakene har hatt en økning på henholdsvis 18 og 13 prosentpoeng siden forrige undersøkelse. Det anbefales imidlertid å gjennomføre risikoanalyser først og deretter bestemme sikringstiltak ut fra disse.

Svarene på både dette og andre spørsmål kan tyde på at det er for liten kunnskap om informasjonssikkerhet blant daglig leder, økonomiansvarlig og andre roller som ikke har informasjonssikkerhet som sin primære arbeidsoppgave. Det er en gjennomgående trend at Sikkerhetsansvarlig gir flere positive og færre vet ikke-svar både når det gjelder tiltak og registrerte hendelser.

Anbefaling:

- Risikoanalyser før sikringstiltak implementeres
- Opplæring

8.2.2 Oppdatering av programvare

Det er små endringer fra 2008 til 2010, men resultatene kan tyde på at det er færre som aldri oppdaterer sin programvare eller gjør det på tilfeldig basis.

Det anbefales at all programvare oppdateres automatisk eller umiddelbart så snart en patch eller en ny versjon er tilgjengelig og tilfredsstillende testet i virksomhetens miljø. Hvis vi slår sammen disse to gruppene så blir

Tabell 19: Sikringstiltak	2008	2010	Endring i %
Fysiske autentiseringsmekanismer	19 %	26 %	37 %
Biometrisk autentisering	6 %	4 %	-33 %
Personlig brannmur	50 %	64 %	28 %
IDS	27 %	30 %	11 %
VPN	61 %	61 %	0 %
Ulike sikkerhetssoner	54 %	63 %	17 %
Avlåst datarom	69 %	72 %	4 %
Kryptering av bærbare media	19 %	23 %	21 %
Duplisering av kritiske komponenter	50 %	53 %	6 %
UPS	76 %	71 %	-7 %
Digital signatur	12 %	20 %	67 %
Filter mot uønsket web-trafikk	52 %	70 %	35 %
Admin-rettigheter på PC er fjernet	-	41 %	-
IT-systemene herdes	-	54 %	-

tallene 85 %, 56 %, 41 % og 26 % for henholdsvis anti-virus, OS, annen SW og rutere. De aller fleste oppdaterer anti-virus programvaren sin, og over halvparten oppdaterer også operativ-systemet. Men når det gjelder annen programvare og nettverkskomponenter er situasjonen mye dårligere. Og det er disse programmene som i stadig større grad brukes av uvedkommende for å få tilgang til informasjon eller ressurser.

Det blir mer vanlig at sårbarheter i programmer som Flash Player, Adobe Reader og Microsoft Office utnyttes av kriminelle. Da er det ikke bra at 12 % av de som har svart på undersøkelsen sier at denne typen programvare aldri oppdateres eller at det kun skjer tilfeldig.

Anbefaling:
I tillegg til at all programvare bør holdes oppdatert til enhver tid, bør alle programmer som ikke lenger er i bruk avinstalleres for å hindre at svakheter i disse kan utnyttes av kriminelle.

8.3 Prosesser og rutiner

8.3.1 Gjennomgang av logger
Det er de minste virksomhetene som er dårligst til å logge. Her er det 16 % som sier at de ikke logger, og det er kun 18 % som gjennomgår loggene regelmessig. Her er det også hele 28 % som ikke vet noe om dette temaet. Av de største virksomhetene er det kun 3 % som ikke logger, mens 10% ikke gjennomgår loggene eller ikke vet om de gjør det.

70 % gjennomgår loggene en eller annen gang. Dette er det samme som i 2008. Men det er kun 29 % som gjennomgår loggene sine regelmessig. Virksomhetene lever tydeligvis i god tro og setter sin lit til at eventuelle uønskede hendelser oppdages på andre måter. Dette er sannsynligvis en av hoved-årsakene til at virksomhetene rapporterer om så få uønskede hendelser i sine nettverk. Når man ikke går gjennom loggene sine, vet man heller ikke hva som skjer på nettverket.

Anbefaling
Gjennomgang av loggene er nødvendig for å oppdage uønskede hendelser, og det anbefales at loggene gjennomgås regelmessig og systematisk.

8.3.2 Risikovurderinger
70 % sier de gjennomfører risiko-vurdering løpende eller regelmessig på eksisterende systemer. Bare 23 % gjennomfører vurderingene sjelden.

I utvalget er det små variasjoner, og forskjellene avhenger i stor grad av virksomhetenes størrelse. Blant små virksomheter gjennomføres risiko-vurderinger løpende/regelmessig i 61 %, mens for store virksomheter gjennom-føres det i 77 %.

Anbefaling
I henhold til god sikkerhetspraksis, bør alle virksomheter gjennomføre risiko-vurdering ved endringer i organisasjon og ved større teknologiske endring-er. Dette er et godt virkemiddel til å bevisstgjøre lederne og ansatte om verdier og sikkerhetsaspekter som bør vurderes i virksomheten. Vi dere anbefaler det at virksomhetene gjennomfører en verdivurdering for å kartlegge kritisk informasjon med tilhørende sikkerhetsbehov.

Andelen virksomheter som deler nettet i sikkerhetssoner er dobbelt så stor blant de største virksomhetene som blant de minste (79 % kontra 40 %).

9 PERSONOPPLYSNINGSLOVEN

9.1 Datainnsamling

Datainnsamling og analyse

Det er 80 % som bekrefter at personopplysningsloven er kjent i undersøkelsen. Blant de virksomheter som har en sikkerhetsansvarlig er svarprosenten 94 % i motsetning til virksomheter hvor daglig leder og andre funksjoner har sikkerhetsansvaret i virksomheten, der svarene er henholdsvis 78 % (daglig leder) og 77 % (andre) som kjenner personopplysningsloven.

Se tabell 20

På dette området finner vi forskjeller innenfor sektorene privat, offentlig virksomhet. Datakrimutvalget antar at informasjonskampanjer og fokus fra datatilsynet innefor offentlig virksomhet viser en effekt på 2 og 3.

Analyse

Datakrimutvalget finner det urovekkende at nesten halvparten av virksomhetene ikke har utarbeidet oversikt over personopplysningene som de behandler i virksomheten. Endringen fra 2008 viser imidlertid en svak økning på 17 %. Det er liten forskjell på svarene blant virksomhetene innenfor de ulike størrelseskategoriene.

Se tabell 21

Som tabellen viser er det forskjell mellom offentlig virksomhet og privat sektor innenfor behandling av personopplysningene i virksomhetene. Offentlig sektor har en klar fremgang på etablering av rutiner og kontroller. Det offentlige har vært gjenstand for økt fokus og kampanjer innenfor personopplysningsloven, svarene i undersøkelsen indikerer at kampanjene har virket.

Det er imidlertid stor spredning blant de ulike funksjonene i virksomheten som svarene bekreftende på å ha kjennskap til personopplysningsloven, fra 51 % blant IT-ansvarlig til 67 % blant sikkerhetsansvarlig. Her får vi ulike svar avhengig av hvem som svarer på undersøkelsen. Utvalget tror dette har sammenheng med kunnskap og hva lederne får av rapporter.

Det er 67 % som sier de har etablert formelle rutiner for behandling av personopplysninger.

Det er også her overraskende stor forskjell på svarene fra de ulike funksjonene i virksomhetene. Blant økonomiansvarlig svarer 55 % ja til å ha etablert rutiner, mens daglig ledere lever i den tro at de har etablert rutiner, da 75 % svarer ja. Sikkerhetsansvarlig bekrefter i 75 % av tilfellene, mens det blant de som har IT-ansvarlige, er det 64 % som svarer ja, noe som er nærmest gjennomsnittet i undersøkelsen.

Med formelle rutiner burde det være en nær knytning til oppfølging eller intern kontroll blant virksomhetene. Svarene viser at det bare er 51 % som har intern kontroll med knytning til behandling av personopplysninger som er 16 % lavere enn de som har formelle rutiner etablert. Av dette leser vi at det ikke er fokus på intern kontroll i virksomhetene, utover de som blir testet.

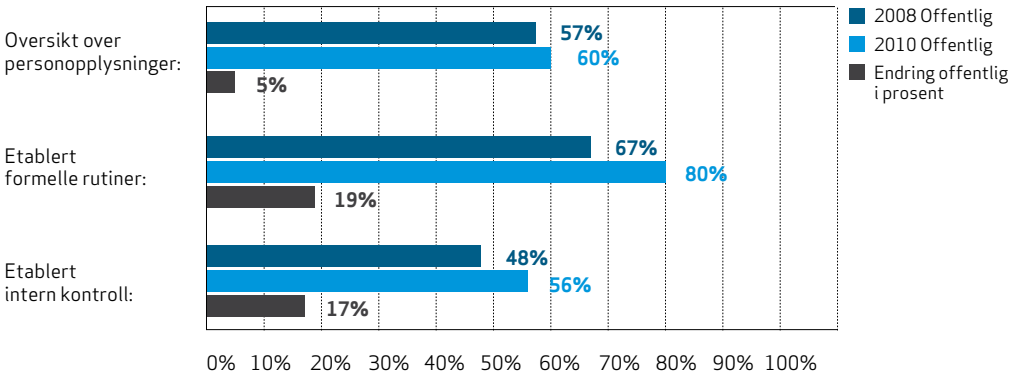
Tabell 20: (Det er 20 % i utvalget som ikke har fått spørsmålet)

Personopplysningsloven	2008	2010	Endring i prosent
Utarbeidet oversikt over personopplysninger som behandles? (Prosentvis av antallet virksomheter)	 JA: 48% NEI: 38% VET IKKE: 14%	 JA: 56% NEI: 33% VET IKKE: 11%	 17%
Etabler formelle rutiner for POL? (Prosentvis av antallet virksomheter)	 JA: 65% NEI: 23% VET IKKE: 11%	 JA: 67% NEI: 23% VET IKKE: 10%	 3%
Etablert Intern Kontroll for håndtering av Personopplysninger? (Prosentvis av antallet virksomheter)	 JA: 49% NEI: 34% VET IKKE: 18%	 JA: 52% NEI: 34% VET IKKE: 14%	 6%

Anbefalinger
Det bør gjennomføres opplæring og ytterligere informasjonskampanjer mot ansvarlige for at personopplysningsloven skal bli kjent og enkle eksempler på tiltak i henhold til kravene bør gjennomgås med ansvarlige i virksomhetene.

- Utarbeidet en oversikt over alle personopplysninger som behandles i virksomheten?
- Etablert formelle rutiner for personopplysninger?
- Etabler rutiner for behandling av personopplysninger på en sikker måte i hht. retningslinjene med internkontrolltiltak for oppfølging av at etablerte rutiner fungerer.
- Utarbeide oversikt over hvilke personopplysninger som behandles i virksomheten.
- Sette krav til anmeldelse av alle hendelser til politiet hvor personopplysninger er involvert.

Tabell 21: tabellen nedenfor viser offentlig sektor som svarer bekreftende på å ha etablert oversikt og rutiner i hht personopplysningsloven.



MED STØTTE FRA:

FNO Finansnæringens Fellesorganisasjon

TIPPING norsk-tipping.no

FORNYINGS-, ADMINISTRASJONS- OG KIRKEDEPARTEMENTET

SpareBank 1

Microsoft