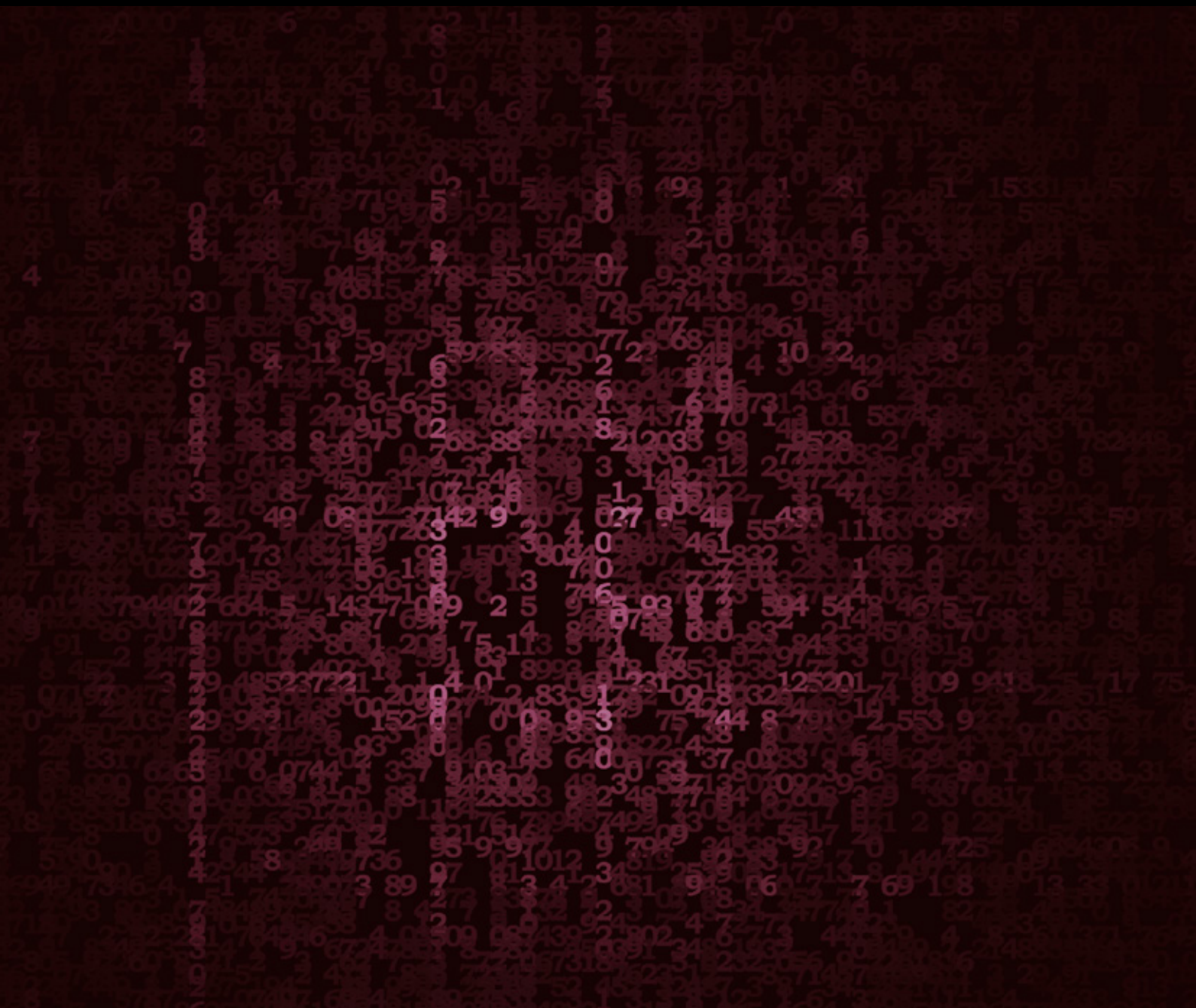
2012

Mørketallsundersøkelsen

- Informasjonssikkerhet og datakriminalitet

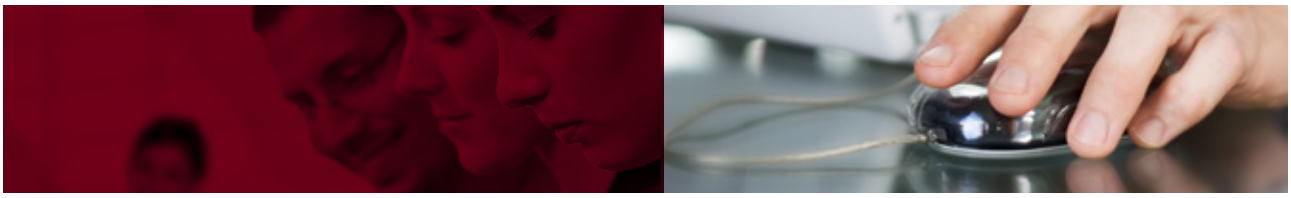


NÆRINGSLIVETS SIKKERHETSRÅD

Innhold

1	Innledning	3
2	Trusselen	4
2.1	Vurdering fra Norman	4
2.2	Vurdering fra Statoil	6
2.3	Vurdering fra NSM	6
3	Hovedfunn	8
4	Avhengigheter og bruk av IT	10
5	Outsourcing av IT-driften	12
5.1	IT-driftens organisering og bruk av IT	12
5.2	Outsourcing til utlandet	12
5.3	Krav til outsourcingspartner	12
5.4	Nettskytjenester	12
6	Hendelser og mørketall	14
6.1	Estimerte mørketall	14
6.2	Virksomheter som er mest utsatt	16
6.3	Informasjon på avveie	18
6.4	Hindre tilsvarende informasjonssikkerhetshendelser	19
6.5	Kostnader knyttet til informasjonssikkerhetshendelser	19
7	Sikkerhetstiltak	20
7.1	Organisatoriske tiltak	20
7.2	Teknologi	22
7.3	Prosesser og rutiner	23
7.3.1	Gjennomgang av logger	22
7.3.2	Risikovurderinger	25
7.4	Personopplysningsloven	25

1 Innledning



Næringslivets Sikkerhetsråd (NSR) har som formål å forebygge kriminalitet i og mot næringslivet. Et av virkemidlene er å informere om de kriminelle og sikkerhetsmessige trusler og trender vi ser i dag og forventer i fremtiden. Mørketallundersøkelsen™ har en sentral plass i opplysnings- og informasjonsstrategien mot næringslivet og offentlige myndigheter.

Mørketallsundersøkelsen™ 2012 er den 8. undersøkelsen som foretas av 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 TNS Gallup i april 2012. Tidsrommet for kartleggingen er 2011. Analysen er utført av Datakrimutvalget som i 2012 består av:

• Arne-Johan Helle, Telenor (leder)	www.telenor.no
• Christophe Birkeland, Norman	www.norman.no
• Eiliv Ofigsbø, NorCERT, Nasjonal sikkerhetsmyndighet (NSM)	www.nsm.stat.no
• Janne Hagen, Proactima	www.proactima.com
• Johnny Mathisen, Telenor Group	www.telenor.com
• Håvard Folkedal, Kriminalpolitisentralen (KRIPOS)	www.politi.no/kripos
• Tore Larsen Orderløkken, Norsk senter for informasjonssikring (NorSIS)	www.norsis.no
• Vidar Østmo, Broadnet /ITakt	www.broadnet.no/www.itakt.no
• Tone Thingbø, Ernst & Young	www.ey.com
• Kristine Beitland, NSR	www.nsr-org.no

I tillegg har Robin Stenvi og Peggy Heie fra NorSIS bistått aktivt i analysen.

Populasjon: Undersøkelsen omfatter norske virksomheter i privat og offentlig sektor med 5 ansatte eller flere. Utenfor undersøkelsen faller virksomheter som barnehager, barneparker, SFO, førskoler, kulturskoler, lønnet arbeid i private husholdninger, kinoer, borettslag, eierseksjonssameie, forening/lag/innretning, sokn/kirkeligfellesråd, og stiftelse m. fl.

Utvalg: Det er trukket ut 6000 virksomheter til undersøkelsen. I bruttoutvalget er det 4500 private virksomheter og 1500 offentlige virksomheter. I undersøkelsen er små virksomheter 5-19 ansatte, mellomstore fra 20-99 ansatte og store virksomheter er virksomheter med mer enn 100 ansatte.

Svarprosent: Totalt har 886 virksomheter svart på årets undersøkelse. Det gir en svarprosent på 15 % (12 % i 2010).

Når vi sammenligner sammensetningen av virksomheter som har svart med 2010, så er det en reduksjon i antall store virksomheter. For analysen av funnene betyr dette at noe av den generelle nedgangen i antall sikkerhetshendelser og sikkerhetstiltak vil kunne forklares ved en endring i bedriftssammensetningen fra 2010 til 2012.

2 Trusselen

Verdien av sensitiv informasjon og truslene mot skjermingsverdig informasjon øker, og tiltak for å redusere sårbarheten utvikles ikke i samme takt.

Politiets sikkerhetstjeneste (PST)[1] og Kripos[2] beskriver en økning i informasjonsspionasje og datakriminalitet. Kripos har i de siste årene registrert flere, hyppigere og mer alvorlige episoder av datakriminalitet, herunder en økning av datainnbrudd og dataskadeverk mot virksomheter. PST forventer mer fremmed etterretningsvirksomhet mot teknologibedrifter som driver med forskning og utvikling (FoU). Mørketallsundersøkelsen™ bekrefter trusselbildet ved at FoU virksomheter rapporterer om flere hendelser.

Hovedfunnene i Mørketallsundersøkelsen™ bekrefter at trusselbildet er økende. For å underbygge dette nærmere har vi hentet inn vurderinger fra offentlige og private aktører. I årets undersøkelse har Norman, Statoil og Nasjonal sikkerhetsmyndighet (NSM) beskrevet hendelser og trender innenfor sikkerhetsområdet.

2.1 Vurdering fra Norman

Norman ASA har fulgt utviklingen av ondsinnet programvare helt siden det aller første dataviruset ble funnet i 1986.

FakeAV og Ransomware

I begynnelsen av 2011 hadde vi mange hendelser med brukere som ble infisert med FakeAV. FakeAV er navnet på ondsinnet kode som, ved å gi brukerne falske meldinger om at de er infisert, lokker brukerne til å betale for å få renset maskinen. I andre kvartal 2011 ble store deler av betalingstjenestene som ble brukt av FakeAV tatt ned, og det resulterte i et kraftig fall i antall hendelser med FakeAV. Siden har dette antallet igjen økt, men likevel vært lavt i forhold til første kvartal. Det kan se ut til at bakmennene har gått over til å bruke Ransomware. Ransomware er en type ondsinnet kode som tar maskinen eller deler av maskinen/filer som «gissel», og krever løsepenger for at du igjen skal få tilgang til filene dine. Typisk fremgangsmåte er at alle dokumenter på maskinen krypteres, og deretter mottar du en melding om at du må betale et bestemt beløp for å få en nøkkel som kan brukes for å dekryptere dokumentene. Slik ondsinnet programvare har vært spredd via flere norske nettsider, og vi har mange rapporterte hendelser om dette.

Banktrojanere i Norge

Banktrojanere er betegnelsen på ondsinnet programvare som er laget for å stjele penger fra brukeres bankkonto. Det er mange typer banktrojanere, men noen få dominerer, særlig de russiske trojanerne Zeus og SpyEye. Deres sterke stilling kommer av at de er kommersialisert hyllevare, som videreselges til kriminelle. Det trengs ingen ekspertise for å bruke slike trojanere. Man trenger kun å konfigurere serverinstallasjonen, definere hvilke banker som skal angripes og på hvilken måte.

I 2011 skjedde det forandringer i forholdet mellom Zeus og SpyEye. For det første ble det rapportert at den mangeårige forfatteren av Zeus, Slavik, hadde solgt Zeus-kildekoden til Gribodemon/Harderman, forfatteren av SpyEye. Et innlegg på et online forum ga inntrykk av at de to trojanerne skulle smeltes sammen til et produkt, og noen likheter i koden til nyere versjoner så ut til å bekrefte dette. Imidlertid var dette trolig kun et rykte. SpyEye blir sannsynligvis ikke lenger oppdatert; den siste offisielle oppdateringen er 1.3.48, fra oktober 2011.

Deretter lekket en av de mest brukte Zeus-versjonene ut på Internett, og ble i praksis til åpen kildekode. Det resulterte i flere nye Zeus-varianter. Siden SpyEye ikke lenger videreutvikles, har mange brukere av SPyEye nå gått over til andre (og billigere) konkurrenter, kanskje særlig Zeus-avleggeren ICE-IX.

På det norske markedet ble 2011 dominert av SpyEye. Flere større norske banker ble forsøkt angrepet, i flere omganger. SpyEye er fremdeles i bruk, men i mindre omfang enn tidligere – igjen ser Zeus-baserte varianter ut til å være i vinden. Standard Zeus, ICE-IX, Citadel, Gameover (også kjent som P2P Zeus) og Gspy har også vært observert. På Internett blir ulike varianter diskutert og vurdert. ICE-IX fremheves som en godt skrevet avansert trojaner med god funksjonalitet, mens Citadel ofte karakteriseres som for kostbar. Noen eksempler på offentliggjorte nettbankangrep mot norske banker i 2011:

- Februar: SpyEye angrep mot flere norske banker.
- April: SpyEye angrep mot DNB NOR
- Mai: Zeus angrep mot DNB NOR
- Juni: SpyEye angrep mot flere norske banker.

[1] **Åpen trusselvurdering 2012**
http://pst.host.asplogon.com/Filer/utgivelser/trusselvurderinger/PSTsTrusselvurdering2012.pdf

[2] **Den organiserte kriminaliteten I Norge – Trender og utfordringer 2011 - 2012**
https://www.politi.no/vedlegg/lokale_vedlegg/kripos/Vedlegg_1581.pdf

APT (Advanced Persistent Threats)
I økende grad utføres industri-, politisk og militær spionasje ved datainnbrudd ved hjelp av ondsinnet programvare. Denne trusselen omtales ofte som "advanced persistent threats" (APT) fordi trusselaktørene tilsynelatende har betydelige ressurser og arbeider målrettet. Vi har sett eksempler på dette fra hele verden – også fra Norge.

Målene for slike innbrudd er nesten alltid informasjon som brukes til overvåking, undertrykking, militær dominans og teknologiske og økonomiske fordeler. I sjeldne tilfeller kan det også dreie seg om sabotasje. Det mest kjente eksemplet på det siste er Stuxnet i 2010.

Et APT angrep består typisk av en skreddersydd epost til en ansatt i en bedrift. Denne eposten er godt skrevet, og stilet til en eller flere navngitte personer i bedriften. Det er gjerne et vedlegg i eposten; alternativt en lenke som man blir oppfordret til å klikke på. Når mottageren av eposten åpner vedlegget, blir hans datamaskin infisert med en trojaner. Dette er gjerne første trinn - "foten i døra" - så og si. Trojaneren åpner for videre fjernstyring og nedlasting av mer avanserte verktøy. På dette stadiet vil det gjerne være reelle personer som logger seg på og utforsker de infiserte datasystemene. De studerer maskinen og nettverkets infrastruktur. De forsøker å få tilgang til flere ressurser på nettverket, og sikrer tilgang til det infiserte systemet ved for eksempel å opprette nye kontoer og justere brukerrettigheter, slik at de har flere veier inn i systemene. Fra nå av dreier det seg kun om hvor mye interessant informasjon de kan hente ut. Bedrifter som har vært utsatt for slike APT angrep, kan være uvitende om det i årevis, og det er sannsynlig at mange av de som har vært kompromittert aldri blir klar over hva som har skjedd.

Konklusjon
Trusselbildet varierer over tid. Driveren er hovedsakelig ROI - return of investment. Trusselaktørene forandrer fokus etter hvor det til enhver tid er lettest å tjene penger. I 2011 ble det vanskeligere å sikre inntjening på FakeAV-malware, og det er trolig forklaringen på oppblomstringen av utpressingsmodeller (Ransomware). Vi ser også at valg av banktrojanere er en kombinasjon av hvilke trojanere som er lettest å bruke, hvilke som har best supportapparat, og hvilke bankløsninger det er enklest å kompromittere.

Målrettede angrep og trusselen fra APT er økende. Kortsiktig gevinst kan være motivasjonen i enkelte scenarier, men det dreier seg også om strategiske mål (for eksempel langsiktige økonomiske interesser), eller innenrikspolitisk overvåkning slik vi har sett eksempler på fra land som Kina og Syria.

Økende gap mellom trussel og sikkerhetstiltak.

2.2 Vurdering fra Statoil

Over de siste årene har vi sett at trusselbildet for nettangrep har endret seg for vårt selskap. Vurderingene tar utgangspunkt i de områdene hvor vi opplever at viktigheten av informasjonssikkerhet har økt.

Forretningsutvikling

Innenfor forretningsutvikling, hvor en arbeider med internasjonale prosjekter med stor strategisk og finansiell betydning, ser vi at eksterne aktører i økende grad forsøker å tilegne seg informasjon. Tilgang til slik informasjon kan utnyttes for å oppnå økonomisk gevinst. Statoil opplever jevnlig målrettet nettangrep i kombinasjon med sosial manipulering (social engineering) mot slike forretningsutviklingsprosjekter.

Teknologiutvikling

Statoil er et selskap som kontinuerlig utvikler ny teknologi og har eierskap i en del patenter. Utvikling og riktig bruk av teknologi har bidratt til å føre Statoil ditt det er i dag, og er et viktig konkurransefortrinn. Informasjon knyttet til teknologiutvikling har en veldig høy verdi i markedet. Forskningsmiljøet er spesielt utsatt for målrettet nettangrep, inklusiv sosial manipulering, og hvor avanserte angrepsformer som Advanced Persistent Threat (APT) blir brukt for uthenting av informasjon.

Industriell IT på anlegg

Industrielle kontrollsystemer, som styrer kritiske systemer på våre anlegg,er i ferd med å ta i bruk mer standard teknologi. Det har medført at disse systemene er nå mer utsatt for de samme type angrep som man har opplevd på de mest brukte operativsystemer og kontorstøtteløsninger. De kjente virusene Stuxnet og Duqu, som var direkte rette mot kontrollsystemer, har bidratt til at verden har fått øynene opp for denne problemstillingen.

Utfordringen innenfor industriell kontrollsystemer er at to ulike fagområder, automasjonsteknologi og informasjonsteknologi, er i ferd med å møte hverandre. Videre er det helt avgjørende at både bransjen og leverandørene av disse løsningene samarbeider for å gjøre disse kontrollsystemene mer sikre.

Aktivisme

Internasjonale olje og gass selskaper er ofte utsatt for oppmerksomhet fra grupperinger som bruker nettangrep som virkemiddel for å få fokus på sine saker. En vanlig angrepsform som benyttes er å overbelaste selskapene hjemmesider slik at de blir utilgjengelig. I de senere år har vi sett at disse grupperingene stjeler informasjon som legges ut på internett. Dette er en trussel som Statoil tar på alvorlig og som følges nøye.

Samhandling og organisasjonsutvikling

Teknologien som benyttes i informasjonsutveksling mellom mennesker utvikler seg raskt og gir nye informasjonssikkerhets utfordringer for virksomheter. Bruk av sosiale medier sammen med nye plattformer (smarttelefoner, nettbrett…) gir nye samarbeidsmønstre. Når vår virksomhet også vokser internasjonalt, som introduserer kulturelle forskjeller, er det viktig at vi lager forståelige retningslinjer for samhandling som reduserer risikoen for at kritisk informasjon havner i de feile hender.

2.3 Vurdering fra NSM

Sikkerhetstilstanden blir fortsatt svekket i Norge. Risikoforståelsen er fortsatt for lav, og viktige tiltak som risikovurderinger, kompetanseheving, rapportering og sikkerhetsrevisjoner blir ikke gjennomført.

Nasjonal sikkerhetsmyndighet (NSM) vurderer at vi har fått en situasjon med økende sikkerhetsmessig risiko. Det er vesentlige mangler i det forebyggende sikkerhetsarbeidet med konsekvenser for den nasjonale sikkerhetstilstanden. Den grunnleggende hovedutfordringen er at den generelle risikoforståelsen på alle samfunnsnivåer er på et utilfredsstillende nivå. Dette representerer en sårbarhetsutfordring, da manglene kan utnyttes av trusselaktører med stadig økende kapabiliteter og kapasiteter.

- Det er generelt slik at de *verdier* vi ønsker å beskytte øker i volum og betydning i takt med samfunnsutviklingen og den økende produksjonen av informasjon.
- Truslene mot skjermingsverdig informasjon er i sterk økning; særlig at den teknologiske oppfinnsomheten med hensyn til utvikling av skadevare på IKT-systemer akselererer. Trusselaktørene blir både mer selektive i sine mål og mer avanserte i sine metoder.
- Sårbarheter som kan utnyttes oppdages stadig, og dette øker mulighetene for at uvedkommende får tilgang til skjermingsverdig informasjon.
- Tiltak for å redusere sårbarheter utvikles ikke i samme takt som truslene og er i utgangspunktet utilstrekkelige.

Store sikkerhetsutfordringer
Det har tidligere vært påvist et økende gap mellom trussel og sikkerhetstiltak. Trenden er at dette gapet fremdeles øker. Samtidig er det slik at verdien av samfunnets sensitive og skjermingsverdige informasjon øker.

NSM har registrert alvorlige sårbarheter hos virksomheter som leverer samfunnskritiske tjenester. Disse sårbarhetene kan bli, og har blitt, avdekket og utnyttet på en måte som kan få store sikkerhetspolitiske og/eller økonomiske konsekvenser.

Mange virksomheter mangler gode styringssystemer for forebyggende sikkerhet. Dette kan føre til sikkerhetsorganisasjoner som ikke er dimensjonert for risikoen de skal håndtere og at ledelsen ikke setter av tilstrekkelig ressurser og kompetanse til arbeidet. Ofte er heller ikke virksomhetenes styringssystem for forebyggende sikkerhet koordinert med andre styringssystemer.

Menneskelige faktorer, som grunnleggende risikoforståelse, kunnskap, kompetanse, vilje, forståelse og holdninger må være på plass for at organisatoriske og tekniske aspekter ved sikkerhetsarbeid skal fungere etter sine intensjoner. Med dårlig risikoforståelse blir kvaliteten på det forebyggende sikkerhetsarbeidet utilfredsstillende. Virksomheter mangler ofte nødvendig oversikt over hvilke verdier de besitter og eventuelt må beskytte. Trusselaktører, med stadig økende resurser og kapasiteter, har en rekke metoder og virkemidler de kan ta i bruk for å utnytte sårbarheter og realisere sine mål. Dette ble bekreftet gjennom avdekking av flere alvorlige spionasjeforsøk i 2011.

Vi lever i et nettverkssamfunn, hvor to eller flere samfunnsfunksjoner ofte er avhengige av hverandre. Et angrep på, eller skader ved en enkelt funksjon eller et objekt kan derfor få konsekvenser som rekker langt utover skadene eller tapet på den direkte rammede samfunnsfunksjonen.

Alvorlige svakheter og hendelser
Viktige IKT-systemer blir ofte ikke tilstrekkelig beskyttet og sikret. Konsekvensen kan blant annet være at spionasjeoperasjoner med potensielt store konsekvenser kan gjennomføres i Norge uten å bli oppdaget. Gjennom inntrengingstesting i både sivil og militær sektor har NSM påvist svært alvorlige svakheter. Svakhetene kan gi tilgang til både å manipulere, endre og slette både svært sensitiv informasjon. Testene viser at det koster lite å bryte seg inn i mange kritiske datasystemer. Dette er svakheter som har kunnet gi en aktør tilgang til, og mulighet til å manipulere, endre og slette, både svært sensitiv informasjon og høyt gradert informasjon.

Finanskriminalitet fra ikke-statlige aktører er vedvarende høy og økende. Kriminell aktivitet på Internett er betydelig høyere enn det antall saker som rapporteres eller anmeldes. Dette inkluderer blant annet kortsvindel, nettbankbedrageri, datainnbrudd og nettaktivisme.

Det også er økende hyppighet og utbredelse av industrispionasje. Denne aktiviteten antas å være mer utbredt enn det som oppdages, da mange bedrifter mangler kapasitet og evne til å detektere og håndtere slike angrep. I Storbritannia ga Cabinet Office i februar 2011 ut en rapport som forsøker å kalkulere kostnadene relatert til internettkriminalitet. Omgjort til norske forhold tilsier rapporten at kostnaden for Norge kan beløpe seg til over 20 milliarder kroner pr år.

Betegnelsen "hacktivister" brukes om personer og grupperinger som fremmer et politisk, religiøst eller nasjonalistisk budskap gjennom forskjellig type aktivitet på Internett. Det har vært flere tilfeller av nettaktivisme i Norge gjennom 2011, for eksempel tyveri og offentliggjøring av norske stortingspolitikeres personnummer og tjenestenektangrep mot politiske partier som støtter datalagringsdirektivet.

Trender
I tiden fremover er det god grunn til å holde øye med følgende trender:
- En fortsatt økning i alvorlige IKT-hendelser
- Mer profesjonell utvikling av ondsinnet programvare
- Målrettede angrep mot lukkede nett
- Forsøk på å infiltrere prosesskontrollsystemer
- Spredning av skadevare over mobile enheter
- Misbruk av og infisering av smartkort og smartkortlesere
- Sårbarheter i leverandørkjeden av IKT-utstyr

3 Hovedfunn

Mørketallsundersøkelsen™ viser at det er et større gap enn tidligere mellom trusler og sikkerhetstiltak blant norske virksomheter parallelt med at IT-avhengigheten øker. Norske virksomheter, særlig ledere, mangler kunnskap om informasjonssikkerhet og har ikke oversikt over trusler og hendelser. Dette kan forklare at mange virksomheter ikke har tatt i bruk tilgjengelige sikkerhetstiltak og heller ikke fokusert på sikkerhetskultur. Under følger de viktigste funnene.

Økt sårbarhet

Virksomheter i Norge tar i bruk mer teknologi, spesielt e-post på mobiltelefoner, og er mer aktive på sosiale medier, men mangler ofte retningslinjer.

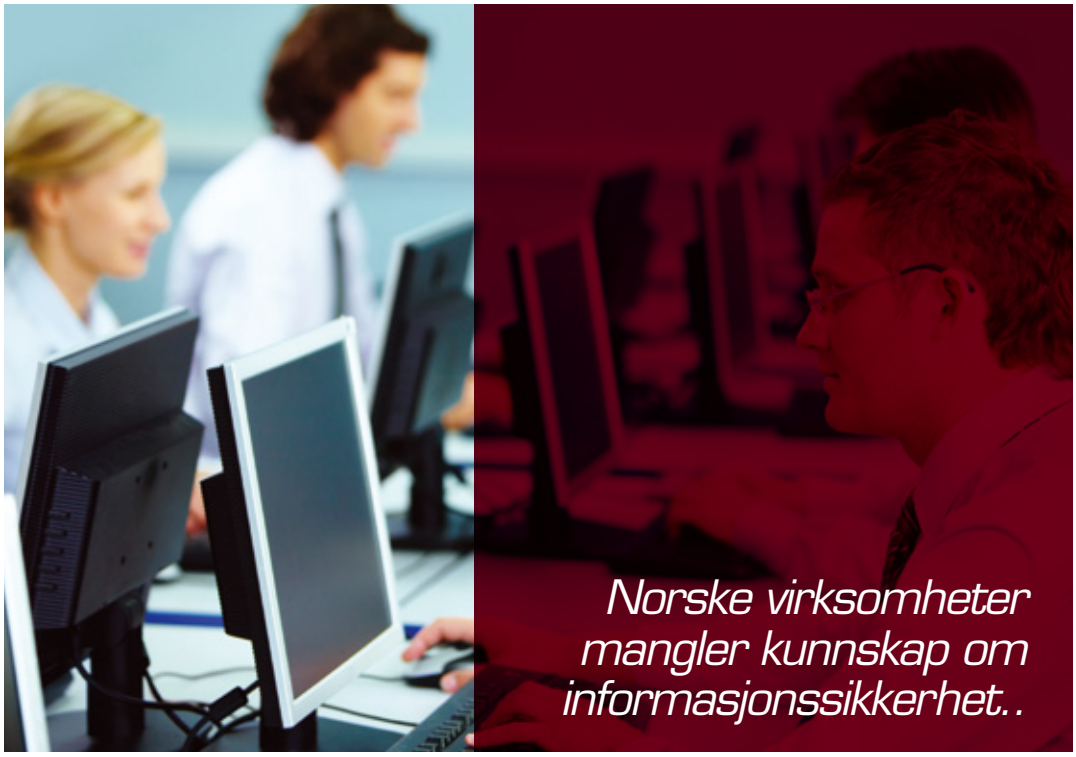
- 62 % av norske virksomheter svarer at det er kritisk når IT- systemene er nede inntil 1 dag.
- Det er en synkende sikkerhetsbevissthet i norske virksomheter, blant annet på grunn av manglende styrings- og monitoreringssystemer av hendelser, til tross for at IT-avhengigheten og trusselen øker.
- Halvparten av virksomhetene har tatt i bruk en form for nettskytjeneste, men et fåtall har retningslinjer.
- Virksomheter tar i bruk ny teknologi uten å foreta risikoanalyser og etablere retningslinjer. Dette gjør virksomhetene særlig sårbare for sikkerhetshendelser.

Hendelser

- Det er store mørketall mellom faktiske hendelser registrert hos virksomhetene, og forhold anmeldt til politiet.
- Den viktigste årsaken til at hendelser ikke blir anmeldt er at virksomhetene mener saken er ubetydelig.
- Store virksomheter som har immaterielle rettigheter (IPR) eller bedriver forskning og utvikling (FoU) er mer utsatt enn andre virksomheter for dataangrep, men er totalt sett bedre sikret.
- 13 % av virksomhetene har opplevd tyveri av IT-utstyr, mens kun 1 % oppgir tyveri av informasjon. Dette viser manglende forståelse for verdi og konsekvensene ved tyveri av informasjon.
- Tap av minnepinne og e-post sendt til feil adressat oppgis som de viktigste årsakene til at informasjon kan ha kommet på avveie det siste året.

Utfordringer i sikkerhetsberedskap og tiltak

- Av daglig ledere, som er øverste ansvarlige for sikkerhet og beredskap, svarer 1 av 5 at de ikke



vet om det gjennomføres risikoanalyser i egen virksomhet.

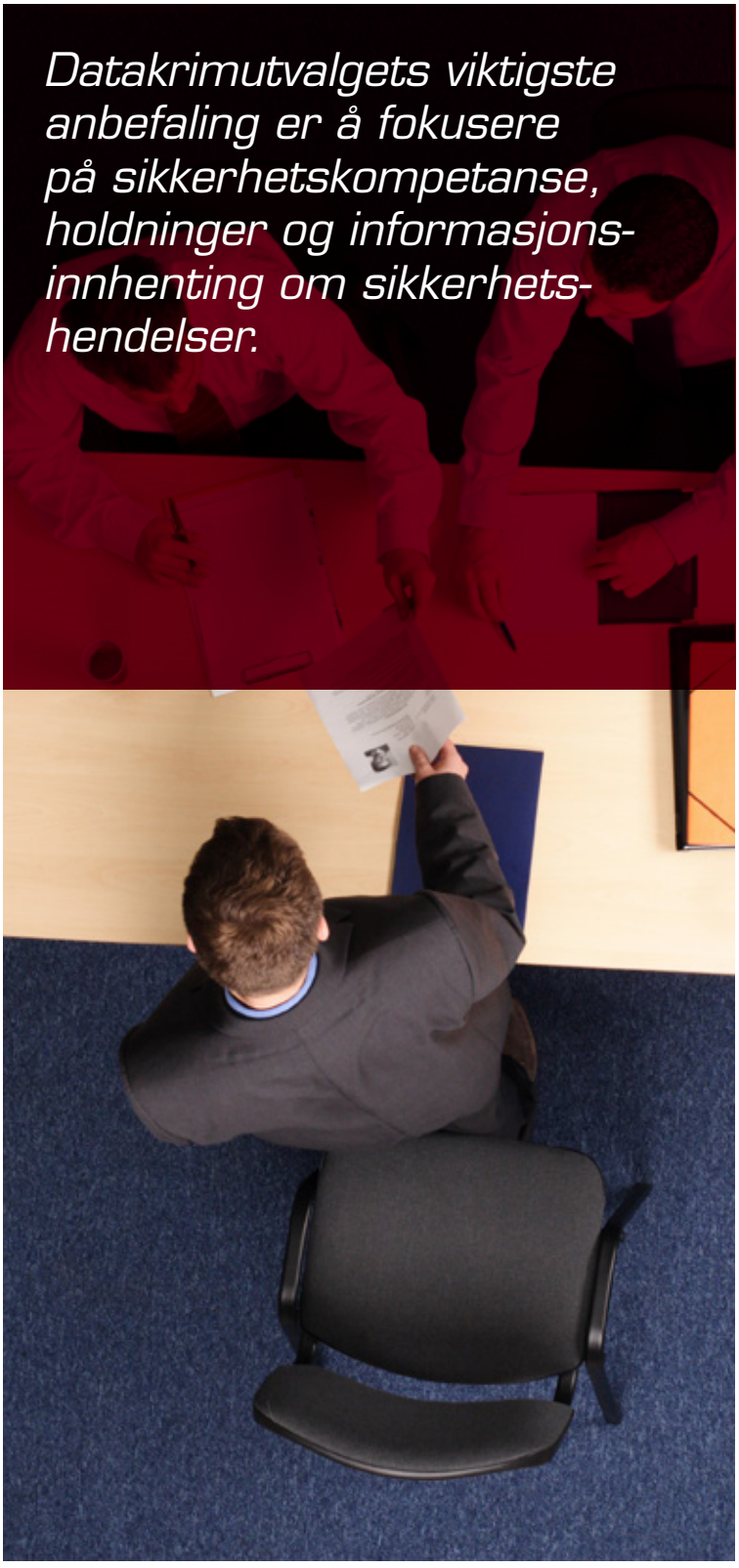
- Bare 1 av 3 virksomheter har beredskapsplaner. Av disse igjen er det 1 av 3 som har krav til at det gjennomføres øvelser.
- 12 % av de som har opplevd en hendelse har ikke fulgt opp med forbedringstiltak for å forebygge nye hendelser.
- Oversikt over hendelser er mangelfull på grunn av lite utbredt monitorering og logging i norske virksomheter, samt hendelsesrapportering til leder.
- Bare 1 av 6 virksomheter har retningslinjer for gjennomføring av verdivurdering.
- 1 av 6 ledere vet ikke om det er utarbeidet en oversikt over virksomhetens personopplysninger.
- Bare 4 av 10 ansatte får opplæring ved nyansettelser. Av disse er det 4 av 10 som får kontinuerlig sikkerhetsopplæring. Dette til tross for at det er ansatte som oppdager flest hendelser, og eksterne angrep er ofte rettet mot ansatte og ikke teknologi.
- Over halvparten av virksomhetene outsourcer hele eller deler av IT-driften, men sikkerhetsbevisstheten synker ved at det stilles færre krav til eksterne leverandører.
- 1 av 3 virksomheter vet ikke kostnaden knyttet til sikkerhetshendelser.

Hovedanbefalinger

Datakrimutvalgets viktigste anbefaling er å fokusere på sikkerhetskompetanse, holdninger og informasjonsinnhenting om sikkerhetshendelser.

- Bevissthet, kompetanse og sikkerhetskultur må økes blant ledere og ansatte.
- Gjennomfør verdivurdering, risikoanalyse og iverksett tiltak.
- Utarbeid beredskapsplaner og gjennomfør øvelser.
- Hendelsesrapportering til ledere, inklusiv verditap.
- Anmeld alle straffbare forhold.
- Utarbeide retningslinjer når ny teknologi tas i bruk, som sosiale medier og nettskytjenester.

I det etterfølgende vil vi gå nærmere inn på de enkelte funnene i undersøkelsen. Under hver av drøftelsene finner en de mest sentrale anbefalingene fra Datakrimutvalget.



4 Avhengigheter og bruk av IT

I Mørketallsundersøkelsen™ har vi kartlagt hva norske virksomheter bruker informasjonsteknologi til. Som tidligere har vi fokusert på mobile enheter. I tillegg har vi i år kartlagt bruk av sosiale medier og nettskytjenester.

Når det gjelder kritisk tid svarer 62 % av norske virksomheter at det er kritisk når IT-systemene er nede inntil 1 dag. 27 % av virksomhetene svarer at de opplever det kritisk når IT-systemene er nede 1 time. Ytterligere 35 % av virksomhetene rapporterer at det er kritisk for virksomheten når viktige IT-systemer er nede 1 dag.

Dette understreker behovet for beredskapsplaner, og at virksomheter øver på realistiske scenarioer for raskt å gjenopprette normal drift etter en sikkerhetshendelse. De øvrige virksomhetene opplever det ikke kritisk om IT-systemene er nede i mer enn en dag. 2 % som svarer «vet ikke». Dette er svært bekymringsfullt, og viser manglende forståelse blant ledere for beredskapsarbeidet.

55 % av virksomhetene har satt bort hele eller deler av IT-driften til en ekstern samarbeidspartner. 37 % av disse har ikke krav til tilgjengelighet eller oppetid, se kapittel om outsourcing.

5 om outsourcing av IT-driften

Norske virksomheter fortsetter å ta i bruk informasjonsteknologi på nye områder. Mørketallsundersøkelsen™ viser at sammenlignet med tidligere år er det en klart økende andel virksomheter som sier de mottar e-post på mobiltelefon, hele 71 %. Dette er en økning på 7 prosentpoeng fra 2010. Blant de store virksomhetene er bruken av e-post på mobil hele 86 %.

Halvparten av norske virksomheter benytter en eller annen form for nettskytjenester, men kun 9 % har retningslinjer for bruk.

På tiltakssiden er det bare 24 % av virksomhetene som krypterer bærbare media, og 29 % har retningslinjer for sikker bruk av mobiltelefon. Virksomhetene er således særlig sårbare ved tap/tyveri av IT-utstyr. Gapet mellom offentlig og privat sektor minsker når det gjelder bruk av e-post på mobil.

I tillegg har sosiale medier stor betydning. 16 % av virksomhetene benytter sosiale medier for intern kommunikasjon. 36 % av virksomhetene har tatt i bruk sosiale medier for ekstern kommunikasjon, men kun 36 % av disse har utarbeidet retningslinjer for sikker bruk.

Se tabell 1

Anbefalinger

- Utfør risikoanalyse før ny teknologi tas i bruk.
- Utarbeid retningslinjer for bruk av sosiale medier og nettskytjenester. Les mer om hvordan du kan gjøre dette hos NSR
- Beskytt bærbart utstyr

62 % av norske virksomheter svarer at det er kritisk når IT-systemene er nede inntil 1 dag.

Viktige tiltak for å beskytte bærbart utstyr:

- Tilgangskontroll.
- Kryptering, spesielt hvis enheten inneholder sensitiv/virksomhetskritisk informasjon.
- Fjernsletting, fjernsporing og maks antall passord som kan tastes inn.
- Retningslinjer på hva ansatte har lov til å gjøre (eksempel administrasjonsrettigheter).

Tabell 1: Hvordan bruker virksomhetene informasjonsteknologi?

	2008	2010	2012
Mottak av e-post på mobil	54 %	64 %	71 %
Selger varer og nettbaserte tjenester	27 %	25 %	20 %
Kjøper varer og nettbaserte tjenester	66 %	71 %	67 %
IP-telefoni	29 %	33 %	33 %
Instant Messenger	31 %	33 %	26 %
Trådløse nettverk	61 %	72 %	76 %
Internettkommunikasjon mellom avdelingskontor[3]	48 %	46 %	64 %
Kunder/partnere har tilgang	39 %	35 %	41 %
Sosiale medier for intern kommunikasjon	-	-	16 %
Sosiale medier for ekstern kommunikasjon[4]	3 %	22 %	39 %

[3] **2010**: WAN-kommunikasjon mellom avdelingskontorer

[4] **2010:** Legger ut informasjon på internettsamfunn (Facebook, Twitter, blogger etc.)

5 Outsourcing av IT-driften

Det er relativt stabile tall fra 2008 og frem til i dag blant de som outsourcer. Det er en svak nedgang blant de som drifter IT som en del av egen virksomhet; fra 47 % i 2008 til 42 % i 2012, og en svak oppgang blant de som setter ut hele IT-driften til andre; fra 15 % i 2008 til 20 % i 2012.

5.1 IT-driftens organisering og bruk av IT

Det er en vesentlig større andel offentlige virksomheter som drifter selv, sammenlignet med private; henholdsvis 57 % mot 34 %. Tilsvarende forskjeller finnes mellom store og små virksomheter; blant store virksomheter har litt under halvparten satt ut hele eller deler av IT-driften, mens for virksomhetene med under 100 ansatte er det 3 av 5 som gjør det samme.

Se tabell 2

5.2 Outsourcing til utlandet

Det er bare 12 % som benytter outsourcingstjenester i utlandet helt eller delvis. Her er det en markant forskjell mellom private og offentlige virksomheter, med henholdsvis 15 % og 2 %. Årsaken er trolig den store mengden personopplysninger, virksomhetskritisk og samfunnskritisk informasjon som finnes i IT-systemene til offentlige virksomheter. Den samme forskjellen ser vi også mellom store og små virksomheter; 22 % av de største virksomhetene benytter outsourcingstjenester i utlandet i større eller mindre grad, mens blant virksomheter med mellom 5 og 19 ansatte er det kun 4 % som gjør det samme.

5.3 Krav til outsourcingspartner

Når en setter ut IT-driften til andre er det viktig at kontrakten inneholder krav til bl.a. tilgangskontroll, taushetsplikt, tekniske sikringstiltak, tilgjengelighet, innsyn i dokumentasjon, økonomisk ansvar ved hendelser og eventuelle sanksjoner dersom krav ikke oppfylles. Det er derfor nedslående å konstatere at det er en stabil nedgang på alle disse områdene fra 2008 og fram til i dag. Her er det ingen forskjell mellom private og offentlige virksomheter. Større virksomheter synes å stille strengere krav til leverandøren. Det er særlig bekymringsfullt at det er nedgang på områdene; krav om rett til innsyn, og krav til tilgangskontroll og tekniske sikringstiltak. Det kan synes som at ledere ikke bare outsourcer oppgaver, men også sikkerhetsansvar. Dette er urovekkende sett i forhold til at 62 % svarer at det er kritisk når IT-systemene er nede inntil 1 dag.

Andelen som har svart «vet ikke» har økt med rundt 10 prosentpoeng siden forrige undersøkelse. Det kan indikere manglende kunnskap på området. Det bekreftes ytterligere ved at kun halvparten av virksomhetene på spørsmålet om ressurser til oppfølging svarer at de har avsatt interne ressurser med innsikt i informasjonssikkerhet for å følge opp kontrakt og leveranse med tjenesteleverandører og underleverandører. Dette underbygger igjen påstanden om at virksomhetene er for dårlige til å følge opp kvaliteten på de tjenestene som kjøpes. Situasjonen er riktignok noe bedre i de største virksomhetene. Blant virksomhetene med over 100 ansatte svarer 3 av 5 bekreftende på dette spørsmålet, mens kun 2 av 5 gjør det samme i virksomheter med mindre enn 100 ansatte. Situasjonen er også noe bedre i offentlig enn i privat sektor med henholdsvis 56 % mot 45 % positive svar. Det er likevel liten tvil om at mange virksomheter har et stort forbedringspotensiale når det gjelder oppfølging av inngåtte kontrakter.

Se tabell 3

5.4 Nettskytjenester

Spørsmålet om nettskytjenester er nytt i årets undersøkelse, og vi ønsker å følge denne utviklingen de neste årene. Nesten halvparten av virksomhetene (46 %) benytter en eller annen form for nettskytjeneste. Av disse er det rundt 1 av 5 som bruker gratistjenester som Gmail, Dropbox etc. Resten benytter en form for betalt tjeneste der de leier infrastruktur (Infrastructure as a Service), plattform (Platform as a Service) og/eller programvare (Software as a Service).

Andelen som benytter en form for nettskytjeneste er noe høyere blant virksomhetene i privat sektor enn i offentlig sektor. Det er eksempelvis 16 % av virksomhetene i offentlig sektor som leier infrastruktur mens tallet for privat sektor er 28 %. Det er ellers liten variasjon i tallene med tanke på geografi, bransje eller virksomhetenes størrelse.

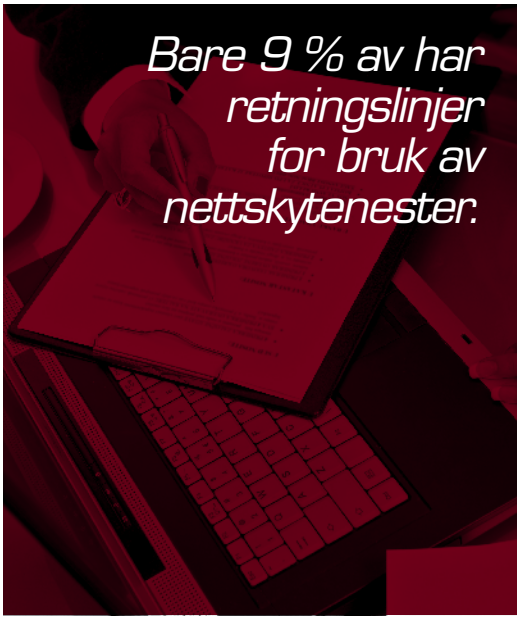
Halvparten av alle virksomhetene sier at de ikke har noen planer om å ta i bruk nettskytjenester de neste 12 månedene. Dette er helt uavhengig av regioner, bransjer, størrelser eller om virksomheten tilhører offentlig eller privat sektor. 1 av 3 svarer at de er

usikre på om de i fremtiden vil ta i bruk nettskytjenester, men av de som per i dag ikke bruker slike tjenester svarer 1 av 4 at de planlegger å ta de i bruk i løpet av det neste året.

Bare 9 % svarer at de har utarbeidet retningslinjer for bruk av nettskytjenester. Se for øvrig punkt 7.3.2 om risikovurderinger.

Anbefalinger

- Bruk veiledningen om outsourcing fra NSR.[5]
- Still klare krav til informasjonssikkerhet i kontrakten med IT-driftspartner.
- Gjennomfør risikovurderinger før nettskytjenester tas i bruk.
- Utarbeid retningslinjer og gjennomfør opplæring som sikrer at virksomhetskritisk informasjon beskyttes.
- Se egen veiledning om bruk av nettskytjenester fra Datatilsynet.[6]



Tabell 2: Hvordan er IT-driften organisert i virksomheten?

	2008	2010	2012
Som del av egen virksomhet	47 %	43 %	42 %
I andres regi (outsourcing)	15 %	18 %	20 %
En kombinasjon	37 %	38 %	35 %
Vet ikke	1 %	2 %	3 %

Tabell 3: Krav til levereandøren ved outscourcing.

	2008	2010	2012	Endring 08 – 12 i prosentpoeng
Krav til tilgangskontroll til informasjon	66 %	57 %	54 %	-12 %
Krav til taushetsplikt	71 %	68 %	67 %	-4 %
Krav til tekniske sikringstiltak	66 %	65 %	57 %	-9 %
Krav til tilgjengelighet / oppetid	67 %	65 %	63 %	-4 %
Rett til innsyn i dokumentasjon	51 %	47 %	38 %	-13 %
Økonomisk ansvar ved hendelser	34 %	31 %	26 %	-8 %
Sanksjoner dersom krav ikke oppfylles	32 %	27 %	24 %	-8 %
Vet ikke	18 %	14 %	25 %	7 %

[5] **NSR** Veiledning for outsourcing av IT" av september 2010.

[6] **Cloud computing** – en veileder I bruk av nettskytjenester: http://www.datatilsynet.no/Global/04_veiledere/Cloud-Computing_veil.pdf

6 Hendelser og mørketall

IKT-kriminalitet er definert av politiet som straffbare handlinger som begås ved utnyttelse av informasjonsteknologi[7]. Mørketallsundersøkelsen™ på sin side omfatter i tillegg data- og informasjonssikkerhetshendelser.

Sammenholdt med tidligere undersøkelser viser tallene en nedgang i alle typer hendelser. Det er en nedgang i antall virksomheter som har vært utsatt for tyveri av IT-utstyr. Andel virksomheter som melder om tyveri av informasjon holder seg stabilt lavt på 1 %, som er markant lavere enn de som melder om tyveri av IT-utstyr.

Se tabell 4

6.1 Estimerte mørketall

Mørketall er differansen mellom anmeldte forhold registrert hos politiet og de hendelser virksomhetene og privatpersoner faktisk blir utsatt for. Mørketallsundersøkelsen™ viser at virksomhetene i tillegg til ofte å mangle kapasitet og evne til å oppdage hendelser ikke anmelder hendelser til politiet når de blir oppdaget. Dette fører til en stor forskjell mellom politiets statistikker og antall faktiske hendelser.

Statistikken hos politiet er basert på anmeldelser registrert i politiets straffesaksregister (STRASAK). Kriminalstatistikken skiller imidlertid ikke mellom privatpersoner eller virksomheter som fornærmet, eller om vinningskriminaliteten er knyttet til IT-utstyr.

Mørketallsundersøkelsen™ tar ikke utgangspunkt i de forskjellige straffebudene. Det er derfor som tidligere gjort et utvalg av forskjellig typer av datakriminalitet.

På bakgrunn av de rapporterte hendelsene har Datakrimutvalget estimert totalt antall hendelser i norske virksomheter til ca. 45.000.

Se tabell 5

Det har blitt rapportert om 270 tilfeller av tyveri av IT-utstyr, en økning fra 137 i 2010. Hendelsene er i hovedsak utført av ukjente gjerningsmann, og de fleste anmeldes til Politiet. Det er rapportert 139 hendelser som omhandler misbruk av IT-ressurser i hovedsak begått av ansatte og innleid personell, uten at dette anmeldes.

I følge Datakrimutvalgets estimater ble norske virksomheter utsatt for 3 200 datainnbrudd. Nedgangen skyldes trolig manglende monitorering og logging, samt hendelsesrapportering til ledelsen. Nedgangen er særlig bekymringsfull med tanke på trusselbildet som forventer en økning av datainnbrudd. Det er også en høyere andel av «vet ikke» gjennom hele undersøkelsen. Dette gjelder både sikkerhetstiltak og kostnader knyttet til sikkerhetshendelser.

Kategorien dataskadeverk og –bedrageri omfatter uautoriserte endringer/sletting av data, målrettede aksjoner for å redusere tilgjengelighet, og bedrageri ved misbruk av kredittkort over Internett. Totalt er det rapportert 299 hendelser i alle tre kategoriene som utgjør et estimat på ca. 33 000. Bare 143 hendelser er anmeldt til politiet.

I spredning av ulovlig/opphavsrettslig beskyttet materiale er det rapportert 252 hendelser, en markant nedgang fra 713 i 2010. Det er knyttet stor usikkerhet til dette tallet, idet flere virksomheter ikke har kunnskap om hva IPR er eller om virksomhetene har IPR. Virksomheter som har IPR er mer utsatt for sikkerhetshendelser enn øvrige virksomheter, se pkt. 6.2. En annen medvirkende faktor kan være nedgang i fildeling grunnet andre alternativer på Internett.

Ser man på tyveri av informasjon er det rapportert 13 hendelser hos de største virksomhetene. Blant små og mellomstore virksomheter er det ikke registrert noen hendelser. Dette er igjen en nedgang fra 23 i 2010, og i sterk kontrast til statistikken over frastjålet ITutstyr der det oppgis 270 hendelser. Dette tyder på at mange ikke helt ser sammenhengen mellom stjålet IT-utstyr og informasjon som lagres på IT-utstyret. Dette bekrefter at virksomhetene ikke har oversikt over verdien av informasjonen de sitter på.

Totalt er det rapportert 745 hendelser i disse fem kategoriene i 2012. Sett i forhold til den registrerte kriminaliteten i politiets registre på 361 anmeldte forhold innenfor de samme kategorier er det her mørketall. Under analysen fremkommer det imidlertid klare indikasjoner på underrapportering blant virksomhetene som svarer på undersøkelsen. Mørketallene forsterkes sett opp mot våre estima-

[7] **Den organiserte kriminaliteten I Norge** – Trender og utfordringer 2011 - 2012 https://www.politi.no/vedlegg/lokale_vedlegg/kripos/Vedlegg_1581.pdf

ter på ca. 45.000 saker i de samme kategoriene.

Mørketallsundersøkelsen™ bekrefter tidligere undersøkelser som viser store mørketall for datakriminalitet. Datakrimutvalget er bekymret over at ikke flere anmelder IT-kriminalitet. Underrapportering fører til et uriktig kriminalitetsbilde. NorSIS har utarbeidet egen veiledning for anmeldelse av IT-kriminalitet [8].

Undersøkelsen gir ingen klar indikasjon på årsaken til forskjellen mellom de sikkerhetshendelser som faktisk skjer og det som blir anmeldt. Den viktigste årsaken oppgis å være at virksomheten ser på hendelsen som ubetydelig. På andre og tredje plass kommer henholdsvis, at de tror det ikke er mulig å finne gjerningsmannen og at angrepet ikke var rettet mot deres virksomhet.

Tabell 4: Prosentandel virksomheter utsatt for hendelser hvor en virksomhet kan ha en eller flere hendelser

Type hendelse:	2008	2010	2012
Datainnbrudd (hacking)	3 %	5 %	3 %
Tyveri av informasjon	2 %	2 %	1 %
Uautorisert endring / sletting av data	4 %	5 %	3 %
Misbruk av IT-ressurser (PC/nett/server)	9 %	11 %	5 %
Spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering)	3 %	5 %	4 %
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)	4 %	4 %	2 %
Trusler om å angripe IT-systemer (utpressing)	0 %	1 %	0 %
Bedrageri ved misbruk av kredittkort over Internett	2 %	2 %	2 %
Tyveri av IT-utstyr (PC, server, mobile lagringsmedier, etc.)	24 %	18 %	13 %
Tap av opplysninger underlagt Personopplysningsloven	-	1 %	1 %

Tabell 5: Rapporterte anmeldelser fra Mørketallsundersøkelsen™ samt estimater ihht. svarene i undersøkelsen rundet av til nærmeste hundre[9]

Type hendelse	Estimat	Anmeldelser
1) Datainnbrudd (hacking)	3 200	144
2) Dataskadeverk og – bedrageri	33 000	
a. Uautorisert endring/sletting av data	2 300	
b. Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten	900	143
c. Bedrageri ved misbruk av kredittkort over internett	29 800	
3) Misbruk av IT-ressurser	2 600	47
4) Spredning av ulovlig/opphavsrettslig beskyttet materiale	5 900	0
5) Tyveri av informasjon	100	27
Totalt	**44 800**	**361**

Estimatene er basert på opplysningene fra årets undersøkelse, samt SSBs statistikk over næringsstrukturen i Norge fordelt på antall ansatte.

[8] https://norsis.no/veiledninger/ledelse/Anmeldelse.html

[9] Det er stor usikkerhet i disse tallene da det er stor underrapportering i undersøkelsen og mange virksomheter mangler rutiner og prosedyrer for å detektere informasjonssikkerhetshendelser.

Anbefalinger

- Etabler gode rutiner for hendelsesrapportering.
- Anmeld straffbare forhold.
- Bevissthet og kompetanse må økes blant ledere.
- Etabler en sikkerhetskultur gjennom kontinuerlig opplæring og holdningsskapende arbeid.

Anbefalinger til myndighetene

- Samarbeidet næringslivet og politi- og sikkerhetsmyndigheter må forsterkes på det operative og forebyggende plan.
- Opprettelse av et nasjonalt register over IKT-sikkerhetshendelser må utredes nærmere.
- Politiets ressurser innen forebyggende datakriminalitet må styrkes.
- Politiets straffesaksregister (STRASAK) må utbedres med kodeverk i tråd med teknologiutviklingen.

6.2 Virksomheter som er mest utsatt

I tråd med trusselbildet og i likhet med tidligere år viser Mørketallsundersøkelsen™ at virksomheter som driver med FoU og IPR er mer utsatt for informasjonssikkerhetshendelser.

For å unngå de store forskjellene mellom store og små virksomheter har vi kun sett på store virksomheter, dvs. de med flere enn 100 ansatte. Dette utgjør 323 virksomheter. Av disse er det 123 som oppgir at de har IPR og 174 som oppgir at de driver med FoU. Det er stor overlapp mellom gruppene da 78 % av de som har IPR også bedriver FoU. Fortsatt er IPR-virksomheter mer utsatt for informasjonssikkerhetshendelser. De samme forskjellene kan vi se i bruk av sikkerhetstiltak; virksomheter som har IPR er litt bedre.

Virksomheter som driver med FoU er mer utsatt enn virksomheter som ikke driver med FoU på tre områder: datainnbrudd (11 %), tap av personopplysninger (4 %) og varsling fra Internet Service Provider (ISP)(11 %). For virksomheter som ikke driver med FoU er tallene henholdsvis 2 %, 0 % og 4 %.

Se tabell 6

Forskjellene er større når man sammenligner de som har IPR opp mot de som ikke har IPR. Noen av de største forskjellene er datainnbrudd (14 % mot 3 %), misbruk av IT-ressurser (19 % mot 8 %) og hendelse som har medført varsling fra ISP (14 % mot 5 %). Hele 42 % av IPR-virksomheter har mistet eller blitt frastjålet datautstyr. Tilsvarende tall for ikke-IPR virksomheter er 18 %.

Se tabell 7

IPR-virksomheter er litt bedre sikret enn virksomheter som ikke har IPR. Det er merkbare forskjeller både på organisatoriske og tekniske tiltak. 70 % av IPR-virksomheter krever at ansatte undertegner retningslinjer for bruk at IT-utstyr, hos virksomheter som ikke har IPR er tallet 48 %. Forskjellen er også stor når det gjelder kryptering av bærbare media; 52 % hos IPR-virksomheter mot 29 % hos virksomheter som ikke har IPR. Tilsvarende gjelder for verdivurdering av informasjon.

Se tabell 8

Datakrimutvalget har to mulige forklaringer på forskjellen i antall hendelser mellom virksomheter med IPR/FoU og andre virksomheter.

IPR- og FoU-virksomheter har mer verdifull informasjon og er dermed mer attraktive mål. Dette underbygges av økt varsling fra ISP både hos IPR-

Tabell 6: Har virksomheten vært utsatt for følgende hendelse?

Hendelse	FOU-virksomheter	Ikke FoU-virksomheter
Datainnbrudd	11 %	2 %
Tap av opplysninger underlagt Personopplysningsloven	4 %	0 %
Hendelse som har medført varsling fra Internet Service Provider	11 %	4 %

Tabell 7: Har virksomheten vært utsatt for følgende hendelse?

Hendelse	IPR-virksomheter	Ikke IPR-virksomheter
Datainnbrudd	14 %	3 %
Tyveri av IT-utstyr	42 %	18 %
DoS-angrep	11 %	1 %
Spredning av ulovlig opphavsrettslig materiale	18 %	5 %
Misbruk av IT-ressurser	19 %	8 %
Tap av opplysninger underlagt Personopplysnings-loven	4 %	0 %
Hendelse som har medført varsling fra Internet Service Provider	14 %	5 %

Tabell 8: Sikkerhetstiltak gjennomført

Sikkerhetstiltak	IPR-virksomheter	Ikke IPR-virksomheter
Risikovurdering av IT-løsninger	81 %	83 %
Må undertegne retningslinjer for bruk av IT-syste-mer	70 %	48 %
Ingen lagring eller behandling på privateid utstyr er tillatt	43 %	45 %
Verdivurdering av informasjon	51 %	21 %
Retningslinjer for behandling av informasjon ifm. FoU prosjekter	35 %	9 %
Oppfølging av retningslinjer - sosial manipulering	7 %	1 %
Sentralisert konfigurasjonsstyring	90 %	88 %
Innbruddsdeteksjonssystem	52 %	31 %
VPN	90 %	70 %
Avlåst datarom	97 %	87 %
Kryptering av bærbare medier	52 %	29 %
Reservestrøm	94 %	82 %
Adm. rettigheter på PC er fjernet	50 %	61 %

virksomheter og de som driver med FoU. Den samme gruppen er over dobbelt så utsatt for tyveri av IT-utstyr.

Virksomheter som driver med FoU eller har IPR er bedre på sikkerhetstiltak og dermed oppdager flere hendelser. Dette underbygges ved at disse virksomhetene har flere sikkerhetstiltak implementert.

Anbefalinger

- Gjennomfør verdivurdering
- Gjennomfør risikovurderinger
- Gjennomfør tiltak for å øke sikkerhetsbevisstheten rundt det økte trusselbildet mot FOU- og IPR-virksomheter

6.3 Informasjon på avveie

Virksomhetene oppgir minnepinner på avveie og eposter sendt til feil adressat som de mest sannsynlige årsaker til at informasjon kan ha kommet på avveie, med henholdsvis 26 % og 32 %. Halvparten av virksomhetene sier de ikke har hatt noen hendelser der informasjon kan ha kommet på avveie.

For alle typer hendelser er det et stort sprik i virkelighetsoppfatning avhengig av hvem som har svart på undersøkelsen. På spørsmålet om informasjon kan ha kommet på avveie som en konsekvens av minnepinner på avveie svarer 13 % av daglige ledere at dette kan ha skjedd, mens blant sikkerhetsansvarlige og IT-ansvarlige er det henholdsvis 44 % og 38 % som svarer det samme. Denne trenden gjelder også de som har svart at de ikke har noen slike hendelser. 68 % av daglige ledere sier at de ikke har hatt noen slike hendelser, mens 35 % av de IT-ansvarlige sier det samme.

Dette kan tyde på at personell med IT/sikkerhetsfaglig funksjon og kompetanse anser risikoen for at informasjon kommer på avveie som langt høyere enn daglig leder og økonomiansvarlig. I 84 % av tilfellene der daglig leder har svart på undersøkelsen representerer de virksomheter under 100 ansatte som ikke nødvendigvis har en stor IT/sikkerhetsorganisasjon med tilhørende kompetanse, og dette kan være årsaken til resultatene. En annen årsak kan være at det i mange tilfeller eksisterer en ulik virkelighetsoppfatning ved at IT-ansvarlige og sikkerhetsansvarlige med sin ekspertise vurderer trusselen markant høyere enn personer i lederstillinger.

Se tabell 9

Privateid utstyr

Bruk av privateid utstyr til virksomhetsinformasjon er økende. Dette medfører en ny risiko for norske virksomheter. Privateid utstyr brukes i mange flere sammenhenger, og er koblet til flere ulike nettverk. Dette gjør det vanskeligere å beskytte mot angrep.

Bruk av privateid utstyr vanskeliggjør også rapportering og kontroll over informasjonen. En ansatt vil kanskje ikke føle seg like forpliktet til å rapportere tap av privat smarttelefon med virksomhetsinformasjon, som hvis smarttelefonen tilhørte virksomheten. Det er bekymringsfullt at 29 % av virksomhetene ikke har noen retningslinjer for bruk av privateid utstyr i jobbsammenheng.

Tabell 9: Kan informasjon ha kommet på avveie grunnet følgende hendelse?

	Totalt	Daglig leder	Økonomi-ansvarlig	Sikkerhets-ansvarlig	IT - ansvarlig
Minnepinner på avveie	26 %	13 %	21 %	44 %	38 %
Smarttelefoner på avveie	12 %	4 %	10 %	21 %	20 %
PC-er på avveie	12 %	7 %	6 %	18 %	20 %
Dokumenter/filer på avveie	16 %	7 %	8 %	34 %	23 %
E-poster sendt til feil adressat	32 %	19 %	28 %	48 %	44 %
Ingen slike hendelser	51 %	68 %	67 %	34 %	35 %

Utfør en verdivurdering, og bruk denne for å bestemme hva som kan lagres på privateid utstyr. Vær bevisst på ny risiko ved bruk av privateid utstyr, og ta hensyn til dette i risikovurderingen.

Anbefalinger

- Utarbeid retningslinjer for bruk av privateid utstyr og rapportering av hendelser

6.4 Hindre tilsvarende informasjonssikkerhetshendelser

185 virksomheter har rapportert en form for informasjonssikkerhetshendelse. For å hindre tilsvarende hendelser har 41 % av virksomhetene investert i opplæringstiltak og/eller forbedring av sikringsrutiner

Det er forskjeller mellom hvordan privat og offentlig sektor velger å forbedre sikkerheten. Privat sektor velger i høyere grad opplæringstiltak; 46 % mot 33 % i offentlig sektor. Det samme gjelder forbedring av sikringsrutiner, hvor 45 % i privat sektor har gjort det mot 36 % i offentlig sektor.

Hele 12 % av virksomhetene valgte å ikke gjøre noe for å forbedre sikkerheten, og bare 10 % valgte å avsette flere personer/mer tid til sikkerhetsarbeid.

Anbefalinger

- Evaluere hendelsen
- Revidere planverk og iverksett nødvendige tiltak

6.5 Kostnader knyttet til informasjonssikkerhetshendelser

Datakriminalitet har vidtrekkende konsekvenser for næringslivet. Det er mørketall også på kostnadssiden. The UK Cabinet Office har i undersøkelsen, "The Cost of Cybercrime", estimert at datakriminalitet koster UK[10] 27 mrd pund. NorCERT har regnet om dette til norske forhold som tilsier at datakriminalitet koster Norge 20 mrd NOK i året[11]. Det er stor usikkerhet knyttet til dette tallet da det kun er nedskalert basert på innbyggertall. Tallet kan likevel underbygges av hendelser rapportert til NorCERT; en virksomhet alene ble utsatt for et målrettet angrep og tapte posisjon i kontraktsforhandlinger verdt flere hundre millioner kroner. En annen virksomhet blir stadig utsatt for angrep via e-post, og har regnet ut at et vellykket angrep kan koste flere titalls millioner i direkte tap.

Det største tapet er tyveri av immaterielle eiendeler. Dette bekreftes i Mørketallsundersøkelsen™ hvor virksomheter som har immaterielle rettigheter rapporterer flere hendelser og høyere kostnader knyttet til sikkerhetshendelser.

I Mørketallsundersøkelsen™ har norske virksomheter oppgitt kostnadene for datakriminalitet. Funn viser at en av tre ikke vet omfanget av verken direkte eller indirekte kostnader. En tredjedel oppgir ikke å ha indirekte kostnader i det hele tatt, og 14 % har ingen direkte kostnader. De aller fleste som har oppgitt kostnader har også kostnader mindre enn 50 000 NOK.

Undersøkelsen viser at det er store mørketall på kostnadssiden relatert til sikkerhetshendelser. Manglende verdivurdering og hendelsesrapportering er årsaken til mørketallene på dette området.

Anbefalinger

- Virksomheter bør kvantifisere og evaluere tap som følge av informasjonssikkerhetshendelser
- Det bør etablere rutiner for å kunne fastsette direkte og indirekte kostnader knyttet til sikkerhetshendelser
- FØR hendelser inntreffer gjennomføre risikovurdering på alle sine viktigste informasjonsverdier i henhold til fastlagte kriterier, inkludert akseptabelt økonomisk tap
- Ledelsen bør årlig be om oversikt over alle inntrufne hendelser, inkludert estimert økonomisk tap som følge av hendelsene

[10] **The cost of cybercrime.** A Detica report in partnership with the Office of Cyber Security and Assurance in the Cabinet Office. http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf nedlastet 26. juni 2012.

[11] **NorCERT kvartalsrapport for 1. Kvartal 2012** https://www.nsm.stat.no/Documents/NorCERT/2012/Q1_2012_WEB.pdf

7 Sikkerhetstiltak

Det er en klar sammenheng mellom virksomhetens størrelse og bruk av sikkerhetstiltak. Store virksomheter tar i bruk en rekke flere sikkerhetstiltak sammenlignet med små virksomheter.

7.1 Organisatoriske tiltak

Kun 4 av 10 virksomheter gir opplæring i sikker bruk av IT ved nyansettelser. Av disse igjen er det kun 4 av 10 som fortsetter med kontinuerlig opplæring for alle ansatte. Dette er en nedgang fra 2010.

Trusselbildet forandrer seg raskt. Angrepene rettes i større grad mot mennesker og ikke teknologi. Kunnskapen til ansatte må oppdateres innenfor informasjonssikkerhet. Det er viktig å etablere en god sikkerhetskultur i virksomheten.

Undersøkelsen viser at halvparten av de rapporterte sikkerhetshendelsene kan spores tilbake til egne ansatte/innleid personell. Dette kan skyldes både tilfeldige feil grunnet manglende opplæring og mer målrettede handlinger.

Det er stor forskjell på hvordan virksomheter velger å skaffe seg kompetanse. Større virksomheter er mye mer aktive i å skaffe seg kompetanse internt i bedriften. De mindre virksomhetene skaffer hoveddelen av kompetanse fra eksterne tjenester. Det er en klar sammenheng mellom anskaffelse av kompetanse og oppdagelse av hendelser. Virksomhetene som er mer aktive på å skaffe seg kompetanse oppdager flere hendelser. De innfører også flere organisatoriske tiltak. Det er vår oppfatning at de andre virksomhetene også har hendelser, men at de ikke oppdager disse.

Sikkerhetsansvarlig er høyt representert når det gjelder å skaffe seg kompetanse. Daglig leder er derimot veldig lavt representert. Som øverste ansvarlig for sikkerheten må daglig leder inneha nok kunnskap om sikkerhet til å være ansvarlig. En leder kan delegere oppgaver innen sikkerhet, men ikke ansvaret.

Beredskap

Ca. en tredjedel av virksomhetene har utarbeidet planer for håndtering av de viktigste informasjonssikkerhetshendelsene. Bare en tredjedel av disse har imidlertid krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap. Det betyr at kun 1 av 9 har tilfredsstillende krav til beredskap.

Se figur 1

Det er klare forskjeller mellom små og store virksomheter. Kun 1 av 5 virksomheter med 5-19 ansatte har planer for håndtering av de viktigste informasjonssikkerhetshendelser. For virksomheter med over 100 ansatte er tallene bedre. Her har halvparten planer for håndtering av de viktigste informasjonssikkerhetshendelser.

Av de som oppgir å få problemer innen én time om IT-systemet var nede, er det svært bekymringsfullt at bare 43 % har etablert beredskapsplaner for håndtering av de viktigste informasjonssikkerhetshendelsene. Den samme gruppen er enda svakere på systematiske øvelser knyttet til IT-beredskap. Bare 15 % har krav om øvelser.

De som foretar risikovurderinger av viktige IT-systemer er mer forberedt og sterkere på beredskap. Av de som har foretatt en risikovurdering har 44 % laget planer for håndtering av de viktigste informasjonssikkerhetshendelsene, i motsetning til 15 % hos de som ikke har foretatt en risikovurdering.

Mørketallsundersøkelsen™ gir således en klar indikasjon på manglende beredskap hva gjelder informasjonssikkerhetshendelser.

Figur 1: Beredskap og øvelser

Verdivurdering er et verktøy for virksomheten til å avdekke hva som er virksomhetssensitive opplysninger, kritiske objekter med videre, og som av denne grunn må beskyttes. Viktige spørsmål som bør stilles er:

- Hva er konsekvensen dersom denne informasjonen blir offentlig tilgjengelig?
- I hvilket tidsrom har informasjonen verdi?
- Hvem kan misbruke informasjonen?
- Hvordan kan informasjonen misbrukes?
- Hva med beskyttelse for kilden?

Retningslinjer

Over halvparten av de som bruker sosiale medier for intern kommunikasjon og 64 % av de som bruker sosiale medier for ekstern kommunikasjon, har ikke retningslinjer for sikker bruk. Totalt har bruken av sosiale medier gått kraftig opp, mens retningslinjer for bruk har gått ned fra 30 % i 2010 til 24 % i år[12].

Informasjonssikkerhetsarbeidet henger ofte litt etter teknologien. 55 % har retningslinjer for sikker bruk av PC, mens kun 29 % har retningslinjer for sikker bruk av smarttelefoner. 24 % har retningslinjer for sikker bruk av sosiale medier. Kun 9 % har retningslinjer for ansattes bruk av nettskytjenester (G-mail o.l.). Noe av grunnen til denne forskjellen er andelen som bruker de ulike teknologiene, men dette forklarer ikke hele forskjellen. Det kan se ut som virksomheter venter med å ta i bruk nye sikkerhetstiltak til det skjer en hendelse.

Kun 1 av 6 har retningslinjer for identifisering og klassifisering av virksomhetsinformasjon (verdivurdering). Det antas at de resterende enten ikke utfører verdivurderinger eller mangler faste prosedyrer slik at gjennomføringen blir unøyaktig. En verdivurdering av virksomhetsinformasjon er en stor del av informasjonssikkerhetsarbeidet. Ledere må være bevisst hvilken informasjon i virksomheten som er viktig for inntjening og fremtiden, og hvordan den skal beskyttes. Det er vanskelig å utarbeide sikringstiltak før en vet hva som er viktig informasjon for virksomheten.

Oppfølging av retningslinjer

Oppfølging av retningslinjer er den eneste måten å sjekke om retningslinjene blir fulgt. Hver tredje virksomhet har liten eller ingen oppfølging av retningslinjer. Av de som har oppfølging av retningslinjer oppgir de fleste å foreta intern revisjon (37 %), sikkerhetsgjennomganger (25 %), samt rapportering av avvik til ledelse (22 %).

Se tabell 10

Tabell 10: Oversikt over organisatoriske tiltak

	2008	2010	2012
Retningslinjer for ansattes bruk av informasjonssystemer	67 %	71 %	71 %
Retningslinjer for sikker drift av IT-infrastruktur[14]	82 %	77 %	65 %
Planer for håndtering av de viktigste informasjonssikkerhetshendelser	40 %	40 %	36 %
Krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap[15]	12 %	11 %	15 %
Retningslinjer for håndtering av informasjonssikkerhetshendelser utenfor arbeidstid[16]	48 %	47 %	27 %
Krav om at det skal utpekes en informasjonssikkerhetsansvarlig[17]	-	57 %	26 %
Må undertegne taushetserklæring	59 %	66 %	67 %
Skal gis opplæring i sikker bruk av IT ved ansettelse	-	42 %	42 %
Skal gis opplæring i sikker bruk av IT regelmessig	-	31 %	24 %
Må undertegne retningslinjer for bruk av IT-systemer	-	34 %	35 %

[12] Spørsmålet er stilt litt annerledes og tallene er ikke helt sammenlignbare.

[13] **Veiledning i bakgrunnssjekk:** http://www.nsr-org.no/publikasjoner/veiledning-i-bakgrunnssjekk-article148-143.html

[14] **2008:** Virksomheten har etablert retningslinjer for sikker drift og IT-infrastruktur

[15] **2010:** gjennomfører systematiske øvelser knyttet til IT-beredskap

[16] **2010:** er i stand til å håndtere IT-sikringsbrudd utenfor arbeidstiden

[17] **2010:** har utpekt en IT-sikkerhetsansvarlig

Tabell 11: Brukes følgende sikringstiltak?

	2010	2012	Endring i prosentpoeng:
Personlig brannmur på mobile PC-er[18]	64 %	56 %	-8 %
Inbruddsdetekteringssystem	30 %	26 %	-4 %
Virtuelt privat nettverk	61 %	56 %	-5 %
Ulike sikkerhetssoner i nettet	63 %	61 %	-2 %
Avlåst datarom	72 %	70 %	-2 %
Kryptering av bærbare media	23 %	24 %	1 %
Duplisering av kritiske komponenter	53 %	49 %	-4 %
Reservestrøm UPS	71 %	66 %	-5 %
Filter mot uønsket web-trafikk	70 %	69 %	-1 %
Administrasjonsrettigheter på PC fjernet	41 %	45 %	4 %
IT-systemene herdes	54 %	56 %	2 %

Anbefalinger

- Etabler en sikkerhetskultur gjennom kontinuerlig opplæring og holdningsskapende arbeid blant alle ansatte.
- Gjennomfør verdivurdering og risikovurdering for å avdekke behovet for tiltak.
- Utarbeid retningslinjer og følg de opp.
- Utarbeid beredskapsplaner for informasjonssikkerhetshendelser og øv regelmessig.
- Gjennomfør bakgrunnssjekk av medarbeidere i henhold til virksomhetens verdivurdering. Se veiledning fra NSR[13] .

Anbefalinger til myndighetene

- Informasjonssikkerhet må inn som obligatorisk fag i utdanningsinstitusjoner på alle nivåer, med særlig vekt på lederutdanninger.

7.2 Teknologi

Sikringstiltak

Det er en svak nedgang i tekniske sikringstiltak på de fleste områder. Årsaken kan ligge i at en mindre andel av store virksomheter har svart på årets undersøkelse.

Kryptering av bærbare media fortsetter å øke fra 19 % i 2008 til 23 % i 2010 og 24 % 2012. Dette er et svært viktig tiltak i lys av at flere bruker mobiltelefoner til e-post og 13 % oppgir å ha blitt frastjålet IT-utstyr. Det er likevel bekymringsfullt at kun 1 av 4 krypterer bærbare media.

Bruk av reservestrøm/UPS gikk tilbake i år også; fra 76 % i 2008 til 71 % i 2010 og videre ned til 66 % i år. Det er bekymringsfullt at bruk av innbruddsdetekteringssystem minker med 4 prosentpoeng sett i lys av den økte trusselen for datainnbrudd.

Se tabell 11

Oppdatering av programvare

Det er liten forskjell fra 2010 til 2012 når det gjelder oppdatering av programvare. Automatisk oppdatering av operativsystem (OS) har stagnert på 42 % i år, etter sterk økning fra 33 % i 2008 til 42 % i 2010. Dette er et viktig tiltak for å beskytte datamaskinen, og det er bekymringsfullt at denne gode trenden ser ut til å ha stoppet opp.

Automatisk oppdatering av programvare for å beskytte mot virus har gått litt ned fra 77 % i 2010 til 74 % i år.

Andelen som svarer vet ikke har økt siden 2010. 18 % av de som har svart sier de ikke vet hvordan oppdateringsrutinene er for operativsystemet deres, mot 15 % i 2010. Andelen er høyest hos daglig leder og avdelingsleder der henholdsvis 1 av

3 og 4 av 10 svarer at de ikke vet hvordan rutinene er for oppdatering av operativsystemet.

Anbefalinger

- Bruk automatisk oppdatering hvis tilgjengelig. Oppdater jevnlig de programmer som ikke oppdateres automatisk.
- Avinstaller alle programmer du ikke bruker.
- Beskytt sensitiv informasjon som oppbevares på mobile enheter (for eksempel smarttelefoner og nettbrett).

7.3 Prosesser og rutiner

7.3.1 Gjennomgang av logger

System- og aktivitetslogger er viktige for å forstå, avdekke og undersøke hendelser, samt for å forebygge og begrense faren for fremtidige skader eller sikkerhetsbrudd. Loggene må gjennomgås ved jevne mellomrom. Mye verdifull informasjon ligger i loggene, men om de ikke gjennomgås og kun lagres mister man det «forebyggende aspektet». Gjennomgang av logger er en viktig aktivitet for å oppdage og hindre hendelser som er i ferd med å skje. Konsolidering av logger fra ulike systemer kan avdekke hendelser fra et system som gir negative utslag i et annet system, og gir god oversikt over sammenhenger i hendelser og risikosituasjoner.

System- og brannmurlogger skal gi objektiv informasjon, og bør behandles med samme sensitivitet som man gjør med personopplysninger. Tilgangen til logger bør derfor begrenses til autorisert personell. Logger må omfattes av normale backup-rutiner.

Se figur 2

Hvorfor er logging nyttig?

Logging og gjennomgang av logger gir:

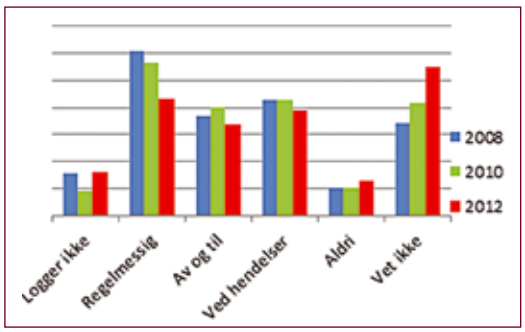
- Læring
- Kunnskap om uventet trafikk og innbrudd
- Praktisk verktøy for etterlevelse av regler (compliance)
- Synliggjøring av kvalitetsproblemer
- Avdekker feilaktige eller bevisste konfigurasjonsendringer og kan hindre uheldige utslag av disse
- Kan avdekke avvik i produksjons- og informasjonssystemer
- Gir virksomheten kunnskap til å restituere seg etter et angrep, og muliggjør riktigere valg av tiltak for å forebygge tilsvarende hendelser i fremtiden
- Sikrer spor som kan være avgjørende ved anmeldelser og etterforskning

Logging bør minimum være IP-informasjon, protokoll- og portinformasjon, alle endringer i operativsystemer, konfigurasjoner samt logger fra applikasjonsserverene. Ofte vil det være nødvendig å sette av litt arbeidstid til både analyse og for å avdekke årsak til avvik.

Mørketallsundersøkelsen™ gir et bilde av hvor liten oppmerksomhet selskapene vier sine loggdata. Trenden viser at «vet ikke» kategorien er blitt betydelig høyere fra år til år. Fra 17 % i 2008 til 28 % i år.

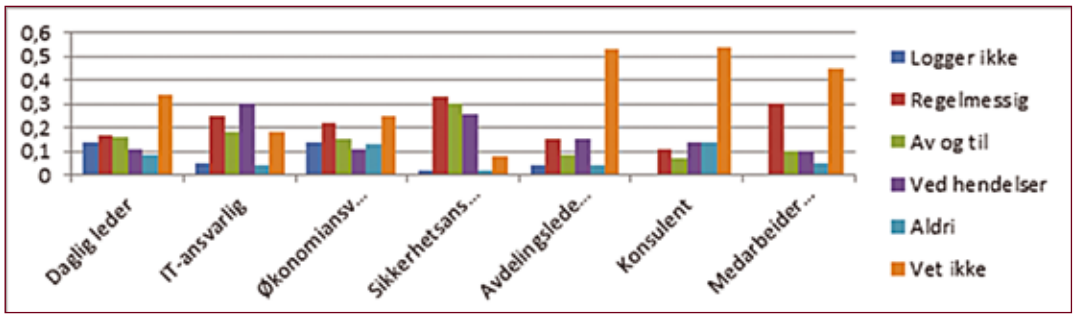
Offentlige virksomheter har fått gradvis dramatisk mindre fokus på logging over de siste tre undersøkelsene. Antallet «vet ikke» i offentlige virksomheter har økt dramatisk de siste årene, og det er bekymringsverdig i en tid da teletjenester og IT blir mer og mer kritisk. Vi er også urolige for utviklingen med mangel på retningslinjer i offentlig sektor. Dette kan medføre en dårligere evne til å detektere og spore sikkerhets-

Figur 2: Gjennomgang av logger

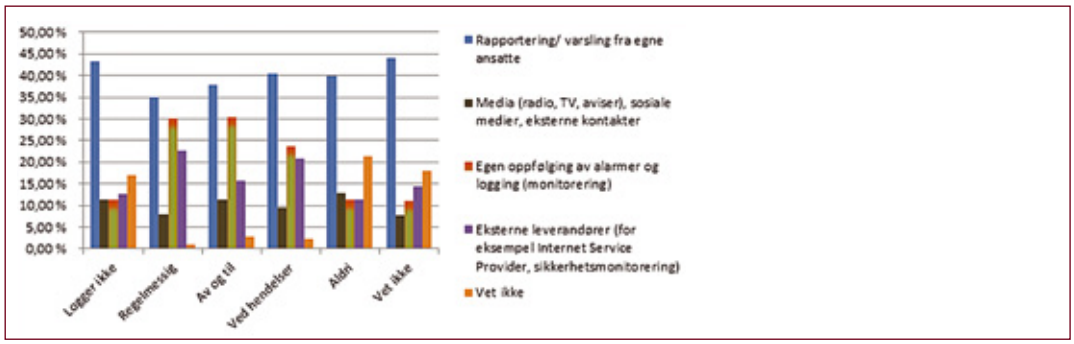


[18]2010: Personlig brannmur

Figur 3: Kunnskap om logging



Figur 4: Hvordan oppdages hendelsene?



brudd, og derved større sårbarhet for hendelser.

Det er ikke overraskende at sikkerhetsansvarlige har langt bedre oversikt over nettet enn daglig leder, IT-ansvarlige og annet personell. Dette understreker behovet for å øke sikkerhetsbevisstheten i virksomhetene. Det kan faktisk lønne seg å ha en sikkerhetsansvarlig med ansvar for å ivareta virksomhetens informasjonssikkerhet.

Se figur 3

Undersøkelsen spurte virksomhetene om hvordan hendelser ble oppdaget. Her er det egentlig bare tre kategorier som stikker seg frem: Media, egen oppfølging og eksterne leverandører, med henholdsvis 16 %, 38 % og 30 %.

Logging er ganske komplekst og krever at man kontinuerlig har fokus på problematikken. Kompleksitet krever at man bruker ressurser (og penger) på saken, og det er tydelig en nedgående trend i villighet til dette. Figuren under viser at alle virksomheter i omtrent like stor grad oppdager hendelser etter observasjoner fra egne ansatte. Virksomheter som har oppmerksomhet på egne logger svarer i mye lavere grad «vet ikke». Det er absolutt å anbefale at man tar denne viktige informasjonskilden alvorlig.

Se figur 4

Det er grunn til å merke seg at de som ikke vier sine egne logger oppmerksomhet i stor grad heller ikke oppdager hendelser på andre måter.

Anbefalinger

- Systematisere og aktivt monitorere logger fra brannmurer, nettverksenheter og av forretningskritiske IT-systemer.
- Loggene bør jevnlig analyseres og avvik rapporteres til ledelsen.
- Større virksomheter bør la sitt eget sikkerhetspersonell monitorere sine logger. Virksomheter som setter ut sin IT- og nettverksdrift til tredjepart bør forsikre seg om at logger blir gjennomgått av leverandørens sikkerhetspersonale for å avdekke avvik fra normal drift.
- Logging bør minimum være IP-informasjon, proto-

koll- og port-informasjon, kritiske endringer på operativsystemer og konfigurasjoner samt logger fra applikasjonsserverne. For at logger enkelt skal kunne konsolideres på tvers av ulike systemer er det viktig at klokkene på disse systemene går riktig og er synkronisert.

7.3.2 Risikovurderinger

72 % av virksomhetene gjennomfører risikovurderinger av viktige IT-systemer ved anskaffelse eller betydelige endringer. Det er kun 38 % av disse som gjennomfører risikoanalyser hver gang det innføres nye løsninger.

Det er bra at 72 % sier at de gjennomfører risikoanalyser av viktige IT-systemer, men på oppfølgingsspørsmålet kommer det fram at 43 % gjør det kun av og til avhengig av hvilken løsning det er snakk om, 31 % gjør risikoanalyser i henhold til rutiner og 38 % gjør det hver gang.

Av IT-ansvarlige og sikkerhetsansvarlige svarer 80 % at det gjennomføres analyser ved endringer i viktige IT-systemer. Blant daglige ledere og økonomiansvarlige er det henholdsvis 66 % og 72 % som bekrefter at de gjennomfører risikoanalyser. Blant daglige ledere er det hele 20 % som ikke vet om det gjennomføres risikoanalyser. Dette er svært bekymringsfullt med tanke på at daglig leder har overordnet ansvar for sikkerheten i virksomheten.

Anbefalinger

- Gjennomfør risikovurdering for å avdekke behovet for tiltak.
- Utarbeid retningslinjer og rutiner for risikovurderinger. Når risikovurderinger eller analyser gjennomføres må faste rutiner for metodikken følges for å muliggjøre sammenligning av analysene/systemene/avdelingene seg imellom.

7.4 Personopplysningsloven

Litt over halvparten av de som har svart på undersøkelsen har utarbeidet en oversikt over personopplysninger som finnes i virksomheten. Dersom man ikke har en oversikt, kan en ikke vite hvilke tiltak som må implementeres. Da er det vanskelig å finne ut om tiltakene blir fulgt, og om personopplysninger kommer på avveie. 65 % har etablert rutiner for håndtering av personopplysninger. Kun 44 % har etablert intern kontroll som omhandler personopplysninger. 73 % av de som har utarbeidet formelle rutiner for personopplysninger, har utarbeidet en oversikt over personopplysninger. 82 % av de som har etablert intern kontroll for personopplysninger har utarbeidet en oversikt. Det er bekymringsfullt at flere virksomheter utarbeider rutiner og kontroll uten å ha laget en oversikt.

Det er manglende kompetanse hos virksomhetene, spesielt hos daglig leder som er ansvarlig ifølge personopplysningsloven. 1 av 6 daglig ledere vet ikke om det er utarbeidet en oversikt over personopplysninger i deres virksomhet. 13 % av daglig ledere vet ikke om det er utarbeidet intern kontroll for personopplysninger. Leder er ansvarlig for sikkerheten og må ha oversikt over hvordan sikkerheten er implementert.

Tallene henger godt sammen med Datatilsynets undersøkelse av kommuner[19]. Denne viste at litt over halvparten mente de hadde etablert intern kontroll for håndtering av personopplysninger, men det var kun 7 % som hadde tilfredsstillende intern kontroll ifølge Datatilsynet sine krav. I Mørketallsundersøkelsen™ svarer 58 % av offentlig sektor[20] at de har etablert intern kontroll for personopplysninger.

Flere og flere samler inn personopplysninger til diverse formål, og flere av disse er små organisasjoner, idrettslag o.l. Når små virksomheter i denne undersøkelsen (5-19 ansatte) er så mye svakere enn de største virksomhetene, så stilles det spørsmål ved hvordan sikkerheten er i de minste organisasjonene.

Anbefalinger

- Utarbeid oversikt over alle personopplysninger før du utarbeider tiltak.
- Etabler formelle rutiner og intern kontroll for behandling av personopplysninger.

[19] **Kommuneundersøkelsen 2010-2011** http://www.datatilsynet.no/Global/04_analyser_utredninger/Kommuneunders_2010_2011_internkontroll_informasjonssikkerhet.pdf

[20] **Tallene er ikke direkte sammenlignbare** siden tallet fra Mørketallundersøkelsen™ dekker offentlig sektor, men Datatilsynets undersøkelse dekker kommuner.

Datakrimutvalget 2012

Arne Johan Helle

Leder av datakrimutvalget. Han er Certified Information Security Manager (CISM), og Certified in the Governance of Enterprise IT (CGEIT). Arne Johan er i dag IT Compliance ansvarlig i Telenor Norge. Tidligere partner og fagansvarlig for IT-revisjons og IT-sikkerhetsoppdragene i PWC. Han har mer enn 25 års erfaring fra IT-sikkerhetsarbeid i ulike bransjer innenfor offentlig og private virksomheter.

Vidar Østmo

Chief Information Security Officer Vidar Østmo har mange års erfaring innen informasjonssikkerhet. Han innehar CISSP og GCIH sertifiseringer og er til daglig Chief Information Security Officer hos Broadnet AS. Han er også styreleder i Internett og Telebransjens Anti-Kriminalitets Tiltak (ITAKT). ITAKT har som formål å bekjempe svindel og misbruk av tjenester og infrastruktur i forbindelse med virksomheten til norske internett- og teleoperatører.

Kristine Beitland

Direktør for Næringslivets sikkerhetsråd.Utdannet jurist. 16 år i politiet som leder og påtalejurist. Tidligere stilling som avdelingsdirektør i Politiets utlendingsenhet. Ledet seksjonen for Organisert kriminalitet i Politidirektoratet, og Oslo politidistrikts største påtalegruppe, Grønland politistasjon.

Tore Larsen Orderløkken

Direktør for Norsk senter for informasjonssikring (NorSIS) siden 2006. Utdannet Master i informasjonssikkerhet. Tidligere leder av Center of Excellence information security i Telenor Konsern, informasjonssikkerhetsrådgiver Telenor Konsernstab Sikkerhet, 15 år i forsvaret med ulike sambands, kommunikasjons og sikkerhets oppgaver.

Johnny Mathisen

Utdannet sivilingeniør i telematikk og har også en mastergrad i informasjonssikkerhet. Han har jobbet i Telenor siden midten av 80-tallet, hvorav de siste 20 årene med informasjonssikkerhet. Han har erfaring fra både teknisk og ikke-teknisk side og jobber i dag som seniorrådgiver i Telenor Group med bl.a. policyer, retningslinjer og holdningsskapende arbeid for hele Telenorkonsernet

Eiliv Ofigsbø

Avdelingsdirektør og leder for NorCERT i Nasjonal sikkerhetsmyndighet. Utdannet Cand Scient i Informatikk samt militær utdannelse. Tidligere stilling som Bransjesjef for informasjonsikkerhet i NATOs hovedkvarter. Har hatt ulike lederstiillinger i NSM og Forsvaret før dette.

Tone Thingbø

Senior Manager i Ernst & Youngs rådgivingsenhet for informasjonssikkerhet. Utdannet samfunnsviter med påbygging innen IT-ledelse. Gjennomført Forsvarets Høgskole. Tidligere arbeidet i Etterretningstjenesten, Nasjonal Sikkerhetsmyndighet og OSSE. Var i fire år Informasjonssikkerhetssjef i Norges Bank

Christophe Birkeland

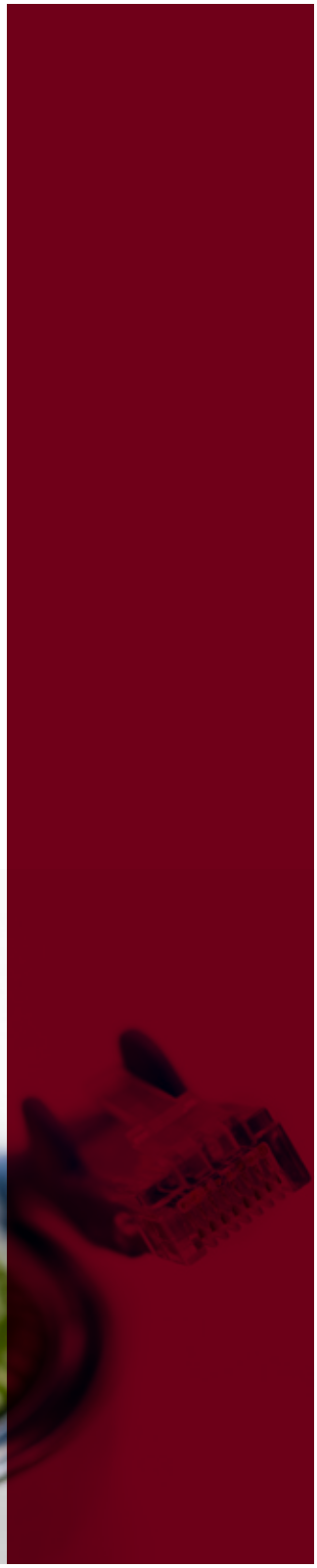
Teknologidirektør i Norman. Doktoringeniør fra NTNU 1997, sivilingeniør fra NTH 1993. Tidligere utviklingsdirektør i Norman, og avdelingsdirektør i Nasjonal sikkerhetsmyndighet (NSM) der han bygget opp den nasjonale CERT funksjonen NorCERT. Har i mange år analysert og formidlet IKT-trusselbildet for enkeltpersoner, virksomheter og Norge som nasjon.

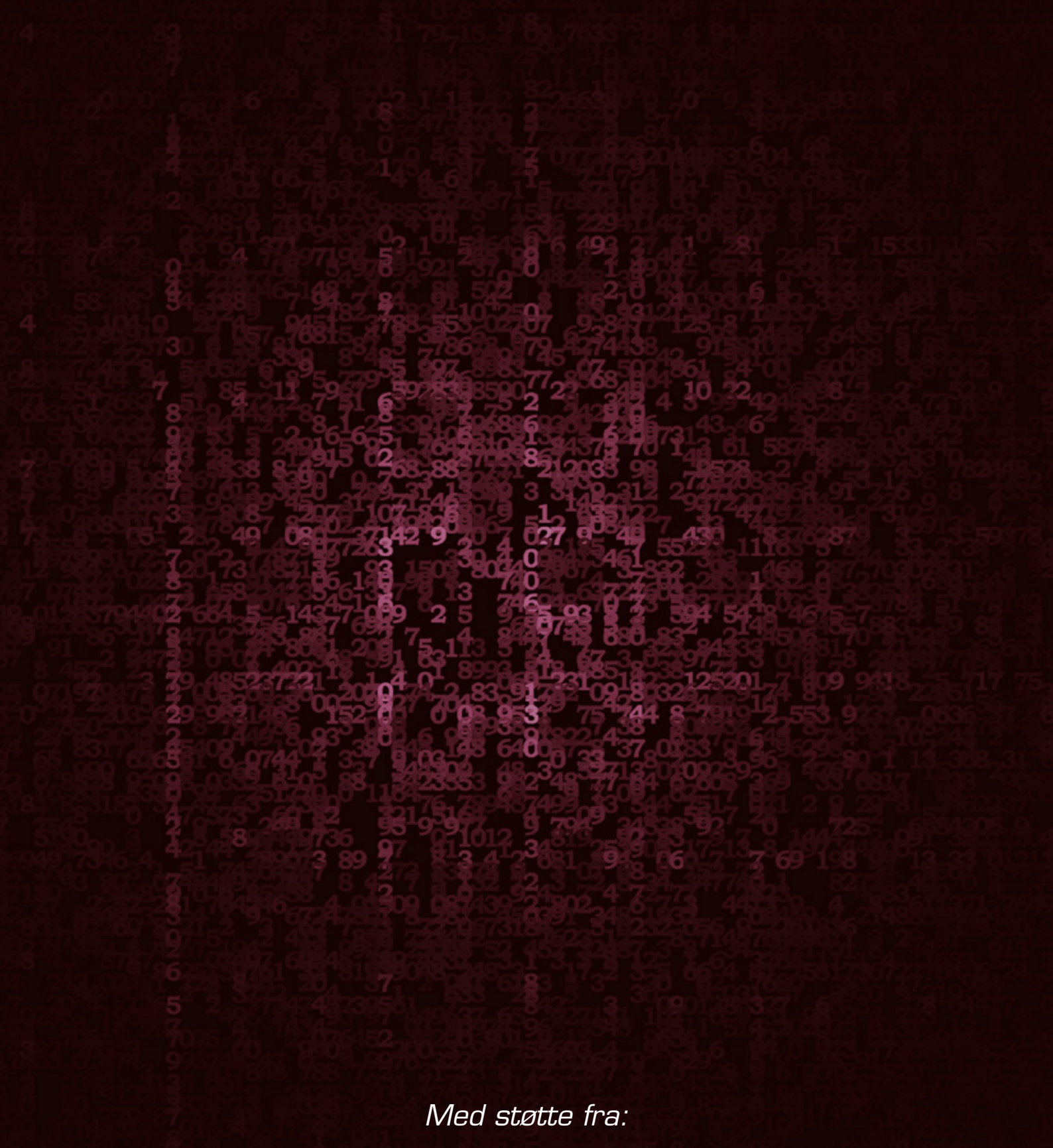
Janne Hagen

Konsulent hos Proactima AS, arbeidsområde risikostyring og beredskap. PhD i informasjonssikkerhet. 14 år hos Forsvarets forskningsinstitutt som forsker innen samfunnssikkerhet og beredskap. Tidligere forsker ved Transportøkonomisk institutt og gjesteforsker hos Naval Postgraduate School, California.

Håvard Folkedal

Bred erfaring fra politi- og lensmannsetaten siden 1995. Arbeidet de siste 2 årene som politioverbetjent/etterforskningsleder ved seksjon for datakrimetterforskning på Kripos.





Med støtte fra:

FORNYINGS-, ADMINISTRASJONS- OG KIRKEDEPARTEMENTET

ITAKT
Internet og Telekombransjens Anti - Kriminalitets tiltak

NORMAN

Oberthur Technologies

WATCHCOM Security Group

Microsoft

telenor