Nasjonal sikkerhetsmyndighet

Rapport om sikkerhetstilstanden 2010

Sammendrag

Trusselen mot skjermingsverdig informasjon og kritisk infrastruktur er under kontinuerlig utvikling. Gapet mellom de kapasitetene som trusselaktørene innehar, og mottiltakene virksomhetene iverksetter økte i 2010. Dette betyr at sikkerhetstilstanden forverres.

Mange virksomheter – offentlige så vel som privat, underlagt sikkerhetsloven eller ikke – har ikke nødvendige forebyggende sikkerhetstiltak og systemer for å vedlikeholde disse. Dette gjelder både i forhold til å beskytte informasjon som har sensitivt innhold – som sikkerhetsgradert dokumenter – og informasjon som er viktig for å styre kritiske objekter, funksjoner og prosesser i samfunnet – som kraftforsyning, olje- og gassanlegg, bank- og finanstjenester, militære installasjoner, med mer.

Nasjonal sikkerhetsmyndighet (NSM) ser mer eller mindre store mangler innen følgende områder som påvirker sikkerhetstilstanden i virksomhetene spesielt, og dermed samfunnet generelt:

- Verdiforståelse og bevissthet rundt hva som er skjermingsverdig
- Oversikt over egen sikkerhetstilstand
- Ledelsesengasjement
- Styringssystem for sikkerhet
- Kompetanse
- Sikkerhetskultur
- Rutiner ved sikkerhetsklarering
- Autorisasjon av personell
- Plan ved og beskyttelse mot sikkerhetstruende hendelser
- Dokumentsikkerhet
- Fasiliteter for sikkerhetsgraderte samtaler
- IKT-sikkerhet
- Leverandørkjeden (for IKT-komponenter)

NSM observerer en situasjon med økende sikkerhetsmessig *risiko*. Det er til dels vesentlige mangler i det forebyggende sikkerhetsarbeidet med konsekvenser for den nasjonale sikkerhetstilstanden. Dette representerer en sårbarhetsutfordring, da manglene kan utnyttes av trusselaktører med stadig økende ondsinnede kapabiliteter og kapasiteter. Det kan observeres at:

- det generelt er slik at de *verdier* vi ønsker å beskytte øker i volum og betydning i takt med samfunnsutviklingen og den økende produksjonen av informasjon, blant annet sikkerhetsgradert informasjon.
- *truslene* mot sikkerhetsgradert og annen skjermingsverdig informasjon er i sterk økning; særlig den teknologiske oppfinnsomheten med hensyn til at utvikling av skadevare på IKT-systemer akselererer.
- *sårbarheter* knyttet til IKT-systemer og -prosesser øker, noe som igjen 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.

Sikkerhetsarbeidet for å beskytte den økende mengden viktig informasjon, og kritiske samfunnsinfrastrukturer og -objekter har stagnert. Dette tilsier at sikkerhetstilstanden forverres. NSM har tidligere rapportert om et økende gap mellom trusselaktørers kapasiteter og eksisterende sikkerhetstiltak. Trenden er at dette gapet fortsetter å øke.

1 Innledning

NSM avgir årlig en gradert rapport om sikkerhetstilstanden til Forsvarsdepartementet og Justisdepartementet. Dette er en ugradert versjon av rapporten for 2010, som redegjør for etterlevelsen av sikkerhetsloven med forskrifter, og gir en vurdering av kvaliteten på det forebyggende sikkerhetsarbeidet.

Forebyggende sikkerhetsarbeid innebærer å legge forholdene til rette for god sikring av informasjon og objekter som kan være mål for spionasje-, sabotasje-, og terroraktivitet. Dette betyr blant annet å kontrollere og vurdere etterlevelsen av kravene i sikkerhetsloven, så vel som andre sikkerhetsrelevante forhold utenfor sikkerhetsloven, særlig innenfor NorCERTs arbeidsområde.[1]

Det observeres mange mangler og utfordringer rundt sikkerheten ved samfunnskritiske virksomheter hvert år, noe som representerer en stadig økende sårbarhetsutfordring for landet vårt. I dag viser analyser at de mest avanserte ondsinnede metodene tilsynelatende ikke nyttes til ytterste negative konsekvens – selv ikke av sabotører eller terrorister. Ut fra en teknisk vurdering kan det gjennomføres langt mer avanserte operasjoner enn de som til nå er oppdaget. Hvorvidt enkelte operasjoner og metoder forekommer i dag uten at de oppdages, er uvisst men trolig.

Sikkerhetstilstanden er vurdert med utgangspunkt i kjente trusselaktører og deres metoder og virkemidler. NSM gir i denne rapporten sin vurdering av hvordan mangler og svakheter ved det forebyggende sikkerhetsarbeidet i virksomheter spesielt og ved sikkerhetstilstanden generelt kan bidra til at trusselaktører realiserer sine mål.[2]

---

[1] Norwegian Computer Emergency Team; Norges nasjonale senter for håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

[2] Rapporten gir en vurdering av tilstanden innen forebyggende sikkerhet basert på tilgjengelig empiri gjennom:

- NSMs tilsynsvirksomhet.
- Innrapporterte og observerte sikkerhetstruende hendelser og sikkerhetsbrudd.
- Tekniske sikkerhetsundersøkelser.
- Inntrengingstester.
- Emisjonssikkerhetstester.
- Personkontroll.
- Monitoring.
- Øvelser.
- NorCERT sin oversikt over og håndtering av hendelser på Internett.
- Andre sikkerhetsmessige forhold av interesse for sikkerhetstilstanden.

2 Risikobildet

Risikobildet som beskrives er hovedsakelig knyttet til informasjonssikkerhet.[3] Det er sammensatt av en vurdering av trusselbildet, verdier som må beskyttes, og de sårbarheter som kan utnyttes.

Redegjørelsen for trusselaktører i punkt 2.2. nedenfor er primært basert på informasjon fra Etterretningstjenesten (E-tjenesten) og Politiets Sikkerhetstjeneste (PST). Det vises konkret til PSTs ugraderte trusselvurdering[4] for nærmere omtale. Etterretningsaktivitet mot Norge og norske interesser vurderes som generelt høy, mens etterretningsaktivitet ved hjelp av IKT spesielt vurderes som stadig økende.

2.1 Samfunnsverdier

Digitaliseringen av samfunnet eksponerer stadig større mengder informasjon. Store mengder sensitiv informasjon[5] er tilgjengelig via åpne kilder og ugraderte informasjonssystemer på Internett. Dette gjelder både informasjon fra offentlig og internasjonal forvaltning og informasjon fra norsk industri og næringsliv. Sensitiv og kritisk[6] informasjon gjøres ofte tilgjengelig over IKT-systemer. Slik informasjon kan være viktig for beskyttelse av rikets sikkerhet og vitale nasjonale interesser. Kritiske samfunnsfunksjoner og infrastrukturer representerer fundamentale verdier som kan settes på spill dersom sensitiv eller kritisk informasjon kommer på avveie, manipuleres, eller blir gjort utilgjengelig.

På samme måte som at private virksomheter utenfor sikkerhetsloven ser en økende uønsket aktivitet rettet mot seg, er risikoen stor for at offentlige virksomheter – som alle er underlagt sikkerhetsloven – og private virksomheter underlagt sikkerhetsloven også blir utsatt for økt uønsket aktivitet. Slik aktivitet kan rettes mot ugraderte så vel som graderte informasjonssystemer.

2.2 Trusselaktører

Trusselaktørene legger ofte ned store ressurser i å gjøre det vanskelig å spore aktiviteten sin. Dette gjør det svært ofte krevende å knytte spesifikke aktører til en konkret aktivitet. EOS[7]-tjenestene omtaler derfor ofte trusselaktørene gjennom å referere til kategorier.

Alle trusselaktører kan potensielt ta i bruk et bredt spekter av metoder, gitt nødvendig tilgang, kompetanse og resurser. Trusselbildet skilles ikke lenger av landegrenser. Det er ofte vanskelig å skille mellom statlige og ikke-statlige aktører. I tillegg vil samme type hendelser kunne ha konsekvenser både for sivile og militære, offentlige og private,

[3] Objektsikkerhet iht. sikkerhetsloven er ikke behandlet i denne rapporten, ettersom de utfyllende regler om objektsikkerhet i loven, samt forskrift om objektsikkerhet, først trådte i kraft 1. januar 2011.

[4] www.pst.politiet.no

[5] Sikkerhetsgradert eller på annen måte sensitiv informasjon hva angår rikets eller virksomheters sikkerhet.

[6] Eksempelvis av avgjørende betydning for virksomheters fremtid.

[7] Etterretning, overvåking og sikkerhet.

virksomheter. De mest kostnads- og ressurskrevende – og dermed dimensjonerende – metodene, er det i dag fremmede stater som besitter. Ikke-statlige aktører, ofte med litt andre motiv, intensjoner og kapasiteter enn fremmede stater, utgjør imidlertid også alvorlige trusler mot personer, virksomheter og samfunnet generelt. Blant disse opererer stadig flere innen finanskriminalitet og industrispionasje. I tillegg øker aktiviteten fra "hacktivister" – personer eller grupperinger som fremmer religiøse, politiske eller nasjonalistiske budskap gjennom aktivitet på Internett.

Nedenfor følger en fremstilling av noen kategorier trusselaktører som utnytter svakheter i det forebyggende sikkerhetsarbeidet for å nå sine mål:

- **Fremmede staters etterretningstjenester** har de største kapasitetene og står bak de mest avanserte metodene. De søker primært å innhente informasjon[8] som kan fremme landets politiske og økonomiske interesser. I følge PST er det vedvarende høy etterretningsaktivitet mot Norge og norske interesser. Aktiviteten er hovedsakelig rettet mot forsvars- og sikkerhetspolitikk, olje- og gassektoren, høyteknologi, samt eksilmiljøer.[9] Denne trusselen må være dimensjonerende for den forebyggende sikkerhetstjenesten.
- **Finanskriminalitet og industrispionasje** fra ikke-statlige, og trolig noen statlige[10], aktører er et vedvarende problem. Det må antas at utbredelsen av industrispionasje er betydelig og underrapportert.[11] Kostnadene for samfunnet som resultat av IKT-basert kriminalitet er store. Til sammenlikning ble eksempelvis denne kostnaden estimert til rundt 250 milliarder kroner i Storbritannia i 2010[12]. Det er forventet at organiserte kriminelle vil ta i bruk stadig mer avanserte virkemidler for å nå sine mål.
- Betegnelsen **"Hacktivister"** brukes om personer eller grupperinger som fremmer et politisk, religiøst eller nasjonalistisk budskap gjennom forskjellige typer aktivitet på Internett, som for eksempel *defacing* av nettsider og tjenestenektsangrep (se punkt 2.2.1) mot nettsider eller nettadresser. Angrepene på *Regjeringen.no* i januar 2010 og *Dagbladet.no* i februar 2010 eksemplifiserer slik aktivitet.

2.2.1 Metoder og virkemidler

Risikoen for at virksomheter blir utsatt for uønsket aktivitet mot graderte og ugraderte systemer antas å være økende. Slik aktivitet blir stadig mer alvorlig og vanskelig å håndtere.

[8] Dette kan være både informasjon som er åpent tilgjengelig (åpne kilder) eller sensitiv informasjon som skal eller bør beskyttes.

[9] PSTs ugraderte trusselvurdering 2011.

[10] Det er ofte vanskelig å skille mellom eller bekrefte med sikkerhet hvem som står bak slik aktivitet, da det blant annet er relativt enkelt å skjule spor, eller rette disse mot andre aktører enn de som faktisk står bak.

[11] Kilde: Mørketallsundersøkelsen 2010, Næringslivets sikkerhetsråd m.fl.

[12] *The Cost of Cybercrime, 2011*, Cabinet Office Report, Storbritannia.

Selv den mest avanserte teknologiske skadevaren[13] avdekket mot norske interesser har vist relativt lav kompleksitet, spesielt i forhold til hva som er teknisk mulig. De mest avanserte metodene benyttes tilsynelatende ikke.

Nedenfor følger eksempler på de vanligste angrepsmetodene via **Internett**:

- *Defacement* er et angrep som har som formål å vandalisere eller endre nettsider, og er en form for elektronisk graffiti.
- En *Trojaner* er en ondsinnet, skjult programkode som legger til rette for uautorisert tilgang til et system. Trojanere blir ofte benyttet til å stjele sensitiv informasjon.
- *Phishing* er en betegnelse på innhenting av sensitiv informasjon. Begrepet brukes ofte i forbindelse med innhenting av passord til nettbanker eller kredittkortnummer.
- Et *Botnet* er et nettverk av trojanerinfiserte datamaskiner. Et Botnet bruker datakraft for å gjennomføre et angrep.
- Et *Tjenestenektangrep* (DoS[14]) er et angrep hvor nettsider eller nettadresser blir overbelastet av trafikk og satt ut av spill. Et tjenestenektangrep mot IKT-systemer i virksomheter med kritiske samfunnsfunksjoner vil kunne få alvorlige samfunnsmessige konsekvenser.

Det er kjent at en mengde gradert informasjon er tilgjengelig på Internett, enten lagt ut bevisst eller på grunn ubevisste handlinger. Slik informasjon kan identifiseres og utnyttes med negativ intensjon av trusselaktører.

Avlytting og avlesning er utbredte og ofte vellykkede metoder. Alt elektronisk utstyr avgir stråling, og er dermed utsatt for uønsket informasjonsinnhenting gjennom avlytting og avlesning. Denne strålingen kan blant annet komme fra kabel, tastatur, skjerm eller skriver. Metoder og utstyr som brukes i forbindelse med avlyttings- og avlesingsoperasjoner er under stadig utvikling.

Mobiltelefoner inneholder mye informasjon som uvedkommende kan få tilgang til. Mobilbruk kan overhøres og mobiltelefoner kan spores, avleses eller avlyttes. Spionprogramvare og virus kan lett installeres på mobiltelefoner. I tillegg er kontor og møterom utsatt for avlytting og avlesning. Markedet for avlyttings- og avlesningsutstyr er voksende.

Sosial manipulering[15] benyttes for å påvirke mennesker til å gi fra seg sensitiv informasjon eller utføre handlinger som de normalt ikke ville ha gjort. Dette er vanlig i forbindelse med inntrengning i informasjonssystemer. Sosial manipuleringen kan skje under direkte menneskelig omgang og kommunikasjon eller ved elektronisk kommunikasjon, for eksempel via e-post, direktemeldinger (*chat*) og ved bruk av sosiale medier.

[13] Skadelig programvare, på engelsk ”malware”.

[14] Denial of Service.

[15] Social engineering.

Innsideraktivitet kan begås av nåværende eller tidligere ansatte, konsulenter, vedlikeholdspersonell eller andre.[16] En innsider behøver ikke nødvendigvis selv å ha onde hensikter, men kan være sårbar overfor uvedkommende som er ute etter skjermingsverdig informasjon, enten gjennom forledelse, overtalelse eller press.

2.3 Sårbarhetsbildet

Funn fra NSMs tilsyn i virksomheter og annen empiri[17] fra 2010 viser at det eksisterer en rekke mer eller mindre vesentlige mangler i det forebyggende sikkerhetsarbeidet, og ved den nasjonale sikkerhetstilstanden. Disse representerer en sårbarhet som kan utnyttes av trusselaktører. Sårbarheter i forhold til bruk av IKT-systemer og annen behandling og kommunikasjon av sensitiv informasjon forsterkes av at mange virksomheter viser manglende vilje og evne til å prioritere og gjennomføre forebyggende sikkerhetsarbeid.

3 Sikkerhetstruende forhold

Her gir NSM sin vurdering av mangler og svakheter ved det forebyggende sikkerhetsarbeidet og hvordan disse kan lette eller tilrettelegge for sikkerhetstruende virksomhet[18]. Sikkerhetstruende forhold er vurdert opp mot at fremmede staters etterretningstjenester eller spesialavdelinger er den dimensjonerende trusselaktør.

NSM ser ofte at flere av manglene forekommer i en og samme virksomhet. DSS[19]-saken, hvor en rekke svakheter i informasjonssystemene som betjener en rekke norske departementer ble vurdert og oppdaget, er et eksempel på dette.

3.1 Verdiforståelse og bevissthet

Sikkerhetstiltak og prosedyrer må iverksettes i forhold til den trussel sikkerhetsgradert informasjon kan bli utsatt for.

Mange virksomheter underlagt sikkerhetsloven har mangelfull risikoforståelse. Dette får sitt uttrykk gjennom lav bevissthet for hvilke trusler de faktisk står overfor, hvilke verdier de har behov for å skjerme, samt hvilke sårbarheter som kan utnyttes.

Mange virksomheter viser også mangelfull kjennskap til, eller forståelse av, kravene i sikkerhetsloven. Det erfares videre at enkelte offentlige virksomheter, og deres ledere, ikke engang er klar over at virksomheten er underlagt sikkerhetsloven.

Manglende forståelse for, og bevissthet omkring hvilken verdi sikkerhetsgradert informasjon har for virksomheten, eller for samfunnet, kan føre til ukontrollert spredning av

[16] Wikileaks-saken er et antatt eksempel på dette.

[17] Blant annet Riksrevisjonen (revisjon av statsregnskapet) og NSM (se fotnote 2).

[18] Sikkerhetstruende virksomhet defineres her, og iht. sikkerhetsloven, som: forberedelse til, forsøk på og gjennomføring av, spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet.

[19] Departementenes servicesenter.

informasjonen, og dermed tap av verdier. For eksempel kan informasjon om alvorlige sårbarheter av samfunnsmessig betydning bli alminnelig kjent og utnyttet.

3.2 Oversikt over egen sikkerhetstilstand

Virksomhetens leder må kjenne til hvilken skjermingsverdig informasjon virksomheten håndterer. Ledere må også kjenne til mulige trusler og sårbarheter overfor sikkerhetsgradert informasjon.

Det er NSMs vurdering at mange virksomhetsledere, og dermed hele eller deler av organisasjonen, er lite bevisst hva som er virksomhetens sikkerhetsutfordringer og sikkerhetstilstand.

Virksomhetsleder etterspør ofte ikke informasjon om sikkerhet, og er ikke involvert i evaluering av sikkerhetsarbeidet eller resultatrapporteringen. Ofte finnes det ingen oversikt over virksomhetens sikkerhetsmessige utfordringer, ikke noe system for logg eller rapport over sikkerhetstruende hendelser, ingen retningslinjer for hvordan sikkerhetstruende hendelser skal håndteres, og heller ingen skriftlig evaluering av egen sikkerhetstilstand.

Veldig sjeldent blir virksomhetsleder eller NSM gjort kjent med eventuelle sikkerhetstruende hendelser[20] og eventuelle sikkerhetsbrudd[21], før et tilsyn blir gjennomført. Dette fordi rapporteringsrutiner ofte ikke ivaretas i tilstrekkelig grad. Videre er det sjeldent etablert systemer for informasjon eller varsel om sikkerhetsmessige forhold til virksomhetsleder. Manglende rapportering til NSM medfører at vi ikke får tilstrekkelig informasjon om sikkerhetstilstanden nasjonalt.

Som et resultat av manglende kjennskap til hendelser og brudd svekkes virksomhetens evne til læring og forbedring. Dette kan føre til at det ikke iverksettes sikkerhetstiltak som står i forhold til virksomhetens, og dermed potensielt rikets, faktiske sikkerhetsbehov.

3.3 Ledelsesengasjement

Virksomhetsledelsen må kjenne til hvordan den forebyggende sikkerhetstjenesten utøves og fungerer i egen virksomhet, for deretter å sørge for de nødvendige forbedringer.

Virksomhetsledere og andre i ansvarlige posisjoner engasjerer seg ikke tilstrekkelig i det forebyggende sikkerhetsarbeidet. Dette kan medføre nedprioritering og bremsing av iverksettelse av nødvendige sikkerhetstiltak, blant annet innen IKT-sikkerhet. NSM finner at ledere sjeldent blir målt på resultatoppnåelse i forhold til forebyggende sikkerhet, og aldri på et nivå som kan sammenlignes med målingen i forhold til økonomiske resultater.

Virksomhetenes sikkerhetsorganisasjon er ofte underdimensjonert, og dermed ikke i stand til å ivareta det forebyggende sikkerhetsarbeidet. I flere virksomheter finner NSM at verken

[20] Inkludert bevisst sikkerhetstruende virksomhet; alvorlig sikkerhetsbrudd, som gjentatte og systematiske brudd på sikkerhetsreglene; eller sikkerhetsmessig systemfeil.

[21] Enkeltstående brudd på sikkerhetsreglene.

leder eller sikkerhetspersonell er i stand til å svare på hva som er virksomhetens viktigste sikkerhetsutfordring(er).

NSM har gjort flere observasjoner som tyder på at virksomhetene bevisst velger å ikke etterleve sikkerhetsloven med forskrifter. Dette gjelder også regler knyttet til sikkerhetsgradering av informasjon. Virksomheten utsetter dermed potensielt andre og samarbeidende virksomheter for skade.

Manglende ledelsesengasjement innen forebyggende sikkerhet fører til manglende forankring, ressursbruk og prioritering. Begrenset anerkjennelse og engasjement fra virksomhetens ledelse gjør det krevende for sikkerhetspersonellet å utføre sikkerhetsarbeidet.

Sikkerhetsorganisasjonens eventuelt manglende tilgang og/eller store avstand til virksomhetsledelsen kan føre til at sikkerhetsmessige utfordringer ikke blir håndtert, og at sikkerhetsmessige akuttsituasjoner ender galt. Virksomhetsledelsen utsetter med dette potensielt også andre virksomheter for skade.

3.4 Styringssystem for sikkerhet

De beslutninger og føringer som ligger til grunn for den forebyggende sikkerhetstjenesten må beskrives i styrende dokumenter. Den forebyggende sikkerhetstjenesten må, så langt det er praktisk og tjenlig, samordnes med virksomhetens styringssystem for øvrig. Det må også være klare skiller mellom utøvende og kontrollerende oppgaver.

Virksomhetenes styringssystemer inkluderer ofte ikke forebyggende sikkerhet, og systemer for kvalitetsstyring på dette området er til dels fraværende. Manglende systemer for risikostyring er en gjenganger i så henseende.

Manglende styringssystem for sikkerhet fører til at virksomhetens oppfølging av det forebyggende sikkerhetsarbeidet ikke ivaretas på en systematisk og god nok måte. Dette vil også svekke virksomhetens mulighet for forbedring og læring. Sikkerhetsarbeidet blir preget av tilfeldigheter og uforutsette oppdukkende utfordringer.

Innen forebyggende sikkerhet blandes ofte utøvende og kontrollerende roller. Det vil si at man ofte ender opp med å kontrollere seg selv.

Virksomhetene har ofte manglende eller mangelfull dokumentasjon av eget sikkerhetsarbeid. Store virksomheter synes å gjøre en bedre jobb enn små, men disse er også gjerne eksponert for større risiko. Private virksomheter er ofte sertifisert i ISO 9000-serien og synes å ha bedre intern kultur for å følge opp sikkerhetsproblemer enn offentlige virksomheter.

Manglende dokumentasjon fører til at det ikke finnes tilstrekkelige kriterier for å kontrollere sikkerhetsarbeidet opp mot regelverket. Kvaliteten på sikkerhetsarbeidet, herunder grad av måloppnåelse, blir dermed utilstrekkelig belyst. En konsekvens av dårlig oppfølging er at det

ikke blir mulig å måle utviklingen fra år til år. Manglende dokumentasjon fører også til at eventuelt fungerende sikkerhetsarbeid ikke gjennomføres eller tas hensyn til.

3.5 Kompetanse

Virksomhetsledelsen må sørge for at personellet har den kompetanse som er nødvendig for sikker arbeidsutførelse. Sikkerhetsorganisasjonen må ha tilstrekkelig personell, kompetanse og verktøy.

NSMs tilsyn viser at mange ledere, og personell tillagt konkrete sikkerhetsoppgaver, ofte mangler kompetanse om hvordan oppgaver tilknyttet forebyggende sikkerhet skal eller kan løses. Få ledere har skolering i sikkerhetsstyring, sammenlignet med det de har for eksempel innen økonomistyring.

Selv når den grunnleggende sikkerhetsbevisstheten er til stede, finner NSM ofte at kompetanse med hensyn til konkrete sikkerhetstiltak er fraværende. Dette har som regel sammenheng med manglene opplæring og kompetanseplaner i virksomheten. NSM treffer arbeidstakere som vet at de mangler nødvendig kompetanse, men som ikke har fått nok støtte eller rom for kompetanseoppbygging. Profesjonelt arkivpersonale har som regel gode forutsetninger for og god kompetanse til å ivareta dokumentsikkerheten. Dette potensialet blir ofte for dårlig utnyttet; både rent operativt og til å spre kompetanse innad i virksomheten.

Når kompetansen mangler, blir det begått sikkerhetsfaglige feil som i seg selv skaper sikkerhetsrisiko og sårbarhet. Dette vil igjen legge til rette for at trusselaktører kan realisere sine mål ved hjelp av enklere og mindre kapasitetskrevende metoder og virkemidler enn de ellers ville ha brukt.

3.6 Sikkerhetskultur

Uønskede hendelser skal rapporteres og registreres internt i virksomheten. Hendelsene må håndteres for å begrense skade og hindre gjentakelse. Ved sikkerhetstruende hendelser[22] skal det rapporteres til NSM. Slike hendelser skal også vurderes rapportert til politiet.

Det begås både bevisste og ubevisste sikkerhetsbrudd. Det blir behandlet informasjon med høyere sikkerhetsgrad enn det et gitt informasjonssystem er godkjent for. Det er ved flere tilfeller påvist lav bevissthet omkring sårbarheter og trusler knyttet til bruk av mobiltelefoner og andre håndholdte kommunikasjonsenheter.

NSM har gjort observasjoner som tyder på at virksomhetsledere er kjent med at sikkerhetsloven ikke etterleves. Virksomhetene har ofte ikke systemer for negative sanksjoner i slike tilfeller. Det er svært uheldig dersom det gjøres en bevisst kalkulering med at man ikke blir oppdaget, både på ledelsesnivå og nedover i organisasjonen.

[22] Se https://www.nsm.stat.no/Arbeidsomrader/Rapportering-av-sikkerhetstruende-hendelse/, for kategorier av, og definisjon og eksempler på sikkerhetstruende hendelser.

Sikkerhetskulturen svekkes i virksomheter der sikkerhetstruende hendelser og sikkerhetsbrudd begås uten at dette får konsekvenser. Manglende sikkerhetskultur kan føre til at risikoadferd opprettholdes og dermed øker sannsynligheten for sikkerhetstruende virksomhet og ubevisste kompromittering av skjermingsverdig informasjon.

3.7 Rutiner ved sikkerhetsklarering

Personell må sikkerhetsklareres før de autoriseres og gis tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere.

Klareringsmyndigheters gjennomføring av personellklarering er ofte ufullstendig, noe som kan føre til at personell som ikke skulle vært klarert, faktisk blir det, og dermed utgjør en potensiell og langvarig trussel. Klareringsmyndighetene har i varierende grad gjennomført sikkerhetssamtaler, og i liten utstrekning dokumentert å ha innhentet utdypende opplysninger for bedre å belyse klareringssakene før avgjørelser ble fattet.

Manglende kompetanse og rutiner ved sikkerhetsklarering kan medføre at personell som ikke er sikkerhetsmessig skikket får sikkerhetsklarering og autoriseres for tilgang til skjermingsverdig informasjon.

3.8 Autorisasjon av personell

Personell må autoriseres før tilgang til sikkerhetsgradert informasjon gis.

Virksomhetene unnlater ofte å autorisere personell som i praksis har tilgang til sikkerhetsgradert informasjon. Dette kan være på systematisk basis ved tildeling av arbeidsoppgaver, eller mer tilfeldig ved at fysisk tilstedeværelse på arbeidsplassen gir mulighet for tilgang. Ofte forstår ikke virksomhetens ledelse forskjellen på klarering og autorisering, og tror at klarering er tilstrekkelig.

Når vilkårlige personer kan ha fått tilgang til sikkerhetsgradert informasjon uten at det finnes noen oversikt, er konsekvensen at denne informasjonen må anses som kompromittert.

3.9 Beredskap mot sikkerhetstruende hendelser

Det må eksistere beredskap for situasjoner som innebærer økt risiko for tap eller kompromittering av sikkerhetsgradert informasjon. Risikovurderinger må omfatte vurderinger av sannsynlighet for uønskede hendelser.

Mange virksomheter mangler evne til å sikre gradert materiale i krisesituasjoner.

Håndtering av sikkerhetstruende hendelser er ofte mangelfullt beskrevet og planlagt. Risiko- og sårbarhetsanalyser (ROS) i forhold til kontinuitetsplanlegging er ofte for enkle, da de ikke omfatter behovet for å videreføre sikkerhet i en krisesituasjon. Mangelfull ROS og beredskapsplanlegging kan medføre unødvendig stor grad av sikkerhetsrisiko i krisesituasjoner.

3.10 Dokumentsikkerhet

Skjermingsverdig informasjon må sikkerhetsgraderes i forhold til den skade som kan oppstå dersom informasjonen blir kjent for uvedkommende. Beskyttelsestiltak følger av graderingsnivå.

Virksomhetene har ofte mangelfull journalføring av, samt oversikt og kontroll over, graderte dokumenter. Dette er særlig tilfelle i virksomheter som håndterer store mengder gradert informasjon. Det forekommer at virksomheter ikke kan gjøre rede for hvor graderte dokumenter befinner seg. Dette kan føre til at slike dokumenter kommer på avveier. Tilstanden er som regel best der hvor arkivpersonalet gis full kontroll over dokumentflyten.

3.11 Fasiliteter for sikkerhetsgraderte samtaler

Sikkerhetsgraderte samtaler på høyere graderingsnivå skal kun finne sted i rom som er tilstrekkelig sikret og godkjent for dette formålet.

Det er ofte manglende bevissthet rundt avlyttingstrusler og hvilke administrative og tekniske mottiltak som er nødvendige for å avverge slike. Dette kan være en medvirkende årsak til at det eksisterer forholdsvis få fasiliteter som egner seg for sikkerhetsgraderte samtaler, særlig på høyt graderingsnivå. Som et resultat foregår sikkerhetsgraderte samtaler på uegnede steder.

3.12 Fysisk sikring

Skjermingsverdig informasjon må behandles og oppbevares innenfor sikrede områder. Beskyttelsestiltak skal sikre mot uautorisert fysisk tilgang til skjermingsverdig informasjon.

NSM finner at flere virksomheter mangler klart definerte og avgrensede områder for behandling av gradert informasjon. Ved mange virksomheter er det ikke vakthold utenom normal arbeidstid. I andre tilfeller er det installert anlegg for innbruddsalarm som ikke er underlagt jevnlig funksjonskontroll og ettersyn. Mangelfulle rutiner kan føre til at uvedkommende har adgang i lang tid uten at det oppdages.

Uobservert fysisk tilgang til datamaskiner gir oftest mulighet for uautorisert inntrengning i maskinene, med tap av konfidensialitet og integritet på informasjonen som følge. All informasjon i IKT-systemer uten tilstrekkelige og oppdaterte sikkerhetstiltak kan potensielt avleses, fjernes eller endres uten at det oppdages.

3.13 IKT-sikkerhet

Avhengigheten av IKT er blitt en strategisk sikkerhetsutfordring. Alvorlige IKT-angrep mot virksomheter med kritiske samfunnsfunksjoner må kunne oppdages og håndteres. Sikker informasjonshåndtering er i økende grad avgjørende for å sikre og videreutvikle viktige samfunnsverdier.

Man plikter å hindre at uvedkommende får adgang til sikkerhetsgradert informasjon. Dette inkluderer sikring av IKT-systemer som oppbevarer og behandler slik informasjon.

NSM har håndtert i overkant av 5000 hendelser av varierende størrelse og alvorlighetsgrad i 2010. De mest avanserte og mest bekymringsfulle IKT-hendelsene NSM har håndtert i 2010 (både åpne og lukkede nett) har vært rettet mot departementer og større norske bedrifter. Her er noen eksempler:

- En ansatt i et departement mottok i november 2010 en e-post som tilsynelatende var sendt fra en internasjonal organisasjon. E-posten inneholdt et vedlegg med en hittil ukjent ondsinnet programvare (en trojaner), som gir angriperen kontroll over datamaskinen og mulighet til å stjele informasjon fra denne. Andre tjenestemenn i Europa fikk trolig samme e-post, uten trojaneren innebygd.
- Flere departementer mottok i november 2010 mistenkelige e-poster som omtalte en annen internasjonal organisasjon. E-posten var sendt fra en forfalsket avsenderadresse og inneholdt et vedlegg med en trojaner.
- I juli 2010 ble det oppdaget mistenkelig nettverkstrafikk fra en datamaskin tilhørende en ansatt i et departement. Det ble oppdaget to ulike trojanere. Det ene trojaner-viruset samlet inn alle dokumenter opprettet den siste uken og klargjorde disse til å bli sendt til angriperen. Det andre var av samme type som infiserte Pentagon i 2009, og førte til at det amerikanske forsvaret forbød bruk av minnepinner.
- I juni 2010 skulle det holdes en tilstelning ved en norsk offentlig etat. Det ble sendt e-post med invitasjon til embetsmenn i inn- og utland. Kort tid etter ble en ny e-post vedrørende samme sak sendt til de samme mottakerne, men fra en falsk avsender. Et av vedleggene inneholdt en trojaner.
- I april 2010 oppdaget en ansatt hos en norsk bedrift en e-post som utga seg for å være fra en ansatt i NASA. E-posten inneholdt et dokument som forsøkte å laste ned en trojaner fra Internett. Denne trojaneren var et fjerninnloggingsverktøy som ville gitt angriperen full kontroll over kompromitterte maskiner.
- En annen norsk bedrift avdekket fire målrettede angrep med trojanere i 2010. Emnene i e-postene var relatert til forsvarsindustrien. Trojanerne var ulike versjoner av fjerninnloggingsverktøy som ville gitt angriperen full kontroll over kompromitterte maskiner.
- I april 2010 ble flere ansatte i en tredje bedrift som jobbet med et bedriftskonfidensielt prosjekt utsatt for målrettede trojanere i e-post. E-postene med trojanerene kom fra falske avsendere og ga inntrykk av å være sendt fra personer involvert i prosjektet.
- Det er påvist flere forsøk på å stjele penger fra norske nettbanker i 2010, men ingen har, så vidt vi vet, lykkes. Flere trojanere er nå spesialtilpasset norske nettbanker. Dette gjør at brukeren vanskelig forstår at han logger seg inn på en falsk nettbank[23].

[23]Informasjonsstjelende trojanere kan også stjele kontoinformasjon, brukernavn, passord og kredittkortinformasjon. Tyveri av kredittkortnumre er en daglig problemstilling på Internett, også i Norge.

- Banktrojaneren *Zeus* var en av de mest omtalte informasjonsstjelende trojanerne i 2010. Den distribueres i stadig nye versjoner, samtidig som det er lav grad av nødvendig deteksjonskapasitet blant antivirusprogrammer.
- I januar 2010 ble nettsidene til flere offentlige myndigheter utsatt for et distribuert tjenestenektangrep (DDoS)[24]. Flere andre nettsteder har opplevd det samme i løpet av 2010, blant annet nettsidene til aviser, bedrifter og interesseorganisasjoner.
- I 2010 dukket dataormen *Stuxnet* opp som en kvalitativt ny trussel mot informasjonssystemer. *Stuxnet* er en målrettet dataorm, som kan reprogrammere og sabotere en eller flere spesifikke industriprosesser. Den spres ved hjelp av forskjellige metoder. Dette er den første kjente skadevaren som rettes spesifikt mot prosesskontrollsystemer, og den første skadevaren som bruker stjålne sertifikater fra kjente leverandører som Microsoft stoler på. Det har krevd betydelige ressurser å lage *Stuxnet*. Irans president Ahmedinejad innrømmet i desember 2010 at *Stuxnet* har påvirket landets atominstallasjoner.

Virksomhetene klarer oftest ikke å vedlikeholde tilfredsstillende sikkerhet i forhold til IKT-systemer. Typiske avvik i administrasjon av IKT-systemer er:

- Manglende sikkerhetsoppgradering (*patching*).
- Mangelfull passordadministrasjon.
- Testing av ny programvare eller applikasjon uten å fjerne testapplikasjonen og pålogging til den etterpå.
- Mangelfull fjerning av gamle versjoner ved oppdateringer.
- Manglende oppmerksomhet på tidsbegrensinger i anti-virus-programvare[25].
- Manglende begrensninger i brukernes muligheter til å laste ned tredjeparts programvare.

Samfunnet baserer seg i økende grad på digitale løsninger for kommunikasjon, oppbevaring av informasjon og styring av viktige prosesser. Uønsket aktivitet over Internett utgjør risiko for stor skade mot Norge og norske interesser.

3.14 Svakheter i leverandørkjeden for IKT-utstyr

Leverandørkjeden for informasjonssystemer som skal behandle gradert informasjon må kontrolleres.

Produsenter, leverandører og distribusjonsnettverk kan infiltreres slik at produkter kan kompromitteres før det når frem til systemeier og sluttbruker. For brukeren av kompromitterte systemer vil utstyret fungere som forventet. Ved bruk av IKT-utstyr som skal behandle og lagre skjermingsverdig informasjon, representerer dette en betydelig risiko. Uvedkommende vil kunne få ubemerket tilgang til all informasjon i systemet.

[24] Et DDoS angrep betyr at web-tjenerene blir bombardert med forespørsler fra angripende datamaskiner, noe som gjør at vanlige brukere ikke fikk tilgang til websidene. De fleste slike angrep får man raskt (i løpet av timer eller dager) kontroll på hvis man har en god beredskap. Jf. definisjonen i punkt 2.2.1.

[25] Nyere versjoner av programvaren stopper ofte ikke gammel og antatt ukurant skadevare.

4 Konklusjon om sikkerhetstilstanden

Avhengigheten av velfungerende IKT er blitt en strategisk sikkerhetsutfordring. Samfunnet baserer seg i økende grad på digitale løsninger for kommunikasjon, oppbevaring av informasjon og styring av viktige prosesser. Uønsket aktivitet over Internett utgjør en stor skaderisiko for Norge og mot norske interesser. Sikker informasjonshåndtering er i økende grad avgjørende for å sikre og videreutvikle viktige samfunnsverdier.

Til nå har terrorgrupper først og fremst benyttet Internett til kommunikasjon og trening. Det antas dog at alvorlige sabotasjeangrep, som *Stuxnet*-angrepet mot Iran – eventuelt designet som terrorverktøy – vil kunne brukes igjen. Det er sannsynlig at slike angrep kan og vil nyttes til å ødelegge eller overta prosesstyringssystemer innen samfunnskritisk infrastruktur, som for eksempel ved kraftverk, oljeinstallasjoner eller ved militære anlegg og systemer. Vi vet lite om sannsynligheten for at slike angrep i fremtiden rettes mot norske interesser eller mål. Det vi derimot har kunnskap om, er at muligheten og kapasitetene eksisterer der ute. I den sammenheng må det også tas forbehold om at sårbarheter i norske IKT-systemer kan utnyttes for å ramme en tredjepart, som for eksempel våre allierte og samarbeidspartnere. Olje- og gassleveranser er et tankekors i så henseende.

Avlytting og avlesning er utbredte og ofte vellykkede metoder, som ofte gjennomføres uten å bli detektert dersom tilfredsstillende mottiltak ikke eksisterer eller innføres. Alt elektronisk utstyr avgir stråling, og denne vil i økende grad utnyttes med negativ hensikt. Mobiltelefoner vil bli et økende mål for avlytting fra fremmed etterretning. Fysiske fasiliteter, som ambassadelokaler eller militær infrastruktur med umiddelbar nærhet til andre etasjer eller bygninger, vil fortsette å være mål for avlytting i overskuelig fremtid.

Sosial manipulering benyttes til å påvirke mennesker til å gi fra seg sensitiv informasjon eller som inngangsport til slik informasjon. Dette vil i økende grad skje via inntrengning i informasjonssystemer som e-post, *Facebook* og lignende, men også gjennom personlig kontakt fra etterretningsagenter, industrirepresentanter eller lignende.

NSM observerer en situasjon med økende sikkerhetsmessig *risiko*. Det er til dels vesentlige mangler i det forebyggende sikkerhetsarbeidet med konsekvenser for den nasjonale sikkerhetstilstanden. Disse representerer en sårbarhetsutfordring for det norske samfunn, som kan utnyttes av trusselaktører med stadig økende kapabiliteter og kapasiteter. Det observeres at:

- Det generelt er slik at de *verdier* vi ønsker å beskytte øker i volum og betydning i takt med samfunnsutviklingen og den økende produksjonen av informasjon, blant annet sikkerhetsgradert informasjon.
- *Truslene* mot sikkerhetsgradert og annen skjermingsverdig informasjon er i sterk økning; særlig akselererer den teknologiske oppfinnsomheten med hensyn til utvikling av skadevare på IKT-systemer.
- *Sårbarheter* knyttet til IKT øker, noe som øker mulighetene for at uvedkommende får tilgang til skjermingsverdig informasjon.

- *Tiltak* for å redusere sårbarheter utvikles ikke i takt med truslene, og er i utgangspunktet utilstrekkelige.

Disse observasjonene tilsier at sikkerhetstilstanden forverres. NSM har tidligere rapportert om et økende gap mellom trusselaktørers kapasiteter og eksisterende sikkerhetstiltak. Trenden er at dette gapet fortsetter å øke. Dessuten er det svært uheldig at sikkerhetstruende forhold vedvarer uten iverksettelse av nødvendige mottiltak og korrigeringer. Det er derfor behov for beslutninger om, samt vilje og ressurser til å iverksette tiltak som har til hensikt å redusere sårbarheter og øke evnen til å oppdage og håndtere de oppdukkende truslene.

5 Trender

Trusselaktører med flere og mer avanserte kapasiteter vil i fremtiden kunne bruke ulike metoder og virkemidler til å utnytte mangler i det forebyggende sikkerhetsarbeidet. Basert på erfarte sikkerhetshendelser og sikkerhetsavvik i virksomheter de siste årene, forventes en fortsatt økning i alvorlige IKT-hendelser over de kommende år. Selv robuste IKT-systemer, og samfunnskritisk infrastruktur som i dag ansees som sikre, vil ikke være sikret mot kjente og ukjente tekniske trusler og avanserte aktiviteter. Den mest skremmende mulige trusselutfordringen i fremtiden, er at et massivt destruktivt angrep gjennomføres mot Norge og/eller våre allierte.

I tiden fremover er det god grunn til å holde øye med følgende trender:

- Økende utfordringer rundt klarering av personell med tilknytning til andre stater.
- Mer profesjonell utvikling av ondsinnet programvare.
- Målrettede angrep mot lukkede nett. Det har vist seg at lukkede nett ikke er så sikre som antatt, særlig med hensyn til uforsiktig bruk av minnepinner og tilkobling av annet eksternt (mobilt) utstyr i driftssammenheng.
- Økt spredning av skadevare over mobile enheter som mobiltelefoner, særlig ”smarttelefoner” og diverse ”pads”.
- Flere sårbarheter i leverandørkjeden av IKT-utstyr.
- Flere forsøk på å infiltrere prosesskontrollsystemer.
- Økende, ofte usikker, lagring av informasjon i nettskyen.

I lys av kortsiktige trender, hvor det forebyggende sikkerhetsarbeidet har stagnert, kan fremtiden se enda mer dyster ut på lang sikt. Såfremt man ikke bryter med den gjeldende sikkerhetstrenden, og den teknologiske utviklingen fortsetter, vil avhengighet av posisjoneringsdata og en tendens til tettere kobling og sterkere gjensidige avhengigheter mellom forskjellige samfunnskritiske funksjoner forventes å øke på lang sikt. Dette vil ha implikasjoner for sikkerhetsarbeidet, ikke minst innen forsvarssektoren.

Hvis vi forutsetter at det ikke kommer vesentlig trendbrudd vil forebyggende samfunnssikkerhet på lang sikt utfordres av følgende aspekter:

- Både statlige og ikke-statlige aktører får økte IKT-kapasiteter.
- Ondsinnet programvare vil gradvis bli mer avansert.
- Internett og andre IKT-systemer og tilhørende verktøy vil i økende grad bli benyttet til alle former for krigføring.
- Innføring av ny teknologi vil medføre nye måter å manipulere og utnytte sårbarheter i IKT-systemer.
- Tekniske sårbarheter vil forsterkes som følge av for svake administrative rutiner og menneskelig adferd.

Som enkelthendelse, eller synkroniserte i serier, er sabotasje- eller terrorangrep mot prosesskontrollsystemer for kritisk infrastruktur, den største trusselen vi i dag vet om. Med den økende avhengigheten mellom forskjellige samfunnskritiske komponenter, kan flere kritiske mål og/eller funksjoner i samfunnet skades, eller lammes i ett enkeltstående angrep.

Basert på eksisterende samfunnsverdier og den risiko disse utsettes for gjennom mulige trusler og eksisterende sårbarheter, er det svært viktig at nødvendige mangler og svakheter i det forebyggende sikkerhetsarbeidet utbedres både på kort og lang sikt. Hvis dette ikke skjer tyder mye på at vi vil gå en høyst usikker fremtid i møte.