Nasjonal sikkerhetsmyndighet

Rapport om sikkerhetstilstanden 2009

Ugradert versjon

I denne rapporten redegjør Nasjonal sikkerhetsmyndighet (NSM) for etterlevelsen av sikkerhetsloven med forskrifter samt vurderer kvaliteten på det forebyggende sikkerhetsarbeidet. Rapport om sikkerhetstilstanden baseres hovedsakelig på resultater fra tilsyn, innrapporterte hendelser, og medieovervåkning.

NSM har ansvar for å føre tilsyn med sikkerhetstilstanden i virksomheter som er underlagt sikkerhetsloven, og at lovpålagte krav til forebyggende sikkerhetstjeneste er oppfylt. NSM er videre gitt i oppdrag å bistå, veilede og gi råd til virksomheter som behandler sikkerhetsgradert informasjon eller råder over skjermingsverdige objekter.

God sikkerhetstilstand, i virksomhetene og i samfunnet helhet, forutsetter effektivt sikkerhetsarbeid gjennom en planlagt og systematisk forebyggende sikkerhetstjeneste. Dette er virksomhetenes ansvar.

1 Sammendrag

Det er et forbedringspotensial når det gjelder sikkerhetstilstanden i Norge. I denne rapporten redegjør NSM for sin bekymring knyttet til forhold som manglende lederforankring, manglende organisering av sikkerhetsarbeidet, samt andre sentrale forhold av betydning for sikkerhetstilstanden.

Det er NSMs overordnede vurdering at sikkerhetstilstanden i Norge, og kvaliteten på virksomhetenes sikkerhetsarbeid ikke er tilstrekkelig, sett i forhold til dagens trusselbilde. Etterretningstrusselen mot Norge, og mot norske interesser, er i følge PST vedvarende høy. Mye av denne virksomheten foregår via IKT-systemer.

Særlig de to siste årene har IKT-trusselen økt betraktelig. Denne trusselen er teknisk avansert og dynamisk. Risikoen for at virksomheter underlagt sikkerhetsloven kan bli utsatt for forsøk på etterretning er økende.

På bakgrunn av tilgjengelig informasjon i 2009 samt utviklingen tidligere år har NSM lagt vekt på følgende tendenser og temaer:

- Manglende ledelsesengasjement
- Mangelfull organisering
- Mangelfull kompetanse og bevissthet
- Mangelfull deteksjon, rapportering og håndtering av hendelser
- Mangler i sikkerhetsklarering og autorisasjon
- Mangelfull håndtering og oppbevaring av graderte dokumenter
- Mangler innen håndteringen av graderte IKT-systemer

Manglende forståelse, både for risikonivå og trusselbildet
Omfanget av avvik knyttet til sikkerhetsledelse kan tyde på manglende forståelse, både for risikonivå og trusselbildet, og for behovet for å beskytte skjermingsverdig informasjon og skjermingsverdige objekter. Det kreves ikke at den enkelte leder har sikkerhetsfaglig spisskompetanse,. Det er imidlertid et krav at virksomhetsledelsen kjenner sikkerhetslovens formål og betydning for virksomheten. De skal også være kjent med verdier virksomheten råder over og ta ansvar for de sikkerhetstiltak som er nødvendig.

Utilstrekkelig organisering
Avvikene tyder også på at det forebyggende sikkerhetsarbeidet er utilstrekkelig organisert. Forebyggende sikkerhet bør være en integrert del av virksomhetenes ordinære styringssystem. Dette er som regel godt utviklet og har gode rutiner for å oppdage og korrigere avvik innen styringsområder som HMS eller økonomi.

Økende gap mellom risikobilde og sikkerhetsarbeid
NSM har i tidligere rapportering uttrykt bekymring for et økende gap mellom et dynamisk risikobilde og et stillestående sikkerhetsarbeid. Det er grunn til å gjenta denne bekymringen. Det er et behov for å sette sterkt fokus på årsaker til at sikkerhetsarbeidet ikke prioriteres godt nok. Det er lederen i den enkelte virksomhet som sitter med nøkkelen til en god sikkerhetstilstand.

2 Innledning

I denne rapporten gis en vurdering av tilstanden innen forebyggende sikkerhet basert på tilgjengelig informasjon i 2009. Rapporten omtaler i stor grad sårbarheter forbundet med utilsiktede og skadelige konsekvenser av menneskelig aktivitet (eller svakheter).

Det forebyggende sikkerhetsarbeidet som NSM gjennom sikkerhetsloven er satt til å føre kontroll med, er et forebyggende tiltak som i vesentlig grad handler om å redusere sårbarheten overfor bevisste ondsinnede handlinger eller trusler.

Måling av sikkerhetstilstanden avhenger av mengde og kvalitet på tilgjengelig informasjon. NSM har tidligere signalisert at denne er utilstrekkelig. Særlig registrerer vi underrapportering av sikkerhetstruende hendelser, både internt i virksomhetene og til NSM. Dette gir usikkerheter ved vurdering av sikkerhetstilstanden, og utilstrekkelig grunnlag for virksomhetenes eget arbeid med kontinuerlig sikkerhetsforbedring.

Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) uttaler seg om trusler, trusselutøvere og trusselaktører mot rikets sikkerhet og vitale nasjonale sikkerhetsinteresser[1]. I forhold til NSMs rapport om sikkerhetstilstanden er det særlig relevant at PST vurderer at *etterretningstrusselen er høy*.

Etterretnings-, overvåknings- og sikkerhets- (EOS) tjenestene mener at trusselnivået knyttet til IKT-baserte virkemidler har økt de siste årene. Erfaringer fra Varslingssystemet for digital infrastruktur (VDI) i NSM påviser et økende antall IKT-hendelser. Disse er stadig mer alvorlige og vanskeligere å håndtere. Et økende antall sikkerhetspolitiske konflikter har et element av cyberaktivitet i seg. Det er et ledd i denne utviklingen at mange stater bygger opp etterretnings- og angrepskapabiliteter til bruk i cyberspace.

NSM er gitt i oppdrag å rapportere om trusler mot IKT. Koordineringsgruppen for IKT-trusselbildet er omtalt i St. meld. nr. 22 (2007-2008) fra Justisdepartementet. Den består av representanter fra EOS-tjenestene og ble opprettet som et resultat av en felles forståelse for at enkelte hendelser ikke lot seg håndtere uten et nært samarbeid. IKT-trusselbildet kan i økende grad settes i sammenheng med PSTs vurdering av etterretningstrusselen, da etterretningsvirksomhet via Internett er sterkt økende.

Risikoen for at virksomheter underlagt sikkerhetsloven kan bli utsatt for vellykkede forsøk på etterretning via Internett er økende.

3 Trender og funn

NSM gjennomfører tilsyn for å vurdere samsvar mellom tilsynsobjekters beskyttelse av skjermingsverdig informasjon og bestemmelser gitt i eller i medhold av sikkerhetsloven.

Tilsynene gjennomføres i henhold til internkontrollprinsippet, det vil si som undersøkelser av tilsynsobjektenes styringssystem, understøttet av undersøkelser av konkrete sikkerhetstiltak og -prosedyrer som tilsynsobjektene har iverksatt.

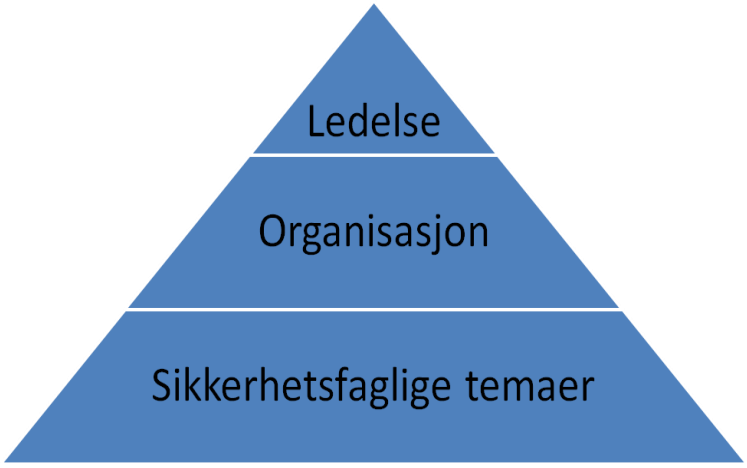
[1] Noe forskjellig beskrevet i ulike lover

Tilsyn utføres overfor offentlige virksomheter og med private virksomheter som er underlagt sikkerhetsloven, enten gjennom særskilt vedtak eller som leverandør i sikkerhetsgradert anskaffelse. Det kan konstateres at det er en rekke forbedringspunkter.

Det enkelte avviket er i seg selv av begrenset interesse. Avvikene tenderer imidlertid til å peke i retning av noen overordnete konklusjoner om sikkerhetsarbeidet og sikkerhetstilstanden:

- Mangler i overordnet ledelse og ledelsesengasjement i form av utilstrekkelig styring og oppfølging av sikkerhetsarbeidet
- Mangler i organisering av sikkerhetsarbeidet

Manglende ledelsesengasjement regnes som det mest overordnede. Mangler ved sikkerhetsledelsen vil gi utilstrekkelig sikkerhetsorganisering som igjen vil medføre mangler ved utvikling og gjennomføring av sikkerhetstiltak.



Figur 1: Hierarki: ledelse, organisering og sikkerhetsfaglige temaer

3.1 Manglende ledelsesengasjement

Det er NSMs generelle vurdering at det er betydelig forbedringspotensialet knyttet til ledelsens engasjement i sikkerhetsarbeidet. Denne vurderingen underbygges av følgende typiske avvik avdekket gjennom tilsyn:

- Mangelfull kommunikasjon av forventninger til organisasjonen og den til enkelte medarbeiders sikkerhetsforståelse og sikkerhetsarbeid
- Mangelfull delegasjon av ansvar og fordeling av oppgaver internt.
- Mangelfull oppfølging av underlagte organer og virksomheter
- Manglende evaluering av sikkerhetstilstanden i virksomheter, herunder manglende oppfølging av resultater fra sikkerhetsrevisjoner
- Mangelfull rapportering av sikkerhetstruende hendelser.

Dette er sentrale lederoppgaver. Disse manglene kan neppe eksistere dersom virksomhetsleder engasjerer seg i sikkerhetsarbeidet. Det kreves ikke at den enkelte leder har sikkerhetsfaglig spisskompetanse, men det er et krav at virksomhetsledelsen kjenner sikkerhetslovens formål og betydning for virksomheten, og er kjent med de verdier virksomhetene råder over og tar ansvar for de sikkerhetstiltak som er nødvendig.

3.2 Mangelfull organisering

Det forebyggende sikkerhetsarbeidet tenderer til ikke å være underlagt samme styring som andre oppgaver.

Ved en rekke tilsyn finner man avvik som disse:

- Mangelfull samordning mellom styringssystemer for forskjellige typer sikkerhet.
- Mangelfull, underdimensjonert og ressurssvak sikkerhetsorganisering i forhold til sikkerhetsbehovet
- Mangelfull gjennomføring av sikkerhetsfaglige tiltak innen forebyggende sikkerhet.

De fleste virksomheter er enten pålagt å ha styringssystemer for egen virksomhet, eller har dem av ren egeninteresse. Disse systemene er som regel godt utviklet og har gode rutiner for å oppdage og korrigere avvik innen forskjellige styringsområder som HMS eller økonomi. Forebyggende sikkerhet tenderer til ikke å være inkludert i slike systemer. Virksomhetsleder bør iverksette den type tiltak som ellers er vanlig i virksomhetsstyringen, slik at disse også gjelder for den forebyggende sikkerhet.

Sikkerhetsloven med forskrifter har klare krav om skille mellom slike oppgaver slik at ikke en og samme medarbeider blir satt til å kontrollere eget sikkerhetsarbeid. Når utførende og kontrollerende oppgaver tillegges samme medarbeider skaper dette uklarheter. Regelverkets prinsipp er at sikkerhet utøves av linjeorganisasjonen og kontrolleres av sikkerhetsorganisasjonen. Dette prinsippet følges ikke alltid.

3.3 Mangelfull kompetanse

NSMs tilsyn avdekker gjennomgående svakheter med personellets forståelse, kunnskaper og ferdigheter knyttet til forebyggende sikkerhetsarbeid.

Flere medarbeidere i virksomheter NSM har ført tilsyn med har ikke tilstrekkelig og relevant kompetanse i forebyggende sikkerhetstjeneste tilpasset den enkeltes oppgaver. Et typisk trekk er manglende forståelse for og ferdigheter knyttet til fortløpende risikovurdering og –håndtering.

3.4 Mangelfull deteksjon, rapportering og håndtering av hendelser

Det er ikke etablert gode nok rutiner for deteksjon, rapportering og håndtering av hendelser i virksomhetene, verken internt eller i forhold til NSM.

Antallet innrapporterte sikkerhetstruende hendelser og sikkerhetsbrudd til NSM var lavt i 2009. Det er på det rene at det er en betydelig underrapportering. Dette er et forhold NSM påpekte i rapport om sikkerhetstilstanden i 2008. Situasjonen har ikke bedret seg nevneverdig i 2009. NSMs tilsyn viser at verken virksomhetsleder, lokal sikkerhetsorganisasjon eller NSM får tilfredsstillende rapportering om hendelser.

3.5 Mangler i sikkerhetsklarering og autorisasjon

For å få tilgang til sikkerhetsgradert informasjon er det en forutsetning at man er sikkerhetsklarert og/eller autorisert. For flere virksomheter er det avdekket mangler ved at personell blir gitt tilgang til sikkerhetsgradert informasjon uten nødvendig sikkerhetsklarering eller autorisering.

En av utfordringene for virksomhetene er ofte at delegasjon av myndighet til å autorisere er uklar, ved at dette gjøres uformelt og ikke skriftlig.

3.6 Mangelfull håndtering og oppbevaring av graderte dokumenter

Graderte dokumenter håndteres og oppbevares på en usikker måte i mange virksomheter.

Typiske avvik har vært at graderte dokumenter:

- Ikke var journalførte.
- Ikke fremkom av journal som sikkerhetsgraderte.
- Ble behandlet, sendt og mottatt utenfor arkivkontroll.

Intern distribusjon av sikkerhetsgraderte dokumenter blir ofte dårlig kontrollert i den forstand at man ikke vet hvem som besitter et bestemt dokument.

Dessuten forekommer det at personer uten sikkerhetsklarering har adgang til slike dokumenter. Tilsyn har vist at det forekommer at virksomheter har generelt mangelfull kontroll med sikkerhetsgraderte dokumenter.

Virksomheter sitter ofte på for mye sikkerhetsgradert materiale som ikke benyttes i saksbehandling og som kan avhendes.

Tilsvarende finnes det ofte utilstrekkelig håndtering og kontroll av graderte lagringsmedier.

3.7 Mangler innen håndteringen av graderte IKT-systemer

Mange virksomheter håndterer ikke graderte IKT-systemer i samsvar med regelverket og det forekommer også avvik fra bestemmelser om håndtering av krypto.

Sikkerhetsgradert informasjon blir ofte behandlet på informasjonssystem som ikke er sikkerhetsgodkjent og som ofte ikke er merket slik at det er mulig å identifisere maskinvaren som sikkerhetsgradert. Utfordringen er unødvendig ettersom det i mange tilfeller er mulig for virksomheten å enkelt sikkerhetsgodkjenne og merke informasjonssystemet selv.

Videre viser NSMs tilsyn at sikkerhetsgraderte informasjonssystemer ofte er mangelfullt dokumenterte og registrerte. Blant annet mangler vurdering av risiko i forbindelse med plassering og bruk. Det samme gjelder ofte andre sikkerhetsgraderte lagringsmedier, særlig minnepinner.

Instrukser for sikker bruk av sikkerhetsgraderte informasjonssystemer mangler ofte helt eller er svært mangelfulle. NSMs tilsyn viser at sikkerhetsvilkår knyttet til IKT-tjenesteleveranse oftest ikke er regulert i avtale eller på annen måte.

4 Sikkerhetsrelaterte hendelser på Internett

4.1 Kort om IKT-trusselbildet

Med **IKT-trusler** menes alle uønskede handlinger, herunder reelle og potensielle, som kan rettes mot nettverk og elektroniske informasjonssystemer.

Med **IKT-trusselbildet** menes informasjon om 1) trusselaktører og deres intensjoner og kapasiteter, 2) metoder som trusselaktører benytter eller kan tenke seg å benytte, 3) hvilke mål som kan være attraktive for trusselaktører å angripe eller utnytte og 4) erfarte hendelser.

IKT-trusselbildet er komplekst. Det er hensiktsmessig å gruppere truslene i følgende kategorier:

- destruktive og forstyrrende angrep,
- etterretning
- kriminalitet
- aktivisme
- vandalisme og hevn

Omfattende destruktive eller forstyrrende angrep i "cyberspace" representerer alvorlige, men sjeldent forekommende ekstremtilstander. Etterretning, kriminalitet, aktivisme og vandalisme er dagligdagse hendelser og utgjør vedvarende sikkerhetsutfordringer.

Felles for de fleste av truslene er at de utnytter ulike sårbarheter og svakheter, både menneskelige og tekniske. Ellers er type, omfang, alvorlighetsgrad og motivasjon like mangeartet som i den fysiske verden.

4.2 Målrettede trojanere

NSM har i løpet av 2009 mottatt informasjon om og bidratt til å avdekke og håndtere et økende antall saker som involverer informasjonsinnsamling med målrettede trojanere. Dette er programvare som er særskilt egnet til etterretningsvirksomhet.

Det er ikke usannsynlig at store mengder informasjon er på avveie som følge av disse datainnbruddene. I de fleste av disse sakene har det vært avdekket at berørte systemer har vært kompromittert over lengre tid.

Det er lenge advart mot spredning av uønsket kode via e-post og kompromitterte nettsteder. I begynnelsen av 2009 opplevde man også en betydelig spredning av programkode via USB-tilkoblede enheter som minnepinner.

4.3 Banktrojanere

Sofistikerte trojanere som f. eks Clampi[2] og Zeus[3] blir benyttet til omfattende informasjonsinnsamling. Et av hovedmotivene bak disse trojanerne er nettbanksvindel, men

[2] Clampi http://www.secureworks.com/research/threats/clampi-trojan/

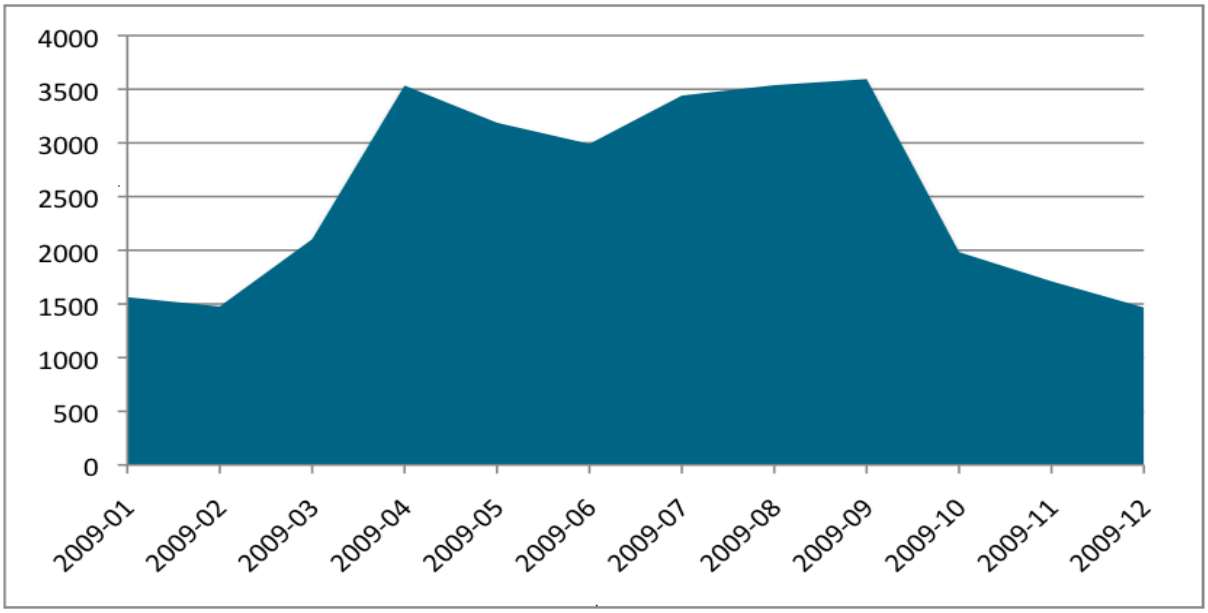
de benyttes også for innsamling av annen informasjon som kan tenkes å ha verdi for de som står bak operasjonen. Antivirusdeteksjon for slike trojanere er vanskelig. Dette oppnås ved å distribuere koden i relativt lavt antall for å unngå at den skal fanges opp og analyseres. Trojaneren er i stand til å forsere sikkerhetstiltak som brukernavn, passord, PIN-koder og to-faktor autentisering. I USA er det kjent at disse trojanerne har blitt benyttet i omfattende svindel av banksektoren.

Omfanget av Zeus-infiserte maskiner i Norge er ukjent. NSM har observert trafikk mot IP-adresser som er kjent som ufrivillige kommando- og kontrolltjenere i Zeusnettverk, men IP-adressene benyttes også til legitime tjenester.

4.4 Conficker

Confickerormen som begynte å spre seg i 2008 og som fikk mye omtale i løpet av 2009, fikk betydelige konsekvenser for enkelte organisasjoner i Norge. Sikkerhetsoppdateringen for denne sårbarheten ble publisert av Microsoft 23. oktober 2008. Likevel fikk ormen stor utbredelse, blant annet fordi sikkerhetsoppdateringen ikke hadde blitt installert på samtlige maskiner.

Conficker har også utnyttet flyttbare lagringsenheter (eksempelvis minnepinner) for spredning. Det var en markant økning i trafikk generert av Conficker fra november 2008 til mars 2009. Noe av trafikken kan sannsynligvis tilskrives annen programkode som forsøkte å utnytte den samme sårbarheten. Det vises forøvrig til rapport om Conficker publisert på NSMs hjemmesider[4]. Conficker er fremdeles aktiv og spres fortsatt i stort omfang.



Figur 2: Antall kompromitterte maskiner for hver måned i 2009 (Conficker)

[3] Zeus/ Opachki http://www.secureworks.com/research/threats/opachki/
[4] Rapport om Conficker publisert på NSMs hjemmesider: https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Forsideartikler-NorCERT/Conficker-spesialrapport/

4.5 Andre sikkerhetsutfordringer

NSM har tidligere beskrevet utfordringene rundt internasjonale tjenesteleverandører som garanterer for at sider i deres nettverk ikke skal tas ned, selv om de mottar henvendelser om å gjøre dette fra sikkerhetsselskaper og myndigheter. Tilsvarende utfordringer forekommer også til en viss grad i Norge.

I løpet av året har det blitt observert flere tilfeller av at sårbarheter i dataprogrammer har blitt utnyttet i begrensede, målrettede angrep før sikkerhetsoppdateringer har vært tilgjengelig. Disse angrepene er det svært vanskelig å beskytte seg mot.

Majoriteten av alle cyberangrep går mot sårbarheter hvor det finnes sikkerhetsoppdateringer og andre sikkerhetstiltak. Likevel observeres det at mange mindre sofistikerte angrep er vellykkede. Det er urovekkende. Sikkerhetsbarrierene er ofte unødvendig lave. Det finnes store mangler i forhold til vedlikehold og oppdatering av sårbare systemer.

Ondsinnede aktører viser fortsatt stor interesse for å knytte infiserte PC-er sammen i nettverk[5] for å utnytte datakraft. Slik datakraft kan utnyttes for målrettede angrep mot samfunnskritiske IKT-systemer. PC-er med svak sikkerhet er særlig utsatt for å bli utnyttet. På denne måten kan sikkerhetsnivået til den enkeltes private hjemme-PC være av betydning for samfunnssikkerheten.

NSM ser en mulighet for at spredning av ondsinnet kode via mobiltelefon kan komme til å bli en betydelig utfordring. Den første uønskede programvarekoden som ble distribuert via SMS (Short Message Service)[6] ble observert i begynnelsen av 2009. For NSM kan det synes som det er lav bevissthet om sårbarheter og trusler knyttet til bruk av mobiltelefoner. Det er en kjent sak at mobiltelefoner kan spores og samtaler kan avleses, også på avstand.

5 Tiltak for å bedre sikkerhetstilstanden

5.1 NSMs reaksjonsformer

Gjennom tilsyn avdekker NSM brudd på lovpålagte krav til sikring av sikkerhetsgradert informasjon. Tilsynsrapportene, og medfølgende pålegg, er utformet slik at tilsynsobjektene skal være i stand til å korrigere underliggende forhold, for dermed å hindre at avvikene gjentar seg. Tilsynsrapportene omhandler forbedringspunkter og er ment som bidrag til virksomhetens kontinuerlige arbeid med å videreutvikle og forbedre den forebyggende sikkerhetstjenesten.

Pålegg om utbedring av sikkerhetstilstanden gis i hovedsak som krav om korrigering av de avvik som er avdekket. Ved alvorlige forhold er det aktuelt å kreve at tilsynsobjektet redegjør for de tiltak som iverksettes, både umiddelbart og som permanent korrigering. Ved særlig alvorlige avvik er det aktuelt å gi pålegg om stans i aktuelle deler av informasjonsbehandlingen. Ved alvorlige sikkerhetsbrudd kan det også være nødvendig å anbefale etterforskning av brudd på sikkerhetsloven

Eventuelle reaksjoner vurderes i det enkelte tilfellet. Det kan foretas oppfølgende tilsyn mellom trinnene i eskaleringen.

---

[5] Botnets, ”robot networks”, av infiserte datamaskiner som kontrolleres av ondsinnet aktør uten at eierne vet om det
[6] Short Message Service benyttes til oversendelse av tekst mellom mobiltelefoner

5.2 Andre mulige virkemidler

- Gi informasjon for å motivere til arbeid med forebyggende sikkerhet.
- Være tilgjengelig for veiledning med hensyn til etterlevelse av sikkerhetsloven.
- Utarbeide brukerrettede skriftlige veiledninger.
- Ta initiativ til og bidra til revisjon av regelverk.
- Ta initiativ til og bidra til utvikling av tekniske løsninger.
- Varsel og underretning til overordnet myndighet

6 Konklusjon om sikkerhetstilstanden

Norge er i dag et sårbart samfunn. Mye informasjon ligger offentlig tilgjengelig. I henhold til Politiets sikkerhetstjenestes (PSTs) åpne trusselvurderinger er etterretningsaktiviteten mot norske interesser høy. NSM har erfart et stadig økende antall saker med forsøk på målrettet dataspionasje. Den økende forekomsten av målrettede trojanere og annen ondsinnet programvare gir grunn til bekymring. Denne trusselen er dynamisk og utvikler seg raskt. Det synes derfor som om risiko i forbindelse med behandling av informasjon på IKT-systemer er økende. I dette bildet blir det spesielt viktig å redusere sårbarhetene gjennom et godt forebyggende defensivt sikkerhetsarbeid.

Som hovedregel er sikkerhetsarbeidet relativt statisk. Det er oftest et stort forbedringspotensial. NSM har i tidligere rapportering beskrevet en bekymring for et økende gap mellom et dynamisk risikobilde og et stillestående sikkerhetsarbeid. Det er grunn til å gjenta denne bekymringen.

Det er et behov for å sette sterkt fokus på årsaker til at sikkerhetsarbeidet ikke prioriteres godt nok. Det må særlig tas tak i manglende lederengasjement og manglende organisering og eventuelle bakenforliggende årsaker til dette. Forebyggende sikkerhetsarbeid i alle sektorer må prioriteres av ledelsen. Det betyr at det må settes av både tid og ressurser til å styrke dette arbeidet.

Det er NSMs overordnede vurdering at svakheter ved sikkerhetstilstanden og mangler ved den forebyggende sikkerhetstjenesten skyldes at virksomhetsledelsen i utilstrekkelig grad ivaretar sin rolle i sikkerhetsarbeidet.

God sikkerhet oppnås gjennom aktiv, engasjert og ansvarlig sikkerhetsledelse.