Nasjonal sikkerhetsmyndighet

Versjonsnr.:1.0 (21.desember 2009)

Nasjonal strategi for cybersikkerhet

Forebygging og håndtering av IKT-hendelser med store samfunnsmessige skadefølger

Dato	Versjon	Endringer	Godkjent av
2009-12-21	1.0		Dir NSM

Sammendrag

Avhengigheten av IKT og internett er i dag blitt en strategisk sikkerhetsutfordring. Både Forsvaret, sivile myndigheter og store norske bedrifter med kritiske samfunnsfunksjoner er avhengig av IKT for å levere tjenestene de skal. Samlet sett har dette har gjort samfunnet mer sårbart.

Elektronisk informasjonsuthenting blir benyttet til spionasje både mot stater, mot militære styrker, og mot private selskaper. Angrep på IKT-systemer blir benyttet i konfliktsituasjoner og er en del av moderne krigføring. Angrep over nett kan lamme strømforsyning, industriprosesser og andre samfunnskritiske funksjoner. Kriminaliteten på internett er i sterk vekst. I Norge har både Forsvaret, store virksomheter, tjenesteleverandører og toppledere i offentlig og privat sektor blitt utsatt for alvorlige IKT-hendelser.

Cybersikkerhet er et tema internasjonalt. NATO ser på truslene mot IKT-systemer med økende bekymring. NATOs parlamentarikerforsamling fremholder at cyberangrep sammen med terrorisme og spredning av kjernevåpen nå er en av de mest alvorlige asymmetriske truslene alliansen og medlemsstatene står overfor. En rapport fra Det hvite hus om cybersikkerhet slår fast at cybersikkerhet utgjør en av de mest alvorlige økonomiske og nasjonale sikkerhetsutfordringer nasjonen står overfor i det 21. århundre.

Denne **nasjonale strategien for cybersikkerhet** trekker opp hovedlinjene for videreutvikling av nødvendige samordnende og sektorovergripende tiltak for helhetlig beskyttelse av kritiske IKT-systemer mot alvorlige IKT-hendelser. Med helhetlig beskyttelse menes så vel forebygging som effektiv håndtering av hendelser.

Dette er status i Norge i dag:

- Vi har ikke tilstrekkelig situasjonsoversikt og forståelse. Det foreligger flere utredninger knyttet til behov og metodikk for å identifisere kritiske IKT-systemer, også på tvers av samfunnssektorer. Disse er imidlertid ikke operasjonalisert og implementert.
- Det er uklart i hvilken grad samtlige kritiske IKT-systemer er underlagt spesifikke krav til sikkerhet med tilhørende tilsyns- og kontrollregimer.
- Det er manglende bevissthet i organisasjoner om hvordan organisasjonskultur og sikkerhetskultur påvirker holdninger, atferd og bruk av IKT-systemer.
- Evnen til å oppdage, varsle om og håndtere IKT-hendelser er sterkt varierende.
- Etterforskning av datakriminalitet er svært krevende. Det er store utfordringer knyttet til å identifisere og ansvarliggjøre gjerningspersoner.

I strategien blir det foreslått 22 tiltak for å styrke Norges evne til å forebygge og håndtere alvorlige IKT-hendelser. Strategiens hovedmål er å:

- Etablere en felles situasjonsoversikt og forståelse
- Bygge og opprettholde robuste og sikre IKT-systemer
- Bevisstgjøre, opplyse og påvirke
- Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser
- Bekjempe og etterforske IKT-hendelser
- Styrke samordningen av cybersikkerhetsarbeidet

Innhold

1. Bakgrunn

1.1 Hvorfor trenger vi en strategi?

Samfunnets økende avhengighet av IKT-systemer sammenholdt med et dynamisk IKT-risikobilde, krever en målrettet satsning også i Norge for å motstå alvorlige angrep. Virksomhetene selv og sektormyndigheter har primæroppgaven for den defensive beskyttelsen. De mest alvorlige hendelsene må møtes med en mer samordnet og sektorovergripende tilnærming, som ser defensive og offensive tiltak i sammenheng.

Vi lever i et nettverksbasert samfunn. De fleste sektorer i samfunnet er avhengig av datanettverk for å fungere. Små forstyrrelser i nettverkene kan få store konsekvenser. Sektorene er i tillegg blitt gjensidig avhengig av hverandre. Hendelser i én sektor kan dermed få store konsekvenser for andre. Avhengigheten går også over landegrenser. Det innebærer at hendelser i Norge kan få konsekvenser for andre land, og omvendt.

Skade kan inntreffe som følge av teknisk og menneskelig svikt, eller som et resultat av andre mer tilfeldige hendelser. Skade kan også oppstå om ondsinnede aktører ønsker å ramme oss gjennom å angripe eller skaffe seg tilgang til IKT-systemer, og særlig om disse aktørene har høy kompetanse og kapasitet. Om slike angrep eller hendelser får kritiske samfunnsfunksjoner til å bryte sammen for en lengre periode, eksempelvis ved at strømforsyningen blokkeres, at Forsvarets systemer skades, eller ved at det oppstår avbrudd i det finansielle systemet[1] kan konsekvensene bli store. Det er også svært skadelig at ondsinnede aktører ved å utnytte svakheter i IKT-systemene får tilgang til informasjon som av nasjonale grunner vurderes som sensitiv.

Virksomhetene gjør i dag mye godt arbeid for å sikre egne IKT-systemer, gjerne etter pålegg fra sektormyndigheter og iht. sektorregelverk, eller basert på en sektorovergripende tilnærming[2]. Hendelser som skyldes ondsinnede aktører er imidlertid utfordrende å beskytte seg mot, spesielt om trusselaktøren har høy kompetanse og store resurser. Trusselaktiviteten fra slike aktører må forventes å være utformet for å unngå å bli oppdaget, eller for på annen måte å tilstrebe maksimal effekt. At informasjonen som genereres, lagres eller kommuniseres i IKT-systemer har vært gjenstand for spionasjeforsøk har vært kjent lenge. Internasjonalt ser vi imidlertid at IKT-systemer nå også angripes eller utnyttes ved konflikter og at dette kan få store konsekvenser. Hendelser i forbindelse med urolighetene i Estland i 2007 var med å sette informasjonssikkerhet på den sikkerhetspolitiske dagsorden, likeså Georgia og Gaza i 2008 og valget i Iran i 2009[3]. Angrep på IKT-systemer vil høyst sannsynlig være et element i enhver sikkerhetspolitisk konflikt fremover. Informasjonssikkerhet er blitt en strategisk sikkerhetsutfordring.

Øvelseserfaringer nasjonalt og internasjonalt de siste årene viser at vi og andre vestlige land fortsatt har utfordringer med å håndtere alvorlige IKT-hendelser. Det er i den forbindelse særlig krevende å ha god situasjonsforståelse ved hendelser som rammer bredt, men også å oppnå en tilstrekkelig samordnet håndtering. Øvelsene har bidratt til å synliggjøre behovet for bedre tverrsektoriell koordinering, informasjonsdeling og tydeliggjøring av roller og ansvar[4].

Den teknologiske utvikling gir betydelige utfordringer i forhold til å ha tilstrekkelig sikring av IKT-systemer mot alvorlige hendelser. Utfordringene er knyttet både til menneskelige, prosedyremessige og teknologiske sårbarheter. Men juridiske aspekter (hva som er legalt) og policyavklaring (hva som er ønsket praksis) må ivaretas. Sikkerhetstiltakene skal beskytte, ikke utfordre, grunnleggende rettigheter. Ved regelverksutvikling må følgelig rettssikkerhet og personvern veie tungt.

[1] Beskyttelse av samfunnet 5 (BAS5) gikk inn på IKT-infrastrukturens betydning for de forskjellige samfunnsfunksjoner (”Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport)
[2] For en overordnet gjennomgang av eksisterende relevante etaters og virksomheters roller, ansvar og myndighet vises til vedlegg A til denne strategien.
[3] Se nærmere omtale av disse sakene i kap. 1.4.
[4] Sivil nasjonal øvelse (SNØ) 2008, øvelse IKT-08, Overordnet evaluering (offentlig utgave)

På den annen side er beskyttelse av kritiske IKT-systemer avgjørende for samfunnets funksjonsdyktighet, enten det dreier seg om å opprettholde sentrale samfunnsfunksjoner, videreutvikle velferd og trygghet for den enkelte eller legge til rette for næringsutvikling. Under sikkerhetspolitiske kriser og i væpnet konflikt vil enkelte av systemene også kunne være avgjørende for å trygge demokratiet og vår nasjonale handlefrihet og i ytterste konsekvens sikre vår selvstendighet overfor andre stater[5].

Det bør legges en betydelig innsats i å forebygge og motvirke alvorlige IKT-hendelser. Når de likevel skjer må skaden begrenses og skadefølgene håndteres på en mest mulig effektiv måte.

Kort om strategien og enkelte kjernebegreper:

Den **nasjonale strategien for cybersikkerhet** trekker opp hovedlinjene for videreutvikling av nødvendige samordnende og sektorovergripende tiltak for helhetlig beskyttelse av kritiske IKT-systemer mot alvorlige hendelser. Strategien vil måtte følges opp med mer detaljerte handlingsplaner. Det vil i den forbindelse være nødvendig å identifisere og involvere aktuelle interessenter - både private og offentlige aktører - som utvikler, regulerer, drifter, eier eller er brukere av kritiske IKT-systemer.

Begrepet **cybersikkerhet** representerer i denne strategien en videreutvikling av informasjonssikkerhetsbegrepet, og gjenspeiler samfunnets stadig økende avhengighet av IKT-systemer bundet sammen i cyberspace[6].

Med **helhetlig beskyttelse** menes så vel forebygging som effektiv håndtering av hendelser.

Med **kritiske IKT-systemer** menes systemer som kritiske samfunnsfunksjoner er avhengig av. Dette kan være så vel informasjons- som kommunikasjons- og styringssystemer. Systemene omfatter infrastruktur, programvare og informasjonsinnhold. Systemene kan være åpne eller lukkede/graderte.

Med **alvorlige IKT-hendelser** menes generelt at disse kan få store samfunnsmessige skadefølger. IKT-hendelser er i denne sammenheng bredt definert, og inkluderer også påkjenninger over tid[7]. Fokuset i denne strategien er å motvirke uønskede villede handlinger, men strategien vil også langt på vei bidra til å redusere og håndtere konsekvenser av mer tilfeldige påkjenninger som naturskade (lynnedslag, jordskjelv, flom, etc.), teknisk og menneskelig svikt eller uhell. Uønskede, villede handlinger vil som oftest ha et eller flere av følgende kjennetegn: kraftfulle, fordekte, målrettede, koordinerte eller indirekte.

Det finnes ulike **trusselaktører** med forskjellig grad av ressurser og kompetanse.
Denne strategien tar høyde for trusler fra andre staters spesialorganer som kan tenkes involvert i såkalte statsdrevne informasjonsoperasjoner, herunder etterretningsinnhenting, sabotasjeforberedelser, psykologiske operasjoner eller fysisk ødeleggelse. Tiltak innrettet mot slike trusselaktører vil også bidra til effektivt å forebygge og håndtere ondsinnet aktivitet fra aktører med mindre kompetanse og ressurser.

[5] NOU 2006:6 Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner

[6] Cyberspace er etter hvert blitt et allment kjent begrep. Wikipedia beskriver cyberspace som "*the interdependent network of information technology infrastructures (ITI), telecommunications networks—such as the internet, computer systems, integrated sensors, system control networks and embedded processors and controllers common to global control and communications"*

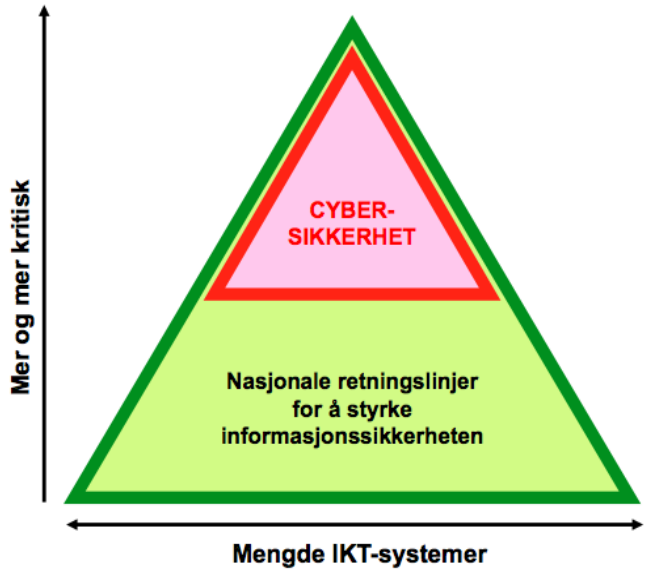
[7] Eksempelvis favner definisjonen av hendelser vedvarende informasjonsinnhenting, inntrenging og infiltrasjon av datasystemer.

1.2 Forholdet til Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010

Den nasjonale strategien for cybersikkerhet konkretiserer og utdyper de nasjonale retningslinjene for informasjonssikkerhet, når det dreier seg om beskyttelse av de mest samfunnskritiske systemer. Strategien bringer i tillegg inn et aktørfokus.

Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010, utgitt i desmeber 2007, ble utarbeidet i et samarbeid mellom Fornyings- og administrasjonsdepartementet (FAD), Samferdselsdepartementet (SD), Forsvarsdepartementet (FD) og Justisdepartementet (JD)[8]. Retningslinjene har et bredt formål og fokuserer på innsatsområder for beskyttelse av informasjonssikkerheten i samfunnet i stort, herunder beskyttelse av kritiske IKT-systemer. Hovedtyngden av innsatsområdene som trekkes opp vil først og fremst bidra til den generelle grunnsikring i hele samfunnet. Den nasjonale strategien for cybersikkerhet bygger videre på dette fundamentet, men retter seg mot forebygging og håndtering av de mest alvorlige typer av IKT-hendelser som beskrevet ovenfor. Det betyr at tiltakene konkretiserer og utdyper retningslinjene. Mange av de samme temaer gjenfinnes i så vel denne strategien som retningslinjene, men følgelig med noe forskjellig betoning når det gjelder tiltak.

Figuren under illustrerer hvordan den nasjonale strategien for cybersikkerhet utdyper de nasjonale retningslinjene:



I tillegg til den defensive beskyttelsen i form av forebygging og håndtering inneholder strategien også offensive aktørfokuserte tiltak. Dette representerer en metodisk utvidelse i forhold til de eksisterende retningslinjene.

[8] En arbeidsgruppe under KIS utarbeidet et utkast til departementene. Retningslinjene bygget på "Nasjonal strategi for informasjonssikkerhet (2003)".

1.3 Internasjonale tilnærminger til cybersikkerhet

Internasjonalt er cybersikkerhet (Cyber Defence, Cyber Security osv.) et område som av mange land og internasjonale organisasjoner fremheves som stadig mer viktig for samfunnssikkerheten og den nasjonale sikkerhet. Mange land er i ferd med å utarbeide strategier for cybersikkerhet av hensyn til samfunnets og den nasjonale sikkerhet. De enkelte lands forpliktelser overfor fellesskap og allianser understrekes mer og mer

I **FN** har cybersikkerhet vært diskutert, men dette har så langt ikke resultert i konkrete tiltak[9]. FN-organet ITU (International Telecommunication Union) lanserte imidlertid i 2007 en *Global Cyber Security Agenda,* som har til hensikt å danne et rammeverk for koordinering av tiltak knyttet til cybersikkerhet. Fokuset i rammeverket er å bygge partnerskap og samarbeid mellom alle relevante parter for å møte cybertruslene[10].

Europarådets datakrimkonvensjon (Cyber crime convention) er foreløpig det eneste bindende internasjonale tiltak som eksisterer mot datakriminalitet. Konvensjonen er nå ratifisert i 26 land, og ytterligere 20 har signert[11]. Norge undertegnet konvensjonen i 2001, og regjeringen nedsatte som følge av dette Datakrimutvalget. Utvalget konkluderte med at det ikke var nødvendig med endringer i norsk rett for å oppfylle konvensjonens krav. Det er fortsatt en utfordring internasjonalt at få stater har ratifisert, eller at den ikke er implementert fullt ut.

I **EU** eksisterer det flere ulike program og tiltak for informasjonssikkerhet, blant dem EPCIP-direktivet[12] fra 2008 og en *communication* for beskyttelse av Europa mot storskala cyberangrep og sammenbrudd som ble lansert i 2009[13]. EPCIP-direktivet omfatter beskyttelse av både tilsiktede og utilsiktede uønskede hendelser, men trusselen fra terrorangrep har en uttrykt prioritet. Direktivet utgjør det første steget i en trinnvis tilnærming til å identifisere og utpeke kritisk europeisk infrastruktur. Direktivet konsentrerer seg i første rekke om energi- og transportsektorene, men det er forutsatt at EU tar sikte på å innta IKT-sektoren i direktivet på et senere tidspunkt[14].

NATO på sin side har som følge av Estland-saken i 2007 satt Cyber Defence på dagsorden. 20. desember 2007 vedtok alliansen en politikk for dette området, NATO Policy on Cyber Defence[15]. Norge har gjennom dette policydokumentet en rekke forpliktelser overfor alliansen, herunder å sørge for tilstrekkelig beskyttelse av infrastruktur for NATO-systemer på norsk jord, systemkoblingene mellom NATO-systemer og nasjonale systemer, og nasjonale systemer som inngår i krisehåndtering eller systemer som opprettholder kritiske samfunnsfunksjoner. NATOs policy stiller også krav til sikring av sivile infrastrukturer. NATO ser på truslene på nett med økende bekymring. NATOs parlamentarikerforsamling har fremstilt cyberangrep, sammen med terrorisme og spredning av kjernevåpen, som en av de mest alvorlige truslene alliansen og medlemsstatene står overfor[16].

Også i de enkeltes sektormyndigheters dialog med tilsvarende organer i andre land har informasjonssikkerhet og IKT-sikkerhet en fremtredende plass. Særlig gjelder dette der samarbeidsrelasjonene er tette fra før. Et eksempel på slike diskusjoner er de som finanssektoren fører internasjonalt innen rammen av FI-ISAC[17].

Den internasjonale debatten dreier seg – i tillegg til å omtale IKT-risikobildet og utveksle informasjon om praksis for beskyttelse i det enkelte land – om å forsøke å besvare en rekke spørsmål, som blant annet:

---

[9] "NATO and Cyber Defence" (173 DSCFC 09 E bis), rapport til NATOs parlamentarikerforsamling 2009.
[10] "Global Cyber Security Agenda (GCA) – A framework for international cooperation."
[11] Informasjon gitt på Cyber Conflict Legal and Policy Conference, Tallinn, september 2009.
[12] Council Directive 2008/114/EF. EPCIP = European Programme for Critical Infrastructure Protection.
[13] "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009)149).
[14] Hentet fra omtalen av EPCIP-direktivet på Europaportalen (Regjeringen.no)
[15] C-M(2007) – NATO Policy on Cyber Defence (NATO Restricted)
[16] "NATO and Cyber Defence" (173 DSCFC 09 E bis), rapport til NATOs parlamentarikerforsamling 2009.
[17] FI-ISAC = Financial Information Sharing and Analysis Center (www.fi-isac.org)

- Hva er cyberspace, og hvordan skal det sikres?
- Hva er et angrep?
- Hvordan skal man fastslå hvor angrep kommer fra? Hvilke krav skal man ha til bevis i denne sammenheng?
- Hvilket ansvar ligger på statene i forhold til angrep/hendelser som har sitt utspring i deres land?
- Hvordan legge til rette for effektiv etterforsking og håndtering av hendelser som krysser flere landegrenser?
- Hvilket ansvar ligger på statene i forhold til egne offensive kapasiteter?

Dette er diskusjoner av strategisk karakter. Mye arbeid gjenstår når det gjelder internasjonalt samarbeid innen utvikling av regelverk, operativt samarbeid og harmonisering av begreper og tilnærminger.

Mange land med høy grad av IKT-bruk har utarbeidet, eller er i ferd med å utarbeide strategier for cybersikkerhet, men ansvarsforhold og de rettslige rammer knyttet til cybersikkerhetsarbeidet er uavklarte – også internasjonalt. Noen fellesnevnere fra de ulike lands strategier innebærer å finne metoder for å utnytte cyberspace bedre – og samtidig beskytte seg mot potensielle motstandere. Samarbeid mellom private og offentlige myndigheter fremheves som en kritisk suksessfaktor. Det samme gjelder internasjonalt samarbeid – blant annet i forhold til regelverksutvikling og hendelseshåndtering. Både USAs og Storbritannias strategier fremhever at sterk koordinering er essensielt, og at det er viktig med plassering av et tydelig ansvar for oppfølging av strategier og tiltak innenfor cybersikkerhet.

Styrker datasikkerheten i Storbritannia
Britiske myndigheter gikk i år inn for å styrke datasikkerheten gjennom en egen cybersikkerhetsstrategi. Blant tiltakene er å etablere et sektorovergripende program for å nå prioriterte områder i strategien, etablere et strategisk senter for cybersikkerhet og opprette et eget operasjonssenter.
(Kilde: Cyber Security Strategy of the United Kingdom; safety, security and resilience in cyber space)

Styrker datasikkerheten i USA
Cybersikkerhetsarbeidet blir styrket i USA. Gjennom rapporten White House Cyberspace Policy Review blir det foreslått en rekke tiltak. Blant tiltakene er å utnevne en egen embedsmann for cybersikkerhet i Det hvite hus, etablere et eget koordinerende direktorat under National Security Council, og forberede en nasjonal strategi for å sikre IKT-infrastrukturen. Cybersikkerhet utgjør en av de mest alvorlige økonomiske og nasjonale sikkerhetsutfordringer nasjonen står overfor i det 21. århundre, slår rapporten fast.
(Kilde: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)

Vil styrke cybersikkerheten i Sverige
Ansvarsfordelingen og organiseringen av samfunnets informasjonssikkerhet skal utredes i Sverige. Formålet med utredningen er å skape bedre forutsetninger for å forebygge og håndtere IT-hendelser. Det er den svenske regjeringen som har bestilt utredningen.
(Kilde: Pressemelding fra det svenske forsvarsdepartementet 19. 11.2009)

Australia oppretter eget cybersenter
Australia oppretter to nye organisasjoner for å styrke datasikkerheten. Et eget Computer Incident Response Team og et Cyber Security Operations Centre skal bidra til å stå bedre rustet mot dataangrep. Australias nasjonale sikkerhet, økonomiske fremgang og sosiale velferd er kritisk avhengig av tilgjengelighet, integritet og konfidensialitet i en rekke informasjons- og kommunikasjonsteknologier, står det i Australias cybersikkerhetsstrategi. (Kilde: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy)

1.4 Kort om IKT-risikobildet

Trusselnivået i cyberspace øker. Spionasje og organisert kriminalitet er blant de viktigste truslene. Mange stater bygger opp evnen til etterretning og angrep på nett. Samtidig kommer det til nye sårbarheter – særlig tekniske – som trusselaktører utnytter før gode sikkerhetstiltak er utviklet og implementert.

IKT-risikobildet består av tre elementer; IKT-trusler, sårbarheter og verdien av det som ønskes beskyttet. Det siste elementet drøftes ikke nærmere, utover generelle betraktninger om IKT-systemenes samfunnsmessige betydning i kap. 1.1 ovenfor.

IKT-trusler

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

Med **IKT-trusselbildet**[18] 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.

EOS-tjenestene[19] mener at trusselnivået knyttet til IKT-baserte virkemidler har økt de siste årene. Mange stater bygger opp etterretnings- og angrepsevne til bruk i cyberspace. Nasjonale operative erfaringer viser at det oppdages et økende antall aktiviteter og operasjoner med høy alvorlighetsgrad. Erfaringer fra NorCERT viser at disse er mer og mer alvorlige og vanskeligere å håndtere[20]. Spesielt er antall alvorlige målrettede forsøk på spionasje, både mot offentlige og private virksomheter, økt kraftig de siste årene. Ut fra disse erfaringene er det grunn til å fremheve etterretning og organisert kriminalitet som de viktigste truslene i Norge i dag[21]. I situasjoner med økt spenning og konflikt må det også forventes forsøk på sabotasjeanslag. Forberedelser til slike kan imidlertid ikke utelukkes alt i fredstid.

Etterretningsvirksomhet mot Norge og norske interesser

Flere sektorer innenfor det norske samfunnet er attraktive etterretningsmål, og aktiviteten til utenlandske staters etterretningstjenester mot Norge og norske interesser er høy. Etterretningsvirksomheten er i hovedsak rettet mot politiske beslutningstakere, embetsverk, sentraladministrasjon og ulike private aktører. Informasjonen søkes særlig innenfor olje og gass, forskning og utvikling, teknologi samt forhold knyttet til NATO.
(Kilde: PST's åpne trusselvurdering 2009).

IKT-trusselbildet er komplekst og dynamisk[22]. Det kan være vanskelig å skille typer av trusselaktivitet og ikke minst aktører fra hverandre i et bilde som omfatter alt fra såkalte "script kiddies" (ungdom som er fortrolig med dataverktøy og som tar i bruk tilgjengelige programmer uten å tenke over konsekvensene) til hacktivister (aktivister som gjennomfører ulovlige demonstrasjoner i cyberspace) som organiserte kriminelle og representanter for stater involvert i informasjonsoperasjoner.

[18] Disse definisjonene er utarbeidet av Koordineringsgruppen for IKT-trusselbildet, se vedlegg A.
[19] Etterretningstjenesten, Politiets Sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet, se vedlegg A
[20] Det er stor forskjell på ressursbruken knyttet til håndtering av de ulike hendelsene, fra noen minutter til flere årsverk.
[21] For en mer utfyllende beskrivelse av IKT-risikobildet henvises det til Bakgrunnsstudien (under utarbeidelse mellom EOS-tjenestene)
[22] Risikobildet oppdateres jevnlig og er tilgjengelig på NSMs nettsider

Det er viktig å understreke at statsdrevede informasjonsoperasjoner opererer i hele konfliktspennet, også i fredstid, og utgjør trolig den mest alvorlige formen for anslag mot kritiske IKT-systemer.

Internasjonal erfaring viser at de som blir utsatt for spionasje gjennom IKT-systemer typisk vil være virksomheter i statsadministrasjonen, høyteknologisk industri, herunder innen elektronikk, forsvar og petrokjemi, menneskerettighetsorganisasjoner og andre som besitter særlig personsensitiv informasjon[23]. Som regel er det ledere eller spesialister, på ulike nivåer, som gjennom sosial manipulering, blir lurt til å åpne e-post vedlegg som inneholder trojanere[24], som er skreddersydd for å stjele informasjon fra virksomhetens eller den enkeltes datasystemer.

Internasjonalt blir en rekke alvorlige IKT-hendelser satt i en sikkerhetspolitisk kontekst. Fra andre land har man eksempler på at det kan være motsetninger mellom personer, politiske partier eller etter omstendighetene endog stater som gjør at noen ønsker å svekke motparten gjennom å utføre IKT-angrep. Angrepene oppstår ofte i parallell med og forsterker tradisjonelle demonstrasjoner og protestaksjoner som skjer på gateplan. En av de mest omtalte hendelsene er den ovenfor omtalte Estland-saken i 2007, der en rekke samfunnsviktige funksjoner ble satt ut av spill som følge av tjenestenektangrep[25]. Hendelsene oppsto i kjølvannet av omfattende demonstrasjoner i gatene i Tallinn, etter at estiske myndigheter fjernet et eldre russisk krigsmonument fra sentrum i byen. Det er registrert alvorlige IKT-hendelser i forbindelse med de fleste internasjonale sikkerhetspolitiske konflikter etter dette (Gaza-konflikten i 2008, Georgia-krigen i 2008, valget i Iran i 2009, m.fl).

Økonomisk IKT-kriminalitet øker kraftig[26]. Mange nye angrepsmetoder er utviklet for å gjennomføre avansert økonomisk svindel. Det er gjerne organiserte kriminelle grupperinger med store ressurser som står bak, og de anvender personer og miljøer med god kompetanse på å utvikle ondsinnet programvare. Tyveri av identiteter, tyveri og misbruk av kredittkortnummer og nettbanksvindel er noen av områdene som har hatt stor vekst.

[23] NSMs sikkerhetsvarsel 2008 nr. 1 Om målrettede trojanere i Norge
[24] En trojansk hest eller trojaner er en type dataprogram som utgir seg for å være nyttig, men som i virkeligheten er skadelig. Det er en type ondsinnet kode som krever at mottageren på en eller annen måte starter programmet, ofte ved at trojaneren gjemmer seg inne i et annet program.
[25] I et tjenestenektsangrep (DoS) forsøker en angriper å hindre legitime brukere i å få tilgang til en tjeneste eller informasjon. Ved å angripe din maskin, eller maskiner på nettstedet du forsøker å bruke, kan en angriper hindre at du får tilgang til e-post, nettsteder, nettbanken din, osv.
[26] Internet Crime Complaint Center (IC3), FBI rapport publisert 9.mars 2009.

Sårbarheter

Med **sårbarhet** menes tekniske, administrative og menneskelige svakheter som kan utnyttes målrettet eller mer tilfeldig for å ramme IKT-systemer. Det motsatte av sårbarhet er robusthet.

Det eksisterer mange tekniske sårbarheter i IKT-systemer som blir utnyttet av trusselaktører. Mange sårbarheter skyldes krav til brukervennlighet og funksjonalitet som ofte går utover sikkerheten. I tillegg bidrar sammenkobling av datasystemer til nye sårbarheter og avhengigheter. Tekniske sårbarheter finnes i alle typer programvare (applikasjoner) og operativsystemer. Internasjonalt rapporteres følgende fire punkter som de mest aktuelle tekniske sårbarheter i 2009[27]

- Sårbarheter i utbredt programvare som for eksempel Office pakken, Adobe PDF Reader og Flash utnyttes fortsatt av trusselaktører, ved at brukerens egen datamaskin ikke er tilstrekkelig sikret. Det er som regel manglende rutiner for oppdatering av programvaren som muliggjør dette. Brukerens datamaskin blir så brukt til å spre ondsinnet kode videre i virksomhetens nettverk.
- Svakheter i nettsider blir utnyttet slik at disse begynner å spre ondsinnet kode til de som oppsøker nettsiden. Selv om antallet hendelser av denne typen er stort og har fått mediaoppmerksomhet, er det fortsatt mange nettsteder som utnyttes og misbrukes av trusselaktører som ønsker å spre ondsinnet kode.
- Operativsystemer synes å bli mer robuste, og ormer[28] som utnytter sårbarheter i operativsystemer opptrer sjeldnere. I 2009 har likevel Conficker ormen fått store konsekvenser for flere store virksomheter[29].
- Antallet zero-day[30] sårbarheter har økt. Noen av disse er ikke rettet opp (patchet) på to år. I kombinasjon med for lite tilgjengelig relevant kompetanse hos både leverandører og brukere av IKT-systemer, blir det vanskelig å beskytte seg mot slike sårbarheter.

Tekniske sårbarheter forsterkes som følge av for svake administrative rutiner og menneskelig adferd. God sikkerhetsstyring og kontrollrutiner vil derfor være avgjørende. Et godt eksempel er bruken av minnepinner, som er lette å miste, enkle å stjele og kan spre virus. Samme minnepinne brukes altfor ofte ukritisk i åpne og lukkede datanettverk, og forbigår på denne måten tekniske sikkerhetstiltak. På tross av strenge administrative rutiner har denne sårbarheten vist seg vanskelig å redusere. Andre eksempler på utfordringer knyttet til manglende sikkerhetsbevissthet er ukritisk bruk av e-post og dårlig passordbeskyttelse.

Systematisk svikt i gjennomføringen av sikkerhetstiltak representerer en stor sårbarhet. Tilsynserfaringer med etterlevelsen av sikkerhetsloven viser eksempelvis at det er en del gjengangere i forhold til manglede gjennomføring av tiltak[31]. Enkelte av disse skyldes at tiltakene kan være krevende å implementere, men mange kan tilskrives manglende prioritering av sikkerhetshensyn – altså sviktende ledelsesfokus – i virksomheten. Gjennom samtaler med ledere og sikkerhetspersonell synes det klart at risikoforståelsen er nokså svak og tilfeldig. Det bedømmes at dette også er medvirkende årsak til svak etterlevelse. Et eksempel på slik systematisk svikt er den svake ivaretakelsen av sikkerheten i forbindelse med omorganiseringer og flytteprosesser.

[27] SANS The Top Cyber Security Risks September 2009
[28] En orm er et dataprogram som sprer seg automatisk over et datanettverk. Noen ormer er laget for å utføre oppgaver som å stjele passord eller legge inn en bakdør på datamaskinen.
[29] Helse Vest og Politiets data- og materielltjeneste (PDMT) er eksempler på virksomheter som har hatt utbrudd av denne ormen i 2009.
[30] En zero-day sårbarhet er en sårbarhet som utnyttes før eller rett etter at den blir kunngjort (før sikkerhetshull er tettet).
[31] Det vises til NSMs årlig rapport om sikkerhetstilstanden med tanke på etterlevelse av sikkerhetsloven i virksomhetene. Denne utgis årlig. Denne rapporten avgis til FD og JD, og en generell versjon sendes til virksomhetene underlagt loven. En ugradert versjon ligger på NSMs websider.

Angrep Telenorkunder
To store Telenorkunder ble i 2007 utsatt for et angrep som lammet flere tjenester. Angrepet var så stort at det gav ringvirkninger også for Telenors andre tjenester. Teknisk var angrepet langt større enn dataangrepet mot Estland i 2007 som rammet flere sektorer i flere dager. (Kilde: Telenor (på NSMs sikkerhetskonferanse 2007)/NorCERT)

Forsvaret utsatt for dataangrep
Fremmed etterretning har i flere år angrepet Forsvarets lukkede datanettverk. Angrepene har vært sofistikerte og nytenkende i datasammenheng, og er utført på en helt ny måte. FOST ser svært alvorlig på saken og mye av organisasjonens virksomhet på Jørstadmoen har vært fokusert på inntrengerne.
(Kilde: Forsvarets forum, 25.08.2009, http://www.fofo.no/Daglige+spionangrep.b7C_w7nI1L.ips)

Norsk toppleder ble offer for spionasje
En norsk toppleder ble kompromittert av en målrettet trojaner i 2007. Trojaneren kom inn gjennom vedlegg på e-post, og ble først oppdaget i 2008. NorCERT har vært med i håndteringen av flere liknende tilfeller i norske offentlige virksomheter.
(Kilde: NorCERT)

2. En helhetlig strategi for cybersikkerhet

Arbeidet med cybersikkerhet i Norge må styrkes. Sektorovergripende virkemidler står sentralt for å styrke sikkerheten i cyberspace.

Cybersikkerhet er ikke noe nytt. Utgangspunktet for denne strategien er det sikkerhetsarbeidet som alt i dag utføres av virksomheter som utvikler, eier, regulerer, drifter eller opererer kritiske IKT-systemer slik de er definert i kapittel 1. At disse virksomhetene både er private og offentlige, må derfor tas hensyn til ved utforming av tiltakene.

De overordnede prinsipper for nasjonalt sikkerhets og beredskapsarbeid (ansvar, likhet og nærhet) ligger fast. Men det er helt nødvendig å styrke prinsippet om samordning og få til sektorovergripende løsninger, for å kunne møte de utfordringer det nettverksbaserte samfunnet gir i en krisesituasjon. En hovedutfordring er at hendelser som rammer virksomheter raskt kan spres og få konsekvenser for andre virksomheter, andre sektorer eller endog samfunnet som helhet. En forutsetning for å være i stand til å møte et komplekst og dynamisk IKT trusselbildet er å styrke situasjonsforståelsen og evnen til å oppdage, rapportere om og reagere på sikkerhetstruende hendelser, som et tillegg til de øvrige forebyggende defensive sikkerhetstiltakene i samfunnet. Evnen til deteksjon og håndtering må styrkes både lokalt, i sektorene og på nasjonalt nivå.

En strategi for cybersikkerhet i Norge vil måtte ha en defensiv innretting. Strategien er til for å bidra til å gjøre vårt samfunn mer robust. Det er likevel nødvendig å se defensive og offensive kapasiteter i sammenheng, for på denne måten å kunne innrette våre felles ressurser slik at de ved synergi får den nødvendige effekt i beskyttelsen av informasjonsinfrastrukturen og bekjempelsen av ulovlig eller uønsket cyberaktivitet. Dette stiller imidlertid store krav til rolle- og prosessforståelse hos representantene for de etater som samarbeider, og at aktivitetene underlegges en tillitvekkende kontroll.

Tiltak som er av en slik karakter at de virker inngripende i forhold til private rettssubjekter krever hjemmel i lov. Nasjonal og internasjonal regelverksutvikling er derfor avgjørende for den nasjonale cybersikkerheten. Så vel tiltaks- som regelverksutvikling må veie sikkerhetsmessige behov opp mot enkeltindividets krav på personvern og rettsikkerhet.

Strategien har seks hovedmål:

- Etablere en felles situasjonsoversikt og forståelse
- Bygge og opprettholde robuste og sikre kritiske IKT-systemer
- Bevisstgjøre, opplyse og påvirke aktuelle målgrupper
- Styrke evnen til å oppdage, varsle og håndtere hendelser i kritiske IKT-systemer
- Aktivt avverge, bekjempe og etterforske hendelser i kritiske IKT-systemer
- Styrke samordning av cybersikkerhetsarbeidet

Under hvert hovedmål er det gitt en begrunnelse for valg av mål, og status er forsøkt illustrert med utsagn som er hentet fra erfaringer i NSM, tilbakemeldinger under utarbeidelse av strategien, nasjonale undersøkelser og internasjonale rapporter.

2.1 Etablere en felles situasjonsoversikt og forståelse

Norge må etablere en sektorovergripende kontinuerlig prosess for å velge ut hva som er kritiske IKT-systemer, koordinere forskning og utvikling, styrke arbeidet med et felles IKT-risikobilde, styrke det internasjonale samarbeidet på området, og etablere et bærekraftig partnerskap mellom det offentlige og private.

Hvorfor?

Alle samfunnsfunksjoner er i dag sterkt avhengige av velfungerende IKT-systemer. Det er behov for økt kunnskap om disse avhengighetene, på tvers av sektorene og over landegrenser. En totalsikring av cyberspace er ikke mulig. Det bør derfor legges vekt på å etablere prosesser for å identifisere de mest kritiske IKT-systemene, som representerer den største sårbarheten, som har størst sannsynlighet for å bli angrepet og som har størst skadepotensial. En felles situasjonsoversikt er en forutsetning for å styrke evnen til å utvikle og iverksette nødvendige sikkerhetstiltak.

Valg av tiltak bør videre være risikobaserte, og det forutsetter oppdatert og detaljert kunnskap om IKT-trusselbildet, dvs kunnskap om trusselaktører, deres intensjoner, kapasiteter og metoder, om mål som kan være attraktive for trusselaktører å angripe eller utnytte, om erfarte hendelser og om sårbarheter.

Status:

- Det foreligger flere utredninger knyttet til behov og metodikk for å identifisere kritiske IKT-systemer, også på tvers av samfunnssektorer. Disse er imidlertid ikke operasjonalisert og implementert.
- Noen sektorer har etablert løpende prosesser for å kartlegge sin samfunnsviktige IKT-infrastruktur – i andre sektorer er ikke dette arbeidet prioritert32.
- IKT-risikobildet er komplekst og i stadig utvikling. IKT-risikobildet er i for liten grad analysert, vurdert og formidlet.
- I 2008 ble koordineringsgruppen for IKT-trusselbildet opprettet av NSM, PST og Etterretningstjenesten for å etablere og vedlikeholde et nasjonalt IKT-trusselbilde. Se nærmere omtale i vedlegg A.
- Til tross for gjensidige avhengigheter landene imellom er det begrenset internasjonalt forpliktende samarbeid om cybersikkerhet.

Tiltak:

1. Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer

I flere samfunnssektorer er det etablert prosesser for å kartlegge IKT-systemer av betydning for sektoren. Prosessene er imidlertid ikke samordnet. Gjennom sikkerhetslovens bestemmelser om informasjonssikkerhet og objektsikkerhet får man et sektorovergripende grunnlag for utvelgelse av systemer av vital nasjonal sikkerhetsinteresse.

Direktoratet for samfunnssikkerhet og beredskap (DSB) er også i ferd med å starte et utredningsarbeid på dette området. Post og teletilsynet (PT) på sin side arbeider med prioriteringsordninger knyttet til elektroniske informasjonssystemer. Basert på eksisterende prosessmekanismer og eksisterende kunnskap bør det nå iverksettes en samordnet prosess for løpende kartlegging og verdivurdering av kritiske IKT-systemer i alle sektorer. Samtlige sektormyndigheter med sikkerhetsansvar bør trekkes aktivt inn i arbeidet.

[32] DSBs tilsynserfaringer i departementene viser at en viktig årsak til at mange har unnlatt å ta tak i disse problemstillingene er at ikke finnes noen klar definisjon av hvilke infrastrukturer som faller inn under samfunnskritisk og heller ikke beskrevet hvordan slike infrastrukturer skal identifiseres.

2. Målrettet satsning på forskning og utvikling

Forsknings- og utviklingsaktivitetene på sikkerhetsområdet kan oppfattes som fragmentert. Det har vist seg å være en utfordring å igangsette større og vedvarende aktiviteter med nødvendig grad av forutsigbarhet, da prosjektene ofte vil være avhengig av midler fra flere departementer og etater. For å skape en mest mulig helhetlig prioritering og langsiktighet i FOU-aktiviteter på cybersikkerhetsområdet bør JD og FD, med faglig støtte av etatene, gå sammen om å etablere et langsiktig FOU-program. Dette bør omfatte så vel sikkerhetsfaglige prosjekter som juridiske og policymessige. Norges forskningsråd (NFR) og relevante institusjoner innen akademia og blant øvrige forskningsinstitutter bør trekkes aktivt inn.

3. Styrke kapasitet for vedlikehold og formidling av IKT-risikobildet

Kunnskap om IKT-risikobildet er viktig med tanke på cybersikkerhetsarbeidet generelt, herunder målrettet tiltaksutvikling, håndtering av hendelser og formidling av motiverende informasjon.

NSM har fra 2008 hatt i oppdrag å utvikle og vedlikeholde IKT-trusselbildet. Til støtte for dette arbeidet er det etablert en koordineringsgruppe mellom NSM og de øvrige EOS-tjenestene slik at bildet blir beskrevet på en mest mulig helhetlig måte. Situasjonen er at metodikk og rutiner er innarbeidet for gruppens arbeid, men den mangler empiri for et større analysegrunnlag enn i dag. Dette skyldes delvis manglende innrapporteringsrutiner fra sektorene for data om hendelser og tilhørende vurderinger. Det er viktig at dette kommer på plass. En viktig forutsetning vil antakelig være etableringen av CSIRT-miljøer i den enkelte sektor (se tiltak nr. 15 nedenfor). Gitt Kripos og Økokrims ansvar for trusselvurderinger når det gjelder organisert kriminalitet vil det være viktig å trekke de inn i dette arbeidet.

Det er også viktig å utvikle det internasjonale samarbeidet slik at man også der mottar relevant oppdatert informasjon.

4. Styrke det internasjonale samarbeidet om cybersikkerhet

Utfordringer knyttet til cybersikkerhet kan ikke løses innenfor rammene av nasjonalstaten. Industrialiserte nasjoner harmoniserer sine tiltak gjennom overnasjonale og mellomstatlige organer som eksempelvis NATO og EU. I dag skjer dette samarbeidet basert på tillit og er i liten grad forpliktende regulert i internasjonale avtaler. Norge bør derfor være en pådriver for internasjonal harmonisering og regulering av cybersikkerheten, herunder internasjonale forpliktende samarbeid. Norge må søke å inngå i et forpliktende internasjonalt samarbeid for effektiv håndtering gjennom informasjonsdeling, men også etterforskning og straffeforfølging av kriminell aktivitet. For å fremstå som en profesjonell part i det internasjonale samarbeidet, er det viktig med kompetanse, å være koordinert, delta aktivt i debatter og bidra med forslag til løsninger.

5. Etablere partnerskap mellom offentlige myndigheter og private aktører

Mange kritiske IKT-systemer er under eierskap, drift og kontroll av private aktører, som styres av bedriftsøkonomiske hensyn og ikke nødvendigvis er underlagt samme regler som offentlige virksomheter. Det må legges til rette for at private ser nytten av og etablerer partnerskap med det offentlige, slik at cybersikkerheten ivaretas, og det utvikles ordninger og tiltak som støtter opp under det løpende sikkerhetsarbeidet. NorCERT der private virksomheter, offentlige myndigheter og etater samarbeider alt i dag for å oppdage og håndtere alvorlige IKT-hendelser er et eksempel på slikt partnerskap, og kan stå som modell for andre sider av cybersikkerhetsarbeidet.

Det finnes også frivillige initiativer hvor grupper av enkeltpersoner med kompetanse og engasjement bidrar til økt informasjonssikkerhet. Det bør tas stilling til om og hvordan slike miljøer skal stimuleres og hvordan samarbeidet om nødvendig kan formaliseres.

2.2 Bygge og opprettholde robuste og sikre IKT-systemer

Vi må stilles felles krav til kritiske IKT-systemer, styrke og samordne tilsyn, etablere sikre kommunikasjonsløsninger i krisesituasjoner, styrke beredskapen, og vurdere lovgivningen i cyberspace.

Hvorfor?

Robuste og sikre IKT-systemer er viktig for å øke evnen til å motstå de mest sannsynlige og alvorlige former for IKT-hendelser. Økt sammenkobling av systemer stiller virksomheter overfor en rekke utfordringer når det gjelder risikoanalyser, beredskapstiltak, systemovervåkning m.m. Dette innebærer at det er et sterkt behov for kontinuerlig videreutvikling, der tilbakeføring av erfaringer fra eksempelvis tilsyn og hendelseshåndtering er viktige faktorer. Det er krevende å utvikle tiltak i tråd med den teknologiske utviklingen, og det er en utfordring å sette av tilstrekkelige ressurser til forebyggende sikkerhetstiltak, tiltak man gjerne ikke ser nytten av før en eventuell alvorlig IKT-hendelse i systemene inntreffer.

Det er ikke gitt hvilke metoder en trusselaktør vil benytte seg av. Nye metoder for blant annet misbruk, påvirkning og kompromittering av IKT-systemer blir stadig utviklet. Denne utfordringen må møtes med gode og balanserte sikkerhetskrav. Prinsippet om forsvar i dybden, med flere lag med barrierer, er ment å møte utfordringen med uforutsette angrepsformer. Dersom et tiltak svikter vil et nytt ta over.

Status:

- Det er uklart i hvilken grad samtlige kritiske IKT-systemer vil være underlagt spesifikke krav til sikkerhet med tilhørende tilsyns- og kontrollregimer.
- Utenfor sikkerhetslovsområdet er reguleringen av IKT-sikkerheten i hovedsak innrettet sektorvis og det stilles få krav til sertifisering av sikkerhet i systemer og produkter.
- Markedsmekanismer, samfunnsutviklingen og den teknologiske utviklingen har medført at drifting av datasystemer har blitt lagt til land med kompetanse og lavt kostnadsnivå (såkalt offshoring). Dette skaper sårbarheter.
- Regelverk er ikke oppdatert i forhold til et dynamisk IKT-trusselbilde.
- Nasjonale øvelseserfaringer viser behov for videreutvikling av det nasjonale beredskapssystemet (NBS) med tanke på IKT-tiltak.

Tiltak:

6. Stille felles krav til kritiske IKT-systemer

Det finnes teknologiske og administrative mottiltak som i sum kan utgjøre et godt forsvar i dybden mot mange typer angrep. Krav og tiltak som forutsettes til stede i kritiske IKT-systemer, inkludert hvordan disse bør designes, konfigureres, driftes og vedlikeholdes med tanke på best mulig sikkerhet er ikke godt nok utviklet. Tiltakene bør derfor videreutvikles og nedfelles i krav som er felles for kritiske IKT-systemer. Dette inkluderer også å se på krav til fysisk beskyttelse, retningslinjer for offshoring m.m.

Forebyggende sikkerhet i informasjonssystemer kan styrkes vesentlig ved at virksomhetene anskaffer godkjente og veldokumenterte løsninger gjennom å bruke etablerte sertifiseringsordninger og følge anerkjente internasjonale standarder[33]. Det må vurderes å stille krav til sertifiserte produkter ved anskaffelser i offentlig sektor og virksomheter som er en del av samfunnskritisk infrastruktur. Videre bør kritiske IKT-systemer tilfredsstille anerkjente internasjonale standarder for å sikre at disse driftes og vedlikeholdes på en sikker måte gjennom hele levetiden.

7. Styrke tilsyn med IKT-sikkerhet

Det er viktig gjennom tilsyn å følge opp at IKT-sikkerhetstiltak er implementert på en god måte i virksomheter med samfunnskritiske funksjoner. Tilsyn med IKT-sikkerhet gjennomføres i dag av flere myndighetsorganer som i liten grad utveksler tilsynserfaringer. Det samlede tilsynsarbeidet med sikkerheten i IKT-systemene, så vel tverrsektorielt som sektorvis, bør kartlegges og gjennomgås med tanke på forbedringer og samordning. Erfaringene bør samles og analyseres, og gi føringer for videreutvikling av sikkerhetstiltak og koordinert gjennomføring av tilsyn.

[33] Med etablerte sertifiseringsordninger menes eksempelvis SERTIT under NSM. Et eksempel på en anerkjent internasjonal standard er ISO-standarden ISO/IEC 27001 beskriver krav til styringssystemet for informasjonssikkerhet.

8. Utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering

Status i dag er at graderte kommunikasjonsløsninger til bruk i kriser i hovedsak består av kryptotelefon og fax. Øvelseserfaringer[34] har vist at disse ikke fungerer tilfredsstillende. Nødnettet er under utbygging, men er ikke ment å erstatte disse systemene. Evne til håndtering av hendelser forutsetter fungerende graderte kommunikasjonsløsninger som også motstår angrep fra trusselaktører. Det bør utredes hvordan kommunikasjonsbehovet ved kriser kan ivaretas på en måte som sikrer tilgjengelighet, konfidensialitet og integritet.

9. Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak

Det er viktig at man så langt det er mulig har forberedt tiltak for å forsterke evnen til cybersikkerhet som raskt kan iverksettes i en krisesituasjon. Øvelseserfaringer har avdekket et spesielt behov for å videreutvikle det nasjonale beredskapssystemet (NBS). Det bør i tillegg utarbeides veiledningsmateriale til støtte for virksomhetenes arbeid med egne beredskapsplaner.

10. Behov for regulatorisk forankring av cybersikkerhet

Ny teknologi legger ofte premissene for samfunnsutviklingen. De muligheter teknologien gir kan imidlertid utfordre andre viktige interesser som enkeltindividets personvern og rettsikkerhet. Sikkerhetstiltak som implementeres må derfor ha et rettsgrunnlag, og innenfor denne rammen ut i fra en forholdsmessighets vurdering, fremstå som samfunnsmessig ønskelige og nødvendige. Det er behov for en helhetlig gjennomgang av eksisterende relevant regelverk og det bør nedsettes et lovutvalg som ser på de rettslige aspekter knyttet til cybersikkerhet.

2.3 Bevisstgjøre, opplyse og påvirke

Holdningsskapende arbeid og utdanning må prioriteres og det må gjennomføres flere øvelser.

Hvorfor?

Kompetanse og kunnskap om IKT-sikkerhet er avgjørende for en god forebygging og håndtering av IKT-hendelser. Den teknologiske utviklingen har gjort risikoen knyttet til menneskelig adferd mye større. Når det tekniske forsvaret styrkes vender angripere oppmerksomheten mot brukerne av IKT-systemer. Enkeltindividets sikkerhetsbevissthet og adferd utgjør samfunnets førstelinjeforsvar mot trusler på nett.

Utviklere, eiere og brukere av kritiske IKT-systemer må ha en grunnleggende forståelse for risikoen cyberspace innebærer og dermed nødvendigheten av sikkerhetstiltak.

Status:

- Det gjennomføres få IKT-øvelser som gir erfaring og kompetanse for effektiv håndtering av alvorlige hendelser. Brukernes atferd og holdninger er i for liten grad med som element i øvelser.
- Brukernes forståelse for risiko, og følger av egen uønsket atferd, er svak.
- Sikkerhetsforståelsen hos eiere av systemer og infrastruktur er liten**,** og det kan i for liten grad dokumenteres IKT-sikkerhetskompetanse hos driftspersonellet.
- Det er manglende bevissthet i organisasjoner om hvordan organisasjonskultur og sikkerhetskultur påvirker holdninger, atferd og bruk av IKT-systemer.

[34] Eksempelvis ”Øvelse Oslo 2006”, ”Øvelse IKT-08” og ”NCDEX09 (NATO Cyber Defence Exercise 2009 – Cyber Coalition)”.

Tiltak:

11. Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid
Tiltak for bevisstgjøring og holdningsskapende arbeid rettet mot personell knyttet til kritiske IKT-systemer må utvikles og tilpasses de stadige endringene i IKT-trusselbildet. Tiltakene bør utvikles i et samarbeid mellom tilsynsmyndigheter, næringslivet og private organisasjoner. Kampanjer og kontinuerlig fokus på økt sikkerhetsbevissthet må gjennomføres i virksomhetene, og sikkerhetskulturarbeidet må styrkes. Styrking av sikkerhetsbevisstheten hos driftspersonell og brukere av kritiske IKT systemer bør tillegges spesiell vekt.

Virksomhetene må satse på sikkerhetsutdanning og kompetanseheving av personell på ulike nivåer i organisasjonen, og det bør stilles krav til dokumentert sikkerhetskompetanse for nøkkelpersonell.

12. Arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale)
Det er kontinuerlig behov for å arrangere realistiske øvelser for å vurdere samfunnets robusthet og evne til å håndtere alvorlige IKT-hendelser. Det er et behov for fellesøvelser – mellom sikkerhetsfaglig ekspertise, jurister og "policymakers" – der man kan fokusere på interaksjonen mellom de som utvikler lovverket, de som kjenner teknologien og de som skal ta beslutninger. Videre må det øves på tverrsektoriell samhandling og på tvers av landegrenser.

2.4 Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser

Det må opprettes sektorvise miljøer for håndtering av alvorlige IKT-hendelser. Evne til oppdagelse og rapportering av IKT-hendelser må bli bedre.

Hvorfor?

Samfunnet må ha evne til å oppdage IKT-hendelser som utløser behov for skjerpet sikkerhet, og må være forberedt på å håndtere endringer i IKT-risikobildet. Hendelseshåndtering skjer på mange ulike nivåer; i den enkelte virksomhet, på sektornivå og på nasjonalt nivå, strategisk og operativt. Formålet med håndteringen er å gjenopprette sikkerhet og funksjonsevne i virksomhetenes systemer. I tillegg til håndtering av selve angrepet må også de samfunnsmessige konsekvensene av angrepet håndteres.

Det er en utfordring å forstå hendelsenes tekniske karakter og omfang, det vil si å skille mellom hendelser som skyldes et målrettet villet anslag eller en teknisk eller menneskelig svikt i IKT-systemet. I mange tilfeller vil en teknisk forståelse av angrepet forutsette analyse av ondsinnet kode. Dette er tidkrevende, og få miljøer har nødvendig spisskompetanse for dette.

En annen utfordring er å knytte IKT-hendelser til en bestemt aktør. Det å skjule sin identitet på Internett er forholdsvis enkelt. I praksis vil analyser av hendelser først og fremst gi indikasjoner på hvem som kan stå bak, og sikrere identifikasjon vil som regel forutsette tilleggsinformasjon fra kilder som politi-, etterretnings- og CSIRT[35] miljøer, nasjonalt og internasjonalt.

Ved håndtering av IKT-hendelser vil ulike tiltak og reaksjonsformer kunne iverksettes. I noen tilfeller vil økt årvåkenhet være tilstrekkelig for å møte et endret IKT-risikobilde. Andre hendelser vil kreve aktiv forebygging, for eksempel gjennom omdirigering/ruting av uønsket nettverkstrafikk hos tjenesteleverandører. Parallelt med slike tiltak vil berørte virksomheter gjennomføre skadevurderinger, og oftest søke å gjenopprette sikkerheten i sine systemer. Av og til vil det iverksettes aktørrettede tiltak (se kapittel 2.5). Et kort tidsvindu for reaksjon stiller spesielle krav til forhåndsdefinerte prosesser og rutiner, både operative og strategiske, i forhold til valg av reaksjonsform, rolleavklaring og myndighet ved håndtering av IKT-kriser (se kapittel 2.6).

[35] Begrepet CSIRT (Computer Security Incident Response Team), brukes som en fellesbetegnelse for CERT, (Computer Emergency Response Team), IRT og andre akronymer med samme betydning.

Status:

- Det er stor variasjon i hvilke hendelser som registreres og rapporteres til myndighetene, og hvordan denne informasjonen systematiseres i arbeidet med å styrke IKT sikkerhetstilstanden.
- Få virksomheter har nødvendige rutiner og deteksjonsmekanismer for å oppdage og varsle om uønskede IKT-hendelser. VDI[36] er etablert i NSM, og har evne til å oppdage eksterne trusler mot et utvalg offentlige og private virksomheter, men ikke i alle virksomheter med kritiske samfunnsfunksjoner.
- Den nasjonale operative koordineringen av dataangrep mot Norge er lagt til NorCERT, som er etablert i Nasjonal sikkerhetsmyndighet.
- Operative CSIRT-miljøer i sektorene er kun etablert i Forsvaret og i akademia, men det arbeides med slike tiltak innenfor bl.a. telekom, kraft, helse, bank- og finans og justissektoren. Slike miljøer må ses i sammenheng med eksisterende sektorsamarbeid.

Tiltak:

13. Styrke samfunnets evne til å oppdage trusler og sårbarheter

Effektiv deteksjon av nye trusler og sårbarheter forutsetter i økende grad registrering og analyse av datakommunikasjon. Evnen til å oppdage aktivitet som representerer trusler og sårbarheter må styrkes både sentralt og lokalt i den enkelte virksomhet og i det enkelte system. Samfunnets samlede deteksjonskapabiliteter må utvikles fortløpende med tanke på å oppdage alvorlig aktivitet. På nasjonalt nivå foreslås omfanget av VDI utvidet slik at sensorsystemet dekker en større andel av virksomhetene med kritiske IKT-systemer. I tillegg må det etableres prosesser for å hente ut synergier mellom VDI og annen innsamling som beskriver IKT-trusselbildet.

14. Legge til rette for innrapportering av hendelser

En viktig kilde til sikkerhetsvarsler og arbeidet med IKT-risikobildet er registrering og videreformidling av hendelser. Alle sektorer bør ha prosedyrer for innrapportering av alvorlige hendelser som grunnlag for varsling og behov for eskalering i hele sektoren. Økt rapportering, systematisering og analyse av dataene vil gi alle virksomheter et bedre grunnlag for å gjennomføre risikoanalyser og prioritere riktige sikkerhetstiltak. Sektormyndighetene må sørge for at rapporteringen gir nytteverdi til virksomhetene, og om nødvendig innføre krav til rapportering. For å avdekke sektorovergripende utfordringer, bør det etableres rutiner for videreapportering fra sektormyndigheter til sentralt nivå.

15. Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter

Hendelser i kritiske IKT-systemer som rammer én virksomhet kan ha betydning for andre virksomheter i sektoren, men også for andre sektorer. Det må derfor legges til rette for rask og systematisk varsling ved alvorlige hendelser mellom berørte virksomheter og offentlige myndigheter, på tvers av sektorene. Systematisk informasjonsutveksling innebærer juridiske og rettslige problemstillinger som må adresseres og som forutsetter kompetanseheving.

En viktig forutsetning for effektiv håndtering av IKT-hendelser er at det etableres operative sektorvise CSIRT-miljøer, som samarbeider på tvers av sektorene og med NorCERT. Disse er ikke nødvendigvis nye organisatoriske enheter, men som regel nettverksbaserte møteplasser, som trekker på eksisterende fagmiljøer i den enkelte sektor. I noen sektorer kan eksisterende varsling og beredskapssamarbeid gjenbrukes, men det forutsetter IKT-faglig kompetanse. Det anbefales at CSIRT-miljøer i første omgang etableres i særlige samfunnsviktige sektorer som forsvarssektoren, justissektoren, utenrikssektoren, olje- og gassektoren, telekomsektoren, kraftsektoren, helsesektoren og i finanssektoren.

[36] Varslingssystem for Digital Infrastruktur (VDI) organiserer og drifter et nasjonalt nettverk av innbruddsdeteksjonssensorer på Internett som detekterer om noen prøver å utføre uønsket aktivitet mot kritisk digital infrastruktur i Norge.

2.5 Etterforske og bekjempe IKT-hendelser

Kompetansen og evnen til å etterforske og håndtere målrettede dataangrep må styrkes. Evnen til å identifisere trusler og trusselaktører i cyberspace må videreutvikles. Behovet for endringer i regelverket bør vurderes.

Hvorfor?

Cyberspace er en viktig arena for handel og økonomiske transaksjoner, og samfunnets kritiske infrastruktur knyttes i økende grad til internett. Dette gjør cyberspace til en attraktiv arena også for kriminalitet, spionasje, og også i ytterste konsekvens krigføring i en krise/krigssituasjon. Etterforsking av datakriminalitet er svært krevende. En av hovedutfordringene knyttet til dette er at cyberspace er uregulert i sin natur. Det vil på ethvert tidspunkt foreligge utfordringer med hensyn til det legale grunnlaget for etterforskning for å holde følge med, og være i forkant av, den teknologiske utvikling.

En god strategi for cybersikkerhet innebærer at trusselaktører ikke kan forberede eller gjennomføre kriminelle handlinger uten betydelig risiko for å bli oppdaget.

Status:

- Etterforskning av datakriminalitet generelt og målrettede dataangrep spesielt er svært utfordrende, og krever særlig kompetanse. Det er få miljøer i politiet som i dag har denne kompetansen.
- Det store flertallet av datakrimsaker har et internasjonalt tilsnitt, der kilder til etterforskning ligger i mange land. Etterforskningsskritt i utlandet er svært krevende, både tidsmessig og regulatorisk.
- Få trusselaktører er dømt for planleggingen eller gjennomføringen av alvorlige IKT-hendelser i Norge.
- Det er store utfordringer knyttet til å identifisere og ansvarliggjøre gjerningsmenn. Offensive tiltak blir derfor vanskelige å gjennomføre, fordi man ofte ikke vet hvem de skal rettes mot.
- Det foreligger utfordringer knyttet til det legale grunnlaget for etterforskning
- Man er ofte prisgitt nasjonale og internasjonale private aktørers evne og vilje til samarbeid.

Tiltak:

16. Styrket kapasitet og kompetanse for håndtering av målrettede dataangrep

For å bygge robuste fagmiljøer i politiet må det iverksettes en langsiktig satsning for å heve kompetansen innen etterforskning og håndtering av målrettede dataangrep. Et nært samarbeid mellom de operative miljøene i KRIPOS, PST og NSM vil bidra til å styrke den nasjonale kompetansen på området.

17. Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning

Etterforsking av datakriminalitet krever data. Om slike data slettes for tidlig vil muligheten for å etterforske effektivt hemmes. Det er dessuten en samfunnsmessig utfordring om cyberspace – som vi alle blir mer og mer avhengig av – blir oppfattet som et lovløst rom. Samfunnet må derfor legge til rette for en effektiv etterforsking.

18. Utrede behov for endringer i det legale grunnlaget for etterforskning

Det er viktig med dynamikk i både det nasjonale og internasjonale regelverket, slik at det enkelt kan ta opp i seg stadige endringer i teknologien. Det internasjonale samarbeidet må styrkes, sammen med en harmonisering av regelverket og forenkling av internasjonal etterforsking. Eventuelle endringer av det legale grunnlaget for etterforskning av datakriminalitet er en kompleks og tidkrevende oppgave. For å sikre at man til enhver tid har de nødvendige legale verktøy må behovet for endringer utredes nærmere.

19. Avdekke og identifisere trusler og trusselaktører

Spesifikk kunnskap om trusler og trusselaktører er viktige forutsetninger for effektiv beskyttelse av samfunnets verdier og infrastruktur, og utarbeidelse av trusselvurderinger er en sentral del av dette arbeidet. Innhenting og systematisering av informasjon må derfor utvikles i takt med endringene og forskyvningene i trusselbildet. Bekjempelse av nye og komplekse trusler bør ikke bare innrettes defensivt, men etter behov også som kilde til kunnskap om trusselaktørens oppfatninger og prioriteringer.

Innhenting og systematisering av informasjon i den hensikt å avdekke og identifisere trusler og trusselaktører vil i prinsippet være etterretningsorienterte aktiviteter. Kontraetterretning[37]- og kriminaletterretning[38] i forhold til IKT-trusler må utvikles og gis innhold i samsvar med behovet for spesifikk informasjon og kunnskap.

20. Offensive kapasiteter

Cyberspace er blitt en stor arena for menneskelig interaksjon. Mange av de konfliktlinjer som er kjent fra den fysiske verden vil også gjøre seg gjeldende her. Cyberspace vil imidlertid aldri bli et virtuelt territorium som kan okkuperes. Det strategiske utfallet av en konflikt vil heller ikke avgjøres i cyberspace.

Norge har utviklet en deployerbar enhet for militære informasjonsoperasjoner (CNO-enheten[39]). Enheten bidrar til å bygge kompetanse og kapasitet til å beskytte Forsvarets informasjonsinfrastruktur og har en viss kapasitet for å påvirke en motstanders informasjonssystemer. Det er viktig å se ulike nasjonale kapasiteter, defensive og offensive, i sammenheng, og styrke den nasjonale evnen til etterretning, kontraetterretning og inntrengningstesting. Dette åpner også for deltakelse i internasjonalt og alliert samarbeid.

2.6 Styrke samordningen av cybersikkerhetsarbeidet

Det er behov for forsterket samordning, tydeliggjøring av det politiske ansvaret og videreutvikling av den nasjonale operative evnen. Ved å etablere samordningsmekanismer legges grunnlaget for gjennomføring og oppfølging av de øvrige tiltakene i strategien.

Hvorfor?

Ved IKT-hendelser er det selv i en sikkerhetspolitisk krise og konflikt, vanskelig å identifisere en eventuell trusselaktør. Er dette alminnelig kriminalitet eller en trussel mot nasjonale vitale samfunnsinteresser? Er trusselaktøren norsk, oppholder han seg i Norge eller er dette en utenlandsk trussel? Står det statlige trusselaktører bak? IKT-hendelser vil variere i et spekter fra enkelthendelser i en kritisk virksomhet via nasjonal krise til eventuell krig. Usikkerheten er stor og i en konkret håndteringssituasjon er det ikke umiddelbart gitt hvilke hensyn som skal gå foran om ikke alle kan realiseres. Virksomhetene vil normalt ha et ønske om å redusere skade og bringe sikker tilstand tilbake så raskt som mulig. Politiet må ta stilling til hensynet til etterforsking, Etterretningstjenesten hensynet til informasjon om angrepet og eventuelle aktører som står bak. Det vil derfor være viktig å få gode krisehåndteringsmekanismer på plass som sørger for at hensyn avveies og at dette skjer på det rette ansvarlige nivå.

Operativ og effektiv håndtering av alvorlige IKT-hendelser forutsetter derfor et godt samarbeid mellom EOS-tjenestene, Politiet og andre i det daglige. Det er også bakgrunnen for at VDI opprinnelig ble lansert som et samarbeid mellom de tre tjenestene, og offentlige og private virksomheter. Alvorlige

[37] Kontraetterretning blir tradisjonelt oppfattet som den mer aktive delen av sikkerhetstjenesten, med oppgave å avdekke de metoder og midler et fremmed lands etterretningstjeneste benytter. Kontraetterretning i oppdatert og utvidet betydning må ta høyde både for endringer i trusselbildet og anvendelsen av nye metoder.
[38] Kriminaletterretning blir ofte beskrevet som en prosess der politiet innhenter, systematiserer og analyserer informasjon om kriminelle og deres aktivitet, i den hensikt å bedømme og trekke slutninger av kriminalitetsbildet, påpeke potensielle problemer og kriminell aktivitet med intensjon om straffeforfølgning eller å kartlegge kriminelle trender. Strategisk kriminaletterretning er rettet mot alvorlige former for kriminalitet som reelt eller potensielt utgjør sikkerhetsutfordringer for samfunnet.
[39] CNO: Computer Network Operations

hendelser som etterretningsaktivitet og spionasje mot norske interesser er økende i omfang, og samarbeidet mellom EOS-tjenestene, som har ulike roller og ansvar, bør styrkes.

IKT-trusselbildet er dynamisk og komplekst, og større IKT-hendelser vil normalt være grenseoverskridende og globale. Det er et kontinuerlig kappløp mellom trusselaktørene som utnytter mulighetsrommet og myndigheter og sikkerhetsselskaper som søker å beskytte mot disse truslene. Forebygging og håndtering er ressurskrevende, og det er derfor nødvendig med felles satsning på å etablere og vedlikeholde fagmiljøer med nok kompetanse og ressurser til å møte IKT-trusselbildet.

Status:

- Varslingssystem for digital infrastruktur (VDI) ble i 2000 etablert som et prøveprosjekt, i et samarbeid mellom EOS-tjenestene, offentlige og private virksomheter. I 2003 ble VDI permanent etablert som en del av NSM.
- NorCERT, med nasjonalt ansvar for å koordinere håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon ble etablert i NSM i 2006.
- Koordineringsgruppen for IKT-trusselbildet ble etablert i 2008 som et samarbeid mellom EOS-tjenestene for å sikre en helhetlig beskrivelse av IKT-trusselbildet.
- NorCERT har inngått privatrettslige avtaler med privat næringsliv, og er det nasjonale og internasjonale kontaktpunktet for tilsvarende CERT-funksjoner.
- Ansvaret knyttet til cybersikkerhet er fordelt på flere departementer og etater.

Tiltak:

21. Opprette en gruppe for faglig støtte til Justisdepartementet og Forsvarsdepartementet

Justisdepartementet har et overordnet samordningsansvar for samfunnssikkerheten og beredskapsplanleggingen i fredstid, og utgjør sammen med Forsvarsdepartementet de to departementene med størst ansvar for nasjonal sikkerhet og sektorovergripende sikkerhetsutfordringer. Disse departementene har derfor et særlig politisk og overordnet faglig ansvar for oppfølging av den nasjonale strategien for cybersikkerhet.

Å ta dette ansvaret forutsetter at departementene øker sin kompetanse og dedikerer medarbeidere til oppfølgingen av strategien. Departementene må i tillegg få faglig støtte fra underliggende ledd og EOS-tjenestene spesielt. Dette foreslås løst gjennom at det etableres en gruppe med fokus på alle sider ved cybersikkerhet, hvor disse inngår. Gruppen bør trekke inn erfaring og kompetanse fra offentlige myndigheter og privat næringsliv ved behov.

22. Etablere et nasjonalt cybersenter

Det er behov for en operativ funksjon rettet inn mot nye og endrede behov knyttet til ivaretakelse av cybersikkerheten. Dette behovet dekkes gjennom etablering av et nasjonalt cybersenter. Målene for senteret vil være å styrke Norges evne til effektivt å håndtere og respondere på alvorlige IKT-hendelser og situasjoner, bedre og mer omforent forståelse av sikkerhetsutfordringene, bedre utnyttelse av kritisk kompetanse, synliggjøring av nasjonal innsats og tilrettelegging for nærmere internasjonalt og nasjonalt samarbeid. Dette inkluderer videreutvikling av modeller for operativt samarbeid mellom offentlige myndigheter og private virksomheter.

Et nasjonalt cybersenter bør omfatte følgende funksjoner:

- NorCERT, med nasjonalt ansvar for å koordinere håndteringen nasjonalt og internasjonalt av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.
- Varslingssystem for digital infrastruktur (VDI).
- Tverrfaglige analysefunksjoner i et samarbeid mellom de 3 EOS-tjenestene, og eventuelt andre ved behov, for å sikre en helhetlig analyse og vurdering av IKT risikobildet. Dette er i praksis en videreutvikling og operasjonalisering av Koordineringsgruppen for IKT-trusselbildet.

- Partnerskap med privat næringsliv – modeller for operativt samarbeid mellom offentlige myndigheter og private virksomheter som er utviklet i NorCERT vil videreutvikles og favne enda bredere.
- Koordinering av det internasjonale operative samarbeidet på området.

De tre tjenestene – NSM, PST og E-tjenesten – arbeider ut fra tilstøtende virksomhetsgrunnlag. Et viktig tiltak er å forsterke og utfylle den samlede innsatsen gjennom å skape en felles arena hvor relevante deler av tjenestenes virksomhet bringes tettere sammen. I arbeidet med tverrfaglige analyser er tjenestene likeverdige i den forstand at den enkelte tjenestes hjemmelsgrunnlag må legges til grunn. Tilsvarende vil være tilfelle i forhold til Politiet eller andre samarbeidspartnere. En viktig oppgave vil være å koordinere ansvarsforhold ved utarbeidelse av rapporter og analyser, og ved håndtering av hendelser.

Etablering av et nasjonalt cybersenter er et viktig virkemiddel for å styrke evnen til å etterforske og bekjempe IKT-hendelser (se kapittel 2.5), og samle fagmiljøer. Arbeidet i senteret vil legge forholdene til rette for nødvendig informasjonsdeling. Juridiske forutsetninger og spørsmål knyttet til formelt ansvar må avklares nærmere, og detaljerte prosessbeskrivelser utarbeides.

Det understrekes at nærhets, likhets og ansvarsprinsippene fortsatt er styrende i forhold til beredskapsarbeidet, og det må parallelt med utviklingen av et nasjonalt cybersenter jobbes målrettet for å styrke sektorenes evne til beskytte egne kritiske IKT-systemer.

Vedlegg A: Eksisterende roller, ansvar og myndighet nasjonalt

Cybersikkerhet er en videreutvikling av informasjonssikkerhetsarbeidet med fokus på beskyttelse av de kritiske IKT-systemene mot særlig alvorlige hendelser. En rekke organisatoriske enheter eksisterer allerede, og bidrar til å beskytte Norge mot uønskede IKT-hendelser. Følgende aktører har derfor en særskilt rolle også i arbeidet med cybersikkerhet:

- Politiets sikkerhetstjeneste (PST) er tillagt oppgaven som nasjonal sikkerhetstjeneste og ivareta ansvaret for landets indre sikkerhet. PST samler og analyserer informasjon, og treffer tiltak mot forhold som kan true nasjonens sikkerhet. Sikkerhetstjenesten er tillagt påtalemyndighet, og ivaretar oppgaver knyttet til forebygging og etterforskning av mulige sikkerhetsmessige lovbrudd.
- Etterretningstjenesten (E) er tillagt oppgaven som nasjonal tjeneste for sivile og militære utenlandsetterretninger. Etterretningstjenesten innhenter, bearbeider og analyserer informasjon om fremmede stater, organisasjoner og individer som kan utgjøre en reell eller potensiell trussel mot norske interesser.
- Nasjonal sikkerhetsmyndighet (NSM) er et direktorat for forebyggende defensiv sikkerhetstjeneste, og har som hovedoppgave å koordinere utviklingen og kontrollere etterlevelse av de forebyggende sikkerhetstiltak iht. sikkerhetsloven med forskrifter. NSM ivaretar også oppgaven som nasjonal CERT-funksjon (Computer Emergency Response Team) gjennom NorCERT.
- KRIPOS er den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet, og har blant annet ansvaret for Datakrimavdelingen.
- Post- og teletilsynet (PT) er tildelt et særskilt myndighetsansvar for sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester.
- Forsvaret har innenfor cyberområdet, i tillegg til å beskytte egne systemer, også et ansvar for å styrkeprodusere CNO-avdelingen[40] (CNO = Computer Network Operations).

Øvrige sektormyndigheter, som Kredittilsynet, Norges Vassdrags- og energidirektorat, Petroleumstilsynet, Helsedirektoratet og Oljedirektoratet, har ansvar for å ivareta sikkerheten innenfor sine respektive sektorer, og vil komplettere og utfylle de ovennevnte aktørers arbeid med cybersikkerhet. Også tjenestetilbydere som eksempelvis Telenor vil ha bestemte roller i forbindelse med cybersikkerhet, bl.a. i forbindelse med å tilrettelegge for politiets kriminalitetsbekjempelse.

Utover dette har Datatilsynet en viktig rolle i forhold til å informere og gi råd i forhold til personvernet generelt og farer for personvernet spesielt. Næringslivets Sikkerhetsråd, NorSIS og Nettvett.no en sentral rolle i forhold til bevisstgjørings- og veiledningsarbeid, spesielt rettet mot små og mellomstore bedrifter i privat og offentlig sektor, inkludert kommunene, samt hjemmebrukere.

I 2008 ble koordineringsgruppen for IKT-trusselbildet opprettet av NSM, PST og Etterretningstjenesten for å etablere og vedlikeholde et nasjonalt IKT-trusselbilde. Gruppen skal i tillegg til å koordinere felles analyseprodukter også være premissgiver for et teknisk og operativt samarbeid mellom de tre tjenestene[41].

På det politiske nivå er det også fordelt ansvar og etablert strukturer som har betydning for den nasjonale cybersikkerheten[42]. Hovedprinsippet i beredskapsarbeidet er at det departement som har ansvar for en sektor til daglig, også har ansvaret for beredskapsplanlegging og tiltak i en krisesituasjon. Justisdepartementet har imidlertid et samordningsansvar for samfunnets sivile sikkerhet og ansvar for tilsynsarbeidet med dette gjennom Direktoratet for samfunnssikkerhet og

[40] CNO-avdelingen er omtalt i St prp. nr. 48, pkt 6.9.4 og 6.11.1
[41] St meld 22 (2007-2008) om Samfunnssikkerhet
[42] St mld. nr. 17 (2006-2007) Eit informasjonssamfunn for alle

beredskap (DSB), NSM, Politidirektoratet (POD), PST, de to hovedredningssentralene og Fylkesmennenes beredskapsarbeid. Forsvarsdepartementet har ansvar for utforming og iverksetting av norsk forsvarspolitikk.

Regjeringens kriseråd (RKR) har som hovedoppgave å sørge for strategisk koordinering, og vil samles dersom en krise er av en slik karakter at flere departementer er involvert og det er behov for koordinering[43]. Dette gjelder spesielt håndtering av de samfunnsmessige konsekvensene av alvorlige IKT-hendelser. Den nasjonale operative koordineringen av dataangrep mot Norge er lagt til NorCERT, som er etablert i Nasjonal sikkerhetsmyndighet.

Samferdselsdepartementet (SD) har som sektordepartement ansvar for IKT-sikkerheten i elektroniske kommunikasjonsnett og -tjenester. Fornyings- og administrasjonsdepartementet (FAD) har et nasjonalt og internasjonalt samordningsansvar for IKT-politikk. Dette er forankret i samordningsansvaret for IKT-politikken og gjelder forebyggende, tverrsektorielt arbeid med IKT-sikkerhet. Både SD og FADs ansvar avgrenser seg mot JDs og FDs særskilte ansvar på samfunnssikkerhetsområdet[44].

Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS), som ble opprettet i 2004 er et tverrsektorielt koordineringsorgan for regelverksforvaltere og tilsynsmyndigheter med ansvar innen informasjonssikkerhet[45]. Utvalget ledes av FAD.

[43] St.mld. 37 (2004-2005) Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering
[44] St mld. nr. 17 (2006-2007) Eit informasjonssamfunn for alle
[45] Mer om KIS på www.kis.stat.no