Koordineringsgruppen for IKT-risikobildet

Vår referanse: 2010/00719/430

Bakgrunnsnotat

Cybersikkerhet

2010-06-01

Innhold

Innhold 2
Innledning 3
Nye sikkerhetsbehov 4
Om IKT-infrastruktur 5
IKT-sårbarhet 6
  Kommunikasjonsinfrastruktur 7
  Prosesskontrollsystem 8
IKT-trusler 9
  Trusselkategorier 9
  Angrepsvektorer 11
    Sosial manipulering 11
    E-post… 11
    Nettsider 12
    USB-enheter 12
  Teknikker 13
    Filformater 13
    Verktøykasser 13
    Botnettverk (botnet) 13
  Kapabilitet 14
  Mål… 14
Erfaringer fra IKT-hendelser og øvelser 15
  Målrettede operasjoner 15
  Store tjenestenektsangrep 15
  Banktrojanere 16
  Kompromitterte datamaskiner 16
  Nettsidehærverk 17
  Elektronisk forvaltning 17
  Øvelser 18
    IKT 08.. 18
    NATO Cyber Defence Exercise 2009 18
    Cyber Storm II 18
    IWWN COMEX/ALEX Quick response 19
Koordineringsgruppen for IKT-risikobildet 20
Termer og definisjoner 21

Innledning

I dette bakgrunnsnotatet gis en beskrivelse av trender og utviklingstrekk ved dagens IKT-risikobilde. Notatet er utarbeidet av Koordineringsgruppen for IKT-risikobildet (Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet). Det anbefales at notatet ses i sammenheng med Nasjonal sikkerhetsmyndighets nasjonale strategi for cybersikkerhet, som er sendt til Justisdepartementet og til Forsvarsdepartementet.

Moderne organisasjonsformer, tett samhandling og ikke minst den gjennomgående bruken av IKT-systemer har gjort samfunnet nettverksbasert. Dagens nettverkssamfunn løser oppgaver på nye og bedre måter, utnytter ressurser mer effektivt, men utviklingen gir samtidig opphav til et nytt risikobilde. Sentralt i denne sammenheng er bruken av IKT-systemer. Avhengigheten av en velfungerende og sikker IKT-infrastruktur har medført at vi er blitt sårbare for uønskede hendelser i denne infrastrukturen.

Norge er i dag et sårbart samfunn. Mye informasjon ligger offentlig tilgjengelig. Det er en kjensgjerning at:

- 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 vil kunne lamme eller påvirke strømforsyning, industriprosesser og andre kritiske samfunnsfunksjoner.
- kriminaliteten på Internett er sterkt økende.
- 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 som står høyt på dagsorden i mange stater og internasjonalt. NATO ser på truslene mot IKT-systemer med økende bekymring, og cyberangrep er nå vurdert som en av de mest alvorlige asymmetriske truslene alliansen og medlemsstatene står overfor. I USA har en rapport fra Det Hvite Hus om cybersikkerhet slått fast at cybersikkerhet utgjør en av de mest alvorlige økonomiske og nasjonale sikkerhetsutfordringer nasjonen står overfor i det 21. århundre.

EOS-tjenestene mener at trusselnivået knyttet til IKT-baserte virkemidler har økt de siste årene. Mange stater er i dag i ferd med å bygge opp etterretnings- og angrepskapabiliteter til bruk i cyberspace. Trusselen er derfor dynamisk og utvikler seg raskt.

I henhold til Politiets sikkerhetstjenestes (PSTs) åpne trusselvurdering er etterretningsaktiviteten mot Norge og norske interesser høy. NSM har erfart at antall målrettede forsøk på dataspionasje har økt kraftig de siste årene.

For effektivt å forebygge og motvirke sikkerhetstruende virksomhet mot den samfunnskritiske IKT-infrastrukturen og informasjon som genereres, lagres eller transporteres i denne, er det viktig at våre nasjonale etterretnings- og sikkerhetsmyndigheter har et realistisk og oppdatert risikobilde.

Nye sikkerhetsbehov

Det norske samfunnet er i økende grad avhengig av IKT-baserte eller IKT-styrte systemer. Både drift og styring av disse IKT-systemene er i stor grad automatisert. I tillegg blir en stadig større del av offentlig kommunikasjon og tjenesteproduksjon konsolidert i felles systemer.

Dette har bidratt til å endre måten individer, organisasjoner og det offentlige samhandler seg i mellom, og med eksterne aktører. Samtidig medfører denne utviklingen økt sårbarhet. Fleksibilitet og høy grad av integrasjon av ulike IKT-systemer innebærer at tradisjonelle sikkerhetsbarrierer svekkes. Integrasjon av flere ulike systemer medfører forhøyet risiko for at både tilsiktede og utilsiktede hendelser i en del av nettverket vil skape vekselvirkninger med andre nettverk og få ødeleggende effekter for IKT-systemet som helhet.

Dette er sårbarheter ved dagens IKT-struktur som trusselaktører kan utnytte for å gjennomføre handlinger som tidligere ikke har vært mulig. Det er derfor trolig at vi i fremtidige interessekonflikter mellom stater, eller mellom stater og ikke-statlige grupperinger vil se økt angrep på, og utnyttelse av IKT-systemer.

Norge har en åpen økonomi og et internasjonalisert næringsliv. Sentrale deler av vår infrastruktur, blant annet innen telekommunikasjon, er i dag internasjonalt orientert. Dette innebærer samtidig at norske borgere og nasjonale interesser kan rammes av konflikter der vi i utgangspunktet er en perifer eller utenforstående aktør. Det er derfor viktig å unngå at Norge oppfattes som, eller reelt sett fungerer som et digitalt fristed for grupper som ønsker å gjennomføre sabotasje mot IKT-nettverk. Ved siden av å kunne stille norske borgere og selskaper til ansvar for handlinger som rammer andre land, eller selskaper og individer utenfor Norge, er det viktig å forhindre at norske IKT-ressurser utnyttes av én eller flere parter i en konflikt utenfor Norge.

Beskyttelse av samfunnets institusjoner og ressurser har tradisjonelt lagt de overordnede rammene for samfunnets sikkerhetstiltak. I dette ligger det overordnede målet om å sikre samfunnets eksistens. Den dimensjonerende trusselen har tradisjonelt hatt form av et militært angrep rettet mot samfunnets styreform, økonomi og naturressurser. En rekke utviklingstrekk, som for eksempel slutten på den kalde krigen og økt globalisering og internasjonal samhandling, innebærer imidlertid at trusselbildets karakterendres.

En effekt av globaliseringen er fremveksten av transnasjonale domener. Disse kommer typisk til uttrykk gjennom bruk av moderne telekommunikasjon, samt økt markedsorientering og transnasjonal organisering av både privat og offentlig tjenesteproduksjon. De transnasjonale domenene utfordrer nasjonal handlefrihet både ved at de er vanskeligere å regulere og begrenser mulighetene til overvåkning. I tillegg gir de transnasjonale domenene trusselaktører nye muligheter til å skjule sine handlinger og spor, blant annet gjennom bruk av stedfortredere og stråselskaper. Situasjonen bidrar samlet sett til et mer uoversiktelig sikkerhetspolitisk bilde.

Beskyttelse av sensitiv informasjon og samfunnskritiske IKT-nettverk mot spionasje og sabotasje er strategisk viktig for samfunnets funksjonsevne.

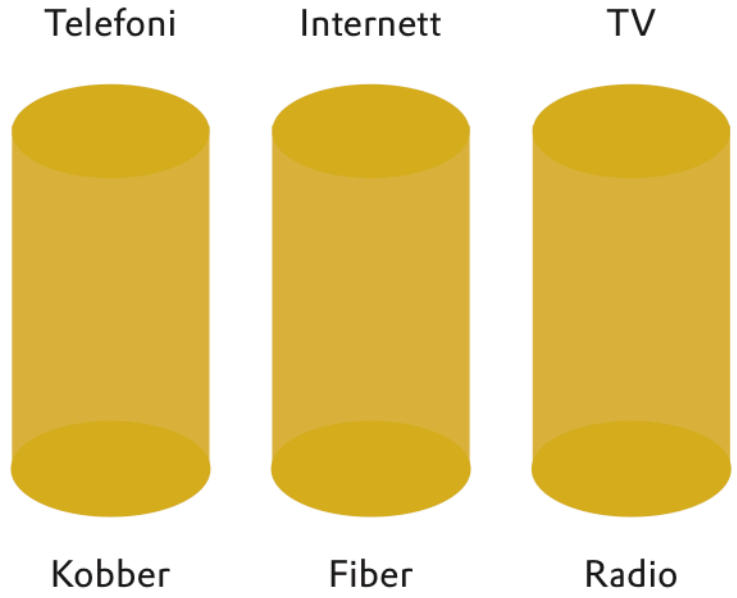
For å ivareta sikkerheten til norske IKT-nettverk er det viktig å balansere mellom å 1) forebygge uønskede og samfunnstruende aktiviteter og hendelser gjennom ulike sikringstiltak, 2) håndtere og begrense konsekvenser av hendelser som likevel inntreffer, og

3) avdekke og motvirke trusler. Behovet for respons må vurderes på grunnlag av de økonomiske, sosiale, politiske virkninger som de ulike truslene kan ha. Prinsippet om proporsjonalitet vil være sentralt også i cyberspace.

En strategi for å beskytte mot de nye truslene bør bestå av flere tiltak. Tradisjonell forebyggende sikkerhet, løpende risikohåndtering og eventuelt speilede mottiltak bør inngå som faste elementer som må bygges ut gjennom mobilisering og samarbeid. Behovene innebærer blant annet oppbygging av sentrale overvåknings- og analysefunksjoner i samvirke med distribuerte sensor- og responssystemer.

Om IKT-infrastruktur

Tradisjonell telekommunikasjon er basert på siloer med nettverk og en tjeneste på topp. Internett, telefon, TV og interne nettverk befant seg ofte på separate fysiske føringsveier hvor de forskjellige tjenestene benyttet sin egen teknologi som bærer.



Figur 1. Tradisjonell kommunikasjonsplattform.

Dette er en kostbar og krevende infrastruktur å vedlikeholde for leverandørene slik at man har sett på måter å integrere alle behov i en løsning med en felles bærer.

Moderne leverandører av tele-/datakommunikasjon bygger i dag sine nettverk med IP (internettprotokoll) som et bindeledd mellom den fysiske infrastrukturen og tjenestene. Det snakkes i denne forbindelse om Next Generation Networking (NGN) der prinsippet er at ett nettverk brukes som bærer for all informasjon og alle elektroniske tjenester (eksempelvis tale, data, og video). Dette er gjort mulig ved at all kommunikasjon i dette nettverket er basert på en felles standard (IP) for overføring av data. "Alt over IP" er også et uttrykk benyttet for å vise transformasjonen mot NGN. Der man tidligere hadde vertikal integrasjon mellom infrastruktureierskap og tjenesteleveranse, har overgangen til IP tilrettelagt for vertikal separasjon mellom disse rollene.

Telenor annonserte i en pressemelding[1] i 2005 at de skulle ha "Alt over IP" innen år 2010. Status er at målet i store trekk er nådd.

Figur 2. Konsolidert kommunikasjonsplattform.

Den nye måten å innrette infrastruktur på innebærer et mer fleksibelt, kosteffektivt og enklere tjenestetilbud. IP-protokollen som bærer av de ulike tjenestene gir bedre mulighet for redundans og om-ruting. Samtidig har infrastrukturens kritikalitet økt som følge av at samfunnet er blitt mer *avhengig* av at den fungerer. Dette har sammenheng med at flere og flere tjenester benytter denne infrastrukturen og et gradvis bortfall av tilgjengelige *alternative infrastrukturer* for å få levert disse tjenestene. Det er videre en *tett kobling* mellom tjenestene, jf. den felles kommunikasjonsstandarden (IP), som fører til at svikt eller bortfall av én tjeneste kan få umiddelbare og alvorlige konsekvenser for andre tjenester. I tillegg til dette har risikoen for kompromittering av data økt, som følge av at sensitiv trafikk overføres på samme fysiske bærer og via samme fysiske nettverksenhet som ikke-sensitiv datatrafikk.

IKT-sårbarhet

IKT-systemer er komplekse systemer som omfatter avansert elektronikk og programvare. Dette gjør det vanskelig å få full oversikt over alle sikkerhetsutfordringene knyttet til IKT.

[1] http://www.telenor.com/no/nyheter-og-media/nyheter/2005/joint-press-release-from-telenor-asa-juniper-networks-and-siemens-communication

Generelt har fokuset på IKT-sikkerhet økt de siste årene, men samtidig har systemene blitt mer komplekse, sammenkoblede og homogene. Store, komplekse IKT-systemer øker muligheten for feil og uønsket tilgang (tilgangspunkt), da det er mer krevende å få en fullstendig oversikt. I større nettverk vil det ofte eksistere datamaskiner og systemer som ikke er tilstrekkelig dokumentert, og som ikke oppdateres og vedlikeholdes i henhold til anbefalte rutiner.

De gjensidige avhengighetene mellom kritiske samfunnsfunksjoner og den økende IKT-sårbarheten kan utnyttes og være en "force multiplier", i den forstand at små og relativt enkle angrep kan få alvorlige og samfunnsmessige konsekvenser. Dette understreker viktigheten av sårbarhetsreduserende tiltak.

En annen utfordring er at stadig flere systemer benytter det samme operativsystemet og den samme programvaren, slik at maskinparken blir veldig homogen. Det er gjerne snakk om kjent teknologi, velkjente programmer, kjente operativsystemer og kjent maskinvare. Konsekvensen blir ofte at dersom en sårbarhet eksisterer i ett system, så vil sårbarheten trolig også være tilstede i alle de andre tilsvarende systemene. Resultatet blir at en trusselaktør kun trenger å fokusere på et fåtall systemer, etter som det er lite variasjon i systemene som benyttes. En større variasjon i systemene vil mest sannsynlig gjøre jobben vanskeligere for en trusselaktør.

Det er ofte et krav i dag om økt tilgjengelighet for den enkelte person i en organisasjon eller bedrift. Mobiltelefoner og datamaskiner kobles opp i nettverk og er alltid tilgjengelige. De fleste enhetene benytter den samme infrastrukturen, og den samme teknologien for kommunikasjon. Tilgjengeligheten kan være en utfordring sikkerhetsmessig, da hver enkelt enhet alltid vil være tilgjengelig for trusselaktøren som ønsker å ta kontroll over dem. Trusselaktøren har god tid til rekognosering og gjennomføring dersom enhetene de ønsker å nå alltid er tilgjengelige.

Kommunikasjonsinfrastruktur

Stadig mer elektronisk utstyr blir utviklet for å kunne kommunisere via internettprotokoll (IP). Flere og flere enheter utvikles for å kunne kommunisere felles over samme kommunikasjonsinfrastruktur. Samtidig er kommunikasjonsinfrastrukturen blitt mer mobil og automatisert. Det oppleves en kraftig vekst i antall brukere av IKT, som følge av at det teknologiske gapet mellom den industrielle verden og utviklingsland er i ferd med å tettes.

Den globale IP-standarden er en bærebjelke i direkte kommunikasjon mellom flere og flere datasystemer. Utviklingen er i stor grad markedsstyrt, og redundans bygges på grunnlag av markedshensyn og i liten grad på myndighetspålagt krav. Systemene er lokalisert på tvers av ulike sektorer, både i private og offentlige.

Kommunikasjonsinfrastrukturen er hovedsakeligavhengig av tre protokoller/tjenester: IP for transport, BGP-4 for ruting og DNS for navngiving. Sårbarheter i disse tjenestene kan utgjøre en vesentlig risiko. For de fleste brukere er funksjonaliteten som ligger innebygd i infrastrukturen ukjent, helt til noe går galt og systemene ikke lenger fungerer. Det ukjente sårbarhetsbildet gjør det vanskelig for brukere å iverksette sikkerhetstiltak.

Utplassering av ny maskin- og programvare, innebærer samtidig introduksjon av nye sårbarheter. Sårbarhetene og svakhetene kan utnyttes av ulike trusselaktører, og bli kilde til nye sikkerhetsutfordringer.

Prosesskontrollsystem

Prosesskontrollsystem er betegnelse på store datasystemer som benyttes for styring og prosesskontroll innenfor mange virksomheter som leverer varer og tjenester, f.eks industrien, kraftproduksjon og distribusjon, olje- og gasssektoren, transportsektoren osv. De binder sammen store, sentrale driftssentraler med de enkeltdelene av de prosessene som skal styres. Tradisjonelt har disse systemene vært isolerte datasystemer, uten tilkopling til eksterne nettverk. Den eneste måten å utføre et anslag mot disse var ved fysisk tilgang. I de senere årene har trenden vært at mange av disse systemene har blitt koblet sammen med bedriftenes øvrige datanettverk, samt direkte til Internett. Dette gjør systemene vesentlig mer sårbare, ved at det kan være mulig å ta kontroll over dem via datanettverkene. Det finnes eksempler på at disse systemene er blitt utsatt for angrep og trusler fra trusselaktører via internett. Systemer som er tilknyttet kritisk infrastruktur har blitt eksponert for trusselaktører. Det er ikke usannsynlig at det kan gjennomføres målrettede sabotasje- eller terrorangrep via internett mot prosesskontrollsystemer, eksempelvis i kombinasjon med fysiske angrep

IKT-trusler

Cyberspace kan betraktes som et kompleks hvor både teknologiske, sosiale, økonomiske, politiske og kulturelle dimensjoner gjør seg gjeldende. Dette betyr at fenomener og trusler som i prinsippet er kjent fra den fysiske verden vil kunne gjenskapes og gjenfinnes i den digitale infrastrukturen.

Trusselkategorier

Trusler kan analyseres ut fra en rekke dimensjoner; motivasjon, metode, verktøy, mål, modus med flere. En trussel skapes av mennesker og kan ses i lys av de kapabiliteter og intensjoner som en aktør besitter. Følgende typeinndeling gir et utgangspunkt for å beskrive trusler i form av ulike fenomener (kategoriene er ikke gjensidig utelukkende):

- Destabiliserende og strategiske angrep
- Politisk, teknologisk og økonomisk etterretning
- Organisert kriminalitet
- Politisk aktivisme
- Opportunistisk vandalisme

Sammenlignet med tradisjonelle konvensjonelle trusler, er det imidlertid svært vanskelig å beskrive, vurdere og håndtere IKT-trusler. Det er flere grunner til dette, bl.a.:

- Trusselutløseren har i stor grad anonymitet i tidsrommet mellom handling, hendelse og effekt. Avansert krypteringsteknologi er gjort allment tilgjengelig og distribueres på internett.
- Politiske og geografiske utfordringer, både i forhold til å forebygge og reagere på angrep. Dette forsterkes av mulighetene for å villede/distrahere gjennom å plante falske spor.
- Hurtig teknologisk utvikling, innebærer at så snart man oppdager og publiserer en sårbarhet, så utvikles det teknologi som kan utnytte disse sårbarhetene.
- Det er lave kostnader og enkelt å tilegne seg de nødvendige midlene for et angrep.
- Angrep er blitt mer automatiserte.

IKT-angrep vil være et svært effektivt virkemiddel i en konflikt, nettopp fordi det er vanskelig å reagere på en hensiktsmessig måte mot slike angrep og på grunn av skadepotensialet ved slike angrep. Det hersker en del usikkerhet mht. utvikling av kapasiteter, men det er en kjensgjerning at flere land utvikler angrepskapasiteter for å kunne utføre IKT-angrep. Det som gjør denne utviklingen bekymringsfull er at det ikke eksisterer internasjonale avtaler som regulerer slik våpenteknologi og heller ikke mekanismer for å sikre gjensidig avskrekking slik det var under den kalde krigen.

Det er en bekymring i cybersikkerhetsmiljøer i mange land at beskyttelsestiltakene ikke synes å stå i proporsjon til truslene fra høykapasitetsaktører.

Angrep eller fare for angrep vil kunne skape betydelig frykt i samfunnet, og i ytterste konsekvens true liv, helse og velferd, økonomisk stabilitet, eller andre grunnleggende verdier.

Politisk, teknologisk og økonomisk etterretning i form av skjult og plantet informasjonsinnhenting innebærer forsering av systembarrierer og planting av fremmed kode. Formålet er innsamling og formidling av informasjon uten at operasjonen avsløres. Også i Norge finnes etter hvert flere eksempler på operasjoner som det antas er utført av fremmede stater, eller som ledd i fremmede staters interesser. Bruk av flyttbare medier (typisk USB minnepinner) på lukkede systemer er en sårbarhet som utgjør en mulig smitte- og transportkanal.

IKT har gitt nye instrumenter for organisert kriminalitet. Organisert kriminalitet har økonomisk vinning som hovedformål, og omfatter blant annet utpressing, tyveri, svindel og smugling. Organisert kriminalitet bør derfor bekjempes ikke bare ut fra økonomisk omfang, men i stor grad også på basis av det generelle potensialet for undergravende virksomhet, og faren for nye trusselkonstellasjoner.

Politisk aktivisme har i denne sammenheng så langt hovedsaklig gjort seg gjeldende ved hendelser med politisk eller sosial uro. I særlig grad har hensikten vært å vise misnøye ved å nekte eller forstyrre tjenestetilgangen og bringe oppmerksomhet til den politiske agendaen. Skadeomfanget må sies å være begrenset, og virkningene er i hovedsak å finne på det psykologiske planet.

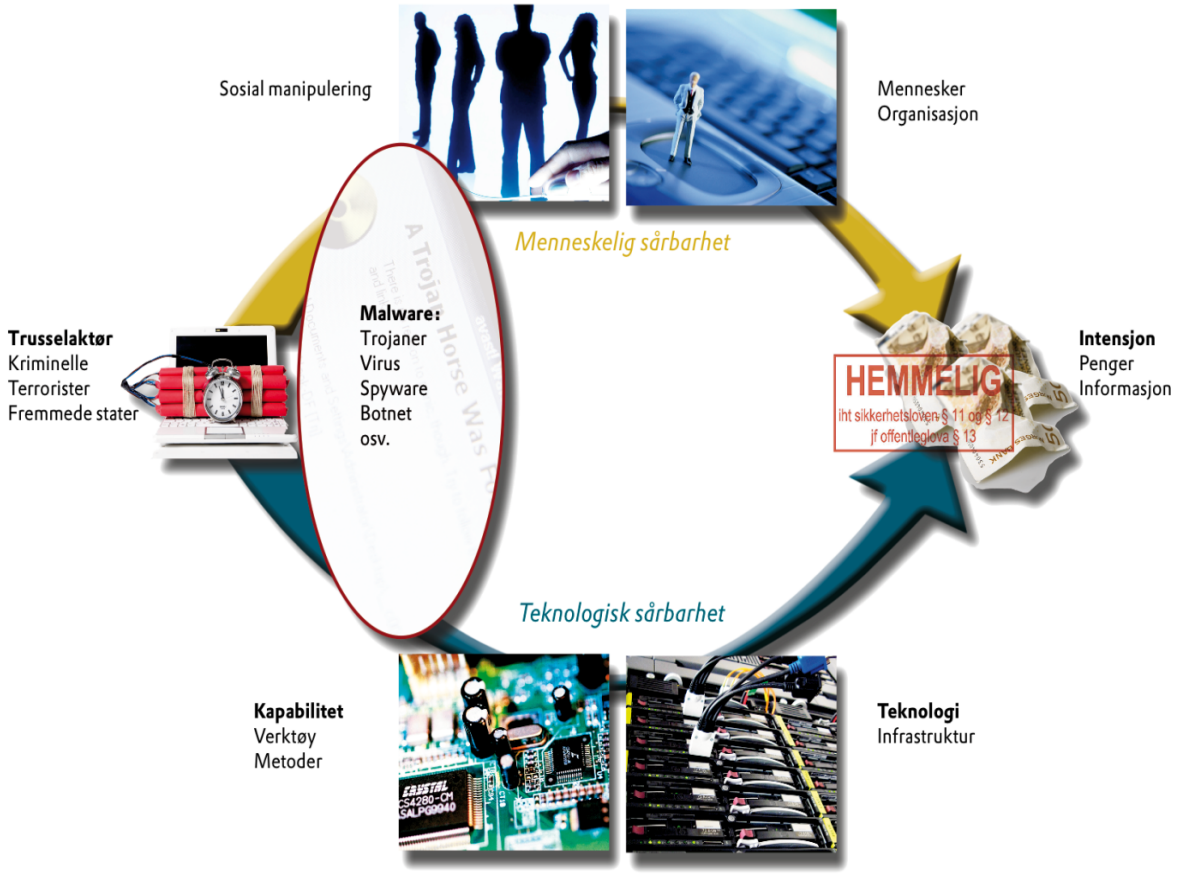
Opportunistisk vandalisme er her ment som betegnelse på asosial eller destruktiv adferd. Kriminalisering vil kunne ha en viss effekt som mottiltak. I tillegg må samfunnet innrettes slik at slik adferd fanges opp i skole og annet forebyggende arbeid.

Felles for disse truslene er at de utnytter ulike sårbarheter og svakheter – både menneskelig og teknisk. Et viktig unntak er såkalte overfyllingsangrep som medfører tjenestenekt.

Anvendelse av omfattende destruktive angrep kan så langt ikke påvises, og bør foreløpig antas som teoretiske fenomener. Eventuell anvendelse vil være ledsaget av usikkerhet og andre operasjonelle begrensninger, og det er vanskelig å hevde faktisk og fremtidig bruk ved vurderinger av trusselbildet. Informasjonsinnhenting, kriminalitet, aktivisme og vandalisme er derimot dagligdagse hendelser og utgjør vedvarende sikkerhetsutfordringer.

Trusseltypene kan karakteriseres som ulike poler i et risikobilde. Angrep representerer konseptuelt alvorlige, men sjeldent forekommende ekstremtilstander som krever ekstraordinær innsats for håndtering og bekjempelse. Kriminalitet, aktivisme og vandalisme opptrer langt hyppigere, og mottiltak bør ligge innenfor rammen av samfunnets ordinære innsats.

Det oppdages et økende antall aktiviteter og operasjoner med høy alvorlighetsgrad. Det er grunn til å fremheve informasjonsinnhenting og organisert kriminalitet som de viktigste truslene.



Figur 3. Sammenheng mellom trusler og sårbarhet.

Angrepsvektorer

Sårbarhetene som utnyttes for å oppnå ønsket målsetning kan generaliseres i to hovedkategorier, teknologisk og menneskelig sårbarhet. Trusselaktører bruker forskjellige metoder for å utnytte disse sårbarhetene, og ofte brukes flere sårbarheter i samme operasjon.

Sosial manipulering

Sosial manipulering er teknikker som benyttes for å manipulere mennesker til å gi fra seg informasjon (brukernavn, passord, og lignende) eller utføre handlinger som de normalt ikke ville ha gjort. En trusselaktør kan manipulere mennesker gjennom å utnytte deres tillit til systemet, organisasjonen eller enkeltpersoner. Ved å utgi seg for å være en annen person, og ved å konstruere en situasjon der mange vil føle at de er nødt til å oppgi sensitive opplysninger, kan trusselaktører tilegne seg sensitiv informasjon.

E-post

Å sende en e-post med et vedlegg som inneholder skadelig kode til en bestemt mottaker, er en vanlig metode for å kompromittere datamaskiner og tilegne seg informasjon. E-posten inneholder ofte en interessant tekst som gjør at mottakeren ønsker å åpne vedlegget. Når vedlegget åpnes vil skadevare forsøke å kompromittere maskinen. Dersom maskinen

kompromitteres vil det ofte legges inn en skjult bakdør, som innebærer at trusselaktøren har full tilgang til maskinen.

Nettsider

Trusselaktører ønsker ofte å spre skadevare til flest mulig datamaskiner på Internett. En effektiv måte å gjøre dette på er å kompromitterte populære nettsider og legge inn skadelig kode som deretter spres gjennom nettsidebesøk. Enkelte nettsider har flere millioner unike besøkere hver uke, og det er potensielt mulig å kompromittere tusenvis av datamaskiner på denne måten.

USB-enheter

Det er stadig mer utbredt at USB-enheter, som for eksempel minnepinner, utnyttes for å distribuere skadelig kode. Sårbarheten ved spredning av kode via USB-enheter er spesielt utfordrende da slike enheter fysisk kan bæres på innsiden av sikkerhetsbarrierer som er ment å motvirke kompromittering. På denne måten kan USB-enheter med skadelig kode føre til kompromittering av lukkede nettverk. Når USB-enheten er koblet til det lukkede nettet vil koden kunne være programmert til å skanne og lagre informasjon, og når enheten er koblet til et internett-tilknyttet nett vil den lagrede informasjonen kunne eksfiltreres via internett.

Teknikker

Det er flere ulike teknikker som benyttes av trusselaktører. Noen av disse er nevnt nedenfor:

Filformater

Det har vært flere kjente sårbarheter i filformater, slik som dokumenter av typen Word, Excel, PowerPoint og PDF. Sårbarhetene har gjort det mulig for trusselaktører å legge inn skadelig kode i dokumentene. En vanlig teknikk er å modifisere et dokument ved å legge inn skadelig kode som er skreddersydd til å utnytte sårbarheten. Deretter sendes dokumentet som et vedlegg til en bestemt mottaker. Dersom mottakeren åpner dokumentet, og vedkommende har en sårbar versjon av programmet som skal behandle dokumentet, så vil den skadelige koden kjøres og mottakerens datamaskin blir kompromittert. Det har vært en rekke ulike sårbarheter i filformater den siste tiden, som har gjort denne teknikken spesielt populær.

Verktøykasser

En verktøykasse i IKT-sammenheng er en programpakke som inneholder flere programmer som er nyttige ved gjennomføringen av en operasjon. En slik programpakke kan som ofte hentes ned fra Internett, og dette forenkler operasjonen betraktelig. En slik verktøykasse inneholder gjerne verktøy for å kartlegge offeret, utnytte, ta kontroll over, og deretter å administrere de kompromitterte datamaskinene. Det finnes en rekke ulike verktøykasser tilgjengelige i dag, hvorav flere trolig er utviklet av profesjonelle, og som ikke krever omfattende teknisk kunnskap for å benytte dem.

Botnettverk (botnet)

Et botnet er en betegnelse på flere datamaskiner som er kompromittert, koblet sammen via en form for kontrollmekanisme, og under eierskap og styring av en uvedkommende aktør. Typisk kompromitteres tusenvis av datamaskiner gjennom vedlegg i e-post, eller via mye besøkte nettsider. Botnet-eieren kan gi instruksjoner til maskinene i botnettverket. Det kan for eksempel være å angripe andre system, eller å hente ut alle dokumenter som er tilgjengelig på maskinen. Botnet kan også benyttes til distribuerte tjenestenektangrep som blokkerer internettforbindelsen til andre brukere på Internett.

Kapabilitet

Kapabilitet sier noe om en trusselaktørs evne til å gjennomføre en operasjon.

Det observeres i dag operasjoner og angrep av svært ulikt teknisk nivå. Hvor teknisk avansert de er, sier sjelden noe om i hvilken grad de er vellykkede. Med andre ord kreves det ikke nødvendigvis store ressurser for å kunne utføre en vellykket operasjon eller angrep.

Også i målrettede operasjoner observeres det tilfeller hvor det benyttes lite sofistikert teknologi. På tross av dette er operasjonene overraskende ofte vellykkede. Det kan være e-poster som inneholder skadelig kode i vedlegg, eldre sårbarheter hvor det eksisterer sikkerhetsoppdateringer, sosial manipulering der brukeren selv er med på å kompromittere sin egen datamaskin og lignende.

Det dukker stadig opp innovative løsninger og forbedringer i måten operasjonene utføres. Bruk av kryptering har vært lite utbredt, men har i større grad blitt tatt i bruk i nyere versjoner av skadelig kode.

Trusselaktørene ser ut til å ha en større evne til å håndtere store operasjoner og administrere store datamengder. En del skadelig kode driver informasjonsinnsamling i stor skala, og dette setter store krav til håndtering av data i store databaseløsninger. Den stjålne informasjonen kategoriseres og kan eventuelt selges basert på hva kundene er ute etter. Hvordan og hvilke data som brukes varierer mellom de ulike trusselaktørene.

Mål

En datamaskin eller et datasystem som blir kompromittert trenger ikke å være det endelige målet, men inngå som en ressurs og et trinn i en større operasjon.

Alle er i utgangspunktet utsatt for trussel om kompromittering. Hver datamaskin som er tilknyttet Internett har en potensiell verdi. Datamaskinen kan blant annen benyttes som mellomledd i videre operasjon eller angrep, lagringsplass for ulovlige filer, tyveri av bankopplysninger og mye annet.

I forbindelse med målrettede operasjoner, er det noen aktører i samfunnet som er spesielt utsatt. Nedenfor er det listet noen av målene som operasjonene ofte er rettet mot.

- Ledere på ulike nivåer som innehar viktig informasjon.
- Forsvarssektoren med underleverandører (konsulentselskaper og lignende)
- Høyteknologiske selskap innen elektronikk-, forsvar-, fly-, farmasøytisk og petrokjemisk industri.
- Alle virksomheter med konkurransefortrinn, eller spisskompetanse innefor et område.
- Organisasjoner eller personer som besitter personsensitiv informasjon, som for eksempel menneskerettighetsorganisasjoner og advokater, og andre politisk interessante virksomheter.

Erfaringer fra IKT-hendelser og øvelser

Basert på informasjon fra EOS-tjenestene presenteres noen erfaringer fra IKT-hendelser og øvelser.

Målrettede operasjoner

I løpet av de siste årene har NorCERT håndtert en rekke alvorlige saker som involverer informasjonsinnsamling med målrettede trojanere. I Norge har flere virksomheter og flere toppledere innenfor både offentlig og privat sektor blitt utsatt for målrettede operasjoner. De mest alvorlige av disse sakene har blitt løftet fra å bli håndtert av NorCERT alene til å bli håndtert i felleskap mellom EOS-tjenestene.

Målrettede trojanere sendes ofte skjult i vedlegg til e-post. En trojaner er skadelig kode som ofte forsøkes gjemt i eller blant annen programvare. Et eksempel kan være programkode gjemt i et Word-dokument. Trojanere bringer ofte med seg en skjult bakdør inn i en datamaskin. Dokumenter og programmer kan deretter transporteres inn eller ut av datamaskinen uten at dette oppdages. De rammer som regel en liten og klart definert målgruppe. Trojanere er gjerne designet for å stjele sensitiv informasjon. I de mest sofistikerte tilfellene er programkoden i trojaneren skreddersydd for spesifikke operasjonen mot en begrenset målgruppe.

Denne typen operasjoner foregår i all hovedsak mot nettverk som ikke er sikkerhetsgraderte, men som inneholder sensitiv informasjon. Siden 2007 har det vært noen hendelser hvor USB-media brukes som en komponent i operasjonene, for å få tilgang til sikkerhetsgraderte systemer eller andre fysisk adskilte datanettverk.

Det er vanskelig å si noe bestemt om hvem som står bak i hvert enkelt tilfelle, uten en grundig analyse.

Store tjenestenektsangrep

Høsten 2007 ble to viktige Telenor-kunder utsatt for et stort tjenestenektangrep. Dette resulterte i en kraftig økning i trafikken over Telenors kjernenett. Fra et teknisk perspektiv var dette et langt mer alvorlig angrep enn angrepet mot Estland i 2007, som fikk stor oppmerksomhet internasjonalt og i media.

Med 20 internettlinjer på 1 Mbit/s som er sårbare for DNS-amplifikasjonsangrep kan en trusselaktør generere 1,5 Gbit/s med angrepstrafikk. De fleste virksomhetene i Norge har ikke mer enn 100 Mbit/s og med et slikt angrep kunne man tatt ut de fleste bedriftene i Norge fra Internett. Det finnes mange systemer på Internett som er sårbare og som kan brukes til å utføre denne typen angrep.

Det største angrepet som NorCERT kjenner til internasjonalt var 80 Gbit/s, og var så kraftig at det påvirket transatlantisk datatrafikk.

Det er billig og enkelt å utføre store tjenestenektsangrep, men slike angrep tiltrekker seg mye oppmerksomhet og kriminelle trusselaktører som besitter denne kompetansen bruker det i begrenset omfang. De er selv avhengig av IKT-infrastrukturen for å tjene penger og utfører heller mindre tjenestenektsangrep.

Rett før kommune- og fylkestingsvalget i 2007 ble et norsk politisk parti offer for et tjenestenektsangrep mot en av sine nettsider. Tjenestenektsangrepet ble sporet tilbake til stort botnettverk, kalt Storm. Det var et av de store nettverkene i 2007, men har siden blitt erstattet av andre. Et direktorat i Norge ble videre utsatt for et distribuert tjenestenektsangrep i 2008. NorCERT analyserte angrepet og koblet det til et kjent botnettverk som stadig utfører tjenestenektangrep mot ulike nettsider verden over. Det interessante for denne saken er at noen dager før tjenestenektsangrepet ble det spurt på et diskusjonsforum om noen kunne utføre et tjenestenektsangrep mot direktoratets nettsider.

Foruten tjenestenektsangrep mot offentlig forvaltning har også andre norske virksomheter blitt utsatt for slike angrep. Det eksisterer mange store botnettverk som til enhver tid utfører tjenestenektsangrep. Også norske nettsider utsettes til stadighet for slike, ett eksempel er angrepet som tok ned Dagbladet etter publiseringen av en Muhammed-karikatur i februar 2010. Dette er relativt små angrep som ikke har alvorlig innvirkning på kritisk infrastruktur, og håndteres av sluttkunde eller tjenesteleverandørene selv.

Banktrojanere

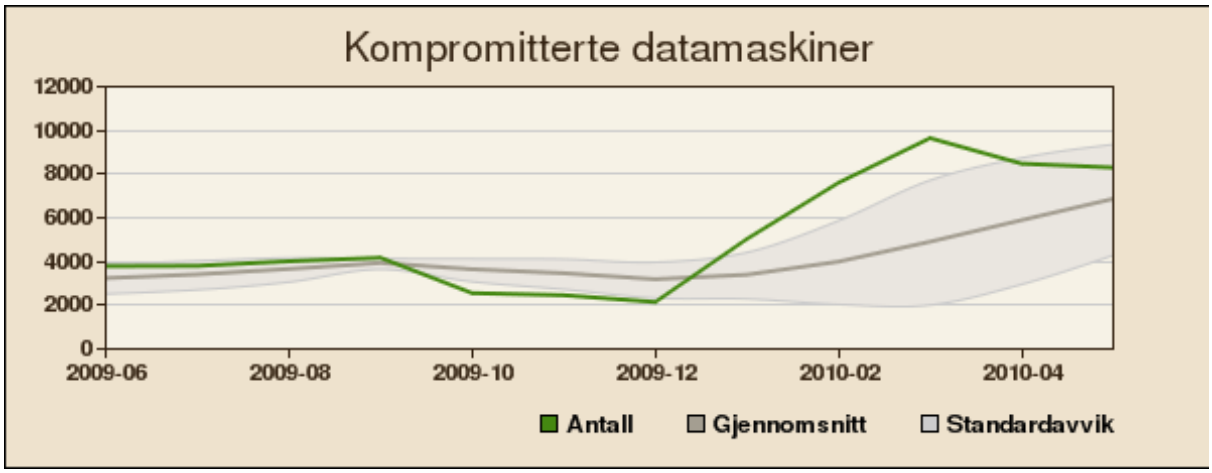
Det finnes trojanere eller skadelig programkode som er spesielt rettet mot bank- og finansnæringen. Disse trojanerne blir ofte omtalt som banktrojanere fordi de brukes til å stjele fødselsnummer, kontoinformasjon og passord fra bankkunder, for deretter å bruke denne informasjonen til å svindle nettbanker.

Norske banker bruker nå for det meste to-faktor autentisering for at kunder skal kunne logge seg inn i sin nettbank. To-faktor autentisering vil si at det benyttes minst to informasjonselementer til identifikasjon og autentisering av brukere. I norske nettbanker benyttes ofte en elektronisk kodebrikke i tillegg til et passord. Flere av banktrojanerne som finnes i dag har mulighet til å omgå to-faktor autentisering med relativt enkle grep.

Banktrojanere også har vært rettet mot norske banker, men majoriteten av banktrojanerne er fortsatt rettet mot større markeder i utlandet. Enkelte av banktrojanerne er en del av verktøykasser (kits) som gjør at den skadelige koden kan tilpasses målet trusselaktøren ønsker å utnytte, som også kan være norske banker. NorCERT kjenner en rekke saker hvor norske datamaskiner har vært kompromittert med banktrojanere.

Kompromitterte datamaskiner

NorCERT mottar fortløpende informasjon fra samarbeidspartnere om norske kompromitterte datamaskiner. Den største andelen gjelder brukermaskiner som har blitt kompromittert med en skadelig kode, og som er en del av et botnett. Se figur 4 som viser en oversikt over kompromitterte datamaskiner i Norge som ble håndtert av NorCERT i 2009.



Figur 4. Antall kompromitterte datamaskiner per måned, hentet fra NorCERTs saksbehandlingssystem

Mange av botnettverkene brukes til å sende store mengder søppelpost, som kan inneholde informasjonsstjelende trojanere eller brukes til svindel og ID-tyveri. Kompromitterte maskiner i et botnettverk kan også benyttes til å utføre distribuerte tjenestenektsangrep mot forskjellige nettsider, slik at disse nettsidene ikke lengre er tilgjengelige for normale brukere.

Mange kompromitterte nettsider brukes til såkalte ”phishing”, hvor målet er å lure brukere til å oppgi personinformasjon og passord. Dette gjøres for eksempel ved å presentere en falsk nettside som utgir seg for å være en nettbank. NorCERT har kjennskap til tilfeller der også norske nettbanker har blitt brukt i phishing-angrep mot norske kunder.

Nettsidehærverk

Norske nettsider er ikke forskånet fra nettsidehærverk hvor trusselaktøren forandrer utseende til nettsider. Enkelte trusselaktører utfører nettsidehærverk for å demonstrere sine ferdigheter for andre i undergrunnsmiljøene, men nettsidehærverk har også blitt benyttet i politisk konflikter for å ødelegge for motstanderne. Det har foreløpig vært relativt få store norske nettsider som har blitt offer for nettsidehærverk.

Etter Dagbladets trykking av en Muhammed-karikatur tidlig i februar, ble et hundretalls norske nettsider vandalisert med et politisk budskap. Forsiden på nettsidene ble byttet ut med en advarende tekst og signert med ”1923TURK-GRUP”.

Elektronisk forvaltning

Flere store offentlige virksomheter har ved feil distribuert CD-ROM-plater inneholdende fødselsnummer. Når personsensitiv informasjon er elektronisk tilgjengelig øker også faren for at andre sensitive data kan komme på avveie eller misbrukes. Spesielt hvis informasjonen er tilgjengelig på elektroniske medier, som USB-minnepenner, eller på bærbare datamaskiner som mistes eller stjeles. Det har også vært et tilfelle hvor en mobiloperatør hadde sikkerhetshull på sine nettsider som gjorde det mulig å hente ut personnummer. Også utdanningsinstitusjoner har hatt tilfeller hvor personopplysninger har vært allment tilgjengelig på Internett.

Øvelser

Det har vært gjennomført en rekke øvelser nasjonalt og internasjonalt de senere år. Under følger en kort oppsummering av erfaringer fra den siste tids øvelser nasjonalt og internasjonalt.

IKT 08

I 2008 ble det gjennomført en sivil nasjonal øvelse som hadde til hensikt å øve etater og private virksomheter innenfor hovedsaklig finans-, kraft- og telekomsektoren. Scenarioet som ble øvd var knyttet til et samordnet og massivt angrep på IKT-infrastruktur gjennom Internett, og delvis ved hjelp av interne utro tjenere. Hendelsene var rettet mot norske ISPer, norske myndigheter og selskaper med kritiske samfunnsfunksjoner. Selv om det i sluttrapporten konkluderes med at samfunnet vil være rustet til å møte hendelser som den som ble øvd, ble det identifisert en rekke forbedringspunkter.

Én av utfordringene er tilstrekkelig situasjonsforståelse ved hendelser som rammer bredt. Spillmedia bidro i stor grad til situasjonsbildet, mens innrapportering var vanskelig å få til (særlig fra offentlige etater og myndigheter). Samordningsbehovet viste seg å være stort, og øvelsen bidro til å synliggjøre behovet for koordinering og informasjonsutveksling på tvers av sektorer. Sluttrapporten konkluderte med at det ved særlig komplekse og tverrsektorielle kriser er behov for å peke ut et tydelig lederdepartement. En annen viktig erfaring var at gjeldende beredskapssystem (SBS) er lite hensiktsmessig i hendelser som dette, og at planverket bør revideres og oppdateres. Sluttrapporten vektlegger behovet for gjennomgang av sentrale problemstillinger knyttet til ansvar, roller og informasjonsflyt i en krise som rammer store deler av samfunnet samtidig.

Det var også et forbedringspotensial med hensyn til sektorvise tiltak som opprettelse av sektor-CSIRT og nødvendigheten for en beredskapsorganisasjon i de enkelte organisasjoner. Forhåndsutpekte og tydelige kontaktpunkter mangler, og spesielt med hensyn til kommunikasjon med gradert eller sensitiv informasjon er sikker distribusjon vanskelig å få til.

NATO Cyber Defence Exercise 2009

Høsten 2009 ble NATOs Cyber Defence Exercise 2009 gjennomført. Erfaringene fra forberedelsene og gjennomføringen av denne øvelsen avdekker et behov for å gjennomføre flere internasjonale øvelser i regi av NATO. Dette kan ha sammenheng med at det er en relativt ny type øvelse, og at ansvarsforholdet for Cyber Defense ikke er tilstrekkelig klargjort i deltakerlandene.

Forberedelsene til det nasjonale spillet i Norge viser behov for klarere ansvarsforhold, og nødvendigheten av å foreta egne øvelser innenfor forsvarssektoren. Øvelsen avdekket også et behov for bedre krisekommunikasjonsløsninger mellom virksomheter og mellom sektorene, spesielt ift deling av gradert informasjon. Videre er erfaringsgrunnlaget med hensyn til operativ hendelseshåndtering sterkt begrenset. Øvelsen viser så langt at deltakelse gir trening og kunnskap til å håndtere reelle hendelser.

Cyber Storm II

Cyber Storm II var en stor IKT-sikkerhetsøvelse i regi av US Department of Homeland Security, National Cyber Security Division, og ble arrangert våren 2008. Dette var den største myndighetssponsede IKT-øvelsen i sitt slag, og NSM deltok som observatør.

Aktørene deltok i øvelsen fra sine egne kontorer eller operasjonssentre. Øvelsen tok utgangspunkt i et angrep på virksomheter innen informasjonsteknologi, kommunikasjon, kjemikalier og transport (jernbane og gassledninger). Øvelsen hadde en varighet på fire dager (11.-14. mars 2008), og involverte flere tusen deltakere i fem land. Et hovedmål var å styrke nasjonale IKT-forberedelser og responskapasiteter gjennom å øve de deltakende virksomhetenes planverk, prosesser og prosedyrer i forhold til å oppdage og respondere på IKT-hendelser som rammet kritisk IKT-infrastruktur.

Noen av erfaringene som kom fram under øvelsen var følgende:

Effektiv respons økes ved rutinemessig gjennomgang og testing av prosedyrer og planer for hendelses- og krisehåndtering. God kommunikasjon mellom aktører forut for en krise vil styrke håndteringen under en krise. Prosedyrer for krisekommunikasjon, med kontaktpunkter, må være formalisert i planverket. IKT-kriser krever en etterfølgende respons som tar hensyn til mange gjensidige avhengigheter. Å fastsette grenser for intern rapportering og ekstern varsling styrker effektiv hendelseshåndtering ved å skape større situasjonsforståelse.

IWWN COMEX/ALEX Quick response

Øvelsen IWWN COMEX/ALEX QUICK RESPONSE ble arrangert i perioden 23.-30. Mars 2009, og ble arrangert av NSM ved NorCERT i samarbeid med SITIC (den nasjonale CERTen i Sverige). Øvelsen ble arrangert for medlemmene i IWWN, International Watch and Warning Network. Dette var en alarm- og kommunikasjonsøvelse, hvor målet var å informere, kommunisere og respondere ved en IKT-krise.

Erfaringene fra øvelsen viser at det varierer i hvilken grad kontaktpunktene i ulike land er tilgjengelige under en krise. Informasjon via e-post blir ikke alltid lest, og informasjonen blir ikke nødvendigvis mottatt. Dette gjelder også informasjon sendt i forkant av øvelsen. I en krisesituasjon vil kontakt via telefon trolig være det mest effektive både med tanke på hurtig respons og forsikring seg om at informasjonen har blitt mottatt.

Koordineringsgruppen for IKT-risikobildet

Koordineringsgruppen for IKT-risikobildet består av:

- Etterretningstjenesten (E) med nasjonalt ansvar for å utarbeide trusselvurderinger knyttet til utenlandske trusselaktører.
- Politiets sikkerhetstjeneste (PST) med ansvar for å forebygge og etterforske alvorlig kriminalitet som gjelder nasjonens sikkerhet, herunder lovbrudd knyttet til terrorvirksomhet, ulovlig etterretningsvirksomhet, spredning av masseødeleggelsesvåpen og av utstyr, materiale og teknologi for produksjon og bruk av slike våpen, samt voldelig ekstremisme. Tjenesten har videre et særlig ansvar for å forebygge trusler som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.
- Nasjonal sikkerhetsmyndighet (NSM) med nasjonalt ansvar for beskyttelse og sikring av skjermingsverdig informasjon og objekter mot sabotasje, spionasje og terrorisme. NSM har ansvaret for NorCERT, som er Norges nasjonale senter for å håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.

I Norge er det Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E) som har ansvaret for å utarbeide trusselvurderinger for henholdsvis indre og ytre forhold. Nasjonal sikkerhetsmyndighet (NSM) ble ved etableringen av NorCERT-funksjonen (jf St.prp. nr.1 (2005-2006) for Moderniseringsdepartementet) og senere gjennom årlige iverksettingsbrev pålagt å holde og utvikle et oppdatert nasjonalt IKT-trusselbilde. Denne oppgaven er også beskrevet i Stortingsmelding 22 (2007-2008). Det forutsettes i nevnte stortingsmelding at dette arbeidet skal utføres i et nært samarbeid med de øvrige EOS-tjenestene.

Formålet med å etablere og vedlikeholde et oppdatert IKT-risikobilde er å gjøre tjenestene bedre i stand til å håndtere hendelser når de oppstår, samt å gi beslutningstakere et best mulig grunnlag for å iverksette tiltak.

Koordineringsgruppen for IKT-risikobildet er kontakt- og koordineringspunkt ved alvorlige hendelser relatert til IKT-sikkerhet. I tillegg til å behandle henvendelser løpende vil EOS-tjenestene ved behov etablere en ”utvidet gruppe” for å behandle og informere om viktige hendelser. Koordineringsgruppen for IKT-risikobildet samarbeider tett med aktører innen fagområdet både nasjonalt og internasjonalt.

Termer og definisjoner

Term	Definisjon	Kilde
Angrep	Vanligvis to, delvis overlappende betydninger: 1) Alle villede og rettede eksterne hendelser som reelt eller potensielt undergraver, krenker eller korrumperer systemets integritet 2) Aggressiv, offensiv, skadepåførende operasjon av en viss intensitet og frekvens som søker å realisere et overordnet mål Den ene eller andre betydningen vil oftest fremkomme av konteksten. På sikt bør betydningen i større grad harmoniseres med juridisk og folkerettslig bruk.	Egen[2]
Angrepsvektor	Kjede av suksessiv sårbarhetsutnyttelse som kan anvendes ved gjennomføring av angrep	Egen
Botnett	Nettverk av datamaskiner som er kompromittert av skadevare med dedikert funksjonalitet. Hver enkelt programvarero*bot* kommuniserer med en sentral styringsfunksjon (kommando- og kontrollnode).	Egen
CSIRT	Computer Security Incident Response Team (CSIRT) er en ekspertgruppe for håndtering av IKT-sikkerhetshendelser.	Egen
Cyber-	(en), kyber- (no), prefiks av Κυβερνήτης [kybernētēs] (gr) styrmann	Wikipedia (en), SNL[3]
Cyberspace	Betegnelse på en informasjonsteknologisk mediert virkelighet formet gjennom digital representasjon, kommunikasjon og presentasjon hvor systemer og infrastruktur i økende grad består av felles teknologi, tjenester og komponenter.	Egen
Cybersikkerhet	Cybersikkerhet omfatter tiltak for beskyttelse mot reelle og potensielle trusler som kanaliseres via IKT-infrastruktur. Cybersikkerhet er en underkategori til IKT-sikkerhet. IKT-sikkerhet favner et mer generelt og bredere spekter av farer og trusler, inkludert naturkatastrofer, uhell og fysisk ødeleggelse. Cybersikkerhet i nasjonal kontekst kan muligens i noe	Egen

[2] "Egen" innebærer at definisjonen et utarbeidet av Koordineringsgruppen for IKT-risikobildet eller en av de tre EOS-tjenestene
[3] Store Norske Leksikon - nettutgave

	større grad enn IKT-sikkerhet hevdes å være spesifikt orientert mot samfunnssikkerhet. IKT-sikkerhet vil på sin side være mer spesifikt egnet som adresse for tiltak knyttet til ivaretakelse av menneskelig sikkerhet.	
Defacement	Se nettsidehærverk.	Egen
Infeksjon	Infiltrasjon av fremmed og skadelig kode (skadevare) i et datamaskinsystem.	Egen
Integritet	Sikring mot fortsettlig eller uaktsom endring, tap eller ødeleggelse av systemets funksjoner eller systembåret informasjon. Systemintegritet kan også sies å omfatte virkemåte, funksjonsdyktighet, troverdighet og/eller styringsmodell.	Egen
Kompromittering	Kompromittering vil si å skaffe uautorisert tilgang til kommunikasjons- eller informasjonsinnhold, eller påføre tap, skade eller ødeleggelse av et systems virkemåte og integritet.	Egen
Konfidensialitet	Sikring mot kompromittering eller uautorisert innsyn i systemets funksjoner, systembåret informasjon eller systemets informasjonsflyt.	Egen
Malware	Av (en) malicious software. Se *skadevare*.	Egen
Nettsidehærverk	Skadetilføyelse på nettside som innebærer at visningen endres.	Egen
Offensiv operasjon	En offensiv nettverksoperasjon omfatter én eller flere av følgende aktiviteter; 1) rekognosering, 2) infiltrasjon, 3) implantering, 4) informasjons-innhenting, 5) ødeleggelse, skadepåføring, disrupsjon eller nektelse, og 6) villedning.	Egen
Operasjon	En sammenhengende og avgrenset serie av aktiviteter som har til hensikt å oppfylle et definert mål. Mer generelt kan operasjon forstås som ett av flere prinsipper eller kategorier for organisering av virksomhet. Øvrige virksomhetskategorier kan for eksempel være aktivitet, prosjekt og daglig virksomhet.	Egen
Risiko	Kombinasjon av sannsynligheten for at en uønsket hendelse skal inntreffe og konsekvensen av den svikt som oppstår, det vil si skadeomfang.	Egen
Risikobilde	…en nyansert fremstilling av risiko med hensikt å gi brukere og beslutningstakere et mest mulig komplett bilde av alle risikoforhold som er av betydning for den aktuelle virksomheten/aktiviteten	NFR[4]
Sikkerhetstilstand	Med sikkerhetstilstanden menes i hvilken grad det man ønsker å beskytte (for eksempel informasjon, objekter,	Egen

[4] Norges forskningsråd (ROS-definisjoner)

	personer eller funksjoner) er identifisert og eventuelt klassifisert, og i hvilken grad forebyggende sikkerhetstiltak er iverksatt i virksomhetene og virker som forutsatt.	
Sikkerhetstiltak	Med forebyggende sikkerhetstiltak menes tiltak som skal skjerme mot sikkerhetstrusler og andre uønskede hendelser, samt tiltak for å avdekke slike hendelser, reagere og gjenopprette sikkerheten. Tiltakene kan være av administrativ, personellmessig og teknisk art. Tiltakene kan i enkelte tilfeller være pålagt, i andre tilfeller kun anbefalt. En forutsetning for alt sikkerhetsarbeid er at man er bevisst hvilken skade som kan oppstå om trusler og andre uønskede hendelser inntreffer. Med defensive sikkerhetstiltak menes tiltak som iverksettes for å skjerme mot anslag eller som reduserer muligheten for at sikkerhetsbrudd vil inntreffe som følge av teknisk eller menneskelig svikt.	Egen
Skadevare	Kompromitterende kode som har infisert eller blitt implantert i et datamaskinsystem.	Egen
Skadeverk	Skadetilføyelse på annen manns system eller informasjonsobjekt, inkludert manipulasjon, endring og sletting av data, og endring av virkemåte eller systemtilstand. Jmf *vandalisme*.	SNL, egen
Sårbarhet	En svakhet som reduserer eller begrenser evnen til å motstå et angrep som kan eller vil negativt påvirke en verdi, eller til å gjenopprette en ny stabil tilstand dersom en uønsket hendelse inntreffer.	Egen
Tilgjengelighet	Sikring mot fortsettlige, uaktsomme eller tilfeldige avbrudd, feil eller nektelser i systemets funksjoner.	Egen
Trusselaktør	Entitet som utgjør en reell eller potensiell trussel mot et identifiserbart mål eller i en avgrenset og identifiserbar sammenheng	Egen
Vandalisme	Hensynsløs ødeleggelse, grovt hærverk, grovt skadeverk	SNL, egen
Verdi	En materiell eller immateriell ressurs som hvis ødelagt, kompromittert, forstyrret eller på annen måte utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier eller forvalter ressursen.	Egen
Verdivurdering	Kartlegging og rangering av en entitets verdier innenfor en gitt sikkerhetsmessig kontekst.	Egen
Villedning	Aktivitet eller operasjon som har til hensikt å forlede en motstander gjennom manipulasjon, forvrengning og forfalskning av informasjon.	FFOD, 2207 Egen