Det kongelige fornyings- og administrasjonsdepartement
Det kongelige justis- og politidepartement
Det kongelige forsvarsdepartement
Det kongelige samferdselsdepartement

Retningslinjer

Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010

Forord

Vi lever i eit informasjons- og mediesamfunn, der vi dei siste åra er vorte meir og meir avhengige av IKT (informasjons- og kommunikasjonsteknologi). Internett vert stadig viktigare, nasjonalt og internasjonalt, for næringslivet, forvaltninga og kvar einskild brukar. Omfanget av elektronisk samhandling aukar og det er ofte verksemdskritisk informasjon som vert utveksla.

Bortfall av fungerande IKT-infrastruktur kan få store konsekvensar for ei verksemd, ein sektor eller for samfunnet som heilskap. Det er difor svært viktig at alle er medvitne på at risiko og sårbarheit må førebyggjast kontinuerleg.

Informasjonstryggleik handlar ikkje berre om dei teknologiske løysingane som vert valde, men like mykje om fordeling av ansvar og oppfølging av rutinar og planverk.

Informasjonstryggleik inneber ei heilskapleg tilnærming til val og innføring av tryggleiksteknologiar, ansvarleggjering av den einskilde, bevisstgjering, utdanning, erfaringsdeling og opplæring i trygg bruk.

Informasjonstryggleik er eit leiaransvar. Grunnlaget for eit vellukka informasjonstryggingsarbeid er at leiinga i kvar einskild verksemd, anten det dreier seg om privat, statleg eller kommunal sektor, innser at IKT-infrastrukturen er ein kritisk faktor for å nå dei mål verksemda har.

Utfordringa i mange verksemder er å få prioritert tryggingsarbeidet når alt "går som smurt", inntil det skjer ei katastrofe. Då vert spørsmåla mange: Kva for felles informasjon vert forvalta i verksemda? Kvar finst den? Kva verdi har den? Kva skjer når den er tapt eller kompromittert?

Vi har fått utarbeidd retningslinjene for å beskrive utviklingstrendar innanfor informasjonstryggleik og utfordringar dei fører med seg, og i tillegg peike på nasjonale innsatsområde som kan vere med på å møte utfordringane. Dokumentet skal også bidra til å leggje vekt på informasjonstryggleik som eit kritisk element i leiinga av ei verksemd. Vi vil gjere leiarar merksame på nasjonale prioriteringar, slik at vi saman kan medverke til styrka informasjonstryggleik i Noreg.

Oslo, desember 2007

Heidi Grande-Røys

Liv Signe Navarsete

Anne Grete Strøm-Erichsen

Knut Storberget

Innhold

1 Innledning

© Fredrik Naumann/Samfoto

1.1 Formålet med dette dokumentet

Formålet med å utgi nasjonale retningslinjer for å styrke informasjonssikkerheten er å skape en felles forståelse for hvilke utfordringer vi står overfor, og identifisere områder der det er behov for å gjøre en ekstra innsats for å styrke den nasjonale informasjonssikkerheten. Retningslinjene skal bidra til å fremme en bedre forståelse for hvordan alle brukere, utviklere og tilbydere av IKT (Informasjons- og kommunikasjonsteknologi) kan dra fordel, og bidra til utviklingen av, en sikkerhetskultur på området.

Retningslinjene for det nasjonale arbeidet med informasjonssikkerhet har en tidshorisont fram til 2010.

1.2 Mål for arbeidet med informasjonssikkerhet

Regjeringen peker i St.meld. nr. 17 (2006-2007) på behovet for å sørge for godt vern av den norske informasjonsinfrastrukturen gjennom *forebyggende* tiltak, å kunne svare effektivt på IKT-sikkerhetshendelser gjennom *beredskapstiltak*, og å sørge for *bærekraft* i sikkerhetsarbeidet gjennom blant annet kompetanseutvikling og standardisering.

Regjeringen har tre overordnede mål for informasjonssikkerhetsarbeidet:

1. Robust og sikker kritisk infrastruktur og støttesystemer for kritiske samfunnsfunksjoner,
2. God sikkerhetskultur ved utvikling og bruk av informasjonssystemer og ved elektronisk informasjonsutveksling,
3. Høy kompetanse og fokus på forskning om informasjonssikkerhet.

Arbeidet med IKT-sikkerhet vil primært være innrettet mot vern og utvikling av informasjonssystemer og nett. I tillegg handler IKT-sikkerhet om å arbeide for å innføre nye tenke- og handlemåter ved bruk av informasjonssystemer og nett, og ved utveksling og informasjon. Innsatsen som gjøres på dette området vil også bidra til å styrke personvernet, selv om personvernet ikke har hovedfokus i denne sammenhengen.

Det skal til enhver tid være tilstrekkelig IKT-beredskap i samfunnet. Alt beredskapsarbeid i virksomhetene i sektorene må inkludere IKT-beredskap – også i de tilfeller der dette ikke er pålagt gjennom regelverket.

1.3 Målgruppe

Retningslinjene er innrettet mot offentlige myndigheter i staten. Gjennomføring av retningslinjene kan også berøre kommuner, fylkeskommuner, næringsliv, private organisasjoner, husstander og enkeltpersoner.

Det er departementene og underlagte etater som er ansvarlige for å iverksette tiltak innenfor innsatsområdene i disse retningslinjene. Ledelsen i fylkeskommunene, kommunene og næringslivet bør, på eget initiativ, ta ansvar for å gjennomføre tiltak og fremme en sikkerhetskultur som er i overensstemmelse med disse retningslinjene. Sentrale myndigheter vil i denne sammenheng ha en rolle som pådriver for at fylkeskommuner, kommuner og næringsliv blir inkludert i arbeidet ved gjennomføring av tiltak med tverrsektoriell karakter.

1.4 Bakgrunn

Kompleksiteten i dagens informasjons- og kommunikasjonsteknologi øker. Den økte utbredelsen av tjenester som blir understøttet av IKT innenfor alle samfunnsområder, medfører økt avhengighet av teknologien i den enkelte virksomhet, mellom virksomheter, mellom samfunnssektorer og på tvers av landegrenser. Bortfall av slike tjenester kan få store konsekvenser for en virksomhet, en sektor eller for samfunnet som helhet. Det er derfor en forutsetning at de teknologiløsningene som velges er pålitelige, sikre og bidrar til å skape tillit hos den enkelte bruker. Teknologiens kompleksitet og avhengighetsforholdene gjør at strategiske valg som foretas for å styrke informasjonssikkerheten må ses i sammenheng.

Med *informasjonssikkerhet* menes her beskyttelse mot brudd på konfidensialitet, integritet eller tilgjengelighet av den informasjonen som blir behandlet i et system, eller beskyttelse av informasjonssystemer og nett i seg selv. God informasjonssikkerhet forutsetter at brukerne og utviklerne av system og nett har bevissthet om, og forståelse av IKT-sikkerhetspørsmål.

Informasjonssikkerhet er i dag en integrert del av flere lover og forskrifter. Eksempler på slike lover kan være sikkerhetsloven med forskrifter, personopplysningsloven med forskrifter, esignaturloven med forskrifter, forvaltningsloven og offentlighetsloven med forskrifter. Også sektorinnrettet regelverk omhandler informasjonssikkerhet, med ekomloven med forskrifter og pasientopplysningsloven med forskrifter som fremste eksempler.

Disse nasjonale retningslinjene er forankret i gjeldende regelverk. Samtidig identifiserer retningslinjene noen utfordringer som bør vurderes ved forvaltning og videreutvikling av dette regelverket.

Nasjonal strategi for informasjonssikkerhet ble lagt frem i 2003. I løpet av strategiperioden 2003-2006 er det gjennomført en rekke tiltak og aktiviteter. Hovedtyngden i dette sikkerhetsarbeidet har foregått i sektorene, primært i den enkelte virksomhet. Sikring av samfunnskritisk IKT-infrastruktur er blitt prioritert. Organiseringen av det tverrsektorielle arbeidet er blitt styrket. Departementenes samordnings- og sektoransvar for IKT-sikkerhet er presisert og ansvaret for nasjonal koordinering av varsling, rådgivning og assistanse for informasjonssikkerhet er avklart. Videre ble Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS) opprettet i 2004. Utvalget består av representanter for sentrale departementer og direktorater på IKT-sikkerhetsområdet. Utvalgets mandat omfatter både alminnelig IKT-sikkerhet og spørsmål knyttet til rikets sikkerhet, vitale nasjonale sikkerhetsinteresser og kritiske samfunnsfunksjoner.

2 Sikkerhetsutfordringer og trender

Etter lanseringen av Nasjonal strategi for informasjonssikkerhet i 2003, er det først og fremst fire teknologiske og bruksmessige utviklingstrekk som er blitt mer fremtredende:

- Samfunnets avhengighet av IKT og Internett har økt. Samfunnet som helhet er blitt mer sårbart for selv kortere driftsavbrudd i systemer og nett. Den økte sårbarheten skyldes blant annet økt kompleksitet i systemer og nett.
- Det er en økt tendens til målrettede, skreddersydde, og profesjonelle angrep.
- Finansiell vinning fortsetter å være den viktigste motivasjonsfaktoren for angriperne, som i økende omfang arbeider i det skjulte og stjeler konfidensielle data. Det er klare tegn på profesjonalisering av den kriminelle virksomheten. Det eksisterer i dag et illegalt marked for omsetning av verktøy for å begå sikkerhetsbrudd.
- Den store økningen i antall brukere av PC og Internett, med varierende kompetanse, har medført et økende behov for bevisstgjøring, informasjonsdeling og opplæring. Det er nødvendig at alle brukere får en bedre forståelse av sitt ansvar overfor andre brukere av nettet, og kunnskap til å ivareta dette ansvaret på en god måte.

Personvernet blir også utfordret av nye måter å kommunisere og bruke informasjonssystemer og nett på. Brukerne må derfor bli bedre til å ta i bruk eksisterende verktøy som kan bidra til å styrke personvernet. Ved utvikling av nye sikkerhetsløsninger må disse også ta høyde for å møte utfordringene på personvernområdet.

I det følgende omtales de mest sentrale sikkerhetsutfordringene og trendene på informasjonssikkerhetsområdet.

2.1 Gjensidig avhengighet til samfunnskritisk infrastruktur øker

Kritisk infrastruktur defineres i denne sammenhengen som de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Elektronisk kommunikasjon, kraft, vann- og avløp, mv. er identifisert som kritiske infrastrukturer. Felles for de kritiske infrastrukturene er at svikt eller ødeleggelse av disse kan få alvorlige konsekvenser for samfunnet.

I dag er det et sterkt gjensidig avhengighetsforhold mellom IKT og elektrisk kraft. Denne gjensidige avhengigheten representerer en vesentlig sårbarhet i samfunnet. Tilbydere av IKT-infrastruktur og -tjenester har i varierende grad beskyttet seg mot uregelmessig tilførsel av elektrisk kraft. Der det gamle telefonnettet fungerte selv om brukerne var uten elektrisitet er bredbåndstelefoni avhengig av at den enkelte bruker får levert elektrisk kraft, eller har egen nødstrøm i form av batteri eller generator. Sikker tilgang på strøm vil derfor være særlig kritisk for tilbydere av IKT og for virksomheter som er avhengig av IKT.

Kunnskap om gjensidig avhengighet har avgjørende betydning for sårbarhetsreduserende arbeid og bør derfor utvikles videre. Dette vil være spesielt viktig når det gjelder det gjensidige avhengighetsforholdet mellom samfunnskritisk IKT-infrastruktur, IKT-virksomhet og kraftforsyningen.

IKT inngår som en integrert del av samfunnskritisk infrastruktur og samfunnsfunksjoner (virksomheter) som baserer seg på denne. Virksomheter som er ansvarlig for kritisk infrastruktur har et særlig ansvar for å beskytte informasjon, systemer og nett. Andre virksomheter vil også kunne ha ansvar for samfunnskritisk IKT-infrastruktur i den forstand at de er leverandører av tjenester, produkter eller innehar kompetanse som er helt nødvendig for at de samfunnskritiske funksjonene skal ivaretas.

2.2 Avhengigheten av Internett øker

Samfunnsutviklingen de siste årene har gjort oss mer avhengig av en sikker og velfungerende kommunikasjon over Internett. Internett blir stadig viktigere, så vel nasjonalt som internasjonalt, for store deler av næringslivet, og for den enkelte bruker. Det er en klar tendens til at flere og flere foretak baserer hele eller sentrale deler av sin virksomhet på IKT, og benytter Internett for å tilby et stadig økende antall tjenester. Behovet for overføringskapasitet øker, noe som igjen øker betydningen av en sikker og robust kommunikasjonsinfrastruktur.

Økt bruk av internettjenester i forretningsvirksomheten har gjort at mange norske virksomheter er blitt mer sårbare for selv kortvarige driftsavbrudd. Stadig flere virksomheter opplyser at de vil få vesentlige problemer ved driftsstans i én dag, noen til og med etter bare en time.

Samfunnet står overfor en økende elektronisk samhandling, der omfanget av informasjon som utveksles stadig øker, herunder også sensitiv informasjon. Innbyggernes og virksomhetenes utnyttelse av den stadig mer integrerte økonomiske servicestruktur i Norge – og globaliseringen i det hele tatt – kan bli bremset av mangel på mekanismer som elektronisk ID (eID), som gjør det mulig å inngå bin-

dende avtaler på nettet. Bruk av eID kan også redusere risikoen for misbruk av personlige opplysninger. En slik utvikling stiller krav til de løsningene som benyttes for å sikre informasjon og transaksjoner på nettet. Slike krav gjelder særlig autentisering, integritet, konfidensialitet og uavviselighet av elektroniske meldinger eller transaksjoner. I tillegg kommer krav til autorisasjon av de samhandlende parter.

eID kan benyttes til autentisering og kan realiseres med ulike teknologier, herunder PIN-koder, sms-passord, PKI osv. Elektronisk signatur er løsninger som knytter et innhold til en identitet på en uaviselig måte. Løsningene kan realiseres gjennom bruk av PKI eller bruk av eID i kombinasjon med andre teknologier, for eksempel logging og sporing.

2.3 Samfunnet blir mer sårbart for angrep på IKT-infrastruktur

Svikt i tilgangen til Internett kan medføre store konsekvenser for dem som benytter Internett til å yte service og tjenester. Økt internettbruk kan føre til hurtigere spredning av ondsinnet kode og tjenestenektangrep. Et tjenestenektangrep kan i ytterste konsekvens føre til at en tjeneste blir utilgjengelig som følge av et målrettet angrep, ofte i form av store mengder nettverkstrafikk. Et økt antall brukere av IKT og Internett høyner også risikoen for at uønskede hendelser oppstår som følge av menneskelige feil.

Trenden er at internettangrep i økende grad er økonomisk motivert. Internasjonalt ser vi en økning i svindelforsøk ved å tilegne seg personopplysninger som kan benyttes til økonomisk vinning ved hjelp av e-post. Over 90 prosent av alle forsøk på phishing er rettet mot finansielle institusjoner for å få tak i bank- og kredittkortopplysninger og annen informasjon. Angrepene er mer målrettet og tilpasset mindre målgrupper enn tidligere. Forsendelse til mindre grupper gjør det vanskelig å oppdage og reagere på svindelforsøk.

Hensynet til effektivisering har ført til at mange virksomheter har knyttet styringssystemer for kritisk infrastruktur til virksomhetens administrative systemer som igjen er blitt knyttet opp mot Internett. Faren er at ondsinnet programvare, bevisst eller ubevisst, kan bli lastet ned fra det åpne nettet og spres via det administrative nettet til styringssystemet. En slik «tunnel» inn i styringssystemet kan bevisst utnyttes av kriminelle eller i ytterste konsekvens terrorister til å utføre sabotasje eller det åpner for spionasje ved at det er mulig å få tilgang til virksomhetssensitiv informasjon. Dersom den rammede virksomheten har betydning for samfunnskritiske funksjoner er skadepotensialet stort, særlig under kriser eller krig.

© Mimsy Møller/Samfoto

2.4 Nett, terminaler og tjenester smelter sammen og skaper kompleksitet og uoversiktlighet

Telefoni, radio og TV beveger seg i retning av anvendelse av en enhetlig fysisk infrastruktur der trafikken i hovedsak baserer seg på bruk av internettprotokoller (IP). Internett benyttes i dag blant annet til e-post, søking og innhenting av informasjon, interaktive e-tjenester som e-handel og nettbank, fildeling og interaktive spill.

En ny trend er at flere har tatt i bruk IP-telefoni, tale over Internett, ofte også ledsaget av bildeoverføring. Når mange tar i bruk denne formen for telefoni, til erstatning for vanlig telefoni, vil behovet for robusthet og tjenestekvalitet i Internettet øke. Konvergens gjør det derfor nødvendig å bygge ut den norske delen av Internettet på en robust måte. Internetteknologien kan bruke forskjellige typer fysisk infrastruktur som fiber, kabel, kobber og radio. Dette kan gjøre det lettere å etablere en robust infrastruktur hvor brukere har flere alternative tilknytninger, men det gir også mulighet til å velge rimelige løsninger hvor mange ulike kommunikasjonstjenester bruker en enkelt fysisk tilknytning. Da skapes en infrastruktur som er sårbar. Det er av stor betydning at det etableres alternative trafikkveier for å gjøre viktige kategorier brukere, for eksempel redningsetater, helse- og sosialsektoren, mindre sårbare. Forstyrrelser og avbrudd i IP-telefo-

© Scanpix

nitjenesten kan for enkelte brukere utgjøre en trussel mot liv og helse. En sannsynlig utvikling er at flere aktører tar i bruk IP-teknologi til å produsere tjenester, men beholder dette som lukkede private nett. Slike nett vil dele den fysiske infrastrukturen med Internettet, men vil fremstå som atskilte nett.

2.5 Trådløse nett og mobile tjenester skaper nye bruksmønstre og økt sårbarhet

Økende bruk av mobilt utstyr og mobile nettverkskomponenter gir nye utfordringer når tjenester basert på Internett utvikles. Mobilt dataverktøy har hittil hatt svakere sikkerhetsbeskyttelse enn PC-er. Tilknytningen skjer både via trådløse nett og mobilnett. Usikrede trådløse aksesspunkter gir en høy grad av anonymitet på nettet og en maskering for dem som vil angripe spesifikke tjenester eller nettet generelt.

2.6 Nye sårbarheter i programvare er et problem

Det å utforme, sette i produksjon, og deretter forvalte et avansert informasjonssystem er en komplisert og krevende oppgave. Det er derfor viktig å gjennomføre sikkerhetsvurderinger for å verifisere at krav til tilgjengelighet, integritet og konfidensialitet, samt autentisering og autorisasjon blir ivaretatt på en tilfredsstillende måte. Et IKT-system er ikke statisk. Ny funksjonalitet blir lagt til, og oppgraderinger av program og maskinvare skjer med jevne mellomrom. Det er ikke kjent hvor mange datasikkerhetsbrudd norske virksomheter har på grunn av selvpåførte feil, men antallet antas å være betydelig. Det snakkes ikke mye om dette. En virksomhet som er utsatt for en slik hendelse ønsker som regel ikke at offentligheten eller myndighetene skal få kunnskap om at den har hatt alvorlige problemer som følge av utilgjengelige IKT-systemer. Fra tid til annen kan vi likevel lese om at for eksempel nettbanker eller mobilnettverk er ute av funksjon.

Brukere av dominerende programvareplattformer blir oftere enn andre brukere utsatt for ondsinnet kode og virus.

2.7 Manglende sikkerhetsbevissthet blant brukerne utgjør en høy og økende risiko

En av de største utfordringene for informasjonssikkerheten er manglende sikkerhetsbevissthet hos brukere. Mange virksomheter og enkeltindivider undervurderer risikoen ved dårlig informasjonssikkerhet. Manglende forankring og prioritering i virksomhetens ledelse er også en utfordring. En av årsakene til fravær av oppmerksomhet i ledelsen er manglende sårbarhets- og risikoanalyser og manglende dokumentasjon av nytten av god informasjonssikkerhet i forhold til kostnadene. Enkeltindivider, enten de er hjemmebrukere eller ansatt i en virksomhet, ser ut til å ha en generell mangel på kunnskap og bevissthet omkring behovet for informasjonssikkerhet, og hvilken rolle de selv spiller som aktør i et nett. Datamaskiner uten beskyttelse kan, uten eierens viten, fjernstyres og dermed utnyttes for eksempel som plattform for tjenestenektangrep (DoS-angrep) mot blant annet Internetts infrastruktur. Et tjenestenektangrep mot kritiske deler av Internetts infrastruktur kan få konsekvenser for internettbruken nasjonalt, regionalt og globalt. Dette stiller krav til at alle internettbrukere tar et større ansvar for egen atferd på Internett og sikkerhet i eget datamiljø. Sikkerhetsproblemene på Internett er i dag komplekse. For at den enkelte skal kunne opptre sikkert på Internett og sikre sitt eget miljø kreves det bevissthet og kunnskap om de ulike sikkerhetsutfordringene.

2.8 Kompetanseutfordringene øker i takt med økt kompleksitet

Økt kompleksitet i systemer og nett gjør det vanskeligere for bestillere av systemer og nett å stille klare og presise

krav til sikkerhet. Å foreta valg av IKT-systemer og produkter som skal oppfylle bestemte sikkerhetskrav fordrer inngående kjennskap til løsningenes styrker og svakheter. Mangel på slik kunnskap kan føre til feilinvesteringer eller utilstrekkelig informasjonssikkerhet. Kompleksiteten gjør det dessuten vanskeligere for den enkelte bruker å ha oversikt over alle sikkerhetsmessige utfordringer som kan knytte seg til bruk av IKT.

PC-er blir stadig kraftigere, og er tilgjengelige døgnet rundt med bredbåndstilknytning. De får stadig flere bruksområder, og blir dermed også et mer fristende mål for inntrengere. Som en følge av denne utviklingen utgjør usikrede hjemme-PC-er en større risiko nå enn tidligere. Dette skyldes blant annet økt utbredelse av såkalte botnet, en samling PC-er som kan fjernstyres fra en sentral kilde. De infiserte PC-ene kan fjernstyres ved hjelp av ondsinnet programkode og kan deretter benyttes til pengeutpressing ved at de kommanderes til å sette i gang blokkeringsangrep mot sentrale datamaskiner hos et firma eller annen virksomhet.

2.9 Økt internasjonalisering bidrar til at nasjonale nett og systemer i økende grad kommer utenfor nasjonal kontroll

Overvåking av drift og håndtering av alvorlige feil og forstyrrelser i nettene krever personell med høy kompetanse som er tilgjengelig døgnet rundt. Av kostnads- og effektiviseringsårsaker arbeider tilbydere av elektroniske kommunikasjonsnett og tjenester kontinuerlig med å komme frem til mer automatisert og sentralisert drift. Økt globalisering vil innebære at mange nasjonale og internasjonale tilbydere vil tilby å utkontraktere driftsentraler og oppgaver til land med lavere kostnader. En slik sentralisering og fjernstyring av trafikken gjør elektronisk kommunikasjon mer avhengig av fungerende forbindelser på tvers av landegrenser. Økt utkontraktering kan føre til at deler av vår samfunnskritiske infrastruktur styres utenfor Norge. Tilsyn vanskeliggjøres når deler av virksomheten ivaretas i utlandet og påvirkes av vertslandets regelverk. På sikt kan en offensiv bruk av utkontraktering av deler av kritisk IKT-infrastruktur utenfor landets grenser bidra til nedbygging av kompetanse og kapasitet. Dette kan i neste omgang svekke evnen til å ivareta den nasjonale informasjonssikkerheten på en hensiktsmessig måte.

Nye måter å løse oppgaver på, som igjen gir opphav til nye anvendelsesområder, kan også åpne for nye former for misbruk. Selv om de fleste nyvinninger ikke er direkte truende for personvernet eller informasjonssikkerheten, er det en utfordring å ivareta disse hensynene i en globalisert verden.

2.10 Endringer i måten teknologi tas i bruk av organisasjoner skaper nye sikkerhetsutfordringer.

Programvare som er i bruk i mange organisasjoner er i dag mye mer standardisert enn tidligere. Utviklingen innen moderne IKT legger til rette for gjenbruk av programvare, og for sammenkobling av datasystemer ved hjelp av Internett på tvers av organisasjonsstrukturer. Dette skjer på en helt annen måte i dag enn tidligere. Såkalt serviceorientert arkitektur (SOA) muliggjør teknologisk integrasjon av verdikjeder over Internett som utfordrer etablerte samarbeidsmønstre mellom organisasjoner. En kunde kan raskt forflytte seg mellom datasystemer hos flere virksomheter for å bestille en vare eller en tjeneste. Overføring av brukerdata fra system til system for å gi brukere adgang uten ny autentisering og autorisasjon, også kalt føderering, kan kreve revurdering av ansvarsprinsipper for informasjonssikkerhet i egen organisasjon. Likedan er trenden med etablering av felles portaler, som Altinn og MinSide, en utfordring for deltakende virksomheter med hensyn til det helhetlige ansvaret for informasjonssikkerhet. Utkontraktering eller utskilling og profesjonalisering av deler av egen IKT-virksomhet skaper lignende problemstillinger.

Det er i denne forbindelse viktig å avklare hvor ansvaret ligger til enhver tid, slik at viktige komponenter i et nettverk eller system som overskrider organisasjonsgrenser, ikke faller mellom to stoler og blir et sårbarhetspunkt for mulige angrep.

2.11 Internett skaper nye sosiale trender – og økt sårbarhet for deltagere i sosial interaksjon på nettet

Utviklingen mot det så kalte web 2.0 – eller deltagelsesweb – åpner for et hittil ukjent omfang og type sosial interaksjon over Internett. Nettsteder som MyPage, MySpace, YouTube, Facebook og lignende trekker til seg millioner av brukere og skaper et potensielt arnested for spredning av ondsinnet programvare eller andre former for angrep. Pratekanaler åpner for direkte angrep av typen «sosial manipulasjon» (social engineering), med alvorlige konsekvenser som følge.

Denne utviklingen skaper en kompetanse- og bevisstgjøringsutfordring. Brukere av slike tjenester trenger kunnskap om personvern, potensielle sikkerhetsfarer, og det ansvaret som hver enkelt har for å hindre spredning av ondsinnet programkode, og påfølgende konsekvenser for andre brukere av nettet. Eksponering av egne personopplysninger kan også utgjøre en trussel for personer som har betrodde stillinger innen informasjonssikkerhet i ulike typer virksomheter, ved at opplysningene kan benyttes til utpressing eller annen form for manipulasjon.

3 Innsatsområder

Innsatsområdene som beskrives i dette kapittelet er definert på bakgrunn av identifiserte sikkerhetsutfordringer og regjeringens hovedmål for arbeidet med informasjonssikkerhet. Innsatsområdene understøtter ett eller flere av disse målene. Beskrivelsen av det enkelte innsatsområde er holdt på et overordnet nivå. Prosesser for den videre konkretiseringen av innsatsområdene og gjennomføring av konkrete tiltak er beskrevet i kapittel 4.

3.1 Samfunnskritisk IKT-infrastruktur må beskyttes bedre

Alle virksomheter som eier samfunnskritisk IKT-infrastruktur må innføre beskyttelsestiltak og etablere reserveløsninger som sikrer opprettholdelse av drift og leveranser. Beredskapen for håndtering av brudd i samfunnskritisk IKT-infrastruktur må styrkes både hos tilbydere og brukere.

Beskyttelse av samfunnskritisk IKT-infrastruktur er et virksomhetsansvar. Svikt i denne infrastrukturen kan føre til umiddelbare og alvorlige konsekvenser for store deler av samfunnet. Alle virksomheter som eier samfunnskritisk IKT-infrastruktur må innføre beskyttelsestiltak og etablere reserveløsninger som sikrer opprettholdelse av drift og leveranser. Både virksomhetene selv og tilbyderne av IKT bør vektlegge tiltak for å sikre robusthet, blant annet ved å dublere viktige komponenter. Rask gjenoppretting etter brudd er både et kommersielt og samfunnsmessig mål. Beredskapen for håndtering av brudd bør derfor styrkes både hos tilbydere og brukere.

Samfunnet er kritisk avhengig av en omfangsrik IKT-infrastruktur, og for svært mange virksomheter er IKT en virksomhetskritisk faktor. Et viktig tiltaksområde er øvelser i å håndtere hendelser hvor kritiske IKT-funksjoner svikter. Øvelser kan avdekke svakheter i organisasjon og gi økt kompetanse og viktig erfaring med å gjenopprette normal funksjon. Regelmessige øvelser gjør det mulig å redusere negative konsekvenser av alvorlige hendelser som rammer IKT-infrastruktur. Øvelser bør gjennomføres på alle samfunnsnivåer. De vil også bidra til å redusere sårbarhet knyttet til svikt i IKT-systemene til den enkelte virksomhet.

Identifisering av samfunnskritisk IKT-infrastruktur er viktig for at virksomhetene skal kunne prioritere forebyggende tiltak og beredskapstiltak. Det enkelte fagdepartement har et ansvar for å identifisere samfunnskritisk IKT-infrastruktur i sektoren og sørge for at den blir beskyttet, jf. ansvars-, likhets- og nærhetsprinsippet. Det bør, med utgangspunkt i eksisterende verktøy, etableres et metodeverk som hjelp til å identifisere samfunnskritisk IKT-infrastruktur og kritiske funksjoner avhengig av IKT.

Utkontraktering av tjenester er blitt mer utbredt. Virksomheter med ansvar for samfunnskritiske IKT-systemer har et særskilt ansvar for å påse at hensynet til sikkerhet og beredskap blir ivaretatt ved utkontraktering. Gjennom avtaler med leverandører av tjenester må virksomhetene sørge for at også sikkerhets- og beredskapsforpliktelsene blir ivaretatt på en tilfredsstillende måte. Myndighetene bør gi råd om de sikkerhets- og beredskapsmessige konsekvensene av utkontraktering.

Leverandører av internettjenester bør tilby sikkerhetsløsninger inkludert i tjenesteleveransen. Det bør fremgå av løsningen som tilbys hvilke forutsetninger løsningen er basert på samt hvilke sikkerhetsrisikoer løsningen dekker. Arbeidet med å oppnå et tilfredsstillende sikkerhetsnivå når det gjelder elektroniske kommunikasjonstjenester bør først og fremst søkes oppnådd gjennom selvregulering, men myndighetene må følge utviklingen i bransjen nøye. Dersom myndighetene vurderer at det ikke oppnås et tilstrekkelig sikkerhetsnivå gjennom selvregulering, kan det være aktuelt med pålegg for å bedre sikkerheten. Manglende sikkerhet kan imidlertid også skyldes mangel på kunnskap om IKT-sikkerhet. En videre satsning på bevisstgjøringstiltak overfor brukere av internettjenester, og andre elektroniske kommunikasjonstjenester, vil derfor være vel så viktig, jf. punkt 3.5.

Ansvar for gjennomføring: Alle departementer som har identifisert samfunnskritisk IKT-infrastruktur i sin sektor samt Justisdepartementet i kraft av sitt tilsyn med departementenes sikkerhets- og beredskapsarbeid.

3.2 Regelverk knyttet til informasjonssikkerhet må gjøres mer konsistent og forståelig

Regelverk som regulerer informasjonssikkerhet skal gjennomgås med sikte på å tilrettelegge for størst mulig grad av harmonisert begrepsbruk og forenkling. Myndighetene må kommunisere bedre innbyrdes og med virksomhetene som omfattes av regelverkene. Veiledningsvirksomheten må intensiveres – spesielt mot kommuner og små og mellomstore virksomheter.

Mye av utviklingen av regelverket i Norge er styrt av internasjonale beslutninger og påvirkes av regelverk utviklet utenfor Norge. Dette medfører en rekke forpliktelser, og er samtidig en av årsakene til den inkonsistente begrepsbruken innenfor dette området. Ved utforming av lov- og forskriftstekster som berører informasjonssikkerhet, bør det

derfor legges vekt på at disse skal være lette å forstå samtidig som det tilstrebes et felles begrepsapparat på tvers av sektorer. Veiledere kan bidra til riktig tolkning og bedre implementering av regelverkene, slik at ordlyd, definisjoner og tolkning gjøres mest mulig konsistent. I motsatt tilfelle vil tolkningstvil gjøre det vanskeligere for virksomheter som er underlagt flere ulike regelverk å overholde sine forpliktelser. Utforming av nytt regelverk bør i størst mulig grad koordineres med eksisterende regelverk, slik at omfanget av nye bestemmelser begrenses.

Departementer og tilsyn skal forbedre kommunikasjonen med virksomhetene som omfattes av regelverkene. Dette gjelder særlig kommuner og små og mellomstore virksomheter. Kunnskap om erfaringer og synspunkter på hvordan regelverket oppfattes og fungerer, er et viktig grunnlag for regelverksutvikling og et mål for denne kommunikasjonen. Det må forutsettes at myndighetsorganer i nødvendig grad samarbeider og koordinerer seg i forhold til å formidle informasjon om regelverk. Eksisterende samarbeidsarenaer mellom regelverksforvaltere bør videreføres og videreutvikles.

Ansvar for gjennomføring: alle departementer som forvalter regelverk innenfor IKT-sikkerhet, herunder også IKT-sikkerhet i sektorregelverket.

3.3 Informasjon og informasjonssystemer bør klassifiseres for at tiltak lettere skal kunne tilordnes

Alle IKT-systemer og all informasjon som blir behandlet i IKT-systemene med betydning for rikets sikkerhet eller personvernet skal iht. gjeldende regelverk være klassifisert. Eiere av informasjon og informasjonssystemer som ikke omfattes av regelverket skal oppfordres til å gjennomføre verdivurderinger for å identifisere hvilken informasjon som er nødvendig å beskytte.

Det kan være ulike hensyn som begrunner beskyttelse, herunder hensynet til personvernet, skjerming av bedriftshemmeligheter, hensynet til rikets sikkerhet, tilgjengelighet mv. I enkelte tilfeller er dette hjemlet i lov, for eksempel i sikkerhetsloven og personvernopplysningsloven. Klassifisering av informasjon og informasjonssystemer skaper økt bevissthet om betydningen og verdien som informasjonen eller IKT-systemet i virksomheten representerer. Et annet mål er at en slik klassifisering vil forenkle arbeidet med sikring av IKT-systemene og informasjonen.

Eiere av informasjon og informasjonssystemer som ikke omfattes av regelverket, skal oppfordres til å gjennomføre

© Scanpix

verdivurderinger for å identifisere hvilken informasjon som er nødvendig å beskytte. Tilsvarende må det gjennomføres verdivurderinger for å identifisere hvilke IKT-systemer som er nødvendig å beskytte.

Klassifisering av informasjon og IKT-systemer bidrar til å klargjøre hva som skal defineres som kritisk informasjon eller et kritisk IKT-system. En felles tilnærming til hvordan informasjon og IKT-systemer skal klassifiseres vil redusere sannsynligheten for at virksomheter som samarbeider om et felles prosjekt klassifiserer samme type styrings- og kontrollsystemer og administrative systemer ulikt, og eventuelt krever ulikt sikkerhetsnivå på samme type informasjon.

Ansvar for gjennomføring: alle departementer og underlagte virksomheter.

3.4 Risiko- og sårbarhetsanalyser bør gjennomføres av alle - spesielt av alle eiere av kritisk infrastruktur

Virksomheter som ivaretar samfunnskritisk IKT-infrastruktur eller IKT-virksomhet har et særlig ansvar for å gjennomføre regelmessige risiko- og sårbarhetsanalyser (ROS-analyser). Myndighetene må, i samarbeid med relevante aktører, legge forholdene til rette for at ROS-analyser gjennomføres, og aktivt søke å heve kompetansen hos aktørene ved å bidra med råd og veiledning. Der regelverket forutsetter det skal gjennomføring av ROS-analyser inngå i et fastlagt styringssystem for risikohåndtering i virksomheten. ROS-analyser må være forankret hos ledelsen.

Gjennomføring av ROS-analyser er et nødvendig tiltak for risikohåndtering og setter virksomheten i stand til å avdekke sårbare og risikoutsatte områder. I enkelte tilfeller er pålegg om ROS-analyser hjemlet i lov, men slike analyser bør være del av en kontinuerlig aktivitet i enhver virksomhet. Analysen bør gjennomføres jevnlig eller ved særlige behov. Gjennomføringen av analysen bør inngå i et fastlagt styringssystem for risikohåndtering i virksomheten og må være forankret hos ledelsen. Det er i den enkelte virksomhets egen interesse å gjennomføre ROS-analyser også i de tilfeller der virksomheten ikke er underlagt regelverk som stiller krav til dette.

Selv om ROS-analysen primært er et virksomhetsansvar må departementene, i samarbeid med underliggende etater og relevante aktører, legge forholdene til rette for at ROS-analyser blir gjennomført. Departementene skal gjennom sine underlagte etater aktivt søke å heve sikkerhetskompetansen hos aktørene i sektorene. Der det er nødvendig må sektormyndighetene sikre gjennomføring av ROS-analyser gjennom regulering. I enkelte sektorer er dette allerede etablert, og det finnes også tverrgående reguleringer som krever bruk av ROS-analyser for bestemte områder.

Virksomheter som ivaretar samfunnskritisk IKT-infrastruktur, eller samfunnskritiske funksjoner avhengig av IKT, har et særlig ansvar for å gjennomføre regelmessige ROS-analyser. Det er også behov for veiledning i valg av ROS-metode for den enkelte virksomhet. Myndigheter med ansvar for sikkerhet og beredskap må bidra til realisering av dette.

Ansvar for gjennomføring: alle departementer og underlagte virksomheter.

3.5 Innsatsen for bevisstgjøring og kunnskapsspredning må økes

Alle skal ha tilgang til informasjon om trusler og tiltak for å forebygge truslene. Det skal legges til rette for at bevisstheten og kunnskapen hos brukerne av IKT og Internett øker. Etablerte bevisstgjøringsaktiviteter skal videreføres og videreutvikles. Dette gjelder aktivitetene til Norsk senter for informasjonssikring (NorSIS) og Post- og teletilsynets opplysnings- og veiledningsaktiviteter inkludert sikkerhetsportalen Nettvett.no. Det bør etableres et langsiktig samarbeid mellom myndighetene og næringslivsorganisasjonene for å utvikle programmer for bevisstgjøring, opplæring og oppbygging av en god sikkerhetskultur.

Det finnes en rekke avhengigheter mellom virksomheter og mellom de ulike sektorene i samfunnet når det gjelder bruk av IKT. Dette gjør det vanskelig for den enkelte virksomhet å vurdere de totale konsekvensene for samfunnet av manglende innsats knyttet til informasjonssikkerhet. For å redusere samfunnets sårbarhet skal informasjon om trusler, sårbarhet og tiltak deles. Myndigheter med ansvar for sikkerhet og beredskap har ansvar for å innhente og formidle informasjon om trusselsituasjonen på nasjonalt og overordnet nivå. For at alle skal ha tilgang til samme informasjon om trusler og tiltak for å redusere truslene, bør alle eiere av, og leverandører av komponenter til, samfunnskritisk IKT-infrastruktur i offentlig og privat sektor bli invitert til å delta på felles arenaer for informasjonsdeling. Også andre virksomheter oppfordres til å delta på arenaer der slik informasjonsutveksling foregår.

Ansvaret for informasjonssikkerhet ligger hos ledelsen i den enkelte virksomhet. Virksomhetens ledelse må være kjent med hvilken risiko virksomheten løper ved innføring av nye IKT-verktøy i hele eller deler av virksomheten. Virksomhetens ledelse må også inneha den nødvendige bestillerkompetanse for innkjøp av nye IKT-verktøy, bruk av ekstern konsulentbistand eller utkontraktering av virksomhetens IKT-tjenester. Ledelsen skal ut fra en risikovurdering fastlegge sikkerhetsnivået i virksomheten og påse at kravene til informasjonssikkerhet følges opp av alle innenfor organisasjonen. Virksomhetene bør følgelig ha et system for bevisstgjøring og kompetansebygging innen informasjonssikkerhet. Systemet bør omfatte alle i virksomheten. Holdningsendringer er vanskelig og tidkrevende å oppnå. Det bør derfor etableres et langsiktig samarbeid mellom myndighetene og næringslivsorganisasjonene for å utvikle programmer for bevisstgjøring, opplæring og oppbygging av god sikkerhetskultur.

Bevissthet om risikoer og tilgjengelige beskyttelsestiltak er den første forsvarslinjen for sikkerheten i IKT-systemer. Bevisstheten og kunnskapen hos befolkningen generelt skal derfor økes. Etablerte og målrettede tiltak for å styrke bevisstheten om IKT-sikkerhet skal videreføres. Dette gjelder blant annet aktivitetene til Norsk senter for informasjonssikring (NorSIS) og Post- og teletilsynets opplysnings- og veiledningsaktiviteter inkludert sikkerhetsportalen Nettvett.no. God ressursutnyttelse på området tilsier et tett samarbeid mellom myndighetene, næringslivet og private organisasjoner. Myndigheter med ansvar for sikkerhet og beredskap skal derfor, i samarbeid med privat sektor, bidra til bevisstgjøring om trusler, opplyse om tiltak og påvirke til gode holdninger. Leverandører av produkter og systemer vil bli oppfordret til å legge til rette for at alle produkter og systemer rettet mot massemarkedet ledsages av lettfattelig opplysnings- og opplæringsmateriale om informasjonssikkerhet.

Ansvar for gjennomføring: ledere i alle statlige virksomheter.

3.6 Varsling og hendelseshåndtering skal skje raskt og koordinert

Sikkerhetshendelser og trusler mot samfunnskritisk IKT-infrastruktur og samfunnskritiske funksjoner avhengige av IKT må oppdages og rapporteres raskt. Gjennom en systematisk rapportering og deling av erfaringer knyttet til IKT-sikkerhetshendelser sikres en større grad av kompetanse og læring. Dette vil også bidra til at myndighetene kan gi gode råd om sikkerhetssituasjonen ut fra preventive hensyn.

Avhengigheten av nett, herunder Internett, samt økt globalisering, gjør at behovet for koordinert varsling og rådgivning er stort. Det er behov for at virksomheter rapporterer om IKT-sikkerhetshendelser til relevante sektormyndigheter. Eksisterende samarbeid og informasjonsdeling mellom varslingsinstansene og hjelpeapparatet skal videreføres og videreutvikles. Gjennom systematisk rapportering og deling av erfaringer knyttet til IKT-hendelser sikres en større grad av kompetanse og læring. Dette vil også bidra til at offentlige instanser kan gi gode råd om sikkerhetssituasjonen ut fra preventive hensyn.

Norwegian Computer Emergency Response Team (NorCERT) hos Nasjonal sikkerhetsmyndighet er kontakt- og koordineringspunkt nasjonalt og internasjonalt, for å beskytte mot og respondere på sikkerhetshendelser med alvorlig eller akutt påvirkning på Internett.

© Jann Lipka / Mira/Samfoto

NorCERT, KRIPOS, Politiets sikkerhetstjeneste (PST) og Forsvaret bør samarbeide tett for å utveksle erfaringer om trusselbildet, gi hverandre faglig hjelp og tydeliggjøre nasjonal arbeidsdeling i kampen mot uønskede hendelser på Internett.

Ansvar for gjennomføring: Forsvarsdepartementet, Justisdepartementet og Samferdselsdepartementet.

3.7 Alle departementer bør fremme bruk av standarder, sertifisering og egenregulering

Systemer som er utviklet i samsvar med anerkjente standarder for informasjonssikkerhet er i hovedsak mer sikre. Sektormyndighetene bør stimulere alle virksomheter og leverandører til å ta i bruk sertifiserte løsninger. Fornyings- og administrasjonsdepartementet vil vurdere om det skal stilles krav om sertifisering eller selvdeklarering (egenkontroll) av informasjonssikkerhet for offentlige virksomheter. Norske myndigheter må bli mer aktive og fremme funksjonalitets- og sikkerhetskrav i forbindelse med utvikling av nasjonale og internasjonale standarder for informasjonssikkerhet.

Leverandører og produsenter av informasjonssystemer og nett som har betydning for samfunnskritisk IKT-infrastruktur må kunne dokumentere at systemene er utviklet og implementert i samsvar med anerkjente standarder på IKT-området.

Det offentlige må innta en mer aktiv rolle med hensyn til å spesifisere og kreve dokumentert informasjonssikkerhet ved anskaffelser. Fornyings- og administrasjonsdepartementet vil vurdere om det skal stilles krav til offentlige virksomheter om sertifisering eller selvdeklarering (egenkontroll) av informasjonssikkerhet.

Standarder innen informasjonssikkerhet etableres i internasjonale standardiseringsorganisasjoner. Fra norsk side vil det være viktig å delta i dette arbeidet for å påvirke utviklingen av standardene samt sikre kunnskap om, og implementering av, resultatene. Informasjonsformidlingen omkring tilgjengelige IKT-sikkerhetsstandarder bør styrkes.

Myndighetene bør oppfordre alle virksomheter og leverandører til å ta i bruk sertifiserte løsninger. Dette vil bidra til at IKT-industrien benytter anerkjente standarder i forbindelse med utvikling, implementering og driftsoppgaver.

Internasjonale standarder får en stadig større betydning for den nasjonale bruken av IKT. Harmoniseringen av gjeldende tekniske sikkerhetskrav og operative sikkerhetsnivåer er en kontinuerlig prosess. Standardiseringsarbeidet drives først og fremst av aktørene i næringslivet. Offentlig sektor har hittil deltatt i begrenset utstrekning. Dette kan ha medført at samfunnsinteressene ikke alltid blir tilstrekkelig representert i forbindelse med utvikling av standardene. Norske myndigheter må derfor, eventuelt i samarbeid med andre lands myndigheter, bli mer aktive med å fremme funksjonalitets- og sikkerhetskrav i forbindelse med utvikling av internasjonale standarder for informasjonssikkerhet.

Nærings- og handelsdepartementet har gitt Standard Norge i oppdrag å utarbeide en nasjonal strategi for økt bruk av standarder og styrket deltakelse i nasjonalt og internasjonalt standardiseringsarbeid innen 31. desember 2007. IKT vil være et viktig område for en slik strategi. IKT-sikkerhet vil få en økende betydning og vil derfor være et naturlig fokusområde. Standard Norge har allerede i dag har et omfattende arbeid på områdene ID-kort, e-signaturer, biometri og IKT-sikkerhet.

Standarder for informasjonssikkerhet bør understøtte konkurranse i IKT-markedet og det generelle arbeidet med åpne standarder på IKT-området.

Ansvar for gjennomføring: Fornyings- og administrasjonsdepartementet, Nærings- og handelsdepartementet, øvrige departementer.

3.8 Departementer bør fremme FoU, utdanning og kompetanseutvikling innen informasjonssikkerhet

Norske virksomheter og befolkningen skal ha høy kompetanse innen informasjonssikkerhet. Forskning og utvikling innenfor informasjonssikkerhet må styrkes nasjonalt, og det bør stimuleres til norsk deltakelse på internasjonale arenaer.

Kunnskapen om informasjonssikkerhet må styrkes. Læreplanverket for Kunnskapsløftet har IKT som en av fem grunnleggende ferdigheter, og IKT inngår i de faglige kompetansemålene. Informasjonssikkerhet bør derfor inngå som en naturlig del av bruken av IKT i læringsarbeidet i skolen. Dette setter krav til grunnutdanning og kompetanseutvikling for lærere, og til undervisningsmateriell.

Det er viktig at norske universiteter og høgskoler har et utdanningstilbud med fordypning innenfor informasjonssikkerhet. IKT-fag på universitetene og høgskolene bør ha en egen modul om informasjonssikkerhet.

Videreutdanning og kompetanseheving innen informasjonssikkerhet må styrkes for brukere av IKT. Sertifisering er et virkemiddel som sikrer godkjent kompetanse hos sikkerhetspersonell. Departementene bør sørge for at sertifisering innen IKT-sikkerhet blir et kriterium for ansettelse av IKT-personell.

Offentlig og privat sektor bør legge bedre til rette for at studenter av informasjonssikkerhet på masternivå får anledning til å arbeide med aktuelle sikkerhetsproblemstillinger innenfor en sektor, eller i en enkelt virksomhet, gjennom å foreslå konkrete temaer for masteroppgaver innen informasjonssikkerhet.

Det må legges til rette for at forskningsmiljøene innen grunnforskning og anvendt forskning kan ha god interaksjon med ledende IKT-bedrifter og fagmiljøer på tvers av sektorer. Det er viktig at anvendt forskning innen informasjonssikkerhet tidlig fanger opp endringer i teknologi og metoder. Forskningsarbeidet innen informasjonssikkerhet må styrkes både nasjonalt, og ved at det stimuleres til norsk deltakelse på internasjonale arenaer. Ut over direkte bevilgninger til FoU har det offentlige også en viktig rolle som kunde og bestiller av ulike produkter, utviklingsprosjekter og tjenester. IKT-sikkerhet bør også være integrert i andre relevante forskningsprogram.

Ansvar for gjennomføring: Kunnskapsdepartementet, Nærings- og handelsdepartementet, Fornyings- og administrasjonsdepartementet.

3.9 Det bør etableres et samordnet opplegg for identitetshåndtering og elektronisk signatur på tvers av sektorer

Det bør etableres et felles rammeverk for autentisering og signering i elektronisk kommunikasjon med og i offentlige sektor. Samtrafikk for elektronisk ID og -signatur må ivaretas.

Ved valg av sikkerhetsnivå for en gitt elektronisk samhandling skal alle offentlige virksomheter i henhold til gjeldende regelverk gjennomføre en risikoanalyse, og deretter velge løsninger for eID eller e-signatur i samsvar med dette. Til hjelp for slike vurderinger skal det legges til grunn et felles rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Flere land har utviklet slike rammeverk, med det formål å samordne risiko- og sikkerhetsvurderinger der elektronisk samhandling berører publikum og næringslivet.

For å gjøre bruken av eID og e-signatur enklere for brukere er det formålstjenlig med en felles ordning for utstedelse av eID på et sikkerhetsnivå som gjør det mulig at eID kan benyttes i flere ulike sammenhenger. Dette kan være en eID med middels sikkerhetsnivå, men tilstrekkelig for sikring av mange typer transaksjoner. Det kan også være en meget sikker eID og en elektronisk signatur.

For at offentlige virksomheter kan ta i bruk eID og e-signatur i elektronisk samhandling med publikum og næringslivet på en enkel og kostnadseffektiv måte, må samtrafikken ivaretas.

Ansvar for gjennomføring: Fornyings- og administrasjonsdepartementet, Justisdepartementet, Nærings- og handelsdepartementet.

3.10 Departementenes internasjonale samarbeid om informasjonssikkerhet skal videreutvikles

Departementer som arbeider med informasjonssikkerhet på internasjonalt nivå skal ha felles internasjonal tilnærming til alle strategisk viktige spørsmål av tverrsektoriell karakter knyttet til sikker bruk av IKT og Internett.

Norge deltar aktivt på flere internasjonale fagarenaer hvis formål er å styrke den tverrsektorielle informasjonssikkerheten. Arbeidet skjer i hovedsak innenfor rammene av internasjonale organisasjoner som EU (ENISA), OECD, Internet Governance Forum (IGF) m.fl. Deltakelsen i dette arbeidet bidrar til større informasjonssikkerhet i Norge. Det gir også Norge en anledning til å være med på å utforme en internasjonal policy for et globalt sett sikrere Internett.

Det er viktig at departementer som deltar på de internasjonale arenaene for tverrsektoriell sikring av IKT og Internett har felles tilnærming til alle strategisk viktige spørsmål. Den norske deltakelsen på dette området skal samordnes og videreutvikles for å få ytterligere effekt ut av den innsatsen.

Ansvar for gjennomføring: alle departementer som arbeider med IKT-sikkerhet på internasjonalt nivå.

3.11 Informasjonssikkerhetsarbeidet skal samordnes gjennom Koordineringsutvalget for forebyggende informasjonssikkerhet

Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS) skal videreføres og videreutvikles som et tverrsektorielt koordineringsorgan på informasjonssikkerhetsområdet for sentrale departementer og underlagte etater. Kontaktflaten mellom KIS og aktørene i akademia og privat sektor skal styrkes.

Fornyings- og administrasjonsdepartementet har et samordningsansvar for forebyggende og tverrsektorielt arbeid med informasjonssikkerheten. Det enkelte fagdepartement har et ansvar for å ivareta informasjonssikkerheten innenfor sin sektor. Fagdepartementene vurderer også hvilke tiltak som er nødvendige å iverksette innenfor sin sektor.

Gjennom etablering i 2004 av Koordineringsutvalget for forebyggende informasjonssikkerhet, som ledes av Fornyings- og administrasjonsdepartementet, er det lagt til rette for en bedre samordning av myndighetenes forebyggende arbeid med informasjonssikkerhet. Kontaktflaten mellom KIS og aktørene i akademia og privat sektor skal styrkes.

Ansvar for gjennomføring: Fornyings- og administrasjonsdepartementet.

4 Gjennomføring

© David Trood/Samfoto

Informasjonssikkerhet er først og fremst et virksomhetsansvar. Gjennomføring av tiltak på de ulike innsatsområdene forutsetter imidlertid en effektiv medvirkning fra næringsliv, sentrale og lokale myndigheter og den enkelte bruker.

I samvar med ansvarsprinsippet vil det enkelte departement ha ansvar for å følge opp retningslinjenes innsatsområder innenfor sitt ansvarsområde. Departementene skal i samarbeid med underlagte virksomheter sørge for sektorvis oppfølging, og at tiltak i nødvendig grad blir koordinert med andre departementer. Fornyings- og administrasjonsdepartementet har et overordnet samordningsansvar for oppfølging.

Sterk dynamikk i fagfeltet tilsier korte strategiperioder. Disse retningslinjene vil bli lagt til grunn for regjeringens arbeid med informasjonssikkerhet i perioden 2007-2010. Samtidig som gamle sikkerhetsproblemer løses, dukker det nye opp som følge av innføring av ny teknologi, endringer i bruksmønster og endringer i trusselbildet. Følgelig vil også sikringsstiltak som kan være aktuelle i dag kunne være utdaterte i morgen. Regjeringen har derfor i dette overordnede dokumentet valgt å fokusere på innsatsområder fremfor konkrete tiltak. Det blir opp til aktørene i den enkelte sektor å finne frem til de til enhver tid mest egnede tiltak innenfor det enkelte tiltaksområde når arbeidet med styrket informasjonssikkerhet skal gjennomføres.

Iverksetting av konkrete tiltak innenfor de ulike innsatsområdene kan blant annet skje i forbindelse med utarbeidelsen av departementenes årlige tildelingsbrev til underliggende virksomheter, hvor mål og prioriteringer for virksomhetene blir gitt. Tiltak som berører næringslivet skal gjennomføres i nært samarbeid med næringslivets egne organer. Tiltak som berører forbrukerne bør gjennomføres i samarbeid med forbrukerorganisasjonene. I den grad sikkerhetstiltakene også berører personvernet bør personvernmyndighetene involveres ved gjennomføring.

Regjeringen vil følge utviklingen innenfor informasjonssikkerhet gjennom regelmessige undersøkelser for å kartlegge status og utfordringer på området. Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS) vil ha et ansvar for å holde oversikt over gjennomføringen av tiltak på innsatsområdene, og kan via Fornyings- og administrasjonsdepartementet rapportere til regjeringen om samlet status ved behov. KIS vil også ha en rolle når det gjelder å identifisere tverrsektorielle utfordringer på IKT-sikkerhetsområdet som må følges opp. KIS kan også opptre som pådriver for å igangsette tiltak av tverrsektoriell karakter, uten at dette endrer det enkelte departements sektoransvar. Det kan i denne sammenheng være aktuelt å opprette arbeidsgrupper i regi av KIS for å utarbeide konkrete tiltak på bakgrunn av tiltaksområdene. Departementene kan bruke koordineringsutvalget til å drøfte samordning og prioritering av tiltak. Det vil også bli lagt opp til en dialog med næringslivet og kommunal sektor i forbindelse med iverksetting av tiltak. KIS kan være arena for slike dialogmøter.

5 Økonomiske og administrative konsekvenser

© Robert Bråthen/Samfoto

Primæransvaret for sikring av informasjonssystemer og nett ligger hos eier eller operatør, og ligger innenfor ledelsens linjeansvar. Sikkerhetsarbeidet må ivaretas i daglig oppgaveløsning og finansieres innenfor rammene for finansiering av den ordinære virksomheten. Hvert fagdepartement har et overordnet sektoransvar. Tiltak i sektorene skal finansieres innenfor gjeldende budsjettrammer.

Forslag til finansiering av ekstraordinære tiltak skal fremmes i den ordinære budsjettprosessen. Samordningsansvaret som Fornyings- og administrasjonsdepartementet har for informasjonssikkerhet skal kun gjelde forebyggende, tverrsektorielt arbeid.

Ord og uttrykk

Autentisering	Mekanisme for verifisering av påstått identitet – at man er den man utgir seg for å være.
Autorisering	Prosessen med å gi tillatelse til å få tilgang til bestemte IKT-ressurser, eller rett til å utføre bestemte handlinger i et system.
Biometri	Autentiseringsløsninger som benytter måling av fysiske egenskaper ved en person (typisk karakteristika ved fingeravtrykk, ansiktsform, ol.)
Botnet	En samling av datamaskiner som kan fjernstyres fra en sentral kilde. Den infiserte datamaskinen fjernstyres ved hjelp av et bot-program og omtales som en (ro)bot eller zombie. Botnet kan f.eks. benyttes i forbindelse med pengeutpressing der datamaskinen kommanderes til å sette i gang distribuerte tjenestenektangrep (DDoS) mot en virksomhets nettsted.
Brannmur	En samling komponenter som er plassert mellom to nettverk, og som til sammen har følgende egenskaper a) all trafikk fra innsiden til utsiden, og motsatt, må passere gjennom brannmuren, b) kun autorisert trafikk, som er definert i lokalt oppsett, vil kunne passere gjennom brannmuren, og c) brannmuren er selv immun mot inntrengning.
CERT	*Engelsk: Computer Emergency Response Team.* Ekspert-team som håndterer sikkerhetshendelser. CERT er et registrert varemerke for Carnegie Mellon University. Mange benytter derfor forkortelsen C(S)IRT; Computer (Security) Incident Response Team.
Digital signatur	PKI-basert elektronisk signatur. Et dataelement som følger en elektronisk melding eller et dokument, som binder dokumentet til en identitet. Digital signatur genereres ved først å lage et digitalt "fingeravtrykk" av dokumentet, og deretter kryptere det med den private nøkkelen til den som skal signere. Se også PKI.
Digitalt sertifikat	En elektronisk legitimasjon for eieren av en privat og en tilhørende offentlig nøkkel som viser at den offentlige nøkkelen tilhører vedkommende. Se også PKI.
Distribuert tjenestenekt	Et tjenestenektangrep som utføres fra flere maskiner mot samme mål samtidig. (Se også Botnet og Tjenestenekt.)
Domenenavnsystem (DNS)	Tjeneste i Internett som oversetter domenenavn (f.eks. www.regjeringen.no) til IP adresser (f.eks. 195.225.0.230).
eID	Elektronisk identifikasjon av en person, en virksomhet, et datasystem el. Kan utføres vha. brukernavn, passord, PIN-kode eller annen egnet teknologi.
Elektronisk spor	Elektronisk lagret informasjon som kan benyttes som bevis eller dokumentasjon. Også kalt elektronisk bevis eller digitalt bevis.
E-signatur	Data i elektronisk form som er knyttet til andre elektroniske data, og som kan brukes som autentiseringsmetode.
Hash-algoritme	Matematisk funksjon som lager et «digitalt fingeravtrykk» av en mengde data. En god hash-algoritme vil alltid lage ulike fingeravtrykk for ulike mengder data, selv om forskjellen mellom data bare er én bit.
Hacking	Slangpreget betegnelse på å gjøre små endringer i datamaskinprogrammer. Brukes ofte i negativ betydning, og da om endringer som gjøres av uautoriserte personer med uhederlige hensikter.

Ikke-benekting (uavviselighet)	Sikkerhet for at en som har sendt en melding gjennom et informasjonssystem ikke kan benekte eller avvise at det er vedkommende som har foretatt handlingen.
Informasjonssikkerhet	Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet for den informasjon som behandles av systemet og systemet i seg selv.
Infrastruktur	Grunnleggende strukturer og systemer som er nødvendige for en organisasjon, en samling organisasjoner eller et land for å fungere på en effektiv måte.
Integritet	Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.
Konfidensialitet	Sikring av at kun autoriserte personer får tilgang til informasjon.
Konvergens	Sammensmelting av medier med basis i digital teknologi. Internett har vært drivkraften for at telekommunikasjon, kringkasting og informasjonsbehandling smelter sammen. Konvergens medfører at skillet mellom data-, telekommunikasjons- og medieesektorene blir utydelig.
Kryptering	Å forvanske en tekst (eller et bitmønster) til en uleselig, uforståelig såkalt chiffertekst som bare kan dekrypteres ved hjelp av en krypteringsnøkkel.
Ormer	Programvare som er i stand til å spre seg selv fra maskin til maskin. I tillegg til å kunne spre seg selv, vil programvaren foreta uønskede handlinger som å legge igjen ondsinnet programvare som tastaturloggere, tjenerer for fjerntilgang til datamaskinen, botnet etc.
Phishing	Forsøk på å tilegne seg uberettiget informasjon som f.eks. passord og bankopplysninger. Et typisk eksempel er en falsk e-post fra banken, der mottakeren blir bedt om å følge en lenke til en falsk nettside som tilsynelatende tilhører banken. Der blir mottakeren bedt om å om oppgi personlige bankopplysninger, som deretter benyttes til tyveri eller svindel.
PKI	*Engelsk: Public Key Infrastruckture.* En samling sikkerhetstjenester, sikkerhetskomponenter og aktører som gjør det mulig å bruke digitale signaturer i stor skala. Baserer seg på asymmetrisk kryptografi og bruk av offentlig og privat nøkkel som henger sammen gjennom en matematisk funksjon.
Samfunnskritiske funksjoner	Funksjoner som dekker samfunnets grunnleggende behov og befolkningens tryggheтsfølelse f.eks. bank- og finanstjenester, helse- og omsorgstjenester mv. Se også samfunnskritisk infrastruktur.
Samfunnskritisk infrastruktur	Samfunnets funksjonsdyktighet er svært avhengig av en rekke fysiske og tekniske infrastrukturer. Ved alvorlig svikt i disse infrastrukturene er samfunnet ikke i stand til å opprettholde de leveranser av varer og tjenester som befolkningen er avhengig av (jf. samfunnskritiske funksjoner). Disse infrastrukturene kan omtales som kritiske for samfunnet.
Samtrafikk	Samtrafikk innebærer et samspill mellom ulike tjenesteleverandører på fire nivå: teknisk, policymessig, forretningsmessig og juridisk. Samtrafikk mellom to eID-leverandøres løsninger vil si at man som bruker av deres tjenester kun trenger å forholde seg til en av dem (i likehet med telefontjenester).
Social engineering	Sosial manipulasjon. En måte å manipulere andre menneskers oppfatninger på som bidrar til å skape troverdighet for en aktør med kriminelle hensikter og derigjennom skaffer adgang til å gjennomføre ulovlige handlinger.

Spam	Søppel e-post. Dette dreier seg i hovedsak om masseutsendelse av reklame via e-post. Trusselen ligger i ressursforbruket knyttet til behandling av disse meldingene, samt at legitime meldinger kan drukne i all spamen. Spam kan også benyttes til å spre virus. Tilsvarende som spam benyttes om e-post, benyttes spim om spam via øyeblikksmeldinger (Instant Messages - IM).
Sårbarhet	Sårbarheten til et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten for at trusler vil materialisere seg i en sikkerhetshendelse (eksempler på spesielle omstendigheter kan være størrelse, kompleksitet, at mange aktører er involvert, geografisk spredning, hyppige endringer og utsatt beliggenhet).
Tilgjengelighet	Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.
Tjenestenektangrep	Denial of Service Attack (DoS/DDoS). Angrep mot et nettsted i form av forespørsler for å gjøre det vanskelig for andre å oppnå kontakt med tjenesten som ønskes rammet. I verste fall kan dette føre til at det angrepne nettstedets tjenere vil bryte sammen. Slike angrep kan innebære bruk av flere kraftige datamaskiner (evt. et nettverk av datamaskiner) samtidig (se også Botnet).
Trojanere	Ondsinnet programvare forkledd som et legitimt program. Formålet kan f.eks. være å gi fjerntilgang til datamaskinen, eller å lekke informasjon fra datamaskinen. Den kan enten ligge i dvale og vente på en ekstern hendelse, eller arbeide aktivt i bakgrunnen.
Virus	Ondsinnet program som reproduserer seg selv. Det ligger gjerne som en del av et annet program. Når dette programmet kjøres, kjøres også virusprogrammet.
VPN	*Engelsk: Virtual Private Network.* Nettverk definert via brannmurer, krypteringsalgoritmer osv. for å opprette en beskyttet forbindelse mellom sender og mottaker, normalt over et offentlig nettverk som for eksempel Internett.

Utgitt av:
Fornyings- og administrasjonsdepartementet

Offentlige institusjoner kan bestille flere
eksemplarer av denne publikasjonen fra:
Departementenes servicesenter
Post- og distribusjon
E-post: publikasjonsbestilling@dss.dep.no
Telefaks: 22 24 27 86

Oppgi publikasjonskode: P-0942 B
Trykk: DSS Hurtigtrykk 11/2007 - opplag 1000
Design: www.lucas.no