Informasjonssikkerhet for alle - hvordan er det mulig?

Førsteamanuensis Arild Jansen
Avdeling for forvaltningsinformatikk, Universitetet i Oslo

Foredrag på AFINs jubileumskonferanse 7.september 2004

Er våre liv blitt sikrere? Aldri har vi brukt mer penger og ressurser på sikkerhet. Likevel vil mange hevde at vi er på mange områder blitt mindre sikre enn før. Det er mange grunner til dette; en mer åpen verden, økt kompleksitet og ikke minst den sterkt voksende bruk av nye tekniske systemer. Sosiologen og filosofen Ulrich Beck snakker om "the risk society", hvor han bruker dette begrepet i sin argumentasjon for at vårt samfunn er blitt mer uforutsigbart, og derved økt risiko, gjennom blant at en stadig en økende mengde hendelser som påvirker hverandre og våre liv, og som et resultat av økende avhengighet av stadig mer avanserte tekniske løsninger som også gir uforutsette og uønskede resultater.

Mitt tema er *informasjonssikkerhet for alle*? Hva innebærer dette? Det omfatter selvsagt hele befolkningen, uansett alder, sosial og etnisk bakgrunn, yrkesrolle osv, men også i alle situasjoner i livet, i jobben, i privatlivet og fritiden, på ferie, dvs. i alle roller vi kan ha. Det inkluderer også den sikkerheten knyttet til bruk av ulike typer informasjonssystemer som næringslivet og forvaltningen kan tilby oss.

Dette er et svært omfattende tema; det omfatter alle trusler vi utsettes for og de risikoer løper, både bevist og ubevist, selvforskyldt og uforskyldt, og likeledes de tiltak og foranstaltninger vi kan iverksette. Jeg vil her i hovedsak begrense meg til å snakke om våre felles interesser i sikre *informasjonsinfrastrukturer* og hvilke utfordringer som ligger i dette.

Jeg vil i innlegget begrunne to påstander:

1. Den teknologiske utvikling er ikke lineær eller deterministisk, men har hatt og vil alltid ha både uventede og utilsiktede virkninger mange av disse medfører også svært ofte uønskede konsekvenser. Dette mener jeg også er uunngåelig i framtida; også de nye tekniske løsningene vi utvikler for å løse bestemte problemer også vil skape nye trusler og skadelige virkninger. Elektrisiteten, bilen, flyet, TV-en, datamaskinen, mobiltelefonen har alle negative konsekvenser.
2. Videre vil jeg hevde at truslene og risikoelementene er større og mer komplekse i infrastrukturer enn i enkeltsystemer. Følgelig er de også vanskeligere å håndtere og feil i disse har større konsekvenser. Den økende bruk og avhengighet av nasjonale og internasjonale digitale nettverk og informasjonssystemer skaper en verden det blir stadig vanskeligere å kontrollere. Internett er et godt eksempel på dette, på godt og vondt.

Dersom en aksepterer en slik forståelse av den verden vi lever, må det også få konsekvenser for hvordan vi håndterer utfordringene knyttet til sikkerhet, hvor vi i større grad må være innstilt på å møte uforutsette og uønskede hendelser og konsekvenser og hvem

som skal betale kostnadene ved dette. Med dette mener jeg ikke å uttrykke en generell teknologipessimisme, men heller at vi i større grad må erkjenne disse negative sider og ta de inn i vår håndtering av teknologiutviklingen. Her tror jeg vi har mye å lære av utviklingen av Internett, både på godt og mindre godt.

Det er kanskje på sin plass å klargjøre hvor jeg står- hva er min bakgrunn.

- Jeg er informatiker og faktisk med utgangspunkt i matematikken, opplært til å tro at det er mulig om vi kan lage programmer som det kan beviser er riktige [forutsatt gitte betingelser], men at dette kan være meget krevende,
- Samtidig har jeg lært gjennom arbeid som programmerer og ikke minst som bruker at det i praksis viser seg at datasystemer er svært sjeldne feilfrie. Riktignok viser erfaringene at mange systemer synes å være både svært riktige, robuste og driftssikre, men samtidig har vi nok av eksempler på at systemer ikke fungerer som de skal.
- Jeg har, i arbeidet med bruk av IKT i organisasjon mange ganger erfart at vi kan ikke bare snakke om datasystemer, men også informasjonssystemer, som omfatter menneskelige aktiviteter, som i samspill med omgivelsene gir mange uforutsigbare konsekvenser
- Videre har studier av infrastrukturer vist at de har andre egenskaper enn informasjonssystemer…]

Hva er informasjonssikkerhet?

Vi nyter i dag utstrakt grad av frihet til styre våre egne aktiviteter, ikke minst fordi elektroniske tjenester er tilgjengelige hele tiden. Vi ønsker i dag på den ene siden tilgang til nye og bedre tjenester til alle tider av døgnet: 24-timers banken og 24 timers forvaltningen, butikken, underholdningstilbudet osv. Men på den andre siden ønsker vi maksimal sikring av våre verdier. Vi ønsker også å eksponere oss over nettet for stadig flere, men da uten at andre misbruker opplysninger om oss? Vi lever i en tid med stor endringstakt. Dette må med nødvendighet skape uforutsigbarhet. Men skal også vi måtte avfinne oss med at vår hverdag og våre omgivelser blir mer og mer usikre?

Informasjonssikkerhet er knyttet til trygghet og kontroll over informasjon, gjerne formulert slik: Beskyttelse mot brudd på *konfidensialitet, integritet* og *tilgjengelighet* for informasjonen og også for det informasjonssystemet som informasjonen inngår i. Eller sakt på en annen måte: At vi har robuste og effektive informasjonssystemer, som gir *korrekt informasjon* til *rette personer* til *rett tid.* (Jeg vil ikke i dette foredraget skille mellom informasjons- og datasikkerhet, men det er vikt*ig å g*jøre det i arbeidet med sikkerhet.)

Et kort historisk tilbakeblikk

Problemstillinger knyttet til informasjonssikkerhet ikke er nye, menneskene har alltid vært opptatt av informasjonssikkerhet, både når det gjelder det personlige og nære, og på alle nivåer i samfunnet. I The Code book peker forfatteren Simon Singh at interessen knyttet til informasjonssikkerhet og blant kryptering er av gammel data, og nevner eksempler fra det gamle Hellas, Romerriket, Dronning Mary av Skottland for å nevne noe.

Fra Seip til Seip og Willoch

Debatten om overvåkningssamfunnet knyttet til utbredelsen av datateknologien startet vel i Norge for alvor på slutten 60-tallet, vi fikk lov om personregistre i 1978 og utredningen om samfunnets sårbarhet ble lagt fram i 1986, med daværende Direktør for datatilsynet, nå dessverre avdøde Helge Seip. Utredningen skapte en god del debatt, men Helge Seip var nok svært skuffet over at den gang ansvarlig myndighet ikke tok utredningen fullt på alvor, Det ble konkludert med at oppgavene med å ivareta sikkerhet og sårbarhet på de enkelte samfunnsområder stort sett var det enkelte sektororgans ansvar og myndighet. At totaliteten av usikkerheten og truslene som skaper samfunnets sårbarhet er mer enn summen av den enkelte områders sårbarhet ble nok ikke forstått av sentrale beslutningstakere. Og spesielt ble ikke sikkerhets- og sårbarhetsproblematikken knyttet til felles infrastrukturer tatt alvorlig: Det at det enkelte individ eller organisasjon ivaretar sin sikkerhet, betyr ikke helheten er ivaretatt. Til det er avhengigheten og samvirke mellom oss for stort. En tilsynelatende liten hendelse i et ledd kan få uante konsekvenser i andre deler av samfunnet.

Hva er situasjon i dag? Det er blitt et langt større fokus på sikkerhet de siste 10-15 år, ikke minst på grunn av Internettets utbredelse med sterkt voksende omfang av elektronisk samhandling og forretningsmessige transaksjoner. Likevel sier den siste sårbarhetsutvalget (som ble ledet av Kåre Willoch) at vi i dag har et mye mer uoversiktig trusselbilde, og at sårbarheten er større enn før. Likevel er utvalgets visjon et trygt og robust samfunn som avverger trusler og overvinner kriser. Jeg tror dette er en urealistisk visjon, jeg tror vi må akseptere at den stadige raskere teknologiske utviklingen også vil medføre økende negative konsekvenser. Det er prisen vi må betale for alle de positive sider dette har.

Vi har i dag fått flere nye lover som omfatter sikkerhet; som eksempelvis Lov om personopplysninger omtalt tidligere i dag, Ekom-loven og Lov om elektronisk signatur, sammen med endringer i eksisterende lover. En svært foreløpig gjennomgang gjort ved AFIN (en senere foredragsholder her i dag) indikerer at vi finner sikkerhetsrelaterte bestemmelser i et stort antall lover og forskrifter. Det kan synes som om sikkerhetsområdet langt på vei overregulert, og at dette antakelig medfører overlappende regelverk, lite konsistent begrepsbruk og uklare ansvarsforhold. Jeg sier antakelig fordi vi per i dag ikke har full oversikt over rettstilstanden på området.
Det pågår nå et arbeid i regi av AFIN hvor vi søker å klarlegge den faktiske rettstilstanden og om dette synes å være nødvendig med endringer i lovgivningen på dette området. Vi ønsker også som ledd i dette arbeidet å måle effekten av reguleringsstrategier (internkontroll, tilsyn, graderingar osv.) I dag brukes mange ulike strategier vi ikke fullt ut vet effektene av .

Hva er trusselbildet? Risikokostnad – konsekvensene når uønskede hendelser finner sted.

Den siste sårbarhetsutredningen starter med et sitat av Aristoteles: *"Det er sannsynlig at nye usannsynlig vil skje"*. Dette sitatet burde nok flere ta inn over seg. Sikkerhet har [også] sin motsats i usikkerhet og uforutsigbarhet, men også utrygghet.

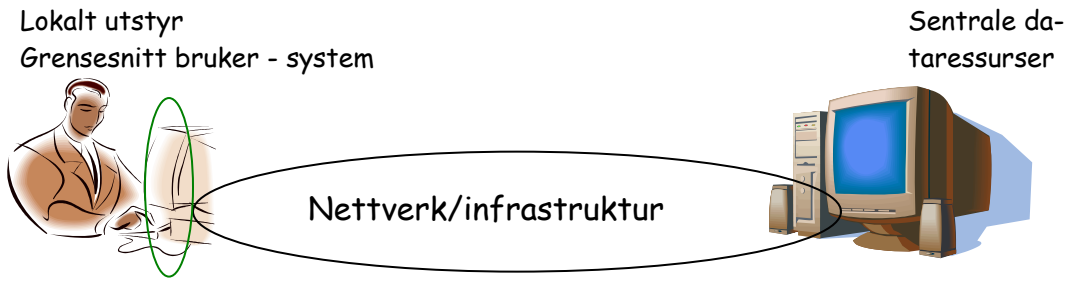
Arbeidet med sikkerhet må ta utgangspunkt en vurdering av trusler og konsekvensene av noen slike trusler realiseres i gjennom uønskede hendelser, som gjerne omtales som *risikovurdering (*også omtalt som *risikoanalyse),* dvs. å beskrive *hva* som skal sikres, videre at en søker å klarlegge hvilke *trusler og farer* som kan føre til uønskede *hendelser* og *sannsynligheten* for at disse inntreffer og likeledes de *konsekvense*r (skadeomfang) slike hendelser kan medføre for virksomheten eller samfunnet (f eks i form av skade eller tap av menneskeliv, økonomiske tap osv). Dette foreligger ulike framgangsmåter og metoder som kan anvendes, en vanlig måte er å beregne den såkalte risikokostnaden på denne måten:

risikokostnad *= skadekostnad* ***x*** *skadefrekvens.*

for derved å kunne iverksette adekvate tiltak som kan sikre tilstrekkelig sikkerhet uten at kostnadene(eller ulempene) ved de enkelte tiltak blir uforholdmessig høye. Det er her prioriteringene kommer inn; det er viktig å sette inn tiltak det risikokostnadene er uakseptable.

Trusler ved vår bruk av IKT

Bruk av moderne IKT-løsninger innebærer mange trusler og risikoer, som forenklet kan illustreres ved denne figuren:



Denne figuren skal illustrere at bruken av et informasjonssystem er avhengig av 3 sett av komponenter:

1. *Brukerens lokale ressurser og hennes* brukergrensesnitt eller interaksjon *med datasystemet*
2. Nettverket *eller infrastrukturen for kommunikasjon mellom bruker og datasystem*
3. Selve datasystemet - *som kan være enkelt eller mer komplisert.*

Summen av truslene vil være trusler rettet mot så vel brukerutstyret og grensesnittet mot brukeren som de rettet mott nettverket og de sentrale dataressursene. Men en ren matematisk summasjon gir ikke et riktig bilde, fordi de ulike hendelsene og deres virkninger kan forsterke hverandre, og derved medføre langt med dramatiske konsekvenser enn de enkeltvis ville gi.
Det er f eks. mulig å avlytte brukerutstyret, som avgir elektromagnetisk stråling, nettverket kan avlyttes og sentrale anlegg kan tappes eller på andre måter angripes.

Arbeidet med sikkerhet vil derfor måtte omfatte sikring av disse komponentene hver for seg, og i tillegg se truslene som skapes gjennom avhengigheten og samspillet mellom dem. I risikovurderingene vil vi se på truslene knyttet til brukerens interaksjon med datasystemet, videre til overføringen av data via et eller annet form for nettverk, og truslene som er forbundet med lagring, bearbeiding og eventuell videre transport av dataene. Sårbarheten i nettverkene og kommunikasjonssystemene er større enn for de lukkede informasjonssystemene fordi de er langt flere brukere og typer anvendelser. Det er så godt som umulig å kontrollere alle brukere. Videre er det ofte vanskelig å klarlegge ansvarsforholdene mellom de ulike deler dersom nettverket omfatter større organisasjoner, ofte er flere virksomheter knyttet sammen ved at deres lokalnett er knyttet til Internet.

Hva bør så den enkelte gjøre? Det er en rekke tiltak vi kan gjøre på vårt eget utstyr og vår egen bruk: Velkjente ting som å passe på brukernavn og passord, ikke engang gi det til egne barn (jeg vil aldri la mine egne barn eller barnebarn bruke min konto, og spesielt ikke for å surfe på Internett). Vi må passe på våre data, backup mm, være restriktive med hva vi gir fra oss av personopplysningar. Noe om PET:

Etter kvart som den økende del av kommunikasjonen foregår trådløst, vel dette medføre økte trusler og risiko, fordi disse er vanskeligere å beskytte. Dette gjelder ikke minst bruk av trådløse lokalnett (såkalte WAN), hvor det er bygget inn lite sikkerhetsmekanismer. Vi har tidligere sett at drosjesjåfører sitter parkert uten Informatikkbygget på Blindern og surfer gratis på Internett via bygget trådløse nettverk. I dag tilbys trådløs oppkobling på kafeer, hoteller, bensinstasjoner etc. for å lokke til seg kunder. Mange har det også hjemme. Jeg vil anbefale at dere bruker trådløse nett med varsomhet, spesielt ved overføring av følsomme opplysninger.

Det er også grunn til å tro at etter kvart som mobiltelefonen blir bruk som betalingsmiddel (lommebok), er faren for misbruk og tyveri av identiteter større. Allerede nå er det mange eksempler på misbruk av identitet på nettet, modemtyveri. Mange med faste linjer, f eks. bredbåndsabbonnement opplever at uvedkommende "låner" deres forbindelse og identitet. Det anbefales derfor å koble seg ned så snart en er ferdig med en sesjon

Særlig når det gjelder personopplysninger som har økonomisk verdi eller på anen måte er følsom bør en være svært varsom. De fleste av oss er ikke klar over hvor raffinerte mange programmer er i å samle opp og "rapportere" tilbake bestemte nettsteder våre aktiviteter på Internett (såkalte cookies – eller kjeks). Dette gjelder jo ikke minst det velkjente selskapet Mikrosoft, som faktisk insisterer på å kunne kontrollere og rapportere tilbake til hvordan vi bruker vår datamaskin når vi kjører deres produkter. Dette er ikke primært et sikkerhetsproblem, men innebærer en form for overvåkning vi ikke aner konsekvensene av. Dataene de samler inn sendes over nettet som kan representerer mange trusler. Men det finnes etter hvert en del såkalte personvern-økende tekniske løsninger, hvor en på ulike måter søker å redusere faren personopplysninger kommer på avveie eller blir misbrukt.

Kan vi kontrollere den teknologiske utviklingen?

Det synes for å være et paradoks at når vi oppdager at en ny teknologi skaper uforutsette trusler og risikoer, så bruker vi langt på vei de samme teknologiene for å bøte på problemene. Dette skyldes vår urokkelig tro på at nye og bedre tekniske systemer kan løse dagens problemer, både når det gjelder sikkerhet og andre problemer.

Jeg vil påstå at dette bygger på en noe naiv forestilling av hva teknologisk utvikling innebærer. Erfaringene gjennom hundrer av år har vist at den teknologiske utvikling er ikke lineær eller deterministisk, men har både uventede og utilsiktede virkninger, og mange av disse medfører også svært uønskede konsekvenser. Nye tekniske systemer som skal bidra til å løse bestemte problemer eller utføre gitte oppgaver vil også innebære nye og uønskede problemer. Trafikkproblemer, miljøkonsekvenser, er eksempler på dette. Fra IKT-sektoren kan vi nevne systemfeil, virus og ormer etc., hacking og andre former for datakriminalitet osv.

Et konkret eksempel. Ved innføring av bankkort bedyret bransjen at slike systemer var tilnærmet 100 % sikre dersom pin-koder ble hemmeligholdt. De la alt ansvar over på brukerne hvis noen urettmessig klarte å skaffe seg ulovlig adgang til en konto. I ettertid har det vist seg at disse kortene og bankterminalene langt fra er sikre. Men en rekke uskyldige brukere har måttet slite for bevise sin uskyld og få sin rettmessige erstatning. Nå erkjenner bransjen at systemene er usikre. Men fortsatt må nok kunder slåss for å få rettmessige penger tilbake.

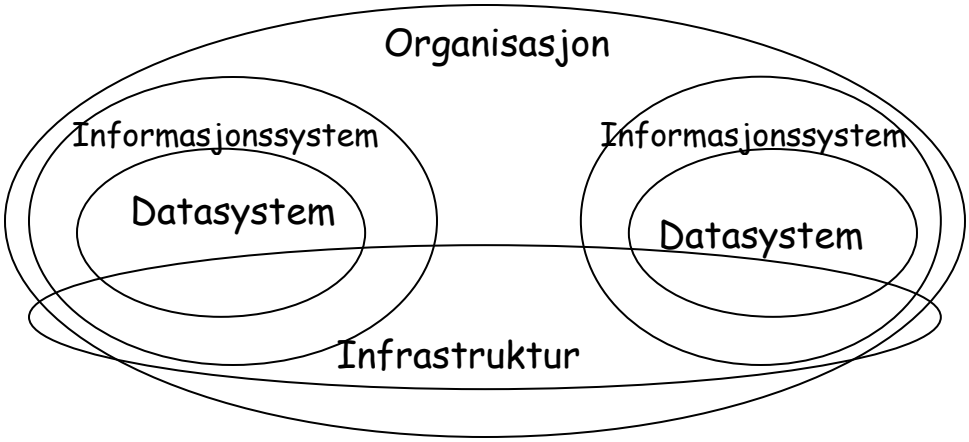
Et annet eksempel er nøkkelkort, som jeg personlig har mange negative erfaringer med.

Nå mener jeg ikke at vi skal gi opp slike nye tekniske løsninger. Men vi må regne med at de ikke fungerer, særlig i de innledende faser, og derfor ha forberedt tiltak som kan bøt e på dette.

Jeg frykter at noe tilsvarende vil skje når de nye digitale signaturene. Uten å gå i detalj er det ikke så vanskelig å se at det vil medføre nye sikkerhetsproblemer som vi nok ikke er tilstrekkelig forbredt på. Likeledes tror jeg at nye biometriske eller andre identifikasjonsløsninger vil innebære nye trusler, særlig fram kriminelle miljøer..

Informasjonssikkerhet og infrastrukturer

Når år vi går fra å se på den enkelte bruker og hans/hennes bruk av IKT til å se på infrastrukturer mer generelt blir bilde som sagt langt mer komplekst.
Denne enkle modellen være hensiktsmessig, hvor vi da tenker på infrastrukturer i organisasjoner, men modellen kan også utvides til i å gjelde i samfunnet generelt.



Figur I: Sammenheng mellom datasystem, informasjonssystem, infrastruktur og organisasjon

Problemet med datakvalitet er velkjent, og vi vil i økende grad være avhengig av at dataene om oss er korrekte.

Vi vil peker på at en infrastruktur har blant annet disse egenskaper

- en ressurs som er *åpen* og *felles* som kan *deles av mange*
- *generelt tilgjengelig* på en *konsistent* måte for alle potensielle brukere
- *tilretteleggende og muliggjørende (enabling*), ved å kunne utgjøre en basis for alle brukergrupper, ulike typer anvendelser og organisasjonsformer,
- Har et s*tandardisert* grensesnitt mot omverdenen, og bygger på internasjonale standarder
- varighet - *stabil* over tid og økonomisk *'stabilitet'*, ved å kunne møte behov hos både tilbydere og brukere, men samtidig hele tiden under utvikling.
- Den er *heterogen* ved at består av mange ulike typer komponenter og er en *sosioteknisk* konstruksjon, lagdelt

Videre bygger en infrastruktur på en "*installert base"*, dvs. en forhistorie av tekniske, organisatoriske og sosiale strukturer den må forholde seg til. Som illustrasjon kan nevnes at dagens sporbredde på togene har sin bakgrunn i avstanden mellom hjulene på oksekjerrene under romerriket, og vårt tastatur på PC-en ble utformet for å fungere på de første mekaniske skrivemaskiner for ca 150 år siden.

Likeledes kan det pekes på at fungerer som en *integrert* del av *praksis*, den oppleves 'usynlig', som først blir synlig *ved sammenbrudd* og derved demonstrerer vår avhengighet av denne. Den kan derfor (normalt ikke) 'avgå med døden, men gradvis erstattes med noe annet som viderefører de ønskede egenskapene.

Dette skiller informasjonsinfrastrukturer fra vanlige informasjonssystemer som har begrenset bruksmåter og brukergrupper, begrenset levetid og [som oftest] kan erstattes. Normalt blir de utviklet og kontrollert av en organisasjon.

Disse egenskapene og kravene til en infrastruktur innebærer at arbeidet med så vel utvikling som vedlikehold og videreutvikling av en generell IKT infrastruktur langt mer krevende enn for enkeltstående IKT-løsninger. Vi må hele tiden ta hensyn til både fortiden, nåtiden og forventninger om framtida. Mange vil hevde at en del av disse egenskapene synes å være i motstrid med hverandre, i alle fall når det gjelder arbeid med innformasjonssikkerhet. Tilstrekkelige sikkerhetsløsninger kan skape et problem i forhold til at en skal være åpen, generelt tilgjengelig og deles av mange. Nye sikkerhetsløsninger kan forhindre kompatibilitet med gammelt utstyr eller med nødvendig fleksibilitet osv. Dersom en oppdager et alvorlig sikkerhetshull og ønsker å ta den ned for en periode, vil dette kunne ha dramatiske konsekvenser for store brukergrupper, og oppfattes som uakseptabelt.

Dette tilsier en annen form for 'styring' enn måten vi tradisjonelt håndterer IKT-systemer. I faglitteraturen bruker en derfor begreper som "drifting" og "kultivasjon" for å illustrere at det dreier seg om å håndtere store dynamiske og organiske strukturer som utvikler seg i uforutsette retningar. Mange aktører, både på utvikler- og brukersiden drar i ulike retninger, og er ikke under styring av en sentral ledelse med alle "fullmakter". Utvikling og drift av informasjonsinfrastrukturer kan derfor ikke planlegges og styres slik som f eks. tradisjonelle kvalitetssikringssystemer forutsetter. [eksemplet SMS som tillegg til mobiltelefonen].

Her mener jeg vi kan lære av Internets utvikling, som ikke var basert på topp-styrt, spesifikasjonsdrevet utvikling hvor alle krav skulle oppfylles med første versjon, men snarere en evolusjonær, skritt-for-skritt utvikling med minimumsløsninger og fleksibilitet og forbedringer etter hvert som det viste seg nødvendig. Samtidig har vi sett hvordan både sikkerhetsproblemene og andre problemer med Internett har vært og nok fortsatt er sterkt undervurdert. Det anslås at konsekvenser av kriminaliteten knyttet til bruk av Internett utgjør i dag flere hundre Mrd. €. Meg bekjent er det gjennomført få omfattende sårbarhetsanalyser av konsekvensene ved bruk av Internett til sivile formål.

Disse utfordringene gjelder ikke bare tradisjonelle tekniske infrastrukturer, men i minst like stor grad når generelle informasjonssystemer får karakter av informasjonsinfrastrukturer. Når en økende mengde felles kritiske informasjonssystemer inngår i vår felles informasjonsinfrastruktur, vil dette skape en kvalitativt ny type sårbarhet. I dag er f eks. de elektroniske betalingssystemene med databaser inneholdende våre konti en del eksempel på dette. Vi kan i kortere perioder klare oss med kontanter og kredittkort, men neppe over mange dager.

Innen det offentlige ønsker vi at en rekke personopplysninger skal være tilgengelige for mange offentlige etater. Mange peker på de store gevinster både den enkelte og samfunnet vil ha av at viktige helseopplysninger om oss (blodtype, sykdomshistorien, allergier osv.) etter hvert genetiske opplysninger er tilgjengelig til enhver tid for å sikre rask og korrektbehandling. Dette høres jo umiddelbart meget fornuftig ut. Men har vi gjennomført en tilstrekkelig omfattende sikkerhets- og sårbarhetsanalyse hvor konsekvenser både for samfunnet og enkeltmennesker er vurdert når systemer ikke fungerer eller gi feilakti-

ge data. F eks. vil for strenge sikkerhetstiltak kunne redusere tilgjengeligheten slik at datakvaliteten blir for dårlig, slik at viktige oppdateringer ikke blir foretatt når de skulle.

Jeg påstår, basert på tidligere erfaringer, at ingen større IKT-systemer og spesielt ingen infrastrukturer er i nærheten av 99 % sikkerhet, og jo mer komplekse disse systemer blir, jo vanskeligere blir sikkerhetsarbeidet. Derfor blir en avveining mellom sikkerhet, tilgjengelig, funksjonalitet og sårbarhet ekstra viktig.

Mitt avslutningsspørsmål blir da:
- Hva er akseptabel risiko og hvordan bestemmer vi den?

Vi må også stille spørsmålet om hvor stor risiko er vi villig til å ta; og hvem bør eller skal bære kostnadene ved dette. Vi kan ikke bare uten videre akseptere at forvaltninga og næringsliv- i samfunnets interesse utvikler nye løsninger hvor det er borgerne som må bære "kostnadene" når noe går galt.

Kunnskaper om risiko og konsekvenser av nye teknologiske løsninger kan vi imidlertid ikke få i tilstrekkelig grad ved skrivebordet. Det kan vi bare få gjennom praktisk bruk. Men det er viktig at vi går noe forsiktig fram når nye store systemer skal settes i drift, hvor vi legger til grunn at vi må regne med feil og sammenbrudd, og foreberede oss på et.

Jeg vil derfor avslutte med 4 "råd" jeg tror kan bidra til informasjonssikkerheten blir bidra – om ikke så god vi kunne ønske oss

1. I utvikling av nye IKT-løsninger og spesielt infrastrukturer må vi i langt større grad må erkjenne at disse systemer innebærer en betydelig risiko og sårbarhet, og at det legges realistiske sårbarhetsvurderinger til grunn omfanget så vel som bruksmåter
2. Vi må ikke alene fokusere på å lage sikre datasystemer isolert, men å forstå dem som komplekse heterogene, sosio-tekniske konstruksjoner hvor de organisatoriske og menneskelige aspekter er like viktige som de teknologiske
3. Videreutvikle lovgivningen på området slik at den framstår mer konsistent og blir forstått av alle berørte parter
4. Vi må derfor arbeide interdisiplinært så vel faglig som metodisk på dette området, noe som også er kjernen i avdelingen for forvaltningsinformatikk.