NÆRINGS- OG HANDELSDEPARTEMENTET

2002

OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk

Mot en sikkerhetskultur

OECD OCDE

ORGANISASJON FOR ØKONOMISK SAMARBEID OG UTVIKLING

e-norge

ORGANISASJON FOR ØKONOMISK SAMARBEID OG UTVIKLING

I henhold til artikkel 1 i konvensjonen som ble undertegnet i Paris 14 desember 1960, og som trådde i kraft 30 september 1961, skal organisasjonen for økonomisk samarbeid og utvikling (OECD) fremme politikk for å:

- Oppnå høyest mulig bærekraftig økonomisk vekst og sysselsetting og økt levestandard i medlemslandene, samtidig som finansiell stabilitet skal opprettholdes, og dermed bidra til utvikling av verdensøkonomien.
- Bidra til sunn økonomisk utvikling i medlemsland og som ledd i det økonomiske utviklingsarbeidet også i land som ikke er medlemmer, og
- bidra til utvidelse av verdenshandelen på multilateralt og ikke-diskriminerende grunnlag i henhold til internasjonale forpliktelser.

De opprinnelige medlemmene av OECD er Østerrike, Belgia, Canada, Danmark, Frankrike, Tyskland, Hellas, Island, Irland, Italia, Luxemburg, Nederland, Norge, Portugal, Spania, Sverige, Sveits, Tyrkia, Storbritannia og USA. Følgende land ble deretter medlemmer på følgende tidspunkter: Japan (28 april 1964), Finland (28 januar 1969), Australia (7 juni 1971), New Zealand (29 mai 1973), Mexico (18 mai 1994), Tsjekkia (21 desember 1995), Ungarn (7 mai 1996), Polen (22 november 1996), Sør-Korea (12 November 1996), og Slovakia (14 desember 2000). EU- Kommisjonen deltar i OECDs arbeid (Artikkel 13 i OECD konvensjonen).

Opprinnelig publisert på engelsk og fransk av OECD under titlene:
OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

Forord

Disse *OECD retningslinjene for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur* ble vedtatt som en anbefaling av OECDs Råd på rådets 1037. sesjon 25 juli 2002.

INNHOLDSFORTEGNELSE

RETNINGSLINJER FOR SIKKERHET I INFORMASJONSSYSTEMER OG NETTVERK

MOT EN SIKKERHETSKULTUR

INNLEDNING

Bruken av informasjonssystemer og nettverk og informasjonsteknologimiljøet i sin helhet har gjennomgått store endringer siden 1992, da OECD offentliggjorde *Retningslinjer for informasjonssystemers sikkerhet*. Disse kontinuerlige endringene byr på betydelige fordeler, men krever også at regjeringer, foretak, andre organisasjoner og individuelle brukere som utvikler, eier, leverer, forvalter, vedlikeholder og bruker informasjonssystemer og nettverk (heretter kalt "aktører"), retter langt større oppmerksomhet mot sikkerheten.

Stadig kraftigere personlige datamaskiner, konvergerende teknologier og den utbredte bruken av Internett har erstattet det som en gang var avgrensede systemer med begrenset kapasitet i nettverk som hovedsakelig var lukket. I dag er aktørene i stadig større grad forbundet med hverandre, og forbindelsene krysser landegrensene. I tillegg støtter Internett kritiske infrastrukturer som f.eks. energi, transport og finans, og spiller en viktig rolle i måten firmaer gjør forretninger på, måten det offentlige leverer tjenester til innbyggere og foretak på, og måten individuelle personer kommuniserer og utveksler informasjon på. Arten og typen teknologier som utgjør infrastrukturen for kommunikasjon og informasjon har også endret seg vesentlig. Antallet og typen utstyr som gir tilgang til denne infrastrukturen er mangedoblet og omfatter faste, trådløse og mobile enheter, og en stadig økende andel tilknytninger er av typen ”alltid på”. Som følge av dette har arten, omfanget og sensitiviteten til informasjon som utveksles, økt betraktelig.

Som et resultat av økende sammenkopling, er informasjonssystemer og nettverk i dag utsatt for stadig flere forskjellige trusler og sårbarhetsfaktorer. Dette reiser nye spørsmål om sikkerhet. Disse Retningslinjene retter seg derfor mot alle aktører i det nye informasjonssamfunnet og peker på behovet for økt bevissthet om og forståelse av sikkerhetsspørsmål samt nødvendigheten av å utvikle en "sikkerhetskultur".

I. MOT EN SIKKERHETSKULTUR

Disse Retningslinjene svarer på et sikkerhetsmiljø i stadig endring ved å fremme utviklingen av en sikkerhetskultur, det vil si å fokusere på sikkerheten ved utvikling av informasjonssystemer og nettverk og å innføre nye tenke- og handlemåter ved bruk av informasjonssystemer og nettverk og ved utveksling av informasjon. Retningslinjene signaliserer et tydelig brudd med en tid der sikker utvikling og bruk av nettverk og systemer altfor ofte bar preg av tilfeldigheter. Aktørene blir stadig mer avhengige av informasjonssystemer, nettverk og tilknyttede tjenester, som alle må være pålitelige og sikre. Kun en tilnærming som tar behørig hensyn til interessene til alle aktørene samt til arten systemer, nettverk og tilknyttede tjenester, kan sørge for effektiv sikkerhet.

Hver aktør spiller en viktig rolle i arbeidet med å styrke sikkerheten. Aktørene må, i tråd med sine respektive roller, være bevisste på risikoer knyttet til sikkerheten og egnede beskyttelsestiltak, påta seg ansvar og treffe tiltak for å styrke sikkerheten til informasjonssystemer og nettverk.

Innarbeiding av en sikkerhetskultur vil kreve både lederskap og omfattende deltakelse, og må resultere i en styrket prioritering av sikkerhetsplanlegging og -administrasjon så vel som en forståelse for sikkerhetsbehovet hos alle aktørene. Sikkerhetsspørsmål må være gjenstand for interesse og ansvar på alle nivåer i offentlig og privat sektor og hos alle aktører. Disse Retningslinjene utgjør et grunnlag for utvikling av en sikkerhetskultur i hele samfunnet. Det vil gjøre aktørene i stand til å innarbeide sikkerhet som en integrert del av utvikling og bruk av alle informasjonssystemer og nettverk. Retningslinjene foreslår at alle aktører innfører og fremmer en "sikkerhetskultur" som en måte å tenke, analysere og handle utfra når det gjelder drift og andre forhold knyttet til informasjonssystemer og nettverk.

II. FORMÅL

Formålet med Retningslinjene er:

- å fremme en sikkerhetskultur blant alle aktører som en måte å beskytte informasjonssystemer og nettverk på.

- å øke bevisstheten om risikoer knyttet til informasjonssystemer og nettverk, om politikk, rutiner, tiltak og prosedyrer som er tilgjengelige for å ta hånd om disse risikoene, og om behovet for at de vedtas og iverksettes.

- å skape større tillit blant alle aktører til informasjonssystemer og nettverk og til måten de utvikles og benyttes på.

- å utarbeide en generell referanseramme som vil hjelpe aktørene med å forstå sikkerhetsrelaterte problemer og å respektere etiske verdier under utarbeidelsen og iverksettingen av samordnet politikk, rutiner, tiltak og prosedyrer vedrørende sikkerhet i informasjonssystemer og nettverk.

- å fremme hensiktsmessige former for samarbeid og informasjonsdeling blant alle aktører under utarbeidelsen og innføringen av politikk, -rutiner, -tiltak og -prosedyrer.

- å fremme hensynet til sikkerheten som en viktig målsetting blant aktører som er involvert i utarbeidelsen eller innføringen av standarder.

III. PRINSIPPER

De følgende ni prinsippene utfyller hverandre og må leses i sin helhet. De retter seg mot aktører på alle nivåer, inkludert politiske og operasjonelle nivåer. Ifølge disse Retningslinjene varierer ansvarsområdene til aktørene etter hvilke roller de har. Alle aktører kan gjennom økt bevisstgjøring, utdanning, informasjonsdeling og opplæring få en bedre forståelse av sikkerhetsrelaterte problemer og innføre bedre rutiner på dette området. Tiltak som tar sikte på å forbedre sikkerheten til informasjonssystemer og nettverk må respektere verdiene i demokratiske samfunn, særlig behovet for åpen og fri flyt av informasjon og grunnleggende prinsipper for personlig integritet.[1]

1) Bevisstgjøring

Aktørene må være bevisste på behovet for sikre informasjonssystemer og nettverk og hva de kan gjøre for å forbedre sikkerheten.

Bevissthet om risikoer og tilgjengelige beskyttelsestiltak er den første forsvarslinjen for sikkerheten til informasjonssystemer og nettverk. Informasjonssystemer og nettverk kan utsettes for både interne og eksterne risikoer. Aktørene må forstå at sikkerhetsbrudd i vesentlig grad kan skade systemer og nettverk under deres kontroll. De må også være oppmerksomme på den potensielle skaden som kan påføres andre som følge av informasjonssystemenes og nettverkenes sammenkopling og gjensidig avhengighet. Aktørene må være oppmerksomme på systemenes konfigurasjon, tilgjengelige systemoppdateringer, systemets plass i nettverkene, gode rutiner som kan innføres for å forbedre sikkerheten samt behovene til andre aktører.

2) Ansvar

Alle aktører er ansvarlige for sikkerheten til informasjonssystemer og nettverk.

Aktørene er avhengige av informasjonssystemer og nettverk som er sammenkoplet på lokalt og globalt nivå. De må forstå hvilket ansvar de har når det gjelder sikkerheten til disse informasjonssystemene og nettverkene og påta seg dette ansvaret på en måte som er i tråd

[1] I tillegg til disse Retningslinjene for sikkerhet har OECD utarbeidet utfyllende anbefalinger vedrørende retningslinjer for andre aspekter som er av betydning for det internasjonale informasjonssamfunnet. Disse omhandler privatlivet (OECDs retningslinjer for personlig integritet og internasjonal trafikk av persondata over landegrensene, 1980) og krypto (OECDs retningslinjer for kryptopolitikk, 1997). Disse Retningslinjene for sikkerhet må leses sammen med de nevnte Retningslinjene.

med deres individuelle roller. Aktørene må regelmessig gjennomgå og vurdere sin egen politikk, rutiner, tiltak og prosedyrer for å sikre at de er tilpasset deres miljø. De som utvikler, utformer og leverer produkter og tjenester må ta hensyn til sikkerheten til systemer og nettverk og utgi hensiktsmessig informasjon, inklusive oppdateringer, til rett tid, slik at brukerne bedre kan forstå sikkerhetsfunksjonene til produkter og tjenester og hvilket ansvar de har i forhold til sikkerheten.

3) Reaksjon

Aktørene må reagere raskt og på en samarbeidsrettet måte for å forebygge, oppdage og reagere på sikkerhetshendelser.

Som følge av sammenkoplingen mellom informasjonssystemer og nettverk og muligheten for en rask og omfattende spredning av skade, må aktørene handle raskt og på en samarbeidsvillig måte for å ta hånd om sikkerhetshendelser. De må dele informasjon om trusler og sårbarhetsfaktorer på en hensiktsmessig måte og innføre prosedyrer som sikrer et raskt og effektivt samarbeid for å kunne forebygge, oppdage og reagere på sikkerhetshendelser. Dersom det er tillatt, kan dette omfatte informasjonsdeling og samarbeid på tvers av landegrenser.

4) Etikk

Aktørene må respektere andre aktørers rettmessige interesser.

Informasjonssystemer og nettverk gjennomsyrer våre samfunn, og aktørene må være innforstått med at deres handling eller mangel på handling kan skade andre. Etiske handlemåter er derfor av avgjørende betydning. Aktørene må strebe etter å utvikle og innføre "best practices" samt å fremme handlemåter som tar hensyn til sikkerhetsbehov og som respekterer de rettmessige interessene til andre aktører.

5) Demokrati

Sikkerheten til informasjonssystemer og nettverk må være forenlig med grunnleggende verdier i et demokratisk samfunn.

Sikkerhet må innføres på en måte som respekterer anerkjente verdier i demokratiske samfunn, herunder frihet til å utveksle tanker og ideer, fri flyt av informasjon, fortrolighold av informasjon og kommunikasjon, nødvendig beskyttelse av personopplysninger, åpenhet og innsyn.

6) Risikovurdering

Aktørene må gjennomføre risikovurdering.

Risikovurdering identifiserer trusler og sårbarhetsfaktorer. Vurderingen må være basert på et så bredt grunnlag at de omfatter de viktigste interne og eksterne faktorer, som f.eks. teknologi,

fysiske og menneskelige faktorer, sikkerhetspolitikk samt tjenester fra tredjepart som har innvirkning på sikkerheten. Risikovurdering vil gjøre det mulig å bestemme hva som er akseptabelt risikonivå, og bidra til å velge egnede kontrolltiltak for å ta hånd om risikoen for potensiell skade på informasjonssystemer og nettverk i lys av arten og viktigheten av informasjonen som skal beskyttes. På grunn av den økende sammenkopling av informasjonssystemer, må risikovurderinger ta hensyn til den potensielle skaden som kan forårsakes av andre eller som kan påføres andre.

7) Sikkerhetsdesign og iverksettelse

Aktørene må gjøre sikkerheten til en integrert del av informasjonssystemer og nettverk.

Systemer, nettverk og politikk må utformes, iverksettes og koordineres riktig slik at de optimaliserer sikkerheten. Et viktig, men ikke utelukkende aspekt i dette arbeidet er utformingen og innføringen av egnede beskyttelsestiltak og løsninger for å unngå eller begrense potensiell skade fra identifiserte trusler og sårbarhetsfaktorer. Både tekniske og ikke-tekniske beskyttelsestiltak og løsninger er påkrevd og må stå i forhold til verdien av informasjonen i virksomhetens systemer og nettverk. Sikkerhet må være et grunnleggende element i alle produkter, tjenester, systemer og nettverk, og en integrert del av systemdesign og -arkitektur. For sluttbrukere består sikkerhetsdesign og iverksettelse hovedsakelig av utvelgelse og konfigurering av produkter og tjenester for deres systemer.

8) Sikkerhetsadministrasjon

Aktørene må innføre en helhetlig tilnærming til sikkerhetsadministrasjon.

Sikkerhetsadministrasjon må være basert på risikovurderingen. Den må være dynamisk og omfatte alle nivåer av aktørenes aktiviteter og alle aspekter av deres virksomhet. Den må omfatte langsiktige reaksjoner på nye trusler og dekke forebygging, identifisering og reaksjon på hendelser, systemgjenoppretting, løpende vedlikehold, gjennomgang og revisjon. Politikk, rutiner, tiltak og prosedyrer vedrørende sikkerheten til informasjonssystemer og nettverk må koordineres og integreres for å skape et samordnet sikkerhetssystem. Kravene til sikkerhetsadministrasjon avhenger av graden av engasjement, aktørenes rolle, den aktuelle risikoen og systemkrav.

9) Løpende vurdering

Aktørene må løpende gjennomgå og vurdere sikkerheten til informasjonssystemer og nettverk og foreta hensiktsmessige endringer i politikk, -rutiner, -tiltak og -prosedyrer.

Nye eller endrede trusler og sårbarhetsfaktorer avdekkes kontinuerlig. Aktørene må derfor løpende gjennomgå, revurdere og endre alle sikkerhetsaspekter for å ta hånd om disse nye eller endrede risikoene.

ANBEFALING AV OECDs RÅD VEDRØRENDE RETNINGSLINJER FOR SIKKERHET I INFORMASJONSSYSTEMER OG NETTVERK

MOT EN SIKKERHETSKULTUR

RÅDET,

Som viser til konvensjonen av 14 desember 1960 om Organisasjonen for økonomisk samarbeid og utvikling, særlig artikkel 1 b), 1 c), 3 a) og 5 b);

som viser til Rådets anbefaling av 23 september 1980 vedrørende retningslinjer for beskyttelse av personlig integritet og flyt av persondata over landegrensene [C(80)58/FINAL];

som viser til erklæringen vedrørende dataflyt over landegrensene, vedtatt av regjeringene i OECDs medlemsland 11 april 1985 [Vedlegg til C(85)139];

som viser til Rådets anbefaling av 27 mars 1997 vedrørende retningslinjer for kryptopolitikk [C(97)62/FINAL];

som viser til erklæringen av 7-9 desember 1998 vedrørende beskyttelse av personlig integritet på globale nettverk [Vedlegg til C(98)177/FINAL];

som viser til ministererklæringen av 7-9 desember 1998 vedrørende autentisering for elektronisk handel [Vedlegg til C(98)177/FINAL];

som erkjenner at informasjonssystemer og nettverk blir stadig mer brukt og er av økende verdi for offentlige virksomheter, private foretak, andre organisasjoner og individuelle brukere;

som erkjenner at den stadig mer betydningsfulle rollen til informasjonssystemer og nettverk og den økende avhengigheten av dem når det gjelder stabile og effektive nasjonale økonomier og internasjonal handel samt i det sosiale, kulturelle og politiske liv, krever spesielle tiltak for å beskytte og øke tilliten til dem;

som erkjenner at informasjonssystemer og nettverk og deres verdensomspennende utbredelse er blitt ledsaget av nye og stadig flere risikoer;

som erkjenner at data og informasjon lagret på eller overført via informasjonssystemer og nettverk er utsatt for trusler som følge av forskjellige former for uautorisert tilgang, bruk, urettmessig tilegnelse, endring, overføring av ondsinnede koder, fornekting av tjeneste eller ødeleggelse, og krever egnede beskyttelsestiltak;

som erkjenner at det er nødvendig å arbeide for økt bevissthet om risikoer knyttet til informasjonssystemer og nettverk og tilgjengelig politikk, rutiner, tiltak og prosedyrer som skal beskytte mot disse risikoene, og å fremme egnede handlemåter som et avgjørende skritt i utviklingen mot en sikkerhetskultur;

som erkjenner at det er behov for å gjennomgå gjeldende politikk, rutiner, tiltak og prosedyrer for å bidra til å sikre at de møter de nye utfordringene samfunnet står overfor som følge av risikoer knyttet til informasjonssystemer og nettverk;

som erkjenner at det er i allmennhetens interesse å fremme sikkerheten til informasjonssystemer og nettverk gjennom en sikkerhetskultur som fremmer internasjonal koordinering og samarbeid for å møte utfordringene knyttet til den potensielle skaden som sikkerhetsbrudd kan påføre nasjonale økonomier, internasjonal handel og deltakelse i det sosiale, kulturelle og politiske liv;

og som videre erkjenner at *Retningslinjene for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur*, som er beskrevet i vedlegget til denne Anbefalingen, er frivillige og ikke berører nasjonenes suverene rettigheter,

og erkjenner at formålet med disse Retningslinjene ikke er å foreslå at det finnes én unik sikkerhetsløsning, eller at en bestemt politikk, rutiner, tiltak og prosedyrer skal tilpasses gitte situasjoner, men snarere å bringe til veie et sett prinsipper for å fremme en bedre forståelse av hvordan aktørene både kan dra fordel av og bidra til utviklingen av en sikkerhetskultur;

TILRÅR at offentlige virksomheter, private foretak, andre organisasjoner og individuelle brukere som utvikler, eier, leverer, forvalter, vedlikeholder og bruker informasjonssystemer og nettverk, iverksetter disse *Retningslinjene for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur*,

ANBEFALER at medlemslandene:

Etablerer ny eller endrer gjeldende politikk, rutiner, tiltak og prosedyrer for å avspeile og ta i betraktning disse *Retningslinjene for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur* ved å innføre og fremme en sikkerhetskultur i overensstemmelse med Retningslinjene.

Samrår, samordner og samarbeider på nasjonalt og internasjonalt plan om iverksettingen av Retningslinjene.

Gjør Retningslinjene kjent for alle deler av offentlig og privat sektor, inkludert offentlige virksomheter, private foretak, andre organisasjoner og individuelle brukere, for å fremme en sikkerhetskultur og oppmuntre alle aktører til å være ansvarlige og til å treffe de nødvendige tiltak for å iverksette Retningslinjene på en måte som står i forhold til deres respektive roller.

Gjør Retningslinjene tilgjengelige for land som ikke er medlemmer så snart som mulig og på en hensiktsmessig måte.

Gjennomgår Retningslinjene hvert femte år med sikte på å fremme det internasjonale samarbeidet om saker som angår sikkerheten til informasjonssystemer og nettverk.

INSTRUERER OECDs komite for informasjon, data og kommunikasjonspolitikk (ICCP-komiteen) i oppgave å fremme iverksettingen av Retningslinjene.

Denne Anbefalingen erstatter Rådets anbefaling av 26 november 1992 vedrørende retningslinjer for informasjonssystemers sikkerhet [C(92)188/FINAL].

PROSEDYREMESSIG FORLØP

OECDs opprinnelige retningslinjer for informasjonssikkerhet forelå i 1992 og ble revidert i 1997. Det foreliggende revisjonsarbeidet ble foretatt av arbeidsgruppen for informasjonssikkerhet og personvern (WPISP), i henhold til mandat fra komiteen for informasjons- data- og kommunikasjonspolitikk (ICCP), og fremskyndet i kjølvannet av 11 september tragedien.

Utforming av retningslinjene ble utført av en ekspertgruppe under WPISP som møtte i Washington DC, 10-11 desember 2001, Sydney 12-13 februar, 2002, og Paris 4 og 6 mars 2002. WPISP møtte i Paris 5-6 mars 2002, 22-23 april 2002 og 25-26 juni 2002.

De foreliggende *OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur* ble vedtatt som en Anbefaling av OECDs Råd på rådets 1037. sesjon 25 juli 2002.