OECD:s riktlinjer för säkerheten i informationssystem och nät

PÅ VÄG MOT EN SÄKERHETSKULTUR

ORGANISATIONEN FÖR EKONOMISKT SAMARBETE OCH UTVECKLING

ORGANISATIONEN FÖR EKONOMISKT SAMARBETE OCH UTVECKLING

Enligt artikel 1 i den konvention som undertecknades i Paris den 14 december 1960 och trädde i kraft den 30 september 1961 skall Organisationen för ekonomiskt samarbete och utveckling (OECD) verka för en politik som går ut på att

- åstadkomma högsta hållbara ekonomiska tillväxt och sysselsättning och en ökad levnadsstandard i medlemsländerna med bibehållen finansiell stabilitet, och på så sätt bidra till världsekonomins utveckling,
- bidra till en god ekonomisk utveckling i medlemsländerna och i icke-medlemsländer inom ramen för den ekonomiska utvecklingsprocessen, och
- bidra till världshandelns utveckling på multilateral och icke-diskriminerande basis i enlighet med internationella åtaganden.

De ursprungliga medlemsländerna i OECD är Österrike, Belgien, Kanada, Danmark, Frankrike, Tyskland, Grekland, Island, Irland, Italien, Luxemburg, Nederländerna, Norge, Portugal, Spanien, Sverige, Schweiz, Turkiet, Förenade kungariket och Förenta staterna. Följande länder blev medlemmar den dag som anges inom parentes: Japan (28 april 1964), Finland (28 januari 1969), Australien (7 juni 1971), Nya Zeeland (29 maj 1973), Mexiko (18 maj 1994), Republiken Tjeckien (21 december 1995), Ungern (7 maj 1996), Polen (22 november 1996), Sydkorea (12 december 1996) och Republiken Slovakien (14 december 2000). Europeiska gemenskapernas kommission deltar i OECD:s arbete (artikel 13 i OECD-konventionen).

Originally published by the OECD in English and in French under the titles:
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

Published by arrangement with the OECD, Paris.
The quality of the Swedish translation and its coherence with the original text is the responsibility of the Ministry of Industry, Employment and Communications.

Originalets titel: 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

Översättning: ÖD-översättargruppen AB

Utgiven av Näringsdepartementet efter en överenskommelse med OECD.

Version 5, 26 augusti 2005.

FÖRORD

OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur antogs som en rekommendation från OECD-rådet vid dess 1 037:e session den 25 juli 2002.

INNEHÅLL

RIKTLINJER FÖR SÄKERHETEN I INFORMATIONSSYSTEM OCH NÄT

PÅ VÄG MOT EN SÄKERHETSKULTUR

FÖRORD

Användningen av informationssystem och nät och hela IT-miljön har förändrats dramatiskt sedan 1992, när OECD först gav ut sina Riktlinjer för säkerheten i informationssystem. Dessa fortgående förändringar innebär betydande fördelar men kräver också ett mycket starkare säkerhetstänkande av alla de myndigheter, företag, organisationer och enskilda användare som utvecklar, äger, tillhandahåller, förvaltar, underhåller och använder informationssystem och nät (”deltagare”).

I stället för de tidigare begränsade, isolerade systemen i till största delen slutna nät har vi fått allt kraftfullare persondatorer, konvergerande teknik och en utbredd användning av Internet. I dag är deltagarna allt oftare uppkopplade mot varandra och uppkopplingarna går över nationsgränserna. Dessutom stöder Internet viktiga infrastrukturer, såsom inom energi-, transport- och finanssektorerna, och spelar en viktig roll för företagens affärstransaktioner, hur stater tillhandahåller tjänster till medborgarna och hur enskilda medborgare kommunicerar och utbyter information. Också tekniken inom kommunikations- och informationsinfrastrukturen har förändrats påtagligt. Antalet varianter av accessutrustningar har mångdubblats och omfattar såväl fasta, trådlösa som mobila utrustningar, och allt fler anslutningar sker genom ständig uppkoppling. Som en följd av detta har den utväxlade informationen förändrats påtagligt i fråga om egenskaper, volym och känslighet.

På grund av den ökade möjligheten att koppla samman informationssystem och nät blir dessa nu utsatta för ett ökande antal och en större mångfald av hot och sårbarheter. Detta medför nya säkerhetsproblem. Dessa riktlinjer vänder sig därför till alla deltagare i det nya informationssamhället och pekar på behovet av en större medvetenhet och insikt om säkerhetsfrågorna och nödvändigheten att utveckla en ”säkerhetskultur”.

I. PÅ VÄG MOT EN SÄKERHETSKULTUR

Dessa riktlinjer har föranletts av att säkerhetsmiljön är i ständig förändring och de syftar till att främja utvecklingen av en säkerhetskultur. Detta betyder att de särskilt fokuserar på säkerhet vid utvecklingen av informationssystem och nät samt införande av nya sätt att tänka och beteenden vid användning av och interagerande inom dessa. Riktlinjerna innebär en tydlig brytning med den tid då säkerheten vid utformning och användning av informationssystem och nät alltför ofta var ett resultat av efterklokhet. Deltagarna blir alltmer beroende av informationssystem, nät och tillhörande tjänster, som måste vara tillförlitliga och säkra. Det är bara genom att ta vederbörlig hänsyn till alla deltagares intresse och systemens, nätens och de berörda tjänsternas natur, som man kan skapa verklig säkerhet.

Varje deltagare spelar en viktig roll för säkerheten. Deltagarna måste, alltefter sin roll i sammanhanget, vara medvetna om säkerhetsriskerna och förebyggande åtgärder, ta sitt ansvar och agera för att öka säkerheten i informationssystem och nät.

Att bygga upp en säkerhetskultur kommer att kräva både ledarskap och ett brett deltagande och bör leda till att säkerhetsplanering och säkerhetshantering får högre prioritet. Likaså måste förståelse skapas hos alla deltagare för behovet av säkerhet. Säkerhetsfrågorna bör hanteras med omsorg och ansvar på alla nivåer i myndigheter och företag och av alla inblandade deltagare. Dessa riktlinjer lägger grunden för arbetet med att införa en säkerhetskultur i hela samhället. På så sätt kommer deltagarna att kunna verka för att säkerheten skall bli en integrerad del i utformningen och användningen av alla informationssystem och nät. Alla deltagare bör införa och främja en säkerhetskultur som ett sätt att tänka, analysera och agera på vid hantering av informationssystem och nät.

II. MÅL

Dessa riktlinjer har som mål att

- främja en säkerhetskultur bland alla deltagare som ett sätt att skydda informationssystem och nät,
- göra deltagarna medvetna om riskerna för informationssystem och nät, om de regler, förfaranden, åtgärder och rutiner som står till buds för att ta itu med dessa risker och om nödvändigheten att införa och tillämpa dessa,
- främja ett ökat förtroende hos alla deltagare för informationssystem och nät och för det sätt på vilket de tillhandahålls och används,
- skapa en allmän referensram som hjälper deltagarna att förstå säkerhetsfrågorna och ta hänsyn till etiska värderingar vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner för säkerheten i informationssystem och nät,
- uppmuntra alla deltagare att samarbeta och utbyta relevant information vid utformningen och användningen av regler, förfaranden, åtgärder och rutiner som rör säkerheten,

– arbeta för att alla som deltar vid utveckling och införande av standarder skall uppfatta säkerhet som ett viktigt mål.

III. PRINCIPER

Följande nio principer kompletterar varandra och skall ses som en helhet. De rör deltagare på alla nivåer, bl.a. beslutsfattare och användare. Deltagarnas ansvar varierar beroende på deras roll. Alla deltagare har nytta av medvetenhet, utbildning, informationsutbyte och praktisk träning som kan leda till ökad förståelse för området och ett bättre säkerhetsarbete. Insatserna för att förbättra säkerheten i informationssystem och nät bör vara förenliga med ett demokratiskt samhälles värderingar, särskilt behovet av ett öppet och fritt informationsflöde och en grundläggande omsorg om personlig integritet[1].

1) Medvetenhet

Deltagarna bör göras medvetna om behovet av säkerhet i informationssystem och nät och om vad de kan göra för att förbättra säkerheten.

Medvetenhet om riskerna och tillgängliga skydd är det första steget för att öka säkerheten i informationssystem och nät. Informationssystem och nät kan hotas av både inre och yttre risker. Deltagarna bör förstå att säkerhetsbrister kan vålla allvarlig skada för system och nät som de kontrollerar. De bör också vara medvetna om att de riskerar att skada andra på grund av systemens sammankopplingar och inbördes beroenden. De bör känna till de egna systemens konfiguration och tillgängliga uppdateringar, systemets plats i nätet, vedertagna metoder för att förbättra säkerheten samt andra deltagares behov.

2) Ansvar

Alla deltagare är ansvariga för säkerheten i system och nät.

Deltagarna är beroende av sammankopplade lokala och globala informationssystem och nät och bör förstå sitt ansvar för säkerheten i dessa. Deras ansvar bör vara anpassat till deras respektive roller. Deltagarna bör regelbundet se över de regler, förfaranden, åtgärder och rutiner som de själva tillämpar och bedöma om dessa är lämpliga för deras miljö. De som utvecklar, utformar och tillhandahåller produkter och tjänster bör ta hänsyn till säkerheten i system och nät. De bör sprida lämplig information, om bl.a. uppdateringar, i rätt tid, så att användarna bättre kan förstå produkternas och tjänsternas säkerhetsegenskaper och vilket deras eget säkerhetsansvar är.

3) Reaktion

Deltagarna bör agera snabbt och samarbeta för att förhindra, upptäcka och reagera på säkerhetsincidenter.

[1] Utöver dessa säkerhetsriktlinjer har OECD utformat kompletterande riktlinjer om andra frågor som är viktiga för det globala informationssamhället. De behandlar skydd för personlig integritet (1980 års *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)* och kryptering (1997 *OECD Guidelines for Cryptography Polic*y). Föreliggande säkerhetsriktlinjer bör läsas tillsammans med dessa dokument.

På grund av informationssystemens och nätens sammankoppling och risken för snabb och omfattande spridning av skador bör deltagarna agera skyndsamt och i samverkan för att hantera säkerhetsincidenter. De bör på lämpligt sätt utbyta information om hot och sårbarheter och införa rutiner för snabbt och effektivt samarbete för att förhindra, upptäcka och reagera på säkerhetsincidenter. Om det är tillåtet kan detta innefatta informationsutbyte och samarbete över nationsgränserna.

4) Etiska aspekter

Deltagarna bör respektera andra deltagares rättmätiga intressen.

Eftersom informationssystemen och näten är så spridda i våra samhällen måste deltagarna vara medvetna om att deras agerande eller underlåtenhet att agera kan skada andra. Ett etiskt uppförande är därför absolut nödvändigt, och deltagarna bör försöka utforma och använda goda förfaranden och sträva efter ett uppförande som tar hänsyn till säkerhetsbehoven och respekterar andra deltagares rättmätiga intressen.

5) Demokrati

Säkerhet i informationssystem och nät bör vara förenlig med de grundläggande värderingarna i ett demokratiskt samhälle.

Säkerhetsarbetet bör genomföras på ett sätt som ligger i linje med de värden som erkänns av demokratiska samhällen, bl.a. friheten att utbyta tankar och idéer, det fria informationsflödet, konfidentialitet för information och kommunikation, skydd för personuppgifter samt öppenhet och insyn.

6) Riskbedömning

Deltagarna bör genomföra riskbedömningar.

Vid riskbedömning kartläggs hot och sårbarheter. Riskbedömningen bör vara tillräckligt omfattande så att den täcker alla viktiga inre och yttre faktorer, t.ex. teknik, fysiska och mänskliga faktorer, regelverk och tredjepartstjänster som kan påverka säkerheten. Riskbedömningar gör det möjligt att fastställa en godtagbar risknivå. Med utgångspunkt i hur den information som skall skyddas är beskaffad och utformad underlättar riskbedömningen också urvalet av lämpliga åtgärder för att hantera risken för möjliga skador på informationssystem och nät. På grund av den ökande sammankopplingen av informationssystem, bör riskbedömningen innefatta den möjliga skada som andra deltagare kan komma att vålla eller utsättas för.

7) Utformning och genomförande av säkerhetsåtgärder

Deltagarna bör införliva säkerheten som ett centralt inslag i informationssystem och nät.

System, nät och regler måste utformas, användas och samordnas på ett sätt som optimerar säkerheten. En viktig inriktning, men inte den enda, är utformningen och

användningen av lämpliga skydd och lösningar för att undvika eller begränsa potentiella skador från identifierade hot och sårbarheter. Det krävs både tekniska och icke-tekniska skyddsåtgärder och lösningar och de bör stå i proportion till värdet av informationen i organisationens system och nät. Säkerheten bör vara ett grundläggande inslag i alla produkter, tjänster, system och nät och integreras vid utformningen och uppbyggnaden av system. För slutanvändarna består skyddsåtgärderna till stor del i att välja och konfigurera produkter och tjänster till sina system.

8) Säkerhetshantering

Deltagarna bör ha ett helhetsgrepp om säkerhetsarbetet.

Säkerhetsarbetet bör grundas på riskbedömning och bör vara dynamiskt, gälla alla nivåer av deltagarnas verksamhet och alla aspekter av deras användning. Säkerhetsarbetet bör ske med framförhållning när det gäller hur man skall reagera på nya hot och gå ut på att förebygga, upptäcka och agera vid incidenter, återställning av system, fortlöpande underhåll, översyn och revision. Regler, förfaranden, åtgärder och rutiner som rör säkerheten i informationssystem och nät bör samordnas och integreras för att skapa ett sammanhängande säkerhetssystem. Kraven på säkerhetshantering beror på graden av delaktighet, deltagarens roll, den aktuella risken och systemkrav.

9) Omprövning

Deltagarna bör se över och ompröva säkerheten i informationssystem och nät och vidta nödvändiga förändringar i fråga om regler, förfaranden, åtgärder och rutiner på säkerhetsområdet.

Nya och föränderliga hot och sårbarheter upptäcks fortlöpande. Deltagarna bör kontinuerligt se över, ompröva och anpassa alla aspekter av de egna säkerhetssystemen för att hantera denna riskutveckling.

REKOMMENDATION FRÅN RÅDET OM RIKTLINJER FÖR SÄKERHETEN I INFORMATIONSSYSTEM OCH NÄT

PÅ VÄG MOT EN SÄKERHETSKULTUR

RÅDET,

som beaktar konventionen om Organisationen för ekonomiskt samarbete och utveckling av den 14 december 1960, särskilt artiklarna 1 b, 1 c, 3 a och 5 b,

som beaktar rådets rekommendation om Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data av den 23 september 1980 [C(80)58(Final)],

som beaktar förklaringen om Transborder Data Flows vilken antogs av regeringarna i OECD:s medlemsländer den 11 april 1985 [Bilaga till C(85)139],

som beaktar rådets rekommendation om Guidelines for Cryptography Policy av den 27 mars 1997 [C(97)62/FINAL],

som beaktar ministerförklaringen om the Protection of Privacy on Global Networks av den 7–9 december 1998 [Bilaga till C(98)177/FINAL],

som beaktar ministerförklaringen om Authentication for Electronic Commerce av den 7–9 december 1998 [Bilaga till C(98)177/FINAL],

som erkänner att informationssystem och nät får allt större användning och är till allt större nytta för offentlig förvaltning, företag, organisationer och enskilda användare,

som erkänner att informationssystemens och nätens allt viktigare roll och det ökande beroendet av dem för stabila och effektiva nationella ekonomier och för den internationella handeln, liksom i det sociala, kulturella och politiska livet, gör att det behövs särskilda skyddsinsatser och förtroendeskapande åtgärder på området,

som erkänner att informationssystemen och näten och spridningen av dem över hela världen har gett upphov till nya och ökande risker,

som erkänner att data och information som lagras i och sprids via informationssystem och nät hotas av olika typer av obehörig åtkomst, användning, orättmätigt tillägnande, förändring, missbruk, överföring av sabotageprogram, tillgänglighetsattacker eller förstöring och kräver lämpliga skydd,

som erkänner att det är viktigt att höja medvetenheten om de risker som hotar informationssystem och nät, att sprida kunskap om de regler, förfaranden, åtgärder

och rutiner som står till buds för att hantera dessa risker och att uppmuntra till ett lämpligt uppförande som ett avgörande steg på väg mot en säkerhetskultur,

som erkänner att nuvarande regler, förfaranden, åtgärder och rutiner måste ses över så att de kan möta de ökande hoten mot informationssystem och nät,

som erkänner att det finns ett gemensamt intresse att främja säkerheten i informationssystem och nät genom en säkerhetskultur som bygger på internationell samordning och samarbete, för att möta de utmaningar som ligger i de potentiella skador som säkerhetsbrister kan vålla nationella ekonomier, internationell handel och deltagandet i det sociala, kulturella och politiska livet,

som vidare erkänner att de *Riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* som återfinns i bilagan till denna rekommendation är frivilliga och inte inverkar på nationernas suveräna rättigheter, och

som erkänner att syftet med dessa riktlinjer inte är att hävda att det finns en enda lösning på säkerhetsfrågan eller att fastställa vilka regler, förfaranden, åtgärder och rutiner som är bäst i en given situation, utan att de bara syftar till att ge ett ramverk för att åstadkomma en bättre förståelse för hur deltagarna både kan dra nytta av och bidra till utvecklingen av en säkerhetskultur,

ÖVERLÄMNAR dessa *Riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* till de myndigheter, företag, organisationer och enskilda användare som utvecklar, äger, tillhandahåller, förvaltar, underhåller och använder informationssystem och nät,

REKOMMENDERAR medlemsländerna att

införa och arbeta för en säkerhetskultur enligt beskrivningen i *OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur* och se till att regler, förfaranden, åtgärder och rutiner på säkerhetsområdet utformas i enlighet med dessa riktlinjer,

samråda, samordna och samarbeta på nationell och internationell nivå för att främja användningen av riktlinjerna,

sprida riktlinjerna inom den offentliga och privata sektorn, bl.a. myndigheter, företag, organisationer och enskilda användare, för att främja en säkerhetskultur och uppmuntra alla berörda parter att ta sitt ansvar och vidta nödvändiga åtgärder för att använda riktlinjerna på ett sätt som är avpassat för deras individuella roll,

ställa riktlinjerna till förfogande för icke-medlemsländer utan dröjsmål och på lämpligt sätt,

se över riktlinjerna vart femte år för att främja internationellt samarbete om frågor kring säkerheten i informationssystem och nät,

ANMODAR the OECD Committee for Information, Computer and Communication Policy att arbeta för att riktlinjerna skall användas.

Denna rekommendation ersätter rådets rekommendation om Riktlinjer för säkerheten i informationssystem av den 26 november 1992 [C(92)188/FINAL].

BAKGRUND

Säkerhetsriktlinjerna sammanställdes första gången år 1992 och reviderades år 1997. Den aktuella översynen företogs under 2001 av the Working Party on Information Security and Privacy (WPISP), enligt ett uppdrag från the Committee for Information, Computer and Communications Policy (ICCP), och påskyndades efter händelserna den 11 september.

Den slutliga versionen sammanställdes av en expertgrupp från WPISP som sammanträdde i Washington, DC, den 10–11 december 2001, i Sydney den 12–13 februari 2002 och i Paris den 4 och 6 mars 2002. WPISP sammanträdde i Paris den 5–6 mars 2002, 22–23 april 2002 och 25–26 juni 2002.

OECD:s riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur antogs som en rekommendation från OECD-rådet vid dess 1037:e session den 25 juli 2002.

Originalets titel: **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. ISBN 9264059172, © 2002, Organisation for Economic Co-operation and Development (OECD), Paris.

Översättningen utgiven efter en överenskommelse med OECD, det är inte en officiell OECD-översättning.

The original version of this book was published under the title **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. ISBN 9264059172, © 2002, Organisation for Economic Co-operation and Development (OECD), Paris.

This translation is published by arrangement with the OECD. It is not an official OECD translation.

www.oecd.org/publishing/translations – Translated versions of OECD publications
www.oecdbookshop.org – OECD online bookshop
www.sourceoecd.org – OECD e-library
www.oecd.org/oecddirect – OECD title alerting service