Sertifisering av IT-sikkerhet

Innhold

Forord

I NOU 2000:24 "Et sårbart samfunn", også kjent som Willoch-utredningen, står det: "Det er behov for å fastsette klare sikkerhetskrav i forbindelse med etablering og drift av kritiske IKT-systemer. Sertifiseringsarbeidet er et viktig fundament for dette arbeidet".

Nasjonal strategi for informasjonssikkerhet for perioden 2003-2006 peker på at "kritiske IT-systemer og –infrastruktur bør beskyttes gjennom sertifiserte sikkerhetsløsninger". I "Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007 – 2010" blir det understreket at "myndighetene bør oppfordre alle virksomheter og leverandører til å ta i bruk sertifiserte løsninger".

Det er komplisert å danne seg et korrekt bilde av hvilket sikkerhetsnivå et IT-produkt har, og det er ikke gitt at offentlig eller privat sektor selv har nødvendig bestillerkompetanse. Stadfestelse av om sikkerhetskrav er oppfylte fordrer særskilt kompetanse, utstyr, standard og metodikk. Det er både samfunns- og bedriftsøkonomisk mest rasjonelt at slike vurderinger utføres i et spesialisert miljø av en uhildet tredjepart med internasjonal forankring.

SERTIT er en offentlig myndighet med rett til å utstede internasjonalt anerkjente sertifikater. Det er utvilsomt et konkurransemessig fortrinn å kunne vise til gyldige sikkerhetssertifikater som demonstrerer at produktet er grundig testet og dokumentert. For den som skal anskaffe er det betryggende å vite at produktet har sertifiserte sikkerhetsegenskaper.

Hensikten med denne brosjyren er å gi en introduksjon til IT-sikkerhet, sertifisering av IT-sikkerhet og internasjonalt samarbeid. For ytterligere informasjon om sertifisering eller sertifiseringsordningen vises til SERTITs nettsted, sertit.no.

Bærum, oktober 2009

Kjell W. Bergan
leder for SERTIT

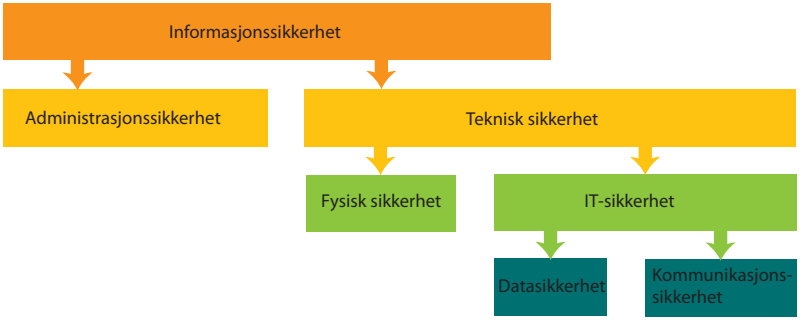
IT-sikkerhet

Samfunnets avhengighet til IT er vokst i takt med nye løsninger for lagring, sammenkobling, bearbeiding og distribusjon av informasjon. Norge ligger langt fremme i å ta i bruk nye løsninger sammenliknet med mange andre land. Økt avhengighet til IT innebærer samtidig økt sårbarhet for samfunnet og den enkelte innbygger, noe som er grundig omtalt blant annet i sårbarhetsutvalgets utredning. Det kan eksempelvis være vanskelig å balansere behovet for ny funksjonalitet mot behovet for robusthet i løsningen og adekvat beskyttelse av informasjonen. Samfunnets og det enkelte individs avhengighet til IT er betydelig, og behovet for stabile og robuste IT-systemer er større enn noen gang. Det er behov for å vite at informasjonen er tilgjengelig til rett tid, i rett form og med tilstrekkelig beskyttelse der det er nødvendig. Det er derfor viktig å kjenne IT-produktenes tilstand og robusthet når IT-systemet skal utformes.

For at din organisasjon skal ha tillit hos samarbeidspartnere og brukere og utføre oppgavene, er dere helt avhengige av velfungerende og robuste IT-løsninger. Virksomheter med ansvar for kritisk infrastruktur står i en særstilling når det gjelder krav til sikkerhet i IT-løsningene.

Sikre IT-systemer

IT-systemer blir stadig mer sammensatte og komplekse, og det er et økende behov for å koble sammen ulike systemer. Et godt eksempel på dette er det gjensidige forholdet mellom el-, tele- og IT-systemer der feil i ett av systemene kan få store konsekvenser for de andre. Den samfunnskritiske informasjonsstrukturen er samtidig en del av øvrig samfunnskritisk teknisk infrastruktur og påvirker alle deler av samfunnet.



En kontinuerlig forbedring av sikkerheten i informasjonssystemene er en

grunnleggende forutsetning for informasjonssamfunnet. All bruk av IT er avhengig av at IT-produktene har de sikkerhetsegenskapene som gir den beskyttelsen som kreves og loves.

Standardisering og IT-sikkerhet

Formålet med standardisering er å forenkle virksomheter/aktiviteter i samfunnet. Det forutsetter derfor samarbeid og enighet mellom representanter for de ulike samfunnsinteresser. Standardiseringen skal tilgodese behov og ønsker fra mange forskjellige parter og bør så langt det er mulig møte alles interesser.

En kjøper skal kunne stole på at sertifiserte produkter tilfredsstiller gitte sikkerhetskrav. En utvikler eller leverandør angir kravene i et eget dokument, kalt "Security Target". En tredjepart – et evalueringsfirma – gjennomfører evalueringen og nødvendige tester. Sertifiseringen uføres av sertifiser-ingsmyndigheten, og dersom kravene er oppfylte kan sertifikat utstedes.

Common Criteria (CC)

CC ble opprinnelig utviklet i et samarbeid mellom USA, Canada, Storbritannia, Frankrike, Nederland og Tyskland basert på eksisterende nasjonale kriterier. Første offisielle versjon ble utgitt i 1999 og gjeldende utgave, versjon 3.1 ble utgitt i 2007. CC er også en ISO/IEC standard. I mai 2000 ble det etablert et internasjonalt arrangement (CCRA) som forvalter og videreutvikler CC.

Common Criteria er en standard for å stille krav, angi og evaluere IT-sikkerhet. Kravene til IT-sikkerhet i CC stilles på to ulike områder:

- Krav til sikkerhetsfunksjonalitet, dvs hvilke sikkerhetsfunksjoner som er nødvendige for å møte gitte trusler.
- Krav til tillit, dvs hvor grundig sikkerhetsfunksjonene skal vurderes og verifiseres.

CC er derfor et rammeverk som beskriver de funksjonelle krav til IT-sikkerhet og en samling krav for å vurdere tillit til produktet.

CC angir 7 tillitsnivåer, Evaluation Assurance Levels (EAL), der EAL 1 er det laveste nivået og EAL 7 er det høyeste. Nødvendig tillitsnivå avhenger av faktorer som eksempelvis beskyttelsesverdien, driftsmiljøet, trusselbildet, og akseptabel restrisiko. Tillitsnivåene gir en mulighet tilå balansere behovet for tillit til IT-produkter. Figuren på neste side gir en forenklet fremstilling av noen mulige bruksområder

for de ulike tillitsnivåene.

Krav til IT-sikkerhet

Kravene til IT-sikkerhet kan gis i form av kravprofiler, Protection Profiles (PP), som gir generelle sikkerhetskrav til en viss type produkter. Det finnes sertifiserte PP-er for blant annet brannmurer, databaser, IDS, smart-kort, VPN, WLAN og operativsystemer.

Implementerte krav spesifiseres i et dokument, Security Target (ST).

Kravdokumentet (ST) skal følge de formkrav som er gitt i CC. Dette gjør det mulig å sammenligne ulike produkters sikkerhetsmessige egenskaper.

CC stiller krav om dokumentasjon av hvordan IT-produktet settes i sikker drift, og hvilke krav som stilles til miljøet og administrativ sikkerhet.

Common Criteria består av tre deler:
Del 1 gir en introduksjon til metode, terminologi og aktuelle aktører,
del 2 angir de funksjonelle sikkerhetskravene,

del 3 angir tillitskravene.

I tillegg finnes Common Evaluation Methodology (CEM) (ISO/IEC 18045) som er en standardisert metodikk som i detalj regulerer prinsippene for og trinnene i en sikkerhetsevaluering i henhold til CC.

ISO/IEC Guide (ISO/IEC TR 15446) er en veiledning for å skrive kravprofiler (PP) og kravdokumenter (ST).

Sertifiseringsprosessen

Når et IT-produkt skal sertifiseres, skjer det gjennom en prosess som består av to hoveddeler; evaluering og sertifisering.

Evaluering

Evaluering er en gransking av om de tekniske sikkerhetskravene er oppfylte og har tilstrekkelig tillit. Evalueringen utføres av en uhildet, spesielt godkjent tredjepart – et evalueringsfirma – etter metodikken angitt i CEM.

Resultatene fra evalueringen er fremstilt i en teknisk evalueringsrapport som gir grunnlaget for sertifiseringen.

Sertifisering

Sertifiseringsmyndigheten kontrollerer om de fremlagte evalueringsbevisene er tilstrekkelige og konsistente. Dersom evalueringsrapporten blir funnet i orden stadfestes resultatet ved at det utarbeides en sertifiseringsrapport og utstedes et sertifikat. Sertifiseringsrapporten angir blant annet:

- Tillitsnivå og relevant funksjonsstyrke
- Funksjonell og organisatorisk sikkerhetspolicy
- Truslene som produktet beskytter mot
- Forutsetninger
- Krav til produktets omgivelser

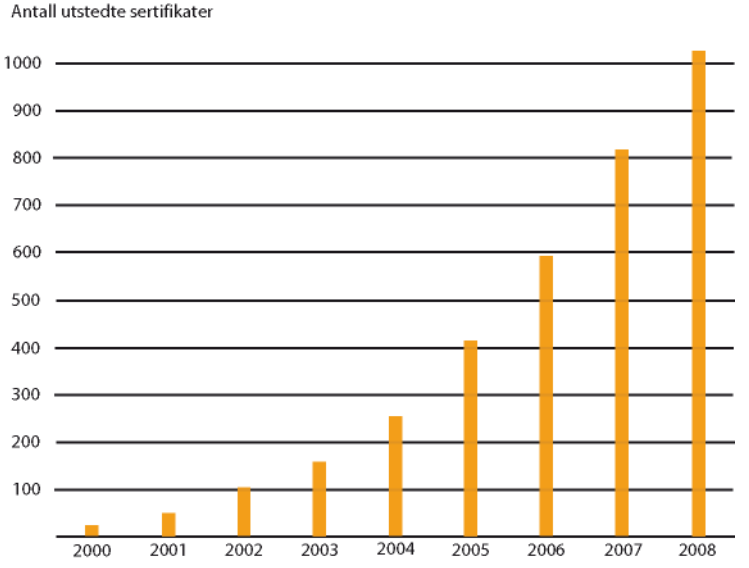
- Sårbarhetsanalyser
- Resultater av funksjonelle tester
- Resultater av penetrasjonstesting
- Eventuelle anbefalinger

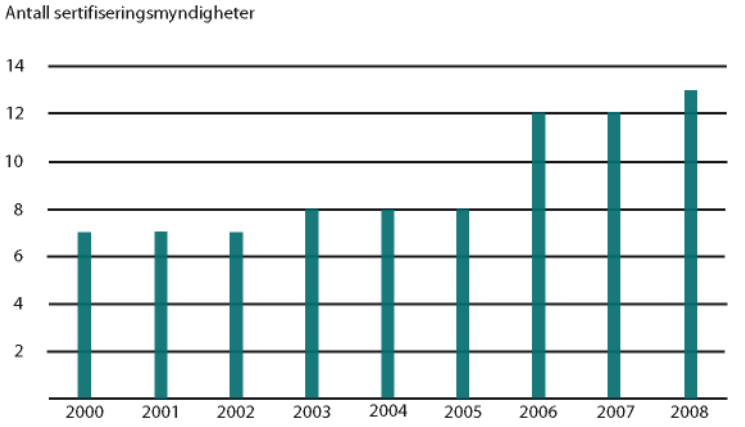
Oppsummering av noen fordeler med sertifiserte produkter

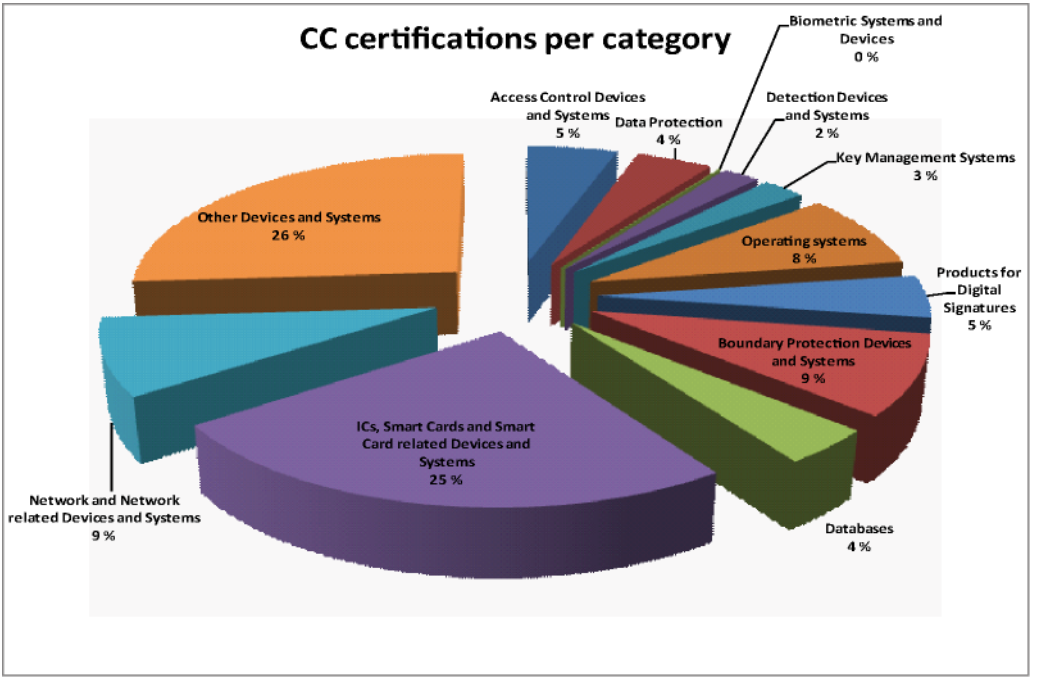
- Produktet er gjort gjenstand for en uhildet tredjepartsundersøkelse
- Produktet er klassifisert ved at det tilfredsstiller et bestemt tillitsnivå
- Sikkerhetsegenskapene er velprøvde og dokumenterte
- Sertifiseringen er basert på en anerkjent internasjonal standard og metodikk
- Innbyr til økt tillit til virksomheten
- Bidrar til bedre beskyttelse av virksomhetskritisk informasjon
- Bidrar til bedre tilgjengelighet gjennom et mer pålitelig IT-system
- Gir bedre forutsigbarhet

Common Criteria Recognition Arrangement

Norge er medlem av Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA). Som navnet sier er det et arrangement som innebærer gjensidig anerkjennelse av sertifikater utstedt av medlemslandene.




Antall sertifiseringsmyndigheter
14
12
10
8
6
4
2
2000
2001
2002
2003
2004
2005
2006
2007
2008


CC certifications per category
Biometric Systems and Devices 0 %
Access Control Devices and Systems 5 %
Data Protection 4 %
Detection Devices and Systems 2 %
Key Management Systems 3 %
Other Devices and Systems 26 %
Operating systems 8 %
Products for Digital Signatures 5 %
Boundary Protection Devices and Systems 9 %
ICs, Smart Cards and Smart Card related Devices and Systems 25 %
Network and Network related Devices and Systems 9 %
Databases 4 %

CCRA arbeider for å:

- Sikre at evalueringen skjer med høy troverdighet og konsistens.
- Øke tilgjengeligheten av sertifiserte produkter og kravprofiler (PP).
- Eliminere behovet for dublerte evalueringer.
- Kontinuerlig utvikle CC med tilhørende metodikk.
- Godkjenne og føre tilsyn med sertifiseringsmyndighetene.

Ved inngangen til 2010 er det 26 medlemmer i CCRA. Det er to typer medlemskap:

Sertifikatkonsumerende medlem

Sertifikatkonsumerende medlemmer i CCRA kan ikke utstede internasjonalt anerkjente sertifikater, men står fritt til å utstede nasjonale sertifikater. Nye medlemmer kan først vurderes som sertifikatproduserende medlemmer etter to år.

Sertifikatproduserende medlem

Sertifikatproduserende medlemmer i CCRA utsteder internasjonalt anerkjente sertifikater. Dette betyr at sertifikater automatisk anerkjennes av samtlige medlemmer i CCRA. Denne anerkjennelsen er ikke det samme som en godkjenning for bruk og må heller ikke forstås som en produktanbefaling. Anerkjennelsen betyr at medlemslandene går god for kvaliteten på sertifiseringen.

Norge er godkjent som sertifikatproduserende medlem i CCRA.

For oversikt over alle medlemmene i CCRA vises det til:
www.commoncriteriaportal.org

Sertifiseringsmyndigheten for IT-sikkerhet – SERTIT

SERTIT ble opprettet gjennom en stortingsbeslutning i 1998 som et resultat av en utredning i regi av Rådet for IT-sikkerhet fra 1997.

SERTIT er lagt til Nasjonal sikkerhetsmyndighet (NSM). Det er etablert et Fagråd for SERTIT oppnevnt av Forsvarsdepartementet i samråd med Justis- og politidepartementet og Fornyings- og administrasjonsdepartementet.

SERTITs hovedoppgaver

- utstede sertifikater og sertifiseringsrapporter.
- utforme rammevilkår og regler for sertifisering.
- påse at reglene følges av alle parter.
- godkjenne evalueringsfirma og føre tilsyn med disse.
- fører tilsyn med evalueringene.
- representerer Norge i CCRA.
- formidle kunnskap om sertifiseringsordningen og Common Criteria

Den norske sertifiseringsordningen

Det er flere aktører som kan være involvert i evaluerings- og sertifiseringsprosessen i den norske sertifiseringsordningen:

- SERTIT –den offentlige sertifiseringsmyndigheten for IT-sikkerhet.
- EVIT –godkjente evalueringsfirma under den norske ordningen som utfører selve evalueringen av IT-produktet.
- Oppdragsgiver - organisasjon eller person som anmoder om en sertifisering for et bestemt IT-produkt. En oppdragsgiver kan derfor ha ulik tilknytning til IT-produktet eller systemet som skal sertifiseres. En oppdragsgiver kan være en utvikler leverandør, anskaffer eller andre.
- Utvikler - bedrift som produserer IT-produktet som skal sertifiseres. I de tilfeller utvikler ikke har rollen som oppdragsgiver, forutsettes et samarbeid mellom partene i forbindelse med evalueringsprosessen.

For en fullstendig oversikt over evalueringsfirma under den norske sertifiseringsordningen, se sertit.no.

Sertifisering av IT-sikkerhet

Utgitt av: Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT)

Layout: SERTIT

Dokumentet er basert på det svenske dokumentet IT-säkerhetsstandarden Common Criteria (CC) - en introduktion, ISBN: 978-91-85797-02-8, utgitt av Krisberedskapsmyndigheten (KBM). Dokumentet er oversatt til norsk og bearbeidet etter tillatelse fra Sveriges certifieringsorgan

Sd 028 v. 1.0 29.10.2009

SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet
SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Telefon: 67 86 40 00 Fax: 67 86 40 09
E-post: post@sertit.no Internett: www.sertit.no