Ny standard för säkerhetsprodukter

Common Criteria

HJÄLPER ANVÄNDARE OCH LEVERANTÖR

Den breda uppslutningen kring common criteria-certifikatet hjälper både kunder och leverantörer att höja säkerhetsnivån i den ojämna kampen mot angripare.

Text: Ralf Andersson, IT- och organisationskonsult. **Illustration:** Ola Rehnberg

Behovet av IT-säkerhet ökar ständigt. Internet har öppnat våra system mot omvärlden och dess möjligheter. Men också blottat oss mot dess hot. Konsumenter, leverantörer och IT-avdelningar för idag en ständig kamp mot potentiella angripare. Och det är en ojämn sådan. En angripare behöver ju bara hitta en enda svaghet, medan konsumenten eller IT-avdelningen måste hitta alla tänkbara möjliga svagheter i sitt system.

Det finns två huvudfrågor man måste ställa sig: **Vilka säkerhetsfunktioner behöver vi?** Det vill säga funktioner som lösenord, smarta kort etcetera. Och **hur noga ska funktionskraven utvärderas och verifieras?** Till exempel i form av sårbarhetsanalyser och penetrationstester.

Både konsumenter och IT-avdelningar kan ställa krav på att system ska vara säkra. Men hur vet vi att systemen vi använder uppfyller dem?

Det är här Common Criteria kommer in i bilden. CC är både ett certifikat och ett internationellt samarbete kring den välbehövliga utvecklingen av standarder för säkerhetsutrustning. Standarden heter ISO/IEC 15408 och ska tillhandahålla en metodik och ett ramverk för att säkerhetsutvärdera IT-produkter och IT-system.

Common criteria är framför allt tänkt som ett stöd för potentiella IT-köpare, både konsumenter och IT-avdelningar, i allt från att välja produkter till att ställa relevanta säkerhetskrav. Med en enhetlig standardmärkning ska det helt enkelt bli enklare att jämföra IT-produkter ur säkerhetssynpunkt. Det gör det i sin tur enklare att balansera säkerhetskostnader mot rimliga risknivåer. Dessutom gynnas den fria konkurrensen då produkter från hela världen kan certiferas under samma standard . På så vis minskar kostnaderna då fler produkter får tillgång till en global marknad.

Även leverantörerna kan således ha nytta av standardiseringen, på så vis att de kan varudeklarera sina produkter i enlighet med den.

COMMON CRITERIA HAR utvecklats som svar på ett växande behov av en gemensam internationell standard. Den baseras på tidigare standarder från 1980- och 1990-talen, närmare bestämt europeiska Itsec, kanadensiska Ctcpec och amerikanska Tcsec. De som deltog i projektet deltog samtidigt i en ömsesidig överenskommelse kallad *Common Criteria Recognition Arrangement (CCRA)* i vilken alla undertecknare erkänner certifikat utfärdade av repektive lands certifieringsorgan.

Idag finns det 24 nationella medlemsländer och undertecknare eller representant för avtalet i Sverige är *Krisberedskapsmyndigheten*.

Försvarets materielverk (FMV) har å sin sida regeringens uppdrag att verka som nationellt certifieringsorgan. Man har därför bildat en självständig enhet inom verket, Sveriges certifieringorgan för IT-säkerhet eller *CSEC*. Dess uppgift är att utveckla och förvalta den nationella certifieringsordningen, det vill säga de regler, processer och dokument som styr hur common criteria tillämpas. I arbetet ingår tillsyn och stöd vid utvärdering av produkter, att licensiera evalueringsföretag, att tolka common criteria och certifieringsordningen, att utfärda certifikat samt att informera, utbilda och samverka internationellt.