Offentlig sertifisering av IT-sikkerhet

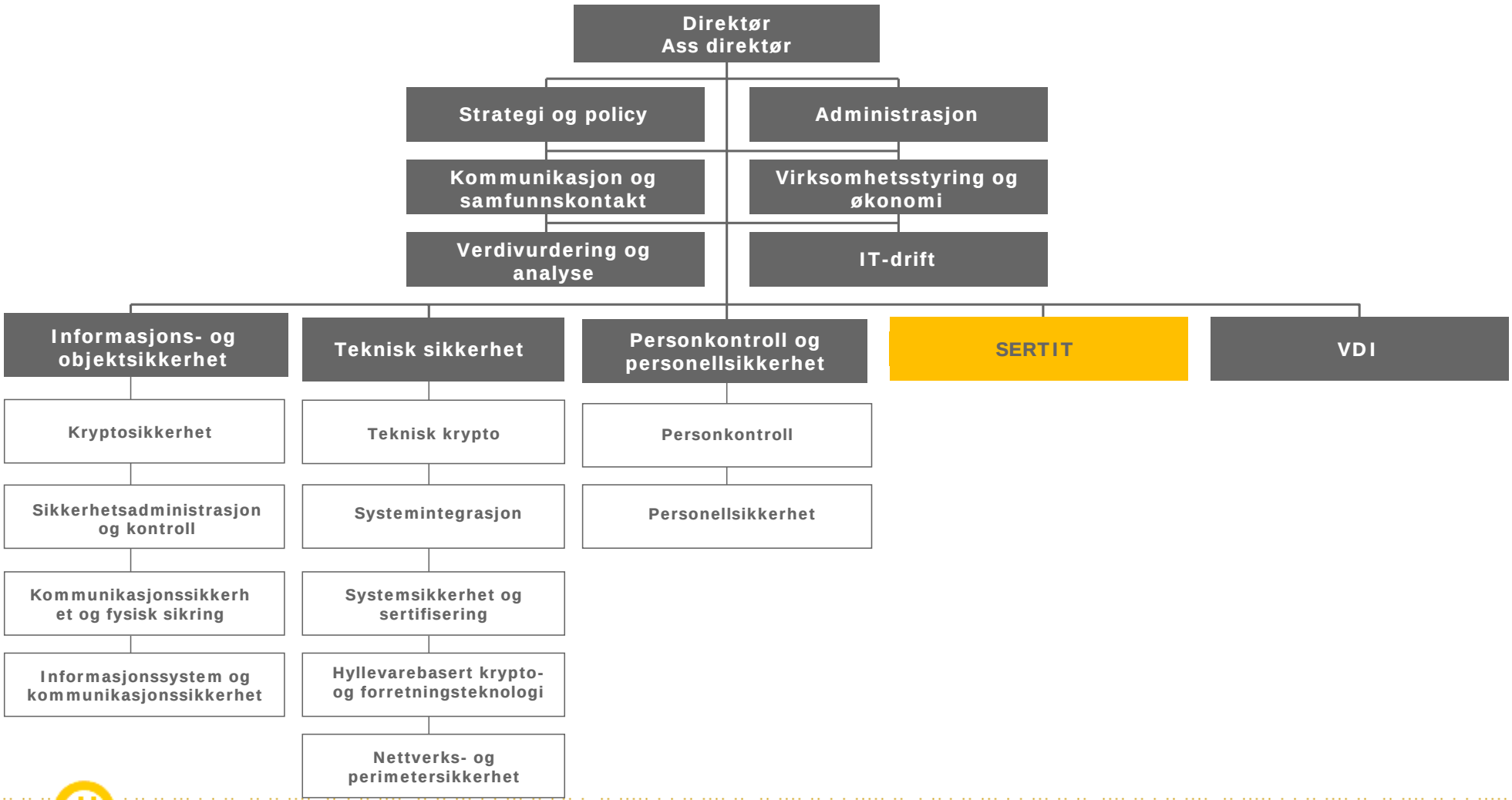
Seminar om sikkerhet og tillit,
22. september 2005

Lars Borgos, SERTIT

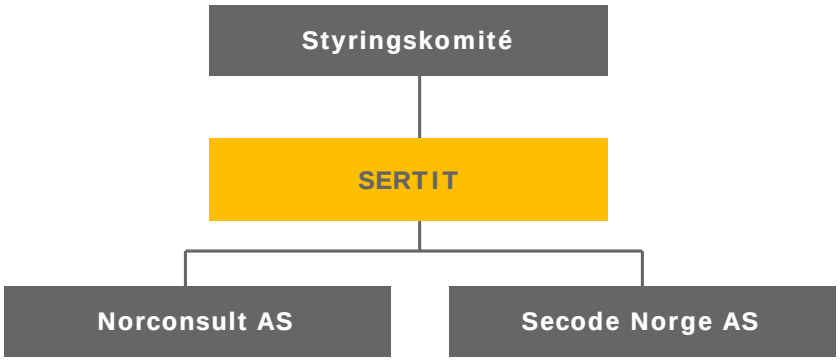
Tema

- Om ordningen
- Sertifisering ift forebyggende sikkerhet
- Nytteverdi

SERTIT i NSM


Direktør
Ass direktør
Strategi og policy
Administrasjon
Kommunikasjon og samfunnskontakt
Virksomhetsstyring og økonomi
Verdivurdering og analyse
IT-drift
Informasjons- og objektsikkerhet
Teknisk sikkerhet
Personkontroll og personellsikkerhet
SERTIT
VDI
Kryptosikkerhet
Sikkerhetsadministrasjon og kontroll
Kommunikasjonssikkerh et og fysisk sikring
Informasjonssystem og kommunikasjonssikkerhet
Teknisk krypto
Systemintegrasjon
Systemsikkerhet og sertifisering
Hyllevarebasert krypto- og forretningsteknologi
Nettverks- og perimetersikkerhet
Personkontroll
Personellsikkerhet

Sertifiseringsordningen



SERTIT:
4,5 årsverk
- 1 leder (50%)
- 1 senioringeniør
- 3 overingeniører

Styringskomité:
Forsvarsdepartementet
Justis- og politidepartementet
Moderniseringsdepartementet
Nasjonal sikkerhetsmyndighet
Datatilsynet
Norsk Akkreditering
Standard Norge
Abelia

Sekretariat:
SERTIT

EVIT:
Minimumsbemanning:
- 4 personer

I praksis:
- 6 – 7 personer

Formål med ordningen

- å gjennomføre **uhildet tredjepartsvurdering** av IT produkter- og systemer
- å **styrke tilliten** til og bedre sikkerhetsnivået i IT produkter og systemer
- å **styrke IT-sikkerheten** i offentlig sektor
- å **skape tillit til e-handelsløsninger** og annen kommunikasjon nasjonalt og internasjonalt
- å bidra til å gjøre Norsk IT-industri mer **konkurransedyktig** overfor utlandet
- å gjøre det **enklere for anskaffer** gjennom tillit til at forhåndsdefinerte sikkerhetskrav er tilfredsstilt

SERTITs mandat

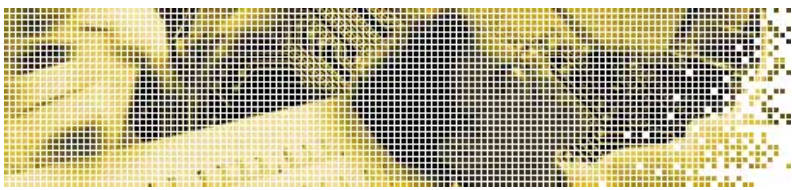
- Godkjenne og føre tilsyn med EVIT
- Sertifisere produkter- og systemer og utstede sertifikater
- Internasjonal anerkjennelse av sertifikater
- Representere Norge i CCRA
- Utforme og utgi rammevilkår og publikasjoner
- Informere om ordningen
- Sekretariat for styringskomiteen

Status for sertifiseringsordningen

- To evalueringsfirmaer er godkjent som EVIT
- Utgitt to sertifikater
  - Thales OTA
  - Sospita QX Operating System
- Rammeverk, avtaler og retningslinjer er ferdig
- Kvalitetssystem iht NS-EN 45011 er ferdig
- De fleste publikasjoner er ferdigstilt
- Tilfredsstillende kompetanse i ordningen
- Pågår prosess om internasjonal godkjenning

Hva er sikkerhetsevaluering?

- Teknisk undersøkelse av om et produkt eller system oppfyller gitt krav (til sikkerhet)
- Grunnlag for en slik sikkerhetsevaluering vil være internasjonale kriterier, Common Criteria



Hva er sertifisering?

- Godkjenne noe på grunnlag av en teknisk sikkerhetsevaluering
- Den tekniske sikkerhetsevaluering skjer hos et firma godkjent for formålet
- Det utstedes et sertifikat og sertifiseringsrapport

Certificate

Product Manufacturer: Softwarecompagniet ASA
Product Name: Lunix Cyberspace
Type of Product: Operating System
Version and Release Numbers: 12.6, release H
Protection Profile Conformance (if applicable): Maismenus PGP
Evaluation Platform (optional): Macintosh EDB
Name of IT Security Evaluation Facility: System Sikkerhet ASA, Norway
Name of Certification Body: SERTIT The Norwegian Certification Authority for IT Security
Certification Report Identifier: Common Criteria for IT Security Evaluation version 2.1 and Common Methodology for IT Security Evaluation version 1.0, Report number R-001/01
Assurance Package: EAL 3+
Date issued: 25 october 2001

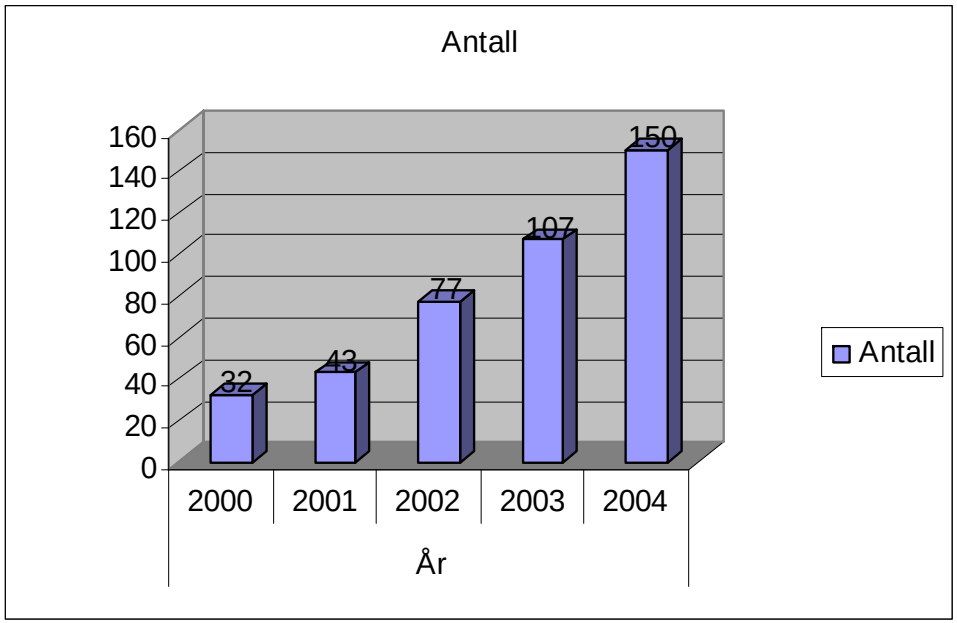
Kjartan Eiesones Arne H. Hage Lars Borgos

SERTIT

Hva er CC?

- Katalog med kriterier og et sett av verktøy for å utforme krav:
- Kravene tjener som en:
  - Utviklerguide
  - Guide for anskaffer
  - Guide for evaluering

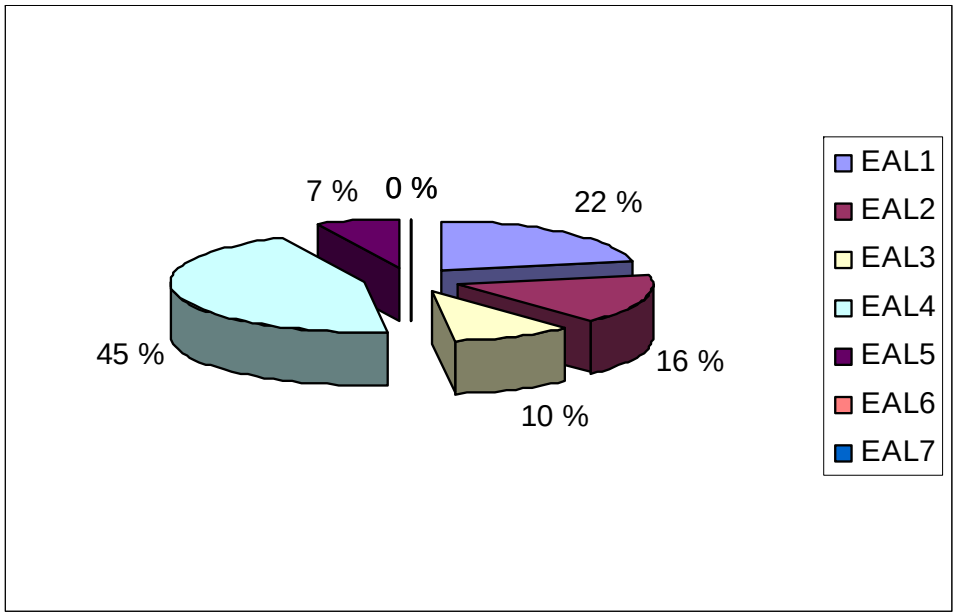
CC-sertifikater – utviklingen internasjonalt



Kilde: 2000-2003, BSI Annual report 2003
2004: anslag av SERTIT basert på QP websider

Common Criteria

CC- sertifikater pr tillitsnivå



Kilde: Foredrag på 4th ICCC, Stockholm, 2003

Common Criteria Recognition Arrangement

- Etablert 23. mai 2000, Baltimore
- 22 nasjoner deltar
- Gjensidig anerkjennelse
- CC som felles standard
  - 20 års utvikling bak CC
- Begrensninger
  - Tom EAL 4
  - Nasjonal sikkerhet

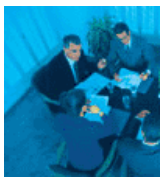
Kvalifisering, verifisering, sertifisering

- Romfart
- Luftfart
- Offshore
- Maritim
- Bilindustri
- Helse
- Miljø
- M.fl.

CE 0470

Nemko EMC

◁ HAR ▷



E 17

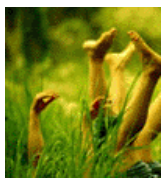
TRUSTED COMPANY DNV PROVIDING TRUST

EN 17

DFINS

Nemko GS

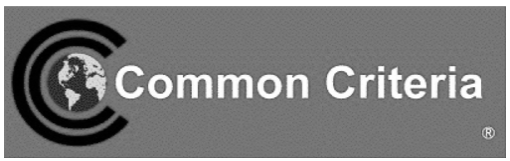
NS



Kilder: DN, DNV, NEMKO

Merking av IT-produkter, IT-sikkerhet i produkter og -systemer

- Enkelte områder av betydning for helse og miljø er dekket
- Ikke mange krav til sikkerhet i IT-produkter og -systemer, enda IT griper inn i de fleste samfunns- og virksomhetskritiske områder og prosesser
- CC er en mulig vei å gå



Noen rammer for sertifisering

- Nasjonal strategi for informasjonssikkerhet
  - IX (Sertifisering av kritiske systemer)
- Forskrift om informasjonssikkerhet (FD), jf kap 5,
  - Funksjonalitet og tillitsnivå
- Forskrift om offentlige anskaffelser (NHD),
  - Dokumentasjon av leverandørens tekniske kvalifikasjoner

Strategien skal bidra til

- Å redusere sårbarheten ved alminnelig bruk av IT og i kritisk IT-infrastruktur
- Å legge til rette for trygg elektronisk forretningsdrift i privat og offentlig sektor samt sikre og pålitelige nettjenester fra det offentlige

6 IX Sertifisering og standarder

- SERTIT bør tas bredere i bruk av norske virksomheter
- Offentlige og private IT-anskaffelser
  - Kjøp av produkter
  - Kjøp av tjenester
  - Kjøp av utviklingsoppdrag
- Styrkning av norsk deltakelse i standardiseringsarbeid innen IT-sikkerhet
- Styrkning av informasjonstiltak

Andre områder ift forebyggende tiltak

- Kritisk infrastruktur
- Samordning av regelverk
- ROS
- Bevisstgjøring av aktører
- Leverandører av IT-produkter og tjenester
- Godkjenning på bakgrunn av sertifisering
  - Forenkler ulike godkjenningsordninger

5 NSMs rolle som nasjonal sertifiseringsmyndighet

- Internasjonal standard og metodikk (CC, CEM)
- Gjensidig aksept over landegrensene
- →behov som faller utenom sikkerhetslovens regulering
- →CC og CEM som grunnlag for sikkerhetsmessig godkjenning også under sikkerhetslovens ansvarsområde

Ønsket utvikling - Bransjekrav

- Spesielle bransjer stiller krav om bruk av sertifiserte produkter/systemer, f eks
- Forsikringsbransjen (redusert premie)
- Kreditt-/finansnæringen
  - Pengetransaksjoner
  - Nettbanker
  - E-faktura
- Kraftforsyningen
  - Kritisk infrastruktur
  - Måleravlesning
- Elektroniske postforsendelser
  - E-kurertjenester

Ønsket utvikling – Offentlige krav

- Anmodning om eller krav om bruk av sertifiserte produkter/systemer, f eks
- Offentlige anskaffelser der sikkerhet er viktig og nødvendig
- Elektroniske signaturer/PKI løsninger, jf EU-krav om godkjenningsordning for signaturfremstillingssystemer for kvalifiserte signaturer
- Forsvaret benytter SERTIT ifm produktanskaffelser
- Datatilsynet gir anbefalinger om bruk av sertifiserte produkter

Ønsket utvikling - synlighet

- SERTIT som den foretrukne merkevaren blant aktørene i markedet
- SERTIT-sertifisering av produkter og systemer blir et kvalitetsstempel på linje med andre sertifiseringsordninger innen andre områder

Hva sier brukerne?

BEDRIFTPROFILEN

SERTIT:

– Be om sertifikat!

– Krev at produsenten kan fremvise sertifikat som dokumenterer IT-sikkerheten, oppfordrer senioringeniør Lars Borgos i den offentlige sertifiseringsmyndigheten SERTIT. Sertifisering av IT-sikkerhet i løsninger og produkter kommer både utviklere og innkjøpere til nytte, sier han.

Sertifisering av IT-løsninger og IT-produkter er satt i system av SERTIT. Sertifiseringsordningen retter seg både mot utviklere og mot de som kjøper informasjonsteknologi. – Vi oppfordrer både utviklermiljøene og de som har innkjøpsfunksjonen å satse sterkere på sertifisering. Det er viktig å kunne dokumentere et tillitsnivå, sier Borgos.

– For de som går til anskaffelse av et nytt IT-system, det være seg et sykehus, en fylkeskommune eller en norsk bedrift, er det viktig å vite hvor sikkert systemet er. Man migrerer ikke til en ny plattform hvis sikkerheten i den nye plattformen er dårligere enn den gamle. Men hvordan vet man at sikkerheten er god nok? Skal man stole på produsenten og leverandøren? Eller skal man gjøre sine egne undersøkelser?

Unngå ubehagelige overraskelser

Borgos tar spørsmålet henge i luften. – Når man tenker mer enn ett sekund på denne problemstillingen går det opp for de fleste at disse alternativene strengt tatt ikke er gode nok. Det er mye som slippes på markedet uten at det er godt nok testet, og det siste man ønsker er en ubehagelig overraskelse knyttet til sikkerhet. Det er høyst variabelt hva du får ved å stole på produsentens forsikringer, sier han.

Å gjøre egne undersøkelser er svært ressurskrevende, og det er heller ikke mange personer her i landet som har kompetansen til å gjennomføre slike sikkerhetsanalyser.

Krevende undersøkelser

– SERTIT har godkjent to private bedrifter som evalueringsinstanser. Secode System Sikkerhet ASA og Norconsult AS er etter en omfattende kvalifiseringsprosess funnet skikket til å evaluere sikkerhetsaspekter rundt IT på en tilstrekkelig god måte.

Har produsenten de nødvendige sertifikatene som dokumenterer sikkerhetsnivået? Hvis ikke, send anbudet i retur, oppfordrer Lars Borgos, Marte Rasmann Moksnes, Arne Høye Rage og Kjartan Jæger Krassnes i SERTIT. Leder for SERTIT, Gøril W. Bergan, hadde ikke anledning til å være tilstede.

Vi skjønner godt hvorfor innkjøperne bør stille krav om sertifisering, men hva med utviklerne? Hva taler for at de bør sertifisere løsninger og produkter? – Kort oppsummert: konkurransefortrinn, svarer Borgos. Å kunne tilby sertifiserte produkter og løsninger vil i økende grad være et pre i konkurranse med ulike tilbydere.

Sertifikat etterspurt

– Vi har et ferskt eksempel i bedriften Thales Norway AS. De har sertifisert produktet Thales Operator Terminal Adapter, et produkt som brukes i militære operasjonsrom for å skille gradert og ugradert tale mellom militære flygeledere og flygere. – Det var helt avgjørende at vi fikk sertifisert produktet for å lande kontrakten med NATO, kommenterer Kjell K. Kristiansen i Thales Norway AS. – Vi valgte internasjonal sertifisering for å slippe nye godkjenningsrunder i alle NATO-landene som skal ta produktet i bruk.

– Underveis i sertifiseringsprosessen fant vi sikkerhetshull som måtte utbedres. Prosessen gjorde altså produktet bedre, sier Kristiansen.

SERTIT, som er lagt til Nasjonal sikkerhetsmyndighet, utsteder sertifikat etter den internasjonale IT-sikkerhetsstandarden Common Criteria. – Internasjonalt går etterspørselen etter CC-sertifiserte IT-produkter kraftig oppover. I USA er det i mange sammenhenger et krav at produkter og løsninger som skal brukes i forsvarstjenesten er sertifiserte. Asia viser stor interesse, og også i Europa skjer det ting. Skal norske bedrifter eksportere sine løsninger og produkter vil sikkerhetssertifikater være en nødvendighet i fremtiden, mener Borgos.

SERTIT

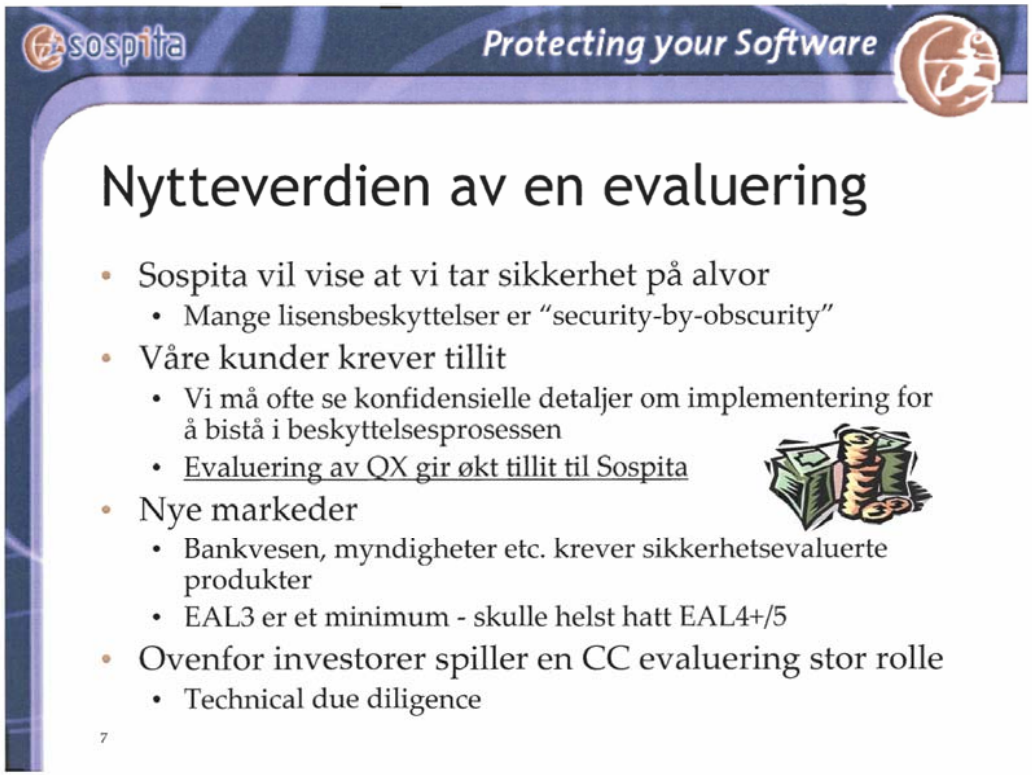
Postboks 14
1306 Bærum postterminal
Telefon 67 86 40 00
www.sertit.no

Kilde: Særtrykk fra Bedriftsprofilen nr 8 / 2004

Thales Norway AS

- Det var helt avgjørende at vi fikk sertifisert produktet for å lande kontrakten med NATO, kommenterer Kjell K. Kristiansen i Thales Norway AS.
- Underveis i sertifiseringsprosessen fant vi sikkerhetshull som måtte utbedres. Prosessen gjorde altså produktet bedre, sier Kristiansen.

Hva sier brukerne?



Kilde: Foredrag fra Sospita ifm IT-tinget, Lillehammer 2002

Sammendrag

- Forebyggende tiltak gjennom sertifisering er god policy for skadebegrensning
- Behovet for ny funksjonalitet med mulig risiko for økt sårbarhet bør avveies mot velprøvde og veldokumenterte løsninger som gir redusert sårbarhet
- CC fremmer god utvikling og gir bedre produkter
- Det bør stimuleres til økt etterspørsel av sertifiserte produkter

Mer informasjon

- SERTIT-konferansen 2005, 1. november, Oslo kongressenter
- NSMs sikkerhetskonferanse, 22-23. november, Oslo kongressenter
- Sertit.no
- www.commoncriteriaportal.org