Sertifioinnin rooli tietoturvallisuudessa

atbusiness tietoturvatorstai
18.9.2003

Jari.Pirhonen@atbusiness.com
Tietoturvallisuuspäällikkö ja -konsultti, CISSP, CISA
AtBusiness Communications Oyj

www.atbusiness.com
www.iki.fi/japi/

Maailma muuttuu

	1970	1980	1990	2000
Sovellus	Suurkone-sovellus	PC	Client-server, n-tier, web-sovellus	Web Services, multi-organization
GUI	ASCII-pääte	Grafiikka, ikkunointi	Erikokoiset näytöt, selainversiot, pluginit	päätelaitteiden kirjo, vaihteleva verkon kapasiteetti, sovellusten välinen kommunikointi
Tietoturva	Hallinta helppoa ja keskitettyä, IBM RACF	Käyttäjille valtaa ja vastuuta, virukset	verkottuminen, palomuurit, VPN, client-sovellus epäluotettava, sovelluskäyttö rajoitettua, ”linnakemalli”	palvelut epäluotettavia, luottosuhteet palveluketjuissa, sovelluskäyttö aina ja kaikkialta, PKI + XML, ”torimalli”, tietosuoja, imago ja strategia, sertifiointi

Henkilölle - CISSP

- Certified Information Systems Security Professional
- Myöntäjä www.isc2.org
- Kirjallisen testin lisäksi vaaditaan 4 vuoden työkokemus, CISSP:n suositus ja sitoutuminen eettisiin sääntöihin
- Osoittaa sertifioidun omaavan laajan tietoturvaosaamisen
  - 10 osa-aluetta: pääsynvalvonta, sovelluskehitys, jatkuvuussuunnittelu, salausmenetelmät, lait ja etiikka, fyysinen tietoturva, operatiivinen tietoturva, arkkitehtuurit, tietoverkot ja tietoturvan johtaminen
- Sertifikaatti vanhenee 3 vuodessa – ylläpidettävä kouluttautumalla
- ”Suunnittelu- ja johtotason” sertifikaatti
- Sertifiointi ei takaa tietyn tuotteen, tekniikan tai osa-alueen erityisosaamista
- Sertifioinnin tarkoitus vakuuttaa hyvästä ja laajasta tietoturvallisuuden perusosaamisesta ja ymmärryksestä

Tuotteelle - CC

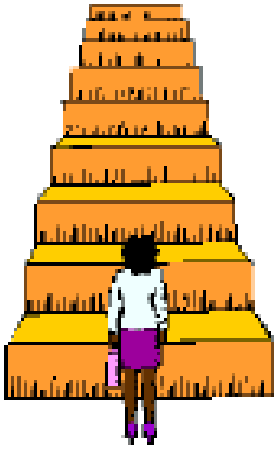
- Common Criteria for IT Security Evaluation, ISO 15408, http://csrc.ncsl.nist.gov/cc/, www.commoncriteria.org
- Standardi tapa esittää kohteen (TOE, Target of Evaluation) tietoturvallisuusvaatimukset – ”yhteinen kieli”
- Tuotteen toimittaja dokumentoi tietoturvallisuusvaatimukset (PP, Protection Profile) ja -toteutuksen (ST, Security Target)
- Evaluointilaboratorio evaluoi tuotteen toiminnallisuuden ja vakuuttavuuden määriteltyä vaatimustasoa vasten
- Sertifiointitasot EAL1 – EAL7 (Evaluation Assurance Levels), kertovat, kuinka tuotetta on evaluoitu ja testattu
  - EAL4: menetelmällisesti suunniteltu, testattu ja katselmoitu
- CC sertifioinnin tarkoitus vakuuttaa tuotteen tietoturvasuunnittelusta ja -toteutuksesta. Huomioitava kuitenkin paitsi sertifiointitaso, myös vaatimukset.

Yritykselle – BS7799

- British Standard 7799, http://www.bsi-global.com/, ISO 17799, http://www.iso-17799.com/
- Standardi kuvaa mitä pitäisi huomioida tietoturvallisuuden osalta, ei kerro miten toteutetaan
- Yritys tekee itse riskiarviointinsa ja päättää tietoturvallisuusvaatimuksista ja -toimenpiteistä
- SFS-Sertifiointi Oy arvioi pistokokein tietoturvallisuuden hyvyyttä ja yrityksen tietoturvallisuusvaatimusten toteutumista
- BS7799-sertifioinnin tarkoitus vakuuttaa organisaation tekevän tietoturvatyötä suunnitelmallisesti
- Sertifiointia pitäisi arvioida riskiarvioinnin kautta

Yrityksen turvatason portaat

5. Ylivoimainen suojaustaso
   - Turvallisuus on yrityksen kilpailutekijä
4. Edistyksellinen suojaustaso
   - Turvallisuus on osa yrityskulttuuria
3. Perussuojaustaso
   - Turvallisuus on osa toimintaprosesseja
2. Vähimmäissuojaustaso
   - Johto sitoutuu turvallisuuden kehittämiseen
1. Lähtötaso
   - Yritysjohto tiedostaa turvallisuuden merkityksen



Juha E. Miettinen, Yritysturvallisuuden käsikirja

Tietoturvan merkitys yritykselle

Luottamuksen ja turvallisuuden merkitys	rajoitetut	kattavat
suuri	Heikkous	Mahdollistaja
pieni	Ei kiinnosta	Suojaava

Tietoturvatoimet riskien minimoimiseksi

Tie BS7799 sertifiointiin

1. Best practices
2. Uhka-analyysi ja tietoturvastrategia
3. Tietoturvallisuuden kehittäminen
4. BS7799 yhteensopivuuden varmistaminen
5. Sertifiointi

Työkaluja

- RFC 2196 – Site Security Handbook
- ISF Standard of Good Practice for Information Security
- COBIT
- GASSP (Generally Accepted System Security Principles)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- NIST ASSET (Automated Security Self-Evaluation Tool)
- Valtionhallinnon suositukset (Vahti)

Gartner: Top 10 tietoturvahaasteet 2003

- Web Services
- WLAN
- Käyttäjätietojen hallinta ja provisiointi (Identity Mgmt)
- Hyökkäysten estojärjestelmät (IPS)
- Tapahtumien korrelointi: raportointi, monitorointi, hallinta
- Virukset, madot
- Pikaviestimet (Instant Messaging)
- Kansallinen tietoturvastrategia, lainsäädäntö (Homeland security)
- Taktinen tietoturva —> tietoturva-arkkitehtuuri
- Tietopääoman suojaaminen (Intellectual Property)
- Transaktioiden luottamuksellisuus/auditointi

Quality = Security

We start confusing quality with elegance, brightness, weight, and other subjective things. Then even those get compared when we talk about good quality, bad quality, high and low quality, and all those things. So far today we've used the word quality fifteen or twenty times, and each meaning has been different. If we're going to have a quality improvement program, we have to agree on what the word means. We don't want an elegance improvement program, do we?

-- Philip B. Crosby, Quality is Free