Achtergrond

Verdringt de ISO 21827 de ISO 17799?

11-05-2005, 09:14 door **Redactie**

Dag in dag uit verschijnt er reparatie software voor beveiligingslekken, in het jargon “security patches” genoemd, gemiddeld verschijnen er ongeveer 7 per dag. (bron: security.nl). Alleen al hiermee wordt een hele tak van de IT security branche aan het werk gehouden.

Het is dus logisch dat de roep om fout vrije software (in het jargon bug vrije software genoemd) groot is. Hoewel bugs onvermijdelijk zijn, hebben programmeurs wel een verantwoordelijkheid, namelijk het veilig coderen van de software. Uiteindelijk betalen de gebruikers van de software de prijs voor het slechte programmeerwerk.

ISO/IEC 21827 kan een oplossing bieden om deze problemen onder controle te krijgen. Wat is ISO/IEC 21827 en wat kan de security gemeenschap er mee? Dit artikel gaat nader in op deze vragen.

Door Ronald Eygendaal

ISO/IEC 21827

Op 11 juli 2003 is versie 3 van SSE-CMM van ISO/IEC 21827 Information Technology - Systems Security Engineering - Capability Maturity Model
(SSE-CMM) gepubliceerd door de International Standards Organization (ISO). Het is daarmee naast de bekende ISO/IEC 17799:2000, beter bekent als BS7799, een mondiaal gedragen standaard geworden. Versie 3 bevat onder andere verwijzingen naar gerelateerde ISO Standaarden zoals ISO/IEC 15504 (SPICE) Software Process Assessment, ISO/IEC 15288, Systems Engineering-System Life Cycle Processes, ISO/IEC 15408 Security techniques -- Evaluation criteria for IT security en ISO/IEC TR13335 Guidelines for management of IT Security.

Historie

SSE-CMM vindt zijn historie bij de Amerikaanse defensie industrie waar men op zoek was naar een methodiek om leveranciers te kunnen evalueren. Onder andere door sponsering van de van de National Security Agency (NSA) is rond 1990 de eerste aanzet gemaakt voor het Systems Security Engineering Capability Maturity Model (SSE-CMM). Onderleiding van het Software Engineering Institute van de Carnegie Mellon University en een bedrijvencollectief, van 42 bedrijven, is SSE-CMM verder ontwikkeld.

Na enkele succesvolle workshops in 1995 over SSE-CMM heeft in 1996 de eerste officiële versie het Systems Security Engineering Capability Maturity Model het levenslicht gezien. SSE-CMM model vindt zijn oorsprong uit Capability Maturity Model (CMM)

SSE-CMM verzorgt een internationaal erkend (ISO IEC 21827) framework voor evalueren van beveiliging, techniek en middelen. Verder geeft het een methodiek
voor het meten van prestaties en het verbeteren van diensten om vitale informatie te beschermen.

ISSEA International Systems Security Engineering Association

ISSEA.

De International Systems Security Engineering Association (ISSEA) is opgericht in 1999. De ISSEA is een internationale non-profit, op lidmaatschap gebaseerde organisatie, met als doel te fungeren als spreekbuis tussen de security gemeenschap en de International Standards Organization met betrekking tot ISO 21827 System Security Engineering Capability Maturity Model (SSE-CMM).

De ISSEA fungeert als soort van college van deskundige voor het ISO/IEC 21827 System Security Engineering Capability Maturity Model (SSE-CMM). Een minstens zo belangrijke taak van de ISSEA is het geven van voorlichting en educatie aangaande ISO 21827.

De ISSEA kent anno 2003 het individuele lidmaatschap, het bedrijfslidmaatschap en het onderzoeksinstelling lidmaatschap. De bedrijven en organisaties die financieel sponsor zijn geweest voor de tot stand komen van SSE-CMM hebben een special zogenaamd “chater” lidmaatschap. Chater leden worden niet meer geaccepteerd door de ISSEA.

De ISSEA heeft op drie continenten leden te weten; Australië, Europa en Amerika. De organisatie is sterk groeiende in het Europese continent.

ISSPCS
De International Systems Security Professional Certification Scheme (ISSPCS) is een certificatie instelling voor persoonscertificatie. ISSPCS is een onafhankelijke non-profit organisatie met een internationaal certificatie programma wat open is voor een ieder werkzaam in het IT werkveld.

Onder andere voor de ISSEA heeft de ISSPCS een persoonscertificatie schema ontwikkeld wat gebaseerd is op ISO 21827.

ISSPCS zorgt met behulp van communicatie over en weer met de security gemeenschap dat het Certificatie programma actueel en bij de tijd blijft. Het certificatie programma is gebaseerd op de essentiële security principes en gefocust op processen en discipline. Deze unieke aanpak kenmerkt zich door de wijze waarmee de integratie van security in alle proces stappen geborgd is.

ISSPCS wordt ondersteunt door universiteiten, Computer Emergency Response Teams (CERT) en Electronic Warfare organisaties.

“ISSPCS Certified” moet de klachten over onvoldoende mondiaal draagvlak zoals die er zijn over, de veel al Amerikaans georiënteerde persoonscertificeringen zoals, CISSP, CISM, SANS ondervangen. De ISSPCS certificering is gebaseerd op de internationaal geaccepteerde standaarden van de International Standards Organization (ISO) . De belangrijkste ISO standaarden op het gebied van informatiebeveiliging vormen de Common Body of Knowledge (CBK) voor de ISSPCS.

- ISO 21827 System Security Engineering Capability Maturity Model (SSE-CMM)
- ISO/IEC 13335 Information Technology - Security Techniques - Guidelines for the Management of IT Security
- ISO/IEC 17799:2000
- ISO 15408 ("Common Criteria")

Om in het bezit te komen van “ISSPCS Certified” moet examen worden gedaan. Dit examen toetst de inhoudelijke kennis van de belangrijkste ISO standaarden op het gebied van informatiebeveiliging.

Conclusie
Ondanks het relatief jonge bestaan van de ISSEA heeft het in vergelijking met andere organisaties zoals de Information Systems Security Association (ISSA) al veel bereikt. Het feit dat de ISSPCS zijn CBK ontleed aan ISO standaarden maakt hun een serieuze speler op het gebied van persooncertificatie.

Bronnen

http://www.sse-cmm.org

http://www.isspcs.org
http://www.issea.org/

Over de auteur

Ronald Eygendaal is werkzaam als Senior Security & Fraud Consultant heeft meer dan 12 jaar ervaring in beveiliging, fraude onderzoeken en informatiebeveiliging in het bijzonder; is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN); is Certified In Security Supervision and Management (CSSM) en Certificate in Information Security Management Principles (CISMP)
e-mail: ronaldeygendaal@protectioncompany.com