# ISO 21827 steeds belangrijk

**Gemiddeld verschijnen er dagelijks zo'n zeven 'security patches', reparatiesoftware voor beveiligingslekken. Alleen al hiermee wordt een hele tak van de IT-beveiligingsbranche aan het werk gehouden. Het is dus logisch dat de roep om foutvrije software 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 slecht programmeerwerk. ISO 21827 kan een oplossing bieden om deze problemen onder controle te krijgen. Wat is ISO 21827 en wat kan de beveiligingsbranche er mee?**

De ISO 21827-norm verwijst naar het Systems Security Engineering Capability Maturity Model (SSE-CMM) en beschrijft de kenmerken voor inbedding van informatiebeveiliging in het ontwikkelproces. Het betreft de volgende kenmerken. Het model heeft betrekking op de gehele 'trusted product or secure system life cycle' met inbegrip van de ontwikkeling, de exploitatie, het onderhoud en de ontmanteling van een systeem. Het is toepasbaar in alle sectoren en organisaties, waaronder management-, organisatie- en engineering-activiteiten. Gelijktijdige interacties met andere disciplines zijn mogelijk, zoals systeemsoftware en hardware, menselijke factoren, test engineering, systeembeheer, operaties en onderhoud. Dit geldt eveneens voor interacties met andere organisaties, waaronder aankoop, systeembeheer, certificering, accreditatie en evaluatie. Met het model worden 'best practices' meetbaar (KPI's). De ISO 21827 kan worden gezien als referentiemodel voor 'security engineering' en als raamwerk voor assessment van de volwassenheid ('maturity') van een organisatie die software ontwikkelt en ook als raamwerk voor verbetering van het ontwikkelproces van software.

**Process Areas** De ISO 21827 kent in totaal 22 'Process Areas' en vijf niveaus. Van deze 22 'Process Areas' zijn er elf zogenaamde 'Security Engineering Process Areas': PA01 - Administer Security Controls, PA02 - Assess Impact, PA03 - Assess Security Risk, PA04 - Assess Threat, PA05 - Assess Vulnerability, PA06 - Build Assurance Argument, PA07 - Coordinate Security, PA08 - Monitor Security Posture, PA09 - Provide Security Input, PA10 - Specify Security Needs en PA11 - Verify and Validate Security. Daarnaast zijn er elf 'Process Areas' die betrekking hebben op de organisatie en projecten. Deze elf kunnen worden gebruikt om afstemming met de ISO 15288 (Systems and software engineering - System life cycle processes) te vergemakkelijken. Het gaat om PA12 - Ensure Quality, PA13 - Manage Configuration, PA14 - Manage Project Risk, PA15 - Monitor and Control Technical Effort, PA16 - Plan Technical Effort, PA17 - Define Organization's Systems Engineering Process, PA18 - Improve Organization's Systems Engineering Process, PA19 - Manage Product Line Evolution, PA20 - Manage Systems Engineering Support Environment, PA21 - Provide Ongoing Skills and Knowledge en PA22 - Coordinate with Suppliers.

**Niveaus** Bijna geheel in lijn met CMM kent de ISO 21827 vijf niveaus van volwassenheid ('maturity levels'). Formeel kent SSE-CMM nog een extra level. Dit Level 0 (Not Performed) wordt echter verder niet gebruikt. Het model bevat de generieke processen, de processen die van toepassing zijn op alle 'maturity levels'. Deze generieke processen zijn gegroepeerd op basis van gemeenschappelijk kenmerk en vaardigheidsniveau welke van toepassing is op alle levels.

Level 1 - Performed Informally. Dit is het laagste niveau ('initial', geen proces gedefinieerd, de organisatie werkt ad hoc).

Level 2 - Planned and Tracked. Dit level richt zich op projectdefinities, planning en performance issues. Kortweg een aantal basiszaken zijn geregeld per project (nog niet per se uniform voor de hele organisatie). Hierbij moet worden gedacht aan de subprocessen: Planning Performance, Disciplined Performance, Verifying Performance en Tracking Performance.

Level 3 - Well Defined. Er is een volledig beschreven proces (zowel de primaire software-ontwikkelprocessen als de managementprocessen) voor de hele organisatie. Dit betreft aanvullend op de processen van level 2 de volgende subprocessen: Defining a Standard Process, Perform the Defined Process

# er bij ontwikkeling software


en Coordinate Practices.
Level 4 - Quantitatively Controlled: statistische procesbeheersing is ingevoerd. Dit betreft aanvullend op de processen van levels 2 en 3 de volgende subprocessen: Establishing Measurable Quality Goals en Objectively Managing Performance.
Level 5 - Continuously Improving: processen en technologie worden continu verbeterd op basis van statistische procesbeheersing. Dit betreft aanvullend op de processen van levels 2, 3 en 4 de volgende sub-processen: Improving Organizational Capability en Improving Process Effectiveness.

**SSAM** Om het 'maturity level' vast te stellen is de Systems Security Appraisal Method (SSAM) ontwikkeld. Doel hiervan is het verkrijgen van de baseline van de actuele situatie met betrekking tot beveiligingstechniek binnen de organisatie of project. Een ander doel van SSAM is het oprichten en/of ondersteunen van een momentum voor verbetering binnen meerdere niveaus van de organisatiestructuur. SSAM is een onderzoeksproces met een aantal fases. Dit zijn de planningsfase, een voorbereidingsfase, onsite fase en uiteindelijk een post-evaluatie fase. Het team dat SSAM uitvoert doet dit via de volgende stappen. Het verzamelen van informatie (ten behoeve van de vragenlijst), in een voorlopige data-analyse aangeven wat te zoeken/vragen, verzamelen gegevens en valideren met de betrokkenen, interviews met de betrokkenen en presenteren van de uiteindelijke data-analyse aan de sponsor. Uiteindelijk ontstaat er per proces een 'maturity level' en een 'overall maturity level'.

**Historie** SSE-CMM is ontwikkeld door de Amerikaanse defensie-industrie die op zoek was naar een methodiek om leveranciers te kunnen evalueren. Onder andere door sponsering van de National Security Agency (NSA) is rond 1993 de eerste aanzet gemaakt voor het SSE-CMM. Onder leiding van het Software Engineering Institute van de Carnegie Mellon ▸


University en een collectief van 42 bedrijven is SSE-CMM verder ontwikkeld. Het SSE-CMM model vindt zijn oorsprong in het Capability Maturity Model (CMM) en verzorgt een internationaal framework voor het evalueren van beveiliging, techniek en middelen. Verder omvat het een methodiek voor het meten van prestaties en het verbeteren van diensten om vitale informatie te beschermen.
In 1996 werd de eerste officiële versie (v1.0) van het Systems Security Engineering Capability Maturity Model gepresenteerd. Drie jaar later kwam de tweede versie uit en in 2002 heeft de International Standards Organization (ISO) de derde versie van SSE-CMM gepubliceerd als de ISO/IEC 21827 Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM). In 2004 heeft de International Systems Security Engineering Association (ISSEA) het proces ingeregeld om te komen tot een Appraiser Certification Body conform de ISO/IEC 17024, General Requirements For Bodies Operating Certification Schemes For Persons. Daarmee ontstond de mogelijkheid voor certificering van personen en organisaties volgens de ISO/IEC 21827. In 2008 werd een update van de standaard gepubliceerd, die daarmee naast de bekende ISO/IEC 2700X een mondiaal gedragen industriestandaard is geworden.

**Praktijk** In de praktijk blijkt dat ISO 21827 in Amerika, Azië en delen van West-Europa wordt toegepast als procescertificering. Het gaat hier veelal om leveranciers van beveiligingsdiensten, ontwikkelaars van beveiligingsproducten en ontwikkelaars en integrators van beveiligde systemen die dit toepassen ten behoeve van het certificeren van software ontwikkelprocessen. Mondiaal opererende certificatie-instellingen zoals de ICS Group en Eurotech certificeren bedrijven volgens de ISO/IEC 21827. Bedrijven kunnen tegen verschillende volwassenheidsniveaus worden gecertificeerd. Zo is bijvoorbeeld softwarebouwer SRIT uit India gecertificeerd op SSE-CMM level 5 en Tech Mahindra op level 3. Daarnaast gaat de ISO 21827 een steeds prominentere rol spelen bij het bepalen van de volwassenheid van zowel bestaande Information Security Management systemen als van bestaande Business Continuity Management systemen. De ISO 21827 wordt steeds belangrijker bij de ontwikkeling van software en het vaststellen van ‘maturity levels’.

■ Ronald Eygendaal
Ronald Eygendaal schrijft regelmatig over informatiebeveiliging, elektronische en technische beveiliging, fraudedetectie en -bestrijding, bewaking en beveiliging. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN).

Bronnen

http://www.pqm-online.com/assets/files/standards/iso-iec_21827-2002.pdf
http://www.renaissance-it.com/corporate_factfile.php
http://www.csc.com/ca_en/offerings/54254/54277-security
http://www.cs2consulting.com/about/
http://www.mahindra.com/What-We-Do/Information-Technology/Companies/Tech-Mahindra