DuD
Datenschutz und Datensicherheit

SSE-CMM

Petra Barzin

Qualität von Software

Die Qualität von Software hängt wesentlich von den Entwicklungsprozessen bei der Softwareerstellung ab. Hier ist eine Zertifizierung auf Basis des Qualitätsstandards ISO 9000 weniger geeignet, da diese Normenreihe nicht speziell auf Softwareentwicklungsprozesse ausgerichtet ist. Zur Überprüfung und Einschätzung des Reifegrades von Softwareprozessen gewinnen Modelle wie SSE-CMM (ISO 21827) und CMM(I) an Bedeutung, da sie darauf abgestimmt sind, zur Prozessverbesserung beizutragen. Das Capability Maturity Model (CMM, deutsch: Reifegradmodell) ist ein Prozessmodell zur Einschätzung des Reifegrades von Softwareprozessen (Softwareentwicklung, Wartung, Konfiguration etc.).

Hintergrund

CMM bzw. SW-CMM (Software CMM)[1] war das erste existierende Capability Maturity Model. Es wurde von dem Software Engineering Institute (SEI) der Carnegie Mellon University/Pittsburgh entwickelt. Im Jahr 2000 wurde CMM durch Capability Maturity Model Integration (CMMI) ersetzt. Die erste Version von CMMI erschien im Jahr 2002. CMMI (CMM Integration) ist die aktuelle Version des CMM-Modells.

ISO/IEC 21827 ist ein internationaler Standard, der auf dem System Security Engineering Capability Maturity Model (SSE-CMM) beruht. SSE-CMM begann als Initiative der National Security Agency (NSA) im April 1993 und wurde 1996 als Version 1.0 veröffentlicht. Dabei wurden bereits existierende CMM Modelle berücksichtigt. Drei Jahre später folgte SSE-CMM v2. Zur Fortführung von SSE-CMM wurde die International Systems Security Engineering Association (ISSEA) gegründet. Im Jahr 2002 wurde SSE-CMM Version 3 als Standard ISO/IEC ISO 21827 „Systems Security Engineering Capability Maturity Model“ veröffentlicht.

ISO/IEC 21827 dient als spezialisiertes Prozessmodell zur Bewertung und Verbesserung von Sicherheit im Softwareentwicklungsprozess. Im Folgenden wird SSE-CMM synonym für ISO/IEC 21827 verwendet.

[1] Das Capability Maturity Model wird sowohl als CMM als auch als Software CMM (SW-CMM) bezeichnet.

Werkzeuge zur Prozessverbesserung

Capability Maturity Modelle definieren keine Softwareentwicklungsprozesse, sondern bieten einen Leitfaden zur Definition und Verbesserung der Prozesse. Sie beschreiben, WELCHE Aktivitäten durchgeführt werden müssen, aber nicht WIE dies zu erfolgen hat.

Wie andere CMMs definiert auch das SSE-CMM die wesentlichen Eigenschaften für sichere Softwareentwicklungsprozesse und kennzeichnet die Reife der Prozesse im Hinblick auf die Implementierung von Sicherheit. Dabei berücksichtigt das Modell den kompletten Software Development Lifecycle. Es wird kein bestimmtes Softwareentwicklungsmodell gefordert, sondern das SSE-CMM Modell setzt auf dem im Unternehmen eingesetzten Softwareentwicklungsmodell auf.

SSE-CMM beschreibt, welche Praktiken und Prozesse für eine hochwertige Softwareentwicklung insbesondere im Hinblick auf die Implementierung von Sicherheit notwendig sind. Dabei definiert SSE-CMM drei Prozesskategorien:

- Organizational Processes
- Project Processes
- Security Engineering Processes

Jeder dieser Kategorien sind verschiedene Prozessgebiete zugeordnet. Insgesamt gibt es 22 Prozessgebiete, von denen elf Gebiete Security Engineering-Aspekte betreffen und die restlichen elf die allgemeineren Prozessanforderungen der beiden Kategorien „Project Processes“ und „Organizational Processes“ abdecken.

Die allgemeineren Prozessanforderungen sind in Anlehnung an CMM(I) entstanden. Die Prozessgebiete der Prozesskategorie „Security Engineering“ gehen über CMM(I) hinaus. Sie beschreiben Prozesse zur Risikoanalyse und -bewertung, sichere Entwicklungsprozesse und Prozesse zur Vertrauensbildung.

Reifegrade

SSE-CMM unterscheidet fünf Stufen von Reifegraden (capability levels), die der Herstellungsprozess von sicherer Software in einem Unternehmen aufweisen kann:

- Stufe 1 – Formlos umgesetzt
  Es existieren zwar einzelne Maßnahmen. Ein wirklicher Prozess ist aber kaum organisiert und noch sehr instabil
- Stufe 2 – Geplant und weiterverfolgt
  Ein stabiler Prozess existiert und wird in Projekten mit einem Projektmanagement gelebt.
- Stufe 3 – Gut definiert
  Ein Prozess ist definiert und es existiert ein Prozessmodell, dass eine konsistente Implementierung des Prozesses sicherstellt.
- Stufe 4 – Quantitativ kontrolliert
  Es existieren Prozessmessungen und Prozessdatenanalysen, die für die Weiterentwicklung des Prozesses genutzt werden.
- Stufe 5 – Kontinuierlich verbessernd
  Das Management ist regelmäßig in die Prozessbewertung und die weitergehende Prozessoptimierung einbezogen.

Die verschiedenen Reifegrade ermöglichen die Bewertung und kontinuierliche Verbesserung der einzelnen Entwicklungsprozesse.

Fazit

SSE-CMM ist ein Standard zur Bewertung der Prozessreife von Softwareprozessen im Hinblick auf die Implementierung von Sicherheit. Mit Hilfe eines Fragenkatalogs kann ein Reifegradprofil für die eigenen Prozesse erstellt und somit auch ein Benchmarking durchgeführt werden.

Referenzen

[1] Systems Security Engineering Capability Maturity Model 3.0, http://www.sse-cmm.org/docs/ssecmmv3final.pdf

[2] ISO/IEC 21827:2002 „Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)“, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731