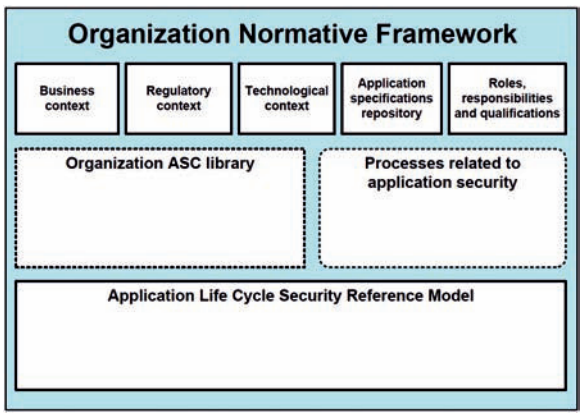
Sichere Softwareentwicklung nach ISO 27034

Der vorliegende Beitrag gibt einen kurzen Überblick über die ISO 27034-1 zur Anwendungssicherheit und zeigt, wie sie auf den „Security Development Lifecycle" von Microsoft angewendet werden kann.

Von Hartmut Pohl und Jochen Klein, Köln

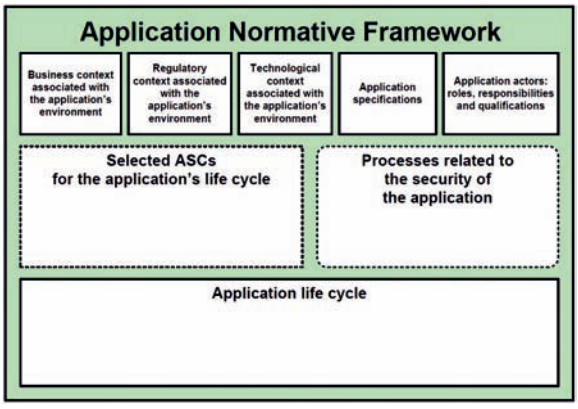
Durch die rasante Entwicklung und die Tatsache, dass Software heute fast überall – und teils sehr im Verborgenen – wirkt, entsteht eine Unmenge an Risiken, deren mögliche Folgen kaum abzusehen sind. Einen allgemeinen Ansatz zum Management von Applikationssicherheit liefert die 2011 von der International Standards Organization (ISO) verabschiedete ISO 27034-1: Die Norm mit der Bezeichnung „Information technology – Security techniques – Application security" bietet hierfür eine hersteller- und technologieunabhängige Grundlage; sie definiert Konzepte, Frameworks und Prozesse, die Unternehmen helfen Application-Security in ihren Entwicklungszyklus zu integrieren. Hohe Kompatibilität und leichte Skalierbarkeit vereinfachen die Integration in bereits bestehende Strukturen und lassen erwarten, dass die Norm zügig von der Industrie adaptiert wird.

Abbildung 1: Organization Normative Framework (ONF)



Quelle: ISO 27034-1

Abbildung 2: Application Normative Framework (ANF)



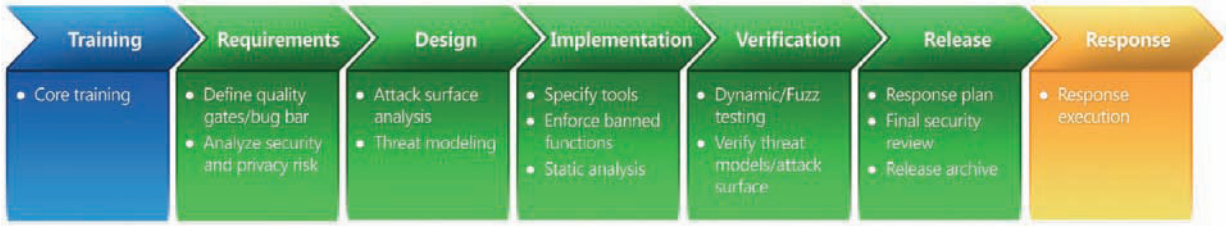
Quelle: ISO 27034-1

Einordnung

Wenn in der Geschäftswelt von IT-Sicherheit gesprochen wird, fällt fast ausschließlich das Schlagwort ISO 27001: In dieser Norm wird auf die Anforderungen für Informationssicherheits-Managementsysteme (ISMS) eingegangen, also ein Konzept für das Management von Informationssicherheit in Unternehmen. Hierunter fällt natürlich auch die Sicherheit von Applikationen, allerdings bietet die ISO 27001 für dieses komplexe Thema kein eigenes Framework.

Aus diesem Grund hat das für die ISO-270xx-Reihe zuständige Joint-Technical-Committee der International Standards Organization die ISO-27034-Normenreihe entworfen, von welcher bisher Teil 1 veröffentlicht wurde: Sie liefert den Rahmen, um ein umfassendes Applikationssicherheits-Programm aufzustellen und zu betreiben. Die Norm betrachtet Applikationssicherheit aus einer ganzheitlichen Perspektive, das heißt es fließen neben Sicherheitsanforderungen auch geschäftliche und regulatorische Anforderungen ein.

Um in der unternehmenseigenen Softwareentwicklung ein ausreichendes Maß an Applikationssicherheit zu gewährleisten, kommt die ISO 27034-1 zum Einsatz. Die Ergebnisse fließen dann auch in die Umsetzung der ISO 27001 (bzw. das ISMS) ein. Des Weiteren hilft die Norm, den Geltungsbereich des Risikomanagements nach ISO 27005 auf Applikationen auszuweiten.



Quelle: Microsoft

Abbildung 3: Security Development Lifecycle (SDL)

ISO 27034-1

Die ISO 27034-1 ist eine so genannte „High Level Structure"-Norm und gibt keine konkreten Maßnahmen zur Umsetzung vor. Daher lässt sie sich mit relativ geringem Aufwand in bestehende Software-Development-Lifecycle-Modelle adaptieren. Hierfür führt die Norm zwei Schlüssel-Frameworks ein, die Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen während der Softwareentwicklung helfen:

Organization Normative Framework (ONF): Im ONF werden alle von einem Unternehmen anerkannten Security-Best-Practices gespeichert, abgeleitet und präzisiert (vgl. Abb. 1). Es bildet die Basis für Applikationssicherheit im Unternehmen und alle die Applikationssicherheit betreffenden Entscheidungen werden auf dieser Basis getroffen.

Application Normative Framework (ANF): Ein ANF ist eine auf eine spezifische Applikation zugeschnittene Ableitung eines ONF. Sämtliche Security-Best-Practices des ONF, die eine spezifische Applikation zum Erreichen eines bestimmten Vertrauenslevels erreichen muss, werden aus dem ONF in das zur Applikation gehörende ANF übernommen.

Darüber hinaus definiert die Norm den Application-Security-Management-Process, welcher die Steuerung und die Pflege der ANFs gewährleistet, sowie den ONF-Management-Process. Letzterer soll dafür sorgen, dass jede zu sichernde Applikation vom gesammelten

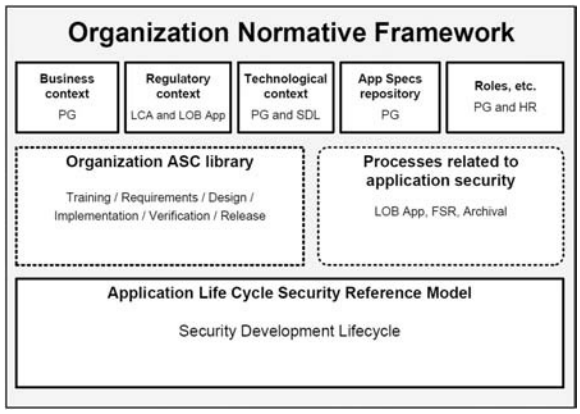


Abbildung 4: Mapping von ISO 27034-1 auf den Microsoft SDL

Wissen des Unternehmens profitiert. Außerdem werden Rückmeldungen und Erfahrungen aus der Sicherung von Applikationen verarbeitet und fließen in die kontinuierliche Verbesserung des ONF ein.

Ausblick

Die ISO 27034-1 ist nur der erste von acht unter dem Titel „Information technology – Security techniques – Application security" geplanten Teilen der Norm. Weitere Teile befinden sich in Bearbeitung. Die Inhalte sind voraussichtlich:

- Overview and concepts
- Organization normative framework
- Application security management process
- Application security validation
- Protocols and application security control data structure – XML schemas (1)
- Security guidance for specific applications
- Application security assurance prediction
- Protocols and application security controls data structure – XML schemas (2)

Security Development Lifecycle (SDL)

Der „Security Development Lifecycle" (SDL) von Microsoft ist ein Prozess zur Qualitätssicherung in der Softwareentwicklung, insbesondere unter Sicherheitsaspekten. In Abbildung 3 sind die Phasen des SDL vereinfacht dargestellt.

Neben der den gesamten Lifecycle andauernden Trainingsphase und der Response-Phase zur schnellen Reaktion bei Vorfällen, besteht der Lifecycle aus fünf weiteren Phasen, die dem Software-Development zugeschrieben sind: Jede dieser Phasen umfasst Schlüsselprozesse und zu erfüllende Meilensteine, die sicherstellen, dass Software auf einem angemessenen Sicherheitsniveau entwickelt wird. Die Phasen sind darauf ausgelegt, potenzielle Sicherheitslücken so früh wie möglich zu identifizieren und zu korrigieren.

Um zu verdeutlichen, wie sich die ISO 27034-1 auf bestehende Strukturen anwenden lässt, wird in Anhang A der Norm ein Mapping zwischen ihr und dem SDL beschrieben. Unternehmen, die auf Basis des SDL von Microsoft entwickeln, dürften es damit besonders leicht haben, Konformität zur ISO 27034-1 zu erreichen.

Abbildung 4 bindet SDL-Elemente in ein ONF nach ISO 27034-1 ein: Die Sicherheitsanforderungen werden hierbei von den im SDL üblichen Regulatorien „Product Group" (PG), „Legal and Corporate Affairs" (LCA), „Human Resources" (HR) und „Line of Business Applications" (LOB App) abgeleitet. Hieraus können sich zum Beispiel länderspezifische Datenschutzanforderungen oder besonders hohe Sicherheitsanforderungen an Banking-Applikationen ergeben.

Die nötigen „Application Security Controls" (ASC) werden den SDL-Prozessen entnommen. So fordert der SDL in der Designphase beispielsweise ein Threat-Modeling: Eine entsprechende ASC könnte lauten, dass die folgende Implementationsphase erst beginnen darf, wenn ein vollständiges Threat-Modeling des Designs durchgeführt wurde.

Die Applikationssicherheit betreffende Prozesse sind „Line of Business Applications", „Final Security Review" und „Archival" – es müssen zum Beispiel alle Informationen und Daten zu einer Software archiviert werden, um diese auch nach dem Release optimal pflegen zu können. Des Weiteren sorgt ein „Final Security Review" dafür, dass die Applikation auch tatsächlich das notwendige Vertrauenslevel erreicht.

Das SDL-Model wird in das „Application Security Life Cycle Reference Model" gemapped – dieses Mapping ermöglicht es Unternehmen, die ihren Entwicklungsprozess SDL-konform ausgelegt haben, ohne größere Umstellungen Konformität zur ISO 27034-1 zu erlangen. Ähnlich dem SDL kann auch jeder andere Software-Entwicklungsprozess Normkonformität erlangen, unter Umständen sind hierfür aber einige Anpassungen oder Erweiterungen notwendig. ■

Prof. Dr. Hartmut Pohl ist geschäftsführender Gesellschafter der softScheck GmbH. B. Sc. Jochen Klein ist Consultant bei softScheck.