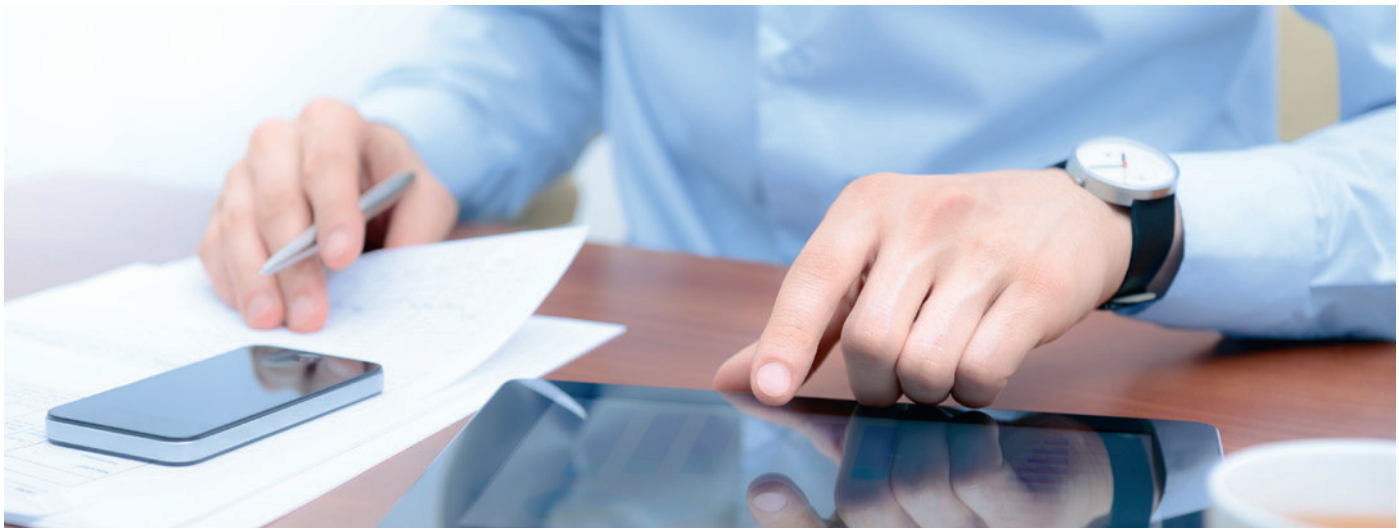


Mehr Sicherheit durch Security-Testing

Ein Prozessleitfaden zur ISO 27034 „Application-Security“

Hartmut Pohl & Thomas Bötner

IT-Security zum Schutz vor Cyberkriminalität sowie Spionage- und Sabotage-Angriffen wird von Unternehmen und Behörden eine immer größere Bedeutung beigemessen. Die fortschreitende Digitalisierung in den Unternehmen mit All-IP, „Industrie 4.0“, „Internet-of-Things“ und die interagierenden – auch mobilen – Endgeräte wie Handys, Smartphones, Tablets, Wearables und weitere vergrößern die Angriffsflächen und wecken gleichzeitig immer mehr Begehrlichkeiten bei Angreifern aus Geheimdiensten und insbesondere der Organisierten Kriminalität.

Die damit verbundenen Herausforderungen sind enorm – technisch, organisatorisch und rechtlich – denn Vorstand und GmbH-Geschäftsführer haften persönlich nach AktG § 91 II bzw. GmbHG § 43 Abs. 1 mit der Sorgfalt eines ordentlichen Geschäftsmannes für ‚ein System zur frühzeitigen Erkennung von den Fortbestand des Unternehmens bedrohenden Entwicklungen und Risiken‘ (KonTraG). IT-Security ist also angesichts der möglichen hohen finanziellen Verluste längst Chefsache geworden. Dies gilt nicht nur für den internen Geschäftsbetrieb sondern auch für die Beziehungen zu Kunden und Geschäftspartnern. Die technischen Aspekte sollen hier anhand der ISO 27034 dargestellt werden.

Sicherheitslücken identifizieren und beheben

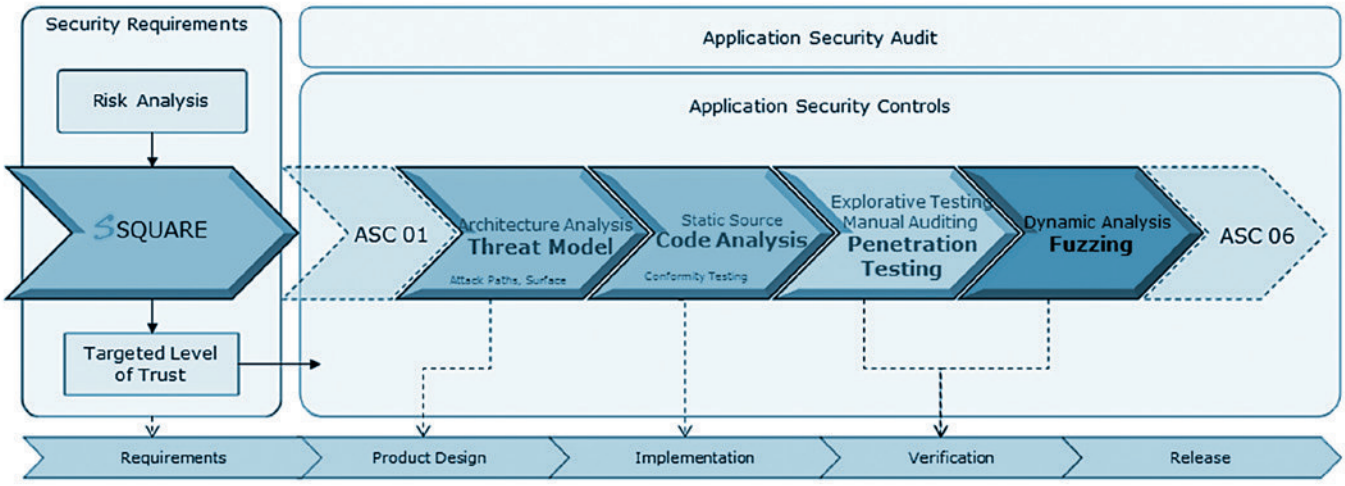
Vermutlich wird jegliche digitale (und auch die analoge) Kommunikation von den Sicherheitsbehörden insbesondere aber von der Organisierten Kriminalität vollständig abgehört („jedes Gerät, überall, jederzeit“). Gespeicherte Daten (Forschungsdaten, Personendaten, Meinungen, Dokumente, Bilder, Industriesteuerungen – auch von (Kern-)Kraftwerken, Wahlergebnisse, Gesundheitsdaten) werden vollständig ausgelesen oder werden per Tauschhandel von Anderen erworben.

Alle abgehörten und ausgelesenen Daten werden für die – eventuell zukünftige – Auswertung gespeichert. Daten werden – bei Bedarf auch in Echtzeit – manipuliert. Die mögliche Manipulation und die Sabotage bis hin zur vollständigen Stilllegung des Betriebsablaufs stellen ernsthafte Bedrohungen für Unternehmen aller Größen dar. Diese Angriffe werden meist gar nicht erkannt. Systematisches Security-Testing ist unverzichtbar, weil funktionales Testen und Penetration-Testing nicht ausreicht.

Technische Maßnahmen helfen weder gegen Abhören noch gegen Manipulation der Kommunikation! So ist z.B. die „Ende-zu-Ende“-Verschlüsselung nur sicher, wenn sie selbst und die erforderliche umfangreiche Sicherheitsinfrastruktur tatsächlich sicher implementiert ist – also z.B. keine Backdoors und Sicherheitslücken enthält.

Sicherheitsmaßnahmen wie Firewalls, Intrusion-Detection und Prevention-Systems, Virensuchprogramme, digitale Signatur, Verschlüsselung – auch „Ende-zu-Ende“ – können umgangen oder geknackt werden.

Jedoch kann das Eindringen in Computer durch die Identifizierung der Sicherheitslücken (und deren Behebung) vollständig verhindert werden, denn alle Cyberangriffe basieren auf der Ausnutzung sicherheitsrelevanter Fehler bzw. Sicherheitslücken in Software und Firmware. Es gilt: Ohne Sicherheitslücke kein erfolgreicher Angriff! Daher muss es das Ziel sein, möglichst alle Sicherheitslücken zu identifizieren und zu patchen.



Prozessleitfaden zur ISO 27034 konformen sicheren Software-Entwicklung mit fünf Tool-gestützten Methoden.

ISO 27034 bietet Rahmen

Einen allgemeinen Ansatz zum Management von Software-Sicherheit liefert die 2011 veröffentlichte ISO 27034-1: „Information technology – Security techniques – Application security". Die Norm unterstützt die Integration von Konzepten, Frameworks und Prozessen zur Application-Security in den unternehmerischen Entwicklungszyklus. Die ISO 27034 liefert damit einen Rahmen, um alle Sicherheitsprozesse auf Organisationsebene zu steuern – inkl. Beschaffung und Outsourcing der Software-Entwicklung.

Den Kern der ISO 27034 bildet eine unternehmensweite Bibliothek mit allen Sicherheitsaktivitäten für die Softwareentwicklung. Gemäß den Anforderungen für das jeweilige Software-Projekt werden ausgewählte Sicherheitsaktivitäten angewandt und in der Verifikationsphase auf ihre erfolgreiche Implementierung hin überprüft.

Zur Identifizierung bisher unbekannter und nicht veröffentlichter bzw. nicht erkannter Sicherheitslücken (Zero-Day-Vulnerabilities) werden von der Norm die folgenden fünf Methoden vorgeschlagen:

1. Security-Requirements-Analysis: Identifizierung und Überprüfung exakter Sicherheitsanforderungen.
2. Security-by-Design: Threat-Modeling überprüft die Software-Architektur kritischer IT-Infrastrukturen und Netzwerke.
3. Code-Review: Static-Source Code-Analysis – semi-automatisiertes Scannen des Quellcodes auf Sicherheitslücken zur Identifizierung von Sicherheitslücken wie Race-Conditions, Deadlocks, Zeiger- und Speicherverletzungen.
4. Penetration-Testing: Dynamische Sicherheitsprüfung mit bekannten Angriffen zur Identifizierung bekannter Sicherheitslücken.
5. Dynamic-Analysis – Fuzzing: Dynamische Sicherheitsprüfung – mit erfahrungsgemäß erfolgreichen Angriffsdaten werden bisher neuartige Angriffe gefahren zur Identifizierung von Zero-Day-Vulnerabilities.

Zur sicheren Software-Entwicklung wird ein Prozessleitfaden vorgeschlagen, der auf der Basis der ISO 27034 mit fünf Tool-gestützten Methoden SQUARE (Threat-Modeling, Static-Source-Code-Analysis, Penetration Testing und Dynamic Analysis – Fuzzing insbesondere zur Identifizierung bisher nicht-bekannter Sicherheitslücken (Zero-Day-Vulnerabilities)) beruht. Der Prozessleitfaden soll dem Ziel dienen, Tool-gestützt sichere ISO 27034 konforme Software-Entwicklung zu implementieren. Das aufwändige Einarbeiten aller Projektbeteiligten in die Norm ist bei der Verwendung des Prozessleitfadens nicht notwendig. Auch bereits bestehende Sicherheitskonzepte und Maßnahmen lassen sich mit dem Prozessleitfaden zusammenführen.

Praxis-orientierter Prozessleitfaden

Der vorgeschlagene Prozessleitfaden ist unabhängig vom verwendeten Software-Development-Lifecycle (vom Wasserfallmodell, über V-Modell bis hin zu modernen agilen Ansätzen wie Scrum). Mit einem ISO 27034 konformen Entwicklungsprozess und dem darin vorgeschlagenen Security-Testing-Process können Software, Firmware und Apps gegen Cyberangriffe gesichert werden. ■

Thomas Bötner, B.Sc, ist als Consultant bei der softcheck GmbH tätig.

Prof. Dr. Hartmut Pohl ist geschäftsführender Gesellschafter der softcheck GmbH.