Schulungen und Workshops

Wir transportieren auch gern unser gesamtes Wissen in Ihr Unternehmen, bilden Ihre Mitarbeiter in allen Aspekten der Informationssicherheit aus und coachen Ihre Mitarbeiter im täglichen Betrieb anhand Ihrer Projekte.

Alle Workshops sind praxisorientiert, dies zeichnet sich vor allem durch begleitende realistische Übungen aus, die jeder Teilnehmer an einem von uns vorkonfigurierten Übungsrechner durchführt.

softScheck bietet Workshops beispielsweise zu den folgenden Themen an:

- Security Testing Process
- ISO 27034–konforme Softwareentwicklung – SASM
- Security Requirements – SSQUARE
- Threat Modeling
- Static Source Code Analysis
- Penetration Testing
- Fuzzing
- Web Application Security
- IT Forensics
- Mobile Security & BYOD
- Backdoor Detection
- Sicherheitsprodukte (Firewall, WAF, VPN Gateway, etc.): Auswahl von Produkten und Bewertung

Wir bieten alle Workshops und Schulungen als 1-tägige Kompaktkurse und 2- bis 3-tägige Intensivkurse an. Unsere Workshops und Schulungen werden ausschließlich von im jeweiligen Bereich qualifizierten Beratern durchgeführt.

Ist ihr gewünschtes Thema der Informationssicherheit nicht dabei? Gerne erstellen wir auch maßgeschneiderte Individual-Workshops.

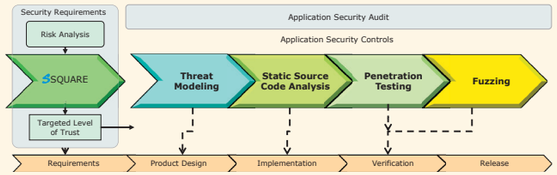
Application Security Management

ISO 27034-konforme Softwareentwicklung

Der Prozessleitfaden **SASM** unterstützt die ISO 27034-konforme Software Entwicklung. Angelehnt an unseren Security Testing Process werden die 5 Methoden als Security Bausteine (Application Security Controls ASCs) in die ISO 27034 vollständig und Tool-gestützt gemappt.

Der Integrationsaufwand wird dabei so gering wie möglich gehalten.

Ein aufwendiges Einarbeiten aller Projektbeteiligten in die ISO-Normen entfällt, da alle relevanten Norminhalte verständlich aufbereitet im gesamten **SASM** integriert sind.



SASM – softScheck Application Security Management

- Einfacher Start – keine Einarbeitung in die Norm
- ISO 27034–konforme Softwareentwicklung
- Kürzere Entwicklungszeit
- Minimierung der Entwicklungskosten
- Vermeidung von Sicherheitslücken schon während der Entwicklung

softScheck
we identify vulnerabilities others don't

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter
softScheck GmbH Köln
www.softScheck.com
Büro: Bonner Straße 108, 53757 Sankt Augustin, Deutschland
Tel.: +49 2241 25543-0
Fax: +49 2241 25543-29
prof.dr.hartmut.pohl@softScheck.com

softScheck
we identify vulnerabilities others don't

Wir machen Software sicher.

Security Testing

Methodisches, Tool-gestütztes Security Testing auf dem aktuellen Stand der Technik ISO 27034 basierend und Security Development Lifecycle (SDL): Steigerung des Sicherheitsniveaus durch Identifizierung von Sicherheitslücken in Software-, Hardwareprodukten und Ihrer IT-Infrastruktur.
softScheck ist mit seinem Security Testing Process seit mehr als 10 Jahren erfolgreich in diesen Anwendungsbereichen:

- Software: ERM, CRM, SCM, ERP, E-Business, CIM – Clouds
- Webanwendungen: E-Commerce, ERP, E-Banking, CMS
- Mobile Systeme: Apps & mobile Webanwendungen für smart and mobile Devices, MDM (Mobile Device Management)
- Sicherheitsprodukte: Firewalls, Web Application Firewalls, Router, Gateways, Verschlüsselung, Intrusion Detection & Prevention
- IT-Infrastrukturen: Netzwerke, Client-Server, VoIP, SAP
- Automatisierung: ICS, ROS, PLC/SPS, HMI, embedded Systems, SCADA (Supervisory Control and Data Acquisition), Smart Grid

Plus Leistungen & Entwicklungen

- Workshops und Coaching in Projekten
- Klassische IT-Sicherheitsberatung (Grundschutz bis Hochsicherheit)
- Entwicklung des bisher weltweit einzigen ISO 27034 basierten Prozessleitfadens zur Erstellung sicherer Software: **SASM** – softScheck Application Security Management.

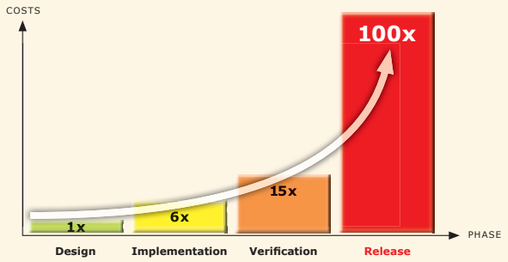
Prof. Dr. Hartmut Pohl – Geschäftsführender Gesellschafter, softScheck GmbH, Sankt Augustin/Köln

Identifizierung von Sicherheitslücken

Insbesondere bisher nicht-erkannte Zero-Day-Vulnerabilities

Das softScheck Alleinstellungsmerkmal ist seit mehr als 10 Jahren der kostengünstige und sehr erfolgreiche Security Testing Process zur Identifizierung von Sicherheitslücken (Vulnerabilities) und insbesondere bisher nicht-erkannten **Zero-Day-Vulnerabilities** in jeder Art Software und Firmware.

Dies verhindert Angriffe und erhöht das Sicherheitsniveau. Denn: Ohne Sicherheitslücken kein erfolgreicher Angriff. Zudem erspart es dem Hersteller und den Anwendern der eingesetzten Software (internationale Unternehmen – große, mittlere und auch kleine, sowie Behörden) bis zu 99% der Wartungs- und Fehlerbehebungskosten.



Kosten der Fehlerbehebung in den Software-Entwicklungsphasen

Eigene Untersuchungen in Projekten von softScheck zeigen, dass der Aufwand zur rechtzeitigen Identifizierung kritischer Vulnerabilities – insbesondere der bisher nicht-erkannten Zero-Day-Vulnerabilities – mit Security by Design – Requirements Analysis, Threat Modeling, Static Source Code Analysis, Penetration Testing und Fuzzing vergleichsweise gering ist.

Security Testing Process

softScheck arbeitet erfolgreich Tool-gestützt mit den folgenden 5 Methoden gem. ISO 27034, um Sicherheitslücken – insbesondere nicht bekannte Zero-Day-Vulnerabilities – zu identifizieren:

① **Security Requirements – SSQUARE:** Methodische und Tool-gestützte Entwicklung und Analyse exakter Sicherheitsanforderungen mit softScheck **S**ecurity **QUA**lity **R**equirements **E**ngineering

② **Threat Modeling:** Überprüfung der Sicherheitsarchitektur auf Sicherheitslücken

③ **Static Source Code Analysis:** Semi-automatisierte Prüfmethode des Source Codes

④ **Penetration Testing:** Simulated Attacks u.a. zur Überprüfung auf bereits bekannte Sicherheitslücken und manuelles Auditing

⑤ **Dynamic Analysis – Fuzzing as a Service®:** Test der ausführbaren, kompilierten Zielsysteme mit erfahrungsgemäß erfolgreichen Angriffsdaten

Mit jeder dieser Methoden werden andere (!) Fehler und Sicherheitslücken identifiziert: Design-, Implementierungs- und Laufzeit-Fehler.
Zum Nachweis identifizierter Sicherheitslücken programmieren unsere Security Experten auch die (Sicherheitslücken ausnutzenden) Exploits und beheben (fixen, patchen) sie: Fehlerkorrekturen im Design und im Quellcode. Damit kann sehr zeitnah ein Patch veröffentlicht werden.

softScheck bietet ergänzend **Backdoor Detection** an: Analyse und Identifizierung nicht-dokumentierter, verdeckter und versteckter Funktionen.

Security Quality Requirements Engineering

softScheck entwickelt und analysiert Tool-gestützt die exakten Anforderungen an die Sicherheitsarchitektur. Dabei werden diese Security-Anforderungen mit Hilfe der **SSQUARE** Methode vollständig identifiziert, definiert und validiert mit dem Ziel, das Sicherheitsdesign eines Produkts zu entwickeln.
Dabei unterstützt unser Tool **SSQUARE**. Es hilft, alle Prozess-Schritte effektiv und effizient durchzuführen und liefert die notwendigen Security Requirements. Ihre Vorteile im Überblick:

- Einfacher Start – keine Einarbeitung in den **SSQUARE** Prozess
- Verringerung der Kosten
- Time-to-market optimiert
- Sichere Software Architektur von Beginn an
- Minimierung des Entwicklungsrisikos

Threat Modeling

Da etwa die Hälfte der sicherheitsrelevanten Fehler auf Designfehler zurückzuführen ist, überprüft softScheck das Sicherheitsdesign eines Softwaresystems:

- Identifizierung sicherheitsrelevanter **Kommunikationskanäle und Prozesse**
- Spezifikation und Ausbau des **Threat Models**.
- Identifizierung der **Threats** (Bedrohungen), **Vulnerabilities** und der zugehörigen **Sicherheitsmaßnahmen**.

Es lassen sich sowohl neue als auch schon bestehende Systementwürfe und Architekturen verifizieren.

Static Source Code Analysis – Code Reading

Semi-automatisiertes Scannen des Quellcodes auf Sicherheitslücken zur Identifizierung von Race Conditions, Deadlocks, Zeiger- und Speicherverletzungen etc. Die Qualität und Quantität des Analyse-Resultats hängt also maßgeblich von der Auswahl geeigneter Tools – und geschultem Fachpersonal – ab.
softScheck setzt diese verfügbaren 3 Tool-Klassen ein:

- Style Checking
- Semantic Analysis
- Deep Flow Analysis

Dynamic Analysis

Penetration Testing & Manual Auditing

Dynamische Sicherheitsprüfung, bei der bekannte Angriffe auf ein System simuliert werden, um in dieses einzudringen. Damit werden bekannte Sicherheitslücken identifiziert und damit das Sicherheitsniveau ermittelt.

Ziel ist es auf Basis der identifizierten Sicherheitslücken Sicherheitsmaßnahmen zu erarbeiten und damit das Sicherheitsniveau des Zielsystems anzuheben.

softScheck führt Penetration Tests auf der Grundlage und Klassifizierung der Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch.

softScheck setzt darüber hinaus manuelles Auditing ein, für das ein hoher Grad an Expertise notwendig ist, z.B. in diesen Bereichen:

- Sichere Programmierung
- Sichere Architekturen
- Aktuelle Angriffstechniken

Fuzzing as a Service®

Dynamische Sicherheitsprüfung, bei der erfahrungsgemäß erfolgreich Angriffsdaten an die Eingabeschnittstellen gesendet werden, um Anomalien zu erzeugen. Herbeigeführte Anomalien werden im nächsten Schritt reproduziert und untersucht mit dem Ziel, unbekannte, nicht-veröffentlichte Sicherheitslücken **(Zero-Day-Vulnerabilities)** zu identifizieren. Als dynamische Testmethode benötigt Fuzzing keinen Quellcode (Black-Box Test).

Beispielsweise können Sonderzeichen in die Eingabedaten eingestreut, bestimmte Zeichen mehrfach wiederholt oder auch überlange Eingaben generiert werden, um z.B. Buffer Overflows zu erreichen.

softScheck setzt dazu proprietäre Fuzzer, Open Source Produkte und auch Eigenentwicklungen (Fuzzer oder Fuzzing-Module) ein.