softScheck
we identify vulnerabilities others don't

**Pressemitteilung**

**Security Testing as a Service Process** angewandt auf **Industrial Control Systems (ICS)**
auf der IPC SPS Drives 27. - 29. Nov. 2012 in Nürnberg Halle 7A Stand 751

---

Das europaweite Alleinstellungsmerkmal von softScheck ist die kostengünstige und erfolgreiche Identifizierung bisher nicht-erkannter Sicherheitslücken (Zero-Day-Vulnerabilities) in jeder Art Software (und Hardware). Dies ist relevant, weil Angriffe unverzichtbar Sicherheitslücken benötigen: Ohne Sicherheitslücke kein erfolgreicher Angriff!

**1. Standardisierter Tool-gestützter 'Security Testing as a Service' Process**

Dazu bietet softScheck einen **standardisierten Tool-gestützten Security Testing Process** an - bestehend aus den folgenden 8 Verfahren:

1. **Security by Design**: Entwicklung von Sicherheitsarchitekturen für Software
2. **Threat Modeling**: Überprüfung der Sicherheitsarchitektur auf Sicherheitslücken
3. **Static Source Code Analysis (White Box)**
4. **Penetration Testing** zur Überprüfung auf bereits bekannte Sicherheitslücken
5. **Dynamic Analysis - Fuzzing**: Test des ausführbaren, kompilierten Programmcodes – kein Quellcode erforderlich (Black Box),
6. **Explorative Testing** und manuelles Code Auditing
7. Identifizierung und Analyse von **Covert Functions** – undokumentierte, verdeckte Funktionen – u.a. auch auf mobile Devices.
8. **Exploit Programming** zum **Nachweis** identifizierter Sicherheitslücken: Dazu programmieren unsere Security Experten auf Wunsch auch die (Sicherheitslücken ausnutzenden) Exploits und beheben (fixen) (auf Wunsch) die identifizierten Sicherheitslücken: Fehlerkorrekturen im Quellcode. Dadurch wird das Software-Entwicklerteam in die Lage versetzt, sehr zeitnah einen Patch zu veröffentlichen.

Die Verfahren werden u.a. vom Bundesamt für Informationssicherheit (BSI) unterstützt. Das BSI und das ICS-CERT warnen vor zunehmenden Angriffen auf Industriesteuerungen, speicherprogrammierbare Steuerungen / Programmable Logic Controller (SPS/PLC). Das BSI listet die konkreten Bedrohungen: „Industrial Control System Security - Top 10 Bedrohungen" (ICSS-Top 10). Wir zeigen am Stand auf, welche Bedrohungen der ICSS Top 10 Liste des BSI zutreffen.

Mit diesem **standardisierten Tool-gestützten Security Testing Process** ist es erstmals gelungen, in sehr kurzer Zeit neue, bisher nicht-erkannte Sicherheitslücken (Zero-Day-Vulnerabilities) zu identifizieren.

Dabei arbeitet softScheck eng mit den einschlägigen Herstellern von Software und Hardware für Industrial Control Systems (ICS) zusammen und übermittelt die identifizierten (bisher nicht-erkannten) Sicherheitslücken (Zero-Day-Vulnerabilities) an die jeweiligen Hersteller entgeltfrei. Auf dem softScheck Messestand wird die Identifizierung bisher nicht-erkannter Sicherheitslücken mittels der Verfahren Threat Modeling und Fuzzing auf einer betriebsfertigen Anlage hands-on präsentiert.

Allein mit dem Verfahren Threat Modeling wurden in einer Stichprobe aus 40 Projekten ca. 1.000 Threats identifiziert und ca. 100 hoch-kritische, bisher nicht-erkannte Sicherheitslücken. Insgesamt konnten in dieser Stichprobe die folgenden Ergebnisse (insgesamt 156 Zero-Day-Vulnerabilities) erreicht werden:

| Method | No. Zero-Day-Vulnerabilities | No. Tools used |
|---|---|---|
| Threat Modeling | 112 (986 Threats) | 1 - 2 |
| Static Source Code Analysis | 17 | 3 – 5 |
| Penetration Testing | (76 known Vulnerabilities) | 4 + |
| Dynamic Analysis: Fuzzing | 27 | > 60 |

Ein Beispiel für den erfolgreichen Einsatz des softScheck Security Testing Process ist unser Technologiepartner OpenLimit: OpenLimit wendet in der Entwicklung eines Smart Metering Gatewaysvon der Designphase bis in den Testbereich moderne Techniken zur Erkennung und Beseitigung von Schwachstellen an. Dieser Aufwand rechnet sich am Ende für die Kunden: Sicherheitslücken werden bereits im Vorfeld konsequent ausgeschaltet und sichern die langfristige Verfügbarkeit der Technik.

## 2. Branchen

softScheck ist in den folgenden Branchen aktiv:

- Automotive
- Chemie-, Pharma- und Getränkeindustrie
- Finanzdienstleister
- Gesundheit
- IT-Sicherheit
- Software
- Versorger (u.a. Smart Grid Security)

Auf der Messe hält unser Seniorberater Herr Gürkan Aydin, B.Sc. einen **Vortrag** am **Donnerstag, den 29.11.2012 um 9:30 Uhr** im **Raum Seoul**:

**„Stuxnet, seine Derivate und die Zukunft sicherer Prozesssteuerung".**

Darüber hinaus werden wir täglich in Vorträgen auf unserem Stand über unsere Arbeitserfolge berichten – auch zusammen mit

**Herrn Lunkeit, Geschäftsführer unseres Technologiepartners OpenLimit SignCubes AG**.

**Über** softScheck

Die IT-Sicherheitsberatung softScheck GmbH hat sich in den letzten Jahren mit der Identifizierung von bisher nicht-erkannten Sicherheitslücken in Software (und auch Hardware) neue, attraktive Wachstumsfelder erschlossen.

softScheck führt regelmäßig **Sicherheitsprüfungen** von Software und Hardware durch. Daneben bietet softScheck selbstverständlich auch die klassische IT-Sicherheitsberatung an vom Grundschutz (ISO 27000-Familie) bis hin zur Hochsicherheit in der Informationsverarbeitung (Redundanz und Diversität) – auch mit Consulting, Coaching und Forensics.

**Über OpenLimit**

Die OpenLimit SignCubes AG ist ein international führender Anbieter zertifizierter Software für elektronische Signaturen und Identitäten. Mit Niederlassungen in der Schweiz sowie in Deutschland arbeitet die Unternehmens-Gruppe daran, Kunden technologisch ausgereifte und praxisgerechte Lösungen für ein rechtssicheres und effizientes Dokumenten- und Identitätsmanagement in allen Geschäftsfeldern zu ermöglichen sowie Technologien für die sichere Datenkommunikation anzubieten. Die OpenLimit Signaturtechnologien unterstützen neben den gängigsten Signaturkarten des deutschsprachigen Markts auch viele internationale Smartcards. Die Zertifizierung nach dem Sicherheitsstandard für Software-Produkte Common Criteria EAL4+ bürgt für ein Maximum an Sicherheit der OpenLimit Software-Lösungen.

**Kontakt:**


Anja Wallikewitz
Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29
anja.wallikewitz@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com