SCHWACHSTELLEN IN INDUSTRIEANLAGEN ERKENNEN UND BEHEBEN

INDUSTRIAL SECURITY TESTS

magnetisch digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

DIE GEFAHR WÄCHST

„Hackerangriff auf kritische Industrieanlagen“ – solche Schlagzeilen schaffen es immer häufiger auf die Titelseiten diverser Nachrichtenmagazine. Die Zeiten in denen es Angreifer nur auf Webseiten im Internet abgesehen haben sind längst Vergangenheit. Vielmehr haben sie es mittlerweile auf kritische Infrastrukturen abgesehen. Dabei macht die stetig steigende Vernetzung von Industrieanlagen in IP-basierten SCADA-Netzwerken es den Angreifern immer einfacher ganze Produktionsstraßen zu kompromittieren. Hat der Angreifer Zugriff zum Netzwerk erlangt, kann er beliebig die vernetzten Anlagen manipulieren. Als Einfallstor können hier Fernwartungszugänge über das Internet, verfügbare WLAN-Netze, Schnittstellen an Field-Stations oder das Office-Netzwerk der jeweiligen Firma dienen.

VERHEERENDE AUSWIRKUNGEN

Die Auswirkungen, wenn Industrieanlagen durch einen Angreifer attackiert werden, sind meist besonders verheerend. Wasser-, Strom und Gasversorgung sowie unzählige Produktionsanlagen werden mithilfe von SCADA-Systemen gesteuert. Gelingt es einem Angreifer solch ein System zu manipulieren, kann das im schlimmsten Fall Gefahr für Leib und Leben bedeuten. Im Allgemeinen bedeutet ein erfolgreicher Angriff aber zumindest einen erheblichen finanziellen Schaden und einen Imageverlust für die jeweilige Organisation.

IHRE VORTEILE AUF EINEN BLICK

- **Schwachstellen erkennen und beheben**
- **Speziell angepasstes Testvorgehen**
- **Produktionsausfälle verhindern**
- **Auswirkungen von Angriffen eindämmen**
- **Folgeschäden minimieren**
- **Kosten senken**

T · · Systems ·

RISIKEN FRÜHZEITIG ERKENNEN UND MINIMIEREN

Die T-Systems Multimedia Solutions GmbH bietet speziell an die Anforderungen von SCADA-Systemen angepasste Security-Testleistungen. Diese basieren auf dem Durchführungskonzept für Penetrationstests des BSI und werden inhaltlich durch den NIST Standard 800-82 komplettiert. Unsere Security Experten analysieren im Rahmen eines SCADA Security Tests Ihre Systeme aus der Sicht eines potentiellen Angreifers und decken so Schwachstellen in Ihrem System auf, bevor sie ein Angreifer ausnutzt. Anschließend zeigen wir Ihnen Möglichkeiten, wie Sie die gefunden Schwachstellen beheben können, bevor Ihnen durch diese ein erheblicher Schaden entsteht.

MÖGLICHE TESTSCHWERPUNKTE

Physischer Schutz

- Zugangs- und Zutrittsbeschränkungen zu Produktionsstätten und Field Stations
- Zugriffsbeschränkungen auf Arbeitsplatzsysteme/Terminals
- Schutz der IT-Systeme / Serverräume
- Überwachungssysteme
- Gebäudeschutz

Netzwerktopologie

- Überprüfung der Gesamt-Netzwerktopologie
- Authentifizierung der Clients/Produktionssysteme und Server untereinander
- Separierung des Firmennetzwerks von SCADA-Netzwerk
- Firewall, Router, IDS, IPS Konfigurationen
- VLANs, DMZs
- Remote Zugriffe
- WAN-Verbindungen

Plattformtests

- Patch Management, Backup- und Logging-Strategien
- Sichere Standardkonfiguration der eingesetzten Clients
- Rollen- und Rechtevergabe
- Einschränkung der Nutzerprivilegien auf den eingesetzten Systemen (HMIs, RTUs)
- Passwortrichtlinien
- Antivirus Lösungen
- Redundanz der Systeme / Failover
- Unnötige Services

Notfallmaßnahmen

- Test der Notfallpläne (Business Continuity Planning, Disaster Recovery)
- Ist das Personal entsprechend vorbereitet und fähig im Notfall richtig zu handeln

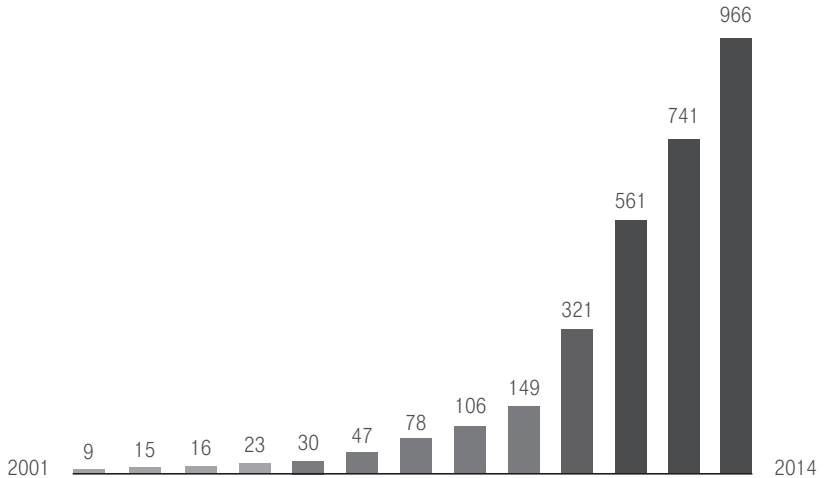
HERAUSGEBER

T-Systems Multimedia Solutions GmbH
Riesaer Straße 5
D-01129 Dresden
Tel.: +49 (0) 351 - 2820 - 0
www.t-systems-mms.com

IHR ANSPRECHPARTNER

Thomas Haase
Tel: +49 (0) 351- 2820 - 2206
Mobil: +49 (0) 175 - 5884 475
E-Mail: t.haase@t-systems.com

T · · Systems ·



ANZAHL DER SCHWACHSTELLEN

Quelle: www.osvdb.org