Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln – von der Stromerzeugung und -verteilung über die Gas- und Wasserversorgung bis hin zur Produktion, Verkehrsleittechnik und modernem Gebäudemanagement. Für Betreiber solcher Anlagen ist es angesichts zunehmender IT-Sicherheitsrisiken und Schwachstellen unerlässlich, sich mit der Sicherheit dieser Systeme zu befassen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit erheblichem Aufwand durchgeführten spezifischen Cyber-Angriffen gegen ICS-Infrastrukturen berücksichtigt werden.

Das vorliegende Kompendium legt den Schwerpunkt auf die Grundlagen sowie Empfehlungen zur Cyber-Sicherheit für Betreiber industrieller Anlagen. 2014 erfolgt die Fortschreibung des Kompendiums, in der weitere Sicherheitsthemen beispielsweise mit Blick auf Hersteller, Maschinenbauer und Integratoren ergänzt werden.

Zum Download des „ICS Security Kompendium": *https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html*

ENISA: besserer Schutzes von SCADA-Systemen erforderlich

Wie lange können wir es uns noch leisten, sensible IT-Infrastrukturen mit nicht gepatchten SCADA-Systemen zu verwenden, fragt die Europäische Agentur für Netz- und Informationssicherheit (ENISA). ENISA argumentiert, dass die EU und ihre Mitgliedstaaten verpflichtendes Patch-Management einführen könnten, um somit Sicherheitslücken zu überbrücken, Cyber-Attacken abzuschwächen und für die Gesellschaft wichtige Infrastruktur zu schützen.

Ein großer Teil der sensiblen Infrastruktur in Europa kann in den Bereichen Energie, Beförderungsmittel und Wasserversorgung gefunden werden. Diese Infrastrukturen sind weitgehend von sogenannten SCADA-Systemen (Supervisory Control and Data Acquisition gemanaged (eine Unterkategorie von Industriellen Steuerungssystemen (ICS)). Die SCADA-Technologie hat sich im letzten Jahrzehnt maßgeblich entwickelt und von einzelnen abgeschlossenen Systemen wegbewegt. Heutzutage operieren SCADA-Technologien in offenen Architekturen und mit Hilfe von Standardtechnologien, welche stark mit anderen Netzwerken sowie dem Internet verbunden sind. Als Konsequenz zu diesen Veränderungen sind SCADA-Systeme nun verstärkt für Attacken von außerhalb des Systems angreifbar. Zurzeit sind die bedeutendsten Probleme mit Patching der Fehlerrate (60%)[1] und der Nichtexistenz des Patchens an sich; weniger als 50% der 364 als kritisch eingestuften, öffentlichen Infrastrukturen hatten Patches[2] für SCADA zur Verfügung.

ENSIA hat verschiedene Best Practices und Empfehlungen herausgestellt, welche den Sicherheitsstatus von SCADA-Systemen durch Patchings maßgeblich verbessern. Anbei sind einige Beispiele:

- Kompensierende Kontrollen:
  - Eine Verstärkung der Verteidigung durch Netzwerkeinteilung um vertrauenswürdige Zonen aufzubauen, welche durch Zugangskontrollen miteinander kommunizieren;
  - Eine Verbesserung des SCADA-Systems durch das Entfernen von unnötigen Leistungen;
- Patch-Management und Dienstleistungsverträge:
  - Eigentümer sollten auch einen Dienstleistungsvertrag für das Patch-Management aufstellen und somit klar die Verpflichtungen des Verkäufers und des Konsumenten im Patch-Managementprozess festlegen;
  - Eigentümer sollten immer ihre eigenen Tests, entweder virtuell oder durch ein separates System durchführen.
  - Zertifizierte Systeme sollten nochmals ratifiziert werden, nachdem ein Patch angewendet wurde.

Web-Zertifikate „Made in Germany" von der Bundesdruckerei

Sichere Identitäten sind ein Schlüsselthema im 21. Jahrhundert. Im Zeitalter des Internets und der weltweiten Mobilität ist es zu einer anspruchsvollen Aufgabe geworden, persönliche Daten zu schützen und Identitäten, Webserver und Webseiten zuverlässig zu verifizieren. Die Bundesdruckerei ist nicht nur führend im Wert- und Banknotendruck, sondern vor allem bei innovativen Lösungen rund um die „Sichere Identität". Als deutsches Unternehmen bietet die Bundesdruckerei ihren Kunden aus Wirtschaft und Verwaltung daher SSL- /TLS-Zertifikate „Made in Germany". Von der Verwaltung des deutschen Wurzelzertifikats bis hin zur Erzeugung eines kundenindividuellen Webserver-Zertifikats gewährleistet die D-TRUST GmbH, das Trustcenter der Bundesdruckerei, ein zuverlässiges und sicheres Management aus einer Hand. Sämtliche Serverzertifikate erfüllen die hohen europäischen Sicherheitsstandards und sind mit den Betriebssystemen und Browsern von Microsoft, Mozilla, Google, Opera und Apple kompatibel.

Passende Zertifikate für eBusiness und eGovernment

Kunden der Bundesdruckerei profitieren von der sicheren und interoperablen Verschlüsselung der Kommunikation zwischen Webservern und Endgeräten mittels SSL- /TLS-Zertifikaten, die auf deutschen Wurzelzertifikaten beruhen. eBusiness- und eGovernment-Dienste können sich somit vor gefälschten Server-Identitäten und dem Missbrauch sensibler Daten bei Zahlungsverkehr, Bürgerdiensten und Gesundheitsdaten schützen. Ausgestellt werden die Zertifikate durch das bei der Bundesnetzagentur akkreditierte Trustcenter D-TRUST GmbH, eine hundertprozentige Tochtergesellschaft der Bundesdruckerei. Sämtliche Trustcenter-Dienstleistungen werden ausschließlich am Standort der Bundesdruckerei in Berlin erbracht und kontinuierlich durch interne und externe Sicherheitsexperten überprüft. Geschäftspartner, Kunden und Mitarbeiter vertrauen darauf, dass ihre Zahlungsdaten, persönlichen Informationen, Passwörter oder andere sensible Daten sicher übertragen werden. D-TRUST bietet für verschiedene Anforderungen und Verwendungszwecke das passende SSLZertifikat:von der Einstiegsversion bis hin zum weltweit höchsten Zertifikatsstandard.

Weitere Informationen unter *http://www.bundesdruckerei.de/de/167-d-trust-ssl-zertifikate*

1 „In 2011, ICS-CERT hatte eine Fehlerrate von 60% bei Patches welche bekanntgegebene Schwachstelle in Kontrollsystemen beheben sollten."

2 Weniger als 50% der 364 von ICS-CERT identifizierten Schwachstellen hatten Patches zur Verfügung." (SCADA Security Scientific Symposium (S4) Jänner 2012, McBride