TeleTrusT
Pioneers in IT security.

TeleTrusT-Auditorium (it-sa 2016)

Nürnberg, 19.10.2016

Industrie 4.0 braucht Digitale Souveränität

Pamela Krosta-Hartl, LANCOM Systems

Industrie 4.0

- Intelligente Vernetzung von Entwicklung, Produktion, Logistik & Kunden bietet enorme Wachstumspotentiale
- Industrie 4.0 soll den Industriestandort Deutschland nachhaltig sichern

Bildquelle: BITKOM

- Virtuelle und reale Welten verschmelzen, Daten & Sensoren steuern Maschinen
- Angriffe haben reale, physische Auswirkungen:
  - Manipulation von Produkteigenschaften
  - Sabotage von Anlagen und Systemen

Angriffe auf industrielle Systeme

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

Erpressung durch Hacker

Cyberattacke in der Keksfabrik

Hacker richten mit Cyberangriffen nach Schätzungen von Experten Schäden von Hunderten Millionen Euro an. Sichtbar werden die Attacken auf die Industrie aber selten: Den Tätern geht es um Erpressung.

Von Uli Ries

Fabrik (Symbolbild): Die Steuerungsanlagen stehen oft unges

WELT N24 DIGITAL ZEITUNG TV

HOME LIVE TV MEDIATHEK POLITIK WIRTSCHAFT SPORT ABO MEHR

HOME » NEWSTICKER » DPA » INFOLINE » COMPUTER (DPA) » Fraunhofer-Institut: Hacker bedrohen Industrieanlagen

COMPUTER (DPA) FRAUNHOFER-INSTITUT

Hacker bedrohen Industrieanlagen

Stand: 29.09.2015 | Lesedauer: 2 Minuten

Nürnberg - Industrieanlagen sind immer häufiger Angriffen von Hackern ausgesetzt. Darauf hat die Leiterin des Fraunhofer-Instituts für angewandte und integrierte Sicherheit, Claudia Eckert hingewiesen. Viele Kraftwerke und Chemieanlagen könnten über das Internet inzwischen aus der Ferne gesteuert und gewartet werden.

«Damit sind sie aber offen und keine abgeschotteten Systeme mehr», sagte Eckert am Dienstag auf der IT-Sicherheitsmesse it-sa in Nürnberg.

JETZT 4 WOCHEN GRATIS TESTEN

Handelsblatt

Digitalpass Finanzen Unternehmen Politik Technik Auto Sport Pano

IT + Internet Gadgets Forschung + Innovation Medizin Energie + Umwelt

Handelsblatt > Technik > IT + Internet > IT-Schwachstellen bei Industrieanlagen: Angriffsziel Wasserwerk

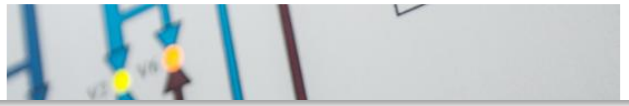
IT-SCHWACHSTELLEN BEI INDUSTRIEANLAGEN

Angriffsziel Wasserwerk

von: Sebastian Neef und Tim Philipp Schäfers
Datum: 15.07.2016 16:05 Uhr
Quelle: Golem.de

Wasserwerke lahmlegen, fremde Wohnungen überhitzen oder einen Blackout auslösen: Wer weiß, wo er suchen muss, kann all dies über das Internet tun. Und viele Betreiber wichtiger Anlagen haben keine Ahnung von der Gefahr.

Facebook Twitter Google+ Xing Linkedin

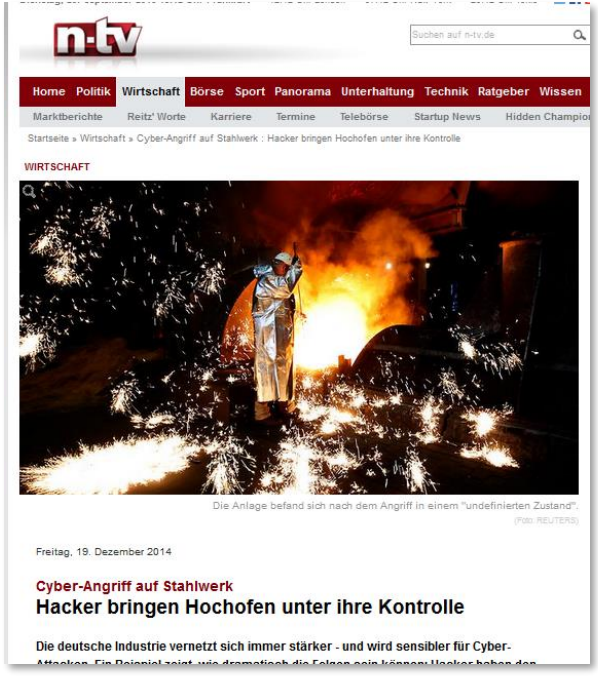


16

Herausforderungen

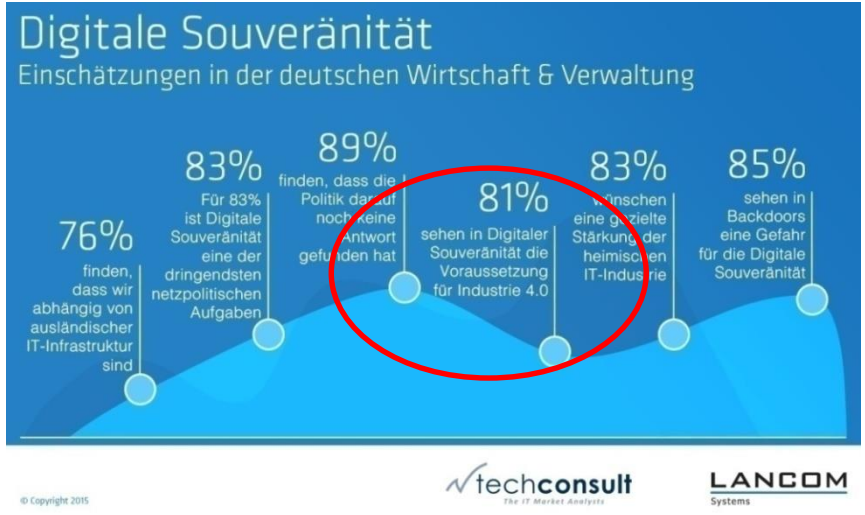
- Industrie 4.0 setzt eine durchgängige Vernetzung von Anlagen/Systemen voraus
- Daten (ICS/SCADA) müssen jederzeit zuverlässig und sicher übertragen werden
- Die meisten industriellen Steuerungssysteme wurden für den Einsatz in isolierten Anlagen entwickelt

- Risiken: Schwachstellen in den Systemen, mangelnde Absicherung, fehlende Vertrauenswürdigkeit von Komponenten
- 91% der Anlagen sind nicht ausreichend geschützt
  (Studie Kaspersky Lab, 2015, über 188.000 untersuchte industrielle Systeme)



Faktor Digitale Souveränität

- Neben mehr IT-Sicherheit ist die volle Kontrolle über die digitalen Systeme/Übertragungswege nötig (= Digitale Souveränität)
- Fehlende Vertrauenswürdigkeit von Komponenten gefährdet diese Kontrolle (z. B. durch Backdoors)
- Anfälligkeit für externe Einflüsse (Kriminelle, Drittstaaten, Industriespione) steigt



- **Gefahren:** Datenklau, Sabotage (Netze ausschalten, Pakete abfangen), Manipulation (Produkteigenschaften)

Orientierung

- Unabhängige Sicherheitszertifizierungen durch das BSI, z. B. gemäß *Common Criteria*
- Qualitätszeichen *"IT Security made in Germany"* für garantiert Backdoor-freie Produkte, die in Deutschland entwickelt und gefertigt werden
- Für Cloud-Angebote: z. B. *Anforderungskatalog Cloud Computing* des BSI bezüglich Informationssicherheit (einschließlich Datenlokation)

Vielen Dank!

- Pamela Krosta-Hartl
- LANCOM Systems GmbH
- pamela.krosta-hartl@lancom.de