Compass Security

[The ICT-Security Experts]

Hacking Industrial Control Systems - Angriff am Fließband
[Compass Beertalk – Jona – 21.03.2013]

Marco Di Filippo

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Darf ich mich vorstellen?

Marco Di Filippo

- Seit 2008 bei Compass, ab 2012 als Managing Director CSDG
- verheiratet, eine Tochter
- Werdegang: Von der Elektrotechnik, über TK-Security zur IT-Security
- Kompetenzen
  - Empirische Sicherheitsprüfungen
  - ICT- Security
    (VoIP, PSTN, GSM …)

Hobbys

- Meine zwei Frauen
- Fußball-Schiedsrichter
- Electronic Music
- ICT-Security

Nach Feierabend...

Compass Security

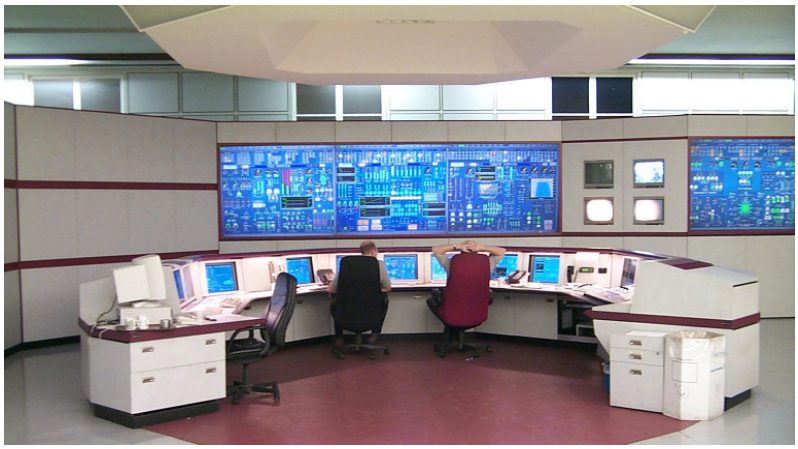
Probieren geht über Studieren...

Einführung

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Automatisierung im Alltag



Automatisierung im Alltag

Fertigung

http://www.youtube.com/watch?v=Kpvr2MVZjws&feature=plcp

http://www.youtube.com/watch?v=YFbBVzYaH_E

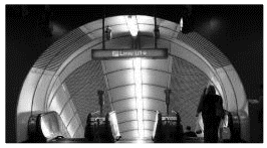
Qualität
Produktivität

Prozesse

Bikinger, „Raffinerie Schwechat“, CC-Lizenz (BY 2.0)

Paul-Gerhard Koch, „Kaprun“Bikinger, CC-Lizenz (BY 2.0)

Gebäude



teakettle, „u1“, CC-Lizenz (BY 2.0)

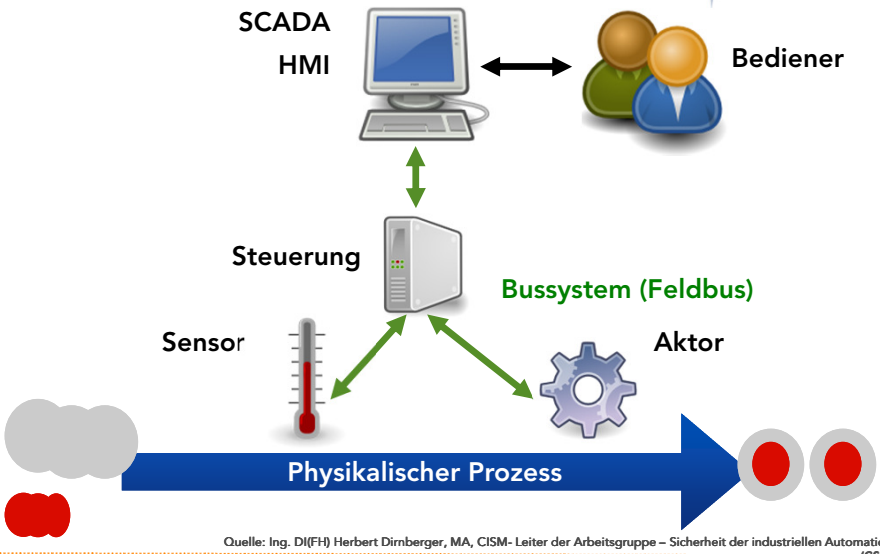
Transport

kritische Infrastruktur

http://creativecommons.org/licenses/by/2.0/de/deed.de
Alle Bilder stammen aus der kostenlosen Bilddatenbank www.piqs.de

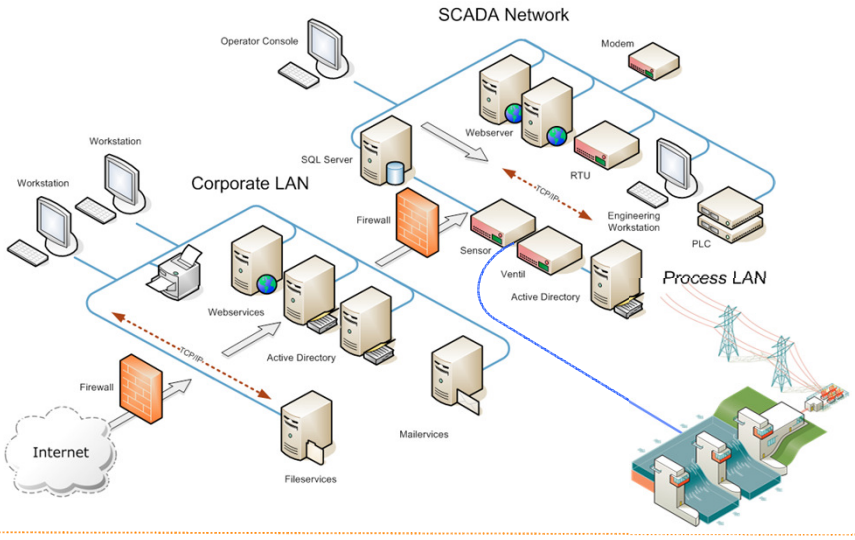
Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Automatisierung in 2 min.



Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Industrial Network Architecture



Verständigung

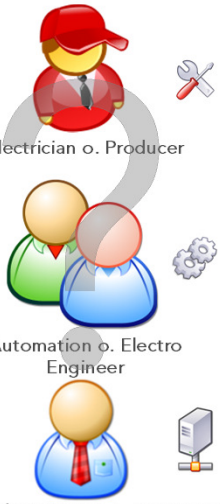
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Gegenseitiges Verständnis

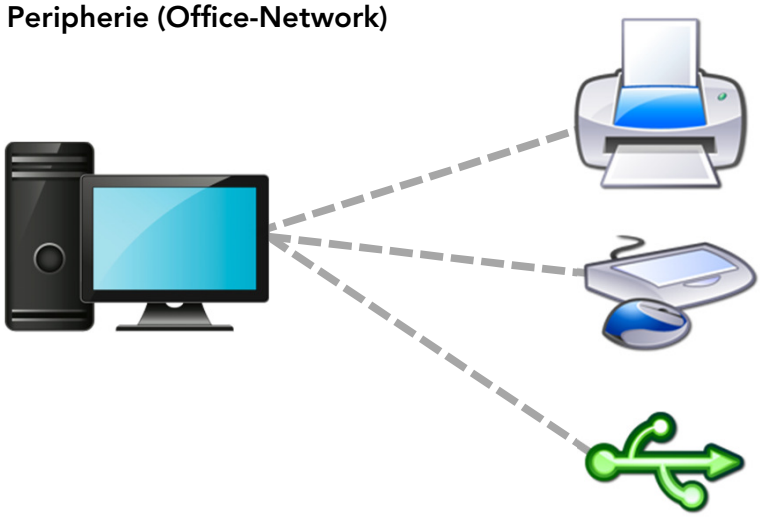
Verantwortlichkeit

Wer ist verantwortlich für die IT-Sicherheit der ICAS?



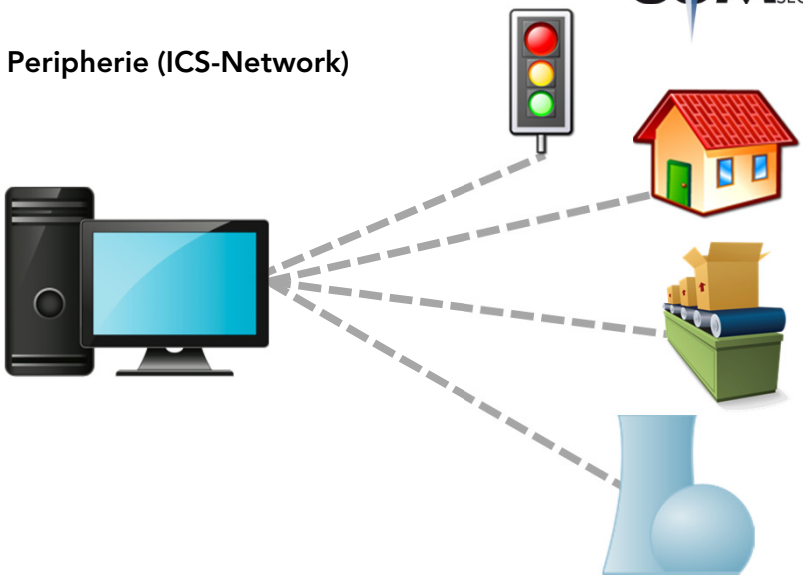
Gegenseitiges Verständnis

Peripherie (Office-Network)



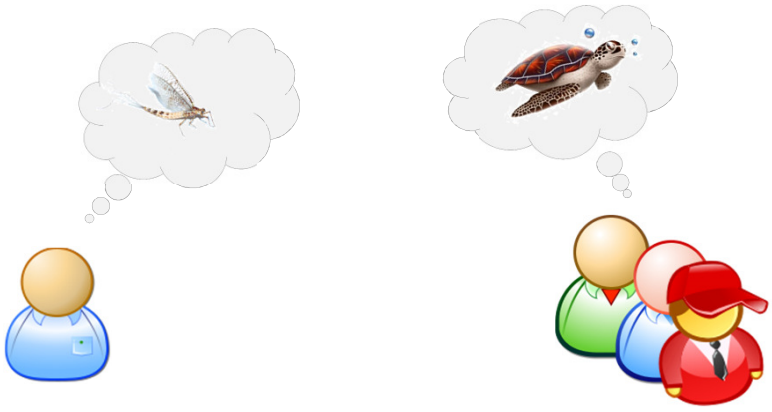
Gegenseitiges Verständnis

Peripherie (ICS-Network)



Gegenseitiges Verständnis

Lebenszyklen

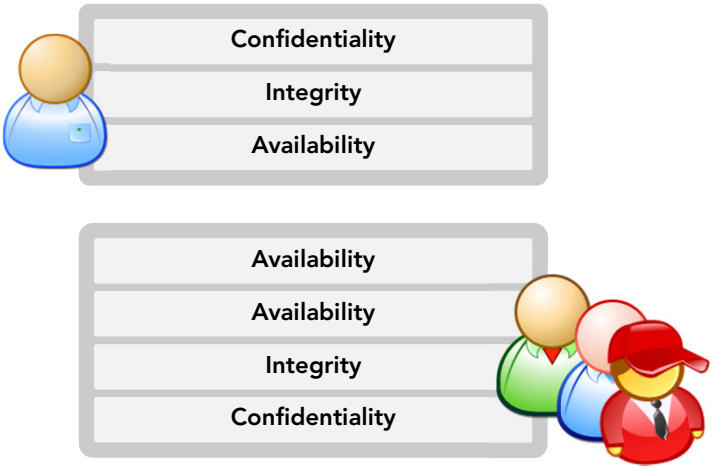


Gegenseitiges Verständnis

Security vs. Safety

Gegenseitiges Verständnis

Schutzzielpriorisierung



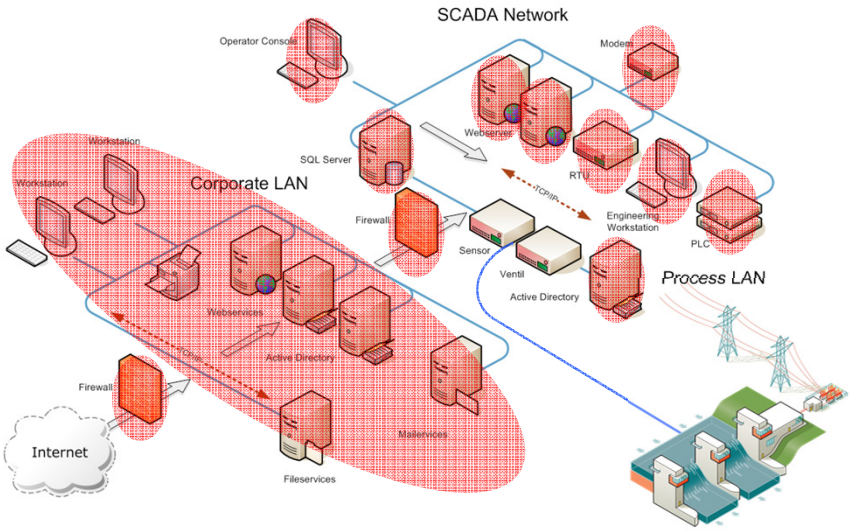
Angriffsflächen

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Industrial Network Architecture

Ansatzpunkte möglicher Angriffe

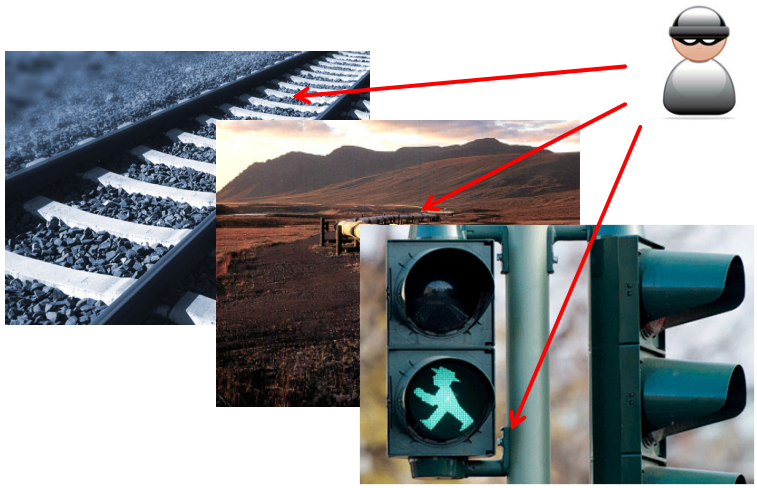


Industrial Network Architecture

The Real World...

Industrial Network Architecture

The Real World...



Industrielle IT-Security - Hype oder Notwendigkeit?

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

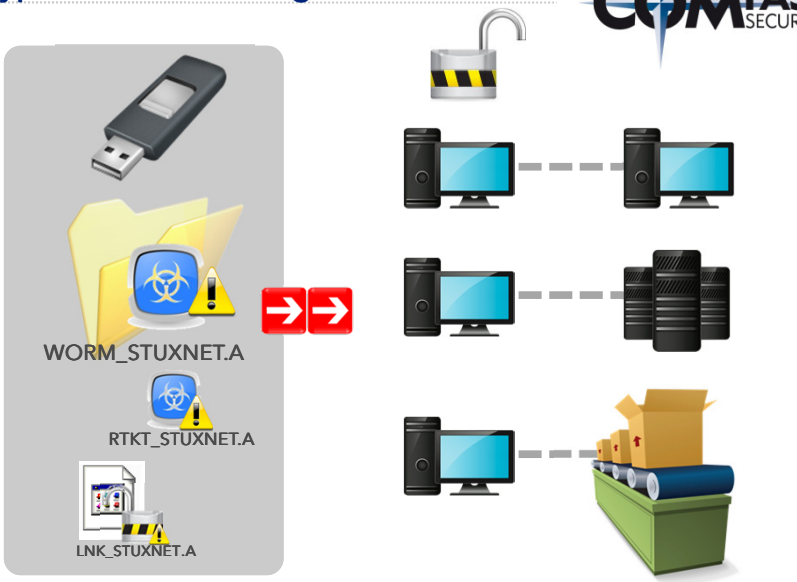
Hype oder Notwendigkeit?

Hallo, darf ich mich kurz vorstellen?

- Ich wurde im Juni 2010 entdeckt
- Ich beherrsche die Sabotage von Siemens SCADA-Komponenten (Simatic S7, WinCC)
- Mein Ziel ist der Eingriff im Frequenzumrichter (Vacon)
- Ich nutzte mehrere Zero-Day Exploits und ein Rootkit
- Fortgepflanzt habe ich mich via USB und Netzwerk
- Ich habe die Welt kurzzeitig in Angst und Schrecken versetzt

Mein Name ist „Stuxnet“

Hype oder Notwendigkeit?



Konzept: http://about-threats.trendmicro.com/dumpImages/0210201014951.jpeg

Hype oder Notwendigkeit?

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
A	Remote Intrusion Solution				
1	FinSpy				
1.1	FinSpy Software				
1.1.1	FinSpy Proxy License FinSpy Master License FinSpy Generation License	FSPL FSML FSGL	1	188,549.00	188,549.00
1.1.2	FinSpy Agent License (per client)	FSAGL	2	12,887.00	25,774.00
				SUBTOTAL	280,787.00
				Freight	6,350.00
				TOTAL	287,137.00

Hype oder Notwendigkeit?

Die Nachkommen!

- 2012 durch Kaspersky Labs entdeckt
- Seit spätestens März 2010 aktiv
- Infizierung über die Windows Update-Funktion
- Nutzt gefälschtes Code-Signing-Zertifikat
- Selbstzerstörung bei Entdeckung
- Ähnlichkeit zu Stuxnet und Duqu
- Ressourcenträchtig

Hype oder Notwendigkeit?

Bundesamt für Sicherheit in der Informationstechnik

BSI-Analysen zur Cyber-Sicherheit

GRUNDLAGEN | STATISTIK | BERICHTE

Industrial Control System Security

Top 10 Bedrohungen

Automatisierungs-, Prozesssteuerungs- und -leitsysteme – subsumiert unter dem Begriff Industrial Control Systems (ICS) – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln – von der Stromerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Produktion, Verkehrsleittechnik und modernem Gebäudemanagement. Dabei wurden in der Vergangenheit Aspekte der Cyber-Sicherheit nachrangig behandelt oder gar vernachlässigt. Betreiber solcher Anlagen müssen sich angesichts zunehmender Vorfälle und Schwachstellen dringend dieser Thematik annehmen. So muss das Risiko und Schadenspotenzial sowohl von nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit erheblichem Aufwand durchgeführten spezifischen Angriffen gegen ICS-Infrastrukturen berücksichtigt werden. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können.

Aktuelle Bedrohungslage

Im Rahmen seiner Analysen zur Cyber-Sicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS-Systeme derzeit ausgesetzt sind. Im Zuge der geplanten Fortschreibung dieser Top 10 sollen zudem Trends bzgl. der kritischsten Bedrohungen aufgezeigt werden. Die Rangordnung der Bedrohungen ergibt sich aus einer Betrachtung von Aspekten wie beispielsweise Täterkreis, der Verbreitung und Ausnutzbarkeit der Schwachstellen sowie der möglichen technischen und wirtschaftlichen Folgen eines Angriffs. Dabei wurden u.a. etablierte Vorfallsdatenbanken ausgewertet.

Nicht in diesen Top 10 enthalten sind weitere Bedrohungen, die derzeit als nachrangig zu den hier Dargestellten erachtet werden. Hierzu gehört z.B. der Einsatz von Smartphones zu Steuerungszwecken oder der Trend hin zu Cloud Computing. Gleichwohl sind solche und alle weiteren im konkreten Einzelfall relevanten Bedrohungen für die Absicherung im jeweiligen Anwendungsfall geeignet zu berücksichtigen. Darüber hinaus wird der Safety-Aspekt explizit nicht behandelt.

BSI-A-CS 004 | Version 1.00 vom 12.04.2012 Seite 1 von 2

BSI-Analysen zur Cyber-Sicherheit

Top 10 Bedrohungen

Nr.	Bedrohung	Erläuterung
1	Unberechtigte Nutzung von Fernwartungszugängen	Wartungszugänge sind bewusst geschaffene Öffnungen des ICS-Netzes nach außen, die häufig jedoch nicht hinreichend abgesichert sind.
2	Online-Angriffe über Office- / Enterprise-Netze	Office-IT ist i.d.R. auf vielen Wegen mit dem Internet verbunden. Meist bestehen auch Netzwerkverbindungen vom Office- ins ICS-Netz, sodass Angreifer über diesen Weg eindringen können.
3	Angriffe auf eingesetzte Standardkomponenten im ICS-Netz	IT-Standardkomponenten (commercial off-the-shelf, COTS) wie Betriebssysteme, Application Server oder Datenbanken enthalten in der Regel Fehler und Schwachstellen, die von Angreifern ausgenutzt werden. Kommen diese Standardkomponenten auch im ICS-Netz zum Einsatz, so erhöht dies das Risiko eines erfolgreichen Angriffs auf die ICS-Systeme.
4	(D)DoS Angriffe	Durch (Distributed) Denial of Service Angriffe können Netzwerkverbindungen und benötigte Ressourcen beeinträchtigt und Systeme zum Absturz gebracht werden, z.B. um die Funktionsfähigkeit eines ICS zu stören.
5	Menschliches Fehlverhalten und Sabotage	Vorsätzliche Handlungen – ganz gleich ob durch interne oder externe Täter – sind eine massive Bedrohung für sämtliche Schutzziele. Daneben sind Fahrlässigkeit und menschliches Versagen eine große Bedrohung insbesondere bzgl. der Schutzziele Vertraulichkeit und Verfügbarkeit.
6	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Der Einsatz von Wechseldatenträgern und mobilen IT-Komponenten externer Mitarbeiter stellt stets eine große Gefahr bzgl. Malware-Infektionen dar. Dieser Aspekt kam z.B. bei Stuxnet zum Tragen.
7	Lesen und Schreiben von Nachrichten im ICS-Netz	Da die meisten Steuerungskomponenten derzeit über Klartextprotokolle und somit ungeschützt kommunizieren, ist das Mitlesen und Einspielen von Steuerbefehlen oftmals ohne größeren Aufwand möglich.
8	Unberechtigter Zugriff auf Ressourcen	Insbesondere Innentäter oder Folgeangriffe nach einer Penetration von außen haben leichtes Spiel, wenn Dienste und Komponenten im Prozessnetz keine bzw. unsichere Methoden zur Authentisierung und Autorisierung implementieren.
9	Angriffe auf Netzwerkkomponenten	Netzwerkkomponenten können durch Angreifer manipuliert werden, um z.B. Man-in-the-Middle Angriffe durchzuführen oder um Sniffing zu erleichtern.
10	Technisches Fehlverhalten und höhere Gewalt	Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind immer möglich – Risiko und Schadenspotential können hier lediglich minimiert werden.

Danksagung

Die Auflistung der Bedrohungen ist in enger Zusammenarbeit zwischen BSI und Vertretern der Wirtschaft entstanden. Besonderer Dank gilt: Michael Kasper (CASED), Ingo Jensen (E.ON Netz GmbH), Dr. Stephan Beirer (GAI NetConsult GmbH), Alfred Pohl (Hauni Maschinenbau AG), Jörn Maier (HiSolutions AG), Jonathan Pollet (Red Tiger Security), Siemens AG (Industry Sector), Steffen Zimmermann (VDMA), Adrian Hehl (VICCON Gmbh), Rolf Strehle (Voith GmbH), Dr. Peer Wichmann (WIBU-SYSTEMS AG).

Mit den BSI-Analysen veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) Statistiken und Berichte zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise richten Sie bitte an: cs-info@bsi.bund.de.

Bundesamt für Sicherheit in der Informationstechnik

BSI-A-CS 004 | Version 1.00 vom 12.04.2012

Hype oder Notwendigkeit?

EU Cybersecurity Strategie

- Jedes Mitgliedsland muss eine nationale NIS (Network and Information Security)-Behörde einrichten, bei der Sicherheitsvorfälle zentral gemeldet werde.
- Diese Behörden sollen auch als ICS-CERT fungieren.
- Kernbereiche (Energie, Transport, Banking, Finanz Transfer, Netz-Anbieter, Öffentliche Einrichtungen) müssen über ein geeignetes Risikomanagement die Bedrohungen aufzeigen und analysieren, sowie die identifizierten Informationen an die nationale NIS-Behörde weiterleiten.
- Diese nationalen Behörden sind erforderlich, um ein EU-weites Netzwerk zu bilden, welches mit der ENISA (European Network and Information Security Agency) zusammen an der Verbesserung der EU-weiten Cybersicherheit arbeitet.

Gesetzestext und weitere Infos : http://ec.europa.eu/digital-agenda/en/cybersecurity

Hype oder Notwendigkeit?

Control Systems Security Program (CSSP)

Industrial Control Systems Cyber Emergency Response Team

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to

- respond to and analyze control systems related incidents,
- conduct vulnerability and malware analysis,
- provide onsite support for incident response and forensic analysis,
- provide situational awareness in the form of actionable intelligence,
- coordinate the responsible disclosure of vulnerabilities/mitigations, and
- share and coordinate vulnerability information and threat analysis through information products and alerts.

Table of Contents

- ICS-CERT Monthly Monitor Newsletters
- Control Systems Advisories and Reports
- Other Resources
- Reporting
- Notable Critical Infrastructure News Feed

The ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts.

Learn more

ICS-CERT Monthly Monitor Newsletters

- ICS-CERT Newsletter, the "ICS-CERT Monthly Monitor," September 2012
- ICS-CERT Newsletter, the "ICS-CERT Monthly Monitor," August 2012
- ICS-CERT Newsletter, the "ICS-CERT Monthly Monitor," June-July 2012

Monthly Monitor Archive

Control Systems Advisories and Reports

Most Downloaded

ICS-CERT Advisory "ICS-CERT Incident Summary Report"
This Report summarizes ICS-CERT incident response activities from 2009 - 2011. (June 28, 2012)

ICS-CERT ALERT "ICS-ALERT-12-046-01 - Increasing Threat to Industrial Control Systems"
This ALERT informs critical infrastructure and key resource (CIKR) asset owners and operators of recent and ongoing activity concerning increased risk to CIKR assets, particularly Internet accessible control systems. (February 15, 2012)

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

Hype oder Notwendigkeit?

ProductCERT Security Advisories

Siemens ProductCERT publiziert Security Advisories zu Siemens-Produkten und -Lösungen.

2012

- SSA-938777 (Last Update 2012-10-08): Possible Remote Code Execution in SiPass Integrated
- SSA-279823 (Last Update 2012-10-08): Cross-Site Scripting Vulnerability in the SIMATIC S7-1200 Web Application
- SSA-240718 (Last Update 2012-09-13) Insecure storage of HTTPS CA certificate in S7-1200 V2.x
- SSA-864051 (Last Update 2012-09-10) Multiple Vulnerabilities in WinCC 7.0 SP3
- SSA-622607 (Last Update 2012-08-31) RuggedCom Private Key Vulnerabilities for HTTPS/SSL and SSH
- SSA-312568 (Last Update 2012-08-10): Security Vulnerability in COMOS
- SSA-617264 (Last Update 2012-07-30): Security Vulnerability in SIMATIC S7-400 V5 PN CPUs
- SSA-589272 (Last Update 2012-07-30): Security Vulnerability in SIMATIC S7-400 V6 PN CPUs
- SSA-283911 (Last Update 2012-07-30): Security Vulnerability in Synco OZW Devices
- SSA-110665 (Last Update 2012-07-23): Security Vulnerability in SIMATIC STEP7
- SSA-027884 (Last Update 2012-07-23): Security Vulnerability in SIMATIC WinCC
- SSA-826381 (Last Update 2012-06-14): Multiple Security Vulnerabilities in RuggedCom ROS-based Devices
- SSA-223158 (Last Update 2012-06-05): Multiple Security Vulnerabilities in WinCC 7.0 SP3
- SSA-268149 (Last Update 2012-04-05): Multiple Security Vulnerabilities in Siemens Scalance S
- SSA-130874 (Last Update 2012-04-05): Multiple Security Vulnerabilities in Siemens Scalance X Switches
- SSA-345442 (Last update 2012-01-26): Multiple Vulnerabilities in WinCC flexible and WinCC V11 (TIA Portal)
- SSA-850510 (Last update 2012-01-19): Siemens Tecnomatix FactoryLink Multiple ActiveX Vulnerabilities

Hype oder Notwendigkeit?

Sicherheitslücke in CODESYS V2.3 Laufzeitsystem

Kempten, Oktober 2012: Umgehung des Passwortschutzes für Zugriff auf CODESYS-Steuerungen möglich

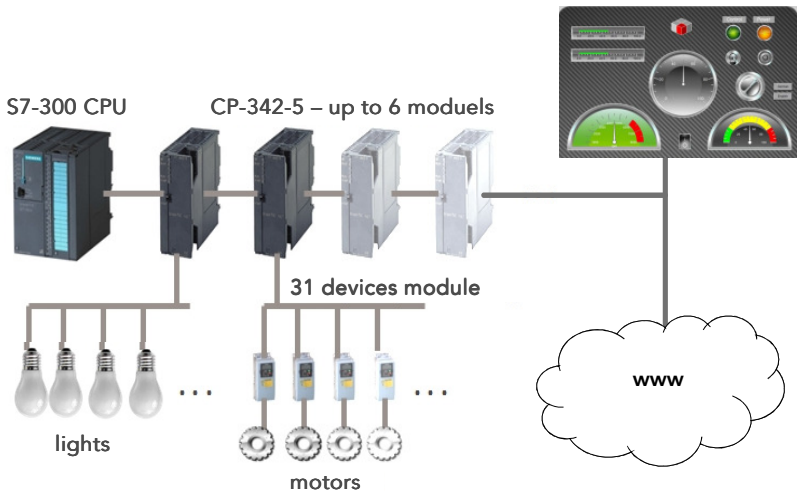
In zahlreichen Internetportalen wird derzeit auf eine Sicherheitslücke im CODESYS V2.3 Laufzeitsystem hingewiesen: Eine passwortgeschützte und öffentlich zugreifbare CODESYS Steuerung ist trotz Passwortschutz noch ansprechbar. So können, wie bei einer SPS ohne Passwort, mit Hilfe eines externen Tools weiterhin etwa Kommandos mit der Shell der Steuerung ausgeführt oder Applikationen geladen werden.

Natürlich nehmen wir diese Problematik sehr ernst. Im Download-Bereich des Kundenportals finden direkte OEM-Kunden eine entsprechende Fix-Version, die den aufgedeckten Fehler behebt.

Generell stellen wir in CODESYS keine Bordmittel zur Verfügung, die eine Steuerung vor einem ernsthaften Angriff aus dem Internet schützen sollen. Sollten wir dieses mit der vorhandenen Passwort-Funktion suggeriert haben, war das nicht beabsichtigt. Für die vollständige Absicherung eines SPS-Laufzeitsystems auf einer im Internet verfügbaren Steuerung ist der Einsatz von gängigen Sicherheitsmechanismen (Firewall, VPN-Zugang) zwingend erforderlich.

Zurück

24h Honeypot-Test



24 h Honeypot-Test

Ergebnisse

- 24 Angriffsversuche auf Anwendungsebene (XXS, API etc.)
- 13 nicht autorisierte Zugriffe auf Feldbusebene
- 4 direkte Eingriffe in den Steuerungsprozess

```
AWL   FUP   KOP   Netzwerk 1
HACKED AND FUCK OFF//
   0        U    E        1.1
   1        =    A        0.2
   2        SET M 100.7
   3        =    A        0.4
```

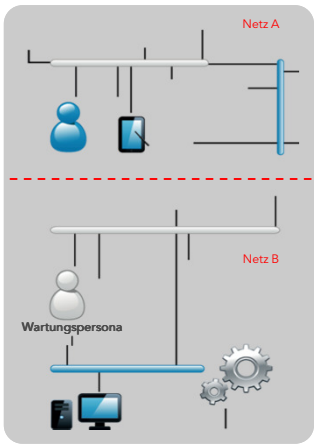
Situation und Entwicklung

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Ursprüngliche Anforderungen

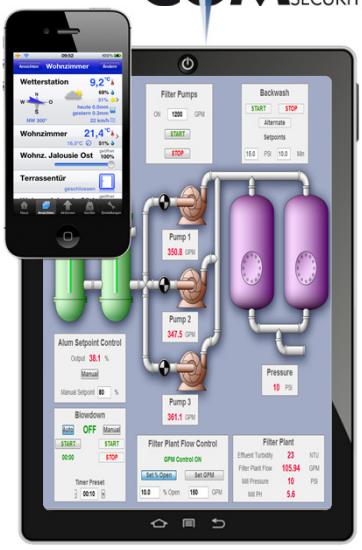
- Autarke Netzfragmente
- Komplexe proprietäre u. technologie-spezifische Protokolle
- Kopplung an überlagerte Systeme erfolgte in der Regel direkt
- Lokal begrenzte Störungen und Bedrohungen
- Fernwartung ausschließlich per Modem bei geringer Bandbreite



Situation und Entwicklung

Aktuelle Anforderungen

- Echtzeitfähigkeit
- Einheitliche Kommunikationsinfrastrukturen
- Standardprotokolle (TCP/IP, Web, Dateifreigaben)
- Durchgängige Kommunikation von der Managementebene bis in die Feldebene
- Verknüpfung von ERP, MES & Automation Systems
- Zentrale/s Steuerung und Reporting
- Onlineüberwachung und breitbandige Fernwartung

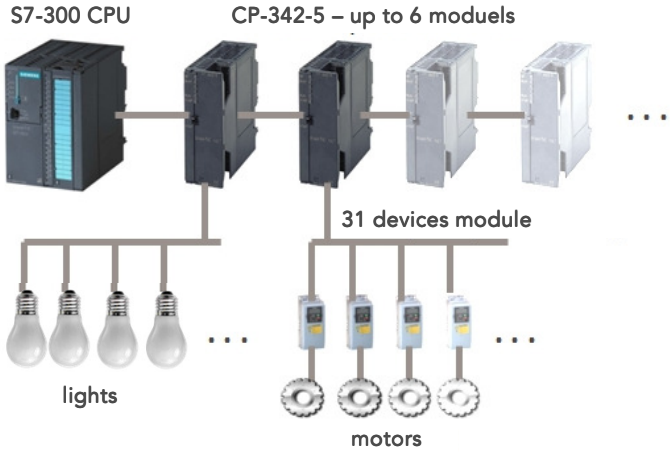


LiveDemo [Attack Industrial Control Systems]

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

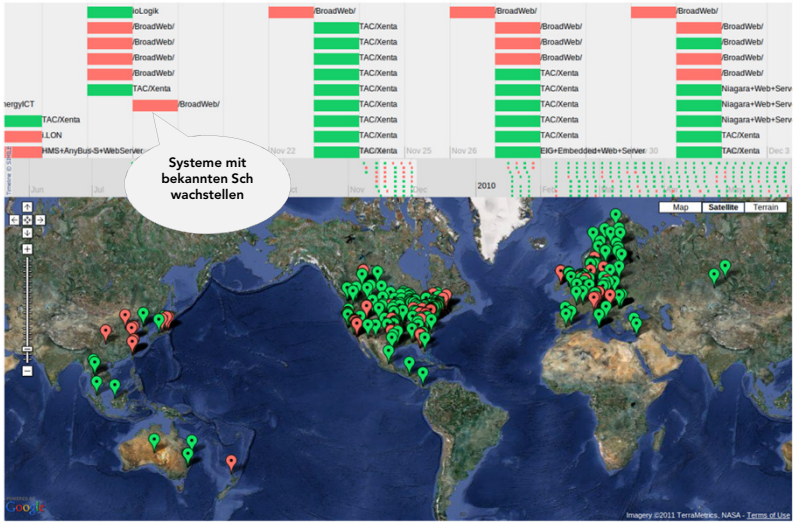
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Simulationsaufbau



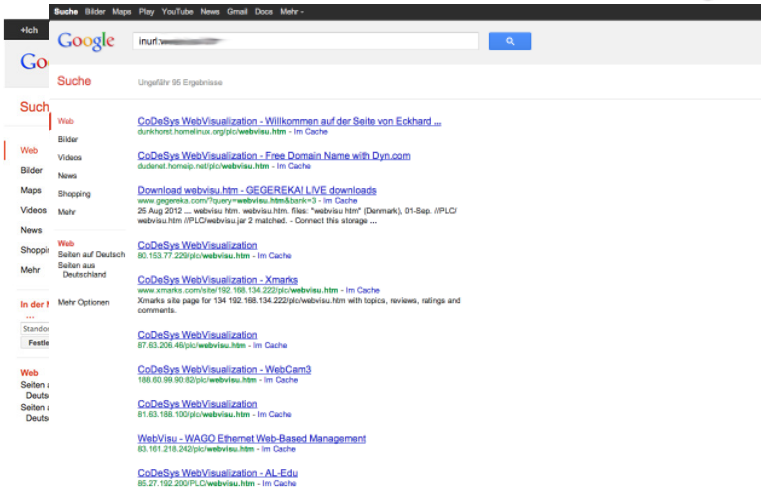
Gute Gründe für Industrial Security

Weltweit öffentlich zugängliche Systeme

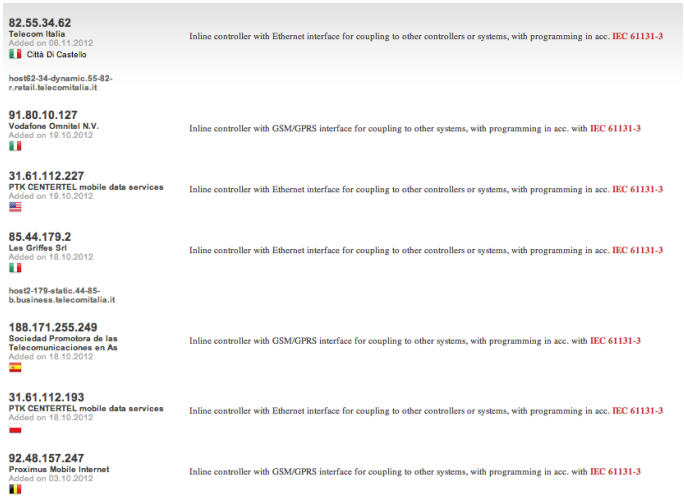


Quelle: Éireann P. Leverett - Quantitatively Assessing and Visualising Industrial System Attack Surfaces

Öffentlich zugängliche Systeme



Öffentlich zugängliche Systeme



Öffentlich zugängliche Systeme

```
Terminal — bash — 132×4
mdf-macbook:plcscan mdifilippo$ python icsscan.py
Scan start...
:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                  : 6ES7 151-8AB00-0AB0  v.0.2
  Basic Hardware          : 6ES7 151-8AB00-0AB0  v.0.2
  Basic Firmware          :                      v.2.7.1
  Unknown (129)           : Boot Loader           A
  Name of the PLC         :
  Name of the module      : IM151-8 PN/DP CPU
  Plant identification    :
  Copyright               : Original Siemens Equipment
  Serial number of module : S C-X7UR74342009
  Module type name        : IM151-8 PN/DP CPU
Scan complete
mdf-macbook:plcscan mdifilippo$
```


Beispiele

Gute Gründe für Industrial Security

Aber wie?

Netzwerk

- Segmentierung des Produktionsnetzes
- Fernwartungskonzept
- Perimeter Security Gateway (Firewalls, IDS/IPS)
- Security Information and Event Management (SIEM)

Schnittstelle

- Geräte- und Daten-Management (Device Control)

System

- Systemsicherheit durch Härtung durch Whitelisting-Technologie (nicht scan-basierende Technologie)
  - API Aufrufe von Prozessen, die sich nicht auf der Whitelist befinden werden unterbunden
  - Schutz vor Buffer Overflows

The Real World Needs Real Solutions Today

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Gute Gründe für Industrial Security

Wissen ist Macht...

- Wir wollen niemanden zur einer Straftat anstiften!
- Alle gezeigten Informationen dienen ausschließlich dazu sie zu sensibilisieren! Denn nur wer um die Gefahren weiss, kann sich davor schützen.
- Wenn sie Fragen im Bereich IT-Sicherheit haben, sprechen sie uns an.

Offene Diskussion

Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit!

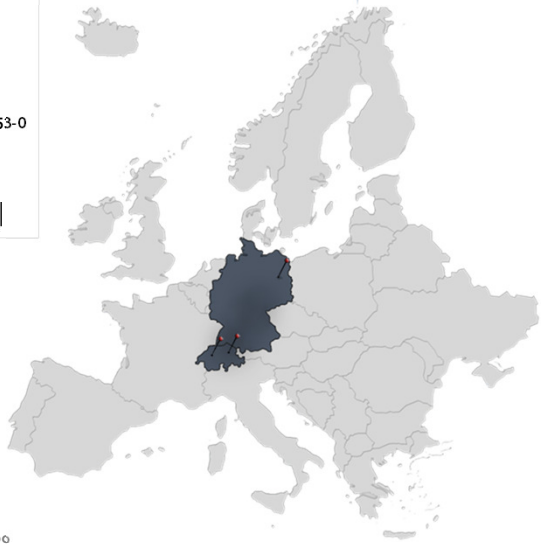
Kontakt

Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin
Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

Secure File Exchange: www.filebox-solution.com



Slideconcept: Marco Di Filippo
Review: Laura-Louise Di Filippo