Bundesamt
für Sicherheit in der
Informationstechnik

Was passiert mit Industrie 4.0, wenn man nicht an die Security denkt?

Jens Wiesner, Leiter Referat CK23: Cyber-Sicherheit in Industrieanlagen
Forum Industrie 4.0 meets the Industrial Internet
Hannovermesse 2018

Motivation

… und alles hängt von IT ab!

Schnell ändernde IT-Landschaften

Massive Vernetzung:

- Cloud
- IoT
- Industrie 4.0
- Digitaler Zwilling

Neue Bedrohungen durch zunehmende Digitalisierung

Theorie:
Defence in Depth

Traditionelle Herangehensweise an IT-Sicherheit:

- Hohe Mauern
- Wächter
- Burgtore

ISO/IEC62443: Zones and Conduits

VDMA
Leitfaden Security für den Maschinen- und Anlagenbau
Der Weg durch die IEC 62443

Bundesamt
für Sicherheit in der
Informationstechnik

Wirklichkeit:

Viele Gelegenheiten

Bundesamt
für Sicherheit in der
Informationstechnik

Motiv

Vorfälle Februar 2018: Malware in Industrieanlagen

heise online > News > 02/2018 > Bitcoin-Mining mit dem Supercomputer: Ingenieure von...

Bitcoin-Mining mit dem Supercomputer: Ingenieure von Atomforschungszentrum festgenommen

10.02.2018 15:23 Uhr – Jo Bager vorlesen

Mitarbeiter des russischen Forschungszentrums für Experimentalphysik wollten offenbar im Nebenjob Bitcoins minen - auf Hardware des Instituts.

Mitarbeiter des russischen Forschungszentrums für Experimentalphysik (RFNC-VNIIEF) sind beim Versuch festgenommen worden, Rechnerkapazität der Einrichtung für das Mining von Bitcoins zu missbrauchen. Das berichtet die Nachrichtenagentur Interfax.

https://heise.de/-3965055

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS Subscribe (Free) | CISO Forum 2018 | I

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Secur

Home › SCADA / ICS

Cryptocurrency Mining Malware Hits Monitoring Systems at European Water Utility

By Mike Lennon on February 08, 2018

Tweet Empfehlen 31 RSS

Malware Chewed Up CPU of HMI at Wastewater Facility

Cryptocurrency mining malware worked its way onto four servers connected to an operational technology (OT) network at a wastewater facility in Europe, industrial cybersecurity firm Radiflow told *SecurityWeek* Wednesday.

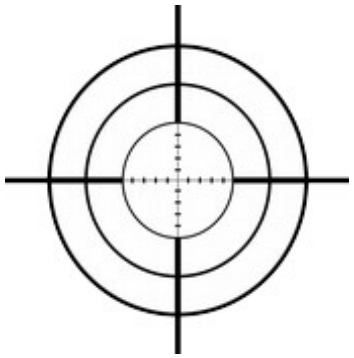
Radiflow says the incident is the first documented cryptocurrency malware attack to hit an OT network of a critical infrastructure operator.

The servers were running Windows XP and CIMPLICITY SCADA software from GE Digital.

"In this case the [infected] server was a Human Machine Interface (HMI)," Yehonatan Kfir, CTO at Radiflow, told *SecurityWeek*. "The main problem," Kfir continued "is that this kind of malware in an OT network slows down the HMIs. Those servers are responsible for monitoring physical processes."

https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility

Gezielte und ungezielte Angriffe



Ungezielte Angriffe
- Vergleichsweise einfach
- Ärgerlich
  Eigentlich sollten Planungen und Anleitungen existieren, damit umzugehen

Gezielte Angriffe
- Aufwendig
- Erpressung
- Beeinträchtigung der Produktion
- Verringerung der Qualität
- Diebstahl geistigen Eigentums

Schon mal gehackt worden?
Nein? - Wieso sind Sie so sicher?

Professionelle Strukturen „der Bösen“

Büroarbeitszeiten
Arbeitsteilung
Hacking as a Service
Call-Center Support

Alternatives Motiv

Vorfall Sommer 2017: Trition/TRISIS
Angriff auf Safety Systeme

heise online > News > 03/2018 > Saudi-Arabien: Cyberangriff hätte Explosion auslösen können –...

Saudi-Arabien: Cyberangriff hätte Explosion auslösen können – Ermittler sind alarmiert

15.03.2018 15:42 Uhr – Martin Holland vorlesen

Ölraffinerie (Bild: anekoho/Shutterstock.com)

Vor wenigen Monaten hat es in Saudi-Arabien angeblich einen Hackerangriff gegeben, der Menschen ihr Leben hätte kosten können. Dass es die angepeilte Explosion in einem Kraftwerk nicht gegeben hat, war einem Bericht zufolge nur glückliche Fügung.

https://heise.de/-3996010

Bekannt werden: Dezember 2017

Opfer:
Chemieanlage im Mittleren Osten

Vorgehen:
Manipulation der Firmware im Safety Controller
Keine Auslösung im Anforderungsfall

Ziel:
Zerstörung der Anlage
Möglicher Verlust von Menschenleben

Vorfall März 2016: Dragonfly 2.0(?)

Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-074A) More Alerts

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Print | Tweet | Send | Share

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders

https://www.us-cert.gov/ncas/alerts/TA18-074A

Bekannt werden: März 2018

Opfer:
Kritische Infrastrukturen
(Energie, Wasser, Luftfahrt, kritische Produktion)

Vorgehen:
Verschiedenes, mehrstufiges Eindringen

Ziel:
Spionage
Informationen über Kritische Infrastrukturen sammeln

Angriffe auf industrielle Steuerungssysteme sind immer noch zu einfach!

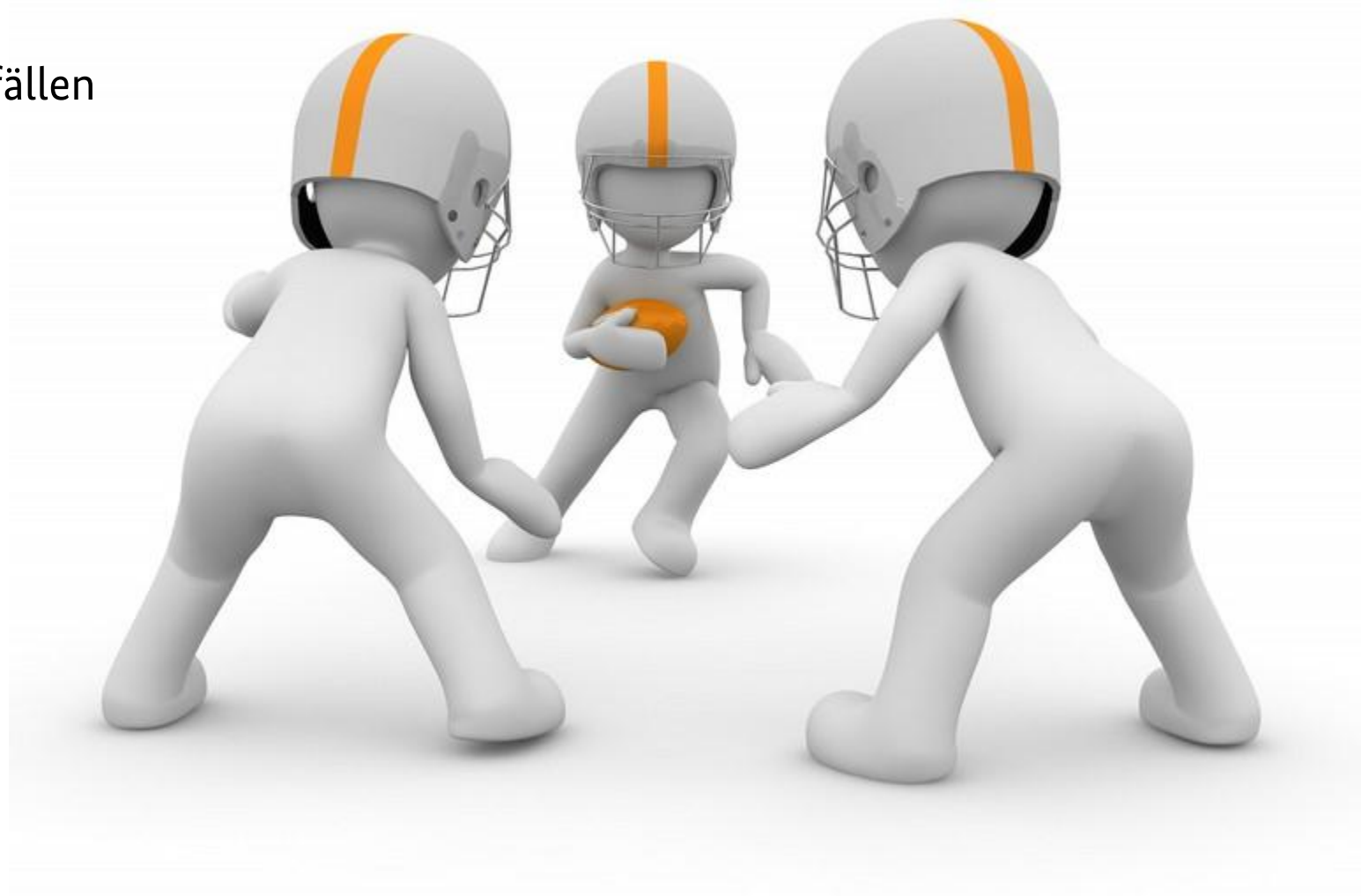
Zusammenarbeit aller Beteiligten notwendig

Betreiber
Erhöhte Sensibilität & Meldung von Vorfällen
Einfordern von IT-Sicherheit

Hersteller
Verbessern IT-Sicherheit der Produkte

Integratoren
Angebot von mehr IT-Sicherheit

BSI
Informationsaustausch
Geräte(Basis)zertifizierung
Mehr qualifizierte Dienstleister
Mehr Unterstützung



Rolle des BSI

„Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“

Gründung 1991 per Gesetz
Mitarbeiter: 768 (Stand: Dezember 2017)
Stellenzuwachs im Jahr 2017: 180
Standort: Bonn

BSI Grundschutz

IND.1: Betriebs- und Steuerungstechnik

1 Beschreibung

1.1 Einleitung

IND.2.1: Allgemeine ICS-Komponente

1 Beschreibung

1.1 Einleitung

Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschin
ist damit Bestandteil eines industriellen Steuerungssystems (engl. Industrial
einer Betriebstechnik (engl. Operational Technology, OT). Solche Komponent
Steuerungen (SPS, engl. Programmable Logic Controller, PLC), Sensoren, Akt
eines ICS sein.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen
dingungen (Klima, Staub, Vibration, Korrosion) wurden ICS-Komponenten s
her Zuverlässigkeit und langer Lebensdauer konstruiert.

ICS-Komponenten werden normalerweise über Spezialsoftware des jeweili
grammiert. Das wird entweder über sogenannte Programmiergeräte (z. B.
Linux) oder über eine Engineering-Station durchgeführt, die die Anwendung
mierbaren Steuerungen lädt.

Die Rolle des Beauftragten für Informationssicherheit für den Bereich der
nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeic
heitsbeauftragter (ICS-ISB) ist auch Industrial Security Officer.

1.2 Zielsetzung

Ziel des Bausteins ist die Absicherung aller Arten von ICS-Komponenten, ur
satzzweck und -ort. Er kann für ein einzelnes Gerät oder ein aus mehreren K
Gerät verwendet werden.

1.3 Abgrenzung

Die Anforderungen sind für eine generische Komponente erarbeitet. Für spe
ter IND.2 *ICS-Komponenten* zusätzliche Bausteine verfügbar, in denen Anfo
die generischen Anforderungen dieses Bausteins hinausgehen und eventuell

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherun
sen die Anforderungen des Bausteins IND.1 *Betriebs- und Steuerungstechni*

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein
von besonderer Bedeutung:

2.1 Beeinträchtigung durch schädliche Umgebungseinflüsse

ICS-Komponenten in industriellen Umgebungen sind häufig besonderen Bedi
Betrieb beeinträchtigen können. Beispiele hierfür sind extreme Wärme, Kält
auch ätzend oder korrodierend wirkende Atmosphären. Häufig treten auc
Durch solche schädlichen Umgebungseinflüsse können ICS-Komponenten s
fallen.

IND.2.2: Speicherprogrammierbare Steuerung (SPS)

1 Beschreibung

1.1 Einleitung

Eine speicherprogrammierbare Steuerung (SPS, engl. Programmable Logic Controller, PLC)
nente. Sie übernimmt Steuerungs- und Regelaufgaben in der Betriebstechnik (engl. Operatio
Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind heute fließend: So
Fernwirkgerät (engl. Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen ode
Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs
ist die SPS immer noch das klassische Automatisierungsgerät, sodass in diesem Baustein die
verwendet werden.

Eine SPS verfügt über digitale Ein- und Ausgänge, ein Echtzeitbetriebssystem (Firmware) sowi
len für Ethernet oder Feldbusse. Die Verbindung zu Sensoren und Aktoren erfolgt über die ana
Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit Prozessleitsystemen f
Ethernet-Schnittstelle und IP-basierte Netze statt.

Die möglichen Realisierungen sind vielfältig: Eine Speicherprogrammierbare Steuerung kann al
gerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden.
treffen sind modulare Speicherprogrammierbare Steuerungen , die aus verschiedenen funktio
zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualisie
Protokollieren durch die SPS realisiert.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extre
dingungen (Klima, Staub, Vibration, Korrosion) wurden ICS-Komponenten schon immer als ro
her Zuverlässigkeit und langer Lebensdauer konstruiert.

Eine SPS wird normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw
wird entweder über sogenannte Programmiergeräte (z. B. als Anwendung unter Windows o
eine Engineering-Station durchgeführt, die die Daten über ein Netz verteilt.

1.2 Zielsetzung

Ziel des Bausteins ist es, alle Arten von speicherprogrammierbaren Steuerungen abzusichern,
steller, Bauart, Einsatzzweck und -ort. Er kann für eine einzelne SPS oder eine zusammenhän
setzte Baugruppe angewendet werden.

1.3 Abgrenzung

Der vorliegende Systembaustein ist anzuwenden, um alle Arten von speicherprogrammierbare
eine SPS und Geräte, die gleiche oder ähnliche Funktionen integrieren) abzusichern. Er e
IND.2.1 *Allgemeine ICS-Komponente*. Bei der Anwendung ist dieser daher auch zu berücksic

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komp
sen die Anforderungen des Bausteins IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werd
Bereich funktionale Sicherheit (Safety) nicht behandelt.

IND.2.3: Sensoren und Aktoren

1 Beschreibung

1.1 Einleitung

Sensoren sind als elektronische Komponente mit Mikroprozessor und Software ausgeführte Messumformer, die eine physikalische Größe in einen elektrischen Ausgabewert wandeln. Dieser wird als normiertes Einheitssignal (häufig 4 bis 20 mA, 0 bis 10 V) an einer seriellen Schnittstelle oder als digitale Informationen, die über einen Feldbus oder Ethernet-Protokolle übertragen werden, bereitgestellt. Messumformer stellen neben den Messwerten

IND.2.4: Maschine

1 Beschreibung

1.1 Einleitung

Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Produkte auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System unter Nutzung eines Programms gesteuert, das die entsprechenden Arbeitsanweisungen und -schritte vorgibt. Solche Maschinen werden auch als Automaten bezeichnet.

Meistens werden Maschinen von Maschinenbauern konstruiert und mit bestimmten vordefinierten Funktionen ausgestattet. Der Betreiber der Maschine kann allerdings noch die Parameter bestimmen, nach denen sie arbeiten soll. So lassen sich beispielsweise Formen, die gefräst werden sollen, oder Kalibrierungen für bestimmte Materialien einstellen. Damit der Betreiber die Parameter verändern kann, verfügen Maschinen über verschiedene Schnittstellen, z. B. für Wechseldatenträger, spezialisierte Programmiergeräte oder Netzzugriffe.

Häufig werden von Maschinenbauern auch Fernwartungsdienstleistungen angeboten, um frühzeitigen Verschleiß zu erkennen oder in Problemsituationen schnell reagieren zu können.

1.2 Zielsetzung

Der Baustein beschreibt, wie elektronisch gesteuerte halb- oder vollautomatische Maschinen (z. B. CNC-Maschinen) unabhängig von Hersteller, Bauart, speziellem Einsatzzweck und -ort abgesichert werden können.

1.3 Abgrenzung

Der vorliegende Baustein ergänzt den übergeordneten Baustein IND.2.1 *Allgemeine ICS-Komponente* und setzt voraus, dass dieser umgesetzt wurde. Darüber hinaus werden nur Anforderungen für Maschinen definiert, auf deren interne Strukturen eine Institution nicht zugreifen kann.

Auch werden keine Sicherheitsanforderungen für Betriebs- und Steuerungstechnik beschrieben. Dafür muss der Baustein IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden. Ebenso wird der Bereich der funktionalen Sicherheit (Safety) nicht behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein IND.2.4 *Maschine* von besonderer Bedeutung:

2.1 Ausfall oder Störung durch ungenügende Wartung

Wenn Maschinen nicht regelmäßig gewartet werden, funktionieren sie früher nicht mehr korrekt oder fallen ganz aus. Durch Fehlfunktionen können z. B. Mitarbeiter gefährdet oder die Produktion kann erheblich beeinträchtigt werden.

2.2 Gezielte Manipulationen

Sind die Schnittstellen einer Maschine ungenügend geschützt, können Angreifer die Parameter der Maschine manipulieren, z. B. über lokale Programmiergeräte oder Netzdienste. Dadurch können Werkstücke beschädigt werden oder ganze Produktreihen fehlerhaft sein. Die Angreifer können aber auch die Maschine selbst beschädigen, sodass auch dadurch ein wirtschaftlicher Verlust entsteht.

Bundesamt
für Sicherheit in der
Informationstechnik

Veröffentlichungen

https://www.bsi.bund.de/ICS

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Hr. Jens Wiesner
Referatsleiter
jens.wiesner@bsi.bund.de
Tel. +49 (0) 22899 9582-6022
Fax +49 (0) 22899 109582-6022

Bundesamt für Sicherheit in der Informationstechnik
Referat CK 23 Cyber-Sicherheit in Industrieanlagen
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de/ICS