



IT-Sicherheit in der Industrial IT

IT Tag Saarland 2011
Daniel Buhmann



Wer ist KORAMIS?

- Die KORAMIS GmbH ist heute einer der führenden Anbieter von Industrial IT Security Lösungen im deutschsprachigen Raum
- **Seit** ihrer Gründung in **1985** bietet KORAMIS **Dienstleistungen und Lösungen** rund um die **Prozess-** und **Netzleittechnik**.
- Die **KORAMIS GmbH** steht für einen Unternehmensverbund mit 80 MA verteilt auf 7 regionale Niederlassungen in Deutschland und Schweiz



Wandel industrieller Systeme ...



...hin zu modernen IT-Infrastrukturen



- Zunehmende **Dezentralisierung** der Automatisierungsfunktionen

- **Vielfältiger** Einsatz von Informationstechnologie

- PC-/Windows-basierte Automatisierungslösungen



- Einsatz von Ethernet bis ins Feld

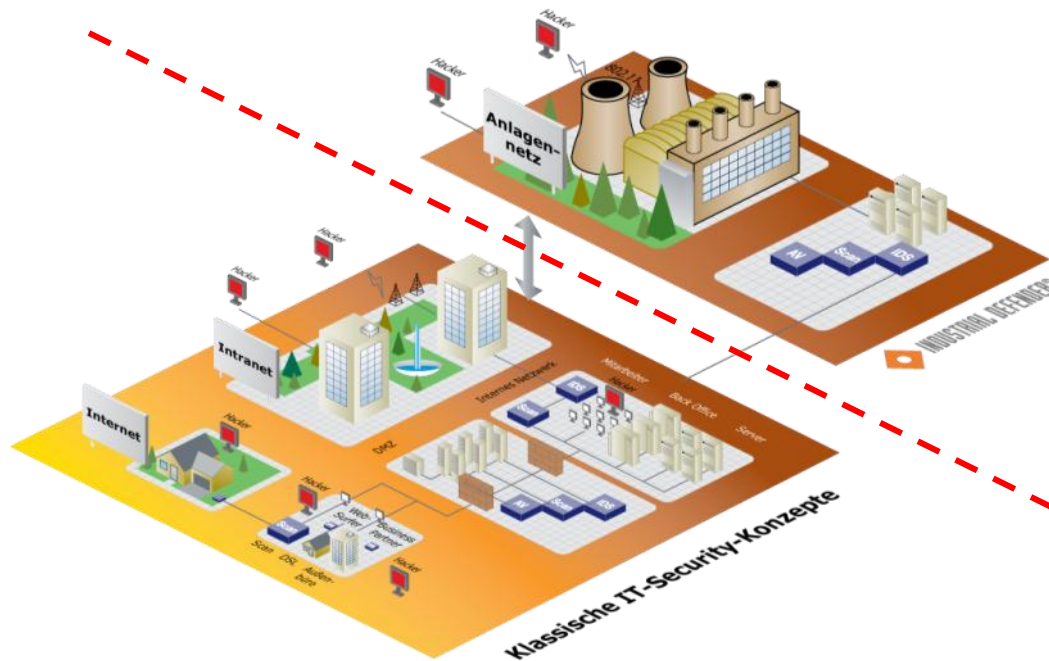
- Einsatz internetbasierender Dienste (z.B. Fernwartung)

- Techniken wie z.B. OPC, XML oder TCP/IP

- Vertikale Integration von **Geschäfts-** und von **technischen Prozessen**



Was unterscheidet Industrial IT gegenüber Business IT ?



Industrial-IT:

1. Verfügbarkeit
2. Integrität
3. Vertraulichkeit

Business-IT:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit

- klare Trennung der Zuständigkeiten
- wenig Kommunikation

Industrial Security wird immer wichtiger!

Handelsblatt

CYBER-ANGRIFF 01.07.2011, 18:35 Uhr

Bayer von Computer-Hackern angegriffen

...Die Störungen dauern dem Unternehmens-Sprecher zufolge seit einer Woche an...

"Immense Schäden"

Friedrich warnt vor Cyberattacken



Vor der Eröffnung des Cyber-Abwehrzentrums in Bonn hat Innenminister Friedrich vor zunehmenden Hackerattacken auf die Strom- und Wasserversorgung gewarnt. Sie könnten immense Schäden anrichten.



"Die Gefahr von Cyberangriffen wächst ständig": Innenminister Hans-Peter Friedrich
© Christophe Karaba/DPA

Bundesinnenminister Hans-Peter Friedrich (CSU) befürchtet eine Zunahme von **Cyberangriffen** auf die Strom- und Wasserversorgung in Deutschland. "Kritische Infrastrukturen wie etwa die Strom- und Wasserversorgung kommen heutzutage ohne hochmoderne IT-Systeme nicht mehr aus", sagte er der

"Frankfurter Rundschau". "Die Gefahr von Cyberangriffen auf diese Systeme wächst ständig." Derartige Attacken könnten nach Aussage des Ministers immense Schäden anrichten, die erhebliche Teile der Bevölkerung direkt betreffen würden. "Um dies zu verhindern, hat die Bundesregierung eine Cyber-Sicherheitsstrategie entwickelt."

RP ONLINE

4.12.2010 14:46:50 Uhr

Wirtschaft schlecht gegen Kriminalität geschützt

Der frühere BND Präsident August Hanning warnt: „ Im Bereich der Wirtschaft, speziell bei kleinen und mittleren Unternehmen, haben wir noch erhebliche Defizite. Viele Manager seien sich der Gefahr digitaler Attacken noch immer nicht bewusst.“

Angriffe auf leittechnische Systeme ...



ZEITUNG ONLINE | INTERNET

STARTSEITE POLITIK WIRTSCHAFT MEINUNG GESELLSCHAFT KULTUR WISSEN DIGIT

Internet | Datenschutz | Mobil | Games

HACKER

Angriff am Fließband

Ein neuer Trojaner gefährdet die Steuercomputer von Industrieanlagen und Kraftwerken

© Thomas Starke/Getty Images



Auch die Steuerungssoftware von Atomkraftwerken, hier Grohnde, könnte Ziel von Trojaner-Angriffen werden

Wer mehrere Hunderttausend Euro für die Entwicklung eines Computerprogramms ausgibt, hat in der Regel Großes vor. Selbst Konzerne investieren nur selten so viel Geld, um neue Software schreiben zu lassen. Dass Unbekannte aber eine solche Summe ausgegeben haben, um eine

- Vielfältiger Virenbefall
- Stuxnet Trojaner

- Stuxnet auf Systemen von 40% der Betreiber kritischer Infrastrukturen entdeckt
- Nur wenige reagierten mit Risikoanalysen oder sonstigen Security-Maßnahmen
- 2010 wurden 6.253 Software-Schwachstellen gemeldet
- 3 Milliarden Schadsoftware-Attacken durch 286 Millionen Varianten von Schadsoftware wurden 2010 bekannt - 93% mehr als 2009
- Stuxnet nutzte 14 Zero-Day Schwachstellen - alleine 4 für Windows Zero-Days
- Der Fokus der Hacker wandert verstärkt in Richtung Industrial IT – mehrere Schwachstellen bereits entdeckt

- Plötzlicher Anlagenstillstand
- Spionage
- Imageverlust



An der **Bedrohung** können Sie nichts ändern.



Schwachstellen können Sie vermeiden!

Unternehmen:

Produzent von Halbfertigwaren mit über 2.000 MA

Problemstellung:

Virusbefall im Bereich der Industrial IT wurde von den vorhandenen Systemen nicht erkannt und verhindert – der Produktionsstillstand war die Folge.

KORAMIS Lösung:

Nach Durchführung einer Risikoanalyse wurden Maßnahmen (technisch & organisatorisch inkl. Personalschulungen) eingeleitet. Die Implementierung erfolgte im laufenden Betrieb ohne Einschränkung der Systemverfügbarkeit.

Ergebnis:

Die umgesetzten Maßnahmen führten dazu, dass Schadsoftware zukünftig rechtzeitig erkannt und deren Ausführung verhindert wird. Prozesse wurden neu definiert und Know-how im Unternehmen aufgebaut.

Unternehmen:

Stadtwerke mit 880 MA

Problemstellung:

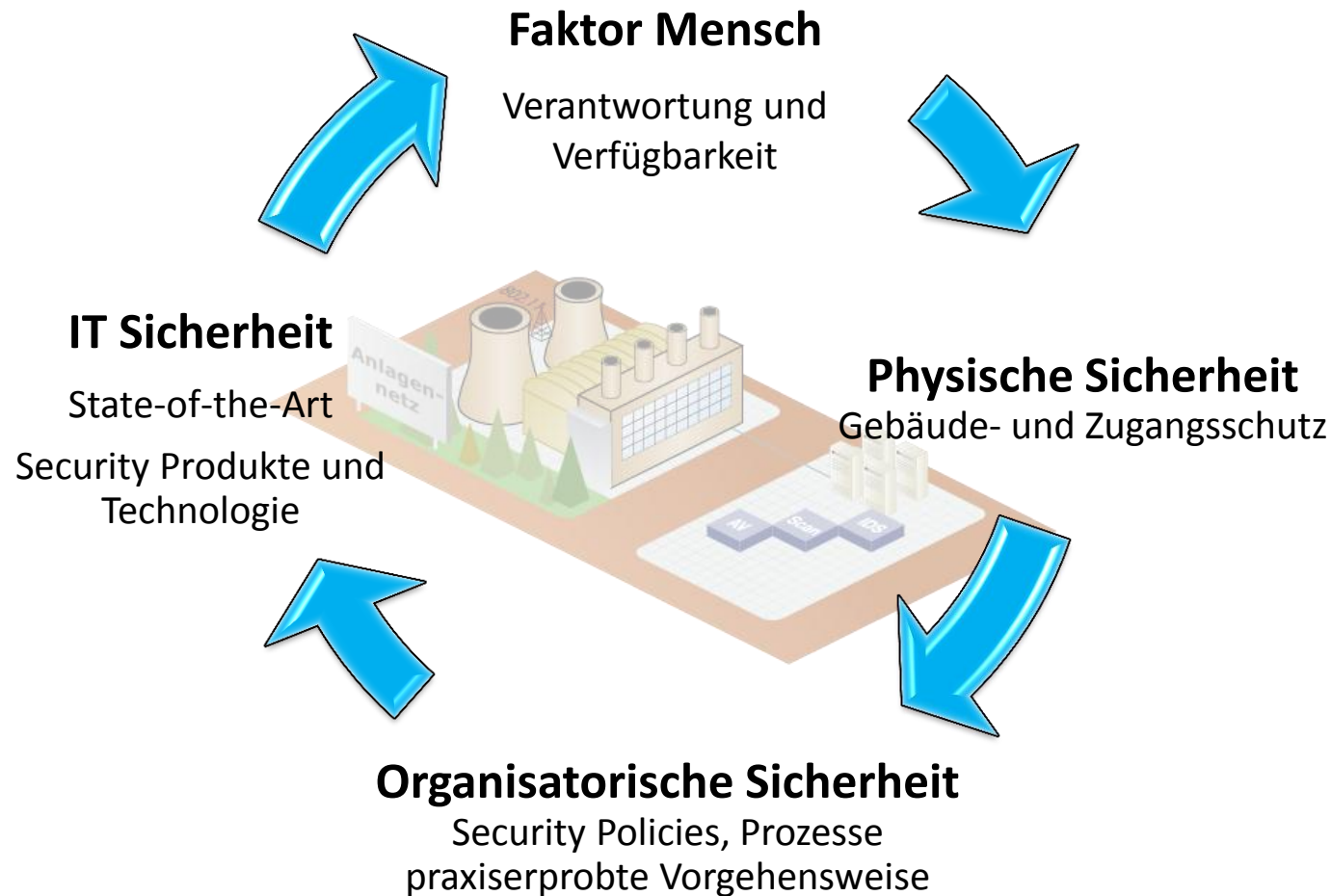
Systemstörung im Bereich einer Erzeugungsanlage hervorgerufen durch externe Manipulation.

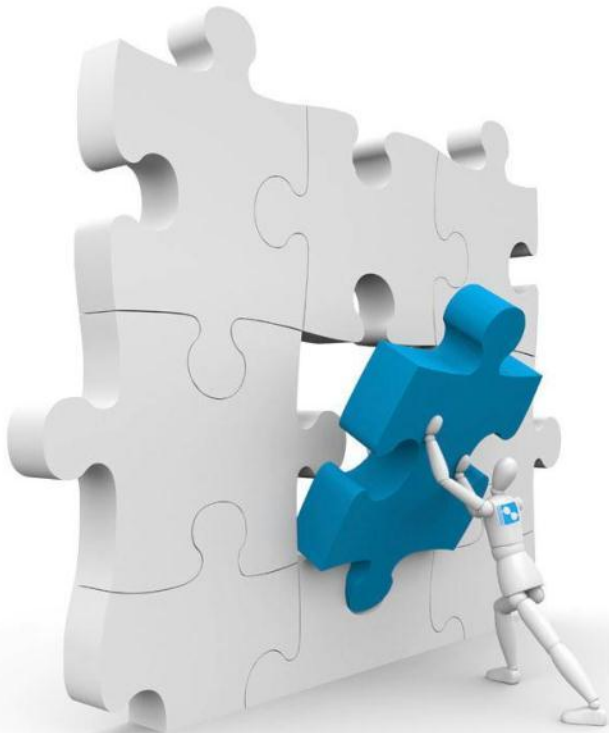
KORAMIS Lösung:

Definition und Einführung eines Perimeterschutz-Konzeptes. In der Folge wurden weitere Schwachstellen im Bereich der Industrial IT erkannt und eliminiert.

Ergebnis:

Aufdeckung aller Schwachstellen, Verhinderung externer Angriffe durch Schutzmaßnahmen und Einführung neuer Monitoring-Tools.





- Identifikation von vorhandenen Schwachstellen
- Kontinuierliche Sicherheitsüberwachungen in Echtzeit
- Eliminierung von externen und internen System-Manipulationen
- Verhinderung von unbefugtem Ausführen von Programmen
- Definition und Einhaltung spezifischer Security Policies
- Aufbau von Security Know-how und Prozesswissen im Unternehmen
- Minimierung von Ausfallzeiten und Sicherstellung einer gleichbleibenden Produktivität



Individuelle
Risikoanalyse

Definition von
Security-Strategien



Einführung von
Security- Strategien



Compliance (inkl.
Auditierungs-
prozesse)





- **Individuell**
Die Einführung von KORAMIS Lösungen erfolgt ausschließlich vor dem Hintergrund Unternehmens-individueller Anforderungen und Prozesse.
- **Flexibel**
KORAMIS Lösungen sind modular aufgebaut. Die KORAMIS Bausteine (Risikoanalyse, Einführung, Auditierung) können auch unabhängig voneinander implementiert werden.
- **Einfach**
KORAMIS Lösungen stellen ganzheitliche Systeme dar, die von einer Management-Konsole aus einfach bedient und analysiert werden können.

- **Unterschätzen Sie das Thema Industrial IT Security nicht!**
- **Bedrohungspotential entsteht dann ...**





Unternehmenssitz

Ensheimer Strasse 37
66386 St. Ingbert
Tel.: +49 (0)6894 / 9630780
info@koramis.de
www.koramis.de

Automation & IT-Security

Neumühler Weg 32.1
66130 Saarbrücken
Tel.: +49 (0)681 / 968 1910
info-sb@koramis.de
www.koramis.de

