



Bundesamt  
für Sicherheit in der  
Informationstechnik

# Fernwartung, was kann da schon schiefgehen?

Erfahrungsberichte aus dem BSI

# 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: ca 750 (Stand: Anfang 2018)  
Stellenzuwachs im Jahr 2017: **180**  
Standort: Bonn

# Target Black Friday Hack

Wann: 2013  
Wo: USA  
Ausmaß: 10 Mio. \$ Schadensersatz  
Dauer: ca. 14 Tage

Ursache: Nicht separierte  
Netzwerksegmente  
Ziel: Informationsdiebstahl

- Eindringen über Wartungszugang des Druckers
- Abgriff von bis zu 40 Mio. Kreditkarten und 70 Mio. weitere Daten
- Datenabfluss während Weihnachtszeit (27.11-15.12)
- Rücktritt des CEO und weiterer Verantwortlicher



# Dragonfly Kampagne/ Havex

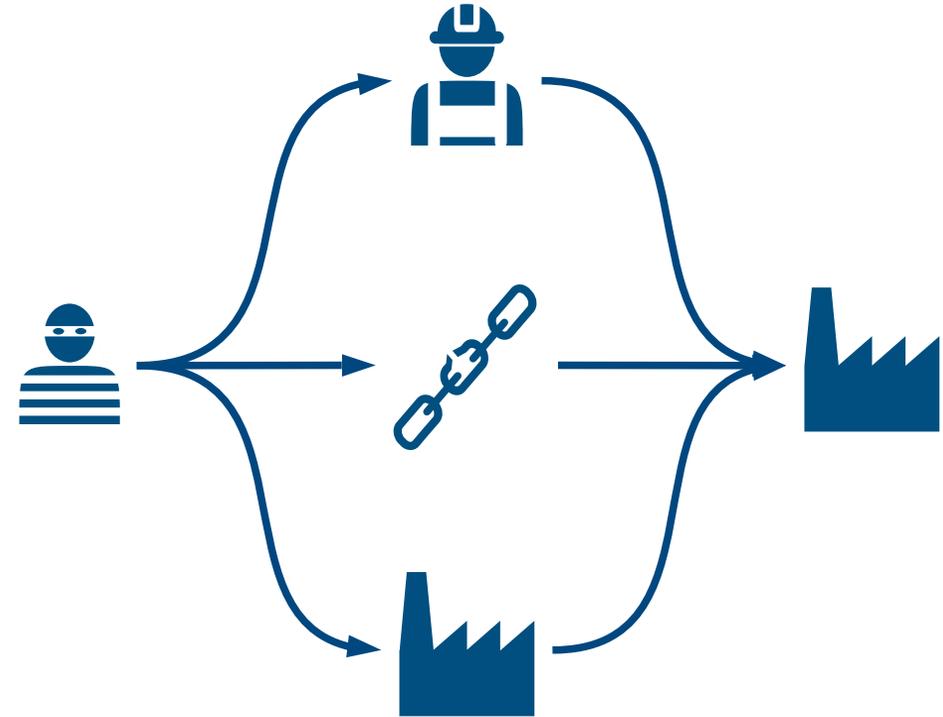
Wann: 2011-2014  
Wo: Europa, Nordamerika  
Ausmaß: lokal  
Dauer: mehrere Jahre

Ursache: Spear-Phishing,  
Watering Hole Attacken,  
Kompromittierung  
von Herstellerseiten  
Ziel: Spionage

- Bei der Dragonfly Kampagne wurden verschiedene Methoden benutzt um den Remote Access Trojaner (RAT) zu verbreiten:
  - Spear-Phishing-Mails, die die Malware enthielten
  - Watering Hole Attacken, die Besucher auf Webseiten mit Exploit Kits weitergeleitet haben
  - Infizierung von legitimer Software von drei verschiedenen ICS-Komponenten Herstellern von Fernwartungslösungen aus D, CH, BE

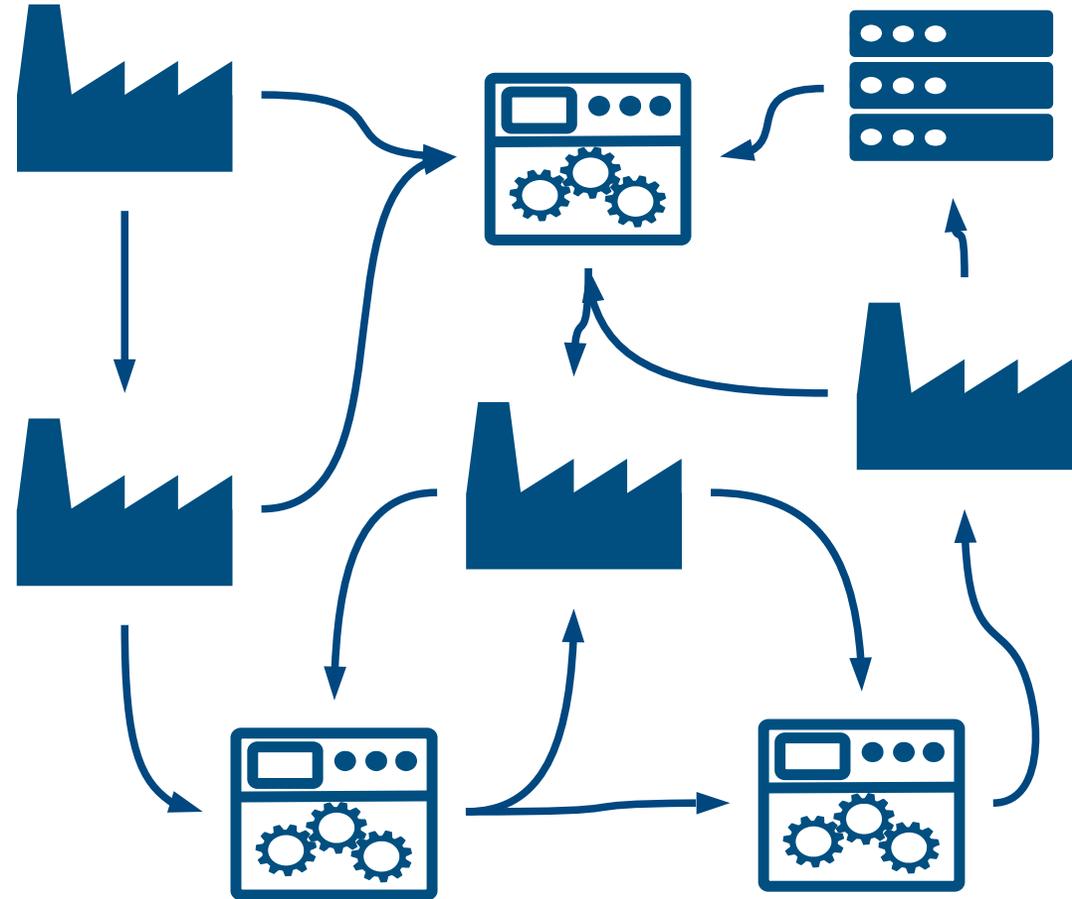
# Angriffswege auf Unternehmen

- Mitarbeiter
  - Phishing
  - Allgemein Social-Engineering
  - Sorglosigkeit
- Systeme
  - unzureichend geschützte Systeme
  - direkte Verbindungen zum Internet
  - Fernwartungsmöglichkeiten
  - Fehlkonfigurationen
- Wertschöpfungsnetzwerk
  - bei zu hohem Schutz erfolgt der Einstieg über verbundene Unternehmen mit niedrigerem Schutz
  - Water-Hole-Attacken

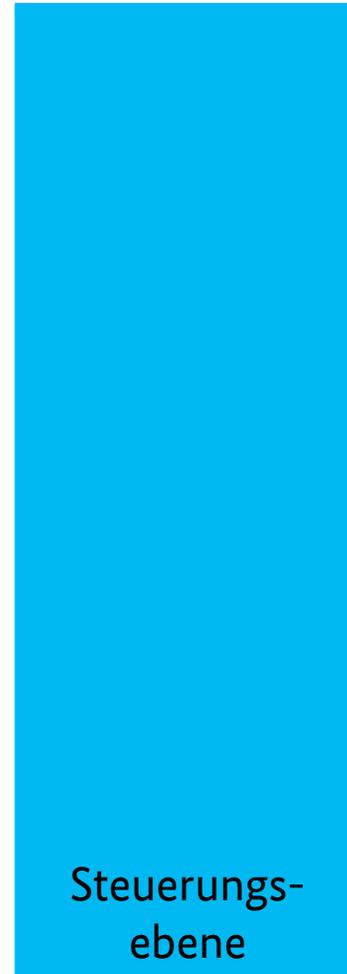
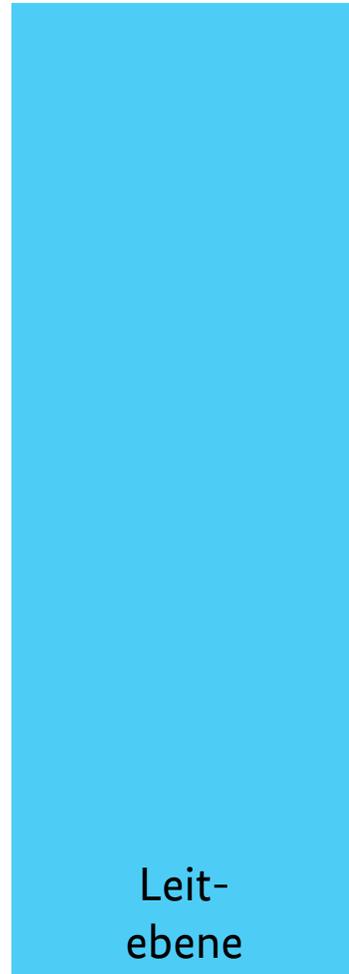
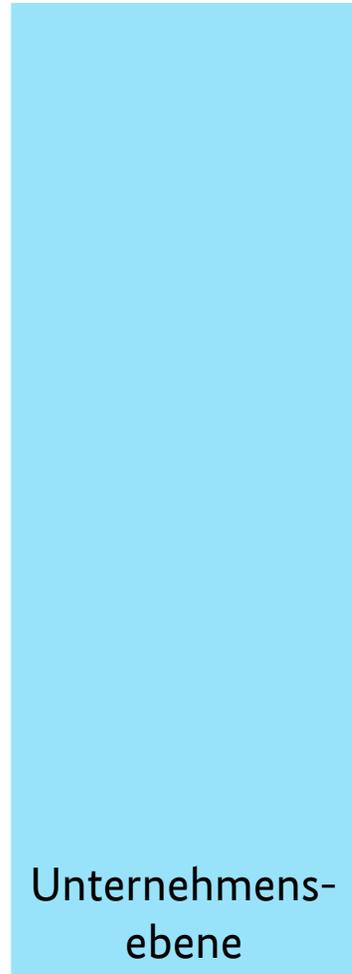


# Bedrohung für Produktionssysteme

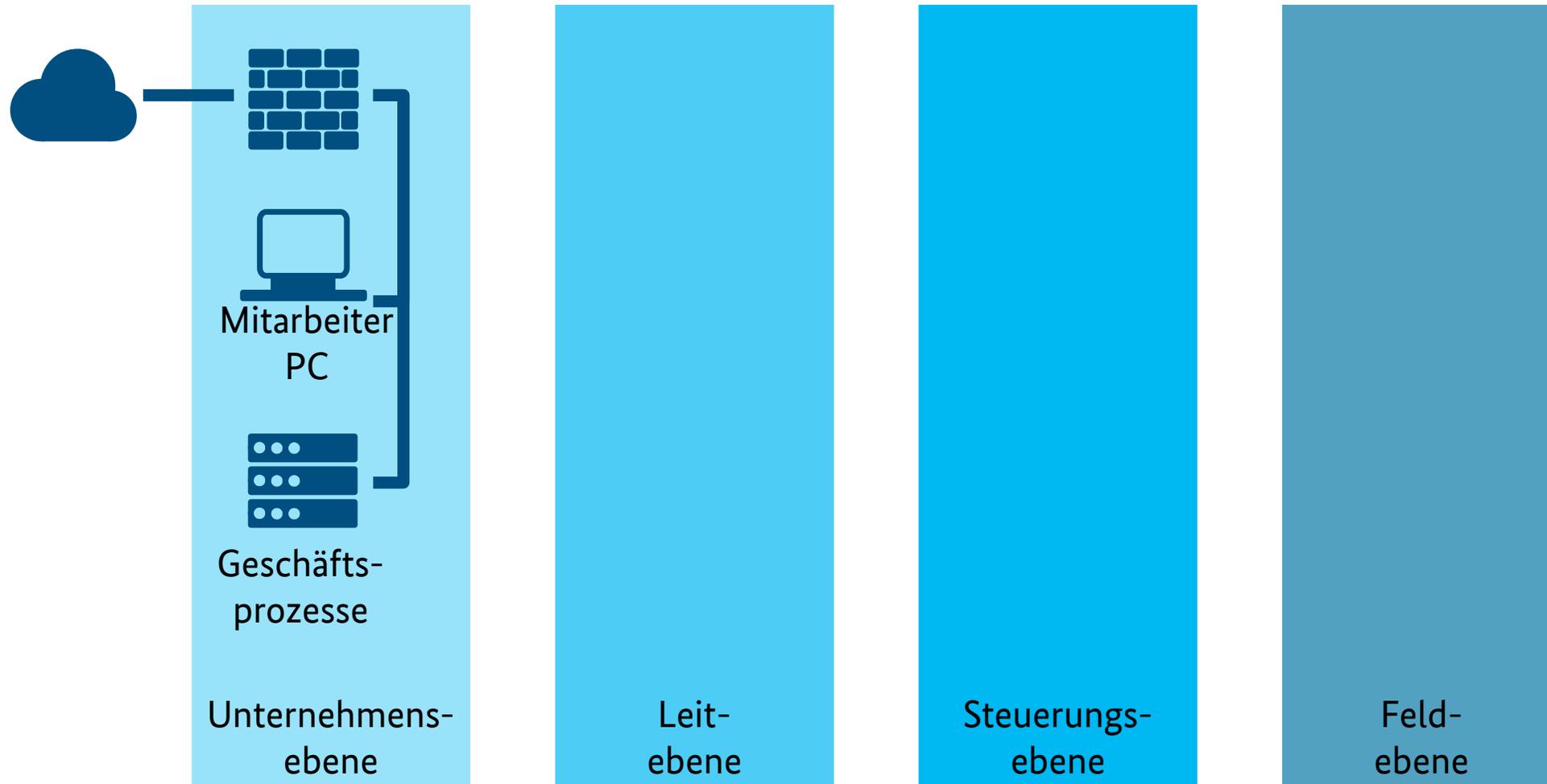
- Vernetzung ermöglicht
  - Zugriffe auf bisher abgeschottete Bereiche
  - Zugriffe aus den abgeschotteten Bereichen in das Unternehmen / Internet
- Abhängigkeiten von Infrastruktur/anderen Unternehmen nimmt zu
- Gefahr von DoS / Ausfall
- Unberechtigte Zugriffe über manipulierte Systeme



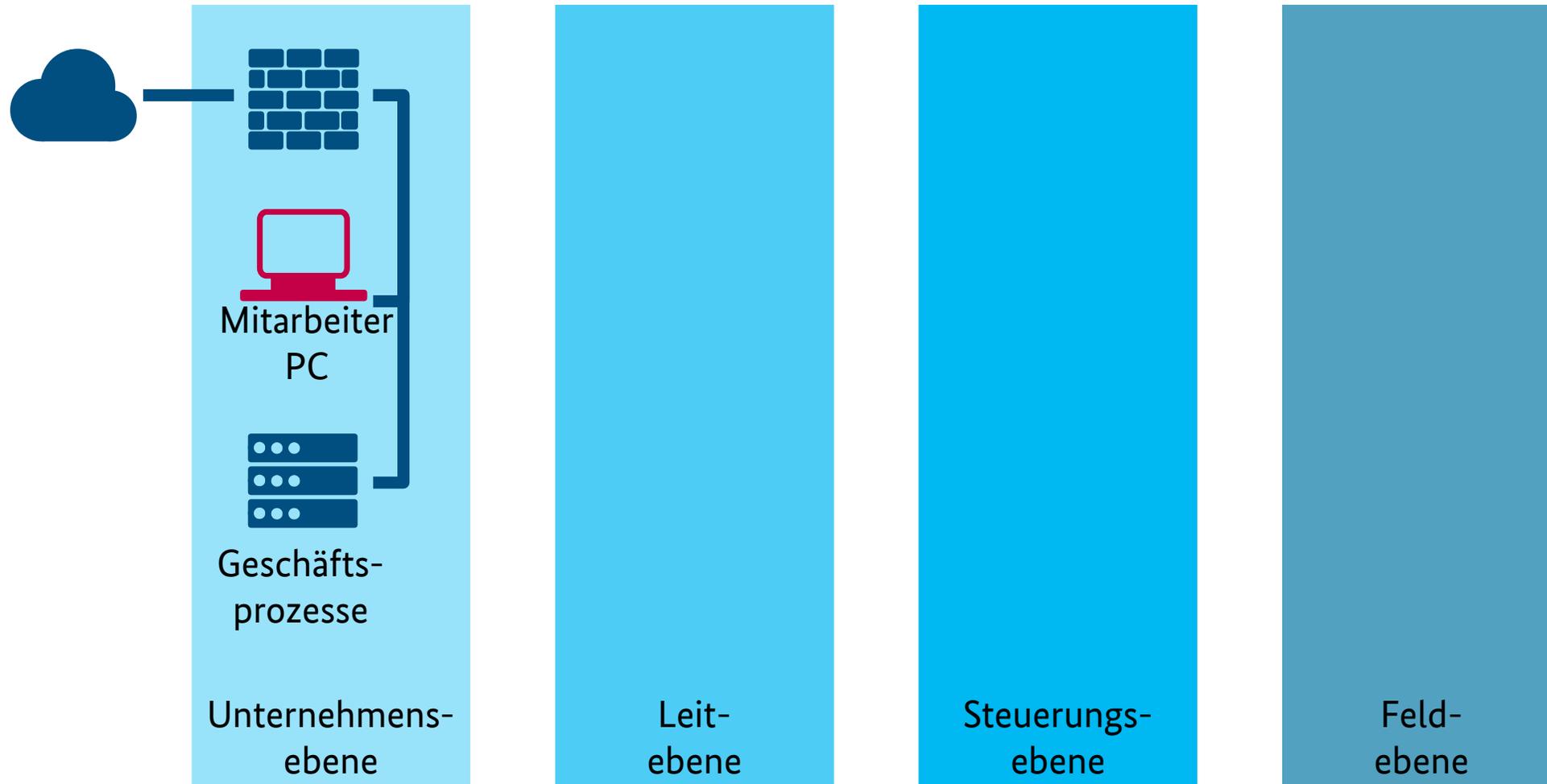
# Übersicht des Unternehmens



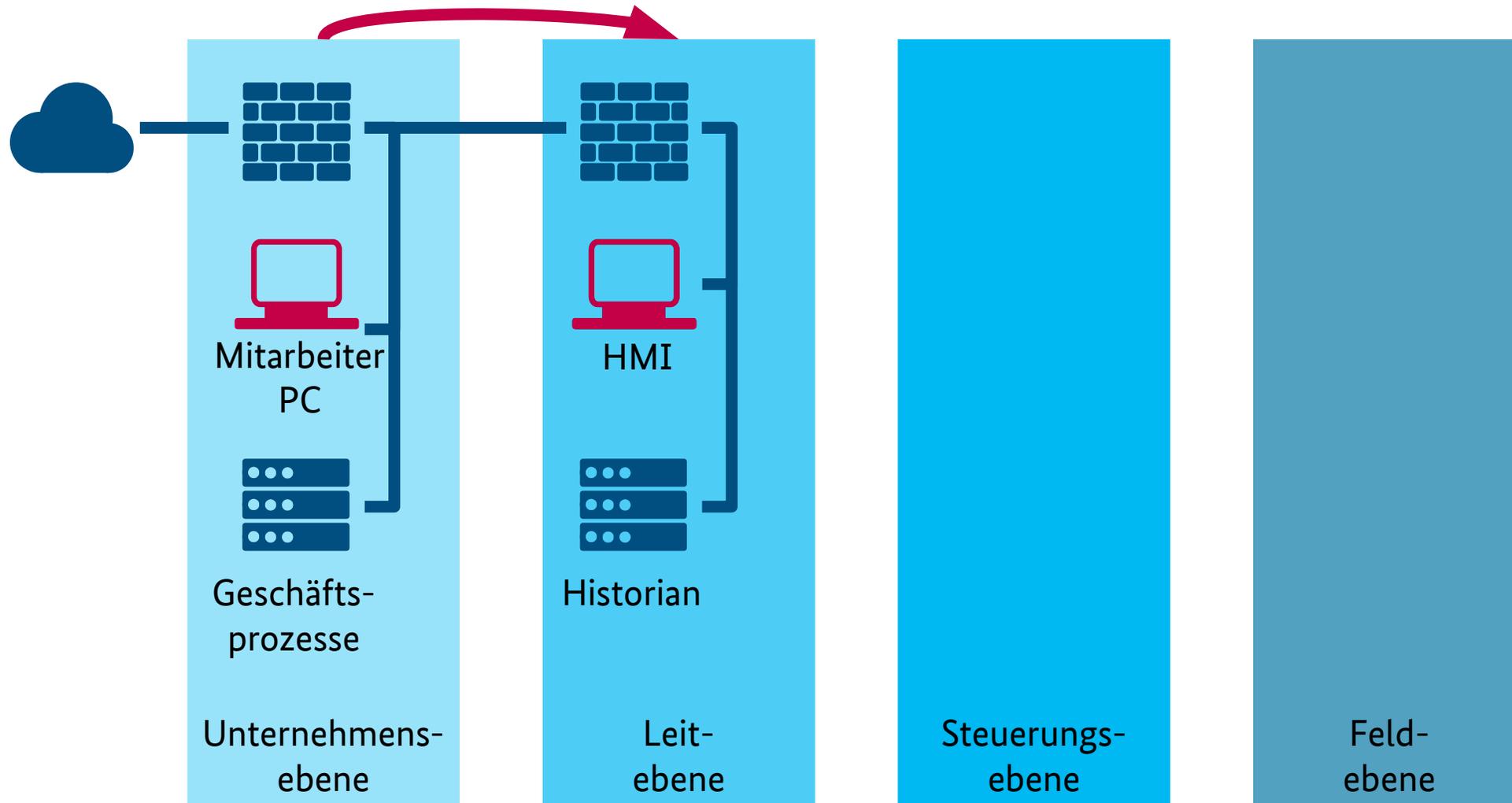
# Einstieg in Unternehmensebene



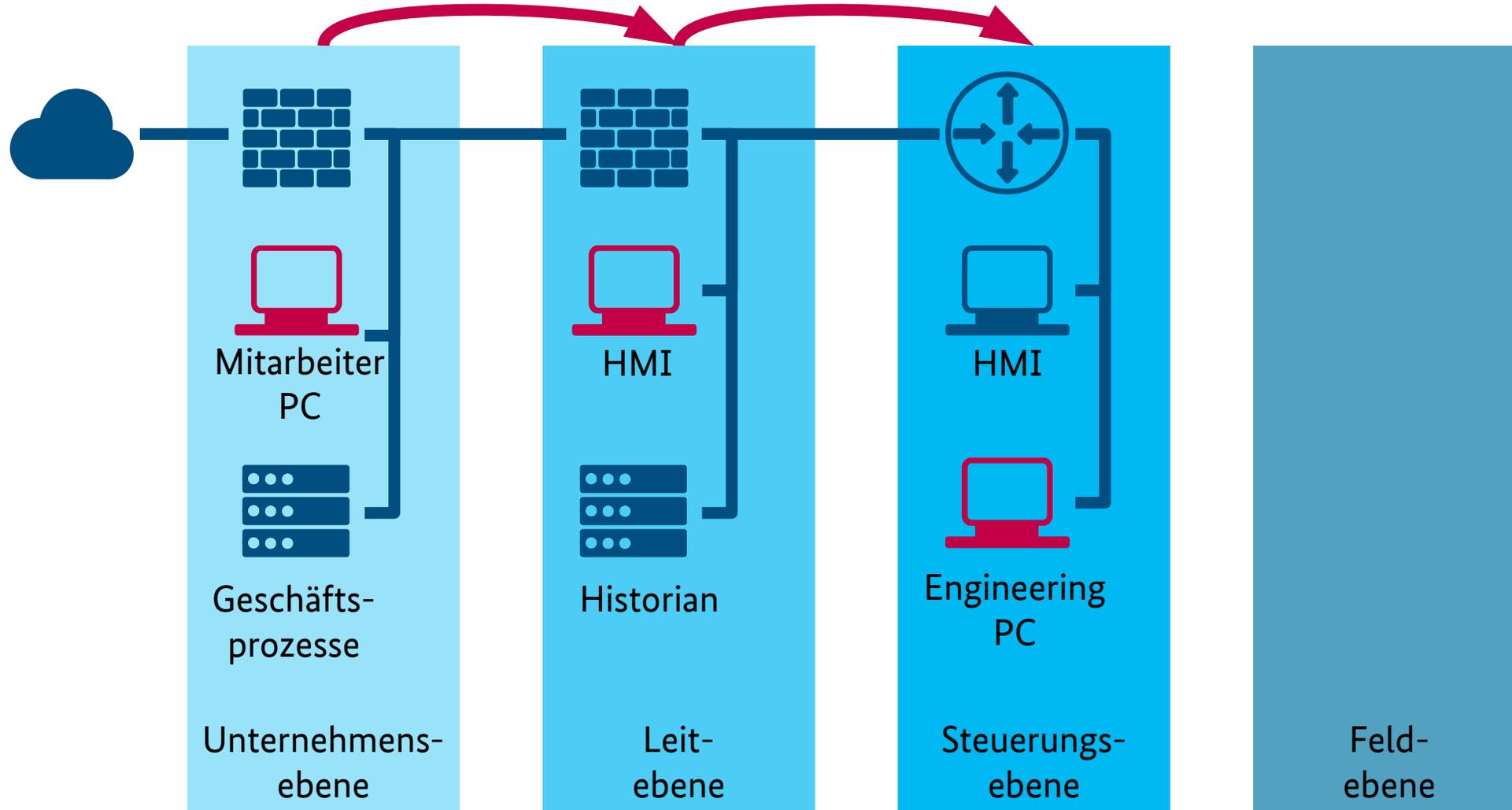
# Einstieg in Unternehmensebene



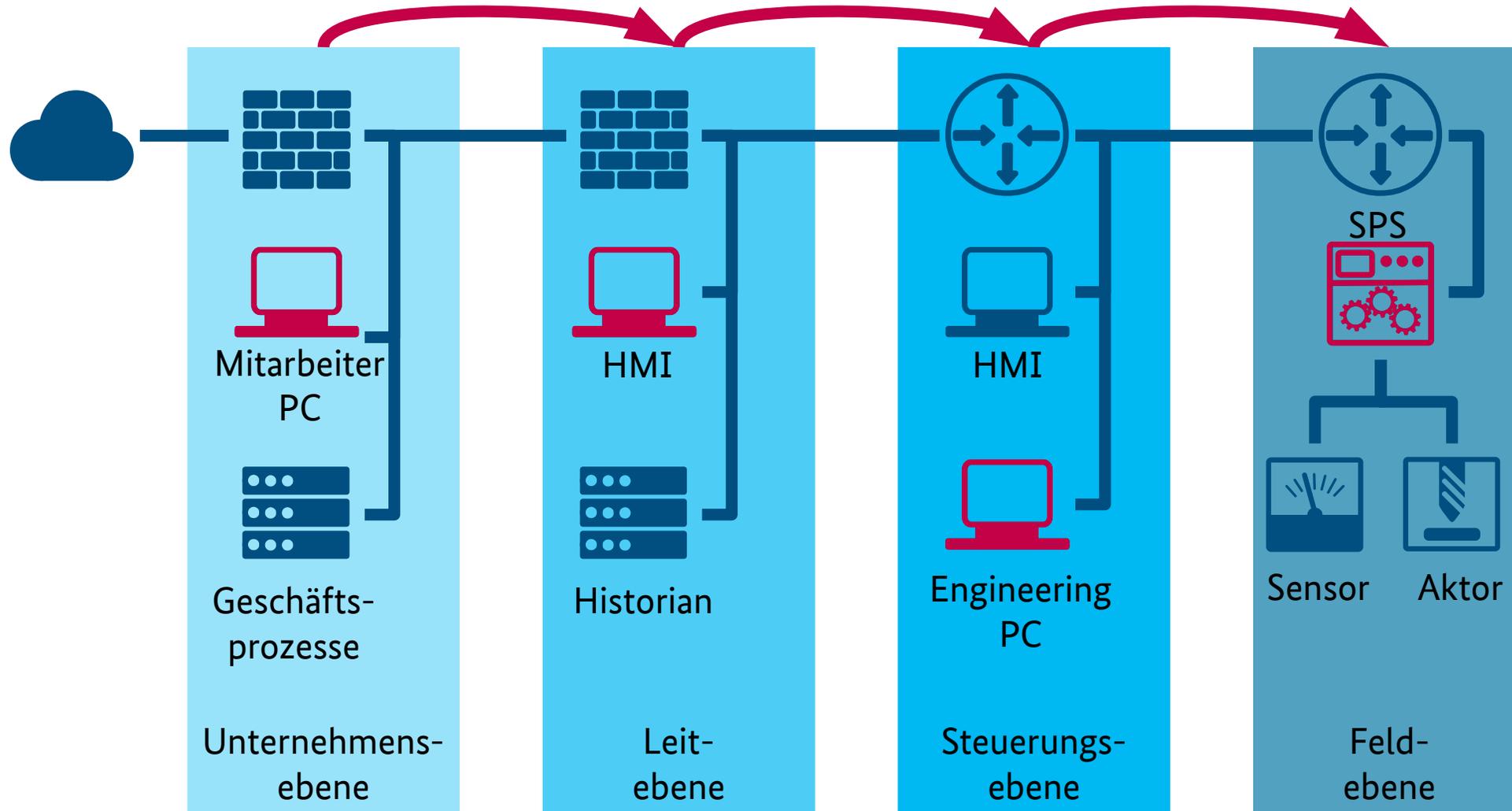
# Sprung in die nächste Ebene ...



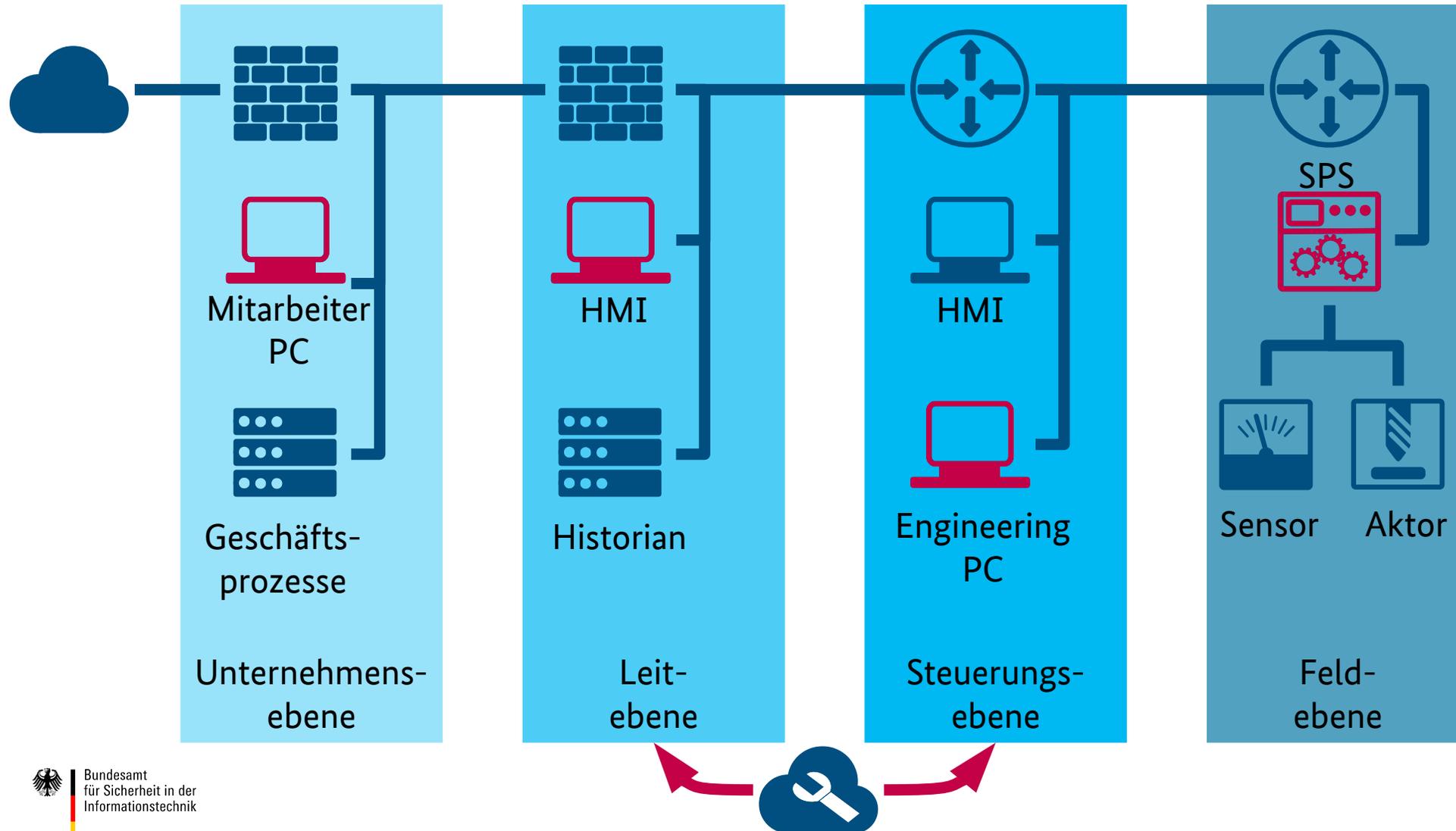
# Sprung in die nächste Ebene ...



# Sprung in die nächste Ebene ...



# Abkürzungen?



# Häufige Fehler und Einfallstore bei Fernwartungszugängen

- Uneingeschränkte, dauerhaft verbundene Zugänge
- Umgehen der Firewall und keine DMZ (demilitarisierte Zone)
- Zugriff auf das gesamte ICS-Netz
- Hardware für den Fernzugriff wird noch für andere Arbeiten benutzt
- Schlecht konfigurierte VPN-Zugänge
- Veraltete Software mit Schwachstellen für den VPN-Zugang
- Einsatz veralteter Protokolle (z.B. SSL statt TLS)
- Nutzung unzureichend starker kryptographischer Verfahren
- Schwache Authentisierungsmechanismen (nur Name & Passwort)
- Ausgesonderte Fernwartungskomponenten mit noch gültigen Zugangsdaten im Internet verkauft

# Maßnahmen zur Absicherung von Fernwartungszugängen

- 2-Faktor-Authentifizierung z.B. One-Time-Key-Generator, Zertifikate, USB-Token
- Zeitliche begrenzte Freigabe der Fernwartungszugänge
- Freigabe der Zugänge durch Mitarbeiter in dem Unternehmen
- Aufbau der Verbindung aus dem OT-Netz in die DMZ
- Monitoring/Logging/ Videomitschnitt der durchgeführten Arbeiten/Änderungen
- Verwendung aktueller Protokolle (TLS 1.2 und 1.3)
- Patchmanagement für Fernwartungskomponenten

# Dokumente zur Absicherung von Fernwartungslösungen

- BSI-CS 108: Fernwartung im industriellen Umfeld
- BSI-CS 054: Grundregeln zur Absicherung von Fernwartungszugängen
- BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- BSI IT-Grundschutz-Kompendium: Betrieb OPS 2.4 - Fernwartung
- IEC-62443: Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme
- NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security

# BSI Grundschutz

Unternehmen und Wirtschaft

Bundesamt für Sicherheit in der Informationstechnik

## IT-Grundschutz-Kompendium

1. Edition 2018



Bundesanzeiger Verlag

IND.1

Bundesamt für Sicherheit in der Informationstechnik

### IND.1: Betriebs- und Steuerungstechnik

#### 1 Beschreibung

##### 1.1 Einleitung

IND.2.1

Bundesamt für Sicherheit in der Informationstechnik

### IND.2.1: Allgemeine ICS-Komponente

#### 1 Beschreibung

##### 1.1 Einleitung

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

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

ICS-Komponenten werden normalerweise über Spezialsoftware des jeweiligen Herstellers programmiert. Das wird entweder über sogenannte Programmiergeräte (z. B. Linux) oder über eine Engineering-Station durchgeführt, die die Anwendung mienbaren Steuerungen löst.

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

##### 1.2 Zielsetzung

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

##### 1.3 Abgrenzung

Die Anforderungen sind für eine generische Komponente erarbeitet. Für sp ter IND.2 ICS-Komponenten zusätzliche Bausteine verfügbar, in denen Anfo die generischen Anforderungen dieses Bausteins hinausgehen und eventuel Der Baustein enthält keine organisatorischen Anforderungen zur Absicheru 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 Bed Betrieb beeinträchtigen können. Beispiele hierfür sind extreme Wärme, Käl auch ätzend oder korrosiv wirkende Atmosphären. Häufig treten au Durch solche schädlichen Umgebungseinflüsse können ICS-Komponenten s fallen.

IT-Grundsutz-Kompendium: Stand Februar 2018

IND: Industrielle IT



IND.2.2

Bundesamt für Sicherheit in der Informationstechnik

### 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 oder 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 au 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 a gerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden. i treffen sind modulare Speicherprogrammierbare Steuerungen, die aus verschiedenen Funktio zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualise Protokollieren durch die SPS realisiert.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft est 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, i 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 berücksi Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komg sen die Anforderungen des Bausteins IND.1 Betriebs- und Steuerungstechnik umgesetzt wert Bereich funktionale Sicherheit (Safety) nicht behandelt.

IT-Grundsutz-Kompendium: Stand Februar 2018

IND.2.3

Bundesamt für Sicherheit in der Informationstechnik

### IND.2.3: Sensoren und Aktoren

#### 1 Beschreibung

##### 1.1 Einleitung

IND.2

Bundesamt für Sicherheit in der Informationstechnik

### IND.2.2: Speicherprogrammierbare Steuerung (SPS)

#### 1 Beschreibung

##### 1.1 Einleitung

IND.2.4

Bundesamt für Sicherheit in der Informationstechnik

### 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 Produktionen fehlerhaft sein. Die Angreifer können aber auch die Maschine selbst beschädigen, sodass auch dadurch ein wirtschaftlicher Verlust entsteht.

IT-Grundsutz-Kompendium: Stand Februar 2018

# Veröffentlichungen



## ICS-Security-Kompandium



BSI-Veröffentlichungen zur Cyber-Sicherheit

### Sicherer Einsatz von ICS-spezifischen Apps

Im industriellen Anlagen (Industrial Control Systems, ICS), wie der Fabrikautomation oder Prozesssteuerung, verbindet sich zunehmend das Trend zum Einsatz von Apps. Smartphones und Tablets als diese werden meist, ähnlich wie konventionelle Host-Mechanismen (Intercom-IP), zur Visualisierung und Prozesssteuerung verwendet. Dies birgt ein weiteres Anwendungsrisiko, wie die Integration in Konzepte für Fernwartung und Ferndiagnose.

Die vorliegende Empfehlung liefert einen Überblick über die Maßnahmen, die bei der Auswahl und der Nutzung von ICS-spezifischen Apps zu berücksichtigen sind, um eine sichere Nutzung zu gewährleisten.

Diese Maßnahmen können getrennt oder auf weiteren Anwendungsbereichen übertragen werden, die typischerweise nicht unter dem Begriff ICS subsumiert werden. An wen die Empfehlungen für den Consumer-Bereich, z. B. Home Automation sind daher nicht beabsichtigt.

- #### 1 Gefährdungslegte
- Bei Smartphones und Tablets kommt eine Ausführungsgebung hinzu, die es ermöglicht, mehrere Funktionen auf sich zu übertragen. Neben der Möglichkeit, mobile Anwendungen zu installieren, sind auch die Funktionen, wie die Integration in Konzepte für Fernwartung und Ferndiagnose, zu berücksichtigen.
- #### 2 Grundlegende Empfehlungen
- Für einen sicheren Einsatz von ICS-spezifischen Apps empfiehlt das BSI folgende Grundlegende Empfehlungen:
- 1. Der Einsatz von Apps im Kontext von Industrial Control Systems darf nicht zu einer Abnahme der Cyber-Sicherheit der Anlage führen.
  - 2. Der Einsatz von Apps im ICS-Kontext erfordert ein geeignetes Risiko-Management.
  - 3. Auf den Einsatz von Apps, die eine erhebliche Anzahl an Anlagen und/oder Manipulationsmöglichkeiten erfordern, sollte besonderes Augenmerk bei der Auswahl und der Nutzung zu legen.



## Handhabung von Schwachstellen

### Empfehlungen für Hersteller

Viele Unternehmen verfügen bei der Information über Schwachstellen häufig die Prinzipien „Security by Obscurity“. Es ist weniger bekannt oder nur unvollständige Informationen über wichtige geschäftliche Schwachstellen veröffentlicht, jedoch keine genaue Beschreibung dieser Schwachstellen existieren, wenn sie bei einer Schwachstellenanalyse erregt werden. Dies führt zu einer unzureichenden Kenntnis der Schwachstellen, die zu einer unzureichenden Bewertung der Schwachstellen führt. Eine Schwachstellenanalyse ist ein zentraler Bestandteil der Cyber-Sicherheit. Eine Schwachstellenanalyse ist ein zentraler Bestandteil der Cyber-Sicherheit. Eine Schwachstellenanalyse ist ein zentraler Bestandteil der Cyber-Sicherheit.

### Umgang mit dem Ende des Supports für Windows XP

Am 8. April 2014 kündigte die Microsoft die Support für Windows XP an. Die Unterstützung für Windows XP wird am 8. April 2014 beendet. Dies hat Auswirkungen auf die Cyber-Sicherheit von ICS-Systemen. Es ist empfohlen, die Unterstützung für Windows XP zu beenden und die Unterstützung für Windows 7 oder höher zu übernehmen. Es ist empfohlen, die Unterstützung für Windows XP zu beenden und die Unterstützung für Windows 7 oder höher zu übernehmen.

### Veränderung von Schwachstellen durch State- und federierte Zugangsdaten

Embedded Devices können mittlerweile in erheblichem Maße durch die Integration von State- und federierten Zugangsdaten verändert werden. Dies führt zu einer Veränderung der Schwachstellen von Embedded Devices. Es ist empfohlen, die Schwachstellen von Embedded Devices zu überprüfen und die Schwachstellen von Embedded Devices zu überprüfen.

### LARS ICS (Version 1.0)

Light and Right Security ICS – Ein Werkzeug für die industrielle Cyber-Sicherheit



### Fallbeispiel Fernüberwachung

#### „Ist mein Mobilfunkmodem?“

Lesen vom Mitarbeiter von Mobilfunkbetreibern

Lesen vom Mitarbeiter von Mobilfunkbetreibern

### Fallbeispiel Servicetechniker

#### Der Virus kommt zu Fuß!

Das BSI wurde von einem Betreiber einer vertriebenen Industrieanlage darüber informiert, dass es in mehreren Leitungen vermutlich zu einem Virusinfekt gekommen sei. Der Betreiber wurde von einem Betreiber einer vertriebenen Industrieanlage darüber informiert, dass es in mehreren Leitungen vermutlich zu einem Virusinfekt gekommen sei.

### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

Es schien häufig wurde das BSI über einen Störungsangriff informiert, welcher mit dem Internet verbunden ist. In diesem besonderen Fall bestätigte die Betreiberin, dass es sich um einen Störungsangriff handelt, der mit dem Internet verbunden ist.

### Sichere Passwörter in Embedded Devices

#### Veränderung von Schwachstellen durch State- und federierte Zugangsdaten

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

Durch die zunehmende Vernetzung von Maschinen und Anlagen in Automatisierungslösungen, wie der Fabrikautomation, sind die Schwachstellen dieser Anlagen zu berücksichtigen. Es ist empfohlen, die Schwachstellen dieser Anlagen zu berücksichtigen.

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)



### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

### Sichere Passwörter in Embedded Devices

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)



### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

### Sichere Passwörter in Embedded Devices

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)



### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

### Sichere Passwörter in Embedded Devices

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)



### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

### Sichere Passwörter in Embedded Devices

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)



### Fallbeispiel Schwimmbad

#### Ab heute ist jeden Tag Warmbadetag!

### Sichere Passwörter in Embedded Devices

### Sicherheitspezifische Empfehlungen für Maschinenbauer und Integratoren

### Sicherer Einsatz von ICS-spezifischen Apps

### LARS ICS (Version 1.0)

### Sicherer Einsatz von ICS-spezifischen Apps

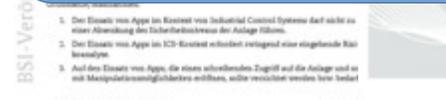
### LARS ICS (Version 1.0)



# Veröffentlichungen



## ICS-Security-Kompendium



**Fallbeispiel Fernüberwachung**  
Warnet mein Mobilfunkmodem?  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Handhabung von Schwachstellen**  
Empfehlungen für Hersteller  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Umgang mit dem Ende des Supports für Windows XP**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Sichere Passwörter in Embedded Devices**  
Veränderung von Schwachstellen durch Staat und freisetzte Zugangsdaten  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Sicherheitsspezifische Empfehlungen für Maschinenbauer und Integratoren**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Anforderungen an netzwerkfähige Industriekomponenten**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Fernwartung im industriellen Umfeld**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Fallbeispiel Servicetechniker**  
Der Virus kommt zu Fuß  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Fallbeispiel Schwimmbad**  
Ab heute ist jeden Tag Warmbadetag!  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Industrial Control System Security**  
Top 10 Bedrohungen und Gegenmaßnahmen 2016  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Fallbeispiel Schwimmbad**  
Ab heute ist jeden Tag Warmbadetag!  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld**  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

**Fallbeispiel Schwimmbad**  
Ab heute ist jeden Tag Warmbadetag!  
Bundeskamt für Sicherheit in der Informationstechnik  
Erfahrungen aus der industriellen Sicherheitsberatung

# www.bsi.bund.de/ICS



# Kontakt

## Halle 8 Stand C 13

### ics-sec@bsi.bund.de

Hr. Jens Kluge  
Jens.Kluge@bsi.bund.de  
Tel. +49 (0) 22899 9582 5938  
Fax +49 (0) 22899 9582 10 5938

Bundesamt für Sicherheit in der Informationstechnik  
Referat CK23 Cyber-Sicherheit in Industrieanlagen  
Godesberger Allee 185-189  
53175 Bonn  
[www.bsi.bund.de/ICS](http://www.bsi.bund.de/ICS)

