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

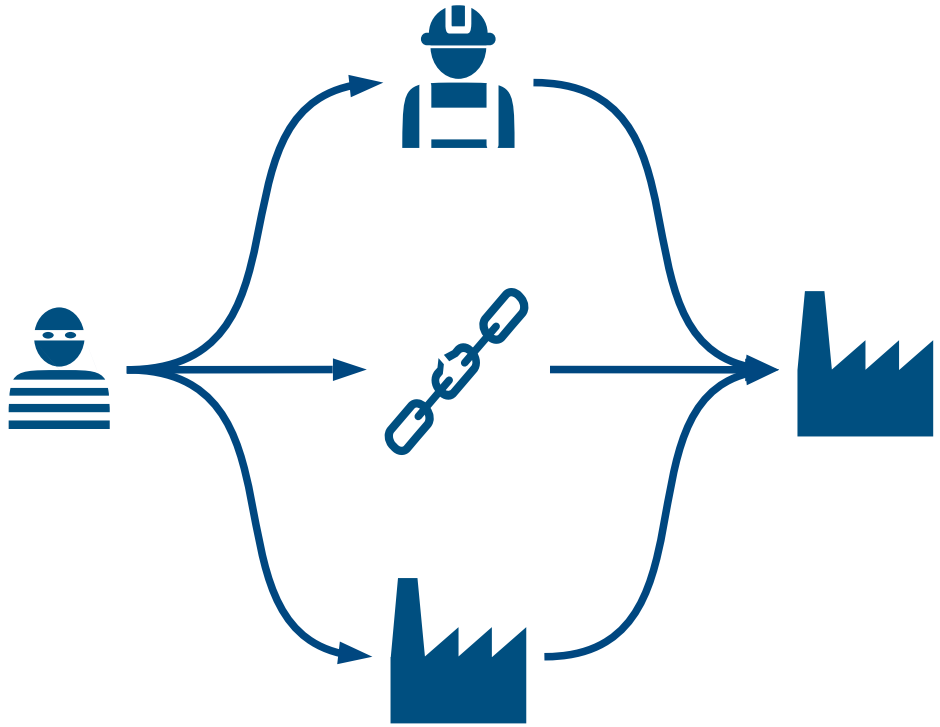
Dragonfly Kampagne/ Havex

Wann:	2011-2014	Ursache:	Spear-Phishing, Watering Hole Attacken, Kompromittierung von Herstellerseiten
Wo:	Europa, Nordamerika		
Ausmaß:	lokal		
Dauer:	mehrere Jahre	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

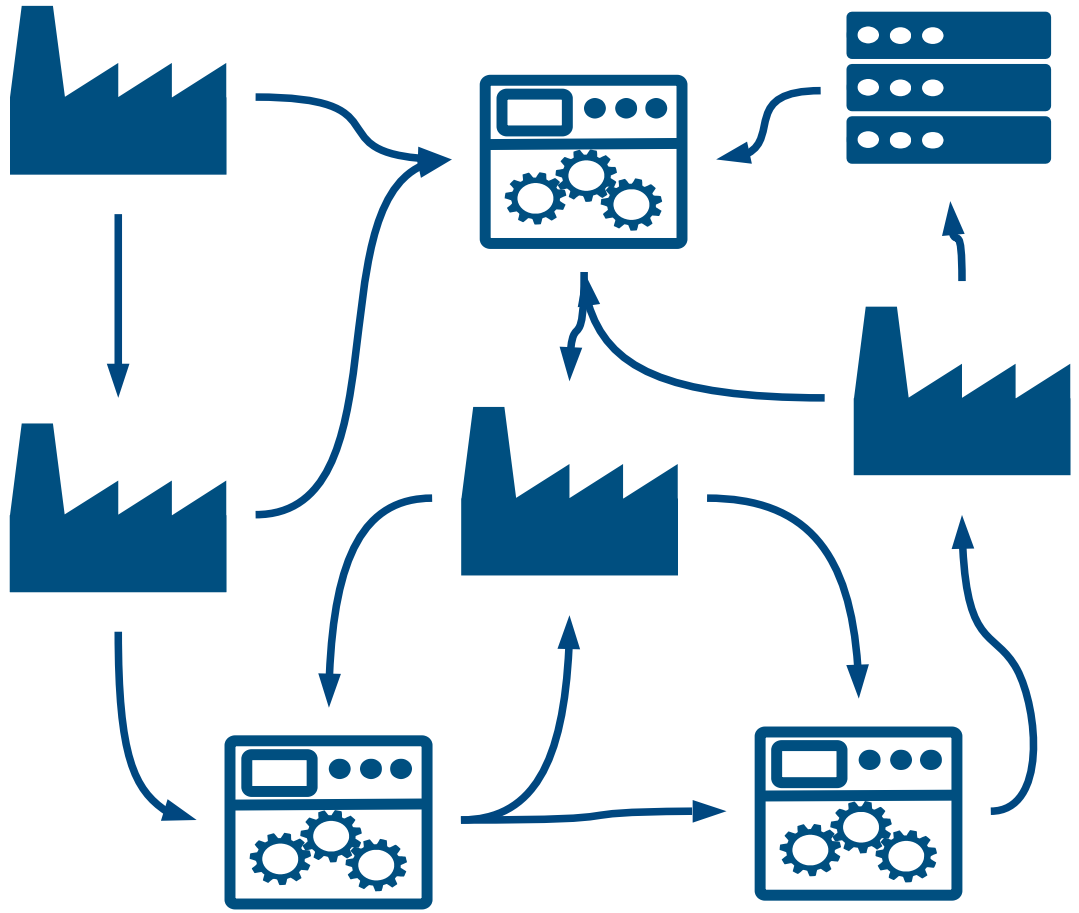
Angriffswege auf Unternehmen

- 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

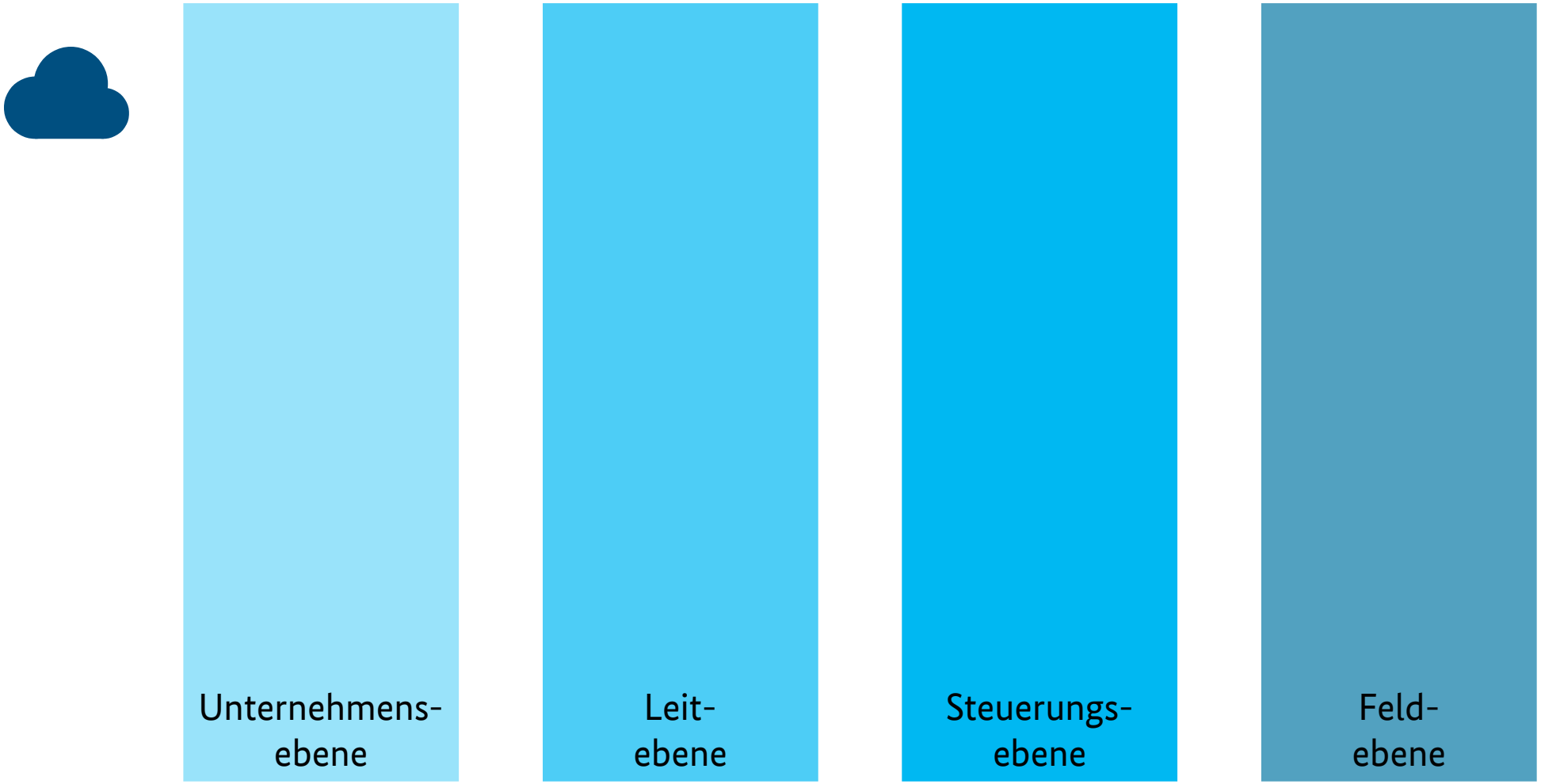


Bedrohung für Produktionssysteme

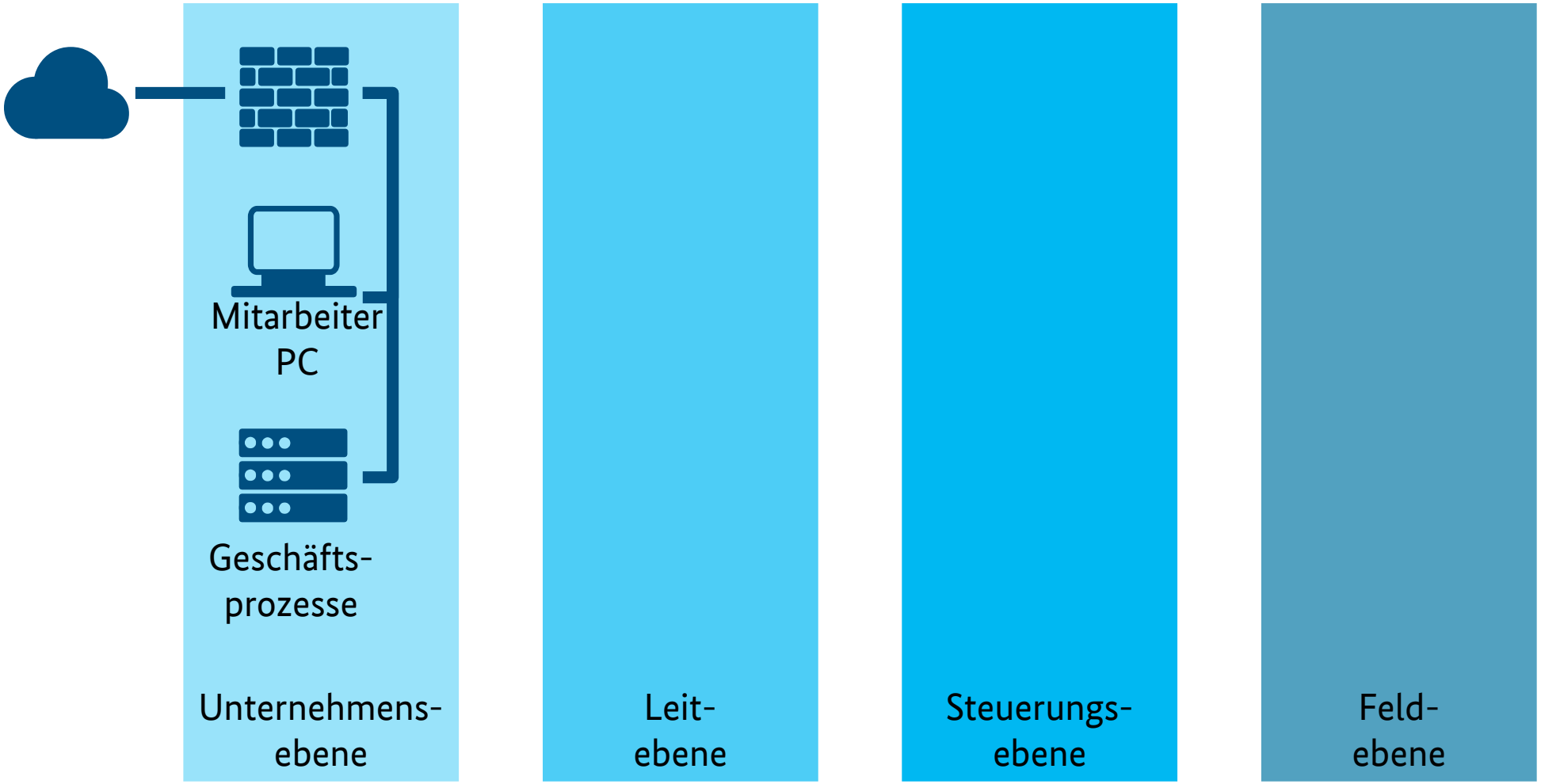
- Vernetzung ermöglicht
  - ➢ Zugriffe auf bisher abgeschottete Bereiche
  - ➢ Zugriffe aus den abgeschotteten Bereichen in das Unternehmen / Internet
- Abhängigkeiten von Infrastruktur/anderen Unternehmen nimmt zu
- Gefahr von DoS / Ausfall
- Unberechtigte Zugriffe über manipulierte Systeme



Übersicht des Unternehmens

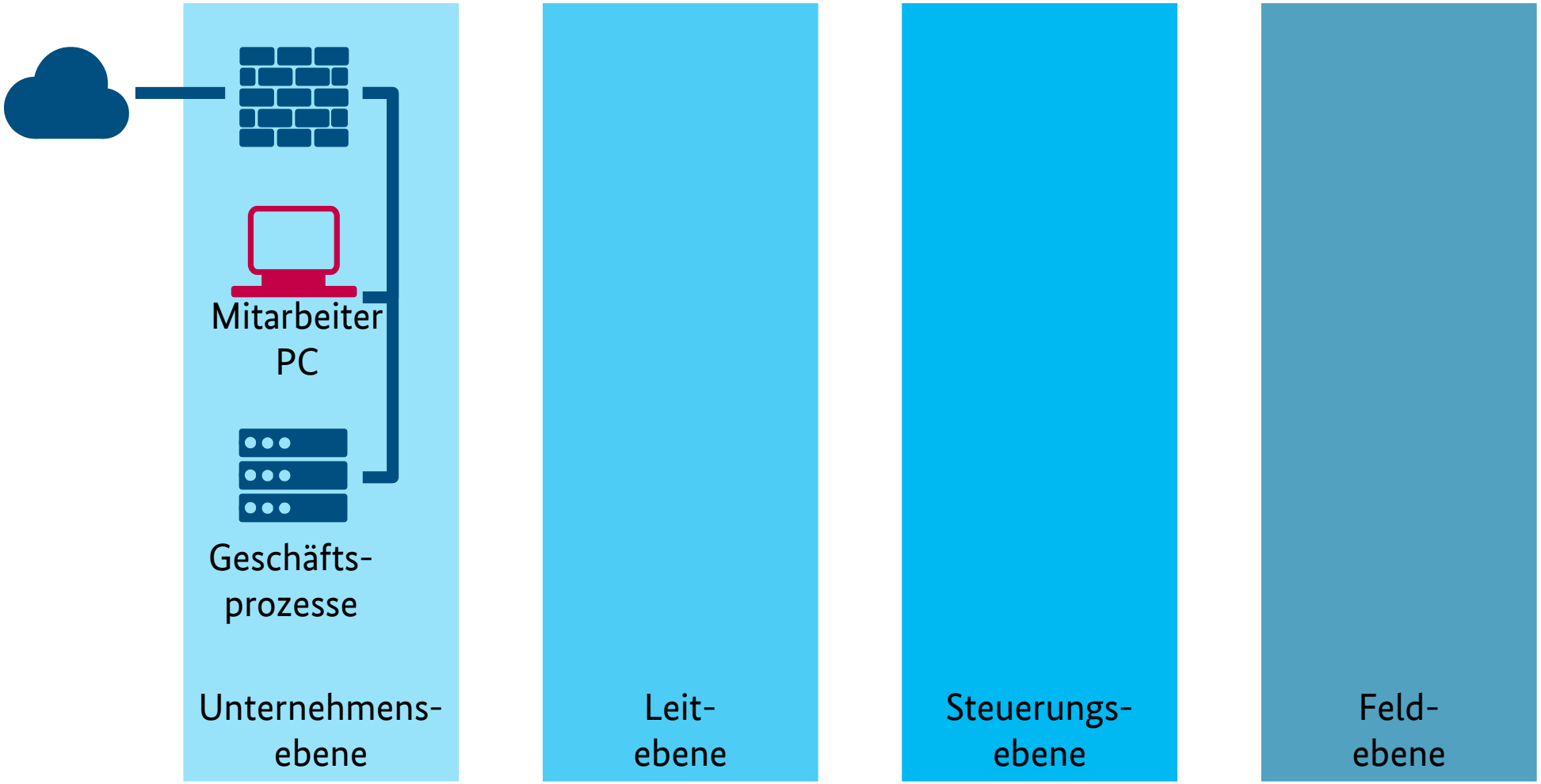


Einstieg in Unternehmensebene

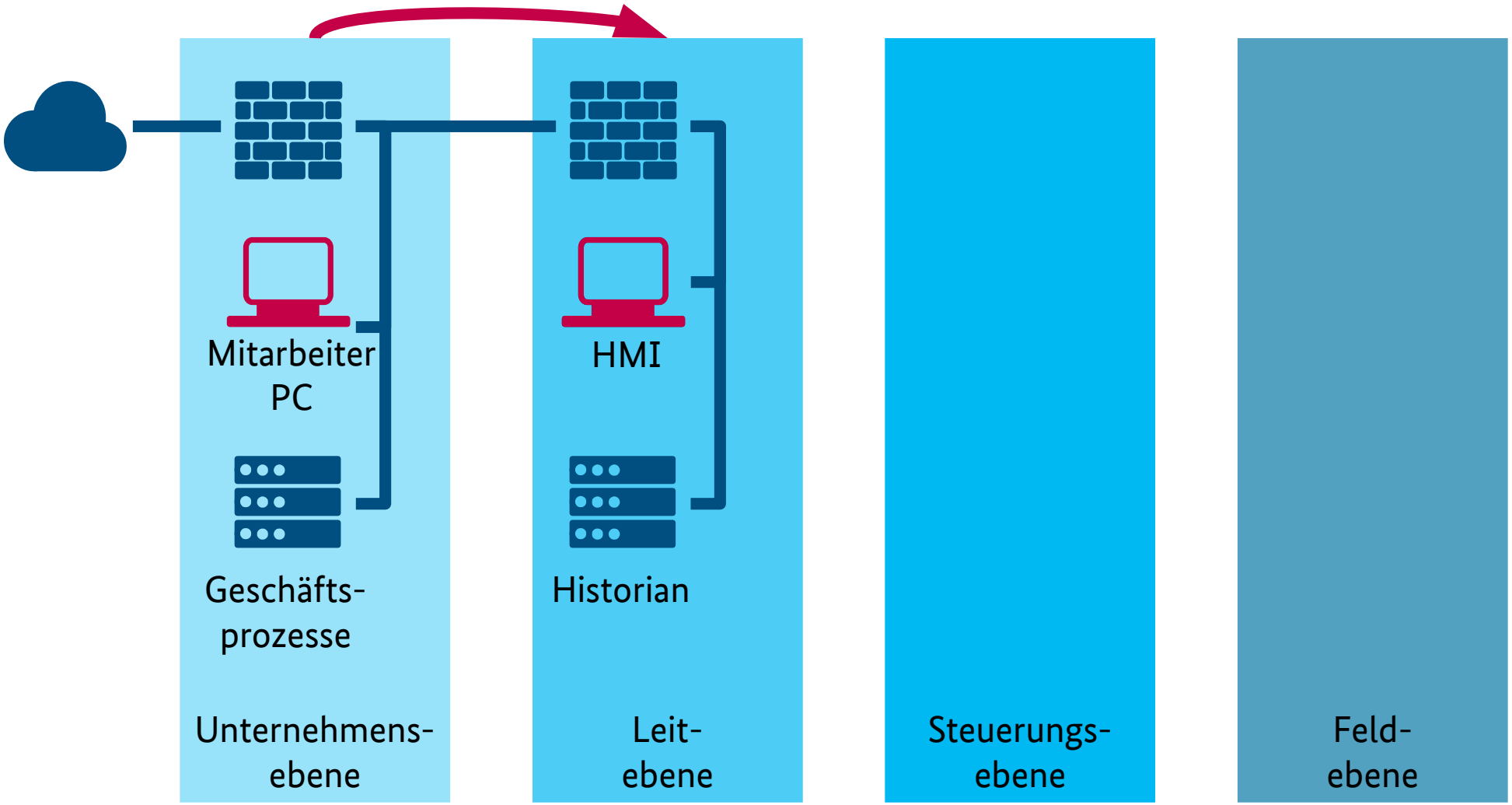


Bundesamt für Sicherheit in der Informationstechnik

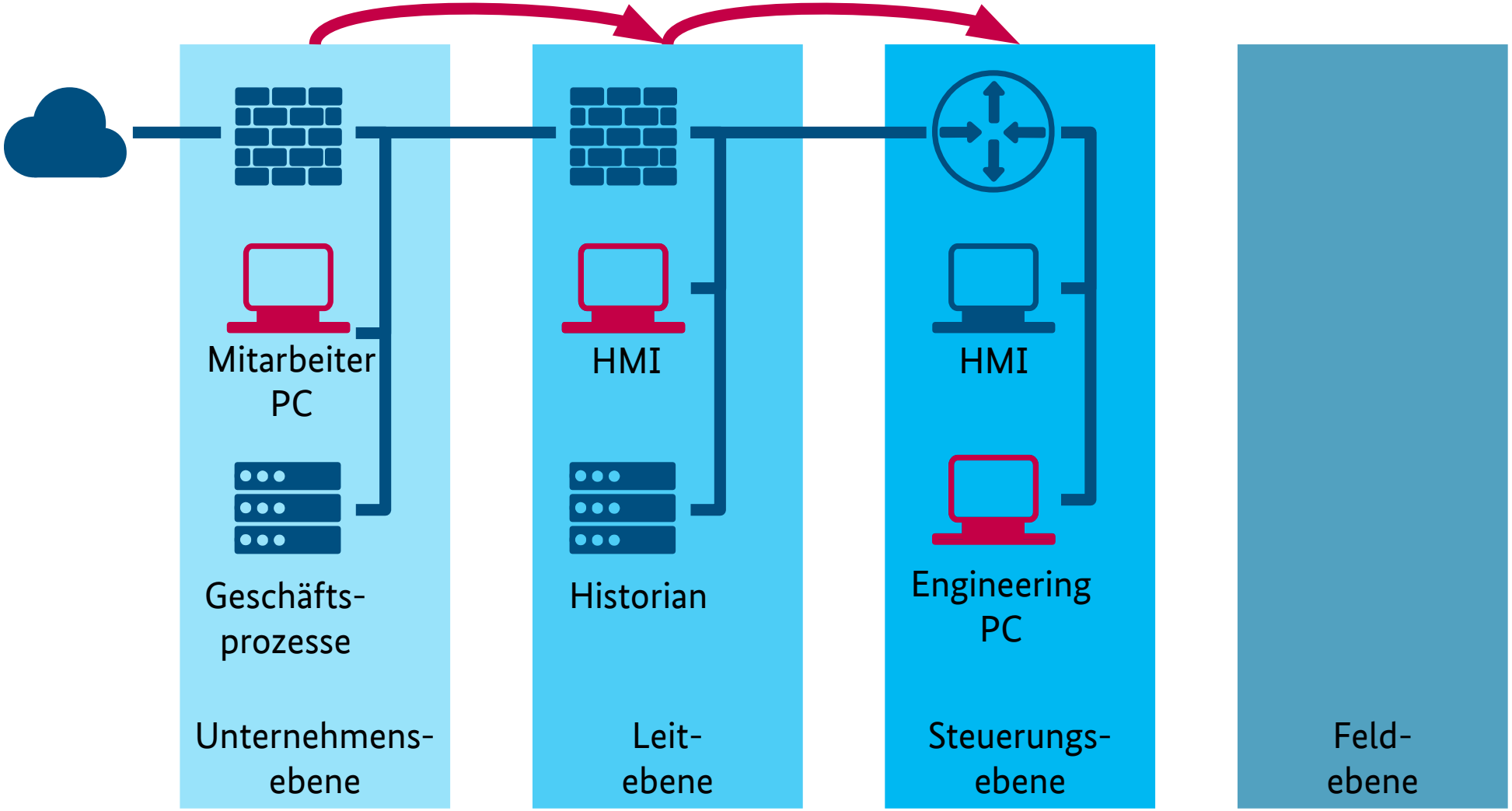
Einstieg in Unternehmensebene



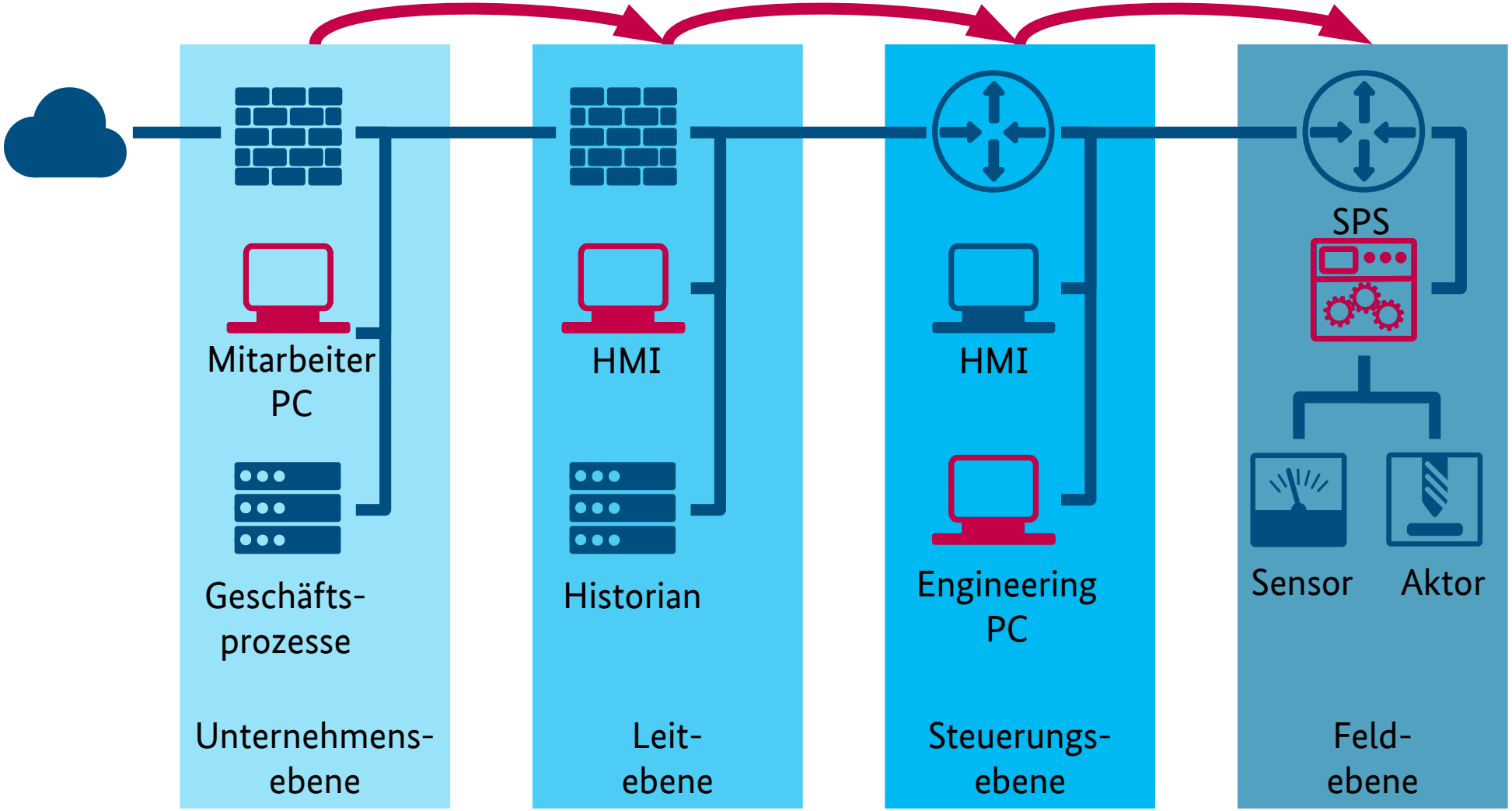
Sprung in die nächste Ebene …



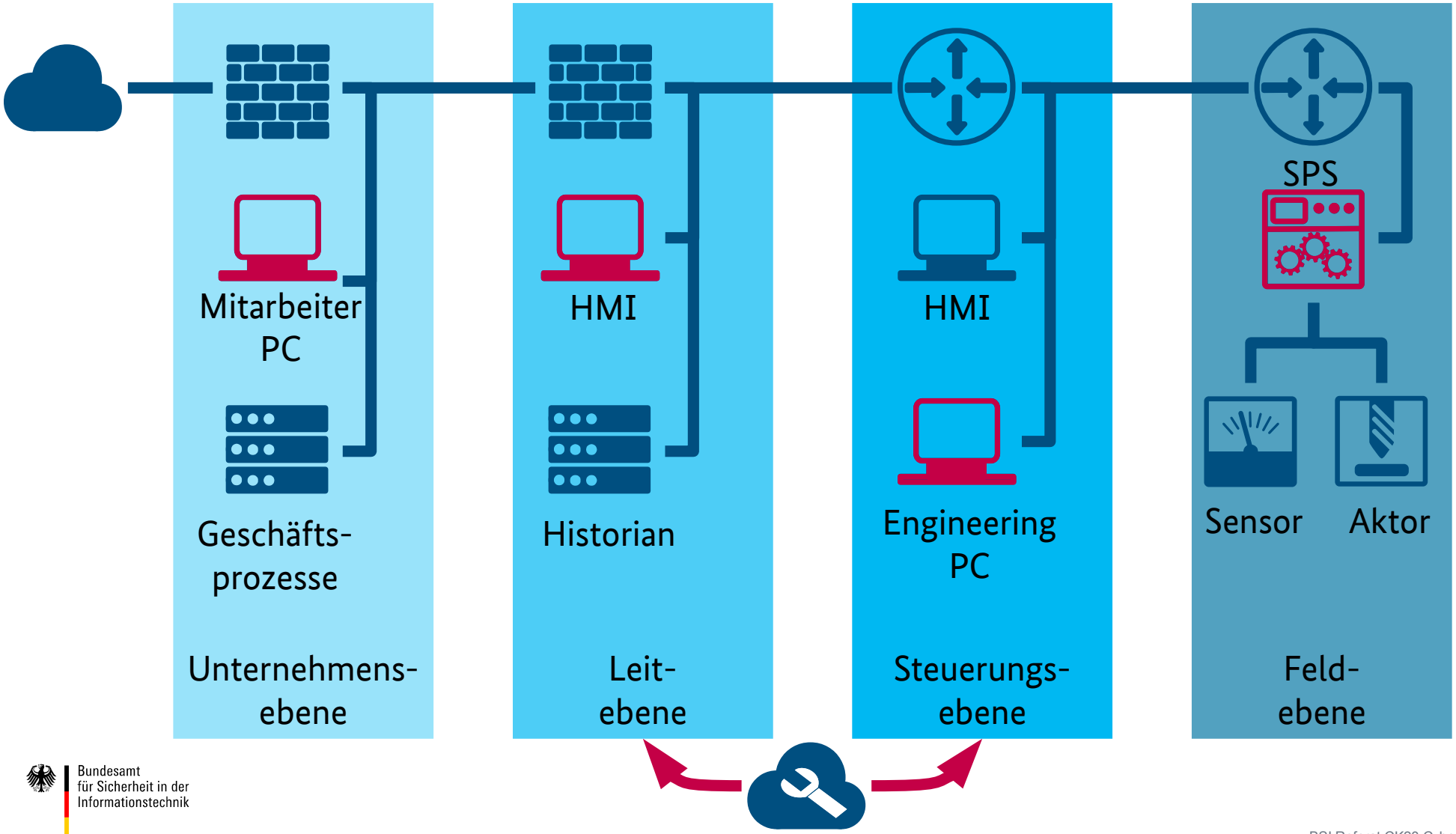
Sprung in die nächste Ebene …



Sprung in die nächste Ebene …



Abkürzungen?



Häufige Fehler und Einfalltore 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 Authenitisierungsmechanismen (nur Name & Passwort)
- Ausgesonderte Fernwartungskomponenten mit noch gültigen Zugangsdaten im Internet verkauft

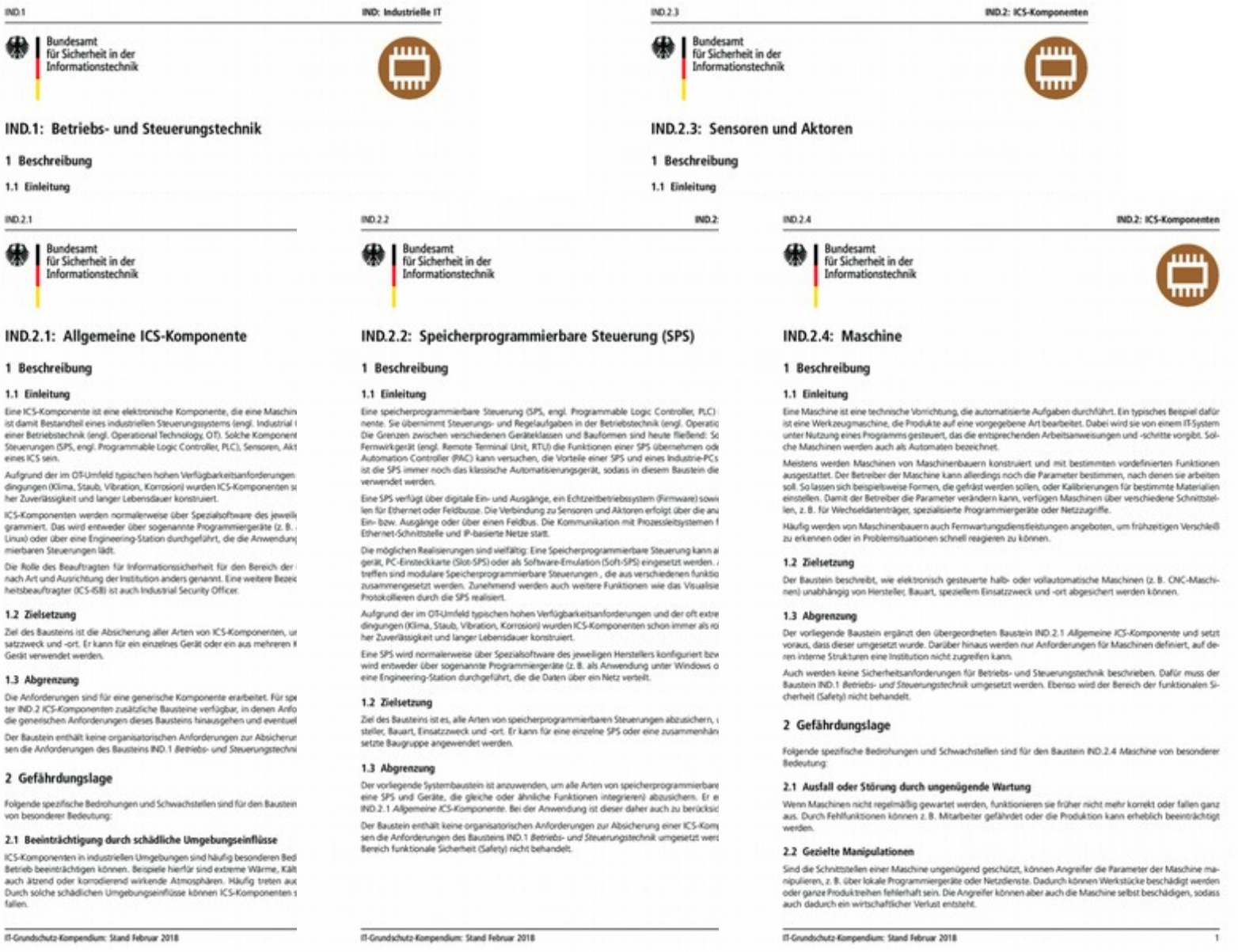
Maßnahmen zur Absicherung von Fernwartungszugängen

- 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


IND.1 IND: Industrielle IT

Bundesamt für Sicherheit in der Informationstechnik

IND.1: Betriebs- und Steuerungstechnik

1 Beschreibung

1.1 Einleitung

IND.2.3 IND.2: ICS-Komponenten

Bundesamt für Sicherheit in der Informationstechnik

IND.2.3: Sensoren und Aktoren

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

1.2 Zielsetzung

1.3 Abgrenzung

2 Gefährdungslage

2.1 Beeinträchtigung durch schädliche Umgebungseinflüsse

IT-Grundschutz-Kompendium: Stand Februar 2018

IND.2.2 IND.2:

Bundesamt für Sicherheit in der Informationstechnik

IND.2.2: Speicherprogrammierbare Steuerung (SPS)

1 Beschreibung

1.1 Einleitung

1.2 Zielsetzung

1.3 Abgrenzung

IT-Grundschutz-Kompendium: Stand Februar 2018

IND.2.4 IND.2: ICS-Komponenten

Bundesamt für Sicherheit in der Informationstechnik

IND.2.4: Maschine

1 Beschreibung

1.1 Einleitung

1.2 Zielsetzung

1.3 Abgrenzung

2 Gefährdungslage

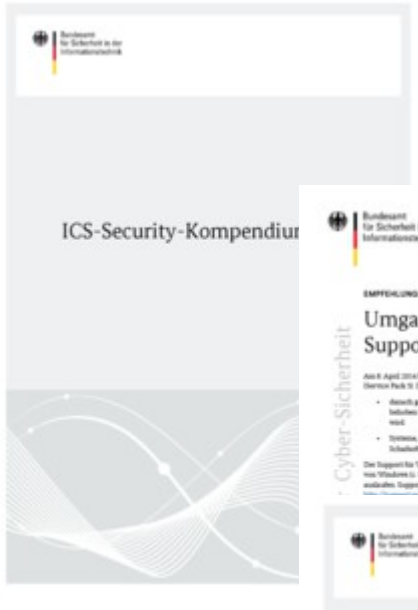
2.1 Ausfall oder Störung durch ungenügende Wartung

2.2 Gezielte Manipulationen

IT-Grundschutz-Kompendium: Stand Februar 2018 1

Bundesamt
für Sicherheit in der
Informationstechnik

Veröffentlichungen



Veröffentlichungen

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

Bundesamt
für Sicherheit in der
Informationstechnik