



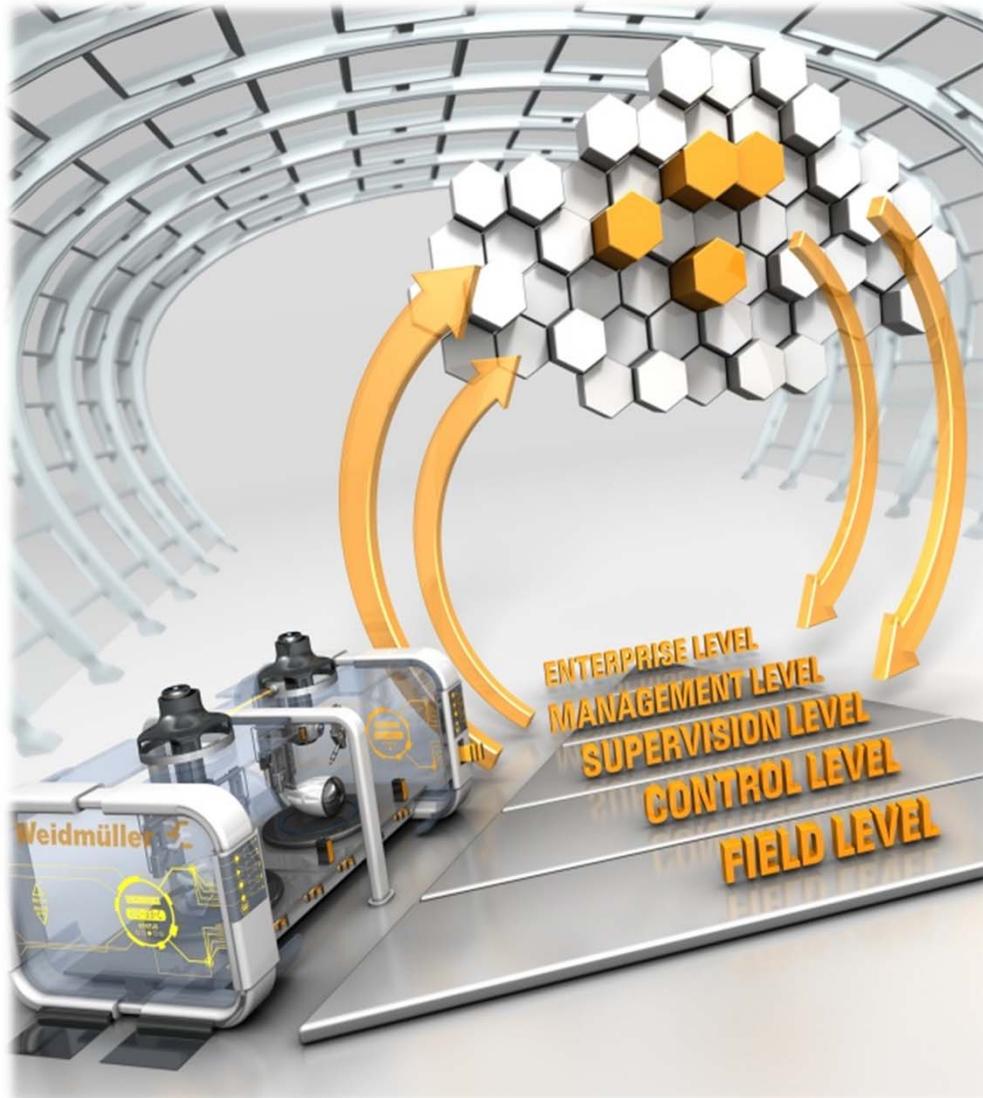
CERT@VDE

Schwachstellen im Umfeld von Prozess-IT

CERT@VDE Workshop, Hannover

Dr.-Ing. Kai Lorentz, Weidmüller

Vom Feldbus zur Cloud



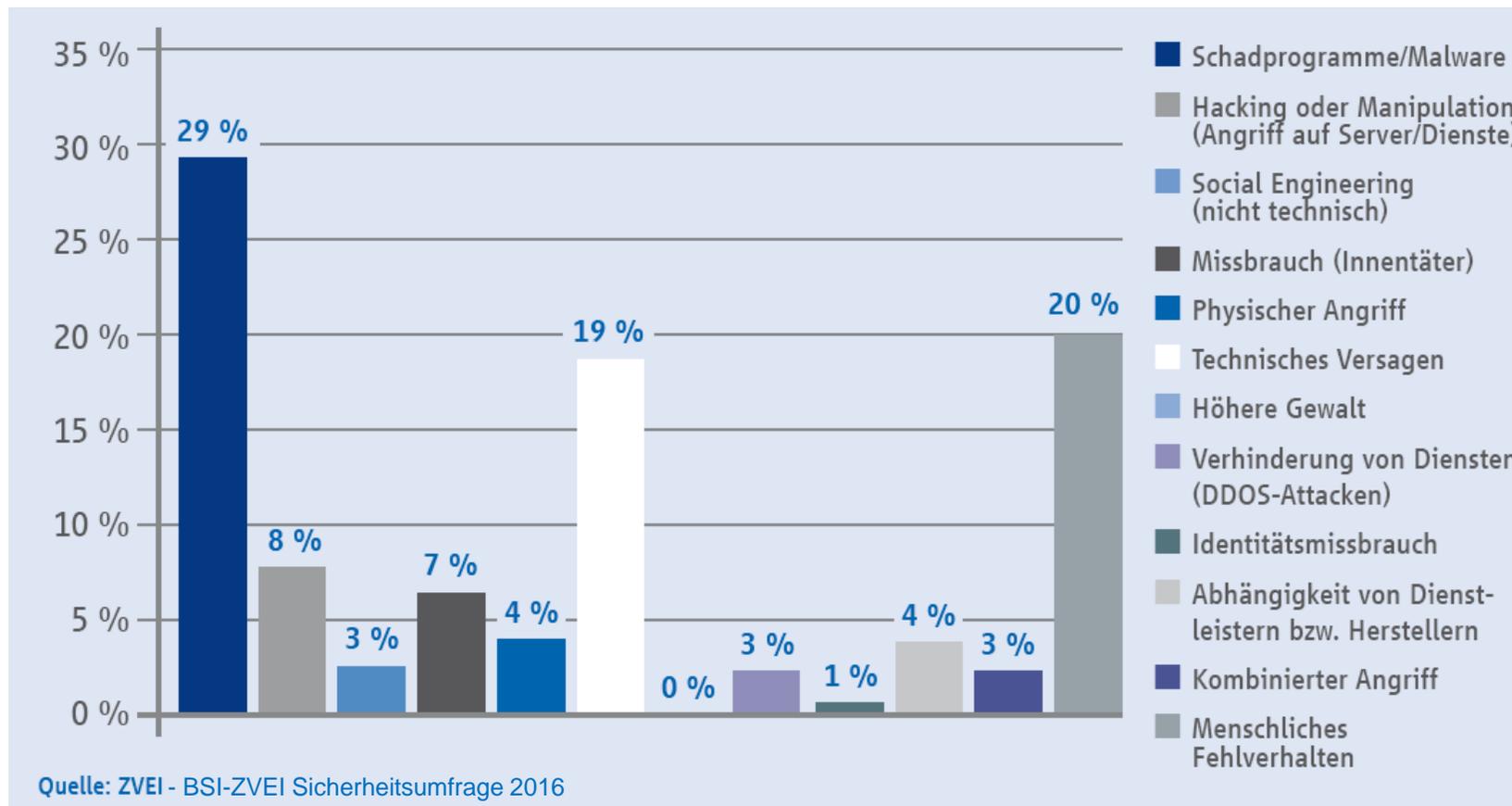
**Zugang zu der Fabrikhalle durch die Cloud:
Weltweiter Zugriff bis zum Sensor**

**Geräte-, Prozess- und Zustands-
informationen sind verknüpft und
über Dienste im Netzwerk verfügbar**

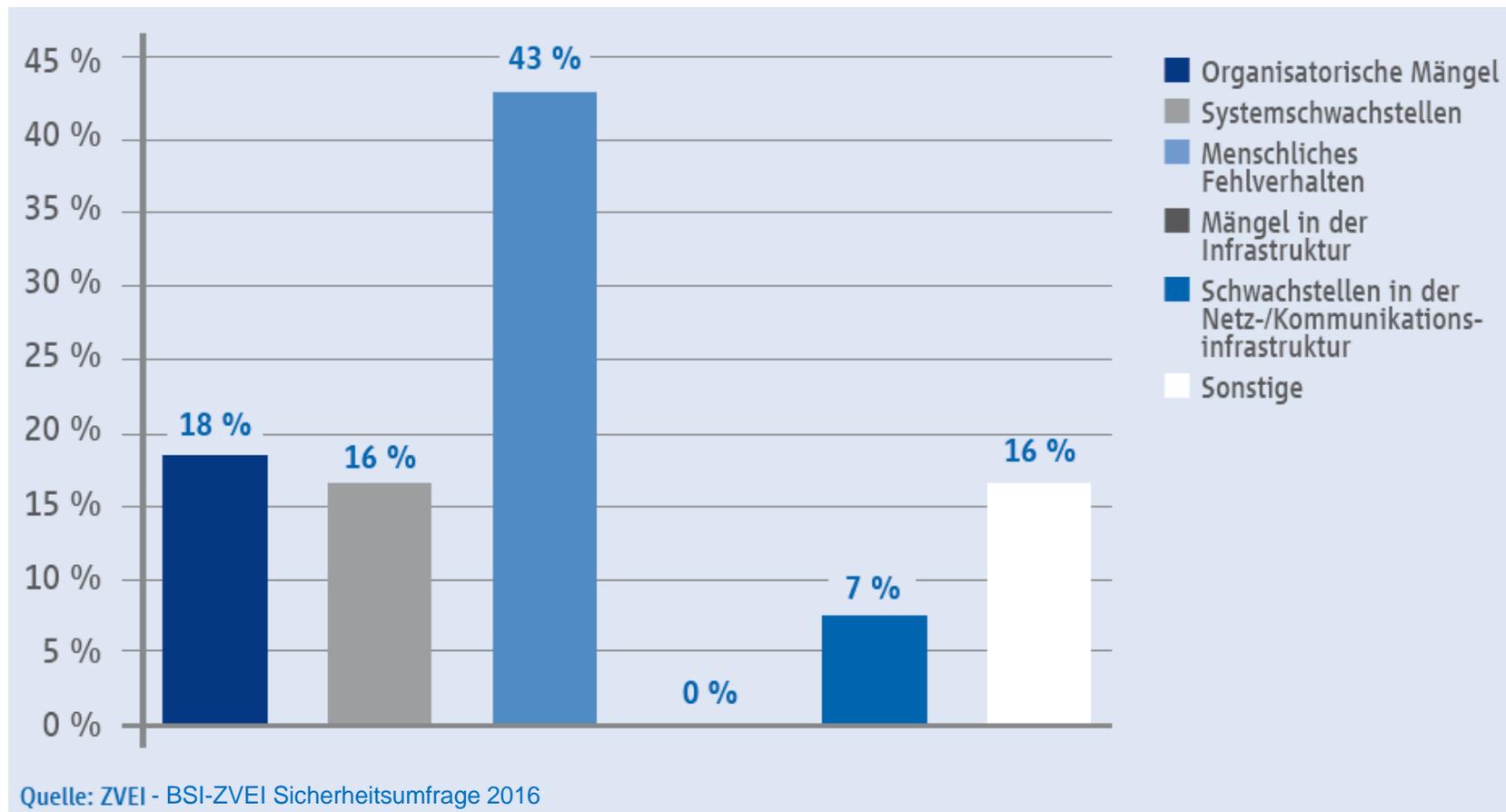
**IT basierte Automatisierungsgeräte
finden zunehmend Anwendung:
Klassische Betriebssysteme**

**Klassische Feldbusse werden durch
Ethernet basierte Busse ersetzt:
Durchgängigkeit bis zum Sensor**

Top-Bedrohungen



Top-Schwachstellen



Angriffe auf Industrieanlage 2014



3.3.1 APT-Angriff auf Industrieanlagen in Deutschland

Sachverhalt

Gezielter Angriff auf ein Stahlwerk in Deutschland.

Methode

Mittels Spear-Phishing und ausgefeiltem Social Engineering erlangten Angreifer initialen Zugriff auf das Büronetz des Stahlwerks. Von dort aus arbeiteten sie sich sukzessive bis in die Produktionsnetze vor.

Schadenswirkung

Es häuften sich Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen. Die Ausfälle führten dazu, dass ein Hochofen nicht geregelt heruntergefahren werden konnte und sich in einem undefinierten Zustand befand. Die Folge waren massive Beschädigungen der Anlage.

Zielgruppen

Betreiber von Industrieanlagen.

Fazit

- Technische Entwicklungen wie I4.0 und IoT führen zu einer durchgängigen Vernetzung von der Sensorebene bis in die Cloud.
 - Dabei kommen immer mehr IT-Technologien zum Einsatz – Betriebssysteme, Kommunikationsprotokolle.
 - Im Gegensatz zu den herkömmlichen Automatisierungstechnologien leben diese IT-Technologien und müssen gepflegt werden.
- Security wird aufgrund dieser Entwicklungen immer wichtiger und ist ein „moving target“, das ständig gepflegt und aufrecht erhalten werden muss!