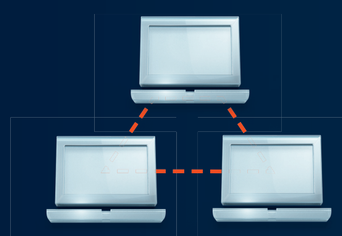
INDUSTRIAL SECURITY

COPADATA

BETRIFFT ES MICH?

Die Tore der Produktionsanlagen stehen offen.

Können unbefugte Personen sich einfach Zutritt verschaffen?



Meine Kollegen arbeiten auch in der Produktion mit PCs.

Gibt es Richtlinien, z.B. zur Passworterstellung?

Ich nutze mobile Endgeräte.

Greife ich damit auf Produktionsdaten zu?

Die Produktions-IT und die Office-IT sind zwei unterschiedliche Systeme.

Wie findet der Datenaustausch zwischen ihnen statt?

Ich bin nach außen mit meinen Kunden und Lieferanten vernetzt.

Sind diese Verbindungen entsprechend gesichert?

Meine Computer sind mit dem Internet verbunden.

Wie schütze ich mich vor Schadsoftware?

In meinem Unternehmen werden weit verbreitete Softwarelizenzen benutzt.

Werden auftretende Sicherheitslücken mit Hilfe von Updates regelmäßig geschlossen?

BIN ICH EIN INTERESSANTES ANGRIFFSZIEL?

WESENTLICHES KAPITAL MEINES UNTERNEHMENS IST ...

QUALITÄT, PERFORMANCE, VERFÜGBARKEIT

Sensible Prozesse, deren Fehlfunktionen zu erheblichen Schäden führen könnten.

SYSTEME KÖNNEN MANIPULIERT WERDEN.

KNOW-HOW

Wissen, das für Dritte interessant sein könnte.

INFORMATIONEN KÖNNEN GESTOHLEN WERDEN.

WELCHE POTENZIELLEN SCHWACHSTELLEN HAT MEIN UNTERNEHMEN?

MENSCH

- Unberechtigter Zugang zu sensiblen Anlagenbereichen, Schaltschränken, Netzwerkkomponenten
- Unbefugter Zugang zu Produktionsdaten
- Sorgloser Umgang mit dem IT-System

TECHNIK

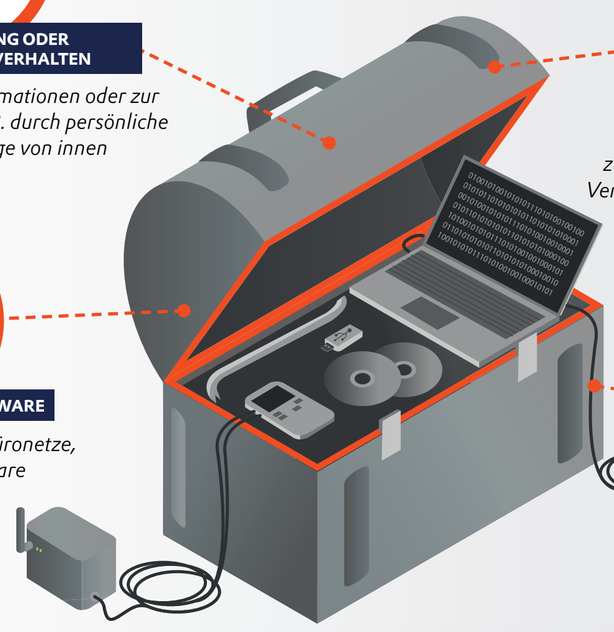
- Unverschlüsselte Protokolle
- Zugriff auf Daten und Prozesse via Smartphone
- Veraltete Software-Systeme und fehlende Sicherheitsupdates
- Direkte Verbindung der Steuerungskomponenten mit dem Internet
- Unsicherer Datenaustausch zwischen den Unternehmensbereichen
- Erreichbarkeit über Fernwartungssysteme

ORGANISATION

- Unzureichende Überprüfung der Sicherheit der Konfigurationen von Netzwerkkomponenten (Router, Firewalls, Switches etc.)
- Unzureichendes Patch-Management
- Fehlende Sensibilisierung und zu wenig Know-how über IT-Security im Unternehmen

WELCHE WERKZEUGE & TECHNIKEN BENUTZEN POTENZIELLE ANGREIFER?

Die Werkzeugkiste der Angreifer



SOCIAL ENGINEERING ODER MENSCHLICHES FEHLVERHALTEN

unbefugter Zugang zu Informationen oder zur technischen Infrastruktur, z.B. durch persönliche Kontakte oder Sabotage von innen

AUSNUTZUNG EXTERNER ZUGRIFFE

zum Beispiel über Fernwartungssysteme, Vernetzung mit Zulieferern oder Abnehmern

INFEKTION MIT SCHADSOFTWARE

über das Internet gekaperte Büronetze, Intranet, externe Hardware

KOMPROMITTIERUNG

von Smartphones im Produktionsumfeld, Extranet und Cloud-Komponenten

Welche Normen & Richtlinien gibt es?

- **USA**
  NERC CIP (North American Electric Reliability Corporation / Critical Infrastructure Protection)
- **...**
- **IEC 62443**
- **Deutschland**
  IT-Sicherheitsgesetz (oft auch KRITIS-Gesetz genannt)
- **ISO 27000**

WELCHE HACKER-TYPEN GIBT ES?

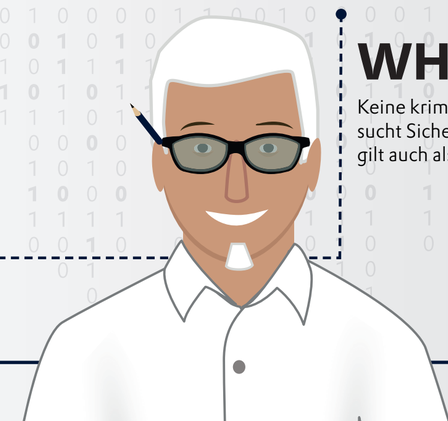
HACKER-TYPEN

BLACK HAT

Kriminelle Absichten,
Elite-Ausbildung,
Experte auf seinem Gebiet.

GREY HAT

Macht auf Sicherheitslücken aufmerksam, bewegt sich in einer legalen Grauzone.



WHITE HAT

Keine kriminelle Motivation,
sucht Sicherheitslücken,
gilt auch als Sicherheitsforscher.