rt-solutions.de
experts you can trust.

Cyberkriminalität
Panikmache oder Realität?

Dipl. Inform. Volker Jaenisch

Bonn, 15. Dezember 2022

Die rt-solutions.de…

Wer wir sind

Unsere Kunden

- AXA
- Bafin
- BASF
- Deutsche Bahn
- Douglas
- ERGO
- Generali
- Henkel
- Rentenbank
- REWE
- Siemens
- Telefonica
- …

Unser Fahrplan für heute

1. **Die Situation heute**
2. **So schützen sich Unternehmen**
3. **Für „Normalos“: Cyberrisiken als allgemeines Lebensrisiko?**

An „der Front“ ist die Hölle los

Zunehmendes Ziel: Industrieanlagen

WannaCry
Ransomware (Erpressungstrojaner)
75.000 betroffene Systeme in 100 Ländern

Yahoo
Benutzernamen und Passwörter
(MD5-verschlüsselt), ~1 Mrd. Benutzer

Sony Playstation Network
Kreditkartennummern ~77 Mio. Benutzern,
4 Wochen Ausfall, Schaden ~170 Mio. USD

Denial-of-Service Angriffe
…via Botnetz: Amazon, Mastercard, VISA, PayPal, Twitter, NYT,… => nicht erreichbar

Stuxnet
Erste „Cyberwaffe“ der Welt, Ziel: SCADA-Systeme (Siemens). Verbreitung via USB-Stick (autorun)

Havex-Angriff - Industriespionage
Remote-Access-Trojaner in Installationsroutinen von ICS- und SCADA Systemen

Cyber-Angriff auf Stahlwerk (Hochofen)
Phishing-Angriff via Emails, Ausfall einzelner Komponenten bis zum Kontrollverlust

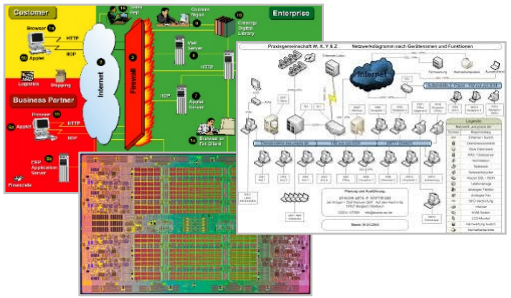
An „der Front“ ist die Hölle los

… und so kann das dann aussehen

Warum haben es die Angreifer so einfach?

Nur einige Beispiele

Komplexität der IT



Fehlende Verantwortlichkeiten

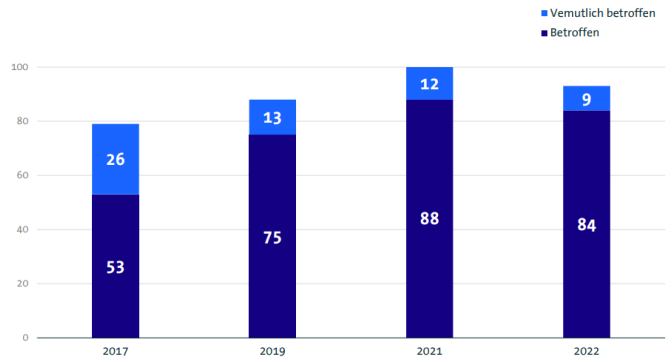
Fehlende Regeln, kein Budget

Benutzer – ohne Worte…

Ein paar Statistiken

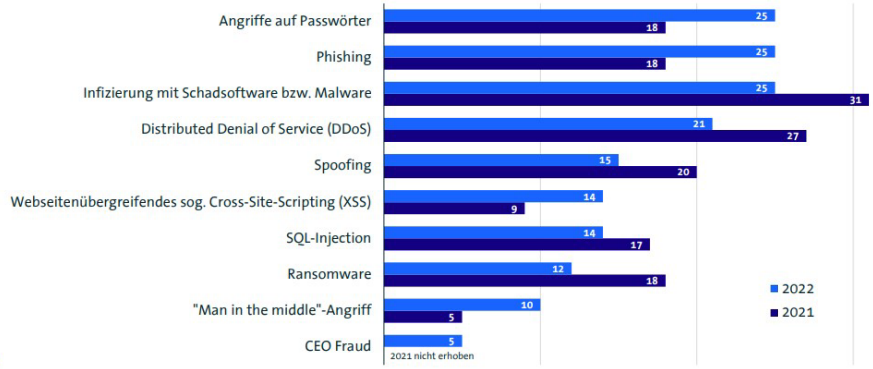
… und was wird im Cyberraum so angestellt?

Es erwischt fast alle…



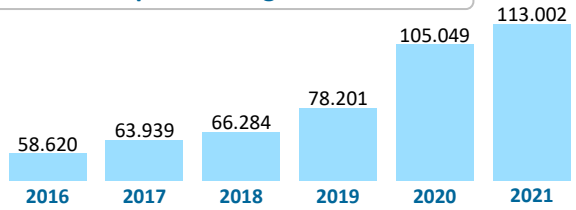
Quelle: Bitkom Research 2022 – 1.066 befragte Unternehmen

Angriffsarten der jeweils letzten 12 Monate



Quelle: Bitkom Research 2022 – 1.066 befragte Unternehmen

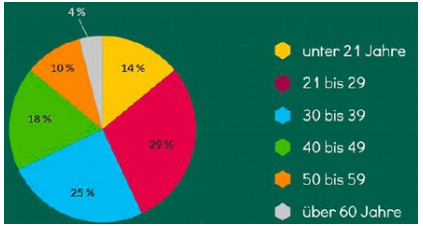
Fälle von Computerbetrug in Deutschland



Quelle: Statista 2022

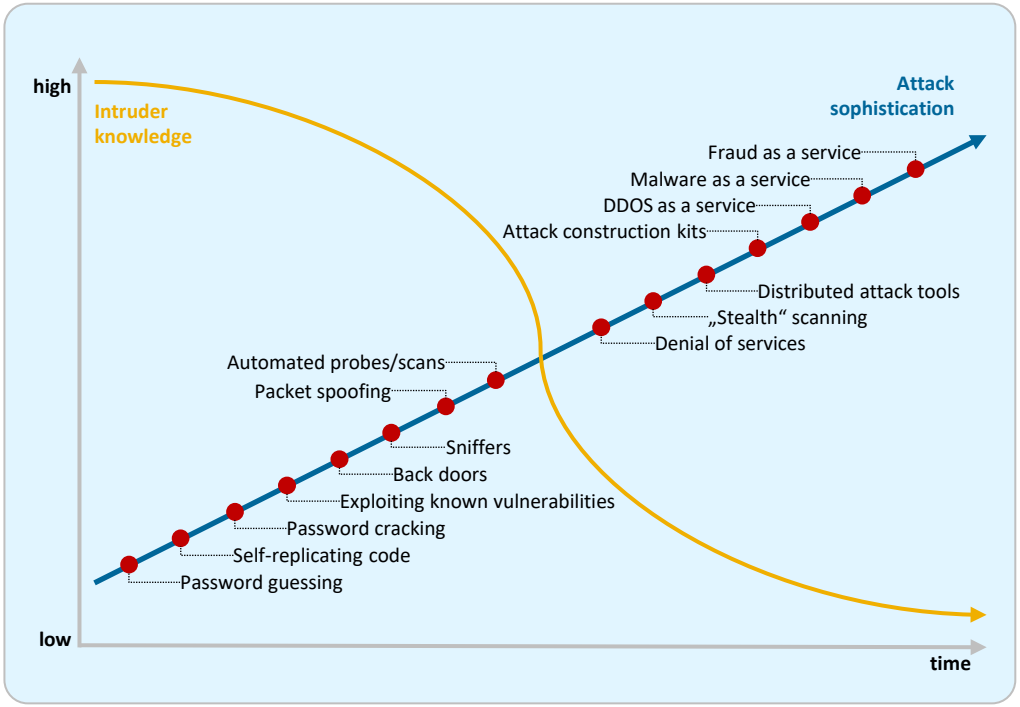
Die Angreifer

- 77% der Tatverdächtigen waren Männer
- 57% der Tatverdächtigen waren älter als 30 Jahre



Quelle: BKA 2015

Kompetenz der Angreifer



Das heißt…

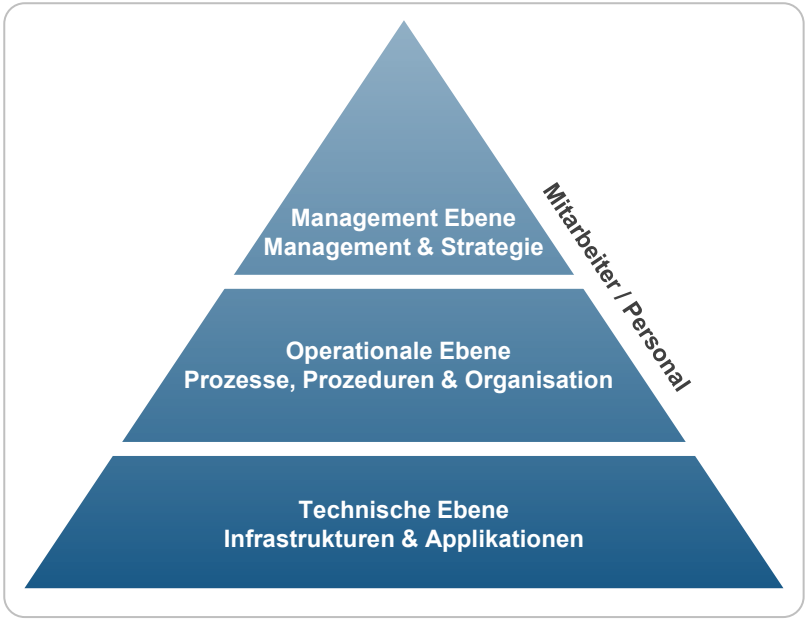
- Die Angriffe werden immer komplexer
- Die Angreifer werden immer „doofer“

Der Grund

- Wenige schlaue Köpfe erstellen Tools / Services
- Diese sind (einfach) im Internet zu finden

So schützen sich Unternehmen

Technik alleine ist keine Lösung



Sicherheit zur Chefsache machen

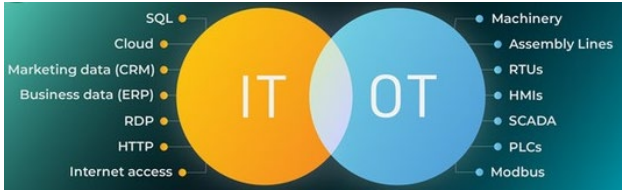
Operationale Sicherheit erhöhen

Technische IT-Sicherheit steigern

Personelle Sicherheit verbessern

Office IT und Operational IT

Was ist denn jetzt der Unterschied?

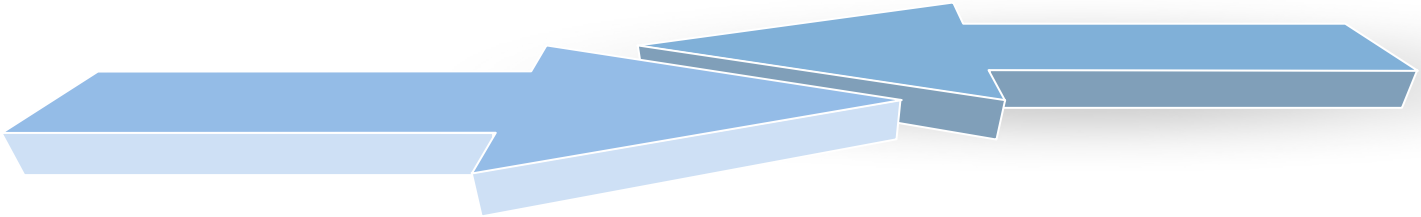


Office IT

- Hauptsächlich TCP/IP
- Fortgeschrittene Tools
- Standard Betriebssysteme
- Geplante Unterbrechungen sind akzeptabel
- Fokus auf Schutz der Daten,
  Security ist übergeordnet
- Prio: Confidentiality → Integrity → Availability

Operational IT

- Heterogene Protokolle
- Lange Lebensdauer der Komponenten – veraltet!
- Vielfältige Gerätetypen, proprietäre Systeme
- 24/7 Verfügbarkeit
- Fokus auf Aufrechterhaltung der Produktion,
  Security darf den Betrieb nicht beeinflussen
- Prio: Availability → Integrity → Confidentiality



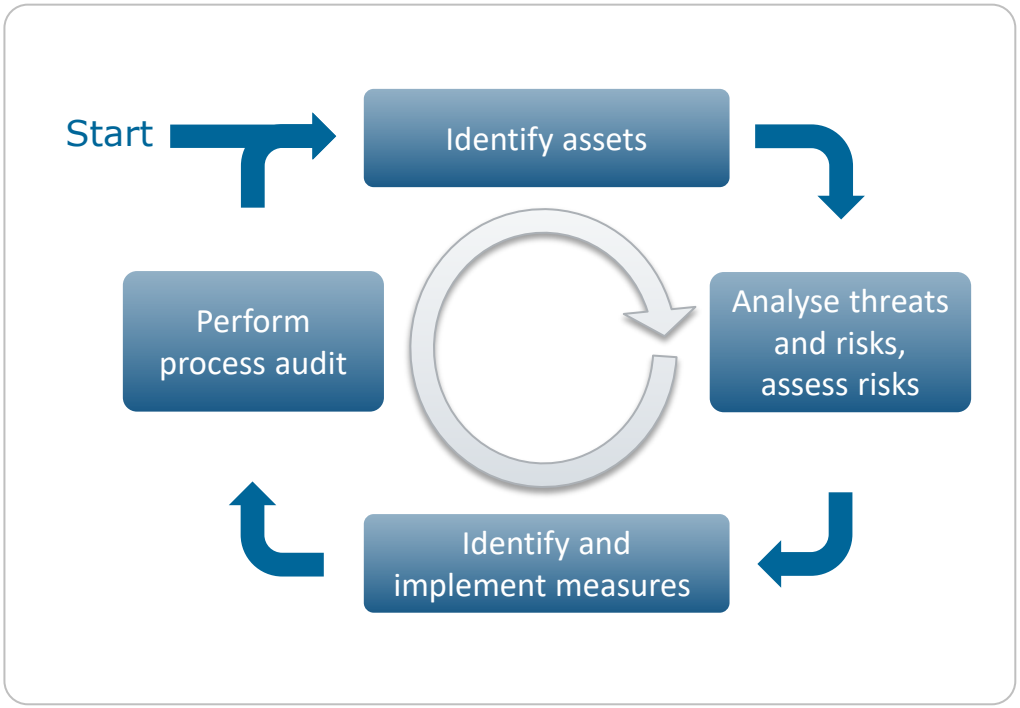
Office IT und Industrial IT

… und die Probleme mit den „klassischen“ Methoden

Office IT		Operational IT
Patch management	aber	Risiko der eingeschränkten Verfügbarkeit
Malware protection software	aber	Negativer Einfluss auf den Betrieb der Anlage
Network vulnerability scan	aber	Belastung des Netzes, Ausfall von Komponenten

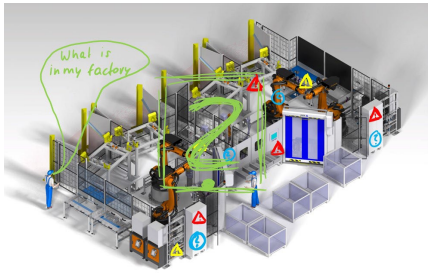
Best practice

Wie gehen Unternehmen jetzt vor?



Die Probleme bei OT

- Identifikation der Assets



- Weniger Kontrolle über die Komponenten – Hersteller / Integratoren haben das KnowHow
- Skills / Erfahrungen der beteiligten OT-Mitarbeiter im Zusammenhang mit Security

Und was ist jetzt die Konklusion?

Tatsache: Alle Unternehmen werden angegriffen – legt es ein Angreifer darauf an (und hat er ausreichend Ressourcen), dann wird er Erfolg haben. Es wird unterschieden zwischen

- einem Sicherheitsvorfall (Incident)
- einem (wirtschaftlichen) Schaden durch einen Sicherheitsvorfall (Breach)

Es gibt Unternehmen, die angegriffen werden und den Angriff

- gar nicht mitbekommen ODER
- (zeitnah) identifizieren und reagieren können

Das bedeutet

- Prävention ist wichtig. Die Systeme und Netzwerke sind systematisch zu schützen
- Detektion darf aber NICHT vernachlässigt werden: Intrusion Detection and Response – Sicherheitsvorfälle rechtzeitig identifizieren und richtig reagieren

Fazit

Es kann jeden erwischen – also auch Euer Unternehmen!

1. Angreifer haben es teilweise sehr einfach
2. Es passiert tatsächlich – keine Branche ist davor sicher
3. Cyberattacken haben zunehmend Industrieanlagen im Visier
4. Es gibt eine Vielzahl von Angriffsvektoren – (Spear-) Phishing ist sicherlich die problematischste
5. Neben präventiven Maßnahmen sind auch Intrusion Detection sowie die Reaktion auf Sicherheitsvorfälle besonders wichtig!

Cyberkriminalität – Panikmache UND Realität

Angriffe im täglichen Leben

In solche Situationen kommen wir alle mal!

- Auf dem Flughafen … der Akku ist schwach.
  Zum Glück gibt es eine **USB-Ladestation**
  - Und in der Zwischenzeit kann man sich im **Gratis-WLAN** die Zeit vertreiben
    - **Software-Updates** müssen sein – natürlich auch für Mobilgeräte.
      Wenn einen der IT-Support persönlich anschreibt, ist es wichtig
  - Vom **Lobby-PC** noch schnell die E-Mail mit dem Rückflugticket ausdrucken
- Zu Hause wartet eine Rechnung in der **Inbox** –
  schnell checken, bevor eine Mahnung kommt

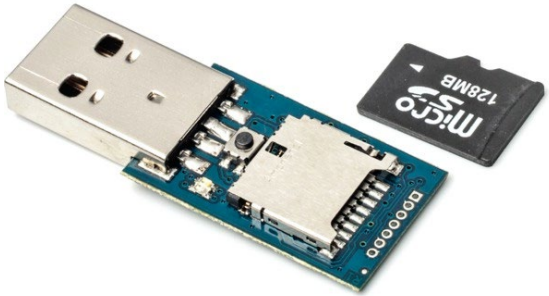
Diese Angriffe sind leicht nachzustellen und benötigen nichts aus der NSA-Trickkiste zur Durchführung

USB Rubber-Ducky

… ein USB-Stick kann auch eine Tastatur sein

Scenario

- Man bekommt einen tollen neuen USB-Stick als Werbegeschenk zugeschickt
- Der manipulierte USB-Stick simuliert eine Tastatur und lädt mit Windows-Kommandos Trojaner aus dem Internet nach
- Der Angreifer kann Daten lesen, den Laptop beliebig fernsteuern und als Wanze nutzen



Vielen Dank!