

TeleTrust-Auditorium (it-sa 2016)

Nürnberg, 19.10.2016

Wie kann Industrie 4.0 starten, wenn IT-Sicherheit 3.0 noch nicht gelöst ist?

Dr.-Ing. Thomas Sinnwell, CEO R&D
consistec Engineering & Consulting GmbH

Industrielle Revolution - Abgrenzung



"Unter **Industrie 4.0** versteht man
die intelligente Vernetzung von Produkten und Prozessen
in der industriellen Wertschöpfung."

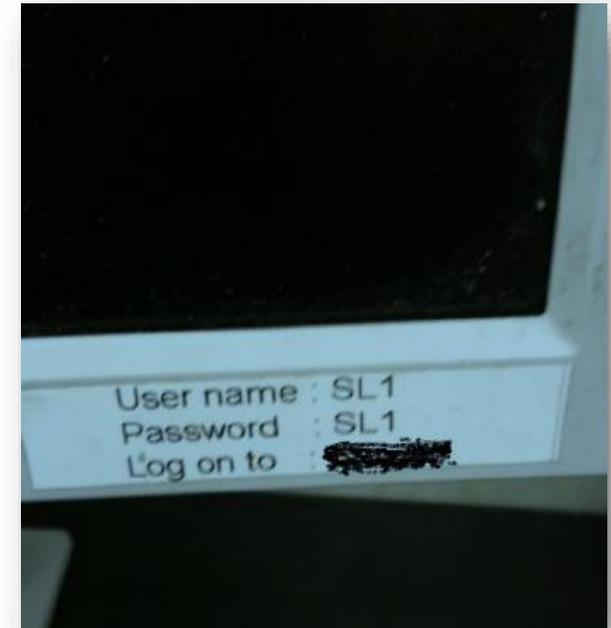
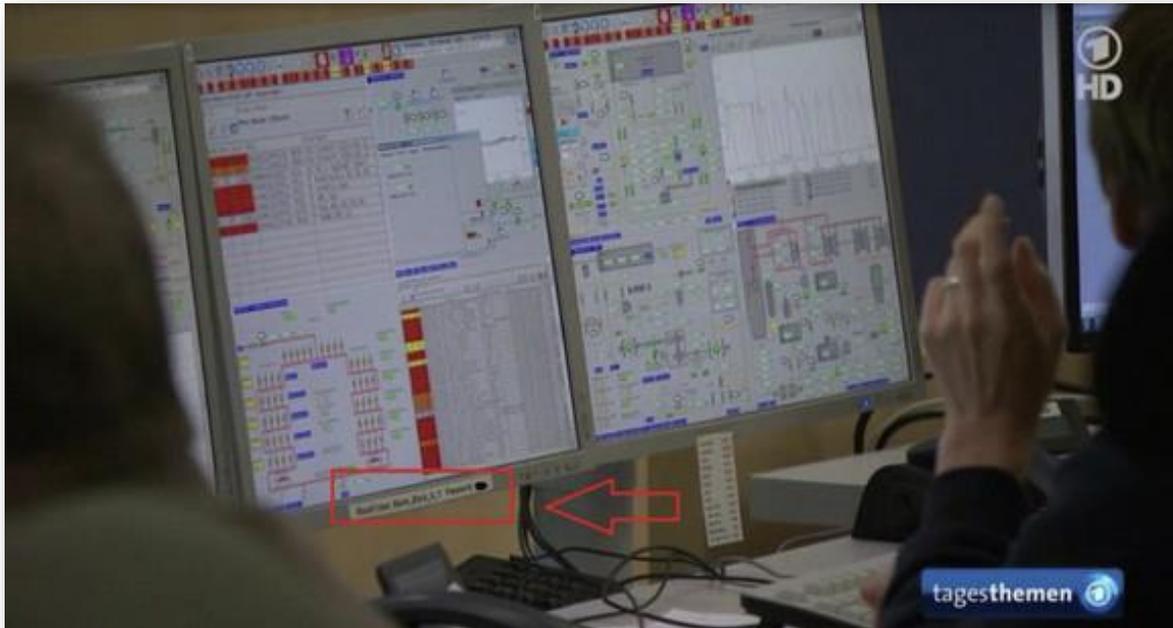
Quelle: BITKOM, Industrie 4.0 – Volkswirtschaftliches Potential für Deutschland, Studie, 2014

Handlungsfelder für den Weg zur digitalen Revolution:

- 1. Daten besser nutzen** → *Wartungsvorhersagen*
- 2. Fähigkeiten aufbauen** → *Datenanalyse*
- 3. Zugang zum Kunden sichern** → *Strategische Schnittstellen sichern*
- 4. Schneller werden** → *Two-Speed IT*
- 5. Datensicherheit erhöhen** → *Vorstandsagenda*

Quelle: McKinsey, Industry 4.0, Studie 2015

Real world findings:



Bildquelle: ARD - Tagesthemen

Security Topics	Business IT	Industrial IT
Lebensdauer	3 - 5 Jahre	5 - 20 Jahre
Patch-Management	oft	selten (Freigabe v. Anlagenhersteller erforderlich)
Änderungen	häufig	selten
Verfügbarkeit	akzeptabel	24 x 7
Sicherheitsbewusstsein	In der Regel gut	In der Regel schlecht
Physische Sicherheit	abgesichert, bemannt	großflächig, unbemannt
Virenschutz	sehr verbreitet	schwierig bis unmöglich

Security Topics

Business IT	Priorität	Industrial IT
Vertraulichkeit	1.	Sicherheit (Safety)
Integrität	2.	Verfügbarkeit
Verfügbarkeit	3.	Integrität
	4.	Vertraulichkeit



- ICS 3.0: Mischung aus alter Automatisierungstechnik und neuer, PC-basierter Infrastruktur
- **Früher:** "security through obscurity"
- **Heute:** vergleichbare Security-Risiken wie bei der Office-IT

Bildquelle: fotolia , 93312053

Top 10 ICS-Security Bedrohungen

(Quelle BSI)

Nr.	Top 10 2016
1	Social Engineering und Phising
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3	Infektion mit Schadsoftware über Internet und Intranet
4	Einbruch über Fernwartungszugänge
5	Menschliches Fehlverhalten und Sabotage
6	Internet-verbundene Steuerungskomponenten
7	Technisches Fehlverhalten und höhere Gewalt
8	Kompromittierung von Extranet und Cloud-Komponenten
9	(D)DOS Angriffe
10	Kompromittierung von Smartphones im Produktionsumfeld

Evolutionäre Handlungsfelder für den Weg zur digitalen Revolution:

1. Fähigkeiten aufbauen

- **Praktikable Konzepte für Security** in der Industrial IT entwickeln
- Industrie 4.0 Know-how in allen Unternehmensbereichen aufbauen

2. Datensicherheit erhöhen

- Bewusstsein schaffen, Risiken erkennen und bewerten, Sicherheitskonzepte erarbeiten
- Best Practice-Maßnahmen schrittweise umsetzen

3. Daten besser nutzen

- **Wirksamkeit** der ergriffenen Security-Maßnahmen **überprüfen**
- M2M, M2P

- Die IT ist nicht nur Akteur bei Industrie 4.0, vielmehr ist sie das prägende Fundament auf der die digitale Revolution stattfindet.
- Die Herausforderung dabei ist, bestehende Strukturen und Organisationen mit praktikablen IT-Security-Konzepten für die neuen Anforderungen aufzustellen.
- Da es keine 100-prozentige Sicherheit gibt, muss die Wirksamkeit der ergriffenen Maßnahmen mit einfach anwendbaren Werkzeugen überprüft werden können.

Vielen Dank für Ihre Aufmerksamkeit.



Dr.-Ing. Thomas Sinnwell
CEO FuE consistec GmbH