KPMG

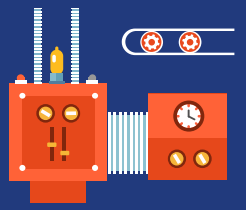
Komfort oder Katastrophe

IIoT-Security in der Welt von morgen

SECMGT-Workshop: IoT – ein Thema für den CISO?

29. März 2019

1 (I)IoT-Security: Status quo



2 IIoT-Security: Die größten Herausforderungen für Unternehmen

3 IIoT-Security: Die häufigsten Fehler in der Praxis

4 How-to: Der Weg zum sicheren IIoT-Device

5 The future is now: Zusammenfassung und Ausblick

KPMG in Deutschland

KPMG Cyber Security Expertise

Unsere Fokusbereiche

- Cyber resilience / BCM
- Cyber governance
- Cyber strategy & roadmap
- Privacy & data protection
- Cyber risk management

Strategy & governance

Security transformation

- Cloud / mobile / connected
- Industry 4.0 / ICS
- IOT / Digital
- Security transformation
- Identity & access mgmt.

- CERT / SOC / SIEM
- Penetration testing
- Advanced Cyber Defence
- Incident response
- Application security

Cyber defence services

Assessments & assurance

- ISO 27001 certification
- "KRITIS" / "IT-SiG"
- Cyber maturity assessments
- Privacy assessments
- 3rd party risk management

Unsere Standorte

>2.950
Mehr als 2.950 globae Cyber Security Experten

>200
Mehr als 200 Cyber Security Experten in Deutschland

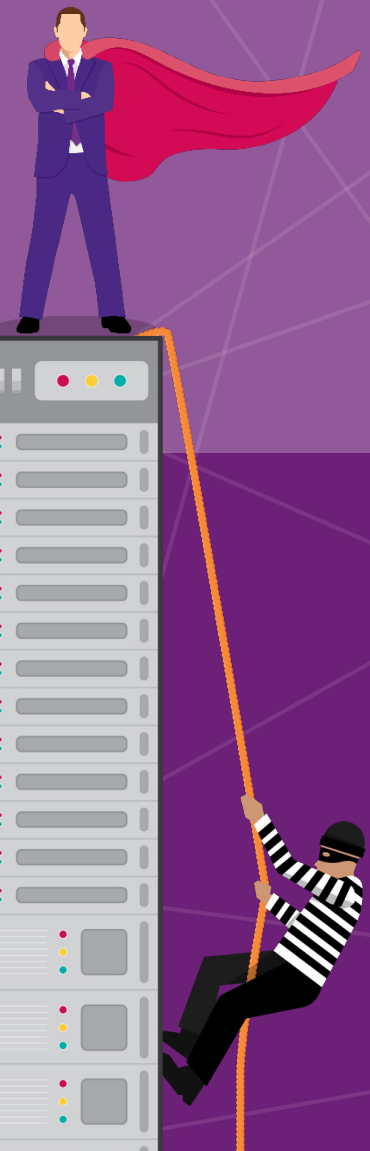
GLOBAL LEADER

>20
Mehr als 20 Jahre Cyber Security Erfahrung

>1000
Hunderte von erfolgreichen Cyber Security Projekten in den letzten Jahren

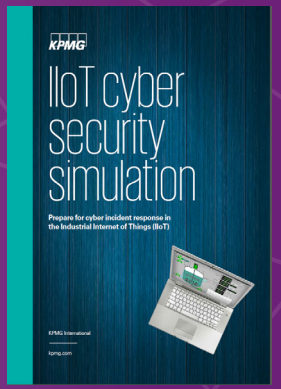
KPMG in Deutschland

Wir sind immer einen Schritt voraus, wenn es um Cyber Security geht



2017

2017



2017

2018

2018

2018

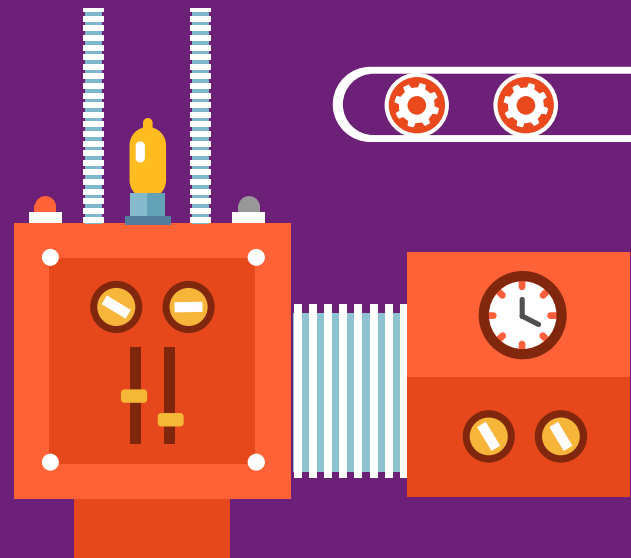
2018

2019

KPMG

1 | (I)IoT-Security:

Status quo



Gestern vs. Heute

(I)IoT-Security: Status quo

GESTERN

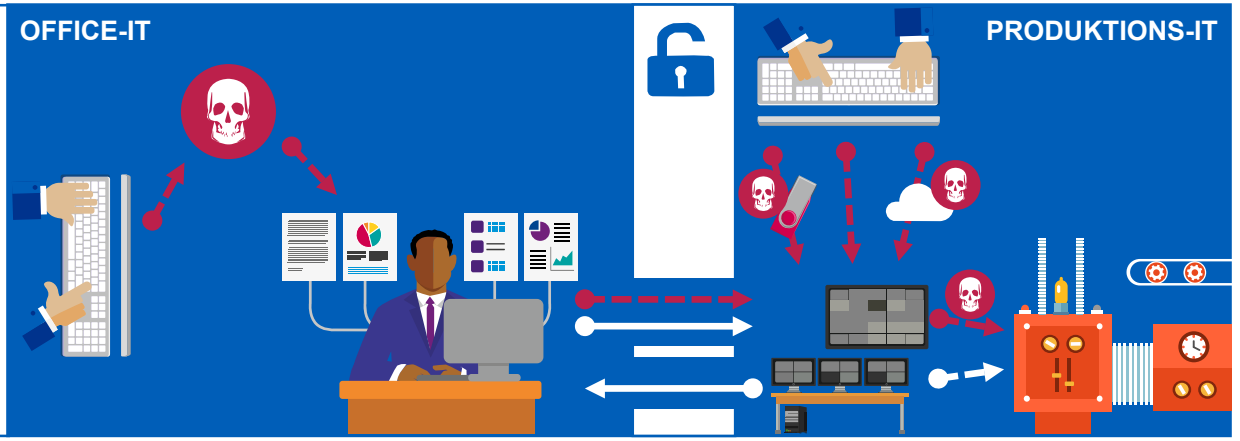
In der Vergangenheit waren Office-IT und Produktions-IT komplett getrennt (Air Gap).

Ein Cyber Angriff von innen oder außen war dadurch nahezu unmöglich.

HEUTE

Heute ist aus Effizienz- und Kostengründen (IoT, Industrie 4.0) eine fortschreitende Vernetzung von Produktionssystemen zu beobachten (u.a. Office-IT, Dienstleister).

Ein Cyber Angriff von innen oder außen wird dadurch wesentlich wahrscheinlicher.



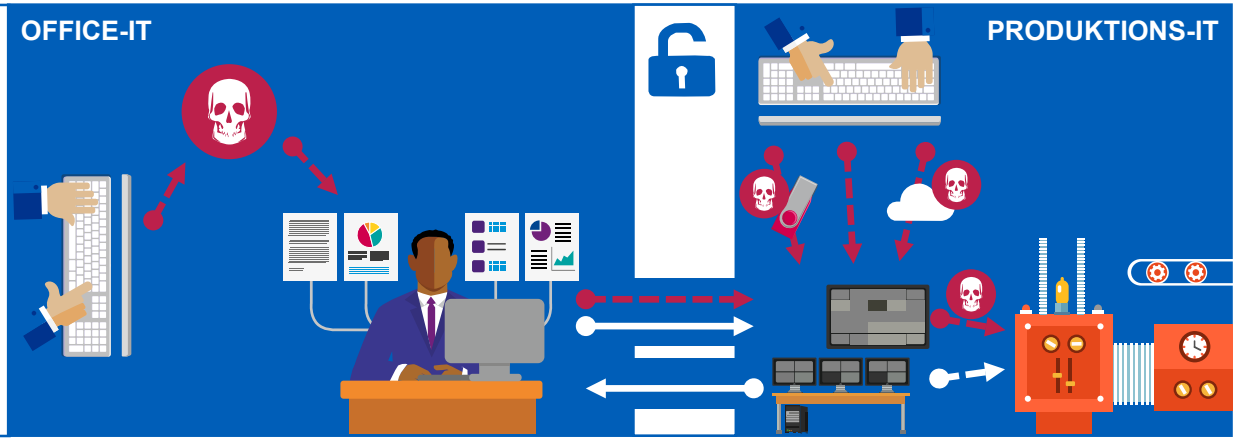
Heute vs. Morgen

(I)IoT-Security: Status quo

HEUTE

Heute ist aus Effizienz- und Kostengründen (IIoT, Industrie 4.0) eine fortschreitende Vernetzung von ICS-Systemen zu beobachten (u.a. Office-IT, Dienstleister).

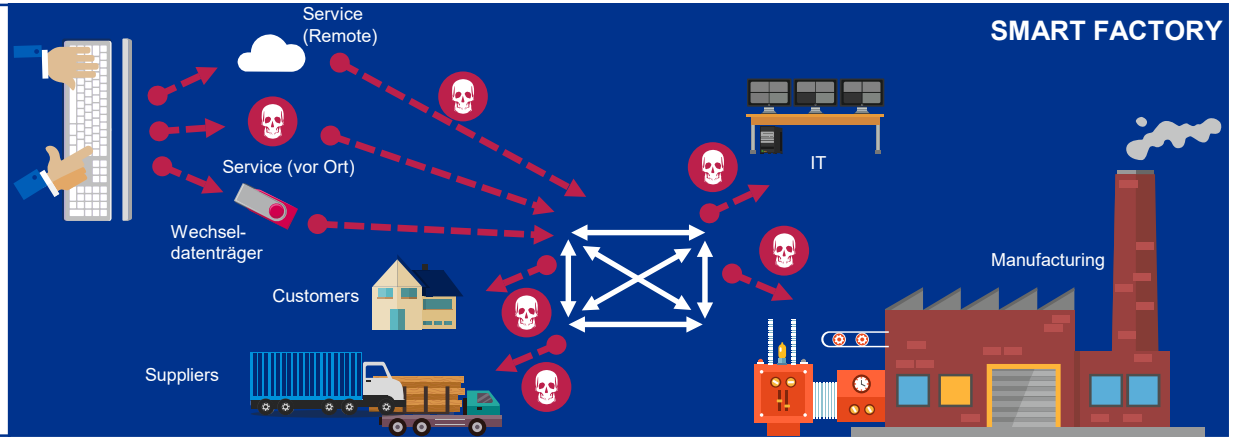
Ein Cyber Angriff von innen oder außen wird dadurch wesentlich wahrscheinlicher.



MORGEN

Morgen wird die Vernetzung aller Komponenten - vom Zulieferer bis hin zum Kunden - Realität sein.

Durch die vollkommene Vernetzung wird ein Cyber Angriff von innen oder außen erheblichere Auswirkungen auf die komplette Lieferkette haben.



Entwicklung der Geräte

(I)IoT-Security: Status quo

GERÄTE 31 MILLIARDEN 2018 [1]

5.4 Milliarden Gewerblich genutze IoT-Geräte mit einem jährlichen Anstieg von 24,4% (2013-2030)[1]

406 Millionen verwendete medizinische IoT-Geräte mit einem jährlichen Anstieg von 20,8% (2013-2030) [1]

GERÄTE 100 MILLIARDEN 2025 [2]

928 Millionen IoT-Geräte, die in der Automobilindustrie und Produktion eingesetzt werden, mit einem jährlichen Anstieg von 21,4% (2013-2030)[1]

5,9 Milliarden IoT-Geräte (Consumer) im Einsatz mit einem Jahresumsatz von 13,8% (2013-2030)[1]

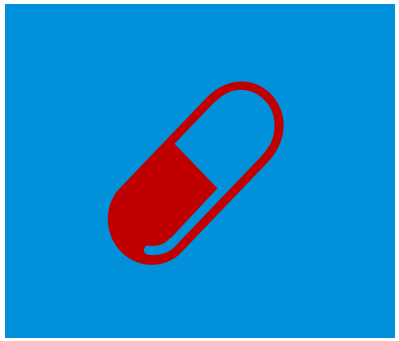
Die Anzahl der IoT-Geräte nimmt dramatisch zu und dementsprechend werden Cyber Attacken aggressiver, technisch ausgefeilter und sind besser organisiert.

[1] IHS Markit – IoT Trend Watch 2018

[2] BIS Research - Global Sensors in Internet of Things (IoT) Devices Market, Analysis & Forecast

The future is now: IoT-Geräte werden angegriffen

(I)IoT-Security: Status quo

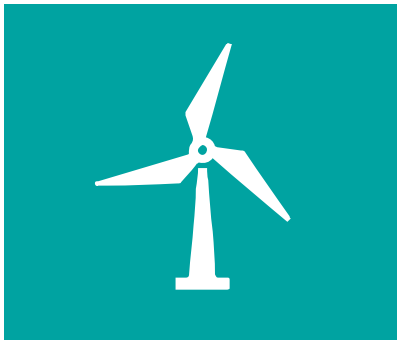


CONSUMER IOT ALS ANGRIFFSZIEL

- Ein Herzschrittmacher in den USA wies erhebliche Schwachstellen auf, welche dazu führen konnten die Batterien zu entleeren und unerwartete Impulse zu geben

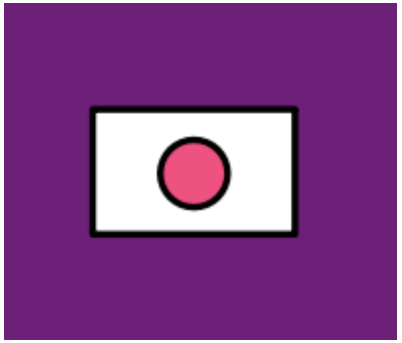
DDOS ANGRIFFE AUF SPORT EVENTS

- Das Champions League Finale 2018 in Kiev drohte aufgrund russischer DDoS Cyberangriffe auszufallen. Ein gehacktes IoT Netz wurde verwendet um das Event zu beeinflussen



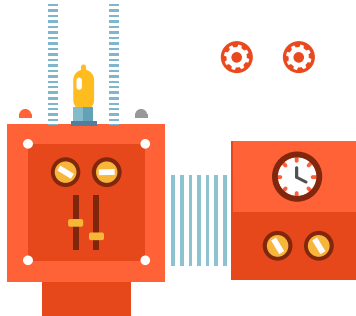
HACK AUF WINDTURBINEN

- Hacker übernehmen die Kontrolle über ein ganzes Netzwerk von Windkraftanlagen in einem US-Windpark mit einem IoT Modul für den Fernzugriff auf programmierbare Automatisierungssteuerungen



JAPAN HACKT IOT GERÄTE

- Die Regierung plant 200 Millionen IoT-Geräte zu hacken, die in Japan installiert sind
- IoT-Geräte gelten als eine große Bedrohung für die Olympischen Sommerspiele



KPMG

2 | IIoT-Security:

Die größten Herausforderungen für Unternehmen

Der Unterschied zwischen der IT und der OT

IIoT-Security: Die größten Herausforderungen für Unternehmen

Das Hauptziel eines industriellen Steuerungssystems ist die Verfügbarkeit und Funktionalität.

Schutzmaßnahmen	IT	Produktions-IT
Virenschutz	sehr beliebt	schwierig oder **unmöglich**
Life cycle	3-5 Jahre, regelmäßige Updates	10-25 Jahre, teilweise sehr alte Sicherheitsschwachstellen, teilweise ohne Sicherheitskonzept
Outsourcing	beliebt	**selten**
Patch management	Häufig (manchmal mehrmals am Tag)	Selten und **langsam** (Herstellerfreigabe erforderlich)
Change management	regelmäßig	selten oder **nie**
Real-time processing	Verzögerungen können (oft) toleriert werden.	**kritisch,** Maschinen müssen in Echtzeit arbeiten (ms sind wichtig).
Verfügbarkeit	Ausfallzeiten sind tolerierbar	**24/7/365** erforderlich
Security skills & awareness	relativ gut	Nur **geringes** oder **schwaches** Wissen
Security testing	sehr beliebt	**Hohe kritische, exzellente IKS-Kenntnisse sind erforderlich.**
Physische Sicherheit	in der Regel sicher und lokal zugänglich	Zugang meist entfernt, Einrichtungen oft unbemannt
Risko	**Datenverlust** und **Vertraulichkeit**	Verlust von **Menschenleben**, **Verfügbarkeit** und **Funktionalität** der Industrieanlage

Was sind die größten Herausforderungen?

IIoT-Security: Die größten Herausforderungen für Unternehmen

1 ORGANISATORISCH

KNOWHOW

BUDGET

ROLLEN & VERANTWORTLICHKEITEN

LIFE CYCLE MANAGEMENT

2 TECHNISCH

PATCH MANAGE-MENT

MONITORING

INVENTORY

MICRO-SEGMENTIERUNG

SKALIERUNG

SYNERGIEEFFEKTE

3 COMPLIANCE

RICHTLINIEN

Security by Design

GDPR

FRAMEWORKS

METHODEN

STANDARDS

ZERTIFIZIERUNG

KPMG

3 | IIoT-Security:

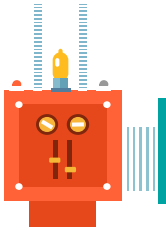
Die häufigsten Fehler in der Praxis

Was sind die häufigsten Fehler in der Praxis?

IIoT-Security: Die häufigsten Fehler in der Praxis

Management

- Unentschlossenheit darüber, wer für IIoT-Geräte und deren Sicherheit verantwortlich ist.
- Im Unternehmen fehlen Cyber Security Experten und Knowhow, um IIoT-Geräte sicher einzubinden.
- Spezifische Mitarbeitersensibilisierung und Schulung für IIoT fehlt.
- Schlechte Kommunikation zwischen Ingenieuren und Management



Technologie

- Bei der Entwicklung von IIoT-Geräten fehlt ein Security by Design Framework.
- Kritische Prozesse sind nicht vollumfänglich bekannt und werden nicht berücksichtigt.
- Unzureichende Netzwerksegmentierung bei IIoT-Geräten zum Schutz von kritischen Geräten.
- Sicherheits- und Firmware-Updates werden nicht regelmäßig installiert.

Cyber Sicherheit entwickelt sich für produzierende Unternehmen immer mehr vom reinen Kosten- zum Wertschöpfungsfaktor.

KPMG

4 | How-to:

Der Weg zum sicheren IIoT-Device

Top 10 Bedrohungen im IIoT-Umfeld

Der Weg zum sicheren IIoT-Device

1.  Unsichere Web Interfaces
2.  Unzureichende Authentifizierung / Autorisierung
3.  Unsichere Netzwerkdienste
4.  Fehlende Transportverschlüsselung
5.  Datenschutzmissbrauch
6.  Unsichere Cloud Interfaces
7.  Unsichere mobile Interfaces
8.  Unzureichende Sicherheitskonfiguration sfähigkeit
9.  Unsichere Software/Firmware
10.  Schlechte physische Sicherheit

First steps to IoT Security - Best Practices für Cyber Hygiene

Der Weg zum sicheren IIoT-Device

Eine umfassende Inventarisierung der Hard- und Softwareausstattung muss durchgeführt werden

Sichere Authentifizierungsmittel müssen verwendet verwendet (Sichere Passwörter, Lockout, 2FA…)

Netzwerkverschlüsselungen müssen verwendet werden (SSL/TLS) und die physische Sicherheit muss gewahrt werden

Eine klare Netzwerktrennung muss stattfinden und die Netzwerk- und Geräteaktivität sollten gemonitort bzw. gelogt werden

Regelmäßige Software und Firmware Updates über sichere Updatekanäle müssen implementiert werden

Lessons Learned: Wie man sichere IIoT Produkte entwickelt

Der Weg zum sicheren IIoT-Device

Modelling	Design	Zusätzliche Sicherheitsebenen
Definition der Bedrohungslandschaft und der Methodik	Design von Sicherheitskontrollen auf der Hardware	Sichere Aktualisierung und Authentifizierung
Entscheidung über die Programmiersprache	Implementierung der Kommunikationssicherheit	Sicheres Key Management
Berücksichtigung des Datenschutzes	Schutz von Schnittstellen	Protokollierungsmöglichkeiten
		Durchführung eines Security Review

KPMG

5 | The future is now:

Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

The future is now: Zusammenfassung und Ausblick

Cyber Security muss ein integraler Bestandteil des gesamten Produktlebenszyklus sein (u.a. Security bei Design).

Es muss ein verstärktes Zusammenspiel von Geräteherstellern, Maschinenintegratoren und Anlagenbetreibern geben.

Cyber Security entwickelt sich für produzierende Unternehmen immer mehr vom reinen Kosten- zum Wertschöpfungsfaktor.

Der Faktor Mensch ist einer der wichtigsten Faktoren für eine erfolgreiche Digitalisierung. Daher müssen relevante Skills im Unternehmen aufgebaut werden.

Die Welt der vernetzten Dinge entwickelt sich zu einem milliardenschweren Wachstumsmarkt – auch für Cyberkriminelle. Die Angriffe auf IoT-Geräte nehmen zu, werden aggressiver, technisch ausgefeilter und sind professionell organisiert.

KPMG

Vielen Dank

Ihr Kontakt

Thomas Gronenwald
Senior Manager, Cyber Security
T +49 151 1552 3309
tgronenwald@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Alfredstraße 277
45133 Essen

Sundeep Singh Kang
Assistant Manager, Cyber Security
T +49 151 5763 7805
sundeepsinghkang@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Alfredstraße 277
45133 Essen

www.kpmg.de/socialmedia

www.kpmg.de