OT Cyber Security

Von der Idee zur erfolgreichen Realisierung!

08. Oktober 2019
Daniel Rüth

EY 160 JAHRE in Deutschland

EY Building a better working world

Über uns

Daniel Rüth, Partner bei EY

- Verantwortet den Bereich OT/Industrial Cybersecurity in GSA bei EY
- Spezialisiert auf große Transformationsprogramme
- Mehr als 15 Jahre Erfahrung im Industrial Cyber Security Umfeld

Unsere Kompetenzzentren weltweit

Wir sind in allen geografischen Gebieten vertreten. Dies ermöglicht uns eine optimales und regionales Sourcing sowie schnellere Durchführung.

Cyber Security bei EY

GSA

180+ Experten

für Cybersicherheit, Informations-sicherheitsmanagementsysteme, GDPR, Cyber Threat Management und Datenforensik und **7200+ Experten weltweit**

Weltweit

12 Security Zentren

für Managed Security Services, Incident Response, Threat Intelligence und Penetration Testing.

Weltweit

International führend

Quelle: The Forrester Wave™: Information Security Consulting Services, Q1 2016, Forrester Research, Inc. Jan, 2016

Bestandsaufnahme und die größten Cyberrisiken in der Fertigung

Ist unsere IT/OT Archi-tektur noch zeitgemäß?

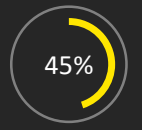
20.000 Lücken gefunden!
Was nun?

Wie soll unsere Digitalisierung und Cyberstrategie aussehen?

Zu-nehmende Anzahl an Cyber Angriffen

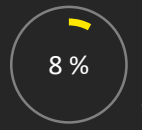
Wie sind wir im Vergleich zu unseren Markt-begleitern aufgestellt? Welche Maßnahmen sind notwendig?

Kernzahlen & Risiken



Nur 45% von Unternehmen haben den **„Schutz vor Cyber-Bedrohungen“** in ihre **Unternehmens-strategie** aufgenommen

38% von Unternehmen glauben, dass sie einen **komplexen Cyberangriff** nicht bemerken würden



Nur 8 % von Unternehmen verfügen über **zufriedenstellende Informationssicherheits-funktionen**

Risiko #1:
Nicht alle OT-Systeme sind bekannt

Risiko #2:
Rollen und Verantwortlichkeiten sind nicht definiert

Risiko #3:
Fehlendes betriebliches Kontinuitätsmanagement (Disaster Recovery)

Risiko #4:
Mangelhafte OT-Sicherheitsarchitektur

Risiko #5:
Mangelhaftes Monitoring (z. B. Anomalien in der Produktion)

Risiko #6:
Unklares Drittanbieter-Management (z. B.: Fernzugriff)

!

Die Digitalisierung ermöglicht neue Chancen, jedoch auch neue Risiken, insbesondere Cyberrisiken.

Eine erprobte Roadmap ist notwendig, um ein OT Projekt erfolgreich zu Realisierung!

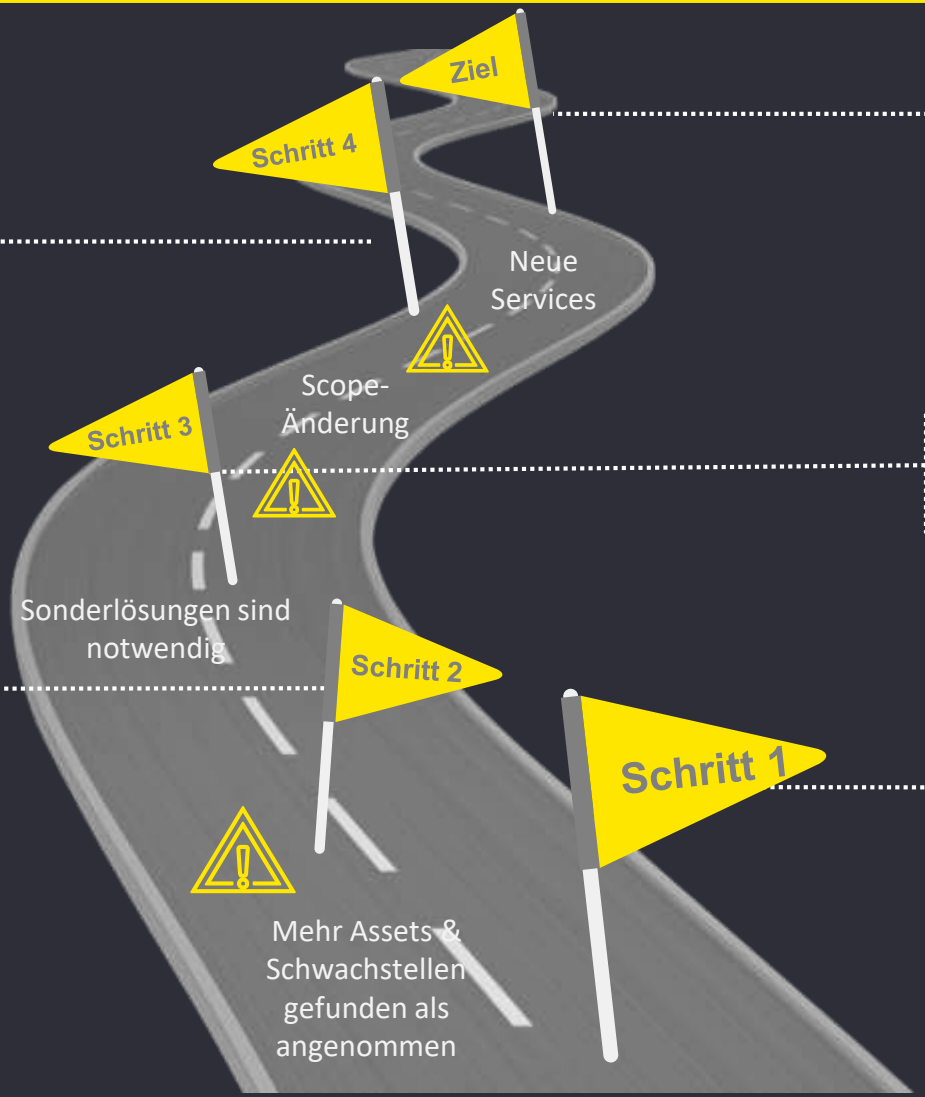
Roadmap zur erfolgreichen Realisierung eines OT-Projekts

Globaler Rollout

- Einführung von Services an allen Standorten
- Anwendung der Erkenntnisse aus den Piloten
- Integration mit SOC
- Datenqualität gewährleisten
- Scope prüfen
- Regeln wie „neues“ Inventar betrachtet werden soll
- IT/OT Organisationmodell optimieren
- Betrachtung von Spezialfällen

Globales OT Cyber Security Programm

- Aufsetzen eines IT & Automation OT Projekts
- Festlegung des Sicherheitslevels
- Umfang, Investitionsbedarf und Laufzeit festlegen
  - Entwicklung eines globales OT-Sicherheitsframework, eines OT Security Governance- und Betriebsmodell
  - Risikomanagement, Sanierungsplanung und technische Umsetzung



Übergabe an BAU

- Prozesse optimieren
- Hardening-Aktivitäten festlegen
- Neue Rollen definieren und trainieren
- Lifecycle von Hardware und Prozessen definieren

Pilotlösung

- Auswahl der richtigen Piloten
- Entwicklung des Proof of Concepts
- Ausrollen und Überprüfung des PoC bei den Piloten
- Dienste/Anwendungen implementieren und testen

OT Security Vorabbewertung

- Auswahl der Standorte für Hypothesen Bewertung
- Auswahl und Integration der Stakeholder
  - Technische und organisatorische Überprüfung
  - Identifizierung von Hauptrisiken
  - Priorisierung der notwendigen Aktivitäten

Zur erfolgreichen Umsetzung muss folgendes sichergestellt sein

Verfügbarkeit der Mitarbeiter

Verfügbarkeit der richtigen Mitarbeiter und Verantwortlichen zur richtigen Zeit am richtigen Ort.in den Werken

Buy in der Standorte

Buy-in und Integration der Standorte in die Planung und Umsetzung

Sicherstellung von Wartungsfenstern

Gewährleistung von Wartungsfenstern zur Umsetzung

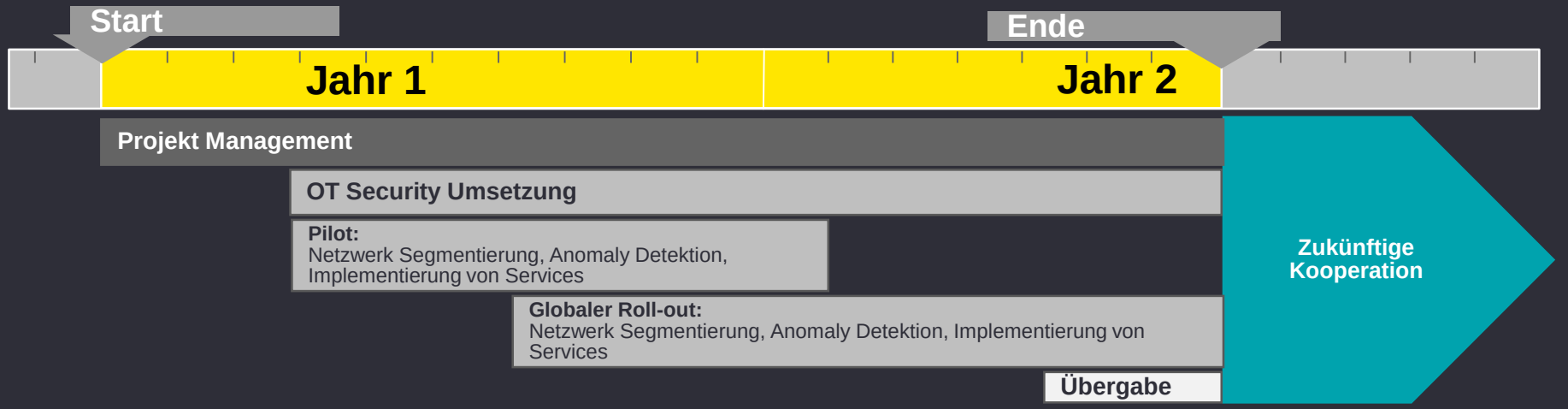
Akzeptanz von IT und OT

Akzeptanz und Synergie zwischen der IT- und OT-Abteilung

Gewährleistung von Datenqualität

Hohe Datenqualität

Überwachung von Budget, Scope und Zeit



Key Takeaways

Integrieren Sie die Stakeholder, die Standorte und die internen Organisation in das Programm. Übersetzen Sie OT <> IT

Stellen Sie sicher, dass das OT Cyber Security Programm eine gemeinsame Initiative von IT und Automation/Engineering ist

Achten Sie auf die Qualität der erhobenen Daten und nutzen sie soweit möglich in der OT erprobte Tools

Stellen Sie sicher, dass maßgebliche architekturelle OT/IT Entscheidungen getroffen und nicht verschoben werden

Setzen und kommunizieren Sie ein klares und messbares Ziel für das OT Security Remediation Programm

EY | Assurance | Tax | Transactions | Advisory

About the global EY organization
The global EY organization is a leader in assurance, tax, transaction and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the capital markets and in economies the world over. We are ideally equipped for this task — with well trained employees, strong teams, excellent services and outstanding client relations. Our global purpose is to drive progress and make a difference by *building a better working world* — for our people, for our clients and for our communities.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity's acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

In Germany, EY has 20 locations. In this publication, "EY" and "we" refer to all German member firms of Ernst & Young Global Limited.

ABC JJMM-123
ED None

ey.com/de