IT-SICHERHEITS-MANAGEMENT

für Industrie 4.0

AUFTAKT OBERFRANKEN 4.0

Dipl.-Kffr. Olga Bürger

13.10.2016

Themenschwerpunkt zu Industrie 4.0

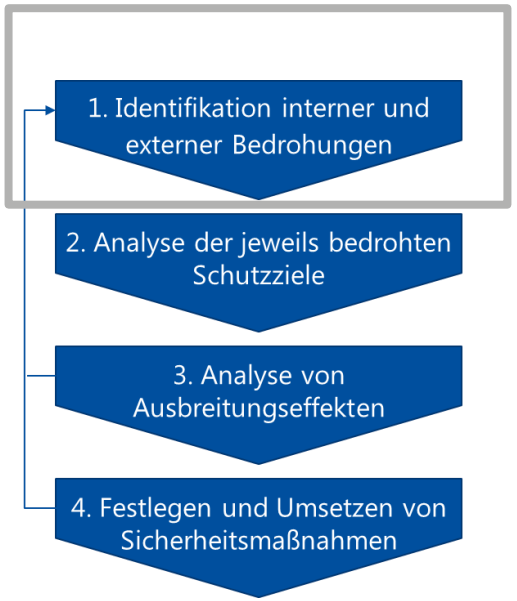
IT-Sicherheitsmanagement für Industrie 4.0

Inhalt des Teilprojektes in Oberfranken 4.0

Entwicklung eines Frameworks zur Einführung bzw. Verbesserung eines IT-Sicherheitsmanagements im Industrie-4.0-Kontext

Demonstration für die Anwenderfabrik 4.0

- Aufzeigen der Top-Bedrohungen für IT-Infrastruktur
- Live Demo: Smartphone vs. Demonstrator (frühestens Herbst 2017)
- Schnellcheck der IT-Sicherheit (5-Minuten-Risikoanalyse-App mit geleitetem Interview)



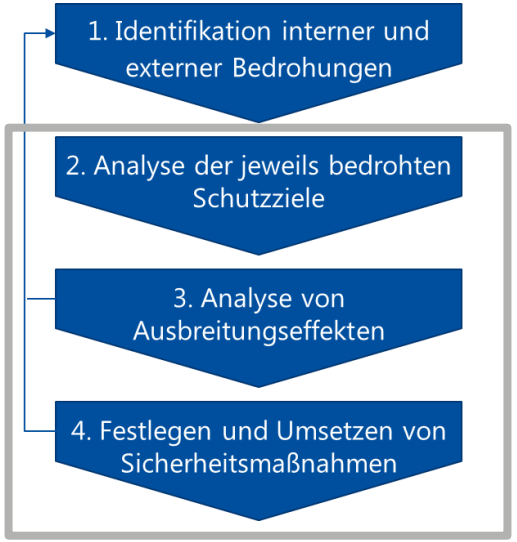
Wissenstransfer der Ergebnisse in die Unternehmen

_ Show Cases und Workshops in der Anwenderfabrik

_ Ermittlung eines Reifegrades des IT-Sicherheitsmanagements (bspw. durch Checkliste)

_ Risikobewertung (bspw. Scoring Modelle)

_ Roadmap für Einführung / Verbesserung des IT-Sicherheitsmanagements



Potenziale für Unternehmen

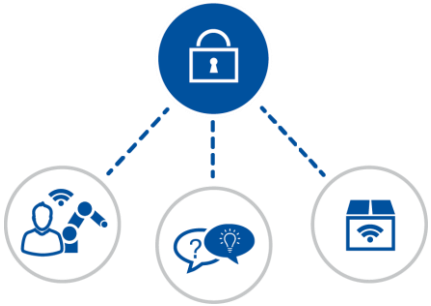
_ Systematische Risikoidentifizierung (insb. frühzeitige Erkennung neuer Risiken)

_ Unternehmensspezifische Risikoanalyse

_ Ableitung von Gegenmaßnahmen

_ Umsetzung von Gegenmaßnahmen

_ Integriertes IT-Sicherheitsmanagement



VIELEN DANK FÜR DIE AUFMERKSAMKEIT

FRAGEN – ANTWORTEN – DISKUSSION

AUFTAKT OBERFRANKEN 4.0

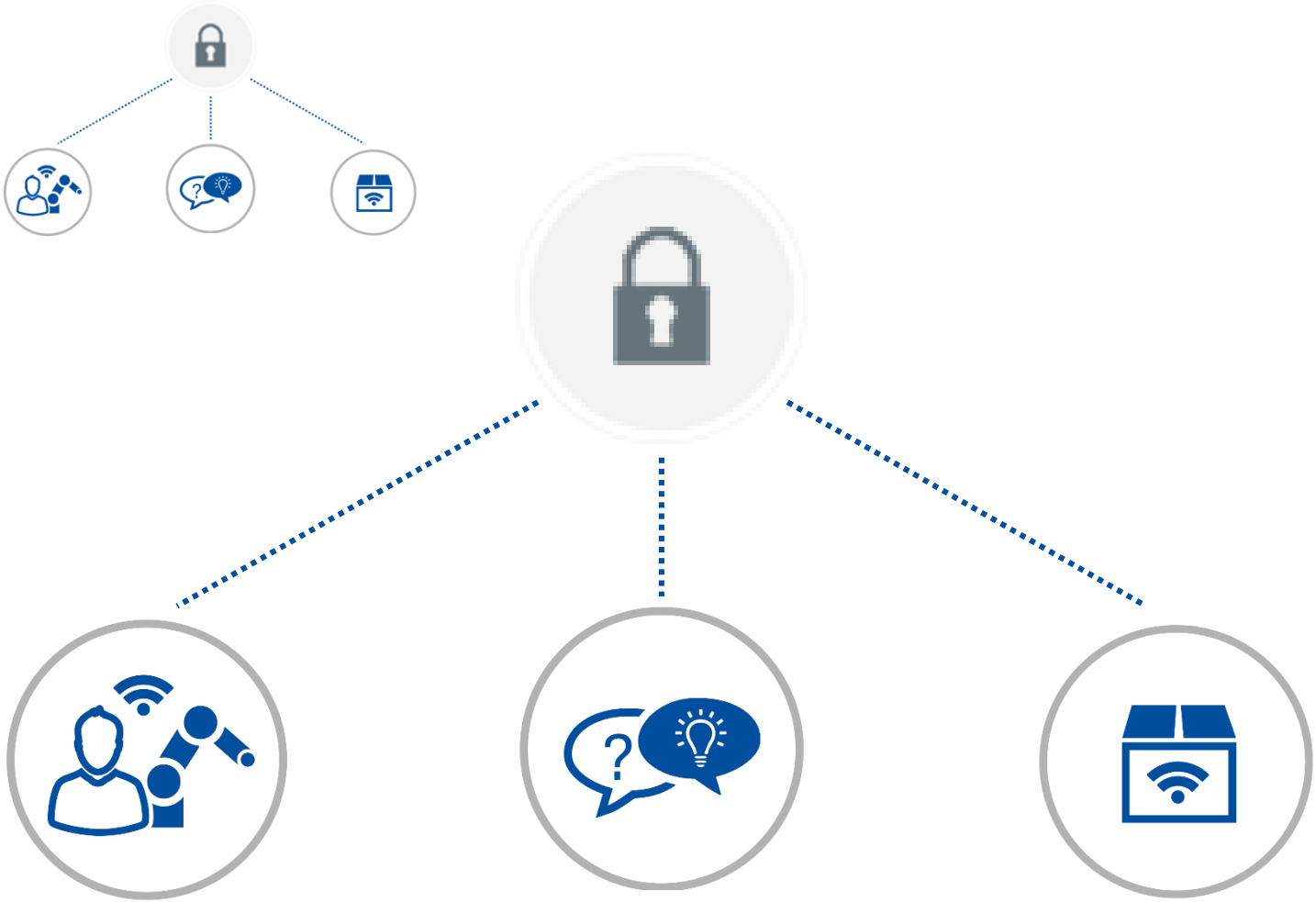
Dipl.-Kffr. Olga Bürger

13.10.2016

Quellen

- Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2014, BSI – CS 005, Bonn 2014
- Hertel, M. (2015). Risiken der Industrie 4.0–Eine Strukturierung von Bedrohungsszenarien der Smart Factory. HMD Praxis der Wirtschaftsinformatik, 52(5), 724-738.

BackUp



TOP-BEDROHUNGEN

INDUSTRIAL CONTROL SYSTEM SECURITY MANAGEMENT

1) Infektion mit Schadsoftware über Inter-/Intranet
Durch die unternehmensübergreifende Vernetzung sind ICS für Angreifer über eine Vielzahl externer Systeme indirekt erreichbar.

2) Einschleusen von Schadsoftware über externe Hardware
Durch den Einsatz externer, möglicherweise infizierter Hardware können unternehmenseigene Systeme kompromittiert werden.

3) Social Engineering
Durch das Ausnutzen menschlicher Eigenschaften (Angst, Respekt…) können sich Angreifer Zugang zu sensiblen Daten verschaffen.

4) Menschliches Fehlverhalten, Sabotage
Häufig verschulden nicht technische Mängel, sondern menschliches Fehlverhalten das entstehen massiver Sicherheitslücken.

5) Einbruch über Fernwartungszugänge
Über für Wartungszwecke eingerichtete externe Zugänge zu ICS können Angreifer weitgehende Kontrolle über das System erlangen.

Quelle: BSI (2014)

VORGEHEN FÜR AUSGEWÄHLTE KONSORTIALPARTNER

INDUSTRIAL CONTROL SYSTEM SECURITY MANAGEMENT

1. Identifikation interner und externer Bedrohungen

Welche Bedrohungen (intern und extern) können Ursachen von Sicherheitsrisiken sein?

2. Analyse der jeweils bedrohten Schutzziele

Welche Schutzziele sind bei welchen Akteuren und Objekten bedroht? Wie hoch ist der potenzielle Schaden?

3. Analyse von Ausbreitungseffekten

Sind durch die Bedrohung weitere Schutzziele bei anderen Akteuren oder Objekten bedroht oder entstehen neue Bedrohungen?

4. Festlegen und Umsetzen von Sicherheitsmaßnahmen

Welche Maßnahmen müssen ergriffen werden, damit Sicherheitsrisiken erkannt, verhindert und Beeinträchtigungen beseitigt werden können?

Quelle: Hertel (2015)

ERGEBNISSE ANWENDERFABRIK UND WISSENSTRANSFER

INDUSTRIAL CONTROL SYSTEM SECURITY MANAGEMENT

1. Identifikation interner und externer Bedrohungen
   - Top-ICS-Bedrohungen
   - Live Angriff: Smartphone – Demonstrator (frühestens Herbst 2017)
2. Analyse der jeweils bedrohten Schutzziele
   - Schnellcheck ICS-Sicherheit (5-Minuten-Risikoanalyse-App auf einem iPad oder auf einem Smartphone)
3. Analyse von Ausbreitungseffekten
   - Reifegrad des ICS-Sicherheitsmanagements (Checkliste)
   - Risikobewertung (Scoring Modelle)
4. Festlegen und Umsetzen von Sicherheitsmaßnahmen
   - Roadmap für Einführung / Verbesserung des ICS-Sicherheitsmanagements

Bedeutendste Bedrohungen für Industrial Control Systems (ICS)

1) Infektion mit Schadsoftware über Inter-/Intranet

Durch die unternehmensübergreifende Vernetzung sind ICS für Angreifer über vielerlei Systeme auch indirekt erreichbar.

Ursachen:

- Schwachstellen in anderen, vernetzten Systemen
- Angriffe über die Website des Unternehmens

Maßnahmen:

- Segmentierung der Netze durch Firewalls und VPN-Lösungen
- Regelmäßiges, zeitnahes Updaten der Betriebssysteme
- Überwachung von Logfiles

2) Einschleusen von Schadsoftware über externe Hardware
3) Social Engineering
4) Menschliches Fehlverhalten, Sabotage
5) Einbruch über Fernwartungszugänge

Bedeutendste Bedrohungen für Industrial Control Systems (ICS)

1) Infektion mit Schadsoftware über Inter-/Intranet
2) Einschleusen von Schadsoftware über externe Hardware

Durch den Einsatz externer, möglicherweise infizierter Hardware können unternehmenseigene Systeme kompromittiert werden.

Ursachen:

- Verwendung privater, infizierter Wechseldatenträger
- Nutzung betriebsfremder Notebooks im ICS-Netz

Maßnahmen:

- Etablierung technischer Vorgaben und Kontrollen
- Einrichtung von Quarantänenetzen für externe Rechner
- Inventarisierung zugelassener Wechseldatenträger

3) Social Engineering
4) Menschliches Fehlverhalten, Sabotage
5) Einbruch über Fernwartungszugänge

Bedeutendste Bedrohungen für Industrial Control Systems (ICS)

1) Infektion mit Schadsoftware über Inter-/Intranet
2) Einschleusen von Schadsoftware über externe Hardware
3) Social Engineering

Durch das Ausnutzen menschlicher Eigenschaften (Angst, Respekt…) können sich Angreifer Zugang zu sensiblen Daten verschaffen.

Ursachen:

- Pishing-Angriffe verschaffen Angreifern Zugang zu persönlichen/ sensiblen Daten mit Hilfe gefälschter Nachrichten

Maßnahmen:

- Zielgruppenspezifisches Security-Awarenesstraining
- Erstellung und Durchsetzung von Sicherheitsrichtlinien
- Nutzung technischer, autom. Sicherheitsmechanismen

4) Menschliches Fehlverhalten, Sabotage
5) Einbruch über Fernwartungszugänge

Bedeutendste Bedrohungen für Industrial Control Systems (ICS)

1) Infektion mit Schadsoftware über Inter-/Intranet
2) Einschleusen von Schadsoftware über externe Hardware
3) Social Engineering
4) Menschliches Fehlverhalten, Sabotage

Häufig verschulden nicht technische Mängel, sondern menschliches Fehlverhalten das entstehen massiver Sicherheitslücken.

Ursachen:

- Unautorisierte Installation und Gebrauch von Soft-/Hardware
- Fehlkonfiguration sicherheitsrelevanter Komponenten

Maßnahmen:

- Veranstaltung von Qualifizierungs-/Fortbildungsseminaren
- Automatische Überwachung von Systemkonfigurationen
- Deaktivierung des Internetzugangs produktionsnaher Systeme

5) Einbruch über Fernwartungszugänge

Bedeutendste Bedrohungen für Industrial Control Systems (ICS)

1) Infektion mit Schadsoftware über Inter-/Intranet
2) Einschleusen von Schadsoftware über externe Hardware
3) Social Engineering
4) Menschliches Fehlverhalten, Sabotage
5) **Einbruch über Fernwartungszugänge**

Über für Wartungszwecke eingerichtete externe Zugänge zu ICS können Angreifer weitgehende Kontrolle über das System erlangen.

Ursachen:

- Mangelnde Authentisierung & Autorisierung
- flache Netzhierarchien

Maßnahmen:

- Nutzung ausreichender Authentisierungsverfahren
- Hinreichend granulare Netzwerksegmentierung
- Protokollierung von Fernzugriffen