TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

"Technische Umsetzung einer Sicherheitsrichtlinie in einer Produktionsumgebung – Fallbeispiel"

Olaf Mischkovsky (CISSP, CCSK, TSO Security Specialist EMEA Central)
Symantec

"Technische Umsetzung einer Sicherheitsrichtlinie in einer Produktionsumgebung – Fallbeispiel"

Olaf Mischkovsky CISSP, CCSK
TSO Security Specialist EMEA Central

Olaf Mischkovsky
CISSP, CCSK

olaf_mischkovsky@symantec.com

0049 172 36 49 284

Mehr als 20 Jahre Erfahrungen in IT Security

7 Jahre als Senior Security Consultant

12 Jahre bei Symantec

Mitarbeit im Arbeitskreises FA 5.22 (VDI 2182 Richtlinie – Industrial Security)

Security PR und Pressesprecher für Symantec

Operation CLEAVER

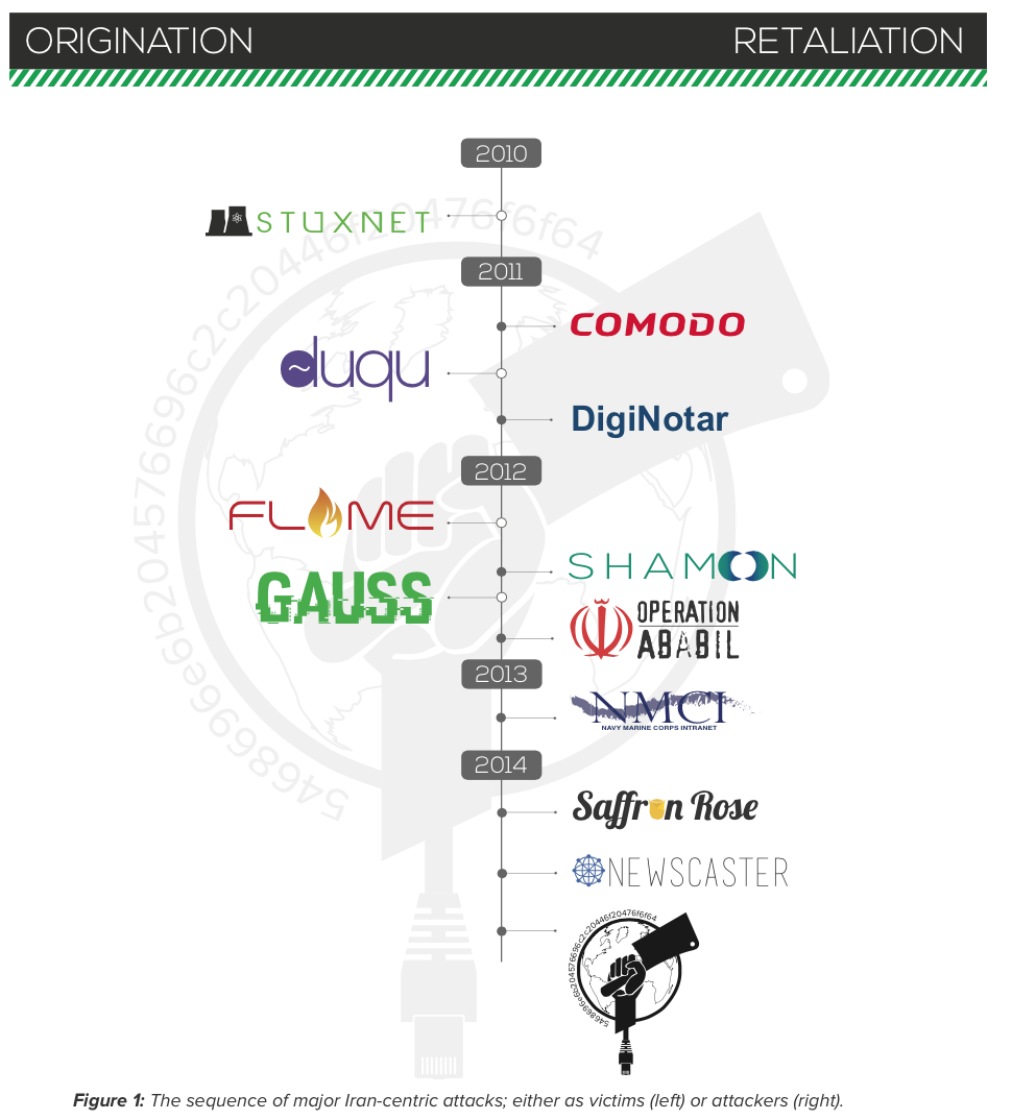


Figure 1: *The sequence of major Iran-centric attacks; either as victims (left) or attackers (right).*

Quelle: Cylance_Operation_Cleaver_Report.pdf

Zwei Welten – Große Unterschiede

Business Netzwerk

1.) Vertraulich
2.) Integrität
3.) Verfügbarkeit

Produktions Netzwerk

1.) Verfügbarkeit
2.) Integrität
3.) Vertraulichkeit

… werden allerdings auch immer stärker eingefordert …

Richtlinien

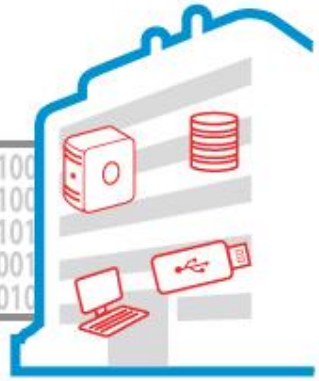
Regulierende Behörden

31. Juli 2014 05:15 Cybersicherheit

Bosch versichert sich gegen Hacker-Attacken

Externe Bedrohung

Interne Bedrohung



Der Elektronikkonzern Bosch ist das erste Unternehmen, das sich gegen Schäden aus Cyberangriffen im dreistelligen Millionenbereich versichert hat. Bis vor Kurzem war eine solche Deckungssumme unvorstellbar.

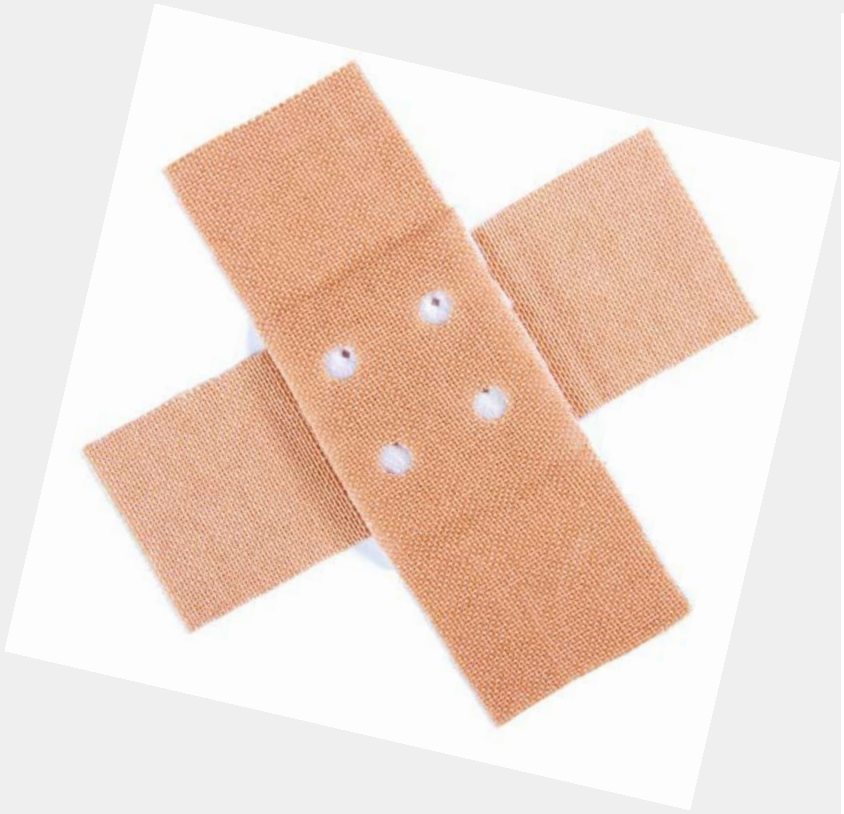
ANZEIGE

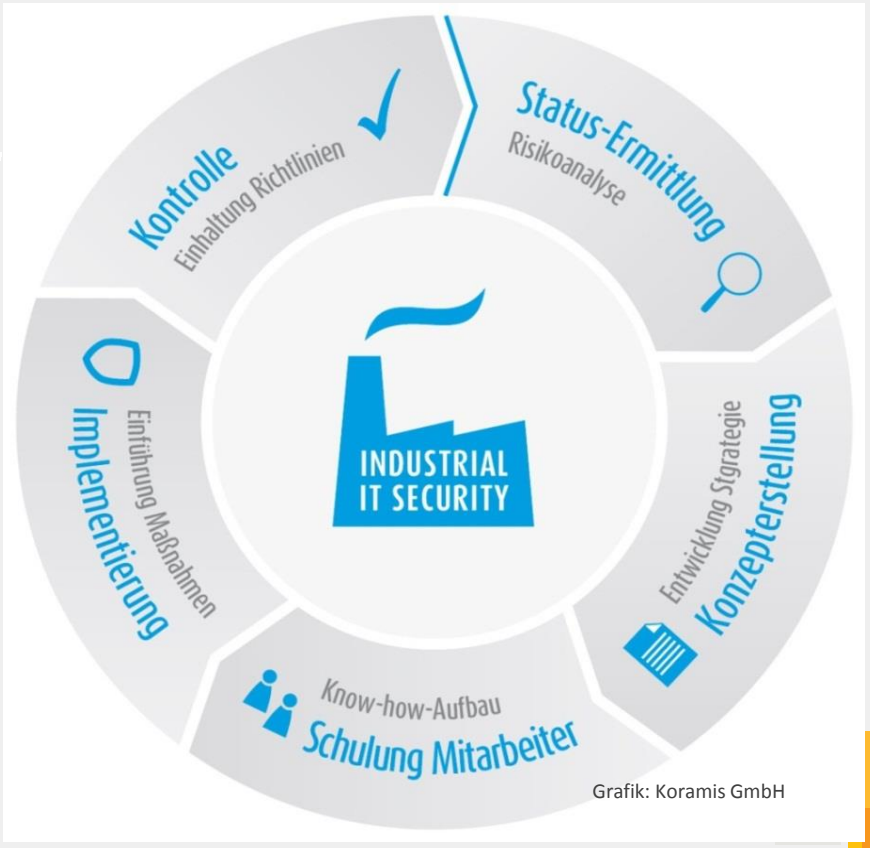
Banken Wirtschaftsprüfung

Versicherungen

… Markt nähert sich auf zwei Herangehensweisen…

Industrial Security aus der Praxiserfahrung

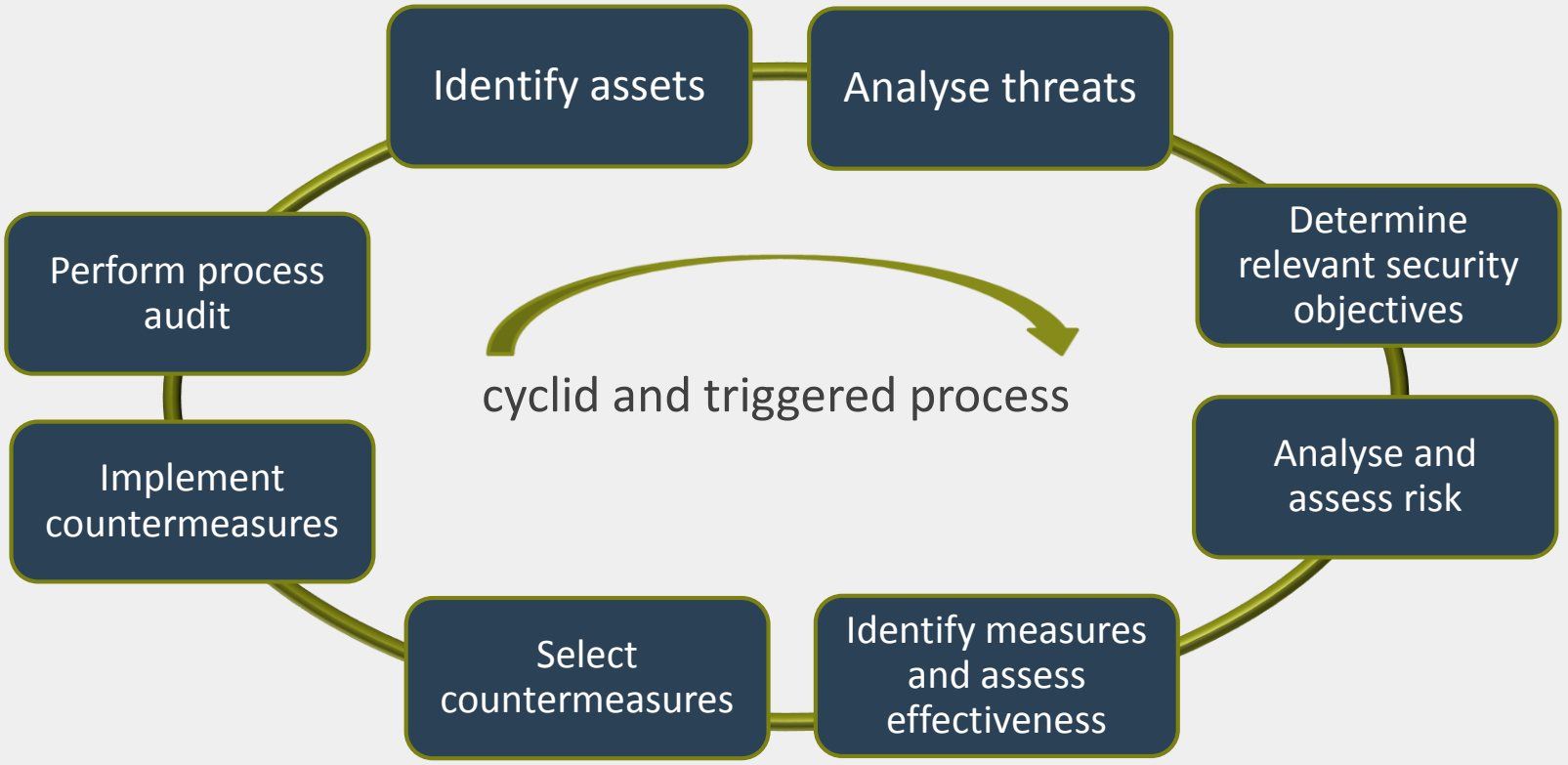




Grafik: Koramis GmbH

Die VDI, VDE 2182 Richtlinie

VDI
The Association of German Engineers



Praxisbeispiel

Einführen einer Schutzmaßnahme in der Produktion

Identify assets | Analyse threats | Determine relevant security objectives | Analyse and assess risk

- Feststellen der SCADA Systeme (Automatisch und Manuell)
- Analyse der Angriffsvektoren (SOCKS, CERT, externe Zuarbeit)
- Erstellen einer Entscheidungsmatrix basierend auf einem Risikomodell (Eintrittswahrscheinlichkeit und Businessimpact)
- Zeit: 3 Monate

Praxisbeispiel

Einführen einer Schutzmaßnahme in der Produktion

Identify measures and assess effectiveness

Select countermeasures

Implement countermeasures

Perform process audit

- Basierend auf der Entscheidungsmatrix , Auswahl der Maßnahme
  - System Änderung , Antivirenlösung, System Härtung, Firewall, Awareness Training, starke Authentifizierung,
- Implementierung der Lösungen
- Dokumentation
- Testen der Lösungen (intern und extern)
- Zeit: 6 Monate

Thank you!

Olaf Mischkovsky

olaf_mischkovsky@symantec.com