EKT

Energie.
Daten.
Zukunft.

Kundenportal, Data- & Cyber-security: was es zu beachten gilt

Kundenportal, Cybersecurity: was es zu beachten gilt

Andreas Plüer, 24.02.2022

Agenda

- Ausgangslage Cybersicherheit im OT-Umfeld
- Herausforderungen und Empfehlungen zur Umsetzung Grundschutz für OT
- ISMS bei EKT in der Praxis
- Empfehlungen Portal-Sicherheit

Ausgangslage – Cyberangriffe im OT-Umfeld

Menu Search **Bloomberg** Sign In Subscribe

Technology | Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra
4. Juni 2021, 21:58 MESZ

Forbes

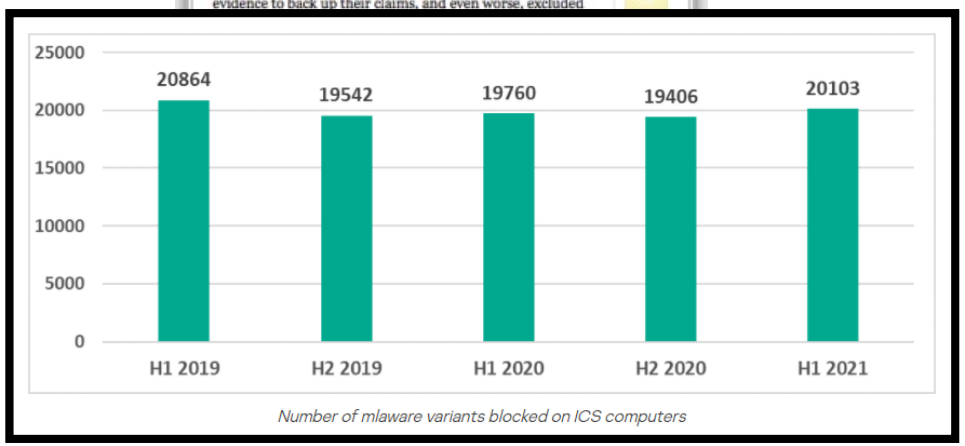
Jeffrey Carr
DIGITAL DAO

TECHNOLOGY

The New York Times Fails To Deliver Stuxnet's Creators

The New York Times

Yesterday the New York Times published a major story by William J. Broad, John Markoff and David E. Sanger which named the U.S. and Israel as co-developers of the Stuxnet worm. Unfortunately for their millions of readers, they provided almost no verifiable evidence to back up their claims, and even worse, excluded



Number of mlaware variants blocked on ICS computers

Unternehmen

SPIONAGE

Thyssen-Krupp deckt Cyberangriff auf

VON HELMUT BÜNDER, DÜSSELDORF · AKTUALISIERT AM 08.12.2016 · 16:55

Hacker sind in die Rechner des Stahlkochers eingedrungen. Ihr Ziel war Industriespionage. Doch der große Datenklau blieb aus.

MERKEN

Vor wenigen Tagen hatte es die Deutsche Telekom erwischt, wo ein Hackerangriff Hundertausende von Internetanschlüssen lahm legte. Jetzt berichtet Thyssen-Krupp, dass es Ziel einer Cyberattacke wurde. Nach Erkenntnissen des Essener Stahl- und

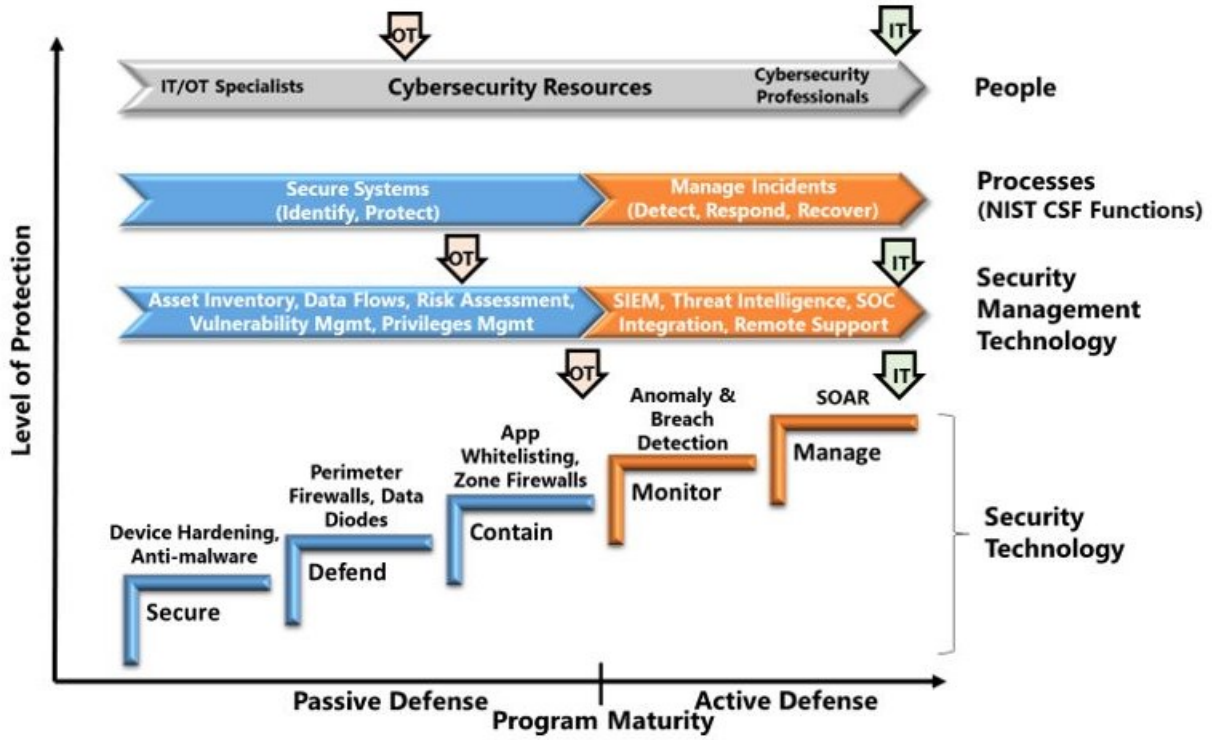
Ausgangslage

Cyberangriffe auf kritische Infrastrukturen nehmen - wie in der übrigen Geschäftswelt - dauernd zu.

Durch eine zunehmende IT/OT-Konvergenz, d.h. eine Integration von Systemen der Informationstechnologie (IT) mit Systemen der Betriebstechnologie (OT) ist eine komplette Abschottung der OT-Systeme kaum mehr möglich

VSE empfiehlt für Verteilnetzbetreiber und Energieerzeugungsanlagen den «Grundschutz für Operational Technology in der Stromversorgung» mit dem Ansatz «Defense-in-Depth», verbunden mit einem gesamtheitlichen Prozess nach dem NIST-Framework mit den Komponenten Identifizieren (Identify), Schützen (Protect), Erkennen (Detect), Reagieren (Respond) und Wiederherstellung (Recover).

Umsetzung «Grundschutz für OT» in der Theorie



ARC Cybersecurity Model Shows Current State of Industrial Cybersecurity Programs

Informationssicherheit wird nur durch ein Zusammenwirken von

- **Menschen**
- **Prozessen**
- **Technologien**

erreicht

Herausforderungen für EVU

EVU betreiben oft komplexe Infrastrukturen, werden immer stärker mit externen Netzwerken (z.B. Lieferanten) und vermehrt Cloud Services verbunden.

Die IT/OT-Konvergenz führt dazu, dass sich ICS-/SCADA-Systeme immer weniger vollständig isolieren lassen. Über eine Infizierung eines IT-Arbeitsplatzes, der auch Zugriff auf die OT-Systeme hat, können ICS-Umgebungen angegriffen werden.

Arbeitslast und Aufgabenvielfalt lassen selten einen Fokus auf einzelne Themen wie Cybersecurity oder die Einführung eines ISMS zu. Gerade hier ist aber sind Expertenwissen und Zeit nötig.

Empfehlungen für EVU

Informationssicherheit intern oder extern (Lieferanten, Spezialisten) adressieren:

Menschen

- Internen oder externen Chief Information Security Officer (CISO) nominieren
- Sensibilisierung der Mitarbeitenden durch regelmässige Awareness-Massnahmen

Prozesse

- Überblick über Assets erhalten, z.B. Asset Management. Bedrohungen, Risiken und Massnahmen für diese Assets festlegen
- Einführung eines Managementsystem für die Informationssicherheit prüfen, z.B. ISO 27001

Technologien

- Systemarchitektur härten, z.B. durch
  - Abtrennung oder Schutz der Übergänge zwischen IT und OT durch Firewalls
  - Kontrollierte Zugänge für Lieferanten
  - Perimeter-Schutz mittels Firewall, Intrusion Detection System, VPN, Malware-Schutz, geschützte Zonen-Übergänge
  - System- und Software-Wartung (Patch-Management)
  - Überprüfung der Infrastruktur auf Schwachstellen und mögliche Angriffspunkte

Empfehlungen Portal-Sicherheit

- Regelmässige Aktualisierung der eingesetzten Technologien durch den Portal-Partner (Content Management Systeme, Webserver, Datenbank-Management-Systeme, Backend-Umgebungen, etc.)
- Einsatz einer «2 Faktor-Authentifizierung» für Administratoren und Nutzer, sichere Passwörter
- Erstellen interner Weisungen und Richtlinien für die sichere Nutzung von ausgelagerten Dienstleistungen (z.B. Einhalten lokaler Gesetze bei länderübergreifenden Dienstleistungsvereinbarungen, Speichern von Daten etc.).
- Überwachung der Leistungserbringung und Einhaltung der Service Levels und Sicherheit, z.B. durch unabhängige Dritte (z.B. Penetration Tests, Schwachstellenprüfung)
- Einhaltung von Datenschutz-Normen (z.B. DSGVO, Verschlüsselung)
- Regelmässige Backups der Daten und sichere externe Ablage

EKT:
Kundenportal, Data- & Cybersecurity

Energie.
Daten.
Zukunft.

EKT AG
Bahnhofstrasse 37
9320 Arbon
T 071 440 61 11
info@ekt.ch
www.ekt.ch

Andreas Plüer
Bereichsleiter Digital Services

D 071 440 63 33
andreas.plueer@ekt.ch