IT-Sicherheitssituation in der deutschen Wirtschaft

Berlin, 29.11.2018, TeleTrust Mitgliederkonferenz

Vision

> WE ARE THE LEADING ENABLER OF COMMUNITY-DRIVEN CYBER-DEFENSE FOR THOSE IN NEED.

Structure of Advisory and Customer Boards

Advisory Board

- Company representatives, usually CIOs
- Representatives of authorities / research institutions / associations
- DCSO Managing Directors

CISO Panel

- CISOs of all Advisory Board companies
- BSI representative

Sharing and Research Groups

Threat Intelligence Sharing

Cloud Vendor Assessment

Hybrid Cloud Security Architecture

Multi Factor Authentication

Enterprise Security Metrics (KPIs)

Cyber PPPs

Working Groups for DCSO Services

Technology Scouting & Evaluation

Audit Platform

Threat Intelligence (Aggregation & Reporting)

Threat Detection & Hunting

Supply Chain Auditing

Thought Leadership Community

Customer Boards

VDA Side

DCSO Advisory Board - Members

DCSO Portfolio incl. Service Components

Community Information Services

- Technology Scouting & Evaluation (TSE)
  - Community
  - neu Portal
- Service & Enterprise Assessment (SEA)
  - TISAX
  - Supplier Risk Mgmt.
- neu Cloud Vendor Assessment (CVA)

Cyber Defense Services

- Threat Intelligence (TI)
  - TI Community Sharing
  - TI Reporting
  - TI Indicators
- neu Internet Monitoring
- Threat Detection & Hunting (TDH)
- Incident Response (IR)
  - neu Compromise Assessment
  - neu Readiness Assessment
- neu Merger & Acquisition

Professional Services

- Governance, Risk & Compliance Consulting
- Technical Consulting
- Integration Consulting

- **Think Tank:** Research & Prototyping

Statements

ICS Angriffe nehmen in der Zukunft massiv zu

APT Angriffe sind in 2018 gestiegen und erfordern andere Abwehr-Maßnahmen

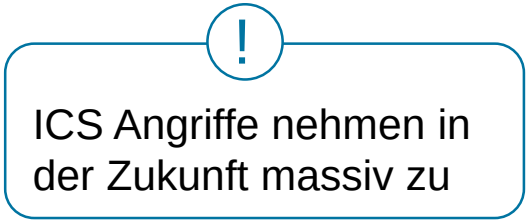
Security Architekturen werden immer komplexer

Zulieferer spielen eine immer wichtigere Rolle im Cyber-Security Ecosystem

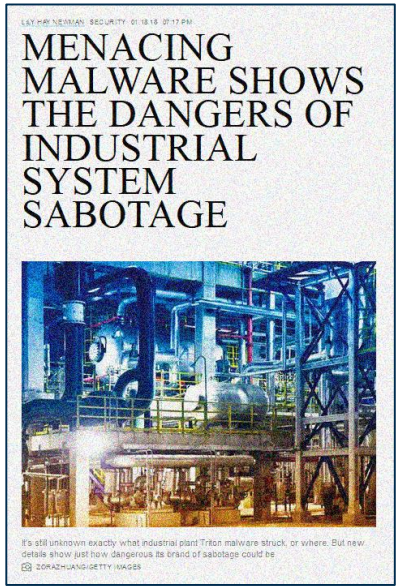
Fachpersonal für den Cyber-Security Bereich werden immer knapper

Cyber-Security in M&A wird immer wichtiger und konsequenter eingesetzt

Statements



Excerpt of daily reports on attacks against ICS



LILY HAY NEWMAN SECURITY 01.18.18 07:17 PM

MENACING MALWARE SHOWS THE DANGERS OF INDUSTRIAL SYSTEM SABOTAGE

It's still unknown exactly what industrial plant Triton malware struck, or where. But new details show just how dangerous its brand of sabotage could be.

ZORAZHUANG/GETTY IMAGES

https://www.darkreading.com/operations/fireeye-finds-new-clues-in-triton-trisis-attack/d/d-id/1332008

Hackers Behind 'Triton' Malware Attack Expand Targets

By Eduard Kovacs on May 24, 2018

The threat group responsible for the recently uncovered attack involving a piece of malware known as Triton, Trisis and HatMan is still active, targeting organizations worldwide and safety systems other than Schneider Electric's Triconex.

The actor, which industrial cybersecurity firm Dragos tracks as Xenotime, is believed to have been around since at least 2014, but its activities were only discovered in 2017 after it targeted a critical infrastructure organization in the Middle East.

The attack that led to the cybersecurity industry uncovering Xenotime was reportedly aimed at an oil and gas plant in Saudi Arabia. It specifically targeted Schneider Electric's Triconex safety instrumented systems (SIS) through a zero-day vulnerability.

The targeted organization launched an investigation and called in FireEye's Mandiant after the SIS caused some industrial systems to unexpectedly shut down. Researchers believe the shutdown was caused by the attackers by accident.

Dragos has also analyzed the initial Triton/Trisis incident and more recent attacks launched by Xenotime. The company says the group has targeted organizations globally, far outside the Middle East.

The security firm has not shared any details on present attacks, but it did note that the hackers are active in multiple facilities, targeting safety controllers other than Triconex.

Some researchers believe Iran is behind the attacks, but Dragos has not shared any information on attribution. The company did point out that it has not

https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/

Cyber-Angriffe auf deutsche Energieversorger

Ort	Bonn
Datum	13.06.2018

Deutsche Unternehmen aus der Energiewirtschaftsbranche sind Ziel einer großangelegten weltweiten Cyber-Angriffskampagne. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet intensiv an einer Vielzahl von Verdachtsfällen, analysiert gemeinsam mit betroffenen Unternehmen das Vorgehen der Angreifer und weist auf nötige Schutzmaßnahmen hin. Demnach nutzen die Angreifer unterschiedliche Methoden, die ihnen in einigen Fällen Zugriff auf Büro-Netzwerke der Unternehmen ermöglicht haben. In mehreren Fällen konnten zudem Spuren der Angreifer nachgewiesen werden, die auf Angriffsvorbereitungen zur späteren Ausnutzung hindeuten. Derzeit liegen keine Hinweise auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke vor.

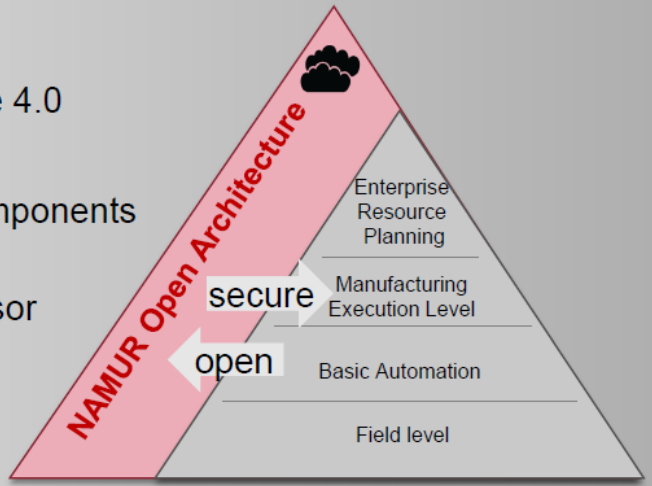
Dazu erklärt BSI-Präsident Arne Schönbohm: *"Diese Angriffe zeigen, dass Deutschland mehr denn je im Fokus von Cyber-Angriffen steht. Dass bislang keine kritischen Netzwerke infiltriert werden konnten, zeigt, dass das IT-Sicherheitsniveau der deutschen KRITIS-Betreiber auf einem guten Level ist. Das ist auch ein Verdienst des IT-Sicherheitsgesetzes. Die bekanntgewordenen Zugriffe auf Büro-Netzwerke sind aber ein deutliches Signal an die Unternehmen, ihre Computersysteme noch besser zu schützen. Diese Entwicklung offenbart, dass es womöglich nur eine Frage der Zeit ist, bis kritische Systeme erfolgreich angegriffen werden können. Wir müssen daher das IT-Sicherheitsgesetz fortschreiben, so wie es bereits im Koalitionsvertrag der Bundesregierung festgehalten wurde. Die Bedrohungslage im Cyber-Raum hat sich*

Open Architecture by NAMUR
Normenausschuss Mess- und Regeltechnik

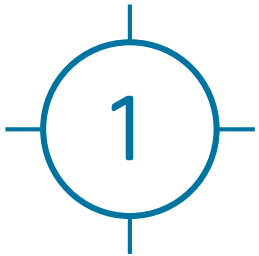
Namur Open Architecture

Enhancement of existing approaches as a baseline for the efficient and flexible utilization of Industrie 4.0 with the process industry

- Additive to existing structures
- Open for new approaches within Industrie 4.0
- Based on existing standards
- Simple integration of fast changing IT components from field level up to enterprise level
- Significant improvements of cost per sensor due to open and integrative approaches
- No risk of availability and safety of installed base

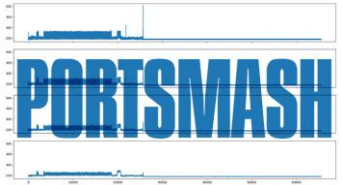


High Level Situational Awareness



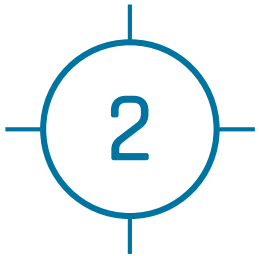
Side-channel attacks on the rise

Side-channel attacks on the rise



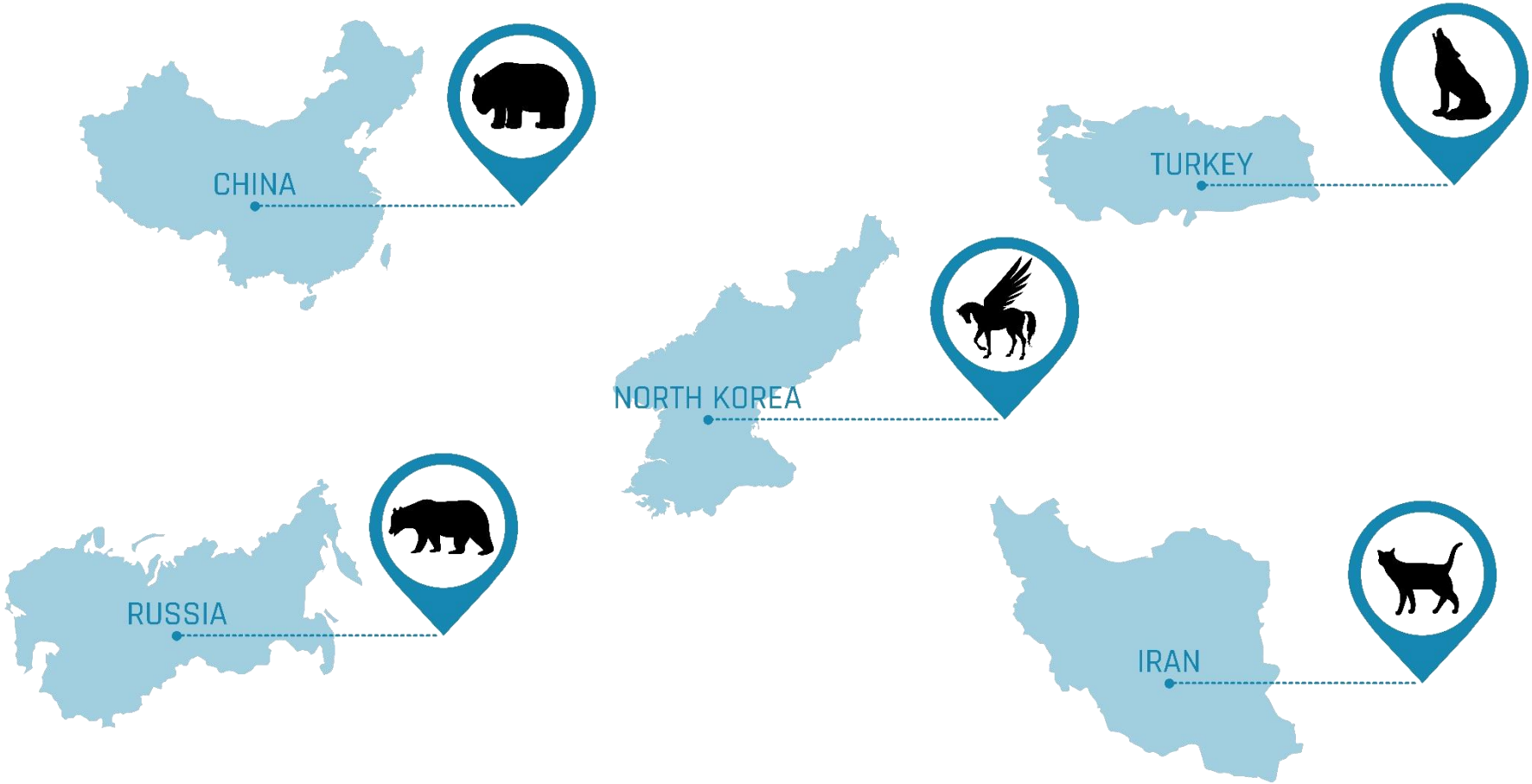
Chip exploits - Summary

- We really have a new era of chip-level exploits
- CPU-design has to change significantly
- Until then: Install patches where possible
- Don’t panic, not all parts of your infrastructure suffer from all vulnerabilities with the same urgency



Fuzzy lines between “crime” and “APT”

Continuously high level of industrial & political espionage in Germany


CHINA
TURKEY
NORTH KOREA
RUSSIA
IRAN

Cyber conflicts increasingly politicized

Cyber goes Real World Politics

Coping Strategies

Coping Strategies

- Intense cooperation between all relevant parties:
  - Law Enforcement
  - Intelligence Community
  - Private sector security providers
  - Economy at large
- Supply chain security
- Cooperation of corporate security and cyber security
- IT Architecture Resiliency