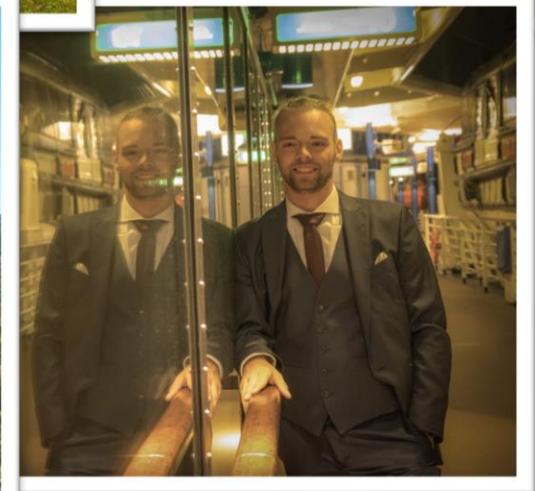
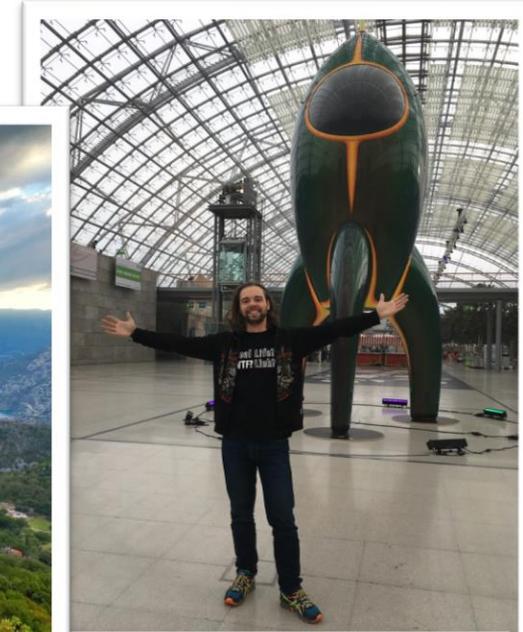


Cybersecurity in IoT

Part 1: Cybersecurity – An Introduction

Marius Hansen

- Cybersecurity Manager with EY Switzerland
- Background:
 - Cybersecurity expert with a focus on Enterprise Security Architecture and Behavioral Biometrics
 - IT coaching and database administration
 - Tutor, teacher and research assistant
- World explorer and jungle guide
- Hobby programmer and gamer



Cybersecurity in the Internet of Things

Motivation: Stuxnet (2010)

- In 2010 an extremely sophisticated computer worm crippled the **Iranian Nuclear Program**
- The malware propagated through the facilities for years before finally striking and **destroying the facilities centrifuges**
- It was designed to attack **uranium enrichment** facilities and targeted mainly **Iranian facilities**
- Developed and deployed by the **US and Israelian intelligence agencies** under the codename: «Operation Olympic Games»
- The worm used the **Industrial IoT nature** of the air-gaped ecosystem inside of the facility to infect all devices and propagate
- Ultimately it reached the **control elements** of the centrifuge to then destroy them by altering the speed component



Cybersecurity in IoT

Overview of the Presentation

Cybersecurity Basics

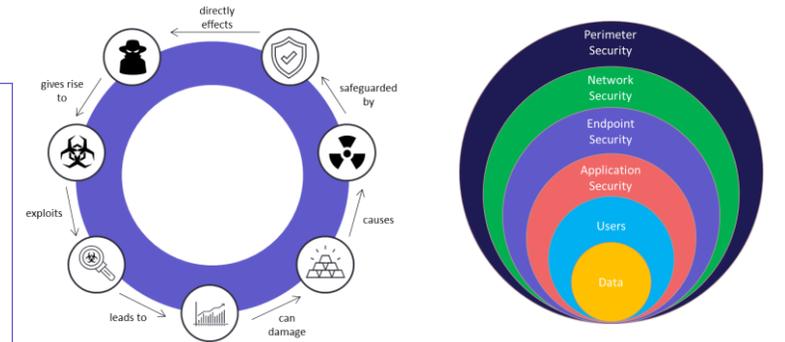
- During the first part we will explore the **fundamentals** of **Cybersecurity** and get an understanding of the **processes, mechanics and terminology**.
- This will be taught on a **very high level** and we will not go into the details of different mechanics, protocols and algorithms.

Cybersecurity Domains

- The second part focuses on the different **domains of Cybersecurity**.
- This part is inspired by **CISSP, NIST and the lecturers personal experience** and will give a broad understanding of Cybersecurity from a **business PoV**.
- The goal is to know the parts of a **Cybersecurity Program** to be able to **search** for the **right** services, processes, tool and frameworks when needed.

Cybersecurity in the Internet of Things

- In the last chapter we will learn about the Cybersecurity challenges of IoT, how to mitigate the correlated risks.
- To achieve that a set of three real-life incidents are presented and assessed.
- We will then focus on a number of important policies, processes and tools to understand the overall ecosystem of Cybersecurity in IoT.



Agenda

- 1** What is Cybersecurity?
- 2** The CIA Triad
- 3** Threat Landscape
- 4** Defense In-Depth
- 5** Security Control Types
- 6** Malware, Attacks and Motivations
- 7** Cybersecurity Fundamentals: Q&A

What is Cybersecurity?

Cyber Security (NIST)

*Prevention of damage to, **protection** of, and restoration of **computers**, electronic communications systems, electronic communications services, wire communication, and electronic communication, **including information** contained therein, to ensure its **availability, integrity, authentication, confidentiality, and nonrepudiation.***

Information Security (NIST)

*The **protection** of **information** and **information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability.***



The CIA Triad

	Description	Threats	Measure & Controls
Confidentiality	Assurance of secrecy and un-authorized disclosure of information.	<ul style="list-style-type: none">• Packet Sniffer• Password attacks• Keylogger• Phishing attacks	<ul style="list-style-type: none">• Encryption• Access control• Training
Integrity	Assurance and reliability of information systems (prevention of modification)	<ul style="list-style-type: none">• Man-in-the-Middle• Session hijacking• Accidental deletion/ modification of data	<ul style="list-style-type: none">• Hashing• Digital signatures• Cyclic redundancy
Availability	Ensuring reliably and timely access of systems and data to authorized individuals.	<ul style="list-style-type: none">• (D)DoS• Natural disasters• Power outages• Misconfiguration	<ul style="list-style-type: none">• Load balancing• Backups• Co-locations

Threat Landscape

Threat Agent

An entity that acts as a threat.
e.g. hacker or a natural disaster

Threat

Potential danger that could exploit a vulnerability. e.g. malware attack or fire

Vulnerability

Weakness in a system that could be exploited.
e.g. weak password or open port in a firewall

Risk

Likelihood of threat exploiting vulnerability and impact.
e.g. likelihood of malware attack breaching the system

Countermeasure

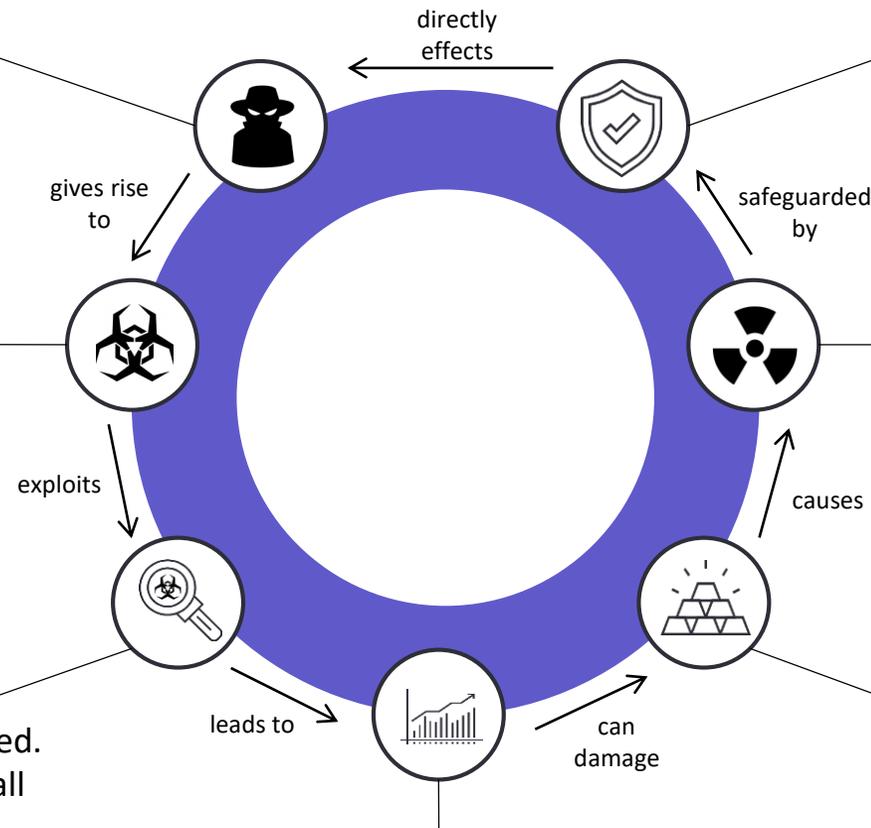
Mitigation for a potential risk for exposure. e.g. anti-malware system

Exposure

Instance of negative impact by exploited vulnerability. e.g. server down

Asset

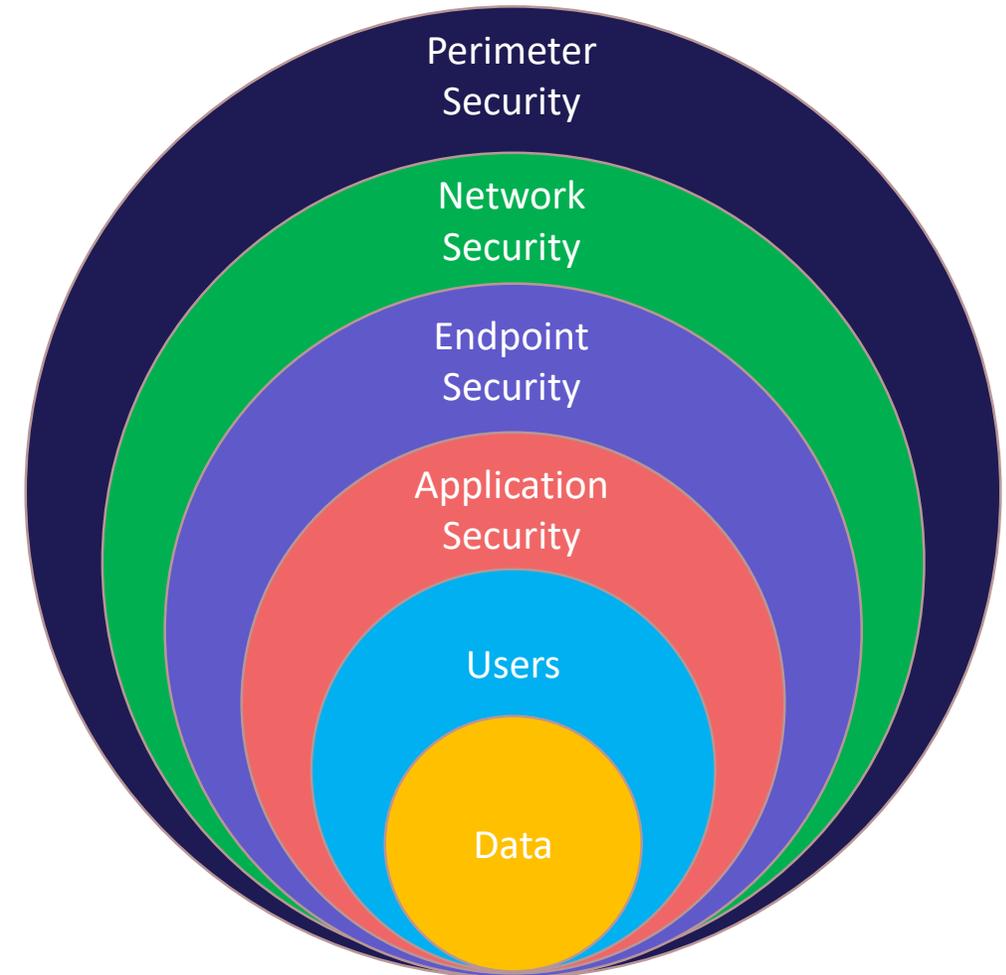
A valuable resource of a system to be protected. e.g. server or patient data



Defense In-Depth: Overview

Defense In-Depth is an approach by which information and information systems are protected by layers of controls. This reduces the risk of a successful attack, because an attacker would need to overcome a multitude of protection mechanisms.

Perimeter Security	The outer layer of a corporate defense in-depth strategy is physical security. This includes e.g. fences and makes it harder for an attacker to gain physical access.
Network Security	To reduce the likelihood of an attacker gaining access to certain parts of a companies infrastructure, countermeasures like firewalls, IDS' and VPNs are implemented.
Endpoint Security	Endpoint security is about the protection of devices, like servers, computers or smart devices. This can be achieved using controls like passwords or patch management.
Application Security	This layer addresses attacks on the application layer, after a possible attacker gained access to a device. Typical safeguards are anti-virus software and access control.
Users	Awareness and security trainings are an important part of any security program. People are still considered the weakest link in terms of cybersecurity.
Data	The information to be protected. On this level there are also controls in place, like for example encryption or tokenization of data.



Defense In-Depth: Security Control Types

		Administrative Controls (Management)	Technical Controls (Software and Hardware)	Physical Controls (Personal and facilities)
Preventative	Intended to avoid an incident from occurring.	<ul style="list-style-type: none"> • Security Policies • Awareness Training 	<ul style="list-style-type: none"> • Antivirus Scanner • Encryption 	<ul style="list-style-type: none"> • Locks • Badge System
Detective	Helps to identify an incidents activities and potentially an intruder.	<ul style="list-style-type: none"> • Segregation of Duties • Monitoring 	<ul style="list-style-type: none"> • Audit Logs • Intrusion Detection Systems 	<ul style="list-style-type: none"> • Cameras • Motion Detectors
Corrective	Fixes components or systems after an incident has occurred.	<ul style="list-style-type: none"> • Business Continuity 	<ul style="list-style-type: none"> • Server Images 	
Deterrent	Intended to discourage a potential attacker.	<ul style="list-style-type: none"> • Job Rotation • Laws & fines 		<ul style="list-style-type: none"> • Fences • Security Guard
Recovery	Intended to bring the environment back to regular operations.	<ul style="list-style-type: none"> • Disaster Recovery 	<ul style="list-style-type: none"> • Backups 	<ul style="list-style-type: none"> • Offsite Facility
Compensation	Provides an alternative measure of control.	<ul style="list-style-type: none"> • Can be any control that might be possible to cover another. • An example would be using security guards instead of fences. 		

Malware, Attacks and Motivations I



Hacker Types by Motivation

Black Hat Hack with malicious intent	White Hat Hack to defend and harden systems
Gray Hat Hack as they please	Script Kiddie Use scripts and tools, usually unskilled
State Sponsored Hackers Act in the interest of a government	Hacktivist & Cyber Terrorists Usually political or religious motives



Types of Malware

Virus Spreads with user interaction	Spyware Monitors your activities	Blended Threat Multiple malware in one attack
Worms Spread automatically	Adware Maliciously feeds you ads	Remote Access Controls PC from distance
Trojan Disguised as legitimate software	Rootkit Hides deep within the PC	Exploit Kit Hunts software vulnerabilities

Malware, Attacks and Motivations II



PHISHING & SOCIAL ENGINEERING

Sending fake emails or text messages that appear to be from trusted sources.

- Awareness trainings
- Check URL before clicking
- Check e-mail for errors



SQL INJECTIONS

Inserting malicious code into a SQL database.

- Apply least-privilege model
- Validate SQL data inputs
- Exclude dynamic SQL



PASSWORD ATTACKS & CREDENTIAL REUSE

Exploiting weak or common passwords to gain unauthorised access to a network.

- Awareness trainings
- Password policies
- Account lockout policies



ZERO-DAY EXPLOIT

Until a known software vulnerability is mitigated, hackers can be adversely exploiting it.

- Secure Wi-Fi system
- Use SSL (HTTPS)
- Update and Patch often



DENIAL-OF-SERVICE ATTACKS

Crashing or flooding specific web servers with nonsense requests that stop regular users from connecting.

- Anti-DoS protocols
- On-premise protection
- Cloud-based counteraction



CROSS-SITE SCRIPTING (XSS)

A hacker injects malicious script into a trusted website exposing other end users visiting that web page.

- Awareness trainings
- Run XSS vulnerability tests
- Sanitise the data input



MAN-IN-THE-MIDDLE

A hacker inserts themselves between two legitimate hosts.

- Use SSL (HTTPS)
- Intrusion Detection Sys.
- Use VPN



DRIVE-BY-DOWNLOADS

Takes advantage of an operating system, web browser or app that has vulnerabilities due to a lack of security updates.

- Update and Patch often
- Reduce attack surface
- Secure points of entry

