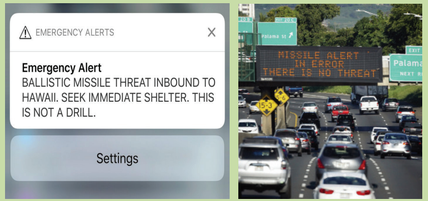
Smart City

Permanent zur Verfügung stehende Daten, zum Beispiel über Verkehrsfluss und Luftqualität oder über Parkraum und den öffentlichen Verkehr sowie die Einbindung der Bewohner mittels Apps oder Sensoren im Haushalt, ermöglichen neue Geschäftsmodelle und lösen Herausforderungen, die sich Städten stellen. Diese werfen jedoch auch Fragen in puncto Datenschutz und Cyber Security auf. So tragen autonome Systeme (auch zukünftige autonome Fahrzeuge) und die Vernetzung all der verfügbaren Daten zur Optimierung von Energieverbrauch, Verkehr, Luftqualität etc. bei. Auf der anderen Seite entstehen Angriffsflächen für Manipulationen und Datendiebstahl.



Fallbeispiel: Chaos durch Falschmeldung

Welche Auswirkungen mögliche Falschalarme haben können zeigte sich Anfang 2018, als auf Hawaii die Meldung „BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL." über Fernsehen, Radio und Mobiltelefone verbreitet wurde und sich mehr als 10 Minuten lang ohne Dementi durch die verantwortlichen Stellen ausbreitete. In diesem konkreten Fall führte ein Fehlverhalten eines Mitarbeiters dazu, jedoch könnten durch Spear-Phishing bzw. Social Engineering ähnliche Attacken getriggert werden.[5]

Wie das Fallbeispiel zeigt, könnte auch durch geänderte Ampelsteuerungen oder Fake Warnmeldungen für Sicherheitskräfte Chaos ausgelöst werden. Solche Störungen könnten in einem kriminellen Kontext bewusst eingesetzt werden.

Anfang 2018 hat IBM X-Force Red und Threatcare verschiedene Smart-City-Systeme getestet, welche auf der ganzen Welt im Einsatz sind[6]. Bei der Analyse konnten 17 Schwachstellen mit unterschiedlicher Kritikalität gefunden werden. Die Sicherheitslücken beruhten unter anderem auf der Verwendung von Default Passwörtern, unzureichendem Identitymanagement bzw. Authentifizierungs-Bypass, SQL-Injektion, unverschlüsselte Kommunikation und Plaintext Passwörtern.

Industrie 4.0 / Anlagenbau

In Produktionsumgebungen und im Anlagenbau kommt es zu einer zunehmenden Vernetzung. Dies betrifft nicht nur Produktionssysteme und Steuerrechner selbst, sondern die gesamte mit der Planung in CAD-Systemen beginnende Kette und führt dadurch zur informationstechnischen Koppelung zwischen IT (Office) Netz und der sogenannten Operational Technology (OT) (Produktionsumgebung). Die weitere zunehmende digitale Vernetzung der eigenen Produktionsumgebungen mit der gesamten Wertschöpfungskette und die damit verbundene Einbindung externer Zulieferer inklusive Logistik bringt besondere Anforderungen an die Zuverlässigkeit und Sicherheit mit sich. In der Fabrik der Zukunft ist der freie Daten- und Informationsaustausch eine der wichtigsten Voraussetzungen, wobei diese digitalen Informationen ähnlich wie Rohstoffe und Komponenten mit der Außenwelt auszutauschen sind. Dieser freie Datenfluss stellt jedoch große Herausforderungen an die Datensicherheit, um ein angemessenes Sicherheitsniveau zu gewährleisten.

Fallbeispiel: Cyber Security als neues Geschäftsmodell in einem Industriebetrieb

ANDRITZ entwickelte ein Angebot für Cybersicherheit und bietet damit Unternehmen mit digitaler IT/OT-Konvergenz ein allumfassendes Service zur Überwachung industrieller Cyberrisiken von der Analyse und Beratung bis hin zur kontinuierlichen Risikoüberwachung und -senkung.
Es können Cyber Attacken simuliert (Penetration Testing) und die Verletzlichkeit der kritischen Infrastruktur erhoben werden, ohne den tatsächlichen Produktionsprozess zu stören oder zu gefährden. Aufbauend auf der Ist-Situation der Netzwerkstruktur sowie vorhandener Schutzmechanismen werden mögliche Vektoren für Cyber Attacken entwickelt, um sicherheitstechnische Lücken der Kunden-OT zu identifizieren. Die Ergebnisse und Implikationen des Penetration Testing werden zusammen mit dem Kunden analysiert und Strategien zur Stärkung der OT-Sicherheit entwickelt.

Eine Segregation der Netzwerke (physikalisch oder virtuell), um ein abgeschottetes Netz für die Geräte der Operational Technology (OT) zu bewerkstelligen, ist zwingend notwendig. Die Absicherung sollte zumindest auf Netzwerkbasis (IP – z.B. durch Access Control Lists oder Firewalls) erfolgen, idealerweise jedoch kryptographisch durch zertifikats- oder benutzerbasierte VPN-Lösungen. Alle Kommunikationssysteme sollten redundant ausgelegt sein und eine entsprechende Datenpufferung vorgenommen werden, um die Produktionssysteme bei Ausfällen von vorgelagerten Komponenten (z.B. Ausfall der Datenverbindungen) so lange wie möglich autonom im operativen Betrieb zu halten. Weitere spezialisierte Überwachungssysteme wie beispielsweise IDS und IPS (Intrusion Detection und Intrusion Prevention System), die industrielle Protokolle wie IEC 60870-5-104 überwachen, aber auch Client-Sicherheitslösungen für Steuerrechner sollten eine mehrschichtige Verteidigungsstruktur bilden. Zusätzlich sollten Maßnahmen zur Behandlung von sogenannten Legacy-Systemen (Application Whitelisting für Industriesysteme) und Embedded Systems getroffen werden.

[5] *https://www.npr.org/sections/thetwo-way/2018/01/30/581853255/hawaii-missile-drill-stated-this-is-not-a-drill-resulting-in-false-alert*
[6] *https://securityintelligence.com/outsmarting-the-smart-city/*

Best Practices in Cyber Security

Durch die zunehmende Vernetzung und den raschen Einzug des Internets der Dinge im Zuge der Digitalisierung muss sich die Sicherheit für diese hochkomplexen und flexiblen Netze der Gegenwart und der nahen Zukunft weiterentwickeln und neben traditionellen perimeterbasierten bzw. statischen Ansätzen neue Wege beschreiten – unter anderem durch das Einbeziehen von KI. Eine hundertprozentige Sicherheit kann nie erreicht werden. Es wird immer ein Restrisiko bestehen, das gemanagt werden muss. Mittels einer Risikoabschätzung muss das richtige Mittelmaß zwischen Aufwand und Kosten einerseits und etwaigem Schaden andererseits gefunden werden. Risiken im Cyberbereich können in den Kategorien Hardware, Softwareentwicklung, Informationsmanagement, Netzwerk und menschliche Risken zugeordnet werden und wurden auch in der Radargrafik dementsprechend gegliedert.

Für jede dieser Kategorien gibt es Maßnahmen, die einen angemessen Basisschutz gewährleiten. In der menschlichen Kategorie sind Mitarbeiterschulungen, sogenannte Awareness Trainings, unverzichtbar, um Richtlinien zu verinnerlichen und eine entsprechende Bewusstseinsbildung zu fördern. Damit soll Social Engineering und Spear-Phishing vorgebeugt werden. Securityzertifizierte Mitarbeiter sind eine weitere Maßnahme, um in einem Unternehmen die Cyber Sicherheitspraktiken und -Prinzipien zu gewährleisten und auszubauen.

Würden meine Mitarbeiter/innen einen gefundenen USB-Stick im Unternehmen verwenden?

Auf der Hardwareebene sollten wirklich nur unbedingt erforderliche physikalische Schnittstellen nach außen geführt werden. Ein entsprechendes HW-Design ist notwendig, um Schwachstellen wie Spectr und Meltdown zu begegnen, die vor allem in Public Cloud-Umgebungen fatale Auswirkungen haben können.

Auf der Netzwerkebene sind vor allem Segregationsmaßnahmen wichtig, um das Netzwerk entsprechend zu unterteilen und mittels Layered Perimeter ausreichend Schutz für die einzelnen Teilbereiche wie IT und OT zu erreichen.

Neben der Netzwerksebene sind besonders die Maßnahmen, die der Informationsmanagementebene zugeordnet sind, unumgänglich.

- Etabliertes Patch und Change-Management
- Identity Management
- Multifaktor-Authentifizierung
- Kryptographische Maßnahmen
- Defense-in-Depth Prinzip
- Maleware Protection
- Monitoring & Logging
- Backup & Recocery
- SIEM – Security Information and Event Management

Bei der Softwareentwicklung sind Trustworthy Computing und Security Development Lifecycle wichtige Paradigmen. Die Firmware bzw. der Betriebssystem-Kernel sollte entsprechend gehärtet sein. Ihr Weg zu einer Cyber Security Strategie führt vom Erkennen von Schwachstellen über das Setzen von konkreten Maßnahmen hin zur Lösung. Dafür stehen Ihnen spezialisierte Partner zu Verfügung welche wir Ihnen noch im Folgenden empfehlen dürfen.

Ansprechpartner

JOANNEUM RESEARCH
Christian Derler

F&E, Cyber-Sicherheitsmodelle, Tools, Analyse u. Verifikation

christian.derler@joanneum.at
www.joanneum.at/cybersecurity

ANDRITZ
Klaus Glatz

IT/OT-Konvergenz, Cyber Security bei Andritz

klaus.glatz@andritz.com
www.andritz.com

FH JOANNEUM
Klaus Gebeshuber

Ausbildung – Berufsbegleitender Studiengang im Bereich Cyber Security, Sicherheitsforschung

klaus.gebeshuber@fh-joanneum.at
www.fh-joanneum.at/it-und-mobile-security/master/

Know Center
Robert Ginthör

Secure IoT, Cryptographic Technologies, Data Anonymization, Privacy-preserving Data Analytics

rginthoer@know-center.at
www.know-center.tugraz.at/

Raiffeisen Rechenzentrum
Ingo Peitler

Cloud Sicherheit, Sicherheitslösungsgesamtanbieter

ingo.peitler@rrz.co.at
www.rrz.co.at

Secinto
Stefan Kraxberger

Zertifizierungen, Beratung, Penetration Testing

office@secinto.com
www.secinto.com

TU Graz – Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
Stefan Mangard

IT Security, Cloud Computing

stefan.mangard@iaik.tugraz.at
www.iaik.tugraz.at/

Ausgearbeitet von Johann Koinegg (Green Tech Cluster) gemeinsam mit Christian Derler und Heribert Vallant (JOANNEUM RESEARCH – Digital, Kompetenzgruppe Cyber Security and Defence).

Green Tech Cluster Styria GmbH
Waagner-Biro-Strasse 100, 8020 Graz
+43 316/40 77 44, welcome@greentech.at
www.greentech.at

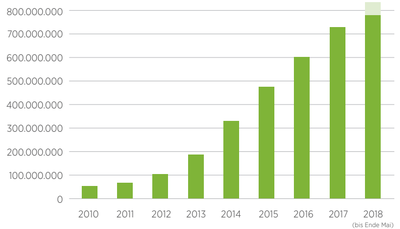
GREEN TECH CLUSTER

Cyber Security

Grundbaustein der Digitalisierung in Industrie, Energiewirtschaft und Smart City

Schutz vor Bedrohungen aus dem Cyberraum

Vernetzte IT-Infrastrukturen sind mittlerweile ein nicht mehr wegzudenkender Bestandteil unseres wirtschaftlichen und gesellschaftlichen Lebens. Die Digitalisierung vergrößert jedoch auch die Angriffsfläche für Attacken aus der Cyberwelt. Das World Economic Forum (WEF) bezeichnet in seinem „Global Risk Report 2018" Cyberkriminalität als eines der Top-4 Risiken weltweit.[1] Der jährlich vom Bundeskriminalamt veröffentlichte Lagebericht verzeichnet seit 2014 einen stetigen Anstieg an Cyber Crime Vorfällen in Österreich. 2017 gab es etwa 30 % mehr Tatbestände als im Jahr davor.[2] Laut AV-Test[3] werden im Durchschnitt täglich rund 390.000 neue Schadprogramme für PCs und monatlich etwa 690.000 neue Schadprogramme für das Mobilbetriebssystem Android beobachtet.

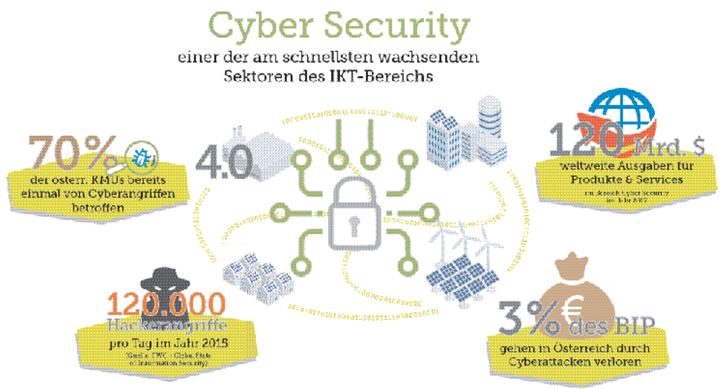


Gesamt bekannte Schadprogramme, Quelle: AV-Test, Stand 2018

Namhafte Industrievertreter sprechen davon, dass Informationssicherheit das zentrale Element der Digitalisierung ist. Ohne Sicherheit keine Digitalisierung. Cyber Security ist daher der am schnellsten wachsende Sektor des IKT-Bereichs. 2017 stiegen die weltweiten Ausgaben für Produkte und Services für Cyber Security auf mehr als 120 Milliarden US-Dollar. In den letzten zehn Jahren wuchs der Markt um 8–10 % pro Jahr, während die Prognosen für 2017–2020 ein weiteres stabiles Wachstum vorhersagen und die kumulativen Ausgaben für Cyber Security in diesem Zeitraum auf 1 Billion USD geschätzt werden[4].

> *"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."*
>
> **John Chambers**
> ex-CEO of Cisco

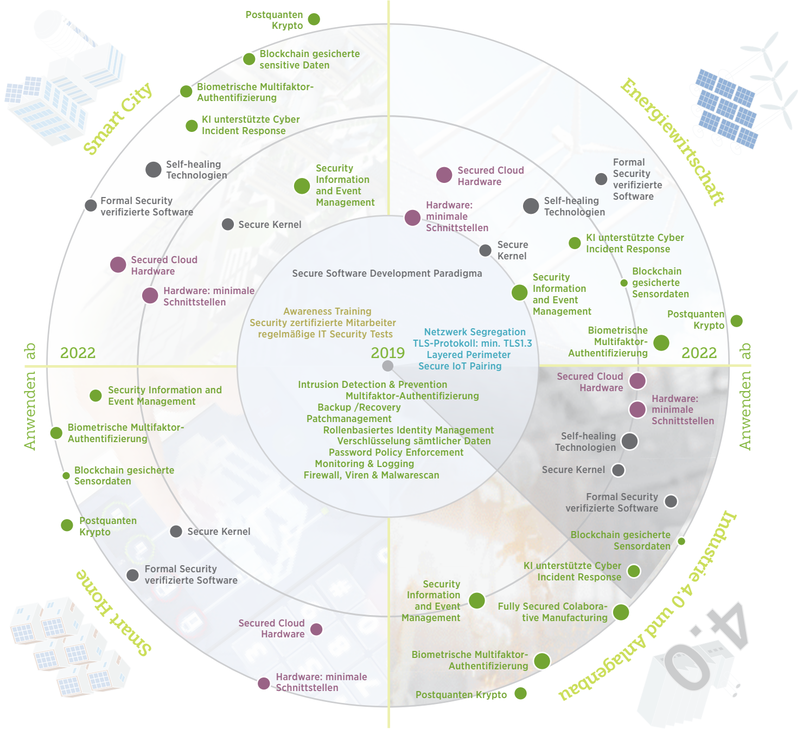
Digitalisierung entlang von Wertschöpfungsketten bewirkt eine Vernetzung verschiedener Domänen mit unterschiedlichem Schutzbedarf. Im **Energiesektor** steigert die Anbindung dezentraler Energieerzeugungsanlagen und Batteriespeicher im Endkundenbereich einerseits die Effizienz im Verteilnetz, andererseits trägt auch das Equipment beim Kunden, das in Kombination mit einem **Smart Home** System den Eigenversorgungsanteil optimiert, zum Cyber-Risiko bei. In einer **Smart City** bewirkt die Digitalisierung urbaner Lebensweisen den bestmöglichen ökonomischen und ökologischen Nutzen. Permanent zur Verfügung stehende Daten sowie die Einbindung der Bewohner mittels Apps oder Sensoren im Haushalt ermöglichen neue Geschäftsmodelle, werfen jedoch auch Fragen in puncto Datenschutz und Cyber Security auf. In der **Industrie 4.0 und im Anlagenbau** kommt es zur digitalen Vernetzung verschiedener Domänen auf unterschiedlichem Sicherheitsniveau auf der gesamten Wertschöpfungskette. Das schwächste Glied der Kette bestimmt jedoch auch hier die Sicherheit des vernetzten Systems. Städte, Gemeinden und Unternehmen jeglicher Größe (natürlich auch Endkunden) müssen sich darüber im Klaren werden, wo mögliche Schwachstellen, Eintrittspunkte und damit Sicherheitslücken im jeweiligen Umfeld sind.



[1] *https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready*
[2] *https://bundeskriminalamt.at/306/files/Cybercrime_17_web.pdf*
[3] *https://www.av-test.org/de/*
[4] *2nd issue of the European Cybersecurity Market, CYBERSEC, June 2017*

Cyber Security Maßnahmen

Die Radargrafik gibt einen Überblick über jene Absicherungsmaßnahmen, die in Bezug auf Cyber Security angewendet werden müssen. Das Radar zeigt im Zentrum jene Security Maßnahmen, die bereits heute in allen Bereichen im Einsatz sein sollten. Jene die erst in Zukunft, wie z.B. Postquantenkryptographie, zu berücksichtigen sind, finden sich in den äußeren Bereichen je nach Sektor in einer unterschiedlichen Position. Diese Einordnung ergibt sich aus einer Expertenbefragung innerhalb der Kompetenzgruppe Cyber Security und Defence. Alle im Einsatz befindlichen Maßnahmen müssen fortlaufend betreut und gemanagt werden.



Energiewirtschaft (Erzeugung und Netzbetrieb)

Fallbeispiel: Stromausfall durch Cyber Attacke

Am 23. Dezember 2015 kam es aufgrund einer Cyber Attacke zu einem großflächigen Stromausfall in der Ukraine, bei dem 30 Umspannwerke von drei unterschiedlichen Betreibern in der westukrainischen Region Iwano-Frankiwsk betroffen waren und insgesamt ca. 225.000 Kunden für einige Stunden ohne Stromversorgung ausharren mussten.

Energiesysteme sind Teil der kritischen Infrastruktur, also Einrichtungen, die eine essentielle Rolle für das Gemeinwesen darstellen. Deren reibungslose Funktion hängt heutzutage in hohem Maße von zuverlässiger Informationstechnik ab. Eine Störung der Energieversorgung oder gar ein Black-out durch eine Cyber Attacke hat je nach Umfang und Dauer nicht nur schwerwiegende Folgen für die Wirtschaft durch Produktionsausfälle, sondern auch für die öffentliche Sicherheit durch nachhaltig wirkende Versorgungsengpässe.

Die NIS Richtlinie der EU hat zum Ziel, Netz- und Informationssystemen in allen Mitgliedsstaaten auf ein hohes gemeinsames Sicherheitsniveau zu heben. In Österreich ist die Umsetzung dieser Richtlinie gerade in Begutachtung und sieht verbindliche Mindest-Sicherheitsstandards und eine Meldepflicht für schwere Sicherheitsvorfälle vor.

In einem Smart Grid werden eine Unzahl von Informationen und Steuerbefehle über unterschiedliche Trust Boundaries übertragen. Daher ist auch die Angriffsfläche für Cyber Attacken besonders groß. Deshalb muss das System mit entsprechender Sorgfalt abgesichert werden. Alle Perimeter sollten über Segregationsmaßnamen (z.B. Stateful Firewalls, idealerweise mit Deep Packet Inspection) sowohl gegenüber unerlaubten Zugriffen von außen als auch von innen abgesichert sein.

Kryptografische Maßnahmen sind eines der stärksten Mittel zur Sicherung von Verbindungen und Geräten und bieten neben Verschlüsselung auch Integritätsprüfung und Authentifizierung.

Nach dem Defense-in-Depth Prinzip sollte der Zugriffschutz (Segregation, Authentifizierung, Autorisierung) nicht nur an zentralen Netzwerkpunkten (Perimeter) vorgenommen werden, sondern zusätzlich an jedem Gerät. Dadurch wird verhindert, dass das Kompromittieren eines zentralen Services nicht das Gesamtsystem kompromittiert.

Systemkritische sowie sicherheitskritische Ereignisse (Fehlerzustände, erfolgreiche und fehlgeschlagene Anmeldevorgänge, Manipulationen der Benutzerdatenbank, Beenden sicherheitsrelevanter Services) müssen protokolliert werden und sollten mittels nachgelagertem SIEM (Security Information and Event Management) über eine echtzeitnahe Alarmierung eine effektive Bewältigung von Cyber-Sicherheitsvorfällen auslösen.

Besonders in kritischen Infrastrukturen ist eine individuelle Beurteilung der einzelnen Komponenten in Form eines Threatmodellings kombiniert mit einer Risikobewertung angebracht.

Smart Home

Im Smart Home gibt es eine Vielzahl am Markt befindlicher Geräte und Systeme für die Einsatzbereiche Sicherheitstechnik, Energiemanagement, smarte Haushalsgeräte sowie persönliche Assistenten mit Sprachsteuerung (Lifestyle, Active and Assisted Living, Wearables). Smart-Home-Systeme entwickeln sich weg von einzelnen Einsatzbereichen, wie z.B. Alarmanlagen ausschließlich als Einbruchschutz, hin zu All-in-One-Lösungen mit weiteren Features wie Energiespar- oder Komfortfunktionen. Diese Öffnung führt zu einer höheren Komplexität, die wiederum neue Sicherheitsrisiken mit sich bringt. Sobald nur ein Gerät verwundbar ist, können Angreifer auch die Kontrolle über vermeintlich sichere Geräte übernehmen. Verschiedene IoT-Protokolle auf unterschiedlichem Sicherheitsniveau (Z-Wave, ZigBee, EnOcean, Bluetooth, LoRa, etc.) nehmen Einzug ins smarte Heim, und müssen jeweils korrekt konfiguriert bzw. durch einen sicheren Pairing Prozess eingebunden werden. Eine Verknüpfung von sicherheitskritischen Funktionen wie Türschlösser oder Alarmanlagen mit Sprachassistenten muss gut überlegt und jedenfalls entsprechend sicher umgesetzt sein.

Fallbeispiel: Eintrittspunkt Sprachsteuerung

Die sogenannte Dolphin-Attacke setzt valide Sprachkommandos auf einer für Menschen nicht hörbaren Frequenz ab. Dies ermöglicht es einem Angreifer unbemerkt unerwünschte Befehle abzusetzen.

Trotz Verwendung von sicheren Protokollen können sich Verwundbarkeiten durch die Qualität der jeweiligen Herstellerimplementierung ergeben. Weiters sollte die Rückwärtskomptabilität deaktiviert sein, um Unsicherheiten durch ältere Sicherheitsmechanismen durch Downgrade-Attacken zu vermeiden.