INDUSTRIE 4.0 ÖSTERREICH

DIE METALLTECHNISCHE INDUSTRIE
Österreichs stärkste Branche

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Cyber Sicherheit: Roundtable Diskussion zu Bedrohungsszenarien und Prävention

CYBER SECURITY ALS INNOVATIONSTREIBER FÜR EINEN NACHHALTIGEN WETTBEWERBSVORTEIL

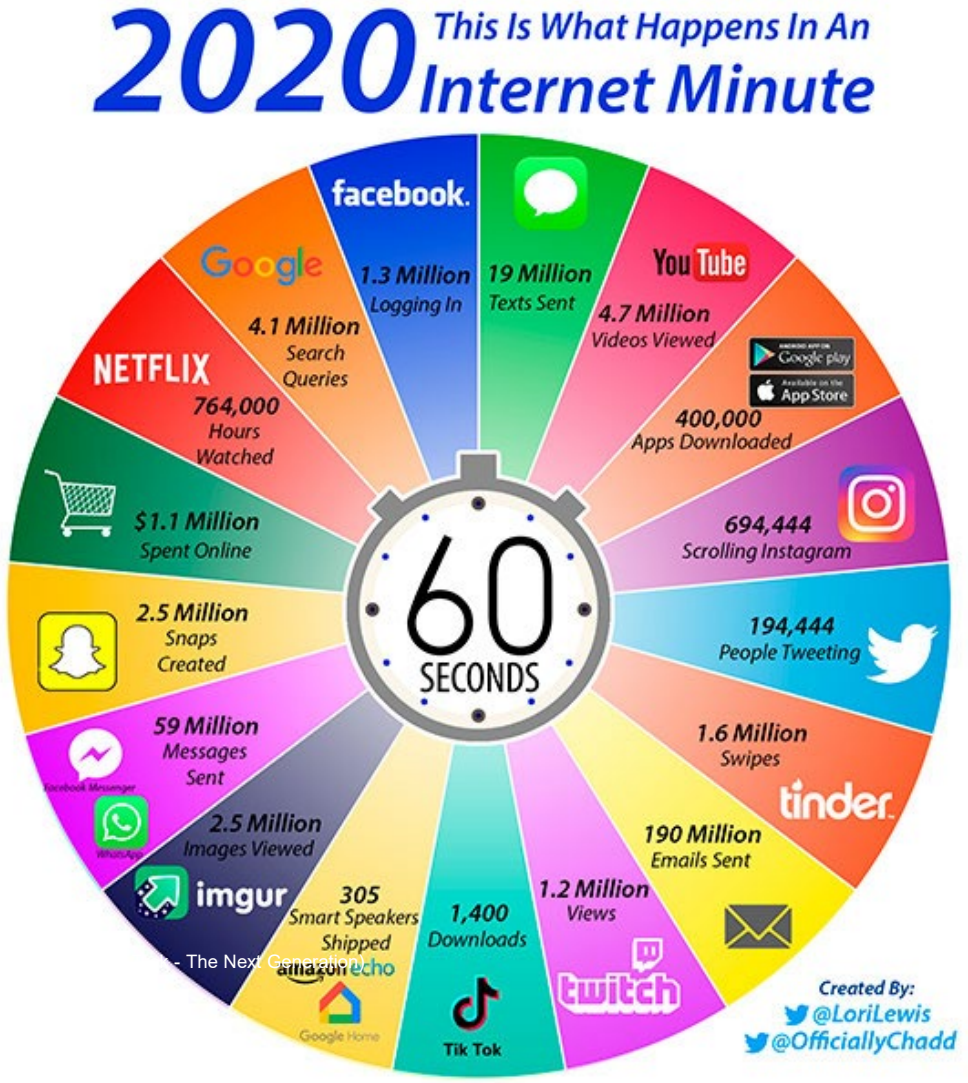
Helmut LEOPOLD
Head of Center for Digital Safety & Security
AIT Austrian Institute of Technology

Wien, 5. Dezember 2022
(v1.0)

MEGATRENDS DER DIGITALISIERUNG

Cloud Shift

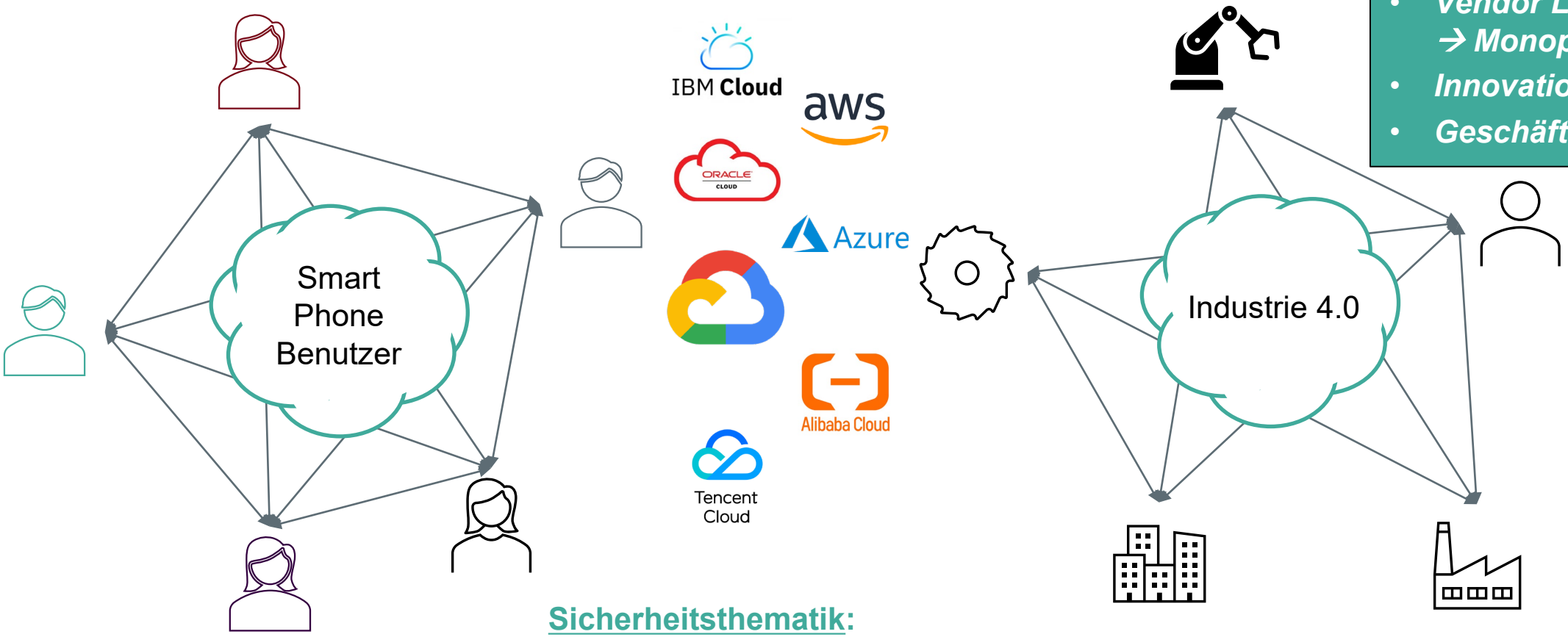
Quelle:: Paramount Television - Original publication: May 10, 1992 Immediate source: http://tng.trekcore.com/hd/thumbnails.php?album=132&page=6



„CLOUD SHIFT“ OHNE EUROPA

Geschäftsmodellthemati:

- *Verlust der Datenhoheit*
- *Vendor Lock-in Effekte → Monopole*
- *Innovationshemmend*
- *Geschäftsmodellverlust*



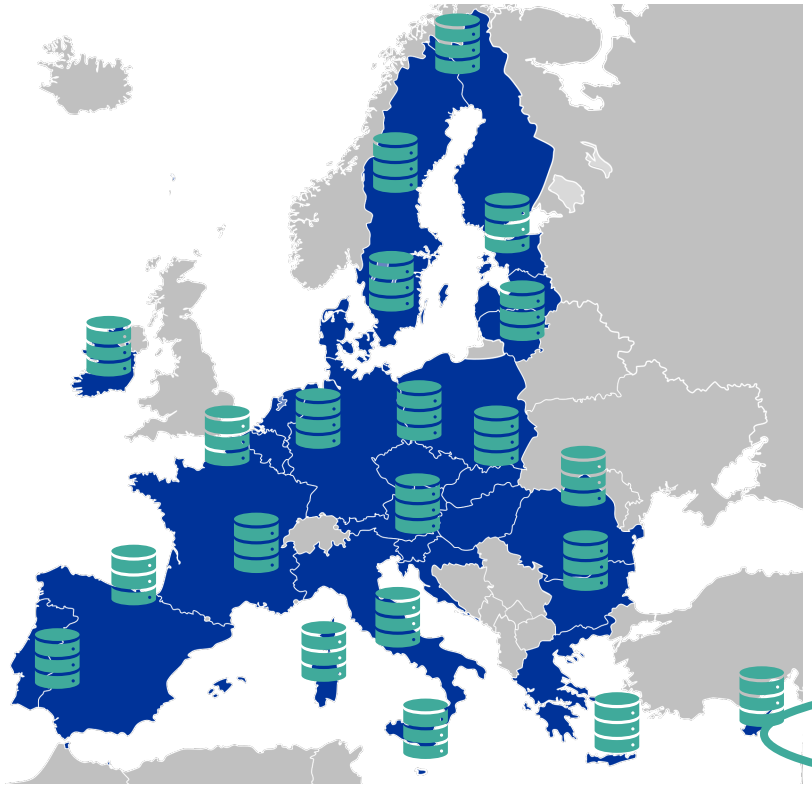
Sicherheitsthematik:

CLOUD Act: Cloud-Unternehmen müssen Zugang zu gespeicherten Daten auf jedem Server gewähren, den sie besitzen und betreiben

Ähnliche Passagen im National Intelligence Law der VR China

EUROPÄISCHE CLOUD INITIATIVE – DATENSOUVERÄNITÄT – GAIA-X

Datensouveränität und Datensicherheit sind die Imperative unserer wirtschaftlichen & gesellschaftlichen Zukunft



Social media

eHealth

Industry 4.0

Smart City

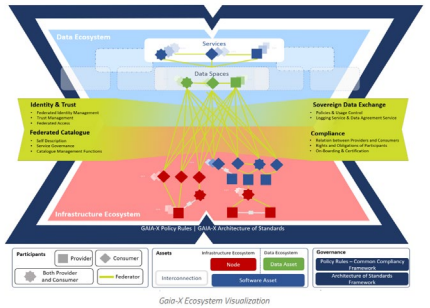
Connected Cars

Digital Transport

Smart grid

Datenautonomie: Entscheidungsfreiheit, Unbeeinflußbarkeit

- **Global wettbewerbsfähige Dateninfrastrukturen und Services**
- **Freier Austausch von Daten – Data Sharing –** Interoperabilität & Portabilität - Standardisierung
- Einfaches Wechseln zwischen Cloud-Anbietern
- Europäische **interoperable federated Cloud Services – Open Source**
- **Höchst sichere Datenaustausch und -verarbeitungsplattform**



Gaia-X Ecosystem Visualization

gaia-x Hub Austria

www.gaia-x.at

Bundesministerium Finanzen
Staatssekretariat für Digitalisierung

Federal Ministry Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

05/12/2022 Quelle: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-Europe

CYBER SECURITY

Safety & Security
IT Security
OT Security
EUROQCI
OpKoord Operativen Koordinierung
Security by Design
ÖSCS Österreichischen Strategie für Cyber-Sicherheit
IKDOK Innerer Kreis der operativen Koordinierungsstrukturen (für Cybersicherheit)
CAIS Cyber Attack Information System
Side Channel Attack
Virus
Vulnerability
Malware
CERT Computer Emergency Response Team
Cyber Security
SOC Security Operation Center
Post Quantum Sicherheit
Exploits
APT Advanced Persistent Threats
Information Security
Phishing
CISERT Computer Information Security Emergency Response Team
Computer Security
DDoS Distributed Denial of Service
IT-Sicherheitshygiene
Physische Sicherheit
Secure Coding
Cyber Resilienz
Trojaner
Remote Access Trojans (RAT)
Cyber Attack
Passwortsicherheit
Zero Day Vulnerability
Ransomware
Cyber Espionage
Penetration Test
IoT Security
Cyber Incident
Cyber Crime
Cyber Risk
Wurm
Cyber Range
Cyber Meldung
Cyber War
Supply Chain Security
Risk Management
Cyber Training
QCI Quantum Communication Infrastructure
Verschlüsselung
NIS Netz- und Informationssicherheit

https://fut

Cyberangriffe auf das österreichische Außenministerium angeblich erfolglos

"Schadsoftware konnte keine Auswirkungen entfalten." Angreifer hatten versucht, sich mithilfe von Phishing-Mails in interne Systeme

Hackerangriff auf Kärnten: 80.000 Stammdatenblätter ausgelesen

Im Rahmen des Leaks sind Datenblätter mit Namen, Geburtsdaten, Adress und Telefonnummern aufgetaucht

10. Juni 2022, 15:04, 300 Postings

https://www.derstandard.at/story/200013646 stammdatenblaetter-ausgelesen

IT-SICHERHEIT

Cyberangriff auf I Uni: Erste Daten i aufgetaucht

Unter anderem dürften Reisepässe, worden sein. Den Angriff beanspruch für sich

Mickey Manakas, Andreas Proschofsky

27. Juni 2022, 17:02, 83 Postings

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

https://www.derstandard.de/story/2000136948190/cyb uni-erste-daten-im-darknet-aufgetaucht

OÖNplus WIRTSCHAFT

Cyberangriff auf Gunskirchner Motorenhersteller BRP-Rotax

steiermark ORF.at 6.9.2022

Steiermark-News | Steiermark-Magazin | Der ORF Steiermark | Volksgruppen | Ganz Österrei

CHRONIK https://steiermark.orf.at/stories/3172339/

Hackerangriff legt Feldbacher EDV lahm

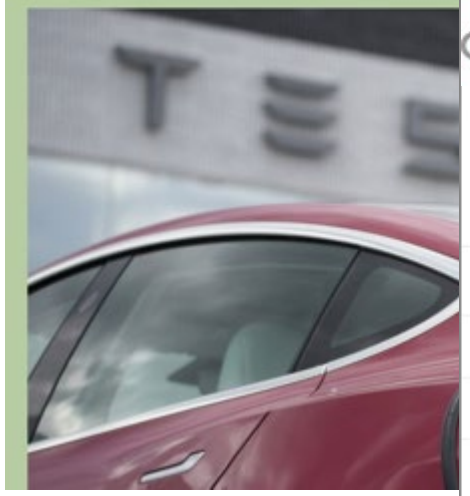
Am Wochenende ist die Stadt Feldbach Opfer eines Hackerangriffs geworden: Das EDV-System wurde übernommen; sollte die Stadt ihre Daten wiederhaben wollen, müsse Lösegeld bezahlt werden.

CYBER ANGRIFFE - SUPPLY CHAIN, IOT & KONSEQUENZEN

25 Teslas unter seine Kontrolle

Unter anderem war es ihm möglich, von außen Türen und Fenster zu entsperren und das Auto zu starten. Die Attacke lief über eine Drittsoftware

14. Jänner 2022, 08:00, 806 Postings



https://www.derstandard.at/story/200
teslas-unter-seine-kontrolle

4 Mrd USD Verlust & CEO Rücktritt

Source: https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html

Übernahme der Kontrolle: Google + ***öffentliche Info vom Hersteller***

Live-Demonstration auf der „BMLV IKT-Sicherheitskonferenz“, 1-2 Oktober 2019, Fürstenfeld

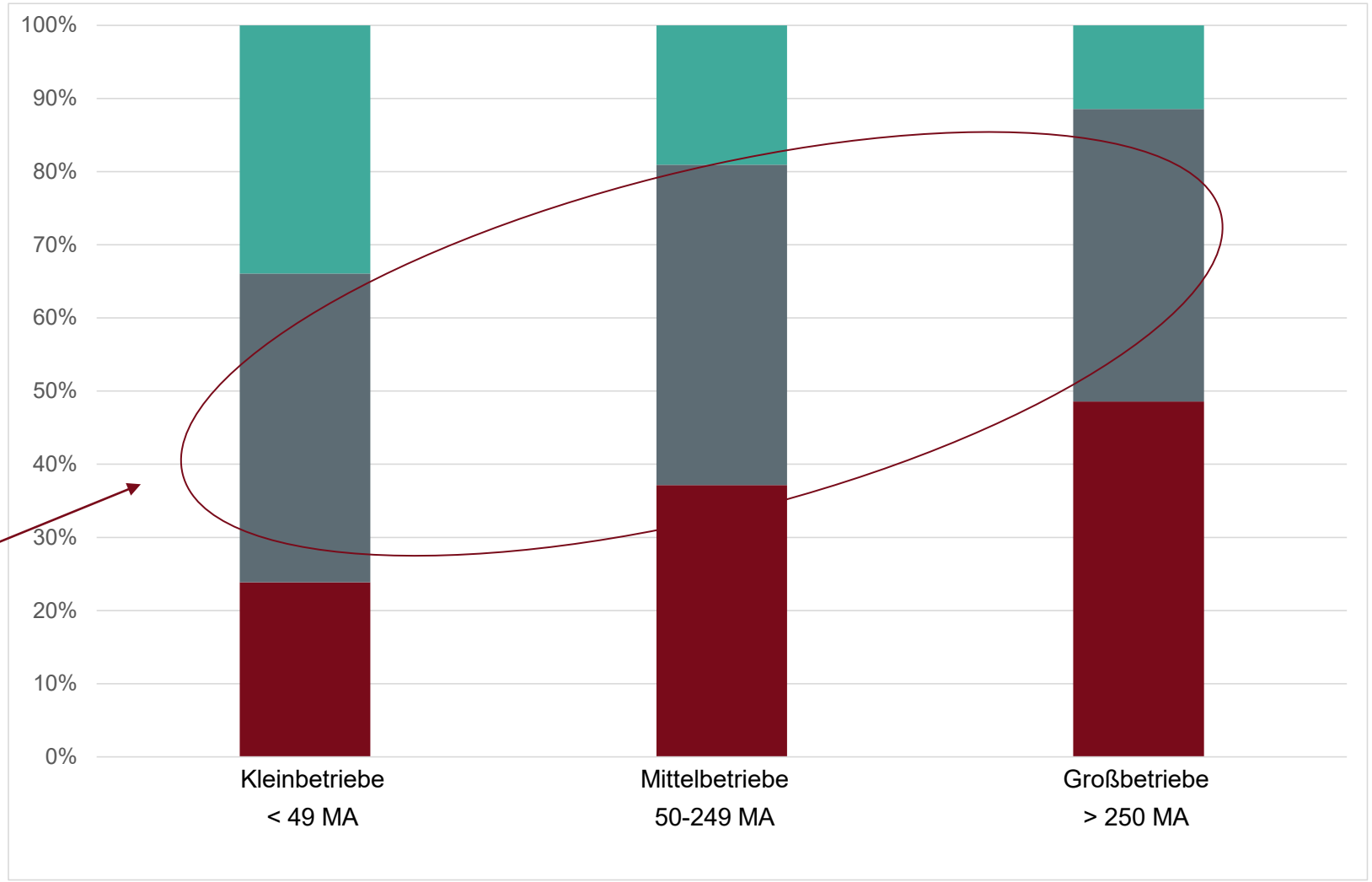
SICHERHEITSBEWUSSTSEIN IN UNTERNEHMEN

Stellen Cyber-Angriffe eine relevante Gefährdung Ihres Betriebes dar?

Marktanalyse – Projekt SIGI „*Sicherheit für die digitale Transformation der Produktion*“, 2019-2020

INDUSTRIE 4.0 ÖSTERREICH

Federal Ministry
Republic of Austria
Climate Action, Environment,
Energy, Mobility,
Innovation and Technology



„unbekannt“

Das Bewusstsein für Cyberangriffe ist im Management heimischer Betriebe zwar gestiegen, wirklich vorbereitet sind aber viele dennoch nicht!

Social media

eHealth

Industry 4.0

Smart City

Connected Cars

Digital Transport

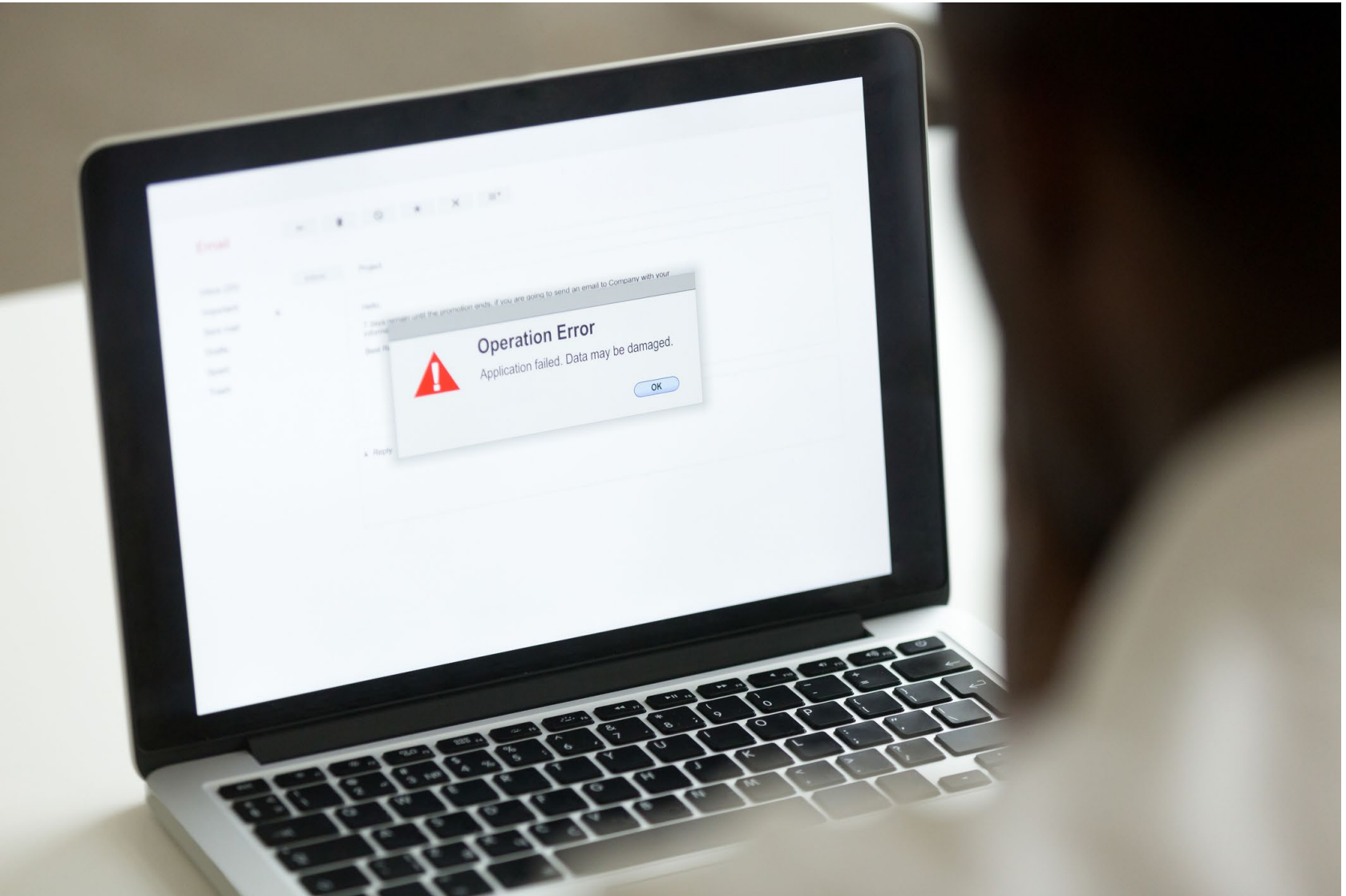
Smart grid

Die Verfügbarkeit und Funktion; d.h. die Resilienz unserer digitalen und vernetzten Infrastrukturen ist nicht mehr garantiert.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Cyber Security
Das grundsätzliche Problem

BEDROHUNG 1: JEDE SOFTWARE HAT FEHLER - "ZERO DAY VULNERABILITIES"

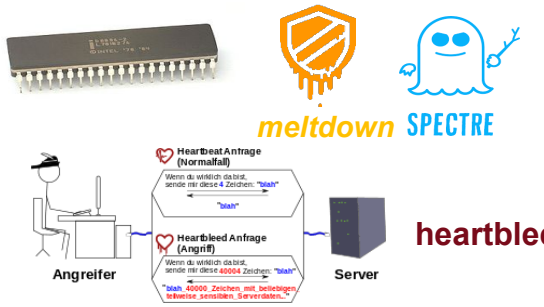


- **ca. 200k bekannte Schwachstellen**
- **70 neue Sicherheitslücken pro Tag**

7 Tage, um Schwachstellen auszunutzen

176 Tage zum Schließen von Sicherheitslücken - bis zu niemals...

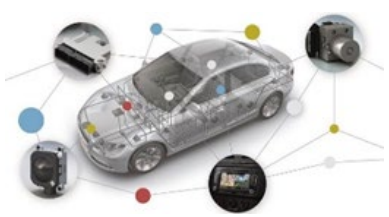
Side Channels - sichere Implementierung?

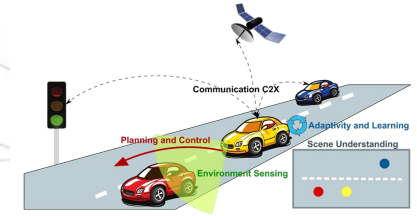


heartbleed

BEDROHUNG 2: "CYBER SECURITY IST NICHT MEHR MANUELL BEHERRSCHBAR"

- Umfassende Digitalisierung & Vernetzung
- Cloud-Shift
- Service-Shift - von Produkten zu Dienstleistungen
- Hohe Systemkomplexität
- Nutzer:innen digitaler Systeme sind mit erhöhter "Komplexität„ konfrontiert

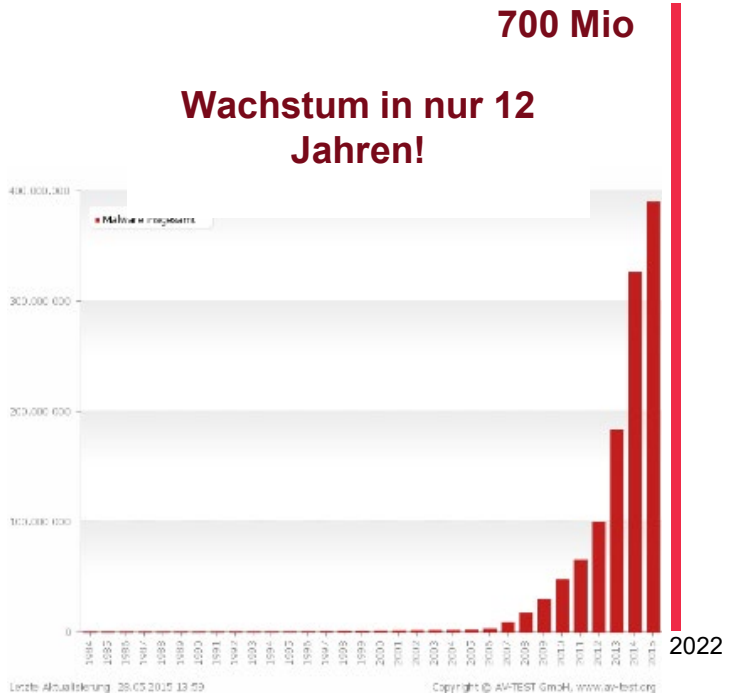




- 100 Mio Lines of Code
- 150 Steuerungssysteme
- 4 Bussysteme
- Interaktion mit Internet & Apps

BEDROHUNG 3: "THE UNKNOWN UNKNOWN"
DER ANGREIFER KENNT DEINE SCHWACHSTELLEN BEFORE DU SIE KENNST”

Über 700 Mio bekannte Malware-Typen
100-200k neue Malware pro Tag



Quelle: AV Test, SECURITY REPORT 2019/2020

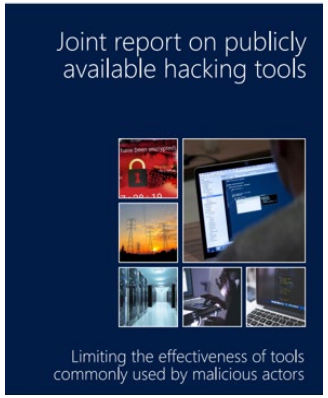
BEDROHUNG 4: “DU BIST VON ÜBERALL IN DER WELT AUS ANGREIFBAR”

- IoT
- Remote Access

SHODAN

CIA Hack 2017

Remote Access Trojans (RAT)

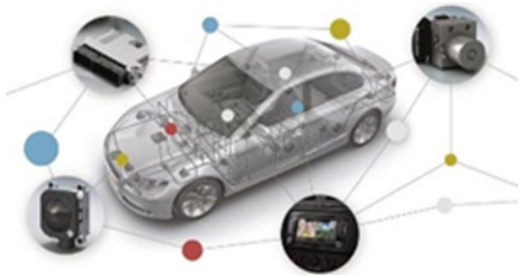


BEDROHUNG 5: “DAS BEDROHUNGSSZENARIO VERÄNDERT SICH LAUFEND”

https://images.app.goo.gl/qyHoo7ePNnxajSrg6

optischer Telegraph (Teletype), 1792/1793

elektrischer Telegraf, 1832



moderne IT-Systeme

- **Systematischer Schutzansatz**: Schutzkonzepte auf der Grundlage von Bedrohungsszenarien und Verwundbarkeitsanalysen.
- **Risk management:** Cybersicherheit erfordert eine permanente Überarbeitung der Schutzkonzepte → kontinuierliche Aktualisierung des Bedrohungsmodells für Schwachstellen und Bedrohungen.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Cyber Security Markttreiber: Gesetze & Regulierung

CYBER SECURITY MARKET DRIVERS – LAWS & REGULATION

EU Network & Information Security (NIS) for critical infrastructure operators – national laws (2018)

→ **NIS-2 (2024)**

- **Notification** within 24 hours
- **Penalties**: up to 10 million euros or up to 2% of global annual turnover
- **NIS-2**: From a few critical infrastructure operators to much more companies

For safer & more secure digital products → certification

Cybersecurity is taken into account in planning, design, development, production, delivery and maintenance phase; All cybersecurity risks are documented.

- Ensure that products with digital elements placed on the EU market have fewer vulnerabilities and that manufacturers remain responsible for cybersecurity throughout a product's life cycle;

UNECE WP29 defines clear requirements for type approval for the automotive industry - mandatory July 2024!

OEMs have to comply with UN R155 for type approval → OEMs have the requirement to manage the cybersecurity in their supply chain: design, production, Maintenance

- UN R155 - Cyber security and cyber security management system
- Cybersecurity by design to lower the risk in the supply chain

Bedrohung 1: "Jede" SW hat einen Fehler: "Zero Day Vulnerability"

Bedrohung 2: " Cybersicherheit lässt sich nicht mehr manuell verwalten"

Bedrohung 3: " Der Angreifer kennt Ihre Schwachstelle, bevor Sie sie kennen & wir müssen das Unbekannte vorhersehen (unknown unknown)

Bedrohung 4: "Jeder" kann von " überall" angreifen

Bedrohung 5: "Das Bedrohungsszenario verändert sich ständig"

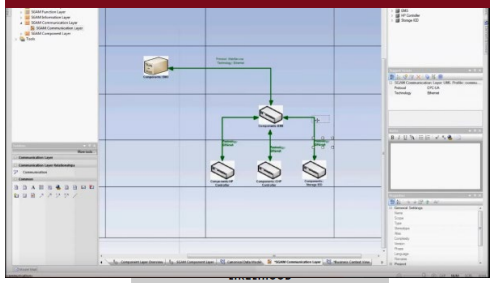
Empfehlungen für sichere IT-Systeme

EMPFEHLUNGEN

1. Positionierung der Cybersicherheit als strategisches Thema → CEO-Priorität
2. Schärfung des Bewusstseins für Bedrohungen im Unternehmen & Einführung eines Risikomanagements
3. Implementierung grundlegender Schutzkonzepte: Geschäftsprozesse, IT-Architektur, Firewalls, Virenschutz, intelligente Back-up-Systeme (!), Penetration Tests, Zugangsschutz usw. → *"IT-Sicherheitshygiene"*
4. Anwendung von Sicherheitsstandards und Zertifizierungen → Produktentwicklung und Geschäftsprozesse
5. **Implementierung moderner Schutzmechanismen für die Cybersicherheit → „High-Tech made in Austria"**

THREATGET
www.threatget.com

Security by Design



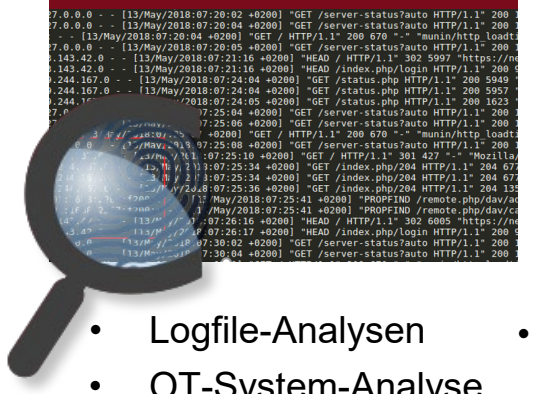
IMPACT	1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain	
1 Trivial	1	2	3	4	5	Low 1:5
2 Minor	2	4	6	8	10	Medium 6:10
3 Moderate	3	6	9	12	15	High 11:16
4 Major	4	8	12	16	20	Extreme 17:25
5 Critical	5	10	15	20	25	

LieberLieber

msg PLAUT

ÆCID
www.aecid.ait.ac.at

Artificial Intelligence attack/Anomaly Detection Online Monitoring



- Logfile-Analysen
- OT-System-Analyse
- Run-time Verification

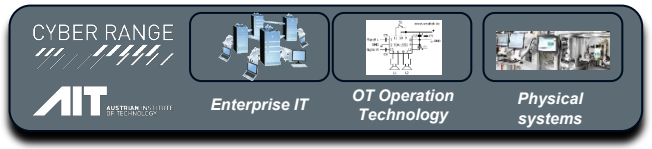
fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS
CATCH. DIRECT
www.fragmentix.com
www.catch.direct

Smart Encryption

- Hochsichere Cloud-Speicher - Post-Quantum-Safe
- Sichere verteilte Marktplätze

CYBER RANGE
AUSTRIAN INSTITUTE OF TECHNOLOGY
www.cyberrange.at

Ausbildung, Training, Qualifikation, Praxis



SAFETY & SECURITY BY DESIGN FOR AUTOMOTIVE

Model-based system development

Standards Compliance

Safety & Security modelling

EN 50128 | ISO 27001 | ISO 26262 | ISO 21434 | IEC 62443

FMVEA
Model based System Design

Threats, vulnerabilities monitoring

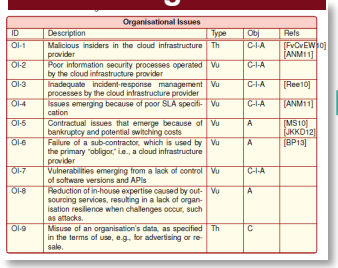
AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center

CVE

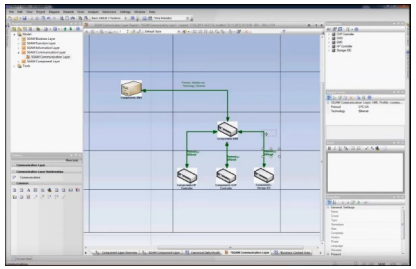
NVD

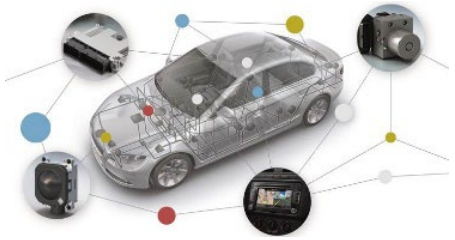
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Threat intelligence



Organisational Issues				
ID	Description	Type	Obj	Refs
OI-1	Malicious insiders in the cloud infrastructure provider	Th	C-I-A	[FvOvEW10] [ANM11]
OI-2	Poor information security processes operated by the cloud infrastructure provider	Vu	C-I-A	
OI-3	Inadequate incident-response management processes by the cloud infrastructure provider	Vu	C-I-A	[Ree10]
OI-4	Issues emerging because of poor SLA specification	Vu	C-I-A	[ANM11]
OI-5	Contractual issues that emerge because of bankruptcy and potential switching costs	Vu	A	[MS10] [JKKD12]
OI-6	Failure of a sub-contractor, which is used by the primary 'obligor,' i.e., a cloud infrastructure provider	Vu	A	[BP13]
OI-7	Vulnerabilities emerging from a lack of control of software versions and APIs	Vu	C-I-A	
OI-8	Reduction of in-house expertise caused by outsourcing services, resulting in a lack of organisation resilience when challenges occur, such as attacks.	Vu	A	
OI-9	Misuse of an organisation's data, as specified in the terms of use, e.g., for advertising or resale.	Th	C	





Threat analyses report

IMPACT	LIKELIHOOD: 1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain	
1 Trivial	1	2	3	4	5	Low 1:5
2 Minor	2	4	6	8	10	Medium 6:10
3 Moderate	3	6	9	12	15	High 11:16
4 Major	4	8	12	16	20	Extreme 17:25
5 Crirtical	5	10	15	20	25	

THREATGET
DEVELOPED BY AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

www.threatget.com

THREATGET – INTERNATIONAL INNOVATION FEASIBILITY

https://www.securecav.com/automotive-threat-modelling-off-the-shelf-solutions/

https://www.threatget.com/

MARKET PLACE 4.0 – SECURE AUCTION OF PRODUCTION CAPACITY

- Auction platform for production capacity
- Security and trust by design
- No central data storage
- decentralised data analytics (matching on encrypted data)
- Data can NOT be seen and analysed by the stakeholders of the system

CATCH. DIRECT

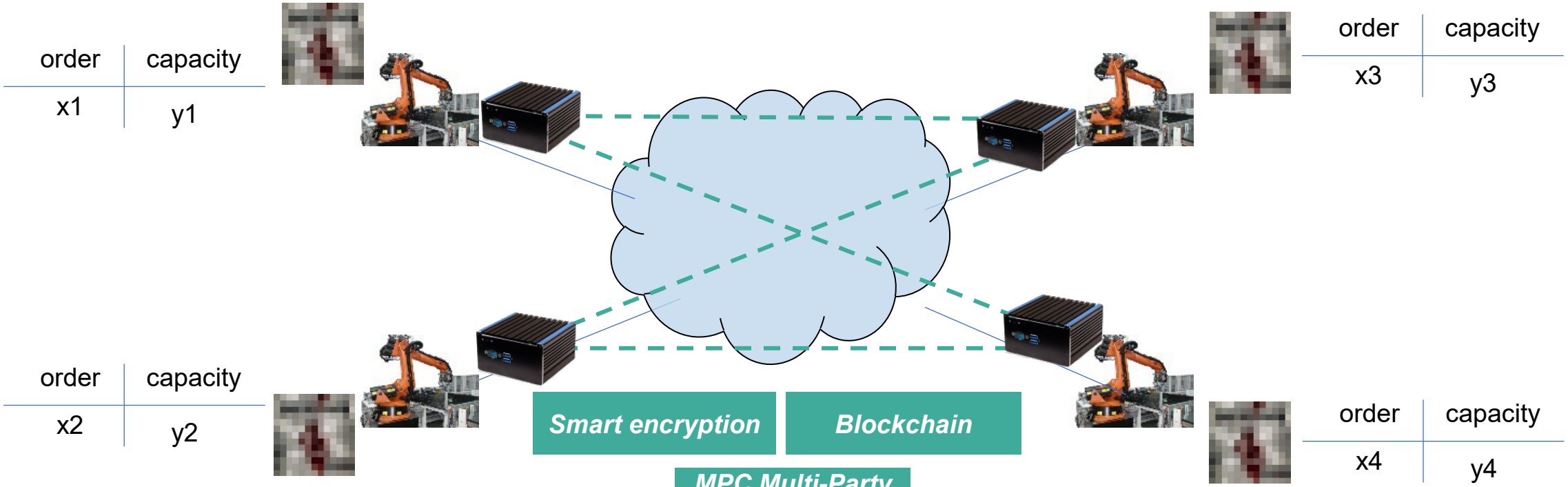
www.catch.direct/

DIGITAL LEADER AWARD

EBNER® Industrieofenbau GmbH

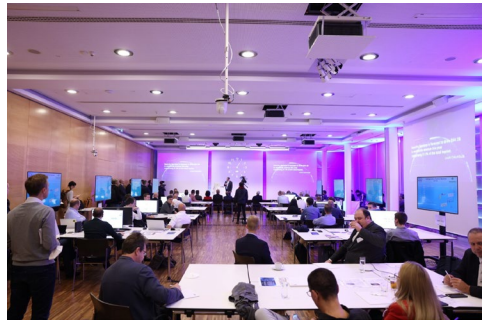
NET SERVICES

AUSTRIAN INSTITUTE OF TECHNOLOGY



AIT CYBER RANGE

AUSTRIAN INSTITUTE OF TECHNOLOGY




Advanced Persistent Threat (APT)


Ran-somware


Trojaner / Remote Access Trojaner


Botnets


Data breach (DSGVO)


Phishing


Vul-nerability


DDoS


Miconfig-uration


News


Simulation of Stakeholder (z.B. CERT, Trust Circle)


And many more…

» Learners »

Aus- und Weiterbildung sowie Zertifizierung (Kompetenzen) für verschiedene Expertenstufen

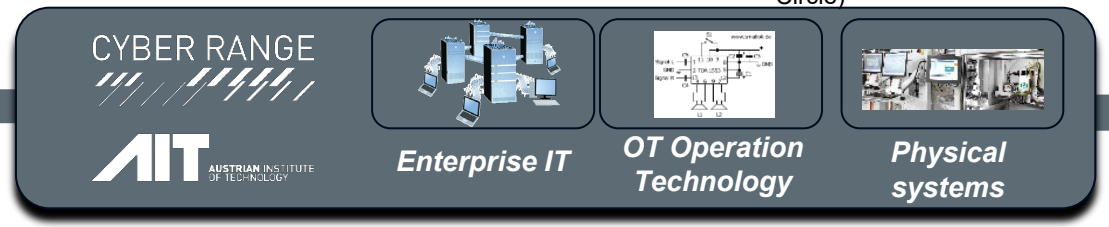
IAEA International Atomic Energy Agency

AIT Austrian Institute of Technology GmbH

IAEA Collaborating Centre

for

Information and Computer Security for Nuclear Security



« Übungen »

IKT, Prozesse, Strukturen, Richtlinien

- Training zur Bewältigung von Szenarien - Krisenteams und Management
- Testen von Schutzmechanismen und -verfahren
  - Notfallpläne und -prozesse
  - Kommunikationskanäle
- Erkennung, Analyse und Gegenmaßnahmen bei Cyberangriffen - mit IT-Tools

KSÖ Kompetenzzentrum Sicheres Österreich

CERT.at

Federal Chancellery Republic of Austria

Federal Ministry Interior

Federal Ministry Republic of Austria Defence

https://kompetenzzentrum-sicheres-oesterreich.at/wp-content/uploads/2021/09/KSOe-PLANSPIEL-2021-v2.mp4.mp4

Digital Factory Vorarlberg · Verbund · AT&S · WIEN IT · EVN · SALZBURG AG

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

DANKE!

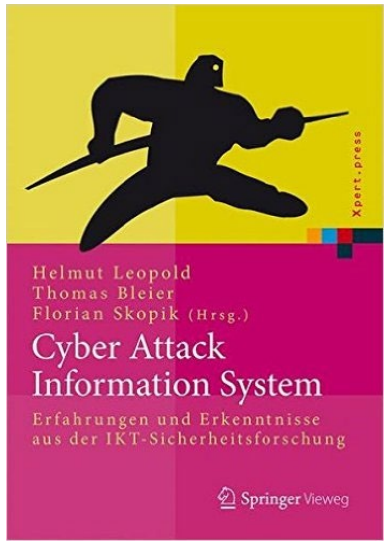
Dipl.-Ing. Helmut LEOPOLD, PhD

Head of Center for Digital Safety & Security
AIT Austrian Institute of Technology
Chair Gaia-X Hub Austria

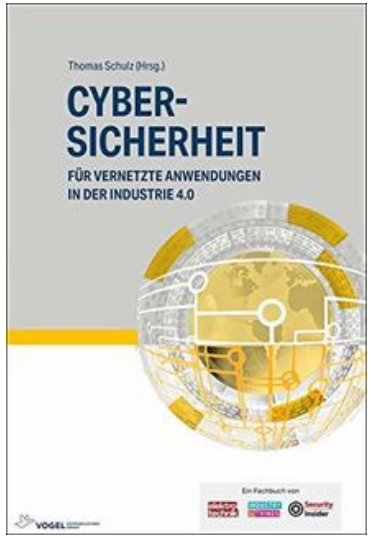
LITERATURE – FURTHER INFORMATION

- Cyber Security Expert Group of the Austrian Industry 4.0 Platfor https://plattformindustrie40.at/
- CSP Cyber Security Platform of the Austrian Federal Chancellery https://www.digitales.oesterreich.gv.at/
- Cyber Security Austria https://www.cybersecurityaustria.at/
- Vienna Cyber Security & Privacy Cluster https://visp.wien/

http://www.czernin-verlag.com/buch/30-ideen-fur-europa



https://link.springer.com/book/10.1007/978-3-662-44306-4



https://vogel-fachbuch.de/maschinenbau/automatisierung/672-cybersicherhe

https://plattformindustrie40.at/wp-content/uploads/2020/05/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf

https://thertoinnovationsummit.eu/sites/default/files/inline-files/Cybersecurity_Discussion_Paper_Final_Layout_20201023%20%281%29_0.pdf

www.bmk.gv.at/themen/innovation/publikationen/produktion/sigi.html

BILDQUELLEN

1. Slide 2:
   - Paramount Television - Original publication: May 10, 1992 Immediate source: http://tng.trekcore.com/hd/thumbnails.php?album=132&page=6
   - TrekCore is not endorsed, sponsored or affiliated with CBS Studios Inc., Paramount Pictures, or the Star Trek franchise; All STAR TREK images, trademarks and logos are owned by CBS Studios Inc. and/or Paramount Pictures — inclusion in reviews and news reporting intended as fair use under 17 U.S. Code § 107.
2. Slide 6:
   - Der Standard, 14.1.2022, 25 Teslas unter seiner Kontrolle, https://www.derstandard.at/story/2000132518550/19-jaehriger-hacker-brachte-weltweit-25-teslas-unter-seine-kontrolle
   - heise online, News, 09/2017, Hacker-Jackpot: Credit Bureau Equifax gehackt, https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html
   - Spiegel Online, https://www.spiegel.de/politik/ausland/dick-cheney-angst-vor-terroranschlag-auf-den-herzschrittmacher-a-9
   - ntv, Panorama, Fernbedienung wurde deaktiviert - Cheney fürchtete seinen Herzschrittmacher, 19.10.2013, https://www.n-tv.de/panorama/Cheney-fuerchtete-seinen-Herzschrittmacher-article11570761.html
3. Slide 12:
   - AV Test, SECURITY REPORT 2019/2020, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2018-2019.pdf
4. Slide 14:
   - Credit: SHEILA TERRY, SCIENCE PHOTO LIBRARY Early telegraph message 1794, https://images.app.goo.gl/qyHoo7ePNnxajSrg6