BUSINESS-RISIKEN DURCH CYBER-BEDROHUNGEN – CYBERSICHERHEIT ALS ERFOLGSFAKTOR

MICHAEL REITER // 04.05.2022

MELDUNGEN IM TAGESTAKT

19. April 2022
Unbefugter Zugriff auf Daten einer Uni-Bibliothek in Deutschland
Universitätsbibliothek Leipzig, Leipzig, Deutschland
Betroffen sind ca. 70.000 Datensätze mit personenbezogenen Daten.
SICHERHEITSLÜCKE IN DER UNIVERSITÄTSBIBLIOTHEK
https://www.ub.uni-leipzig.de/aktuelles/...

19. April 2022
Cyberangriff auf eine Stadt in Baden-Württemberg
Schriesheim, Baden-Württemberg, Deutschland
Rathaus: Es war ein Hackerangriff
https://www.rnz.de/nachrichten/bergstras...

18. April 2022
Cyberangriff auf Stadtwerke in Bayern
Donau-Stadtwerke Dillingen-Lauingen (DSDL), Dillingen an der Donau, Bayern, Deutschland
Cyberangriff auf die Donau-Stadtwerke DSDL
https://www.augsburger-allgemeine.de/dil...

18. April 2022
Cyberangriff auf einen Technologiedienstleister in Deutschland
TÜV NORD GROUP, Hannover, Niedersachsen, Deutschland
IT-Systeme nach Cyberattacke zügig wiederhergestellt
https://www.tuev-nord-group.com/de/newsr...

18. April 2022
Cyberangriff auf einen Dienstleister für Bibliotheken in Reutlingen
ekz.bibliotheksservice GmbH, Reutlingen, Baden-Württemberg, Deutschland
Kundeninformation über einen Cyber-Angriff bei der ekz.bibliotheksservice GmbH
https://www.ekz.de/

18. April 2022
Cyberangriff auf ein IT-Systemhaus in Bayern
Reitzner AG, Dillingen an der Donau, Bayern, Deutschland
Cyber-Angriff auf die Dillinger Unternehmen Reitzner AG und Donau-Stadtwerke
https://www.augsburger-allgemeine.de/dil...

17. April 2022
Cyberangriff auf einen Luftfahrt-Bodendienstunternehmen in Deutschland
AHS Aviation Handling Services GmbH, Hamburg, Deutschland
AHS Opfer eines Hackerangriffs – seit über einer Woche
https://www.aerotelegraph.com/abfertigun...

15. April 2022
Hackerangriff auf einen Anlagenbauer in Nordrhein-Westfalen
IMA Schelling Group, Lübbecke, Nordrhein-Westfalen, Deutschland
IT Incident

Handelsblatt
Internetsicherheit: Hackerangriff auf Microsoft: Tausende Mittelständler in Deutschland könnten betroffen sein
Internetsicherheit Hackerangriff auf Microsoft: Tausende Mittelständler in Deutschland könnten betroffen sein. Ein großer Cyberangriff auf...
08.03.2021

Handelsblatt
Colonial Pipeline : Cyberangriff legt Betrieb großer Benzin-Pipeline in den USA lahm
Die Täter wollen Colonial Pipeline offenbar erpressen: Das Unternehmen ... eine professionelle Gruppe namens „Darkside“ hinter dem Angriff.
09.05.2021

FAZ
Solarwinds-Hacker nehmen Dutzende Tech-Firmen ins Visier
Die Hacker hinter der folgenschweren Cyberattacke auf den IT-Dienstleister Solarwinds haben seit Mai rund 140 Technologie-Dienstleister...
25.10.2021

Handelsblatt
Cyberangriff: Hacker legen IT-Systeme des Autozulieferers Eberspächer lahm
Cyberangriff Hacker legen IT-Systeme des Autozulieferers Eberspächer lahm. Der Auspuffhersteller spricht von einem organisierten Angriff. Auch...
26.10.2021

IPS Infopoint Security
Der Schutz kritischer Infrastrukturen ist für die OT-Security relevanter denn je
Angesichts der weltweit anhaltenden Cyberangriffe steht die Sicherheit ... generationenübergreifenden IT/IoT/OT-BES-Umgebungen erfordert ein...
vor 3 Wochen

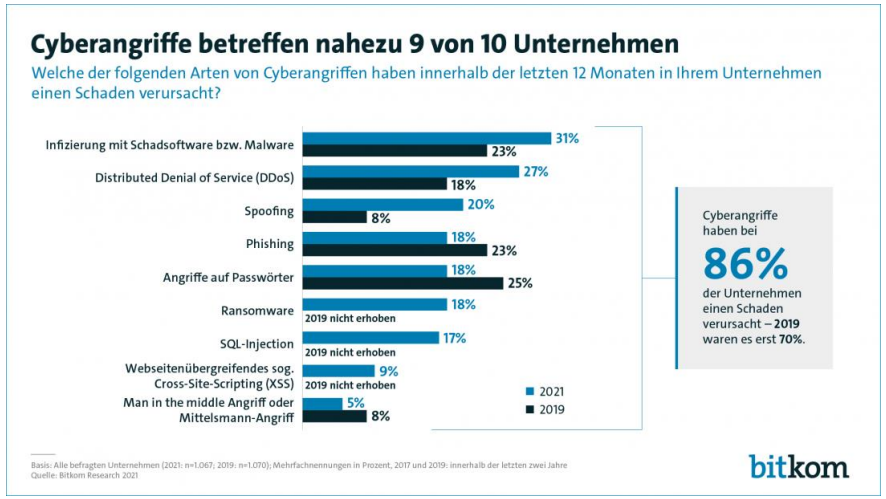
Quelle: https://konbriefing.com/de-topics/hackerangriff-deutschland.html

ES KANN JEDES UNTERNEHMEN TREFFEN

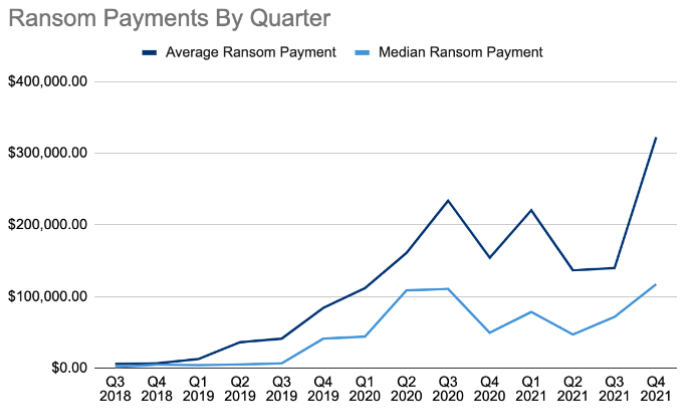
ZDF

- Diebstahl, Spionage, Sabotage:
  Neun von zehn Unternehmen wurden Opfer
- Erpressung, Systemausfälle und
  Betriebsstörungen mehr als vervierfacht
- Bereits jedes zehnte Unternehmen sieht seine
  geschäftliche Existenz bedroht
- Spitze des Eisbergs
  Dunkelziffer vermutlich wesentlich höher

Quelle: https://de.cleanpng.com/png-7rbal4/download-png.html

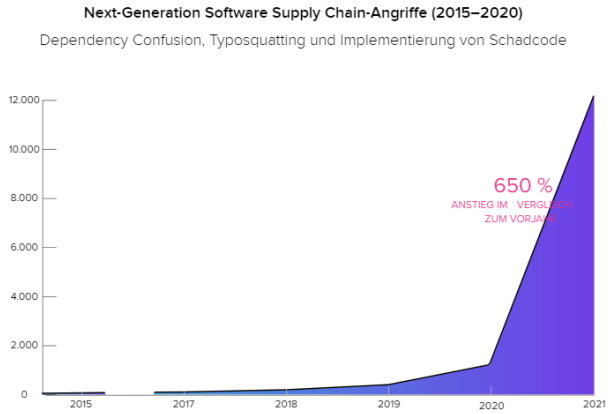


Quelle: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr



COVEWARE

Quelle: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021



Quelle: https://de.sonatype.com/resources/state-of-the-software-supply-chain-2021

CYBER WELTWEITES TOP-RISIKO

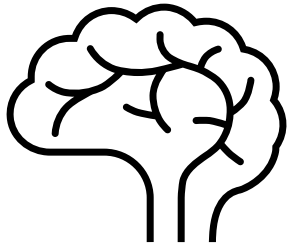
GRÜNDE

- Starke Zunahme von Ransomware-Angriffen
- Besorgniserregende Trends, wie z. B. „doppelte Erpressungstaktiken“, bei denen die Verschlüsselung von Systemen mit Datendiebstahl kombiniert wird
- Massive Zunahme an Supply-Chain-Angriffen
- Ausnutzung von Softwareschwachstellen, die potenziell Tausende von Unternehmen betreffen (z.B. Log4J, Kaseya)
- Angriffe auf kritische physische Infrastrukturen (z.B. Colonial-Pipeline, USA; Eberspächer, DE;...)

Quelle: Allianz Risk Barometer 2022

Quelle: Allianz Global Corporate & Specialty

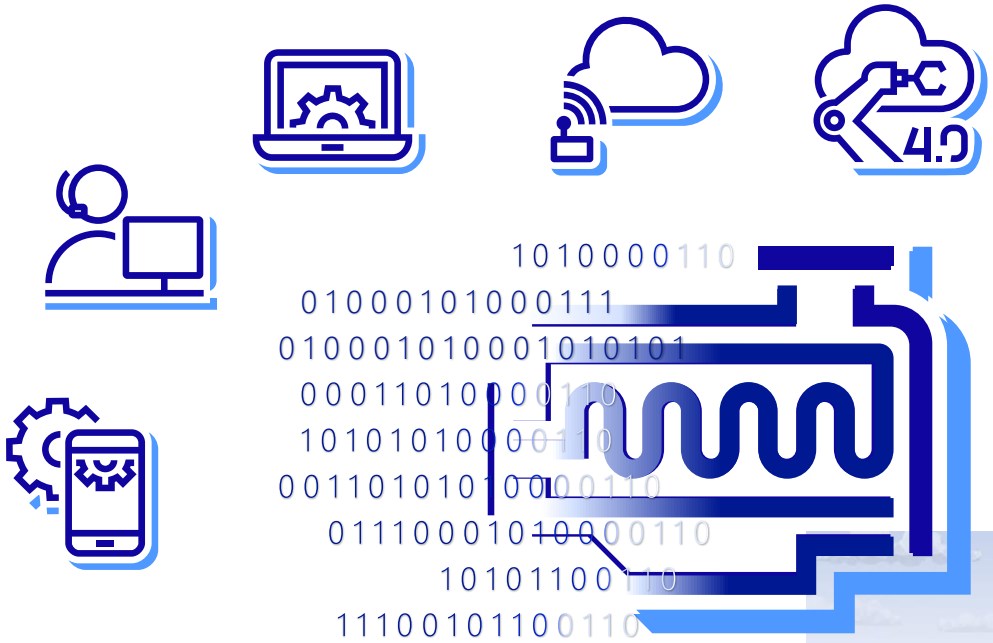
CYBER SECURITY NEU DENKEN

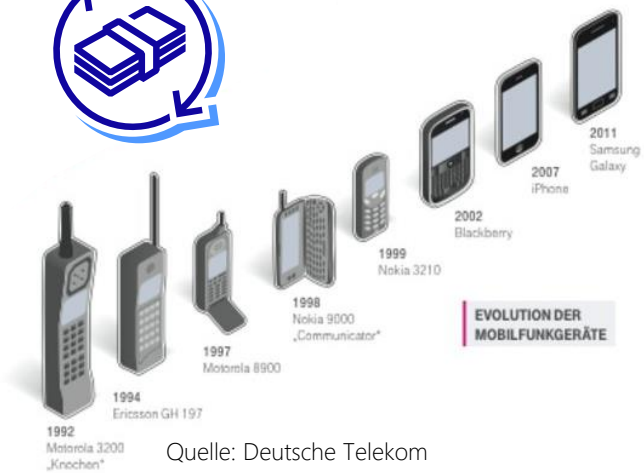


BASELINE RISK MITIGATION

BUSINESS VALUE CREATION

POTENZIALE VON IIOT





Quelle: Deutsche Telekom

ENDKUNDE	PARTNER/OEM
hohe Leistungsdaten	variabel einsetzbar
niedriger Verbrauch	effiziente Produktionseinbindung
wenig Emissionen	wenig Ausschuss
hohe Verarbeitungsgüte	niedrige Toleranzen
Wartungsarm	niedrige Fertigungskosten
hohe Zuverlässigkeit	hohe Haltbarkeit
Bestellbar	Lieferfähigkeit

Quelle: Rolls-Royce Power Systems AG

0 — 10 — 20 — 30 — Jahre

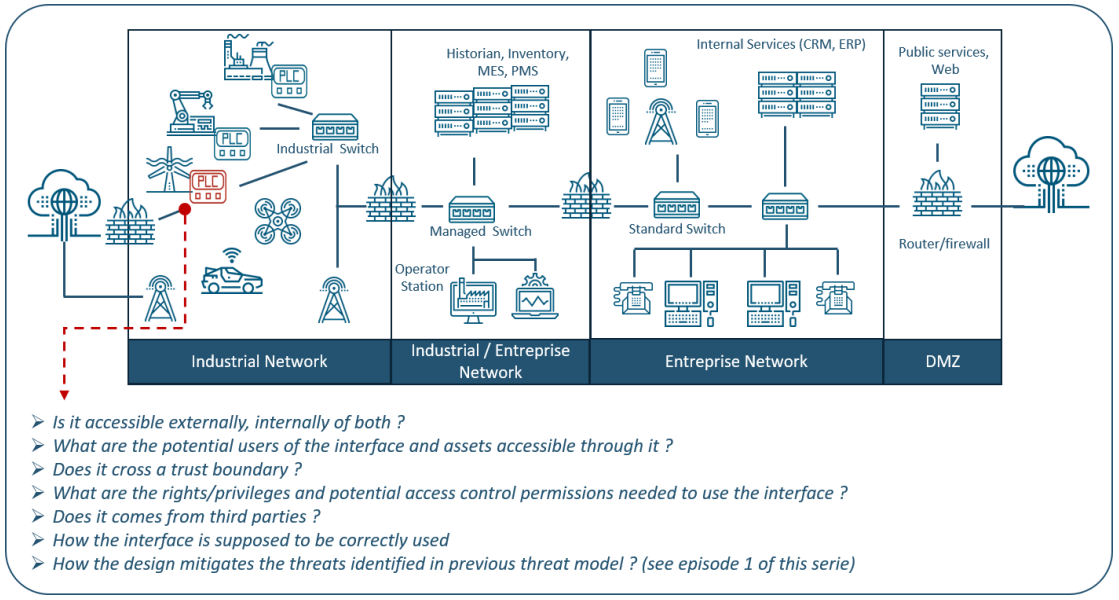
VERLÄSSLICHER PARTNER AUF DEM WEG IN DIE DIGITALE WERTSCHÖPFUNG

Herausforderungen

- Nach außen offene Schnittstellen – volle Vernetzung - kein IoT/IIoT arbeitet isoliert
- lange Lebensdauer von IoT/IIoT in Verbindung mit den raschen Fortschritten beim Wissen und Technologie (z.B. Post-Quantum Kryptografie)
- (Hacker-)Werkzeuge zur Ausnutzung von Schwachstellen werden Commodity – Zugang/Anfälligkeit steigt mit der Betriebsdauer
- Sicherstellung von Resilienz und Integrität über gesamte Lebensdauer hinweg notwendig
- Vertrauensanker (Root-of-Trust) ist tief im System integriert und ist im Allgemeinen nicht per Software upgradefähig
- Produkt/IoT unterliegt je nach Einsatzort unterschiedlichen Anforderungen & Rahmenbedingungen (Gesetze, Standards,…)
- Schwachstellen in Soft- und Hardware in Verbindung mit Trend zu Angriffen auf Supply-Chain ändern Haftung/Verantwortung

Chance: Secure by design/default

- Secure by design: ganzheitliche Betrachtung des gesamten Ökosystems und insbesondere Ziel-Einsatzort (Branchen, Umfeld,…)
- Risikobetrachtung nicht auf Cyberbedrohungen und Hackerangriffe beschränken – gesamten Produkt-Lifecycle betrachten
- Fähigkeiten und Secure by design/Secure by default transparent machen, aktiv kommunizieren und vermarkten – einen Unterschied machen!



Quelle: https://certx.com/de/cybersecurity/how-to-implement-cyber-security-acc-to-iec-62443-ep-2-secure-design/

„Erfolg besteht darin, dass man genau die Fähigkeiten hat, die im Moment gefragt sind."

Henry Ford (1863-1947)

„Einen Ruf erwirbt man sich nicht mit Dingen, die man erst tun wird."

Henry Ford (1863-1947)

CYBERSICHERHEIT MACHT PRODUKTE UND DIENSTE ZUVERLÄSSIGER, SICHERT DAS VERTRAUEN DER KUNDEN UND ERHÖHT DIE WETTBEWERBSFÄHIGKEIT

SECURE BY DESIGN UND SECURITY BY DEFAULT SIND ESSENTIELL FÜR EIN RESILIENTES PORTFOLIO UND DIE HANDLUNGSFÄHIGKEIT BEI VERÄNDERUNGEN IN DER ZUKUNFT

INVESTITIONEN IN DIE CYBERSICHERHEIT SIND INVESTITIONEN IN DEN GESCHÄFTSERFOLG

TAKE AWAYS

DISCLAIMER

Die Informationen in diesen Unterlagen sind vertraulich und dürfen nicht ohne vorherige schriftliche Genehmigung durch All for One Group SE bekannt gegeben werden. Alle Texte, Bilder und Grafiken unterliegen dem Urheberrecht und anderen Gesetzen zum Schutz des geistigen Eigentums. Alle Rechte an diesen Unterlagen sind der All for One Group SE vorbehalten.
All for One Group SE stellt diese Unterlagen ohne jegliche Verpflichtung, Gewährleistung oder Garantie, weder ausdrücklich noch stillschweigend, zur Verfügung. All for One Group SE übernimmt keine Verantwortung für Fehler oder Irrtümer in diesem Dokument, es sei denn, derartige Schäden beruhen auf Vorsatz oder grober Fahrlässigkeit. Der Inhalt dieser Unterlagen kann von All for One Group SE jederzeit geändert werden. Diese Unterlagen dienen ausschließlich informativen Zwecken und dürfen in keinen Vertrag aufgenommen, für Handelszwecke weiterverwendet oder an Dritte weitergegeben werden, soweit sie nicht für eine solche Verwendung gekennzeichnet sind oder eine vorherige schriftliche Genehmigung von All for One Group SE vorliegt.