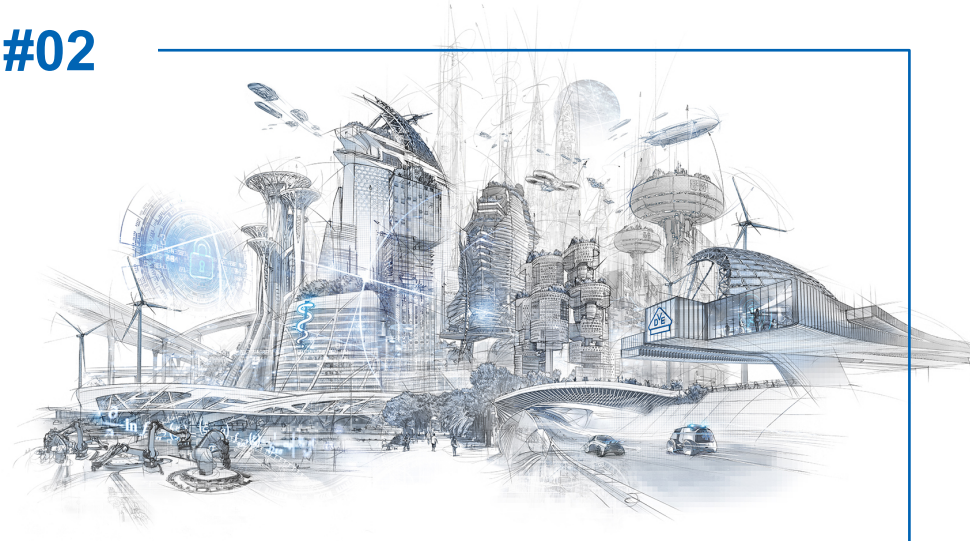

Cybersicherheit: Handlungsdruck steigt dramatisch

Ausgangssituation

Unternehmen, Behörden und Organisationen vernetzen sich im digitalen Raum. So steigt das weltweit versendete Datenvolumen zwischen 2020 und 2025 um 300 Prozent auf 175 Zettabyte. Hintergrund sind unter anderem Cloudanwendungen, Industrie 4.0 und verheißungsvolle Entwicklungen im Bereich der Künstlichen Intelligenz, sowie die exponentiell wachsende Anzahl der vernetzten „Dinge“ im globalen „Internet der Dinge“ (IoT, Internet of Things). Der Bedarf nach Cybersicherheit wächst entsprechend und gewinnt durch den Corona-bedingten Homeoffice-Boom nochmals an Bedeutung.

Problemlage

Die EU-Arzneimittelbehörde EMA, die MDax-Konzerne Symrise und Software AG, die Düsseldorfer Uniklinik – selbst der Vatikan und viele andere sind Opfer von Cyberattacken geworden. Produktionsstätten wurden heruntergefahren, an der Düsseldorfer Uniklinik musste im September 2020 sogar die Notaufnahme schließen. Kennzahlen und Bedrohungsszenarien:

- **Kosten:** Laut Bitkom-Erhebung belaufen sich die Schäden der massenhaften Cyberangriffe deutschlandweit auf über 100 Milliarden Euro pro Jahr. Weltweit veranschlagt das Center for Strategic and International Studies (CSIS) für 2020 die Schäden auf 1 Billion US-Dollar – das ist gegenüber 2018 eine Verdopplung.
- **Fokus Mittelstand:** KMU mangelt es oft an Ressourcen, um Cybersecurity Strategien aufzustellen und umzusetzen. Das produzierende Gewerbe ist besonders betroffen: 30 Prozent der Chemieunternehmen und 31 Prozent der Maschinenbauer wurden bereits durch Cyberangriffe geschädigt. Deshalb meiden KMU oftmals das Thema Industrie 4.0 und digitale Geschäftsmodelle. Damit riskieren die Verantwortlichen die Zukunftsfähigkeit ihres Unternehmens – eine massive Gefahr für den Standort Deutschland und unsere Volkswirtschaft.
- **Fokus KRITIS:** Mögliche Attacken auf die Kritische Infrastruktur (KRITIS) wie zum Beispiel, Stromversorgung, Behörden und Krankenhäuser bergen ein erhebliches Gefährdungspotenzial. Dazu erklärte das Bundeskriminalamt im September 2020: „Es ist insgesamt davon auszugehen, dass Cyberkriminelle die Notlage von KRITIS-Einrichtungen (v.a. aus dem Bereich des Gesundheitswesens) ausnutzen.“
- **Erpressung:** Erpressungen nehmen einen immer breiteren Raum ein. Dabei spionieren Kriminelle die digitalen Systeme gezielt aus und verschlüsseln Daten mittels sogenannter Ransomware. Bei den betroffenen Firmen führen die Attacken mitunter zum Betriebsstillstand. Erst nach Zahlung hoher Bitcoin Lösegelder geben die Erpresser die Daten wieder frei.
- **Industriespionage:** Cyberkriminelle spionieren zunehmend wertvolle Daten und Innovationsideen aus. Geschäftsmodelle und Existenzen von Unternehmen können dadurch akut gefährdet werden. Gleichzeitig wird die Reputation der angegriffenen Unternehmen geschädigt.

- **Geopolitische Motive:** Hinter den Cyberattacken beispielsweise auf den Deutschen Bundestag 2015 oder auf ein israelisches Wasserkraftwerk im April 2020 werden vielfach staatliche Auftraggeber vermutet. Das Bundesinnenministerium nennt namentlich Russland, China und den Iran – allerdings ist die Beweisführung schwierig bis unmöglich. Auch „befreundete“ Staaten nutzen den Cyberraum zur Spionage in Deutschland.

Wo sollte die Politik anpacken?

Die aktuell wichtigste Aufgabe der Bundesregierung lautet: Die Cyber-Sicherheitsstrategie (CSS) von 2016 zu überarbeiten und bis Mitte 2021 im Kabinett zu verabschieden. Dabei kommt es auf folgende Punkte an:

- Schnellere Reaktionszeit: Je schneller etwaige Schwachstellen in Softwareanwendungen bekannt sind, desto zügiger können betroffene Unternehmen etwaige Gefahren durch Updates beheben. Die CSS 2021 muss die Industrie zu einer freiwilligen Selbstverpflichtung motivieren.
- KMU unterstützen: KMU können die steigende Gefahrenlage schon aus Ressourcengründen nicht alleine beherrschen. Im Rahmen der CSS 2021 müssen Anreize gesetzt werden, damit sie sich auf einer unabhängigen Plattform zu IT-Sicherheits-Problemen unterstützen und etwaige Maßnahmen koordinieren.
- Standardisierung und Zertifizierung vorantreiben: Schon in der Entwicklungsphase muss die Sicherheit bei Schlüsseltechnologien höchste Priorität genießen. Grundlage dieses sogenannten Security-by-design-Ansatzes ist die internationale und europaweite Standardisierung. Staatliche Akteure wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind dabei zu beteiligen.
- Informationsaustausch verbessern: Staat und Wirtschaft müssen intensiver zusammenarbeiten. Austauschplattformen wie UP KRITIS und Normungsgremien sollten dazu genutzt und deren Arbeit eng verzahnt werden. Auch freiwillige Selbstverpflichtungen der Industrie zahlen auf dieses wichtige Ziel ein.
- Sichere Hardware verbauen: Damit Europa mittelfristig eine souveräne und sichere Datenintrastruktur zur Verfügung steht – Stichwort GAIA-X – dürfen nur vertrauenswürdige Ausrüster zum Zuge kommen.

Wie kann der VDE unterstützen?

Sicherheit ist Kernbestandteil der DNA der Technologieorganisation VDE. Genauso wie sich die Wertschöpfung mehr und mehr in den digitalen Raum verlagert, wird der VDE seiner Aufgabe gerecht, Sicherheit auch in diesem Bereich zu fördern:

- **Normung:** Der VDE erarbeitet in seiner Normungsorganisation DKE globale Standards, um kritische Infrastrukturen zu schützen – siehe die Normenreihe IEC 62443 zum Thema Cybersicherheit in der Industrieautomation oder die IEC 62351 zur sicheren Kommunikation in der Energieversorgung.
- **Standardisierung:** KRITIS-Betreiber wie Energieversorger oder Banken müssen branchenweite Mindeststandards erarbeiten und diese vom BSI genehmigen lassen. Die Normungsorganisation VDE DKE unterstützt Branchen und Behörden dabei.
  Beispiel: Damit deutschlandweit die Ampelanlagen jederzeit sicher funktionieren, hat VDE DKE alle interessierten Kreise – von den Stadtwerken bis zu den Herstellern zusammengebracht und gemeinsam entsprechende Standards erarbeitet.

Ihr Ansprechpartner

Markus B. Jaeger, Head of Political Affairs
VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

Bismarckstraße 33, 10625 Berlin
Mobil +49 171 7631986
markusb.jaeger@vde.com