Hyperkonnektivität verursacht Hyperrisiken – und verlangt nach Hyperresilienz. Am besten digital souverän!

Von Joachim Jakobs

Mit „Hyperkonnektivität“ bezeichnen Protagonisten die Digitalisierung/Automatisierung durch breitbandig vernetzte (industrielle) Dinge, die Auswertung der Kommunikation zwischendrin sowie die (Fern-)Steuerung der Geräte durch cloudbasierte KI-Quantencomputer; damit sollen für den Industriestandort Deutschland gewaltige Möglichkeiten für neue Produkte und deren Fertigung, die Kundenbetreuung, Energiewirtschaft oder auch das Gesundheitswesen einhergehen. Der Verbrauch natürlicher Reserven lässt sich reduzieren und gleichzeitig der Nutzen erhöhen. Der Verband der Elektro- und Digitalindustrie hofft auf eine Wertschöpfung bis 2035 in Höhe von 182 Milliarden Euro – was einer Verdopplung gegenüber 2025 entsprechen soll. In 10 Jahren könnte die Technik außerdem 1,5 Millionen bislang fehlende Arbeitskräfte in Deutschland ersetzen.

Umgekehrt gehen mit der Hyperkonnektivität allerdings auch Hyperrisiken einher – so sind in den Lieferketten Lieferengpässe, Überbestände oder Verschwendung zu befürchten, wenn die Algorithmen fehlerhaft sein sollten. Ganz zu schweigen davon, dass Kriminelle von der KI nur „nutze Sicherheitslücken aus“ verlangen müssen, um Betriebssysteme und Anwendungen aller Art zu kompromittieren. Selbst Laien sind in der Lage, gewaltige Schäden zu verursachen. Was bisher Tage oder Wochen dauerte, läuft nun in Sekunden ab.

Diese Entwicklung zwingt die Verantwortlichen zum Umdenken. Konzerne, Behörden und Kleinstunternehmen müssen ihre Sicherheitsstrategie von „reaktiv“ zu „proaktiv“ umstellen. Denn Prävention ist günstiger als Reaktion:

Nach einem Cyberangriff

- Systeme neu aufzubauen,
- Lösegeld,
- Bußgeld,
- Kosten für rechtliche Beratung,
- Gutachten,
- Gerichte
- Schadenersatzforderungen sowie
- den beschädigten Ruf wiederherzustellen

ist wesentlich teurer als von Beginn an in den Schutz vor Cyberbedrohungen zu investieren. Jedes Unternehmen muss die Prävention individuell auf ihre Strategie abstimmen.

Das ist keine Empfehlung, sondern für viele Unternehmen durch die zweite „Richtlinie zur Sicherung von Netz- und Informationssystemen (NIS-2)“ der Europäischen Union Pflicht. Diese „Rechenschaftspflicht“ der NIS-2 gilt seit Ende letzten Jahres und verlangt nach einer ganzen Batterie von Maßnahmen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
2. Bewältigung von Sicherheitsvorfällen;
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Diese Maßnahmen „müssen“ der Gesetzgeberin zufolge „unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.“

„Als Stand der Technik“ gilt der Bundesregierung „der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst in der Praxis mit Erfolg erprobt worden sein.“

Stand der Technik ist außerdem für

- die Datenschutzgrundverordnung (DSGVO),
- das Cybersicherheitsgesetz (Cyber Resilience Act, CRA) für Produkte mit „Digitalen Elementen“ und
- die Verordnung zur digitalen operationalen Resilienz (DORA) in der Finanzwirtschaft

maßgeblich.

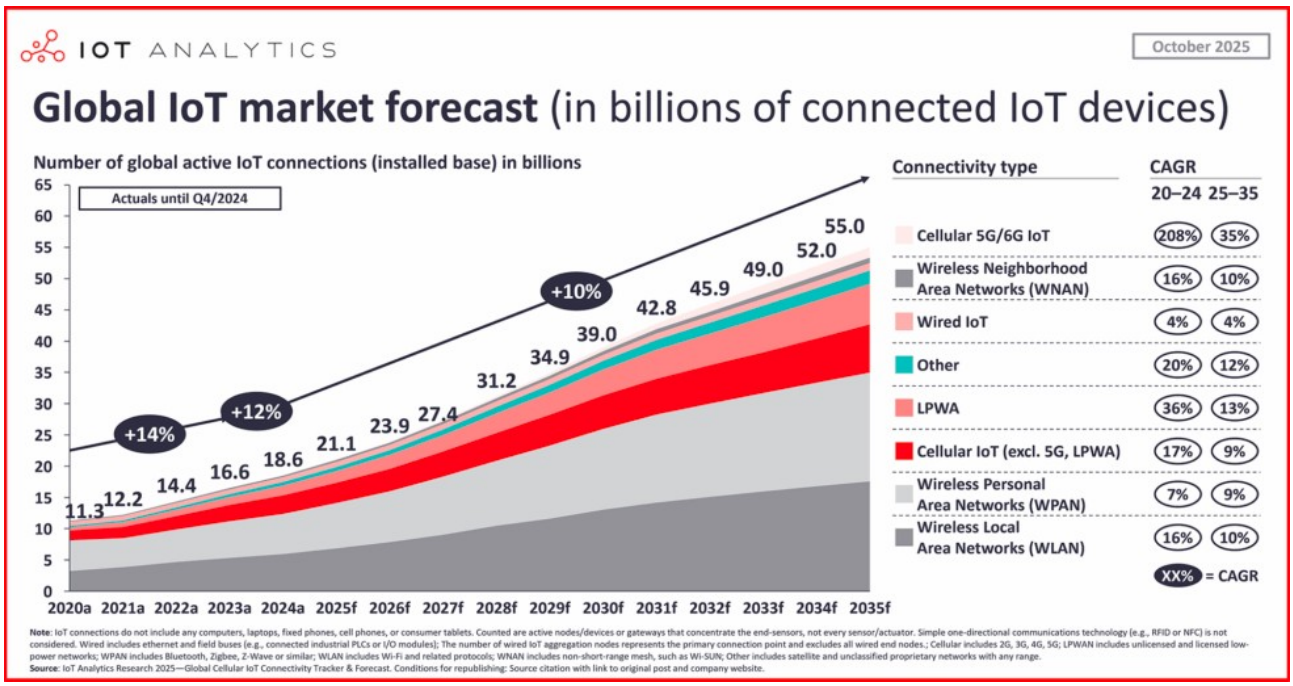

Bild: IoT-Analytics

Doch da droht ein besonderes Problem: Angriffe auf Industriell vernetzte Geräte (wie Industriemotoren) sollen 2025 um 87 Prozent zugenommen haben – was „lebensbedrohliche“ Konsequenzen nach sich ziehen könnte. Etwa durch fehlerhaft vernetzte Autos oder medizinische Implantate. Tödliche Unfälle mit Robotern hat es bereits gegeben. Warnungen vor ebensolchen Angriffen auch. Deshalb „sind Produkte mit digitalen Elementen in den folgenden fünf Ausnahmesektoren: Medizinprodukte, Fahrzeuge, In-vitro-Diagnostika, zivile Luftfahrt und Produkte im Kontext der nationalen Sicherheit“ vom CRA ausgenommen. Für diese gelten besondere Vorschriften.

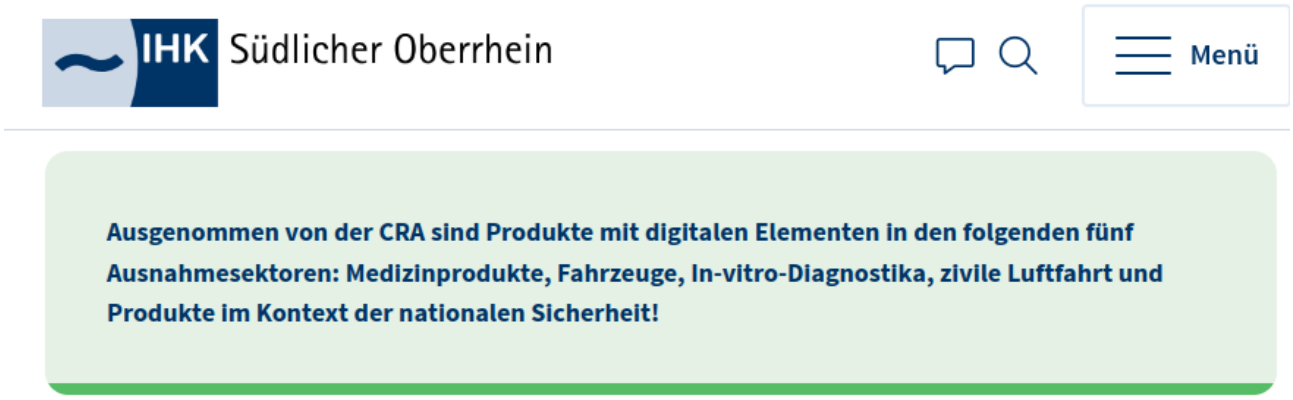

Bild: IHK Südlicher Oberrhein

Das diesbezügliche Bewusstsein scheint jedoch ausbaufähig zu sein:

- Neu angeschaffte Maschinen ohne Cybersicherheitsprüfung,
- Industrieanlagen mit unsicheren Fernzugriffsbedingungen,
- Industriegeräte mit veralteter Software,
- Unternehmen ohne Fachabteilungen für die Sicherheit Operativer Technik,
- ein unvollständiger Überblick über „die technologischen Abhängigkeiten innerhalb des Unternehmens“ sowie
- ein nicht vorhandenes Risikomanagement

deuten darauf hin, dass bislang nicht alle Verantwortlichen den Zusammenhang aus Digitalisierung, Risiken und Rechtsfolgen verstanden haben. Das wiederum könnte damit zusammenhängen, dass die IT-Regelkonformität sogar von Spitzenpolitikern und der Wirtschaftspresse diskreditiert werden. Warum sollte sich eine Mittelständlerin mit der Rechenschaftspflicht beschäftigen, wenn sie doch aus allen Rohren erfährt, dass Datenschutz nur was für Doofe ist?! Nicht einmal das Wissen darüber, dass sich „Datenschutz“ und „Datensicherheit“ nicht nur syntaktisch, sondern vor allem auch semantisch unterscheiden könnten, dringt ins Großhirn!

Mit der Folge, dass das BSI den meisten Firmen nicht mal das "Seepferdchen" zubilligt, „um sicher an den Beckenrand schwimmen zu können“. Das Seepferdchen ist ein „CyberRisikoCheck“ der einen wirkungsvollen „Schutz für kleine und Kleinstunternehmen nach DIN SPEC 27076“ verspricht. Ob der Schutz tatsächlich „wirkungsvoll“ ist, ist noch dazu strittig.

UNO-Generalsekretär António Guterres warnt zu Recht vor dem böswilligen Einsatz von KI-Systemen „zu terroristischen, kriminellen oder staatlichen Zwecken“ was „ein schreckliches Ausmaß an Tod und Zerstörung, ein weit verbreitetes Trauma und tiefe psychologische Schäden in unvorstellbarem Ausmaß verursachen“ könnte.

Daher ist es notwendig, IT-Sicherheitslücken in fraglichen Hardwareprodukten als „Konstruktionsfehler" zu bewerten, wenn diese ohne Rücksicht auf den „Stand von Wissenschaft und Technik“ verkauft werden. Darunter versteht die Bundesregierung den „Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgegebene Ziel für erforderlich gehalten werden und das Erreichen dieses Ziels gesichert erscheinen lassen.“

Darüberhinaus können Konstruktionsfehler Schadenersatzklagen begründen – auch gegen die Verantwortliche persönlich.

Hypervernetzte Unternehmen, ihre Entscheider, Geschäftspartnerinnen und Geldgeber sind technisch, rechtlich und finanziell gefährdet; um das damit verbundene Risiko zu begrenzen, ist „Hyperresilienz“ notwendig; das bedeutet, sie müssen über die Fähigkeit verfügen, Risiken mithilfe automatisierter, datengesteuerter und vernetzter Systeme proaktiv zu erkennen, intelligent zu mindern und sich schnell davon zu erholen.

Die Gesetzgeberin verlangt, dass die dazu notwendigen Prozesse (samt den Daten) innerhalb des gesicherten Europäischen Rechtsrahmens stattfinden. Die mögliche Erpressung (nicht nur durch die US-Amerikanische Bundesregierung) unterstreicht, wie wichtig es ist, dass Betriebssysteme, Rechenzentren, Kommunikations- und Zahlungsdienste innerhalb Europas kontrolliert werden. Insbesondere, wenn Menschen an Leib und Leben bedroht werden könnten. Ärger könnte jedoch auch dadurch entstehen, dass ein Anbieter beschließt, Betriebssysteme/Anwendungen

nicht länger zu unterstützen. Es ist ein wichtiges Signal, dass die Bundesregierung im Mai 2026 die Förderung von KDE GNU/Linux mit 1,3 Millionen Euro bekanntgegeben hat. Ein wichtiges Signal für die Bedeutung Digitaler Souveränität! In dem Maß, in dem Ausfälle Unternehmen, Kunden, und Lieferanten belasten, werden die Anbieterinnen von Eigen-/Fremdkapital sowie (Cyber-)Versicherungen die Daumenschrauben bezüglich digital souveräner Regelkonformität anlegen.

Darüberhinaus wärs gut, wenn der Staat für das notwendige Bewusstsein – insbesondere der Verantwortlichen! – sorgen würde. Denn ‚Verantwortlich' zu sein, bedeutet nicht nur, für eigene Pflichtversäumnisse grade zu stehen, sondern auch für die Versäumnisse derer zu haften, die im Auftrag tätig sind. Das sind Alle, die auf Geheiß der Verantwortlichen an der Planung, Entwicklung, Einrichtung, Verwaltung oder Nutzung von Software beteiligt sind, mit deren Hilfe vernetzte Geräte gesteuert oder personenbezogene Daten verarbeitet werden sollen. Innerhalb und außerhalb der eigenen Institution. Wenn diese Verantwortlichen das verinnerlicht haben, werden sie damit beginnen, die erforderlichen „Technischen und Organisatorischen Maßnahmen“ zu ergreifen, um „Hyperresilienz“ zu erzielen.

Dann – und nur dann! -- werden sich gewaltige Möglichkeiten für den Industriestandort Deutschland durch die Hyperkonnektivität ergeben!