»Handlungsfähigkeit entsteht vor dem Angriff«

Cyberangriffe legen Produktionslinien still, unterbrechen Lieferketten und kosten Vertrauen. Gleichzeitig verlangen NIS2, der Cyber Resilience Act und die KI-Regulierung von Unternehmen neue Nachweise. Wie der industrielle Mittelstand beides zusammenbringt, erklären Dr. Maria Wolf und Rolf Strehle. Sie führen gemeinsam die ditis Systeme, ein Unternehmen der Voith-Gruppe, das seit über 25 Jahren IT- und OT-Infrastrukturen in der Industrie schützt. Ihr Befund: Wer Cybersicherheit als reine IT-Aufgabe behandelt, verliert im Ernstfall die Kontrolle. Resilienz ist Führungsaufgabe.

Rolf Strehle und Dr. Maria Wolf auf der Wilhelmsburg in Ulm (Quelle: KI-generiert)

Viele Unternehmen beschäftigen sich derzeit mit NIS2, dem Cyber Resilience Act, der KI-Regulierung – und mit steigenden Angriffszahlen. Warum reicht klassische IT-Sicherheit heute nicht mehr aus?

Strehle: Weil ein Cyberangriff heute selten nur einzelne Systeme trifft. Er trifft Abläufe, die Produktion, die Lieferfähigkeit und am Ende das Vertrauen der Kunden. Gerade in der Industrie hängen Office-IT, Anlagen, Netzwerke und Geschäftsprozesse eng zusammen. Wer nur die Büro-IT absichert, übersieht die Hälfte des Risikos. Deshalb sprechen wir von Cyberresilienz. Es geht nicht mehr allein darum, Angriffe zu verhindern. Unternehmen müssen ihre Schwachstellen kennen, Angriffe früh erkennen, schnell reagieren können – und den Wiederanlauf vorbereitet haben. Das zusammen entscheidet, ob ein Vorfall ein Zwischenfall bleibt oder zur Existenzfrage wird.

Wolf: Die Regulatorik macht dabei nur sichtbar, was Unternehmen ohnehin brauchen: klare Verantwortlichkeiten, dokumentierte Prozesse und belastbare Entscheidungswege. Cyberresilienz ist keine technische Zusatzaufgabe, sondern Teil guter Unternehmensführung. Wer erst während eines Vorfalls klärt, wer entscheidet, wer meldet, wer kommuniziert und wie der Betrieb weiterläuft, verliert die Zeit, die dann am meisten fehlt. Diese Fragen lassen sich vorher beantworten. Das erwarten Gesetzgeber, Kunden und Versicherer inzwischen auch. Für die Geschäftsführung kommt hinzu: Mit NIS2 ist die Verantwortung ausdrücklich auf der Leitungsebene angekommen. Aufgaben kann man delegieren, die Verantwortung nicht.

Herr Strehle, Sie sprechen von »Cybersecurity made in Germany«. Warum ist digitale Souveränität für europäische Unternehmen ein Sicherheitsfaktor?

Strehle: Souveränität heißt für mich nicht Abschottung. Es heißt, die Kontrolle über kritische Entscheidungen, Datenflüsse und Sicherheitsarchitekturen zu behalten. Kein Unternehmen kann Cybersecurity heute rein national abbilden. Wir brauchen die Innovationskraft globaler Technologiepartner. Aber die Kunst liegt in der souveränen Orchestrierung: Wir arbeiten bewusst nach BSI-Vorgaben, ISO-Normen und europäischen Standards, um globale Spitzentechnologie so in die deutsche Industrie zu integrieren, dass die Datenhoheit und die operative Kontrolle hier vor Ort bleiben. Unternehmen müssen wissen, wem sie ihre sicherheitskritischen Daten, Systeme und Prozesse anvertrauen. Für den Maschinen- und Anlagenbau, Automotive, Energieversorger oder die Logistik ist das keine abstrakte Frage. Dort hängen Produktionsfähigkeit und Lieferketten unmittelbar daran.

> »Cyberresilienz ist keine technische Zusatzaufgabe, sondern Teil guter Unternehmensführung.«
>
> – Dr. Maria Wolf

Was sollten Unternehmen jetzt konkret tun, um Schutz, Regulatorik und Nachweisfähigkeit zusammenzubringen?

Wolf: Zuerst Klarheit schaffen: Welche Anforderungen betreffen uns wirklich – NIS2, ISO 27001, der Cyber Resilience Act, Datenschutz, EU AI Act? Viele Unternehmen bearbeiten alles gleichzeitig und nichts richtig. Danach priorisieren: Welche Prozesse, Daten, Systeme und Lieferbeziehungen sind kritisch und wer trägt wofür Verantwortung? Wichtig ist: Dokumentation ist kein Selbstzweck. Sie muss Entscheidungen im Alltag, Audits und im Ernstfall die Krisensteuerung unterstützen. Dafür braucht es Struktur. Wir haben mit dem CyberSec Hub ein modulares Werkzeug entwickelt, mit dem Unternehmen Informationssicherheit, Datenschutz, Business Continuity und KI-Governance selbst steuern können.

Strehle: Technisch beginnt alles mit einem ehrlichen Lagebild: Schwachstellen-Scans, Penetrationstests und Übungen zeigen, wo Angreifende heute durchkämen. Darauf baut die Überwachung auf, etwa durch ein »Security Operations Center«, das rund um die Uhr hinschaut. Und es braucht eingespielte Abläufe für den Ernstfall – am besten geübt, bevor er eintritt, etwa in Red-Team-Übungen, bei denen unsere Expertinnen und Experten einen echten Angriff simulieren. Prevent, Detect, React – Vorbeugen, Erkennen, Reagieren – gehören zusammen. Wer nur in Prävention investiert, merkt oft wochenlang nicht, dass Angreifende längst im Netz sind. Und noch einmal: IT und OT müssen gemeinsam betrachtet werden. Sonst entstehen blinde Flecken dort, wo es am teuersten wird: in der Produktion.

Frau Dr. Wolf, KI verändert die Cybersicherheit auf beiden Seiten. Welche Risiken unterschätzen Unternehmen – und wo kann KI helfen?

Wolf: KI-Sicherheit ist in erster Linie ein Governance-Thema, kein Tool-Thema. Wir begleiten Unternehmen von der Auswahl bis zum sicheren Betrieb – ob ChatGPT, Microsoft Copilot oder eigene KI-Lösungen. Dabei geht es uns keineswegs nur um Verbote, sondern um echte Innovation. Der industrielle Mittelstand darf den Anschluss bei generativer KI nicht verpassen. Aber nachhaltige Innovation braucht ein sicheres Fundament. Nur wer Leitplanken für Datenschutz und IT-Sicherheit einzieht, schafft den vertrauensvollen Raum, in dem Teams kreativ und produktiv mit KI experimentieren können. Sichere KI ist der Schlüssel zu Wettbewerbsfähigkeit und neuen Geschäftsmodellen. Dennoch senkt KI die Einstiegshürden für Angreifende. Phishingmails sind heute fehlerfrei und persönlich zugeschnitten, die Vorbereitung von Angriffen läuft teilweise automatisiert, Täuschungen werden schwerer erkennbar. Wie überzeugend das inzwischen ist, sehen Sie übrigens am Bild zu diesem Interview. Es zeigt Rolf Strehle und mich im Gespräch auf der Wilhelmsburg. Aufgenommen wurde es nie, es ist KI-generiert. Auf der anderen Seite hilft KI der Verteidigung. Sie erkennt Muster schneller, ordnet Sicherheitsereignisse ein und verkürzt Reaktionszeiten. Deshalb müssen Unternehmen den eigenen KI-Einsatz regeln: Welche Tools sind erlaubt? Welche Daten dürfen hinein? Wer prüft die Ergebnisse?

Beim Cyber Resilience Forum auf der Wilhelmsburg in Ulm bringen Sie im September Führung, IT, OT, Recht, Krisenmanagement und Kommunikation zusammen. Warum ist dieses Zusammenspiel im Ernstfall entscheidend?

Strehle: Im Ernstfall zählen Minuten, nicht Organigramme. Die IT muss wissen, welche Systeme kritisch sind, die Produktion muss ihre Abhängigkeiten kennen, die Führung muss Prioritäten setzen – und zwar abgestimmt, nicht nacheinander. Die Wilhelmsburg ist dafür übrigens ein schönes Bild: Die größte Festung Europas wurde nie angegriffen. Aber die besten Mauern nützen nichts, wenn innen niemand weiß, wer im Ernstfall was zu tun hat. Genau das üben wir beim Forum: mit Workshops, Live-Demos zu KI-gestützten Angriffen und Darknet-Forensik, mit IT- und OT-Perspektiven, Business-Continuity und dem Cyber Resilience Act. Dazu kommen Unternehmen, die einen Angriff selbst erlebt haben und offen darüber sprechen, was sie heute anders machen würden ...

Wolf: ... und zwar bewusst über die Technik hinaus. Recht, Kommunikation und Geschäftsführung müssen früh am Tisch sitzen, denn Meldepflichten, Haftungsfragen und die Information von Kunden und Mitarbeitenden laufen im Vorfall parallel. Resilienz entsteht, wenn Unternehmen vor dem Angriff gemeinsam üben, wie sie entscheiden. Dazu laden wir herzlich ein: am 29. September 2026 auf die Festung Wilhelmsburg in Ulm. Das Forum richtet sich an Geschäftsführung sowie Fach- und Führungskräfte aus IT, OT, Business-Continuity, Recht, Krisenmanagement und Kommunikation. Die Teilnahme ist kostenfrei, die Plätze sind begrenzt.

Hier gehts zum Cyber Resilience Forum:

ditis
The Security Company