PRESSEMITTEILUNG

Cybersecurity für Unternehmen: Zwischen realer Bedrohung und regulatorischer Pflicht

Berlin/Rostock, 27. Januar 2026 – Die Bedrohungslage im Cyberraum bleibt angespannt. Ransomware, KI-gestützte Angriffe und Vorfälle entlang der Lieferkette dominieren das Bild. Parallel dazu verschärft sich der regulatorische Rahmen deutlich, wie durch das Inkrafttreten der NIS2-Richtlinie oder des Cyber Resilience Act. Für Unternehmen bedeutet das: Cybersecurity wird im Jahr 2026 zur strategischen, rechtlichen und operativen Kernaufgabe. Was Unternehmen konkret tun sollten, weiß das Software- und Beratungshaus Net Group.

1. Wenn Cyberangriffe Maschinen stoppen

Ein falscher Klick, ein manipuliertes Update oder ein kompromittierter Dienstleister und Produktionsstraßen stehen still. Moderne Angriffe zielen nicht mehr nur auf Daten, sondern direkt auf industrielle Steuerungssysteme (ICS), OT-Netze und Mensch-Maschine-Schnittstellen. Das Problem: Während klassische IT-Systeme oft vergleichsweise gut abgesichert sind, treffen in Fabrikhallen Legacy-Technik und neue Vernetzung aufeinander. Diese Kombination ist für Angreifer ideal und für Unternehmen hochriskant. Cybersecurity bedeutet hier nicht Datenschutz, sondern Betriebssicherheit.

2. Dominoeffekte: Warum Lieferketten besonders gefährdet sind

Eine der tückischsten Entwicklungen sind Angriffe über Drittanbieter und Software-Updates. Manipulierte Patches oder kompromittierte Komponenten verbreiten sich schnell entlang ganzer Lieferketten. Der Schaden bleibt nicht lokal, sondern wirkt systemisch. Das führt zu Stillständen mehrerer Werke, Vertragsstrafen und Reputationsschäden und Kettenreaktionen bis zu branchenweiten Ausfällen. Cyberrisiken sind damit kein isoliertes Unternehmensproblem, sondern ein Standort- und Wettbewerbsfaktor.

3. Von Bits zu echten Gefahren

Besonders kritisch wird es, wenn Angreifer gezielt ICS-Protokolle missbrauchen und so bei einem Angriff etwa Motoren überhitzen lassen, Ventile blockieren und für fehlgesteuerte Pumpen sorgen. Dadurch können konkrete kinetische Risiken für Mitarbeitende, Umwelt und Infrastruktur entstehen. Damit ist Cybersecurity auch Arbeitsschutz und Produktsicherheit.

4. Warum die Angriffsfläche weiter wächst

Die Ursachen sind oft hausgemacht:

- Veraltete Systeme ohne moderne Sicherheitsmechanismen
- Fehlende oder mangelhafte Trennung zwischen IT und OT
- Unklare Zuständigkeiten zwischen Produktion, IT und Management
- Blindes Vertrauen in Updates, Hardware und externe Dienstleister
- Industrie 4.0 steigert Effizienz – aber jede neue Schnittstelle ist potenziell ein Einfallstor. Sicherheit muss mitwachsen, nicht hinterherlaufen.

5. Regulierung als Gamechanger: Cybersecurity wird Pflicht

Mit dem Cyber Resilience Act verschiebt sich Cybersicherheit endgültig vom „Nice-to-have" zur Marktzugangsvoraussetzung. Produkte ohne nachweisbare Sicherheit riskieren künftig ihr CE-Kennzeichen – und damit den Zugang zum EU-Markt.

Unternehmen müssen Cybersicherheit

- früh in die Produktentwicklung integrieren
- über den gesamten Lebenszyklus denken
- dokumentierbar und überprüfbar umsetzen
- Hersteller ebenso wie Betreiber industrieller Systeme einbeziehen.

6. Was Unternehmen jetzt konkret tun sollten

Cybersecurity lässt sich nur mit einem strukturierten Vorgehen beherrschen. Unternehmen sollten zunächst prüfen, ob sie unter NIS2 oder andere regulatorische Vorgaben fallen, und die Verantwortung klar auf Geschäftsleitungsebene verankern. Darauf aufbauend gilt es, die kritischsten Geschäftsprozesse sowie IT- und OT-Systeme systematisch zu identifizieren und zu bewerten, um Schutzmaßnahmen gezielt zu priorisieren. Strukturell empfiehlt sich die Einführung eines Informationssicherheits-Managementsystems (ISMS), klar definierte

Zuständigkeiten und die feste Verankerung von Cyberrisiken im unternehmensweiten Risikomanagement. Technisch gehören Mehr-Faktor-Authentifizierung, strikte Netzwerksegmentierung zwischen IT und OT, Zero-Trust-Ansätze, kontinuierliches Monitoring, saubere Update-Strategien sowie regelmäßig getestete Backups zur Pflicht. Organisatorisch sind regelmäßige Schulungen, Notfallübungen, ein vollständiges Software- und Abhängigkeitsinventar sowie verbindliche Sicherheitsanforderungen für Dienstleister entscheidend. Normen wie ISO 27001 bieten wichtige Leitplanken, ersetzen jedoch keine gelebte Sicherheitskultur.

7. Sicherheit ist Teamarbeit und Chefsache

Cybersecurity scheitert selten an fehlender Technik, sondern an Organisation, Kultur und Führung. Unternehmen, die vorbereitet sind, zeichnen sich dadurch aus, dass sie den Ernstfall regelmäßig üben, offen über Risiken kommunizieren, Produktion, IT und Management zusammenbinden und Sicherheit als Investition, nicht als Kostenblock verstehen.

Fazit: Bedrohung und Chance zugleich

Die Bedrohungslage wird sich weiter verschärfen. Gleichzeitig bietet Cybersicherheit Unternehmen die Chance, Resilienz, Vertrauen und Wettbewerbsfähigkeit aufzubauen. Die entscheidende Frage lautet nicht, ob Angriffe kommen, sondern ob Unternehmen vorbereitet sind. Wer jetzt handelt, schützt nicht nur Maschinen und Daten, sondern die eigene Zukunftsfähigkeit.

Über Net Group

Net Group ist ein estnisches Software- und Beratungshaus mit über 25 Jahren Erfahrung in der digitalen Transformation. Das Unternehmen beschäftigt mehr als 120 Spezialist:innen und entwickelt individuelle Lösungen für Unternehmen, Start-ups und öffentliche Einrichtungen in der gesamten EMEA-Region. Der Fokus liegt auf digitaler Geschäftsmodellinnovation, KI-gestützten Anwendungen, Cybersecurity, skalierbarer Softwareentwicklung sowie e-Government-Systemen. Besonders stark ist Net Group in den Bereichen digitale Verwaltung, Digital Health und Informationssicherheitsmanagement, mit spezialisierten Teams, die zukunftsweisende Technologien einsetzen.

Seit der Übernahme der deutschen Cloud Ahoi GmbH mit Sitz in Rostock bildet dieser Standort die Net Group Deutschland. Cloud Ahoi war auf Informationssicherheitsmanagement spezialisiert und unterstützte

insbesondere kleine und mittelständische Unternehmen sowie öffentliche Einrichtungen bei der Optimierung ihrer IT-Sicherheitsstandards und der Umsetzung von Compliance-Anforderungen wie NIS2 und ISO 27001. Dieses Know-how ist nun fester Bestandteil des Net Group Portfolios.

Net Group steht für Projekte mit langfristiger Wirkung: Lösungen, die verändern, wie Menschen arbeiten, lernen und leben.