Cybersecurity und Resilienz von Unternehmen stärken

Empfehlungen der Unternehmen der Schwarz Gruppe für eine effektive Cybersicherheitspolitik

Die Cybersicherheitspolitik der aktuellen Legislaturperiode ist durch europäische Gesetzgebung wie die NIS2-Richtlinie, den CRA (Cyber Resilience Act) und CER-Richtlinie (Critical Entities Resilience) geprägt, die nun in deutsches Recht umgesetzt werden. Dies ist für ein einheitliches Cybersicherheitsniveau und die europaweite Harmonisierung der Cybersicherheitsregulierung ein notwendiger Schritt, denn Datendiebstahl, Industriespionage oder Sabotage verursachten im vergangenen Jahr Schäden von 267 Milliarden Euro (Bitkom, Wirtschaftsschutzstudie Deutschland 2024).

Insbesondere kleine und mittelständische Unternehmen (KMU) sind nur bedingt auf Cyberangriffe vorbereitet. Häufig reagieren sie erst, nachdem der Schaden schon entstanden ist, und das kann in Einzelfällen existenzbedrohend sein. Auch kritische Infrastrukturen, die öffentliche Hand und Politik stehen immer stärker im Zentrum von Cyberangriffen. Es gilt daher: Die Stärkung von Cybersecurity und Resilienz zu unterstützen.

1. Resilienz stärken und Grundlagen legen

- Zusammenarbeit über Behörden und föderale Strukturen hinaus, bei Erkennung und Erkenntnissen von Cyberattacken und Bedrohungen ermöglichen
- Automatisierte (werkzeuggestützte) Prüfung und 24/7 Analyse der vorhandenen KRITIS Infrastrukturen auf mögliche Schwachstellen umsetzen
- Automatische Erfüllung von NIS2 Anforderungen, bei richtigem Einsatz von zertifizierten Werkzeugen und Dokumentation realisieren
- Aufbau und permanentes Training von Krisenteams- und Dienstleistern (nach Vorgabe) für den Notfall eines Angriffs sicherstellen

2. Schutz der Industrie und des Mittelstands in den Mittelpunkt stellen

- Steuerliche Anreize für neu beschaffte Produkte, Dienstleistungen, Schulungen sowie ein dezidiertes Digitalbudget zur Förderung der Cybersicherheit sind essenziell, um das Sicherheitsniveau und die Attraktivität des Wirtschaftsstandorts Deutschland signifikant zu erhöhen. Mögliche Instrumente wären in dem Zusammenhang auch KMU-freundliche Förderprogramme durch z.B. die KfW zur finanziellen Begleitung und Unterstützung bei Cybersicherheitsmaßnahmen aufzusetzen.
- Förderprogramme sind bürokratie- und aufwandsarm zu gestalten. Diese können dafür z.B. mit Unternehmen der deutschen Industrie gemeinsam entwickelt und angeboten werden. Zum Beispiel durch fixe Lizenzpreise beziehungsweise Ausbildung von Unternehmen zur

Unterstützung bei der Implementierung nach Schulung und Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

3. Präventive Sicherheitsmaßnahmen stärken[1]

- Incentivierung eines Versicherungsangebots, das die Überwachung von präventiven Maßnahmen in den Vordergrund stellt und im Schadensfall durch Dienstleister und Dienstleistungen wirkt (u.a. Incident Response Teams).
- Neben Systemen zur Angriffserkennung sollten stärker Systeme zu Angriffsprävention eingesetzt werden. Diese basieren auf Konzepten und technischen Maßnahmen für eine kontinuierliche Risikoanalyse, um die Sicherheit der IT-Systeme zu gewährleisten.
- Für die Gewährleistung eines hohen Sicherheitsstandards sind regelmäßige Evaluierung und Adaptierung von Sicherheitsstrategien in Reaktion auf neue Bedrohungslagen zwingend notwendig. Ein zentraler Bestandteil dieser Strategien sollte die kontinuierliche Schulung und Sensibilisierung der Mitarbeitenden sein, um menschliche Fehler zu reduzieren, die oft das größte Einfallstor für Cyberangriffe darstellen. Zudem muss darauf hingewirkt werden, dass die Führungsebene Cybersicherheit als vorrangige Aufgabe betrachtet und entsprechende Ressourcen bereitstellt.

Ziel dieser Empfehlungen ist die Schaffung einer Umgebung, die insbesondere kleine mittelständische Unternehmen aufklärt, verpflichtet und dann mit den richtigen Werkzeugen ausstattet sowie mit den notwendigen Prozessen zur Überwachung, Einhaltung und Hilfe begleitet. Grundvoraussetzung dafür ist eine aktive Industriepolitik, verbunden mit einer Unterstützung aus Produkt und Dienstleistungsperspektive.

[1] Cyberversicherung bieten Möglichkeiten Risiken zu externalisieren, allerdings bis zu einem gewissen Grad. Sie sind aber kein Ersatz für ein adäquates Niveau für Cyberhygiene. Diese Aufgaben lassen sich nicht externalisieren.