5 Schlüsselstrategien zur Stärkung der Cyber-Resilienz

Als strategische Entscheiderinnen und Entscheider stehen Aufsichtsräte und CEOs an der Frontlinie, wenn es um die Cyber-Sicherheit geht. Franziska Hain, Geschäftsführerin der BDO Cyber Security GmbH, gibt fünf Handlungsempfehlungen, um die digitale Abwehrkraft zu stärken.

1 **Eine Cyber Attack Response Strategie entwickeln lassen:** Eine gut durchdachte Strategie ist elementar, um auf Cyber-Angriffe zu reagieren. Die Unternehmensführung sollte einen Plan erarbeiten lassen, der klar definiert, wie auf verschiedene Arten von Cyber-Angriffen reagiert wird. Dieser umfasst die Identifizierung von Schlüsselpersonal, die Zuweisung von Rollen und Verantwortlichkeiten sowie das Aufstellen eines Kommunikationsplans, der sowohl interne als auch externe Kommunikation abdeckt. Dazu gehört auch der Umgang mit einer Lösegeldforderung.

2 **Regelmäßige Cyber-Angriffssimulationen umsetzen:** Unternehmen sollten den Ernstfall simulieren und die Response-Strategie üben. Cyber-Simulationen helfen dabei, die Response-Fähigkeit des Unternehmens zu testen und Reaktionspläne zu schärfen. Diese Übungen sollten unter möglichst realistischen Bedingungen durchgeführt werden, um die Wirksamkeit der Notfall- und Reaktionsstrategien zu überprüfen und kontinuierlich zu verbessern.

3 **Konformität zur Regulatorik einfordern:** Es gilt einmal mehr, Führungskräfte für die Umsetzung von Anforderungen z. B. aus dem Digital Operational Resilience Act (DORA) oder der Netz- und Informationssysteme-Richtlinie (NIS2) zu sensibilisieren. Um die Konformität zu gewährleisten, können interne Audits helfen, die Einhaltung des DORA zu überprüfen, während gezielte Schulungen das Team mit den Anforderungen der Regulatorik vertraut machen.

4 **Kosten-Nutzen-Effizienz aufzeigen lassen:** Die Wirksamkeit von implementierten Sicherheitsmaßnahmen sollte im Verhältnis zu getätigten Investitionen stehen. Hier kann z. B. mittels einer Business-Impact-Analyse das finanzielle Schadenspotenzial unter Annahme eines IT-Ausfalls über einen definierten Zeitraum ermittelt und gegen die Kosten der Präventionsmaßnahmen gelegt werden.

5 **Ein Cyber Resilience Dashboard etablieren und berichten lassen:** Um eine Aussage über den Reifegrad der Cyber-Resilienz treffen zu können, sind die folgenden drei Themenfelder mittels KPIs im Rahmen eines Dashboards auszugestalten.

Cyber Resilience Dashboard

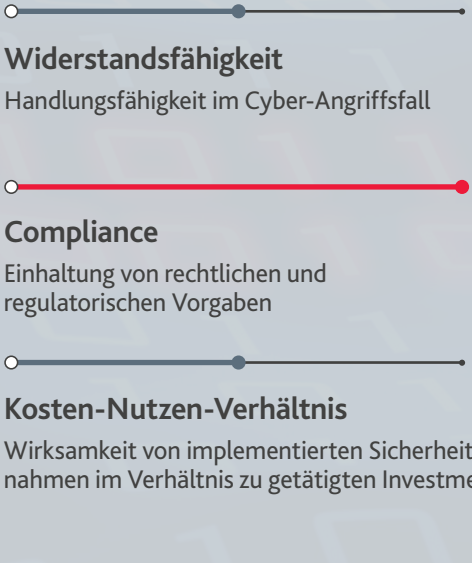

Foto: Adobe Stock