Ressourcen – was sie angreifbarer macht. Eingeschränkte Budgets, veraltete Systeme und unzureichendes Engagement auf Führungsebene vergrößern die Kluft weiter. Laut World Economic Forum schätzen weltweit über ein Drittel der kleinen Organisationen (35 %) ihre Cyberresilienz als unzureichend ein – ein siebenfacher Anstieg seit 2022.[1] Im öffentlichen Sektor sind die Zahlen sogar noch etwas höher: Dort berichten 38 Prozent von unzureichender Resilienz, während es in privaten Organisationen nur 10 Prozent sind.

Der weltweite Mangel an Sicherheitsexperten schüttet weiter Öl ins Feuer. Während kapitalkräftige Sektoren die besten Fachkräfte anziehen, haben Organisationen mit geringeren Budgets Schwierigkeiten, erfahrenes Sicherheitspersonal für sich zu gewinnen. Wie zuvor erwähnt, sind Organisationen des öffentlichen Sektors weltweit weiterhin am schlechtesten aufgestellt: 49 Prozent berichten von einem Fachkräftemangel, der ihren Cyber-Sicherheitszielen im Weg steht – 33 Prozent mehr als 2024.[1] Die entstehenden Schwachstellen machen weniger gut aufgestellte Sektoren als Angriffsziel für Cyberkriminelle und staatlich finanzierte Akteure immer attraktiver und intensivieren das wachsende Risiko für grundlegende Dienste und die öffentliche Sicherheit. Dringender denn je muss diese Lücke geschlossen werden.

Praxistipps

- **Halten Sie sich an anerkannte Frameworks:** Bauen Sie Ihre Strategie, unabhängig von regulatorischen Anforderungen, auf bewährten Richtlinien, wie ISO 27001 und NIST CSF, auf.
- **Kollaborieren Sie mit Regulierungsbehörden:** Arbeiten Sie proaktiv mit den regulierenden Instanzen Ihres Sektors zusammen. Entwickeln Sie gemeinsam praktische Richtlinien, von denen die gesamte Branche zum Wohle ihrer Sicherheit profitieren kann.
- **Verteilen Sie die Verantwortung auf verschiedene Abteilungen:** Sicherheitsteams sollten nicht die Ineffizienzen anderer Abteilungen ausbügeln müssen. Stellen Sie sicher, dass die richtigen Teams für OS-Patching, Code-Härtung und das Aufspüren veralteter Systeme zuständig sind und dass die Verantwortung für entstehende Risiken klar zugewiesen wird.
- **Orientieren Sie sich an reiferen Branchen:** Vernetzen Sie sich mit Organisationen in stark regulierten Sektoren und finden Sie heraus, welche Schutzmaßnahmen diese für mehr Resilienz einführen. Nutzen Sie günstigere Alternativlösungen, die die Anforderungen Ihrer Branche erfüllen.
- **Nutzen Sie neue Kanäle, um Fachkräfte zu gewinnen:** Bauen Sie Partnerschaften mit Universitäten und Fachschulen für die Bereiche auf, in denen Ihnen Fachkräfte fehlen. Bieten Sie Praktikums- und Ausbildungsplätze an, um vielseitig qualifizierte Fachkräfte anzuziehen.
- **Informieren Sie alle Teams über Sicherheitsstrategien:** Als CISO in weniger stark regulierten Branchen und kleineren Organisationen sollten Sie sicherstellen, dass Ihre Cyber-Sicherheitsstrategie klar und einfach umsetzbar ist. So können auch weniger technische Teams, wie zum Beispiel Fabrikarbeiter, aktiv zur Verteidigung der Organisation beitragen.

1 **World Economic Forum (2025).** Global Cybersecurity Outlook.