Einhaltung gesetzlicher Vorschriften

für Sicherheitsverantwortliche und IT-Entscheidungsträger

Einführung

Die Entwicklung von regulatorischen Rahmenbedingungen und Standards ist aus der Notwendigkeit entstanden, sich mit den Herausforderungen und Anforderungen beim Management der Informationstechnologie und dem Schutz von Daten auseinanderzusetzen. Diese Rahmenbedingungen und Standards haben sich nicht nur im Laufe der Zeit weiterentwickelt, sondern wurden auch durch technologische Fortschritte und neue Cybersicherheitsbedrohungen geprägt. Die Entwicklung von Frameworks und Standards wurde in erster Linie durch die folgenden Faktoren vorangetrieben:

- **Aufsichtsbehörden** betonen, wie wichtig es für Unternehmen ist, Verantwortung für ihre Cybersicherheitspraktiken zu übernehmen und bestimmte Standards und Vorschriften einzuhalten.
- **Moderne Cyberbedrohungen** treten immer häufiger auf und richten immer mehr Schäden an. Kriminelle und „Hacktivists“ gehen dabei mittlerweile mit einer Raffinesse vor, die früher nur für von staatlichen Akteuren ausgehende Bedrohungen typisch war.
- **Kritische Infrastrukturen und essenzielle Services** (z. B. im Gesundheitswesen oder der Energie- und Finanzbranche), die für das Funktionieren von Gesellschaft und Wirtschaft von entscheidender Bedeutung sind. Dazu gehören US-amerikanische Gesetze, wie z. B. der Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) vom März 2022.
- **Mangelnde Einheitlichkeit** der Cybersicherheitspraktiken in unterschiedlichen Sektoren und Regionen. Inkonsistente Konzepte können zu Sicherheitslücken und Compliance-Problemen führen.
- **Die Verordnung** zur Verbesserung der Cybersicherheit des Landes, die im Mai 2021 vom Präsidenten der Vereinigten Staaten erlassen wurde.

Unternehmen müssen widerstandsfähig gegenüber Cyberbedrohungen sein, den unterbrechungsfreien Geschäftsbetrieb sicherstellen und Systeme nach Störungen schnell wiederherstellen können. Mit der wachsenden Menge an personenbezogenen Daten, die gesammelt und verarbeitet werden, besteht ein erhöhter Bedarf, diese Daten vor Cyberbedrohungen und Datenschutzverletzungen zu schützen. Cybervorfälle haben nicht nur erhebliche wirtschaftliche Auswirkungen, die zu finanziellen Verlusten führen und das Vertrauen der Wirtschaft zu digitalen Services insgesamt untergraben, sondern können in manchen Fällen auch Menschenleben kosten, insbesondere wenn die Gesundheitsbranche das Ziel von Angriffen ist.

Die Einhaltung gesetzlicher Vorschriften ist entscheidend für die Resilienz von Unternehmen. Unternehmen, die das volle Ausmaß ihrer Risiken erfassen, wissen, dass Compliance nicht nur eine Checkbox-Aktivität ist, sondern ein grundlegender Bestandteil einer umfassenden Sicherheitsstrategie. Durch die Einhaltung regulativer Vorschriften und die Umsetzung von Best Practices für Sicherheit können sich Unternehmen besser positionieren, um den meisten Cyberangriffen wirksam zu begegnen und sich schnell davon erholen zu können. Ein solches Konzept sorgt dafür, dass im Krisenfall die Voraussetzungen für schnelle Wiederherstellungen bereits geschaffen sind.

1.

Cyberangriffe

Wird die digitale Infrastruktur eines Unternehmens angegriffen, kann das weit über den reinen Datenverlust hinausgehen. Ausfallzeiten, der Verlust von Kernfunktionen, potenzielle Umsatzeinbußen und die negative Wahrnehmung des Unternehmens sind mögliche Folgen eines Cybervorfalls.

Im Zusammenhang mit diesen Möglichkeiten sind Auswirkungen auf das Leben von Menschen der wichtigste Faktor, den es im Blick zu behalten gilt. Bei Finanzdienstleistern (Financial Service Industries, FSI) und im Gesundheitswesen (Healthcare, HC) können Cyberbedrohungen ernsthafte Auswirkungen auf das Leben von Menschen haben, besonders im Zusammenhang mit Rechnungen, Zahlungen sowie dem Zugang zu medizinischer Versorgung und anderen kritischen Services. Bedenken und Risiken wie diese sind ein guter Grund für Unternehmen, ihre Sicherheitslage zu verbessern, indem sie die Compliance innerhalb ihrer Branchenvorschriften befolgen.

Warum Compliance wichtig ist

Compliance umfasst die Einhaltung von Gesetzen und Vorschriften, die für die Branche und Region des Unternehmens gelten. Die Einhaltung von Bestimmungen kann dazu beitragen, Auswirkungen auf Ihr Unternehmen zu verringern, die von Umsatzeinbußen aufgrund von Lösegeldzahlungen bis hin zu Betriebsunterbrechungen, Datenschutzverletzungen, behördlichen Bußgeldern und Reputationsschäden reichen können. Compliance-Standards ändern sich rasant und werden dies auch weiterhin tun. Heute für die Herausforderungen unserer Zeit formulierte regulatorische Vorschriften reichen in der Zukunft möglicherweise nicht mehr aus. Sich an die neuen Rahmenbedingungen und Vorschriften und die damit verbundenen neuen Erwartungen zu halten, ist ein todsicherer Weg, um Ihr Unternehmen zu schützen.

Vorschriften vs. Rahmenbedingungen

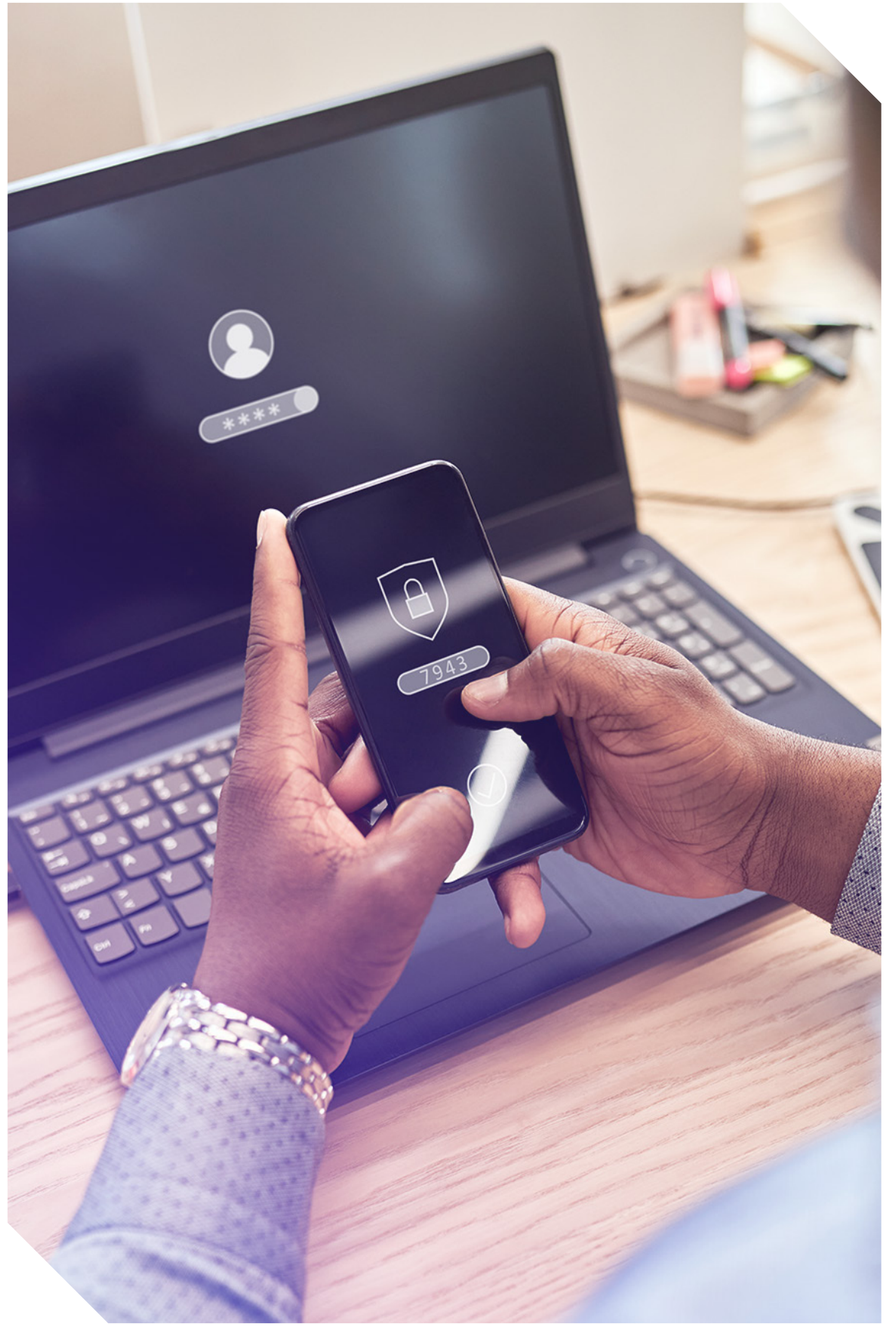
Der Hauptunterschied zwischen regulatorischen Bestimmungen und Frameworks besteht darin, was jeweils damit erreicht werden soll. Frameworks bieten einen strukturierten Satz von Richtlinien, Best Practices und Standards, mit denen Unternehmen ihre Cybersicherheit im Griff behalten und verbessern können. Im Gegensatz dazu handelt es sich bei regulatorischen Vorschriften um gesetzliche Anforderungen, die von Regierungen oder Aufsichtsbehörden erlassen werden, um in Unternehmen einen Mindeststandard für Cybersicherheitspraktiken durchzusetzen. Einige weit verbreitete regulatorische Vorschriften sind:

- **DSGVO** (Datenschutz-Grundverordnung) — Verordnung der Europäischen Union für den Schutz von Daten und Privatsphäre.
- **HIPAA** (Health Insurance Portability and Accountability Act) — US-amerikanische Regulierung für den Schutz von Daten im Gesundheitswesen.
- **SOX** (Sarbanes-Oxley Act) — US-amerikanische Regulierung für Finanzpraktiken und Corporate Governance.
- **PCI DSS** (Payment Card Industry Data Security Standard) — Standards für die Sicherung von Kreditkartentransaktionen.
- **FISMA** (Federal Information Security Management Act) — US-amerikanisches Gesetz zum Schutz von Behördeninformationen.

Verordnungen wie diese gehen Hand in Hand mit Rahmenwerken. Beispielsweise bilden Frameworks die Grundlage für die Einhaltung regulatorischer Vorschriften, die wiederum die Nutzung von Frameworks unterstützen. Frameworks helfen Unternehmen auch, über die gesetzlichen Mindestanforderungen hinauszugehen und Compliance und Auditierungen zu erleichtern, während regulatorische Vorschriften ein konsistentes Grundsicherheitsniveau in allen Sektoren gewährleisten. Zu den weit verbreiteten Frameworks gehören:

- **NIST Cybersecurity Framework (CSF)** — bietet einen umfassenden Ansatz für das Management von Cybersicherheitsrisiken.
- **CIS-Kontrollen** — eine Reihe von Best Practices zum Schutz vor Cyberbedrohungen.
- **COBIT** — bietet einen Rahmen für IT-Management und -Governance mit einem starken Fokus auf Kontrollziele für die IT, einschließlich Cybersicherheit.

Frameworks bieten Best Practices für das Management der Cybersicherheit, während Vorschriften Mindeststandards durchsetzen, um die grundlegende Sicherheit in allen Sektoren zu gewährleisten.



Risikomanagement und Compliance

Ein risikobasierter Ansatz beginnt mit einer gründlichen Risikobewertung. An diesem Prozess sollten verschiedene Interessengruppen beteiligt sein, darunter Sicherheitsteams, IT-Mitarbeiter, Rechtsexperten und Führungskräfte.

Beispielsweise kann ein Anbieter im Gesundheitswesen dem Schutz elektronischer Patientenakten (Electronic Health Records, EHRs) aufgrund der Sensibilität dieser Daten und der potenziellen Folgen von Sicherheitsverstößen, etwa des Verlustes von Patientendaten oder behördlicher Bußgelder gemäß HIPAA, oberste Priorität geben. Durch die Priorisierung der EHR-Sicherheit kann sich der Anbieter auf die Implementierung von Kontrollen konzentrieren, die die größten Risiken mindern.

Da die regulatorischen Anforderungen immer komplexer werden, setzen Unternehmen zunehmend auf Governance-, Risikomanagement- und Compliance-Tools (GRC), um ihre Compliance-Prozesse zu rationalisieren, die Transparenz zu erhöhen und eine kontinuierliche Überwachung und Verbesserung zu gewährleisten.

Ein risikobasierter Compliance-Ansatz passt die Sicherheitsbemühungen an die individuellen Risiken jedes Unternehmens an und stellt sicher, dass kritische Bedrohungen priorisiert werden.

GRC-Tools und ihre Vorteile im Überblick:

GRC-Tools wurden entwickelt, um Unternehmen bei der Automatisierung und Verwaltung verschiedener Aspekte der Compliance zu unterstützen, wozu die Entwicklung von Richtlinien, Risikobewertungen, Audit-Trackings und Reaktionen auf Vorfälle gehören. Diese Tools bieten mehrere wesentliche Vorteile:

- **Zentrales Compliance-Management:** GRC-Tools ermöglichen es Unternehmen, Compliance-Aktivitäten auf einer einzigen Plattform zu konsolidieren.
- **Automatisierung von Compliance-Aufgaben:** Durch die Automatisierung von Compliance-Routineaufgaben, wie z. B. die Überwachung von Zugriffsprotokollen oder die Erstellung von Audit-Berichten, gewinnen GRC-Tools wertvolle Zeit.
- **Verbesserte Transparenz und einfacheres Reporting:** GRC-Tools bieten Echtzeit-Transparenz für den Compliance-Status und erleichtern Sicherheitsverantwortlichen, Fortschritte zu verfolgen, Lücken zu identifizieren und die Einhaltung der regulatorischen Vorschriften gegenüber Aufsichtsbehörden und Prüfern nachzuweisen.
- **Kontinuierliche Überwachung und Verbesserung:** GRC-Tools unterstützen die kontinuierliche Überwachung von Compliance-Aktivitäten und ermöglichen es Unternehmen, Probleme proaktiv statt reaktiv zu identifizieren und anzugehen.

2.

Warum es wichtig ist, Compliance-Vorschriften zu übernehmen

Bei der Kenntnis und Bewältigung der Risiken, denen Ihr Unternehmen ausgesetzt ist, geht es nicht darum, Fehler zu finden. Vielmehr ist es wichtig, Fakten zu finden, damit Sie Ihr Unternehmen schützen und voranbringen können. Auch wenn Führungskräfte vielleicht sicher sind, dass ihr Unternehmen vorbereitet und cyberresilient ist, könnte die Realität ganz anders aussehen und von erheblichen Risiken geprägt sein.

Die Sicherstellung, dass die Unternehmensleitung einbezogen ist und sich für die Sache engagiert, ist der wichtigste Weg, um Compliance zu erreichen. Unternehmen müssen eine Compliance-Kultur im gesamten Unternehmen fördern, um Risiken zu reduzieren. Das Management ist verantwortlich für die Implementierung von Prozessen und Technologien gemäß den Vorschriften. Dabei ist es wichtig, innezuhalten und dafür zu sorgen, dass Gesetze und Vorschriften im Kontext der Branche und der geographischen Lage des Unternehmens befolgt werden.

In dem Maße, wie die Branche weiter wächst und sich verändert, werden sich auch die Compliance- und Regulierungsstandards verändern. Sie müssen jedoch verhindern, dass Ihr Unternehmen bei seinen Compliance-Aktivitäten zurückfällt, denn sonst riskieren Sie, dass Nachlässigkeit um sich greift und Führungskraft oder Vorstandsmitglied sich strafbar machen. Ein Ausfall oder ein Ransomware-Angriff kann Bußgeldzahlungen und Reputationsschäden nach sich ziehen. Doch je ausgereifter Ihr Unternehmen im Hinblick auf die Einhaltung unterschiedlicher gesetzlicher Vorschriften ist, umso größer sind die Chancen, dass es sich nach einem Angriff schnell wieder erholt.

Compliance weltweit

Derzeit gibt es auf der Welt insgesamt über 150 Länder, die irgendwelche Arten von Gesetzen zur Cybersicherheit haben. Einige davon sind DORA in der EU sowie NIS/NIS2 im Vereinigten Königreich. In Japan gibt es FSA- und im Nahen Osten NESA- und DIFC-Datenschutzgesetze. Weltweit können sich Länder an NIST orientieren. Wenn Menschen in den USA an Ransomware und regulatorische Strafen denken, denken sie vor allem an die Security and Exchange Commission (SEC). Trotz der vielfältigen regulatorischen Möglichkeiten gibt es in weniger als 100 Ländern Vorschriften für kritische Infrastrukturen. Dies zeigt, dass sich viele Länder nicht ausreichend mit dem Thema Sicherheit befassen, obwohl eine Konzentration auf kritische Infrastrukturumgebungen von größter Wichtigkeit ist. Betrachtet man speziell die Gesundheitsbranche und einschließlich Forschung und Biotechnologie, so gelten oft unterschiedliche Regeln von Land zu Land.

Compliance-Vorschriften stellen sicher, dass Ihr Unternehmen auf Cybervorfälle vorbereitet ist. Die Beteiligung der Vorstandsebene ist für die Förderung einer Sicherheitskultur von entscheidender Bedeutung.

Unterschiede zwischen der Finanz- und der Gesundheitsbranche

In den USA listet der Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) 16 kritische Branchen auf, für die die Einhaltung unterschiedlicher regulierender Vorschriften erforderlich ist. Wenn man an kritische Branchen denkt, kommen einem normalerweise Staudämme, Stromnetze und natürlich das Gesundheitswesen in den Sinn. Die Gesundheits- und die Finanzbranche spielen entscheidende Rollen im Alltag von Menschen auf der ganzen Welt. Die negativen Auswirkungen, die fehlende Sicherheitscompliance auf Organisationen im Gesundheitswesen haben kann, betreffen direkt das Leben vieler Menschen.

HIPAA ist eine der wichtigsten Vorschriften, an die viele beim Thema Compliance im Gesundheitswesen denken. Die HIPAA-Datenschutzregel legt nationale Standards für den Schutz bestimmter Gesundheitsinformationen fest, während die HIPAA-Sicherheitsregel eine Reihe nationaler Sicherheitsstandards für den Schutz bestimmter Gesundheitsinformationen festlegt, die in elektronischer Form gespeichert oder übertragen werden. Sind Gesundheitsdienstleister nicht ausreichend geschützt oder halten sie die Vorschriften nicht ein, könnten bei einem Ransomware-Angriff Patientendaten in Gefahr geraten.

In der Finanzbranche ist eine der wichtigsten Vorschriften der GLBA oder der Gramm-Leach-Bliley Act. Dieses Gesetz verlangt von Finanzunternehmen, die Verbrauchern Finanzprodukte oder -dienstleistungen wie Kredite, Finanz- oder Anlageberatung oder Versicherungen anbieten, ihren Kunden ihre Praktiken des Informationsaustauschs zu erläutern und sensible Daten zu schützen. Wenn ein Finanzunternehmen Frameworks oder Vorschriften nicht einhält, läuft es Gefahr, mit finanziellen Verlusten, Geldbußen, wirtschaftlicher Instabilität und Reputationsschäden konfrontiert zu werden.

Unternehmen müssen sich kontinuierlich an neue Vorschriften anpassen, um die Compliance aufrechtzuerhalten und neuen Cyberbedrohungen immer einen Schritt voraus zu sein.

3.

Best-Practice-Empfehlungen und Implementierung

Bei der Compliance geht es niemals nur um einmalige Überlegungen. Gesetzliche Vorschriften sind nicht statisch; sie entwickeln sich im Laufe der Zeit immer weiter, wenn neue Bedrohungen auftreten und Bestimmungen aktualisiert werden. Daher gibt es einige Best Practices, die Sie implementieren müssen, um sicherzustellen, dass Ihr Unternehmen bei allen wichtigen Rahmenbedingungen und Vorschriften an der Spitze bleibt.

Kontinuierliches Monitoring

Die kontinuierliche Überwachung ist ein wichtiger Bestandteil eines effektiven Compliance-Managements. GRC-Tools erleichtern das kontinuierliche Monitoring durch Integration in die vorhandene Sicherheitsinfrastruktur, z. B. in SIEM (Security Information and Event Management)-Systeme, um Compliance in Echtzeit nachverfolgen zu können.

Beispielsweise kann ein Finanzdienstleistungsunternehmen, das SOX unterliegt, ein GRC-Tool verwenden, um den Zugriff auf Finanzsysteme kontinuierlich zu überwachen und sicherzustellen, dass nur autorisiertes Personal Zugriff auf sensible Finanzdaten hat. Durch die Integration von GRC-Tools in ihre Cybersicherheitsstrategien können Unternehmen ihre Compliance-Bemühungen rationalisieren, das Risiko von Verstößen verringern und sicherstellen, dass sich ihre Sicherheitspraktiken im Einklang mit den gesetzlichen Anforderungen weiterentwickeln.

Regelmäßige Audits und Assessments

Bei einem Angriff geht es nicht nur darum, ob Sie einen Plan für die Reaktion auf Vorfälle haben. Sie müssen sicher sein, *dass* Ihr Plan funktioniert. Eine der besten Möglichkeiten, dies zu gewährleisten, sind Tests. Indem Sie den Plan Ihres Unternehmens testen und nachweisen, dass der Test erfolgreich war, stellen Sie sicher, dass die Compliance eingehalten wird .

Wichtige Schritte für die Compliance

Bei der Betrachtung der Vorschriften, die Organisationen implementieren können, um Compliance zu gewährleisten, ist es wichtig, einen ganzheitlichen Ansatz zu verfolgen. Jeder Teil Ihres Unternehmens kann einen anderen Aspekt Ihrer Umgebung berühren. Planung und Voraussicht spielen eine große Rolle, wenn es darum geht, die Compliance Ihres Unternehmens sicherzustellen. Einige Schritte, die dabei berücksichtigt werden sollten, sind:

- **Entwicklung eines Risikomanagementprozesses:** Dazu gehören die Identifizierung aller potenziellen IT-Risiken, die sich auf Ihr Unternehmen auswirken könnten, sowie die Bewertung Ihrer Schwachstellen.
- **Analyse und Priorisierung Ihrer Risiken:** Dies kann durch die Entwicklung einer Strategie zur Risikominderung und die Schulung Ihrer Mitarbeiter erreicht werden.
- **Entwicklung eines Plans für die Reaktion auf Vorfälle:** Dabei können Sie unter anderem den Risikotransfer berücksichtigen und zugleich Transparenz und Einblicke in Ihre Umgebung sicherstellen.
- **Etablierung einer Sicherheitskultur:** Dies kann bedeuten, alle relevanten Stakeholder einzubeziehen, stets die richtigen Technologien zu wählen und niemals zu vergessen, die Vorgänge erschöpfend zu dokumentieren.

Entwickeln Sie einen Risikomanagementprozess, priorisieren Sie Risiken und etablieren Sie eine Sicherheitskultur, um die Compliance aufrechtzuerhalten und die Resilienz zu verbessern.

Schluss-folgerung

Die Zukunft der Einhaltung gesetzlicher Vorschriften wird sich auf Resilienz konzentrieren. Unternehmen müssen neue Vorschriften antizipieren und anpassungsfähige, proaktive Compliance-Programme entwickeln.

Das regulatorische Umfeld ist dynamisch und es ist unwahrscheinlich, dass sich das Tempo des Wandels auf diesem Gebiet verlangsamen wird, insbesondere da Regierungen und Regulierungsbehörden auf die rasanten technologischen Fortschritte unserer Zeit reagieren müssen. Vor diesem Hintergrund sollten Unternehmen ihre Sicherheits-Frameworks anpassen und weiterhin die gesetzlichen Vorschriften einhalten. Ein zweites Ziel wäre die Standardisierung von Best Practices für die Sicherheit, um einen Zustand zu erreichen, bei dem die Sicherheitsposition des Unternehmens ein akzeptables Niveau hat.

Zusammenfassend lässt sich sagen, dass die Einhaltung gesetzlicher Vorschriften eine fortlaufende Reise ist, die kontinuierliche Anstrengungen, Anpassungen und Zusammenarbeit erfordert.

Es reicht nicht aus, einfach nur Compliance zu erreichen. Unternehmen müssen sich bemühen, ihre Compliance-Programme angesichts der sich entwickelnden Bedrohungen und Vorschriften aufrechtzuerhalten und zu verbessern. Sicherheitsverantwortliche und IT-Entscheidungsträger spielen in diesem Prozess eine entscheidende Rolle, indem sie ihre Unternehmen zu einer Compliance-Strategie führen, bei der es nicht nur darum geht, Strafen zu vermeiden, sondern auch darum, eine stärkere, cyberresilientere Organisation aufzubauen. Durch die Integration von Compliance in das Gefüge der Betriebsabläufe und der Unternehmenskultur sowie durch kontinuierliche Agilität und Informiertheit zu Veränderungen können Unternehmen die Komplexität der regulatorischen Landschaft mit Zuversicht und Erfolg bewältigen.