D 7465

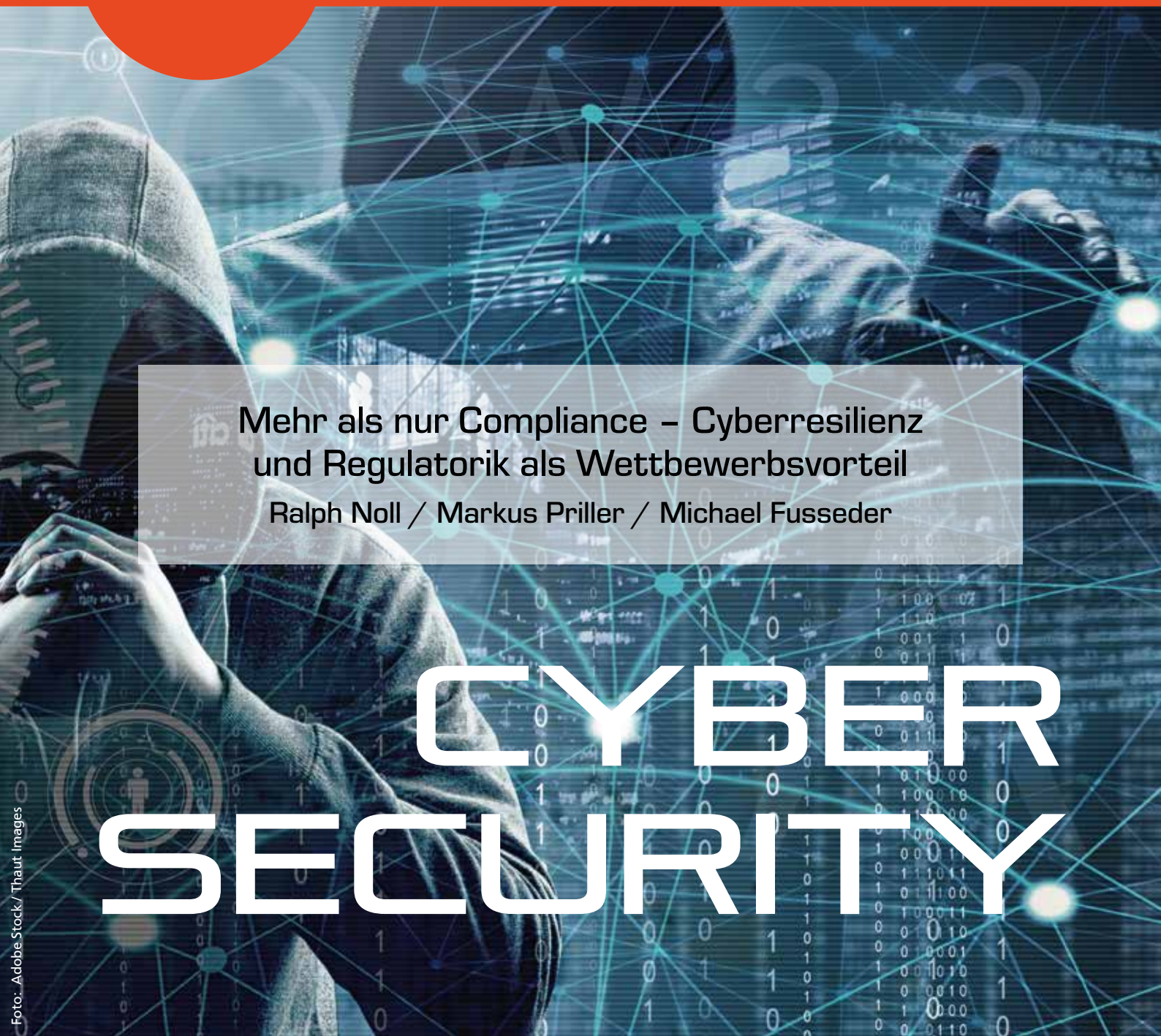
Zeitschrift für das gesamte
KREDITWESEN

76. Jahrgang · 1. März 2023

5-2023

Digitaler Sonderdruck

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019



Mehr als nur Compliance – Cyberresilienz und Regulatorik als Wettbewerbsvorteil

Ralph Noll / Markus Priller / Michael Fusseder

CYBER SECURITY

Foto: Adobe Stock/ Thaut Images

Ralph Noll / Markus Priller / Michael Fusseder

Mehr als nur **Compliance** – **Cyberresilienz** und Regulatorik als **Wettbewerbsvorteil**

Neue Regulationen für eine neue Zeit: In der Digitalära eröffnen innovative Technologien enorme Wachstumspotenziale, schaffen aber ebenso zusätzliche Risiken. Die Regulatoren in den weltweiten Märkten reagieren und entwickeln entsprechende neue aufsichtliche Anforderungen. Unter anderem durch eine moderne, zukunftsgerichtete Cyberstrategie sorgen Unternehmen für regulatorische Compliance – und erzielen darüber hinaus betriebswirtschaftliche Vorteile. Dies ist auch für Branchen und Unternehmen relevant, die selbst (noch) nicht entsprechend stark reguliert sind.

Welche Cyberregulatorik ist in naher Zukunft zu erwarten, was bedeutet sie für betroffene Unternehmen? Besonders in hoch regulierten Branchen wie dem Finanzsektor und der Versicherungswirtschaft werden solche Fragen aktuell diskutiert. Denn die Digitalisierung ist hier wie in vielen anderen Bereichen längst in voller Fahrt begriffen. Etwa im Bankensektor, wo seit Jahren bereits Filialnetze schrumpfen und digitale Ansätze expandieren. Durch Nutzung neuer Technologien beispielsweise in der Cloud werden speziell in der Finanzdienstleistungsbranche viele Vorteile erzielt: Kostenreduktion, Prozessverschlankung, Effizienzgewinne. Allerdings setzen sich Unternehmen mit den digitalen Prozessen auch neuen Risiken aus, die gemanagt werden müssen. Das hat auch die Regulatoren auf den Plan gerufen.

IT im Kern der Geschäftsprozesse

Die IT hat sich heutzutage in den Unternehmen von einer klassischen Support- zu einer Core-Funktion entwickelt. IT-Risiken werden somit auch zu Kerngeschäftsprozessrisiken – und das in vielen Branchen. Somit sind regulatorische Trends etwa der Finanzindustrie auch über die zunächst direkt betroffenen Unternehmen hinaus wesentlich. Sie deuten schon heute an, wo es auch in anderen Bereichen regulatorisch bald hingehen könnte: Über einen zeitlichen Versatz von einigen Jahren könnten die Trends auch andere Branchen betreffen. Die regulatorischen Ansätze markieren zudem, welche Vorgaben selbst nicht unmittelbar betroffene Unternehmen möglicherweise beachten müssen, wenn sie als Zulieferer von Unternehmen der kritischen Infrastruktur tätig sind. Und schließlich liefern diese Trends ganz grundsätzlich wertvolle Anregungen für einen zeitgemäßen Cyberansatz, der sich auf vielfältige Weise auszahlt und einen echten Wettbewerbsvorteil darstellen kann.

In diesem Artikel werden daher regulatorische Trends in bestimmten Branchen wie der Versicherungswirtschaft vorgestellt, um allgemeine Ansätze für eine bessere Cyberaufstellung abzuleiten. Wichtige neue Regelwerke sind hier etwa die VAIT-Novelle und die DORA-Regulatorik der EU, die beispielsweise Vorgaben zur Risikoverantwortung für Third Party Provider, zu Tests und zur Übung von Szenarien beinhalten. Auch in der Automobilindustrie sind IT-relevante Regulationen zu beachten (Tisax), ebenso in der Medizintechnik. In vielen Branchen wirken IT-Risiken somit nun auf das Kerngeschäft ein.

Es ist zunächst wichtig zu unterstreichen, dass die aufsichtlichen Anforderungen langfristig im Eigeninteresse der Unternehmen sind. Natürlich ist das Vermeiden von hohen Strafen (bis zu 1 Prozent des weltweiten Umsatzes bei DORA) an sich schon ein ausreichender Motivationsfaktor, um eine resiliente Cyberaufstellung aufzubauen. Aber viele entsprechende Maßnahmen sind auch aus internen Gründen geboten. Beispielsweise besteht für Unternehmen heutzutage ein hohes Risiko, dass durch Cyberattacken zentrale Geschäftsprozesse lahmgelegt werden. Es sollte daher bei der Cyberstrategie berücksichtigt werden, wie viel IT-Downtime operativ überbrückbar ist. Denn die Kosten wachsen im Falle eines erfolgreichen Cyberangriffs exponenziell, das digitale Geschäftsmodell leidet. Vertrauen wird zerstört, Reputationsschäden und Ad-hoc-Meldungen sind weitere typische Folgen. Moderne Cyberstrategien schaffen heutzutage deswegen viel mehr als „nur" Compliance. Sie erfüllen neue Forderungen von Kunden und Investoren, und sie verbessern die operative Resilienz ebenso wie das Business Continuity Management.

Aktuelle Cyberrisiken: Praxisbeispiel DDoS

DDoS Attacken (Distributed Denial of Service) werden bislang bezüglich ihres Schadenspotenzials deutlich unterschätzt, dabei liegen sie hier nur knapp hinter Ransomware. Hacker verursachen dabei missbräuchlich massenhafte digitale Serveranfragen. Dadurch werden IT-Strukturen überlastet und brechen zusammen. Der komplette Datenaustausch von Unternehmen kann auf diese Weise blockiert werden. Beispielsweise kam es 2020 durch eine DDoS-Attacke zu einem

mehrtägigen Handelsausfall an der Börse Neuseelands. Aber auch in kritischen Bereichen wie Gesundheit oder Infrastruktur drohen potenziell katastrophale Folgen. Die Täter zielen dabei oft auf Erpressung ab, teils spielen auch geopolitische Motive eine Rolle. Im ersten Halbjahr 2021 hatte die Zahl der Angriffe massiv zugenommen. 2022 ist diese zwar wieder zurückgegangen, dafür nahm die Intensität der Attacken jedoch weiter zu.

Die Zunahme solcher Cyberangriffe geht einher mit einer stark erhöhten Verletzlichkeit von Unternehmen. Im Zeitalter der Digitalisierung sind IT-Fähigkeiten und Datenaustausch längst essenziell für die Kernprozesse geworden. Auch die indirekten Risiken wachsen, da viele der entsprechenden Fähigkeiten heute von Dienstleistern etwa in der Cloud erbracht werden. Zugleich werden die Angriffe immer komplexer und professioneller. Auch die Cyberkriminellen nutzen nun die Möglichkeiten neuer Ansätze wie Cloud-Technologie oder Automatisierung. Dadurch können sie das Schadenspotenzial ihrer Angriffe massiv steigern.

Zunehmend raffinierte Methoden machen DDoS-Multivektor-Attacken gefährlicher denn je. Bestehende Konzepte der IT-Sicherheit sind allerdings kaum in der Lage, diese große Bedrohung abzuwehren. Der Standardschutz beispielsweise eines Telekommunikationsanbieters bietet meistens keine ausreichende Kapazität. Die Abwehr mit lokaler Hardware wiederum erfordert einen sehr großen Aufwand. Deshalb bedarf es neuer Ansätze für Cybersecurity, etwa durch Risikoorientierung, Zero-Trust-Paradigma und Automatisierung. Bevor zielführende Schritte zu mehr Cyberresilienz erörtert werden, soll zunächst die regulatorische Lage dargestellt werden.

Neue Regulationen und sinnvolle Maßnahmen

Regulatorik strahlt weit aus – auch auf selbst nicht regulierte Bereiche. Unternehmen sollten sich durch entsprechende Maßnahmen daran ausrichten. Dabei ist eine enge Abstimmung von Business-Strategie und IT-Risikomanagement zu empfehlen. Diese eröffnet die Chance auf ein integriertes Gesamtkonzept, bei dem im Rahmen der Digitalisierung alles ineinandergreift. Welche Regelwerke müssen dabei konkret beachtet werden? Besonders wichtig ist zweifellos der Digital Operational Resilience Act der EU (DORA). Er ist am 16. Januar 2023 in Kraft getreten und bringt vor allem eine hohe Verantwortung für Drittanbieter mit sich, beispielsweise für Cloud-Provider. Neben DORA verschärft in der Bankbranche auch die bereits am 16. August 2021 in Kraft gesetzte Novelle der nationalen bankaufsichtlichen Anforderungen an die IT (BAIT) die Vorgaben. Die bislang oft eher allgemein gehaltenen Anforderungen mit hohem Interpretationsspielraum werden seitdem viel detaillierter gefasst. Somit entfällt der bisherige implizite Anreiz für Unternehmen, nur das Mindestniveau zu erfüllen.

Im Einzelnen nimmt die BAIT-Novelle einige Aspekte von DORA vorweg. So muss die IT-Strategie in angemessenem Umfang beschrieben werden, einschließlich Personaleinsatz, Budget, Aufbau und vorhandenen Abhängigkeiten von Drittanbietern. Auch regelmäßige Tests sind vorgeschrieben. Bei DORA kommt eine Reihe anspruchsvollerer Regelungen hinzu. Im Zentrum stehen zwei besonders wichtige neue Anforderungen: Erstens liegt die Verantwortung für die Governance eines externen Anbieters (Third Party Provider, TPP) nun noch einmal stringenter bei dem Unternehmen, das ihn beauftragt. Hier bestehen nun signifikante Haftungsrisiken. Ein entsprechendes IT-Risikomanagement sollte sich also auf den Zulieferer ausdehnen und auch eine Exit-Strategie für betreffende Provider beinhalten. Kritische TPP müssen gegenüber dem Regulator benannt werden.

Zweitens verlangt DORA neben systematischer Threat Intelligence die regelmäßige Übung von Angriffsszenarien, ähnlich wie es die TIBER-Regeln (TIBER steht für Threat Intelligence-Based Ethical Redteaming, siehe dazu auch Seite 12) aus dem Bankensektor als freiwillige Maßnahme vorsehen. Dazu gehören auch Tests in Produktivsystemen und beispielsweise Red Teaming – also der Versuch von selbst beauftragten Firmen eigene Sicherheitsvorkehrungen zu überwinden, um Schwachstellen zu identifizieren. Zu-

Ralph Noll

Partner, Cyber Risk, Deloitte GmbH, Düsseldorf

Markus Priller

Director, Risk Advisory Insurance, Deloitte GmbH, Köln

Michael Fusseder

Senior Manager, Cyber & Strategic Risk, Deloitte GmbH, München

Die Nutzung neuer Technologien bringt der Finanzdienstleistungsbranche viele Vorteile wie Kostenreduktion und Prozessverschlankung. Allerdings setzen sich die Institute dadurch auch neuen Risiken aus, die gemanagt werden müssen. Das hat laut den Autoren auch die Regulatoren auf den Plan gerufen. Sie betonen jedoch, dass die aufsichtsrechtlichen Anforderungen langfristig im Eigeninteresse der Unternehmen sind, auch, aber nicht nur, um hohe Strafen zu vermeiden. Als besonders wichtiges Regulierungswerk sehen Noll/Priller/Fusseder den Digital Operations Resiliance Act (DORA) an. Besonders anspruchsvolle Anforderungen seien unter anderem die Verantwortung für die Governance der Third Party Provider und auch die Pflicht, regelmäßige Übung von Angriffsszenarien durchzuführen. Durch solche Maßnahmen steige der Aufwand erheblich. Da auch zukünftig die regulatorischen Anforderungen bei diesem Thema steigen würden, raten die Autoren zu regulatorischer Voraussicht. (Red.)

dem werden Fehler-Ursachen-Analysen nach bestimmten Vorfällen verlangt. Durch solche Maßnahmen steigt der Aufwand erheblich. Mindestens ebenso groß sind aber die über reine Compliance hinausgehenden Vorteile für das Unternehmen. Bei den bislang verbreiteten „Tabletop"-Tests werden Vorfälle lediglich hypothetisch durchgespielt. Demgegenüber sind die zukünftig durchzuführenden Überprüfungen wesentlich aussagekräftiger. So steigt nicht zuletzt auch die operative Resilienz.

Schritte zur Cyberresilienz

Vorgaben zur Informationssicherheit werden auch in anderen Bereichen immer relevanter. Für Unternehmen der Automobilbranche sind die Branchenstandards des Tisax-Regelwerks einschlägig, das Richtlinien für die Informationssicherheit festlegt. Lieferanten müssen nachweisen, dass sie diese Bestimmungen erfüllen. Der Anforderungskatalog basiert auf der Norm ISO/IEC 27001. An Anbieter von Zahlungsservices richtet sich das Zahlungsdiensteaufsichtsgesetz (ZAG). Paragraf 53 ZAG verlangt von betroffenen Unternehmen Minimierungsmaßnahmen und Kontrollmechanismen zu operationellen und sicherheitsrelevanten Risiken.

Die regulatorischen Trends zeichnen den Weg vor, den eine umfassende Cyberstrategie heutzutage einschlagen muss. Auch an sich unregulierte Unternehmen sollten sich dieses Themas jetzt annehmen. Empfehlenswert ist ein mehrdimensionales Herangehen. Unternehmen sollten sich zunächst eine Übersicht der eigenen Cyberlage verschaffen, um dann in verschiedenen Szenarien Risiken durchzuspielen – auch die Fälle, in denen diese schon eingetreten sind. Hierbei bieten Experten für Business Continuity Management wertvolle Unterstützung. Die Vorbereitung sollte konkrete Pläne enthalten, mit denen die Auswirkungen von Cyberattacken mitigiert werden können. Der Ansatz muss auf die individuelle Wertschöpfungskette abgestimmt und strategisch eingebettet werden. Zur Umsetzung gehört unter anderem schließlich auch die regelmäßige Auditierung. Ziel der Aktivitäten ist ein „lebendiges" Informationssicherheits-Managementsystem. Es beinhaltet Messmöglichkeiten zur laufenden Risikoerfassung und schafft so eine weitgehende Sichtbarkeit der Risiken. Durch im operativen Betrieb gesammelte Erfahrungen kann das System kontinuierlich immer weiter verbessert werden.

Angesichts der dynamischen Bedrohungslage wird es bei der Umsetzung notwendig, auch auf technisch-konzeptioneller Ebene neue Wege zu gehen. Gewohnte Abwehrmethoden wie Firewall, Virenschutz und ordnungsgemäßes Patchen bleiben natürlich weiterhin wichtig, doch sie reichen längst nicht mehr aus. Einen wegweisenden Ansatz für Cybersecurity stellt das oben erwähnte Zero-Trust-Paradigma dar. Einen abgekapselten sicheren „Innenraum" im Unternehmen gibt es hierbei nicht mehr. Stattdessen muss sich zukünftig jede einzelne Instanz in den Datensystemen über alle Kommunikationswege hinweg in Echtzeit legitimieren.

Regulatorik und Cybersecurity – vielfältige Motive, klare Vorteile

Möglich wird dies unter anderem durch gestiegene Rechenleistung und Technologien wie künstliche Intelligenz oder maschinelles Lernen. Sie erlauben eine weitgehende Automatisierung der Prozesse, was die Leistungsfähigkeit und die Effizienz massiv steigert. Dadurch kann der Schutz am faktischen Risiko ausgerichtet werden: Ressourcen lassen sich maximal effektiv einsetzen, besonders sensible Bereiche werden entsprechend robust verteidigt. Den Bedrohungen des Cloud-Zeitalters wird dabei ebenfalls mit Cloud-basierten Ansätzen begegnet. Der Zugriff auf Cloud-Server zur Abwehr erhöht die Skalierbarkeit und Resilienz. Um mit der aktuellen Dynamik der Entwicklung Schritt halten zu können, bietet sich die Zusammenarbeit mit spezialisierten Anbietern schon aus Effizienzgründen an.

Die Tendenz ist eindeutig: Die regulatorischen Anforderungen werden in Zukunft weiterhin zunehmen und eine kontinuierliche Beschäftigung mit ihnen erfordern. Deshalb lohnt sich ein frühzeitiges Engagement schon aus Gründen der regulatorischen Voraussicht – ganz abgesehen vom unmittelbaren operativen Mehrwert und den strategischen Vorteilen. Je nach individueller Situation des Unternehmens können auch weitere Motive vorliegen.

So ist heutzutage beispielsweise für eine Vielzahl von Unternehmen und Branchen ein hinreichender Cyberversicherungsschutz immer schwieriger am Markt zu erhalten. In anderen Fällen verlangen ambitionierte Kunden auch ohne expliziten regulatorischen Zwang höhere Standards von ihren Zulieferern. Immer mehr sind Mittelständler betroffen, etwa als Zulieferer von Unternehmen der Kritischen Infrastruktur.

Frage des Ambitionslevels

Speziell im Mittelstand wird derzeit auch verstärkt auf die Cyberimplikationen der aktuellen geopolitischen Lage geachtet, ein zusätzliches Motiv für mehr Cybersecurity. In diesem Bereich reichten bisher die regulatorischen Anforderungen nicht weit genug, was nun aufgeholt werden muss. Und auch im Hinblick auf die Kostenrisiken ist zeitnahes Handeln in diesem Feld geboten. Nicht zuletzt durch das eingangs erwähnte Risiko einer Strafzahlung bei Verstößen. Es erhöht sich dabei noch bei einem Verstoß gegen mehrere Regularien zugleich, zum Beispiel DORA und EU-DSGVO. Dazu kommen jeweils die operativen Kosten eines Cybervorfalls sowie der Reputationsschaden, der in Zeiten sozialer Medien deutlich schneller und schärfer auftreten kann.

Grundsätzlich handelt es sich bei der Umsetzung einer zukunftsweisenden Cyberstrategie auch um eine Frage des Ambitionslevels. Unternehmen mit einem gewissen Anspruch an die eigene Wettbewerbsfähigkeit können es sich schlicht nicht mehr leisten, im Bereich der Regulatorik nur die Mindestanforderungen zu erfüllen. Wer als Unternehmen die Risiken jetzt angeht, Regulationen umsetzt und die Resilienz erhöht, profitiert in jedem Fall – auf kurze ebenso wie auf lange Sicht.