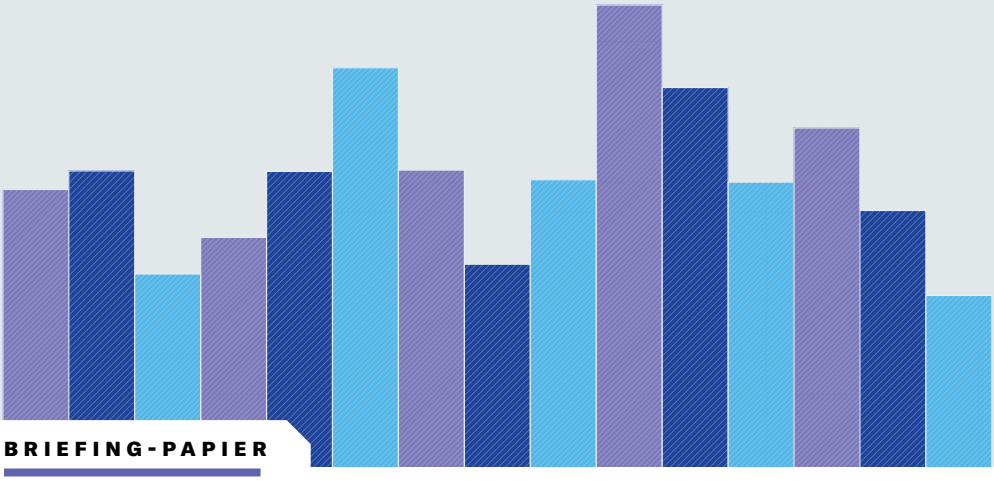
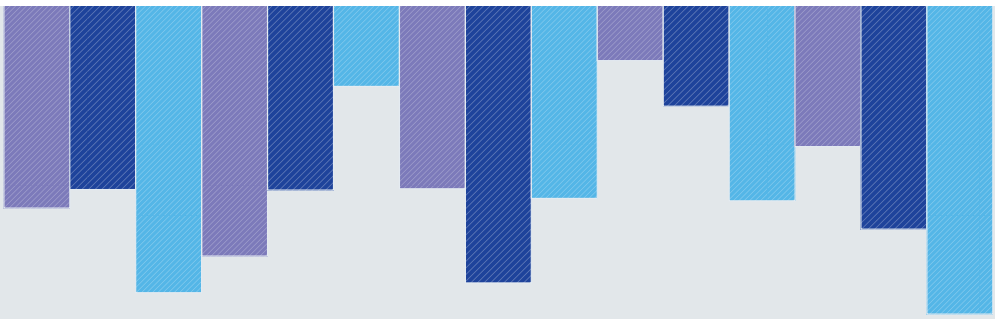
Harvard Business Review
ANALYTIC SERVICES



BRIEFING-PAPIER

Cyber-Resilienz im Zeitalter strenger Compliance-Vorschriften



Gesponsert von

Commvault®

Aufgrund des zunehmenden Drucks, der durch die Komplexität der IT, die behördliche Kontrolle und Ransomware-Angriffe entsteht, sind Investitionen in ein aktives Compliance-Programm für Unternehmen und die Unterstützung durch die Geschäftsführung der wichtigste Indikator für die Bereitschaft und Widerstandsfähigkeit gegenüber Cyberangriffen. Unternehmen sind gefordert, proaktiv zu handeln und Programme für Bereitschaft, Wiederherstellung und Resilienz zu entwickeln, um einen kontinuierlichen Geschäftsbetrieb zu gewährleisten. Warum?

Der Grund dafür ist, dass man sich auf einen Notfall vorbereiten muss, bevor er eintritt. Für die Cyber-Resilienz müssen drei verschiedene Teams einsatzbereit sein. Diese drei Teams arbeiten gleichzeitig, aber getrennt voneinander:

1. Team für die Reaktion auf und die Behebung von Sicherheitsverletzungen
2. Team für regulatorische und rechtliche Fragen
3. Team für die Geschäftsfähigkeit

Resilienz lässt sich durch funktionsübergreifende Zusammenarbeit, Tests und dynamische Prozesse erreichen. Fehlt ein solides Bereitschaftsprogramm, ist ein Unternehmen ständig im Aufholmodus, spielt bei einer Sicherheitslücke „Katz und Maus“, kämpft darum, schlechte Akteure aus den Systemen zu entfernen, und versucht gleichzeitig herauszufinden, was und wann es mit Kunden und dem Markt kommunizieren soll und wie es die Anforderungen der Aufsichtsbehörden einhalten kann. Das ist eine echte Katastrophe.

Dieses umfassende Dokument, welches von Harvard Business Review Analytic Services für CommVault erstellt wurde, beschreibt die Lösung für das Chaos. Diese Studie verdeutlicht die Notwendigkeit einer kontinuierlichen Compliance, um die wirtschaftliche Tragfähigkeit und die operative Belastbarkeit aufrechtzuerhalten, und untersucht die Herausforderungen bei der Einrichtung eines robusten Programms zur Stärkung der Cyber-Resilienz sowie die Bedeutung der Einhaltung globaler regulatorischer Anforderungen zum Schutz von Daten.

In diesem Bericht, der mit Kommentaren sowie Erkenntnissen von Branchenführern und Experten gespickt ist, finden Sie eine Anleitung für jede Organisation, die sich in der komplexen Landschaft von Cyber-Bedrohungen und behördlichen Anforderungen zurechtfinden muss.

Wir erhoffen uns, dass dieser Bericht Ihnen auf Ihrem Weg zu proaktiver Compliance und Resilienz behilflich sein wird: In der heutigen digitalisierten Welt sind wir alle im selben Team, wenn es um den Schutz von Daten und Systemen geht.

Danielle Sheer
Chief Trust Officer
Commvault

Cyber-Resilienz im Zeitalter strenger Compliance-Vorschriften

ÜBER DIE DENKWEISE von Risiko-, Compliance- und Sicherheitsexperten gibt es wenig Rätselhaftes. Daten- und Cyber-Störungen machen ihnen Angst. Aus dem im Oktober 2023 veröffentlichten Bericht, den das in Toronto ansässige Informationskonglomerat Thomson Reuters im Rahmen seiner Umfrage zu Risiken und Compliance veröffentlicht hat, geht hervor, dass 82 % der Risiko- und Compliance-Experten Daten- und Cybersicherheitsbedenken als das größte Risiko für ihre Organisation nannten – und damit fast doppelt so viele Antworten auf diesen Bereich fielen, wie auf das Problem, dem die nächstgrößte Relevanz beigemessen wurde.[1] **ABBILDUNG 1** Unterdessen ergab die Umfrage zu globalen Krisen und Resilienz 2023 von PwC, die im Dezember 2023 von dem in London ansässigen professionellen Dienstleistungsunternehmen veröffentlicht wurde, dass 96 % der Organisationen in den letzten zwei Jahren Störungen erlebt haben, wobei 76 % angaben, dass die schwerwiegendste Störung einen mittleren bis hohen Einfluss auf den Betrieb hatte.[2]

Diese Einstellung offenbart, was Risiko-, Compliance- und Sicherheitsexperten genau verstehen: Unternehmen sollten das Thema Cyber-Resilienz nicht auf die leichte Schulter nehmen – insbesondere, da die Vorbereitung auf Cyber-Ereignisse komplizierter ist als je zuvor. Die Ära der kontinuierlichen Compliance ist angebrochen. Die wirtschaftliche Stabilität der Welt erfordert ständig verfügbare Cloud-Dienste und kompromisslosen Datenschutz. Während viele Unternehmen noch dabei sind, die wachsende Bedeutung der künstlichen Intelligenz (KI) für die Sicherung beider Aspekte zu verstehen, haben Regulierungsbehörden auf mehreren Kontinenten strenge digitale Sicherheitsvorkehrungen getroffen, die hohe Geldstrafen für die Nichteinhaltung von Vorschriften für Organisationen vorsehen, die diese strengen Anforderungen nicht erfüllen.

Tatsächlich wird die nahezu vollständige Beseitigung schwerwiegender Betriebsstörungen und der Beitrag der KI dazu die größte Bedeutung für die Widerstandsfähigkeit gegenüber Cyberangriffen haben, so die Prognose von Michael Rasmussen, Governance-, Risiko- und Compliance-Analyst bei GRC 20/20 Research, einem globalen Marktforschungsunternehmen mit Sitz in Milwaukee. „In den nächsten drei bis fünf Jahren ist davon auszugehen, dass KI-gestützte Dienste noch ausgefeilter werden. Fortschritte beim maschinellen Lernen ermöglichen prädiktive Sicherheitsmaßnahmen, die Bedrohungen vorhersehen und neutralisieren können, bevor sie eintreten."

Organisationen dürften bereits mit Gesetzesentwürfen vertraut sein, die entweder auf den Schutz von Daten (Datenschutz-Grundverordnung, Data Governance Act, European Data Act), die Gewährleistung der System- und Informationssicherheit (Network and

HIGHLIGHTS

Resilienz erfordert gemäß vieler Definitionen, dass Organisationen die Fähigkeit erlangen, **von Menschen verursachte oder natürliche Katastrophen vorherzusehen, Störungen mit geringen Schäden zu überstehen** und **Daten und Vorgänge danach fast sofort** wiederherzustellen.

Die Integration neuer Compliance-Funktionen in bestehende Geschäftsprozess-Workflows **ist besonders schwierig für Organisationen, die keine Compliance-Kultur fördern und zu wenig in die kontinuierliche Überwachung und Verbesserung investieren**.

Fortschritte in der Forschung im Bereich der künstlichen Intelligenz könnten eine wichtige Rolle dabei spielen, **Organisationen bei der Bewältigung aller Aufgaben zu unterstützen – von der Gefahrenabwehr bis hin zur automatischen Erstellung von Compliance-Berichten,** die den globalen regulatorischen Anforderungen entsprechen.

„In den nächsten drei bis fünf Jahren können wir davon ausgehen, dass KI-gestützte Dienste noch ausgefeilter werden. Fortschritte beim maschinellen Lernen ermöglichen vorausschauende Sicherheitsmaßnahmen, die Bedrohungen antizipieren und neutralisieren können, bevor sie eintreten“, sagt Michael Rasmussen, Analyst für Governance, Risk und Compliance bei GRC 20/20 Research.

Information Security Directive 2 (NIS2), Cyber Resilience Act, Critical Entities Resilience Directive) oder auf spezifische Anwendungsfälle (EU-KI-Gesetz) abzielen. Dieses Regelwerk bildet die Grundlage für die vielleicht größte Herausforderung im Bereich der Compliance: das Digital Operational Resilience Act (DORA) der Europäischen Union, das strenge Risikomanagement-Rahmenbedingungen, Resilienzprüfungen und die Meldung von Vorfällen vorschreibt.

Organisationen, denen es in einer global vernetzten digitalen Wirtschaft gut gehen soll, müssen sich in diesem Buchstabensalat aus komplexen Vorschriften zurechtfinden und die Resilienz aufbauen, um Fehler und Angriffe zu überstehen, die nicht nur ihre Lieferketten, Rechenzentren, Netzwerke und Cloud-Operationen stören, sondern auch ihren Partnern, Kunden und Aktionären schaden. Der Regulierungsansatz läuft in der Regel auf ein grundlegendes Konzept hinaus, wobei es keine Rolle spielt, um welche Region oder Branche es sich handelt: Stärken Sie jedes einzelne Glied in der digitalen Kette, von den ressourcenreichen bis zu den ressourcenarmen, und ziehen Sie Organisationen für ihre Aktionen zur Rechenschaft.

„Ich bin der Meinung, dass viele dieser Vorschriften darauf abzielen, sicherzustellen, dass die Gesellschaft angesichts unserer enormen wirtschaftlichen Interdependenz nicht von Unternehmen beeinträchtigt wird, die ihr eigenes Risiko nicht verstehen oder nicht dafür sorgen“, erklärt Jonathan Fairtlough, Principal bei KPMG, einer strategischen Unternehmensberatung mit Sitz in London. Cyberrisiken, für die einst Computerteams zuständig waren, sind zu einem „entscheidenden Bestandteil der Geschäftsplanung, der Kontinuitätsplanung und der Risikobewertung“ geworden, so Fairtlough. „Aus diesem Grund werden in immer mehr Vorständen Möglichkeiten geschaffen, Cyberrisiken zu überwachen und zu verstehen, da sie ihre grundlegende Rolle im Unternehmen betreffen.“

Aufgrund dieser aktuellen und anstehenden Vorschriften stehen Organisationen in Nordamerika, Europa und im asiatisch-pazifischen Raum zunehmend unter dem Druck, robuste Programme zur Stärkung der Cyber-Resilienz zu etablieren und in die richtigen Tools und Talente zu investieren, um sowohl eine ordnungsgemäße Datenverarbeitung und -sicherung als auch die Speicherung sensibler Daten in Bezug auf ihre Produkte, Dienstleistungen, Kunden, Partner und Mitarbeiter zu gewährleisten. Die Erfüllung dieses Mandats ist keine leichte Aufgabe. Das Etablieren von Cyber-Resilienz unterliegt hohen Maßstäben. Gemäß vieler Definitionen erfordert Resilienz, dass Organisationen die Fähigkeit erlangen, von Menschen verursachte und natürliche Katastrophen vorherzusehen, Störungen mit geringen Schäden zu überstehen und Daten und Vorgänge danach fast sofort wiederherzustellen. Um diese hohen Standards der betrieblichen Resilienz zu erfüllen, müssen Organisationen bewährte Verfahren anwenden, wie z. B. häufige Wiederherstellungstests, Cyber-Reinräume (isoliert von externen Bedrohungen), bessere Berichtsfunktionen und robuste Cloud-native Cyber-Abwehrmaßnahmen.

Dieser Artikel befasst sich mit den wesentlichen Komponenten der Einhaltung von Vorschriften und der Cyber-Resilienz im digitalen Zeitalter und hebt die enormen Herausforderungen hervor, denen sich Organisationen auf der ganzen Welt gegenübersehen, wenn sie versuchen, Resilienz gegenüber starken und sich weiterentwickelnden Bedrohungen, einschließlich neuer, zu entwickeln. Darüber hinaus wird die zunehmende regulatorische Aufsicht hervorgehoben, die Organisationen mit erheblichen Strafen für Datenmissmanagement und unvorsichtige Aktionen bedroht, die Märkte und Lieferketten schädigen. Ferner wird untersucht, wie Organisationen ihre operative Resilienz verbessern und stärken können, ohne ihre geschäftliche Agilität zu beeinträchtigen.

Kostspielige Störung des Geschäftsbetriebs

Im wirtschaftlichen Kontext spiegelt die bevorstehende und beispiellose Regulierungswelle das weit verbreitete und abgestimmte Interesse der Regierungen wider, das Risiko kostspieliger kommerzieller Störungen zu verringern, wenn nicht sogar zu beseitigen. Am häufigsten treten Probleme durch schlecht verwaltete Cloud-Rechenzentren und fehlerhafte cloudbasierte Anwendungen von Softwareanbietern auf, die zu schädlichen Systemausfällen und Betriebsunterbrechungen führen können, wie beispielsweise der weit verbreitete CrowdStrike-Ausfall am 19. Juli 2024. Ein Bericht, der kurz nach dem mehrtägigen Ausfall von Parametrix, einem in New York ansässigen Cyber-Versicherer, erstellt wurde, bezifferte die Kosten des Vorfalls für US-amerikanische Fortune-500-Unternehmen auf 5,4 Milliarden US-Dollar, ganz zu schweigen von möglichen Reputationsschäden, Prozesskosten, behördlichen Strafen oder dem Verlust von Unternehmenswert.[3]

Im Kampf gegen Serviceunterbrechungen und zur Einhaltung immer strengerer Datenschutzbestimmungen müssen Organisationen eine umfassende Strategie entwickeln, die eine größere betriebliche Resilienz sowohl gegen natürliche als auch gegen von Menschen verursachte Störungen ermöglicht, einschließlich solcher, die auf eine unsachgemäße

Datenverwaltung zurückzuführen sind. Die Sache duldet keinen Aufschub. Der Bericht des Weltwirtschaftsforums mit dem Titel „Global Cybersecurity Outlook 2023“ mit Sitz in Cologny, Schweiz, kam zu dem Schluss, dass „Cyber-Angreifer sich eher auf Geschäftsunterbrechungen und Rufschädigung konzentrieren werden“. Bemerkenswerterweise glauben mehr als neun von zehn Führungskräften aus den Bereichen Cybersicherheit und Wirtschaft, die an der Studie teilgenommen haben, dass ein „weitreichendes, katastrophales Cyberereignis in den nächsten zwei Jahren zumindest etwas wahrscheinlich ist“.[4]

Gemäß Rasmussen von GRC 20/20 bedeutet „in einer Welt, in der Unternehmensrisiken immer komplexer und vernetzter werden, Compliance und Resilienz, dass Ihre Organisation regulatorischem Druck standhalten, kritische Vermögenswerte schützen und Kontinuität und Resilienz inmitten des Chaos des geschäftlichen Wandels gewährleisten kann.“

Er sieht einen strategischen Vorteil darin, diese Komplexität zu überwinden. „Strategisch positioniert diese [Compliance-Bemühung] die Organisation als vertrauenswürdige Einheit, die in der Lage ist, Kunden und Stakeholdern einen gleichbleibenden Mehrwert zu bieten und gleichzeitig Störungen und die damit verbundenen Kosten zu minimieren.“

Große Herausforderungen für die Resilienz

Cédric Burton, globaler Co-Vorsitzender und Partner für Daten, Datenschutz und Cybersicherheit im Brüsseler Büro der in Palo Alto, Kalifornien, ansässigen Anwaltskanzlei Wilson Sonsini, empfiehlt multinationalen Unternehmen, die Resilienz gegenüber Cyberangriffen als eine Notwendigkeit zu betrachten. „Wenn man heutzutage als Unternehmen erfolgreich sein will, muss man sich um solide Cyberpraktiken kümmern, d. h. man muss über eine gewisse Resilienz im Cyberbereich verfügen“, sagt er. „Sonst geht das Vertrauen verloren.“

Unbestritten ist, dass die Resilienz im Bereich der Cybersicherheit einer der wesentlichen Bausteine der Weltwirtschaft ist. Aber die Spielregeln für die Cyber-Resilienz haben sich geändert. Vor nicht allzu langer Zeit konzentrierten sich Organisationen hauptsächlich darauf, sich schnell von Katastrophen zu erholen, anstatt sie zu verhindern. Vor der Einführung der Cloud schickten Organisationen LKW-Ladungen mit Daten, die auf Bandspulen gespeichert waren, zur sicheren Aufbewahrung in externe Lagerhäuser. Diese Band-Backups hielten nicht ewig und waren quasi unzugänglich – das genaue Gegenteil der modernen Anforderungen an die Resilienz von Unternehmen. Zwar bieten Cloud-Dienste Unternehmen eine Vielzahl attraktiver Wiederherstellungsoptionen, wie z. B. globale Datenredundanz, doch erhöht die Cloud auch das Unternehmensrisiko in Form von allgegenwärtigen Cyberangriffen, einschließlich Ransomware, bei denen Organisationen Hackern bis zu Millionen von Dollar für den Zugriff auf ihre gestohlenen und verschlüsselten Datensätze zahlen müssen.

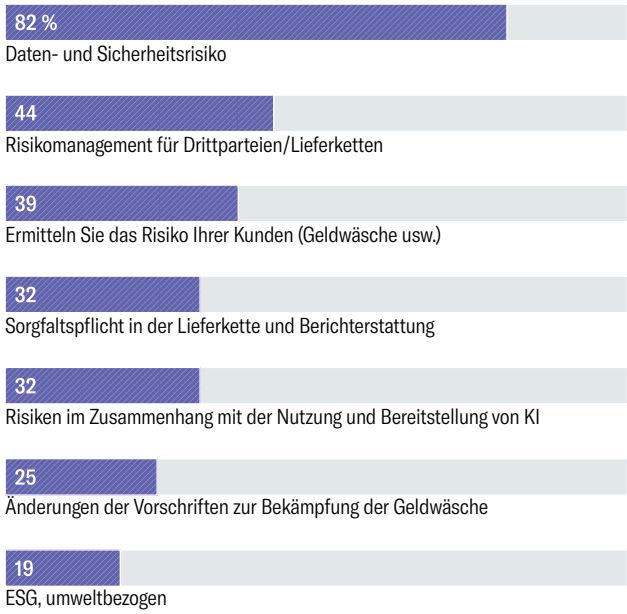
Der Betrieb in der öffentlichen Cloud bedeutet nicht, dass die Verantwortung für die betriebliche Resilienz abgegeben wird. Unternehmen, die die Dienste von Cloud-Anbietern in Anspruch nehmen, müssen sich auch dem „Modell der gemeinsamen Verantwortung“ anschließen, bei dem die Sicherheit eine gemeinsame Aufgabe ist, bei der der Anbieter die Infrastruktur und die Netzwerke verwaltet und der Kunde die Datensicherheit und die Anwendungen überwacht. Cloud-Kunden müssen Strategien für Datenschutz und Cyber-Resilienz unter Berücksichtigung des Modells der gemeinsamen Verantwortung formulieren.

ABBILDUNG 1

Risiko trifft auf Compliance

Organisationen betrachten Daten als ihr größtes Risiko

Welches der folgenden Konzepte stellt das größte Risiko für Ihre Organisation dar?



Unternehmen, insbesondere in regulierten Branchen, sind in Zeiten strenger globaler Regulierungskontrollen der drohenden Gefahr finanzieller Strafen und Rufschädigung durch Datenschutzverstöße ausgesetzt. Clouds und Software-Lieferketten sind zu Datenverwaltungs- und Regulierungs-Minenfeldern geworden. Leider, so der Hinweis von Rasmussen, „kann das Modell der gemeinsamen Verantwortung für die Cloud-Sicherheit zu Verwirrung darüber führen, wer wofür verantwortlich ist, was das Risiko von Fehlkonfigurationen und Datenlecks erhöht.“

Resilienz ist kein Kinderspiel und erfordert die Übernahme bewährter technologischer Rahmenbedingungen und eine sorgfältige Bewertung der laufenden Risiken und Chancen. „Die betriebliche Resilienz ist mehr als eine Vorschrift“, so der Hinweis von Rasmussen. „Jede Organisation braucht ein Konzept für den Umgang mit Integrationsrisiken und sollte ihre aktuelle Compliance-Haltung und ihre Resilienz-Fähigkeiten bewerten“, fügt er hinzu. „Diese [Bewertung] beinhaltet die Kartierung ihrer Lieferketten, die Identifizierung kritischer Abhängigkeiten und die Bewertung der potenziellen Auswirkungen von Störungen.“

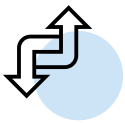
Wenn eine Organisation potenzielle Schwachstellen identifiziert, empfiehlt Burton von Wilson Sonsini eine Analyse der Lücke zwischen den aktuellen Praktiken und den Anforderungen eines geltenden Rechtsrahmens. „Sobald Sie die Lücke identifiziert haben, sollten Sie versuchen, sie zu schließen, indem Sie einen Rahmen schaffen [oder übernehmen], der es Ihnen ermöglicht, die Lücken zu schließen und zu überbrücken", rät er.

Nach Abschluss dieser Schritte empfiehlt Burton, den Plan zu prüfen, zu testen und einer „laufenden Überprüfung zu unterziehen, um sicherzustellen, dass er sich ständig verbessert. Die einzige Möglichkeit, vorbereitet zu sein, ist die Praxis." Ein Ansatz besteht in der Durchführung von Planspielen, bei denen die Rolle jedes Teammitglieds bei der Reaktion auf einen Cyber-Notfall simuliert wird. Organisationen haben die Möglichkeit, die Messung der Verbesserung anhand von Leistungskennzahlen wie der durchschnittlichen Wiederherstellungszeit, der Systemverfügbarkeit, der Teamschulung und der Häufigkeit der Aktualisierung von Reaktionsplänen bei Vorfällen vorzunehmen. Bei einer anderen Form der Vorbereitung werden Reinraumtests durchgeführt, eine Technik zur Identifizierung und Beseitigung von Fehlern, die Software anfällig für Cyber-Bedrohungen machen können. Reinraumtests stellen eine aufstrebende, manchmal kostspielige und komplizierte Praxis dar, die Organisationen dabei hilft, den Aufsichtsbehörden nachzuweisen, dass sie angemessene Messungen zum Datenschutz durchführen.

Allerdings haben die meisten Organisationen eine „Tendenz zur Abschottung", was das Management von Compliance und Resilienz betrifft, erklärt Fairtlough von KPMG. Diese Herangehensweise kann zu einer „Lücke im Verständnis dafür führen, wie alles zusammenhängt". Im Gegensatz dazu können diejenigen, die Risiken ganzheitlich betrachten, ihren Vorständen mitteilen, dass das Risikomanagement zwar einen erheblichen Einfluss auf das Unternehmen hat, aber „mit der bestehenden Geschäftskontinuitäts- und Notfallwiederherstellungsplanung verflochten ist". Infolgedessen, so fügt er hinzu, verbessert die Integration einer ganzheitlichen Risikobetrachtung in die Organisationsplanung die Fähigkeit einer Organisation, „ihre Produktions- und Vertragsanforderungen zu erfüllen", indem Informationssilos beseitigt werden, die die Einhaltung von Vorschriften und bewährte Verfahren zur Cyber-Resilienz behindern.

Schon seit Langem ist bekannt, dass die Unterstützung und Förderung von Führungskräften für groß angelegte Organisationsprojekte dazu beitragen kann, unterschiedliche Geschäftsbereiche aufeinander abzustimmen. Die Integration neuer Compliance-Funktionen in bestehende Geschäftsprozess-Workflows ist besonders schwierig für Organisationen, die keine Compliance-Kultur fördern und zu wenig in die kontinuierliche Überwachung und Verbesserung investieren. Eine Anpassung an die Anforderungen einer komplizierten Cloud-Architektur und einer sich schnell entwickelnden regulatorischen und Cyber-Bedrohungslandschaft ist nichts, was man einfach dem Compliance-Team überlassen kann. Bei dieser Unternehmensinitiative packen alle mit an, was mit erheblichem Planungs- und Investitionsaufwand, Schulungen, Überwachung und Tests verbunden ist.

Der Aufbau einer erfolgreichen Compliance- und Resilienz-Strategie erfordert ein kontinuierliches Engagement des Vorstands, merkt Rasmussen an. Außerdem brauche es „ein tiefes Verständnis für das sich entwickelnde Geschäftsumfeld und die Risiko-/Bedrohungslandschaft sowie eine Kultur, die dem Risiko- und Resilienzmanagement auf allen Ebenen der Organisation Priorität einräumt", sagt er. „Die Schwierigkeit besteht oft nicht in der Technologie selbst, sondern darin, die [kontinuierliche Compliance-] Denkweise und Ausrichtung über verschiedene Unternehmensfunktionen hinweg zu fördern und die Dinge in einem sehr dynamischen und sich verändernden Geschäftsumfeld auf dem neuesten Stand zu halten."



Diejenigen, die Risiken ganzheitlich betrachten, können ihren Vorständen mitteilen, dass das Risikomanagement zwar einen erheblichen Einfluss auf das Unternehmen hat, aber „mit der bestehenden Geschäftskontinuitäts- und Notfallwiederherstellungsplanung verflochten ist", sagt Jonathan Fairtlough, Principal bei KPMG.

Risiko aus kultureller Sicht

Natürlich ist es naheliegend, aber auch riskant anzunehmen, dass die Einhaltung von Vorschriften und Cyber-Resilienz von Regulierungsbehörden auf der ganzen Welt auf die gleiche Weise definiert oder interpretiert werden. Fairtlough argumentiert, dass US-Unternehmen Compliance oft als binäre Bedingung betrachten. „Wir konzentrieren uns auf Wörter wie Compliance, bei denen wir einen Standard wie den NIST-Standard [National Institute of Standards and Technology] heranziehen, daran arbeiten, diesen Standard zu erfüllen, und dies ausführlich dokumentieren, um zu zeigen, dass wir den Standard erfüllt haben." Seiner Meinung nach zeige die Einhaltung der EU-Vorschriften jedoch eine andere Perspektive – nämlich, dass man sich mit dem Risiko auseinandergesetzt hat und einen Plan zu seiner Minderung hat. „Es ist keine Checkliste, sondern eine Risikoanalyse. Was Sie für die Einhaltung vorweisen müssen, ist etwas anders", sagt Fairtlough. „Das wird oft übersehen. Dieses Problem, diese kulturelle Kluft, ist einer der Bereiche, mit denen Unternehmen meiner Meinung nach Schwierigkeiten haben."

Die Entwicklung individueller Rahmenbedingungen für jedes Land oder geltende Vorschriften wäre selbst für riesige globale Organisationen weder praktisch noch kosteneffizient. „Unternehmen können die EU nicht isoliert betrachten", stellt Burton fest. „Man kann kein Datenschutzkonzept nur für ein Land oder einen Kontinent umsetzen. Bedrohungen kommen aus der ganzen Welt und Daten sind global. Das macht die Sache für Unternehmen sehr viel komplexer."

„Man kann kein Datenschutzkonzept nur für ein Land oder einen Kontinent umsetzen. Bedrohungen kommen aus der ganzen Welt und Daten sind global. Das macht die Sache für Unternehmen sehr viel komplexer“, sagt Cédric Burton, globaler Co-Vorsitzender und Partner für Daten, Datenschutz und Cybersicherheit bei Wilson Sonsini.

„Die schiere Menge an Daten, die jetzt verfügbar ist, kann Organisationen, die nicht dafür gerüstet sind, überfordern. Daher ist es von entscheidender Bedeutung, über die richtigen Tools und das nötige Fachwissen zu verfügen, um KI und Big Data effektiv nutzen zu können“, sagt Rasmussen von GRC 20/20 Research.

Auf der anderen Seite ist Rasmussen der Meinung, dass Organisationen einen „einheitlichen Rahmen für das Risikomanagement und die Resilienz schaffen sollten, der sowohl mit globalen als auch mit nationalen Vorschriften übereinstimmt.“ Er sagt, dieser sollte „die Nutzung von Technologie zur kontinuierlichen Überwachung und Förderung einer Kultur der Compliance in der gesamten Organisation“ umfassen. Als praktische Maßnahme rät Rasmussen seinen Kunden, „Compliance in ihre täglichen Abläufe einzubetten“. „Organisationen [können] Strafen vermeiden und ihre allgemeine Sicherheitslage stärken, wodurch sie besser auf Bedrohungen reagieren können.“

Unternehmen, die in asiatisch-pazifischen Ländern wie China tätig sind, unterliegen ebenfalls neuen Vorschriften in Bezug auf Datenschutz, Privatsphäre und Geldwäschebekämpfung. Sowohl Burton als auch Fairtlough warnen davor, dass die zweitgrößte Volkswirtschaft der Welt Unternehmen, die dort tätig sind, vor Compliance-Hürden stellt. „Der chinesische Rechtsrahmen ist sehr schwer zu durchschauen“, sagt Burton. Als Beispiel nennt er Einschränkungen bei der Datenübertragung und gibt den Hinweis: „Wenn Sie in China bestimmte Typen von Daten verarbeiten, benötigen Sie eine behördliche Genehmigung.“ So können Organisationen in China beispielsweise nur dann Verschlüsselung einsetzen, wenn die Regierung ebenfalls Zugriff auf einen „Schlüssel“ hat.

Trotz regionaler Unterschiede stellt Fairtlough eine gewisse Konsistenz bei den Schutzmaßnahmen, Technologien und Prozessen fest, die von Organisationen weltweit eingesetzt werden. „Die technischen Verfahren, die Sie zum Schutz Ihrer Daten einsetzen, werden größtenteils gleich bleiben“, sagt er. „Der Unterschied wird sich durch regulatorische oder gesetzliche Anforderungen wie die Datenlokalisierung ergeben – die Frage, wo Sie diese Daten speichern. Diese regulatorischen Unterschiede ändern auch die erforderlichen Genehmigungen, um einige technische Schutzmaßnahmen zu ergreifen. So kann beispielsweise für bestimmte Typen der Datenüberwachung, die ein Unternehmen in den USA eigenständig umsetzen darf, in Deutschland oder Frankreich die Zustimmung des Betriebsrats erforderlich sein. Sie müssen diese [Erlaubnis] in die allgemeine Risikoanalyse einbeziehen.“

KI verändert alles

Bei Cyber-Resilienz geht es nicht nur darum, Fehler zu überstehen. Es geht darum, die Geschäftskontinuität zu gewährleisten und bei Vorfällen eine schnelle Wiederherstellung zu ermöglichen.

KI kann bei diesem Vorhaben eine große Hilfe sein. „KI spielt beim Schutz von Cloud-Datenspeichern eine entscheidende Rolle, indem sie die Erkennung von Bedrohungen verbessert, Reaktionen auf Vorfälle automatisiert und Schwachstellen identifiziert, bevor sie von Kriminellen ausgenutzt werden können“, so Rasmussen. KI-gesteuerte Tools, sagt er, hätten die Komplexität des Managements von Cyberrisiken und der Einhaltung von Vorschriften „maßgeblich“ verändert. „Diese Technologien erfordern auch robuste Governance-Rahmenbedingungen, um die damit verbundenen Risiken zu managen, wie z. B. algorithmische Verzerrungen und Datenschutzbedenken“, gibt er zu bedenken. „Darüber hinaus kann die enorme Menge an Daten, die jetzt verfügbar ist, Organisationen, die nicht dafür gerüstet sind, überfordern. Daher ist es von entscheidender Bedeutung, über die richtigen Tools und das nötige Fachwissen zu verfügen, um KI und Big Data effektiv nutzen zu können.“

Ungeachtet ihrer positiven Auswirkungen bringt KI auch neue Formen von Cyberrisiken mit sich und macht Organisationen verwundbar, was sich negativ auf die Beziehungen zu Kunden und Partnern auswirken kann. Zwar nutzen Sicherheits- und Netzwerkteams KI-gestützte Überwachungstools, um Cyber-Bedrohungen zu erkennen, doch „haben die Bedrohungsakteure die gleiche Technologie zur Verfügung“, so der Hinweis von Burton. „Einerseits soll KI ein Unternehmensnetzwerk schützen, gleichzeitig wird sie aber auch von Angreifern genutzt, um neue Angriffe zu starten.“ Deepfakes, bei denen das Gesicht und der Körper einer Person aus böswilligen Gründen digital verändert werden, haben sich zu einer „der größten Herausforderungen für Unternehmen“ entwickelt, fügt er hinzu. „Mit Hilfe der KI-Technologie ist es sehr einfach, einen Deepfake zu erstellen.“ Burton ist der Meinung, dass bestehende Vorschriften „aufgrund der sich schnell entwickelnden Technologie schnell veraltet sind“.

Das kürzlich veröffentlichte EU-Gesetz zur künstlichen Intelligenz (KI) soll alles rund um die Nutzung von KI-Systemen innerhalb der EU regeln. Wie bei anderen EU-Verordnungen, z. B. DORA und NIS2, verfolgt das Gesetz einen „risikobasierten Ansatz“, bei dem KI-Systeme nach ihren potenziellen Risiken kategorisiert werden. Je riskanter die Anwendung, desto strenger die Kontrollen. So verbietet das Gesetz beispielsweise die Manipulation von Menschen und „sprachgesteuertes Spielzeug, das gefährliches Verhalten bei Kindern fördert“.[5] Das Gesetz legt unter anderem Standards für Transparenz fest und verpflichtet Organisationen, Kunden darüber zu informieren, dass sie mit einem Chatbot und nicht mit einem Menschen interagieren. Die Bestimmungen des Gesetzes werden in den nächsten drei Jahren schrittweise eingeführt, und es wird davon ausgegangen, dass die Geldbußen bei Nichteinhaltung bis zu 35 Millionen Euro oder zwischen 1 % und 7 % des Jahresumsatzes betragen können, je nachdem, welcher Betrag höher ist.

„KI ist derzeit aus regulatorischer Sicht das wichtigste Thema“, sagt Burton. „Jede Regulierungsbehörde auf der Welt versucht, ein Stück vom Kuchen abzubekommen, und das gilt für das Kartellrecht, das gilt für die Datenschutzbehörden in der EU und das gilt auch für die KI-Regulierungsbehörden mit neuen KI-Vorschriften.“ Er warnt

„KI ist derzeit aus regulatorischer Sicht das Topthema. Jede Regulierungsbehörde auf der Welt versucht, ein Stück vom Kuchen abzubekommen, und das gilt für das Kartellrecht, das gilt für die Datenschutzbehörden in der EU und das gilt auch für die KI-Regulierungsbehörden mit neuen KI-Vorschriften“, sagt Burton von Wilson Sonsini.

Fairtlough von KPMG empfiehlt Organisationen, festzulegen, wie ihre Daten analysiert werden, wo dies geschieht und was die Organisation über die Nutzung der Daten aus datenschutzrechtlicher Sicht weiß.

davor, dass es „für eine Organisation sehr komplex werden wird, jede einzelne Vorschrift zu identifizieren und sicherzustellen, dass sie [ihnen] entspricht".

Um Probleme mit den Vorschriften zu vermeiden, ist Planung erforderlich. Die Grundlagen für den Einsatz von KI zu schaffen, ist ähnlich wie das Verständnis Ihrer finanziellen Situation, sagt Fairtlough. „Wie können Sie eine langfristige Finanzplanung vornehmen, wenn Sie nicht wissen, wie viel Geld Sie haben, welche Konten Sie haben, was Ihnen geschuldet wird und wie hoch Ihre Forderungen sind?" fragt er. „In der Theorie, mit Daten und mit Technologie schaffen diese Dinge einen Mehrwert." Fairtlough empfiehlt Organisationen, festzulegen, wie ihre Daten analysiert werden, wo dies geschieht und was die Organisation über die Verwendung der Daten aus datenschutzrechtlicher Sicht weiß. Er rät dazu, die Auswirkungen potenzieller Probleme wie einer Dienstunterbrechung, eines technischen Problems oder einer regulatorischen Hürde zu bewerten.

Laut Fairtlough sind Organisationen erst nach Abschluss dieser Bewertung angemessen darauf vorbereitet, große Sprachmodelle zu nutzen und ihr volles Potenzial auszuschöpfen, „weil ich weiß, wo ich meine Daten ausrichten muss und welche Daten mir gehören", erklärt er. „Und ich bin in der Lage, eine Governance-Struktur zu schaffen, da ich weiß, dass ich Daten verwende, die ich rechtmäßig sammeln durfte, die Teil meines gesamten Analysesets sind, und ich kann den Ergebnissen vertrauen." Zuletzt stellte er die Frage: „Welche Schritte unternehme ich, um diese Daten entsprechend dem Risiko, das sie für mein Unternehmen darstellen, zu schützen?" Fortschritte in der KI-Forschung könnten eine wichtige Rolle dabei spielen, Organisationen bei der Verwaltung aller Aspekte zu unterstützen, von der Bedrohungsprävention bis hin zur automatischen Erstellung von Compliance-Berichten, die den globalen regulatorischen Anforderungen entsprechen. Rasmussen ist der Meinung, dass KI und maschinelles Lernen in den nächsten drei bis fünf Jahren praktische Dinge für Organisationen tun werden. „KI wird eine Schlüsselrolle bei der Sicherstellung der Compliance, der Automatisierung des Auditierungsprozesses und der Bereitstellung von Echtzeit-Einblicken in die Sicherheitslage einer Organisation spielen", sagt er.

Burton prognostiziert, dass KI-Tools die Erkennung von Bedrohungen erheblich verbessern und Organisationen Echtzeitanalysen drohender Gefahren bieten werden. „Sie werden bei der Wiederherstellung eines Systems effizienter sein, da viele Aufgaben automatisiert werden", sagt er, und er geht davon aus, „dass auch die Verschlüsselung durch KI automatisiert wird – und Ihr Verschlüsselungsmodell in Echtzeit an den Typ der Bedrohung anpasst, mit der Sie konfrontiert sind."

Fazit

Der lange Weg zu Cyber-Resilienz und zur Einhaltung von Vorschriften fängt damit an, dass sich die Geschäftsführung des Problems annimmt, in der Regel mit Unterstützung auf Vorstandsebene. Organisationen, deren Wettbewerb auf globalen Märkten stattfindet, müssen sich an eine wachsende Zahl unterschiedlicher Vorschriften halten, die darauf abzielen, Daten zu schützen und Unternehmen davon abzuhalten, Lieferketten und den digitalen Handel zu stören – Regeln, die darauf abzielen, Unternehmen für ihre Aktionen oder Fehltritte zur Verantwortung zu ziehen.

Jedoch sind es nicht nur die drohenden hohen Bußgelder, die Organisationen dazu motivieren, ihre Resilienz und Cyberabwehr zu verbessern. Auch ungeplante Serviceunterbrechungen wie Netzwerk- oder Cloud-Ausfälle, Ransomware und Datenverluste können das Vertrauen von Kunden, Partnern und Stakeholdern gefährden. Der Hauptgrund, warum Vorstände in die Resilienz von Unternehmen investieren, ist laut 49 % der Befragten in der PwC-Umfrage vom Dezember 2023 die „Reduzierung von Verlusten durch zukünftige Störungen".[6]

Wie werden Organisationen auf die strengen Anforderungen von Vorschriften wie der NIS2 der EU, die Sicherheit gewährleisten, und DORA, die sich mit Resilienz befasst, reagieren? Strenge Tests, Reinräume und ein besseres Risikomanagement können die Cyber-Resilienz stärken. Aber KI wird kein unmittelbares Allheilmittel sein. Die Zahl der KI-bezogenen Tools, die Unternehmen bei der Erkennung von Bedrohungen unterstützen sollen, nimmt zu, aber ebenso die Bedenken von Regierungen und Unternehmen hinsichtlich KI-Cyberrisiken durch Deepfakes und Fehler. Neue EU-Verordnungen und ausstehende Gesetze in Kalifornien zielen darauf ab, algorithmische Verzerrungen zu verringern und Datenschutzverletzungen zu begrenzen.

DORA und andere Vorschriften mögen einige Organisationen dazu zwingen, ihre Cyber-Resilienz zu verbessern, aber es ist auch einfach wirtschaftlich sinnvoll, Daten und Cyber-Operationen so intelligent wie möglich zu verwalten. „Diese Vorschriften zwingen Organisationen dazu, ihre Risikomanagementstrategien zu überdenken und sich stärker auf kontinuierliche Überwachung, Reaktion auf Vorfälle und Wiederherstellungsfähigkeiten zu konzentrieren", erklärt Rasmussen. „Organisationen sollten ihre Vorgehensweise unbedingt anpassen – nicht nur, um die Compliance-Anforderungen zu erfüllen, sondern um sie zu übertreffen. Durch diese Vorgehensweise können sie ihre Betriebsabläufe zukunftssicher gegen neue und unvorhergesehene Herausforderungen machen und sicherstellen, dass sie angesichts sich entwickelnder Risiken konform, robust und anpassungsfähig bleiben."

Abschließende Bemerkungen

1 Thomson Reuters, „The 2023 Thomson Reuters Risk & Compliance Survey Report," 13. Oktober 2023. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/risk-compliance-survey-report-2023/.

2 PwC, „PwC's Global Crisis and Resilience Survey 2023," Dezember 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

3 Parametrix, „CrowdStrike's Impact on the Fortune 500," 24. Juli 2024. https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

4 The World Economic Forum, "Global Cybersecurity Outlook 2023," Januar 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.

5 The European Parliament, "EU AI Act: first regulation on artificial intelligence," 8. Juni 2024. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

6 PwC, „PwC's Global Crisis and Resilience Survey 2023," Dezember 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

Harvard Business Review
ANALYTIC SERVICES

ÜBER UNS

Harvard Business Review Analytic Services ist eine unabhängige gewerbliche Forschungseinheit innerhalb der Harvard Business Review Group, die Forschung und vergleichende Analysen zu wichtigen Management-Herausforderungen und neu entstehenden Geschäftsmöglichkeiten durchführt. Mit dem Ziel Geschäftsinformationen und Erkenntnisse aus der Peer-Group zu liefern, wird jeder Bericht auf der Grundlage der Ergebnisse der ursprünglichen quantitativen und/oder qualitativen Forschung und Analyse veröffentlicht. Quantitative Erhebungen werden mit dem HBR Advisory Council, dem globalen Forschungspanel der HBR, durchgeführt, und qualitative Forschungsarbeiten werden mit Führungskräften der Wirtschaft und Fachexperten innerhalb und außerhalb der Autorengemeinschaft von *Harvard Business Review* durchgeführt. Schicken Sie uns eine E-Mail an hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services

MCCRE54701024