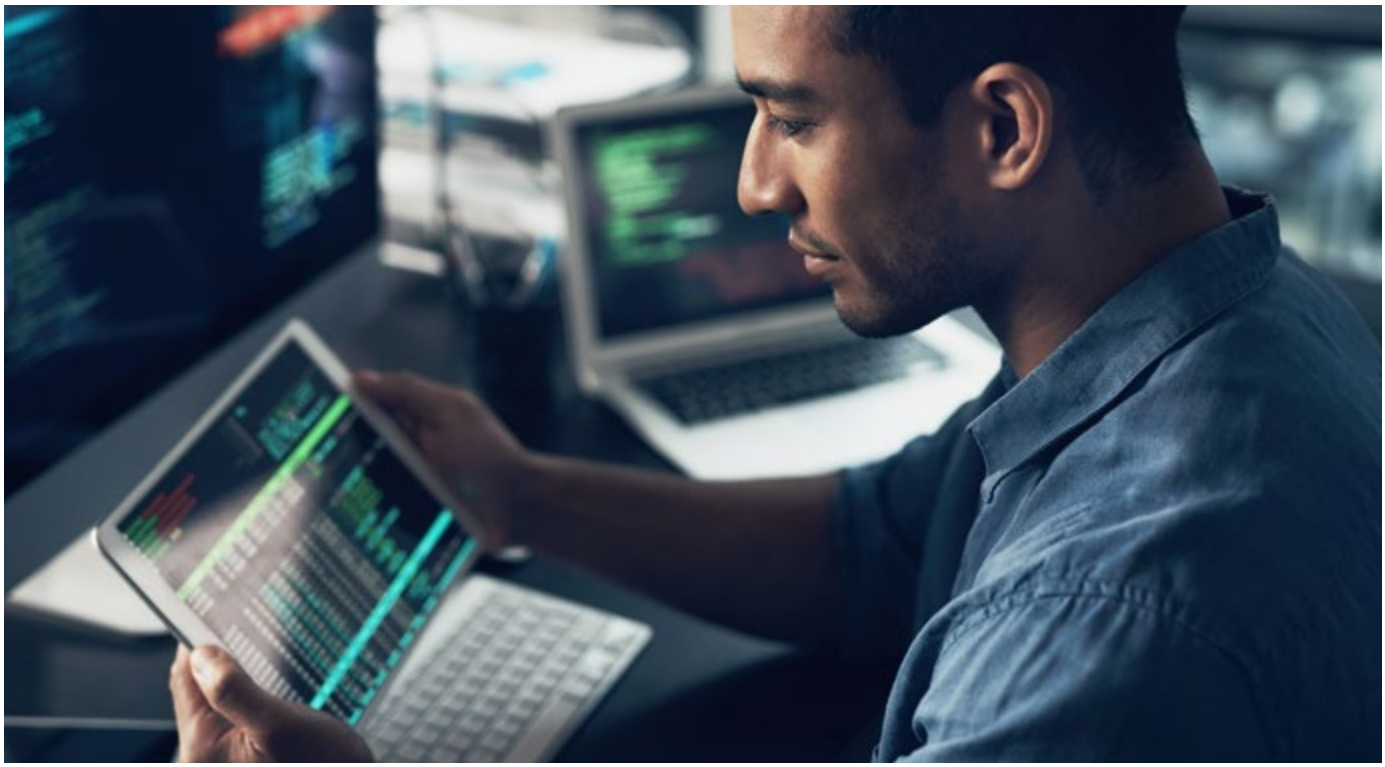
Raconteur

Digital Compliance

digicert®

Inhalt



Ihre Checkliste für einen innovativen Compliance-Ansatz: In fünf Schritten zu nachhaltiger Sicherheit

Cyber-Security-Vorschriften nehmen Einfluss auf die geschäftlichen Risiken. Wie können Unternehmen aus den zunehmenden Sicherheitsanforderungen einen Marktvorteil erzielen? Eine Roadmap für gewinnbringende Compliance in fünf Schritten

Jüngste Vorgaben im Bereich der Cyber Security verändern die globale Geschäftswelt und aktualisierte Compliance-Vorschriften lassen neue Anforderungen entstehen. Unternehmen müssen daher reaktiven Abwehrstrategien den Rücken zukehren und strategische Vorteile für sich schaffen.

Führungsriegen stehen nun vor einem komplexen Unterfangen: Im Zuge der immer vielschichtiger werdenden Cyberangriffe hat sich die Einhaltung gesetzlicher Compliance-Anforderungen von einer Herausforderung für die Betriebsteams zu einem geschäftskritischen Wettbewerbsfaktor entwickelt. Dass man handeln muss, ist klar, doch stellt sich die Frage, wie schnell sich Unternehmen anpassen können.

Unternehmen, die ihre digitale Sicherheit proaktiv gestalten, vermeiden Sicherheitsverstöße und Systemausfälle. Aber vor allem bauen sie einen resilienten Betrieb auf, der schnell auf neue Vorschriften wie DORA reagieren kann. Angesichts der wachsenden Anzahl von Cyber-bedrohungen ist eine starke Compliance zum Synonym für gute Geschäftspraktiken geworden. Nun stehen immense Veränderungen bei den Compliance-Anforderungen an. Am 17. Januar 2025 ist die Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act: DORA) in Kraft getreten, die den gesamten Finanzdienstleistungssektor in Europa und die damit verbundenen Anbieter für Informations- und Kommunikationstechnologie (IKT) betrifft.

Zudem steht dieses Jahr im Vereinigten Königreich die Einführung der Cyber Security and Resilience Bill (CS&R) an, die der europäischen NIS2-Richtlinie von 2022 entspricht. Beide Initiativen regeln die Aufsicht des Cyber-Security-Risikomanagements durch Führungskräfte.

Patrick Beckman Lapré, leitender Verantwortlicher und Digital-Trust-Experte bei DigiCert, sagt dazu: „Ein wichtiger Schritt bei der Stärkung der Sicherheit ist der Aufbau von Resilienz. Wir haben zwar nicht die Kontrolle über alles, können uns aber bewusst machen, wie sich die Auswirkungen eines Cyberangriffs für Ihre Kunden und Ihr Unternehmen minimieren lassen."

Was Führungskräfte im Bereich Sicherheits- und Risikomanagement weltweit benötigen, ist ein strukturierter Ansatz für den Umgang mit der dynamischen Sicherheitslandschaft von heute. Doch die Umsetzung komplexer und sich zum Teil überschneidender Anforderungen verschiedener Vorgaben und Richtlinien in Form von praxistauglichen Strategien erfordert eine klare Roadmap und eine neue Herangehensweise an das digitale Geschäft.

Mit den folgenden fünf Schritten wandeln Führungskräfte die neuen Anforderungen in strategische Vorteile um und sorgen gleichzeitig dafür, dass ihr Betrieb jederzeit auf Audits vorbereitet ist.

01 Machen Sie sich mit Ihren digitalen Assets vertraut

Effektive Cyber Security setzt voraus, dass Führungskräfte die digitalen Assets des Unternehmens kennen. Die automatische Erkennung und kontinuierliche Überwachung von Assets sowie ein klarer Überblick über die Beziehungen zwischen Assets und Dritten sind wichtige Teile des Gesamtbilds.

„Zu den Assets eines Unternehmens gehören PCs, Server, Anwendungen, digitale Zertifikate, Firewall-Regeln, Mitarbeitende und Dritte. Ohne ein umfassendes Bestandsverzeichnis ihrer Assets können Sie nicht sicher sein, dass ihre Schutzmaßnahmen alle erforderlichen Komponenten abdecken", erläutert Simon Lawrence, Leiter und Mitgründer des Cyber-Security- und Risikoberatungsunternehmens i-confidential.

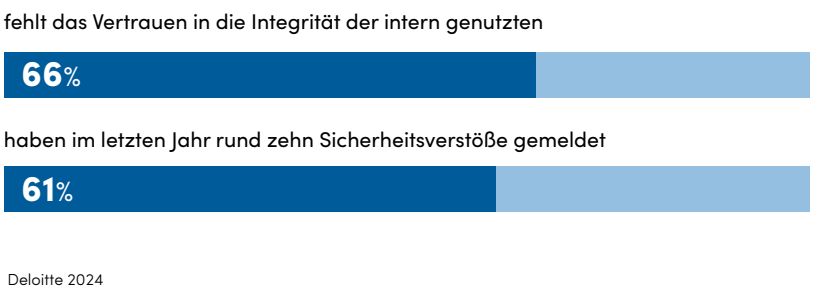
„Wenn in ihrer Konfigurationsmanagement-Datenbank (Configuration Management Database; CMDB) ein Server fehlt, dann weiß Ihr Schwachstellenscanner auch nicht, dass es diesen Server gibt. Das kann dazu führen, dass kritische Sicherheitslücken nicht erkannt werden."

In der Abbildung des IKT-Ökosystems müssen Assets den IT-Systemen zugeordnet sein, von denen sie genutzt werden. Nur so können sie in Bezug auf ihre Kritikalität priorisiert werden, was bedeutet, dass die Auswirkungen auf den Betrieb berücksichtigt werden, falls das Informationssystem kompromittiert wird. Ein solcher Vorfall kann sowohl dem Ruf Ihres Unternehmens schaden als auch einen persönlichen Reputationsverlust mit sich bringen.

„Wenn der Einblick in die Kritikalität fehlt, investieren Unternehmen meist zu wenig in Sicherheitskontrollen für die wichtigsten Systeme und zu viel in weniger gefährdete Systeme. So werden geschäftskritische Systeme erheblichen Cyberrisiken ausgesetzt", bestätigt Lawrence.

Neue Cyberbedrohungen, neue Vorschriften – da benötigen Unternehmen robuste Sicherheitsstrategien

Prozentsatz der Führungskräfte, die sich Sorgen um die Cyber Security machen



Deloitte 2024

Unternehmen benötigen robuste Sicherheitssysteme, die Compliance-Audits standhalten

Prozentsatz der Führungskräfte, die proaktive Cyber-Security-Strategien verfolgen

treffen sich regelmäßig, um sich über Cybersicherheitsmaßnahmen auszutauschen

führen Bereitschaftstests und Lösungssimulationen durch

Deloitte 2024

„Auch die betriebliche Sicherheit wird dadurch beeinträchtigt. Wird ein Unternehmen angegriffen, dann hat das Incident-Response-Team nicht die erforderlichen Informationen, die es benötigt, um die wichtigsten Systeme zu schützen."

02 Legen Sie granulare Zugriffs- und Berechtigungskontrollen fest

Eine zuverlässige Zugriffskontrolle setzt voraus, dass Sie anhand von granularen Berechtigungen definieren, auf welche Ressourcen Nutzer zugreifen und welche Aktivitäten sie ausführen können. Das kann über rollenbasiertes Zugriffsmanagement erfolgen. Dabei werden Berechtigungen den verschiedenen Funktionen und nicht einzelnen Nutzern zugewiesen, was die Verwaltung vereinfacht und Sicherheitsrisiken mindert.

Eine effektive Zugriffskontrolle setzt auf einer zuverlässigen Identitätsprüfung auf, die sich mithilfe digitaler Zertifikate für Nutzer, Geräte und Workloads erreichen lässt. Diese Zertifikate dienen als vertrauenswürdige Authentifizierungsmechanismen, die Identitäten in der gesamten Infrastruktur des Unternehmens prüfen und bestätigen.

> **Ohne ein umfassendes Assetverzeichnis können Sie nicht sicher sein, dass Ihre SchutzmaƏnahmen alle Komponenten ordnungsgemäƏ abdecken.**

Wenn ein Unternehmen zertifikatsbasierte Identitätsprüfungen einsetzt, müssen diese digitalen Identitäten über den gesamten Lebenszyklus hinweg, also von der Ausstellung über die Erneuerung bis hin zum Widerruf, automatisiert verwaltet werden. Dadurch wird sichergestellt, dass Zertifikate nicht unvorhergesehen ablaufen und dass nicht länger benötigte Zertifikate zeitnah widerrufen werden.

Das System speichert ausführliche Prüfpfade für sämtliche Interaktionen und lässt erkennen, wer wann auf welche Ressource zugegriffen hat. Dies ist ein wichtiger Aspekt für die Sicherheitsüberwachung und die Erfüllung von Compliance-Anforderungen.

Die Architektur muss dynamische Updates unterstützen, damit betrieblichen Änderungen Rechnung getragen werden kann und die Sicherheitsintegrität gewahrt bleibt. Dazu gehören automatisierte Abläufe für die Anforderung, Genehmigung und den Widerruf des Zugriffs, die sicherstellen, dass diese Aktivitäten stets schnellstmöglich ausgeführt werden und damit nicht autorisierten Zugriff verhindern.

Eine erfolgreiche Umsetzung stützt sich auf die kontinuierliche Aktualisierung und auf eine klare Definition der Verantwortlichkeiten und Zuständigkeitsbereiche einzelner Rollen. Ohne einen effektiven Prozess, der Aufgaben automatisiert und gleichzeitig den Faktor Mensch berücksichtigt, können Zugriffskontrollen zu einem geschäftlichen Risiko werden, anstatt für Sicherheit zu sorgen.

Das Management der Zugriffskontrolle ist kein einmaliger Vorgang, sondern ein Prozess, der kontinuierlich überwacht und

gesteuert werden muss. Beispielsweise muss dafür gesorgt werden, dass neu eingestellte Mitarbeiter die erforderlichen Berechtigungen erhalten und ausscheidende Personen keine Daten mitnehmen können.

03 Entwickeln Sie klare Frameworks für die Reaktion auf Sicherheitsvorfälle

Sowohl die Führungsebene als auch die SecOps-Teams spielen bei der Reaktion auf Sicherheitsvorfälle eine entscheidende Rolle.

„Die Effizienz und Effektivität der ersten IR-Maßnahmen wirken sich darauf aus, wie groß die betrieblichen Auswirkungen, der Rufschaden und die finanziellen Verluste aufgrund eines Angriffs sind“, so Katherine Kearns, Leiterin des Bereichs Proactive Services EMEA beim Beratungsunternehmen S-RM.

Um diese Risiken so gering wie möglich zu halten, müssen strategische Entscheidungsträger und technische IR-Experten von Anfang an eng zusammenarbeiten.

Sie erklärt, dass regelmäßige Planübungen und andere IR-Simulationen eine gute Gelegenheit zum Testen wichtiger Fertigkeiten und zum Einstudieren von Abläufen ohne reale Risiken bieten. Die dabei gewonnenen Erkenntnisse helfen dem Unternehmen, den Incident-Response-Plan zu verbessern.

„Eine effektive Planübung stellt zentrale Funktionen und Prozesse wie Geschäftskontinuität, Ressourcenmanagement, Systemwiederherstellung, Reaktion auf Bedrohungen, Kommunikation und Einhaltung von Vorschriften auf die Probe.“

04 Implementieren Sie automatisierte Compliance-Kontrollen

Mit der Umstellung von manuellen auf automatisierte Überwachungskontrollmechanismen können Sie sicherstellen, dass Führungskräfte auf Audits vorbereitet sind. Zudem signalisieren Sie Ihren Partnern, dass Ihr Unternehmen Risiken jederzeit effektiv managt.

Noch wichtiger ist es, die Wirksamkeit von Sicherheitskontrollen zu messen, damit eventuelle Lücken oder Schwachstellen in Echtzeit behoben werden können und Ihre Abläufe durchgängig sicher und konform sind.

Viele Unternehmen setzen zwar Sicherheitstechnologien ein, tun aber oft wenig dafür, um ihre Wirksamkeit sicherzustellen. Das kann dazu führen, dass Angreifer Schutzmaßnahmen erfolgreich umgehen.

„Sicherheitskontrollen werden oft mit Kontrolltests gemessen. Dabei werden Assets – meist ein- oder zweimal pro Jahr – stichprobenartig daraufhin geprüft, ob die erforderlichen Kontrollen greifen. Dieser Ansatz vermittelt einen Überblick über die Effektivität der Kontrollen und über die Compliance, hat jedoch seine Grenzen“, führt Lawrence aus.

„Da bei einem Stichprobentest naturgemäß nicht der gesamte Ressourcenbestand geprüft wird, kann es vorkommen, dass Sicherheitslücken unentdeckt bleiben. Bei unregelmässigen oder zu langen Testintervallen können sich Schwachstellen in der Sicherheitsinfrastruktur einschleichen, die das Unternehmen dann beispielsweise ein Jahr lang einem Risiko aussetzen. Außerdem müssen Kontrolltests manuell durchgeführt werden und sind kostspielig. Mittelgroße Unternehmen und Konzerne müssen sogar eigene Testteams dafür abstellen.“

Dieses Risiko lässt sich mit einer CCM-Lösung (Continuous Controls Monitoring) mindern, die die Sicherheitskontrollen automatisch für den gesamten Assetbestand prüft und wöchentliche – oder sogar tägliche – Kontrollprüfungen unterstützt.

05 Stimmen Sie Ihre Cyber-Security-Strategie auf globale Anforderungen ab

Weltweit tätige Unternehmen müssen diverse länderspezifische Cybervorgaben erfüllen, die sich immer wieder ändern. Das erfordert, dass sie sich mit den komplexen aufsichtsrechtlichen Verpflichtungen und Berichterstellungsanforderungen der einzelnen Regionen auskennen.

Skalierbare Frameworks wie ISO 27001 und NIST CSF können das regionsübergreifende Compliance-Management erheblich vereinfachen.

Es ist wichtig, dass die laufende Überwachung auf regulatorische Änderungen und neue Bedrohungen dedizierten Rollen zugewiesen wird.

Da die Teams in den verschiedenen Regionen oft mit ähnlichen Herausforderungen konfrontiert sind, ist eine wirksame Koordinierung erforderlich, damit hinsichtlich der Compliance nichts übersehen wird, aber auch keine Aufgaben doppelt erledigt werden. ●

DORA: Herausforderung und Chance

Manuelle Compliance-Prozesse sind von Haus aus fehleranfällig, weshalb Entscheidungsträger dem Übergang zu automatisierten Sicherheitslösungen eine hohe Priorität einräumen sollten.

Vielerorts wird der Übergang zu automatisierten Sicherheitssystemen hinausgezögert, obwohl die digitalen Risiken steigen und die manuellen Compliance-Prozesse, an denen diese Unternehmen festhalten, ressourcenhungrig und anfällig für kostspielige Fehler sind, die die Compliance und sogar die Geschäftskontinuität gefährden.

Wer versucht, alle Vorgabenänderungen manuell zu verfolgen, läuft Gefahr, etwas zu übersehen und mit Bußgeldern für die Nichteinhaltung bestraft zu werden oder sogar digitales Vertrauen zu verlieren und dem guten Ruf des eigenen Unternehmens dauerhaft zu schaden.

Die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA; (EU) 2022/2554) hat die Compliance mit Cyber-Security-Vorschriften erneut zum Gesprächsthema auf der Chefetage gemacht und vielleicht dazu beigetragen, dass, Deloitte zufolge, 57 % der Entscheidungsträger davon ausgehen, dass ihr Budget für die Cyber Security in den nächsten 12–24 Monaten steigen wird.

Das richtige Kosten-Nutzen-Verhältnis

Patrick Beckman Lapré, leitender Verantwortlicher und Digital-Trust-Experte bei DigiCert, einem weltweit agierenden Anbieter von professionellen Lösungen für PKI und Zertifikatsmanagement, betont, dass die digitale Transformation den manuellen Arbeitsaufwand und die damit verbundenen Kosten radikal senken und Entscheidungsträger dadurch in die Lage versetzen kann, sich auf Strategien zu konzentrieren, die ihre Wettbewerbsposition verbessern.

„Die durch Fehler, Ineffizienz und Strafzahlungen verursachten Kosten können weitaus höher sein als die Einsparungen, die durch das Festhalten an manuellen Ansätzen vermeintlich möglich sind. Mit letzteren können Sie nur auf aktuelle Vorfälle reagieren und diese weder im Detail analysieren noch vorhersehen, welche Konsequenzen sie haben könnten."

Er erläutert, dass kryptografische Agilität – die Fähigkeit, rasch zwischen verschiedenen Methoden zur Verschlüsselung und Sicherung von Daten zu wechseln – für die Wettbewerbsfähigkeit von Unternehmen unerlässlich ist:

„Kryptografie schützt Informationen, indem sie sie in sichere, verschlüsselte Formate konvertiert. Moderne Unternehmen sollten von einem reaktiven zu einem proaktiven Ansatz übergehen, ein vollständiges Inventar ihrer Kryptografietools erstellen und in der Lage sein, anfällige Lösungen rasch zu ersetzen, bevor sie ausgenutzt werden."

„Entscheidungsträger müssen Szenarien modellieren können, bevor sie auftreten. Und wenn es Probleme gibt, muss es Kontrollen und Prozesse geben, mit denen sich die resultierenden Störungen minimieren lassen."

Sicherheit und Compliance sind keine einmaligen Aufgaben, sondern anhaltende Verpflichtungen. Automatisierungsplattformen bieten Monitoring in Echtzeit und weisen auf potenzielle Risiken hin, sodass Unternehmen proaktiv und sehr viel schneller auf sie reagieren können.

Systeme für das Management digitaler Zertifikate reagieren rasch auf neue und aktualisierte Vorgaben wie DORA, sodass nichts übersehen wird und Bußgelder und andere Konsequenzen von Compliance-Verstößen vermieden werden.

Diese Systeme verfolgen und managen digitale Sicherheitszertifikate automatisch, wodurch potenzielle Sicherheitsprobleme erkannt und behoben werden können, bevor sie Störungen verursachen – eine der wichtigsten Anforderungen der neuen DORA-Sicherheitsregeln.

Top-Down-Ansatz für die digitale Transformation

Vorteile von Effizienzsteigerungen bis hin zu einer schnelleren und fundierteren Entscheidungsfindung fügen sich zu einem überzeugenden Business Case für digitale Compliance-Technologie zusammen, doch für ihre erfolgreiche Implementierung ist die Unterstützung der Unternehmensführung erforderlich.

Lapré sagt: „Vielerorts wird die Digitalisierung als rein technischer Prozess betrachtet. Oft setzt die Führungsriege einen CISO ein, ohne sich die Frage zu stellen, was eigentlich mit Cyber Security gemeint ist. Doch die Führungskräfte auf allen Ebenen müssen wissen, was in diesem Bereich geschieht und ihren Beitrag dazu leisten."

„Die Führungsriege entscheidet, in welche Bereiche investiert wird. Wenn jemand Investitionen in die Vermeidung von Gefahren beantragt, aber nicht mit Gewissheit sagen kann, wann diese auftreten werden, neigen Führungskräfte in gehobenen Positionen vielleicht eher dazu, Geld in Projekte zu stecken, von denen sie wissen, dass sie in drei Monaten beginnen werden, sich auszuzahlen. Es braucht also ein Bewusstsein dafür, dass unzureichende Investitionen in die digitale Cyber Security und die diesbezügliche Compliance zum Verlust des digitalen Vertrauens führen und dem Geschäft empfindlich schaden können", fügt er hinzu.

Digitales Vertrauen neu definiert

Robuste digitale Compliance kann auch andere Vorteile mit sich bringen, darunter die frühe Erkennung von Datenlecks, den Schutz wertvollen geistigen Eigentums und die Stärkung des Kundenvertrauens.

Dadurch festigen Sicherheitsinvestitionen die Kundenbindung und zahlen sich somit langfristig aus.

> **Eine Strategie für die digitale Compliance bietet Unternehmen einen besseren Schutz und infolgedessen auch größeres digitales Vertrauen.**

Lapré erklärt: „Die Vorschriften zwingen Organisationen, an ihre Kunden zu denken. Ob Finanzinstitut oder Serviceanbieter – sie müssen Risiken reduzieren und online abgewickelte Geschäftstransaktionen sicherer und vertrauenswürdiger gestalten."

„Wir wissen alle, dass es durch KI und alles, was darum herum passiert, heute sehr viel schwerer ist, herauszufinden, ob etwas echt oder gefälscht ist, und das könnte Unternehmen möglicherweise enormen Schaden zufügen", setzt er hinzu.

Mit der strategischen Auswahl des richtigen Partners für digitale Lösungen können Entscheidungsträger auch ohne zusätzliches Personal für robuste Kontrollen und Prozesse sorgen und die Sicherheit stärken.

Bewältigung neuer Herausforderungen

„Jedes Audit bietet eine Chance für Verbesserungen. Hier bei DigiCert finden jedes Jahr mindestens 26 Audits statt, die unser gesamtes Geschäft und unsere weltweite Präsenz abdecken. Das schafft Vertrauen, denn unsere Kunden wissen, dass wir Prozesse für die Risikominderung haben und nutzen", sagt Lapré.

Sie können zwar nicht alle Risiken ausräumen, aber mit einer belastbaren Cyber-Security-Strategie können sie dafür sorgen, dass sie Ihr Budget optimal ausnutzen und Ihre Reputation schützen.

„Cyberbedrohungen werden immer raffinierter und die Einhaltung einschlägiger Vorschriften immer komplexer und aufwendiger. Eine Strategie für die digitale Compliance bietet Unternehmen einen besseren Schutz und infolgedessen auch größeres digitales Vertrauen."

„Manuelle Prozesse nicht durch eine solche digitale Strategie zu ersetzen, ist ein gewaltiges Risiko, das sich keine Organisation leisten kann", fasst er zusammen.

Warum Ihre Compliance-Strategie nur so stark ist wie Ihr Team

Robuste Cyberstrategien können helfen, Unternehmen zukunftssicher zu gestalten. Erfolgreich sind sie jedoch nur in Kombination mit einem auf die Compliance vorbereiteten Team, das seine Rolle beim Aufbau und Erhalt von Digital Trust versteht.

Trotz erheblicher Investitionen in Tools für die digitale Compliance sind menschliche Fehler nach wie vor eine der Hauptursachen von Sicherheitsverstößen und spielten laut Verizon 2024 bei 68 % der Fälle eine Rolle.

Diese Diskrepanz zwischen technologischen Kapazitäten und menschlicher Leistung macht einen entscheidenden Punkt deutlich: Für eine effektive Cyber Security müssen Sie nicht nur die richtigen Tools implementieren, sondern auch Teams aufbauen, die diese Tools optimal einsetzen können.

Entscheidungsträger sollten daher gleichermaßen in die Compliance-Kenntnisse ihrer Mitarbeitenden und in die Technologie zur Cyberabwehr investieren. Ein solcher ausgewogener Ansatz sorgt dafür, dass die Teams Sicherheitsmaßnahmen sowohl ordnungsgemäß implementieren als auch langfristig pflegen können, sodass eine robuste Infrastruktur zur Abwehr neuer Cyberbedrohungen entsteht.

Wenn Sie komplexen digitalen Herausforderungen jederzeit einen Schritt voraus und gewachsen sein wollen, sollten Sie daran

Nachhaltiger Erfolg setzt voraus, dass Compliance keine Formsache ist, sondern Teil einer flexiblen lernorientierten Unternehmenskultur

Diese Einstellung haben Führungskräfte zur Compliance im Unternehmen

95%

fehlt das Vertrauen in die Integrität der intern genutzten Technologien

90%

haben im letzten Jahr rund zehn Sicherheitsverstöße gemeldet

Deloitte 2024

denken, dass Ihre Cyber-Security-Strategie immer nur so stark ist wie die Personen, die sie implementieren.

Stärkung der kollektiven Verantwortung

Die Verantwortung für die Cyber-Security-Compliance sollte nicht nur von der IT-Abteilung, sondern von dem gesamten Unternehmen gemeinsam getragen werden. Da gesetzliche Vorschriften immer komplexer werden, sollten Unternehmen Compliance-Teams aufbauen, deren Mitglieder ein breites Spektrum unterschiedlicher Kenntnisse und Fähigkeiten mitbringen.

Moderne Cyber-Security-Compliance ist auf die Mitarbeit aller Unternehmensbereiche angewiesen und kann nicht mehr die alleinige Verantwortung der IT-Teams sein. Jedes Teammitglied kann entscheidende Fähigkeiten und Perspektiven beisteuern, die zur effektiven Erhaltung der Compliance beitragen.

Dr. Tommaso De Zan, Senior Manager Data Governance bei dem auf Technologierichtlinien spezialisierten Beratungsunternehmen Access Partnership, formuliert es so: „Die Rollen, die Teammitglieder auf verschiedenen Hierarchiestufen spielen, werden oft übersehen, sind angesichts der immer komplexeren Vorschriften jedoch von entscheidender Bedeutung. Manager sollten ganze Teams darauf vorbereiten, belastbare Sicherheitsprozesse einzuführen – proaktive Teams sind ein großer Vorteil."

Selbst den diszipliniertesten Compliance-Teams fällt es nicht leicht, immer über alle Vorschriftenänderungen auf dem Laufenden zu sein. Die Weiterbildung der Mitarbeiter sollte zu den obersten Prioritäten jedes Unternehmens gehören, denn nur so können sie mit der rasanten Weiterentwicklung der Cyberrisiken Schritt halten.

Diese Risiken führen fortlaufend zu neuen Vorschriften für verschiedene Branchen und Regionen – und letztendlich zu einem komplizierten Geflecht aus Regeln, die Sicherheitsteams verfolgen, interpretieren und einhalten müssen. Dies kann nur gelingen, wenn nicht nur die Compliance-Teams ununterbrochen am Ball bleiben, sondern auch alle anderen Abteilungen engagiert ihren Beitrag zur Aufrechterhaltung der gesetzten Standards und zur Erfüllung neuer Anforderungen leisten.

> **Manager sollten ganze Teams darauf vorbereiten, belastbare Sicherheitsprozesse einzuführen – proaktive Teams sind ein groƏer Vorteil.**

Förderung einer Compliance-first Unternehmenskultur

Compliance darf nicht länger als eine Aufgabe betrachtet werden, die ein für allemal erledigt und abgehakt werden kann, sondern muss zu einem Aspekt der Teamkultur und kontinuierlich weiterentwickelt werden. Dies kann nur gelingen, wenn die Compliance nicht als eine weitere zu erfüllende Anforderung, sondern als gemeinsame Verantwortung und integraler Bestandteil der Arbeitsweise aller

betrachtet wird.

Das kann Unternehmen helfen, das Sicherheitsniveau zu erreichen, das erforderlich ist, um von den Vorteilen der Digitalisierung zu profitieren und die Belegschaft dauerhaft für Sicherheitsbelange zu sensibilisieren.

Casey Ellis, der Geheimdienste in den USA, Australien und im Vereinigten Königreich berät, ist der Meinung, dass gute Compliance als Nebeneffekt solider Geschäftsprozesse erreicht und zur Selbstverständlichkeit werden kann:

„Wenn Sie es richtig machen, ist es effektiv und die Geschäftsbereiche bemerken es gar nicht. Im Endeffekt kann die Security-Compliance von einem externen Zwang zu einer internen Triebkraft werden, wenn Sie die Mitarbeitenden in allen Positionen entsprechend sensibilisieren, Erfolge gebührend feiern und Chancen identifizieren und nutzen, Ihr Sicherheitsniveau als Alleinstellungsmerkmal zu präsentieren. All das trägt dazu bei, eine sicherheitsorientierte Unternehmenskultur zu schaffen, deren Kern die Compliance ist."

Weiterbildungs- und Umschulungsmaϴnahmen

Bemühungen um die Compliance werden durch neue digitale Bedrohungen und veränderte Anschauungen in puncto Datenschutz zusätzlich verkompliziert. Die Teams müssen ermitteln, wie diese neuen Risiken sich auf ihre Compliance-Verpflichtungen auswirken, und sich dazu fortlaufend weiterbilden.

Doch vielen Organisationen fällt es aufgrund von Geld- und Personalmangel schwer, die erforderlichen Compliance-Schulungen zu organisieren.

Dr. De Zan sagt: „Forderungen nach einem adäquaten Budget für qualitativ hochwertige Compliance-Programme können zu Konflikten mit anderen Prioritäten führen, und ein Compliance-Framework, das mehrere Gerichtsbarkeiten abdeckt, stellt eine zusätzliche Komplexitätsebene dar."

„Doch die vielleicht größte Herausforderung ist die unternehmensweite Akzeptanz, denn diese erfordert Verhaltensänderungen und die Förderung einer Compliance-Kultur, die von den Mitarbeitenden auf allen Hierarchieebenen mitgetragen wird", fügt er hinzu.

Unternehmen sollten es nicht bei einmaligen Schulungen belassen, sondern mit kontinuierlichen Bewertungen und Erinnerungen sicherstellen, dass die Mitarbeiter ihre Sicherheitskenntnisse erhalten und anwenden.

Erfolgreiche Compliance erfordert einen ganzheitlichen Ansatz, bei dem die Mitarbeitenden aktiv zum Schutz der digitalen Infrastruktur beitragen. Der effektivste Ansatz ist, die Compliance in die alltäglich genutzten Arbeitsabläufe zu integrieren, wodurch sie allen sehr viel vertrauter wird als durch konventionelle Schulungen.

„Sie sehen das nicht nur in Unternehmen, sondern auch bei externen Auditoren und Regulierungsgremien. In den Niederlanden hat sich die Größe der für die Einhaltung dieser Vorschriften verantwortlichen Teams in den letzten zwei oder drei Jahren verdoppelt oder sogar verdreifacht, und sie wachsen weiter, weil es in Zukunft noch mehr Vorschriften und Standards geben wird", sagt Lapré.

„Sie brauchen Leute, die sie interpretieren, implementieren und verifizieren können, also wird die Nachfrage nach Fachkräften in all diesen Bereichen extrem ansteigen", fügt er hinzu.

Beste Praktiken neu durchdenken

Für Führungskräfte ist es eine ständig präsente Herausforderung, ihre Teams auf die schnelle Einhaltung neuer Vorschriften vorzubereiten, ohne die Effizienz ihrer Arbeitsweisen oder ihre Kreativität zu beeinträchtigen, denn wenn die Teams sich durch Compliance-Anforderungen eingeengt fühlen, kann dies leicht zu Widerstand und Verzögerungen bei der Umsetzung führen.

Ellis sagt: „Letztendlich sollten Organisationen sich bei der Anwendung von Sicherheitsmaßnahmen an ihren eigenen Bedrohungs- und Risikomodellen orientieren, aber da diese von Haus aus dynamisch und oft auch innerhalb der Organisation nicht ausreichend bekannt sind, spielt die Compliance eine wichtige Rolle, wenn es um die Reduzierung menschlicher Fehler, die Anwendung der besten Praktiken und andere Maßnahmen zur Effizienzsteigerung geht."

„Die sorgfältige Anbieterauswahl, die Prioritätensetzung unter Berücksichtigung der eigenen Stärken und die Abstimmung der Sicherheit auf die Anforderungen der umsatz- und produktgenerierenden Geschäftseinheiten sind nicht leicht, können aber, wenn sie gut gemeistert werden, zu Alleinstellungsmerkmalen und Chancen für die Einnahme einer Vorreiterrolle werden", fügt er hinzu. ●

Trends und Veränderungen: die Zukunft der Cyber-Compliance

Von Compliance-Mandaten bis zur Bedrohungsabwehr: Wie können Manager striktere Vorschriften einhalten, effizientes Risikomanagement fördern und eine effektive Governance gewährleisten?

Durch das Priorisieren effektiver MaƏnahmen in Reaktion auf neue Frameworks und Vorschriften lässt sich die Wettbewerbsfähigkeit schützen

Prozentsatz der Führungskräfte, die effektive Compliance als einen Wettbewerbsvorteil ansehen

57% geben an, dass Compliance das Kundenvertrauen stärkt

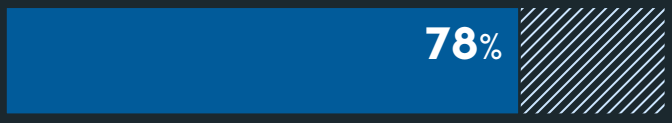
49% geben an, dass Compliance die Markenintegrität und -treue fördert

46% geben an, dass Compliance das Wachstum ankurbelt

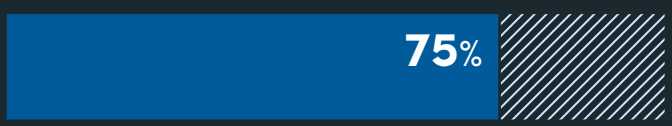
43% geben an, dass Compliance zur Erhaltung der Marktführerschaft beiträgt

Angesichts steigender Compliance-Anforderungen ist Cyber Security zur Chefsache geworden

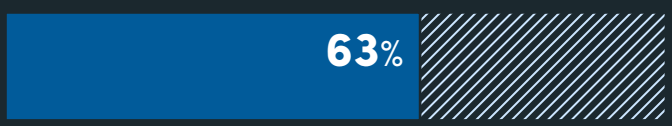
Prozentsatz der Großunternehmen, die der Cyber Security in der Führungsetage Priorität einräumen



78% geben leitenden Führungskräften jedes Quartal ein Update zur Cybersicherheit



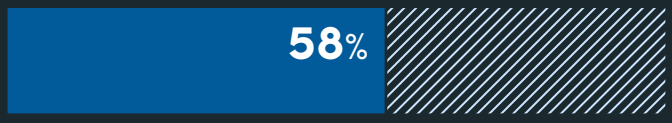
75% stufen die Cybersicherheit als hohe Priorität für die Führungsetage ein



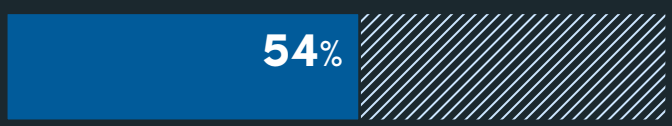
63% weisen Vorstandsmitgliedern und leitenden Managern im Rahmen ihrer Tätigkeit Verantwortung für Cybersicherheit zu

Ein zukunftsfähiger Betrieb setzt ein Gleichgewicht zwischen Sicherheitstools und Compliance-Bewusstsein im Unternehmen voraus

Diese Sicherheitsprioritäten nennen Führungskräfte für die nächsten zwei Jahre



58% Stärkung des Cybersicherheitsbewusstseins bei den Mitarbeitenden



54% Verbesserter Schutz von Daten

45% Konsolidierung und Vereinfachung der Sicherheitstools und -lösungen

digicert®

Als ein marktführender Anbieter hochsicherer **Digital Trust Solutions** sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre **digitale Infrastruktur** und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind. **DigiCert® ONE**, die Plattform für Digital Trust, bietet Unternehmen eine zentrale Anlaufstelle für Einblicke und die Kontrolle über eine Vielzahl von öffentlichen und privaten Anwendungsbereichen, in denen das Vertrauen eine wichtige Rolle spielt. Dazu gehören der sichere Zugriff auf Unternehmenssysteme, sichere Business-Kommunikation sowie der Schutz von Webseiten, Software, Identitäten, Inhalten und Geräten. DigiCert bietet nicht nur preisgekrönte Softwarelösungen an, sondern hat sich nicht zuletzt auch durch seine branchenweite Führungsrolle bei Standards, Support und Betrieb als bevorzugter Anbieter digitaler Vertrauenslösungen bei Unternehmen auf der ganzen Welt einen Namen gemacht.

Weitere Informationen finden Sie unter **www.digicert.com/de** oder folgen Sie **@digicert**

Raconteur

Editor: Larnie Hur
Design: James Lampard, Samuele Motta
Contributors: Alison Coleman