Kiteworks

Whitepaper

NIS-2, DORA & Co. meistern – Setup einer erfolgreichen Compliance-Strategie

Vorwort

IT- und Sicherheitsexperten stehen vor einer doppelten Herausforderung: Es soll nicht nur die nahtlose und plattformübergreifende Zusammenarbeit ermöglicht werden, sondern auch gleichzeitig die Integrität und Vertraulichkeit von Unternehmensdaten gewährleistet sein. Hinzu kommt, dass Cyber-Bedrohungen in ihrer Komplexität zunehmen. Allein im Jahr 2023 verzeichnete das Bundeskriminalamt (BKA) erneut einen signifikanten Anstieg der Cybercrime-Fälle in Deutschland – sowohl in quantitativer als auch in qualitativer Hinsicht. Die durch Cyberkriminalität entstandenen finanziellen Schäden beliefen sich laut bitkom auf insgesamt 205,9 Milliarden Euro.

Reaktion auf Cyberbedrohungen in Europa

Die alarmierenden Zahlen verdeutlichen die dringende Notwendigkeit eines einheitlichen Standards zur Stärkung der IT-Sicherheit und zum verbesserten Schutz vor Cyberangriffen. Als Reaktion darauf hat die Europäische Union im Rahmen ihrer „Digitalen Dekade“ eine Reihe neuer Regulierungen eingeführt, um sicherzustellen, dass Unternehmen und Institutionen stärker gegen die zunehmenden Cyberbedrohungen gerüstet sind. Zu den wichtigsten neuen Regulierungen gehören:

NIS-2 (Network and Information Security Directive): Diese Richtlinie zielt darauf ab, die Cybersicherheit innerhalb der EU zu stärken, indem sie erhöhte Sicherheitsmaßnahmen und Meldepflichten für Betreiber wesentlicher und kritischer Dienste sowie Anbieter digitaler Dienste festlegt. Sie gewährleistet, dass die Mitgliedstaaten angemessene Sicherheitsvorkehrungen treffen und Sicherheitsvorfälle melden.

DORA (Digital Operational Resilience Act): Speziell für den Finanzsektor konzipiert, soll die Verordnung sicherstellen, dass Unternehmen in diesem Bereich über die notwendige digitale Widerstandsfähigkeit verfügen. Dies umfasst die Fähigkeit, Cyberangriffe abzuwehren und die betriebliche Kontinuität auch bei schwerwiegenden IT-Störungen aufrechtzuerhalten.

Cyber Resilience Act: Dieser Akt zielt darauf ab, die Sicherheitsanforderungen für Produkte mit digitalen Elementen zu harmonisieren und zu erhöhen. Das Ziel ist es, sicherzustellen, dass Produkte, die auf dem EU-Markt verkauft werden, von Anfang an sicher konzipiert und betrieben werden.

Diese neuen Regulierungen stellen Unternehmen vor signifikante Herausforderungen, vor allem aufgrund des Fachkräftemangels und begrenzter IT-Ressourcen. Bei Nichteinhaltung drohen hohe Bußgelder und rechtliche Sanktionen, sowie Reputationsschäden und eine erhöhte Anfälligkeit für Cyberangriffe, die zu Datenverlusten und finanziellen Einbußen führen können.

Um also geschäftliche und regulatorische Compliance-Anforderungen effektiv zu erfüllen, ist eine umfassende und integrierte Herangehensweise entscheidend. Compliance betrifft Unternehmen jeder Größenordnung und erfordert Zeit und Akzeptanz der gesamten Belegschaft. Eine gut koordinierte und auf die Bedürfnisse der Anwenderinnen und Anwender ausgerichtete Compliance-Strategie ist hierbei unverzichtbar.

Grundsätze einer erfolgreichen Compliance-Strategie

Die Einführung einer Compliance-Strategie ist kein einmaliges Ereignis, sondern ein kontinuierlicher Prozess, der zentral gesteuert und ständig angepasst werden muss. Es erfordert Zeit und die aktive Beteiligung aller Mitarbeitenden.

Eine erfolgreiche Compliance-Strategie kann durch die gemeinschaftliche Fokussierung auf drei zentrale Grundsätze erreicht werden:
Protect, Track & Control.

Diese Ansätze stellen sicher, dass sensible Daten geschützt, Datenflüsse transparent nachverfolgt und umfassende Kontrollmechanismen implementiert werden, um eine nachhaltige und effektive Compliance-Kultur im Unternehmen zu etablieren.

Eine grundlegende Herausforderung stellt die Umsetzung dieser Best-Practice-Prinzipien in der Praxis dar.

Traditionell kursieren eine Vielzahl von Kommunikationstools und -systemen für den Austausch sensibler Inhalte innerhalb einer Organisation, die oft zu isolierten Insellösungen führen und Schatten-IT entstehen lässt. Dies erschwert die Implementierung konsistenter Sicherheitsmaßnahmen und die Nachverfolgung von Inhalten.

Doch spätestens mit den neuen Richtlinien und den Berichtspflichten, ist es nun notwendig, alle getroffenen Sicherheitsmaßnahmen nachzuweisen und eine effektive IT-Sicherheitsstrategie an die zuständigen Behörden zu melden. Viele Unternehmen sind nun in der Pflicht mit geeigneten Governance-Maßnahmen, die Integrität und Sicherheit der Daten zu gewährleisten und eine geschützte Arbeitsumgebung für alle Mitarbeiterinnen und Mitarbeitern vorzugeben.

Sensible Daten müssen vor unbefugtem Zugriff und Datenklau bzw. Missbrauch geschützt werden. Dies erfordert die Implementierung robuster Sicherheitsmaßnahmen wie Verschlüsselung, Firewalls und Sicherheitsprotokollen.

Es ist notwendig, Prozesse zu etablieren, die die Bewegung sensibler Daten innerhalb der eigenen Systeme sowie bei Drittanbietern verfolgen. Durch die Dokumentation von Datenflüssen, bspw. in Audit-Logs, können potenzielle Sicherheitslücken frühzeitig erkannt und fundierte Entscheidungen über den Umgang möglicher Sicherheitsrisiken getroffen werden.

Mit der Implementierung umfassender Kontrollmechanismen ist es schließlich möglich, die volle Datenkontrolle über sensible Daten sowohl im Bewegungs- als auch im Ruhezustand sicherzustellen.

Fundamente einer robusten Compliance-Strategie

Eine bewährte Herangehensweise zur Verbesserung der Compliance ist die **Zentralisierung und Vereinheitlichung von Kommunikationssystemen**. Durch die Zusammenarbeit mit einem starken IT-Partner und der Implementierung eines Private Content Networks als zentraler Speicherort wird eine geschützte Arbeitsumgebung geschaffen. In dieser können sensible Dateien sicher gespeichert, geteilt und gemeinsam bearbeitet werden, ohne die Datensicherheit zu gefährden. Mit dieser Governance-Maßnahme ist es somit möglich, eine erfolgreiche Compliance-Strategie dauerhaft in der eigenen Organisation zu verankern.

Drei zentrale Bausteine spielen dabei eine entscheidende Rolle, die gemeinsam mit dem IT-Partner bereitgestellt werden können:

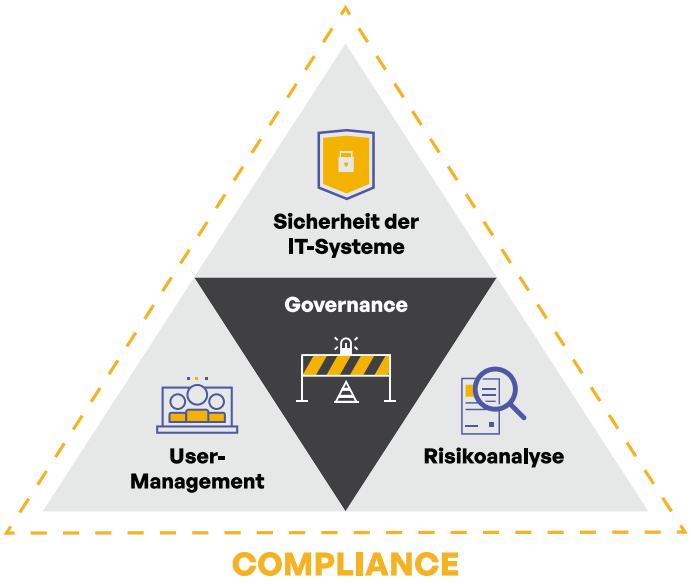

Abb. 1

Sicherheit der IT-Systeme

Der Baustein „Sicherheit der IT-Systeme“ umfasst alle Maßnahmen und Prozesse, die dazu beitragen, IT-Infrastrukturen vor unbefugtem Zugriff, Datenverlust und Cyberangriffen zu schützen. Unter Beachtung des ersten Grundsatzes „PROTECT“ beinhaltet dies die Implementierung Sicherheitsprotokolle, Verschlüsselungsmechanismen und Zugriffskontrollen. Ziel ist es, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten zu gewährleisten.

Ein Private Content Network (PCN) mit seinen fortschrittlichen Sicherheitsfeatures kann dabei erheblich unterstützen und den Sicherheitsprozess beschleunigen. Mit der Bereitstellung von Funktionen wie doppelten Verschlüsselungsmethoden, mehrschichtigen Schutzmechanismen (z.B. mit der proaktiven Löschung von inaktiven Daten) und einer Zero-Trust-Architektur trägt ein PCN dazu bei, die IT-Systeme umfassend zu schützen, Bedrohungen abzuwehren, die Vertraulichkeit der Daten zu gewährleisten und den sicheren Austausch von Informationen (bspw. über Freigabelinks) zu ermöglichen.

Risikoanalyse

Der Baustein „Risikoanalyse“ umfasst die systematische Identifikation, Bewertung und Priorisierung von Risiken, die die IT-Infrastrukturen eines Unternehmens betreffen könnten. Unter Beachtung des zweiten Grundsatzes „TRACK“ beinhaltet die Risikoanalyse die kontinuierliche Überwachung und Bewertung von Bedrohungen und Schwachstellen. Ziel ist es, geeignete Maßnahmen zur Risikominderung zu ergreifen und die Wahrscheinlichkeit der potenziellen Auswirkungen von Sicherheitsvorfällen zu verstehen.

Ein Private Content Network mit seinen fortschrittlichen Features für Risikotracking und -minderung kann dabei unterstützen, Sicherheitslücken schneller zu identifizieren und diese gezielt zu beheben, bevor diese erst auftreten können.

Zu diesen Features gehören individuell anpassbare Reportings, die es ermöglichen, detaillierte Risikoanalysen durchzuführen und spezifische Bedrohungen zu identifizieren. Umfassende Audit-Logs helfen bei der schnellen Identifikation von Sicherheitslücken und ermöglichen eine detaillierte Nachverfolgung von Aktivitäten und Veränderungen innerhalb der IT-Systeme.

Mit der Integration der Sicherheitsdaten aus der gesamten IT-Umgebung in ein SIEM-System können Sicherheitsereignisse und -vorfälle zentral überwacht und konfiguriert werden, um automatisch auf Compli-

Abbildung 1 – Bausteine einer erfolgreichen Compliance-Strategie

ance-Verstöße oder Sicherheitsrisiken hinzuweisen. Dies erleichtert die Erkennung von Bedrohungen und Angriffen, unterstützt die Priorisierung von Sicherheitsrisiken und ermöglicht eine zeitnahe Behebung von Schwachstellen.

User Management

Der Baustein „User-Management“ umfasst alle Maßnahmen und Prozesse, die zur Verwaltung und Kontrolle von Benutzerkonten und Zugriffsrechten innerhalb einer IT-Infrastruktur beitragen. Unter Beachtung des dritten Grundsatzes „CONTROL“ beinhaltet ein umfangreiches User Management die Überwachung und Verwaltung von Zugriffsrechten sowie regelmäßige Sicherheitsschulungen für alle Mitarbeiterinnen und Mitarbeiter.

Ein Private Content Network verhindert unbefugten Datenzugriff mithilfe von sicheren Authentifizierungsmethoden beim Login und stellt sicher, dass nur autorisierte Benutzerinnen und Benutzer Zugang zu sensiblen Daten und Systemen erhalten und (geklaute) Logindaten – bspw. nach einer Phishing-Attacke – nicht missbraucht werden können. Mit der Zuweisung von rollenbasierten Benutzerrechten kann der Zugriff auf sensible Daten weiter eingeschränkt werden und so die Zuweisung von Zugriffsrechten basierend auf den spezifischen Rollen und Verantwortlichkeiten der Benutzenden (Lesen/Schreiben/Löschen) gewährleistet werden.

Auch bietet ein Private Content Network eine geschützte Arbeitsumgebung und einen sicheren Speicherort für sensible Daten, auf die in Echtzeit und von überall zugegriffen werden kann. Dies erhöht die Flexibilität und Effizienz der User erheblich und wird dadurch eher im Arbeitsalltag fest verankert.

Compliance meistern – So gelingt eine dauerhafte Compliance-Kultur

Durch die Kombination der drei grundlegenden Bausteine – Sicherheit der IT-Systeme, Risikoanalyse und User-Management – werden die Fundamente einer robusten Compliance-Strategie geschaffen. Mit Unterstützung eines starken IT-Partners kann die eigene IT-Abteilung entlastet und dem Fachkräftemangel effektiv entgegengewirkt werden. Ein Private Content Network kann langfristig die Sicherheit und Effizienz der IT-Infrastrukturen erheblich verbessern und so die Einhaltung gesetzlicher und regulatorischer Anforderungen unterstützen.
Doch nicht allein das Zusammenspiel dieser Faktoren führt zu einer nachhaltigen und erfolgreichen Compliance-Kultur. Vergessen Sie bei aller Planung von Strategien nicht, einfach miteinander zu reden. Beim Thema Compliance geht es zwar überwiegend darum, passende Maßnahmen zu ergreifen und mit geeigneten Features für mehr Sicherheit zu sorgen. Doch nur durch gegenseitigen Austausch kann sich Compliance als Bestandteil der Unternehmenskultur wirksam etablieren. Zeigen Sie Präsenz in verschiedenen Abteilungen und sprechen Sie über Compliance und alle damit verbundenen Themen (wie bspw. Verhinderung von Schatten-IT oder Reduzierung von Dubletten).
Für eine langfristig und nachhaltig erfolgreiche Compliance-Kultur ist es ratsam, diese in regelmäßigen Abständen zu überprüfen. Analysieren Sie den gesamten Prozess – wie Richtlinien und Verfahren kommuniziert und in Ihr Unternehmen integriert wurden – und bewerten Sie ihn objektiv hinsichtlich seiner Aktualität und Wirksamkeit. Die kontinuierliche Kommunikation und das Engagement aller Beteiligten, insbesondere der Führungskräfte, sind entscheidend, um eine dauerhafte Compliance-Kultur im Unternehmen zu verankern. Führungskräfte sollten als Vorbilder agieren und aktiv zur Einhaltung und Förderung von Compliance beitragen, um die Bedeutung und den Wert dieser Maßnahmen im gesamten Unternehmen zu stärken.

Kiteworks

Über Kiteworks – Private Content Network und starker Pratner für IT-Outsourcing

Kiteworks bietet Ihnen ein Private Content Network, das Sie bei der Erfüllung vieler Compliance-Anforderungen und beim Ausbau Ihrer IT-Sicherheit unterstützt. Unsere Zertifizierungen nach ISO 27001, 27017 und 27018 signalisieren ein hohes Maß an Datensicherheit und bieten eine solide Grundlage für die volle Kontrolle und Integrität Ihrer sensiblen Unternehmensdaten. Kiteworks unterstützt Sie als starker Partner bei der Einhaltung von Compliance-Vorgaben und bietet Ihnen Unterstützung bei der Einführung relevanter Sicherheitsmechanismen (PROTECT), bei der Einhaltung von gesetzlichen Meldepflichten durch die schnelle Verfolgung und Identifizierung von Sicherheitslücken (TRACK) und bei der Datenkontrolle durch die Einführungen von geeigneten Maßnahmen für mehr Cyberhygiene innerhalb Ihrer Organisation (CONTROL).

Überzeugen Sie sich gerne selbst und testen Sie Kiteworks kostenlos oder kontaktieren Sie uns für ein unverbindliches Beratungsgespräch.

Testen Sie jetzt hier unsere kostenlose Demo!

Jetzt testen

Möchten Sie mehr über Compliance für Ihr Unternehmen erfahren?

Mehr erfahren

Kiteworks

Juni 2024

www.kiteworks.com