IBM **Security**

Fünf häufige Probleme beim Datenschutz, die es zu vermeiden gilt

So optimieren Sie Ihre Datensicherheit und halten die Vorschriften noch besser ein

IBM

Inhalte

00 →
Einführung

01 →
Problem 1:
Alleiniger Fokus auf
die Einhaltung von Vorschriften

02 →
Problem 2:
Die Notwendigkeit einer
zentral organisierten
Datensicherheitsstrategie
wird nicht erkannt

03 →
Problem 3:
Es wird nicht festgelegt, wer für
die Daten verantwortlich ist

04 →
Problem 4:
Identifizierte Schwachstellen
werden nicht behoben

05 →
Problem 5:
Moderne
Datenüberwachungsmethoden
werden nicht priorisiert
und nicht eingesetzt

06 →
Was kommt als Nächstes?

07 →
Was für IBM Security spricht.

00

Einführung

Es gibt einen guten Grund dafür, dass das Thema Datensicherheit für Unternehmen oberste Priorität haben sollte

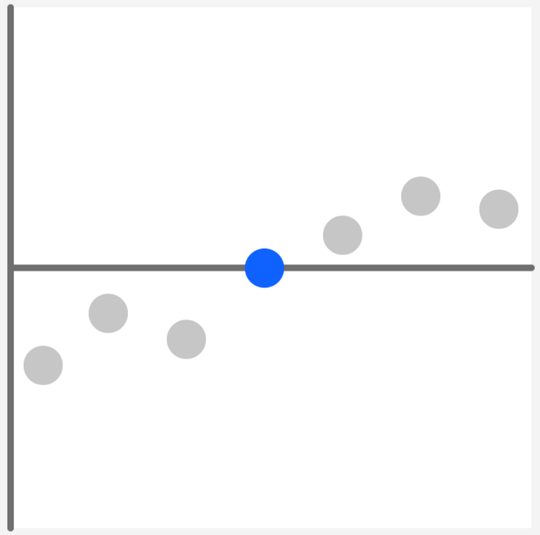
Die IT-Landschaft wird immer dezentraler und komplexer. Deshalb ist es wichtig zu wissen, dass viele Datenschutzverletzungen vermeidbar sind. Die Herausforderungen, vor denen Unternehmen im Bereich der Cybersicherheit stehen, und die Ziele, die sie sich setzen, sind individuell verschieden. Häufig machen Unternehmen jedoch die gleichen, weit verbreiteten Fehler, wenn sie sich mit dem Thema Datensicherheit auseinandersetzen, insbesondere am Anfang Außerdem sehen viele Geschäftsführer diese Fehler als gängige Geschäftspraxis an.

Mehrere interne und externe Faktoren können dazu führen, dass Cyberangriffe erfolgreich sind. Einige Beispiele:

- Erosion der Netzwerkperimeter
- Größere Angriffsflächen durch komplexere IT-Umgebungen
- Die Anforderungen, die Cloud-Dienste an die Cybersicherheitspraktiken stellen, nehmen zu
- Zunehmend ausgefeiltere Formen der Cyberkriminalität
- Weiterhin zu wenige Experten für Cybersicherheit
- Ungenügende Sensibilisierung der Mitarbeiter für Datensicherheitsrisiken

4,45 Mio. US-Dollar

2023 sind die durchschnittlichen Kosten für eine Datenschutzverletzung weltweit gestiegen. Innerhalb von drei Jahren ist ein Anstieg von 15 % verzeichnet worden.[1]



Nächster Abschnitt–

Problem 1: Alleiniger Fokus auf die Einhaltung von Vorschriften

Problem 1: Alleiniger Fokus auf die Einhaltung von Vorschriften

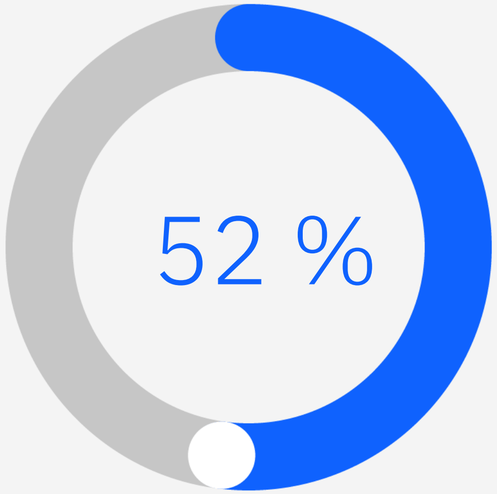
Vorschriften einzuhalten ist nicht notwendigerweise gleichbedeutend mit dem Thema Datensicherheit. Wenn Unternehmen ihre knappen Ressourcen für den Bereich Datensicherheit darauf verwenden, ein Audit oder eine Zertifizierung durchzuführen, besteht die Gefahr, dass sie nachlässig werden. Es gab bereits zahlreiche größere Datenschutzverletzungen in Unternehmen, die die Vorschriften formal gesehen uneingeschränkt befolgt haben. Anhand der folgenden Beispiele wird deutlich, wie sehr die Sicherheit beeinträchtigt werden kann, wenn der Fokus ausschließlich darauf liegt, die Vorschriften einzuhalten.

Unzureichender Schutz
Unternehmen bemühen sich oft, Fehlkonfigurationen von Datenbanken und veraltete Zugriffsrichtlinien vor einem jährlichen Audit zu beheben. Schwachstellen- und Risikobewertungen sollten jedoch fortlaufend vorgenommen werden.

Mindestanforderungen genügen
In vielen Unternehmen werden Datensicherheitslösungen nur deshalb eingeführt, weil Gesetze oder Anforderungen von Geschäftspartnern beachtet werden müssen. Wenn nach der Maxime gehandelt wird: „Wir erfüllen einfach die Mindestanforderungen, das wird schon genügen“, kann dies zur Folge haben, dass Cybersicherheitsrisiken bestehen. Um Daten wirkungsvoll zu schützen, braucht es einen längeren Prozess. Mit einer einmaligen Handlung ist es nicht getan.

Prioritätsverlust
Wenn Vorschriften wie der Sarbanes-Oxley Act (SOX), die General Data Protection Regulation (GDPR), der Payment Card Industry Data Security Standard (PCI DSS) und der California Privacy Rights Act (CPRA), ehemals bekannt als CCPA, in Kraft treten, besteht die Gefahr, dass Unternehmen nachlässiger kontrollieren. Mit der Zeit können Führungskräfte sich weniger Gedanken über die Geheimhaltung, die Sicherheit und den Schutz von Daten machen, die den Vorschriften entsprechen. Doch die Risiken und Kosten, die mit einem Verstoß gegen Vorschriften einhergehen, sind weiterhin gegeben.

Vernachlässigung von Daten, für die keine Vorschriften gelten
Wenn beispielsweise Assets wie geistiges Eigentum verloren gehen, oder an nicht autorisierte Personen weitergegeben werden, bedeutet dies für Ihr Unternehmen ein Risiko. Wenn Unternehmen sich ausschließlich darauf konzentrieren, Vorschriften einzuhalten, übersehen sie gegebenenfalls wertvolle Daten und schützen diese nicht ausreichend.



52 % der Unternehmen sind der Meinung, dass die Komplexität, die durch die Verlagerung von Arbeitslasten in die öffentliche Cloud entsteht, auch die Einhaltung von Vorschriften erschwert.[2]

Betrachten Sie die Einhaltung von Vorschriften als Gelegenheit zur Innovation und zur Verbesserung Ihrer Sicherheitsstandards, um Ihr Unternehmen zu unterstützen.

Lösung: Machen Sie sich bewusst, dass die Compliance lediglich der erste Schritt eines Prozesses ist

Unternehmen, die sich mit dem Thema Datensicherheit befassen, benötigen Strategien, um die geschäftskritischen Daten ihres Unternehmens dauerhaft zu schützen. Es reicht nicht, einfach nur Vorschriften einzuhalten.

Maßnahmen zur Gewährleistung der Datensicherheit und Einhaltung von Vorschriften sollten die folgenden grundlegenden Aspekte berücksichtigen:

- Finden Sie heraus, wo sich Ihre sensiblen Daten befinden, und klassifizieren Sie diese – sowohl lokal als auch in Cloud-Datenspeichern oder Software-as-a-Service (SaaS)-Anwendungen.
- Bewerten Sie Risiken mit kontextbezogenen Erkenntnissen und Analysen.
- Schützen Sie sensible Daten durch Verschlüsselung und flexible Zugriffsrichtlinien.
- Überwachen Sie Datenzugriffs- und Nutzungsmuster, um verdächtige Aktivitäten frühzeitig zu erkennen.
- Reagieren Sie in Echtzeit auf Angriffe.
- Vereinfachen Sie die Einhaltung der Vorschriften und die damit verbundene Berichterstattung.

Als letzter Punkt sind rechtliche Verpflichtungen im Zusammenhang mit der Einhaltung der Vorschriften, mögliche Geschäftsverluste und die damit verbundenen Kosten zu berücksichtigen. Gemeint sind hier nicht Geldstrafen im Zusammenhang mit Verstößen gegen Vorschriften.

Sie sollten das Risiko und den Wert der Daten, die Sie schützen möchten, einer ganzheitlichen Betrachtung unterziehen.

Problem 2: Die Notwendigkeit einer zentral organisierten Datensicherheitsstrategie wird nicht erkannt

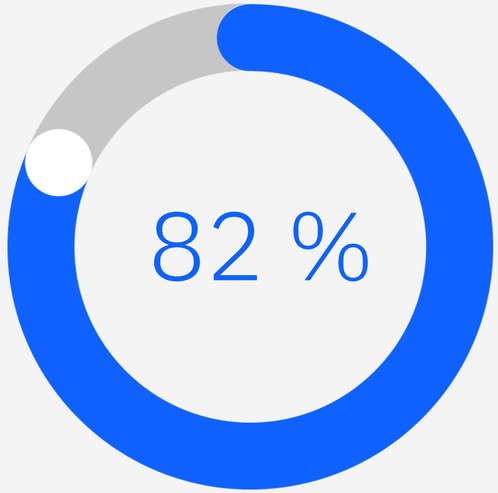
Problem 2: Die Notwendigkeit einer zentral organisierten Datensicherheitsstrategie wird nicht erkannt

Wenn keine umfassenden angelegten Richtlinien zur Einhaltung von Vorschriften für die Themen Datenschutz und Datensicherung vorliegen, besteht die Möglichkeit, dass Geschäftsführer die Notwendigkeit einer einheitlichen, unternehmensweiten Datensicherheitsstrategie aus den Augen verlieren.

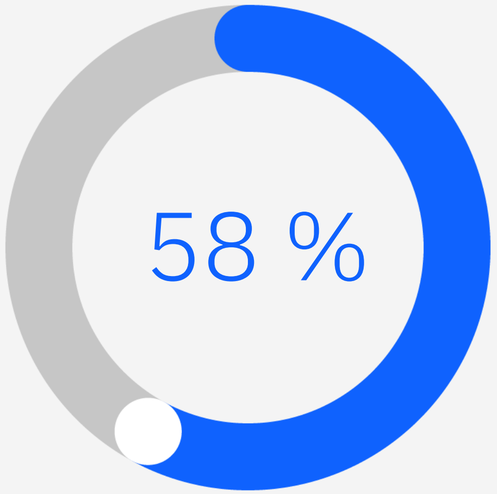
Bei Unternehmen mit hybriden Multicloud-Umgebungen, die einem ständigen Wandel unterliegen und kontinuierlich wachsen, werden gegebenenfalls wöchentlich oder täglich neue Datenquellen erschlossen. Dadurch werden sensible Daten in großem Umfang verbreitet.

Führungskräfte von Unternehmen, die ihre IT-Infrastrukturen ausbauen und erweitern, übersehen oft das Risiko, das mit der veränderten Angriffsfläche verbunden ist. Unter Umständen ist keine hinreichende Transparenz und Kontrolle in Bezug auf die sensiblen Daten gegeben, die in einer zunehmend komplexen und verteilten IT-Umgebung zirkulieren. Werden insbesondere in komplexen Umgebungen keine ganzheitlichen Datenschutz-, Sicherheits- und Schutzkontrollen eingeführt, kann dieses Versäumnis mit sehr hohen Kosten einhergehen.

Wenn Cybersicherheitslösungen zudem isoliert voneinander eingesetzt werden, kann dies zusätzliche Probleme zur Folge haben. Es kann also vorkommen, dass Unternehmen über ein Security Operations Center (SOC) sowie eine Lösung für das Security Information and Event Management (SIEM) verfügen, diese jedoch nicht mit Informationen aus der ebenfalls eingesetzten Datensicherheitslösung versorgen. Auch wenn Sicherheitsteams, -prozesse und -tools nicht reibungslos aufeinander abgestimmt sind, kann es passieren, dass ein Cybersicherheitsprogramm nicht zum gewünschten Erfolg führt.



82 % der Sicherheitsverletzungen betrafen Daten, die in einer Cloud gespeichert waren.[1]



58 % der Unternehmen sind der Ansicht, dass etwa 21 % bis 50 % der in der Cloud gespeicherten sensiblen Daten unzureichend geschützt sind.[2]

Bei Ihrer Cybersicherheitsstrategie sollte die Sicherung sensibler Daten inbegriffen sein.

Lösung: Sie müssen wissen, wo Ihre sensiblen Daten gespeichert sind. Dies bezieht sich sowohl auf lokal gespeicherte Daten als auch auf Daten in einer Cloud und in Saas-Anwendungen

Bei Ihrer Cybersicherheitsstrategie sollte die Sicherung sensibler Daten inbegriffen sein. Wichtig ist nicht nur, dass Sie wissen, wo Ihre sensiblen Daten gespeichert sind. Genauso wichtig ist es, dass Sie wissen, wann und wie auf diese Daten zugegriffen wird. Auch wenn sich diese Informationen schnell ändern. Zudem sollten Sie Ihre Erkenntnisse und Strategien in Bezug auf die Themen Datensicherheit und Datenschutz in Ihr übergeordnetes Cybersicherheitsprogramm integrieren. Es geht darum, eine eng abgestimmte Interaktion zwischen den Technologien zu ermöglichen. Hilfreich ist in diesem Zusammenhang eine Datensicherheitslösung, die mit verteilten Umgebungen und Plattformen kompatibel ist.

Wann ist es an der Zeit, die Datensicherheit mit anderen Kontrollmechanismen für die Cybersicherheit als Teil einer ganzheitlichen Cybersicherheitsstrategie zu integrieren? Nachstehend werden einige Aspekte beschrieben, die darauf hindeuten, dass sich Ihr Unternehmen bereit für diesen Schritt ist.

Risiko des Verlusts wertvoller Daten
Die personenbezogenen, sensiblen und urheberrechtlich geschützten Daten Ihres Unternehmens sind so wertvoll, dass sich ein Verlust dieser Daten nachteilig auf den Fortbestand Ihres Unternehmens auswirken würde.

Problem 2: Die Notwendigkeit einer zentral organisierten Datensicherheitsstrategie wird nicht erkannt

Gesetzliche Auswirkungen
In Ihrem Unternehmen werden Daten erfasst und gespeichert, für die gesetzliche Bestimmungen gelten. Beispiele hierfür sind Kreditkartennummern, andere Zahlungsinformationen oder personenbezogene Daten.

Mangelnder Überblick über die Cybersicherheit
Ihr Unternehmen ist inzwischen derart expandiert, dass es schwierig ist, alle Netzwerkendpunkte zu überwachen und zu schützen. Hierzu zählen auch die Cloud-Instanzen. Wissen Sie zum Beispiel genau, wo, wann und wie Daten sowohl bei Ihnen vor Ort als auch in Ihren Cloud-Datenspeichern und SaaS-Anwendungen abgelegt, freigegeben und abgerufen werden?

Unzulängliche Bewertung
Ihr Unternehmen hat sich nicht für einen ganzheitlichen Ansatz entschieden. Als Folge daraus ist nicht klar erkennbar, wie hoch die Kosten für die einzelnen Cybersicherheitsmaßnahmen sind. Gibt es in Ihrem Unternehmen beispielsweise Prozesse, mit denen Sie den Return on Investment (ROI) in Bezug auf die zur Verringerung des Datensicherheitsrisikos eingesetzten Ressourcen exakt messen können?

Sollte eines dieser Szenarien auf Ihr Unternehmen zutreffen, sollten Sie in Betracht ziehen, sich die erforderlichen Kenntnisse und Lösungen im Bereich der Cybersicherheit anzueignen, um die Datensicherheitsmaßnahmen in Ihre bestehende Sicherheitsstrategie zu integrieren.

Problem 3: Es wird nicht festgelegt, wer für die Daten verantwortlich ist

Problem 3: Es wird nicht festgelegt, wer für die Daten verantwortlich ist

Vielen Unternehmen ist zwar bewusst, dass Datensicherheit wichtig ist, doch sie verfügen nicht über einen Datensicherheitsbeauftragten. Dies wird vor allem ersichtlich, wenn es tatsächlich zu einer Datenschutzverletzung kommt, oder bei einem Audit etwas auffällt und sich niemand im Unternehmen wirklich für das Thema Datensicherheit verantwortlich fühlt.

Wenn sich die Geschäftsleitung in einer solchen Situation an den Chief Information Officer (CIO) wendet, wird dieser vermutlich erklären, dass die entsprechende Abteilung dafür verantwortlich ist, die wichtigsten Systeme am Laufen zu halten. – und sie an jemand anders aus der IT-Abteilung verweisen.

Möglicherweise sind diese IT-Mitarbeiter für mehrere Datenbanken mit sensiblen Daten verantwortlich, verfügen jedoch nicht über ein Budget für den Bereich Cybersicherheit.

Die Mitarbeiter des Chief Information Security Officer (CISO) sind in der Regel nicht direkt für die Daten verantwortlich, die durch das gesamte Unternehmen zirkulieren. Eventuell beraten sie die verschiedenen Line-of-Business (LOB) Manager innerhalb eines Unternehmens. Doch in vielen Unternehmen ist niemand ausdrücklich für die Daten an sich verantwortlich. Daten sind eines der wichtigsten Assets für ein Unternehmen. Wenn sich jedoch niemand für diesen Bereich verantwortlich fühlt, stellt die ordnungsgemäße Sicherung sensibler Daten eine Herausforderung dar.

Wenn es sich um komplexere IT-Umgebungen handelt, ist es unerlässlich, folgende Daten zu berücksichtigen:

Daten, die von verschiedenen

Unternehmensbereichen genutzt werden
Daten, die sich in einer Multi-Cloud-Infrastruktur befinden

Daten, die auf mobilen Endgeräten gespeichert werden

Lösung: Stellen Sie einen Chief Data Officer (CDO) oder Data Protection Officer (DPO) ein, der dafür sorgt, dass mit sensiblen und kritischen Vermögenswerten entsprechend umgegangen wird und sie gesichert werden

Ein Chief Data Officer (CDO) oder Data Protection Officer (DPO) übernimmt derartige Aufgaben. Unternehmen, die ihren Sitz in Europa haben oder Geschäfte mit betroffenen Personen in der Europäischen Union tätigen, sind nach der DSGVO verpflichtet, einen Datenschutzbeauftragten zu benennen. Dadurch wird anerkannt, dass sensible Daten – in diesem Fall personenbezogene Daten – einen Wert haben. Dieser Wert beschränkt sich nicht nur auf den Geschäftsbereich, der diese Daten verwendet. Es unterstreicht auch die Notwendigkeit, innerhalb des Unternehmens eine Stelle zu schaffen, die speziell für die Überwachung von Datenbeständen zuständig ist.

Bei der Auswahl eines CDO oder DPO sollten Sie die folgenden Ziele und Aufgaben im Blick behalten:

Technische Kompetenz und Geschäftssinn
Schätzen Sie das Risiko ab und erstellen Sie einen konkreten Business Case für angemessene Investitionen in die Datensicherheit. Dieser sollte auch für nicht technische Führungskräfte nachvollziehbar sein.

Strategische Umsetzung
Erstellen Sie einen technischen Strategieplan. Dieser sollte Maßnahmen zur Erkennung, Bekämpfung und Datensicherheit beinhalten, um den gewünschten Schutz zu gewährleisten.

Verantwortung für den Compliance-Bereich
Machen Sie sich mit den Anforderungen zur Einhaltung der Vorschriften vertraut. Verstehen Sie, wie Sie diese Anforderungen mit Datensicherheitskontrollen in Einklang bringen können, damit Ihr Unternehmen die Vorschriften einhält.

Problem 3: Es wird nicht festgelegt, wer für die Daten verantwortlich ist

Überwachung und Bewertung
Überwachen Sie die Bedrohungslage und ermitteln Sie, wie effektiv Ihr Datensicherheitsprogramm ist.

Flexibilität und Skalierung
Sie sollten wissen, wann Sie Ihre Datensicherheitsstrategie wie anpassen müssen – beispielsweise durch eine Erweiterung der Richtlinien für den Datenzugriff und die Datennutzung in neuen Umgebungen, wenn fortschrittlichere Tools integriert werden.

Arbeitsteilung
Definieren Sie gemeinsam mit den Anbietern von Cloud-Services die Anforderungen an Service Level Agreements (SLAs) sowie die Zuständigkeiten für Datensicherheitsrisiken und deren Beseitigung.

Maßnahmenplan bei Datenschutzverletzungen
Außerdem sollten Sie sich darauf einstellen, eine zentrale Rolle bei der Ausarbeitung eines strategischen Plans zur Eindämmung von Sicherheitsverletzungen und der entsprechenden Gegenmaßnahmen zu übernehmen.

Der CDO oder DPO sollte die Zusammenarbeit zwischen den Teams und im gesamten Unternehmen im Bereich der Datensicherheit vorantreiben. Alle Beteiligten müssen zusammenarbeiten, um die Unternehmensdaten wirksam zu schützen. Durch diese Zusammenarbeit fällt es dem CDO oder DPO leichter, die Programme und Schutzmaßnahmen zu überwachen, die Ihr Unternehmen zum Schutz seiner sensiblen Daten benötigt.

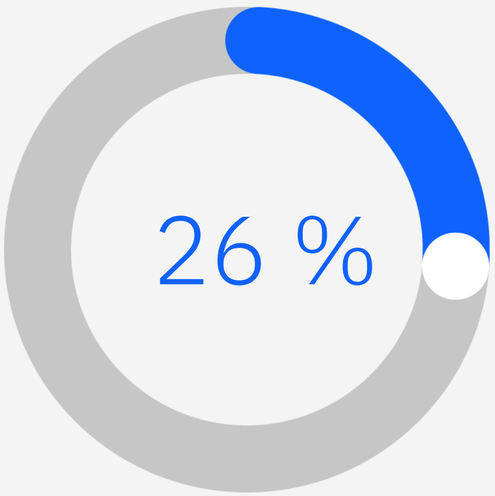
Problem 4: Identifizierte Schwachstellen werden nicht behoben

Problem 4: Identifizierte Schwachstellen werden nicht behoben

Die bekanntesten Sicherheitsverletzungen in Unternehmen sind oft auf bereits bekannte Sicherheitslücken zurückzuführen, die auch nach der Veröffentlichung von Patches nicht behoben wurden. Gelingt es Ihnen nicht, erkannte Sicherheitslücken schnell zu beheben, sind die Daten Ihres Unternehmens in Gefahr. Cyberkriminelle suchen nämlich gezielt nach derartigen Einfallspunkten.

Allerdings ist es für viele Unternehmen eine Herausforderung, Patches schnell zu implementieren. Das liegt an der notwendigen Abstimmung zwischen IT- sowie Sicherheitsabteilungen und operativen Abteilungen. Zudem bedürfen Patches oftmals einer Überprüfung, um sicherzugehen, dass sie keinen Prozess unterbrechen und keine neue Sicherheitslücke verursachen.

Manchmal ist es in Cloud-Umgebungen schwierig zu beurteilen, ob ein Vertragsservice oder eine Anwendungskomponente gepatcht werden sollte. Und selbst wenn eine Sicherheitslücke bei einem Service festgestellt wird, können die Benutzer oft nicht kontrollieren, wie und ob der Service-Anbieter diese behebt.



26 % der neuen Sicherheitslücken basierten auf bereits bekannten Sicherheitslücken.[3]

Gehen Sie proaktiv vor. Führen Sie eine Schwachstellenanalyse Ihrer Datenspeicher durch, um Risiken zu minimieren.

Lösung: Führen Sie ein leistungsfähiges Programm für das Schwachstellenmanagement ein. Dieses sollte auf einer Technologie beruhen, die auch mit einer Erweiterung umgehen kann

Das Schwachstellenmanagement umfasst in der Regel unter anderem Folgendes:

- Erfassen Sie den Bestand Ihrer Daten-Assets sowie deren Ausgangszustand sorgfältig.
- Scannen und überprüfen Sie regelmäßig die Schwachstellen Ihrer gesamten Infrastruktur. Dazu zählen auch Cloud-Assets.
- Setzen Sie Prioritäten bei der Behebung von Schwachstellen. Bringen Sie in dem Zusammenhang in Erfahrung, wie wahrscheinlich es ist, dass eine bestimmte Schwachstelle ausgenutzt wird. Überlegen Sie zudem, welche Auswirkungen dies auf Ihr Unternehmen hätte.
- Nehmen Sie das Schwachstellenmanagement und die Reaktionsfähigkeit in die SLA mit externen Dienstleistern auf.
- Machen Sie sensible oder personenbezogene Daten so unkenntlich wie möglich. Hierfür bietet sich eine Verschlüsselung, Tokenisierung und Schwärzung an.
- Sorgen Sie dafür, dass die Verschlüsselungsschlüssel ordnungsgemäß verwaltet werden. Achten Sie darauf, dass die Verschlüsselungsschlüssel sicher aufbewahrt und ordnungsgemäß ausgetauscht werden, damit Ihre verschlüsselten Daten geschützt werden.

Kein System kann vollständig geschützt werden. Selbst, wenn ein leistungsfähiges Schwachstellenmanagementprogramm eingesetzt wird. Angesichts der Tatsache, dass selbst in bestens geschützte Umgebungen eingedrungen werden kann, sollten Sie Ihre Daten zusätzlich schützen. Mithilfe der richtigen Datenverschlüsselungstechniken und -funktionen können Sie Ihre Daten vor neuen, aufkommenden Bedrohungen schützen.

Problem 5: Moderne Datenüberwachungsmethoden werden nicht priorisiert und nicht eingesetzt

Problem 5: Moderne Datenüberwachungsmethoden werden nicht priorisiert und nicht eingesetzt

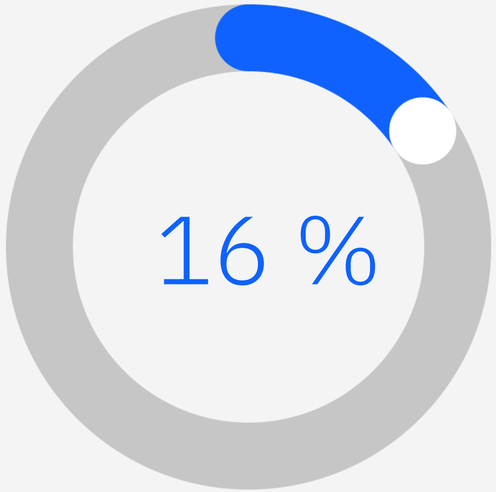
Ein wesentlicher Bestandteil jeder Datensicherheitsstrategie ist die Überwachung des Datenzugriffs und der Datennutzung. Die Unternehmensleitung muss wissen, wer, wie und wann auf Daten zugreift. Folgendes sollte überwacht werden: Ob die entsprechenden Personen über Zugriffsrechte verfügen sollten, ob die entsprechende Zugriffsebene korrekt ist und ob sie ein erhöhtes Risiko für das Unternehmen darstellt.

Benutzer, die über besondere Rechte verfügen, sind oftmals in Insider Threats verwickelt. Ein Datenschutzkonzept sollte eine Echtzeitüberwachung vorsehen. Das Ziel besteht dabei darin zu erkennen, ob Benutzerkonten mit besonderen Rechten für verdächtige oder nicht autorisierte Aktivitäten verwendet werden.

Um etwaige schadhafte Aktivitäten zu verhindern, muss eine Lösung Folgendes leisten:

- Verdächtige Aktivitäten, die gegen Richtlinien verstoßen, blockieren und isolieren.
- Auffällige Sitzungen unterbrechen und beenden.
- Vordefinierte, richtlinienspezifische Workflows in allen Datenumgebungen verwenden.
- Entsprechende Warnmeldungen an IT-Sicherheits- und Betriebssysteme senden.

Es ist nicht immer einfach, die Datensicherheit und die Einhaltung der Vorschriften im Auge zu behalten und zu wissen, wann und wie auf potenzielle Bedrohungen reagiert werden muss. Da autorisierte Benutzer auf mehrere Datenquellen zugreifen, erscheint es oft unmöglich, Daten aus all diesen Schnittstellen zu speichern. Beispiele für die unterschiedlichen Datenquellen sind: Datenbanken, Dateisysteme, Mainframe-Umgebungen, Cloud-Umgebungen und SaaS-Anwendungen. Die effektive Überwachung, Erfassung, Filterung, Verarbeitung und Handhabung der enormen Datenflut stellt eine Herausforderung dar. Wenn Sie keinen angemessenen Strategieplan erstellen, liegen Ihrem Unternehmen möglicherweise mehr Aktivitätsdaten vor, als es bewältigen kann. Dadurch wird der Nutzen der Überwachung von Datenaktivitäten geschmälert.



16 % der festgestellten Vorfälle betrafen den Missbrauch gültiger Konten, bei dem die Angreifer an die Zugangsdaten bestehender Konten gelangten und diese missbrauchten, um sich Zugang zu verschaffen.[3]

Durch den Einsatz einer Lösung zur Überwachung der Datenaktivität können Datensicherheitsanalysten kostbare Zeit sparen.

Lösung: Entwickeln Sie eine umfassende Strategie für die Datensicherheit und die Einhaltung von Vorschriften

Wenn Sie sich also mit dem Thema Datensicherheit befassen, müssen Sie Ihre Überwachungsmaßnahmen so konzipieren und auslegen, dass sie den jeweiligen Anforderungen und Risiken gerecht werden. Dazu wird häufig ein mehrstufiger Ansatz gewählt. Dadurch können Sie Best Practices in Ihrem Unternehmen entwickeln und skalieren. Darüber hinaus ist es entscheidend, dass Sie frühzeitig Gespräche mit den wichtigsten Stakeholdern aus Wirtschaft und IT führen, um die kurz- und langfristigen Geschäftsziele zu erfahren.

Bei diesen Gesprächen sollte auch die Technologie erörtert werden, die zur Unterstützung der wichtigsten Maßnahmen erforderlich sein wird. Angenommen, Ihr Unternehmen plant, Niederlassungen in einer neuen Region einzurichten und dabei eine Mischung aus lokalen, in der Cloud gehosteten Datenspeichern und SaaS-Anwendungen zu verwenden. Dann sollte in Ihrer Datensicherheitsstrategie geprüft werden, wie sich dieser Plan auf die Datensicherheit und die Einhaltung der Vorschriften im Unternehmen auswirken wird. In einem solchen Fall unterliegen die unternehmenseigenen Daten neuen Anforderungen an die Datensicherheit und die Einhaltung der Vorschriften. Beispiele hierfür sind die DSGVO, der CPRA und das brasilianischen Lei Geral de Proteção de Dados (LGPD).

Setzen Sie Prioritäten und konzentrieren Sie sich auf ein oder zwei Quellen, die mit hoher Wahrscheinlichkeit die sensibelsten Daten enthalten. Achten Sie darauf, dass Ihre Datensicherheitsrichtlinien in Bezug auf diese Quellen unmissverständlich und ausführlich formuliert sind, bevor Sie diese Praktiken auf den Rest Ihrer Infrastruktur ausweiten.

Problem 5: Moderne Datenüberwachungsmethoden werden nicht priorisiert und nicht eingesetzt

Sie sollten sich nach einer automatisierten Lösung zur Überwachung von Daten- oder Dateiaktivitäten umsehen. Diese sollte über umfangreiche Analysemöglichkeiten verfügen und sich auf die wichtigsten Risiken und ungewöhnliche Verhaltensweisen von privilegierten Benutzern konzentrieren können. Wenn eine Lösung zur Überwachung von Daten- oder Dateiaktivitäten ein ungewöhnliches Verhalten feststellt, sollten Sie unbedingt automatische Warnmeldungen erhalten. Sie müssen jedoch auch in der Lage sein, schnell zu handeln, wenn Unregelmäßigkeiten oder Abweichungen im Hinblick auf Ihre Datenzugriffsrichtlinien entdeckt werden. Die Schutzmaßnahmen sollten eine dynamische Datenmaskierung oder -sperrung beinhalten.

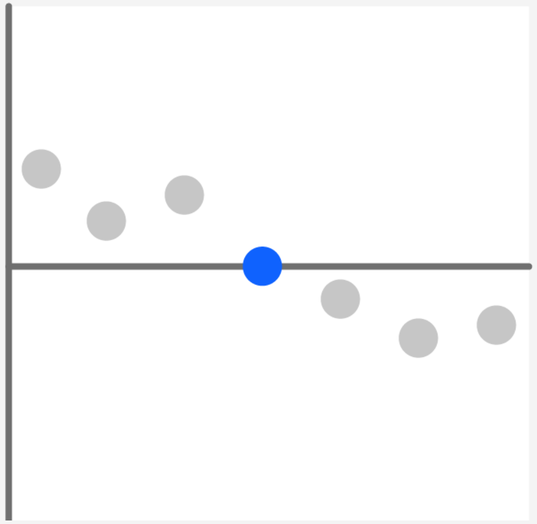
Wenn Sie Pläne zur Überwachung und zum Schutz Ihrer Datenaktivitäten entwickeln, ist es oft hilfreich, über die folgenden Fragen nachzudenken:

- Welches sind meine beiden sensibelsten Datenquellen?
- Welche fünf bis zehn Datenquellen sollte ich aufgrund ihrer Menge an sensiblen Daten als nächstes priorisieren?
- Sind bestimmte Endpunkte oder Cloud-Assets mit Daten mit höherem Risiko verknüpft?
- Werden sensible Daten nach Belieben in und aus lokalen, hybriden und Cloud-Umgebungen verschoben?
- Welchen Benutzern sollte der Zugriff auf die Datenquelle gewährt werden und unter welchen Bedingungen?
- Welche Benutzer, für die ein hohes Risiko besteht oder welche Konten mit besonderen Rechten müssen deaktiviert werden oder bedürfen einer genaueren Überprüfung?
- Unterstützt meine Datensicherheitslösung Funktionen für die Überwachung von Aktivitäten in Echtzeit und den automatisierten Schutz von Daten?
- Gibt es eine Echtzeit-Überwachung von Daten in Dateien, die in Datenspeichern liegen? Zum Beispiel in SQL-Datenbanken (Structured Query Language), Hadoop-Distributionen, NoSQL-Plattformen (Not only SQL) usw.?
- Unterstützt meine Überwachungslösung Datenspeicher in hybriden Multicloud-Umgebungen? Kann ich maßgeschneiderte Berichte erstellen, die zum richtigen Zeitpunkt an die richtigen Personen weitergeleitet werden?
- Verfüge ich über die notwendigen Risikoanalysen und gefilterten Überwachungsfunktionen, um Risiken, Schwachstellen und Sanierungsmaßnahmen effektiv zu priorisieren?

Je genauer Sie die Überwachungsprioritäten und Schutzanforderungen bestimmen können, desto effektiver können Sie die verfügbaren Erkennungs- und Reaktionsressourcen einsetzen.

1,76 Mio. US-Dollar

Die durchschnittlichen Einsparungen für Unternehmen, die KI und Automatisierung im Bereich Sicherheit umfassend nutzen, liegen bei 1,76 Millionen US-Dollar im Vergleich zu Unternehmen, die dies nicht tun.[1]



06

Was kommt als Nächstes?

Wie lassen sich diese gängigen Datensicherheitsfallen vermeiden? Vor allem, da immer mehr Unternehmen hybride Multicloud-Umgebungen einsetzen? Zunächst müssen Sie das Problem erkennen und Ihr Unternehmen in die Lage versetzen, einen proaktiven, ganzheitlichen Ansatz zur Sicherung von Daten zu verfolgen, unabhängig davon, wo sie sich befinden.

In einem Unternehmen mit einer komplexen und hybriden IT-Umgebung ist ein isolierter Ansatz für die Datensicherheit nicht sinnvoll. Sie müssen Strategien für die Datensicherheit und die Einhaltung der Vorschriften einführen. Diese sollten sich auf Ihre gesamte Dateninfrastruktur erstrecken und alle Datentypen unterstützen.

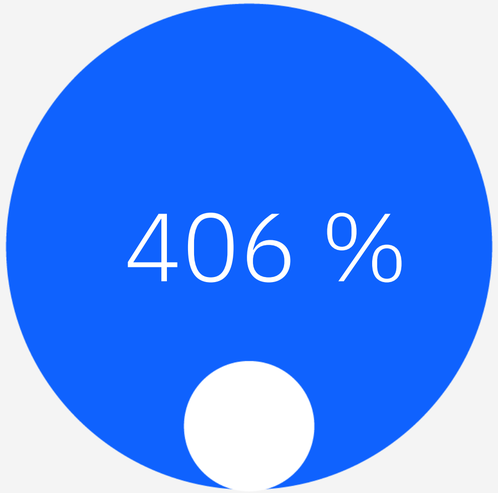
Abgesehen davon sollten Sie die folgenden nächsten Schritte vorsehen, um die wertvollen Daten Ihres Unternehmens zu schützen:

- Erstellung eines Plans für die Datensicherheit und die Einhaltung von Vorschriften. Dieser sollte die kurz- und langfristigen Geschäfts- und Technologieziele Ihres Unternehmens berücksichtigen
- Umsetzung dieses Plans mithilfe der geeigneten Mitarbeiter, Prozesse und Tools
- Planung Ihrer Ressourcen, um sicherzustellen, dass Ihr Programm für Datensicherheit und Einhaltung der Vorschriften effektiv skaliert werden kann, wenn Ihr Unternehmen moderne Technologien einsetzt

Die IBM® Security Guardium Plattform ist eine Lösung für Datensicherheit und Einhaltung der Vorschriften. Die Lösung wurde entwickelt, um Unternehmen dabei zu helfen, ihre kritischen und sensiblen Daten besser und flexibler zu schützen, unabhängig davon, wo sie sich befinden. Erfahren Sie, warum diese Lösung auch für Ihr Unternehmen geeignet sein kann.

Mehr erfahren →

Kontaktieren Sie uns →



Aus einer Studie von Guardium ging ein ROI von 406 % mit Vorteilen von 5,86 Millionen US-Dollar im Laufe von drei Jahren hervor.[4]

07

Warum IBM Security?

IBM Security unterstützt die größten Unternehmen und Regierungen der Welt mit einem integrierten Portfolio von Sicherheitsprodukten und -services, die mit dynamischer KI und Automatisierungsfunktionen ausgestattet sind. Das Portfolio, das von der weltweit anerkannten IBM® X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Bedrohungen vorherzusehen, Daten zu schützen, während sie bewegt werden, und schnell und präzise zu reagieren, ohne geschäftliche Innovationen zu behindern. Tausende von Unternehmen vertrauen IBM als ihrem Partner bei der Bewertung, Strategieentwicklung, Implementierung und Verwaltung von Sicherheitstransformationen.

IBM betreibt eines der weltweit größten Unternehmen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht täglich mehr als 150 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erhalten.

Vorheriger Abschnitt

1. Bericht über die Kosten einer Datenschutzverletzung 2023, IBM, Juli 2023.

2. Die Notwendigkeit von Datencompliance im modernen Cloud-Zeitalter, Enterprise Strategy Group von TechTarget, April 2023.

3. X-Force Threat Intelligence Index 2023, IBM Security, Februar 2023.

4. The Total Economic Impact™ (TEI) of IBM Security Guardium Data Protection, eine von IBM in Auftrag gegebene und von Forrester durchgeführte Studie, Juni 2023.

© Copyright IBM Corporation 2023

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de
IBM Corporation
New Orchard Road
Armonk, NY 10504

Hergestellt in den Vereinigten Staaten von Amerika
September 2023

IBM, das IBM Logo, Guardium, IBM Security und X-Force sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Weitere Produkt- und Servicenamen sind möglicherweise Marken von IBM oder anderen Unternehmen. Eine aktuelle Liste der Marken von IBM finden Sie unter ibm.com/de-de/legal/copyright-trademark.

Das vorliegende Dokument ist ab dem Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN. Die Garantie für Produkte von IBM richtet sich nach den Geschäftsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

Erklärung zu bewährten Sicherheitsverfahren: Kein IT-System oder -Produkt sollte als vollkommen sicher angesehen werden, und kein einzelnes Produkt, kein Service und keine Sicherheitsmaßnahme kann eine missbräuchliche Nutzung oder einen missbräuchlichen Zugriff vollständig verhindern. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor böswilligem oder rechtswidrigem Verhalten von Dritten geschützt sind oder Ihr Unternehmen davor schützen.

Die Einhaltung sämtlicher geltender Gesetze und Vorschriften liegt in der Verantwortung des Kunden. IBM bietet keine Rechtsberatung an und gewährleistet nicht, dass die Services oder Produkte von IBM die Konformität von Gesetzen oder Verordnungen durch den Kunden sicherstellen.