Vermeidung der fünf häufigsten Probleme in puncto Datensicherheit

Erfahren Sie, wie Sie Ihre Sicherheitssituation verbessern können

IBM Security

Inhalt

Datensicherheit erfordert höchste Priorität in Unternehmen – aus gutem Grund.

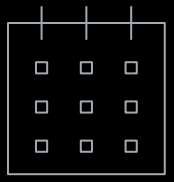
Gerade dann, wenn die IT-Umgebung immer dezentraler und komplexer wird, ist es wichtig zu verstehen, dass viele Sicherheitsverletzungen vermeidbar sind. Die Sicherheitsrisiken und -ziele können zwar von Unternehmen zu Unternehmen sehr unterschiedlich sein, trotzdem machen Unternehmen oft dieselben weit verbreiteten Fehler, wenn sie die Datensicherheit in Angriff nehmen. Zudem akzeptieren viele Führungskräfte in Unternehmen diese Fehler häufig als normale Geschäftspraktik.

Es gibt zahlreiche interne und externe Faktoren, die erfolgreiche Cyberangriffe begünstigen können, einschließlich:

- Verschiebung der Netzwerkgrenzen
- Größere Angriffsflächen durch komplexere IT-Umgebungen
- Steigende Anforderungen an Sicherheitsverfahren durch die Nutzung von Cloud-Services
- Immer ausgereiftere Vorgehensweisen von Cyberkriminellen
- Anhaltender Fachkräftemangel im Bereich der Cybersicherheit
- Fehlendes Bewusstsein von Mitarbeitern für Datensicherheitsrisiken

4,78 Mio. USD

Durchschnittskosten einer Datenschutzverletzung in Deutschland im Jahre 2019[1]



170 Tage

Durchschnittszeit zur Identifizierung und Eindämmung einer Datenschutzverletzung in Deutschland[1]

Wie leistungsstark ist Ihre Datensicherheitspraxis?

Im Folgenden sind fünf der häufigsten – und vermeidbaren – Fehler in Bezug auf die Datensicherheit aufgeführt, die Unternehmen anfällig für potenzielle Angriffe machen. Dazu ist jeweils angegeben, wie diese vermieden werden können.

Compliance beschleunigen

Sicherheit zentralisieren

Eigentümerschaft etablieren

Schwachstellen bewerten

Aktivitäten priorisieren

Problem 1

Nicht über die Compliance hinausgehen

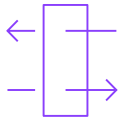
Compliance ist nicht unbedingt gleich Sicherheit. Unternehmen, die ihre begrenzten Sicherheitsressourcen auf die Einhaltung von Audits oder Zertifizierungen konzentrieren, können selbstgefällig werden. Viele große Datenverstöße sind in Unternehmen aufgetreten, die auf dem Papier vollkommen konform waren. Die folgenden Beispiele zeigen, wie sich die ausschließliche Konzentration auf die Compliance eine effektive Sicherheit beeinträchtigen kann:

Unvollständige Abdeckung
Unternehmen bemühen sich häufig vor einer Jahresabschlussprüfung darum, Fehlkonfigurationen von Datenbanken und veraltete Zugriffsrichtlinien zu beseitigen. Schwachstellen- und Risikobewertungen sollten jedoch laufende Aktivitäten sein.

Minimaler Einsatz
Viele Unternehmen führen Datensicherheitslösungen lediglich ein, um die gesetzlichen Anforderungen oder Anforderungen von Geschäftspartnern zu erfüllen. Diese Denkweise, bei der nur ein Mindeststandard implementiert wird um sich anschließend wieder auf das Tagesgeschäft zu konzentrieren, kann kann guten Sicherheitspraktiken entgegenwirken. Effektive Datensicherheit kann nicht im Sprint erreicht werden, dafür ist ein Marathon erforderlich.

Verblassende Dringlichkeit
Unternehmen können in Bezug auf die Verwaltung von Kontrollmechanismen selbstgefällig werden, wenn Verordnungen wie der Sarbanes-Oxley Act (SOX) und die Datenschutz-Grundverordnung (DSGVO) immer ausgereifter werden. Führungskräfte können zwar im Laufe der Zeit weniger rücksichtsvoll mit der Privatsphäre, der Sicherheit und dem Schutz regulierter Daten umgehen, die mit der Nichteinhaltung verbundenen Risiken und Kosten bleiben jedoch bestehen.

1,4



pro Tag

Schätzungen zufolge sind im Jahr 2019 trotz HIPAA-Gesetz (Health Insurance Portability and Accountability Act) im Gesundheitswesen 1,4 Datenschutzverletzungen pro Tag aufgetreten.[2]

Auslassung ungeregelter Daten
Assets wie geistiges Eigentum können Ihr Unternehmen gefährden, wenn sie verloren gehen oder nicht autorisierten Mitarbeitern gegenüber offengelegt werden. Die ausschließliche Konzentration auf die Compliance kann dazu führen, dass Sicherheitsorganisationen wertvolle Daten übersehen und nicht ausreichend schützen.

Lösung

Erkennen und akzeptieren, dass Compliance ein Ausgangspunkt ist, aber kein Ziel

Datensicherheitsorganisationen müssen strategische Programme etablieren, die die geschäftskritischen Daten ihres Unternehmens konsequent schützen, statt einfach nur auf Compliance-Anforderungen zu reagieren.

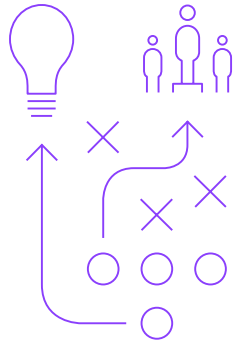
Programme für Datensicherheit und Datenschutz sollten die folgenden grundlegenden Verfahren beinhalten:

- **Erkennung und Klassifizierung sensibler Daten** in Datenspeichern vor Ort und in der Cloud.
- **Bewertung von Risiken** basierend auf kontextbezogenem Wissen und Analysen.
- **Schutz sensibler Daten** durch Verschlüsselung und flexible Zugriffsrichtlinien.
- **Überwachung von Datenzugriffs- und Verwendungsmustern**, um verdächtige Aktivitäten schnell aufzudecken.
- **Reaktion auf Bedrohungen** in Echtzeit.
- **Vereinfachung von Compliance** und Berichterstellung.

Das letzte Element kann Haftungspflichten im Zusammenhang mit der Einhaltung von Vorschriften, mögliche Verluste, die ein Unternehmen erleiden kann, und die potenziellen Kosten dieser Verluste umfassen, die über Geldstrafen wegen Nichtkonformität hinausgehen.

Letztendlich sollten Sie die Risiken und den Wert der Daten, die Sie schützen möchten, ganzheitlich betrachten.

Betrachten Sie die Compliance als Chance zur Innovation und zur Erhöhung Ihrer Sicherheitsstandards, um Ihr Unternehmen zu unterstützen.



Problem 2

Nicht die Notwendigkeit einer zentralisierten Datensicherheit erkennen

Ohne erweiterte Compliance-Vorschriften, die Datenschutz und Datensicherheit abdecken, können Führungskräfte in Unternehmen die Notwendigkeit einer konsistenten, unternehmensweiten Datensicherheit aus den Augen verlieren.

In Unternehmen mit Hybrid-Multicloud-Umgebungen, die sich ständig verändern und immer weiter vergrößern, können wöchentlich oder sogar täglich neue Arten von Datenquellen aufkommen und dazu beitragen, dass sensible Daten immer weiter verstreut werden.

Führungskräfte von Unternehmen, die wachsen und ihre IT-Infrastrukturen erweitern, erkennen möglicherweise nicht das Risiko, das von der sich verändernden Angriffsfläche ausgeht. Ihnen kann es an angemessener Transparenz und Kontroll-mechanismen fehlen, die für die immer komplexere und vielfältigere IT-Umgebung, in der die sensiblen Daten bewegt werden, geeignet sind. Das Versäumnis, umfassende Kontrollmechanismen für Datenschutz und -sicherheit zu etablieren – insbesondere in komplexen Umgebungen – kann sich als sehr kostspielig erweisen.

Durch den Betrieb von Sicherheitslösungen in Silos können zusätzliche Probleme verursacht werden. Beispielsweise können Unternehmen mit einer SOC- (Security Operations Center) und SIEM-Lösung (Security Information and Event Management) das Erfassen von Erkenntnissen aus ihrer Datensicherheitslösung in diesen Systemen vernachlässigen. Gleichermaßen kann ein Mangel an Interoperabilität zwischen Sicherheitspersonal, -prozessen und -tools dazu führen, dass der Erfolg von Sicherheitsprogrammen beeinträchtigt wird.

Verschlüsselung, Business Continuity Management, in den Softwareentwicklungs-prozess integrierte Sicherheit (DevSecOps) und der Austausch von Bedrohungs-informationen können zu geringeren Kosten im Zusammenhang mit Daten-schutzverletzungen beitragen.[1]

Lösung

Wissen, wo sich Ihre sensiblen Daten befinden, einschließlich der Vor-Ort und in der Cloud gehosteten Repositorys

Der Schutz sensibler Daten sollte in Verbindung mit Ihren umfassenderen Sicherheitsbemühungen erfolgen. Sie müssen nicht nur verstehen, wo Ihre sensiblen Daten gespeichert sind, sondern auch wissen, wann und wie auf sie zugegriffen wird – auch wenn diese Informationen ständigen Änderungen unterliegen. Darüber hinaus sollten Sie daran arbeiten, Erkenntnisse und Richtlinien zur Datensicherheit und zum Datenschutz in Ihr gesamtes Sicherheitsprogramm zu integrieren, um eine eng abgestimmte Kommunikation zwischen den Technologien zu ermöglichen. Eine Datensicherheitslösung, die über unterschiedliche Umgebungen und Plattformen hinweg ausgeführt werden kann, ist für einen derartigen Prozess hilfreich.

Wann ist also der richtige Zeitpunkt, im Rahmen eines ganzheitlichen Sicherheitsverfahrens Datensicherheit mit anderen Sicherheits-maßnahmen zu integrieren? Im Folgenden sind einige Anzeichen aufgeführt, die darauf hindeuten, dass Ihr Unternehmen für den nächsten Schritt bereit ist:

Risiko des Verlusts wertvoller Daten
Der Wert der persönlichen, sensiblen und proprietären Daten Ihres Unternehmens ist so signifikant, dass deren Verlust die Überlebensfähigkeit Ihres Unternehmens erheblich beeinträchtigen würde.

Regulatorisch relevante Implikationen
Ihre Organisation erfasst und speichert Daten, für die gesetzliche Bestimmungen gelten, z. B. Kreditkartennummern, andere Zahlungs-informationen und persönliche Daten.

Der Schutz sensibler Daten sollte in Verbindung mit Ihren umfassenderen Sicherheitsbemühungen erfolgen.

Mangelnde Überwachung der Sicherheit
Ihr Unternehmen kann bis zu einem Punkt wachsen, an dem es schwierig ist, alle Netzendpunkte einschließlich Cloudinstanzen zu verfolgen und zu sichern. Haben Sie zum Beispiel eine klare Vorstellung davon, wo, wann und wie Daten gespeichert, gemeinsam genutzt und abgerufen werden, und zwar sowohl vor Ort als auch in Ihren Clouddatenspeichern?

Unzulängliche Bewertung
Ihr Unternehmen hat sich für einen fragmentierten Ansatz entschieden, bei dem es kein klares Verständnis über die genauen Ausgaben für alle Sicherheitsaktivitäten gibt. Verfügen Sie z. B. über Prozesse, mit denen Sie genau den ROI (Return on Investment) in Bezug auf die Ressourcen messen können, die zur Reduzierung von Datensicherheitsrisiken ausgeführt werden?

Wenn eine der aufgeführten Situationen auf Ihr Unternehmen zutrifft, sollten Sie erwägen, sich die Sicherheitskenntnisse und -lösungen anzueignen, die erforderlich sind, um die Datensicherheit in Ihre umfassendere bestehende Sicherheitspraxis zu integrieren.

Problem 3

Nicht definieren, wer für Daten verantwortlich ist

Selbst wenn sie sich der Notwendigkeit der Datensicherheit bewusst sind, gibt es in vielen Unternehmen keinen Verantwortlichen für den Schutz sensibler Daten. Diese Situation wird oft während eines Datensicherheits- oder Audit-Incidents deutlich, wenn das Unternehmen ermitteln muss, wer tatsächlich verantwortlich ist.

Top-Führungskräfte könnten sich an den CIO (Chief Information Officer) wenden, der ihnen entgegen würde, dass seine Aufgabe darin besteht, wichtige Systeme am Laufen zu halten, und dass sie mit einem IT-Mitarbeiter sprechen sollten. Diese IT-Mitarbeiter sind möglicherweise für mehrere Datenbanken verantwortlich, in denen sich sensible Daten befinden, und verfügen trotzdem über kein Sicherheitsbudget.

Normalerweise sind Mitglieder der CISO-Organisation (Chief Information Security Officer) nicht direkt für nicht direkt für die Daten verantwortlich, die durch das Unternehmen fließen.Sie können zwar die verschiedenen Line-of-Business Manager innerhalb eines Unternehmens beraten, aber in vielen Unternehmen ist niemand explizit für die Daten selbst verantwortlich. Für Unternehmen gehören Daten zu den wertvollsten Assets. Doch ohne einen verantwortlichen Eigentümer wird die ordnungsgemäße Sicherung sensibler Daten zu einer Herausforderung.

74%

der befragten Unternehmen geben an, dass der Fachkräftemangel im Bereich der Cybersicherheit ihr Unternehmen beeinträchtigt hat.[3]

„Im Jahre 2018 haben 67,9 % der befragten Unternehmen angegeben, über einen CDO (Chief Data Officer) zu verfügen. Dessen Rolle ist jedoch nach wie vor unklar definiert.“[4]

NewVantage Report
Big Data and AI Executive Survey 2019,
Executive Summary of Findings

Studie lesen →

Lösung

CDO oder DPO einstellen, der für den Schutz und die Sicherheit sensibler und kritischer Datenbestände verantwortlich ist

In komplexen IT-Umgebungen ist es von grundlegender Bedeutung, folgende Daten zu berücksichtigen:

Über Geschäfts-einheiten gemeinsam verwendete

In Hybrid-Multicloud-Infrastrukturen befindliche

Auf mobilen Geräten gespeicherte

Diese Aufgaben können durch einen CDO (Chief Data Officer) oder DPO (Data Protection Officer) übernommen werden. Tatsächlich werden Unternehmen, deren Sitz in Europa ist oder die Geschäfte mit Datensubjekten innerhalb der Europäischen Union tätigen, mit Anforderungen der DSGVO konfrontiert, durch die sie einen DPO einsetzen müssen. Gemäß dieser Verordnung haben sensible Daten – in diesem Fall personenbezogene Informationen – einen Wert, der über die LOB hinausgeht, in der diese Daten verwendet werden. Darüber hinaus wird in dieser Verordnung betont, dass Unternehmen eine Rolle innehaben, die speziell darauf ausgerichtet ist, Verantwortung für die Datenbestände zu übernehmen. Folgende Ziele und Verantwortlichkeiten sind bei der Wahl eines CDO oder DP zu berücksichtigen:

Fachkenntnisse und Geschäftssinn
Er muss Risiken bewerten und praktische Geschäftsfälle entwickeln, die von nicht technischen Führungskräften hinsichtlich angemessener Sicherheitsinvestitionen verstanden werden.

Strategische Umsetzung
Er muss die Umsetzung eines Plans auf technischer Ebene leiten, der Kontrollmechanismen für die Erkennung, Reaktion und Datensicherheit anwendet, um Schutz zu bieten.

Führungsaufgabe in Bezug auf Compliance
Er muss ein Verständnis für die Compliance-Anforderungen entwickeln und wissen, wie diese Anforderungen zu den Kontrollmechanismen für die Datensicherheit zugeordnet werden können, damit Ihr Unternehmen konform ist.

Überwachung und Bewertung
Er muss die Bedrohungslandschaft überwachen und die Wirksamkeit des Datensicherheitsprogramms messen.

Flexibilität und Skalierung
Er muss wissen, wann und wie die Daten-sicherheitsstrategie angepasst werden muss. Ein Beispiel hierfür ist die Erweiterung von Datenzugriffs- und Nutzungsrichtlinien in neuen Umgebungen durch die Integration erweiterter Tools.

Arbeitsteilung
Er muss mit Cloud-Service-Providern die Erwartungen hinsichtlich Service-Level-Vereinbarungen (SLA, Service-Level Agreements) und den Verantwortlichkeiten im Zusammenhang mit Datensicherheitsrisiken und -korrekturen festlegen.

Reaktionsplan auf Datenschutzverletzungen
Schließlich muss er bereit sein, eine Schlüsselrolle bei der Ausarbeitung eines strategischen Plans zur Minderung von Verstößen und zur Reaktion darauf zu übernehmen.

Letztendlich muss der CDO oder DPO bei der Förderung der teamübergreifenden Zusammenarbeit im Bereich der Datensicherheit und im gesamten Unternehmen eine führende Rolle übernehmen, da alle für den effektiven Schutz von Unternehmensdaten zusammenarbeiten müssen. Diese Zusammenarbeit unterstützt den CDO oder DPO bei der Überwachung der Programme und Schutzmaßnahmen des Unternehmens zum Schutz seiner sensiblen Daten.

Problem 4

Nicht bekannte Schwachstellen beseitigen

Bemerkenswerte Verletzungen in Unternehmen sind häufig auf bekannte Schwachstellen zurückzuführen, die auch nach der Veröffentlichung von Patches nicht behoben wurden. Durch das Versäumnis, bekannte Schwachstellen schnell zu patchen, werden die Daten Ihres Unternehmens gefährdet, da Cyberkriminelle aktiv nach diesen einfachen Einstiegspunkten suchen.

Für viele Unternehmen ist es eine Herausforderung, Patches schnell zu implementieren, da ein hohes Maß an Koordination zwischen IT, Sicherheits- und Betriebsteams erforderlich ist. Darüber hinaus müssen Patches getestet werden, um sicherzustellen, dass dadurch kein Prozess unterbrochen und auch keine neue Schwachstelle eingeführt wird.

In Cloudumgebungen ist es manchmal schwierig zu wissen, ob ein vertraglich vereinbarter Service oder eine Anwendungskomponente gepatcht werden sollte. Selbst wenn in einem Service eine Schwachstelle gefunden wird, fehlt den Benutzern oft die Kontrolle über den Korrekturprozess des Service-Providers.

51%

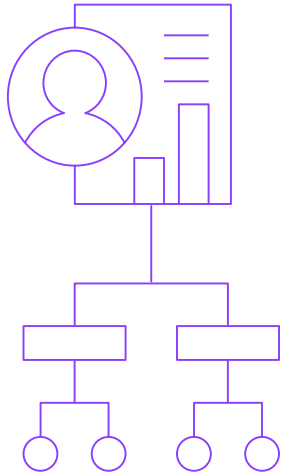
der im Jahre 2019 erfassten Verletzungen wurden durch böswillige Angriffe verursacht. Böswillige Angriffe stellen die häufigste und kostenintensivste Ursache für Verletzungen fest.[1]

Lösung

Etablierung eines effektiven Programms zur Schwachstellenverwaltung mit der geeigneten Technologie zur Unterstützung des Wachstums

Das Schwachstellenmanagement umfasst typischerweise einige der folgenden Aktivitätsebenen:

- Verwaltung eines genauen Inventar- und Ausgangszustands für Ihre Datenbestände.
- Häufige Durchführung von Scans auf Sicherheitslücken und deren Bewertung über die gesamte Infrastruktur, einschließlich Cloudassets
- Priorisierung der Schwachstellenbehebung unter Berücksichtigung der Wahrscheinlichkeit, dass die Schwachstelle ausgenutzt wird, und der Auswirkungen, die dieses Ereignis auf Ihr Unternehmen haben würde.
- Einbeziehung von Schwachstellen-management und Reaktionsfähigkeit als Teil der SLA mit Drittanbietern.
- Nach Möglichkeit Verschleierung sensibler oder personenbezogener Daten. Dies kann durch Verschlüsselung, Zerlegung in Tokens und Schwärzung erreicht werden.
- Ordnungsgemäße Verwaltung der Verschlüsselungsinformationenl und Sicherstellung, dass diese sicher gespeichert und ordnungsgemäß übertragen werden, um die verschlüsselten Daten zu schützen.



Selbst innerhalb eines ausgereiften Programms für das Schwachstellen-management kann kein System perfekt gemacht werden. In der Vermutung, dass ein Eindringen selbst in den am besten geschützten Umgebungen möglich ist, benötigen Ihre Daten ein anderes Schutzniveau. Mit der richtigen Palette an Datenverschlüsselungstechniken und -funktionen können Sie Ihre Daten vor neuen und aufkommenden Bedrohungen schützen.

Problem 5

Nicht die Überwachung von Daten- und Datenaktivitäten priorisieren und nutzen

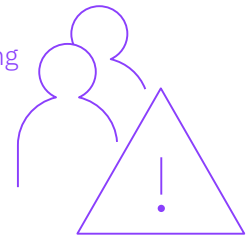
Die Überwachung des Datenzugriffs und der Datennutzung ist ein wesentlicher Bestandteil jeder Datensicherheitsstrategie. Führungskräfte im Unternehmen müssen wissen, wer wie und wann auf Daten zugreift. Diese Überwachung sollte Fragestellungen dahingehend einschließen, ob diese Personen Zugriff haben sollten, ob die Zugriffsebene korrekt ist und ob sie ein erhöhtes Risiko für das Unternehmen darstellt.

Die Identifizierung privilegierter Benutzer ist eine häufige Ursache für Bedrohungen durch Insider.5 Datenschutzpläne sollten Überwachungen in Echtzeit beinhalten, um zu erkennen, ob die Konten privilegierter Benutzer für verdächtige oder unbefugte Aktivitäten verwendet werden. Um mögliche böswillige Aktivitäten zu verhindern, muss eine Lösung die folgenden Aufgaben erfüllen:

- Verdächtige Aktivitäten aufgrund von Richtlinienverstößen blockieren und unter Quarantäne stellen.
- Sitzungen aufgrund von Unregelmäßigkeiten aussetzen und beenden.
- Vordefinierte Workflows gemäß Verordnung über Datenumgebungen verwenden
- Verwertbare Warnmeldungen an IT-Sicherheits- und Betriebssysteme senden.

Die Durchschnittskosten weltweit für eine Bedrohung durch Insider betragen

11,45 Mio. USD.[6]



Es kann sich als schwierig erweisen, die Datensicherheit und Compliance-bezogenen Informationen zu berücksichtigen und zu wissen, wann und wie auf potenzielle Bedrohungen zu reagieren ist. Da autorisierte Benutzer auf mehrere Datenquellen zugreifen, darunter Datenbanken und Dateisysteme sowie Mainframe- und Cloud-Umgebungen, kann die Überwachung und Speicherung von Daten aus all diesen Interaktionen als eine zu große Herausforderung erscheinen. Die Schwierigkeit liegt in der effektiven Überwachung, Erfassung, Filterung, Verarbeitung und Reaktion auf eine riesige Menge von Datenaktivitäten. Ohne einen geeigneten Plan kann Ihr Unternehmen über mehr Aktivitätsinformationen verfügen, als es auf angemessene Weise verarbeiten kann, wodurch wiederum der Wert der Datenaktivitätsüberwachung geschmälert wird.

Lösung

Entwicklung einer umfassenden Strategie zur Erkennung und zum Schutz von Daten

Zu diesem Zweck müssen Sie zu Beginn der Reise zu mehr Datensicherheit das Ausmaß und den Umfang Ihrer Überwachungsbemühungen so festlegen, dass sie den Anforderungen und Risiken gerecht werden. Diese Aktivität beinhaltet oft die Etablierung eines schrittweisen Ansatzes, der die Entwicklung und Skalierung von Best Practices im gesamten Unternehmen ermöglicht. Darüber hinaus ist es von entscheidender Bedeutung, frühzeitig Gespräche mit wichtigen Geschäfts- und IT-Akteuren zu führen, um die kurz- und langfristigen Geschäftsziele zu verstehen.

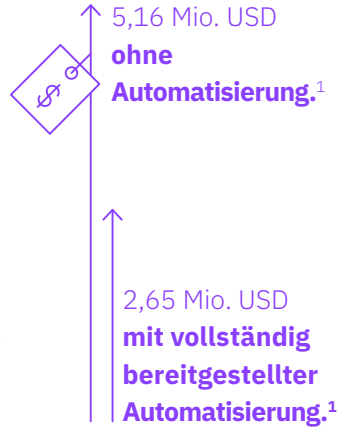
Bei diesen Gesprächen sollte es auch um die Technologie gehen, die zur Unterstützung ihrer Schlüsselinitiativen erforderlich sein wird. Wenn das Unternehmen beispielsweise die Einrichtung von Niederlassungen in einer neuen Region plant und dabei eine Kombination aus lokalen und Cloud-gehosteten Datenspeichern verwendet, sollte Ihre Datensicherheitsstrategie bewerten, wie sich dieser Plan auf die Datensicherheit und die Compliance im Unternehmen auswirkt. Dies gilt auch, wenn die unternehmenseigenen Daten beispielsweise neuen Datensicherheits- und Compliance-Anforderungen wie der DSGVO, dem California Consumer Privacy Act (CCPA) oder Lei Geral de Proteção de Dados (LGPD), dem allgemeinen Datenschutzgesetz Brasiliens, unterliegen.

Sie sollten auch Prioritäten setzen und sich auf eine oder zwei Quellen konzentrieren, die wahrscheinlich die sensibelsten Daten enthalten. Stellen Sie sicher, dass Ihre Datensicherheits-richtlinien für diese Quellen klar und detailliert sind, bevor Sie diese Praktiken auf den Rest Ihrer Infrastruktur ausweiten.

Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung waren im Jahre 2019

95% höher

in Unternehmen ohne Sicherheits-automatisierung.[1]



Sie sollten sich für eine automatisierte Lösung zur Überwachung von Daten und Dateiaktivitäten mit umfangreichen Analysen entscheiden, deren Schwerpunkt auf Schlüsselrisiken und ungewöhnlichen Verhaltensweisen privilegierter Benutzer liegt. Es ist zwar von grundlegender Bedeutung, automatisierte Warnmeldungen zu erhalten, wenn eine Lösung zur Überwachung von Daten- und Dateiaktivitäten Unregelmäßigkeiten entdeckt, trotzdem müssen auch Sie in der Lage sein, schnell zu handeln, wenn Anomalien oder Abweichungen von Ihren Daten-zugriffsrichtlinien entdeckt werden. Die Schutzmaßnahmen sollten eine dynamische Datenmaskierung oder -blockierung umfassen.

Bei der Entwicklung von Plänen zur Überwachung und zum Schutz Ihrer Datenaktivitäten ist es oft hilfreich, die folgenden Fragen zu berücksichtigen:

- Was sind meine beiden wichtigsten Quellen sensibler Daten?
- Welche fünf bis zehn Datenquellen sollte ich aufgrund ihres Volumens an sensiblen Daten als nächstes priorisieren?
- Sind bestimmt Endpunkte oder Cloud-Assets risikoreicheren Daten zugeordnet?
- Können sensible Daten frei zwischen Vor-Ort-, Hybrid- und Cloudumgebungen bewegt werden?
- Welchen Benutzern sollte der Zugriff auf die Datenquelle gewährt werden und unter welchen Bedingungen?
- Welche Benutzer mit hohem Risiko und privilegierten Konten müssen inaktiviert werden oder erfordern eine genauere Prüfung?
- Werden durch meine Datensicherheitslösung die Aktivitätsüberwachung in Echtzeit und automatisierte Datenschutzfunktionen unterstützt?
- Ist Echtzeitüberwachung vorhanden, um Daten in Dateien zu verfolgen, die sich in Datenspeichern wie SQL-Datenbanken (Structured Query Language), Hadoop-Distributionen und NoSQL-Plattformen (Not only SQL) befinden?
- Werden von meiner Überwachungslösung Datenspeicher berücksichtigt, die sich über Hybrid-Multicloud-Umgebungen erstrecken, und ermöglicht sie mir, individuelle Berichte zu erstellen, die zur richtigen Zeit an die richtigen Personen weitergeleitet werden?
- Verfüge ich über die erforderlichen Fähigkeiten zur Risikoanalyse und gefilterten Überwachung, um Risiken, Schwachstellen und Abhilfemaßnahmen wirksam zu priorisieren?

Je spezifischer Sie die Prioritäten und Schutzanforderungen überwachen können, desto effektiver können Sie die verfügbaren Erkennungs- und Reaktionsressourcen einsetzen.

Weitere Schritte

Wie können Sie diese häufig auftretenden Probleme bei der Datensicherheit vermeiden, zumal immer mehr Unternehmen Hybrid-Multicloud-Umgebungen einsetzen? Es beginnt damit, das Problem zu erkennen und Ihr Unternehmen darauf vorzubereiten, einen proaktiven und ganzheitlichen Ansatz zur Datensicherung zu verfolgen, und zwar unabhängig davon, wo sich die Daten befinden.

Wenn Ihr Unternehmen über eine komplexe und hybride IT-Umgebung verfügt, können Sie sich einen isolierten Ansatz zur Datensicherheit nicht leisten. Sie müssen Datenschutzstrategien hinzufügen, die sich über Ihre gesamte Dateninfrastruktur erstrecken und alle Ihre Datentypen unterstützen.

Im Folgenden sind die nächsten Schritte aufgeführt, die Sie unmittelbar unternehmen können, um die geschäftskritischen Daten Ihres Unternehmens zu schützen:

- Aufbau einer Datensicherheitsstrategie, die die kurz- und langfristigen Geschäfts- und Technologieziele Ihres Unternehmens unterstützt
- Umsetzung dieser Strategie mit den richtigen Leuten, Prozessen und Tools
- Planung Ihrer Ressourcen, um sicherzustellen, dass Ihr Datensicherheits- und Compliance-Programm mit der Einführung moderner Technologien in Ihrem Unternehmen effektiv skaliert werden kann

Die IBM Security Guardium-Datenschutzplattform wurde entwickelt, um Unternehmen dabei zu unterstützen, einen intelligenteren und anpassungsfähigeren Ansatz zum Schutz kritischer Daten zu wählen, unabhängig davon, wo sie sich befinden. Finden Sie heraus, warum es für Ihr Unternehmen gut geeignet sein kann.

Weitere Informationen ibm.com/guardium.

>4 Wochen

Die meisten Unternehmen erkennen den Wert von Guardium in weniger als einem Monat.[7]

Warum IBM Security?

IBM Security bietet beim Thema Unternehmenssicherheit eines der innovativsten Produkt- und Serviceportfolios mit dem höchsten Integrationsfaktor. Das Lösungsportfolio, das von der weltweit anerkannten IBM X-Force®-Forschungs- und Entwicklungsgruppe unterstützt wird, stellt Sicherheitsdaten bereit, mit denen Unternehmen mit einem ganzheitlichen Ansatz Mitarbeiter, Infrastrukturen, Daten und Anwendungen schützen können. Hierfür steht eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche zur Verfügung: Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social Media- und andere Geschäftsarchitekturen implementieren.

IBM betreibt eine der weltweit größten Organisationen im Bereich der Forschung, Entwicklung und Bereitstellung von Sicherheitslösungen und verwaltet die Überwachung von

60 Mrd.

Sicherheitsereignissen pro Tag in mehr als 130 Ländern.

IBM besitzt über 3.700 Sicherheitspatente.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Die in diesem Dokument enthaltenen Informationen sind zum Datum der Erstveröffentlichung des Dokuments aktuell und können von IBM jederzeit geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Die genannten Leistungsdaten und Kundenbeispiele dienen nur zur Veranschaulichung. Die tatsächlichen Ergebnisse beim Leistungsverhalten sind abhängig von der jeweiligen Konfiguration und den Betriebsbedingungen. Die Verantwortung für die Auswertung und Prüfung des Betriebs von Produkten oder Programmen anderer Anbieter mit IBM Produkten und Programmen liegt beim Benutzer. Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen.

Erklärung zu geeigneten Sicherheitsvorkehrungen: Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Prävention, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

1 „Cost of a Data Rreach Report 2019“. *IBM Deutschland GmbH IBM-Allee 1 71139 Ehningen* ibm.com/de.databreachcalculator.mybluemix.net/executive-summary

2 „Healthcare Data Breach Statistics“. *HIPAA Journal. www.hipaajournal.com/healthcare-data-breach-statistics*

3 Jon Oltsik. „The Life and Times of Cybersecurity Professionals 2018“. *Enterprise Strategy Group and Information Systems Security Association International*, April 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, „Big Data and AI Executive Survey 2019 Executive Summary of Findings“. *NewVantage Partners,* 2019.newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. „Why Privileged Account Management Is Key to Preventing Insider Threats“. *Security Intelligence,* 20. Juni 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 „Cost of Insider Threats: Global Report 2020“. *Ponemon Institute,* 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 „Ponemon Report: Client Insights on Data Protection with Guardium“. *Ponemon Institute,* August 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-DEDE-00