VARONIS

The Great SaaS Data Exposure

The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure
The Great SaaS Data Exposure

Eine durchschnittliche Organisation ist dem Risiko ausgesetzt, über 28 Millionen USD bei SaaS-Datenlecks zu verlieren.

2022

Table of contents

WICHTIGE BEGRIFFE

Administrator- (Admin-) Konten

User Accounts mit zusätzlichen Berechtigungen, damit die IT Aufgaben wie das Installieren von Software ausführen kann.

Öffentlicher Zugriff

Zeigt Datensätze, Dateien und Ordner an, die über das Internet für alle zugänglich sind.

Sensible Objekte

Zeigt Daten wie Datei-Metadaten an, die in der Cloud gespeichert und zugänglich sind.

Veraltete Benutzerkonten (auch bekannt als „Geisterbenutzer“)

Aktivierte Konten, die inaktiv erscheinen und häufig Benutzern gehören, die nicht mehr bei der Organisation beschäftigt sind.

Sensible Datensätze oder Dateien

Instanzen von personenbezogenen oder anderweitig sensiblen Daten. Eine einzelne Tabellenkalkulationsdatei kann mehrere Datensätze enthalten. Sensible Datensätze und Dateien können Kreditkarteninformationen, Gesundheitsakten oder personenbezogene Daten (PBD) enthalten, die Vorschriften wie PCI, HIPAA, DSGVO und anderen unterliegen.

Organisationsweiter Zugriff

Zeigt Datensätze, Dateien und Ordner an, die für alle Mitarbeitenden zugänglich sind.

Veraltete Daten

Informationen, die für den täglichen Betrieb nicht mehr benötigt werden.

Bevorrechtigte Konten

Bietet erweiterte Berechtigungen für den Zugriff auf Systeme und sensible Daten.

Freigabelinks

Ermöglicht es Benutzern, Daten schnell und einfach mit anderen zu teilen.

ÜBER DEN BERICHT

Unser Forschungsteam hat Folgendes analysiert:

10 Milliarden Objekte

15 Petabyte an Daten

717 Organisationen

Diese Metadaten stammen aus einer Reihe von SaaS- und IaaS-Anwendungen und Services wie Microsoft 365, Box und Okta.

FIRMOGRAFIE

Dieser Bericht beinhaltet Datenanalysen in zahlreichen Branchen:

- Finanzdienstleistungen
- Gesundheitswesen
- Pharma und Biotech
- Fertigung
- Energie und Versorgungsunternehmen
- Einzelhandel
- Technologie
- Schulung
- Staatliche und lokale Behörden

Daten wurden von Unternehmen aus der ganzen Welt gesammelt, darunter die USA, Kanada, das Vereinigte Königreich, Frankreich, Deutschland, Spanien, Brasilien und Australien.

Schlüssel Ergebnisse

Ein durchschnittliches Unternehmen hat eine alarmierende Menge sensibler Daten, die nicht nur allen Mitarbeitenden, sondern in vielen Fällen auch dem gesamten Internet ausgesetzt sind. Das ist eine data-breach Krise, die vorprogrammiert ist.

81 % der Organisationen hatten ausgesetzte sensible SaaS-Daten.

Das durchschnittliche Unternehmen hat:

10 % an Cloud-Daten, die jedem einzelnen Mitarbeitenden ausgesetzt sind

und ein massives internes Risiko darstellen.

4.468 Benutzerkonten ohne MFA

(Multi-Faktor-Authentifizierung) aktiviert, was es Angreifern erleichtert, intern ausgesetzte Daten zu kompromittieren.

Über 40 Millionen eindeutige Berechtigungen

in SaaS-Anwendungen – ein Alptraum für IT- und Sicherheitsteams, die für die Kontrolle und Reduzierung von Cloud-Datenrisiken verantwortlich sind.

Über 12.000 Microsoft 365 Freigabelinks,

die Daten jedem Mitarbeitenden in der gesamten Organisation aussetzen.

157.000 sensible Aufzeichnungen, die allen im Internet zugänglich sind

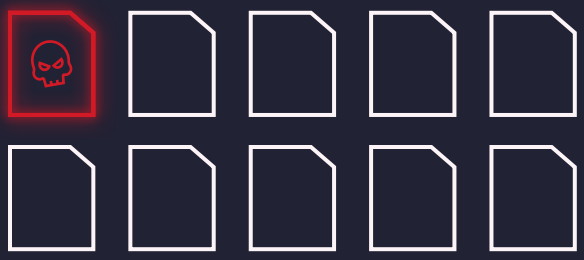
über SaaS-Sharing-Funktionen – was einem Risiko von Datenpannen in Höhe von 28 Millionen US-Dollar entspricht.

33 Super-Admin-Konten

bei über der Hälfte davon ist MFA nicht aktiviert. Durch die Kompromittierung von Super-Admin-Konten können Angreifer mehr Daten stehlen, Hintertüren schaffen und Chaos stiften.

6 % der Cloud-Daten sind dem gesamten Internet ausgesetzt.

Warum diese Krise vorprogrammiert ist:



Jeder 10. Datensatz in der Cloud ist allen Mitarbeitenden ausgesetzt.

Das durchschnittliche Unternehmen hat einen unglaublich großen internen Radius für potenziellen Schaden, der allen Mitarbeitenden einen breiten Zugriff gewährt, um 10 % der Cloud-Daten eines Unternehmens zu stehlen.

Fehlende MFA erleichtert den Angreifern die Arbeit.

Konten, denen grundlegende Sicherheitskontrollen wie MFA fehlen – einschließlich betrügerischer Admin-Konten – erleichtern Angreifern den Zugriff auf SaaS-Apps und das Stehlen intern ausgesetzter Daten.

Das Entwirren des Daten-Exposures in SaaS ist eine gigantische Aufgabe.

SaaS-Anwendungen sind so konzipiert, dass sie automatisch immer Exposure schaffen, aber viele enthalten keine Funktionen, um Exposure zu finden und zu reduzieren. Es gibt exponentiell mehr SaaS-Berechtigungen als zu verwaltende On-premise-Berechtigungen.

IBM Security, **Cost of a Data Breach Report,** Seite 5. In dem Report wurde festgestellt, dass personenbezogene Kundendaten die teuerste Art von Datensatz ist, mit durchschnittlich 180 USD pro verlorenem oder gestohlenem Datensatz. Wir haben herausgefunden, dass ein durchschnittliches Unternehmen 157.000 ausgesetzte Datensätze hat – und das summiert sich auf ein Risiko von 28 Millionen USD in einem durchschnittlichen Unternehmen.

Ein Terabyte in der Cloud

611.478
Dateien

6.116
Sensible Dateien

3.998
extern freigegebene Ordner

4.324
veraltete sensible Dateien

1.924
private Microsoft-Teams-Kanäle (pro Org.)

295
Microsoft Teams (pro Org.)

Im Durchschnitt enthält jedes Terabyte in der Cloud über 6.000 sensible Dateien, fast 4.000 Ordner, die für externe Kontakte freigegeben wurden und über 2,1 Millionen Berechtigungen (Zugriffskontrolleinträge).

Wenn in einem einzigen Terabyte so viel versteckt ist, kann man verstehen, wie Daten außer Kontrolle geraten.

2.152.543
Berechtigungen

Organisationsweites Exposure in Microsoft 365

7 %

der Unternehmen hatten mehr als 10K freigelegte Dateien

10

Unternehmen hatten mehr als 100.000 exponierte Dateien

1

Organisationen hatten mehr als 1,5 Millionen freigelegte Dateien

Der unternehmensweite Zugriff ermöglicht es jedem Mitarbeiter, kritische und vertrauliche Daten im Netzwerk zu erstellen, zu lesen, zu aktualisieren und zu löschen. Wenn alle auf Daten in Organisationen zugreifen können, schafft das eine breite Angriffsfläche, die sehr anfällig für Cyberangriffe wie Ransomware und Insider-Bedrohungen ist.

In der durchschnittlichen Organisation, die Microsoft 365 verwendet:

Eine von zehn sensiblen Dateien ist für jeden Benutzer sichtbar.

Wie kommt es, dass Daten unternehmensweit offengelegt werden?

1.000 (9%) sensible Dateien werden unternehmensweit offengelegt.

97.638 (8%) Ordner sind unternehmensweit verfügbar.

Im Durchschnitt dauert es etwa **sechs Stunden** pro Ordner, um Gruppen mit globalem Zugriff zu finden und manuell zu entfernen, neue Gruppen zu erstellen und anzuwenden und diese Gruppen anschließend mit den richtigen Benutzern zu füllen, die Zugriff auf die Daten benötigen. Bei 1.000 Ordnern sind das 6.000 Stunden manuelle Arbeit!

Fallstudie

Zusammenarbeit, die das Teilen von Daten beinhaltet, ist Teil jeder Organisation – aber sie geschieht selten auf sichere Weise. Ein US-Bezirk stellte fest, dass sensible Informationen über Strafsachen offen und für alle Mitarbeiter in seiner Microsoft 365-Umgebung zugänglich waren. Mit Tausenden von Mitarbeitenden und einer Vielzahl von Berechtigungen machte das IT-Team nicht die notwendigen Fortschritte, um seine Daten zuverlässig zu sperren. Sichtbarkeit, Automatisierung und Warnungen waren der Schlüssel zum Schutz ihrer Daten in der Microsoft-Cloud.

Außer Kontrolle geratene Berechtigungen

Ein durchschnittliches Unternehmen hat über 40 Millionen eindeutige Berechtigungen in SaaS-Anwendungen und schafft damit einen Albtraum für IT- und Sicherheitsteams, die versuchen, die Risiken von Cloud-Daten zu kontrollieren und zu reduzieren.

Wenn es um die Analyse der Zugänglichkeit geht, ist den meisten CISOs nicht klar, wie viele Ordner, Dateien und Datensätze untersucht werden müssen. Ein einziges Terabyte an Daten enthält routinemäßig Zehntausende von Objekten mit spezifischen eindeutigen Berechtigungen, die bestimmen, welche Benutzer und Gruppen Zugriff haben. Organisationen haben jetzt Tausende von Terabyte an Daten. Alle Beziehungen zwischen Benutzern und Gruppen müssen ebenfalls analysiert werden. Erschwerend kommt hinzu, dass jede SaaS-Anwendung Berechtigungsmechanismen unterschiedlich implementiert.

Fallstudie

Bei einem globalen Immobilienunternehmen erhielten ein Dutzend Auftragnehmer Zugriff auf die Salesforce-Instanz des Unternehmens. Monate später, nach Abschluss des Projekts, konnten sich die ehemaligen Auftragnehmer immer noch anmelden und auf alle Aufzeichnungen des Unternehmens zugreifen. Zwei ehemalige Auftragnehmer waren Super-Admins – und einer hatte sich vor Kurzem erst wieder angemeldet. Darüber hinaus konnten 182 Standardbenutzer jeden einzelnen Datensatz exportieren und ein Vertriebsmitarbeiter wurde beim Exportieren von Verkaufschancen und Konten erwischt, nachdem er seine Kündigung eingereicht hatte.

Fallstudie

Bei einer nationalen Bank hatte das Sicherheitsteam keinen Überblick über die Salesforce-Instanz des Unternehmens. Lokale Salesforce-Administratoren hatten zehn „Schatten"-Instanzen geklont und das Sicherheitsteam wusste nichts davon. Innerhalb dieser Instanzen hatten 23 reguläre Benutzer schwierige permission sets, die es ihnen ermöglichten, Passwörter für andere Benutzer zurückzusetzen, neue Benutzer zu erstellen und alle Daten anzuzeigen, zu löschen und zu exportieren. Darüber hinaus war das Sicherheitsteam in Unkenntnis über die laufenden Brute-Force-Versuchen von Angreifern, die versuchten, Zugang zu einer dieser Instanzen zu erhalten.

Die schwächsten Glieder: interne Freigabelinks führen zu übermäßigem Daten-Exposure

>27.000

Freigabelinks zu Informationen in Microsoft 365

12.803

Freigabelinks für alle Mitarbeitenden

Sharing-Links sind hilfreich für die Zusammenarbeit, stellen aber auch ein erhebliches Sicherheitsrisiko dar.

Das einfache Teilen macht den Schutz sensibler Daten zu einer Herausforderung. Wenn Insider oder externe Angreifer Zugriff auf Daten erhalten, den sie nicht haben sollten, sind diese Informationen sofort dem Risiko von Ransomware und Diebstahl ausgesetzt.

Übermäßig freigegebene Links zu sensiblen Daten können diese Daten allen in der Organisation aussetzen. Selbst eine kleine Fehlkonfiguration kann eine große Sicherheitslücke hinterlassen und zu einem Datenleck führen.

Das durchschnittliche Unternehmen hatte Tausende von Freigabeverknüpfungen zu Daten in Microsoft 365, wobei fast die Hälfte davon für alle Mitarbeiter offen war.

Fallstudie

Eine **private Universität** musste das Risiko mindern, das von Bedrohungen wie Ransomware ausgeht. Die hybride On-premise und Cloud-Umgebung der Universität war kompliziert geworden, was das Verwalten der externen Freigabe und das Daten-Exposure erschwerte. Die Visualisierung der vorhandenen Berechtigungsstrukturen für die Microsoft 365-Dateien ermöglichte es dem kleinen IT-Team der Universität, externe Freigaben für Benutzer mit erheblichem Zugriff zu verwalten.

Daten, die allen im Internet ausgesetzt sind

Öffentliche Freigaben machen Daten für alle im Internet zugänglich und das ist so beängstigend, wie es klingt.

Die Verwendung von SaaS- und IaaS-Anwendungen und -Services kann diese Risiken exponentiell erhöhen. Anstatt sensible Daten nur allen Mitarbeitenden auszusetzen, könnten sie nun über das Internet allen und überall ausgesetzt sein.

Viele Organisationen haben Schwierigkeiten, den Zugriff zu sperren. Eine typische Organisation hat über 150.000 Datensätze und Dateien, die öffentlich geteilt werden. Wir haben im Durchschnitt fast 50.000 sensible Datensätze in Microsoft 365 gefunden und über 113.000 sensible Datensätze in SaaS-Anwendungen, die für alle im Internet zugänglich sind. Zu diesen sensiblen Datensätzen gehörten unter anderem HIPAA, CCPA, GLBA und GDPR geschützte Informationen, einschließlich Sozialversicherungsnummern, PCI und sogar Passwörter im Klartext.

In einer durchschnittlichen Organisation gibt es:

157.181
öffentlich freigegebene Dateien

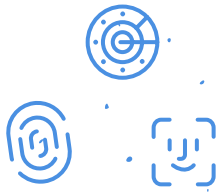
6 %
der Freigabelinks, zugänglich für alle im Internet

18.763
öffentlich freigegebene Ordner

48.896
sensible Datensätze, die öffentlich in Microsoft 365 geteilt werden

113.632
sensible Datensätze, die öffentlich in SaaS-Anwendungen geteilt wurden

Fehlende MFA



Wenn Sie MFA aktivieren, werden sie mit

99 % -iger

Wahrscheinlichkeit nicht gehackt.

4.468

Benutzerkonten ohne aktivierte MFA.

Die Multi-Faktor-Authentifizierung (MFA) ist eine kritische Sicherheitsmaßnahme, die Benutzer selbst dann schützen kann, wenn ihre Passwörter offengelegt werden – aber MFA hilft nur, wenn sie aktiviert und durchgesetzt wird.

Laut CISA-Direktorin Jen Easterly ist die Wahrscheinlichkeit, gehackt zu werden, um 99 % geringer, wenn Sie MFA aktivieren.

Im Durchschnitt hatten Unternehmen 4.468 Benutzerkonten ohne aktivierte MFA — das sind mehr als 4.000 Konten, für die nur die Anmeldeinformationen eines Benutzers erforderlich waren. Organisationen hatten im Durchschnitt 33 administrative Konten, die erweiterte Berechtigungen zum Verwalten und Ändern von Benutzerkonten, Systemen und Einstellungen bereitstellen Davon hatten 18 (55 %) keine aktive MFA.

Ohne MFA haben Angreifer einen einfacheren Weg, eine Organisation zu kompromittieren. Kriminelle Gruppen wie BlackMatter sind dafür bekannt, Benutzernamen und Passwörter aus Datenleck-Deponien im Dark Web zu nutzen. Sie testen jede Zugangsinformation um Systeme mit Internetanschluss über Brute-Force anzugreifen und erhalten Zugriff.

33

Admin-Konten insgesamt

41

Konten mit Berechtigungen insgesamt

55 %

Admin-Konten haben keine MFA

44 %

der Konten mit Berechtigungen haben keine MFA

Sicherheit hört nicht bei der MFA auf. Multi-Faktor-Authentifizierung kann von Angreifern immer wieder geknackt werden. Die Forscher von Varonis Threat Labs entdeckten Techniken, um die **TOTP-basierte MFA von Box und eine andere** für die **SMS-basierte MFA von Box zu umgehen.** Bis Box diese Probleme behoben hatte, konnten Angreifer gestohlene Zugangsdaten aus dem Darknet verwenden, um Box-Konten unbemerkt zu infiltrieren – selbst wenn MFA aktiviert war.

Veraltete Benutzerkonten

Veraltete Benutzerkonten (manchmal auch „Geisterbenutzer“ genannt) sind aktivierte Konten, die inaktiv zu sein scheinen und häufig Benutzern gehören, die nicht mehr bei der Organisation sind.

Veraltete Benutzerkonten bleiben oft aktiviert, aber inaktiv – und können leicht übersehen werden. Diese Konten bieten Zugriff auf Anwendungen und Daten und können es Angreifern ermöglichen, stillschweigend „das Wasser zu testen“ oder einen Brute-Force-Angriff zu versuchen, ohne Geräusche zu erzeugen und Alarme auszulösen, das ein Angriff im Gange ist.

1.197

Inaktive Benutzer

1.322

Anzahl der Gastbenutzer

56 %

Anzahl veralteter Gastbenutzer, die nach 90 Tagen aktiviert bleiben

33 %

Anzahl veralteter Gastbenutzer, die nach 180 Tagen aktiviert bleiben

Fallstudie

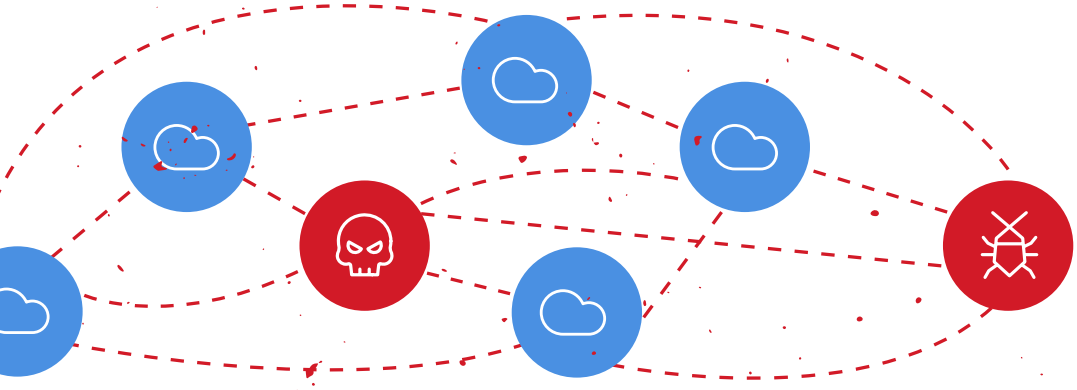
Ein **führender Hersteller** in der Automobilindustrie wurde von mehreren Ransomware-Angriffen getroffen, die schnell hintereinander erfolgten. Das verdeutlichte die Notwendigkeit für moderne Cyber-Security-Lösungen. Nachdem das Unternehmen , Benutzeraktivitäten On-premise und in Microsoft 365 visualisieren konnte, identifizierte und deaktivierte es über 500 veraltete Benutzer und reduzierte Microsoft 365-Gruppen von 280 auf 31.

Zustand der Cloud-Sicherheit

Cloud-Anwendungen und -Services schaffen eine breite, miteinander verbundene Angriffsfläche, die von Insidern und externen Akteuren auf neue Weise kompromittiert werden kann. Die Angriffe sind hochgradig effektiv und wirkungsvoll geworden. Staatliche gesponserte Akteure sind raffinierter geworden und ihre Techniken sind bereits in den kommerziellen Raum eingedrungen, wie sie es schon viele Male zuvor getan haben.

Die Cloud erschließt einen enormen Mehrwert für Unternehmen. Aber neben Zweckmäßigkeit und Zusammenarbeit macht es die Cloud viel schwieriger, Bedrohungen zu erkennen. Jeder Endpoint dient als Zugangspunkt – eine Zugangsrampe zu digitalen Umgebungen mit kritischen und sensiblen Daten. Und SaaS-Anwendungen sind oft die größten toten Winkel von Organisationen, die ihre Daten schützen wollen.

Die Verfügbarkeit von Exploits und Chancen auf eine große Auszahlung durch die Opfer bedeutet, dass Angreifer nicht aufhören werden. Jedes System, Konto und jede Person kann zu jeder Zeit ein potenzieller Angriffsvektor sein. Bei einer derart großen Angriffsfläche müssen Sie davon ausgehen, dass Angreifer mindestens einen Vektor erfolgreich durchbrechen – sofern sie dies noch nicht getan haben.



Checkliste für Cloud-Datensicherheit

- [ ] **Verstehen und reduzieren Sie den potenziellen Schaden Ihrer SaaS**

  Was wäre der potenzielle Schaden, wenn ein Angreifer einen Benutzer kompromittierte? Wenn Sie Ihren potenziellen Schaden in der Cloud – alles, worauf ein Angreifer mit nur einem kompromittierten Konto oder System zugreifen kann – vor einem Angriff reduzieren, erschwert das die Arbeit von Cyberkriminellen.

- [ ] **Achten Sie auf ungewöhnliche Aktivitäten in Ihrer Cloud-Umgebung.**

  Angreifer lösen mit höherer Wahrscheinlichkeit Warnungen aus, wenn sie durch mehr Reifen springen müssen, um auf Ihre sensiblen Daten zuzugreifen. Behalten Sie die Benutzeraktivitäten im Auge und achten Sie auf Anomalien und Aktivitäten, die nicht den Richtlinien entsprechen.

- [ ] **Übernehmen Sie einen Zero-Trust-Ansatz.**

  Zero Trust ist wahrscheinlich Ihr bester Schutz vor Daten-bezogenen Angriffen wie Ransomware. Keine Person, Anwendung und kein System sollte in der Lage sein, auf mehr zuzugreifen oder mehr zu tun, als sie benötigen. Beschränken Sie den Zugriff auf Systeme, Anwendungen und Daten – insbesondere auf sensible Daten.

- [ ] **Überprüfen Sie die Einstellungen Ihrer SaaS-Anwendung.**

  Es ist nur eine Fehlkonfiguration erforderlich, um sensible Daten offenzulegen. Wenn Ihre Konfigurationen nicht perfekt sind, können Sie Ihre Anwendungen – und Daten – einem enormen Risiko aussetzen. Überprüfen Sie die Einstellungen erneut, um sicherzustellen, dass durch Updates keine Daten offengelegt werden. Schränken Sie die Freigabe außerhalb Ihrer Organisation ein und überprüfen Sie die Konfigurationseinstellungen für die Cloud-Freigabe.

- [ ] **Aktivieren Sie MFA für alle Ihre Mitarbeitenden.**

  Dieser einfache Schritt ist entscheidend und wird dennoch häufig übersehen. Aktivieren Sie MFA in Cloud-Apps und -Services und für Service-/Admin-Konten. Schreiben Sie MFA vor und erlauben Sie es Benutzern nicht, sie zu deaktivieren. Zu viele Organisationen erlauben die Ein-Faktor-Authentifizierung bei Internet-Services.

- [ ] **Richten Sie Prozesse für das Offboarding von Benutzern ein und setzen Sie diese durch.**

  Während Unternehmen mehr SaaS-Apps und -Services einführen, erhöht sich auch die Wahrscheinlichkeit, dass Geisterbenutzer – aktivierte, aber ungenutzte Konten – verwendet werden. Stellen Sie sicher, dass Sie Berechtigungen für Ihre Cloud-Services widerrufen, wenn Mitarbeitende oder Auftragnehmer das Unternehmen verlassen.

- [ ] **Finden Sie die richtige Balance zwischen Produktivität und Sicherheit.**

  SaaS-Apps sind häufig wertvoller, wenn sie integriert sind, aber die Interkonnektivität über APIs kann es Angreifern erleichtern, sich lateral zu bewegen. Halten Sie Ausschau nach Fehlkonfigurationen und stellen Sie sicher, dass Sie eine geeignete Cloud-Sicherheitslage haben.

- [ ] **Ihre Daten sind das Wichtigste.**

  Anstatt an mit Endpoints und Vektoren von außen zu beginnen, ist es weitaus praktischer, zuerst Ihre großen, zentralisierten Repositorys zu schützen – und dann von innen nach außen zu arbeiten.

Empfehlungen

Sobald Sie „ein Leck vermuten“, überlegen Sie, wohin ein Angreifer am wahrscheinlichsten navigieren würde, wenn er seinen Gewinn maximieren möchte. Wenn Ihre Organisation wie die meisten ist, dann ist das direkt in Richtung Ihrer größten kritischen Datenspeicher. Ihre Mission ist es, Ihren potenziellen Schaden so gering wie möglich zu halten (d. h. Benutzer können nur auf die Daten zugreifen, die sie benötigen). Außerdem müssen Sie in der Lage sein, einen ungewöhnlichen Zugriff zu erkennen, der auf einen Angriff hindeuten könnte.

Jeder zusätzliche Schritt, zu dem Sie einen Angreifer oder Insider zwingen können, verlangsamt ihn und gibt Ihnen die Möglichkeit, einen Angriff zu erkennen und zu verhindern.

Angenommen, ein Cyberangriff oder bösartiger Insider trifft Ihr Organisation In diesem Fall liegen Sie bereits gefährlich weit zurück, wenn Sie nicht sofort sehen können, was ein kompromittierter Benutzer in Ihren SaaS-Anwendungen und -Services mitgenommen haben könnte oder mitgenommen hat.

Es ist entscheidend, mit einem Daten-Zuerst-Ansatz zu beginnen.

Stellen Sie sich diese wichtigen Fragen:

1. Wissen Sie**, wo Ihre wichtigen Daten gespeichert sind?**
2. Wissen Sie**, dass nur die richtigen Leute Zugang dazu haben?**
3. Wissen Sie, **dass die Daten dort ordnungsgemäß verwendet werden?**

Diese drei Fragen umrahmen die drei Dimensionen des Datenschutzes – Wichtigkeit, Zugänglichkeit und Nutzung. Um sinnvolle Entscheidungen zu treffen und Ihre Risikolage zu verbessern, müssen Sie sehen, wo kritische Daten konzentriert und ausgesetzt sind (gefährdet) und wer sie nutzt bzw. nicht nutzt (veraltet).

Ihre Daten sind das Wichtigste. Anstatt von außen mit Endpoints und Vektoren von zu beginnen, ist es weitaus praktischer, zuerst Ihre großen, zentralisierten Repositorys zu schützen – und dann von innen nach außen zu arbeiten.

Fallstudie

Ein Immobilienunternehmen sichert Salesforce mit Varonis.

Ein führendes Immobilienunternehmen hat DatAdvantage Cloud zum Schutz sensibler Daten in seinen meistgenutzten SaaS-Apps eingeführt, einschließlich Salesforce. Dank besserer Sichtbarkeit und hochpräziser Alarme, die sich nahtlos in vorhandene Sicherheitslösungen integrieren lassen, hat das Unternehmen die Eindämmungs- und Reaktionszeiten verkürzt und die Gewissheit erlangt, dass seine Daten geschützt waren.

„Wir können problemlos Berichte erstellen und sehen, wer Super-Admin- oder Admin-Berechtigungen hat und wo diese sich überschneiden. Die Cloud-übergreifende Sichtbarkeit von DatAdvantage Cloud ist außerordentlich praktisch, weil es fast unmöglich ist, das manuell zu versuchen. Man müsste mit diesem verrückten, riesigen Spinnennetz arbeiten und man würde definitiv etwas übersehen."

Tony Hamil, US-Immobilienunternehmen

Case Study

Möchten Sie sehen, ob Ihre Cloud-Daten gefährdet sind?

Holen Sie sich ein kostenloses Cloud Data Risk Assessment von Varonis. Entdecken Sie schnell und ohne zusätzlichen Arbeitsaufwand, welchen versteckten Risiken Ihre wichtigsten Daten ausgesetzt sind.

Holen Sie sich Ihr Risk Assessment

Über Varonis

Varonis ist ein Pionier im Bereich Datensicherheit und Analytik, spezialisiert auf Software für Datenschutz, Bedrohungserkennung und -reaktion sowie Compliance. Das Software-Unternehmen schützt Unternehmensdaten durch die Analyse von Datenaktivitäten, Perimetertelemetrie und Benutzerverhalten. Es verhindert Katastrophen durch die Sperrung sensibler Daten und sorgt durch Automatisierung effizient für hohe Sicherheit.

www.varonis.com