Wie Varonis einem Energieversorger hilft, kritische Daten in AWS und M365 zu schützen

> Wir haben ein konsolidiertes Dateisystem in AWS, das jahrelang angesammelte Daten enthält. Wir verwalten und schützen unsere Daten im gesamten AWS-Ökosystem mit Varonis.

Über diese Fallstudie:

Unser Kunde ist ein führendes Unternehmen im Energiesektor, für das Varonis ein wichtiger Bestandteil seiner Sicherheitsstrategie ist. Dem Wunsch nach Anonymität sind wir gerne nachgekommen.

HIGHLIGHTS

Herausforderungen

+ Schutz von Daten in M365 und AWS
+ Abdeckung von Hochrisikobereichen in Cloud, E-Mail und S3
+ Umsetzung von Best Practices und Einhaltung zahlreicher Datenschutzbestimmungen

Lösung

Die Cloud-native Datensicherheits-plattform von Varonis:

+ identifiziert und klassifiziert automatisch sensitive Daten
+ überprüft und reguliert den Zugriff auf sensitive Daten
+ erkennt und meldet abnormale Aktivitäten in Echtzeit

Ergebnisse

+ Einsparung von Tausenden Arbeitsstunden durch Automatisierung
+ Absicherung von AWS S3-Buckets
+ Alarmierung bei ungewöhnlichen Anmeldungen durch den CEO zur Validierung
+ Bereinigung von Daten, die sich über Jahre hinweg aus verschiedenen Dateisystemen und Übernahmen in AWS angesammelt hatten
+ Nachweis über die Einhaltung der SEC-Meldeanforderungen in den USA und der DSGVO in der EU
+ Einhaltung des NIST CSF 2.0-Standards zu über 85 Prozent durch Automatisierung

HERAUSFORDERUNGEN

Datensicherheit für M365 und AWS

Der Energieversorger setzt seit langem erfolgreich Technologien zur Verbesserung seiner Prozesse ein. Vor kurzem optimierte das Unternehmen seine IT-Infrastruktur und setzte auf einen Cloud-first-Ansatz. Im Rahmen seiner digitalen Transformation musste das Unternehmen Benutzerberechtigungen und veraltete Daten bereinigen und seine kritischen Daten vor Angriffen schützen.

Der CIO erklärt:

> **„Unsere AWS-Cloud hostet alle Dateiserver und Systeme. Alles befindet sich in der Cloud. Wir benötigten eine Lösung, die unsere risikoreichen Bereiche abdeckt: unsere Cloud-Dateien und -Server, E-Mail und S3.“**

Das schlanke IT- und Security-Team des Energieunternehmens ist dafür verantwortlich, die Sicherheit riesiger Mengen an Cloud-Daten für das globale Unternehmen zu gewährleisten. Entsprechend benötigte das Unternehmen eine Lösung, die mit geringem Verwaltungsaufwand dieselben Funktionen für die gesamte Infrastruktur bereitstellen kann.

Der CIO und der CISO suchten nach einer Lösung, mit der sie ihre Cloud-Daten schützen, internationale Standards einhalten und Bedrohungen in Echtzeit erkennen und abwehren konnten.

Das Energieunternehmen entschied sich für Varonis.

LÖSUNG

Kontrolle über die AWS-Umgebung

Die Varonis Datensicherheitsplattform ermöglicht es dem IT- und Security-Team des Energieversorgers, sensitive Daten zu schützen, Berechtigungen zu bereinigen und Bedrohungen und ungewöhnliche Aktivitäten in AWS, Microsoft 365 und Active Directory zu identifizieren. Und das alles bei gleichzeitiger Umsetzung der Cloud-first-Strategie.

Das Energieunternehmen profitiert dabei von den Funktionalitäten der Varonis Datensicherheitsplattform und erhält zudem erstklassigen Experten-Support.

Der CIO schätzt vor allem das kontinuierliche Engagement von Varonis, um sicherzustellen, dass sein Team das Optimum aus der Plattform herausholt.

> **„Wir wollten nicht einfach nur ein Tool kaufen. Varonis stellt sicher, dass ihre Kunden das Produkt auch wirklich nutzen. Das gefällt uns sehr, da wir nur ein kleines IT-Team haben. Die Kombination aus dem Team von Varonis und unserem Team sorgt dafür, dass es läuft."**

Absicherung von AWS S3-Buckets

Fehlkonfigurationen in der Cloud können dazu führen, dass sensitive Dateien für unbefugte Benutzer und sogar öffentlich im Internet zugänglich sind. So haben falsch konfigurierte AWS S3-Buckets große Mengen sensitiver Daten wie Gesundheitsinformationen (PHI) und personenbezogene Daten (PII) von Millionen Menschen offengelegt.

Der Energieversorger wollte sicherstellen, nicht das nächste Unternehmen zu sein, das versehentlich vertrauliche Daten preisgibt. Der CISO:

> **„S3-Buckets sind in der Hackerwelt ein beliebtes Ziel, weil AWS so weit verbreitet ist. S3-Buckets werden ständig angegriffen."**

Varonis scannt die AWS-Umgebung des Energieunternehmens, um sensitive Daten in der Cloud-Umgebung automatisch zu erkennen und zu klassifizieren. Die Plattform zeigt an, wo AWS-Daten durch übermäßigen Zugriff und Fehlkonfigurationen gefährdet sind. Varonis identifiziert auch aktiv verdächtige Aktivitäten in Bezug auf Daten und Zugriff und gibt entsprechende Warnmeldungen aus.

> **„Wir haben ein konsolidiertes Dateisystem in AWS, das jahrelang angesammelte Daten enthält. Wir verwalten und schützen unsere Daten im gesamten AWS-Ökosystem mit Varonis."**

Umsetzung von Best Practices und Gewährleistung der Compliance

Das Energieunternehmen wollte das NIST Cybersecurity Framework (CSF) 2.0 mit Schwerpunkt auf Governance übernehmen. Die Governance-Komponente des CSF betont, dass die Cyberbedrohungen ein großes Unternehmensrisiko darstellen, auf das sich die Unternehmensleitung genauso konzentrieren sollte wie auf Finanzen und Reputation.

Der CISO sagt dazu:

> **„Wir folgen dem NIST CSF 2.0-Standard. Unser Automatisierungsprozess ermöglicht es uns, diese nationalen Vorgaben einzuhalten und die Compliance sicherzustellen. Mit den Automatisierungsprozessen von Varonis können wir kontinuierlich eine Konformität von über 85 Prozent erreichen."**

Varonis hilft dem Energieversorger, die Einhaltung internationaler Vorschriften in den vielen Ländern, in denen er tätig ist, nachzuweisen – einschließlich der SEC-Meldeanforderungen in den USA und der DSGVO in der EU.

Der CISO:

> **„Cybersicherheit ist von entscheidender Bedeutung. Durch die neuesten SEC-Bestimmungen müssen Unternehmen jetzt innerhalb weniger Stunden auf einen Vorfall reagieren. Wir haben Tausende Mitarbeitende auf der ganzen Welt. Varonis überwacht unsere Umgebung aktiv, liefert uns Echtzeitinformationen und schließt Sicherheitslücken für uns. Varonis ist eine enorme Zeitersparnis und hilft uns, unser Risiko deutlich zu reduzieren."**

ERGEBNISSE

Abnormale Aktivitäten erkennen und melden

Varonis setzt sensitive Daten, Berechtigungen und Aktivitäten in einen Kontext und achtet auf alles, was ungewöhnlich ist und auf frühe Anzeichen eines Angriffs hinweisen könnte. Mit Varonis überwacht das Energieunternehmen aktiv seine Cloud-Umgebung und erhält Echtzeit-Warnungen über ungewöhnliche Aktivitäten.

> **„Varonis hat auffällige Logins von unserem CEO und einem unserer Vorstandsmitglieder an Orten erfasst, an denen sie sich normalerweise nicht aufhalten. Varonis alarmierte uns sofort und wir konnten überprüfen, ob es sich um legitime Aktivitäten handelte. Vor Varonis hatten wir keine Möglichkeit, unübliche Logins zu erkennen", erklärt der CISO."**

Datensicherheitslage verbessern

Varonis unterstützte den Energieversorger dabei, über Jahre hinweg angesammelte Daten aus verschiedenen Dateisystemen und mehreren Übernahmen zu bereinigen und in AWS zu konsolidieren. Dank Varonis konnten zudem inaktive und veraltete Benutzer sowie ungenutzte Dateien aus der Umgebung zu entfernt werden.

Laut dem CIO war Varonis entscheidend, um die Umgebung von diesem Chaos zu befreien:

> **„Hacker lieben Unordnung. Varonis hat uns dabei geholfen, herauszufinden, wo in unseren Systemen in AWS und Entra ID (früher Azure AD) Unordnung herrscht. Es ist eine Sache zu sagen, dass man das Chaos loswerden will. Eine andere Sache ist es, das Chaos zu identifizieren, damit man es tatsächlich beseitigen kann. Varonis hat uns wirklich geholfen, unsere Cloud-Daten sehr gut zu organisieren."**

Tausende Stunden durch Automatisierung einsparen

Das Datenvolumen wächst ständig, Benutzer wechseln ihre Rolle oder verlassen das Unternehmen, und ständig tauchen neue Bedrohungen auf. Deshalb ist für viele Unternehmen wie das globale Energieunternehmen die automatisierte Sanierung von Varonis entscheidend für die Aufrechterhaltung einer starken Datensicherheit.

Die Automatisierung von Varonis arbeitet im Hintergrund und hilft dem Versorger kontinuierlich, Risiken zu reduzieren und seine Daten auf Bedrohungen zu überwachen. Varonis befreit IT- und Security-Teams von manuellen und zeitaufwändigen Security-Prozessen, so dass sie sich auf andere Aufgaben konzentrieren können.

> **„Die Automatisierung von Varonis ist für uns ein echter Quantensprung und hat uns Tausende Arbeitsstunden erspart. Varonis hat uns dabei geholfen, unseren Aufwand zu minimieren, da wir nicht mehr so viel Personal für die Lösung von Problemen einsetzen müssen. Wir haben auch menschliche Fehler eliminiert, die mit diesen manuellen Prozessen einhergehen."**

Mit Varonis sieht das IT- und Security-Team, wo sich alle Daten in ihrer Umgebung befinden, wer darauf Zugriff hat und was er mit diesem Zugriff macht. Varonis stellt dem CISO und CIO auch Berichte zur Verfügung, die belegen, wie das Unternehmen Tausende Anomalien in seiner Cloud-Umgebung behoben und diese Zahl auf null reduziert hat.

Der CISO:

> **„Mit Varonis können wir uns auf das Reporting und die Analyse konzentrieren. Sicherheit ist ein kontinuierlicher Prozess. Durch die Automatisierung von Varonis haben wir die Zahl der Anomalien von Tausenden auf null gesenkt."**

ROI nachweisen

Mit Varonis kann das IT- und Security-Team auf einfache Weise harte Daten sammeln, die die Ergebnisse ihrer Investitionen in die Cybersicherheit belegen. Der CIO kann so dem Vorstand selbstbewusst darlegen, dass das Unternehmen die Best Practices für Data Governance befolgt und Prozesse automatisiert – und das alles bei vollständiger Transparenz des Datenbestands.

> **„Wir haben einen aktiven Vorstand, der sich um die Cybersicherheit sorgt. Ich berichte ihm jedes Quartal und zeige, wie wir unsere Sicherheit mit Varonis sicherstellen. Wir demonstrieren so der Geschäftsführung, dass wir Cybersicherheit ernst nehmen, und Varonis hilft uns dabei."**

“Durch die Automatisierung von Varonis haben wir die Zahl der Anomalien von Tausenden auf null gesenkt.”

Schützen Sie Ihre sensitiven Daten - automatisiert.

Unsere Cloud-native Datensicherheitsplattform entdeckt und klassifiziert kontinuierlich kritische Daten, behebt Schwachstellen und erkennt fortschrittliche Bedrohungen mit KI-gestützter Automatisierung.

Fordern Sie eine Demo an