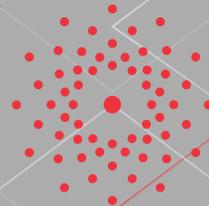




VARONIS FALLSTUDIE:

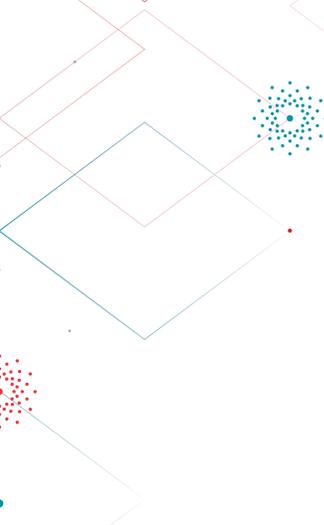
Eissmann Automotive Deutschland GmbH





Wir konnten unsere Zugriffsrechte deutlich vereinfachen und die Komplexität reduzieren. Mit der Software von Varonis konnten doppelte, veraltete und zu umfangreiche Rechte einfach identifiziert und schließlich sicher entfernt werden.

– Alexander Maute, Leiter IT-Infrastruktur/IT von Eissmann



Der Kunde

Standort: Baden-Württemberg, Deutschland

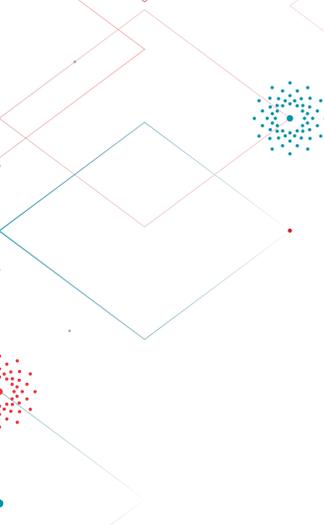
Produkte: [DatAdvantage](#), [DataPrivilege](#)

Branche: Automotive

Sicherheitsgurt für die Daten: Datensicherheit bei der Eissmann Group Automotive

Das Herzstück der deutschen Wirtschaft ist zweifellos der Mittelstand, und das Herzstück eines Unternehmens sind neben den Mitarbeitern sicherlich seine vertraulichen Informationen. Gerade für innovative mittelständische Unternehmen hat deshalb Datensicherheit eine enorme Bedeutung. Angesichts der steigenden Zahl unstrukturierter Daten (also Dateien, die auf NAS, Sharepoint, Exchange oder in der Cloud abgelegt sind) und steigender Bedrohungen durch Datenschutzverletzungen, wird sie zu einer immer größeren Herausforderung. Vor diesem Hintergrund hat sich der Automobil-Zulieferer Eissmann für Sicherheitslösungen von Varonis entschieden.

Aus einem kleinen, schwäbischen Familienbetrieb ist seit der Gründung im Jahr 1964 ein weltweit tätiges Unternehmen mit Produktionsstandorten auf drei Kontinenten gewachsen. Zunächst als Zulieferer erstklassiger Lederinnenausstattung aufgestellt, ist die Eissmann Group Automotive heute ein kompetenter Entwicklungs- und Wertschöpfungspartner der Automobilindustrie. Das Portfolio umfasst dabei hochwertige Bedienmodule, Verkleidungsteile und komplette Fahrzeuginnenräume. Nahezu alle namhaften Hersteller der Automobilbranche zählen zu den Kunden und vertrauen auf die Synergie zwischen traditioneller Handwerkskunst und „*State-of-the-art*“-Produktionsprozessen.



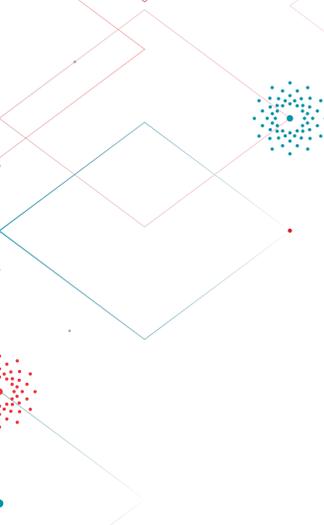
Ausgangslage/Herausforderung

Die Automobilindustrie gilt als einer der Wegbereiter der Digitalisierung. Schon früh setzte man hier auf Automatisierung, elektronischen Datenaustausch und Vernetzung. Als eine Folge nimmt nicht nur bei den Herstellern, sondern auch bei den Zulieferern die Menge an unstrukturierten und sensiblen, geschäftskritischen Daten kontinuierlich zu. Aber nicht nur die Menge steigt, sondern mit ihr auch der Wert und die Bedeutung der Daten. Einhergehend mit der steigenden Komplexität wird es immer schwieriger nachzuvollziehen, wer welche Zugriffsrechte hat und wer auf welche Dateien zugreift. Da es sich hierbei um unternehmenskritische Inhalte handelt, beschloss Eissmann, insbesondere ihre Ordner zu überwachen. Für dieses Monitoring wurde zunächst ein eigenes Programm entwickelt, das jedoch bald an seine Grenzen stieß. Nach umfassender Recherche entschied sich das Unternehmen schließlich für Varonis DatAdvantage, um die Berechtigungen innerhalb der Betriebsumgebung zunächst zu identifizieren und anschließend überwachen zu können. Dabei kombinierte Eissmann die Lösung mit DataPrivilege, um in einem nächsten Schritt Dateneigentümer zu identifizieren, die sich selbst mit Hilfe eines automatisierten Berechtigungsprozesses um die Zugriffsverwaltung kümmern.

„Stand anfangs noch das Monitoring im Vordergrund, erwies sich rasch insbesondere DataPrivilege für unsere IT-Abteilung als echter Mehrwert.“

sagt Alexander Maute, Leiter IT-Infrastruktur/IT von Eissmann

„Zunächst erhielten wir mit DatAdvantage eine Übersicht aller Dateien, die geöffnet, erstellt, verändert oder gelöscht wurden – sortiert nach Benutzern. Also genau das, was das ursprüngliche Ziel des Projekts war. Anhand dieser Parameter konnten wir darüber hinaus die korrekten Dateneigentümer ermitteln und sie an der Vergabe und Verwaltung der Berechtigungen beteiligen. Hierbei hilft DataPrivilege: Durch eine intuitive Oberfläche gestaltet sich der Prozess der Rechtevergabe auch für technisch nicht sehr versierte Anwender sehr einfach. Dauerte es früher mehrere Tage mit diversen Mails, bis die entsprechenden Rechte erteilt wurden, tritt nun an diese Stelle ein vollständig automatisierter Prozess und die gesparte Zeit kann für andere Aufgaben eingesetzt werden.“



Mittlerweile verfügt Eissmann über rund 80 Data Owner, die in ihren Bereichen die Verantwortung für die Dateien tragen, den Zugriff auf die Sicherheitsgruppen verwalten und Zugriff auf geteilte Verzeichnisse gewähren. Dieses Prinzip ist auch insofern sinnvoll, als dass die tatsächlich Verantwortlichen in den jeweiligen Abteilungen besser einschätzen können, wer welchen Zugang zu welchen Informationen benötigt. Auch haben sie einen besseren Überblick darüber, ob diese Rechte im Laufe der Zeit noch nötig sind, da sich beispielsweise Aufgabengebiete verändern oder Mitarbeiter die Abteilungen wechseln.

Wir konnten unsere Zugriffsrechte deutlich vereinfachen und die Komplexität reduzieren. Mit der Software von Varonis konnten doppelte, veraltete und zu umfangreiche Rechte einfach identifiziert und schließlich sicher entfernt werden. Die Erteilung neuer Rechte erfolgt nun durch die Dateneigentümer, was die IT-Abteilung nachhaltig entlastet

so Maute. Hilfreich war die Software auch bei der Erlangung der ISO/IEC 27001-Zertifizierung, da Eissmann mit ihr ein ganzheitliches, aber vor allem individuell abgestimmtes Schutzkonzept, das kontinuierlich verbessert und weiterentwickelt wird, umsetzen kann.

Geschäftlicher Nutzen

Seit dem Einsatz von DatAdvantage und DataPrivilege konnte bei Eissmann eine Transparenz erreicht werden, die es in diesem Maße vorher nicht gab. Durch die Auditing-Funktion kann einfach kontrolliert werden, wer auf Daten zugreift und welche Aktivitäten mit diesen Daten verbunden sind, also wozu Benutzer ihre Berechtigungen verwenden. Das Unternehmen hat so nun eine **vollständige Transparenz über alle Dateiaktivitäten** (Öffnen, Erstellen, Verändern und Löschen), die Benutzer auf den Fileservern ausführen.

Gleichzeitig war es möglich, die **Komplexität deutlich zu reduzieren**. Dazu wurden Rechte- und Gruppenstrukturen vereinfacht, übermäßige Berechtigungen eliminiert und die Anzahl existierender Gruppen deutlich minimiert. Gerade Gruppen, die länger nicht verwendet wurden, und Gruppenmitglieder, die ihren Zugriff nicht länger benötigten, sowie redundante Gruppen blähen gewöhnlich die Systeme auf. Mit Hilfe von Varonis konnten diese überwacht, identifiziert und schließlich entfernt werden.

Um auch zukünftig **schlanke Prozesse und zugeschnittene Berechtigungen** nach dem „need-to-know“-Prinzip sicherzustellen, wurde der Berechtigungsprozess vollständig automatisiert. Die Mitarbeiter beantragen jetzt den Zugriff auf eine Gruppe, den die Dateieigentümer automatisiert erteilen können, ganz ohne Beteiligung der IT-Abteilung. Das beschleunigt nicht nur den Prozess an sich, sondern entlastet auch die IT und setzt Ressourcen für andere Aufgaben frei.

Über Varonis

Varonis ist ein führender Anbieter von Softwarelösungen zum Schutz Ihrer Daten vor Insider-Bedrohungen und Cyberangriffen. Varonis versetzt Unternehmen in die Lage, Ransomware im Keim zu ersticken, zu offen liegende sensible Daten zu erkennen, angreifbare und veraltete Daten zu priorisieren und abzusichern, ohne das ohne den laufenden Betrieb zu unterbrechen. Varonis setzt den Inhalt der Daten und Aktivitäten in einen Kontext, automatisiert die Bedrohungserkennung mit prädiktiven, auf leistungsfähigen Analysen, Benutzerverhalten und maschinellem Lernen aufgebauten Bedrohungsmodellen und überwacht kritische Ressourcen auf verdächtige Aktivitäten, wie z. B. ungewöhnliche Zugriffe auf sensible Daten, auffälliges Benutzerverhalten und auffällige Dateiaktivitäten, um Schutz gegen potenzielle Sicherheitslücken zu bieten.



Bewertung des Datenrisikos

Sie erhalten Ihr Risikoprofil, entdecken Sicherheitslücken und beheben echte Sicherheitsprobleme.

info.varonis.com/express-assessment-de



Live-Demo

Richten Sie Varonis in Ihrer eigenen Umgebung ein, um zu beobachten, wie Ransomware gestoppt und Ihre Daten geschützt werden.

varonis.com/demo-de