VARONIS

Wie sich der Automobil-Zulieferer Knipping mit Varonis vor unkontrolliertem Datenabfluss schützt

> „Mit Varonis ist die Zusammenarbeit extrem gut, weil dort Kundenservice großgeschrieben wird. Ich finde es einfach charmant, wie man miteinander umgeht, dass man diese kurzen Wege hat, dass man schnell Antworten bekommt. Das unterscheidet Varonis von seinen Marktbegleitern.“

HIGHLIGHTS

Herausforderungen

+ Hohe Compliance-Anforderungen im Automotive-Sektor
+ Steigende Cyberrisiken, insbesondere durch Datenabfluss und Ransomware
+ Altlasten durch die Zusammenlegung von zwei IT-Abteilungen

Lösung

+ Leistungsstarke Automatisierung, die Sicherheitsprobleme ohne menschliches Eingreifen behebt
+ Echtzeit-Warnungen bei potenziellen Bedrohungen
+ Integriertes Incident-Response-Team und schnelle Hilfe

Ergebnisse

+ Tiefere Transparenz in Daten- und Nutzeraktivitäten
+ Höherer Datenschutz
+ Einfache Compliance

HERAUSFORDERUNGEN

Die Automobilbranche gilt als Vorreiter der Digitalisierung. Entsprechend müssen die Zulieferer hohe Anforderungen erfüllen. So wurde beispielsweise mit TISAX ein System für die Risikobewertung sowie zum Austausch normierter Prüfergebnisse in der Automobilindustrie geschaffen. Gleichzeitig ist die Branche ein herausragendes Ziel für Cyberangriffe und aufgrund des wertvollen geistigen Eigentums ebenso für Cyberspionage.

Als ein neuer TISAX-Audit durchgeführt werden musste und für die bisher hierfür eingesetzte Lösung kein Know-how mehr zur Verfügung stand, entschied sich Knipping Kunststofftechnik im Dezember 2023 für Varonis.

Das mittelständische Unternehmen entwickelt und produziert komplexe technische Teile und Baugruppen für die Automobil- und Elektroindustrie. Von den sechs Standorten in Leingarten, Talheim, Gummersbach, Ottendorf-Okrilla, Mexiko und Ungarn greifen rund 650 Mitarbeitende auf sensitive Daten zu. Diese werden nun durch Varonis effektiv geschützt.

LÖSUNG

Cybersecurity zur Chefsache gemacht

Am Anfang stand ein Proof of Concept. Hierzu analysierte Varonis bei Knipping 21 Tage den Datenzugriff und erstellte darauf basierend eine Datenrisikobewertung inklusive Empfehlungen zur Verbesserung der Sicherheitslage.

Die Präsentation der Ergebnisse erfolgte dann auf höchster Ebene, inklusive sämtlicher Geschäftsführer:

> **„Die Vorstellung der Ergebnisse war der Weg zum Erfolg, wo es recht schnell und ohne große Widerstände durchgegangen ist“, erklärt Michael Frank, CIO von Knipping. „Durch die Transparenz von Varonis kann man die Dinge zeigen, die eine IT-Abteilung gar nicht oder nur mit ganz viel Aufwand bereinigen kann. Und es muss der Geschäftsführung klar sein, dass wenn sie da nein sagt, sie ihre IT-Abteilung beschneidet und am Ende des Tages dafür auch geradestehen muss.“**

Dabei ist die Präsentation so gestaltet, dass die Security-Herausforderungen auch für Menschen ohne besondere IT-Affinität deutlich werden.

> **„Die Präsentation ist absolut Management-tauglich. Auch die Geschäftsführer, die mit IT nichts am Hut hatten, sind nach dem Meeting herausgekommen und haben gesagt: ‚Das nicht zu machen, wäre grob fahrlässig‘“, so der CIO.**

Schutz vor unkontrolliertem Datenabfluss und Ransomware

Das vordringlichste Ziel von Knipping ist der Schutz vor Datenvorfällen.

> **„Nicht nur durch die DSGVO hat unsere Geschäftsführung natürlich ein großes Interesse daran, dass keine Daten in falsche Hände geraten“, sagt Markus Frenzel, Head of IT von Knipping.**

Dies gilt zum einen für personenbezogene Daten, zum anderen aber gerade auch für geistiges Eigentum:

> **„Der klassische Abfluss von Daten, bei dem eine Datei an eine Mail angehängt wird, spielt bei unseren CAD-Daten weniger eine Rolle, da sie einfach viel zu groß sind, um sie per E-Mail zu verschicken. Aber trotz allem hätten wir gerne für unsere Daten, dass wir auf Knopfdruck sagen können, wo laufen Daten wie weg, was wird mit den Daten gemacht, wo werden Daten gezippt und vielleicht auf einen USB-Stick geschoben“, so CIO Michael Frank.**

Um genau dies zu verhindern, wurden gemeinsam mit Varonis die Alarme relativ granular eingestellt.

> **„Das System muss am Anfang noch lernen. Nach zwei bis drei Monaten haben wir ein paar Filter nachjustiert, weil ein paar Sachen betriebsintern auffallen. Die könnte Varonis von der Logik gar nicht abbilden“, erklärt Markus Frenzel. „Auch beim Thema Ransomware hatten wir anfangs ein paar False Positives: In einer unserer Abteilungen gibt es eine interne Regel, dass Daten, die transferiert werden sollen, vorher verschlüsselt werden müssen. Dies hat ein Mitarbeitender mit ein paar Dateien probiert und ist an Varonis gescheitert. Dadurch haben wir dann gesehen, dass unser Skript funktioniert und die Daten schützt.“**

Dies schlägt auch den Bogen zur Compliance, die auch ein wichtiges Thema für den Automobilzulieferer ist.

> **Markus Frenzel: „Wir haben entsprechende Vorgaben aus Audits heraus. Zudem legen unser Datenschutzbeauftragter (DSB) und unser Informationssicherheitsbeauftragter (ISB) hohen Wert darauf, dass wir jeden Audit bestehen. Mit Varonis haben wir jetzt die Mittel und Möglichkeiten, über Reports zeigen zu können, dass wir die Anforderungen erfüllen.“**

Schnelle Hilfe im Ernst- und Zweifelsfall

Das Security-Team von Knipping kann sich auch jederzeit auf die Unterstützung von Varonis verlassen.

> **„Es gab schon Alarme, bei denen ich mir nicht ganz sicher war, was dahintersteckte. In diesen Fällen konnte ich mich immer schnell und problemlos an Varonis wenden und mir wurde immer sofort und einfach nachvollziehbar geholfen“, sagt Markus Frenzel.**

Neben den Ansprechpartnern vor Ort stand bereits auch das internationale Incident Response Team von Varonis hilfreich zur Seite.

> **„Wenn man Sorge hat, um was es sich bei einem Vorfall handelt, wird einem genau erklärt, woran sich dies im Protokoll an welcher Stelle in welchem Log erkennen lässt. Und dieses Wissen kann man dann nachher auch gut intern weitergeben. Das macht die Bearbeitung zukünftig deutlich einfacher“, so der IT-Leiter.**

„Wir haben entsprechende Vorgaben aus Audits heraus. Zudem legen unser Datenschutzbeauftragter (DSB) und unser Informationssicherheitsbeauftragter (ISB) hohen Wert darauf, dass wir jeden Audit bestehen. Mit Varonis haben wir jetzt die Mittel und Möglichkeiten, über Reports zeigen zu können, dass wir die Anforderungen erfüllen.“

ERGEBNISSE

Transparenz gegen Betriebsblindheit

Das Wichtigste und Wertvollste, was Varonis den Sicherheitsverantwortlichen von Knipping bietet, ist die tiefe Transparenz:

> **„Varonis schützt uns vor der Betriebsblindheit. Wir wissen, wo wir Defizite haben, aber Varonis mach es nochmal transparent und zeigt es uns auf einfachen Dashboards an. Das Schöne ist: Man hat direkt den automatischen Abgleich. Diesen Monat sieht es so aus, nächsten Monat sieht es besser aus, weil man durch monatliche Reports gegensteuern kann“, erklärt Frenzel.**

So konnte in den vier Monaten zwischen dem Ende der Einführungsphase bis zum Start des regulären Betriebs bereits die Anzahl der stale user um 50 Prozent reduziert werden. Dies erfolgte zunächst manuell mithilfe der von Varonis gewonnenen Informationen. Mittlerweile werden nicht mehr genutzte Nutzerkonten automatisiert erkannt und entfernt. Auf diese Weise wurden zudem die stale memberships in Gruppen durch die Automation um 85 Prozent minimiert.

> **„Wir waren zuerst darauf bedacht, die Alarme entsprechend zu bearbeiten und das Active Directory geradezuziehen. Hier haben wir einen gewissen Nachholbedarf, da wir vor nicht allzu langer Zeit zwei IT-Abteilungen zusammengelegt haben. Varonis ist auch hier ein gutes Tool, um diese zwei Strukturen übereinanderzulegen. Wir haben noch etliche Altlasten auf dem File-Server, bei denen nicht einmal langjährige Mitarbeitende sicher sagen können, ob man diese noch benötigt. Durch Varonis erhalten wir jetzt die entsprechende Transparenz und wertvolle Einsichten“, so Frenzel.**

Ohne großen Aufwand erhalten die Sicherheitsverantwortlichen in übersichtlichen Dashboards einen ganzheitlichen Einblick in die Sicherheitslage.

> **„Mit Varonis können wir auch erkennen, wer sich von wo aus mit seinem Handy einloggen will. Das kann ein Azubi sein, der vergessen hat, sein VPN zu deaktivieren, weshalb ich einen Alarm aus Bangladesch bekomme. Es gibt natürlich auch Mitarbeitende, die sich ganz legitim aus dem Ausland einloggen. Das sind dann wunderbare Insights, die wir so nicht direkt ohne großen Aufwand sehen könnten.“**

Verbesserte Datensicherheit und Compliance

Die Transparenz ist jedoch kein Selbstzweck, sondern dient dazu, die Sicherheitslage zu verbessern und Compliance-Vorgaben zu erfüllen.

> **„Die Transparenz ist bei uns nun auf einem wesentlich höheren Level. Der Datenschutz ebenfalls. Wir haben es aktiv gesehen, als Daten offiziell verschickt werden sollten und dies an den entsprechenden Schutzmechanismen von Varonis gescheitert ist“, sagt Frenzel.**
>
> **„Auch die Compliance ist nun ganz anders aufgestellt. Wenn mich heute unser DSB oder ISB fragt, wer Dateien mit Externen teilt, kann ich ihm direkt sagen, wer das war und welche Maßnahmen ich ergriffen habe, um dies zukünftig zu unterbinden. Und das ist das Schöne dabei, dass wir sofort wieder compliant sind.“**

Entscheidend war, auch die Geschäftsführung ins Boot zu holen und ihr die Bedeutung einer funktionierenden IT klarzumachen.

> **CIO Frank: „Ich habe unseren Geschäftsführer gefragt: ‚Wenn wir die IT zwei Wochen schließen, kommen wir dann zurück?‘ Und die Antwort war: ‚Nein, das können wir uns nicht leisten.‘ Das sind die Möglichkeiten, die man als IT-Verantwortlicher hat zu sagen, dann gib mir bitte die Mittel in die Hand, dass ich das Unternehmen auch schützen kann. Man kann nur in dem Rahmen arbeiten, den die Geschäftsführung ermöglicht.“**

Beginn einer langen gemeinsamen Reise

Obwohl in der kurzen Zeit schon viel erreicht wurde, stehen Knipping und Varonis erst am Anfang. So ist basierend auf der automatisierten Klassifizierung, die bereits durchgeführt wird, demnächst ein umfangreiches automatisches Labeling geplant, um die nachgeschalteten DLP-Maßnahmen mittels Microsoft Purview zu unterstützen.

> **„Der Weg geht noch ein Stückchen weiter nach oben, wenn wir erstmal mit Labeling und Co. anfangen. Denn dann sind wir nochmal eine ganze Spur sicherer unterwegs“, so der IT-Leiter.**

Auf diese Weise wird die Partnerschaft weiter ausgebaut.

> **Frenzel: „Mit Varonis ist die Zusammenarbeit extrem gut, weil dort Kundenservice großgeschrieben wird. Ich finde es einfach charmant, wie man miteinander umgeht, dass man diese kurzen Wege hat, dass man schnell Antworten bekommt. Das unterscheidet Varonis von seinen Marktbegleitern. Denen schreibt man zehnmal eine Mail und fragt, wie etwas funktioniert. Und zur Antwort bekommt man dann Knowledge-Base-Artikel nach dem Motto ‚hier, lies selber!‘ Das ist bei Varonis ein ganz anderer Style. Da heißt es ‚komm, setzen wir uns mal schnell zusammen und machen 15 Minuten ein Meeting, ich zeig dir das mal eben‘. Das finde ich heutzutage in der IT state-of-the-art. Da können sich andere eine Scheibe von abschneiden.“**

„Der Weg geht noch ein Stückchen weiter nach oben, wenn wir erstmal mit Labeling und Co. anfangen. Denn dann sind wir nochmal eine ganze Spur sicherer unterwegs.“

Schützen Sie Ihre senitiven 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