VARONIS

Wie sich Woolworth mit Varonis vor Ransomware schützt und seinen Blast Radius reduziert

> „Varonis macht keine leeren Versprechungen. Wenn man sich eine Lösung anschaut, wird einem viel versprochen. Aber ob das stimmt, weiß man immer erst, wenn es wirklich passiert. Varonis hat den Worten auch Taten folgen lassen.“

HIGHLIGHTS

Challenges

+ Schutz der betriebsinternen Daten vor Ransomware und Datenexfiltration angesichts verschärfter Sicherheitslage
+ Unbekannter Explosionsradius
+ Zunehmend verteilte Daten durch steigende Cloud-Nutzung und Expansion

Lösung

+ Maßgeschneiderte Erkennungsmuster und Reaktionen
+ Überwachung und Benachrichtigung über abnormales Verhalten in kritischen Systemen
+ Integrierte Incident Response und schnelle Hilfe

Results

+ Transparenz und Kontrolle von sensitiven Daten und Berechtigungen für Tausende Mitarbeitende
+ Detailliertes, übersichtliches und einfaches Reporting
+ Reduzierung des Blast Radius durch Einführung von Datenverantwortlichen

HERAUSFORDERUNGEN

Effektiver Schutz vor Ransomware bei steigender Cloud-Nutzung

Der Handel steht wie kaum eine andere Branche im Fokus von Cyberkriminellen. Erfolgreiche Ransomware-Attacken auf große Handelsketten in Deutschland zeugen von einer sich stetig verschärfenden Bedrohungslage. Seit der Pandemie müssen zudem immer mehr Remote-Arbeitsplätze in die Sicherheitsstrategie integriert werden, um eine Datenexfiltration effektiv zu verhindern.

Vor diesem Hintergrund entschied sich Woolworth im Mai 2022 für Varonis. Das Unternehmen mit Sitz in Unna ist heute die am stärksten wachsende Handelskette in Deutschland und bietet Produkte des täglichen Bedarfs zu einem fairen Preis an. Mit über 650 Filialen (Stand: Februar 2024) ist Woolworth in der gesamten Bundesrepublik präsent und immer in der Nähe der Menschen.

Durch Varonis werden nun sämtliche betriebsinternen Daten, auf die die rund 10.000 Mitarbeitenden zugreifen, effektiv geschützt.

„Wir haben vieles von Varonis übernommen, erstellen aber auch eigene Muster, da unsere Umgebung sehr vielfältig ist.“

LÖSUNG

Maßgeschneiderte granulare Anpassung der Anomalie-Erkennung

Die Implementierung durch die IT-Abteilung erfolgte in nur wenigen Tagen. Unter der Führung des Abteilungsleiters IT-Systemintegration wurden sukzessive zwei IT-Mitarbeitende am Beginn ihrer Laufbahn an die tägliche Arbeit mit Varonis herangeführt. Die IT-Leitung definiert dabei Ziele und Aufgaben, die dann von diesen adressiert werden. Hierbei stand zunächst die Anpassung der Anomalie-Erkennung an die eigenen Bedürfnisse und Anforderungen im Fokus.

> **„Varonis bietet zahlreiche praktische vordefinierte Erkennungsmuster und Reaktionen, aber man kann alles so einstellen, wie man es für seine Umgebung braucht. Und das haben wir auch ausgereizt“, erklärt John Sellmann, der mit Varonis betraute Sachbearbeiter. „Wir haben vieles von Varonis übernommen, erstellen aber auch eigene Muster, da unsere Umgebung sehr vielfältig ist.“**

Die granulare Anpassungsfähigkeit war dabei die Grundlage dafür, hier ein Gleichgewicht zwischen Sicherheit und Komfort zu finden.

Auch die Alarmierungen wurden an die Workflows angepasst: Sie wurden so konfiguriert, dass alle relevanten Mitarbeitenden immer sofort informiert werden. Bei sicherheitskritischen Alarmen werden zudem automatisiert Gegenmaßnahmen eingeleitet.

Hilfe im Ernstfall

Nicht nur während der Implementierung, sondern auch im täglichen Einsatz kann sich Woolworth auf die Unterstützung von Varonis verlassen.

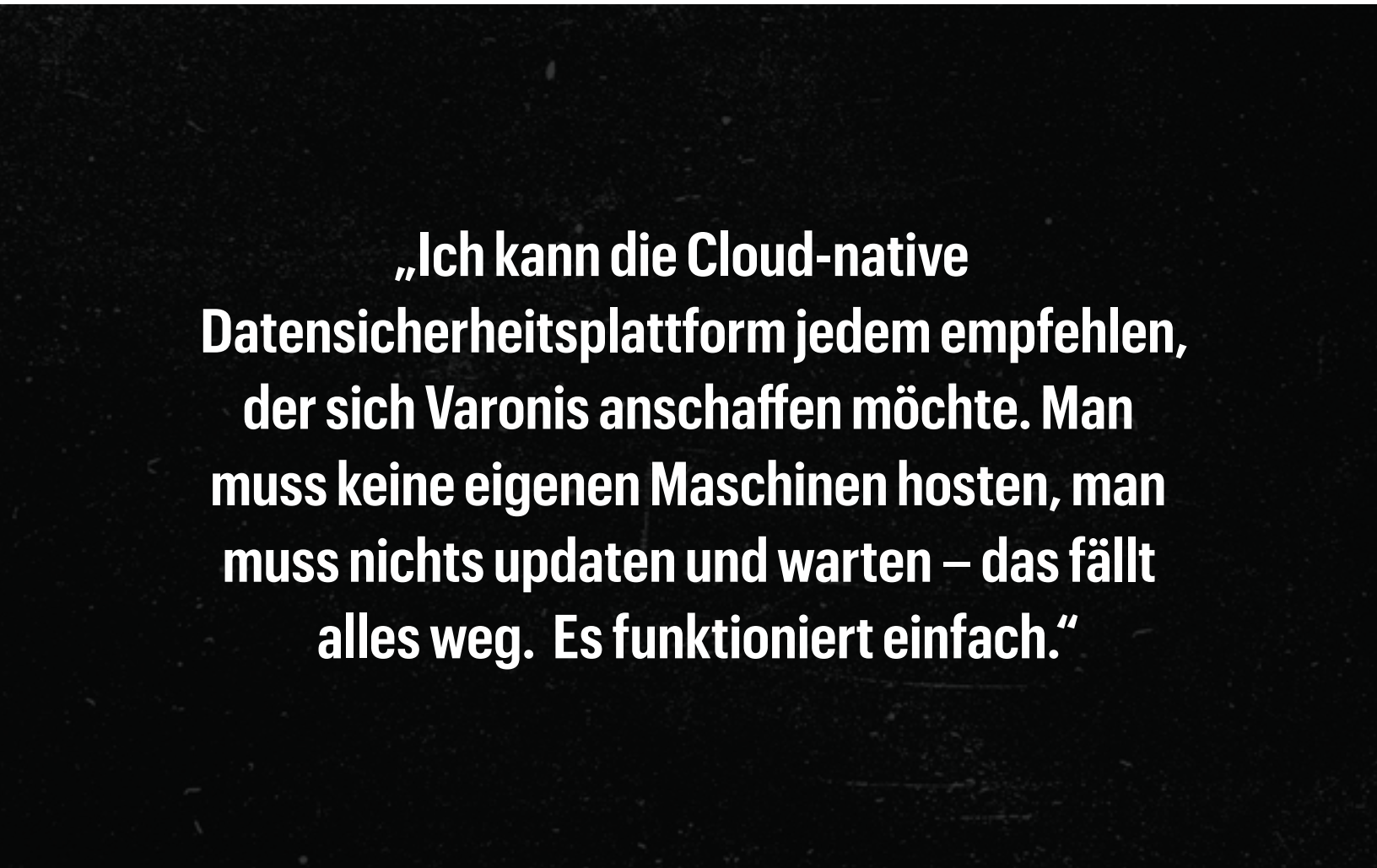
> **„Wenn wir Probleme oder Fragen haben, können wir uns jederzeit an Varonis wenden. Das Varonis-Team hat uns oft geholfen, Sachen zu analysieren, auseinanderzunehmen und zu überprüfen, was passiert ist, woran es gelegen hat und wie man es in Zukunft verhindern kann.“**

Gerade im Ernstfall kommt es auf Geschwindigkeit sowie die richtigen Entscheidungen und Maßnahmen an:

> **„Wir hatten einmal einen kleineren Incident. Meine Erfahrung da war unglaublich. Wir haben direkt unsere Kontaktperson bei Varonis angeschrieben und innerhalb von fünf Minuten waren drei, vier, fünf Leute mit uns online und haben mit uns das Ganze entschärft. Absolut fantastisch," sagt Sellmann.**
>
> **„Varonis macht keine leeren Versprechungen. Wenn man sich eine Lösung anschaut, wird einem viel versprochen. Aber ob das stimmt, weiß man immer erst, wenn es wirklich passiert. Varonis hat den Worten auch Taten folgen lassen."**

Sicherheit in der Cloud

Woolworth hat sich zunächst auf die On-Premises-Welt fokussiert. Durch die zunehmende Nutzung der Cloud und die internationale Expansion des Unternehmens, wurden die Daten jedoch immer verteilter und nicht mehr ausschließlich auf den Fileservern in der Zentrale abgelegt.



> **„Immer mehr Daten wurden in SharePoint und auf OneDrive gespeichert. Für diese Aktivitäten waren wir jedoch blind. Bildlich gesprochen haben wir die Fileserver mit einem Scharfschützen sicherheitsüberwacht, während wir keinen Einblick in die Cloud-Aktivitäten hatten."**

Seit Mai 2023 setzt das Unternehmen deshalb zum Schutz seiner Microsoft 365-Umgebung die neue Cloud-native Datensicherheitsplattform ein. Als SaaS ist die Implementierung innerhalb weniger Stunden umgesetzt und die Unternehmen profitieren sofort von den zahlreichen Vorteilen:

> **„Ich kann die Cloud-native Datensicherheitsplattform jedem empfehlen, der sich Varonis anschaffen möchte. Man muss keine eigenen Maschinen hosten, man muss nichts updaten und warten – das fällt alles weg. Es funktioniert einfach."**

Dabei hebt sich vor allem der Funktionsumfang bei einer gleichzeitigen Benutzerfreundlichkeit von herkömmlichen Lösungen ab:

> **„Die Cloud-native Datensicherheitsplattform ist nicht nur sehr intuitiv und bedienerfreundlich, sondern bietet auch tolle Funktionen, wie die Automatic Remediation, die automatisiert eine Überprivilegierung oder Stale Data erkennt und diese automatisch bereinigt. Oder das integrierte Incident Response Team, wo sich unser Varonis-Security-Analyst automatisch meldet, wenn etwas passiert. Was auch toll ist: Es kommen immer neue Funktionen dazu. Gerade in den letzten Wochen und Monaten sind so viele neue Policies dazugekommen – das macht einfach nur Spaß."**

ERGEBNISSE

Identifizierung und Reduktion des Explosionsradius

Varonis ermöglicht dem Security-Team eine bislang ungekannte Transparenz in die Daten-Aktivitäten und des damit verbundenen Datenrisikos.

> **„Durch Varonis haben wir überhaupt erstmal den Explosionsradius kennengelernt. Ich glaube, viele, die Varonis nicht benutzen, kennen ihn gar nicht und wissen nicht, wie groß er ist. Varonis macht es erst möglich, den Blast Radius zu erkennen, ihn messbar zu machen und zu reduzieren. Was man nicht misst, kann man nicht verändern, weil man nicht weiß, wo man anfangen soll und ob die Maßnahmen auch erfolgreich sind.“**

Die Sicherheitsverantwortlichen von Woolworth setzen sich entsprechend fortlaufend spezifische Ziele für die nächsten Monate, um diese Kennzahlen gezielt zu senken, und damit ihre Cyber-Resilienz sukzessive zu erhöhen. Ein zentrales Element dabei bildet das Dashboard:

> **„Allein durch das Dashboard mit den ganzen Informationen, die da zusammengetragen sind, wird unsere Arbeit wesentlich vereinfacht. Man kann gar nicht genug Leute haben, die die ganzen Logs und Informationen auswerten, bis man die Informationen so vor Augen hat. Das lässt sich gar nicht aufwiegen. Wir erkennen so schnell, wo wir exponiert sind, wo es zu viele Datenzugriffe gibt, oder wo Dateien liegen, die schon lange nicht mehr angepackt wurden.“**

Zudem erlaubt Varonis ein einfaches, maßgeschneidertes Reporting.

> **„Die Sachbearbeiter müssen sich nicht hinsetzen und aufwändig die nötigen Informationen zusammentragen. Dies spart viel Zeit und Geld. Mit Varonis können wir vieles automatisieren und sichtbar machen.“**

Höhere Datensicherheit durch Datenverantwortliche

Um den Explosionsradius weiter und nachhaltig zu reduzieren, möchte Woolworth zukünftig verstärkt auf Datenverantwortliche (Data Owner) setzen. Bislang erfolgt die Rechtevergabe durch die IT. So wird beispielsweise für eine bestimmte Abteilung ein Laufwerk eingerichtet, auf das alle Mitarbeitenden dieser Abteilung Zugriff erhalten sollen.

> **„Jetzt gibt es auf dem Laufwerk jedoch Unterordner, auf das nur die Führungsebene zugreifen soll, oder Projektordner, wo nur spezifische, aber wechselnde Leute Zugriff erhalten müssen, usw. Bei einem Konzern mit 10.000 Mitarbeitenden ist das unmöglich. Es bräuchte Unmengen an Personal, das im Active Directory die ganze Zeit nur Berechtigungen anpasst. Durch Varonis ist es jedoch möglich, dass die Führungskraft, die genau weiß, wer an welchem Projekt arbeitet und Zugriff haben sollte, den Zugriff managt. Zudem können die Berechtigungen auch automatisiert an einem bestimmten Datum wieder entzogen werden. Dadurch kann man die Berechtigungen granularer vergeben und so den Blast Radius immens senken."**

Für die Data Owner stellt dies keine Mehrarbeit, sondern vielmehr eine Entlastung dar. Im Rahmen des Referenz-Projekts, bei dem ein Ordner abteilungsübergreifend geteilt werden musste, wurde dem Datenverantwortlichen das Tool vorgestellt.

> **„Der designierte Data Owner war schnell begeistert und meinte: ‚Bis ich diese Anforderungen wie bisher in ein Ticket schreibe mit den ganzen Leuten in cc und das an den IT-Support schicke und bis die IT das bearbeitet hat, habe ich das in Varonis schon gemacht, bevor ich die E-Mail geschrieben habe.' Am Ende des Tages sind es für den Data Owner nur ein paar Klicks. Wenn die Leute es verstanden und mal benutzt haben, dann erkennen sie das Potenzial und finden es auch toll."**

Am Anfang des Projekts stand der Ransomware-Schutz. Doch durch die Arbeit mit Varonis erkannte Woolworth mehr und mehr das Potenzial der Lösung und einer datenzentrierten Sicherheitsstrategie.

> **„Man kann natürlich nur einen einzigen Alarm wie Crypto-Aktivität anlegen, der bei Ransomware-Angriffen anschlägt. Das ist aber aus meiner Sicht vergeudetes Potenzial. Ich würde dazu raten, sich intensiv mit den vielen Möglichkeiten auseinanderzusetzen, die Varonis bietet. Ich glaube, wenn man Varonis mit seinen ganzen Funktionen voll ausschöpft, gibt es andere Tools, die überflüssig werden."**

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