Wie eine US-Online-Bank ihre verteilten Mitarbeiter während der Corona-Krise sichert

FALLSTUDIE

„Ich kann Protokolle aus unseren VPNs direkt in Varonis ziehen. Jetzt erhalten wir jeden Morgen um 10 Uhr Berichte über verdächtige Logins direkt in unsere E-Mail-Postfächer zugestellt. Das ist ausgesprochen hilfreich, da über 75 Prozent der Mitarbeiter aufgrund der aktuellen Weltlage aus der Ferne arbeiten."

ÜBER DIESE FALLSTUDIE:

Unser Kunde ist eine US-amerikanische Online-Bank. Wir sind ihrem Wunsch, alle Namen und Orte zu anonymisieren, gerne nachgekommen.

HIGHLIGHTS:

HERAUSFORDERUNGEN

- Transformation zu einer vollständig aus der Ferne arbeitenden Belegschaft mit minimalen Betriebsunterbrechungen
- Reduzierung des Risikos für kritische Systeme, das von Remote-Login-Versuchen ausgeht
- Gewährleistung rascher Problemlösungen für Mitarbeiter, die von zu Hause aus arbeiten

LÖSUNG:

Die robusteste Plattform für Datensicherheit:

- **DatAdvantage** für Windows, Exchange und Verzeichnisdienste bildet Aktivitäten und Berechtigungen von Remote-Benutzern ab
- **Data Classification Engine** für Windows und SharePoint lokalisiert sensible Daten
- **DatAlert Suite** überwacht alle Daten und Systeme und gibt Warnmeldungen aus
- **Edge** analysiert Metadaten aus VPNs, DNS und anderen Perimeter-Technologien, um Anzeichen von Perimeter-Angriffen zu erkennen

Vollständige Integration mit Schlüsselsystemen:

- Pulse Secure (VPN)
- Palo Alto GlobalProtect (VPN)
- LogRhythm (SIEM)

ERGEBNISSE:

- Umfassende Login-Berichte werden automatisch aus VPNs gezogen
- Zeitersparnis für Sicherheitsteams und leitende Systemadministratoren
- Verbesserte Datensicherheit und Entlastung der Sicherheitsverantwortlichen beim flächendeckenden Einsatz von Homeoffice-Mitarbeitern

Herausforderungen

Sicherheit bei einer explodierenden Anzahl von Homeoffice-Nutzern

Als eine US-Online-Bank im Jahr 2017 Varonis einführte, ahnte sie nicht, wie wichtig dies für die sichere Fortführung ihres Geschäftsbetriebs und die flexible Schaffung von Homeoffice-Arbeitsplätzen in den folgenden Jahren sein würde.

COVID-19 änderte alles. Es dauerte nicht lange, bis 75 Prozent der Mitarbeiter aus dem Homeoffice arbeiteten. Dies setzte den leitenden Anwendungsadministrator unter immensen Druck, der dafür sorgen musste, dass die Mitarbeiter nahtlos von zu Hause aus arbeiten können.

> „Vor dem Einsatz von Varonis hatten wir keine wirklichen Daten vorliegen, in denen die An- und Abmeldefehler, Kontosperrungen und andere Probleme zusammengefasst und dadurch sichtbar waren, um diese zu reduzieren.“

Das Unternehmen setzte auf zwei VPNs (Pulse Secure und Palo Alto GlobalProtect) zum Schutz von Benutzer- und Unternehmensinformationen. Die Diagnose von Problemen und die Identifizierung von Nutzerproblemen war jedoch sehr zeitaufwändig.

> „Wenn wir nach etwas suchten, mussten wir in jedes einzelne System gehen, um zu sehen, wer zugreift, wie groß die Kapazität ist, wer versucht sich einzuloggen und wer damit Probleme hat, was ausgesprochen zeitintensiv war.“

Schlimmer noch: Die Unterstützung einer großen Zahl von Mitarbeitern, die aus der Ferne zugreifen, erhöhte die Gefahr von Cyberangriffen. Der leitende Anwendungsadministrator musste in der Lage sein, auf einen Blick zu diagnostizieren, ob ein fehlgeschlagener Anmeldeversuch lediglich ein Benutzer war, der sein Passwort falsch eingegeben hatte, oder womöglich ein Angreifer.

> „Die Sicherheit der Bank ruht auf meinen Schultern. Ich muss wissen, wer versucht, auf unsere Daten zuzugreifen, und wer auf sie zugreift. Ich muss diese Informationen jederzeit vor Augen haben.“

Als immer mehr Mitarbeiter begannen, aus der Ferne zu arbeiten, wuchsen die Bedenken der leitenden Mitarbeiter: „Wie sollen wir all diese Personen kontrollieren, die von zu Hause aus arbeiten?“

> „Glücklicherweise hatten wir bereits Varonis im Einsatz“, erklärt der leitende Anwendungsadministrator. „Es war eine einfache und schnelle Angelegenheit, Login-Berichte einzurichten und diese Berichte automatisch per E-Mail an den IT-Leiter zu senden.“

„Die Sicherheit der Bank ruht auf meinen Schultern. Ich muss wissen, wer versucht, auf unsere Daten zuzugreifen, und wer auf sie zugreift. Ich muss diese Informationen jederzeit vor Augen haben.“

Lösung

Reduzierung des Risikos durch umfassendes Monitoring und automatisierte Alarme

Als COVID-19 zu einer globalen Pandemie wurde, hatte die Online-Bank bereits vier Varonis-Produkte eingeführt, um Sicherheitslücken zu schließen und ihre Cyberabwehr zu stärken: DatAdvantage, Data Classification Engine, DatAlert Suite und Edge.

Dies war aus drei Gründen wichtig:

1. Varonis lieferte bereits einen tiefen Einblick in das Datenzugriffsverhalten

DatAdvantage und Data Classification Engine, die ersten beiden Produkte, die die Bank eingeführt hat, bieten mehr Transparenz darüber, auf welche Daten Benutzer zugreifen und wo sie zu viel Zugriff haben.

Zunächst bestand das Ziel der Bank lediglich darin, diese Informationen zur Durchsetzung von Datenschutz und Compliance zu nutzen. Doch als die meisten ihrer Mitarbeiter von zu Hause aus arbeiten mussten, wurde DatAdvantage für Exchange und Verzeichnisdienste besonders wichtig, um die Sicherheit zu gewährleisten.

Während die Benutzer über Exchange zusammenarbeiten und sich per Fernzugriff bei den Servern der Bank anmelden, überwacht Varonis diese Systeme und gibt dem Sicherheitsteam ein umfassendes, nach Prioritäten geordnetes Bild davon, wo die Daten gefährdet sind.

> „Varonis gibt mir die Möglichkeit, jederzeit zu wissen, was in unseren Dateisystemen vor sich geht. Ich muss mich nicht darauf konzentrieren, weil die Software das für mich erledigt", so der Anwendungsadministrator.

2. Bedrohungserkennung und Reaktionsfähigkeiten zum Schutz kritischer Systeme und entfernter Benutzer

Wenn Varonis irgendeine irreguläre Aktivität entdeckt (wie ein Benutzerkonto, das auf Daten zugreift, auf die es normalerweise nicht zugreift, den Versuch, Informationen einzusehen, für die es keine Berechtigung hat, oder das plötzliche Löschen von Dateien), ermöglicht die Echtzeit-Alarmierung und -Überwachung von DatAlert dem Sicherheitsteam der Bank, die Situation sofort in den Griff zu bekommen.

Von Vorteil ist zudem, dass sich Varonis nahtlos in die SIEM-Lösung der Bank (LogRhythm) integriert. Varonis liefert kontextbezogene und unstrukturierte Bedrohungsinformationen an LogRhythm, das seine Fähigkeiten zur Mustererkennung und zum Log-Management auf die Daten anwendet.

Das Ergebnis sind detailreiche Bedrohungserkennungsfunktionen, die das Sicherheitsteam der Bank bereits bei den frühesten Warnzeichen verdächtiger Benutzeraktivitäten alarmieren, noch bevor sie sich möglicherweise zu einer umfangreiche Datenverletzung entwickeln können.

> „Die Warnfunktionen zeigen uns, wenn ein Benutzer massenweise Daten löscht oder mit dem Bereinigen eines Verzeichnisses beginnt, das möglicherweise von jemand anderem benötigt wird. Wir haben bislang noch keine Anzeichen von Angriffen gesehen, aber es ist beruhigend, die täglichen Protokolle durchsehen zu können und zu erkennen, dass legitime Benutzer ehrliche Fehler machen, wie z.B. die falsche Eingabe eines Passworts."

3. Edge bietet zusätzliche Sicherheit bei Remote-Anmeldungen über VPNs

Wenn Remote-Mitarbeiter Pulse oder Palo Alto verwenden, um sich mit dem Unternehmensnetzwerk der Bank zu verbinden, analysiert Edge die Metadaten aus den VPNs und stellt sie in den richtigen Kontext, um Login-Probleme und verräterische Anzeichen für Angriffe auf den Netzwerkrand zu erkennen.

Dieser Einblick ist möglich, weil Edge die Perimeteraktivitäten mit anderen Datenströmen (wie Datei, E-Mail und Active Directory) kombiniert. Wenn man die typischen Zugriffsaktivitäten, die Geolokalisierung und die Mitgliedschaft in Sicherheitsgruppen eines Benutzers zugrunde legt, ist es einfach, den Unterschied zwischen einem Benutzer, der sein Kennwort vergessen hat, und einer potenziellen, gerade stattfindenden Datenverletzung zu erkennen.

Varonis stellt automatisch Informationen aus beiden VPNs zu umfassenden Protokollen zusammen, so dass der Anwendungsadministrator Probleme bei der Anmeldung von Remote-Benutzern bereits im Vorfeld identifizieren kann.

> „Ich kann Protokolle aus unseren VPNs direkt in Varonis ziehen. Jetzt erhalten wir jeden Morgen um 10 Uhr Berichte über verdächtige Logins direkt in unsere E-Mail-Postfächer zugestellt. Das ist ausgesprochen hilfreich, da über 75 Prozent der Mitarbeiter aufgrund der aktuellen Weltlage aus der Ferne arbeiten."

„Varonis gibt mir die Möglichkeit, jederzeit zu wissen, was in unseren Dateisystemen vor sich geht. Ich muss mich nicht darauf konzentrieren, weil die Software das für mich erledigt.“

Ergebnisse

Sichere Homeoffice-Arbeitsplätze

Mit Varonis kann der leitende Anwendungsadministrator jeden Tag mit der Durchsicht eines umfassenden Berichts beginnen, der die Aktivitäten des Vortags aufschlüsselt. Diese Möglichkeit hatte einen enormen Einfluss auf die Sicherstellung der Workflow-Effizienz bei der starken Ausweitung von Homeoffice-Arbeitsplätzen.

> „Wenn ich merke, dass eines unserer VPNs langsamer wird, rufe ich über Varonis einen Bericht über die Benutzeraktivitäten ab. Anhand dieses Protokolls kann ich sehen, wo der Engpass liegt, und schnell eine Lösung finden.“

Die Diagnose und Lösung ähnlicher Probleme in der Zeit vor Varonis war enorm zeit- und ressourcenaufwändig. Jetzt ist dies im Handumdrehen erledigt.

> „Vor Varonis haben wir unser internes Sicherheitsteam die Ereignisprotokolle aller Server durchsuchen lassen, über die sie verfügen. Mit Varonis ist es so, als ob ein zusätzlicher Mitarbeiter sofort eine Aufgabe erledigen würde, für die früher ein Team von fünf Personen einen ganzen Tag brauchte.“

Die Tatsache, dass derzeit die meisten Mitarbeiter von Zuhause aus arbeiten, beunruhigt weder den leitenden Anwendungsadministrator noch die Geschäftsführung. Sie wissen, dass Varonis ihre sensiblen Daten kontinuierlich überwacht und einen Least-Privilege-Ansatz durchsetzt. Auch wenn sie nicht im Büro sind.

> „Jedes Unternehmen braucht Varonis. Es öffnet einem die Augen, wenn man sieht, wie viele private Daten sich im Netzwerk befinden und wie viele Kopien derselben Daten existieren. Wenn man für diese Informationen blind ist, steuert man bereits auf eine Katastrophe zu.“

Zusätzlich stehen die Varonis-Supportteams der Bank stets zur Seite und helfen ihr, die Sicherheit der Homeoffice-Arbeitsplätze zu gewährleisten und die neuen Sicherheitsherausforderungen zu meistern. Darüber hinaus bietet Varonis kostenlose Incident-Response-Dienste und Bedrohungsüberwachung u.a. für O365-Teams, VPN und Active Directory an.

Schützen Sie die Homeoffice-Arbeitsplätze Ihrer Mitarbeiter.

Lassen Sie sich durch unsichere Netzwerke und Geräte nicht davon abhalten, zum „business as usual“ (nur von Zuhause aus) zurückzukehren.

FORDERN SIE EINE DEMO AN