CASE STUDY

Finanzdienstleistungsunternehmen Erhält Einen Realitätscheck Für Seine Assets.

Echtes, umfassendes Asset-Management von einem vertrauenswürdigen, engagierten Anbieter zur Lösung von Kundenproblemen

Kundenprofil

Globales Finanzdienstleistungsunternehmen

Branche

Finanzdienstleistungen

IT-Umgebung

Rund 500 Mitarbeiter in 15 Niederlassungen weltweit, die auf allen Kontinenten vertreten sind

Introduction

Dieses globale Finanzdienstleistungsunternehmen, das seit Jahrzehnten im Geschäft ist, hatte Schwierigkeiten seinen wachsenden Bestand an digitalen Ressourcen zu verwalten. Dies lag zum Teil an der mangelnden Sichtbarkeit seiner wachsenden Cloud-Infrastruktur und seiner Remote-Mitarbeiter, die beruflich viel unterwegs sind. Das Unternehmen kämpfte mit uneinheitlichen und oft widersprüchlichen Daten aus einem Dutzend Quellen und hatte Schwierigkeiten damit, einen besseren Überblick über seine digitale und physische Umgebung zu erhalten. Nach der Implementierung von Armis war das Finanzdienstleistungsunternehmen in der Lage, einen klaren, umfassenden Überblick über seine Assets zu erhalten und Einblicke in Schwachstellen zu gewinnen. Vor allem aber erwies sich Armis als vertrauenswürdiger, kooperativer Partner, der sich der Lösung der Probleme des Unternehmens und der Bewältigung seiner Sicherheitsbedenken widmete.

Bewältigung der Sicherheitsheraus-forderungen bei globalen Operationen.

Dieses schnell wachsende globale Finanzdienstleistungsunternehmen hat seinen Hauptsitz in den USA und verfügt über etwa 15 Niederlassungen weltweit. Viele der rund 500 Remote-Mitarbeiter sind häufig auf der ganzen Welt unterwegs, um mit Partnern und anderen Beteiligten zusammenzukommen. Außerdem nutzt das Unternehmen zahlreiche Cloud-Dienste und -Anwendungen.

In einer stark regulierten Branche wie der Finanzdienstleistungsbranche ist die Aufrechterhaltung strenger Sicherheitskontrollen zum Schutz der Privatsphäre und wertvoller Daten stets von größter Bedeutung.

Der Director of Security Engineering arbeitet täglich mit dem CISO zusammen, um die Sicherheit zu stärken und kontinuierlich zu verbessern. Er betrachtet das Asset-Management als kritische und wesentliche Grundlage für effektive Sicherheit. Jeden Tag prüft er mehrere Datenquellen von verschiedenen Produkten, die zeigen, wie ihre Assets interagieren. Das Problem ist, dass die Daten sehr viele Diskrepanzen aufweisen. Es gab keine eindeutige, zentrale Informationsquelle darüber, was sich im Netzwerk des Unternehmens befand.

„Unsere größte Herausforderung bestand darin, zu verstehen, wie unsere Realität aussieht, d. h. was wir aus der Perspektive der Assets haben. Wie können wir all diese Unterschiede konsolidieren und in Einklang bringen?“, fragt der Director of Security Engineering.

Verständnis für die Bedeutung der Assetinventur in jedem Sicherheitsrahmen.

Der CISO des Unternehmens erklärt: „Die Assetinventur ist das Erste, was man im Griff haben muss, um gut für Sicherheit zu sorgen.“ Er fügt hinzu: „Wenn Sie versuchen, ein Schlachtfeld, eine Burg oder Ihr Zuhause zu schützen, müssen Sie wissen, wo alle Türen und Zugangswege sind sowie alle Schwachstellen kennen, damit Sie diese Sicherheitslücken schließen können. Und wenn Sie Ihre Gegenmaßnahmen einsetzen, müssen Sie wissen, dass sie einsatzbereit sind und so funktionieren, wie sie sollen. In einer komplexen und verteilten Organisation wie der unseren ist es von entscheidender Bedeutung, dass man dies im Blick hat.“

Diesem Gedankengang folgend, traf das Unternehmen die strategische Entscheidung, eine sichere „Umgebung“ um seine Geräte und Benutzer herum aufzubauen, wobei die starke Unternehmensnetzwerkumgebung beibehalten wurde. Doch wie der CISO betont, ist die Konzentration auf die Sicherheit der Netzwerkumgebung ein „fehlerhaftes Modell“, da sich die Umgebung durch die Cloud, das Arbeiten von zu Hause aus und andere technologische Trends, aufgelöst hat. Das Sicherheitsteam musste relevante Details über Benutzer und Geräte erhalten – wo sie sich aufhalten, welche Software sie verwenden, wo sie surfen – und dann Telemetriedaten über all diese Informationen sammeln.

„Wir haben einen langen Weg hinter uns, um Datenquellen mit unserer zentralen Protokollierungsplattform zu verbinden. Wir fühlten uns langsam sicher, dass wir alles im Griff hatten, aber wir konnten es nicht beweisen. Das war der Zeitpunkt, an dem wir begannen, den Weg der Assetinventur einzuschlagen“, erklärt der CISO.

Herausforderungen

- Beherrschung des Asset- Managements in der gesamten Organisation
- Diskrepanzen in den Daten ausnutzen, um ein wahres Bild der Umgebung zu erhalten
- Erfassung von Telemetriedaten über Remote-Benutzer und ihre Geräte
- Verstehen von Schwachstellen und deren Auswirkungen für die Sicherheitslage der Organisation
- Identifizierung eines Anbieters, mit dem die Organisation eng zusammenarbeiten kann, um Probleme zu lösen

Lange Zeit glaubte der CISO, dass das Asset-Management ein Sicherheitsproblem sei, das nie gelöst werden würde. Das Sicherheitsteam untersuchte eine Reihe von Lösungen für das Asset- Management und entschied sich schließlich für Armis.

“„Jede Methodik, die ich mir ansah, war schmerzhaft. Und ich sah, dass keines der neuen Tools so funktionierte, wie es sollte. Die Geschwindigkeit, mit der neue Arten von Assets auftauchen, macht es wirklich schwer, sie zu entdecken, zu kategorisieren und zu inventarisieren“, stellt er fest. „Was ich bis jetzt von Armis gesehen habe, gibt mir Hoffnung. Das liegt daran, dass Armis die Assets ganzheitlicher betrachtet. Wir freuen uns darauf, mit Armis auf die Reise zu gehen.“

Partnerschaftliche Angelegenheiten.

Bei der Entscheidung spielten mehrere Faktoren eine Rolle. Neben dem günstigen Preis und den Fähigkeiten der Lösung war die Beziehung des CISO zum Armis-Team ein entscheidendes Unterscheidungsmerkmal. In seiner vorherigen Position bei einem anderen Unternehmen war der CISO der erste Kunde von Armis in den USA, und in dieser Zeit hat er eine enge Zusammenarbeit mit dem Armis-Team aufgebaut. Wie er sagt: „Die Beziehung ist genauso wichtig wie das Produkt. Und für uns ist das wirklich wichtig. Das ist etwas, was wir von den Konkurrenten nicht bekommen haben, die uns nur als eine Nummer betrachteten, nur eine weitere Kunden-ID in einer langen Liste von Kunden-IDs.“

Als der CISO die Anbieter von Asset-Management-Lösungen auswertete, legte er den Anbietern eine Liste mit den Anforderungen vor, die er und sein Team erfüllen wollten, mit den Dingen, die jede Lösung gut kann und mit den Dingen, die sein Team benötigte, die aber nicht in den Produkten enthalten waren.

„Als wir mit Mitbewerbern sprachen, hatten sie keine wirklichen Antworten oder Zusicherungen, dass sie uns mit dem versorgen würden, was wir wirklich brauchten“, bemerkt der CISO. Er stellte fest, dass andere Partnerschaften, die er mit Anbietern einzugehen versuchte, meistens nicht zum beiderseitigen Vorteil funktionierten.

Ergebnisse der Einführung von Armis

- Zusammenführung und Abgleich von Daten aus verschiedenen Quellen auf einer einzigen, zentralisierten Plattform für mehr Genauigkeit
- Eine gute Assetinventur, die einen Überblick über die Assets von Benutzern, Geräten und Netzwerken bietet
- Bereitstellung grundlegender Daten, die in Zukunft Verhaltensanalysen ermöglichen können

Die meisten Anbieter, so behauptet er, sind nur an einem Verkauf interessiert und es gibt kaum eine echte Interaktion oder Verpflichtung, die über eine reine Anbieter-Kunden-Beziehung hinausgeht.

Bei Armis war das ganz anders. Als der CISO mit seinen Ideen an Armis herantrat, krempelten die Teammitglieder von Armis eifrig die Ärmel hoch und arbeiteten mit seinem Team zusammen, um ihre Probleme zu lösen und ihre Bedenken zu berücksichtigen.

„Armis sah dies als eine Gelegenheit, das Produkt zu verbessern und unser Wissen und unsere Erfahrung zu nutzen. Und wir sahen es als eine Möglichkeit, mit einem Partner zusammenzuarbeiten, der uns auf diesem Weg begleiten würde“, bemerkt der CISO. „Armis erkannte den Wert der Ideen, die wir einbrachten, und das spiegelte sich in der Zusammenarbeit mit uns und in der Preisgestaltung wider. Es war eine wirklich gute Entscheidung. Jetzt, 12 Monate später, habe ich das Gefühl, dass wir die richtige Entscheidung getroffen haben.“

Integrationen tragen zu einer ganzheitlichen Betrachtung der Assets bei.

Ein wichtiger Vorteil von Armis ist seine Fähigkeit, sich leicht in andere Lösungen zu integrieren. Daten fließen in Armis von ca. 12 Quellen: von traditionellen Quellen, wie Microsoft Active Directory und der Microsoft Azure-Cloud-Plattform, und auf der Netzwerkseite von Switches und Firewalls. Armis kann auch agentenlose Geräte problemlos erkennen. Die Aggregation großer Datenmengen an einem Ort ist ein großer Gewinn für das Team.

„Kein anderer Anbieter ist in der Lage, die Lücke zwischen den Datenquellen auf Netzwerkebene und den Datenquellen auf Assetebene zu schließen“, sagt der Director of Security Engineering. „Armis leistet wirklich großartige Arbeit bei der Verbindung dieser beiden Bereiche.“

Das Finanzdienstleistungsunternehmen verfügt nun über eine Übersicht über die Assets, die eng mit der von ihm verwendeten Matrix übereinstimmt, die die NIST-Kategorien für Sicherheitsvorgänge den Assets zuordnet.

Ergebnisse der Einführung von Armis

- Warnung, wenn neue Geräte mit dem Netzwerk verbunden werden und die Schutzmaßnahmen nicht installiert sind, nicht optimal laufen oder nicht richtig konfiguriert sind
- Enge, kooperative Beziehung zu einem betreuenden Anbieter, was zu einer schnelleren Problemlösung und zusätzlichen Produktverbesserungen führt

Die Matrix nennt fünf Assettypen: Geräte, Netzwerke, Benutzer, Daten und Anwendungen. Der CISO merkt an, dass sich die meisten Lösungen zur Assetinventur hauptsächlich auf Geräte und nur selten auf die anderen Kategorien konzentrieren: „Wir waren daran interessiert, Einblick in alle fünf Anlagekategorien zu bekommen, denn das ist was Assetinventur bedeutet. Mit Armis erhalten wir eine ganzheitliche Sicht auf die Assets in den meisten Kategorien. Wir können die Daten sehen und sie an einem Ort entdecken."

Die Stärke und das Potenzial der Armis-Analytik.

Ein weiterer Vorteil von Armis ist die Analyse auf Netzwerkebene. Der Director of Security Engineering ist beeindruckt von der Art und Weise, wie Armis Informationen auf der Basis von Serviceniveau, der Datenverkehrsebene und von Geräteverbindungsniveau anzeigt. Und es geht sogar noch weiter, indem es zeigt, wie sich die Geräte auf der Switch-Ebene mit dem Netzwerk verbinden.

Für die Zukunft plant der Director of Security Engineering die Verwendung von Armis für die Analyse auf Geräteebene. Außerdem plant er, die Technologie des maschinellen Lernens in Kombination mit Armis-Daten zu nutzen, um Analysen des Verhaltens auf Verbindungsebene zu erstellen.

„Diese Art von Daten können wir nicht einfach von anderen Anbietern erhalten. Wir sind zuversichtlich, dass wir dieses Projekt in der Zukunft realisieren können. Armis bietet einen genauen und reichhaltigen Datensatz, der bereits aggregiert ist, sodass ich weiß, dass wir viel mehr tun können als das, was wir im Moment tun – und ich bin davon begeistert", erklärt er.

„Armis ist viel mehr als ein agentenloses Asset-Management-Tool – es ist eine Mindmap, die uns zeigt, wie unsere Assets miteinander verbunden sind und wie sie sich verhalten, und das gefällt mir sehr. Armis ist viel leistungsfähiger als andere Wettbewerber, die wir kennengelernt haben."

Der Director of Security Engineering
Finanzsektor

Zusätzlich, wenn mehr Mitarbeiter wieder vor Ort arbeiten, wird das Team eine weitere Funktion von Armis nutzen, nämlich die Benachrichtigung über neue Geräte, die dem Netzwerk beitreten, über noch nie zuvor gesehene Anwendungen auf einem bestimmten Gerät und über den Status von Sicherheitsmaßnahmen, die möglicherweise nicht korrekt ausgeführt werden oder gar nicht auf dem Gerät installiert sind. Der CISO drückt es so aus: „Es reicht nicht aus, zu wissen, dass ich etwas habe. Ich muss wissen, ob es in gutem Zustand ist und ob es aktualisiert werden muss. Armis leistet in dieser Hinsicht großartige Arbeit und wir planen, in naher Zukunft davon Gebrauch zu machen."

Der Director of Security Engineering ist davon überzeugt, dass Armis dem Unternehmen eine solide Grundlage bietet, auf der sein Team in Zukunft eine stabilere Sicherheitsstrategie und -infrastruktur aufbauen kann.

„Armis ist viel mehr als ein agentenloses Asset-Management-Tool – es ist eine Mindmap, die uns zeigt, wie unsere Assets miteinander verbunden sind und wie sie sich verhalten, und das gefällt mir sehr. Armis ist viel leistungsfähiger als andere Wettbewerber, die wir kennengelernt haben", sagt er abschließend.