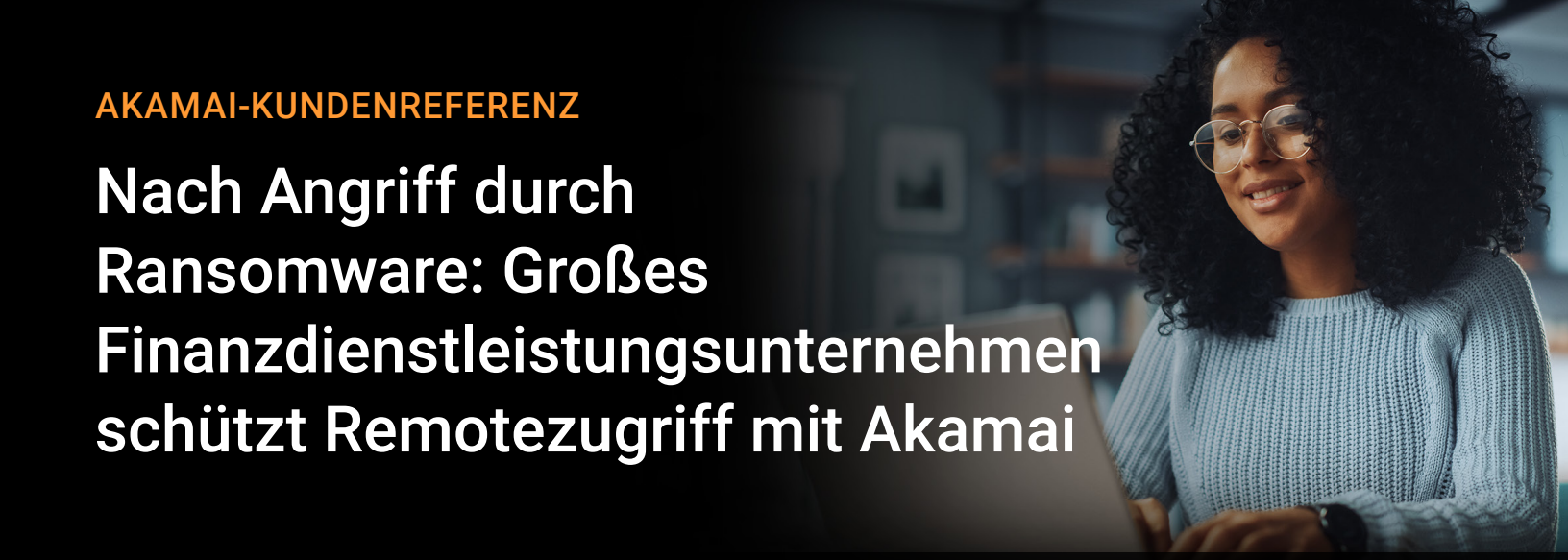
AKAMAI-KUNDENREFERENZ

Nach Angriff durch Ransomware: Großes Finanzdienstleistungsunternehmen schützt Remotezugriff mit Akamai



Umfassende Netzwerktransparenz

Schnelle Einführung von Richtlinien

Sicherer Remotezugriff für Mitarbeiter

Der Kunde

Ein großes Finanzdienstleistungsunternehmen mit Sitz in Brasilien

Die Herausforderung

Vermehrter Remotezugriff

Wie bei vielen anderen Unternehmen führte die Coronapandemie auch bei diesem Finanzdienstleister zu einem erhöhten Bedarf an Remotezugriff: Ein Großteil der IT-Mitarbeiter der Bank wechselte ins Homeoffice, wo sie mit vom Unternehmen verwalteten Geräten arbeiteten. Als Nutzer plötzlich hauptsächlich von außerhalb des sicheren Unternehmensnetzwerks auf die Daten und Anwendungen zugriffen, die sie für ihre Rolle benötigten, wuchs die Angriffsfläche des Unternehmens rapide.

Erfolgreicher Ransomware-Angriff

Kurz nach der Umstellung aufs Homeoffice traf ein erfolgreicher Ransomware-Angriff eine kritische Oracle-Cloud-Datenbank der Bank, die – wie sich später herausstellen sollte – auf eine VDI-Umgebung zurückzuführen war. Sicherheits- und IT-Abteilung wussten, dass sie schnell handeln mussten, um den Verlust vertraulicher Finanzdaten zu begrenzen. Außerdem erkannten sie, dass, wenn sie den ursprünglichen Angriffsvektor nicht bestimmen und schützen konnten, ein reales Risiko bestand, dass sich die Ransomware lateral auf die Backupserver und die Produktionsumgebung des Unternehmens ausbreitete. Und in diesem Fall wäre die Bank definitiv von erheblichen Daten- und finanziellen Verlusten betroffen.

Auswahl der richtigen Lösung

Akamai Guardicore Segmentation war bereits in anderen Bereichen der Bank im Einsatz. Vor dem Ransomware-Angriff war die Plattform für die Verwaltung und Durchsetzung der Segmentierungsrichtlinien für mehr als 23.000 Server zuständig – mit Workloads, die auf On-Premises-, virtuelle, Bare-Metal- und VDI-Infrastrukturen sowie Azure- und OpenShift-Containerumgebungen verteilt waren.

Large Financial Services Company

Branche
Finanzdienstleistungen

Lösung
Akamai Guardicore Segmentation

Die wichtigsten Vorteile

- Verringert die Ausbreitung von Ransomware durch laterale Netzwerkbewegung
- Bietet detaillierte Transparenz der Netzwerkvorgänge
- Schützt den Remotezugriff durch Segmentierung von VDI-Umgebungen
- Ermöglicht eine schnelle Reaktion auf Vorfälle

Akamai

Als softwarebasierte Segmentierungslösung wurde Akamai Guardicore Segmentation bereits zuvor für mehrere Sicherheits- und Compliance-Initiativen der Bank eingesetzt, darunter die Verwaltung des Jumpbox-Zugriffs für Administratoren sowie die SWIFT-Anwendungssegmentierung. Da das Reaktionsteam die Erfolgsbilanz der Plattform in Sachen Transparenz und schnelle Richtlinieneinführung kannte, nutzte es schnell die Funktionen von Akamai Guardicore Segmentation, um den Angriff zu bewältigen.

Vorteile von Akamai Guardicore Segmentation

Transparenz auf Prozessebene

Über die Plattform untersuchte das Reaktionsteam der Bank Vorgänge im Kommunikationsverlauf. Sie verfolgten die erste Einführung der Ransomware bis hin zur Remote-VDI-Verbindung eines Datenbankadministrators, die mit einer Oracle-Cloud-Datenbank kommunizierte.

Schnelle Einführung von Richtlinien

Nachdem der Angriffsvektor identifiziert war, führte das Team eine beschleunigte VDI-Segmentierung durch, die oberste Priorität hatte. Der Prozess der Richtlinienplanung begann an einem Samstag und umfasste die Transparenzfunktionen von Akamai Guardicore Segmentation, um potenzielle Richtlinienanforderungen zu ermitteln. Am darauffolgenden Dienstag verfügte die Bank über durchsetzbare Richtlinien für die mehr als 3.000 VDI-Verbindungen zu Oracle Cloud.

Wiederherstellung nach Ransomware

Das Team implementierte Agents von Akamai in der Backupanwendung und konfigurierte das Anwendungs-Ringfencing, um genau – bis hinunter zur Prozessebene – zu definieren, welche Elemente mit dem Asset kommunizieren können. Dann wurde die Anwendung im angegriffenen Bereich bereitgestellt, wobei die weitere Verbreitung der Ransomware mithilfe globaler Verweigerungsregeln verhindert wurde.

Um das zusätzliche Risiko durch Remotezugriff von Mitarbeitern zu verringern, wurden außerdem Richtlinien für die beiden VDI-Lösungen festgelegt, die Callcenter-Mitarbeiter verwendeten. So wurde die nicht autorisierte laterale Netzwerkbewegung zwischen Endpunkten in der Bank weiter verhindert.

Die Durchsetzung von Segmentierungsrichtlinien in nur drei Tagen ermöglichte es dem Finanzdienstleister, die Auswirkungen des Ransomware-Vorfalls drastisch zu reduzieren und die Sicherheit des Remotezugriffs in Zukunft deutlich zu verbessern.

> Die Transparenz von [Akamai Guardicore Segmentation] war für uns wie ein heller Lichtstrahl, der die Dunkelheit vertrieben hat.
>
> Leiter der Infrastruktursicherheit bei einem großen Finanzdienstleistungsunternehmen

Weitere Informationen finden Sie unter akamai.com/guardicore.