splunk>

CASE STUDY

Die DKB stärkt das Vertrauen ihrer Kunden und reagiert mit Splunk 90 % schneller auf Bedrohungen

Zentrale Herausforderungen

Als die DKB in die Cloud migrierte, hatte das Kreditinstitut Mühe mit dem Monitoring seiner komplexen Systeme und der schnellen Erkennung von Kompromittierungen

Wichtige Ergebnisse

Durch die Einführung von Splunk erhielt die DKB vollständige Transparenz in ihre Infrastruktur, verzeichnete weniger falsch positive Warnmeldungen und beschleunigte ihre Erkennungen und Untersuchungen um 90 %.

DKB
Deutsche Kreditbank AG

Branche: Finanzdienstleister

Lösungen: Security

Vertrauen ist die wichtigste Währung in der Finanzwelt.

Die Deutsche Kreditbank (DKB) ist die zweitgrößte Direktbank Deutschlands. Ihr vertrauen über 4,5 Millionen Menschen, wenn es um Girokonten, Kredite, Finanzierungen, Kreditkarten, Sparguthaben und andere Finanzprodukte geht. Um weiterhin nahtlose Transaktionen, Zahlungen und Prozesse zu gewährleisten, ist die DKB in die Cloud migriert und hat verstärkt in Cybersicherheit investiert. Nachdem das Unternehmen Splunk zunächst über einen Managed-Service-Anbieter bezog, nutzt es die Plattform für einheitliche Sicherheit und Observability heute direkt.

Der Wechsel in die Cloud erwies sich komplexer als erwartet. Die DKB brauchte eine Lösung, mit der sie Einblick in alle Bereiche ihrer hybriden Infrastruktur bekam, von den einzelnen Security-Tools bis hin zu den Cloud- und On-premises-Umgebungen. Und die Bank wollte vollständige Transparenz, um Probleme sofort zu erkennen – denn ein Ransomware-Angriff oder andere Cybersecurity-Vorfälle würden nicht nur die Stabilität der Systeme gefährden, sondern das Vertrauen der Kundschaft aufs Spiel setzen.

Ergebnisse

- 90 % schnellere Bedrohungserkennung und Untersuchungen
- Mehr Transparenz bei allen Tools und Umgebungen
- Weniger falsch positive Warnmeldungen

Keine toten Winkel mehr

Die DKB nutzte Splunk zunächst für Security-Monitoring und Incident-Management sowie in jüngster Zeit auch für Bedrohungsinformationen. Die Bank hatte zwar schon eine Vielzahl unterschiedlicher Sicherheitstools im Einsatz, konnte deren Daten mit Splunk aber vollständig aggregieren und durchsuchbar machen.

Und damit hat die DKB Zeit gespart – sogar eine ganze Menge. Andreas Hennich, Head of IT-Security bei der DKB, sagt: „Der größte Vorteil, den uns Splunk gebracht hat, ist Transparenz. Wir sehen alles. Wir sehen jede Warnmeldung, die in den einzelnen Sicherheitstools und in allen Umgebungen auftaucht, die wir in der Cloud und in der On-premises-Umgebung haben. Weil wir alles an einem Ort haben, können wir diese Daten viel schneller untersuchen und nutzen."

Keine unerkannten Bedrohungen

Durch eine schnellere Reaktion auf Warnmeldungen konnten die DKB-Teams außerdem die Netzwerksicherheit verbessern. Zuvor gab es einfach zu viele Alerts abzuarbeiten, die obendrein an unterschiedlichen Stellen aufschlugen. Das führte zu Verzögerungen und übersehenen Warnungen. „Früher durchsuchten wir die Log-Dateien nach Netzwerkproblemen, aber das war langwierig, und es konnte leicht passieren, dass wir Warnmeldungen übersahen. Jetzt, da wir alle Infrastrukturkomponenten mit Splunk als SIEM verbunden haben, sind viele verschiedene Vorgänge der Netzwerksicherheit schnell sichtbar, und zwar in einer zentralen, korrelierten Datenbank“, erklärt Hennich. „Im Fall einer Kompromittierung können wir die Warnmeldungen schneller wahrnehmen und schneller reagieren.“

Bei bestätigten Bedrohungen konnte die DKB die Zeit für die Untersuchung und Behebung um 90 % reduzieren, wie Hennich berichtet. „Bevor wir Splunk hatten, mussten wir die einzelnen Log-Dateien durchsuchen, zusätzliche Daten finden, Suchanfragen schreiben und so weiter. Mit Splunk geht das viel schneller.“

„Jetzt, da wir alle Infrastrukturkomponenten mit Splunk als SIEM verbunden haben, sind viele verschiedene Vorgänge der Netzwerksicherheit schnell sichtbar, und zwar in einer zentralen, korrelierten Datenbank. Im Fall einer Kompromittierung können wir die Warnmeldungen schneller wahrnehmen und schneller reagieren.“

Andreas Hennich, Head of IT-Security, DKB Service GmbH

24-splunk- 133169 - EMEA DKB Customer Story-102