Die CPP Group setzt für die Sicherheit der Kreditkartendaten ihrer Kunden auf Forcepoint

Die CPP Group, ein partnerorientiertes, globales Produkt- und Dienstleistungsunternehmen, ist auf Finanzdienstleistungen und Versicherungen spezialisiert. Sie setzen auf die DLP-Lösung von Forcepoint, da sie die neuen Compliance-Anforderungen in globalen Märkten erfüllen und gleichzeitig in die Cloud wechseln möchten.

Die CPP Group trägt die Verantwortung für die Sicherheit großer Mengen hochsensibler Daten. Diese stammen zum einen von Direktkunden (v. a. im Bereich Lebensversicherungen) und zum anderen von Banken und Kreditkartenunternehmen, die für ihre Dienstleistungen (Kartenschutz und Betrugsprävention) auf die CPP Group vertrauen. Eine flexible Datensicherheits-Infrastruktur ist für die Sicherheit von dezentralisierten, in der Cloud verteilten Daten in unterschiedlichen Ländern von wesentlicher Bedeutung.

KUNDENPROFIL:
Die CPP Group entwickelt und vertreibt Produkte in den Bereichen Versicherung und Kreditkartenschutz für Verbraucher.

BRANCHE:
Finanzdienstleistungen

HAUPTSITZ:
Vereinigtes Königreich

PRODUKT(E):
- Forcepoint Web Security Cloud
- Forcepoint Data Loss Prevention

Die CPP Group wurde im Jahr 1980 im Vereinigten Königreich gegründet und erwirtschaftet heute ca. 65 % ihres Umsatzes in Indien. Den Großteil machen hierbei die Bereiche Kartenschutz, Garantieverlängerung und Versicherungen für Mobiltelefone aus. Durch die geografische Verlagerung der geschäftlichen Aktivitäten war das IT-Sicherheitsteam der CPP Group mit neuen Herausforderungen konfrontiert.

Insbesondere in den Bereichen Kartenschutz und Telefonversicherung besteht ein erhebliches Sicherheitsrisiko: Hier geht es um die Sicherheit sensibler Finanzdaten von Kunden bei Drittanbietern für Zahlungskarten, z. B. Banken und Kreditkartenunternehmen. Da die CPP Group ihren Hauptsitz im Vereinigten Königreich hat, muss der Umgang mit diesen Daten gemäß der in der EU geltenden Datenschutz-Grundverordnung (DSGVO) erfolgen. Zusätzlich müssen die geschäftlichen Aktivitäten dem Payment Card Industry Data Security Standard (PCI DSS), der ISO 27001 und den nationalen Datenschutzstandards der Länder entsprechen, in denen das Unternehmen agiert.

So wurden in Indien kürzlich Gesetze erlassen, denen zufolge im Land tätige Finanzdienstleistungsunternehmen Daten wie personenbezogene Zahlungskarteninformationen lokal speichern müssen. Auch andere Länder, in denen die CPP Group tätig ist (z. B. die Türkei), erarbeiten derzeit ähnliche Regularien für Finanzdaten.

Wie die neuen Bestimmungen zur Datenhoheit in Indien erfüllt werden können

Laut Patrick Viner, IT Operations Manager bei der CPP Group, stand das Unternehmen vor der Herausforderung, die Daten lokal zu sichern und gleichzeitig eine sichere, bedarfsorientierte Datenübertragung zwischen dem Hauptsitz im Vereinigten Königreich und den internationalen Niederlassungen zu gewährleisten.

Bislang hatte das Unternehmen alle Kartendaten in seinem britischen Rechenzentrum gehostet. Die Verwaltung der Datenbanken erfolgte somit gemäß den geltenden britischen Richtlinien. Nun müssen diese Daten jedoch über eine AWS-Cloud-Umgebung sowie lokal im Vereinigten Königreich, in Indien und an anderen globalen Standorten gesichert werden, während weiterhin die Datenbankrichtlinien des Vereinigten Königreichs gelten und angewendet werden.

Reibungslose Arbeitsabläufe aufrechtzuerhalten und gleichzeitig „der zunehmend komplexen Datensicherheitspolitik gerecht zu werden, da immer mehr Länder auf eine Datenspeicherung innerhalb des Landes bestehen – das ist ein Balanceakt", so Viner. „Derzeit läuft bei uns ein verhältnismäßig großes Projekt: Wir entwickeln eine Plattform, die diesem Modell gerecht wird und mit der wir alle Daten in den Ländern speichern können, in denen wir Dienstleistungen für Zahlungskarten anbieten."

Überführung lokaler Sicherheitsstandards in die Cloud

Die CPP Group vertraut bereits seit vielen Jahren auf die lokalen Web Security-Appliances von Forcepoint – für einen sicheren Internet-Datenverkehr über VPN und Web-Proxys im Rechenzentrum im Vereinigten Königreich. Da das Tagesgeschäft in zunehmendem Maße außerhalb des Vereinigten Königreichs erfolgte (insbesondere in Indien), führte diese Methode zur Verteilung des Datenverkehrs zuletzt vermehrt zu Verzögerungen bei der Übertragung von Informationen und zu Produktivitätseinbußen.

Um diesem Produktivitätsverlust entgegenzuwirken und gleichzeitig die Sicherheit der kundenbezogenen Daten sowie Compliance und Business Continuity zu gewährleisten, beschloss das Unternehmen die Umstellung auf Cloud-basierte IT-Abläufe und ging hierfür eine Kooperation mit Forcepoint ein.

Herausforderungen

Die Verteilung des Datenverkehrs über das Rechenzentrum im Vereinigten Königreich führte vermehrt zu Verzögerungen und Produktivitätseinbußen.

Geschäftsaktivitäten in unterschiedlichen Ländern machten die Einhaltung unterschiedlicher Datensicherheitsstandards zwingend notwendig.

Strategie

Umstellung auf die Forcepoint Web Security Cloud zur Verbesserung des Datenverkehrs bei Gewährleistung der Datensicherheit.

Implementierung der DLP-Lösung von Forcepoint, die eine bessere Transparenz von Datenbewegungen bietet und die Einhaltung komplexer Vorschriften erleichtert.

„Zunächst gingen wir zu einer hybriden Architektur über. Diese beinhaltete den Einsatz von Web Security-Endpunkt-Clients in einigen der Länder, in denen wir Niederlassungen betreiben", so Viner. „Dann beschlossen wir, unser Rechenzentrum im Vereinigten Königreich aufzugeben und auf eine VPC-Umgebung (Virtual Private Cloud) umzustellen. Gleichzeitig entschied ich, die physischen Appliances ganz abzuschalten und vollständig in die Cloud zu wechseln. In den anderen Bereichen möchten wir nun nachziehen."

Forcepoint DLP ermittelt, welches Verhalten Daten gefährdet

Beim Testen der DLP-Lösung von Forcepoint wurden die eigenen Schwachstellen offenbar. So wurde dem Sicherheitsteam der CPP Group bewusst, dass Mitarbeiter und Geschäftspartner in Indien potenziell riskante Aktionen ausführen konnten, z. B. das unkontrollierte Versenden von Tabellenkalkulationen mit Kundendaten per E-Mail, wodurch sensible Daten in falsche Hände geraten können – versehentlich oder mit Absicht. Außerdem fiel dem Team auf, dass keine Vorkehrungen bestanden, die Mitarbeiter am Hochladen von Dateien mit Informationen zu potenziellen Neukunden auf ungesicherte Websites hinderten.

Mit Forcepoint DLP konnte die CPP Group potenziell riskantes Verhalten erkennen und gleichzeitig einem Produktivitäts-verlust entgegenwirken, der aus einer zeitintensiven und die Arbeitsabläufe unterbrechenden Verteilung des Datenverkehrs und Sicherheitskontrollpunkten resultieren würde.

Und damit nicht genug: Laut Viner konnte das Team die unternehmenseigene DLP-Richtlinie auf Grundlage der eigenen Erfahrungen mit den Benutzern anpassen. Die robuste, unmittelbar einsatzbereite Richtlinienbibliothek von Forcepoint DLP enthält vordefinierte Richtlinien, die den regionalen und branchenspezifischen Vorschriften entsprechen (z. B. DSGVO, PCI DSS). Weitere häufig verwendete vordefinierte Richtlinien basieren etwa auf den Vorschriften für geschützte Gesundheitsinformationen (Protected Health Information, PHI), z. B. dem HIPAA (Health Insurance Portability and Accountability Act) nach US-amerikanischem Recht oder den vom Basler Ausschuss für Bankenaufsicht erarbeiteten Finanzrichtlinien in der EU.

> „Dank Forcepoint sind Sicherheit und Produktivität bei uns keine Gegensätze mehr."
>
> **PATRICK VINER,** IT OPERATIONS MANAGER, CPP GROUP

Laut Viner konnte die CPP Group mit den entsprechenden DLP-Richtlinien kleinere Anpassungen vornehmen, so Fehlalarme reduzieren und gleichzeitig alle Compliance-Anforderungen erfüllen, ohne die Produktivität der Mitarbeiter zu beeinträchtigen.

„Wenn man die eigenen Richtlinien zu starr definiert, kann dies die Produktivität beeinträchtigen. Bleiben diese zu locker und das Unternehmen verfügt nicht über Überwachungs- oder Meldungsmechanismen, verursacht man Sicherheitslücken", so Viner. „Dank Forcepoint sind Sicherheit und Produktivität bei uns keine Gegensätze mehr."

Ergebnisse

Erkennung und Eliminierung riskanter Datenbewegungen; gleichzeitig werden Sicherheit und Produktivität in Einklang gebracht.