

KUNDENBERICHT

JTC verhindert personenbedingten Datenverlust mit Proofpoint Adaptive Email DLP

Der weltweite Professional Services-Anbieter verhindert fehlgeleitete E-Mails, falsche Dateianhänge sowie die Exfiltration vertraulicher Daten und gewährleistet die Einhaltung der DSGVO.

Herausforderung

- Schutz vertraulicher Kundendaten
- Verhinderung fehlgeleiteter E-Mails, falscher Dateianhänge und der Exfiltration von E-Mail-Daten, was mit den vorhandenen Tools nicht erreicht werden konnte
- Einhaltung der DSGVO-Anforderungen

Lösung

- Proofpoint Adaptive Email DLP

Ergebnisse

- Zuverlässiger Schutz vor personenbedingtem Datenverlust
- Reduzierung von False Positives für reibungslose Kommunikation
- Automatische Erkennung und Verhinderung von personenbedingtem Datenverlust

Das Unternehmen

Die im Jahr 1987 gegründete JTC Group ist ein weltweiter Professional Services-Anbieter, der sich auf Unternehmens- und Kundenbetreuung spezialisiert hat. Mit mehr als 1.200 Mitarbeitern in den USA, EMEA und Asien verfügt das Unternehmen über mehr als 180 Milliarden US-Dollar an betreutem Vermögen (AUA) und ist an der Londoner Börse sowie im FTSE 250 gelistet. JTC ist seit 2018 Kunde von Proofpoint.

Die Herausforderung

Verhinderung von versehentlichem und vorsätzlichem Datenverlust durch E-Mails

JTC musste personenbedingten Datenverlust verhindern, um Kundendaten zu schützen und die DSGVO-Anforderungen zu erfüllen. Besonders große Sorgen bereiteten Situationen, in denen Mitarbeiter vertrauliche Informationen an unbeabsichtigte Empfänger (fehlgeleitete E-Mails) oder nicht autorisierte Adressen (E-Mail-basierte Datenexfiltration) senden oder versehentlich als Anhang weitergeben (falsch angehängte Dateien).

Nach Meinung von Adam Jeffries, CIO der JTC Group, ließen sich diese Arten von Datenverlust mit der vorhandenen Sicherheitsumgebung nicht effektiv verhindern. Die E-Mail-DLP-Lösung von JTC war regelbasiert und inhaltsorientiert, sodass sie sensible Daten genau identifizieren und deren Weitergabe per E-Mail stoppen konnte. Dieser Ansatz funktionierte gut, wenn Mitarbeiter im Rahmen ihrer Arbeit keine vertraulichen Informationen per E-Mail an interne oder externe Parteien senden mussten. Wenn es jedoch dazu kam, erforderte das die Aufhebung der generellen Einschränkung für das Versenden vertraulicher Daten.

Zu diesem Zeitpunkt konnte die E-Mail-DLP-Lösung die Daten nicht mehr schützen, da es praktisch unmöglich war, Regeln und Richtlinien für die Vielzahl der Möglichkeiten zu erstellen, wie E-Mails mit sensiblen Daten falsch adressiert und Dateien falsch angehängt werden konnten. Und ohne Regeln konnte die E-Mail-DLP-Lösung nicht zwischen legitimer, unbeabsichtigter und böswilliger Datenweitergabe unterscheiden.

Angesichts dieser Lücken in der E-Mail-DLP-Abdeckung war Adam Jeffries sehr daran interessiert, eine umfassende Sicherheitslösung zu finden.

Die Lösung

JTC schützt Kundendaten mit Proofpoint Adaptive Email DLP vor menschlichen Fehlern und böswilligen Absichten

Adam Jeffries implementierte Proofpoint Adaptive Email DLP, da diese Lösung versehentlichen und absichtlichen Datenverlust durch E-Mails verhindert.

Dabei nutzt Proofpoint Adaptive Email DLP verhaltensbasierte KI und Machine Learning, detaillierte Inhaltsprüfungen und den Proofpoint Nexus® Relationship Graph, um kontinuierlich zu lernen und normales Anwenderverhalten zu ermitteln. Dabei wird erfasst, an wen Anwender typischerweise E-Mails senden, wie sie mit vertraulichen Daten umgehen, welche Arten von Anhängen sie häufig weitergeben und in welchem Kontext das geschieht.

Die Lösung nutzt dieses Wissen, um E-Mail-Empfänger intelligent zu überprüfen, Anhänge auf vertrauliche Daten sowie deren Relevanz für den Adressaten zu scannen und mithilfe von Kontextanalysen zu ermitteln, ob vertrauliche Daten an einen bestimmten Empfänger weitergegeben werden sollten. Proofpoint Adaptive Email DLP kann automatisch nicht autorisierte E-Mail-Adressen klassifizieren und erkennen, um Datenexfiltration an private oder nicht autorisierte Konten zu verhindern.

„Proofpoint nutzt sehr fortschrittliche Technologien. Die klassische Methode ist die Verwendung regelbasierter Tools, wo ein Mensch versucht, alle Angriffsmöglichkeiten zu bedenken und dann Regeln aufzustellen, um ihnen entgegenzuwirken. Bei Proofpoint geschieht das alles mithilfe fortschrittlicher Technologien und Machine Learning, das viel flexibler, gezielter und anpassbarer ist. Dadurch können wir enormen Verwaltungsaufwand sparen und Fehler vermeiden.“

Adam Jeffries
CIO, JTC Group



„Proofpoint Adaptive Email DLP verhindert effektiv fehlgeleitete E-Mails, hilft uns bei der Einhaltung von Compliance-Vorschriften und schult die Anwender kontinuierlich.“

Adam Jeffries,
CIO, JTC Group

Zudem deckt Proofpoint Adaptive Email DLP Abweichungen vom normalen Verhaltensmuster in Echtzeit auf und warnt Anwender vor einer bevorstehenden fehlgeleiteten E-Mail, einer falsch angehängten Datei oder einem Verstoß gegen die E-Mail-Richtlinie – noch bevor eine E-Mail gesendet wird. Deshalb können JTC-Mitarbeiter Fehler schnell selbst korrigieren, was die Sicherheitsteams entlastet und das Bewusstsein für E-Mail-Sicherheitsrisiken schärft.

Die Ergebnisse

Zuverlässiger Schutz ohne zusätzliche Belastung für das Sicherheitsteam

Mit Proofpoint Adaptive Email DLP konnte JTC erfolgreich fehlgeleitete E-Mails, falsch angehängte Dateien und an nicht autorisierte Konten gesendete vertrauliche Informationen verhindern. Das IT-Sicherheitsteam erhielt sogar ein Dankeschön von einem leitenden Verantwortlichen, der nur knapp vermeiden konnte, vertrauliche Inhalte an die falschen Empfänger zu senden.

„Proofpoint Adaptive Email DLP verhindert effektiv fehlgeleitete E-Mails, hilft uns bei der Einhaltung von Compliance-Vorschriften und schult die Anwender

kontinuierlich“, erklärt Adam Jeffries. „Nach der Implementierung waren wir selbst überrascht und fragten uns, was uns in den Jahren und Monaten vor der Bereitstellung von Proofpoint entgangen ist.“

Mit Proofpoint konnte das IT-Sicherheitsteam von JTC spezifische Plattformregeln festlegen, um automatisch Mitarbeiter zu blockieren, die vertrauliche Informationen an ein privates Konto zu senden versuchen. JTC berichtet, dass die Zuverlässigkeit von Proofpoint bei der Klassifizierung von Datenexfiltration per E-Mail hervorragend ist und in über drei Jahren zu nur zwei False Positives führte.

„Proofpoint nutzt sehr fortschrittliche Technologien. Die klassische Methode ist die Verwendung regelbasierter Tools, wo ein Mensch versucht, alle Angriffsmöglichkeiten zu bedenken und dann Regeln aufzustellen, um ihnen entgegenzuwirken. Bei Proofpoint geschieht das alles mithilfe fortschrittlicher Technologien und Machine Learning, das viel flexibler, gezielter und anpassbarer ist. Dadurch können wir enormen Verwaltungsaufwand sparen und Fehler vermeiden“, betont Jeffries.

proofpoint®

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: [LinkedIn](#)

Proofpoint ist eine eingetragene Marke bzw. ein registrierter Handelsname von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →