



Italienische Versicherung setzt zum Schutz vor Bedrohungen von innen und außen und zur Wahrung der Vertraulichkeit ihrer Mitarbeiterdaten auf Forcepoint

Eine der größten privaten Versicherungsgesellschaften Italiens schützt ihre sensiblen Finanzdaten und wahrt gleichzeitig die Datenschutzbestimmungen für Mitarbeiterdaten.

Die in Bologna ansässige Versicherung muss nicht nur sensible Kundendaten vor internen und externen Bedrohungen – im eigenen Netzwerk und in der Cloud – schützen, sondern auch die Vertraulichkeit ihrer Mitarbeiterdaten gewährleisten. Auf der Suche nach einer Lösung, die nicht nur diesen komplexen Anforderungen gerecht wird, sondern „passgenau“ auf sie zugeschnitten ist, entschied sich die Versicherung für Forcepoint Web DLP. Damit erfüllt die Datensicherheit des Unternehmen nun sowohl die Datenschutzverordnung als auch die Bestimmungen zum Arbeitnehmerdatenschutz. Ermöglicht wird dies durch eine Kombination von Forcepoint Web Security und Advanced Malware Detection, die alle Geschäftsbereiche zuverlässig vor externen Bedrohungen schützt.

KUNDENPROFIL:

Eine der größten privaten Versicherungsgesellschaften Italiens für Lebens-, Kfz- und Sachversicherungen

BRANCHE:

Finanzdienstleistungen

HAUPTSITZ:

Italien

PRODUKTE:

- › Forcepoint Web Security Hybrid mit DLP
- › Forcepoint Advanced Malware Detection

Dem italienischen Versicherungsunternehmen ist viel daran gelegen, sensible Kundendaten angemessen zu schützen. Als eine der größten Privatversicherungen Italiens muss das Unternehmen seine Daten vor internen und externen Bedrohungen gemäß den Vorgaben zum Datenschutz und Industriestandards schützen und gleichzeitig die Datenschutzbestimmungen der Regierung einhalten. Der Versicherer hat seinen Hauptsitz in Bologna, wo er den Schutz sensibler Kundendaten mit den italienischen Arbeitnehmerschutzgesetzen und den strengen Vorschriften der Stadt hinsichtlich der Persönlichkeitsrechte von Arbeitnehmern in Einklang bringen muss.

Das Unternehmen benötigt folglich eine Datensicherheitslösung, die sowohl die örtlichen Vorschriften für Unternehmen in Bologna als auch die Bestimmungen der Europäischen Union erfüllt, wie zum Beispiel die DSGVO. Dies konfrontiert den Versicherer mit einem heiklen Balanceakt: Er benötigt einen Schutz vor Datenverlusten (Data Loss Protection, DLP) und externen Bedrohungen, der weder zu invasiv noch zu locker, sondern „passgenau“ auf seine Bedürfnisse zugeschnitten ist.

Hinzu kommt, dass das Unternehmen gerade einen langwierigen, mehrjährigen Umstrukturierungsprozess durchlaufen hat, in dem es sein Lebens-, Kfz- und Sachversicherungsgeschäft konsolidiert hat. Seine Cyber-Sicherheitslösung muss sich an die häufig wechselnden Geschäftsbedingungen anpassen lassen, einschließlich eines zunehmenden Einsatzes von Cloud-Anwendungen und -Diensten. Unflexible Sicherheitsprodukte nach Schema F würden diesen Anforderungen nicht gerecht. Deshalb suchte das Unternehmen nach einer anpassungsfähigen Lösung, die mit der dynamischen Entwicklung des geschäftlichen und gesetzlichen Umfelds Schritt halten konnte.

Ein „passgenauer“ Schutz vor Datenverlusten

Der Schutz vor Datenverlusten verlangte von dem Unternehmen ein umsichtiges Vorgehen. Der Versicherer verwendete bereits Forcepoint Web Security, um die Mitarbeiter bei der Internetnutzung zu schützen, und beschloss daher, auch die integrierte DLP-Funktion einzuschalten.

Dadurch profitiert das Unternehmen von einer branchenführenden Verteidigungsstrategie gegen Datendiebstahl und kann künftig Datendiebstahlversuche erkennen und abwehren. Forcepoint Web DLP erkennt unter anderem die folgenden Bedrohungen:

- individuell verschlüsselte Uploads
- Datendiebstahl aus Kennwortdateien
- langsame Datenverluste (Drip-DLP)
- Auslesen von Text in Bildern per OCR (Optical Character Recognition)

Entscheidend war, dass Web DLP dem IT-Team eine umfangreiche, direkt einsatzbereite Richtlinienbibliothek lieferte. Damit konnten die Administratoren fertige DLP-Richtlinien implementieren, die sowohl den allgemeinen Datenschutzbestimmungen, wie der DSGVO, als auch den lokalen Bestimmungen zum Arbeitnehmerdatenschutz in Bologna sowie an anderen Standorten des Unternehmens entsprachen. Dank der umfangreichen Richtlinienbibliothek von Forcepoint gelang es dem IT-Sicherheitsteam, die richtige Balance zwischen sämtlichen für das Unternehmen relevanten Vorschriften und Standards zu finden.



Herausforderungen

Schutz von Daten vor internen und externen Bedrohungen.

Einhaltung von Datenschutzverordnung und Bestimmungen zum Arbeitnehmerdatenschutz.

Sicherere Nutzung Cloud-basierter Anwendungen durch Mitarbeiter.



Strategie

Aktivierung von Forcepoint DLP zum Schutz vor internen Datenverlusten.

Implementierung von Forcepoint AMD zum Schutz vor externen Bedrohungen.

Wechsel zu einer Forcepoint Web Security Hybrid-Implementierung.

Abwehr von internen und externen Bedrohungen

Forcepoint Web DLP bietet mehr als genug Datensicherheit, um die Anforderungen von Finanzdienstleistungsunternehmen an den Schutz vor Datendiebstahl zu erfüllen. Die Lösung ist schnell einsatzbereit und verhindert, dass kritische Daten über Internetkanäle aus dem Netzwerk herausgeschleust werden. Gleichzeitig ist sie dank der einheitlichen Benutzeroberfläche, die Berichterstattung, Datenverwaltung und Richtlinienverwaltung vereint, äußerst einfach im Handling.

Das Unternehmen war zudem in der Lage, seine Verteidigungsmaßnahmen gegen externe Bedrohungen zu stärken. Als Hauptverteidigungslinie gegen Bedrohungen von außen, wie z. B. Malware, nutzte das Unternehmen bereits Web Security. Diesen Schutz verstärkt es künftig mit Forcepoint Advanced Malware Detection (AMD).

Forcepoint AMD nutzt marktführende Technologie, um Zero-Day- und andere komplexe Malware-Angriffe zu erkennen. Die Deep-Content-Inspection-Technologie von Forcepoint AMD simuliert einen vollständigen Host und interagiert mit der Malware, um sämtliche Aktionen verdächtiger Objekte aufzudecken und zu beobachten. Deep Content Inspection erkennt selbst ausgeklügelte Verschleierungstechniken sowie betriebssystem- oder anwendungsspezifische Bedrohungen, führt eine Analyse auf „schlafenden“ Code durch und überwacht sämtliche CPU- und Speicheraktivitäten.

Stetige Anpassung an die Cloud-basierte Welt

Neben der Verbesserung seiner Datensicherheit musste das Unternehmen auch seine Vorgehensweise in puncto Cloud-Sicherheit überdenken. Wie viele Finanzdienstleister setzte auch dieses Unternehmen zunehmend auf Cloud-Anwendungen wie Office 365 und Salesforce. Damit steigt jedoch gleichzeitig die Wahrscheinlichkeit, dass Mitarbeiter für gewisse Aufgaben nicht geprüfte Cloud-Anwendungen nutzen.

Da die Lösung um Forcepoint Web Security Cloud ergänzt wurde, ist es nun möglich, die innerhalb des Unternehmens verwendeten Cloud-Anwendungen zu erkennen und Richtlinien für die Nutzung dieser Anwendungen zu definieren. Um dies zu ermöglichen, musste das Unternehmen auf die Hybridkonfiguration wechseln. Das heißt, es musste seine lokale Web Security-Implementierung um Web Security Hybrid-Module erweitern und diese aktivieren.

Durch diese Konfiguration kann das Unternehmen nun Web Security DLP auf seinen lokalen Appliances und AMD in der Cloud ausführen. So kann besser verhindert werden, dass Benutzer die Unternehmensdaten gefährden, unabhängig davon, um welches Dateiformat es sich handelt oder ob die Daten über physische Geräte oder über die Cloud gespeichert und ausgetauscht werden.

Dank Forcepoint verfügt das Unternehmen über alle Instrumente, um die Compliance-Anforderungen zu erfüllen und die Herausforderungen der Zukunft zu meistern.



Ergebnisse

Ein „passgenauer“ Schutz vor Datenverlusten und externen Bedrohungen, der alle Compliance-Anforderungen erfüllt.

