Bei diesem namhaften Automobilzulieferer läuft der Schutz des geistigen Eigentums auf Hochtouren

Die GG Group schützt sich vor der Gefahr, nicht nur ihr eigenes geistiges Eigentum, sondern auch das ihrer hochkarätigen Automobilkunden zu verlieren.

Die hart umkämpfte Automobilindustrie befindet sich inmitten eines noch schnelleren Wettlaufs um die neuesten und effektivsten Elektrotechnologien für vernetzte Autos und autonomes Fahren. Sie war schon immer ein beliebtes Ziel von Unternehmensspionage mit vielen dokumentierten Beispielen von Mitarbeitern, die Geschäftsgeheimnisse preisgegeben haben, um sich persönliche Vorteile zu verschaffen. Die GG Group, ein globaler Hersteller von Technologielösungen für die Automobilbranche und Industrie, hat sich für Forcepoint entschieden, um Daten und geistiges Eigentum zu schützen und so das Vertrauen ihrer Kunden in Zeiten der Innovation zu festigen.

KUNDENPROFIL:
Einer der führenden Lieferanten von Kabeln und Leitungen für verschiedene Sektoren, darunter Automobile, Industrie und Aufzüge, mit mehr als 4.000 Beschäftigten in neun Ländern.

BRANCHE:
Fertigungsindustrie

HAUPTSITZ:
Österreich

PRODUKT:
Forcepoint Data Loss Prevention

Der schnelle Fortschritt und der zunehmende Wettbewerb auf dem Markt für Elektrofahrzeuge gefährdet das geistige Eigentum führender Automobilunternehmen. Zulieferer wie die GG Group, auf die Automobilhersteller für einige der wichtigsten Komponenten ihrer proprietären Technologien zurückgreifen, müssen dabei nicht nur ihr eigenes geistiges Eigentum schützen. Als vertrauenswürdiger Partner hat die GG Group Zugang zu hochkarätigen Kunden und arbeitet mit ihnen an sehr wertvollen proprietären Bau- und Entwicklungsplänen zusammen.

Durch die Zusammenarbeit auf globaler Ebene sind diese sensiblen kundeneigenen Daten ständig in Bewegung. Da diese Daten schwer zu überwachen und zu kontrollieren sind, brauchte die GG Group eine bessere Möglichkeit, um sie zu schützen. Als das Unternehmen in Länder mit einem bekanntermaßen hohen Risiko des Diebstahls von geistigem Eigentum und der Unternehmensspionage expandierte, wollte es sicherstellen, dass die proprietären Daten für Unbefugte unzugänglich sind. Die Verletzung des geistigen Eigentums eines einzigen Kunden könnte den Verlust des Vertrauens aller Kunden bedeuten – und damit den Ruf und das Ergebnis der GG Group schädigen.

„Einen Anbieter zu finden, der den Wert des geistigen Eigentums für ein Fertigungsunternehmen versteht und einen innovativen, skalierbaren und anpassungsfähigen Schutz vor Datenverlusten bietet, war ein wichtiges Kriterium."

CHUKS OJEME, CISO, GG GROUP

„Sie können sich vorstellen, dass das Unternehmen seinen guten Ruf beim Kunden und am Markt einbüßen würde, wenn kritische Daten, die sich in der Obhut der GG Group befinden, entwendet würden", so Konrad Langhammer, Account Executive bei Forcepoint. „Sobald ein Datendiebstahl bekannt würde, erführen auch andere Kfz-Hersteller davon, was das Geschäft der GG Group in große Gefahr brächte."

Dem Sicherheitsteam des Unternehmens war klar, dass es den Datenschutz sowohl zu seinem eigenen Wohl als auch zu dem seiner Kunden intensivieren musste.

„Für mich als CISO ist es äußerst wichtig, dass wir die internen Anforderungen verstehen, um unsere kritischen Informationen zu schützen. Einen Anbieter zu finden, der den Wert des geistigen Eigentums für ein Fertigungsunternehmen versteht und einen innovativen, skalierbaren und anpassungsfähigen Schutz vor Datenverlusten bietet, war ein wichtiges Erfolgskriterium für das Projekt", erklärt Chuks Ojeme, CISO der GG Group. „Mit Forcepoint haben wir genau diesen Anbieter gefunden."

Hochrisiko-Benutzer und Spionage auf globaler Ebene erkennen

Um diesen Herausforderungen zu begegnen, nahm die GG Group mehrere Data Loss Prevention-Lösungen unter die Lupe. Allerdings erfüllte nur die Lösung von Forcepoint die Anforderungen, die das Unternehmen für notwendig befand, um Aktivitäten von Benutzern mit hohem Risikoprofil zu erkennen und Unternehmensspionage zu stoppen. Insbesondere stellte Forcepoint unter Beweis, dass seine Data Loss Prevention-Lösung speziell darauf abgestimmt werden kann, Datentypen wie Quellcode, technische Zeichnungen, sensible Geschäftsgeheimnisse und andere Daten zu identifizieren, die das Unternehmen als seine „Kronjuwelen" bezeichnet.

Herausforderungen

Schutz des wertvollen geistigen Eigentums seiner hochkarätigen Kunden und des eigenen an allen Unternehmens- und internationalen Standorten.

Sichtbarmachung riskanter Aktivitäten, die auf Unternehmens-spionage hindeuten.

Strategie

Mehr Transparenz und Kontrolle über kritische Daten mit Forcepoint Data Loss Prevention (DLP).

Implementierung vordefinierter Richtlinien mit DLP, um das IT-Team bei der Erfüllung von Compliance-Anforderungen zu unterstützen.

Unterstützung durch Forcepoint-Experten bei der Entwicklung von Unternehmensrichtlinien für die Anpassung von DLP.

Um den Risiken im Zuge einer internationalen Expansion zu begegnen, ermöglicht die Forcepoint-Lösung eine Verschlüsselung der Daten, wenn diese das Unternehmen verlassen und in über 80 Länder übertragen werden. Mit der zentralisierten Richtlinienverwaltung von Forcepoint ist die GG Group beispielsweise in der Lage, die internationale Kontrolle zu verbessern, indem sie angepasste Richtlinien von einer einzigen Konsole aus anwendet – selbst an dezentralen Standorten.

Risikominimierung durch weniger freiwillige Datenbewegungen

Die GG Group ist überzeugt, dass die getroffenen Vorkehrungen zur Sicherung der proprietären Daten der Autohersteller greifen. Um jedoch wirklich effektiv zu sein, darf sich die Datenschutzpolitik nicht allein auf die Technologie konzentrieren – sie muss Teil einer größeren Unternehmensstrategie für Cyber-Sicherheit im Allgemeinen und Datensicherheit im Besonderen sein.

In enger Zusammenarbeit erarbeiteten die GG Group und Forcepoint die Prioritäten und Strategien des Unternehmens, die als Richtschnur und Grundlage für maßgeschneiderte Datenschutzrichtlinien dienen sollten, die den einzigartigen Anforderungen des Unternehmens gerecht werden.

Zum Beispiel half Forcepoint der GG Group, Funktionen wie die selbstständige Beseitigung von Risiken zu integrieren, um die Benutzer über gute Datenhygiene und die Überwachung der daraus resultierenden Dateninteraktionen aufzuklären. Dies ermöglicht es dem Unternehmen, die Benutzer mit dem höchsten Risikoprofil in Sekundenschnelle zu identifizieren, was eine frühzeitige Warnung vor Verstößen gegen die Datenfreigaberichtlinien und vor potenziellen Fällen von Unternehmensspionage ermöglicht.

Datensicherheit wird Teil der Geschäftsstrategie innerhalb einer langfristigen Partnerschaft

Die Einführung konzentrierte sich zunächst auf geografische Gebiete mit hohem Risiko. Künftig wird Forcepoint auch einen weiteren Einsatz an zusätzlichen Standorten unterstützen, um die sichere Zusammenarbeit zwischen den Mitarbeitern der GG Group und ihren Kunden zu unterstützen. Das Unternehmen denkt außerdem über die Ergänzung von Technologien für Internet, E-Mail, Verhaltensanalyse und die Integration mobiler Agenten nach.

„Ein ganzheitliches, integriertes Cyber-Sicherheitsportfolio mit Forcepoint würde der GG Group ein umfassendes Compliance-Profil geben", erklärt Langhammer. „Dieses ist auditierbar und zeigt den Partnern des Unternehmens, dass es sich um einen Großen der Branche handelt."

Eine langfristige Partnerschaft zwischen dem Unternehmen und Forcepoint unterstützt die GG Group außerdem bei der Weiterentwicklung ihrer Unternehmenspolitik und der Feinabstimmung der entsprechenden DLP-Lösung. „Ein DLP-Projekt ist nie wirklich abgeschlossen. Man muss ständig neue Regeln aufstellen, Änderungen der Richtlinien nachverfolgen, neue Anforderungen innerhalb des Unternehmens und für die Kunden erfüllen und so weiter", so Langhammer. „Forcepoint wird dem Unternehmen daher als vertrauenswürdiger Partner zur Seite stehen und ihm dabei helfen, das DLP-Produkt auch weiterhin auf das Unternehmen abzustimmen."

Ergebnisse

DLP-Richtlinien, die auf die Datenschutz- und Compliance-Bedürfnisse der GG Group zugeschnitten sind und bei Änderungen der Unternehmensrichtlinien dynamisch angepasst werden.

Die Möglichkeit, von einer einzigen Konsole aus unterschiedliche Richtlinien auf die einzelnen Standorte anzuwenden.

Weniger Datenbewegungen sowie erklärende Popup-Meldungen, die Benutzern Hinweise zu guter Datenhygiene geben und so das Risiko minimieren.

© 2021 Forcepoint. Forcepoint und das FORCEPOINT-Logo sind Marken von Forcepoint.
Alle anderen hier genannten Marken sind Eigentum ihrer jeweiligen Inhaber.
[GG-Group-Customer-Story-DE] 17Mar2021