



Innovativer Medizintechnik-Hersteller schützt seine Prozesse mit Proofpoint und spart Zeit

Die Herausforderung

- Schutz von E-Mails vor Phishing und anderen Bedrohungen
- Minimierung manueller Prozesse, um die Möglichkeiten des IT-Teams zu erweitern
- Stärkung von Best Practices für Unternehmenssicherheit

Die Lösung

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Domain Discover
- Proofpoint Threat Response Auto-Pull
- Proofpoint Closed-Loop Email Analysis and Response
- Proofpoint Security Awareness

Die Ergebnisse

- Aktuelle E-Mail-Sicherheit minimiert Phishing und andere Bedrohungen
- Automatisierte E-Mail-Sicherheitsprozesse minimieren manuellen Aufwand
- Security-Awareness-Schulungen stärken die Sicherheitslage insgesamt

Das Unternehmen

Mit mehr als 20 Standorten weltweit und fast 8.000 Partnern weiß dieser innovative Medizintechnik-Hersteller, wie wichtig Vertrauen in die digitale Kommunikation ist. Der weltweite Dienstleister hat einen hervorragenden Ruf bei der Entwicklung innovativer, lebensverlängernder medizinischer Geräte. Er setzt alles daran, seine Kunden, Angestellten und die Marke insgesamt zuverlässig zu schützen. Der Hersteller bietet Service und Kundenorientierung, die eher für Kleinunternehmen typisch sind, wobei ihm die Ressourcen eines großen Unternehmens zur Verfügung stehen.

Die Herausforderung

Schutz von Kunden und Angestellten im Gesundheitswesen

Der Medizintechnik-Hersteller hält seinen Wettbewerbsvorteil dank vielfältiger Funktionen, umfassender Integrationen, technischem Know-how und einer konsequenten Konzentration auf seine Kunden und operative Exzellenz. Wie jedes andere weltweite Unternehmen setzt er für all seine Geschäftsprozesse auf eine sichere Netzwerkinfrastruktur.

Angesichts der dynamischen Bedrohungslandschaft stellte das Sicherheitsteam jedoch fest, dass der Zeitaufwand für den Schutz übermäßig hoch ist. Das vorhandene E-Mail-Sicherheitssystem ließ sich nur schwer einrichten sowie an die Anforderungen anpassen und konnte die neuesten Bedrohungen nicht effektiv abwehren.

„Unsere E-Mail-Sicherheit konnte mit unseren Anforderungen nicht Schritt halten“, erklärt der Sicherheitsmanager des Medizintechnik-Herstellers. „Viel zu viele Bedrohungen wurden durchgelassen, einschließlich Phishing und Angriffe zum Erfassen von Anmeldedaten. Wir mussten also viel Zeit und Ressourcen in die Blockierung dieser Angriffe investieren und konnten uns nicht auf unsere vorhandene Lösung verlassen. Die Situation wurde zusätzlich dadurch erschwert, dass unsere Security-Awareness-Schulungen nicht mithalten konnten.“

Der Hersteller entschied sich, ein System zu implementieren, das umfassenden Schutz vor hochentwickelten Bedrohungen wie Phishing, E-Mail-Betrug und schädlichen Nachahmer-Domains bietet. Damit sollten nicht nur die E-Mail-Sicherheitsmaßnahmen gestärkt, sondern auch Analysen und Berichte für bessere und strategischere Entscheidungen integriert werden.

Die Lösung

Wechsel zu einem personenzentrierten Cybersicherheitsansatz

Das Unternehmen sah sich verschiedene E-Mail-Sicherheitsprodukte an, um das am besten für die eigenen Zwecke geeignete zu finden. Es entschied sich für Proofpoint und die umfassendste sowie am besten unterstützte Lösung.

„Wir testeten auch Produkte anderer Wettbewerber. Den größten Unterschied machten für uns der Support sowie die allgemeine Unterstützung, die wir bei Proofpoint erhalten“, so der Sicherheitsmanager. „Proofpoint lieferte uns einen personenzentrierten Überblick über unsere Sicherheitslage.“

„Durch Proofpoint sparen unsere Mitarbeiter erheblich Zeit. Das Team kann einen proaktiveren Sicherheitsansatz verfolgen, anstatt wie bisher lediglich reagieren zu können. In gewisser Weise agiert Proofpoint wie ein weiteres Teammitglied.“

Sicherheitsmanager, Medizintechnik-Hersteller

Der Sicherheitsmanager stellte gemeinsam mit seinem Team mehrere Lösungen bereit, die reibungslos zusammenarbeiten, um Malware, Phishing sowie Betrugsversuche zu stoppen und dabei die Sicherheitsabläufe und Bedrohungsabwehr zu automatisieren.

„Gemeinsam mit Proofpoint Targeted Attack Protection (TAP), Proofpoint Threat Response Auto-Pull (TRAP) sowie Proofpoint Closed-Loop Email Analysis and Response (CLEAR) bildet Proofpoint Email Protection ein geschlossenes System für automatisierte Reaktionen“, so der Sicherheitsmanager. „Dadurch können wir uns die manuelle Untersuchung von Bedrohungen sparen.“

Der Sicherheitsmanager und sein Team nutzten Proofpoint-Schulungen, die einen reibungslosen Onboarding-Prozess und die unkomplizierte Migration zur neuen Lösung gewährleisteten.

„Das Bedienungskonzept hat für uns den Unterschied gemacht“, betont der Sicherheitsmanager. „Proofpoint folgt einem Playbook-Ansatz mit durchdachten Abläufen – und wir konnten dabei das Tempo bestimmen.“

Der Migrationsprozess half dem Unternehmen auch, seine DMARC-Richtlinien (Domain-based Message Authentication, Reporting, and Conformance) für besseren Schutz vor E-Mail-Spoofing und Betrugsversuche zu optimieren.

„Da ich keinen guten Überblick über meine Absender hatte, beschränkten sich unsere DMARC-Richtlinien im Wesentlichen darauf, verdächtige Nachrichten unter Quarantäne zu stellen“, erklärt der Sicherheitsmanager. „Im Verlauf unseres Migrationsprozesses haben wir ein besseres Verständnis unserer Absender und einen Überblick über alle E-Mails erhalten, die über unsere Domain gesendet werden. Das hat uns enorm bei der Implementierung von Proofpoint Email Fraud Defense geholfen.“

Proofpoint Email Fraud Defense bietet dem Unternehmen auch einen Überblick über Doppelgänger-Domains, die für Phishing-Websites und E-Mail-Angriffe verwendet werden können. Um den guten Ruf des Unternehmens zusätzlich zu schützen, hat der Sicherheitsmanager vor Kurzem Proofpoint Virtual Takedown integriert. Dieser zusätzliche Service unterstützt das Unternehmen bei der Blockierung und Stilllegung schädlicher Domains.

Dem Team war die zentrale Rolle der Angestellten für den Schutz des Unternehmens bewusst. Um sie dabei zu unterstützen, integrierte der Sicherheitsmanager Proofpoint Security Awareness, das mit einem datengestützten Ansatz eine Sicherheitskultur mit Best Practices gewährleistet.

„Wir haben ein quartalsweises Schulungsprogramm für alle Partner eingeführt, bei dem die Teilnahme verpflichtend ist“, so der Sicherheitsmanager. „Dabei machen wir keine Ausnahmen.“

Die Ergebnisse

Minimierung von Risiken, Gewinnung von Erkenntnissen

Durch die Integration des vollständigen Portfolios an Proofpoint-E-Mail-Sicherheitslösungen konnte das Unternehmen die Analyse, Abwehr und Behebung von E-Mail-Bedrohungen wie Phishing und Malware stärken und beheben. Die Lösung schützt das Unternehmen sowie seine Kunden und entlastet dabei das Sicherheitsteam.

„Jeder Sicherheitszwischenfall muss in unserem System aufgezeichnet und kategorisiert werden“, erklärt der Sicherheitsmanager. „Von ursprünglich 800–1.000 problembezogenen Tickets pro Monat sind wir jetzt bei weniger als 150. Diese enorme Reduzierung hat unser Team von vielen manuellen Aufgaben befreit.“

Ein weiterer Vorteil von Proofpoint TAP war das Dashboard mit einem Echtzeit-Überblick und Erkenntnisse über Bedrohungen und ihre Ziele. Besonders effektiv war die Lösung beim Schutz von Angestellten mit Zugriff auf vertrauliche Informationen, die am stärksten durch Bedrohungen gefährdet waren. Dank der Proofpoint-Analysen konnte das Unternehmen die Bedrohungsmuster, Trends und Vorgehensweisen bei Angriffen auf ihre Very Attacked People (VAPs)[™] aufdecken.

„Anhand der Informationen über die besonders gefährdeten Personen entwickelten wir eigene Microsoft-Richtlinien für bedingte Zugriffe, die zuverlässigen Schutz gewährleisten“, berichtet der Sicherheitsmanager.

Der Sicherheitsmanager hat auch die Berichterstellungsfunktionen der Lösung zu schätzen gelernt. Dadurch spart das Sicherheitsteam Zeit und kann Führungskräfte unkompliziert über die allgemeine Sicherheitslage des Unternehmens informieren.

„Die Unterstützung durch Proofpoint ist für uns einer der wichtigsten Vorteile“, betont der Sicherheitsmanager. „Durch die Berichte sparen wir viel Zeit und erhalten einen Überblick über alle Daten. Gleichzeitig enthalten sie die Informationen, die wir benötigen, um unser Verhalten ändern und einen proaktiveren Sicherheitsansatz implementieren zu können. Wir können auch verschiedene Präsentationen für die Meetings unserer Führungskräfte erstellen, damit sie die E-Mail-Bedrohungen verstehen und wissen, welche Maßnahmen wir dagegen ergreifen. Die Berichte von Proofpoint Security Awareness fließen in unsere Schulungen ein und helfen uns, das Sicherheitsbewusstsein zu steigern.“

Dank der Produkte, Services und Schulungen von Proofpoint konnte der innovative Medizintechnik-Hersteller von der bloßen Reaktion auf neue Bedrohungen zu einem strategischeren Sicherheitsansatz übergehen, der die Bestleistung von Menschen und Technologie ermöglicht.

MEHR ERFAHREN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

INFORMATIONEN ZU 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.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.