



AGRAVIS schützt mit Proofpoint kritische Netzwerke für Lösungen in der Landwirtschaft



Herausforderung

- Verbesserung der E-Mail-Sicherheit und Minimierung von False Positives
- Schutz der Mitarbeiter und Daten vor Insider-Bedrohungen
- Kontinuierliche Anpassung bewährter Sicherheitsmethoden, um mit Veränderungen Schritt zu halten

Lösung

- Proofpoint Enterprise Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)
- Proofpoint Security Awareness Training (PSAT)
- Proofpoint Insider Threat Management (ITM)

Ergebnisse

- Reduzierte False Positives maximieren Produktivität eines kleinen IT-Teams
- Technologie wurde dank Security Awareness Training mit verbesserten Best Practices ergänzt

Das Unternehmen

Das Geschäft mit Agrarhandelsdienstleistungen ist Teil einer einzigartigen Branche. Die AGRAVIS Raiffeisen AG ist ein führender Anbieter in diesem Bereich. Das Unternehmen mit Sitz in Deutschland unterstützt seine genossenschaftlichen Vertriebspartner, Landwirte und Menschen in ländlichen Gebieten mit einer Vielzahl an Produkten. Das Angebot wird zudem mit kompetenten Beratungsdienstleistungen sowie umfassenden Kenntnissen und Erfahrungen ergänzt. Um seine Daten zu schützen und sich an die veränderten Geschäftsanforderungen anzupassen, benötigte das Unternehmen eine hochentwickelte Cybersicherheitslösung.

Herausforderung

Schutz für eine modernere Geschäfts-E-Mail-Plattform

Das Angebot von AGRAVIS umfasst Unterstützung beim Pflanzenanbau, Tierfutter, Agrar-Technologie sowie -Maschinen und vieles mehr. Aufgrund des wachsenden Geschäfts wurden die Sicherheit sowie Integrität der Netzwerkinfrastruktur und Daten des Unternehmens zur obersten Priorität. Um seine 6.300 Mitarbeiter sowie seine Kunden- und Geschäftsdaten zu schützen, stellte AGRAVIS ein Team von fünf IT-Experten zusammen. Und wie in den meisten Betrieben entwickelte und verbesserte das Unternehmen seine Infrastruktur, um mit den neuen Geschäftsanforderungen Schritt zu halten. Doch als es zu Problemen mit dem bestehenden Secure Email Gateway (SEG) kam, bot sich für AGRAVIS eine Gelegenheit, die Netzwerke zu modernisieren und gleichzeitig die Sicherheitslage zu verbessern.

„Unsere neue IT-Strategie bestand aus einem Wechsel zu Office 365 und Microsoft Exchange Online für Geschäfts-E-Mail“, erklärte David Wydrinna, Senior IT-Security Engineer bei AGRAVIS. „Wir hatten allerdings einige Probleme mit unserem lokalen Secure Email Gateway in Münster. Wir verzeichneten Performance-Probleme, Aussetzer und Zeitüberschreitungen, für die es keine offensichtlichen Ursachen gab. Daher haben wir mit den besten Anbietern ein Proof-of-Concept erarbeitet, um die E-Mail-Sicherheitslösung zu finden, die unsere Bedürfnisse am besten erfüllt.“

Lösung

Proofpoint bietet vollständigen und reaktionsschnellen E-Mail-Schutz

Nachdem sie mehrere Lösungen per PoC evaluiert hatten, entschied sich AGRAVIS für eine umfassende, integrierte E-Mail-Lösung von Proofpoint. Proofpoint Email Protection schützt die Mitarbeiter vor den neuesten E-Mail-Bedrohungen wie Anmeldedaten-Phishing, Ransomware-Angriffen und E-Mail-Betrug. Dank Machine Learning und mehrschichtigen Schutztechniken identifiziert und blockiert die Lösung schädliche E-Mails. Zudem kann das IT-Sicherheitsteam mit Proofpoint Threat Response Auto-Pull (TRAP) E-Mails analysieren und schädliche Nachrichten nach der Zustellung unter Quarantäne stellen.

„Eine der größten Stärken der Lösung war die Möglichkeit, mit dem TRAP-Server E-Mails, die durchgekommen waren, zu identifizieren und anschließend automatisch aus den Postfächern zu entfernen“, so Patrick Hemsing, IT-Security Engineer bei AGRAVIS.

„Die Proofpoint-Lösung ist großartig. Im Vergleich zu unserer alten Lösung können wir Phishing- und Spam-Angriffe jetzt sehr viel effektiver erkennen. Die Zahl der Bedrohungen, die unsere Clients erreicht, ist um 95 % gesunken.“

David Wydrinna, Senior IT-Security Engineer, AGRAVIS

Die Cloud-basierte Umgebung für Geschäfts-E-Mails wird zusätzlich mit den statischen und dynamischen Techniken von Proofpoint Targeted Attack Protection (TAP) geschützt, die Bedrohungen dank Sandbox-Analysen bereits in frühen Phasen der Angriffskette erkennen.

„Die Sandbox-Analysefunktion war eines der ausschlaggebenden Unterscheidungsmerkmale beim Vergleich der Lösungen in unserem PoC“, sagte Patrick Hemsing. „Proofpoint hat im Vergleich zu anderen Lösungen auch ein höheres Maß an Stabilität und Anwenderfreundlichkeit geboten.“

Viele Sicherheitsbedrohungen gehen von Mitarbeitern im Unternehmen aus – unabhängig davon, ob sie fahrlässig, unwissentlich oder böswillig handeln. Um das Unternehmen vor dieser Gefahr zu schützen, führte das IT-Team von AGRAVIS die Lösung Proofpoint Insider Threat Management (ITM) ein. Die Lösung korreliert Anwenderaktivitäten mit Datenbewegungen, sodass das Team Anwenderrisiken präzise bewerten, Insider-bezogene Kompromittierungen erkennen und schnell auf Zwischenfälle reagieren kann.

Ergebnisse

Gewinnung von Sicherheitserkenntnissen und Entlastung des Personals

Proofpoint bietet den nötigen Bedrohungsschutz, damit AGRAVIS seine wichtigen Geschäftsprozesse schützen kann. Gleichzeitig werden Prozesse automatisiert und False Positives minimiert, die wertvolle Arbeitszeit in Anspruch nehmen.

„Mit unserer alten Lösung gab es täglich Probleme“, erinnerte sich Patrick Hemsing. „Jeden Tag wurden etwa 50 E-Mails unter Quarantäne gestellt und ein Mitarbeiter musste stundenlang manuell prüfen, ob es sich um Spam, einen Spearphishing-Angriff oder einen Anwendungsfehler handelte. Proofpoint erspart uns all das. Deshalb haben wir mehr Zeit, uns auf andere Aufgaben zu konzentrieren.“

Dank der Partnerschaft mit Proofpoint hat AGRAVIS nun auch Zugang zu einem vertrauenswürdigen Berater, der neue und umfassende Erkenntnisse zu Bedrohungen bereitstellt, die als Grundlage zur Priorisierung und Entscheidungsfindung bei IT-Fragen dienen können.

„Unser Proofpoint Customer Success Manager rief uns an und berichtete, wie viele Phishing-E-Mails die Lösung abgefangen hat. Das konnten wir dann zum ersten Mal unserem CIO melden“, sagte David Wydrinna. „Unser Manager hat uns ein Dokument geschickt. Darin standen alle unsere Konfigurationen und Statistiken über Angriffe, von denen wir nichts wussten. Zudem enthielt es Verbesserungsvorschläge.“

Proofpoint-Lösungen sind auf Weiterentwicklung und Skalierung ausgelegt – AGRAVIS ist bereits dabei, seine Lösung zu erweitern. Das Unternehmen hat sich für Proofpoint Email Fraud Defense (EFD) entschieden, das die Umsetzung von DMARC-Kontrollen (Domain-based Message Authentication, Reporting & Conformance) vereinfacht. Betrugsversuche können damit gestoppt und die vertrauenswürdige Domäne des Unternehmens geschützt werden. Zudem überwacht und analysiert Proofpoint EFD Forensik-Berichte. AGRAVIS erhält dadurch Erkenntnisse, mit denen schädliche E-Mails, die Spoofing-Domänen enthalten, blockiert werden können.

Außerdem will AGRAVIS seine Mitarbeiter mit Proofpoint Security Awareness Training (PSAT) schulen, um mit der veränderten Bedrohungslandschaft mitzuhalten. Da sich Angriffe stets verändern, möchte das Unternehmen sicherstellen, dass seine Mitarbeiter immer auf dem neuesten Stand sind und somit bestmöglicher Schutz gewährleistet wird.

„In der Vergangenheit benötigten wir mitunter vier Wochen, um so eine Schulung zu organisieren“, berichtete David Wydrinna. „Mit PSAT können wir sie in wenigen Minuten einrichten.“

AGRAVIS ist davon überzeugt, dass es dank der Proofpoint-Lösungen und -Services auch in Zukunft gut gegen neue Sicherheitsbedrohungen gewappnet ist.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter 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 mehr als die Hälfte der Fortune-1000-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.