



# Bechtle verbessert E-Mail-Sicherheit mit Proofpoint

## Proofpoint überzeugt im Gesamtpaket mit technologischem Vorsprung und Professionalität

### HERAUSFORDERUNG

- Ablösung zweier Bestandslösungen in den Bereichen E-Mail-Sicherheit und Anti-Spam
- Höchste Anforderungen an Skalierbarkeit, Sicherheit und Flexibilität der Lösung

### LÖSUNG

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull

### ERGEBNISSE

- Wird als zentrale Lösung für E-Mail-Sicherheit für alle Standorte und 12.000 Mitarbeiter eingesetzt
- Bietet höchste Flexibilität und Self-Service-Funktionen für Anwender
- Erkennt, analysiert und stoppt Schadmails zuverlässig
- Blockierung von Spam-E-Mails und bekannter Bedrohungen im zweistelligen Millionenbereich während eines Monats (70 Prozent des gesamten eingehenden E-Mail Volumens)
- Bietet detaillierte Übersicht über Bedrohungen, Auswirkungen und Trends
- Ausschaltung zielgerichteter neuer Bedrohungen noch vor Zustellung in den Posteingang, davon 40 Prozent mit Anhang und 60 Prozent URL-basierter Bedrohungen, inkl. URL-Rewriting
- Verschiebt auch bereits in Postfächer ausgelieferte Mails in die Quarantäne, sobald sie als Schadmail identifiziert wurden

### Das Unternehmen

Die Bechtle AG ist mit 75 IT-Systemhäusern in Deutschland, Österreich und der Schweiz aktiv und zählt mit 24 E-Commerce-Gesellschaften in 14 Ländern zu den führenden IT-Unternehmen in Europa. Gegründet 1983, beschäftigt der Konzern mit Hauptsitz in Neckarsulm derzeit rund 12.000 Mitarbeiter. Seinen mehr als 70.000 Kunden aus Industrie und Handel, öffentlichem Dienst sowie dem Finanzmarkt bietet Bechtle herstellerübergreifend ein lückenloses Angebot rund um IT-Infrastruktur und IT-Betrieb aus einer Hand.

### Die Herausforderung

Die Suche nach einer neuen E-Mail-Sicherheitslösung hatte für Bechtle strategischen Charakter. Als Spezialist für IT-Infrastruktur und IT-Dienstleistungen war es Bechtle ein Anliegen, hier auf Basis der Möglichkeiten eines neuen Data Centers eine moderne, skalierbare Plattform im Unternehmen zu etablieren.

Die zuvor verwendete Lösung basierte auf Open Source und war stark an die Bedürfnisse von Bechtle angepasst, jedoch sehr arbeitsintensiv. Mit einer Vielzahl neuer Standorte und der damit einhergehenden Komplexität wurde es offensichtlich, dass sie dem größer werdenden Bedarf nicht mehr gerecht werden würde.

Auch die damals im Einsatz befindliche Anti-Spam-Lösung entsprach nicht mehr den Anforderungen des heute gut 12.000 Mitarbeiter zählenden Unternehmens. Im Rahmen des Aufbaus des neuen Bechtle Datacenter in Frankfurt am Main wurde intensiv nach einer neuen, modernen, skalierbaren, sicheren und redundanten Gesamtlösung für den Bereich E-Mail-Sicherheit gesucht. Ziel war es, im Data Center einen zentralen Service für alle Mitarbeiter für eine Vielzahl von Bechtle-Standorten im In- und Ausland zu etablieren.

„Wichtig war uns, dass die Lösung neben der Abdeckung der Standardkomponenten auch flexibel genug ist, um unsere Spezialanforderungen wie eine Vielzahl von Mail-Domains, ein sehr komplexes Mail-Routing usw. abzudecken“, erläutert Matthias Weber, Cyber Security & Risk Management Specialist bei Bechtle. „Das war der Ausgangspunkt für das Projekt.“

## Die Lösung

Für die Wahl der langfristig optimalen Lösung scheute Bechtle dann auch weder Zeit noch Mühen, um verschiedene Angebote unterschiedlicher Anbieter zu evaluieren.

Von Proofpoint gingen zwei Lösungen mit ins Rennen: Email Protection als Mail-Gateway und Targeted Attack Protection (TAP) als Sandbox.

Bei Email Protection überzeugte vor allem die hohe Flexibilität. Eine vollständig anpassbare Richtlinienverwaltung unterstützt die Kontrolle auf globaler, Gruppen- und Benutzerebene, die selbst den höchsten Ansprüchen der komplexesten Unternehmen mehr als gerecht werden. Dank der Self-Service-Funktionen können Mitarbeiter zahlreiche E-Mail-Einstellungen wie Quarantäne-Settings, Listen für sichere und blockierte Absender sowie die Sperrung von Massen-E-Mails selbst vornehmen. Dies reduziert den Administrationsaufwand erheblich.

„Uns hat das Gesamtpaket überzeugt. Die Technologie von Proofpoint stellt sicher, dass wir auf dem neuesten Stand der Technik und immer gegen die neuesten Angriffe gerüstet sind.“

**Matthias Weber**, Cyber Security & Risk Management Specialist bei Bechtle

TAP, als zweite Kernkomponente der von Proofpoint konzipierten Lösung, erkennt und analysiert hochentwickelte Bedrohungen und ist in der Lage, diese zu blockieren, noch bevor sie den Posteingang der Anwender erreichen. Dabei werden nicht nur Angriffe, die über schädliche Anhänge und URLs übertragen werden sollen, entdeckt und gestoppt. Auch Zero-Day-Bedrohungen, polymorphe Malware, manipulierte Dokumente sowie bekannte Phishing-Angriffe können ausgefiltert werden. „Besonders das TAP-Dashboard hat uns überzeugt. Wir haben jetzt einen genauen Überblick über alle Bedrohungen, die sich gegen Bechtle richten, vom Trojaner über Ransomware bis hin zu Phishing-Angriffen“, führt Matthias Weber weiter aus.

„Uns hat das Gesamtpaket überzeugt. Die Technologie von Proofpoint stellt sicher, dass wir auf dem neuesten Stand der Technik und immer gegen die neuesten Angriffe gerüstet sind. Alle Kriterien unseres Anforderungskatalogs, was Flexibilität, Redundanz und Skalierbarkeit anbelangt, wurden erfüllt. Das, in Kombination mit dem Vertrauen in die Kompetenz der Cybersecurity-Experten des IT-Sicherheitsspezialisten, hat uns letztlich überzeugt, der Proofpoint-Lösung den Zuschlag zu geben“, so Matthias Weber.

Nachdem die Entscheidung für Proofpoint gefallen war, wurden im Folgenden alle weiteren Projektschritte gemeinsam durchgeführt. Man entschied sich die neue Lösung parallel zur noch im Betrieb befindlichen Bestandslösung im neuen Datacenter aufzubauen und dann Stück für Stück in den Produktivbetrieb übergehen zu lassen. „Die Test- und Aufschaltphasen liefen absolut reibungslos“, lobt Matthias Weber die Qualität der Lösung.

Nach mehreren Jahren im Produktivbetrieb entschied sich Bechtle Ende 2019 für eine Ergänzung der Lösung durch Proofpoint Threat Response Auto-Pull (TRAP). „TAP hat sich auch während der ernststen Bedrohungslage, die vor allem im zweiten Halbjahr 2019 durch Emotet vorherrschte, absolut bewährt“, führt Weber aus. Doch kann es vorkommen, dass Cyberkriminelle die in einer E-Mail enthaltene URL erst

„vergiften“, nachdem diese E-Mail die Sicherheitsüberprüfungen bereits durchlaufen hat und sie in die Postfächer der Adressaten zugestellt wurde. Hier ist es dann nötig diese Nachricht automatisiert im Nachhinein zurückrufen zu können.

Marco Ebert, Infrastructure Specialist bei Bechtle, ergänzt: „Mit unseren 12.000 Anwendern und Postfächern benötigten wir für diese Aufgabe eine Automatisierung, denn mit jeder zusätzlichen Minute, in der eine E-Mail mit Schadsoftware oder einem Link zu einer Website mit Malware in einem Postfach liegt, steigt die Gefahr, dass sie doch versehentlich geklickt wird.“ TRAP erkennt, wenn diese nachträglich scharf geschalteten Nachrichten weitergeleitet oder an Verteilerlisten gesendet werden und überprüft automatisch die Empfänger, um diese Nachrichten zu finden und zurückzuziehen. Das spart Zeitaufwand und Ärger.



## Die Ergebnisse

Das ursprüngliche Projektziel, eine moderne, skalierbare, sichere und flexible Lösung für Bechtle zu etablieren, wurde vollständig erreicht. „Wir sind heute gemeinsam mit Proofpoint auf dem neuesten Stand der Technik und bleiben idealerweise den Cyberkriminellen einen Schritt voraus“, resümiert Weber. Im Ergebnis gelang es Bechtle, jeden Monat viele Millionen unerwünschter Nachrichten – etwa 70 Prozent des gesamten eingehenden Mailvolumens – durch Proofpoint zu blockieren. Auch neue, sehr zielgerichtete Angriffe werden durch TAP erkannt und abgefangen, wobei diese zu 40 Prozent bösartige Anhänge aufweisen während 60 Prozent URL-basierte Bedrohungen beinhalten.

Neben der technischen Komponente nennt das Unternehmen auch die partnerschaftliche Zusammenarbeit mit Proofpoint als einen Pfeiler des Erfolgs. „Die regelmäßigen Health Checks, die von Proofpoint angeboten und durchgeführt werden, haben sich bewährt und sind gerade bei unserem technischen Team sehr beliebt“, erklärt Weber. „Wir erfahren, wo wir stehen, was optimierbar ist und stellen sicher, immer auf dem aktuellen Stand zu bleiben, ohne Altlasten mit uns zu führen.“

Bechtle nutzt zudem die Integration von Proofpoint mit Splunk, so dass Daten aus dem TAP-Dashboard direkt im SIEM (Security Information and Event Management) des Unternehmens abgerufen werden können, um sie dort mit anderen Daten zu korrelieren.

## MEHR ERFAHREN

Besuchen Sie visit [www.proofpoint.de](http://www.proofpoint.de) für weitere Informationen.

### ÜBER PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital, aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, verlassen sich auf Proofpoints Sicherheits- und Compliance-Lösungen, bei denen der Mensch im Mittelpunkt steht, um ihre wichtigsten Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren. Weitere Informationen finden Sie unter [www.proofpoint.de](http://www.proofpoint.de).

©Proofpoint, Inc. Proofpoint ist ein eingetragenes Warenzeichen von Proofpoint, Inc. in den USA und / oder anderen Ländern. Alle anderen hier erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber. [www.proofpoint.de](http://www.proofpoint.de)