proofpoint.

ANWENDERBERICHT

Bilfinger schützt E-Mail-Kommunikation in der Lieferkette mit Proofpoint Email Fraud Defense

Vertrauen in E-Mails wiederherstellen und Markenmissbrauch mittels Authentifizierung vermeiden

BILFINGER

HERAUSFORDERUNG

- Betrügerische E-Mails, die die legitimen Domains von Bilfinger missbrauchten
- Vertrauensverlust in der Lieferkette, da nicht sicher war, dass eine offensichtlich von Bilfinger stammende Mail auch wirklich echt war
- CEO-Betrug

LÖSUNG

- Email Fraud Defense (EFD) von Proofpoint bietet vollständigen Überblick über ein- sowie ausgehende Bedrohungen, die sich gefälschte Identitäten von Bilfinger zunutze machen
- Bewährte Implementierung für eine schnelle, zuverlässige und risikolose Bereitstellung von EMail-Authentifizierung
- Umfangreiche Expertise der Proofpoint Managed-Service-Consultants
- Von Proofpoint gelieferte B2B-E-Mail-Daten, gerade für B2B-Unternehmen relevant

ERGEBNISSE

- Transparenz erlangen über alle legitimen E-Mail-Ströme
- Domain Spoofing im E-Mail-Verkehr verhindern
- Markenschutz in der E-Mail-Kommunikation und Stärkung des Vertrauens in der Lieferkette

Das Unternehmen

Bilfinger ist ein international führender Industriedienstleister. Der Konzern steigert die Effizienz von Anlagen, sichert eine hohe Verfügbarkeit und senkt die Instandhaltungskosten. Das Portfolio deckt die gesamte Wertschöpfungskette ab: von Consulting, Engineering, Fertigung, Montage, Instandhaltung, Anlagen-Erweiterung und deren Generalrevision bis hin zu Umwelttechnologien und digitalen Anwendungen. Das Unternehmen erbringt seine Leistungen in zwei Geschäftsbereichen: Engineering & Maintenance sowie Technologies. Die Kunden aus der Prozessindustrie kommen u.a. aus den Bereichen Chemie & Petrochemie, Energie & Versorgung, Öl & Gas, Pharma & Biopharma, Metallurgie und Zement. Bilfinger steht mit rund 34.000 Mitarbeitern für höchste Sicherheit und Qualität und erwirtschaftete im Geschäftsjahr 2019 Umsatzerlöse von 4,327 Milliarden Euro. Das Unternehmen ist speziell in Europa, Nordamerika und dem Nahen Osten aktiv.

Die Herausforderung

Mittels betrügerischer E-Mails attackieren Cyberkriminelle die Menschen in den Unternehmen und nicht deren technische Infrastruktur. Eine Methode hierbei ist die Vortäuschung von Identitäten. Im Rahmen dessen wird die tatsächliche Domain des Unternehmens für Phishing Angriffe – oftmals innerhalb des Unternehmens selbst oder innerhalb der Lieferkette – von den Cyberbetrügern genutzt. Unter den Namen BEC (Business E-Mail Compromise) bekannt, verursacht diese Art von Angriff nicht nur hohe Kosten, sie führt zudem zu Vertrauensverlust in die E-Mail-Kommunikation.

Vor dieser Herausforderung stand auch Bilfinger. Eingebunden in komplexe und mehrstufige Wertschöpfungsketten hatte Bilfinger sich das Ziel gesetzt, sicherzustellen, dass jede E-Mail, die augenscheinlich von Bilfinger verschickt wurde, auch tatsächlich vom Unternehmen stammt. Und dies insbesondere, wenn es sich um E-Mails aus dem Leadership Team des Unternehmens handelt – nicht umsonst wird diese Betrugsmasche auch Chefmasche (CEO-Fraud) genannt.

Nachdem andere Proofpoint-Lösungen bereits erfolgreich im Unternehmen zum Einsatz kommen entschied man sich für einen Test der Proofpoint-Email-Fraud-Defense-Lösung. Im Rahmen dieses Tests fanden die Cyber-Security-Experten bereits nach kürzester Zeit Belege dafür, dass der Name Bilfinger tatsächlich für Versuche missbraucht worden war, Malware per E-Mail zu verbreiten. „Das Vertrauen aller Beteiligter unserer Lieferkette in unsere E-Mail-Kommunikation darf nicht aufs Spiel gesetzt werden“, erläutert Herr Lauterbach, CIO von Bilfinger und Bilfinger Global IT GmbH. „So war die Entscheidung für dieses Projekt mit Proofpoint eine logische Konsequenz und sinnvolle Erweiterung.“

Die Lösung

Mittels Email Fraud Defense (EFD) sind Unternehmen in der Lage, BEC-Angriffe, die ihre Domains zu missbrauchen versuchen, bereits an ihrem Ursprung zu stoppen. Die Lösung authentifiziert alle bei dem Unternehmen ein- und ausgehenden E-Mails und schützt so Mitarbeiter, Kunden und Geschäftspartner vor Angriffen mit gefälschten Identitäten. Dadurch wird das Vertrauen in E-Mails wiederhergestellt.

Möglich wird dies mittels des offenen DMARC-Standards, wobei das Implementieren einer DMARC Reject-Richtlinie ein oft aufwändiger und langwieriger Prozess sein kann. Denn eine versehentliche Blockade legitimer E-Mails muss ausgeschlossen sein, bevor die Reject-Richtlinie tatsächlich zum Einsatz kommen kann.

„Letztlich war es aber die herausragende Expertise des Proofpoint-Teams, die die Umsetzung des Projekts erst möglich gemacht hat."

Herr Pfau, Head of CIO Office, Bilfinger Global IT GmbH

So handelt es sich bei Email Fraud Defense von Proofpoint auch um einen Managed Service, in dessen Rahmen dieser Prozess gemeinsam mit dem Kunden beschritten wird. Bilfinger wurde ein dedizierter Managed Services Consultant zur Seite gestellt, der anhand eines individuellen Projektplans zuerst alle Versender von E-Mails identifizierte, die legitim im Namen der Bilfinger Domäne E-Mails versenden dürfen. Hierzu zählen auch externe Dienste wie E-Mail-Versanddienstleister, die im Auftrag und Namen von Bilfinger legitime E-Mails versenden.

Die Proofpoint-EFD-Lösung stellt darüber hinaus vollständige Transparenz über den gesamten E-Mail-Verkehr her, der von Seiten oder im Namen von Bilfinger versandt wird. Bei Proofpoint fließen dabei mehr als 5 Milliarden E-Mail-Nachrichten täglich in die Analyse mit ein, ebenso Daten aus 7.000 Secure Email Gateways und von 120 Internet Service Providern.

Das Sicherstellen der korrekten Authentifizierung aller legitimen Versender stellt den zweiten wichtigen Abschnitt des Projekts dar. EFD lieferte Bilfinger dabei wertvolle Einblicke, die den Authentifizierungsprozess beschleunigten und gewährleisteten, dass legitime E-Mails nicht blockiert werden. Somit konnte erst als sicher war, dass alle legitimen Versender die Bilfinger E-Mails korrekt authentifizieren, die Richtlinie auf „Reject" und damit „scharf" geschaltet werden.

Die Ergebnisse

Die Umsetzung eines solchen Projekts mag in der Theorie einfach erscheinen. In der Praxis ist dies aber höchst komplex. Bei Bilfinger war man – wie bei vielen etablierten Unternehmen – mit gewachsenen Strukturen konfrontiert. So hatten verschiedene Geschäftsbereiche von Bilfinger begonnen, jeweils eigene E-Mail-Versanddienstleister zu beauftragen, E-Mail-Werbung bzw. -Newsletter zu versenden. „Vonseiten der IT gab es keine Transparenz mehr, wer legitime E-Mails mit den Bilfinger-Domänen verschickt. Ohne diese Kenntnisse kann aber keine Reject Policy für DMARC erreicht werden, denn in diesem Fall würden sehr viele legitime E-Mails ebenfalls geblockt werden – mit den entsprechenden negativen Konsequenzen für das Business“, erklärt Herr Graser, Infrastructure Specialist bei Bilfinger Global IT GmbH. „Proofpoint hat uns genau diese Transparenz verschafft.“

Dabei war für Bilfinger als B2B-Unternehmen besonders wichtig, dass Proofpoint auch DSGVO-konforme Transparenz über die gesamte B2B-E-Mail-Kommunikation – inklusive aller Dienstleister – erzeugen konnte. „Das ist ein Kriterium, auf das alle Unternehmen, die mit anderen Unternehmen zusammenarbeiten, bei der Auswahl des Anbieters achten sollten. Transparenz über diese Daten zu haben, kann über den Erfolg eines solchen Projekts entscheiden“, so Herr Graser weiter.

„Letztlich war es aber die herausragende Expertise des Proofpoint-Teams, die die Umsetzung des Projekts erst möglich gemacht hat“, resümiert Herr Pfau, Head of CIO Office, Bilfinger Global IT GmbH abschließend. „Der Consultant muss nicht nur die Technologie verstehen, er muss sich auch tief in unser Unternehmen einarbeiten, um alle legitimen E-Mail-Ströme zu erfassen – um dann mit diesen Drittanbietern zusammenzuarbeiten, um die korrekte Konfiguration und E-Mail-Authentifizierung zu entwickeln. Die nötige Detailarbeit und mögliche Fallstricke dürfen nicht unterschätzt werden. Hier lohnt sich die Zusammenarbeit mit Proofpoint absolut.“ Ausgestattet mit dieser Transparenz und den durch Proofpoint gewonnen Erkenntnissen kann Bilfinger nun auch Konsolidierungspotenziale in Bezug auf externe Mail Provider ausschöpfen und damit letztlich Effizienz- und Kosteneinsparungen erreichen.

„Wenn einer unserer Geschäftspartner jetzt eine Bilfinger-Mail unseres CEOs erhält, kann er sich auch wirklich sicher sein, dass sie tatsächlich von unserem CEO stammt“, erklärt Herr Lauterbach, abschließend den Erfolg des Projekts. „Das sichert die gute und enge Zusammenarbeit in der Supply Chain und unsere vertrauensvollen Geschäftsbeziehungen.“

MEHR ERFAHREN

Besuchen Sie **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 **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**