proofpoint.

LEITFADEN FÜR DIE PLANUNG

Vom alten E-Mail-Gateway zu Proofpoint wechseln

Sichere E-Mail-Gateways (SEGs) wurden einst entwickelt, um Spam und bekannte Malware zu stoppen. Angreifer nutzen heute jedoch raffinierte Bedrohungen und Multi-Vektor-Techniken wie Business Email Compromise (BEC), Kontoübernahmen, QR-Phishing und MFA-Umgehung – Taktiken, für deren Abwehr diese herkömmlichen E-Mail-Gateways nicht ausgelegt sind. Wenn Sie also ein solches Gateway verwenden, besteht ein höheres Risiko, dass es bei Ihrem Unternehmen zu einer Sicherheitsverletzung kommt und die Betriebskosten in die Höhe schnellen.

Wenn Sie zu Proofpoint wechseln möchten, um bessere Sicherheit zu erhalten, hilft Ihnen dieser Leitfaden bei der Planung Ihrer Migration. Er wurde für Kunden von Barracuda, Cisco (IronPort), Forcepoint (Websense), Symantec Email Security.cloud (MessageLabs), Trellix (FireEye/McAfee) und Trend Micro entwickelt.

Diese schrittweise Anleitung hilft Ihnen dabei, die Effektivität Ihres alten Gateways zu bewerten, dessen Kosten zu ermitteln und einen Zeitplan für die Migration zu erstellen. Proofpoint bietet flexible Bereitstellungsoptionen (SEG, API oder einen schrittweisen Ansatz), sodass Sie die für Ihre Umgebung optimale Wahl treffen können. Um diesen Prozess zu vereinfachen, stellt Ihnen Ihr Proofpoint-Team kostenlose Tools wie unsere Risikoanalyse für E-Mail-Sicherheit, einen Bericht zu Lücken in der Abdeckung sowie einen Bericht zum Geschäftswert zur Verfügung, mit denen Sie die Risikoreduzierung und den ROI quantifizieren können.

Schritt 1: Quantifizieren Sie die Wirksamkeit Ihrer aktuellen Schutzmaßnahmen

Den Anfang macht die Transparenz. Schaffen Sie eine klare Ausgangsbasis und ermitteln Sie, wie gut Ihre aktuellen Schutzmaßnahmen funktionieren und was ihnen entgeht.

- Überprüfen Sie False-Negative-Berichte in Administrator-Protokollen und SIEM/IR-Tickets. Dies kann Ihnen helfen, das Ausmaß und den Umfang der nicht erkannten Bedrohungen zu verstehen.
- Dokumentieren Sie den Anteil echter Treffer bei von Anwendern gemeldeten E-Mails. Dies hilft Ihnen dabei, den Zeitaufwand für die Behebung von False Positives zu ermitteln.
- Identifizieren Sie Kontoübernahme-Zwischenfälle, die von anderen Systemen erkannt wurden. Beispiele hierfür sind der Missbrauch von Postfachregeln, unmögliche Ortsveränderungen oder Anwenderstandorte sowie die Umgehung der Multi-Faktor-Authentifizierung (MFA).
- Überprüfen Sie interne/laterale Phishing-Versuche, die von anderen Systemen erkannt oder von Anwendern gemeldet wurden.
- Führen Sie eine Proofpoint-Risikoschnellanalyse durch. Dadurch erhalten Sie datengestützte Einblicke in die Bedrohungen, die Ihr bisheriges Gateway und Ihre Microsoft 365-Konfiguration möglicherweise übersehen.

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Schritt 2: Berechnen Sie die operativen Kosten der bisherigen Vorgehensweise

Bei der Sicherheit geht es nicht nur darum, was Sie blockieren, sondern auch um die Effizienz Ihrer Prozesse. Ermitteln Sie die Belastung der Analysten sowie den Zeit- und Arbeitsaufwand, der mit manueller Triage, False Positives und fragmentierten Arbeitsabläufen verbunden ist. Dies hilft Ihnen, die tatsächlichen Kosten für den Betrieb Ihres bisherigen Gateways zu bewerten.

- Dokumentieren Sie, wie viele Klicks und Minuten/Stunden Ihre Analysten benötigen, um einen einzelnen Phishing-Vorfall zu untersuchen. (Es ist nicht ungewöhnlich, wenn Analysten für die Lösung eines Vorfalls mehr als 12 Klicks sowie mehrere Stunden benötigen.) Identifizieren Sie außerdem, wo es typischerweise zu Verzögerungen kommt.
- Ermitteln Sie, wie viele Stunden Analysten für die Triage von Nachrichten im Abuse-Postfach aufwenden. Berechnen Sie, wie viel Zeit Analysten jede Woche mit der Überprüfung von E-Mails verbringen, die von Anwendern gemeldet wurden. Finden Sie außerdem heraus, wie hoch der Anteil echter Bedrohungen bzw. Fehlalarme bei diesen Meldungen ist.
- Ermitteln Sie die Zeit, die Ihr Team für die Erstellung von Berichten aufwendet. Wie lange dauert es, Sicherheitsmetriken zusammenzutragen und daraus Berichte für Vorgesetzte oder den Vorstand zu erstellen? Oftmals erfordert dies manuelle Datenexporte und Arbeit mit Tabellenkalkulationen.
- Sprechen Sie mit Sicherheitsanalysten und dokumentieren Sie deren tägliche Ärgernisse. Welche Probleme treten am häufigsten auf? Beispiele hierfür sind irrelevante Daten, False Positives und zu viele verschiedene Konsolen.

Schritt 3: Wählen Sie den Weg für Ihre Migration

Ihre Umgebung und Ihre Prioritäten werden sich verändern – und Ihre E-Mail-Sicherheit muss mit diesen Veränderungen Schritt halten. Mit Proofpoint erhalten Sie eine Flexibilität, die Anbieter mit nur einem Modell nicht bieten können. Nur bei Proofpoint können Sie zwischen drei Migrationspfaden wählen:

- **Option 1: Erweiterung des API-basierten Schutzes:** Diese Option ist mit geringem Aufwand verbunden und bietet enorme Vorteile. Integrieren Sie Proofpoint Core Email Protection – API mit Microsoft 365, um sofortigen Schutz vor Bedrohungen wie Business Email Compromise (BEC), Kontoübernahmen und Phishing zu erhalten. Diese Option unterstützt auch Unternehmen, die von ihrem bisherigen E-Mail-Gateway auf ein Microsoft- und Proofpoint-Modell umsteigen möchten, und bietet kontinuierlichen Schutz während und nach der Migration.
- **Option 2: Zunächst Implementierung der API, später Umstieg auf SEG:** Diese Option ist mit mäßigem Aufwand verbunden, bietet jedoch noch mehr Vorteile. Beginnen Sie mit der Proofpoint-API, um schnell von den operativen Vorteilen und der Risikoreduzierung zu profitieren. Später wechseln Sie schrittweise zu Proofpoint SEG, um Routing-Kontrollfunktionen zu erhalten, sich ändernde Compliance-Anforderungen einzuhalten und die hochentwickelten, mehrschichtigen Schutzmaßnahmen nutzen zu können.
- **Option 3: Vollständiger Austausch des SEG:** Stellen Sie Ihr altes E-Mail-Gateway vollständig außer Betrieb und ändern Sie Ihre MX-Datensätze, um Proofpoint SEG zu nutzen und von maximaler Kontrolle und vollständigem Schutz vor der Zustellung zu profitieren.

Schritt 4: Planen Sie Ihre Migration und starten Sie ein Pilotprojekt

Validieren Sie die Ergebnisse, bevor Sie einen vollständigen Rollout durchführen. Mit einem kontrollierten Pilotprojekt können Sie Proofpoint parallel zu Ihrem bestehenden Gateway testen, die zuverlässigere Erkennung und schnellere Reaktionen nachweisen und das Vertrauen bei der Unternehmensführung mithilfe von Daten stärken.

- Legen Sie Ihre Erfolgskriterien im Voraus fest. Was möchten Sie erreichen? Beispiele hierfür sind Verbesserung der Bedrohungserkennung, Reduzierung der False Positives, Beschleunigung der Behebungsmaßnahmen und Vermeidung von Kontoübernahmen.
- Beobachten Sie potenzielle Verbesserungen bei der Erkennung, indem Sie die E-Mail-Schutzlösung von Proofpoint im Hintergrund betreiben.
- Achten Sie während der Pilotphase auf Folgendes:
    - Übersichtliche Gegenüberstellung der von Proofpoint erkannten und von Ihrem bisherigen E-Mail-Gateway übersehenen Bedrohungen
    - Eine leicht verständliche Zusammenfassung der Lücken in der Abdeckung
    - Bericht zum Geschäftswert, der den Geldwert der Zeitersparnis und des reduzierten Risikos quantifiziert

Schritt 5: Erstellen Sie einen Zeitplan

Planen Sie den schrittweisen Umstieg und berücksichtigen Sie dabei Verlängerungszyklen, Ihre Personalsituation und die Risikotoleranz Ihres Unternehmens. Dank der Migrationsunterstützung von Proofpoint können Sie Ihren Schutz modernisieren, ohne Unterbrechungen in Kauf nehmen zu müssen.

- Erstellen Sie einen 3-Phasen-Plan:
    1. Pilotphase
    2. Parallelbetrieb
    3. Umschaltung
- Berücksichtigen Sie Ihren Zeitplan für Lizenzverlängerungen sowie Ihre Budgetzyklen. Prüfen Sie gegebenenfalls Möglichkeiten zur Auflösung bestehender Verträge durch Ablösung.
- Betreiben Sie Ihr altes System parallel als Sicherheitsnetz, bis die Unternehmensführung von Ihrer neuen Bereitstellung überzeugt ist.
- Nutzen Sie Proofpoint Premium Services, um umfassenden Migrationssupport zu erhalten. Unsere Advisory- und Applied-Services-Teams bieten praktisches Fachwissen, das Ihnen hilft, Konfigurationen zu optimieren, die Bereitstellung zu beschleunigen und während der Umstellung kontinuierlichen Schutz zu gewährleisten.

Zusammenfassung

Wenn Sie sich für Proofpoint entscheiden, müssen Sie die Migration nicht allein durchführen. Wir stellen Ihnen Migrationsleitfäden, Vorlagen für Pilotprojekte und Erfahrungsgeschichten unserer Kunden zur Verfügung. Und ganz gleich, ob Sie mit API beginnen, schrittweise auf SEG umsteigen oder Ihr bisheriges E-Mail-Gateway vollständig ersetzen möchten – wir helfen Ihnen bei der Migration und liefern messbare Ergebnisse.

Gründe für Proofpoint

Informationen zu Proofpoint

Personenzentrierter Schutz

3,4 Bill. E-Mails pro Jahr gescannt

>1,4 Bill. SMS/MMS pro Jahr gescannt

124 Mio. BEC-Angriffe pro Monat abgewehrt

>183 Mio. Phishing-Simulationen pro Jahr gesendet

0,8 Bill. Anhänge pro Jahr gescannt

21 Bill. URLs pro Jahr gescannt

177 Mio. Angriffe per Telefon pro Jahr abgewehrt

Marktdurchdringung

>2,7 Mio. Kunden

>150 Weltweite ISPs und Mobil-funkbetreiber

>80 % der Fortune 100 von Proofpoint geschützt

57 % der Fortune 100 nutzen Proofpoint DLP

>63 % der Fortune 1000 von Proofpoint geschützt

proofpoint.

Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →