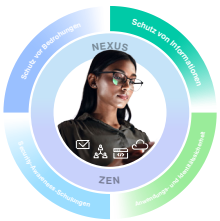
Vermeiden von Datenverlust per E-Mail bei Fusionen und Übernahmen

Proofpoint Adaptive Email DLP verhindert den Verlust vertraulicher Daten bei Fusionen und Übernahmen

Wichtige Vorteile

- Vermeidung von versehentlichem und vorsätzlichem Datenverlust per E-Mail
- Verhinderung von Rufschäden für Ihr Unternehmen
- Verbesserte Sensibilisierung für Sicherheit in Ihrem gesamten Unternehmen
- Effektive E-Mail-Sicherheit mit einfacher Verwaltung und minimalen Störungen der Anwender
- Schnelle Rendite mit vollständigem Schutz in nur 48 Stunden

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



Bei Fusionen und Übernahmen steigt die Zahl der Personen, die vertrauliche Informationen per E-Mail weitergeben, enorm an. Gleichzeitig fällt es IT-Sicherheitsteams schwer, alle beteiligten Mitarbeiter und externen Parteien im Blick zu behalten. Aufgrund dieser Faktoren steigt das Risiko, dass vertrauliche Daten geleakt werden.

Proofpoint Adaptive Email Data Loss Prevention (DLP) löst diese Probleme. Diese Lösung nutzt verhaltensbasierte künstliche Intelligenz (KI), um das E-Mail-Sendeverhalten Ihrer Mitarbeiter, ihre vertrauenswürdigen Beziehungen und ihr Verhalten bei der Weitergabe vertraulicher Daten zu verstehen. Unser Produkt analysiert E-Mails und benachrichtigt Administratoren sofort, wenn ungewöhnliches Verhalten erkannt wird. Gleichzeitig warnt es die Anwender in Echtzeit, noch bevor kritische Daten abfließen können.

Warum Fusionen und Übernahmen das Risiko steigern

Im Zuge von Fusionen und Übernahmen müssen Unternehmen eine Vielzahl von höchst vertraulichen Informationen austauschen, seien es Daten zu Mitarbeitern, Dokumente des Vorstands, Private-Equity-Daten und andere Informationen.

Laut einer Untersuchung von Gartner steigern diese Transaktionen das Risiko von Datenverlust auf folgende Weise:

- Es kann zu Konflikten zwischen den Sicherheitsprozessen der beiden Unternehmen kommen.
- Wenn die Transaktion zu Unsicherheit führt oder geheim gehalten wird, kann das Mitarbeiter beunruhigen und dazu führen, dass sie sich auf ungewöhnliche oder schädliche Weise verhalten.
- Häufig entstehen neue technische Anforderungen. Nach dem Abschluss der Transaktion können Unternehmen beispielsweise vor der Aufgabe stehen, drei unterschiedliche Betriebsmodi für Auflösung, Übergang und Zukunft abzusichern. In dieser Zeit ist die Angriffsfläche wesentlich größer.

So schützt Proofpoint Adaptive Email DLP Ihre vertraulichen Daten

Der Verlust vertraulicher Daten kann den Ruf Ihres Unternehmens schädigen und hohe Kosten nach sich ziehen. Proofpoint Adaptive Email DLP verhindert solche Schäden. Unser Produkt kann mithilfe verhaltensbasierter KI versehentlichen und vorsätzlichen Datenverlust per E-Mail erkennen und stoppen. Die KI analysiert E-Mail-Daten der letzten 12 Monate und lernt auf diese Weise das E-Mail-Sendeverhalten Ihrer Mitarbeiter, ihre vertrauenswürdigen Beziehungen und ihren Umgang mit vertraulichen Daten.

Dank dieses KI-Trainings erkennt Proofpoint Adaptive Email DLP ungewöhnliches E-Mail-Verhalten, sobald es passiert, z. B. wenn Mitarbeiter eine E-Mail an den falschen Empfänger senden, vertrauliche Daten an weniger sichere und unbefugte Konten verschicken oder gezielt Informationen exfiltrieren. Sobald die Lösung Probleme erkennt, zeigt sie den Anwendern in Echtzeit eine Warnmeldung an. Dadurch können sie ihre Aktionen rückgängig machen, um Datenverlust zu vermeiden, ohne dass ein Administrator eingreifen muss.

Bei Fusionen und Übernahmen verhindert Proofpoint Adaptive Email DLP, dass vertrauliche Daten in die falschen Hände gelangen, während wichtige Kommunikation weiterhin fließen kann.

Blockieren fehlgeleiteter E-Mails

Eine E-Mail gilt als fehlgeleitet, wenn ein Anwender sie an den falschen Empfänger sendet. Dies ist eine häufige Ursache von Datenlecks in Unternehmen, die sich mit Regeln und Richtlinien nur schwer verhindern lässt. Da Proofpoint Adaptive Email DLP das E-Mail-Verhalten der Mitarbeiter lernt, kann die Lösung Anwender vor fehlgeleiteten E-Mails warnen, bevor sie abgeschickt werden.

Vermeidung falscher Dateianhänge

Ein Dateianhang gilt als falsch, wenn ein Anwender eine E-Mail zwar an die richtige Person sendet, aber die falsche Datei anhängt. Ebenso wie bei fehlgeleiteten E-Mails nutzt Proofpoint Adaptive Email DLP künstliche Intelligenz zum Erkennen falscher Anhänge, um Anwender in Echtzeit zu warnen.

Stoppen von Exfiltration per E-Mail

E-Mail-Regeln können Datenverlust effektiv stoppen, was jedoch nur bei bekannten, vordefinierten Datentypen wie personenbezogenen Informationen, Zahlungskartendaten sowie Identifikationsnummern funktioniert.

Proofpoint Adaptive Email DLP identifiziert und klassifiziert Ihre vertraulichen Daten und erkennt die privaten E-Mail-Konten der Anwender anhand ihres E-Mail-Verhaltens. Wenn Mitarbeiter versuchen, vertrauliche Daten an sich selbst oder andere Personen zu senden, kann unser Produkt ihre Aktivitäten je nach Konfiguration blockieren oder nachverfolgen.

Abb. 1: Proofpoint Adaptive Email DLP warnt Anwender in Echtzeit vor fehlgeleiteten E-Mails.

Abb. 2: Das Dashboard von Proofpoint Adaptive Email DLP bietet IT-Sicherheitsteams einen vollständigen Überblick über E-Mail-Bedrohungen.

Echtzeitschulungen für Anwender

Dank Echtzeitschulungen können Anwender Fehler und Richtlinienverstöße vermeiden. Proofpoint Adaptive Email DLP ergänzt Security-Awareness-Schulungen, indem die Lösung Anwender über bestehende Risiken in ihren E-Mails informiert. Dank dieser Hinweise können die Anwender ihre Fehler in Echtzeit korrigieren und Datenlecks vermeiden.

Verstehen von Bedrohungen

Im Dashboard von Proofpoint Adaptive Email DLP erhält Ihr IT-Sicherheitsteam einen Überblick über alle E-Mails, die das System überprüft. Dabei zeigt das Dashboard erkannte und blockierte riskante E-Mails (einschließlich fehlgeleiteter E-Mails und falscher Dateianhänge) sowie E-Mail-Exfiltrationsversuche an. Hier sehen Sie auch im Laufe der Zeit erfolgte Sicherheitsverbesserungen für Anwender und das Unternehmen.

Dank Informationen über die wichtigsten benutzerdefinierten Richtlinien sowie die riskantesten Anwender können Analysten sich auf wirklich wichtige Bereiche konzentrieren. Diese Erkenntnisse beschleunigen Untersuchungen und helfen Sicherheitsteams, Anwender bei der Verbesserung ihres Umgangs mit Daten zu unterstützen.

Einfache Verwaltung

Proofpoint Adaptive Email DLP benötigt nur eine minimale Einrichtung und muss kaum konfiguriert werden. In lediglich 48 Stunden beginnt die Lösung, E-Mail-Datenverlust zu verhindern. Sie ermöglicht zuverlässige und effektive Sicherheitsinterventionen, ohne den normalen Arbeitsfluss Ihrer Anwender zu unterbrechen.

MEHR ERFAHREN

Weitere Informationen finden Sie unter **proofpoint.com/de**.