proofpoint.

KURZVORSTELLUNG

Vorteile von Proofpoint Essentials als Sicherheitspartner für Microsoft

Hochentwickelte personenzentrierte Sicherheit für kleine und mittelständische Unternehmen

Lösungen

- Proofpoint Essentials Email Security
- Proofpoint Essentials Security Awareness

Funktionen und Vorteile

- Schutz vor Ransomware, E-Mail-Betrug und Phishing
- Schulung der Mitarbeiter zur Steigerung der Resilienz gegenüber Bedrohungen
- Verringerung des Risikos von Datenschutzverletzungen und Datenverlusten
- Stärkerer, kosteneffizienterer Schutz
- Minimierung des Administrationsaufwands durch einfache Einrichtung und eine zentrale Benutzeroberfläche

Microsoft 365 ist heute die beliebteste Collaboration-Plattform für Unternehmen. Das macht Microsoft zu einem begehrten Ziel für Cyberkriminelle – mit E-Mail als häufigstem Erstzugriffspunkt. Der Fokus auf Microsoft lohnt sich, weil Bedrohungsakteure nur ein einziges Konto kompromittieren müssen, um die Tür zu Millionen Anwendern zu öffnen. Die Taktiken der Angreifer entwickeln sich dabei häufig schneller weiter als sich die nativen Sicherheitstools von Microsoft anpassen können. Kleine und mittelständische Unternehmen (KMUs) sind für derartige Bedrohungen besonders anfällig, sodass die Verbesserung der E-Mail-Sicherheit für sie oberste Priorität haben sollte.

Schutz vor Angriffen gegen Microsoft

In der Regel verfügen KMUs im Gegensatz zu großen Unternehmen nicht über das nötige Budget oder Personal, um hochentwickelte, mehrschichtige Sicherheitslösungen bereitzustellen, sodass sie bei Cybersicherheitsangriffen besonders gefährdet sind. Zudem haben es Cyberkriminelle laut dem Proofpoint-Bedrohungsforschungsteam vor allem auf Unternehmen abgesehen, die sich primär auf die nativen Sicherheitsfunktionen von Microsoft verlassen.

Cyberkriminelle greifen Unternehmen aus einem ganz einfachen Grund über deren Mitarbeiter an: Sie sind das schwächste Glied in der Sicherheitskette, denn sie sind nicht nur manipulierbar, sondern machen mitunter auch banale Fehler.

E-Mail ist der einfachste Weg für Angreifer, diese Mitarbeiter zu erreichen. Mit Social-Engineering-Taktiken gelingt es ihnen, technische Schutzvorkehrungen zu umgehen, direkten Zugriff auf vertrauliche Daten zu erhalten, Daten zu stehlen und Unternehmen um hohe Summen zu betrügen. KMUs, die ausschließlich auf die nativen Sicherheitsfunktionen von Microsoft setzen, sind insbesondere folgenden Risiken ausgesetzt:

- Hochentwickelte Phishing-Bedrohungen
- Business Email Compromise (BEC)
- Malware (z. B. Ransomware)
- Schädliche QR-Codes
- Schädliche URLs
- Angriffe per Telefon

Verbesserung der Microsoft-Sicherheit

Microsoft setzt auf klassische Filtertechniken (z. B. basierend auf der Reputation der IP-Adresse) sowie volumen- und signaturbasierte Virenscans, die jedoch nur grundlegenden Schutz bieten. Angesichts des hohen Innovationstempos der Bedrohungsakteure können diese Tools kaum Schritt halten. Massenhaft versendete Spam-Nachrichten, in komplexen Link-Ketten verborgene Bedrohungen und Betrugstaktiken können weiterhin ihren Weg ins Unternehmen finden. Dadurch steigt nicht nur das Risiko, auch die Benutzerproduktivität ist beeinträchtigt, und der Administrationsaufwand nimmt zu.

33 %

der kleinen Unternehmen verzeichneten 2024 einen Cyberangriff

>250.000 USD

durchschnittliche Kosten durch einen Cyberangriff für kleine Unternehmen

>3,5 Mrd.

E-Mails täglich gescannt

Proofpoint Essentials kann hier helfen: Die Lösung ergänzt die nativ in Microsoft 365 angebotenen Sicherheitsfunktionen und stoppt eine Vielzahl raffinierter Angriffe, darunter Business Email Compromise (BEC), E-Mail-Betrug und Ransomware. Proofpoint Essentials stoppt aber nicht nur mehr Bedrohungen, sondern entfernt auch automatisch E-Mail-Bedrohungen, die Ihre Schutzmaßnahmen überwinden. Dadurch kann sich Ihr Team auf wichtigere Aufgaben konzentrieren.

Proofpoint Essentials macht leistungsstarke Cybersicherheit der Enterprise-Klasse für jedes Unternehmen zum Kinderspiel. Kleine ebenso wie große Unternehmen können die Vorteile von Microsoft 365 weiterhin in vollem Umfang nutzen und dennoch wichtige Sicherheitsanforderungen erfüllen.

Leistungsstarker, KI-gestützter Schutz

Microsoft-Kunden, die ihre E-Mail-Sicherheit stärken wollen, setzen mehrheitlich auf Proofpoint. Mehr als 85 % der Fortune 100-Unternehmen und mehr als 2 Millionen Kunden weltweit haben Proofpoint zu ihrem Sicherheitspartner gewählt, weil unsere Lösungen 99,99 % aller E-Mail-Bedrohungen, Spam- und Graymail-Nachrichten stoppen.

Dieselbe moderne KI-Plattform, die für den Schutz dieser Großunternehmen sorgt, schützt auch unsere KMU-Kunden: Proofpoint Nexus®. Diese Technologie kombiniert Beziehungsdiagramme, Machine Learning, Bilderkennung sowie semantische Analysen und bietet größere Genauigkeit, da sie sich dabei auf Bedrohungsdaten aus mehr als 3,5 Milliarden täglich analysierten E-Mails stützt. Dadurch ist sie in der Lage, Angriffe im gesamten E-Mail-Lebenszyklus zu stoppen: vor, während und nach der Zustellung im Postfach.

Einfache Einrichtung per Plug & Play

Mit Proofpoint Essentials profitieren Unternehmen von zusätzlichem Schutz und können die Bereitstellungsoption wählen, die für ihre spezifische Sicherheitsumgebung am besten passt.

Integrierte Bereitstellung (per API): Diese auf Microsoft 365-Umgebungen zugeschnittene Methode bietet leistungsstarken Schutz und lässt sich mit wenigen Klicks einrichten. Da die MX-Datensätze nicht geändert werden müssen, können Sie Ihre Mitarbeiter noch schneller schützen.

Sicheres E-Mail-Gateway (SEG): Diese leistungsstarke MX-basierte Option ist mit den meisten E-Mail-Anbietern kompatibel und bietet Ihnen mehr Möglichkeiten, Ihren Schutz zu konfigurieren und an die Anforderungen Ihres Unternehmens anzupassen.

Wahlfreiheit und sofort einsetzbare Konfigurationen sorgen dafür, dass Proofpoint Essentials nach dem Einrichten von ganz allein läuft.

Umfassend und kostengünstig

Proofpoint Essentials bietet mehr als E-Mail-Sicherheit. Die Lösung umfasst eine ganze Palette aus Sicherheitstools, die speziell auf die Anforderungen kleinerer Teams zugeschnitten sind. So können KMUs ihre Anbieter konsolidieren und dadurch erhebliche Kosteneinsparungen erzielen. Die Proofpoint Essentials-Plattform bietet Ihnen folgende Vorteile:

- Schutz Ihrer vertraulichen ausgehenden Informationen und Verhinderung von Datenverlust
- Veränderung des Anwenderverhaltens durch Sicherheitsschulungen
- Sicherstellung der Compliance durch E-Mail-Archivierung
- Fortsetzung des Betriebs bei Störungen durch Kontinuitätstools

Proofpoint Essentials bietet zusätzlich zur Konsolidierung viele weitere Vorteile, z. B. weniger Zwischenfälle (und dadurch weniger Unterbrechungen), niedrigere Personalkosten und mehr Zeit für Ihre Teams, sich auf Aufgaben mit hoher Priorität zu konzentrieren. Im Jahr 2024 war ein Drittel aller Kleinunternehmen von einem Cyberangriff betroffen – wobei pro Angriff im Durchschnitt Kosten von mehr als 250.000 US-Dollar entstanden. Wenn Sie auch nur einen Zwischenfall verhindern, haben Sie die Kosten für effektiven Schutz bereits mehrfach amortisiert. Mit Proofpoint können KMUs nicht nur ruhig schlafen, sondern auch ihre Bilanz verbessern.

Komponenten von Proofpoint Essentials

FUNKTION	BESCHREIBUNG
E-Mail-Schutz	Bietet Schutz für Postfächer von Anwendern durch mehrschichtige Spam- und Virenschutzfunktionen, mit denen sich verschiedenste bekannte und unbekannte Sicherheitsbedrohungen stoppen lassen.
Erkennung hochentwickelter Bedrohungen	Schützt vor gezielten Angriffen wie komplexe Malware, Business Email Compromise (BEC), hochentwickeltes Phishing usw. durch KI-gestützte Erkennung und kontinuierliche Sandbox-Analysen von URLs und Anhängen.
Automatische Behebung	Entfernt automatisch schädliche Nachrichten, die auf Zeitverzögerungstechniken basieren oder von den vorgelagerten Sicherheitsebenen nicht erkannt wurden. Dadurch wird der Administrationsaufwand erheblich reduziert.
Security-Awareness-Schulungen	Mehr als 900 interaktive Schulungsmodule und tausende reale Phishing-Simulationen helfen Anwendern, sich selbst zu schützen, Risiken zu identifizieren und ihr Cybersicherheitsverhalten zu verbessern.
Datenverlust-prävention und Verschlüsselung	Stoppt den Verlust vertraulicher Daten wie personenbezogene Daten, Gesundheits- oder Finanz-informationen durch automatische Sperren, Verschlüsselung ausgehender E-Mails und Filterung.
Kontinuierliche E-Mail-Verfügbarkeit	Integrierte Kontinuitätsfunktionen halten den Betrieb Ihres Unternehmens bei unerwarteten E-Mail-Störungen bis zu 30 Tage lang aufrecht.
E-Mail-Archivierung	Gewährleistet Compliance, indem E-Mails bis zu 10 Jahre lang mit einfachen Wiederherstellungsprozessen und minimalem Speicherplatzbedarf gespeichert werden.

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 85 Prozent der Fortune 100-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.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →