proofpoint.

Microsoft 365 und Proofpoint

Gemeinsam sicherer

Das sollten Sie jetzt über Microsoft 365 wissen!

Microsoft hat vor Kurzem die Cloud-Kooperationsplattform Office 365 in Microsoft 365 umbenannt.

Neuer Name, aber dieselben Funktionen

Der **weltweit beliebteste** Cloud-Dienst für Unternehmen

Mehr als **180 Millionen** Nutzer

Von **1,4 Millionen** Unternehmen, Bildungseinrichtungen und Behörden verwendet

Doch Microsoft 365 hat Schwächen:

Erkennung und Blockierung von Hackern + Fehlende Tools zur schnellen Untersuchung und Behebung erfolgreicher Angriffe

Dadurch ist die Plattform eine große Angriffsfläche

1 = **ALLE** = **ZUGRIFF**

1: einziges kompromittiertes Microsoft 365-Konto

ALLE: Anwender im Unternehmen sowie vertrauenswürdige Partner können identifiziert und angegriffen werden

ZUGRIFF: auf eine wahre Goldgrube mit vertraulichen Daten

Die Microsoft 365-Sicherheitsfunktionen lassen sich leicht umgehen.

Sie sind einfach nicht zuverlässig genug.

Unternehmen sollten sich bewusst sein, dass der ausschließliche Einsatz der integrierten Sicherheitsfunktionen von Microsoft 365 – Exchange Online Protection (EOP) und Advanced Threat Protection (ATP) – zu erheblichen Sicherheitslücken und somit zu erheblichen geschäftlichen Risiken führen kann.

SE Labs hat Folgendes festgestellt:[1]

Microsoft EOP erreichte eine Zuverlässigkeit – also eine Kombination aus Erkennung und False Positives – von nur **8 %**

Microsoft ATP erreichte einen Wert von nur **35 %**

Drittanbieterlösungen schafften Werte von mehr als **90 %**

Zudem haben Untersuchungen von Proofpoint ergeben, dass **50 %** der legitimen Websites, die schädliche URLs hosten, von Microsoft gehostet werden![2]

Verlassen Sie sich nicht auf die Microsoft 365-eigenen Sicherheitsfunktionen!

Collaboration-Funktionen in Microsoft 365 ☑

Sicherheits- und Compliance-Funktionen in Microsoft 365 ☒

Microsoft 365 + Proofpoint = sichere Zusammenarbeit SIEGER

FAKT:
Die integrierte Sicherheitsplattform von Proofpoint schließt die Sicherheitslücken von Microsoft 365.

Wie sieht die moderne Bedrohungslandschaft aus?

94 % der Datenschutzverletzungen beginnen mit einer E-Mail.

99 % aller von Proofpoint beobachteten Bedrohungen erfordern eine menschliche Interaktion

ca. 80 % aller externen Datenschutzverletzungen werden durch Brute-Force-Angriffe oder gestohlene Anmeldedaten verursacht[3]

Proofpoint ist FLEXIBEL und auf die Bedrohungslandschaft vorbereitet

MARKTFÜHRER:
Proofpoint ist meist der erste Anbieter auf dem Markt mit neuen Funktionen für die neue Bedrohungslage

— VS —

NACHZÜGLER:
Microsoft 365 hängt beim Bedrohungsschutz 12–18 Monate hinterher

Proofpoint stoppt mühelos mehr Bedrohungen!

PROOFPOINT IST Nr. 1

dank des mehrstufigen Cybersicherheitsansatzes die Nummer 1

Laut dem Proofpoint-Tool zum Melden schädlicher E-Mails in Outlook verzeichnen Anwender, die nur Microsoft 365-Schutz einsetzen, 305 % mehr schädliche E-Mails als Anwender mit Proofpoint Advanced Email Security.

Microsoft 365 ATP vs. Proofpoint[1]

	Microsoft 365 Advanced Threat Protection	Proofpoint
SOZIALE NETZWERKE	83 %	100 %
PHISHING	83 %	95 %
MALWARE	27 %	100 %
STANDARD-BEDROHUNGEN	99 %	100 %

Verbessern Sie mit Proofpoint Ihre Microsoft 365-Sicherheit

Proofpoint verfolgt einen **personenorientierten Ansatz**

Bietet Kontext zum Schweregrad und zur Raffinesse von Bedrohungen und zeigt, ob der betroffene Anwender ein VIP ist (oder auch nicht)

Proofpoint konzentriert sich ganz auf personenorientierte **Sicherheit**

Schützt den Bedrohungsvektor Nr. 1 – die Mitarbeiter und die Daten, die Mitarbeiter erstellen und abrufen

Proofpoint bietet eine integrierte **Sicherheitsplattform**

Schließt alle Microsoft 365-Schwachstellen

Proofpoint liefert detaillierte **forensische Daten**

Unterstützt Unternehmen bei der Abwehr von Bedrohungen durch schädliche URLs, die derzeit 80 % aller Bedrohungen ausmachen

Verlassen Sie sich nicht nur auf unser Wort!

Mit der kostenlosen Analyse der E-Mail-Sicherheitsbedrohungen möchten wir Ihnen zeigen, was genau an Microsoft EOP und ATP vorbei in Ihr Netzwerk gelangt.

- ○ Zeigt, was Proofpoint in Microsoft 365 blockiert hätte und warum
- ○ Bietet einen Überblick über potenziell kompromittierte oder angegriffene Anwenderkonten
- ○ Einrichtungszeit ca. 1 Stunde – MX-Datensatz bleibt unverändert

Wenden Sie sich noch heute an Ihren Proofpoint-Channel-Partner und vereinbaren Sie eine Sicherheitsanalyse.

Quellen

1. https://selabs.uk/reports/email-security-services-2/
2. Proofpoint-Bedrohungsdaten
3. 2020 Verizon Data Breach Investigations Report (Untersuchungsbericht zu Datenkompromittierungen von Verizon für 2020)