Proofpoint-Lösungen für Sicherheit und Compliance mit Microsoft 365

Wenn Ihr Unternehmen zu Microsoft 365 (Office 365) wechselt, müssen Sie Ihre Sicherheits- und Compliance-Maßnahmen anpassen.

WICHTIGE VORTEILE

- Hervorragende Blockierung von Malware und anderen Bedrohungen
- Transparenz und Einblicke über alle Kanäle hinweg
- Risikobasierte Zugriffsberechtigungen
- Automatisierte Reaktion zur Eindämmung und Behebung von Bedrohungen
- Bedrohungsschutz und DLP für E-Mails und Cloud-Anwendungen
- Leicht implementierbare Tools für Archivierung, Überwachung und Compliance

Microsoft 365 verändert die Art und Weise, wie Menschen zusammenarbeiten. Die neue Architektur bringt aber auch neue Risiken mit sich. Sicherheits- und Compliance-Tools für E-Mails und Cloud-Anwendungen, die ihre Aufgaben nur unzureichend erfüllen, können die Vorteile von Microsoft 365 zunichtemachen. Datenschutzverletzungen, kompromittierte Konten oder Compliance-Verstöße können die Reputation Ihrer Marke erheblich schädigen und Ihr Unternehmen finanziell schwer treffen.

Heutige Cyberangriffe richten sich gegen Menschen, um so die vorhandenen Netzwerksicherheitskontrollen zu umgehen. Mit unserem personenorientierten Sicherheits- und Compliance-Ansatz erhalten Sie die erforderlichen Tools, damit Ihre Microsoft 365-Implementierung ein voller Erfolg wird.

SICHERHEIT

Schutz vor Bedrohungen

Wir blockieren raffinierte Angriffe, die den Faktor Mensch und technische Schwachstellen auszunutzen versuchen. Mit unseren E-Mail- und Cloud-Sicherheitslösungen können Sie kompromittierte Konten schnell identifizieren und eine effektive und effiziente Reaktion auf die Kompromittierung in die Wege leiten. So kann das Risiko für internen Betrug oder Datenexfiltration reduziert werden. Zudem schützen wir vor einer ganzen Reihe von Bedrohungen wie:

- Schädlichen Links und Anhängen in Exchange-Postfächern und Apps, einschließlich SharePoint Online und OneDrive

INTEGRATIONSMÖGLICHKEITEN

Zusätzliche Erkenntnisse zu Bedrohungen

- Palo Alto Networks
- Splunk

Durchsetzung von URL-Regeln

- Blue Coat
- Open DNS

Durchsetzung von Netzwerkregeln

- Cisco
- Check Point
- Fortinet
- Juniper
- Palo Alto Networks

Durchsetzung von Benutzerzugriffsregeln

- Active Directory
- CyberArk
- Imperva

- Bedrohungen ohne Malware wie E-Mail-Betrug und Anmeldedaten-Phishing
- Add-on-Apps von Drittanbietern, die auf die Daten Ihres Unternehmens zugreifen, ohne dass Sie dies wissen oder diese Vorgänge kontrollieren können

Wir bieten branchenführenden Schutz mit folgenden Funktionen:

- Mehrstufige Bedrohungsanalysen, die Verhalten, Quellcode und Protokolle untersuchen
- Machine Learning-Algorithmen, die E-Mail-Betrug und -Spoofing erkennen
- Kanalübergreifende Bedrohungskorrelation und Sicherheitstools für Cloud-Zugriff, damit Sie kompromittierte Konten schnell identifizieren und das Problem beheben können
- Prädiktive Analyse zur Identifizierung verdächtiger URLs und Anhänge sowie deren Prüfung in Sandboxes, bevor Benutzer darauf klicken können
- E-Mail-Authentifizierung, die Ihr Unternehmen, Endnutzer und Kunden vor Angreifern schützt, die Ihre Identität missbrauchen
- Phishing-Simulationen, mit denen Anwender lernen, Social-Engineering-Angriffe zu erkennen und zu melden
- Tools für automatisierte Reaktion, die den Zeitraum bis zur Infektionsbestätigung verkürzen, betroffene Postfächer bereinigen und erweiterte Authentifizierung durchführen

Bedrohungsanalyse

Unsere Bedrohungsdaten decken E-Mails, Netzwerke, Cloud-Anwendungen, Mobilgeräte-Apps und Social Media ab. Durch die Integration der Bedrohungsdaten auf all diesen Kanälen können wir Angriffe auf mehreren Vektoren überwachen und verhindern, dass Angreifer mit kompromittierten Anmeldedaten auf vertrauliche Informationen zugreifen. Wenn zum Beispiel ein Endnutzer per Phishing im Exchange-Postfach angegriffen wird, stellen wir sicher, dass die kompromittierten Anmeldedaten nicht zum Stehlen von SharePoint Online- oder OneDrive-Daten missbraucht werden.

Transparenz und Integration

Da Sicherheit mittlerweile auch in der Unternehmensführung diskutiert wird, ist es jetzt noch wichtiger, die Fragen nach dem „Wer, was, wann, wo und wie“ für Zwischenfälle beantworten zu können. Dank der von uns bereitgestellten umfassenden Transparenz und der Echtzeit-Forensikdaten wissen Sie, ob ein Angriff gegen Ihr Unternehmen Bestandteil einer breiter angelegten Kampagne ist, nur Ihre Branche ins Visier genommen wurde oder ausschließlich gegen Ihr Unternehmen gerichtet ist. Außerdem können Sie schnell feststellen, welche Anwender von welchem Gerät auf welchen Link geklickt haben. Zudem erhalten Sie folgende Informationen:

- DNS-Suchen
- Änderungen am Registry Key
- Von Analysten kuratierte Kompromittierungsindikatoren (IOCs)
- und mehr

Dediziertes Sicherheits-Know-how ist schwer zu finden. Unser Threat Operations Center wird rund um die Uhr von einem Team erstklassiger Bedrohungsforscher betrieben. Unsere Mitarbeiter fungieren dabei als Erweiterung Ihres Sicherheitsteams und nutzen hochentwickelte Bedrohungsanalysen, um Ihnen die Kontextinformationen und Erkenntnisse zur Verfügung zu stellen, die Sie zum Verständnis der Angriffe, Akteure bzw. Kampagnenaktivitäten in Ihrer Umgebung benötigten.

Nur mit einem integrierten Ansatz können Sie ein nachhaltiges Sicherheitsprogramm aufbauen. Die Integrationsmöglichkeiten unseres erweiterbaren Ökosystems sorgen dafür, dass Ihre Sicherheitsinvestitionen intelligenter sowie schneller funktionieren und Ihre Rendite steigern.

USER EXPERIENCE

Sie müssen gewährleisten, dass Ihre Geschäftsabläufe auch bei unerwarteten Ereignissen nicht unterbrochen werden. Dies darf nicht zulasten der Flexibilität, Benutzerfreundlichkeit sowie Kosteneinsparungen gehen, die Microsoft 365 bietet. Wir können Sie dabei unterstützen, dass Ihre Führungskräfte und Endnutzer Microsoft 365 gleichermaßen nahtlos einsetzen können.

Mit unseren Funktionen für automatisierte Reaktion können Sie Bedrohungen eindämmen und beheben, bevor sie Ihre Geschäftsabläufe unterbrechen oder Schaden anrichten. Gleichzeitig gewährleisten die Business-Continuity-Funktionen, dass Ihre Anwender auch dann E-Mails, Kontakte und Kalender nutzen können, wenn der Microsoft 365-Service vorübergehend unterbrochen wird. Mit den adaptiven E-Mail-Hygiene-Tools können Anwender schnell auf die gewünschten E-Mails zugreifen, ohne von Massen-E-Mails abgelenkt zu werden. Zudem setzen unsere Cloud-Sicherheits- und DLP-Lösungen auf risikobasierte Authentifizierung, damit legitime Anwender zuverlässig auf erforderliche Dateien zugreifen können und gleichzeitig gewährleistet ist, dass Ihre Daten vor unbefugtem Zugriff geschützt sind.

COMPLIANCE

In allen Regionen und Branchen werden immer striktere und komplexere Vorschriften wie die DSGVO und FINRA eingeführt. Wir unterstützen Sie dabei, Ihre Compliance-Maßnahmen an veränderte gesetzliche und branchenspezifische Vorschriften anzupassen. Mit unseren Tools können Sie Informationen, die in Ihren internen Netzwerken und externen Infrastrukturen wie OneDrive gespeichert sind, zuverlässig finden, verwalten und absichern.

Gleichzeitig verhindern wir, dass vertrauliche Informationen Ihre Umgebung verlassen. Dank durchgängiger Verschlüsselung und ganzheitlichen DLP-Lösungen wird gewährleistet, dass Ihre übertragenen und gespeicherten vertraulichen Daten geschützt sind.

Wenn Ihr Unternehmen Aufbewahrungsrichtlinien für Dateien und andere Inhalte einhalten muss, können Sie mit unseren Enterprise-Archivierungslösungen die Kommunikation in allen Microsoft 365-Services erfassen und archivieren sowie die E-Discovery vereinfachen. Dabei werden folgende Services berücksichtigt:

- Exchange (online und lokal)
- OneDrive
- Yammer
- Skype for Business
- und weitere Services

Für Unternehmen im Finanzsektor und in anderen stark regulierten Branchen können unsere Überwachungstools die Compliance-Workflows vereinfachen und so kostenintensive Geldstrafen vermeiden helfen.

WEITERE INFORMATIONEN

Nutzen Sie die Funktionen für Sicherheit, geschäftliche Resilienz und Compliance, damit Ihre Microsoft 365-Implementierung ein voller Erfolg wird. Wir können Sie dabei unterstützen, die Sicherheits- und Compliance-Maßnahmen vor, während und nach dem Wechsel zu Microsoft 365 zu vereinheitlichen. Weitere Informationen sowie die Möglichkeit, sich für ein kostenloses Microsoft 365-Security-Assessment zu registrieren, finden Sie unter proofpoint.com/office365.

WEITERE INFORMATIONEN

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