FORTINET

Security für Microsoft 365: Drei wichtige Fragen, die Sie bedenken sollten

Inhaltsverzeichnis

Zusammenfassung

Microsoft 365 ist bereits marktbeherrschend und wird dieses Jahr voraussichtlich einen Marktanteil von 75 % erreichen. Die cloudbasierte Produktivitäts-Suite interagiert mit einer Vielzahl von Unternehmensdaten, einschließlich E-Mail (Outlook Online), einzelnen gespeicherten Dateien (OneDrive) und sogar Finanzdaten (Excel Online). In Microsoft 365 sind bereits praktische Security-Tools integriert, die jedoch für einen effektiven Schutz nicht ausreichen. Unternehmen sollten sich deshalb vor der Implementierung von Microsoft 365 folgende Fragen stellen:

- **Kann Microsoft 365 Malware, Spam und Phishing-E-Mails blockieren?** Bei Tests der SE Labs hat Microsoft 365 trotz aktiviertem Advanced Threat Protection (ATP) weniger als 30 % der mit Spam, Phishing und Malware infizierten E-Mails korrekt erkannt. Über 90 % der Malware wird jedoch immer noch per E-Mail verbreitet – und E-Mail-Bedrohungen sind komplexer geworden. Unternehmen müssen daher prüfen, ob die E-Mail-Security von Microsoft angemessen ist, oder ob die Microsoft 365-Umgebung mit einem sicheren E-Mail-Gateway (SEG) geschützt werden muss.[1]
- **Gehören alle Benutzer, die auf Microsoft 365 zugreifen, zu meinen Mitarbeitern? Und werden dabei Geräte verwendet, die unseren Sicherheitsrichtlinien entsprechen?** Die Zugriffskontrolle und der Endpunkt-Schutz sollten Teil jeder Microsoft 365-Implementierung sein. Gestohlene Anmeldedaten sind eine Hauptursache für Datenverluste, wenn die Legitimität und Berechtigungen von Benutzern nur einmalig bei der Netzwerk-Anmeldung überprüft werden. Eine simple Kombination aus Benutzername und ein Passwort sind heute nicht mehr ausreichend.
- **Enthält meine Microsoft 365-Implementierung vertrauliche Daten? Und wer greift darauf zu?** Der Schutz vor Datenverlusten sollte bei der Security für Microsoft 365 im Mittelpunkt stehen. Wie bei den meisten Cloud-Lösungen erlaubt die Standardeinstellung in Microsoft 365 die unbegrenzte interne und externe gemeinsame Nutzung von Dateien und anderen Daten. Unternehmen müssen daher strategisch vorgehen, um Datenverluste zu verhindern.

Die beste Lösung ist ein integrierter Ansatz, der isolierte Daten – sogenannte „Silos“ – eliminiert und alle Sicherheitselemente zusammenbringt. Die Fortinet Security Fabric kann genau das, was auch die sehr guten Bewertungen unabhängiger Dritter belegen. Unternehmen erhalten damit eine Sicherheitslösung, mit der sich die gesamte Security-Infrastruktur zentral überwachen und steuern lässt.

Die Cloud bringt mehr Produktivität – und neue Risiken

Microsoft 365 ist eine leistungsstarke, cloudbasierte Lösung für die Unternehmensproduktivität. Laut Osterman Research verwendeten im Januar 2018 bereits 62,4 % der Unternehmen Microsoft 365 und bis Anfang 2019 prognostizierte das Marktforschungsinstitut einen Anstieg auf 78,1 %.[2]

Wer Cloud-Dienste – insbesondere Microsoft 365 – nutzt, verlagert meistens Workloads in die Cloud, um von kalkulierbaren Kosten, elastischen Kapazitäten sowie Zeitersparnis und personellen Entlastungen beim Infrastruktur-Management zu profitieren. Damit lassen sich nicht nur Kostensenkungen erreichen, auch kann sich das Unternehmen so besser auf sein Kerngeschäft konzentrieren. Allerdings birgt die Verwendung von Microsoft 365 und seiner cloudbasierten Produktivitäts-Tools, E-Mail-Infrastruktur und Datenspeicherung auch erhebliche Risiken in sich, wie z. B.:

- Datendiebstahl und andere Risiken durch falsche Identitäten, wenn Cyber-Kriminelle an die Daten legitimer Benutzer gelangt sind
- interne und externe Verbreitung von Geschäftsinformationen über Microsoft 365
- Einschleusung von Malware per E-Mail mit Outlook Online als Teil von Microsoft 365

In Microsoft 365 E3 sind bereits einige wichtige grundlegende Sicherheitskontrollen integriert. Gegen Aufpreis bietet Microsoft zusätzliche Schutzfunktionen, die in der E5-Version und anderen Lizenzen enthalten sind. Aber reicht dieser Schutz wirklich aus? Im Folgenden finden Sie drei sicherheitsrelevante Fragen, die Sie sich bei der Implementierung von Microsoft 365 stellen sollten.

Kann Microsoft 365 Malware, Spam und Phishing-E-Mails blockieren?

Cyber-Kriminelle lernen ständig dazu und entwickeln ihre Infrastrukturen laufend weiter. Die Internetkriminalität hat damit einen Reifegrad erreicht, durch den die Masse an Bedrohungen und die Schnelligkeit von Angriffen immer mehr zunehmen.

E-Mail ist seit langem ein idealer Angriffsvektor, sowohl für breit angelegte als auch für gezielte Angriffe. In den letzten Jahren waren E-Mails der häufigste Vektor beim Diebstahl von Anmeldeinformationen und Daten sowie bei der Verbreitung von Malware. Die wichtige Frage ist: „Kann Microsoft 365 Malware, Spam und Phishing-E-Mails blockieren?“ Die Antwort lautet: „Nein, bei weitem nicht gut genug.“

Microsoft bietet verschiedene Sicherheitsoptionen zum Härten von M365 an. Unabhängige Tests finden jedoch nur wenige Hinweise auf die Wirksamkeit der Sicherheitslösungen von Microsoft. Microsoft 365 Business Standard bietet keinen Phishing-Schutz und keinen Schutz vor erweiterten Malware-Bedrohungen. Microsoft 365 Business Premium hat diese Sicherheitsfunktionen zwar, aber sie bringen nur wenig. Tests der SE Labs ergaben, dass Microsoft grundsätzlich einen schlechten Schutz bietet – mit oder ohne erweitertem Bedrohungsschutz.[3]

Das bestätigt auch Gartner. Laut dem Marktforschungsinstitut vernachlässigten die meisten Security-Anbieter mit einem großen Portfolio die Entwicklung von sicheren E-Mail-Gateways (SEG) zugunsten anderer Produkte. Die veränderte Bedrohungslage hat sie dann später kalt erwischt, worauf schnell moderne SEGs „zusammengeschustert“ wurden. Dagegen konnten Anbieter, die die ganze Zeit über in ihre SEG-Produkte investiert hatten, dies als Wettbewerbsvorteil nutzen.[4]

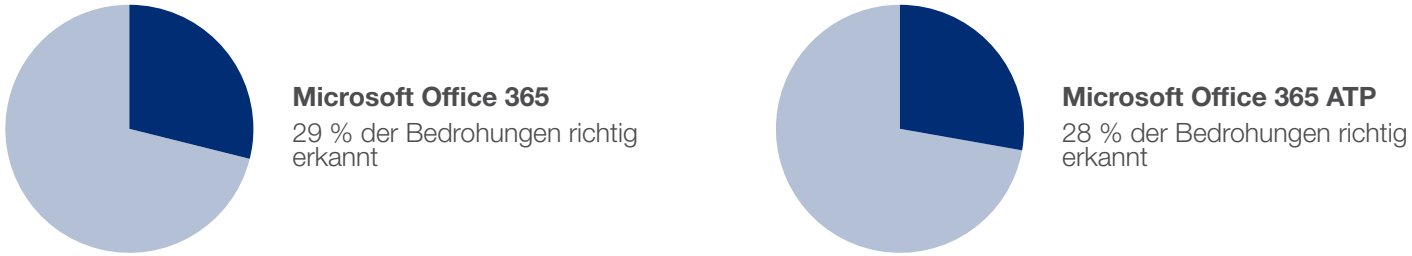

Abbildung 1: Bei Tests der SE Labs von E-Mail-Sicherheitslösungen schnitten Microsoft EoP und ATP bei der korrekten Erkennung von Bedrohungen schlechter als alle anderen Anbieter ab.

Kein Austausch möglich? Ergänzen Sie Sicherheitslücken Ihres jetzigen SEG mit Security-Produkten, die speziell für eine erweiterte Bedrohungsabwehr entwickelt wurden.[5]

Gehören alle Benutzer, die auf Microsoft 365 zugreifen, zu meinen Mitarbeitern? Und werden dabei Geräte verwendet, die unseren Sicherheitsrichtlinien entsprechen?

Laut einer Studie von Verizon waren gestohlene Anmeldedaten im Jahr 2017 die häufigste Ursache für Sicherheitsverletzungen.[6] Legitime Benutzer mit umfassenden Berechtigungen stellen ein besonders hohes Risiko dar, da sie Zugriff auf mehr Daten haben und nach der Anmeldung im gesamten Netzwerk als vertrauenswürdig gelten. Ein Benutzername und ein Passwort reichen heute nicht mehr aus, sondern sollten durch einen mehrstufigen Sicherheitsansatz ersetzt werden.

Die Integration oder gemeinsame Nutzung mehrerer externer Clouds beginnt im Idealfall mit dem Verzeichnisdienst (Directory Service) des Unternehmens. So wird sichergestellt, dass es eine einzige, zuverlässige Datenquelle für Zugriffsrechte gibt – Stichwort „Single Source of Truth“. Darüber hinaus sollten Benutzer idealerweise sowohl durch eine starke Multi-Faktor-Authentifizierung als auch durch eine Aktivitätsprotokollierung überprüft werden.[7] Bei der Multifaktor-Authentifizierung wird die Benutzeridentität mit einem zweiten Schritt verifiziert – z. B. mit einem Hardware- oder Software-Token. Bei der Aktivitätsprotokollierung wird maschinelles Lernen verwendet, um frühere Anmeldeaktivitäten des Benutzers zu analysieren und Anomalien wie Unterschiede bei der Tageszeit oder der Art der abgerufenen Daten zu erkennen.

Sie sollten zumindest die zweistufige Basis-Authentifizierung in Microsoft 365 aktivieren. Viele Unternehmen verwenden jedoch robustere Lösungen für das Identitäts- und Zugangsmanagement, die für eine höhere Sicherheit bei der Identitätskontrolle sowie dem Netzwerk- und Cloud-Zugriff sorgen. Bessere Security-Lösungen funktionieren in verschiedenen Umgebungen und bieten stärkere (und oft einfachere) Methoden für die Multi-Faktor-Authentifizierung. Immer mehr Firmen entscheiden sich auch für einen IDaaS-Dienst (Identity and Access Management as a Service), der den Schwerpunkt auf die Authentifizierung legt. Das Geräte-Management ist ebenfalls kritisch für die Zugriffskontrolle, um zu gewährleisten, dass vertrauliche Daten nur mit aktualisierten, sicheren und regelkonformen Geräten abgerufen werden können.

Identitätskontrolle und -Management bilden die Grundlage bei der geregelten Nutzung externer Clouds.[8]

Enthält meine Microsoft 365-Implementierung vertrauliche Daten? Und wer greift darauf zu?

Laut Gartner machen es die meisten SaaS-Anwendungen einem Benutzern recht einfach, Daten intern – und sogar extern – auf unangemessene Weise mit anderen zu teilen, ohne dass für den Zugriff eine Authentifizierung erforderlich ist. Häufig enthalten diese Anwendungen vertrauliche und/oder geschützte Informationen wie Finanzdaten, geistiges Eigentum oder Kundendaten. Ohne geeignete Sicherheitskontrollen kann Ihre Microsoft 365-Implementierung zu einer „zentralen Verteilerstelle“ für Ihre vertraulichsten Daten werden.

Das Information Rights Management (IRM) von Microsoft 365 bietet im Security & Compliance Center Vorlagen für DLP-Richtlinien zum Schutz vor Datenverlust sowie DLP-Berichte – für den Anfang gar nicht schlecht. Zumindest ist damit Ihre Microsoft 365-Umgebung geschützt. Ihre Daten befinden sich jedoch nicht nur in der Microsoft Suite, sondern auch in Ihrem On-Premises-Netzwerk und in anderen Clouds. Um sämtliche Daten zu schützen, müssen Sie zwei Dinge wissen: wo sich die Daten befinden und um welche Art von Daten es sich handelt. Dies ist auch erforderlich, um die Standards und Vorschriften für einige Arten von Daten einzuhalten – Stichwort „Compliance“.

Laut dem Fortinet Threat Landscape Report nutzt ein Unternehmen durchschnittlich 37 Cloud-Anwendungen.[9] Bei diesen Zahlen wird schnell klar, warum ein einziger Mechanismus zum Identifizieren und Schützen von Daten in mehreren Cloud-Anwendungen sinnvoll ist. Wird diese Security-Funktion auch On-Premises in Datenkontrollen integriert, profitiert das Unternehmen zusätzlich von einer konsequenten Durchsetzung und einem konsolidierten Reporting.

Laut Gartner bieten CASBs einen einheitlichen, unkomplizierten Kontrollpunkt über Benutzeraktivitäten und Benutzerdaten in einer wachsenden Anzahl von SaaS- und anderen cloudbasierten Anwendungen.[10]

CASBs sind zu einem wesentlichen Bestandteil jeder Cloud-Sicherheitsstrategie geworden und helfen Unternehmen dabei, die Nutzung der Cloud zu steuern und sensible Daten in der Cloud zu schützen.[11]

Fazit

Da mehr als drei von vier Unternehmen auf Microsoft 365 umsteigen oder bereits umgestiegen sind, ist die Security dieses leistungsstarken, cloudbasierten Business-Systems von zentraler Bedeutung. Obwohl bei der Microsoft-Standardlizenz E3 viele grundlegende Sicherheitskontrollen enthalten sind (die unbedingt verwendet werden sollten), werden zusätzlich dringend ein sicheres E-Mail-Gateway (SEG), eine Netzwerk-Zugangskontrolle (NAC, Network Access Control) und ein geeigneter Endpunkt-Schutz empfohlen. Nur so lässt sich die Integrität der Microsoft 365-Implementierung gewährleisten und zugleich profitiert das Unternehmen von bewährten Security-Komponenten spezialisierter Drittanbieter.

Fortinet bietet u. a. zusätzliche empfohlene Kontrollfunktionen:

- Identitäts- und Zugangsverwaltung (inklusive softwarebasierter Multi-Faktor-Authentifizierung) mit dem FortiAuthenticator und/oder FortiToken
- Kontrolle über den Netzwerk- und Gerätezugriff mit FortiNAC
- Daten- und Bedrohungsschutz für Microsoft 365 und andere weitverbreitete SaaS-Anwendungen mit FortiCASB, FortiGate und FortiMail
- Erweiterte Bedrohungsabwehr, einschließlich der im SEG Market Guide von Gartner empfohlenen Funktionen der FortiMail-Familie

Gegenüber anderen Anbietern, die ähnliche Komponenten als Einzelprodukte oder in Kombination anbieten, hat Fortinet eine Security-Komplettlösung mit

- einem unabhängigen, einheitlichen Bedrohungsschutz mit Bestnoten für On-Premises- und Multi-Cloud-Umgebungen – einschließlich für Microsoft 365-Komponenten wie Exchange Online und OneDrive,
- einer gemeinsamen Benutzeroberfläche und zentralen Verwaltung für alle Komponenten sowie eine
- kostenlose, unverbindliche Risikobewertung, wie gut Ihre jetzige E-Mail-Lösung 92,4 % der Malware erkennen kann.

[1] „Email Security Services Protection“. SE Labs, Januar bis März 2020.

[2] „Supplementing the Limitations in Office 365“. Osterman Research, März 2018.

[3] „Email Security Services Protection“. SE Labs, Januar bis März 2020.

[4] „Market Guide for Secure Email Gateways“. Gartner, 7. Mai 2017.

[5] Ebd.

[6] „2018 Data Breach Investigations Report“. Verizon, 10. April 2018.

[7] „Clouds Are Secure: Are You Using Them Securely?“. Gartner, 31. Januar 2018.

[8] Ebd.

[9] „Threat Landscape Report Q1 2018“. Fortinet, April 2018.

[10] „Magic Quadrant for CASB“. 30. November 2017.

[11] „Clouds Are Secure: Are You Using Them Securely?“. Gartner, 31. Januar 2018.

www.fortinet.com/de

757904-0-0-DE

7. Dezember 2020, 11:14 Uhr

ebook-questions-microsoft-office_DE