Maximale Sicherheit für Microsoft 365

Wer Microsoft 365 einsetzt, sollte ein grosses Augenmerk auf die Aspekte der Sicherheit werfen. Oft empfiehlt sich der Einsatz ergänzender Security-Lösungen. Patrick Michel, Principal Consultant beim IT-Security-Distributor BOLL, legt im Interview wichtige Security-Aspekte dar.

Microsoft 365 und Security – wie passt das zusammen?
Patrick Michel: Zunächst muss man festhalten, dass Microsoft in puncto Groupware, also Exchange mit E-Mail und Kalender, der klare Marktleader ist. Immer mehr Unternehmen setzen dabei nicht mehr auf einen eigenen Exchange-Server, sondern auf Microsoft 365. Dabei sind die gesamte Funktionalität sowie auch deren Sicherheit in die Cloud ausgelagert. Von Bedeutung ist ferner, dass die E-Mail-Kommunikation noch immer der Hauptangriffsvektor für Cyberattacken ist und dass E-Mail in fast allen Organisationen intensiv genutzt wird. Sicherheit spielt also im Zusammenhang mit Microsoft 365 eine immens wichtige Rolle.

Microsoft 365 bietet diverse integrierte Sicherheitsfunktionen. Genügen diese «Bordmittel»?
Geht es um bekannte Malware, bringt Microsoft 365 eine gute Erkennungs- und Abwehrleistung. Bei noch unbekannten Bedrohungen hingegen, bei Advanced Persistent Threats (APTs) und Ransomware – die Angriffsmethoden der Cyberkriminellen werden immer raffinierter – leisten spezialisierte Lösungen von Herstellern wie Proofpoint, Kaspersky oder Fortinet für die E-Mail-Sicherheit mehr. Die Erkennung neuartiger oder noch unbekannter Malware erfolgt zum Beispiel via Sandboxing. Diese Möglichkeit bietet Microsoft 365 nur im Premium-Paket – und gemäss unabhängigen Tests gibt es auf dem Markt bessere Sandboxing-Lösungen.

Auch Storage wandert immer mehr in die Cloud. Was gilt es hier zu beachten?
Es geht dabei nicht nur um Speicherplatz an sich – wie etwa OneDrive: Unternehmen setzen zunehmend auf unterschiedliche SaaS-Anwendungen, die eigene, in sich geschlossene Daten-Pools enthalten. Die Daten liegen dann auf verschiedenen Plattformen, und es wird schwierig, die Übersicht zu behalten und zu gewährleisten, dass nur Befugte auf die Daten zugreifen können.

Was schafft in derartigen Multi-Cloud- oder Multi-SaaS-Umgebungen Abhilfe?
Hier greifen sogenannte Cloud Access Security Broker (CASB). Sie bilden eine zentrale und automatisierte Schaltstelle für die Steuerung des Zugriffs auf sämtliche eingesetzten Cloud-Dienste. CASB werden in Zukunft ähnlich wichtig werden, wie es heute Firewalls sind. Der CASB-Service selbst wird häufig ebenfalls als SaaS-Dienst angeboten. Die Regelung, welche Benutzer auf die Dienste und somit auf Daten zugreifen dürfen, wird somit wieder zentralisiert. Die Funktionen sind aber vielfältig. Ein CASB kann etwa auch erkennen, wenn sich ein Nutzer kurz hintereinander an völlig unterschiedlichen Standorten anmeldet, und dann Alarm schlagen. Auch in diesem Bereich hat Microsoft mit Cloud App Security eine Lösung – aber sie ist vornehmlich auf die enge Integration mit den hauseigenen Apps und Diensten ausgerichtet. CASB-Produkte von spezialisierten Herstellern wie Bitglass sind universeller orientiert und bieten zusätzliche Funktionen.

Die Erkennung neuartiger oder noch unbekannter Malware erfolgt zum Beispiel via Sandboxing. Diese Möglichkeit bietet Microsoft 365 nur im Premium-Paket.

Patrick Michel, IT-Sicherheitsexperte und Principal Consultant beim IT-Security-Distributor BOLL

Wie sieht es mit dem klassischen Endgeräteschutz aus?
Endgeräte, mit denen auf Microsoft 365 zugegriffen wird, finden sich heute überall: am Firmensitz, im Homeoffice, unterwegs im Zug, Café oder Coworking Space – also auch ausserhalb des Unternehmensnetzwerks. Endpoint Protection ist demnach von grosser Wichtigkeit. Dabei sollte die eingesetzte Schutzlösung nicht nur auf die signaturbasierte Erkennung bekannter Malware begrenzt sein. Vielmehr müssen Endpoint-Security-Lösungen heute in der Lage sein, auch fortgeschrittene, bisher unbekannte Schädlinge und Angriffsmethoden zu erkennen und abzuwehren, bevor diese das Unternehmen kompromittieren können. In diesem Bereich kommt vermehrt künstliche Intelligenz zum Einsatz – wie etwa bei «Traps» von Palo Alto Networks.

Bei aller Technik: Es heisst auch, die wichtigste Schwachstelle sei der Mensch …
Richtig, und genau deshalb ist es gerade im Cloud-Zeitalter essenziell, alle Mitarbeitenden mittels Schulungen für Sicherheitsaspekte zu sensibilisieren – obligatorisch, fortlaufend und überprüfbar. Mit konsequenten Security-Trainings gewinnt man sehr viel Sicherheit. Zu diesem Zweck existieren diverse Security-Awareness-Schulungsplattformen – beispielsweise von Kaspersky und Proofpoint –, die sich auch für KMUs eignen. Diese Lösungen automatisieren die Schulung, prüfen die Mitarbeitenden unter anderem auf ihre Reaktion auf Phishing-Mails und wiederholen alles, was nicht korrekt gelöst wurde, bis es sitzt. So wird individuelles Cybersicherheitstraining fast ohne zusätzlichen Aufwand möglich.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch