Drittanbieterlösungen

Mehr Sicherheit für Microsoft 365

Die integrierten Sicherheitsfunktionen von Microsoft 365 werden immer besser. Trotzdem gibt es noch Lücken – Lösungen von Drittanbietern können aber das Plus an Sicherheit bringen, das erforderlich ist.

→ VON PATRICK MICHEL

DER AUTOR

Patrick Michel
ist IT-Sicherheitsexperte und arbeitet als Principal Consultant beim IT-Security-Distributor Boll.
→ www.boll.ch

Grossunternehmen wie auch KMU setzen für ihre Office-Umgebung, für E-Mail und die digitale Zusammenarbeit vermehrt auf das Cloudangebot Microsoft 365 (M365). Die Microsoft-365-Plattform bietet neben den Hauptfeatures auch Sicherheits- und Compliance-Funktionen. Dabei gilt es eines zu beachten: Mit dem permanenten Datenaustausch zwischen den Systemen im Unternehmen und in der Cloud nimmt die Angriffsfläche für Cyberkriminelle deutlich zu. Der Cybersicherheit kommt in der Cloudwelt folglich eine noch grössere Bedeutung zu als in herkömmlichen On-Premises-Umgebungen.

INTEGRIERTER SCHUTZ NICHT PERFEKT

Microsoft hat den in M365 enthaltenen Bedrohungsschutz in den letzten Jahren stark verbessert und bietet eine gute Abwehr gegen vornehmlich bekannte Malware. Dies genügt angesichts der immer raffinierteren Cyberkriminalität jedoch nicht: Noch unbekannte Bedrohungen wie Advanced Persistent Threats (APTs) und Ransomware werden von der integrierten Cyberabwehr nicht immer zuverlässig identifiziert. Dies gilt besonders im Hinblick auf Endpunktschutz, bei der E-Mail-Sicherheit sowie beim Scannen von Cloudspeichern wie OneDrive, Teams und SharePoint auf schädliche Inhalte.

Lösungen von spezialisierten Drittherstellern haben hier oft die Nase vorn. Solche Securityspezialisten sind ganz auf Cybersicherheit fokussiert, stark auf Innovation ausgerichtet und entwickeln neue, teils disruptive und höchst effektive Technologien für die Cyberabwehr.

ENDGERÄTESCHUTZ IST DIE BASIS

Endgeräte, mit denen man auf Microsoft 365 zugreift, finden sich überall – vom Firmenbüro übers Home Office bis zum Platz im Café oder im Zug, wo die Internetverbindung oft nicht völlig sicher ausgelegt ist. Eine hoch effektive Endpoint Protection ist also äusserst wichtig. Dafür setzen Anbieter wie Palo Alto Networks, Rapid7, Kaspersky und WatchGuard zunehmend auf Machine Learning. So lässt sich die Abwehr von unbekannten Schadcodes stärken und vor allem auch automatisieren.

Noch einen Schritt weiter geht Deep Instinct mit einem interessanten Ansatz: Das Ziel der gleichnamigen Lösung ist Prävention statt Mitigation «after the fact» – Bedrohungen sollen erkannt und eliminiert werden, bevor Schaden entsteht. Dazu nutzt die Lösung eine fortgeschrittene Variante von Machine Learning, genannt Deep Learning. Sie kommt ohne Training der Bedrohungsmodelle durch menschliche Akteure aus und bietet so ein Höchstmass an Automatisierung und Effizienz. Statt des «Trainingspersonals» kommt ein speziell auf Cybersecurity zugeschnittenes Deep-Learning-Framework zum Einsatz: Ein riesiges neuronales Netzwerk lernt aus Millionen von guten und bösartigen Dateien und Scripts und erkennt die «DNA» von Bedrohungen. In der Folge lassen sich so 99 Prozent aller unbekannten Malware abwehren.

Auf den Endgeräten wirkt dabei ein schlanker Agent mit einem Kernstück, das die Erkenntnisse des neuronalen Netzwerks in kompakter Form enthält. Der Agent beansprucht wenig Systemressourcen, muss nur ein- bis zweimal pro Jahr aktualisiert werden und benötigt keine permanente Internetverbindung. Er erkennt und stoppt Bedrohungen wie Ransomware innert 20 Millisekunden – typischerweise beginnt die Ransomware erst nach 15 Sekunden mit der böswilligen Datenverschlüsselung.

E-MAIL-SICHERHEIT MIT DEM GEWISSEN PLUS

Auch punkto E-Mail-Security bieten die Bordmittel von M365 ein durchaus ansprechendes Schutzniveau – aber es geht erstens noch besser, und zweitens unterscheiden sich die verschiedenen M365-Abos bei der E-Mail-Sicherheit. So lässt sich der Schutz vor fortgeschrittenen Bedrohungen der von KMU häufig genutzten Varianten E3 oder

Bilder: Boll, iStock/Jane_Kelly

Um für eine umfassende Sicherheit bei der Nutzung von Microsoft 365 zu sorgen, empfiehlt sich die Nutzung zusätzlicher Cybersecurity-Software

Business Premium durch Einbindung einer dedizierten Lösung für E-Mail-Security signifikant verbessern.

Ein Beispiel ist die speziell auf KMU gemünzte Lösung Proofpoint Essentials, die als rein cloudbasierte Plattform ohne zusätzliche Hardware auskommt. Sie bietet Funktionen wie Targeted Attack Prevention zur Abwehr gezielter Attacken auf bestimmte Personen oder die Analyse von URLs und E-Mail-Anhängen in einer Sandbox auf neustem technischem Stand. Sandboxing ist bei M365 nur in den höherpreisigen Enterprise Subscriptions enthalten.

Weitere interessante Funktionen sind ein Notfalleingang zum Empfang von Mails, wenn M365 ausfallen sollte, sowie ein für Compliancezwecke wichtiges E-Mail-Archiv mit Aufbewahrung der externen E-Mail für bis zu zehn Jahre, das auf der Nachrichtenjournalingfunktion von Microsoft Exchange basiert. Und weil der Mensch ein wesentliches Element jeder Sicherheitsstrategie sein sollte, ist auch eine optional abonnierbare Plattform für das Security Awareness Training integriert.

VEREINFACHTE ZERTIFIKATSVERWALTUNG

Ein weiteres wichtiges, aber oft vernachlässigtes E-Mail-Sicherheitsthema ist die Verschlüsselung und Signierung der Nachrichten, um Authentizität und Integrität der übermittelten Informationen zu gewährleisten. Vernachlässigt deshalb, weil die händische Verwaltung der erforderlichen Zertifikate für die digitalen Identitäten ziemlich aufwendig ist. Eine Verschlüsselungslösung sollte deshalb die Zertifikatsverwaltung, Verschlüsselung und Signierung möglichst vollautomatisch auf Gatewayebene erledigen, sodass die Zertifikate, wie beispielsweise beim Secure E-Mail Gateway des Schweizer Anbieters Seppmail, nicht für jeden einzelnen Nutzer bestellt und in Outlook installiert werden müssen. ←