Cybersicherheit für Microsoft 365 – es braucht mehr

Microsoft 365 wird immer populärer. Zwar haben sich die integrierten Sicherheitsfunktionen im Laufe der letzten Jahre verbessert, weisen aber noch immer Lücken auf. Oft bringen Lösungen von Drittanbietern das nötige Plus an Sicherheit. Patrick Michel, Principal Consultant beim IT-Security-Distributor BOLL, gibt Auskunft.

Microsoft 365 enthält auch Sicherheitsfunktionen. Schützen diese zuverlässig vor aktuellen Cyberbedrohungen?
Patrick Michel: Microsoft hat den Bedrohungsschutz in den letzten Jahren stark verbessert und bietet eine gute Abwehr gegen bekannte Malware. Bei den immer raffinierter werdenden, noch unbekannten Bedrohungen wie Advanced Persistent Threats (APTs) und Ransomware liegen die Lösungen von spezialisierten Herstellern jedoch deutlich vorne. Dies vor allem punkto E-Mail- und Endpoint-Sicherheit sowie beim Scannen von Onlinespeicher, wie etwa in OneDrive, Teams und SharePoint.

Wodurch zeichnen sich die spezialisierten Hersteller aus?
Sie sind ganz auf Security fokussiert, haben langjährige Erfahrung und umfassendes Know-how. Gleichzeitig treiben sie die Innovation voran und entwickeln neue, teils disruptive Technologien, die die Cybersicherheit auf ein höheres Niveau heben. Wenn solche Spezialisten keinen guten Job machen würden und gegenüber breitflächig aktiven Anbietern wie Microsoft kein Plus vorweisen könnten, gäbe es sie womöglich gar nicht mehr. Etwas Weiteres darf man nicht vergessen: Im Mittelpunkt der Sicherheit stehen immer der Mensch und sein Verhalten – und hier können Security Awareness Trainings, wie sie von diversen spezialisierten Unternehmen angeboten werden, wesentlich zur Verbesserung beitragen.

Welche Anbieter liefern verbesserten Endgeräteschutz?
Endgeräte, mit denen auf Microsoft 365 zugegriffen wird, finden sich überall – vom Firmen- übers Heimbüro bis zum Platz im Café. Eine hocheffektive Endpoint Protection ist demnach äusserst wichtig. Anbieter wie Palo Alto Networks, Rapid7, Kaspersky und WatchGuard nutzen dafür vermehrt Machine Learning, um die Abwehr von unbekanntem Schadcode zu stärken und zu automatisieren. Einen sehr interessanten Ansatz verfolgt dabei das Unternehmen Deep Instinct.

Der IT-Sicherheitsexperte Patrick Michel ist Principal Consultant beim IT-Security-Distributor BOLL.

Was ist das Besondere an der Lösung von Deep Instinct?
Deep Instinct setzt auf Prävention statt auf Reaktion «after the fact» und nutzt dafür Deep Learning. Dabei handelt es sich um eine fortgeschrittene Variante von Machine Learning, die ohne menschliches «Trainingspersonal» auskommt. Deep Instinct hat dafür das bisher einzige auf Cybersecurity zugeschnittene Deep-Learning-Framework entwickelt. Das neurale Netzwerk lernt automatisch aus Millionen von guten und bösartigen Dateien und Scripts und erkennt so die «DNA» von Bedrohungen. Deep Instinct vertraut voll auf Deep Learning und verspricht, 99 Prozent aller unbekannten Malware abzuwehren.

Wie unterstützt dies den Endpunktschutz?
Auf Basis der Erkenntnisse des neuralen Netzwerks entsteht das sogenannte Deep Instinct Brain. Dieses bildet den Kern des schlanken Agenten, der auf den Endpunkten installiert wird, nur wenig Systemressourcen beansprucht und nur ein- bis zweimal jährlich aktualisiert werden muss. Der Agent erkennt und stoppt Bedrohungen wie Ransomware innert weniger als 20 Millisekunden, sodass sie ihre schädliche Wirkung gar nicht erst entfalten können. Und er benötigt keine permanente Internetverbindung – ideal auch in abgeschotteten OT- und Hochsicherheitsumgebungen.

Kommen wir zur E-Mail-Sicherheit: Welche Lösungen tragen hier zur Verbesserung bei?
Auch hier gilt: Spezialisten bieten mehr. Ein Beispiel ist Proofpoint mit Lösungen für Grossunternehmen und KMU. Diese bieten unter anderem Targeted Attack Protection zur Abwehr zielgerichteter, komplexer Bedrohungen, bevor sie das Postfach eines Mitarbeitenden erreichen. Darin enthalten ist Sandboxing, eine Technologie zur isolierten Überprüfung potenziellen Schadcodes – ein Feature, bei dem Microsoft auch in der ATP-Variante in Tests häufig nicht gut abschneidet. Ein Notfall-Posteingang ermöglicht überdies, die Arbeit mit E-Mails fortzusetzen, sollte Microsoft 365 einmal ausfallen.

E-Mail-Verschlüsselung ist ein Thema, das vielen zu kompliziert ist. Gibt es dafür Abhilfe?
Die Lösung des Schweizer Anbieters SEPPmail vereinfacht die Verschlüsselung und Signierung von E-Mails dank automatisierter Zertifikatsverwaltung auf Gateway-Ebene und weiteren Funktionen wie Domainverschlüsselung ganz massiv. So müssen die digitalen Zertifikate nicht für jeden Nutzer einzeln bestellt und in Outlook installiert werden. Die Verschlüsselung und die Signatur erfolgen völlig transparent. Diese Toplösung ist als Appliance und neu auch in der Cloud verfügbar.

Die inhaltliche Verantwortung für den Artikel liegt bei BOLL Engineering AG.

KONTAKT

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60,
info@boll.ch, www.boll.ch