Mehr Cybersicherheit für Microsoft 365

Zwar haben sich die integrierten Sicherheitsfunktionen von Microsoft 365 im Laufe der letzten Jahre deutlich verbessert. Sie weisen aber noch immer Lücken auf. Oft bringen Lösungen von Drittanbietern das nötige Plus an Sicherheit – eine Übersicht.

Microsoft hat den in Microsoft 365 integrierten Bedrohungsschutz seit den Anfängen stark verbessert und bietet heute gute Abwehr gegen bekannte Malware. Bei den immer raffinierteren bisher 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 Onlinespeichern, wie etwa in OneDrive, Teams und SharePoint.

Security-Spezialisten im Vorteil

Diese Hersteller 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. Würden solche Spezialisten keinen guten Job machen und gegenüber breitflächig aktiven Anbietern wie Microsoft kein Plus vorweisen, gäbe es sie womöglich gar nicht mehr. Und nicht zu vergessen: Im Mittelpunkt der Sicherheit steht immer der Mensch. Hier können Security Awareness Trainings von spezialisierten Anbietern wesentlich zur Verbesserung beitragen – und gerade in diesem Punkt hat Microsoft kein eigenes Angebot.

Endgeräteschutz auf höherem Niveau

Endgeräte, mit denen auf Microsoft 365 zugegriffen wird, finden sich heute überall – vom Firmenübers 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.

Prävention statt Reaktion dank Deep Learning

Einen sehr interessanten Ansatz auf Basis von eigens entwickelter State-of-the-Art-Technologie verfolgt das Unternehmen Deep Instinct: Dessen Lösung Deep Instinct for Endpoints setzt auf Prävention statt auf Reaktion «after the fact» und vertraut dafür voll auf Deep Learning. Dies ist 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: Ein riesiges neurales Netzwerk lernt automatisch aus Millionen von guten und bösartigen Dateien und Scripts und erkennt so die «DNA» von Bedrohungen. So kann Deep Instinct versprechen, 99 Prozent aller unbekannten Malware abzuwehren.

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. Er beansprucht nur wenig Systemressourcen und muss nur ein- bis zweimal jährlich aktualisiert werden. 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.

Bessere Sicherheit für E-Mails

Auch für die E-Mail-Sicherheit 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.

Ein wichtiges Thema, das oft als zu kompliziert angesehen und deshalb vernachlässigt wird, ist die E-Mail-Verschlüsselung. Die Lösung des Schweizer Anbieters SEPPmail vereinfacht die Verschlüsselung und Signierung von E-Mails ganz massiv durch automatisierte Zertifikatsverwaltung auf Gateway-Ebene und weitere Funktionen wie Domainverschlüsselung. 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.

BOLL
IT Security Distribution

BOLL Engineering AG
Jurastrasse 58
5430 Wettingen

Tel. 056 437 60 60
info@boll.ch

www.boll.ch