Vectra ermöglicht Unternehmen Angriffe auf Office 365 jetzt schneller zu erkennen und zu stoppen

11. Februar 2020

München/Wien/Zürich,den 11. Februar 2020 – Das Cybersicherheitsrisiko wird für Unternehmen weltweit zu einem zunehmenden Problem. Datensicherheitsvorfälle in Zusammenhang mit Office 365 stehen hierbei an vorderster Stelle. Trotz zusätzlicher Sicherheitsmaßnahmen wie z.B. Multi-Faktor-Authentifizierung umgehen die Angreifer die Zugriffskontrollen immer wieder erfolgreich. So sind nach wie vor 30 Prozent der Unternehmen jeden Monat von einer unerlaubten Übernahme von Office 365-Konten betroffen. Datenschutzverletzungen dieser Art kommen immer häufiger in die Schlagzeilen. Für Unternehmen steigen die Kosten durch unmittelbare finanzielle Schäden und Reputationsverlust.

Es ist immer noch viel zu einfach für einen Angreifer, menschliches Verhalten zu manipulieren. Dadurch gelingt es, sich einen privilegierten Zugang zu geschäftskritischen SaaS-Ressourcen zu verschaffen. Dem Earnings Call von Microsoft für das dritte Quartal 2019 zufolge, gibt es mehr als 180 Millionen monatliche Benutzer auf Office 365. Bei so vielen Benutzern ist eine 100%ige Durchsetzung (Enforcement) der Cyberhygiene, also effektiver Vorsichtsmaßnahmen, unmöglich. Erschwerend kommt für Sicherheitsteams hinzu, mit den wöchentlichen Konfigurationsänderungen und neuen Best Practices Schritt zu halten. Wenn Angreifer erst einmal in einer SaaS-Anwendung Fuß gefasst haben, ist es nur eine Frage der Zeit, bis sie sich seitlich weiterbewegen und in andere Teile der Infrastruktur vorarbeiten.

Vor diesem Hintergrund wird das Security Operations Center (SOC) durch eine massive Anzahl von Alerts überflutet. Sicherheitsanalysten müssen viel Zeit dafür aufwenden, manuell zu analysieren und zu priorisieren. Die Frage ist dabei, welche Warnungen tatsächlich kritisch sind. Dies überfordert die Zeitressourcen der Sicherheitsanalytiker und die Sicherheitsbudgets der Unternehmen. Da die Angreifer zudem effizientere Ausweich- und Angriffstechniken anwenden, können die meisten Analysten hier nicht mehr mithalten.

„Die Angreifer gehen stets den Weg des geringsten Widerstands. Oft fällt es ihnen allzu leicht, Cloud-Schwachstellen auszunutzen. Die Erwartungshaltung, das Sicherheitsteams in 100 Prozent der Fälle korrekt entscheiden, ist völlig unrealistisch“, erklärt Hitesh Sheth, CEO von Vectra. „Die Arbeit der Sicherheitsteams soll nicht noch aufwändiger werden. Erforderlich ist eine Technologie, um die Abhängigkeit von

menschlichem Verhalten und menschlichen Fehlern zu beseitigen. Sicherheitsteams müssen die Kontrolle wieder zurückgewinnen. Genau hier setzt Vectra an.“

Der Missbrauch von Zugangsdaten ist der Hauptangriffsvektor bei SaaS, was insbesondere für Office 365 gilt. Vectra AI – als führender Anbieter von Network Detection and Response(NDR)-Lösungen – unterstützt Unternehmen beim effektiven Schutz ihrer Anwendungen. Vectra AI gibt jetzt den Launch von Cognito Detect für Office 365 bekannt. Die Lösung wird unterstützt durch neue Erkennungsmodelle, die sich auf Zugangsdaten und Privilegien in SaaS-Anwendungen konzentrieren. Damit erweitert Vectra die Cloud-Abdeckung von Cognito Detect auf Infrastructure-as-a-Service (IaaS). Mit einhergeht die Fähigkeit, die Aktivitäten von Angreifern zu verfolgen, die zwischen On-Premises, Rechenzentrum, IaaS und SaaS wechseln. Da Angreifer nicht in Silos zugange sind, sollte eine Sicherheitslösung auch nicht silobasiert arbeiten. Vectra liefert vollständige Transparenz über die gesamte Geschäftsumgebung. Angreifer finden keinen Platz, um sich zu verstecken.

„Präventionstechnologie ist seit langem verfügbar. Sie entwickelt sich ständig weiter. Sie garantiert aber nicht, dass die Daten sicher sind. Der wahre Fortschritt liegt in den Erkennungs- und Reaktionsfähigkeiten. Diese fehlen jedoch den meisten Unternehmen“, so Sheth weiter. „Wir bieten die erste und einzige NDR-Lösung, die auf Zugangsprivilegien basierte Erkennungen in SaaS-Anwendungen einsetzt. Unsere KI-gestützte Lösung fügt sich nahtlos in die bestehende Office 365-Bereitstellung ein. Sie erkennt das Verhalten von Angreifern, die sich Privilegien zunutze machen. Unternehmen erhalten dadurch einen vollständigen Einblick in ihre SaaS-Bereitstellungen. Wir stehen weiterhin an vorderster Front der Sicherheitsmaßnahmen, indem wir den Missbrauch von Privilegien während des gesamten Lebenszyklus eines Angriffs in der Cloud schnell erkennen.“