Zero-Trust-Konzept ersetzt den Perimeter Schutz

Zero Trust war das Thema der mbuf-Arbeitsgruppe IT-Security-Management am 23. März. Zwei Vorträge von Microsoft und einer vom Security-Spezialisten Zscaler beschrieben die technischen Facetten dieses Konzepts, und ein Anwendervortrag zeigte auf, wie es sich in der Praxis umsetzen lässt.

„Früher haben Security-Experten den Perimeter-Schutz in den Vordergrund gestellt“, berichtet Arbeitsgruppenleiter Andreas Sternberg. „Aktuell verabschieden sich Unternehmen von diesem Gedanken und gehen stattdessen davon aus, dass auch an den eigenen Standorten und in den eigenen Netzwerken fremde Akteure unterwegs sein können.“ Beim Zero-Trust-Konzept vertraut man daher niemandem. Jeder Akteur und jedes Gerät müssen sich authentifizieren und einen Status vorweisen, bevor ein Zugriff erlaubt wird.

Nach jeder Änderung wird das Vertrauen neu geprüft

Die Authentifizierung ist nicht immer gleich. Stattdessen validieren die Systeme bei jeder Veränderung eines Elements, ob das Vertrauen immer noch gegeben ist. Möglicherweise muss ein Anwender dann eine zusätzliche Authentifizierung vorweisen, oder er bekommt lediglich einen Lesezugriff und kann keine Daten ändern.

Microsoft Security Spezialist Thomas Bufler hat in seinem Grundlagenvortrag das Zero-Trost-Konzept vorgestellt. Über 80 Prozent der Sicherheitsvorfälle lassen sich demnach auf das Missachten einiger weniger Regeln zurückführen. Ein moderner IT-Security-Ansatz stellt Best Practices bereit, die einen Grundschutz gewährleisten. „Beim Zero-Trust-Ansatz gibt es für alle Benutzer, alle Apps und auch für alle Geräte eine Identität“, erläutert der zweite Arbeitsgruppenleiter Norbert Breidohr. „Vor jeder Aktion und vor jedem Datenzugriff werden die Identität und die dazugehörigen Berechtigungen geprüft, und erst dann eine Freigabe erteilt.“ Um diesen Zustand herzustellen, müssen Unternehmen ihre Systeme und ihr Netzwerk sicher konfigurieren, Authentifizierungsregeln erzwingen und zudem Kontrollmechanismen aktivieren.

40.000 Rechte bei drei Cloud-Providern

Mit der Rechtevergabe bei den Cloud-Plattformen Amazon Web Services, Google Cloud und Microsoft Azure beschäftigte sich der Vortrag von Markus Wilhelm-Köstner, Global Back Belt for Entra bei Microsoft. Unter dem Banner Multi Cloud Entitle Management starten Unternehmen ein Assessment, welche Rechte sie Administratoren und Anwendern in den jeweiligen Cloud-Plattformen gegeben haben. Die Sicherheitslösung Microsoft Entra prüft im Detail, welche Rechte bestehen, welche davon besonders kritisch sind, und wie oft diese in der Praxis in Anspruch genommen werden. „Knacken Hacker einen Account mit sehr hohen Rechten, können sie maximalen Schaden anrichten“, berichtet der zweite Arbeitsgruppenleiter Norbert Breidohr. „Diese Accounts sind daher sehr gefährdet und müssen besonders geschützt werden.“

Händisch ist eine derartige Prüfung aufgrund der hohen Zahl nicht zu machen, wie Sternberg erläutert: Allein ein Global Administrator in Microsoft Azure verfügt über rund 12.600 Rechte. In allen drei Cloud-Plattformen zusammen kommt man sogar auf 40.000.“ Nicht alles davon ist ständig erforderlich. So könne es durchaus vorkommen, dass über einen Zeitraum von 90 Tagen lediglich 1000 der mehr als 12.000 Rechte zum Einsatz kommen. Eine Idee für mehr Sicherheit besteht darin, dass auch Administratoren standardmäßig nur mit den unbedingt nötigen Rechten unterwegs sind, und dass sie erst bei Bedarf höhere Rechte aktiv schalten.

Dabei sinkt die Angriffsfläche deutlich. Es gibt allerdings einen gravierenden Nachteil: Manche Cloud-Plattformen übernehmen die geänderten Rechte erst mit einem Zeitverzug, der von einigen Minuten bis hin zu mehreren Stunden dauern kann. Den Grund für diese

Verzögerung kennt aktuell niemand. Um die mit der Einschränkung verbundenen Behinderungen zu umgehen, arbeiten einige Unternehmen aktuell lieber dauerhaft mit den vollen Rechten.

Netzwerk-Kontrolle erweitert die Sicherheit

Wie man über die Kontrolle des Netzwerks die Sicherheit erhöht, berichtete Simon Lindermann, Principal Sales Engineer beim IT-Security-Spezialisten Zscaler. „Die Tools von Zscaler analysieren den Netzwerk-Traffic und kontrollieren auf dieser Basis die Zugriffe der Benutzer und Geräte“, berichtet Breidohr. „Ein Proxy zwischen den Clients und dem Internet stellt sicher, dass die Anwender in der Cloud nur auf zugelassene Ressourcen zugreifen können. Man kann damit beispielsweise erreichen, dass die Anwender zwar Cloud-basierte Office-Programme nutzen können, aber nicht im Internet surfen.“ Darüber hinaus hängen die Rechte von der Einstufung des jeweiligen Endgeräts ab und davon, ob sich ein Benutzer über zwei Faktoren identifiziert hat oder nicht.

Zero Trust in der Praxis: Framework und Mindchange

Wie sich das Zero-Trust-Konzept in der Praxis in einem Unternehmen umsetzen lässt, stellte ein Mitglied der Arbeitsgruppe aus der Erfahrung seines Unternehmens in einem Vortrag dar. „Zero Trust ist ein Framework und ein Mindchange, den man strategisch verfolgen muss“, fasst Breidohr den Vortrag aus seiner Sicht zusammen. „Üblicherweise ist so etwas ein Mammutprojekt, das mehrere Jahre verschlingt.“ Der Finanzbedarf hänge davon ab, wie nah am Framework ein Unternehmen bereits aktuell arbeite. Hinzu komme ein enormer Personalbedarf, der sich nicht senken lasse. „Wenige Unternehmen haben verstanden, dass der Schaden durch ein gehacktes System sehr groß sein kann, und dass man besser fährt, wenn man die Abwehr maximal verstärkt“, so Breidohr.

Das nächste Treffen plant die Arbeitsgruppe IT-Security-Management am 6. Juli im Raum Würzburg. „Wir werden künftig ausschließlich Präsenztreffen veranstalten“, berichtet Breidohr. „Unsere Arbeitsgruppe lebt schließlich vom gegenseitigen Austausch, und dieser Aspekt bleibt üblicherweise bei den Online-Meetings komplett auf der Strecke.“ Die Themen für das nächste Treffen erarbeiten die Arbeitsgruppenleiter anhand des Feedbacks der Teilnehmer und anhand der gerade aktuellen IT-Bedrohungslage. *Jürgen Frisch*