Cybersecurity mit Zero Trust umsetzen

Cloud Computing, weitverbreitetes verteiltes Arbeiten, hyperdigitale Lieferketten und die rasant steigende Zahl vernetzter Geräte bieten Bedrohungsakteuren mehr potenzielle Einstiegspunkte in Unternehmensnetzwerke als je zuvor. Dazu nutzen sie gestohlene Benutzer-Anmeldeinformationen, um in diese einzudringen, so ein aktueller Gartner-Blog, der die wichtigsten Cybersecurity-Trends für 2022 diskutiert.

Identity- und Access Management Systeme (IAM) werden laut Gartner «nachhaltig angegriffen», da sich der digitale Fussabdruck von Unternehmen rapide ausweitet und Netzwerkgrenzen obsolet werden. Kompromittierte Anmeldedaten von Mitarbeitern sind seit langem der bevorzugte Angriffsweg für Cyberkriminelle und nun sogar noch in einem höheren Masse als vor der Pandemie. Gartner weist darauf hin, dass etwa 60 Prozent der Knowledge Worker nach wie vor remote arbeiten und prognostiziert, dass 18 Prozent nie wieder vom Büro aus arbeiten werden. Auch nach zwei Jahren kämpfen IT-Administratoren immer noch mit der Absicherung von Remote-Arbeitskräften und insbesondere mit deren Passwortpraktiken. Wie Gartner jedoch feststellt, sind die Passwortpraktiken der Mitarbeiter nur ein Teil eines grösseren Ganzen. Unternehmen sind heute in hohem Masse von einer Vielzahl von Drittanbietern abhängig, die Software und IT-Services bereitstellen und Zugang zu Unternehmensnetzwerken und -daten haben müssen. Dies hat zu aufsehenerregenden Cyberangriffen auf Lieferketten geführt. Nicht nur der Solarwinds-Angriff im Jahr 2020 hat gezeigt, dass ein Anbieter in der Lieferkette mit unzureichenden Sicherheitsvorkehrungen eine ebenso grosse «Insider-Bedrohung» wie ein unvorsichtiger oder böswilliger Insider ist. Darüber hinaus bedeutet das exponentielle Wachstum von Cloud Computing, Edge Computing, Microservices und Internet of Things (IoT)-Geräten, dass mehr Geräte und Anwendungen als je zuvor mit Unternehmensnetzwerken verbunden sind. Dazu gehört auch die operative Technologie (OT), also die hoch spezialisierten Hardware- und Softwarelösungen, die von modernen Herstellern und in kritischen Infrastrukturen eingesetzt werden. Diese Anwendungen und Geräte verbinden sich über Machine-to-Machine-Credentials wie API-Schlüssel, Datenbankpasswörter und digitale Zertifikate.

Ein ganzheitlicher Ansatz für IAM beginnt mit Zero Trust

Da IAM-Bedrohungen nicht isoliert existieren, muss die Cybersecurity-Abwehr ganzheitlich sein und nicht nur die Logins der Mitarbeiter, sondern auch die Logins von Lieferanten und IT-Geheimnisse von Anwendungen und angeschlossenen Geräten umfassen. Ein ganzheitlicher Ansatz für IAM beginnt mit einem Zero-Trust-Netzwerkzugangsmodell. Anstatt implizit allen Benutzern und Geräten innerhalb eines Netzwerkes zu vertrauen, geht Zero Trust davon aus, dass alles potenziell kompromittiert sein könnte und jeder Benutzer, ob Mensch, Anwendung oder Maschine, überprüft werden muss, bevor auf ein Netzwerk zugegriffen werden kann. Ein

Zero-Trust-Netzwerkzugang bietet IT-Administratoren einen vollständigen Überblick und Benutzer, Systeme und Geräte können sicher kommunizieren, auch über Netzwerkumgebungen hinweg. Dadurch wird das Risiko von passwortbezogenen Cyberangriffen sowie das Risiko der Ausweitung von Berechtigungen im Falle eines Einbruchs in das Netzwerk erheblich reduziert. Die Angriffsfläche des Unternehmens wird minimiert und die Datenumgebung ist insgesamt viel sicherer. Da die Welt immer vernetzter und die Datenumgebungen immer komplexer werden, können Unternehmen mit Zero Trust einen ganzheitlichen Ansatz für IAM verfolgen und alle Verbindungen zu ihren Netzwerken sichern. Die Zero-Trust- und Zero-Knowledge-Passwortmanagement- und Cybersicherheitsplattform von Keeper bietet Unternehmen modernes Privileged Access Management zum Schutz ihrer Passwörter, IT-Geheimnisse und Zero-Trust-Remote-Zugriff auf die IT-Infrastruktur. ■

KEEPER

Keeper Security EMEA Ltd.
King's Terrace, 5A, Lower Glanmire Rd
T23 DX49 Cork, Irland
sales@keepersecurity.com, www.getkeeper.de