Vertraue niemandem: Das Zero-Trust-Security-Modell

Mit der steigenden Bedrohungslandschaft und erhöhten Anforderungen an die Datensicherheit hat das Zero-Trust-Security-Modell bei Unternehmen deutlich an Popularität gewonnen. Die meisten traditionellen Ansätze der Netzwerksicherheit konzentrieren sich auf starke Schutzmaßnahmen gegen unerlaubten Zugang. Deren tendenzielle Schwäche ist jedoch das Vertrauen, welches User und Entitäten automatisch genießen, sobald sie sich im Netzwerk befinden. Denn gelingt es Cyberkriminellen, sich Zugang zum Netzwerk zu verschaffen, gibt es oft sehr wenig, was sie daran hindert, sich dort frei zu bewegen und sensible Daten hinauszuschleusen. Das Zero-Trust-Konzept schlägt deshalb vor, dass der gesamte Zugriff blockiert bleiben sollte, bis das Netzwerk den Benutzer verifiziert und den Grund für seinen Aufenthalt im Netzwerk bestätigt hat.

Hackern das Leben schwer machen: Umsetzung des Zero-Trust-Modells

Viele Unternehmen haben heute kritische Daten in der Cloud gespeichert. Deshalb ist es umso wichtiger, Benutzer ordnungsgemäß zu verifizieren und zu autorisieren, bevor sie Zugang erhalten. Darüber hinaus ist es aufgrund des enormen Anstiegs mobiler Geräte für Mitarbeiter einfacher denn je, von überall und jederzeit auf sensible Daten zuzugreifen, was die Regelung des Zugriffs auf allen Ebenen mit einer Zero-Trust-Richtlinie zusätzlich erforderlich macht.

Zero Trust basiert darauf, eine sichere Umgebung durch eine kontinuierliche Infrastruktur-Transformation zu schaffen. Das Security-Team sollte eine Multi-Faktor-Authentifizierung für den Zugriff auf verschiedene Mikrosegmente des Netzwerks einführen. Dies gewährleistet eine hohe Sicherheit und erschwert es Hackern effektiv, all die Informationen zu erhalten, die sie für den Zugriff auf das Konto eines Nutzers benötigen.

Das Konzept legt zudem den Fokus auf ein ausgeprägtes Risikomanagement, das auf Anomalie-Erkennung und Datenanalyse fußt. Technologien zur Analyse des Nutzerverhaltens, Endpoint Detection and Response (EDR) sowie Data Loss Prevention (DLP) unterstützen bei der Erkennung von verdächtigem Verhalten oder blockieren unautorisierten Zugriff auf sensible Daten. Dies hilft bei der Eindämmung von Sicherheitsbedrohungen und ermöglicht deren schnelle Entdeckung und Abwehr.

Granularer Schutz vor Insider-Bedrohungen: Zero Trust Networking

Zero Trust Networking ist ein zusätzlicher Teil des Zero-Trust-Modells, das darauf ausgelegt ist, laterale Bewegungen innerhalb des Unternehmensnetzwerks zu stoppen. Hierdurch kann der Zugriff eines Benutzers verhindert werden, auch wenn er sich auf der gleichen Unternehmensebene wie ein Kollege befindet, der legitimen Zugriff besitzt. Dies geschieht durch Hinzufügen von Perimetern zur Überprüfung bei jedem Schritt innerhalb des Netzwerks. Hierbei wird die Mikrosegmentierung genutzt und granulare Perimeter an kritischen Stellen im Netzwerk hinzugefügt, um zu verhindern, dass ein böswilliger Insider auf die sensibelsten Daten und Systemprozesse des Unternehmens zugreifen kann. Zero Trust Networking beseitigt damit den Nachteil des traditionellen perimeterbasierten Sicherheitsmodells, indem es das generelle Vertrauen gegenüber internen Nutzern vollständig abschafft, und stattdessen die Sicherheit rund um sensible Daten und kritische Prozesse eines Unternehmens erhöht.

Effektives Zero Trust: Sicherheit aus dem Inneren heraus

Zero Trust beginnt mit der Gewährung des Benutzerzugriffs nur für die Zeit, die Mitarbeiter zur Erfüllung einer bestimmten Aufgabe benötigen, entsprechend den geltenden Richtlinien des Unternehmens. Dies erfordert die Implementierung verschiedener Technologien, einschließlich Multifaktor-Authentifizierung, Scoring, Analytik, Dateisystemberechtigungen und Orchestrierung. Bei Zero Trust geht es jedoch um mehr als nur den Einsatz der richtigen Technologien. Das Modell entwickelt auch Sicherheitsparameter durch das Verständnis, wie wichtige Geschäftsprozesse eines Unternehmens mit den jeweiligen Mitarbeitern und deren Arbeits- und Denkweisen verknüpft sind und bietet damit Sicherheit, die aus dem Inneren heraus konzipiert ist.

Der Hauptvorteil des Zero-Trust-Sicherheitsmodells besteht darin, dass es Unternehmen hilft, die Beschränkungen der perimeterbasierten Sicherheit zu überwinden. Durch regelmäßige Überprüfung der Benutzerzugriffe wird eine wirksame neue Barriere geschaffen, um Anwendungen, Prozesse und Daten sowohl gegen böswillige Insider als auch gegen externe Angreifer zu schützen.