Einführung: Zero Trust ist Ihre Antwort auf KI-Risiken

Das Konzept von Zero Trust ist nicht neu, doch im neuen KI-Zeitalter ist es wichtiger denn je. Forrester Research hat es schon vor Jahren zum ersten Mal vorgestellt und Unternehmen gewarnt, dass es an der Zeit ist, die klassische Methode – also den uneingeschränkten Zugriff für Nutzer oder Anwendungen, sobald sie den Netzwerkrand passiert haben – zu überdenken. Stattdessen sollte jedes Gerät, jeder Nutzer und jeder Netzwerkfluss überprüft werden, bevor vollständiger Zugriff gewährt wird.

Zero Trust gewann immer mehr an Fahrt, da Unternehmen die Zugriffsprobleme im Zusammenhang mit hybrider Arbeit und Cloud-Bereitstellungen lösen wollten. Und heute ist das Netzwerk nicht mehr nur verteilt, sondern dynamisch und arbeitet mit maschineller Geschwindigkeit.

KI hat überzeugende Deepfakes ermöglicht und Large Language Models (LLMs) unterstützen heute flächendeckende Phishing-Versuche mit beispielloser Personalisierung. Noch besorgniserregender ist es, dass Frontier-KI-Modelle schnell Schwachstellen identifizieren können, die sich zuvor jahrzehntelang der menschlichen Erkennung entzogen haben. Damit lautet die Frage nicht mehr, ob, sondern *wann* eine Sicherheitsverletzung auftreten wird – und welchen Schaden sie anrichten wird.

Hinzu kommt der Aufstieg des Ransomware-as-a-Service-Modells, bei dem Entwickler Ransomware erstellen und diese an Cyberkriminelle vermieten, damit sie Angriffe durchführen können. So können selbst unerfahrene Hacker komplexe Attacken ausführen. Kürzlich haben drei der bekanntesten Ransomware-Gruppen – ALPHV/BlackCat, CL0P und LockBit – **vierfache Erpressungsangriffe** durchgeführt. Bei diesen Angriffen verschlüsseln und extrahieren Cyberkriminelle Daten nicht nur, sondern drohen auch DDoS-Angriffe an und wenden sich an Kunden, Partner, Mitarbeiter und Medien eines Opfers, um sie zu zwingen, ein Lösegeld zu zahlen. Gleichzeitig sorgen generative KI und LLMs dafür, dass Häufigkeit und Umfang von Ransomware-Angriffen zunehmen, da sie es technisch weniger versierten Cyberkriminellen erleichtern, komplexe Kampagnen zu starten.

Die manuelle Verteidigung ist zu langsam, um mit dieser neuen Realität Schritt zu halten. Deshalb müssen Unternehmen schnell zu einer KI-gestützten Verteidigungsstrategie umschwenken und jede einzelne digitale Interaktion schützen.

Inmitten dieser dynamischen – und oft verwirrenden – Cybersicherheitslandschaft haben Netzwerk- und Sicherheitssoftware-Anbieter ihren bestehenden Produkte schnell die Bezeichnung „KI-fähig“ hinzugefügt oder neue Produkte eingeführt. Entsprechend haben Sicherheitsteams oft Schwierigkeiten, mit der Entwicklung Schritt zu halten und fundierte Kaufentscheidungen zu treffen, die den Grundstein für eine Zero-Trust-Strategie legen.

Dieser Leitfaden soll Sicherheitsteams einen Blueprint bereitstellen, mit dem sie die richtigen Investitionen in Zero-Trust-Technologie planen können, um die steigenden KI-Risiken in den Griff zu bekommen. Hierzu definiert der Leitfaden die ersten Schritte und erläutert die wichtigsten Unterscheidungsfaktoren zwischen den verschiedenen Technologien.