AKAMAI-LÖSUNGSÜBERBLICK

Schützen Sie sich leichter mit End-to-End-Zero-Trust

Zero Trust ist ein strategischer Ansatz für die Cybersicherheit, der ein Unternehmen schützt, indem er implizites Vertrauen für Nutzer, Geräte, Netzwerke, Daten und Anwendungen beseitigt. Anstatt davon auszugehen, dass alles hinter der Unternehmens-Firewall sicher ist, geht der Zero-Trust-Ansatz jederzeit von einem Angriff aus und wendet auf jede Anfrage unabhängig von ihrem Ursprung einen Zugriff mit minimaler Berechtigungsvergabe an.

Warum Zero Trust jetzt wichtig ist

Zero Trust steht für Unternehmen, die sich effektiver an die sich ständig verändernde moderne IT-Umgebung anpassen müssen, an erster Stelle. Diese Unternehmen suchen nach einem neuen Sicherheitsmodell, das auf eine hybride Belegschaft ausgelegt ist und Nutzer, Geräte und Anwendungen unabhängig vom Standort schützt.

Prinzipien einer modernen Zero-Trust-Architektur

- Explizite, immer kontextabhängige Überprüfung
- Explizite Durchsetzung einer minimalen Berechtigungsvergabe
- Kontinuierliche Überwachung

Konsolidierung ist von entscheidender Bedeutung

Ein integrierter End-to-End-Ansatz

Ein ganzheitlicher Ansatz für Zero Trust sollte sich auf alle Unternehmensressourcen erstrecken, einschließlich aller Identitäten, Netzwerke und Anwendungen. Zero Trust dient als End-to-End-Strategie und muss daher für alle Elemente integriert werden. Die Verwendung mehrerer, locker integrierter Einzellösungen wird diesem strategischen Ansatz nicht gerecht.

Akamai hat ein ganzheitliches, zuverlässiges Portfolio zusammengestellt, um alle Zero-Trust-Lösungen bereitzustellen, die für ein modernes Unternehmen von entscheidender Bedeutung sind. Anstatt mehrere Sicherheitsprodukte zu installieren, zu betreiben und zu reparieren, können sich Unternehmen auf einen einzigen Anbieter verlassen, der alle erforderlichen Technologien liefert, und so von geringeren Kosten und verbesserter Betriebseffizienz profitieren.

Signalverteilung zwischen Lösungen

Akamai bietet im gesamten Zero-Trust-Portfolio integrierte Automatisierungen, die die Komplexität und den Anpassungsaufwand erheblich reduzieren. Auf diese Weise können die Produkte im Portfolio alle auf dieselben Bedrohungsinformationen zugreifen. So wird jedes einzelne Produkt sicherer. Wenn ein Produkt eine Bedrohung identifiziert, kann es diese Informationen an ein anderes Produkt weitergeben, um den Angriff abzuwehren.

Vorteile

- **Remote-Arbeitsmodelle**
  Nutzer können von überall, zu jeder Zeit und auf jedem Gerät sicherer arbeiten
- **Cloudmigration**
  Sichere Zugriffskontrolle auf Cloud- und Hybrid-Cloudumgebungen
- **Risikominderung**
  Stoppen Sie Bedrohungen und minimieren Sie laterale Netzwerkbewegungen von Ransomware und anderen Arten von Malware
- **Compliance**
  Gewährleisten Sie Compliance mit Mikroperimetern um sensible Daten

Ein ganzheitliches End-to-End-Portfolio: Nutzer, Anwendungen und Netzwerk

Den Workload schützen

Akamai Guardicore Segmentation: Zero Trust für Anwendungen

Akamai Segmentation bietet eine branchenführende Mikrosegmentierungslösung, die die Verbreitung von Ransomware und anderer Malware eindämmt. Das Produkt bietet Transparenz und Einblicke in Workloads, Prozesse und Anwendungen sowie die Durchsetzung von Zugriffsrichtlinien.

Das Netzwerk schützen

Enterprise Application Access: Zero Trust Network Access

Die Zero Trust Network Access-Technologie von Akamai wurde als Ersatz für klassische VPN-Technologie für starke Nutzeridentität entwickelt. Statt das gesamte Netzwerk zu gefährden, gewährt Enterprise Application Access Nutzern nur Zugriff auf die Anwendung, die für die Aufgaben ihrer Rolle erforderlich sind. Enterprise Application Access bietet Transparenz in die Nutzeridentität und eine starke Durchsetzung von Identifizierung und Authentifizierung.

Die Nutzer schützen

Secure Internet Access: Zero-Trust-Internetzugriff

Secure Internet Access ist eine sichere cloudbasierte Web-Gateway-Lösung. Secure Internet Access untersucht alle Webanfragen von Nutzern und wendet Echtzeit-Bedrohungsinformationen und fortschrittliche Malware-Analysetechniken an, um dafür zu sorgen, dass nur sichere Inhalte bereitgestellt werden. Schädliche Anfragen und Inhalte werden proaktiv blockiert.

Multi-Faktor-Authentifizierung: starke Zero-Trust-Identität

Akamai MFA schützt Mitarbeiterkonten vor Phishing und anderen Man-in-the-Middle-Angriffen. So wird sichergestellt, dass nur Mitarbeiter auf ihre eigenen Konten zugreifen können, die durch eine starke Nutzerauthentifizierung überprüft wurden. Alle anderen Zugriffsversuche werden verweigert und die Übernahme von Mitarbeiterkonten wird verhindert.

Protokollieren und Prüfen

Hunt: Sicherheitsservices

Die Threat Hunter von Akamai suchen kontinuierlich nach anomalem Angriffsverhalten und komplexen Bedrohungen, die den traditionellen Sicherheitslösungen häufig entgehen. Dabei verfolgen sie einen Ansatz, der auf dem Grundsatz „immer von einem Angriff ausgehen“ basiert. Unsere Threat Hunter informieren Sie umgehend über alle kritischen Vorfälle in Ihrem Netzwerk und arbeiten dann eng mit Ihrem eigenen Sicherheitsteam zusammen, um die Situation zu beheben.

Der Vorteil durch Akamai

Akamai bietet einige Vorteile, die seinen Zero-Trust-Ansatz gegenüber anderen Anbietern einzigartig machen. Wir bieten die umfassendste Abdeckung: alt und modern, Windows und Linux, vor Ort und virtuell, Container und mehr. Dank unserer unübertroffenen Transparenz können Nutzer jederzeit in vollem Kontext erkennen, was jeder Workload tut. Und unsere erstklassigen internen Services zur Bedrohungsbekämpfung („Threat Hunting“) erweitern die Möglichkeiten jedes Sicherheitsteams, damit Ihr Unternehmen Bedrohungen immer einen Schritt voraus ist.

Weitere Informationen zu Zero Trust und Ihren ersten Schritten mit diesem Ansatz finden Sie auf akamai.com.

 | Support | Veröffentlicht: Juni 2022