Akamai

WHITE PAPER

Blueprint für Zero Trust Network Access

An wen richtet sich dieser Leitfaden?

Dieser Leitfaden richtet sich an Netzwerkarchitekten, Sicherheitstechniker, CTOs, CISOs und andere Entscheidungsträger in IT und Sicherheit.

Verantwortliche in den Bereichen Umfangsbestimmung, Konfiguration, Bereitstellung, Implementierung und Verwaltung von Zero Trust Network Access finden in diesem Leitfaden eine umfassende Übersicht über mögliche Vorteile und eine Auflistung der Unterschiede zwischen den verschiedenen Systemen. Der Leitfaden befasst sich mit folgenden Themen:

- Einschränkungen und Sicherheitsmängel älterer Ansätze für den Anwendungszugriff und warum Zero Trust Network Access erforderlich ist
- Die Komponenten und Funktionsweise von Zero Trust Network Access
- Wie Akamai Enterprise Application Access und Akamai MFA schnell und einfach Zero Trust Network Access bereitstellen können

Da die Geschäftswelt sich verändert und Cyberbedrohungen immer mehr zunehmen, überdenken viele Unternehmen ihre Cyberabwehr. Viele haben erkannt, dass die herkömmliche Netzwerkarchitektur, die auf einem zentralen Standort basierte, an dem alle Beteiligten auf Anwendungen zugreifen konnten, sie anfällig für Angriffe macht. Dieses „Zugbrückenprinzip“, bei dem davon ausgegangen wurde, dass alle Nutzer und Geräte innerhalb des Netzwerks sicher sind und nur der Netzwerkrand geschützt werden muss, führt dazu, dass Unternehmen in der heutigen digitalen Landschaft mit mobilen Verbindungen und der Cloud einem hohen Risiko von Cyberangriffen ausgesetzt sind. Stattdessen wenden sich zukunftsorientierte Unternehmen dem Konzept einer Zero-Trust-Architektur zu, um wichtige Assets zu schützen. Ein Kernprinzip jedes Zero-Trust-Projekts ist der Schutz des Netzwerks. In diesem Whitepaper wird erläutert, warum herkömmliche Hub-and-Spoke-Ansätze für die Netzwerksicherheit nicht mehr ausreichen und wie die Umstellung auf Zero Trust Network Access kritische Assets besser schützen und als Schlüsselelement für eine umfassende Zero-Trust-Architektur dienen kann.

Die Geschäftswelt verändert sich aktuell so schnell wie nie zuvor

Die Art und Weise, wie Unternehmen Technologie betreiben und nutzen, entwickelt sich immer schneller. Die Entwicklung des Computing hat sich schnell vom Hosting von Geschäftsanwendungen in Rechenzentren vor Ort hin zu mehreren Public Clouds, Private Clouds oder einem hybriden Ansatz (sowohl vor Ort als auch in der Public/Private Cloud) verlagert.

Die Entwicklung des Geschäftsmodells hat auch zu einer verstärkten Zusammenarbeit zwischen Unternehmen geführt und macht es notwendig, Partnern und Lieferanten Zugriff auf Anwendungen und Ressourcen zu gewähren.

Da Unternehmen weiterhin remote oder hybride Arbeit nutzen, greifen Nutzer nun von überall aus auf Geschäftsanwendungen und -ressourcen zu, und zwar sowohl von verwalteten als auch von nicht verwalteten Geräten.

Mit diesen Veränderungen können ältere Ansätze zur Verwaltung des Anwendungszugriffs nicht mehr mithalten. Unternehmen müssen nun einen neuen Ansatz wählen, der sicheren Zugriff ermöglicht, unabhängig davon, wo die Anwendungen gehostet werden oder wo sich die Nutzer befinden.

Das alte Anwendungszugriffsmodell

Seit über 20 Jahren setzen Unternehmen auf Firewalls, um einen starken Sicherheitsbereich aufzubauen, und vertrauen den Nutzern, die sich innerhalb dieses Bereichs befinden. Dieser Sicherheitsansatz behandelt Netzwerke wie Burgen mit Gräben: Dicke Mauern und schwer gesicherte Tore schützen die Eingänge der Burg (oder in diesem Fall des Netzwerks), und nur Nutzer mit den richtigen Anmeldedaten können eintreten. Sobald sie sich im System befinden, können Nutzer basierend auf ihrer Identität auf bestimmte Anwendungen zugreifen, die über IdP-Lösungen (Identity Provider) wie Microsoft Active Directory bereitgestellt werden.

Bei flachen Netzwerken haben Nutzer jedoch IP-Zugriff auf das gesamte Netzwerk, was bedeutet, dass sie auch andere Server und Anwendungen sehen können. Beispiel: Wenn der IdP richtig konfiguriert ist, kann ein Nutzer den Server finden, auf dem die Anwendung zur Gehaltsabrechnung gehostet wird. Wenn er sich dort jedoch anmelden will, wird ihm der Zugriff verweigert.

Um dieses Problem der uneingeschränkten lateralen Bewegung zu beheben, teilten Unternehmen Anwendungen über virtuelle lokale Zugriffsnetzwerke (VLANs) in separate Segmente hinter einer Firewall auf und erzwangen auf Grundlage von IP-Bereichen Regeln für einzelne Nutzer oder Gruppen, die heutzutage veraltet sind. Das ist mühselig und bietet viel Raum für Fehler. Vielleicht hat gerade jemand Wartungsarbeiten vorgenommen und Geräte in ein neues Rack eingesetzt oder ihnen eine IP in einem neuen Bereich zugewiesen. Plötzlich werden Nutzer gesperrt, und die Supportanrufe häufen sich. Oder vielleicht erfordert ein Software-Upgrade Änderungen an der Architektur einer Anwendung, und Nutzer werden im Rahmen des Workflows auf einen anderen Computer umgeleitet. Dieser Computer ist dann möglicherweise für bestimmte Nutzer oder Gruppen nicht zugänglich, weil die Firewall-Regeln nicht aktualisiert wurden.

Bei einer solch komplexen Architektur ist ein hohes Maß an Kommunikation zwischen Application Owner, Netzwerkadministratoren und Sicherheitsgruppen erforderlich, um Ausfälle zu vermeiden.

Wir wissen, was oft passiert, wenn diese Koordination scheitert. Administratoren wollen Best Practices umsetzen, doch im Notfall kommt schnell die alte Regel IP ANY/ ANY ALLOW zum Einsatz, damit betroffene Nutzer auf alle Ressourcen zugreifen können, bis das Problem gefunden und behoben wurde. Oft bleibt jedoch nicht die Zeit, diese Änderungen wieder rückgängig zu machen, und diese schnellen Korrekturen beeinträchtigen die Sicherheitslage eines Unternehmens im Laufe der Zeit.

VPNs sorgen für Herausforderungen bei Komplexität, Performance und Sicherheit

Für Remotenutzer bietet ein Virtual Private Network (VPN) in der Regel Zugriff auf Anwendungen vor Ort, die innerhalb des Netzwerks gehostet werden und dann direkten getunnelten Zugriff auf das Unternehmensnetzwerk ermöglichen.

Um den Nutzerzugriff auf Anwendungen zu verwalten, fügen Unternehmen häufig dedizierte Application Delivery Controller hinzu oder verwenden die Zugriffskontrollen, die in ihre VPN-Lösungen integriert sind. Das Ziel besteht darin, die Zugriffsberechtigungen für Anwendungen unabhängig vom Standort des Nutzers aufeinander abzustimmen. Wenn einem Nutzer der Zugriff auf die CRM-Anwendung verweigert wird, wenn er sich innerhalb des Netzwerks befindet, sollte ihm der Zugriff auch dann verweigert werden, wenn er über das VPN verbunden ist. Obwohl dies das Ziel ist, kann die Komplexität der Synchronisierung von Anwendungsberechtigungen zwischen den beiden Anwendungsfällen und schnellen Korrekturen dazu führen, dass Nutzer unbeabsichtigten Zugriff auf Anwendungen erhalten.

Anwendungszugriff für Auftragnehmer, Partner und Lieferanten

Unternehmen verwenden oft auch VPNs, um Auftragnehmern, Partnerunternehmen oder Lieferanten den Remotezugriff auf Anwendungen zu ermöglichen. Beispielsweise kann ein Unternehmen externen Zugriff auf seine Finanzsysteme gewähren, damit Lieferanten Rechnungen stellen können. Der Zugriff auf Drittanbieteranwendungen über ein VPN birgt zusätzliche Sicherheitsrisiken, da das Unternehmen keine End-to-End-Sicherheit mehr besitzt. Wenn ein Gerät eines Drittanbieters mit VPN-Zugriff kompromittiert wird, können Angreifer über dieses Gerät auch Zugriff auf das Unternehmensnetzwerk erhalten.

VPNs und Performance

Der gleiche Kompromiss kommt auch bei der Performance zum Tragen. In seiner einfachsten Form leitet ein VPN sämtlichen Traffic zurück an die Rechenzentrums-Infrastruktur. Dies kann zu einem extrem langsamen Zugriff auf Internetressourcen und SaaS-Anwendungen (Software as a Service) aufgrund von Hairpinning führen, wodurch sich der Traffic effektiv verdoppelt.

Um dieses Performanceproblem zu bewältigen, setzen viele Administratoren Split-Tunnel ein und geben auch hier an, welche IP-Bereiche über das VPN und welche direkt an das Internet übertragen werden sollen. Das ist äußerst effektiv und einfach, wenn es nur ein einziges internes Netzwerk gibt. Mit mehreren Rechenzentren und VPC-Anbietern (Virtual Private Clouds) wird dieses Verfahren jedoch deutlich schwieriger. Dann müssen Administratoren entscheiden, ob sie VPN-Aggregatoren in jedem Rechenzentrum installieren, und herausfinden, wie sie Multipoint-Split-Tunnel effektiv managen können.

Das alles soll nicht bedeuten, dass VPNs keine Vorteile bieten. Ganz im Gegenteil, der Zugriff von Standort zu Standort in Infrastrukturen mit mehreren Rechenzentren ist ein Anwendungsfall, in dem sie perfekt zum Einsatz kommen. Der Zugriff auf Netzwerkebene ist jedoch nicht der richtige Ansatz für Nutzer, die auf Anwendungen zugreifen, da der Zugriff auf Netzwerkebene einen ungünstigen Kompromiss zwischen Einfachheit und Sicherheit/Performance erzwingt.

Angreifer freuen sich über netzwerkbasierten Anwendungszugriff

Bisher haben wir uns auf die Risiken und Herausforderungen konzentriert, die mit der Zugriffsgewährung auf Netzwerkebene für alle Mitarbeiter verbunden sind. Dieser Ansatz setzt Unternehmen jedoch auch einem anderen Risiko aus: Cyberkriminelle, die gestohlene Anmeldedaten oder eine Sicherheitslücke ausnutzen, können so gegebenenfalls ungehinderten Zugriff auf das gesamte Netzwerk erhalten. Wenn ein Angreifer beispielsweise mit gestohlenen Anmeldedaten VPN-Zugriff erhält, kann er sich dann lateral durch das Netzwerk bewegen, um hochwertige Ziele zu finden und anzugreifen.

Diese Ansätze öffnen Tür und Tor für katastrophale Sicherheitsverletzungen

Theoretisch ist es möglich, den Anwendungszugriff mit diesen Ansätzen sicher und reibungslos zu verwalten. Vielleicht nutzen Sie bereits eine entsprechende Kombination. Das Problem ist aber, dass es oftmals viel zu komplex ist, über die gesamte Lebensdauer der Implementierung und Verwaltung hinweg ausreichende Sicherheit und Performance zu gewährleisten, sodass mit der Zeit zwangsläufig Fehler passieren. In vielen Fällen reden sich die Verantwortlichen ein, dass alles optimal funktioniert, weil die Mitarbeiter schließlich auf ihre Anwendungen zugreifen können. Wenn die oben erwähnten Workarounds dann zu einem verheerenden Angriff führen oder die Performance plötzlich einbricht oder es sogar zu einem Ausfall kommt, wird die Mitarbeiterproduktivität erheblich beeinträchtigt.

Ein Zero-Trust-Ansatz für den Anwendungszugriff

Angesichts der inhärenten Mängel bei den Sicherheitskonzepten und der besonderen Herausforderungen, die sich bei der Verwaltung des Anwendungszugriffs ergeben, bietet das neue Zero-Trust-Cybersicherheitsmodell eine bessere Alternative. Es wurde 2010 von Forrester Research vorgestellt und ist ein Framework, mit dem Unternehmen ihre IT-Infrastruktur, Sicherheitsrichtlinien und Geschäftsprozesse optimieren können.

Das Prinzip dahinter ist einfach, aber effektiv: Vertrauen sollte nichts mit dem Standort zu tun haben. Sie sollten niemandem einfach vertrauen, nur weil er sich innerhalb Ihrer Firewall befindet. Stattdessen sollte jede Aktion, unabhängig davon, wo sie stattfindet, nur dann als vertrauenswürdig eingestuft werden, wenn sie explizit zugelassen wurde. Letztendlich *kann* dann nur das geschehen, was auch geschehen *sollte*. Beseitigen Sie implizites Vertrauen für alle Aktionen, die nicht unbedingt erforderlich sind – diese schaffen Risiken aber keinen Wert.

Dies erfordert eine starke Authentifizierung und Autorisierung, und Systeme sollten Daten erst dann übertragen, wenn Vertrauen hergestellt wurde. Darüber hinaus dienen Analysen, Filter und Protokollierung dazu, Verhaltensregeln durchzusetzen und den Traffic durchgehend auf Bedrohungen zu überwachen.

Durch diese umfassende Änderung des Sicherheitsmodells lassen sich viele der im letzten Jahrzehnt aufgetretenen Probleme beheben. Angreifer können keine Schwachstellen mehr in Ihrer Firewall ausnutzen und dann vertrauliche Daten stehlen, nur weil sie es in Ihr Netzwerk geschafft haben. Jetzt gibt es keinen Burggraben mehr, den man überqueren kann. Es gibt nur Anwendungen und Nutzer, die vor jedem Zugriff authentifiziert und autorisiert werden müssen.

Zero Trust Network Access

Zero Trust Network Access ist eine Architektur, die auf diesen Prinzipien basiert und auf der Grundlage starker Authentifizierung, Autorisierung und Kontext sicheren Zugriff auf Anwendungen und Ressourcen gewährt. Eine Architektur mit Zero Trust Network Access bietet nur Zugriff auf die Anwendungen, die Nutzer für ihre Arbeit benötigen, nicht auf das gesamte Netzwerk. Bei diesem Ansatz spielt es keine Rolle mehr, wo sich die Nutzer befinden; es gibt kein „innerhalb“ oder „außerhalb“ des Netzwerks mehr. Wenn eine Anwendung gehostet wird, ist es irrelevant, ob dies vor Ort, in einer Public Cloud oder einer Private Cloud geschieht, da authentifizierte Nutzer nur Zugriff auf Anwendungen erhalten, für die sie autorisiert sind.

Beispiel: Ein Vertriebsmitarbeiter hat nur Zugriff auf Anwendungen, die sich auf seine Rolle im Vertrieb beziehen, nicht etwa auf Human-Resources- oder Finanzanwendungen.

Funktionsweise von Zero Trust Network Access

Akamai Enterprise Application Access und Akamai MFA ermöglichen Ihnen die Umstellung auf eine Zero Trust Network Access-Architektur, die einen wichtigen und entscheidenden Schritt auf dem Weg zu Zero Trust darstellen kann.

Enterprise Application Access ist ein identitätsbasierter Proxy (IAP) in der Cloud. Es handelt sich um einen flexiblen und anpassbaren Service mit detaillierter Entscheidungsfindung auf der Grundlage von Echtzeit-Signalen wie Bedrohungsinformationen, Gerätestatus und Nutzerinformationen. Akamai MFA ist ein Multi-Faktor-Authentifizierungsservice, der die stärksten Authentifizierungsstufen bietet, um sicherzustellen, dass ein Nutzer, der Zugriff anfordert, auch wirklich der ist, der er behauptet zu sein.

Zunächst führen Sie eine kleine virtuelle Maschine namens Enterprise Application Access Connector hinter der Firewall aus, die jedoch mit Ihren Anwendungen verbunden ist. Dieser Proxy muss und sollte sich *nicht* in der DMZ befinden. Seine Adresse liegt im privaten IP-Bereich und ist nicht direkt über das Internet erreichbar. Im Grunde funktioniert er wie jede andere Anwendung hinter der Firewall.

Zur Unterstützung von Multicloudumgebungen kann ein Connector in Ihrem Rechenzentrum vor Ort oder in einer Private oder Public Cloud bereitgestellt werden.

Der Enterprise Application Access Connector stellt sofort eine verschlüsselte ausgehende Verbindung zum IAP in der Akamai Connected Cloud her. Sobald die Verbindung mit dem IAP hergestellt ist, lädt der Connector seine Konfiguration herunter und ist bereit, Verbindungen herzustellen. Die Verbindung zwischen dem Connector und dem IAP ist ausgehend, sodass Sie alle eingehenden Firewall-Verbindungen schließen können. So sind die Anwendungen im öffentlichen Internet nahezu unsichtbar.

Der IAP führt alle Vorverarbeitungsvorgänge durch, die vor der Verbindung eines Nutzers mit der Anwendung notwendig sind, einschließlich Authentifizierung, Autorisierung und die Überprüfung von Gerätesicherheit und -status. Wenn ein Nutzer versucht, auf eine Anwendung zuzugreifen, wird er über den DNS-CNAME an Akamai weitergeleitet und mit dem IAP verbunden. Der Endnutzer und sein Gerät müssen dann alle Prüfungen bestehen, damit eine Weiterleitung für Authentifizierung, Multi-Faktor-Authentifizierung und Single Sign-on erfolgt. Anschließend wird die Geräteidentität überprüft.

Wenn Nutzer und Gerät autorisiert wurden, wird eine Verbindung vom Endnutzer zum Enterprise Application Access Connector hergestellt. Traffic aus dieser Nutzersitzung wird über diese IAP-Verbindung übertragen, die wiederum eine Verbindung zu den angeforderten Anwendungen oder Services herstellt. An diesem Punkt besteht die Verbindung von Anfang bis Ende, und alle Zugriffsentscheidungen erfolgen kontinuierlich und dynamisch basierend auf Identität, Gerät und Nutzerkontext.

Diese Zugriffsmethode bietet einige deutliche Vorteile. Die Aktivitäten, die das höchste Maß an Performance und Sicherheit erfordern, finden an der Edge so nah am Nutzer wie möglich statt – an einem von weltweit 4.200 Akamai-Standorten in 134 Ländern.

Darüber hinaus wird der Pfad zu vertraulichen Daten für die Anwendung über einen Reverse-Anwendungstunnel bereitgestellt. So ist die IP des Netzwerks nicht sichtbar, und das Risiko volumetrischer Angriffe wird minimiert.

Da Enterprise Application Access auch dann direkt in die Identitätsinfrastruktur eines Unternehmens integriert werden kann, wenn es mehrere Verzeichnisse und Identity Service Provider umfasst, kann der Zero Trust Network Access-Service schnell bereitgestellt werden, ohne dass die vorhandene Identitätsinfrastruktur oder -architektur geändert werden muss.

Für ältere Anwendungen, die moderne Authentifizierungsprotokolle nicht unterstützen, verfügt Enterprise Application Access über eine IdP-Bridge-Funktion, die eine Authentifizierung für SAML-basierte IdPs ermöglicht und das Authentifizierungstoken in das Authentifizierungsprotokoll übersetzt, das von den älteren Anwendungen unterstützt wird.

Was IAP-basierte Ansätze wie Enterprise Application Access so interessant macht, ist der Zugriff auf Anwendungsebene. Bei Zugriff auf Anwendungsebene sind Performance und Sicherheit *unabhängig* von der Komplexität.

Sie migrieren einfach alle Anwendungen, die irgendwie zusammengehören (z. B. weil sie im selben Rechenzentrum oder derselben virtuellen Private Cloud gehostet werden), in einen privaten IP-Bereich oder ein zugriffsbeschränktes VLAN. Dann platzieren Sie einen Zugangs-Proxy im entsprechenden Mikronetzwerk – fertig. Das war's. Das ist alles.

Application Owner können ihre eigenen Sicherheitsrichtlinien im Zugangs-Proxy festlegen – Richtlinien, die bestimmen, wer auf was zugreifen darf –, und damit ist der Nutzerstandort nicht mehr relevant. Es gibt keine Unterscheidung zwischen innerhalb und außerhalb des Netzwerks, weil es kein Netzwerk gibt, das Endnutzer umfasst. Ein Mitarbeiter im Café ist für das System nichts anderes als ein Mitarbeiter im Büro. Wichtig ist nur, ob der Nutzer autorisiert und ob das verwendete Gerät sicher ist.

Mit dem Zugriff auf Anwendungsebene ist trotz der einfachen Implementierung und Verwendung optimale Performance möglich. Nutzer können einfach das Internet nutzen, um direkt auf Anwendungen zuzugreifen – egal, wo sie gehostet werden oder wo sich der Nutzer befindet. So können Pakete über das Internet an ihr Ziel geroutet werden, ohne dass sie Aggregatoren oder Zwischenstellen durchlaufen müssen.

Mit einem solchen anwendungsbasierten Zugriff werden interne Netzwerke oft zum bloßen Gast-WLAN. Denken Sie daran: Damit Zero Trust wirklich funktioniert, dürfen Sie interne Nutzer nicht anders behandeln als externe Nutzer. Niemand wird standardmäßig als vertrauenswürdig eingestuft.

Der gewünschte Endzustand von Zero Trust Network Access

Alle Nutzer – ob im Unternehmen oder unterwegs – sollten Verbindungen zu Anwendungen über identitätsbasierte Zugangs-Proxys herstellen, egal, wo die Anwendungen gehostet werden. Diese Proxys sollten nicht nur eine Standardauthentifizierung durchführen, sondern auch eine phishing-sichere Multi-Faktor-Authentifizierung wie Akamai MFA verwenden. Darüber hinaus müssen zuverlässige Funktionen für Geräteprofile vorhanden sein, mit denen sich Gerätekriterien für den Zugriff auf bestimmte Anwendungen ermitteln lassen.

Doch Zero Trust Network Access darf unserer Meinung nach nicht bei Authentifizierung und Autorisierung enden. Zur Unterstützung von Zero-Trust-Prinzipien sollten alle Parameter, die in der anfänglichen Authentifizierungs- und Autorisierungsphase überprüft werden, während der Aktivierungssitzung kontinuierlich überwacht werden. Alle erkannten Veränderungen sollten eine Aktion auslösen, z. B. die erneute Authentifizierung des Nutzers, die Aufhebung des Zugriffs auf die Anwendung oder die Beschränkung des Zugriffs auf die Anwendung.

Zusätzlich zu den Zugangs-Proxys sollte auch eine WAAP eingesetzt werden (Web Application and API Protection). Dieses wichtige Sicherheitssystem gewährleistet, dass Endnutzer keine Angriffe auf Anwendungsebene verursachen können – ob versehentlich oder absichtlich. Mit anderen fortschrittlichen Systemen, wie z. B. Mensch/Bot-Erkennung, können Sie bei Sites ohne API gewährleisten, dass sich hinter gültigen Endpoints keine Malware verbirgt. Am IAP kann Akamai WAAP, Boterkennung, Verhaltensanalysen und Caching integrieren. So können wir bestmögliche Performance bieten und potenzielle Bedrohungen weit entfernt von Ihren physischen Standorten, Anwendungen und Daten aufhalten.

Wenn Sie Ihre Anwendungen online über Zugangs-Proxys verfügbar machen, spielt auch der Schutz vor DDoS-Angriffen (Distributed Denial of Service) eine wichtige Rolle. Hier sollten Sie auf Anbieter zurückgreifen, die Angriffe auf Mikronetzwerke und Proxys verhindern und so auch unter massiver Belastung die Verfügbarkeit gewährleisten können.

Schließlich müssen für Ihre Zugangs-Proxys Netzwerke zur Verfügung stehen, die Performancevorteile bieten. Zum einen stellen Sie so eine optimale Performance Ihrer Anwendungen sicher, zum anderen sorgen Sie dafür, dass Ihre Nutzer die neuen Zugriffsmethoden nicht nur annehmen, sondern sie auch optimal nutzen können. Hier können Sie insbesondere CDNs (Content Delivery Networks) und Internet Routing Overlays einsetzen, um nicht nur die Verfügbarkeit zu gewährleisten, sondern auch eine Performance zu erreichen, die mit früheren Methoden undenkbar war.

Bedrohungsschutz

Lösungen wie Akamai Enterprise Application Access können Ihre Anwendungen vor Angriffen schützen. Aber wie sieht es damit aus, Nutzer davor zu schützen, unbeabsichtigt zu einem solchen Angreifer zu werden, beispielsweise über ein durch Malware infiziertes Gerät oder den Diebstahl von Anmeldedaten über einen Phishing-Link und eine Landingpage? Hier kommen die Überwachung und Analyse des Webtraffics ins Spiel.

Ein Ansatz ist die Implementierung einer cloudbasierten DNS-Firewall-Lösung wie Akamai Secure Internet Access. Dieses Produkt untersucht jede DNS-Anfrage von Nutzern und wendet Echtzeit-Bedrohungsinformationen an, sodass sichere Anfragen normal aufgelöst werden, Anfragen an schädliche Domains jedoch proaktiv blockiert werden. Dadurch wird das Risiko verringert, dass die Geräte von Mitarbeitern durch Malware oder Ransomware gefährdet oder Opfer eines Phishing-Angriffs werden.

Zusammenfassung

Die klassische Hub-and-Spoke-Netzwerkarchitektur und der Sicherheitsansatz abgeschotteter Unternehmensnetzwerke bieten in der heutigen, von Cloud und Mobilität geprägten Welt einfach keine ausreichende Performance und Sicherheit. Dies ist ein Problem, das alle Unternehmen angehen müssen, um nicht schutzlos dazustehen. Veraltete Sicherheitsarchitekturen sind die Hauptursache für Datenschutzvorfälle in Unternehmen – und die Anzahl an Vorfällen wird in den kommenden Jahren noch zunehmen. Unternehmen können sich nicht vor dieser Entwicklung schützen, indem sie sich hinter den Mauern ihres internen Netzwerks verstecken. Denn diese Mauern existieren nicht mehr.

Nächste Schritte

Wie funktioniert der Übergang zu einer Zero Trust Network Access-Architektur?

Die Cloud Security Services von Akamai lassen sich kombinieren und schaffen damit eine umfassende Zero Trust Network Access-Architektur, die nicht nur den sicheren Anwendungszugriff über Multicloudtechnologien gewährleistet, sondern die internen Unternehmensnetzwerke fast vollständig überflüssig macht.

Durch unsere fortschrittliche verteilte IAP-Lösung und die phishing-sichere Multi-Faktor-Authentifizierung sowie die Performance der Akamai Connected Cloud können Sie die klassische Netzwerkarchitektur auf einfache Weise hinter sich lassen. Sie können Anwendungen schrittweise migrieren, um Migrationsrisiken zu minimieren, und erhalten Zugang zu der umfassenden Erfahrung, die wir bereits mit unseren Performance- und Sicherheitslösungen gewinnen konnten.

Wir werden Ihre Entwicklung zu Zero Trust auch in Zukunft eng verfolgen und Sie auf jedem Schritt begleiten. Mit unserer Unterstützung schaffen Sie eine Netzwerkarchitektur, die nicht nur den Zugriff auf Ihre Anwendungen und Daten ermöglicht, sondern sich auch einfach verwalten lässt und optimale Sicherheit und Performance bietet.

Erfahren Sie mehr darüber, wie Sie Ihre Geschäftsanforderungen mit dem Zero-Trust-Portfolio von Akamai erfüllen können.