Antworten der Referenten Marlo Ehrlich und Sami Makki zu Fragen der Teilnehmer, die während der Live-Sendung aus Zeitgründen nicht beantwortet werden konnten:

Frage 1:

Ist Microsoft "Always On" mit Zero Trust vereinbar bzw. verknüpfbar?

Antwort:

Microsoft Always On ist eine Art VPN-Lösung. Dies hier erklärt. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-technology-overview.

Es verwendet IKEv2, ein VPN-Tunneling-Protokoll, dessen Hauptvorteil darin besteht, dass es Unterbrechungen in der zugrunde liegenden Netzwerkverbindung toleriert. Wenn beispielsweise die Verbindung vorübergehend unterbrochen wird oder ein Benutzer einen Client-Computer von einem Netzwerk in ein anderes verschiebt, stellt IKEv2 die VPN-Verbindung automatisch wieder her, wenn die Netzwerkverbindung wiederhergestellt wird – alles ohne Benutzereingriff.

Kompatibilität mit Akamais Enterprise Application Access (EAA):

Die Lösung ist vollständig mit EAA kompatibel. EAA kann mit Always On von Microsoft für clientlose EAA-Apps koexistieren. Und wenn EAA-Client erforderlich ist, müssen wir überprüfen, auf welche Anwendungen über Always On zugegriffen wird und auf welche über EAA-Client zugegriffen werden soll. Wir können Whitelists von Zielen erstellen, die wir immer durch den Always On-Client auf dem Gerät senden möchten, anstatt über den EAA-Client und umgekehrt.

Zusammenfassend lässt sich sagen, dass EAA mit Always On VPN kompatibel ist.

Kompatibilität mit ETP (Enterprise Thread Protector):

ETP funktioniert möglicherweise nicht gut mit der Always-On-VPN-Einstellung, wenn vertrauenswürdige DNS-Server definiert sind. Eine Lösung hierfür wäre, "127.0.0.1" zur Liste der vertrauenswürdigen DNS-Server hinzuzufügen

Frage 2:

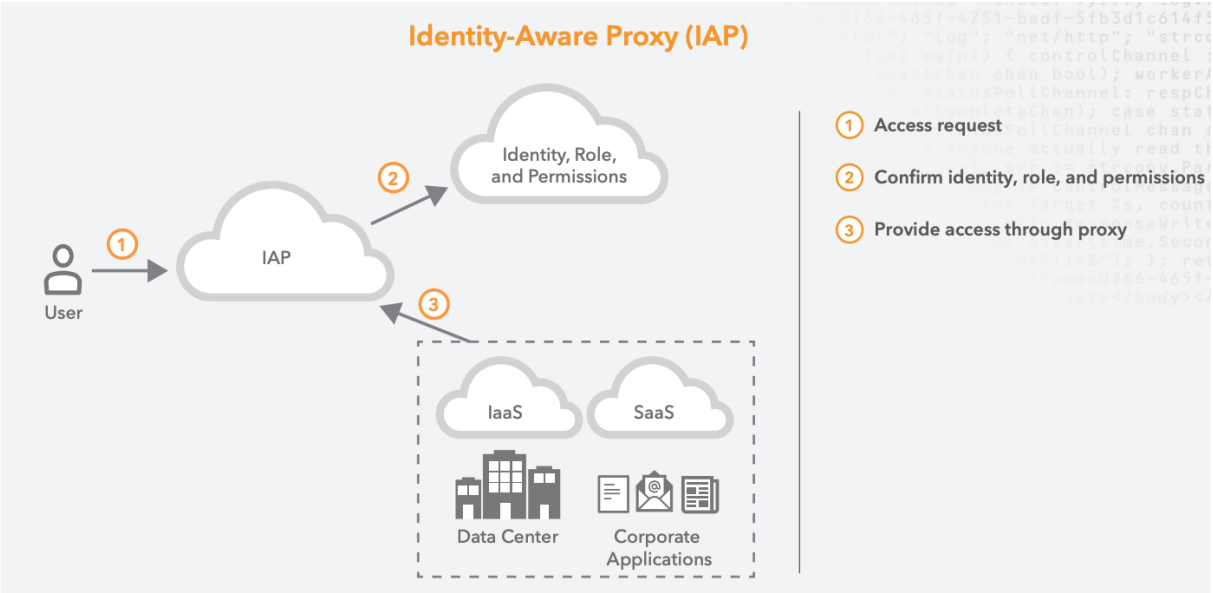
Das sind alles Security Techniken, WAF, Einsatz von Proxys usw... Wie ist denn der Ansatz das der klassische VPN ersetzt wird durch Zero Trust?

Antwort:

Eine Identity-Aware Proxy (IAP)-Architektur bietet Zugriff auf Anwendungen über einen Cloud-basierten Proxy. Identität und Autorisierung erfolgen am Edge und basieren auf „need to know“, den Least-Privilege-Prinzipien, die dem Zugriff über Software-Defined Perimeters

(SDPs) ähnlich sind, aber stattdessen Standard-HTTPS-Protokolle auf der Anwendungsschicht (Layer 7) verwenden. Eine Schlüsselkomponente eines IAP ist eine Identitätsquelle, die das Vertrauen von Benutzern und Geräten (Authentifizierung) und den Zugriffsrechten (Autorisierung) überprüft. Diese Identitätsquelle kann auf Unternehmensverzeichnissen oder Cloud-basierten Identitätsanbietern basieren. Noch bevor die Identität eines Benutzers validiert wird, kann durch die Überprüfung des Gerätezustands sichergestellt werden, dass das Gerät, das versucht, Zugriff zu erhalten, bestimmte Sicherheitskriterien erfüllt, z.B. ob ein Client Zertifikat vorhanden ist, das neueste Betriebssystem Update installiert ist oder bestimmte „Endpoint Detection & Protection Lösungen installiert und betriebsbereit sind.

Ein bemerkenswerter Vorteil von IAP im Vergleich zu anderen Zugangstechnologien: Es werden nicht nur Benutzer verifiziert, sondern auch der Traffic der Benutzer überprüft und einzelne Anwendungsanfragen können beendet, überprüft und autorisiert werden. Sobald eine Transaktion auf dem Proxy beendet wird, können zusätzliche Dienste integriert werden, die eine verbesserte Benutzererfahrung und einen verbesserten Anwendungsschutz ermöglichen.



IAP basiert auch auf Zugriffskontrollen auf Anwendungsebene, nicht auf Firewall-Regeln; konfigurierte Richtlinien können Benutzer- und Anwendungsabsichten widerspiegeln, nicht nur Ports und IPs. Wie SDPs kann dieser Ansatz die Anwendungen und andere Assets in der Cloud oder hinter der Firewall verbergen und ist für Webanwendungen clientlos. Mit zunehmender Cloud-Akzeptanz rückt die Herausforderung der Migration von Unternehmensanwendungen in den Fokus. Viele Unternehmen haben Schwierigkeiten, die Cloud für Cloud-native und traditionelle Anwendungen gleichermaßen zu nutzen. IAP kann nicht nur verwendet werden, um Benutzer für native SaaS-Anwendungen zu authentifizieren, sondern es kann auch verwendet werden, um im Wesentlichen Legacy-Anwendungen im Rechenzentrum zu „SaaS-ify-en“. Darüber hinaus erleichtert ein Proxy die Cloud-Migration und die Anwendungsmodernisierung, ohne auf eine vollständige Rip-and-Replace-Strategie zurückgreifen zu müssen. Auf diese Weise können Unternehmen einen methodischen, schrittweisen Ansatz zur Implementierung von Zero Trust verfolgen und

gleichzeitig den technischen Aufwand reduzieren, der mit alten perimeterbasierten Kontrollen und traditionellen VPNs verbunden ist.

Frage 3:

Gibt es Einschränkungen für Applikationen, welche eine Server > Client-Verbindung herstellen ? Bspw. RemoteAccess, SW-Push o.ä.

Antwort:

In Enterprise Application Access müssen Verbindungen auf der Clientseite beginnen. Das heißt: Remote-Benutzer müssen die Verbindung zu den integrierten Anwendungen herstellen. Diese Lösung soll nicht umgekehrt funktionieren (Server startet die Kommunikation mit Benutzern…)

Frage 4:

Wie ist diese Lösung im Vergleich zu VMware Horizon?

Antwort:

VMWare Horizon ist eine Virtualisierungslösung, mit der Unternehmen virtuelle Desktops, Apps oder Server vor Ort oder in der Cloud ausführen können, um diese Ressourcen remote bereitzustellen. Dies ist ein anderer Ansatz für den Zugriff auf Unternehmensanwendungen.

Mit EAA virtualisieren wir keine App. Wir „onboarden“ Anwendungen, Server usw. auf sehr sichere Weise. Wir veröffentlichen keine internen Ressourcen im Internet. Unsere Konnektoren kommunizieren mit den internen Apps und erstellen dann ausgehende mTLS-Verbindungen zu EAA-Cloudservern. Jede Anwendung hat einen externen Hostnamen, der in eine interne IP/FQDN „übersetzt“ wird. Die Remote-Benutzer rufen die externe URL auf und es startet den Zero Trust IAP-Prozess:

1. Der Benutzer wird durch einen in EAA definierten IDP authentifiziert.
2. Der Benutzer wird autorisiert (Rollen und Berechtigungen werden geprüft)
3. Zwischenregeln für die Access Control Rules, device Posture (Sicherheit des Geräts) usw. können angewendet werden, bevor der Zugriff gewährt wird. Sie können zusätzlich den Authentifizierungsprozess verstärken, indem Sie die MFA-Funktion hinzufügen.
4. Der Zugang zur App wird bereitgestellt.

Dies ist ein „mapping“ des Benutzers zur Applikation auf L7 unter Anwendung des Prinzips der geringsten Rechte (least priviledge).

Frage 5:

In den Ausführungen wird immer der Client in den Fokus gestellt. Bei Zero Trust geht es doch aber einen Identity based Zugriff. Wie wird den mit Sessions von BYOD ohne den angemerkten Zero Trust Client umgegangen?

Antwort:

Ohne den auf dem Gerät installierten EAA-Client (Enterprise Application Access) kann der Benutzer mit dem Gerät über den Browser im clientlosen Modus über EAA auf Anwendungen und Dienste zugreifen. Die Benutzererfahrung wäre die gleiche: Der Benutzer würde auf eine bereitgestellte externe URL zugreifen, er würde aufgefordert, sich über den Identitätsanbieter (IDP) zu authentifizieren, und wenn die Anmeldeinformationen in Ordnung sind und der Benutzer über die entsprechende Autorisierung verfügt, kann er auf die App zugreifen.

Frage 6:

Kann der Zugriff aus SaaS Lösungen darüber eingeschränkt werden, damit kein Whitelisting erforderlich ist?

Antwort:

Nein. Für SaaS-Anwendungen, kann EAA (Akamais Enterprise Application Access) nur für die Kontrolle der Authentifizierung Vorteile bringen, wenn dies über einen in EAA definierten IDP konfiguriert wird. Im Allgemeinen greift EAA bei SaaS-Apps nicht in die Datenströme zwischen Benutzern und Anwendungen ein.

Frage 7:

Wie kann ich in einer ZeroTrust-Umgebung den Zugriff auf Verzeichnisse auf einen FileServer steuern? Gibt es das überhaupt noch oder ist der Zugriff nur auf Applicationsebene möglich?

Antwort:

In EAA (Enterprise Application Access) wird der Zugang auf Anwendungsebene bereitgestellt. Für einen Dateiserver können Sie den Zugriff nur auf die spezifischen Verzeichnisse des Dateiservers konfigurieren, auf die Ihre Remotebenutzer zugreifen müssen.

Frage 8:

Wie managed man das Thema 'Authorisierung' - jede Applikation macht das ja schon 'für sich'

Antwort:

In EAA (Enterprise Application Access) können wir die Authentifizierung + Autorisierung an einen 3rd Party Indentity Provider delegieren oder die Autorisierung von Benutzern selber

durchführen. In letzteren Fall würde EAA auf Anwendungsebene die in der integrierten App vordefinierten Benutzergruppen für den Zugriff auf die Anwendung prüfen. Wenn sich der Benutzer ordnungsgemäß authentifiziert, aber nicht für diese Anwendung autorisiert ist, wird der Zugriff verweigert.

Frage 9:

Im Identity Management war ja der Trend zu Gruppenberechtigungen. Habe ich diese Gruppen bei ZeroTrust auch?

Antwort:

Ja, wenn gewünscht. Wir können in EAA (Enterprise Application Access) ein „directory“ integrieren, um die Berechtigungen eines Benutzers/einer Benutzergruppe zu überprüfen, nachdem der Benutzer authentifiziert wurde.

Frage 10:

Sollte der ZeroTrust-Ansatz auch für alle interne Clients realisiert werden?

Antwort:

Standardmäßig ist die Erfahrung aller Benutzer gleich: Der Benutzer fragt nach einer Ressource, die sich in der EAA Cloud (Enterprise Application Access) befindet. Der Benutzer wird über die mit der Cloud vorgefertigte Konnektorverbindung (die den Zugriff auf die Anwendung ermöglicht) zur App geleitet.

Auf Wunsch können wir jedoch die Funktion der „On-Premises-Netzwerkerkennung“ in der Lösung aktivieren, was bedeutet, dass unser Identitätsanbieter erkennt, dass der Benutzer vom internen Netzwerk aus zugreift, und wenn er/sie intern auf die Ressource zugreifen möchte, würde der Datenverkehr nicht durch die Cloud gehen sondern intern an die App weitergeleitet.

Weitere Erläuterungen finden Sie unter diesem Link: https://learn.akamai.com/en-us/webhelp/enterprise-application-access/eaa-client-connector-admin-guide/GUID-3B6C0E0A-D15E-4406-BD74-4DE7C24F3312.html

Frage 11:

Eignet sich ZeroTrust auch für M2M access?

Antwort:

Es ist nicht der ideale Anwendungsfall. Zero Trust ist eher für den Zugriff von Mensch zu Maschine gedacht, aber wir haben in Projekten gearbeitet, in denen M2M-Zugriff bereitgestellt wurde.

Beispiel: Ein Computer, auf dem ein Skript ausgeführt wird, das Aufrufe an Anwendungen durchführt, die in der Zero Trust Lösung EAA (Akamai Enterprise Application Access) integriert sind. Die Authentifizierung erfolgt automatisch über das im Skript enthaltene Zertifikat und der Zugriff auf die Anwendung erfolgt normal.

Frage 12:

Wenn man sich entscheidet auf Zero Trust umzustellen, gibt es dann überhaupt noch eine Notwendigkeit für ein VPN ?

Antwort:

Einer der Anwendungsfälle von Zero Trust (ZTNA) ist der VPN-Ersatz, aber beides: Zero Trust Remote Access und traditionelle VPNs können nebeneinander existieren.

Frage 13: ***((Ähnliche Fragen von drei Teilnehmern))***

a) Wie ist denn das Lizenzmodell und was kostet eine solche Lösung?

b) Mit welchen ungefähren Kosten muss man für diese Zero-Trust-Technolgie in einem Kleinstbetrieb (< 5 User) rechnen?

c) Preismodell? Auch für kleine Kunden interessant? Partnermodell für Services?

Antwort:

Der Preis richtet sich nach dem Anzahl der User/Mitarbeiter. Kontaktieren sie mich hierfür gerne unter smakki@akamai.com

Frage 14;

Mit hunderten von Applikationen on-prem wird es meistens eine hybridlösung (VPN/App freigabe) geben-. In manchen firmen moglicherweise über Jahre hinweg... Dies ist ein insgesamt ein großes transformations projekt uns umfasst alle unternehmensgruppen (Businesslines, IT, HR).

Antwort:

Mit dem Zero Trust Produkt von Akamai (Akamai Enterprise Application Access kurz EAA ist der ROI recht schnell und die Bereitstellung der Lösung mit Hunderten von Apps dauert nicht so lange. Dies ist eine Frage des angemessenen Umfangs des Projekts. Da keine Änderungen an der Rechenzentrums-/Unternehmensinfrastruktur erforderlich sind und alle unsere Lösungen Cloud-basiert sind, ist die Konfiguration in der Regel recht schnell.

Frage 15:

Was wäre hinsichtlich Zero Trust an einem Terminalserver Zugriff auf den "Unternehmensdesktop" falsch?

Antwort:

Ich versteh die Frage leider nicht ganz.

Wir können mit unserem Zero Trust Ansatz auch Remote-Zugriff auf einen Unternehmens-Desktop mit RDP über https bereitstellen, als normale https-Anwendung, die den RDP-Datenverkehr umschließt. oder mit einer Tunnel-App, die den Datenverkehr des RDP-Clients vom Endbenutzer in die Cloud umschließt.

Frage 16:

Ist der Zugriff auf M365 Dienste über die Akamai Lösung eine Alternative zu Conditional Access bei MS, bei dem nur ein Login durch managed devices möglich ist?

Antwort:

Nein. Für M465, welches eine SaaS-App ist, kann EAA (Akamais Enterprise Application Access) nur für die Kontrolle der Authentifizierung Vorteile bringen, wenn dies über einen in EAA definierten IDP konfiguriert wird. Im Allgemeinen greift EAA bei SaaS-Apps nicht in die Datenströme zwischen Benutzern und Anwendungen ein.