aruba
a Hewlett Packard Enterprise company

LÖSUNGSÜBERBLICK

Netzwerkzugriffs-steuerung mit Aruba ClearPass

FLEXIBLE UND STABILE ROLLENBASIERTE RICHTLINIEN ZUR IMPLEMENTIERUNG EINER ZERO-TRUST-NETZWERKSICHERHEIT IN UNTERNEHMEN

Mit der zunehmenden Nutzung von IoT-Geräten und Initiativen für hybrides Arbeiten hat die Komplexität im Netzwerk zugenommen, und es gibt mehr betriebliche Ineffizienzen. Gleichzeitig steigen die Herausforderungen an die Transparenz und Sicherheit.

Zu wissen, wer und was sich genau mit dem Netzwerk verbindet, ist der erste Schritt auf dem Weg zu Sicherheit in Ihrem Unternehmen. Die Kontrolle durch die automatisierte Anwendung der kabelgebundenen und kabellosen Richtliniendurchsetzung stellt sicher, dass nur autorisierte und authentifizierte Benutzer und Geräte eine Verbindung zu Ihrem Netzwerk herstellen dürfen. Gleichzeitig braucht es Angriffsreaktionen in Echtzeit und Bedrohungsschutz, um interne und externe Audit- und Compliance-Anforderungen zu sichern und zu erfüllen.

Durch die Verwendung von IoT-Geräten auf kabelgebundenen und kabellosen Netzwerken verlagert sich der Schwerpunkt in den IT-Abteilungen. Viele Unternehmen sichern zwar ihre kabellosen Netzwerke und Geräte, haben jedoch die kabelgebundenen Ports in Konferenzräumen, bei IP-Telefonen und im Druckerbereich vernachlässigt. Kabelgebundene Geräte – wie Sensoren, Sicherheitskameras und medizinische Geräte – zwingen die IT-Abteilungen, darüber nachzudenken, wie sie die Millionen von kabelgebundenen Ports sichern, die eine große Angriffsfläche für Sicherheitsbedrohungen bieten. Da diese Geräte in der Regel nicht die notwendigen Sicherheitsmerkmale aufweisen und Zugriff auf externe Verwaltungsquellen, Anwendungen oder Service-Provider benötigen, birgt der Zugriff über kabelgebundene Geräte mittlerweile auch Risikopotenzial.

Der IT ist weiterhin sehr engagiert bemüht, die Kontrolle aufrechtzuerhalten. Daher sind die richtigen Tools erforderlich, um schnell die zugrundeliegende Infrastruktur zu programmieren und den Netzwerkzugriff für alle IoT- und mobilen Geräte zu kontrollieren – für bekannte und unbekannte Geräte. Eines der Grundprinzipien eines Zero-Trust-Sicherheitsframework ist, dass das Netzwerk grundsätzlich nicht vertrauenswürdig ist und der Zugriff auf IT-Ressourcen nicht nur davon bestimmt werden sollte, wo oder wie sich ein Client verbindet. Ein Zero-Trust-Framework sollte den Sicherheits-Lifecycle eines Endgeräts von der Identifizierung, Authentifizierung und Autorisierung bis hin zur kontinuierlichen Überwachung und Reaktion auf Angriffe verwalten. Wenn Sicherheitslösungen für den Netzwerkzugriff den Schutz vor Bedrohungen verbessern und bessere Benutzererfahrung bieten wollen, müssen sie heutzutage das Zero-Trust-Framework in Betracht ziehen.

HYBRIDE ARBEIT UND IoT ÄNDERN UNSERE SICHTWEISE ZUM THEMA ZUGRIFFSKONTROLLE

Initiativen für hybride Arbeitsplätze, IoT und Edge Computing lösen den traditionellen IT-Perimeter auf. Die Unternehmen müssen zeit- und ortsunabhängige Konnektivität gewährleisten, ohne Kompromisse bei der Sicherheit einzugehen sowie Transparenz und Kontrolle aufrechterhalten, ohne das Benutzererlebnis zu beeinträchtigen. Es beginnt mit der Identifizierung aller Personen, die sich mit dem Netzwerk verbinden, der Authentifizierung und Autorisierung dieser Personen und der Durchsetzung robuster Richtlinien im gesamten Netzwerk.

1. **Erkennen**, welche und wie viele Clients verwendet werden, über welchen Kanal sie ins Netzwerk gelangen und welche Betriebssysteme unterstützt werden. Dies ist die Basis für mehr Transparenz. Bei vielen speziell entwickelten IoT-Geräten, wie man sie beispielsweise in einem Krankenhaus oder in einer Fertigungshalle findet, ist das Verständnis des

tatsächlichen Verhaltens der Geräte die einzige Möglichkeit, diese genau zu identifizieren. Kontinuierliche Einblicke in die unternehmensweite Gerätelandschaft und in potenzielle Gefährdungen der Gerätesicherheit sowie Erkenntnisse darüber, welche Elemente hinzukommen oder abgezogen werden, vermitteln Ihnen die erforderliche langfristige Transparenz, um die Endgeräte im Netzwerk zu sichern.

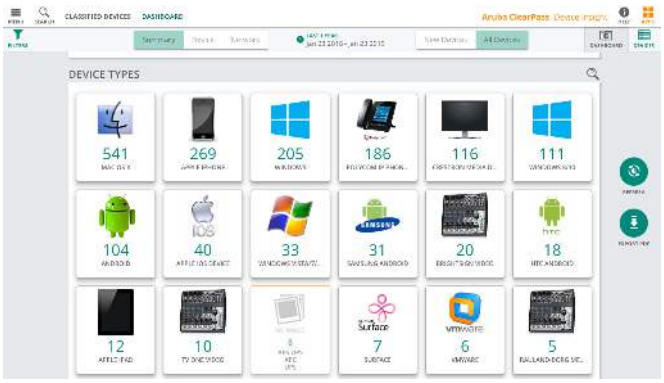
2. **Authentifizieren und autorisieren** der Geräte, die sich mit Ihrem Netzwerk verbinden über Zero Trust nach dem bewährten Prinzip des „geringstmöglichen Zugriffs". Setzen Sie eine Zugriffskontrolle auf, die den ordnungsgemäßen Zugriff durch Benutzer und Geräte unabhängig von Benutzer, Gerätetyp oder Standort regelt. Auf diese Weise wird das erwartete Benutzererlebnis sichergestellt. Unternehmen müssen sich an die heute festzustellende zunehmende Anzahl von Geräten und deren Nutzung gewöhnen – sei es ein Smartphone oder eine Überwachungskamera.
3. **Umsetzen** automatisierter Reaktionen über eine dynamische Richtliniensteuerung und Beseitigung von Bedrohungen in Echtzeit. Dies gilt auch für Systeme von Drittanbietern. Dies ist das letzte Puzzleteilchen. Wenn Sie auch um 3 Uhr morgens auf ungewöhnliches Verhalten im Netzwerk vorbereitet sein wollen, brauchen Sie einen einheitlichen Ansatz, durch den der Datenverkehr blockiert und der Status der Verbindung eines Geräts geändert werden kann.

Unternehmen müssen in ihren Planungen vorhandene aber auch unvorhergesehene Herausforderungen berücksichtigen. Durch die Überlastung der Operations-Teams ist es eher unrealistisch, sich auf die IT und die Help-Desk-Mitarbeiter zu verlassen, damit diese jedes Mal manuell eingreifen, wenn ein Benutzer sich für die Remote-Arbeit entscheidet oder ein neues Smartphone kauft. Bei einer NAC-Lösung (Network Access Control) geht es nicht mehr nur um die Bewertung bekannter Geräte, bevor diese ins Netzwerk gelangen. Bei dieser Lösung handelt es sich um einen entscheidenden Faktor, um das Netzwerk dynamisch zu schützen, wenn neue oder vorhandene Geräte integriert oder verlagert werden, oder neue Services anfordern.

UMFASSENDE NETZWERKÜBERGREIFENDE TRANSPARENZ

Sicherheit beginnt mit umfassender Transparenz zu allen Geräten – Sie können nicht sichern, was Sie nicht sehen. Aruba bietet eine Auswahl an Cloud-basierten und On-Premises-Lösungen für Kundentransparenz und Profilerstellung. Client Insights ist eine KI-basierte, Cloud-basierte Lösung zur Client-Identifizierung und Profilerstellung und wird mit Aruba Central geliefert. Die Installation zusätzlicher Collectors oder Host-Agenten ist nicht erforderlich. ClearPass Device Insight ist eine lokale Geräteerkennungs- und Profilerstellungslösung, die auch mit der Infrastruktur von Drittanbietern funktioniert.

Client Insights und ClearPass Device Insight verbessern die Kernkompetenzen bei der Geräteerkennung und Profilerstellung erheblich, um die breite Palette von IoT-Geräten in zahlreichen Umgebungen zu identifizieren. Dies wird durch eine Kombination aus Deep Packet Inspection (DPI), fortschrittlichem maschinellem Lernen und Crowdsourcing von Geräte-Fingerabdrücken erreicht. Weitere Informationen finden Sie hier.



Echte Sicherheit ist nur durch umfassende Transparenz und Kontrolle zu erreichen. So wird sichergestellt, dass nur authentifizierte oder autorisierte Geräte ins Netzwerk gelangen. Dies hat seine Ursache in einer Richtlinie, die auf Geräte in kabelgebundenen und kabellosen Netzwerken mit Komponenten mehrerer Anbieter abgestimmt wurde.

ROLLENBASIERTER ZUGRIFF UND RICHTLINIENDURCHSETZUNG

Durch die vorlagenbasierte Richtliniendurchsetzung kann die IT-Abteilung Richtlinien für kabelgebundene und kabellose Netzwerke definieren, bei der intelligente Kontextelemente wie Benutzerrollen, Gerätetypen, MDM-/EMM-Daten, Zertifikatsstatus, Standort, Wochentag usw. zum Tragen kommen. Ganz gleich, wie sich Geräte verbinden, setzt Aruba Dynamic Segmentation automatisch konsistente Richtlinien im gesamten kabelgebundenen oder kabellosen Netzwerk durch – basierend auf einem Zugriff auf IT-Ressourcen nach dem Prinzip der geringsten Rechte, indem der Datenverkehr auf der Grundlage der jeweiligen Identität und der zugehörigen Zugriffsberechtigung segmentiert wird. Bei diesem grundlegenden Konzept eines Zero-Trust-Frameworks basiert Vertrauen auf Rollen und Richtlinien – und nicht darauf, wo und wie sich Benutzer oder Endpunkt-Clients wie IoT-Geräte verbinden. Die dynamische Segmentierung vereinheitlicht den rollenbasierten Zugriff und die Richtliniendurchsetzung in kabelgebundenen, kabellosen und WAN-Netzwerken mit zentralisierter Richtliniendefinition und einer Auswahl an Durchsetzungsmodellen – zentralisiert oder verteilt – basierend auf der gesamten Netzwerkarchitektur.

Stabile Netzwerkrichtlinien mit ClearPass Policy Manager

ClearPass Policy Manager (CPPM) bietet Authentifizierungs- und Autorisierungsfunktionen sowie zentralisierte Richtliniendefinitionen, die dem Benutzer im gesamten Netzwerk folgen und einheitlich auf kabellose, kabelgebundene und VPN-Verbindungen angewendet werden. Wenn Benutzer zu einem unbekannten Gerät wechseln oder sich in einem ungesicherten Netzwerk befinden, ändert die Richtlinie automatisch die Berechtigungen.

ClearPass unterstützt die normenbasierte 802.1X-Durchsetzung und andere Techniken zur sicheren Authentifizierung. Der Policy Manager lässt sich in zahlreiche Authentifizierungslösungen integrieren, unterstützt Multifaktor-Authentifizierung und bietet die Möglichkeit, an wichtigen Punkten im Netzwerk eine erneute Authentifizierung zu erzwingen.

ClearPass erhielt eine Anerkennung des begehrten Cyber Catalyst. Das zeigt, dass führende Versicherer glauben, dass Aruba ClearPass zur Reduzierung von Cyber-Risiken beitragen kann und dringend verdient, von Unternehmen in Betracht gezogen zu werden, die nach Lösungen suchen, wie sie ihre Cyber-Risiken erheblich verbessern können

Automatisierte Netzwerkkonfiguration und Richtliniendurchsetzung mit Aruba Central NetConductor

Aruba Central NetConductor ist eine Lösung der nächsten Generation – entwickelt, um die Bereitstellung, die Verwaltung und den Schutz komplexer, global verteilter Unternehmensnetzwerke zu automatisieren und zu beschleunigen.

Für Netzwerke, die über Aruba Central verwaltet werden, stellt NetConductor Cloud-native Sicherheitsservices zur Verfügung, die ein umfassend zentralisiertes Richtlinienmanagement sowie die Konfiguration eines Netzwerks mit einfacher Geschäftslogik-Schnittstelle und Workflows ermöglichen. NetConductor verwendet ein verteiltes EVPN/VXLAN-Netzwerk-Overlay, um die Inline-Richtliniendurchsetzung zu erleichtern.

ClearPass ergänzt Aruba Central NetConductor durch die Bereitstellung von AAA-Services (Authentifizierung, Autorisierung und Abrechnung), die sowohl RADIUS- als auch andere Ansätze ermöglichen, um sicherzustellen, dass Instanzen ordnungsgemäß identifiziert und einer Rolle zugewiesen werden, die ihre Zugriffsrechte definiert.

Kabelgebundene Verbindungen sind heute die neue Gefahrenquelle

ClearPass OnConnect ist eine integrierte Funktion, über die Unternehmen Tausende von kabelgebundenen Ports blockieren können, bei denen keine Durchsetzung von AAA-Richtlinien erfolgte. Es wird keine Gerätekonfiguration benötigt. Sie brauchen lediglich einen Befehlszeileneintrag im Switch. AAA/802.1X-Standardmethoden werden ebenfalls für kabelgebundene und kabellose Verbindungen unterstützt. Dadurch ist eine konsistente Richtliniendurchsetzung und ein durchgängiger Ansatz gewährleistet, der über isolierte AAA-, NAC- und Richtlinienlösungen nicht möglich wäre.

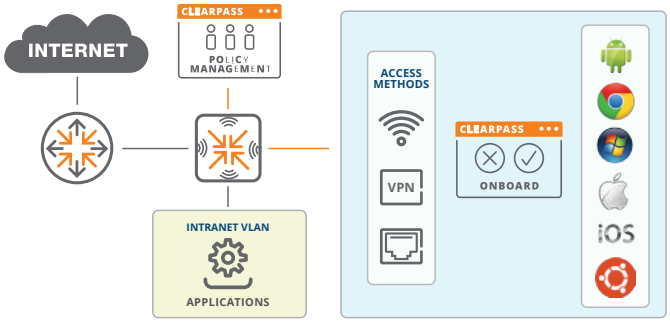
ClearPass kann innerhalb eines Richtlinien-Services mehrere Identitätsspeicher nutzen, beispielsweise Microsoft Active Directory, LDAP-konforme Verzeichnisse, ODBC-konforme SQL-Datenbanken, Token-Server und interne Datenbanken.

Gerätebereitstellung ohne Beteiligung der IT

Die Integration persönlicher Geräte für BYOD-Implementierungen kann für die IT-Abteilungen und Helpdesk-Mitarbeiter ein Problem darstellen und schnell zu Sicherheitsproblemen führen.

Mit ClearPass Onboard können Benutzer auf sichere Weise Geräte für die Verwendung in einem sicheren Netzwerk alleine konfigurieren. Durch gerätespezifische Zertifikate entfällt für die Benutzer die Notwendigkeit, ihre Anmeldedaten mehrmals am Tag einzugeben. Alleine dieser Komfort ist ein Gewinn für die Vereinfachung von Sicherheitsmechanismen. Das zusätzliche Maß an Sicherheit durch diese Zertifikate ist sozusagen ein Bonus für das Operations-Team.

Mithilfe von ClearPass Onboard definiert das IT-Team, wer berechtigt ist, Geräte zu integrieren, welche Gerätetypen integriert werden können und wie viele Geräte pro Person zulässig sind. Über eine integrierte Zertifizierungsstelle kann die IT-Abteilung persönliche Geräte schneller als über einen internen PKI unterstützen. Weitere IT-Ressourcen sind nicht erforderlich.



Gastzugriff – einfach und schnell

Automatische Gerätebereitstellung für sicheren BYOD-Betrieb mit ClearPass Onboard

Beim BYOD-Konzept geht es nicht nur um Geräte von Mitarbeitern. Es geht auch um Besucher, deren Geräte Netzwerkzugriff benötigen – kabelgebunden oder kabellos! IT-Abteilungen brauchen also ein einfach aufgebautes Modell, mit dem das Gerät an ein markenspezifisches

Portal weitergeleitet wird. Dann wird die Bereitstellung der Zugriffsberechtigungsnachweise automatisiert und es werden Sicherheitsfunktionen bereitgestellt, durch die der Datenverkehr im Netzwerk separiert werden kann.

Mit ClearPass Guest können Mitarbeiter, Mitarbeiter am Empfang, Veranstaltungskoordinatoren und andere IT-fremde Mitarbeiter einfach und effizient temporäre Netzwerkzugriffskonten für eine beliebige Anzahl an Gastbenutzern pro Tag erstellen. Mit MAC-Caching wird sichergestellt, dass Gastbenutzer tagsüber ohne großen Aufwand Netzwerkverbindungen herstellen können, ohne im Gastportal ihre Berechtigungsnachweise wiederholt eingeben zu müssen.

Die Selbstregistrierungsmöglichkeiten für Gastbenutzer entlasten Mitarbeiter. Zudem können die Besucher ihre eigenen Berechtigungsnachweise erstellen. Die Anmeldeinformationen werden als gedruckte Ausweise, SMS-Text oder E-Mails bereitgestellt. Diese Nachweise können für einen vorgegebenen Zeitraum in ClearPass gespeichert werden. Der Ablauf der Nachweise kann nach einer bestimmten Anzahl von Stunden oder Tagen automatisiert erfolgen.

Wenn der Gerätezustand die Zugriffsmöglichkeit bestimmt

Beim Autorisierungsprozess muss möglicherweise der Zustand bestimmter Geräte bewertet werden. Dadurch soll sichergestellt werden, dass die Geräte den Unternehmensrichtlinien für Virenschutz, Spyware und Firewalls entspricht. Durch die Prozessautomatisierung werden Benutzer eher motiviert, vor der Verbindung mit dem Unternehmensnetzwerk einen Virenscan durchzuführen.

ClearPass OnGuard bietet integrierte Funktionen, über die Zustandsprüfungen durchgeführt und dadurch Schwachstellen in einer Vielzahl von Betriebssystemen und -versionen eliminiert werden können. Unabhängig davon, ob Sie agentenlose, persistente oder auflösbare Clients verwenden, identifiziert ClearPass zentral kompatible Endpunkte in kabellosen, kabelgebundenen und VPN-Infrastrukturen.

Nachfolgend sind einige Beispiele für erweiterte Zustandsprüfungen aufgeführt, die zusätzliche Sicherheit bringen:

- Verarbeitung von Peer-to-Peer-Anwendungen, Services und Registrierungsschlüsseln
- Ermittlung, ob USB-Speichergeräte oder Instanzen virtueller Maschinen zulässig sind
- Verwaltung der Verwendung von überbrückten Netzwerkschnittstellen und Festplattenverschlüsselung

Vorteile von Drittanbieterlösungen umfassend nutzen

Das letzte, aber nicht minder wichtige Element einer sicheren Infrastruktur ist die schnelle Reaktion auf Ereignisse. Die Fähigkeit, auf Basis der Daten von anderen Anbietern von Sicherheitslösungen schnell auf Attacken zu reagieren, ist absolut wichtig. Mit Aruba 360 Security Exchange, unserem „Best of Breed"-Ökosystem, können die Beseitigung von Sicherheitsbedrohungen automatisiert oder Services optimiert werden, die Drittanbieterlösungen wie Firewalls, MDM/EMM, MFA, Registrierung von Besuchern und SIEM-Tools verwenden. Wenn Unternehmen die in ClearPass enthaltenen Kontextdaten nutzen, können diese umfassende Sicherheit und Transparenz auf Geräte-, Netzwerkzugriffs-, Datenverkehrsprüfungs- und Bedrohungsschutzebene gewährleisten.

Durch die Verwendung einer Common Language API (REST), Syslog-Benachrichtigungen und eines integrierten Repositorys namens ClearPass Exchange tragen automatisierte Workflows und Entscheidung zu einer Vereinfachung der Aufgaben und zum Schutz des Unternehmens bei – komplexe Skriptsprachen und mühselige manuelle Konfigurationen gehören somit der Vergangenheit an. Für eine schnellere Integration können Partner mit ClearPass Extensions eine Erweiterung hochladen, um neue Services in Echtzeit für gemeinsame Kunden bereitzustellen.

Mit ClearPass Exchange können Netzwerke automatisch Maßnahmen ergreifen:

- MDM/EMM-Daten wie der Jailbreak-Status eines Geräts können bestimmen, ob dieses Gerät eine Verbindung zum Netzwerk herstellen darf
- Firewalls können Richtlinien präzise für Benutzer, Gruppen und bestimmte Geräteattribute durchsetzen und mithilfe von ClearPass Abhilfe bei Geräten mit fehlerhaftem Verhalten leisten
- SIEM-Tools können für die Speicherung der Authentifizierungsdaten aller verbundenen Geräte eingerichtet werden
- Benutzer können aufgefordert werden, eine Multifaktor-Authentifizierung zu verwenden, um beim Verbinden mit Netzwerken und Ressourcen ihre Identität nachzuweisen

Bei Ereignissen im Netzwerk können Aufforderungen an Firewalls, SIEM-Tools und andere Tools gesendet werden, um ClearPass zu informieren, dass für ein Gerät Aktionen einzuleiten sind. Die Aktionen werden in beide Richtungen ausgelöst. Wenn ein Benutzer beispielsweise mehrfach ohne Erfolg versucht, sich im Netzwerk zu authentifizieren, kann ClearPass eine Benachrichtigungsmeldung direkt an das Gerät senden oder es auf die Deny-Liste für den Netzwerkzugriff setzen.

Standortunabhängiger sicherer Zugriff auf Arbeitsanwendungen

Die Anmeldung bei Arbeitsanwendungen im Verlauf des Tages muss schnell und ohne Aufwand erfolgen. Aus diesem Grund unterstützt ClearPass Single Sign-On und die automatische Anmeldefunktion von ClearPass. Anstelle einer SSO-Anmeldung, bei der sich jeder Benutzer einmal bei den Anwendungen anmelden muss, wird bei Auto Sign-On eine gültige Netzwerkanmeldung verwendet, um Benutzern automatisch Zugriff auf die mobilen Anwendungen im Unternehmen zu erlauben. Die Benutzer brauchen dann nur noch ihre Daten für die Netzwerkanmeldung oder ein gültiges Zertifikat auf ihren Geräten.

ClearPass kann auch als Identity-Provider (IdP) oder Service-Provider (SP) genutzt werden, wenn Single Sign-On verwendet wird.

Bonjour-, DLNA- und UPnP-Services

Projektoren, Fernsehgeräte, Drucker und andere Mediengeräte, die DLNA/UPnP oder Apple AirPlay und AirPrint verwenden, können von Benutzern in ihrer Aruba WLAN-Infrastruktur gemeinsam genutzt werden. Mit ClearPass lassen sich diese Geräte ganz einfach auffinden und gemeinsam nutzen.

So wird einem Lehrer, der eine Präsentation von einem Tablet zeigen möchte, nur ein im Klassenzimmer verfügbarer Bildschirm angezeigt. Geräte, die sich auf der anderen Seite des Campus befinden, werden nicht angezeigt. Über das Portal lässt sich auch festlegen, wer diese Bildschirme noch verwenden kann – so wird verhindert, dass die Studenten den Bildschirm steuern können.

Ein weiteres Beispiel stammt aus dem Gesundheitswesen – Ärzte können ohne großen Aufwand digitale Bilder, Röntgenbilder und MRI-Bilder von ihren iPads auf eine größere Bildschirmanzeige im Krankenhaus projizieren. Dadurch wird die Kommunikation zwischen Arzt und Patient einfacher. Benutzer- und standortspezifische Kontextdaten dienen als Grundlage sowohl für Sicherheits- als auch Aktivierungstools.

CLEARPASS BIETET SCHUTZ UND EFFIZIENZ FÜR ARUBA SD-BRANCH

Bei Dutzenden, Hunderten oder sogar Tausenden von einzelnen Zweigstellen, die eingerichtet, gesichert und gewartet werden müssen, sind sowohl Sicherheit als auch Effizienz für den Erfolg unabdingbar. Da ClearPass die rollenbasierte Zugriffskontrolle, die einem Benutzer oder Gerät über jede Art von Netzwerkverbindung folgt, zentral einrichtet, werden arbeitsintensive VLAN- und ACL-Einrichtung und Wildwuchs eliminiert. Innerhalb weniger Minuten können Unternehmen Standardberechtigungen für typische Anwender in den Zweigstellen wie Kunden, Mitarbeitende und Manager sowie Geräte wie Kassensysteme, Gebäudesteuerungen und Peripheriegeräte festlegen. Sobald die Richtlinien definiert sind, überträgt ClearPass sie automatisch an jeden Standort und passt den Zugriff basierend auf dem Geräte- und Benutzerstatus dynamisch an.

Durch integrierte Firewalls der nächsten Generation, Deep Packet Inspection und Inhaltsfilterung lesen und wenden Aruba Branch Gateways die Berechtigungen an, die jeder Rolle zugewiesen sind, ohne dass manuelle Änderungen am Netzwerk vorgenommen werden müssen. Im Gegensatz zu anderen Zweigstellenlösungen arbeitet ClearPass mit dem Aruba Branch Gateway zusammen, um Richtlinien bis einschließlich auf die Anwendungsebene zu definieren und durchzusetzen. Eine solche Zugriffskontrolle ist mit einer einfachen VLAN-Segmentierung nicht möglich. Darüber hinaus lässt sich ClearPass nicht nur mit Aruba, sondern mit über 140 Sicherheits- und IT-Lösungen betreiben, darunter Cloud-basierte Sicherheitslösungen von ZScaler, Palo Alto Networks und Checkpoint. So sorgt ClearPass für eine optimierte Sicherheitsstrategie.

ERKENNUNG VON BEDROHUNGEN VOR FOLGESCHÄDEN

Neue Bedrohungen kommen heute auch aus dem Unternehmen selbst – Attacken durch böswillige, gefährdete oder nachlässige Benutzer, Systeme und Geräte. Unternehmen müssen heute den Aspekt Sicherheit aus einem anderen Blickwinkel betrachten. Maschinelles Lernen und Verhaltensanalyse sind die nächsten Schritte zur Lösung der doppelten Krise von besser ausgestatteten Bedrohungsakteuren und unterbewerteten Sicherheitsmaßnahmen. Benutzer- und entitätsspezifische Verhaltensanalysen (User and Entity Behavior Analytics, UEBA) schließen die Lücke zwischen Gerätetransparenz und -kontrolle und der sekundären Bedrohung durch böswilliges Verhalten.

Aruba IntroSpect UEBA erkennt selbst die kleinsten Veränderungen im Verhalten – in einem bestimmten Zeitraum im Kontext betrachtet –, die auf Attacken hinweisen können, die durch die traditionellen Sicherheitsverfahren nicht entdeckt worden wären. Attacken durch gefährdete Benutzer und Hosts sind in der Regel schwer zu erkennen, da Cyberkriminelle Perimeterschutzmechanismen umgehen, indem sie legitime Berechtigungsnachweise verwenden, um auf Unternehmensressourcen zuzugreifen. Phishing Scams, Social Engineering und Malware sind einige der gängigen Mechanismen, die diese kriminellen Elemente nutzen, um sich Zugang zu den Anmeldedaten von Mitarbeitern zu verschaffen.

IntroSpect automatisiert die Erkennung solcher Attacken durch analysegesteuerte Transparenz. Fortschrittliche Technologien, darunter überwachte und nicht überwachte Modelle für maschinelles Lernen auf Daten aus der Netzwerk- und Sicherheitsinfrastruktur angewendet.

Aruba ClearPass NAC spielt eine Schlüsselrolle, wenn es darum geht, den Zero-Trust-Netzwerkzugriff (ZTNA) zu implementieren. Angesichts der größer werdenden Angriffsfläche für Cyberattacken wird eine sichere Netzwerkzugangskontrolle immer wichtiger, um böswillige Angriffe und Schäden für das Unternehmen zu verhindern. Die Anwendungsfälle sind vielfältig – Kontrolle der Gerätekonnektivität, Vereinfachung des BYOD-Konzepts, sicherer Gastzugriff –, die Antwort ist jedoch immer dieselbe. Über 10.000 Kunden in 100 Ländern haben ihr Netzwerk und ihr Unternehmen mit Aruba ClearPass gesichert und für mehr Transparenz, Kontrolle und Reaktionsschnelligkeit gesorgt.

© Copyright 2022 Hewlett Packard Enterprise Development LP. Die enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Die Garantien für Produkte und Services von Hewlett Packard Enterprise sind ausschließlich in der entsprechenden, zum Produkt oder Service gehörigen Garantieerklärung beschrieben. Aus den Informationen in diesem Dokument ergeben sich keinerlei zusätzliche Garantieansprüche. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

SO_ClearPass_SK_031822 a00054160dee