aruba
a Hewlett Packard Enterprise company

LÖSUNGSÜBERSICHT

ARUBA CLEARPASS POLICY MANAGER

Transparenter Zugriff und Sicherheit für kabelgebundene und kabellose Netzwerke

Erinnern Sie noch an die Zeiten, als die IT mit einer Kombination aus strengen Richtlinien und einem vollständigen Ökosystem das Sagen hatte? Diese Zeiten sind längst vorbei. Heutzutage sind IT und benutzereigene Geräte innerhalb und außerhalb der Perimetersicherheit miteinander verbunden.

Die Verwendung von Laptops, Smartphones, Tablets und IoT-Geräten (Internet of Things) am Arbeitsplatz nimmt immer stärker zu. Der erste Schritt zum Schutz Ihrer Daten besteht daher darin, zu erkennen, was im Netzwerk passiert. Durch die automatisierte Durchsetzung von Richtlinien wird sichergestellt, dass nur berechtigte Benutzer und Geräte eine Verbindung herstellen können. Zudem ist ein Echtzeitschutz vor Bedrohungen erforderlich, um interne und externe Audit- und Compliance-Anforderungen zu erfüllen.

Wenn sich die Erwartungen bestätigen, wird sich durch die Verwendung von IoT-Geräten in kabelgebundenen und kabellosen Netzwerken der Fokus der IT verlagern. Die meisten Unternehmen haben zwar für den Schutz ihrer kabellosen Netzwerke und Geräte gesorgt, dabei jedoch die kabelgebundenen Anschlüsse in Konferenzräumen, für IP-Telefone und in Druckerbereichen vernachlässigt. Da viele IoT-Geräte nicht ausreichend mit Sicherheitsfunktionen ausgestattet sind und den Zugriff über externe Administrationsressourcen erfordern, stellt der kabelgebundene Zugriff einen neuen Risikofaktor dar.

Der IT bereitet es Probleme, 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. Aktuelle Sicherheitslösungen für den Zugriff müssen Funktionen für die Profilerstellung, die Durchsetzung von Richtlinien, den Gastzugriff, die BYOD-Einbindung und weitere Funktionen umfassen, damit die IT entlastet, der Schutz vor Bedrohungen erweitert und das Benutzererlebnis optimiert wird.

MOBILITÄT UND IoT ÄNDERN DIE SICHTWEISE IN BEZUG AUF NAC

Die Grenzen der IT-Domäne gehen heutzutage weit über die vier Wände eines Unternehmens hinaus. Das Ziel vieler Unternehmen besteht darin, jederzeit und überall Konnektivität bereitzustellen, ohne Einbußen hinsichtlich der Sicherheit hinnehmen zu müssen. Wie kann die IT die Transparenz und Kontrolle aufrechterhalten, ohne die Geschäftsabläufe und das Benutzererlebnis zu beeinträchtigen? Der erste Schritt ist ein 3-stufiger Plan.

1. **Ermitteln** Sie, welche Geräte verwendet werden, die Anzahl der verwendeten Geräte, von wo aus die Verbindung hergestellt wird und welche Betriebssysteme unterstützt werden – diese Informationen bilden die Grundlage. Die kontinuierlichen Informationen über Änderungen und die Geräte, die sich an- und abmelden, ermöglichen im Lauf der Zeit die gewünschte Transparenz.

2. **Setzen** Sie präzise Richtlinien durch, die den ordnungsgemäßen Zugriff durch Benutzer und Geräte unabhängig von Benutzer, Gerätetyp oder Standort regeln. Auf diese Weise wird das erwartete Benutzererlebnis sichergestellt. Unternehmen müssen sich an die neuen Geräte und deren Verwendung anpassen – ob es sich um ein Smartphone oder eine Überwachungskamera handelt, ist dabei unerheblich.
3. **Schützen** Sie Ressourcen mithilfe einer dynamischem Richtliniensteuerung und der Beseitigung von Bedrohungen, die auch Systeme von Drittanbietern einschließen können. Dies ist das letzte Teil des Puzzles. Damit auch mitten in der Nacht auf ungewöhnliche Netzwerkaktivitäten reagiert werden kann, ist ein einheitlicher Ansatz erforderlich, der die Blockierung des Datenverkehrs und die Änderung des Status einer Geräteverbindung ermöglicht.

Unternehmen müssen auf vorhandene und unvorhergesehene Herausforderungen vorbereitet sein. Es ist nicht sehr realistisch, 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. NAC wird für mehr als die Ausführung von Bewertungen bekannter Geräte vor dem Zugriff eingesetzt.

THE POWER OF CLEARPASS EXCHANGE

VISUALISIERUNG UND VERWALTUNG AN EINEM ORT

Die ClearPass-Richtlinie und die AAA-Lösung umfassen eine integrierte Geräteprofilerstellung, eine webbasierte Verwaltungsschnittstelle und umfassende Berichterstellungsfunktionen mit Warnungen in Echtzeit. Sämtliche gesammelten kontextbezogenen Daten werden genutzt, um sicherzustellen, dass Benutzern und Geräten die geeigneten Zugriffsberechtigungen erteilt werden – unabhängig von Zugriffsmethode und Besitzer des jeweiligen Gerätes. Die integrierte Profilerstellungs-Engine sammelt Echtzeitdaten, die Gerätekategorien, Lieferanten, Betriebssystemversionen sowie weitere Informationen umfassen. Es muss nicht mehr geraten werden, wie viele Geräte mit den kabelgebundenen und kabellosen Netzwerken verbunden sind. Durch die differenzierte Transparenz werden die erforderlichen Daten bereitgestellt, um Audits zu bestehen und um Gründe für Performance- und Sicherheitsrisiken zu ermitteln.

Der eigenständige ClearPass Universal Profiler stellt den Unternehmen, die noch nicht für eine Durchsetzung aller Richtlinien bereit sind, dieselbe Transparenz bei der Profilerstellung bereit. Auch Bereiche, in denen ClearPass nicht von Anfang an bereitgestellt wird, werden berücksichtigt. Die Durchsetzung vorlagenbasierter Richtlinien ermöglicht der IT die Erstellung von Richtlinien für kabelgebundene und kabellose Netzwerke, die auf Benutzerrollen, Gerätetypen, MDM/EMM-Daten, Zertifikatstatus, Standort, Wochentage und mehr zurückgreifen. Durch die Richtlinien können auf einfache Weise Regeln für Mitarbeiter, Studenten, Ärzte, Gäste, Führungskräfte und die von diesen Personen verwendeten Gerätetypen durchgesetzt werden.

Die integrierte Funktion ClearPass OnConnect ermöglicht es Unternehmen, diese Tausende von kabelgebundenen Anschlüssen ohne AAA-Durchsetzung zu sperren. Für die Geräte ist keine Konfiguration erforderlich. Es wird nur ein Eintrag in der Befehlszeile benötigt. Standard AAA/802.1X-Methoden werden für kabelgebundene und kabellose Netzwerke ebenfalls unterstützt.

Auf diese Weise werden eine konsistente Richtliniendurchsetzung und ein End-to-End-Ansatz ermöglicht, die von isolierten AAA-, NAC- und Richtlinienlösungen nicht bereitgestellt werden können. 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 Verwaltung der Einbindung persönlicher Geräte für BYOD-Bereitstellungen kann eine große Belastung für IT- und Help Desk-Ressourcen darstellen und zu Sicherheitsbedenken führen.

Mit ClearPass Onboard können die Benutzer die Geräte für die Verwendung in sicheren Netzwerken eigenständig konfigurieren. Durch gerätespezifische Zertifikate entfällt für die Benutzer die Notwendigkeit, ihre Anmeldedaten mehrmals am Tag einzugeben. Allein das ist schon ein großer Vorteil. Die zusätzliche Sicherheit durch die Verwendung von Zertifikaten stellt einen weiteren Pluspunkt dar.

Das IT-Team legt Folgendes fest: wer Geräte einbinden kann, welcher Gerätetyp eingebunden werden kann und die Anzahl der Geräte, die eingebunden werden können. Durch eine integrierte Zertifizierungsstelle kann die IT persönliche Geräte schneller unterstützen als mit einer internen PKI. Weitere IT-Ressourcen sind nicht erforderlich.

Einfacher und schneller Gastzugriff

Bei BYOD geht es nicht nur um die Geräte der Mitarbeiter, sondern auch um die Geräte von Besuchern, die Netzwerkzugriff benötigen – kabelgebunden oder kabellos. Die IT benötigt ein einfaches Modell, das Geräte an ein Portal weiterleitet, die Bereitstellung der Anmeldeinformationen für den Zugriff automatisiert und auch Sicherheitsfunktionen bereitstellt, die eine Trennung des Unternehmensdatenverkehrs ermöglichen.

ClearPass Guest bietet Mitarbeitern, Empfangsmitarbeitern, Eventkoordinatoren sowie anderen, nicht zur IT gehörenden Mitarbeitern die Möglichkeit, für eine beliebige Anzahl an Besuchern pro Tag temporäre Konten für den Netzwerkzugriff zu erstellen. Mit MAC-Caching wird sichergestellt, dass sich die Besucher im Laufe des Tages nicht wiederholt am Gastportal anmelden müssen.

Über die Selbstregistrierung können Besucher ihre Anmeldeinformationen selbst erstellen, wodurch die Mitarbeiter entlastet werden. Die Anmeldeinformationen werden als gedruckte Ausweise, SMS-Text oder E-Mails bereitgestellt. Sie können für einen bestimmten Zeitraum in ClearPass gespeichert werden. Zudem kann ein automatisches Ablaufdatum, z. B. nach ein paar Stunden oder Tagen, festgelegt werden.

Der Gerätezustand entscheidet über den Zugriff

Während des Autorisierungsprozesses müssen u. U. für bestimmte Geräte Bewertungen des Zustands durchgeführt werden. Auf diese Weise wird sichergestellt, dass diese Geräte die Unternehmensrichtlinien hinsichtlich Virenschutz, Antispyware und Firewalls erfüllen. Durch die Automatisierung werden die Benutzer angehalten, einen Virenscan durchzuführen, bevor sie ihre Geräte mit dem Unternehmensnetzwerk verbinden.

ClearPass OnGuard ist mit integrierten Funktionen ausgestattet, die statusbasierte Systemdiagnosen durchführen, um Sicherheitslücken in einer Vielzahl von Computerbetriebssystemen und Versionen zu schließen. Unabhängig davon, ob Sie persistente oder auflösbare Clients verwenden, identifiziert ClearPass zentral kompatible Endpunkte in kabellosen, kabelgebundenen und VPN-Infrastrukturen.

Beispiele für erweiterte Systemdiagnosen, die zusätzliche Sicherheit bereitstellen:

- 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

Optimale Nutzung von Drittanbieter-Lösungen

Mit ClearPass Exchange können die Beseitigung von Sicherheitsbedrohungen automatisiert oder Services optimiert werden, die Drittanbieterlösungen wie Firewalls, MDM/EMM, MFA, Registrierung von Besuchern und SIEM-Tools verwenden. Die Nutzung der kontextbezogenen Informationen, die ClearPass bereitstellt, ermöglicht es Unternehmen, Sicherheit und Transparenz auf allen Ebenen sicherzustellen: Geräte, Netzwerkzugriff, Datenverkehr und Schutz vor Bedrohungen.

Durch die Verwendung einer Common Language API (REST), Syslog-Benachrichtigungen und eines integrierten Repositorys namens ClearPass Extensions 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. Damit Integrationen schneller erfolgen können, ermöglicht Extensions den Partnern das Hochladen von Erweiterungen, um gemeinsamen Kunden neue Services in Echtzeit bereitstellen zu können.

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 mehrstufige Authentifizierung zu durchlaufen, um ihre Identität beim Verbinden mit Netzwerken und Ressourcen nachzuweisen.

Durch Netzwerkereignisse können Firewalls, SIEM und andere Tools veranlasst werden, ClearPass zur Ergreifung von Maßnahmen auf einem Gerät aufzufordern. Dabei werden Aktionen 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 Blacklist für den Netzwerkzugriff setzen.

Sicherer Zugriff auf Anwendungen von überall aus

Der Zugriff auf arbeitsrelevante Anwendungen muss jederzeit schnell und reibungslos erfolgen. Aus diesem Grund unterstützt ClearPass SSO und die automatische Anmeldefunktion von ClearPass. Anstelle eines Single Sign-On, das die einmalige Anmeldung jedes Benutzers bei den Anwendungen erfordert, nutzt die automatische Anmeldung gültige Netzwerkanmeldedaten, um den Benutzern automatisch den Zugriff auf die mobilen Apps des Unternehmens zu ermöglichen. Die Benutzer benötigen nur ihre Netzwerkanmeldedaten oder ein gültiges Zertifikat auf ihren Geräten.

ClearPass kann darüber hinaus in den Bereichen als Identitätsanbieter (IdP) oder Serviceanbieter (SP) fungieren, in denen Single Sign-On verwendet wird.

Bonjour, DLNA und UPnP-Services

Projektoren, Fernsehgeräte und andere Mediengeräte, die DLNA/UPnP oder Apple AirPlay und AirPrint verwenden, können über die Aruba Wi-Fi-Infrastruktur von mehreren Benutzern gemeinsam genutzt werden. Mit ClearPass gestaltet sich das Erkennen dieser Geräte und die gemeinsame Nutzung äußerst einfach.

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.

Auch im Gesundheitswesen ist die Nutzung möglich – Ärzte haben die Möglichkeit, an jedem beliebigen Ort im Krankenhaus PACS-Bilder von ihren iPads auf größere Bildschirme zu übertragen. So wird die Zusammenarbeit mit den Patienten vereinfacht.

ADAPTIVES FUNDAMENT FÜR SICHERHEIT UND SERVICES

Die Bereitstellung eines reibungslosen Benutzererlebnisses für die mobilen Benutzer von heute und die schnelle Einbindung von IoT-Technologien haben die IT vor zahlreiche neue Herausforderungen gestellt. Um die Sicherheit des Zugriffs auf kabelgebundene und kabellose Netzwerke jederzeit und überall zu gewährleisten, sind Planung, die richtigen Tools und ein starkes Fundament unabdingbar.

ClearPass löst diese Herausforderungen durch die Bereitstellung der Geräteidentität, Richtliniensteuerung, Workflowautomatisierung und den automatisierten Schutz vor Bedrohungen in einer einzigen kohäsiven Lösung. ClearPass erfasst und korreliert kontextbezogene Daten in Echtzeit und ermöglicht so die Definition von Richtlinien, die in jeder Umgebung funktionieren – im Büro, auf dem Campus oder auf dem Sportplatz.

Die neuesten Erweiterungen von ClearPass bewältigen auch neue Herausforderungen bei der Netzwerksicherheit, die mit der Einbindung von IoT, einer besseren Authentifizierung von mobilen Geräten und Apps und mit einer besseren Transparenz bei Sicherheitsvorfällen einhergehen. Der automatisierte Schutz vor Bedrohungen und die intelligenten Servicefunktionen stellen sicher, dass jedem Gerät die entsprechenden Netzwerkzugriffsberechtigungen erteilt werden – bei minimaler Beteiligung der IT.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com SO_ClearPass_111016