aruba
a Hewlett Packard Enterprise company

ÜBERBLICK ÜBER DIE LÖSUNG

DER DIGITALE ARBEITSPLATZ

Enterprise Mobility, von der wir erwarten, jederzeit, überall und auf jedem Gerät zu arbeiten, ist heute eine Voraussetzung für den Geschäftserfolg. Smartphones und Tablets haben durch ihre explosionsartige Zunahme die Art, wie wir kommunizieren, Dienstleistungen in Anspruch nehmen und unseren Alltag organisieren, verändert. Außerdem hat die Kombination von Mobilgeräten und cloudbasierten Apps unser Arbeitsumfeld grundlegend verändert, indem offene, gemeinschaftlich genutzte Arbeitsbereiche und flexible Arbeitszeiten zur Norm werden.

Aber jetzt treibt das Internet der Dinge (IoT) eine noch größere Transformation voran, die alles von den Unternehmen und Geschäftsprozessen bis hin zu Kundenerfahrungen im Gesundheitswesen, Einzelhandel und an großen öffentlichen Veranstaltungsorten beeinflussen wird, um nur einige Beispiele zu nennen. Bisher galt IoT als Phänomen aus dem Consumerbereich, doch mittlerweile erkennen auch Unternehmen sein erhebliches Potenzial für die Schaffung intelligenterer, effizienterer Arbeitsplätze: intelligente Tagungsräume, Ortungsdienste und Überwachung in Echtzeit. Die Kombination von IoT-Geräten mit Kontextinformationen wie Standort, Anwendung und Richtlinien bietet die Chance, Kosten zu senken, Loyalität aufzubauen und Gewinne zu steigern.

Auch wenn das IoT viele Vorteile verspricht, bereitet der Gedanke an all die Geräte, die mit dem Netzwerk verbunden sind, den Sicherheits- und IT-Managern schlaflose Nächte. Das Phänomen BYOD war schon schlimm genug – private Geräte von Mitarbeitern und das riskante Benutzerverhalten, die die Grenzen eines sicheren Perimeters verschwimmen ließen. Diese Herausforderung konnte die IT jedoch bewältigen, indem sie auf bekannten, vertrauenswürdigen Kontextdaten basierende Sicherheitsrichtlinien erstellt hat. Allein schon aufgrund ihrer Anzahl müssen IoT-Geräte in den Gesprächen für die Planung der Netzwerkinfrastruktur für den digitalen Arbeitsplatz eine zentrale Rolle spielen. Das Netzwerk muss intelligent genug sein, um das Verhalten der IoT-Geräte automatisch zu verstehen und zu klassifizieren.

MOBILGERÄTE UND IoT BRINGEN HERAUSFORDERUNGEN MIT SICH

Wissen Sie wirklich, was sich auf Ihrem Netzwerk befindet?

Sicherheit beginnt damit, zu verstehen, was sich auf dem Netzwerk befindet, zum Beispiel nicht verwaltete Smartphones, fehlerhafte Endpunkte und IoT-Geräte, mit denen Benutzer eine Verbindung herstellen können, ohne Rücksprache mit der IT zu halten. All dies bringt neue Bedrohungen mit sich und vergrößert die Angriffsfläche für das Unternehmen. Ein besseres Verständnis dessen, was sich auf dem Netzwerk befindet, durch differenzierte Profilerstellung bietet der IT

die Möglichkeit, jedes Gerät, das eine Verbindung mit dem Netzwerk herstellt, zu identifizieren, unabhängig vom Typ, Besitzer oder von woher die Verbindung hergestellt wird. Dieser Aspekt wird immer wichtiger, wenn unbekannte drahtlose und kabelgebundene IoT-Geräte das Netzwerk überfluten. Die ständige Profilerstellung trägt zur genauen Durchsetzung von Richtlinien auf der Basis des Kategorietyps und der Attribute eines Geräts bei, um automatisch Zugriffsrechte auf interne und externe Ressourcen zu gewähren oder zu verweigern.

DIE 6 SCHRITTE VON ARUBA FÜR DEN DIGITALEN ARBEITSPLATZ

1. Profile für alle drahtlosen und kabelgebundenen Geräte identifizieren und erstellen
2. Mobile und IoT-Geräte mit drahtlosen und kabelgebundenen Netzwerkinfrastrukturlösungen verbinden
3. das Netzwerk mit intelligenten Richtlinien schützen;
4. Das Netzwerk verwalten – lokal oder in der Cloud
5. Erfahrungen mit Standort und Kontext personalisieren
6. Innovation beschleunigen, um die Benutzererfahrung und Sicherheit zu verbessern

Steigerung der Gerätedichte

Die wachsende Anzahl an mobilen und IoT-Geräten belastet alternde Infrastrukturen, die nicht vor dem Hintergrund von Mobilität und IoT konzipiert wurden. Es ist jedoch nicht nur die Anzahl der Geräte, die zu Engpässen und Überlastung führt. Denken Sie nur an das Benutzerverhalten und neue Anforderungen an den Datenverkehr. Mitarbeiter und Gäste

nutzen mehr Videos als je zuvor. Dieses Verhalten stellt noch nie dagewesene Anforderungen an das Netzwerk, das die Infrastruktur benötigt, um Funktionen zur Bandbreitenpriorisierung zu unterstützen, die voneinander unabhängige Datenverkehrstypen erkennen.

Um bei der Lösung des Problems zu helfen, benötigen Unternehmen Verwaltungstools, die erkennen, welche Anwendungen genutzt werden und die ganz einfach Nutzungsrichtlinien erstellen, um Sprach- und Videoanrufe gegenüber Daten für spezifische Anwendungen und Benutzer zu priorisieren. Es wird zunehmend von Bedeutung sein, anschließend die Leistung des Netzwerks auf fortlaufender Basis zu überwachen.

Kabelgebunden ebenso wichtig wie drahtlos

Bei Unternehmen in gewerblichen und industriellen Betrieben kann die Anzahl der erwarteten kabelgebundenen IoT-Geräte je nach Industriezweig zwischen 35 % und über 50 % betragen – etwa durch Bewegungsmelder, medizinische Ausrüstung oder Prozessregler in der Fabrikhalle, um nur einige Beispiele zu nennen. Bisher stand bei der Diskussion um Netzwerkzugangskontrollen vor allem die Frage im Mittelpunkt, wie drahtlose Netzwerke gesichert werden können, da auf diesem Wege die meisten Geräte eine Verbindung mit dem Netzwerk herstellen.

Die starke Fokussierung auf die Sicherung von drahtlosen Netzwerken führte dazu, dass kabelgebundene Netzwerke ungeschützt blieben, da sich die Switches hinter verschlossenen Türen befanden. Die vorherrschende Wahrnehmung war, dass kabelgebundene Netzwerke nicht dieselben Sicherheitslücken aufweisen wie Drahtlosnetzwerke. Mit der Zunahme von kabelgebundenen Netzwerken geriet die einheitliche Überwachung vieler Switches ins Wanken und führte dazu, dass viele Anschlüsse weit offen und für jeden zugänglich wurden. Konferenzräume und Druckerbereiche sind klassische Beispiele für Orte, an denen eher nach Zufallsprinzip für Sicherheit gesorgt wurde. Angesichts der zahlreichen IoT-Geräte, die eine kabelgebundene Verbindung herstellen, ist es an der Zeit, der Sicherung von kabelgebundenen Infrastrukturen das gleiche Maß an Aufmerksamkeit zu schenken.

Traditionelle kabelgebundene, nicht für das IoT optimierte Infrastruktur

Veraltete Switching-Umgebungen wurden bereits vor der Verbreitung von Mobilität und IoT entwickelt. Die Ressourcen befanden sich hinter der Firewall und die IT musste lediglich sicherstellen, dass die Perimeter Bedrohungen von außen fernhielten. Und jetzt betreten wir das IoT – die Switches von heute müssen sicherstellen, dass sich Konnektivität, Sicherheit und intelligente Netzwerkverwaltung gegenseitig ergänzen, sodass sich alle diese Geräte mit dem Netzwerk verbinden können, dabei jedoch nach ihren Zugriffs- und Datenverkehrsanforderungen segmentiert werden.

Es ist teuer, Innovationen voranzubringen und den Vorsprung vor den Hackern zu wahren

Wenn Unternehmen in Technologie und Netzwerksicherheit investieren, ist es nahezu unmöglich, den Vorsprung vor den Hackern zu wahren, wenn man dies alleine versucht. Partnerschaften sind für den Erfolg von großer Bedeutung und die IT braucht Lösungen, die über Architekturen verschiedener Hersteller hinweg funktionieren und gleichzeitig offen für Entwickler sind, um Innovationen zu fördern, die einfach zu realisieren und zu konsumieren sind.

ENTWURF VON ARUBA FÜR MOBILITÄT IM UNTERNEHMEN UND IoT

Die Lösungen von Aruba sind darauf ausgelegt, neue digitale Erlebnisse, die das volle Potenzial der Mobilität und des IoT für Unternehmen, Kunden und Mitarbeiter nutzen, zu ermöglichen und in diese zu investieren.

1. Profile für alle drahtlosen und kabelgebundenen Geräte identifizieren und erstellen

Mobile und IoT-Geräte können die Produktivität am Arbeitsplatz verbessern und Entscheidungen automatisieren, die als Katalysator für neue Produkte und Dienstleistungen fungieren, jedoch nur, wenn Einblicke von Daten stammen, die über sichere Verbindungen und vertrauenswürdige Geräte gesammelt wurden. Aruba ClearPass ermöglicht es der IT, Endpunkttypen und Attribute von IoT-Geräten und traditionellen intelligenten Geräten in Netzwerken mit kabelgebundenem und drahtlosem Zugriff verschiedener Hersteller automatisch zu identifizieren. Damit werden Probleme durch Konnektivität, Leistung und die Möglichkeit zur genauen Festlegung und Durchsetzung von differenzierten Richtlinien gelöst.

2. Mobile und IoT-Geräte mit drahtlosen und kabelgebundenen Netzwerkinfrastrukturlösungen verbinden

Die Anforderungen durch Gerätedichte, wichtige mobile Anwendungen und der Wechsel zu intelligenten Gebäuden bedeuten, dass Unternehmen von heute intelligentere kabelgebundene und drahtlose Infrastrukturen benötigen. Hochgradig mobile Mitarbeiter, die Zunahme der IoT-Geräte und die steigende Auslastung der WLAN-Bandbreite bedeuten, dass auch die kabelgebundene Infrastruktur für Belastbarkeit, Sicherheit und Skalierung optimiert werden muss.

Die drahtlosen 802.11ac APs von Aruba bieten schnellste Gigabit-Datengeschwindigkeiten für eine ausgezeichnete Leistung in Umgebungen mit hoher Gerätedichte und die Intelligenz, nahtloses Roaming und App-Priorisierung zu bieten. Das bedeutet, dass wichtiger Datenverkehr im Unternehmen priorisiert wird und die Nutzer in den Genuss eines nahtlosen Erlebnisses ohne unterbrochene Gespräche kommen.

Die Switches von Aruba bieten ein integriertes Fundament für drahtlose und kabelgebundene Geräte mit Skalierbarkeit, Sicherheit und hoher Leistungsfähigkeit für Campus-Netzwerke.

Die programmierbare ProVision ASICs- und ArubaOS-Switch-Software bieten schnelle drahtlose Aggregation und einfachen rollenbasierten Zugriff auf drahtlose und kabelgebundene Netzwerke durch die Möglichkeit der Identifizierung und Zuweisung von Rollen an Benutzer und IoT-Geräte, um wichtige Unternehmensanwendungen zu priorisieren und gleichzeitig das Netzwerk zu schützen. Die Layer 3-Switches von Aruba können auch benutzer- und portbasiertes Tunneling für Datenverkehr für Mobility Controller nutzen, sodass Richtlinien angewendet, erweiterte Dienste auf Benutzer und IoT-Geräte ausgeweitet und der Datenverkehr verschlüsselt werden können, um das Netzwerk zu schützen.

In dezentralen Unternehmen unterstützen die Aruba Switches Zero Touch Provisioning und optionale cloudgestützte Verwaltungsfunktionen, die es Unternehmen ermöglichen, die Netzwerkbereitstellung zu vereinfachen und Verwaltungskosten zu senken.

3. das Netzwerk mit intelligenten Richtlinien schützen;

Sobald Sie sich einen Überblick über alle Geräte verschafft haben, geht es um die automatische Durchsetzung von Richtlinien. Aruba ClearPass zeigt Ihnen detailliert, was sich in Ihrem Netzwerk befindet und setzt dann rollenbasierte Richtlinien und automatisierte Arbeitsabläufe in kabelgebundenen und drahtlosen Infrastrukturen verschiedener Hersteller durch. ClearPass enthält außerdem Funktionen, die vorhandene Nicht-AAA-Switch-Protokolle nutzen, um Sie beim Sperren kabelgebundener Anschlüsse an anfälligen Stellen wie in Konferenzräumen, an IP-Telefonen und in Druckerbereichen zu unterstützen.

4. Das Netzwerk verwalten – lokal oder in der Cloud

Die Netzwerke von heute müssen mehr als nur Konnektivität liefern – mithilfe hoch entwickelter Analysen müssen sie Einblicke in Netzwerkleistung, Benutzerverhalten und Nutzung von Anwendungen bieten, die es der IT ermöglichen, Probleme vorherzusehen, bevor diese auftreten. Und in dezentralen Umgebungen möchten Unternehmen intelligente Lösungen für Cloud-Netzwerke auswählen können, die ihrem Budget oder ihren IT-Ressourcenzielen entsprechen und eine gleichmäßige Netzwerkverwaltung und Transparenz gewährleisten, die ihnen auch lokale Lösungen bieten.
Die Netzwerkverwaltungslösungen von Aruba bieten die Tools und prädiktiven Analysen, die erforderlich sind, um ein hohes Maß an Benutzervertrauen aufrechtzuerhalten – sowohl lokal mit Aruba AirWave oder in der Cloud mit Aruba Central.

5. Erfahrungen mit Standort und Kontext personalisieren

Mit den Lösungen für Ortungsdienste von Aruba können Unternehmen die BLE-Technologie (Bluetooth Low-Energy) für Standort- und Orientierungsfunktionen für den Innenbereich und umgebungsspezifische Push-Benachrichtigungen für Unternehmen, Stadien, Krankenhäuser und andere öffentliche Veranstaltungsorte einsetzen. Die Aruba Meridian-Software kombiniert mit Aruba Beacons und beliebigen drahtlosen Infrastrukturen verwandelt intelligente Geräte in interaktive Orientierungs- und Benachrichtigungsendpunkte. Heute können Mitarbeiter, Gäste oder Kunden ganz einfach und pünktlich zu nahe gelegenen öffentlichen Toiletten geleitet werden und sie können sich schnell über neue Produkte oder Sehenswürdigkeiten in Innenbereichen informieren. Mithilfe dieser personalisierten Erfahrungen können die Umsatzmöglichkeiten der Veranstaltungsorte gesteigert und die Kundenbindung gestärkt werden.

6. Innovation beschleunigen, um die Benutzererfahrung und Sicherheit zu verbessern

Wir bei Aruba arbeiten mit den besten Technologiepartnern und Anwendungsentwicklern der Branche zusammen, um Lösungen zu bieten, die einfach zu realisieren und zu konsumieren sind. Unsere gemeinsamen Anstrengungen liefern innovative Lösungen, die die Unternehmen und IT-Prioritäten von heute miteinander verbinden.
In Abhängigkeit von Ihrem Geschäftsmodell bieten unsere Partnerprogramme alles von sicherer Konnektivität bis hin zu standortbasierten Diensten und Mobile Engagement.

Wenn Sie mehr über die digitalen Arbeitsplatzlösungen von Aruba erfahren möchten, besuchen Sie www.arubanetworks.com/digitalworkplace.