## Netzwerkzugangssteuerung

# Kein Fischen im Trüben

**Mobiles Arbeiten, BYOD, IoT, sichere Gastzugänge – der Aufwand, Geräte sicher ins Unternehmensnetzwerk einzubinden, wird für IT-Abteilungen immer größer. Wer und was im eigenen Netz unterwegs ist, lässt sich kaum noch zuverlässig kontrollieren. Mit Aruba ClearPass ist eine herstellerunabhängige Netzwerkzugangssteuerung auf dem Markt, die mit automatisierter Geräte- und Benutzererkennung Licht ins Dunkel bringt. Individuelle Richtlinien sorgen dafür, dass sich alle und alles im Netz an die Regeln hält.**

„Was ist das? Loch an Loch und es hält doch – ein Netz. Dieses Kinderrätsel beschreibt erschreckend präzise das Netzwerk vieler Unternehmen. Ob und wie lange es Angriffen und Bedrohungen standhält, ist dabei meist fraglich. Bring your own device (BYOD), der Siegeszug der IoT-Geräte und die Anforderungen des mobilen Arbeitens machen die Netzwerkzugangskontrolle für IT-Verantwortliche zu

einer Sisyphus-Aufgabe. Den Überblick zu behalten, wer und was sich im Netz tummelt, ist kaum möglich. Jedoch ist dieses Wissen die Voraussetzung, um Sicherheitsrisiken zu erkennen und das Unternehmen vor ihnen zu schützen.

Aruba ClearPass löst die drei dringendsten Probleme, die IT-Verantwortliche im Hinblick auf ihr Netzwerk haben: Transparenz, Zugangssteuerung und Schutz vor Cyberangriffen. Im Gegensatz zu anderen Lösungen identifiziert Aruba ClearPass in Echtzeit und ohne den Einsatz von Agents Endpunkte und Netzwerkgeräte in kabelgebundenen und kabellosen Netzwerken. ClearPass ist dabei nicht an die Netzwerkkomponenten eines bestimmten Herstellers gebunden, sondern funktioniert in jedem Netzwerk. Es lässt sich außerdem in über 120 Sicherheits- und allgemeine IT-Lösungen integrieren – z. B. um in Kombination mit Firewalls, SIEM oder Sandboxen auf Cyberangriffe zu reagieren.

## Sicherheit und Compliance: Transparenz ist die Voraussetzung

Nur wer weiß, wer und was in seinem Netz unterwegs ist, kann mögliche Risiken erkennen. BYOD, eine Flut von IoT-Geräten und die Forderung von Anwendern, möglichst von überall Zugang zum Netz zu haben, machen es Netzwerkadministratoren schwer, den Überblick zu behalten. Hinzu kommen die Bereitstellung von Gastzugriffen und die Kontrolle von nicht autorisierten kabelgebundenen und kabellosen Endpunkten. Bisherige Verfahren zur Identifizierung der verbundenen Endpunkte erweisen sich in der Praxis oft als wenig hilfreich, da sie mit Agents arbeiten und regelmäßige Updates der Endpunktdatenbanken erfordern. Letztlich bleibt es bei vielen IT-Abteilungen Handarbeit, den Netzwerkzugang freizugeben und zu kontrollieren.

Mit Aruba ClearPass behalten Administratoren jetzt die Übersicht in ihren Netzwerken. Da ClearPass nicht mit Agents arbeitet, erkennt es auch BYOD-Smartphones und IoT-Geräte. Endpunkte in kabelgebunden und kabellosen Netzwerken werden automatisch identifiziert und kategorisiert. Dies geschieht anhand von Attributen wie Gerätekategorie, Hersteller, Betriebssystem, IP-Adresse, Hostname, Besitzer und anderen. Neue und unbekannte Geräte lassen sich so unmittelbar klassifizieren und der entsprechenden Zugriffsrichtlinie unterwerfen.

## Zugangssteuerung: Wer darf was im Netz?

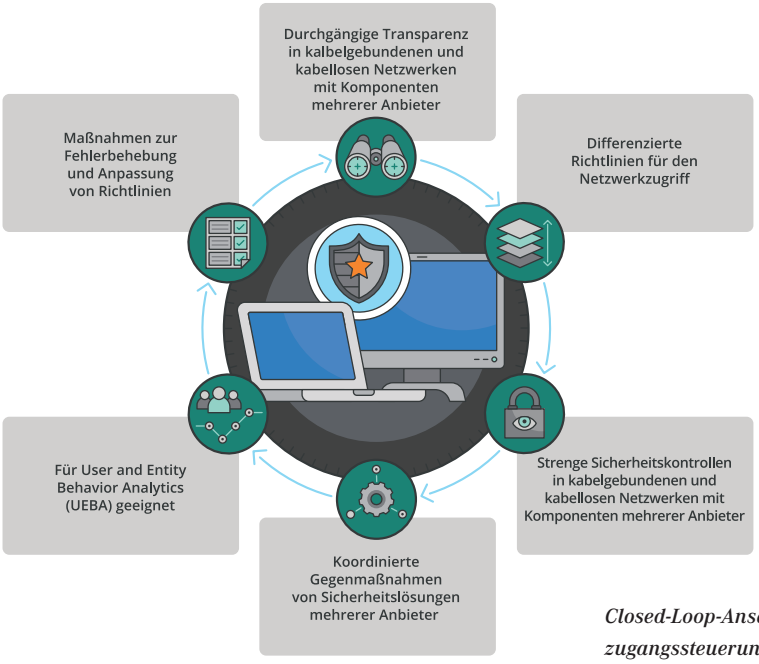
Vom IT-Mitarbeiter bis zum Besucher, vom Server bis zum Drucker: Viele Personen und Geräte brauchen Zugang zum Netzwerk, aber nicht jeder und jedes sollte gleich Zugriff auf alle Ressourcen haben. Über Richtlinien, die unter anderem Faktoren wie Gerät, Tageszeit und Benutzertyp berücksichtigen, vergibt ClearPass Zugriffsrechte, die jedem Benutzer, jedem System und jedem Gerät nur den Zugriff erlauben, der für die jeweilige Rolle notwendig ist. Diese richtlinienbasierte Segmentierung ermöglicht es, Besuchern ein Netzwerk zur Verfügung zu stellen, das vom eigenen Firmennetzwerk getrennt bleibt. Ergänzt durch ein Selbstregistrierungsportal bleibt der IT-Abteilung obendrein viel administrativer Aufwand erspart.

Unabhängig von der jeweiligen Rolle und dem jeweiligen Segment, erlaubt ClearPass im Gegensatz zu einigen anderen Lösungen grundsätzlich nur solchen Geräten und Benutzern den Zugang mit positiver Authentifizierung und der entsprechenden richtlinienbasierten Berechtigung.

## „Farblose Ports“: Das Endgerät bestimmt die Zugriffsrechte

Die sichere Konfiguration von Ports bereitet IT-Abteilungen oftmals Kopfzerbrechen. Besonders in öffentlich zugänglichen Bereichen stellen sie ein Sicherheitsrisiko dar. Die generelle Einschränkung der Zugriffsrechte oder die Konfiguration für bestimmte Anwendungsfälle wie z. B. Drucker macht die Nutzung der Ports unflexibel. Eine Änderung der Nutzung ist immer mit zusätzlichem Aufwand verbunden.

ClearPass ermöglicht die Strategie der „farblosen Ports“. Da ClearPass jedes Gerät erkennt und hinsichtlich seiner Zugriffsrechte prüft, bevor es ins




*Closed-Loop-Ansatz für Netzwerkzugangssteuerung und Reaktion.*

Netz aufgenommen wird, kann jeder Port mit jedem Gerät verbunden werden, ohne die Portnutzung generell einschränken zu müssen. IT-Verantwortliche sparen somit viel Zeit bei der Einrichtung und Konfiguration von Switchen und können gleichzeitig die Portnutzung optimieren.

## Offene und nahtlose Integration: ClearPass in Kombination mit Firewall und Co.

ClearPass bietet einen Closed-Loop-Ansatz zum Schutz von Netzwerken. Das heißt, ein geschlossener Regelkreis sorgt dafür, dass die Sicherheit stets gewährleistet ist, obwohl ständig neue und unbekannte Elemente Teil des Netzwerks werden oder es Cyberattacken ausgesetzt sein könnte.

Den ersten Schritt dazu bildet die umfassende Transparenz, die ClearPass in jedem Netzwerk ermöglicht – unabhängig vom Hersteller der Netzwerkkomponenten oder der Geräte, die auf dieses Netzwerk zugreifen. Differenzierte Richtlinien für den Netzwerkzugriff, die beliebig auf Gerätemerkmale und Rollen der Nutzer angepasst werden können, bilden die Basis für eine sichere Zugangssteuerung in kabelgebundenen und kabellosen Netzwerken. Wird ClearPass in Kombination mit Firewalls, SIEM, Sandboxen und Ähnlichem eingesetzt, können auch Richtlinien als Reaktion auf Cyberangriffe definiert werden. Sobald die Sicherheitslösungen Hinweise auf einen solchen Vorfall melden, löst ClearPass festgelegte Aktionen aus, wie z. B. erneute Authentifizierung, Bandbreitenbegrenzung, Quarantäne oder Blockierung. ClearPass ermöglicht die Erfassung und Analyse des Verhaltens von Nutzern und Geräten im Netz. Diese Daten bilden die Grundlage zur kontinuierlichen Anpassung der Richtlinien und zur Optimierung des Netzwerks.

ClearPass kann noch mehr! Lassen Sie sich beraten, wie ClearPass Ihr Netzwerk sicherer macht, Ihnen hilft, Compliance-Anforderungen zu erfüllen, und dabei Ihre IT-Abteilung entlastet.

aruba
a Hewlett Packard Enterprise company
Solution Provider
SILVER PARTNER

**Ihr Ansprechpartner**

Kai Lauterbach
IT Consulting & Services
Fachbereichsleiter
Netzwerk & Security
T +49 228 9080-675
kai.lauterbach@hug.de