Network Access Control

Erhalten Sie Sichtbarkeit in Echtzeit und Kontrolle über Geräte, sobald sich diese mit Ihrem Netzwerk verbinden.

Herausforderungen für Unternehmen

- Verbesserung der allgemeinen Netzwerksicherheit
- Schutz sensibler Daten vor externen Bedrohungen
- Keine Einschränkung des Zugriffs von Mitarbeitern, Auftragsnehmern und Kunden
- Einhaltung interner Richtlinien sowie externer Regularien
- Ausnutzung vorhandener Sicherheitsinvestitionen

Technische Herausforderungen

- Erkennung von unbekannten Geräte im Netzwerk, die nicht mit Agenten ausgestattet sind
- Identifizierung des Gerätetyp und Gerätestandorts, der Benutzeridentität und -rolle sowie des Compliance-Niveaus
- Hindern von infizierten oder nicht regelkonformen Geräte, Malware zu verbreiten
- Verhindern, dass bei zielgerichteten Angriffen Daten gestohlen oder Netzwerkausfälle verursacht werden
- Finden einer NAC-Lösung, die in jeder Situation die richtigen Maßnahmen ohne menschliches Zutun automatisch ergreift
- Messung der Effizienz von Sicherheitskontrollen und Nachweisen der Einhaltung von gesetzlichen Vorgaben

ForeScout Technologies, Inc. bietet einzigartige Lösungen zum Management und Verwaltung der dramatisch ansteigenden Anzahl und Arten von Geräten, die sich täglich mit Ihrem Netzwerk verbinden. Unser Vorzeigeprodukt, ForeScout CounterACT®, bietet Ihnen Sichtbarkeit in Echtzeit. So können Sie autorisierte *und* nicht autorisierte Geräte umgehend erkennen – und den Zugriff dieser Geräte kontrollieren, sofern Sie diese in Ihr Netzwerk lassen möchten.

Die Herausforderung

Die Unternehmensnetzwerke von heute beherbergen ein breites Spektrum von herkömmlichen und unkonventionellen Geräten und anderen Endpunkten – alles von PCs, Tablets und Smartphones hin zu Industriesteuerungen, virtualisierten Servern, Wireless Access Points und cloudbasierten Anwendungen. Ohne jeden Zweifel werden die Herausforderungen zudem in Bezug auf Geräte immer größer, da BYOD*-, IoT*- und hybride IT-Umgebungen immer häufiger und Hacker immer raffinierter werden. Daher muss Ihre NAC-Lösung in der Lage sein, Ihnen bekannte Geräte Ihres Unternehmens und Ihrer Mitarbeiter sowie die steigende Zahl nicht autorisierter Geräte, die Sie nicht kennen, zu verwalten.

Im Folgenden finden Sie eine Reihe von Fakten, die unterstreichen, weshalb Sie eine umfassende, hochintelligente NAC-Sicherheitslösung benötigen:

- 2020 werden 26 Milliarden verbundene und vernetzte Geräte genutzt.[1]
- 75 Prozent der mobilen Anwendungen werden durch bekannte Sicherheitstests durchfallen.[2]
- 2014 gingen bereits 98,7 Prozent aller verzeichneter Gefährdungen auf das Konto externer Hacker.[3]

IT- Manager und Sicherheitsverantwortliche müssen die Geräte und Systeme in ihrem Netzwerk erkennen, sobald diese auf das Netz zugreifen. Sonst sind sind sie nicht in der Lage entsprechende Sicherheitsstandards umzusetzen.

Die Lösung von ForeScout

ForeScout CounterACT® bietet umfassende NAC-Funktionen und Sichtbarkeit in Echtzeit von Geräten, sobald diese sich mit dem Netzwerk verbinden. Es scannt kontinuierlich das Netzwerk und überwacht die Aktivitäten von bekannten, unternehmenseigenen Geräten sowie von unbekannten Geräten, wie privaten und bösartigen Endpunkten. Zudem bietet es Ihnen die Möglichkeit, richtlinienbasierte Netzwerkzugangskontrollen, Endpunkt-Compliance und Mobilgerätesicherheit zu automatisieren und durchzusetzen. ForeScout CounterACT bietet ein breites Spektrum an automatisierten Aktionsmöglichkeiten, die keine negativen Auswirkungen für die Benutzer haben und dafür sorgen, dass Geschäftsabläufe in einem maximalen Maß durchgeführt werden können.

Die Vorteile und Funktionalitäten von CounterACT können in drei Worten zusammengefasst werden:

See CounterACT bietet die einzigartige Möglichkeit, Geräte zu erkennen, sobald sich diese mit Ihrem Netzwerk verbinden, ohne dass dabei Agenten oder eine vorherige Gerätekenntnis erforderlich sind. Es klassifiziert Geräte, Benutzer, Anwendungen und Betriebssysteme und erstellt Profile zu diesen. Gleichzeitig überwacht es kontinuierlich verwaltete Geräte, private Geräte und andere Endpunkte.

Control CounterACT kann den Netzwerkzugang basierend auf Gerätestatus und Sicherheitsrichtlinien zulassen, verweigern oder einschränken. Durch die Bewertung und Korrektur von schädlichen oder risikoreichen Endpunkten verringert es die Bedrohung durch Richtlinienverletzungen und Malware-Angriffe, die sonst Ihr Unternehmen gefährden würden. Zudem optimiert CounterACT durch das kontinuierliche Monitoring der Geräte in Ihrem Netzwerk und durch die Kontrolle dieser Geräte in Übereinstimmung mit Ihren Sicherheitsrichtlinien Ihre Fähigkeit, die Einhaltung von Branchenstandards und gesetzlichen Vorgaben nachzuweisen.

Orchestrate CounterACT kann dank der ForeScout ControlFabric®-Architektur in mehr als 70 Netzwerk-, Sicherheits-, Mobilitäts- und IT-Management-Produkte** integriert werden. Diese Fähigkeit, Echtzeit-Sicherheitsdaten systemübergreifend zu teilen und einheitliche Sicherheitsrichtlinien durchzusetzen, verringert die Schwachstellen, indem systemübergreifende Reaktionen auf Bedrohungen automatisiert werden. Darüber hinaus können Sie mehr Rendite mit Ihren Investitionen in vorhandene Sicherheitstools erzielen und sparen zugleich Zeit durch die Automatisierung von Arbeitsabläufen.

ForeScout CounterACT verarbeitet eine Vielzahl kontextbezogener Information über den jeweiligen Endpunkt, seinen Standort sowie darüber, wem er gehört und was sich darauf befindet. CounterACT stellt Folgendes sicher:

- Nicht autorisierte Geräte und nicht genehmigte Anwendungen befinden sich nicht in Ihrem Netzwerk.
- Autorisierte Geräte werden mit den neuesten Betriebssystemen konfiguriert, die aktuellste Antiviren-Software wird installiert und läuft und Schwachstellen werden ordnungsgemäß gepatcht.
- Agenten zur Verschlüsselung und zur Verhinderung von Datenverlusten funktionieren ordnungsgemäß.
- Benutzer werden daran gehindert, nicht autorisierte Anwendungen oder dezentrale Geräte im Netzwerk zu betreiben.

Wenn Endpunkte nicht konform mit den Richtlinien Ihres Unternehmens sind, führt CounterACT automatisch ein oder mehrere richtlinienbasierte Durchsetzungs- und Korrekturmaßnahmen durch, von E-Mail-Benachrichtigungen bei mangelnder Compliance über verpflichtende Fehlerbehebung (durch Software-Updates) bis hin zu einer vollständigen Quarantäne und Verhinderung des Zugangs. Beim Verwalten des Zugriffs durch Gäste, der Ortung von Systemen und dem Öffnen oder Schließen von Netzwerkports ist keinerlei menschliches bzw. manuelles Eingreifen erforderlich. Der Netzwerkzugang wird gemäß der geltenden Richtlinie kontrolliert.

Für mehr als 2.000 Unternehmen in mehr als 60 Ländern** bietet ForeScout eine intelligente und kosteneffiziente Netzwerkzugangskontrolle, die den höchsten Standards in Bezug auf Sicherheit und gesetzliche Voraussetzungen gerecht wird und die zudem leicht zu handhaben und zu implementieren ist. CounterACT ist sowohl als virtuelle als auch als physikalische Appliance erhältlich, die in Ihre vorhandene Infrastruktur integriert werden kann. Dabei sind in der Regel keinerlei Änderungen Ihrer Netzwerkkonfiguration erforderlich. Die CounterACT-Appliance wird physikalisch im Handumdrehen installiert, wodurch Latenzzeiten und Probleme in Bezug auf potenzielle Netzwerkausfälle vermieden werden. Zudem kann sie zentral verwaltet werden, um so unzählige Endpunkte von einer Konsole aus zu verwalten.

Weitere Informationen finden Sie unter **www.ForeScout.com**

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, Campbell, CA 95008 USA

Gebührenfrei (USA) 1-866-377-8771
Tel. (intern) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

1 Gartner Research, http://www.gartner.com/newsroom/id/2636073
2 Gartner Research, Sept. 2014, http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/
3 Privacy Rights Clearinghouse Research, http://www.securityweek.com/data-breaches-numbers

*Bring Your Own Device (BYOD), Internet der Dinge (IoT)
**Stand: Januar 2016