FORESCOUT

Gerätetransparenz: Der Schlüssel zu weniger Risiko und besserer Sicherheit

Sechs Wege zur Verbesserung der Sicherheit mit vollständiger Gerätetransparenz

Die Absicherung der Netzwerkinfrastruktur wird von Tag zu Tag komplexer, da die Zahl der IoT-Geräte und Vielfalt der Plattformen explosionsartig zunimmt, die Cloud immer intensiver eingesetzt wird und IT und OT zusammenwachsen. Die große Mehrzahl der neuen Geräte, die in Ihr Netzwerk eingebunden werden, ist nicht für die Unterstützung von Verwaltungsagenten ausgelegt. Das führt zu einer gefährlichen Transparenz- und Risikolücke. Und diese Lücke öffnet sich noch weiter, wenn sich Cloud Computing auch in die hintersten Ecken des verteilten Netzwerks ausbreitet.

Zudem sind verborgene Bedrohungen ebenso gefährlich wie sichtbare. Daher müssen Sie alle Geräte in Ihrem Netzwerk erkennen können – unabhängig davon, ob auf ihnen Agenten installiert sind, ob es sich um physische oder virtuelle Geräte handelt und wo sie sich befinden. Außerdem benötigen Sie kontinuierliche Echtzeit-Überwachung sowie die Möglichkeit, sofort nach dem Herstellen der Netzwerkverbindung ein Profil zu erstellen und das jeweilige Gerät zu klassifizieren.

Die Schließung dieser Transparenzlücke ist die effektivste Möglichkeit, die Netzwerksicherheit und die Maßnahmen zur Risikominderung deutlich zu verbessern. Diese sechs Wege erreichen dieses Ziel mit vollständiger Transparenz:

1 Verschaffen Sie sich agentenlose Transparenz zu allen Systemen – einschließlich BYOD-, IoT- und OT-Geräte

Sie können nur schützen, was Sie sehen.Die logische Schlussfolgerung: Eine zuverlässige Lösung muss einen genauen Echtzeit-Überblick über alle Endgeräte in Ihrem Netzwerk liefern.

Herkömmliche Sicherheitslösungen für Netzwerkzugriffssteuerung (Network Access Control, NAC) erkennen nur Geräte, auf denen ein Agent installiert ist. Sie können jedoch nicht alle BYOD- oder neuartigen Geräte, die sich mit Ihrem Netzwerk verbinden, mit einem Agenten ausstatten. Die Bandbreite dieser Geräte reicht von mitarbeitereigenen Smartphones, Tablets und Wearables über IoT- und OT-Geräte und Laptops von Auftragnehmern bis zu nicht autorisierten Geräten aus unbekannter Quelle. Und alle diese Geräte bringen Risiken mit sich.

Daher benötigen Sie agentenlose Transparenz, sobald sich ein neues Gerät mit Ihrem Netzwerk verbindet.Dabei geht es nicht nur um die einfache Erkennung der jeweiligen IP- oder MAC-Adresse, sondern um detaillierte Informationen zu jedem Gerät, einschließlich Zweck, Eigentümer und Sicherheitsstatus.

2 Führen Sie Transparenz und Kontrolle über alle Rechenzentren, Standorte und Cloud-Umgebungen zusammen

Vor nicht allzu langer Zeit mussten Sie lediglich Ihr Rechenzentrum schützen. Sie wissen aber nur zu gut, dass die Welt deutlich komplexer geworden ist. In vielen Fällen sind aus einzelnen Rechenzentren mehrere geworden, die an mehreren Standorten und mitunter auf der ganzen Welt verteilt sind. Ein weiterer Faktor ist die Cloud.

Sie müssen nicht nur den Perimeter kontrollieren, worin auch immer dieser heute bestehen mag. Vielmehr benötigen Sie sofortigen Echtzeit-Zugriff auf alle Endgeräte im Rechenzentrum, an ihren Standorten und in der Cloud. Es ist nicht mehr möglich, Geräte und Workloads mit separaten spezialisierten Tools und Schnittstellen zu verwalten und abzusichern. **Eine zuverlässige Lösung muss einen konsolidierten Überblick über alle herkömmlichen Systeme, mobilen und IoT-Geräte sowie virtuellen Maschinen und Cloud-Instanzen liefern – ganz gleich, wo diese sich befinden.** Zudem muss sich diese Lösung in erheblichem Maße skalieren lassen, um Ihren wachsenden Netzwerkanforderungen gerecht zu werden.

Dieser neue, von Technologie und Standort unabhängige Ansatz erfordert eine neue Denkweise mit Bezug auf die Interoperabilität von Lösungen (und weniger Bindung an einen individuellen Anbieter). Der Wert einer Technologie wird heute gesteigert, wenn Systeme auf gemeinsamen Dashboards und mit gemeinsamen Kontrollmechanismen zentrale Transparenz bieten. Für diesen neuen Ansatz ist Flexibilität nötig, damit Sie sowohl zentrale als auch verteilte Architektur entsprechend an Ihren sich ändernden Geschäftsanforderungen anpassen können.

3 Halten Sie die Vorgaben für Geräte- und Richtlinien-Compliance ein

„Kläglich gescheitert“ lautet heute das typische Urteil nach Penetrationstests oder Richtlinienn-Compliance-Audits. Die Ursache sind unerkannte IoT-Geräte oder andere Bedrohungen, die falsch segmentiert wurden. Erfolgreiche Sicherheitsstrategien beginnen mit kontinuierlicher Gerätetransparenz und vollständigen Geräte-Inventaren. Andernfalls gehen Sie ein großes Risiko ein – rechtlich ebenso wie finanziell.

Ungenaue ITAM-Daten können zu Verstößen gegen Vorschriften wie DSGVO, oder PCI und damit zu erheblichen Geldstrafen für Ihr Unternehmen führen.

Ganz gleich, ob Sie finanzbezogene, medizinische, industrielle oder „sonstige“ Assets schützen sollen, besteht der erste Schritt zu erfolgreicher Risikominderung und Compliance darin, vollständige Transparenz herzustellen. Sie müssen *Geräte sehen und klassifizieren und anschließend automatisiert kontrollieren sowie den Netzwerkzugriff beschränken können* – basierend auf Autorisierungsstufen, Unternehmenssicherheitsrichtlinien und gesetzlichen Vorgaben.

In Anbetracht zahlreicher staatlicher oder internationaler Vorschriften, die die Bekanntgabe von Sicherheitsverletzungen innerhalb von Stunden nach dem Ereignis fordern, müssen Sicherheitsplattformen zusammenarbeiten, um schnell und effektiv reagieren und Probleme beseitigen zu können.

4 Automatisieren Sie die Pflege und Verwaltung des Geräte-Inventars

Für die effektive Verwaltung und Absicherung Ihrer Unternehmensressourcen benötigen Sie ein genaues Inventar, das alle Geräte in Ihrem Netzwerk abdeckt Bedenken Sie: Für einen erfolgreichen Angriff benötigen Hacker nur ein einziges Gerät, das nicht in Ihrem Inventar erfasst ist oder mit veralteten oder fehlerhaften Konfigurationsdetails geführt wird. Die Geräteerkennung mit herkömmlichen Ansätzen kann mit großem Aufwand und Problemen verbunden sein. Laut Gartner werden „ohne aktive Erkennungsfunktionen bis zum Jahr 2020 etwa 30 Prozent aller Assets im Unternehmen unerkannt bleiben“.

Die manuelle Erkennung kann zu einer unvollständigen und ungenauen Verwaltungsdatenbank für Konfigurationsdaten (CMDB) führen und Ihre Sicherheitsverwaltungsmaßnahmen ad absurdum führen. Die Pflege des Inventars per Excel-Tabelle und anderen manuellen Methoden ist fehleranfällig, zudem sind die Inventardaten schnell veraltet. Zur Beschleunigung der Reaktion benötigen die Helpdesk-Teams jedoch ein aktuelles Geräte-Inventar.Außerdem ist der *sofortige Zugriff auf genaue Gerätedetails dann wichtig, wenn Sicherheitsprozessteams auf gezielte Angriffe reagieren müssen, die auf bestimmte Endgeräte-Betriebssysteme oder IoT-Gerätetypen abzielen.*

Ohne genaue Nachverfolgung der Softwarenutzung riskieren Sie zudem Übernutzung und Nichteinhaltung von Lizenzvereinbarungen und damit empfindliche Strafen.

Durch die Automatisierung des Inventars und der Verwaltung können Sie Kontextdaten an ITAM-Tools (z. B. ServiceNow®) weitergeben und so eine aktuelle Echtzeit-CMDB gewährleisten. Ihr aktuelles Inventar ermöglicht außerdem die effiziente Verwaltung des Gerätelebenszyklus und vereinfacht die Ressourcen-Investitionsplanung.

5 Berücksichtigen Sie bei der Netzwerksegmentierung den Kontext

Netzwerkverantwortliche und Sicherheitsexperten sind sich im Allgemeinen darin einig, dass Netzwerksegmentierung bei der Absicherung Ihres Netzwerks höchste Priorität erhalten sollte. Durch die Bewertung und Segmentierung Ihrer Geräte können Sie die richtlinienbasierte Zuweisung und Durchsetzung von Zugriffssteuerungslisten (ACLs) und VLANs automatisieren und Geräte dynamisch Segmenten zuordnen. Damit setzen Sie Ihre Zugriffskontrollen effektiv durch und schränken den Zugang zu beschränkten Ressourcen ein. Diese Strategie verhindert effektiv, dass Mitarbeiter sich in Netzwerkbereichen bewegen, in denen sie nichts zu suchen haben. Zudem lassen sich auf diese Weise Malware-Ausbrüche eindämmen.

Zusätzlicher Echtzeit-Gerätekontext kann die Sicherheit bei der Zuweisung zu Segmenten aus verschiedenen Gründen deutlich verbessern. So kann eine Lösung mit einer entsprechenden Funktion die Compliance eines Geräts überprüfen, bevor es einem Segment zugewiesen wird. Außerdem kann sie kontinuierlich den Sicherheitsstatus sowie das Geräteverhalten überwachen und ein nicht autorisiertes oder nicht konformes Gerät bei Bedarf schnell einem entsprechenden Segment bzw. einem zugangsbeschränkten VLAN zuweisen (z. B. wenn ein Drucker auf die Datenbank der Personalabteilung oder eine Überwachungskamera auf etwas anderes als den digitalen Videorecorder zuzugreifen versucht). *Diese neue intelligente und dynamische Segmentierungsmethode vereinfacht zudem Netzwerkanpassungen und erlaubt größere Flexibilität bei der Architektur, da die Weitergabe von Kontextinformationen an Firewalls der nächsten Generation und die gemeinsame Koordinierung unterstützt werden.*

Hierfür benötigen Sie eine NAC-Lösung, die sich problemlos mit Switches, virtuellen privaten Netzwerken (VPNs), Cloud-basierten Verwaltungssystemen und Firewalls der nächsten Generation integriert.

6 Verringern Sie daie Anfälligkeitsfläche mit koordinierter Reaktion auf Vorfälle

Netzwerksicherheitsteams verwalten im Durchschnitt bis zu 15 Tools. Das bedeutet, dass Unternehmen bereits viel Geld – und Zeit – in die Lizenzierung, Schulung und Koordination dieser Tools investieren. Gleichzeitig senden die meisten Sicherheitstools zwar viele Benachrichtigungen, können aber keine Maßnahmen durchsetzen. Dadurch sind die Sicherheitsteams mit der riesigen Anzahl an Warnungen überfordert, die sie manuell bewerten und lösen müssen.

Zur Beschleunigung der Reaktion auf Vorfälle müssen Tools stark automatisiert auf Warnmeldungen und bekannte Situationen reagieren können. Zudem müssen sie Sicherheitsanalysten beim Aufkommen neuer Bedrohungen mit priorisierten Einblicken versorgen.

Um diese Tools optimal nutzen zu können, benötigen Sie bereits in der Standardkonfiguration Workflow-Interoperabilität sowie die Möglichkeit, automatisierte Erkennung und Klassifizierung durchzuführen. Die Lösung Ihrer Wahl sollte sich zudem per Plug-and-Play mit Ihren bestehenden Netzwerktools vernetzen, damit Echtzeit-Daten, Warnmeldungen und Reaktionen mit anderen ITAM- und Sicherheitstools koordiniert werden können.

Alle neuen Tools sollten außerdem Netzwerkressourcen mehrerer Anbieter unterstützen – physische und virtuelle sowie alle Ressourcen am Standort, im Rechenzentrum sowie in Ihren Cloud-Umgebungen.

Die Lösung von Forescout

Die Forescout-Plattform für Gerätetransparenz und -kontrolle unterstützt Sie unter anderem dabei, diese sechs Wege zu beschreiten. Sie erkennt kontinuierlich alle per IP-Adresse vernetzten Geräte, sobald sich diese mit Ihrem Netzwerk verbinden. Hierfür sind keine Agenten erforderlich. Die Plattform bietet dank einer Kombination aus aktiven und passiven Erkennungs-, Profilerstellungs- und Klassifizierungstechniken detaillierte Transparenz zu diesen Geräten. Außerdem profitieren Sie von branchenführender Skalierbarkeit: Jede Forescout eyeManage-Appliance unterstützt bis zu zwei Millionen Geräte.

Durch unseren einzigartigen agentenlosen Ansatz erhalten Sie einen umfassenden Überblick über die Geräte: verwaltete und nicht verwaltete, unternehmenseigene und private, drahtgebundene und drahtlose Geräte, sogar mitarbeitereigene BYOD-Systeme, Server, Switches, nicht autorisierte Hardware sowie IoT-Geräte.

Forescout setzt einen neuen Standard für Gerätetransparenz und -kontrolle, damit Sie in ***Ihrem*** gesamten erweiterten Unternehmensnetzwerk Risiken minimieren, die Angriffsfläche verringern und Vorfallreaktionen automatisieren können.

Erfahren Sie mehr über die Forescout-Plattform. Laden Sie unser ***Whitepaper Agentenlose Gerätetransparenz und -kontrolle: Unverzichtbare Funktionen für effektive Cybersicherheit*** herunter, um mehr über die Möglichkeiten der Forescout-Plattform zu erfahren.

Glossar

ACL: Access Control List (Zugriffssteuerungsliste)

BYOD: bring your own device (Bring dein eigenes Gerät)

CMDB: configuration management database (Verwaltungsdatenbank für das Konfigurationsmanagement)

DSGVO: EU-Datenschutz Grundverordnung

IoT: Internet of Things (Internet der Dinge)

IP: Internet Protocol (Internet-Protokoll)

ITAM: information technology asset management (IT-Asset-Management)

MAC: Media Access Control (Medienzugriffskontrolle)

NAC: network access control (Netwerkzugriffskontrolle)

OT: operational technology (operationale Technologien)

PCI: Payment Card Industry (Kreditkarten-Branche)

VLAN: virtual local area network (virtuelles lokales Netzwerk)

VPN: virtual private network (virtuelles privates Netzwerk)

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Tel (Intl): +1-408-213-3191
Support: 1-708-237-6591