Informationen auf einen Blick

Vorteile

- **Zentralisierte, einheitliche Zugriffskontrolle** auf Basis der Rolle im Unternehmen. Dies ermöglicht eine konsistente Anwendung von Netzwerkzugriffsrichtlinien für Endbenutzer, unabhängig davon, ob die Verbindung über ein Kabel-, Wireless- oder VPN-Netzwerk erfolgt.
- **Mehr Transparenz und präzisere Geräteerkennung** mithilfe der Geräteprofilierung und dem Geräteprofil-Feed-Service der Cisco® Identity Services Engine (ISE), wodurch die Anzahl unbekannter Endpunkte verringert wird.
- **Vereinfachter Gastzugriff** für mobile ebenso wie Desktop-Nutzer über vollständig anpassbare Gastportale, die eine unkomplizierte Einbindung und Verwaltung ermöglichen und dank dynamischer visueller Workflows innerhalb weniger Minuten erstellt sind.

Cisco Identity Services Engine

Unternehmensnetzwerke sind heute nicht mehr sicher hinter vier Wänden eingeschlossen, sondern erstrecken sich überall dorthin, wo Mitarbeiter tätig sind und Daten übertragen werden. Mitarbeiter erwarten heute uneingeschränkten Zugriff auf alle Ressourcen, die sie für ihre Arbeit benötigen – unabhängig davon, welches Gerät sie verwenden oder ob dies über ein externes Netzwerk geschieht. Mobilität und das Internet of Everything (IoE) verändern die Art und Weise, wie Menschen leben und arbeiten – und stellen Unternehmen vor neue Herausforderungen. Denn sie müssen eine immer größere Zahl an netzwerkfähigen Geräten unterstützen, dabei aber angesichts unzähliger Bedrohungen jederzeit Sicherheit beim Zugriff auf ihr Netzwerk gewährleisten. Wie wichtig das ist, machen die immer häufigeren Schlagzeilen rund um Datensicherheitsverletzungen deutlich.

Erweiterte Netzwerke bedeuten auch mehr Komplexität bei der Kontrolle des Zugriffs auf Ressourcen, der Verwaltung voneinander getrennter Security-Lösungen sowie der Beherrschung von Risiken. Angesichts der immer umfassenderen Vernetzung im IoE und dem zumeist ohnehin dünn besetzten IT-Personal können die Auswirkungen somit äußerst schwerwiegend sein, wenn Sicherheitsbedrohungen nicht erkannt und beseitigt werden.

Sowohl für das Management als auch die Sicherheit der zunehmend mobilen Unternehmensnetzwerke ist daher ein neuer Ansatz gefragt: die Cisco® Identity Services Engine (ISE).

Weniger Angriffsfläche, geringeres Risiko

Ein effektiver Bedrohungsschutz beginnt mit einem transparenten Überblick über alle Benutzer und Geräte im Netzwerk sowie einer dynamischen Kontrolle, die sicherstellt, dass der Zugriff auf Unternehmensservices nur durch berechtigte Personen und Geräte möglich ist.

Mit der ISE 2.0 lassen sich konsistente Zugriffskontrollen für Kabel- und Wireless-Multivendor-Netzwerke sowie Remote-VPN-Verbindungen jetzt noch einfacher umsetzen. Intelligente Sensor- und Profilierungsfunktionen ermöglichen dabei eine tiefgreifende Analyse des Netzwerks – und damit herausragende Transparenz über alle Benutzer und Geräte hinweg, die auf Ressourcen zugreifen. Durch den Austausch von wichtigen Kontextdaten mit Lösungen unserer Technologiepartner sowie durch die Implementierung von Cisco TrustSec-Richtlinien zur softwaredefinierten Segmentierung verwandelt die Cisco ISE das Netzwerk von einer einfachen Datenleitung in eine Kontrollinstanz, die die Zeit bis zur Erkennung und Beseitigung von Bedrohungen deutlich verkürzt.

- **Schnellere Umsetzung von BYOD- und Mobility-Initiativen** dank unkomplizierter Einrichtung, Self-Service-Geräteeinbindung und -management, internem Zertifikat-Management und integrierter EMM-Partnersoftware (Enterprise-Mobility-Management) für die Geräteeinbindung innerhalb und außerhalb des Unternehmensstandorts.
- **Eindämmung von Netzwerkbedrohungen durch softwaredefinierte Segmentierung** mittels Cisco TrustSec®-Technologie. Diese implementiert rollenbasierte Zugriffskontrollen auf Routing- und Switching-Ebene, wobei eine dynamische Segmentierung auch ohne die Komplexität verschiedener VLANs oder einer Umgestaltung des Netzwerks möglich ist.
- **Austausch umfangreicher Kontextdaten mit Netzwerk- und Security-Lösungen von Partnern**, die auf diese Weise effektiver arbeiten können und eine schnellere Erkennung und Beseitigung von Bedrohungen ermöglichen.
- **Automatische Eindämmung von Bedrohungen** durch die Integration mit Cisco FirePOWER Management Center, da die ISE infizierte Endpunkte zur Behebung, zur Beobachtung oder zum Entfernen unter Quarantäne stellen kann.

Updates und Neuerungen bei ISE 2.0:

- Bereitstellung von Standortdaten durch Integration mit der Cisco Mobility Services Engine (MSE) – dies ermöglicht die Beschränkung des Zugriffs auf einen bestimmten Standort, sodass z. B. medizinisches Personal nur in der Notaufnahme auf Patientenakten zugreifen kann.
- Offene Architektur für die Integration von ISE-Partnerlösungen – dies ermöglicht es Kunden, ihre bestehenden Security-Lösungen zusammen mit der ISE zu verwenden und so Bedrohungen im Netzwerk leichter zu erkennen, einzudämmen und zu beseitigen.
- Unterstützung für Netzwerkzugriffsgeräte und IPv6-Endpunkte von Drittanbietern – auf diese Weise kann die ISE Endpunkt-Compliance für ein breiteres Spektrum von Netzwerken gewährleisten.
- Optimiertes Richtlinienmanagement, einschließlich vereinfachter AAA-Geräteadministration (Authentication, Authorization, Accounting) mit TACACS+ und RADIUS-Zugriffsfunktionen – dies erleichtert die Implementierung von Richtlinien für sicheren Zugriff auf kabelgebundene Netzwerke erheblich.
- Neues Network Visibility Module (NVM) mit Cisco AnyConnect 4.2 – dieses liefert einen bislang unerreichten Einblick in den Anwendungsdatenverkehr von Endpunkten außerhalb des Unternehmensnetzwerks.

Über die Cisco Platform Exchange Grid (pxGrid)-Technologie ermöglicht die ISE zudem den Austausch von wichtigen Kontextdaten mit integrierten Lösungen unserer Technologiepartner, die auf diese Weise Bedrohungen effektiver aufspüren, eingrenzen und beseitigen können. Die Zugriffskontrolle wird zentralisiert und deutlich vereinfacht. So können geschäftskritische Services sicher bereitgestellt, die Infrastruktur besser geschützt, die Compliance jederzeit gewährleistet und Service-Operationen beschleunigt werden.

Durch die Integration mit führenden SIEM- (Security-Information- & Event-Management) und TD-Lösungen (Threat-Defense), gestützt durch tiefgehende Netzwerktransparenz und sichere Zugriffskontrollen, bildet die ISE ein zentrales Element der Cyber Threat Defense-, Network-as-a-Sensor- und Network-as-an-Enforcer-Lösungen von Cisco. Damit liefert die ISE die Transparenz, den Kontext und die dynamischen Kontrollen, die Unternehmen benötigen, um das Netzwerk über das gesamte Angriffskontinuum hinweg effektiv abzusichern: die Verwaltung des Zugriffs vor einem Angriff, Einblicke in und Eindämmung von Bedrohungen während eines Angriffs sowie schnellere Erkennung und Beseitigung nach einem Angriff.

Nächste Schritte

Weitere Informationen zur Cisco ISE erhalten Sie unter http://www.cisco.com/go/ise oder bei Ihrem Ansprechpartner vor Ort.

C45-654884-13 10/15