Informationen auf einen Blick

Diese Technologie steht in Ihrem Cisco Netzwerk bereit, damit Sie:

- Bedrohungen innerhalb Ihrer Infrastruktur schnell isolieren und eindämmen können.
- durch die Segmentierung Ihres Netzwerks den Einfluss von eindringenden Angreifern limitieren können.
- eine präzise und einheitliche Zugriffskontrolle in Abhängigkeit von Benutzer, Gerät, Standort etc. ermöglichen können.

„Mit der Cisco Lösung können wir vom Wireless Access Point oder Switch aus sehr präzise feststellen, welcher Benutzer versucht, auf welche Ressourcen zuzugreifen. So können wir Benutzer in die passende Kategorie einordnen und die richtigen Richtlinien einsetzen, um die Anforderungen der Informationssicherheit zu erfüllen."

Roman Scarabot-Mueller
Leiter des Bereichs Infrastruktur,
Mondi Group International

Cisco Network as an Enforcer

Risikoeindämmung durch Netzwerksegmentierung

In einer Zeit, in der Netzwerkverbindungen immer schneller und schneller werden, ist Ihr Netzwerk ständig Cyberangriffen durch professionelle Hacker ausgesetzt. Jede Netzwerkverbindung – egal ob mobil, über Cloud-Services oder das Internet of Things (IoT) – stellt einen potenziellen Angriffspunkt dar. Sie stehen vor der Herausforderung, den für Benutzer und Geräte notwendigen Netzwerkzugriff so gut wie möglich gegen Risiken abzusichern.

Die gute Nachricht ist, dass Ihr Cisco® Netzwerk bereits über die dazu erforderlichen Tools verfügt. Sie brauchen Sie einfach nur zu aktivieren, und schon unterstützt Ihr Netzwerk die Durchsetzung der Sicherheitsrichtlinien. Sie können zum Beispiel Bedrohungen eindämmen, indem Sie Cisco TrustSec® und die Cisco Identity Services Engine (ISE) einsetzen, um Ihr Netzwerk in kleinere Segmente aufzuspalten. Über einen softwaredefinierten Ansatz bei der Netzwerksegmentierung können Sie die Segmente dann durch separate Gruppenzuweisungen schützen, wodurch der Benutzerzugriff basierend auf Benutzerrollen und den entsprechenden Geschäftsanforderungen festgelegt wird.

Das Ergebnis ist eine sichere Kontrolle des Netzwerkzugriffs, die rollenbasiert und unabhängig von Topologie und Zugriff ist. Sie verringern Ihre „Angriffsfläche" bedeutend. Selbst wenn Hacker in Ihr Netzwerk eindringen, können sie sich nicht frei bewegen und keinen weitflächigen Schaden anrichten.

Dynamische Richtliniendurchsetzung

Mit dem Cisco Netzwerk zentralisieren Sie Ihre Sicherheitsrichtlinien und wenden sie auf das gesamte Netzwerk an. Die richtigen Benutzer und Geräte erhalten den richtigen Zugriff, und die Gefahr eines Angriffs wird eingedämmt. Die Cisco ISE dient als zentralisierte Richtlinien-Engine, die Zugriffskontrollentscheidungen für Cisco Switches, Router und Security-Geräte ermöglicht.

Weiterhin können Sie den Umfang, die Kosten und die Komplexität des Payment Card Industry Data Security Standard (PCI DSS) und des Health Insurance Portability and Accountability Act von 1996 (HIPAA) reduzieren.

Verwenden Sie Cisco als Netzwerk zur Durchsetzung von Richtlinien, um Sicherheitsrisiken zu minimieren, die Effizienz der Betriebssicherheit zu erhöhen und die Einhaltung von Richtlinien zu verbessern.

Nächste Schritte

Weitere Informationen dazu, wie Sie Ihr Cisco Netzwerk zur Durchsetzung von Richtlinien einsetzen können, finden Sie auf der Cisco Enterprise Network Security-Website.

C45-734478-00 05/15