aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

SICHERE NETZWERKZUGRIFFSSTEUERUNG MIT CLEARPASS UND COMMON CRITERIA-ZERTIFIZIERUNG

EINFÜHRUNG

Cyberangriffe sind mittlerweile immer intelligenter, zielgerichteter und schädlicher geworden. Durch neue Trends wie Mobile, BYOD, Cloud und IoT und die dadurch schnell gewachsene Angriffsfläche steigt die Wahrscheinlichkeit erfolgreicher Angriffe weiter an. Ob es sich um eine Behörde handelt, die notwendige Infrastrukturen schützen muss, oder um einen Gesundheitsdienstleister, der sich um den Schutz von Patientendaten kümmern muss – jedes Unternehmen/ jede Organisation muss daran arbeiten, solche Angriffe zu verhindern.

Während Behörden bei der Definition der Kriterien und Prozesse, nach denen Produkte zertifiziert werden, praktisch eine Vorreiterrolle übernommen haben, müssen Sicherheitsteams genau wissen, ob die Produkte, die sie zum Schutz des Unternehmens einsetzen, bestimmte geprüfte Sicherheitsstandards einhalten.

Seit 1999 nehmen Regierungen auf der ganzen Welt an einem Test- und Validierungs-programm gemäß ISO Standard Common Criteria teil. Im Rahmen dieses Programms wird geprüft und sichergestellt, dass IT-Produkte hohe und konsistente Standards erfüllen. Dadurch schafft dieses Programm deutlich mehr Vertrauen in die Sicherheit dieser Produkte. Mittlerweile sind 28 Länder Mitglied des Common Criteria-Konsortiums durch Initiativen wie NIAP in den USA, Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) in Frankreich und Australian Signals Directorate (ASD) in Australien. Resultierend daraus wird die Common Criteria-Zertifizierung in vielen RFP-Listen für das öffentliche Beschaffungswesen als Anforderung geführt.

Aruba ist eines der führenden Unternehmen bei der Common Criteria-Zertifizierung seines gesamten Produktportfolios. Hierzu gehören Wireless Access Points, Controller sowie Remote (VPN)-Verbindungssoftware. Als Schlüsselelement in Arubas 360 Secure Fabric führender Sicherheitslösungen ist ClearPass Policy Manager sowohl FIPS- als auch Common Criteria-zertifiziert.

CLEARPASS IM ÜBERBLICK

Die ClearPass-Produkte für sichere Netzwerkzugriffssteuerung bieten ein breites Leistungs-spektrum wie die einheitliche, umfassende und präzise Profilerstellung sowie Authentifizierung und Autorisierung für Benutzer, Systeme und Geräte, die Zugriff auf IT-Ressourcen benötigen. ClearPass richtet sich gezielt an die wichtigsten Sicherheitsheraus¬forderungen in Unternehmen ohne IT-Grenzen:

- **Umfassende Transparenz.** Wenn der Netzwerkzugriff von fast überall, zu jeder Zeit und über jedes Gerät gewährt werden kann, liegt die erste Herausforderung darin, zu wissen, wer oder was sich im Netzwerk befindet. ClearPass bietet umfassende Funktionen für Erkennungs- und Profilerstellung, damit nicht nur das Sicherheitsteam, sondern die gesamte IT-Abteilung sehen kann, wer und was mit dem Netzwerk verbunden ist. Dies ist besonders wichtig, wenn IoT-Geräte mit dem Netzwerk verbunden werden.
- **Proaktive Steuerung.** Mit ClearPass Policy Manager erhält jeder Benutzer, jedes System und jedes Gerät im Netzwerk Zugriff nur auf die Ressourcen, die für die jeweilige Rolle erforderlich sind. ClearPass authentifiziert jede Entität und vergibt Zugriffsrechte auf der Grundlage von Richtlinien, durch die die Berechtigungen je nach Standort, verwendetem Gerät, Tageszeit, Benutzertyp und anderen Faktoren angepasst werden.
- **Reaktionen auf Basis eines Closed-Loop-Ansatzes.** ClearPass ist sozusagen der Gatekeeper des Netzwerks. Die Richtlinienengine, die den Netzwerkzugriff ermöglicht, kann auch verwendet werden, um auf einen Cyberangriff zu reagieren. Wenn eine Warnung aus dem Sicherheitsökosystem (Firewalls, Sandboxen, Endpunkterkennung und Reaktion, SIEM, UEBA usw.) empfangen wird, kann ClearPass eine Vielzahl von richtlinienbasierten Aktionen durch erneute Authentifizierung, Bandbreitenbegrenzung, Quarantäne oder Blockierung ausführen.

Bildunterschrift: Aruba ClearPass bietet einen Closed-Loop-Ansatz für Netzwerkwerkzugriffssteuerung und Reaktion.

VORTEILE DURCH CLEARPASS

- **Sicherheit durch umfassende Common Criteria-Zertifizierung.** ClearPass ist Common Criteria-zertifiziert für NDcPP (Network Device Collaborative Protection Profile), das alle Aspekte der Zugriffssteuerung wie Verschlüsselung, physische Sicherheit, Zertifikats¬validierung und -verarbeitung sowie SSL-Verarbeitung abdeckt. Darüber hinaus erhielt der ClearPass Authentication Server eine zusätzliche Common Criteria-Zertifizierung, die zentrale Authentifizierungs-, Autorisierungs- und Buchhaltungsfunktionen (AAA) für das branchenübliche RADIUS Client/Server-Protokoll validiert. Durch diese Zertifizierungsstufe funktioniert ClearPass auch in klassifizierten Netzwerken und bei vergleichbaren sensiblen Anforderungen im privaten Sektor.
- **Offene und nahtlose Integration.** Im Gegensatz zu anderen Zugriffssteuerungslösungen, die eine Bindung an die Infrastruktur eines einzelnen Anbieters erfordern, funktioniert ClearPass in jedem Netzwerk optimal. Darüber hinaus lässt sich ClearPass in über 120 Sicherheits- und allgemeine IT-Lösungen integrieren. So können diese Lösungen die von ClearPass generierten Profil- und Gerätekontexte optimal nutzen. Sicherheitsteams verwenden ClearPass auch, um entweder manuell oder automatisch Maßnahmen als Reaktion auf einen Cyberangriff zu ergreifen.
- **Ein Netzwerk, eine Ansicht, eine Richtlinie.** Die Fähigkeit von ClearPass, den Zugriff auf IT-Ressourcen zu kontrollieren, ist nicht nur unabhängig vom Hersteller, der die Geräte liefert, sondern auch davon, ob der Zugriff kabelgebunden, kabellos oder remote erfolgt. Unternehmen entwerfen und implementieren eine Richtlinie pro Benutzer oder Gerät, und ClearPass setzt diese Richtlinie nahtlos in der gesamten Netzwerktopologie durch. Dies führt zu Zeit- und Kosteneinsparungen, die auch bei anderen IT- und Sicherheitsprojekten zum Tragen kommen.
- **Optimierte Netzwerke.** Ein ROI-spezifischer Vorteil von ClearPass ist die richtlinienbasierte Durchsetzung von Portzugriff und -nutzung. Anstatt Ports für bestimmte Anwendungsfälle (für die Verbindung von Druckern, Servern usw.) zuzuweisen, können Unternehmen eine Strategie der „farblosen Ports“ anwenden. Dabei kann jeder Port mit jedem Gerät verbunden werden, während ClearPass die entsprechenden rollenbasierten Zugriffssteuerungen durchsetzt. Dies vereinfacht die Einrichtung und Konfiguration von Switches und optimiert die Portnutzung.
- **Konsequente Zugriffssteuerung: Vertrauen ist gut, Kontrolle ist besser.** Einige Zugriffssteuerungslösungen erlauben jedem Benutzer oder Gerät Zugang zum Netzwerk. Maßnahmen werden erst dann ergriffen, wenn etwas schief geht. Dieser „entspannte“ NAC-Ansatz lädt geradezu zu blitzschnellen Cyberangriffen ein, bei denen Malware innerhalb einer Sekunde in das Netzwerk gelangt und einen langwierigen, extrem schädlichen Angriff startet. ClearPass hingegen erlaubt ohne positive Authentifizierung und entsprechende richtlinienbasierte Berechtigung keinem Benutzer oder Gerät Netzwerkzugriff. Wenn es auf Sekunden ankommt, muss die Zugriffssteuerung von Anfang an beginnen.
- **Wirksame Angriffsabwehr.** Der Grundsatz lautet: „Man kann nicht schützen, was man nicht sehen kann“. Einer der Vorteile der ClearPass-Erkennung und -Profilerstellung ist die vollständige Transparenz. Aber in einer Welt, in der bei der Reaktion auf einen Angriff jede Sekunde zählt, kann man auch Probleme, die man nicht sehen kann, nicht lösen. Wenn Sicherheitsteams mit ClearPass Reaktionen auf Cyberangriffssignale aus dem Sicherheits¬netzwerk vorab definieren, lassen sich Angriffe bereits im Vorfeld unterbinden, bevor sie Schaden anrichten. Gleichzeitig können die Teams dadurch weitere Untersuchungen anstellen und das Ausmaß der Sicherheitsverletzung bestimmen.

ZUSAMMENFASSUNG

Die Common Criteria-Zertifizierung ist ein anspruchsvoller Prozess, bei dem der Aspekt Sicherheit ein integraler Bestandteil der Architektur und Implementierung eines Produkts sein muss. Einst war das Thema Common Criteria nur für Behörden von Bedeutung, die Infrastrukturen und sensible Informationen schützen mussten. Heute ist jedes Unternehmen bei einem erfolgreichen Cyberangriff mit ähnlichen Risiken und Konsequenzen konfrontiert. Für zentrale Lösungen wie beispielsweise Zugriffs-steuerungslösungen ist die Common Criteria-Zertifizierung unerlässlich. Durch die erweiterten Common Criteria-Zertifizierungen bietet ClearPass nicht nur eine sichere Grundlage, sondern ist auch ein entscheidendes Element für die gesamte IT-Sicherheitsstrategie.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com