

OSIATIS Security Services zur Implementierung von selbstverteidigenden Netzwerken

Die Einführung von Cisco NAC (Network Admission Control) als Basis von selbstverteidigenden Netzwerken bietet Unternehmen optimalen Schutz vor bekannten und unbekanntem Attacken.

Die Herausforderung

Ein sicheres Netzwerk ist eine wesentliche Voraussetzung für bestmögliche Performance und maximale Verfügbarkeit, den zwei wichtigsten Faktoren um Kundenzufriedenheit, Effektivität von Mitarbeitern und somit Profitabilität eines Unternehmens zu gewährleisten. Zu den größten Bedrohungen für ein IT-Netzwerk zählen Viren, Würmer, Spyware und gezielte spezifische Attacken (e.g. DoS), die Unterbrechung von angebotenen Diensten, Systemausfälle und Produktivitätsverluste verursachen.

Die gefährlichsten Arten solcher Attacken sind jene, die sich selbst im Netzwerk verbreiten, und der mögliche Schaden ist ungleich höher, wenn interne Server und Arbeitsstationen nicht der Security Policy eines Unternehmens entsprechen bzw. aktuelle Sicherheitspatches nicht oder noch nicht installiert sind.

Um das Unternehmen nach außen vor solchen Attacken zu schützen gibt es punktuelle Firewalls, Intrusion Detection/Protection Systeme (IDS/IPS), Gateway Virens Scanner, etc. Durch die immer größer werdende Anzahl von sogenannten „Mobile Users“ ist jedoch die Quelle obiger Attacken immer öfter innerhalb des Unternehmens im eigenen Netzwerk zu finden.

Um das Unternehmen auch intern bestmöglich zu schützen genügt es nicht sich auf möglicherweise installierte Applikationen zu verlassen, sondern das Netzwerk selbst (i.e. Switches, Router, Wireless Access Points) muss sicherstellen, dass kein Gerät, welches nicht den definierten Sicherheitsrichtlinien entspricht, in das Unternehmensnetzwerk gelangt.

Die Lösung

Durch die Implementierung von Cisco NAC wird sichergestellt, dass der Netzwerkzugriff eingeschränkt oder nicht gewährt wird, wenn beispielsweise:

- kein Virens Scanner installiert ist
- die Virensignatur nicht am aktuellen Stand ist
- nicht das vorgeschriebene Betriebssystem verwendet wird
- das letzte Service Pack nicht eingesetzt wird
- ein bestimmter Hotfix nicht installiert ist
- die Authentifizierung oder Autorisierung fehlschlägt
- eine kritische Anwendung nicht installiert oder aktiviert ist

Durch eine integrierte zentral verwaltete Firewall und ein Intrusion Protection System am Client, werden zusätzlich auch alle nicht genehmigten Aktivitäten gesperrt bzw. auch zur Zeit noch unbekannte Attacks unterbunden und zentral registriert. Dieser Schutz besteht auch dann, wenn sich der Client nicht im Unternehmensnetzwerk befindet; Auffälligkeiten werden beim nächsten Verbinden im Firmen-LAN nachträglich zentral geloggt.

Cisco NAC ist die ideale Security Lösung sowohl für kleine und mittlere Unternehmenszentralen, größere Niederlassungen als auch natürlich für große Unternehmen. Mit Cisco NAC können auch RemoteAccess VPN Verbindungen, Wireless LANs und Dialup Verbindungen geschützt werden.

OSIATIS NAC Services Komponenten

Mit den OSIATIS NAC Services zur Implementierung von selbstverteidigenden Netzwerken, bietet OSIATIS professionelle Unterstützung beim Design, Einsatz und der Wartung von Cisco NAC.

Die Security Consultants von OSIATIS besitzen ein tiefes technologisches Know-How im Netzwerk- sowie Security-Bereich und haben detailliertes Wissen und Erfahrung bei der Planung, dem Design und der Implementierung von NAC Lösungen. Durch die enge Partnerschaft mit Cisco Systems und Herstellern von Antivirensoftware wie etwa Trend Micro, und den entsprechend zertifizierten Mitarbeitern (e.g. CCIE Security), profitieren Kunden beim Design und der Implementation von NAC Lösungen. Die Security Consultants beraten sie mit ihrem Wissen auch bei der Integration von NAC Lösungen in ein gesamtheitliches Security Konzept, welches Firewalls, Intrusion Detection/Protection sowie Content Security, VPN Lösungen, etc. betrifft.

Die Services Komponenten im Detail sind:

NAC Survey

Speziell ausgebildete Mitarbeiter von OSIATIS analysieren die IT-Infrastruktur, inwieweit sie für eine NAC-Lösung geeignet ist. Es werden Netzwerkkomponenten, Systemarchitekturen und definierte Vorgänge der Security Policy bezüglich Voraussetzungen und Ziele für einen erfolgreichen Einsatz von NAC überprüft. Zusätzlich zur Identifikation von Komponenten die NAC nicht unterstützen, wird geprüft ob die Netzwerk Topologie skaliert (i.e. einen schrittweisen Einsatz von NAC ermöglicht) und eine Analyse erstellt, die die Anforderungen für Redundanz und Skalierbarkeit, sowie erforderliche Hard- und Softwareupdates bzw. -upgrades detailliert darstellt.

Voraussetzungen werden im Detail geprüft für:

- Cisco Trust Agent (CTA)
- AntiVirus/-Spyware Software
- Cisco Security Agent (CSA)
- Network Access Devices (NAD)
- Cisco Secure Access Control Server (ACS)
- CiscoWorks VPN/Security Management Solution (CWVMS)

NAC Prototyping

Systems Engineers installieren und konfigurieren eine NAC-Pilotumgebung, um dem Kunden die Möglichkeit zu geben, NAC im eingeschränkten Livebetrieb testen und Erfahrungswerte sammeln zu können. Dieser Pilot kann in einem speziellen Lab oder in Teilen des produktiven Netzwerks (e.g. spezifische Außenstelle oder Abteilung, VPN Umgebung, etc.) aufgesetzt werden. Nach einem definierten Zeitraum und unter Berücksichtigung der Erfahrungswerte des Piloten, kann das NAC Design für das gesamte Unternehmen entwickelt werden.

NAC Design

Zertifizierte Security Consultants veranstalten mit dem Kunden ein gemeinsames Workshop, um spezifische technische, geschäftliche und operative Aspekte zu erörtern. Die Informationen aus diesem Workshop werden für die Entwicklung eines detaillierten Designs für die Integration von NAC in die IT-Infrastruktur herangezogen. Diese *NAC Design Spezifikationen* enthalten unter anderem genaue Netzwerk Diagramme und Beispielkonfigurationen für NAC Komponenten (e.g. NAD, ACS), die definierte Netzwerk Topologie mit Alternativen betreffend Skalierung und Voraussetzungen für die Endgeräte Software Komponenten (e.g. CTA, CSA, AV-Client) sowie für die Management Software.

Weiters wird ein *NAC Deployment Plan* erstellt, der die technischen und personellen Voraussetzungen für die unternehmensweite Implementaion von NAC sowie mögliche Abhängigkeiten analysiert und somit die Basis für einen Projektplan bildet.

NAC Deployment

Um eine möglichst effektive Sicherheit zu erlangen muss die NAC Lösung im gesamten Unternehmen sorgfältig konfiguriert, implementiert und integriert werden. OSIATIS Security Systems Engineers unterstützen das IT-Team des Kunden vor Ort bei der unternehmensweiten Installation und Integration.

Nach der Implementierung laut NAC Deployment Plan, wird eine Dokumentation erstellt, welche die endgültigen NAC Policies, Konfigurationen der NAC Komponenten, sowie die Prozeduren für den Betrieb, das Management, die Wartung und den Support der NAC Lösung beinhaltet.

In einem abschließenden Workshop werden definierte Mitarbeiter des Kunden für den reibungslosen Betrieb und das Management der NAC Lösung geschult.

□ NAC Tuning

Da sich die Netzwerk-Begebenheiten von Zeit zu Zeit ändern, arbeiten die OSIATIS Security Systems Engineers laufend daran, die NAC Lösungen in Anbetracht von Zuverlässigkeit, Effizienz und Skalierbarkeit zu optimieren sowie der neuen Situation anzupassen. Sie unterstützen den Kunden bei der Wartung und dem Support der NAC Infrastruktur und helfen ihnen die Überwachung und Performance zu verbessern um die Effizienz weiter zu steigern.

Unsere Security Spezialisten unterstützen sie auch bei der Auswahl und dem Einsatz neuer Software- bzw. Hardware-Erweiterungen, bei der Implementation neuer Features und Technologien und garantieren ihnen dadurch den bestmöglichen Nutzen der NAC Lösung.

Die Vorteile

Die OSIATIS NAC Services bieten viele Vorteile:

- Minimierung des Sicherheitsrisikos
 - Begrenzung des Schadens verursacht durch Malware (Viren, Würmer, Spyware, Trojaner o.ä.), Access- oder DoS-Attacken
 - Helfen sicherzustellen, dass alle Systeme der Security-Policy entsprechen (e.g. aktuelle Virensignatur, aktivierte Firewall, etc.)
 - Schnelle Umsetzung durch Aufteilung von Aufgaben zwischen OSIATIS und dem Kunden
 - Resultat ist eine vielschichtige Sicherheitslösung zum Schutz vor Attacken aller Art

- Bestmögliche Skalierung und Verbesserung der Produktivität
 - Verkürzung von Implementations- und Migrationszeiten und Minimierung von Implementationsfehlern
 - Effiziente und durchgängige Policies und Prozeduren
 - Helfen, dass die NAC Lösung effizient im gesamten Unternehmen implementiert wird
 - Umfassende NAC Lösung mit effektivem zentralen Management
 - Minimierung eines teuren Re-Designs bzw. teurer Nacharbeiten

- Reduzierung der Total Cost of Ownership (TCO) und Lieferung eines rascheren Return on Investment (ROI)
 - Bestmögliche Integration der NAC Lösung in die bestehende Infrastruktur
 - Optimierung der NAC Lösung für laufendes und effizientes Management sowie Wartung
 - Reduzierung der operativen Kosten durch eine gesicherte Einhaltung der Security Policy im gesamten Unternehmen
 - Berücksichtigung von zukünftigen NAC Features (Phase II) beim Design aktueller NAC Lösungen (Phase I)



Weitere Informationen sowie Preisgestaltung:

OSIATIS Computer Services GmbH

Franzosengraben 12

A-1030 Wien

Tel.: +43 1 795 20 0

E-Mail: office@osiatis.at

Homepage: www.osiatis.at/cisco

**Anmelden zur
NAC LIVE DEMO
Lassen Sie sich überzeugen!**