

Whitepaper

Network Access Control

Integritäts-basierte Zugangskontrolle

Oktober 2006

Zusammenfassung

Network Access Control (NAC) ermöglicht es, den Intranet-Zugang von Rechnern in Abhängigkeit von deren Identität *und* Integrität zu kontrollieren. NAC stellt sicher, dass Geräte, die nicht einer vorgegebenen Sicherheits-Policy genügen, keinen Zugang auf kritische Unternehmensressourcen erhalten und damit kein Risiko für die Sicherheit der anderen Systeme im Netzwerk darstellen. NAC schließt damit eine Lücke in der Netzwerksicherheit, die insbesondere durch den Zugang von potentiell unsicheren mobilen und remote Systemen entstehen kann.

Zur Durchsetzung dieser Ziele werden verschiedene bekannte und erprobte Technologien (wie z.B. RADIUS, IEEE 802.1x, EAP, dynamische ACLs, Virens Scanner) erweitert und kombiniert. Eine NAC-Infrastruktur benötigt sowohl clientseitig als auch serverseitig sowie auch auf Netzwerkkomponenten zusätzliche Software-Komponenten. Es existieren zz. bereits erste Implementierungen, u.a. von Cisco (Network Admission Control - *NAC*) und ab Vista/Longhorn auch von Microsoft (dort Network Access Protection - *NAP* genannt). Diese Implementierung sind bislang noch weitestgehend inkompatibel zueinander und befinden sich z.T. erst im Beta-Stadium. Im Laufe des Jahres 2007 kann mit einer Konsolidierung der de-facto Standards und mit dem Erscheinen von marktreifen Lösungen gerechnet werden, die den Anforderungen von großen Produktivnetzen genügen können.

Inhalt

1	Einführung.....	1
2	Lösungsansätze.....	2
2.1	Erkennen und Prüfen der Clients.....	2
2.2	Durchsetzen der Zugriffsbeschränkungen.....	3
3	Marktüberblick.....	4
3.1	Cisco NAC.....	5
3.1.1	NAC L2 802.1x.....	6
3.1.2	NAC L2/L3 IP.....	6
3.2	Microsoft NAP.....	7
3.3	TNC.....	8
3.4	Weitere Hersteller.....	9
4	Standardisierung.....	10
5	Bewertung der Sicherheit.....	11
6	Fazit und Ausblick.....	12
	Referenzen.....	13

1 Einführung

Viele Firmen haben in den letzten Jahren zahlreiche Sicherheitsvorkehrungen getroffen, um ihre Netzwerkzugänge zu schützen. Vor allem bei Remote-Zugänge (VPN) ist sicherheitstechnisch oft aufgerüstet worden, während intern oft nur der WLAN-Zugang abgesichert wird und LAN-Zugänge oft komplett unberücksichtigt bleiben. Häufig anzutreffende Maßnahmen zur Absicherung der Netzwerkzugänge sind:

- ▶ IEEE 802.1x Authentifizierung für User und Maschinen
- ▶ MAC-Filter
- ▶ VPN mit Tokens (SecureID, diverse SmartCards)

Es handelt sich hier im Grunde um eine Identitäts-basierte Zugangskontrolle, die zweifelsohne unverzichtbarer Bestandteil der Sicherheitsmaßnahmen ist, wobei sich vor allem IEEE 802.1x als flexible und wieder verwendbare Lösung anbietet. Bei dieser „herkömmlichen“ Zugangskontrolle wird jedoch lediglich die Identität eines Nutzers oder einer Maschine geprüft, die jeweilige Integrität wird nicht berücksichtigt. Unabhängig vom „Gesundheitszustand“ wird Eintritt gewährt. Wichtige Faktoren, die die Sicherheit maßgeblich beeinflussen – z.B. aktuelles Patchlevel, neueste Virensignaturen, aktivierte Personal Firewalls usw. – werden nicht für eine Zugangskontrolle herangezogen.

Dies kann fatale Auswirkungen für das gesamte Unternehmensnetzwerk haben. Ein Telearbeiter, der sich mit einem unsicheren und mit Schadcode verseuchten PC in das Firmennetzwerk über VPN einwählt, kann dort ungehindert andere PCs infizieren. Ein Außendienstler, der gelegentlich in die Firma fährt und dort seinen Laptop an einen LAN-Port anschließt, ist ebenso eine Gefahr wie Gäste oder Externe, die mit ihren eigenen Geräten Zugang zum Netzwerk bekommen. Und das alles, obwohl diese Mitarbeiter alle authentifiziert und berechtigt sind, das Netzwerk zu nutzen. Sicherheitszonen und Personal Firewalls im Intranet können dabei ebenso wie Intrusion Detection Systeme nur reagieren und versuchen, größeren Schaden zu verhindern, die eigentliche Ursache können sie nicht angehen. Ebenso sind Versuche, das Problem durch rigide Sicherheitspolicies in den Griff zu bekommen, in einer immer stärker vernetzten Welt zum Scheitern verurteilt. Es ist auf Dauer schwer durchsetzbar und kaum überprüfbar, dass alle mobilen Geräte, die in ein Unternehmensnetz kommen können, außerhalb ausschließlich an vertrauenswürdigen Netzwerken betrieben werden.

Es ist daher nahe liegend, dass nicht nur die Identität, sondern auch die Integrität zentraler Bestandteil der Entscheidung sein muss, ob jemand Zugang zum Netzwerk erhält. Je nach Niveau der Integrität ist zu unterscheiden, welche Zugangsrechte erteilt werden. So kann etwa nur einem Gerät, das sämtliche gestellte Integritätskriterien erfüllt, voller Zugang erteilt werden. Einem Client, der nur einen Teil der Kriterien erfüllt, sollte der Zugang verweigert oder nur beschränkt gewährt werden. Im Falle der Nichterfüllung der Integritätskriterien sollte der Zugang zum Netzwerk vollständig verwehrt werden oder nur Zugriff auf gesonderte Res-

sources erlaubt werden, über die der Client die Möglichkeit erhält, Integritätskriterien zu erfüllen (z.B. Web-Server mit aktuellen Signaturen oder Patches).

Natürlich kann die Integritätsprüfung auch losgelöst von einer zusätzlichen Prüfung der Identität betrachtet werden. Jedoch entfaltet erst eine Zugangskontrolle mit der Kombination aus gemeinsamer Prüfung von Identität und Integrität ihr volles Potential.

2 Lösungsansätze

Grundsätzlich müssen alle Lösungsansätze die folgenden drei Schritte umfassen:

1. Erkennen das ein Client versucht Zugang zum Netzwerk zu erlangen
2. Prüfen des Client und Festlegen der zulässigen Zugriffsrechte
3. Durchsetzen der jeweils festgelegten Zugriffsrechte

Zur Realisierung dieser Schritte werden in den verschiedenen Ansätzen jeweils unterschiedliche Techniken eingesetzt, die im Folgenden näher erläutert werden.

2.1 Erkennen und Prüfen der Clients

Als erstes muss erkannt werden, ob ein Benutzer oder eine Maschine versucht, Zugang zum Netzwerk zu erlangen. Die Erkennung des Zugriffsversuchs geschieht typischerweise durch

- ▶ Feststellen von beliebigem Netzwerkverkehr (mittels In-Line Appliances)
- ▶ Abfangen von DHCP oder ARP Request
- ▶ IEEE 802.1x (EAPOL Start Frames)
- ▶ Physikalischer Link

Nach der Erkenntnis, dass Zugriff verlangt wird, setzt dann üblicherweise die Prüfung der Identität der jeweiligen Maschinen oder des Benutzers ein. Je nach Implementierung einer Integritäts-basierten Zugriffskontrolle wird während dessen oder erst im Anschluss die Prüfung der Integrität durchgeführt.

Ein gängiger Ansatz ist das Installieren zusätzlicher Softwarekomponenten (Agenten-basiert), die den Zustand des Clients (Patches, Signaturen, Sicherheitseinstellungen) an einen zentralen Policy-Server melden. Auf Basis dieser Informationen fällt der Policy-Server (ggf. unter Zuhilfenahme weiterer Policy-Server) die Entscheidung, welche Zugangsrechte gewährt werden.

Ein weiterer Ansatz besteht darin, mobilen Code zu benutzen. Statt der Installation einer Softwarekomponente wird hier dynamisch ausführbarer Code – beispielsweise ActiveX Controls oder Java Applets – auf den

Rechner geladen. Dieser mobile Code führt anschließend eine Prüfung des Rechnerzustandes durch und meldet dies wiederum einem zentralen Policy-Server. Je nach gemeldetem Zustand wird dort entschieden, in welchem Umfang Zugriffsrechte erteilt werden.

Schließlich kann die Integritätsprüfung auch ohne Eingriff auf den Clients erfolgen, d.h. ohne zusätzliche Software und Interaktionen des Benutzers. Bei Zugriff über einen beliebigen Netzzugang wird der Clients von einem Audit-Server untersucht (z.B. mittels Port-Scans, Remote-Prüfung der Registry) und in Abhängigkeit des Ergebnisses werden entsprechende Zugangsrechte erteilt.

Abhängig von der Art des Ansatzes sind verschiedene Detailtiefen bei der Integritätsprüfung realisierbar. Die Installation einer dedizierten Softwarekomponente zur Integritätsprüfung verspricht prinzipiell die genauesten Prüfergebnisse, da alle Eigenschaften der betreffenden Maschine mit genügend Rechten untersucht werden können. Allerdings ist die Installation derartiger Software normalerweise nur auf verwalteten, d.h. zentral erfassten und gewarteten Maschinen möglich. Unter Einsatz von mobilem Code wird zwar auch lokal auf dem zu untersuchenden Rechner Code ausgeführt, jedoch sind die Zugriffsrechte des mobilen Codes auf dem Rechner von verschiedenen Einstellungen abhängig. So muss der Benutzer dem mobilen Code u.U. explizit vertrauen, damit er ausgeführt werden kann. Auch die Browser-Einstellungen sind hier oft relevant. Noch schwieriger ist es, gänzlich ohne das Ausführen spezieller Software auf den zu untersuchenden Maschinen auszukommen, da hier der direkte Zugriff (z.B. Registry, Dateien etc.) i.A. nicht möglich ist.

Einige Hersteller von Integritäts-basierten Zugangskontrolllösungen kombinieren die genannten Ansätze. So wird für die Maschinen eines Unternehmens die Prüfung mittels zuvor installierten Softwarekomponente unterstützt, fremde Rechner (z.B. von Gästen) werden mit Hilfe von mobilem Code oder externem Auditing untersucht.

Die Integritäts-basierte Zugangskontrolle ist jedoch erst dann richtig interessant, wenn passende Schnittstellen zwischen den Anbietern verschiedener Softwarekomponenten existieren. Vor allem die ersten beiden Ansätze (fest installierte Agenten und mobiler Code) erfordern, dass der auszuführende Prüfcode (Agent) mit bestehenden Antivirenprogrammen, Personal Firewalls etc. kommunizieren kann, um so die Attribute der jeweiligen Software abzufragen. Auf der Serverseite ist es nützlich, wenn sich ein zentraler Policy-Server mit Policy-Servern anderer Anbieter (z.B. zentraler Antiviren-Server) verständigen kann, um das Spektrum der unterstützten Applikationen zu verbreitern.

2.2 Durchsetzen der Zugriffsbeschränkungen

Unabhängig von dem Ansatz der Integritätsprüfung muss die Einschränkung der Zugriffsrechte im Falle der Nichterfüllung bestimmter Kriterien über verschiedene Techniken erreicht werden:

- ▶ Zuweisung von VLANs (z.B. mittels SNMP oder IEEE 802.1x)
- ▶ IP-basierte ACLs zur gezielten Einschränkung von IP-Verkehr

- ▶ URL Redirects
- ▶ Dynamische IP-Zuweisung

Je nach Hersteller sind die Techniken mehr oder weniger dynamisch anwendbar. Die einzelnen Techniken unterscheiden sich zudem hinsichtlich ihrer Wirksamkeit. Beispielsweise sind URL Redirects nur begrenzt hilfreich, da sie zwar Auswirkungen auf das Verhalten eines Webbrowsers haben, jedoch andere IP-basierte Anwendungen nicht stoppen. Auch hier ist demzufolge eine Kombination verschiedener Technik häufig sinnvoll oder gar notwendig.

Nicht zuletzt kann eine Unterscheidung der verschiedenen Ansätze zur Integritäts-basierten Zugangskontrolle danach vorgenommen werden, welche Geräte für die Durchsetzung von Zugriffseinschränkungen zuständig sind. Weit verbreitet ist die Herangehensweise, dass die Entscheidung zur Auferlegung von Zugriffsbeschränkungen zentral durch Policy-Server getroffen wird. Diese Entscheidung wird dem jeweiligen Network Access Device (Switch, Access Point, VPN Gateway, etc.) mitgeteilt. Das NAD ist anschließend für die Umsetzung von Zugriffsbeschränkungen verantwortlich. Das NAD kann statische Attribute für bestimmte Verbindung implementieren (z.B. vordefiniertes VLAN) oder aber dynamisch Attribute (ACLs, VLAN, ...) vom Policy-Server beziehen.

Eine spezielle Variante dieses Ansatzes ist es, eine „Enforcement-Box“ zwischen die NADs und bestimmten Netzwerksegmenten zu schalten. Der Policy-Server liefert der Box die Entscheidung, die Box muss den Netzwerkverkehr oder die Funktionen der NADs so kontrollieren, dass die notwendigen Restriktionen eingehalten werden.

Eine weitere Möglichkeit ist die Umsetzung von Zugriffsbeschränkungen direkt auf dem jeweiligen Clients. Beispielsweise können ACLs direkt an einen Client gesendet und dort angewandt werden. Dies erfordert allerdings entsprechende Software auf dem Client, die die auferlegten Restriktionen tatsächlich umsetzt. Dieser Ansatz kann also nicht für Maschinen erfolgen, die nicht kontrolliert werden können und daher die ACLs einfach ignorieren.

3 Marktüberblick

Viele Hersteller haben die Bedeutsamkeit der Integritätsprüfung mittlerweile erkannt. Es existieren daher bereits einige Lösungen am Markt, wobei ein einheitlicher Standard nicht zu erkennen ist. Stattdessen implementiert jeder Hersteller seine eigenen proprietären Lösungen. Allerdings sind auch einige Standardisierungsbemühungen im Gange, die in Kapitel 4 betrachtet werden. Zunächst werden jedoch die unterschiedlichen Produkte und Konzepte einzelner Hersteller beleuchtet. Hauptaugenmerk gilt dabei zunächst den „Platzhirschen“ Cisco, Microsoft und dem TNC Konsortium. Anschließend werden Lösungen weiterer Hersteller kurz vorgestellt.

3.1 Cisco NAC

Cisco ist mit seiner Lösung namens „Network Admission Control“ [1] seit einiger Zeit am Markt präsent. Gegenüber anderen Lösungen ist NAC deutlich weiter und für den Großteil der Cisco-Produkte verfügbar. Allerdings erfordert NAC eine Cisco-Infrastruktur und Cisco-Softwarekomponenten. Mittlerweile haben sich über 70 Hersteller der NAC-Initiative angeschlossen und es sind bereits NAC-fähige Produkte - vor allem Antiviren Produkte - am Markt. Cisco kombiniert dabei mehrere der o.g. Lösungsansätze. Es steht eine Agenten-basierte Lösung mit verschiedenen Arten der Erkennung von Zugriffsversuchen sowie verschiedenen Techniken zur Zugriffsrestriktion zur Verfügung.

Auf den Clients ist die Installation des Cisco Trust Agent erforderlich. Dieser Agent sendet auf Anfrage den Zustand eines Client-Systems an die zentrale Komponente Cisco ACS. Der ACS agiert nun nicht mehr nur als RADIUS-Server, sondern auch als zentraler Policy-Server. Die Entscheidungen, die der ACS fällt, werden dem jeweiligen NAD (Network Access Device) – also Switch, Router, VPN Gateway, Access Point – mitgeteilt, über den der Clients sich einwählt.

Die Cisco-Lösung ist modular aufgebaut. Der Trust Agent ist durch Plugins andere Hersteller (z.B. Hersteller von Antiviren-Produkten) erweiterbar, d.h. der Trust Agent kann nach Installation von Erweiterungen auch den Zustand anderer installierter Softwarekomponenten an den ACS melden. Der ACS wiederum kann entweder selbst entsprechende Regeln für 3rd-party Softwarekomponenten aufweisen oder aber mit weiteren Policy-Servern (z.B. zentraler Antiviren-Policy-Server) kommunizieren (über das sog. GAME Protocol – Generic Authorization Message Exchange), um die Integrität des Clients beurteilen zu können.

Grundsätzlich hat Cisco zwei Ansätze implementiert, wann und wie die Integritätsmechanismen greifen. Zunächst besteht die Möglichkeit, während einer 802.1x-Authentifizierung und damit auf OSI-Schicht 2 zusätzliche die Softwareattribute (Patchlevel, Versionen, ...) an den ACS weiterzureichen. Diese Attribute werden dann für den Ausgang der 802.1x Authentifizierung zusätzlich herangezogen. Cisco bezeichnet dieses Verfahren als NAC L2 802.1x. Der zweite Ansatz greift erst zu einem späteren Zeitpunkt. Die Integritätsprüfung findet genau dann statt, wenn durch Kommunikation (ARP, DHCP) ein Client erkannt wird. Dieses Verfahren wird als NAC L2/L3 IP bezeichnet. Dies kann für Router, VPN Gateways und Access Points verwendet werden. Die beiden Ansätze werden im Folgenden noch näher beleuchtet.

Cisco unterscheidet bei der Integritätsprüfung eines Clients 6 verschiedene Zustände, die sich während oder nach der Prüfung ergeben können:

- ▶ „healthy“ (der Client entspricht vollständig den gestellten Kriterien)
- ▶ „checkup“ (der Client entspricht vollständig den gestellten Kriterien, es sind allerdings bereits Updates für bestimmte Komponenten verfügbar)

- ▶ „transition“ (die Überprüfung ist noch im Gange, bis dahin hat der Client einen definierten Interim-Zugang)
- ▶ „quarantine“ (der Client entspricht nicht den Kriterien)
- ▶ „infected“ (der Client stellt eine aktive Bedrohung dar)
- ▶ „unknown“ (die Integrität des Clients konnte nicht ermittelt werden)

3.1.1 NAC L2 802.1x

Wie dem Namen zu entnehmen ist, findet die Integritätsprüfung während einer 802.1x Authentifizierung statt. Erforderlich ist dafür zunächst ein Cisco-Gerät, das IEEE 802.1x und die NAC-Erweiterungen unterstützt. Mittlerweile sind fast alle Cisco Switches dafür ausgestattet.

Derzeit ist lediglich EAP-FAST als EAP-Variante (TLS-basiert) für die 802.1x Authentifizierung implementiert. Es ist daher ein 802.1x Supplicant auf den Clients erforderlich, der EAP-FAST unterstützt. Der native Microsoft-Client kann dies z. B. nicht leisten. Allerdings ist der kostenfreie Cisco Trust Agent mit einem eigenen Supplicant mit EAP-FAST Unterstützung ausgestattet. NAC L2 802.1x ist derzeit nur für Microsoft Windows verfügbar.

Als RADIUS Server kann nur der Cisco ACS verwendet werden, da nur dieser RADIUS Server die NAC-Erweiterungen aufweist. Die Kommunikation zwischen Client und NAD erfolgt über EAP-Frames, währenddessen die Kommunikation zwischen NAD und ACS mittels RADIUS Paketen (UDP) geschieht.

Das Durchsetzen von NAC-Entscheidungen vollzieht das jeweilige NAD. Bei Einsatz von NAC L2 802.1x ist hier lediglich die dynamische VLAN-Zuweisung als Mittel der Durchsetzung möglich. Der ACS gibt dabei nach Abschluss der 802.1x Authentifizierung das durchzusetzende VLAN vor (z. B. VLAN 1 für integrierte Clients, VLAN 2 für infizierte Clients), ggf. kann der Zugang zum Netzwerk komplett geblockt werden, indem die 802.1x Authentifizierung negativ ausfällt (RADIUS Reject Paket vom ACS an das NAD).

Da sich gerade bei Clients, die ununterbrochen Netzwerkkontakt haben, der Integritätsstatus auch im laufenden Betrieb ändern kann (z. B. Alter der Virensignaturen), kann der Integritätscheck periodisch durchgeführt werden.

3.1.2 NAC L2/L3 IP

Kommt keine 802.1x-integrierte Prüfung in Frage (z. B. aufgrund fehlender 802.1x-Infrastruktur), so kann auf NAC L2/L3 IP zurückgegriffen werden. Die Integritätsprüfung wird in diesem Falle angestoßen, sobald Client-Kommunikation in Form von ARP- oder DHCP-Paketen erkannt wird. Das NAD fordert anschließend den Client auf, seine Integrität zu beweisen. Dabei findet die Kommunikation zwischen Client und NAD mittels EAPoUDP statt, die Kommunikation zwischen NAD und RADIUS-Server mittels RADIUS-Paketen. Auf dem Client ist daher kein 802.1x Supplicant notwendig, jedoch ist auch hier der Trust Agent erforderlich,

wobei der Trust Agent sowohl für Microsoft Windows als auch für Redhat Linux verfügbar ist. Als NAD kommen Cisco Router, APs und VPN Gateways zum Einsatz.

Während die Entscheidung über die Zugangsrechte wiederum zentral am Cisco ACS gefällt wird, ist die Durchsetzung Aufgabe des jeweiligen NAD. Als Techniken können hier „Downloadable ACLs“ und URL-Redirects angewandt werden. Bei ersterer Technik werden dem NAD dynamisch ACLs gesendet, die das NAD für den betreffenden Client anwendet. So kann beispielsweise die Client-Kommunikation auf bestimmte Ports oder Adressen eingeschränkt werden. Die zweite Technik dient dazu, den User bei Nutzung eines Web-Browsers auf eine spezielle Webseite zu leiten (z.B. im Falle alter Virensignaturen auf einen Server, der aktuelle Signaturen zum Download anbietet).

Das Durchreichen der Attribute des Clients (Patchlevel, Versionen, etc.) an den ACS geschieht dabei über einen geschützten Tunnel (EAPoUDP, PEAP-Session), der während der Integritätsprüfung zwischen Client und ACS aufgebaut wird. Auch hier ist eine periodische Wiederholung der Integritätschecks möglich.

3.2 Microsoft NAP

Network Access Protection (NAP) [2] ist Microsofts Variante der Integritäts-basierten Zugangskontrolle und verfolgt ähnliche Ansätze wie Cisco NAC. Allerdings ist NAP bisher kein produktives Feature, da es erst mit Microsoft Longhorn/Vista eingeführt wird. Auch Microsoft implementiert verschiedene Lösungsansätze.

Als Policy-Server kommt ein Longhorn-basierter Rechner zum Einsatz. Als NAP Client wird zunächst nur Vista agieren, später ist auch Unterstützung für Windows XP geplant. Das NAP Konzept führt im Vergleich mit Server 2003 eine Reihe von neuen Komponenten ein. Eine zentrale Rolle spielt der NPS (Network Policy Server), bis dato der Microsoft IAS. Microsoft Clients (Vista) werden zukünftig mit einem NAP Enforcement Client (EC) ausgeliefert, der eine ähnliche Funktion besitzt wie der Cisco Trust Agent. In einigen Fällen wird dynamisch ein „Health“-Zertifikat ausgestellt werden, falls ein Client den Integritätskriterien genügt und für den Zugriff auf bestimmte Services ein derartiges Zertifikat erforderlich ist. Zum Ausstellen dieser Zertifikate dient der Health Certificate Server (HCS). Nicht-integre Clients werden an sog. Remediation Server verwiesen, um beispielsweise aktuelle Patches oder Signaturen beziehen zu können.

Microsoft implementiert 4 NAP Varianten:

- ▶ IEEE 802.1x Authentifizierung

Während der 802.1x-Authentifizierung wird gleichzeitig die Integrität des Clients geprüft. Welche konkreten EAP-Varianten unterstützt werden, ist bisher nicht klar. In jedem Falle wird PEAP unterstützt werden. Allerdings hat Microsoft das EAP-Framework in Longhorn/Vista deutlich generischer gestaltet, so dass eine breite Unterstützung verschiedenster EAP-Varianten zu erwarten ist. Bisher ist

nicht klar, ob diese NAP-Variante auch für Windows XP implementiert wird.

▶ IPsec

Verlangt ein Server vom Client eine IPsec-gesicherte Verbindung, so muss der Client zunächst dynamisch ein Zertifikat über den Health Certificate Server beziehen. Das Zertifikat wird nur dann ausgestellt, wenn der HCS im Zusammenspiel mit dem NPS die Integrität des Clients bestätigen kann. Anderenfalls kann der Client nicht mit dem gewünschten Zielsystem kommunizieren. Das Beziehen des Zertifikates ist web-basiert und geschieht über https.

▶ VPNs

Bei Einwahl über VPN (L2TP/IPsec, PPTP) wird neben der Authentifizierung zusätzlich ein Integritätscheck vollzogen. Die Authentifizierung findet gegen den NPS statt.

▶ DHCP

Diese (sicherheitstechnische schwache) Variante greift dann, wenn der Client eine IP-Adresse von einem Microsoft DHCP-Server beziehen möchte. Der DHCP Server interagiert mit dem NPS, um den Integritätsstatus zu beurteilen und um anschließend je nach Status bestimmte IP-Adressen und weitere verwandte Einstellungen (Router, DNS) an den Client zu vergeben.

3.3 TNC

Trusted Network Connect (TNC) [3] ist ein Ansatz der Trusted Computing Group (TCG), Endpunkt-Integrität unter optionaler Zuhilfenahme eines TPM Chips (Trusted Platform Modul) zu realisieren. Es handelt sich hierbei nicht um eine konkrete Implementierung sondern vielmehr um ein Framework, mit dem Ziel, einheitliche Schnittstellen zu spezifizieren, um letztlich Interoperabilität zwischen einzelnen Implementierungen zu erlangen. Die TNC Architektur zeigt deutliche Parallelen zu den Standardisierungsbemühungen der IETF (siehe Kapitel 4). Konkrete Implementierungen der TNC Architektur sind beispielsweise von Funk (mittlerweile zu Juniper gehörend) verfügbar.

Auch bei TNC handelt es sich wiederum einen Agenten-basierten Ansatz mit zentralen Policy-Servern und Enforcement auf den jeweiligen Access Devices.

Im Kontext von TNC ist der Client, der Zugang zum Netzwerk zu erlangen versucht, ein sog. Access Requestor (AR). Auf dem AR laufen drei unabhängige Softwarekomponenten. Die Komponente „Integrity Measurement Collector“ (IMC) sammelt Informationen über die Integrität des Client. Die Architektur sieht ausdrücklich mehrere IMCs verschiedener Hersteller auf einem System vor. Die „TNC Client“ Komponente dient als Kollektor für die gelieferten Ergebnisse der IMCs. Der „Network Access Requestor“ wiederum kümmert sich um den unmittelbaren Netzwerkzugriff und um den Versand der Informationen des TNC Client.

Auf der Gegenseite gibt es ein oder mehrere zentrale Instanzen (Policy Decision Points, PDP), die über den Zugang eines Clients zum Netzwerk entscheiden. Die vom AR gelieferten Daten über den Zustand eines Clients werden von sog. Integrity Measurement Verifiers (IMV) bzgl. Integrität geprüft. Die IMVs laufen dabei einem TNC Server.

Als vermittelnde Instanz zwischen AR und PDP tritt der sog. Policy Enforcement Point (PEP) in Erscheinung. Hier wird auch die Entscheidung des PDP umgesetzt. In der Praxis ist ein PEP etwa ein Switch, Wireless Access Point oder ein VPN Gateway.

Die TNC Architektur ist in Abbildung 1 noch einmal zusammenfassend dargestellt.

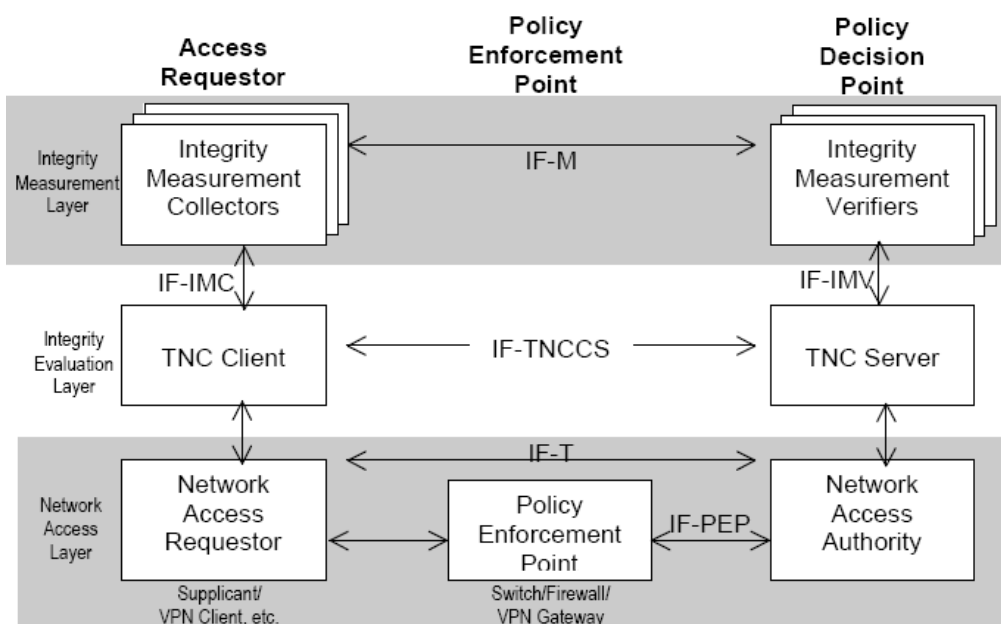


Abbildung 1 - TNC Architektur (Quelle: TCG)

3.4 Weitere Hersteller

Es existieren darüber hinaus eine Reihe von weiteren Produkten, wie die „ID Aware DHCP Solution“ von Infoblox [5], „Endforce Enterprise“ von Endforce [4], der „Lockdown Enforcer“ von Lockdown [7], der „Policy Enforcer“ [8] aus dem Portfolio der Firma McAfee, die Juniper Lösung „Unified Access Control“ [6] sowie die Lösungen anderer Hersteller, wie z.B. Mirage Networks, Nevis, Senforce, StillSecure, Symantec oder Vernier, die im Rahmen dieses Whitepapers nicht betrachtet werden können. Die meisten dieser Lösungen nutzen aber prinzipiell die oben vorgestellten Mechanismen in der einen oder anderen Kombination.

4 Standardisierung

Die verschiedenen NAC Lösungen sind weitestgehend inkompatibel. Viele Hersteller (vor allem Hersteller von Antiviren-Produkten) integrieren zz. einfach mehrere APIs (z.B. Cisco und Microsoft), um kompatibel zu sein.

Angesichts der seit längerem andauernden Kompatibilitäts-Probleme gibt es innerhalb der IETF Bestrebungen, eine Standardisierung zu erreichen. Dazu wurde die NEA Group (Network Endpoint Assessment) ins Leben gerufen. Ein erster Draft zum „Problem Statement“ existiert bereits [9]. Nach dessen Verabschiedung sollen Proposals für konkrete Protokolle erarbeitet werden. Weiterhin ist zurzeit ein Entwurf in Arbeit, der sich mit generellen Anforderungen an „Network Endpoint Assessment“ beschäftigt [10]. Vergleicht man die in Abbildung 2 dargestellten Architektur der NEA Group mit der der TNC, so sind hier viele Parallelen erkennbar. Dies ist nicht unbedingt verwunderlich, da Juniper bei beiden Ansätzen maßgeblich beteiligt ist.

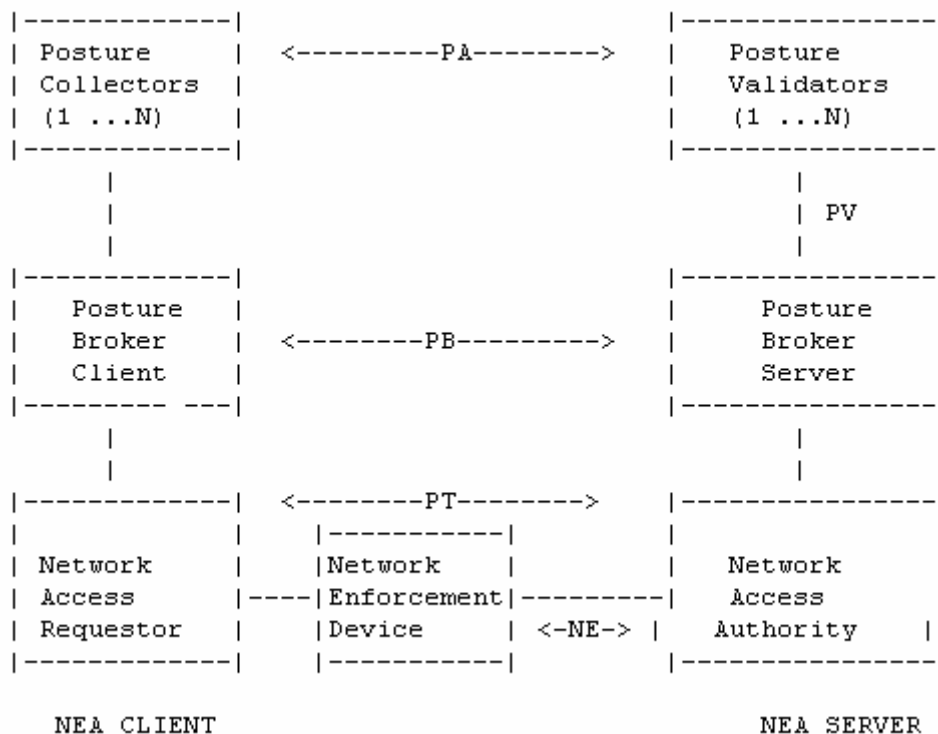


Abbildung 2 - NEA Architektur (Quelle: IETF NEA Group)

Auch die Arbeiten der Trusted Computing Group können als Standardisierungsbemühungen betrachtet werden. Das selbsterklärte Ziel der TCG ist die Entwicklung und Verbreitung von offenen und herstellernerneutralen Industriestandards. Da viele namhafte Hersteller in der TCG vertreten sind, ist durchaus mit einer breiten Akzeptanz und Verbreitung der TNC Technik zu rechnen, zumal hier explizit die optionale Nutzung eines TPM-Chips zur Integritätssicherung vorgesehen ist – und TPM

Chips werden derzeit vermehrt in Standardprodukten (z.B. IBM/Lenovo Laptops) serienmäßig integriert.

Seit Herbst 2006 gibt es auch von Microsoft und Cisco eine Verlautbarung, man wolle zusammenarbeiten und Kompatibilität zwischen NAP und NAC erreichen[11]; jedoch ist dies nur bedingt und vor allem clientseitig gegeben. Microsoft wird den Cisco Trust Agent mit dem eigenen NAP Client integrieren und mit Vista ausliefern bzw. entsprechende Updates zur Verfügung stellen. Auch soll ein von Cisco entwickeltes EAP-FAST-Modul (inkl. EAPoUDP) über den Windows Update-Dienst nachrüstbar sein. Im Gegenzug soll dann die Schnittstelle des Microsoft NAP Enforcement Clients das universelle Interface werden, an dem sich clientseitig third-party Produkte wie Virens Scanner in das System einbinden lassen. Windows XP Rechner müssen aber auch in Zukunft weiter mit zwei getrennten Agenten für NAC und NAP vorlieb nehmen. Serverseitig soll der Microsoft NPS die Überprüfung koordinieren, die Durchsetzung der Zugriffskontrolle an den Netzwerkgeräten (Switches, Routern, etc.) wird aber weiterhin nur über den Cisco ACS erfolgen. Zwar beinhaltet eine solche integrierte Architektur immer noch mindestens einen Server mehr, als ein Anwender sich wünschen würde (nämlich einen Cisco ACS *und* einen Microsoft NPS), aber die Tatsache, dass das entsprechende Whitepaper existiert, lässt zumindest erkennen, dass ein Markterfolg der NAC/NAP-Technologie nur zu erwarten ist, wenn zum einen gemeinsame Protokoll-Standards existieren und zum anderen Rechner und Netzwerkkomponenten-Hersteller zusammen an einem Strang ziehen.

5 Bewertung der Sicherheit

Zuletzt auf der Black Hat USA 2006 von Ofir Arkin [12] vorgetragene Zweifel an der Sicherheit von NAC müssen differenziert betrachtet werden. Es ist ohne Zweifel richtig (aber auch allgemein bekannt), dass insbesondere die DHCP-basierten Verfahren zur Zugangssteuerung z.B. durch die Nutzung von statischen IP-Adressen leicht zu umgehen sind. Gleichwohl stellen diese einzelnen Beobachtungen keineswegs das gesamte Konzept in Frage. Die Nutzung von DHCP kann mehr als ein „Schnellschuss“ für die kostengünstige Umsetzung in bestehenden Netzwerken betrachtet werden. Es existieren heute bereits geeignetere und bislang unwiderlegt sicherere Methoden zur Zugangssteuerung, namentlich IEEE 802.1x-basierte Verfahren.

Es ist weiterhin unbestritten, dass die Einführung von NAC in einem Unternehmensnetz eine komplexe Aufgabe ist, insbesondere, da alle Netzwerkkomponenten und Clients gleichermaßen davon betroffen sind, und dass insbesondere in der Migrationsphase durch Legacy-Geräte verursachte Lücken im Schutzkonzept bleiben können.

Trotzdem stellt alleine die grundsätzliche Tatsache, dass vor dem Netzwerkzugang erst einmal die Identität *und* die Integrität geprüft werden, eine neue Qualität dar, die entsprechend positiv bewertet werden sollte. Ebenso wie z.B. Firewalls und Virens Scanner Kinderkrankheiten und eine lange Entwicklungsgeschichte haben und immer noch ständig weiter-

entwickelt werden, so wird heute niemand mehr deren Nützlichkeit in einem integrierten Sicherheitskonzept abstreiten wollen.

Es steht zu erwarten, dass in dem Maße, wie NAC-Verfahren sich zum Schutz von sensiblen Netzwerken etablieren, auch entsprechend verfeinerte Angriffsverfahren entwickelt werden. Insbesondere die Integrität der Agenten auf den Systemen ist ein weiterer möglicher Schwachpunkt. Ein Angreifer könnte versuchen, die Kontrolle über den Agent zu übernehmen und der NAC-Schnittstelle die Werte eines unmanipulierten Rechners vorzutauschen, so wie heute bereits root-kits versuchen, sich zu verstecken. Hier kommen dann andere sich entwickelnde Technologien wie *Secure Booting* und *Trusted Computing* ins Spiel. Denn wenn es gelingt, die Authentizität eines Agents und seiner Module über das Netzwerk zu überprüfen, können auch diese Lücken geschlossen werden.

6 Fazit und Ausblick

Zusammenfassend lässt sich sagen, dass Network Access Control eine konsequente Weiterentwicklung verschiedener Sicherheitstechnologien ist, die Authentifikation, Zugangskontrolle und Rechnerintegrität sinnvoll zusammenfasst und damit ein wichtiges Problem bei der Absicherung von Firmennetzen adressiert. In Zeiten immer mobilerer Endgeräte und flexiblerer Produktionsabläufe wird es damit möglich, das Intranet besser abzusichern, ohne dabei die Gerätemobilität einschränken zu müssen.

Die aktuell verfügbaren Implementierungen der NAC-Technologie haben zurzeit noch verschiedene Defizite:

- ▶ Sie sind z.T. nur als Spezifikationen oder Beta-Versionen verfügbar. Dies betrifft insbesondere Microsofts NAP, das erst mit Vista im Client-Bereich eingeführt wird, und das Trusted Network Connect der TCG.
- ▶ Sie sind nicht oder nur sehr eingeschränkt interoperabel. Nur homogene Lösungen eines Herstellers sind zurzeit marktreif. Das Zusammenspiel von Komponenten verschiedener Hersteller kann nur als experimentell betrachtet werden.
- ▶ Die Auswahl an unterstützten Komponenten ist klein. Es werden weder alle gängigen Client-Betriebssysteme noch die meisten Netzwerk-Komponenten unterstützt. Eine Nachrüstung ist nur für neuere Systeme möglich.
- ▶ Bestimmte verwendete Methoden, insb. die DHCP-basierten Verfahren, können nur als Zwischenlösung betrachtet werden und sind von Security-Gesichtspunkten her eher fragwürdig.
- ▶ Die Konfiguration und das Management einer NAC-Lösung ist komplex. Insbesondere die Erarbeitung und Pflege von NAC-Policies in Verbindung mit aktuellen Client-Agent-Modulen eröffnen einen Markt für Security-Dienste (ähnlich den heutigen Virensclannern), auf dem es aber bislang noch keine umfassenden Angebote gibt.

In Anbetracht der Marktmacht der Protagonisten und der potentiellen Chancen der NAC-Technologie erscheinen diese Probleme aber überwindbar. Insbesondere mit dem langsamen Zusammenwachsen der Lösungen von Cisco und Microsoft wird sich im Laufe des Jahres 2007 eine Plattform entwickeln, auf der auch third-party Produkte Erfolg versprechend aufsetzen können. Dann wird NAC auch eine technologische Reife entwickelt haben, die einen großflächigen Einsatz in Produktivnetzen möglich und sinnvoll erscheinen lässt.

Es gibt aber auch gute Gründe, sich bereits jetzt mit NAC zu beschäftigen. Wer heute entweder die Vor- und Nachteile einer Vista-Migration abwägt, sollte diesen neuen integralen Bestandteil einer erheblich verbesserten Sicherheitsarchitektur des Systems mit betrachten. Ebenso sollte jeder, der heute eine VPN und/oder IEEE 802.1x-Infrastruktur neu aufbaut, NAC als konsequente Weiterentwicklung und nächsten Schritt der Zugangskontrolle im Auge behalten.

Referenzen

- [1] <http://www.cisco.com/go/nac>
- [2] <http://www.microsoft.com/nac>
- [3] <https://www.trustedcomputinggroup.org/groups/network/>
- [4] <http://www.endforce.com>
- [5] <http://www.infoblox.com>
- [6] <http://www.juniper.com>
- [7] <http://www.lockdownnetworks.com>
- [8] <http://www.mcafee.com>
- [9] <http://tools.ietf.org/id/draft-thomson-nea-problem-statement-03.txt>
- [10] <http://tools.ietf.org/id/draft-khosravi-nea-requirements-01.txt>
- [11] http://download.microsoft.com/download/d/0/8/d08df717-d752-4fa2-a77a-ab29f0b29266/NAC-NAP_Whitepaper.pdf
- [12] <http://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html#Arkin>