Network Access Control

Leitfaden und Best Practice

COMCO AG

27.03.2009

Dipl.-Ing. Friedhelm Zawatzky-Stromberg

Inhaltsverzeichnis

Network Access Control

Einleitung

Die Planung und Implementierung von Network Access Control (NAC) ist eine sehr komplexe Angelegenheit und bedarf einer ausgiebigen Betrachtung der am Markt verfügbaren Systeme um deren Leistungsfähigkeit, Notwendigkeit und Zukunftssicherheit zu beurteilen. Für viele ist der Markt unüberschaubar, da sich viele Systeme nicht unbedingt miteinander vergleichen lassen und dennoch dem Thema NAC zuzurechnen sind. Andere hingegen sind eindeutig dem Thema NAC zuzuordnen, decken aber lediglich einen geringen Teil des Bereichs ab, was nicht immer auf den ersten Blick ersichtlich ist. Darüber hinaus besteht NAC nicht nur aus Hardware und Software, hier kommen wesentliche Anforderungen hinsichtlich der Organisation auf die technischen Abteilungen zu, die nicht nur das gesamte Unternehmen mit all seinen Anforderungen, sondern auch die gesetzlichen Vorgaben berücksichtigen muss. Ein NAC-Projekt kann dabei sehr schnell scheitern, wenn es ausschließlich auf der technischen Ebene angesiedelt wird.

Die einzelnen Prozesse von NAC

Network Access Control (NAC) ist mittlerweile ein geläufiger Begriff in der IT. Es handelt sich dabei um eine ganze Reihe von Sicherheitsmaßnahmen und Prozessen zum Schutz der gesamten Netzwerkinfrastruktur und darüber transportierter Daten eines Unternehmens. Dies ist einerseits die Überwachung der physikalischen Zugänge zum Netzwerk mittels Hardwareerkennung und Authentifizierung, andererseits Benutzerauthentifizierung, Schutz vor Viren und Würmern, Erkennung nicht zugelassener Applikationen und Patchlevelmanagement und und und … Die Aufzählung lässt sich um Etliches erweitern. Die einzelnen Prozesse von NAC können wie folgt charakterisiert und prägnant beschrieben werden:

Erkennung - Lokalisierung - Authentisierung

Die Erkennung und Lokalisierung von neuen Netzwerkgeräten unabhängig von deren Zugangspunkt innerhalb des Netzwerks. Dies schließt den Zugangsbereich der drahtlosen Netzwerke (WLAN) ein.

Die eindeutige Identifizierung von Benutzern und Geräten, um deren Identität möglichst eindeutig sicherzustellen.

Assessment

Schwachstellenprüfung der Hardware und Software zur frühzeitigen Erkennung von Sicherheitslücken gemäß vorgegebener Unternehmensrichtlinien.

Authorization

Zugangssteuerung der Benutzer und Geräte auf vordefinierte Bereiche gemäß den vorhergehenden Überprüfungen. (Gast-, Quarantäne- oder Produktivbereiche)

Remediation

Problembehebung der zuvor festgestellten Sicherheitsmängel in einer möglichst interaktiven Kommunikation mit dem Benutzer. Hier werden beschränkte Zugriffe, Tipps, Anleitungen und Depots für die Herstellung einer den Anforderungen entsprechenden Konformität zur Verfügung gestellt werden.

Monitoring

Auch nach der Überprüfung und Zulassung zum Produktivbereich muss eine permanente Überwachung auf Einhaltung der Richtlinien erfolgen. Hierzu zählen auch die Angriffserkennung durch Adressmanipulation und Angriffe auf die Infrastrukturkomponenten (Router und Switche).

Im Folgenden werden die einzelnen Prozesse betrachtet, Lösungen analysiert, miteinander verglichen und bewertet. Diese Bewertung berücksichtigt nicht zuletzt die Wirtschaftlichkeit und den Nutzen von NAC-Systemen. Hierbei ist das angestrebte Sicherheitslevel insbesondere abhängig von den vorhandenen oder aufzuwendenden Ressourcen. Ebenso sind, neue Technologien zu berücksichtigen, die im Zuge der zyklischen Erneuerung eines Netzwerks ohnehin zum Einsatz kommen würden. In jedem Fall sollte das Ganze unter dem Gesichtspunkt der wirtschaftlichen Betrachtung stehen, Sicherheit unterliegt auch einer Kosten-Nutzen-Optimierung und sollte letztlich auch bezahlbar sein.

Voraussetzungen schaffen

NAC ist kein isoliertes Thema der IT-Abteilung, sondern ein umfangreiches Projekt, welches weitreichende Konsequenzen für die tägliche Arbeit fast aller Mitarbeiter eines Unternehmens zur Folge haben kann. Umso wichtiger ist eine konkrete Vorbereitung, die im Wesentlichen eine Herausforderung für Geschäftsleitung, IT-Abteilung und Sicherheitsverantwortliche darstellt. Der spätere Erfolg solch eines Projektes hängt davon ab, inwieweit jede der zuvor genannten Abteilungen von der Notwendigkeit eines solchen Systems überzeugt ist und die daraus resultierenden Aufgaben erledigt. Deshalb muss in erster Linie die Überzeugung bei allen Verantwortlichen geschaffen werden, dass ein NAC-System nicht dazu dient, Mitarbeiter zu überwachen, sondern das Unternehmen, Mitarbeiter und auch Kunden vor Datenverlust, -missbrauch, -manipulation und Spionage zu schützen. Oftmals ist damit für IT-User auch die Notwendigkeit verbunden, sich einer entsprechenden Disziplin zu unterwerfen, umso wichtiger ist daher die sorgfältige Planung aller notwendigen Schritte.

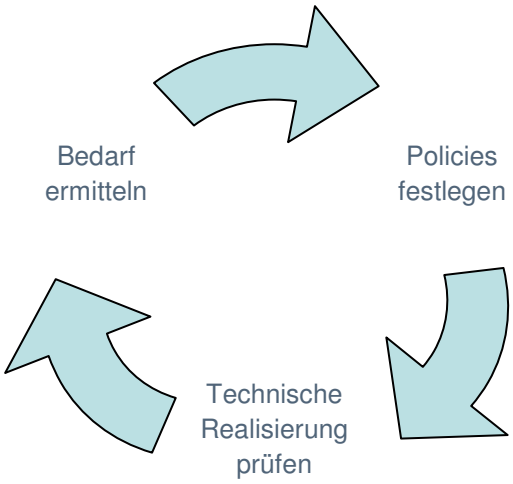
Zunächst sollte eine komplette Bestandsaufnahme der verfügbaren Infrastruktur erfolgen, somit kann ein Überblick über technische Realisierungsmöglichkeiten und notwendige Anschaffungen erfolgen. Als nächstes sollten die erforderlichen Ziele definiert werden, die festlegen wann und in welchen Schritten die einzelnen Prozesse von NAC implementiert werden können. Je nach Größe und Struktur eines Unternehmens kann sich eine vollständige Implementierung über Jahre hinausziehen und schnell unübersichtlich werden. Andererseits kann durch vorhandene Technologie vielleicht schon der erste Schritt zur Erkennung und Authorisierung (pre-connect) durchgeführt werden, ohne neue Infrastruktur anschaffen zu müssen. Damit ist noch keine

vollständige Implementierung von NAC erfolgt, aber ein erheblicher Schritt in Richtung Sicherheit getan.

Alle weiteren Schritte können sukzessive erfolgen und unterliegen keiner festen zeitlichen Zuordnung.

Im Anschluss daran können weitere Aktivitäten hinsichtlich Assessment und Remediation erfolgen, die vermutlich komplexesten, langwierigsten und kostenintensivsten Prozesse. Hier kommt es darauf an, die geeigneten Methoden zur Erkennung und Behebung von Schwachstellen zur Durchsetzung der unternehmensweiten Richtlinien zu ermitteln und zu implementieren. Hier wird festgelegt, welche Applikationen auf den Endsystemen betrieben werden, ob alle notwendigen Systeme mit den aktuellen Patchleveln ausgerüstet sind und ob irgendwelche unberechtigten Prozesse oder Applikationen aktiviert wurden. All dies setzt eine sorgfältige Planung der erforderlichen Policies durch die eingangs erwähnten Abteilungen voraus.

Konzepte erstellen



Wie bereits erwähnt wird eine große Herausforderung die Zusammenarbeit der Bereiche Geschäftsführung, Datenschutz, Security- und IT-Abteilung eines Unternehmens darstellen. Hier wird eine enge und genaue Abstimmung bzgl. der Anforderungen, Realisierbarkeit und wirtschaftlicher Abwägungen erfolgen müssen. Hier muss das Ziel verfolgt werden, mit wirtschaftlich vertretbaren Möglichkeiten unter Einbeziehung der vorhandenen Infrastrukturen und Ressourcen, die größtmögliche Sicherheit in einem vertretbaren Zeitrahmen zu implementieren. Das Angebot an NAC-Lösungen ist in den vergangenen Jahren stark gewachsen, es handelt sich aber immer noch um einen recht jungen Markt, der sich vor Allem technologisch noch stark entwickeln wird. Hier gibt es zurzeit keine Komplettlösung, sondern eine Sammlung aus Einzellösungen und Komponenten, die jeweils nur Teilbereiche abdecken. Die Abstimmung der Hersteller untereinander wird zwar immer häufiger mit Schnittstellen realisiert, diese sind jedoch meistens mit „sieben Siegeln“ behaftet und werden oftmals nur als Alibi zur Verfügung gestellt. Auch Hersteller, die mit ihrem Produktportfolio die gesamte Thematik NAC abdecken, weisen Lücken auf und bieten ein ganzes Sammelsurium an Produkten deren Zusammenspiel oftmals nicht gewährleistet ist.

Hier ein Auszug möglicher Fragen, die einem NAC-Projekt vorausgehen sollten:

1. Gibt es Regelungen, die den Zugriff auf das Netzwerk für Mitarbeiter, Unternehmensgäste und Freiberufler definieren?

2. Ist eine Erkennung und Lokalisierung von Geräten auf Basis der MAC-Authentifizierung möglich und erforderlich?
3. Besteht die Notwendigkeit einer Benutzer-Authentifizierung beim Netzwerkzugang – etwa mittels des Standards 802.1x – und ist sie realisierbar?
4. Dürfen Benutzer auf alle Ressourcen zugreifen oder muss über VLAN-Steuerung eine logische Trennung erfolgen?
5. Sind dafür die Möglichkeiten in der Infrastruktur bereits gegeben?
6. Ist eine Überwachung der Software-Stände und deren Aktualität auf den Endsystemen erforderlich?
7. Gibt es hierfür ein Patchmanagement und ist dafür ein Quarantänenetz vorgesehen?
8. Welche Voraussetzungen gelten für Gäste und Mitarbeiter anderer Unternehmen etwa durch ein Gastnetz?
9. Bedarf es einer Überwachung des Gastnetzes?
10. Soll auch für Gäste eine Überprüfung und Patchmanagement zur Verfügung gestellt werden?
11. Werden im Unternehmen zeitliche Zugangsbeschränkungen praktiziert?
12. Gibt es Regelungen hinsichtlich „Quality of Service“ für Benutzer?
13. Bestehen Verfahrensweisen zur Analyse des Benutzerverhaltens im Verdachtsfall (sFlow/netFlow)?
14. Werden Methoden und Techniken eingesetzt, die bei einem Netzwerkzugang spezielle Gerätetypen (z.B. Router, VoIP, WLAN) automatisch erkennen?
15. Nutzt das Unternehmen Lösungen, die auch solche Infrastrukturangriffe und Konfigurationsänderungen bei Infrastrukturkomponenten erkennen, die nicht detailliert genug in den einzelnen NAC-Prozessen definiert sind?

All diese Fragen zeigen auf, dass NAC nicht so einfach einzugrenzen ist und schon gar nicht durch eine Einzelkomponente implementiert werden kann. Es zeigt auch, dass es äußerst wichtig ist zu verstehen, dass die gesamte Infrastruktur (Applikationen, Router, Switche, Server, Clients, Drucker, WLAN…) darauf abgestimmt sein muss und damit jede Abteilung einen Beitrag zu NAC leisten kann und muss.

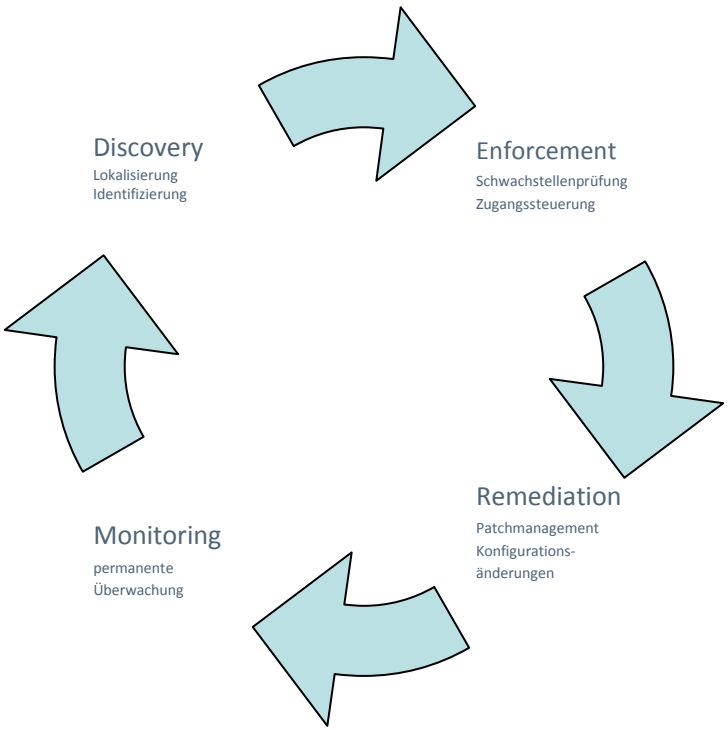
Darüber hinaus muss eine klare Regelung existieren, wer wen überwacht. Gerade in lokalen Netzen sei die Frage erlaubt, ob Administratoren, die die Netzwerkinfrastruktur betreiben, an der Überwachung zur Einhaltung von Policies beteiligt sein sollen und dürfen. Schließlich werden für die Überwachung in lokalen Netzwerken Systeme verwendet, die zumindest Teile der Tätigkeiten von Administratoren überwachen. Zum Beispiel Konfigurationseinstellungen auf Router und Switche. Sollte es hier, und das muss keine böse Absicht sein, zu beabsichtigten oder unbeabsichtigten Fehlkonfigurationen kommen, kann das möglicherweise zu Interessenkonflikten kommen. In manchen Unternehmen genießen Administratoren Sonderstellungen, die nicht immer allen Beteiligten bekannt sind. Dies könnte hohes Konfliktpotential beinhalten.

Ein weiteres Problem besteht darin, bei der Erkennung von Geräten zu erfahren, um welche Art von Gerätetyp es sich handelt und wie bei Erkennung eines solchen Systems zu verfahren ist. Die Schwierigkeit besteht darin, dass nur ein Teil der erkannten Systeme aus Endgeräten wie Laptops und PCs besteht. Ein erheblicher Teil der erkannten Endgeräte besteht aus Servern, Druckern, WLAN, VoIP, Routern etc., die ihrerseits redundante Systeme (Cluster) bilden können. Die Handhabung solcher Systeme ist je nach Hersteller und verwendeten Protokollen durchaus eine große Herausforderung um Fehlalarme auszuschließen. Darüber hinaus finden an solchen Systemen ständig Änderungen, durch Wartungsarbeiten und Failover statt. Dies stellt sich gerade bei der Erstkonfiguration von NAC-Systemen oftmals als sehr problematisch dar. Fehlinterpretationen, die eine Isolierung eines solchen Systems zur Folge hätte, könnten äußerst problematisch sein. Hier sind Systeme notwendig, die eine Reihe von Hilfestellungen bieten, da eine automatische Erkennung oftmals nicht gewährleistet werden kann.

Erschwerend kommt hinzu, dass in den meisten Unternehmen Geräte und Applikationen unter unterschiedlicher administrativer Kontrolle stehen und die Abteilungen häufig autark voneinander arbeiten. Hier muss bei der Einrichtung und beim Betrieb von NAC Systemen auf eine entsprechende Berechtigungsstruktur für den Betrieb der NAC-Systeme geachtet werden.

Ein weiterer wesentlicher Aspekt ist die Kenntnis darüber, wer auf welche Ressourcen zugreifen darf. Der Zugriff von Benutzern auf Ressourcen ist häufig in Verzeichnisdiensten bereits definiert.

Diese Informationen können somit in die Planung einbezogen werden. Der physikalische Zugriff auf beschränkte Bereiche und die zeitliche Eingrenzung lässt sich meistens daraus ableiten.



Bereits zu Beginn eines NAC-Projektes ist es äußerst wichtig, Informationen über alle im Netzwerk aktiven Geräte zu erhalten, da dies wichtige Informationen für ein NAC-Projekt liefert. Je leistungsfähiger ein System zur Erkennung, Lokalisierung und Identifizierung ist, desto besser lässt sich ein NAC-Projekt vorbereiten. Häufig sammeln solche Systeme Informationen, die bis dahin nicht bekannt waren und somit einen wertvollen Beitrag zur weiteren Planung liefern können. Bestens geeignet sind Systeme die im Bereich Netz- und Systemmanagement angesiedelt sind und detaillierte Informationen auch über die Infrastruktur des Netzwerks liefern können.

Implementierung Step by Step

Die Implementierung von NAC lässt sich in einzelnen Schritten durchführen, da die einzelnen Prozesse relativ unabhängig voneinander sind. Dies erleichtert die Implementierung nach den zuvor ermittelten Prioritäten.

Schritt 1: Erkennung – Lokalisierung - Authentifizierung

Im ersten Schritt soll eine Erkennung, Lokalisierung, Inventarisierung und Identifizierung der Hardware erfolgen. Hierbei ist zu berücksichtigen, dass die Erkennung alle Bereiche des lokalen Netzwerks berücksichtigen muss. Die Erkennung sollte so früh wie möglich erfolgen um weitergehende Maßnahmen einleiten zu können. Somit ist ein Wesentlicher Schritt getan, es bestehen Informationen über alle aktiven Geräte im Netzwerk. Wir wissen, welches Gerät an welchem Port und Switch im Unternehmen angeschlossen ist. Eine Aktualisierung muss nach Wechseln des Standortes und Adressänderung (DHCP) erfolgen. Vorteilhaft wäre die Information über die Ersterkennung und die letzte Erkennung. Die Erkennung und Lokalisierung von Endsystemen ist die Grundlage eines jeden NAC-Projektes und sollte bereits vor der eigentlichen Planungsphase erfolgen. Schließlich muss man wissen, welche Systeme sich wo im Netzwerk befinden. Die Authentifizierung des Systems ist ein weiterer Bestandteil der ersten Phase, allerdings erst bei bereits implementiertem NAC. Die Identifizierung der Endgeräte erfolgt sinnvollerweise zunächst über die MAC- und IP-Adresse. Eine mögliche Manipulation dieser Adressen ist zwar möglich, setzt aber zunächst einmal weitere detaillierte Kenntnisse eines potentiellen Angreifers über das Netzwerk voraus. Je eindeutiger eine Identifizierung ist, desto sicherer ist das Gesamtsystem. Eine qualitative Aussage hierzu ist äußerst schwierig und mit Vorsicht zu genießen. Wer hier glaubt, sich auf Herstelleraussagen verlassen zu können, wird eigentlich permanent eines Besseren belehrt. Selbst eine verschlüsselte Kommunikation mit installierten Agenten und Passwortschutz läßt sich gegebenenfalls umgehen. Ein Angreifer wird zunächst einmal physikalischen Zugang zum Netzwerk benötigen. Dazu wird der Angreifer sowohl zugelassene IP- und MAC-Adresse benötigen, die an dem entsprechenden Switchport betrieben werden dürfen. Für die erste Identifizierung eines Systems sollte dies genügen. Weitere Überprüfungen können ggf. in anderen NAC-Systemen erfolgen. Die Frage der hier zu verwendenden Systeme richtet sich nach Aufwand, Budget und der Schutzbedürftigkeit der Ressourcen.

Für eine hohe Schutzbedürftigkeit würde beispielsweise eine Lösung nach dem Standard 802.1x sinnvoll erscheinen, dabei muss jedoch berücksichtigt werden, dass eine solche Implementierung ggf. den Austausch der gesamten Switche voraussetzt. Der damit verbundene finanzielle Aufwand wird vermutlich das Projekt zum Scheitern bringen, zumal damit nur ein Teilbereich eines NAC-Projektes abgedeckt wird.

Mögliche Systeme im Überblick:

802.1x mit Radius

Die wohl zurzeit sicherste Methode ist ohne Zweifel eine portbasierende Authentifizierung (via RADIUS) nach dem Standard 802.1x für Benutzer und Geräte. Die Lösung hat den Vorteil, dass noch bevor ein Zugriff auf das Netzwerk gewährt wird, eine Authentifizierung am Switchport

durchgeführt wird. Bei dieser Authentifizierungsmethode sind allerdings mindestens drei Komponenten (Client, Switch und Radius Server) erforderlich, die aufeinander abgestimmt sein müssen.

Die Schwierigkeit, diesen Standard zu implementieren besteht darin, dass nicht alle Endgeräte die Authentifizierungsmethode unterstützen (ältere Drucker, Scanner etc.). Darüber hinaus sind die Implementierungsmethoden der Switch-Hersteller nicht einheitlich und erschweren damit die Realisierung. Jegliche Änderungen an der Software der Switche müssen eingehend getestet werden um hier keine Überraschungen zu erleben. Der zu verwendende Radius Server muss hochverfügbar und redundant ausgelegt werden, da ein Ausfall die gesamte Kommunikation stören würde.

Die Endgeräte müssen den Standard nach Möglichkeit einheitlich unterstützen. Die ggf. installierten Agenten sollten einfach zu installieren und zu konfigurieren sein. Für einen unternehmensweiten Einsatz bei heterogener Umgebung ist der Standard 802.1x zurzeit noch schwer umzusetzen. Bei Anschaffung einer neuen homogenen Infrastruktur ist dies jedoch eine sinnvolle Alternative.
Bewertung: teuer – aufwendig – sicher

MAC-Authentifizierung

Als Alternative zu 802.1x ist die MAC-basierende Authentifizierung (via RADIUS), vor Allem für Netzwerkumgebungen mit älteren oder auch heterogenen Netzwerken eine mögliche Alternative.

Hierbei wird nur die bei Anmeldung ans Netzwerk erkannte MAC-Adresse vom RADIUS Server überprüft, bevor ein Netzwerkport freigeschaltet wird. Dies ist zwar kein hoher Sicherheitsstandard, bei älteren Endgeräten aber oftmals die einzige Möglichkeit eine Authentifizierung durchzuführen. In vielen Fällen reicht dies auch schon im ersten Schritt aus, da ggf. andere Überprüfungen des Endgerätes nachgeschaltet sind. Die Implementierung erfordert die gleichen Voraussetzungen für die Switche und den RADIUS-Server wie bei 802.1x.

Bewertung: mittlerer Kosten – mittlerer Aufwand – geringe Sicherheit

Web-basierende Authentifizierung

Mit dieser Authentifizierungsmethode ist die Eingabe von Benutzernamen und Passwort an einem eigens zur Verfügung stehenden Webserver erforderlich. Dies ist eine mögliche Alternative für Benutzer, bei denen keine Möglichkeit besteht einen Supplicant für 802.1x zu implementieren.

Bewertung: mittlere Kosten – wenig Aufwand – mittlere Sicherheit

Statische Port - / MAC- Zuordnung

Die statische Port / MAC Konfiguration sieht eine feste Zuordnung von MAC-Adressen und Switch-Ports vor. Dies ist eine sehr aufwändige Methode, da alle kommunizierenden Systeme in die Konfiguration eines jeden Switches eingetragen werden müssen. Jedes neue Gerät und jede Löschung würde eine Konfigurationsänderung auf dem Switch nach sich ziehen. Alles in Allem keine praktische Lösung und nur in kleinen Netzen ohne große Änderungen möglich.

Bewertung: günstig – aufwändig – geringe Sicherheit

Dynamische Port- / MAC -/ IP -Zuordnung mittels SNMP

Eine weitere Möglichkeit der Lokalisierung und Identifizierung von Endgeräten ist die Abfrage der Netzwerkinfrastruktur mittels SNMP. Hierbei wird die vorhandene Infrastruktur genutzt, um Daten über Endsysteme via SNMP auszulesen. Es ist kein Agent auf den Endgeräten notwendig und die gesamte Kommunikation erfolgt mit der Netzwerk-Infrastruktur (Switches und Router). SNMP ist ein weit verbreiteter Standard, der nahezu flächendeckend in Unternehmen Verwendung findet und mit Version 3 auch ausreichend sicher ist. Nahezu alle Netzmanagement-Systeme basieren hierauf. Die Daten werden zyklisch abgerufen und mit der Datenbank verglichen, um Änderungen bzgl. der MAC-, IP-Adresse oder der Lokation des Systems festzustellen und daraufhin weitere Aktionen einzuleiten. Die Leistungsfähigkeit der Systeme hängt davon ab, wie viele Daten über die Endsysteme gesammelt werden. Manche Systeme beschränken sich auf die Abfrage von Layer 2 basierenden Informationen, andere Systeme erweitern die Abfragen auf Layer 3 Informationen. Durch die Verwendung zusätzlicher Tools wie Port-Scanner, VoIP- und WLAN-Module, sFlow/netFlow oder Router-Module können solche Systeme sehr leistungsstark sein und ein Netzmanagement-System nahezu ersetzen. Ein Vorteil dieser Systeme liegt sicherlich in der Möglichkeit die gesamte Infrastruktur mit einzubeziehen und somit auch Schwachstellen auf Switche und Routern erkennen zu können. Dies ist bei fast allen anderen Lösungen bislang vernachlässigt worden. Die Zuverlässigkeit der gesammelten Informationen hängt im Wesentlichen vom Abfragezyklus der SNMP-Agenten ab. Bei dieser Methode ist durch den Zeitversatz der zyklischen Abfrage keine „real time“ Erkennung möglich. Manipulationen durch einen potentiellen Angreifer dauern in der Regel länger als ein paar Minuten, somit relativieren sich hier die Bedenken. Der Vorteil einer solchen Lösung liegt sicherlich darin, dass die zur Verfügung gestellten Informationen von Beginn an für ein NAC-Projekt erforderlich sind und nicht zwangsläufig Policies existieren müssen. Somit lohnt sich der Einsatz bereits vor Start eines NAC-Projektes und liefert auch im Nachhinein noch wichtige Informationen, die andere Systeme nicht zur Verfügung stellen. Bei Ausfall eines solchen Systems ist das Netzwerk nicht mehr geschützt, allerdings ist die Kommunikation nicht gestört und der Anwender bemerkt davon nichts.

Bewertung: günstig – mittlere Aufwand – mittlere Sicherheit

(abhängig von den implementierten Möglichkeiten)

Kerberos Snooping

Mit dieser Methode kann keine Lokalisierung von Endgeräten, sondern ausschließlich eine Authentifizierung von Benutzern vorgenommen werden. Hierzu ist es erforderlich eine „inline“ – Komponente in den Datenstrom zum Anmeldeserver (Active Directory) einzurichten. Für eine Lokalisierung und Authentifizierung von Endgeräten ist diese Variante nicht ausreichend, sondern eher als Ergänzungsprodukt zu bezeichnen.

Bewertung: günstig – geringer Aufwand – mittlere Sicherheit

Zusammenfassung

Hiermit sind nicht alle Methoden aufgezählt, die zur Identifizierung und Lokalisierung in Netzwerken möglich sind, aber die gängigsten Methoden. Die Unterschiedlichkeit der Systeme sollte damit aber schon klar herausgestellt sein. Welche Methode die beste ist, kann hiermit aber auch nicht

beantwortet werden. Dies hängt nach wie vor vom Schutzbedarf, Budget und den vorhandenen Komponenten ab und erfordert daraufhin häufig eine Kombination der Systeme. Von allen vorgestellten Möglichkeiten bieten einige Systeme mit Dynamischer Port- / MAC -/ IP -Zuordnung mittels SNMP viele Zusatzfunktionen aus dem Netz-, System- und Adressmanagement und sind mit anderen Lösungen gut kombinierbar.

Schritt 2: Assessment

Aufgabe des Assessment ist es, die am Netzwerk angeschlossenen Endsysteme auf Schwachstellen im Betriebssystem und Applikationen zu prüfen. Hier wird im Detail darauf geachtet, welche Dienste aktiviert sind, ob das Betriebssystem und die Applikationen die neuesten Patches eingespielt haben und die notwendigen Sicherheitsapplikationen, wie Firewall und Antivirensoftware, aktiv sind und auf dem neuesten Stand gebracht wurden. Diese Überprüfungen sind nach den vorgegebenen Unternehmensrichtlinien zu implementieren. Die Durchführung des Assessments sollte bereits im Anmeldeprozess integriert sein, um das Endgerät den erforderlichen Ressourcen zuführen zu können. Dies geschieht in der Regel mit der Zuordnung in ein entsprechendes VLAN (Gast, Quarantäne, Produktion). Die Integration in den Anmeldeprozess ist allerdings noch nicht weit verbreitet, wird aber bei einigen Standards mittels API zur Verfügung gestellt (NAP, NAC…). Hier bleibt abzuwarten, wie sich dies durchsetzen wird. Die Realisierung des Assessments erfolgt durch eine zentrale Komponente (oder verteilte Systeme), die entweder via installiertem Agenten (temporär oder permanent) mit den Endgeräten kommuniziert, oder dies agentenlos mittels Scannertechnologie ausführt.

Eine agentenlose Lösung hat den Vorteil, keine Software auf den Endsystemen verteilen, konfigurieren und warten zu müssen. Dafür sind aber unter Umständen die Möglichkeiten der Informationsbeschaffung beschränkt und die zyklischen Abfragen der Endsysteme ein Hindernis (Performance). Die beschafften Informationen sind in einigen Fällen nicht sehr zuverlässig, verbessern sich aber mit jeder neuen Version. Ein unternehmensweiter zyklischer Scan bringt ein solches System unter Umständen schnell an seine Grenzen, da die Netzwerklast einfach zu groß ist. Hier in kurzen Zeitabständen Scans auf tausende von Geräten über hunderte von Ports zu konfigurieren ist kaum möglich. Es ist empfehlenswert, vorgefertigte Scans in unterschiedlichen Zyklen und wechselnden Bereichen zu konfigurieren. Das hält die Last in Grenzen und beschränkt die Informationen auf das Notwendigste.

Eine agentenbasierte Lösung verursacht hingegen einen geringen Netzwerkverkehr. Die Agenten benötigen allerdings Ressourcen auf den Endsystemen (Speicher, Prozessor). Es handelt sich dabei um eine Software, die automatisch im Hintergrund aktiv ist und das Endgerät permanent überwacht. Auch diese Agenten müssen zentral konfiguriert und gewartet werden. Nicht alle Endgeräte können mit einem Agenten ausgestattet werden (Drucker, Netzwerkkomponenten…).

Bewertung:

Agentenlos:

schnell zu implementieren – keine Ressourcen notwendig – große Netzwerklast – nicht realtime-fähig

Agentenbasierend:

lange Implementierungszeit – verlangt Ressourcen auf Client - wenig Netzlast – betriebssystemabhängig – realtime-fähig

Zusammenfassung:

Eine generelle Empfehlung hinsichtlich der Verwendung kann erst nach eingehender Kenntnis aller Rahmenbedingungen erfolgen. Auch hier spielen Budget, Schutzbedarf und Ressourcen eine wichtige Rolle. Vermutlich wird auch hier eine Kombination beider Systeme eine sinnvolle Lösung bedeuten. Es gibt auf dem Markt Hersteller, die z.B. Portscanner oder ähnliches bereits in Sicherheitslösungen integriert haben und somit nur eine Ergänzung von agentenbasierenden Systemen benötigt wird. In jedem Fall sind der Konfigurationsaufwand und die Pflege solcher Systeme nicht zu unterschätzen. Ein Blick der über die häufig geringen Anschaffungskosten hinausgeht ist hier besonders empfehlenswert. Da solche Systeme in den Anmeldeprozess mit eingebunden werden sollen, ist hier insbesondere darauf zu achten, wie der Hersteller dies realisiert.

Schritt 3: Authorisierung

Der Authorisierungsprozess ist der Prozess, der mit besonderer Sorgfalt geplant werden muss. Nicht umsonst scheuen sich viele Unternehmen diesen Prozess einzuführen, da es zu eklatanten Problemen kommen kann, wenn dieser Prozess versagt. Nicht nur einzelne Endgeräte, sondern gesamte Unternehmensbereiche oder wichtige Ressourcen können dabei gestört werden oder gar nicht mehr verfügbar sein. Trotzdem ist dieser Prozess unverzichtbar, da gerade dieser Prozess den größten Beitrag zum Schutz des Unternehmens beiträgt. Denn jegliche Erkenntnis darüber, dass ein schadhaftes Verhalten eines Endgerätes vorliegt nützt wenig, wenn das Problem nicht behoben wird. Eine unmittelbare Reaktion ist unerlässlich, ganz gleich, ob der Verursacher in einem Gastnetz isoliert wird, oder ganz vom Netz getrennt wird.

Welche Methode die sinnvollste ist, ergibt sich wie immer aus dem Budget, dem Schutzbedarf, der Ressourcen und der vorhandenen Infrastruktur. In diesem Fall hingegen kommt der vorhandenen Infrastruktur eine besondere Bedeutung, denn es ist sinnvoll den Authorisierungsprozess direkt am Switchport durchzuführen, dies ist schließlich der erste Zugangspunkt zum Netzwerk und dieser Methode wird sicherlich die Zukunft gehören. Natürlich gibt es auch Authorisierungsmethoden durch den Einsatz von Inline-Appliances, jedoch ist dies hinsichtlich Performance, Netzarchitektur und Ausfallproblematik keine gute Lösung. Hier sind Architekturen, wie sie bei Firewalls und IDS gängig sind, nicht empfehlenswert.

Der Einfachheit halber soll hier auch nur die Möglichkeit betrachtet werden, die eine Reaktion am Switchport ermöglicht.

SNMP oder Scripting

Die härteste Vorgehensweise ist die Abschaltung eines Switchports bei einem Verstoß gegen die Policy. Dies ist eine sehr drastische Maßnahme, letztendlich aber konsequent und wirkungsvoll gegenüber potentiellen Angriffen.

Ein Netzwerkteilnehmer, der schwerwiegend gegen die Unternehmensrichtlinien verstößt, sollte keine weitere Möglichkeit besitzen in irgendeiner Form im Netzwerk agieren zu dürfen. Solch eine drastische Maßnahme sollte in jedem Fall zur Verfügung stehen. Diese Möglichkeit ist zielgerichtet mittels SNMP zu steuern und lässt sich relativ unproblematisch auch in heterogenen Netzen unternehmensweit umsetzen.

Darüber hinaus können mittels zentralen Managements die Switchports entsprechenden VLANs (Gastnetz, Produktivnetz) zugeordnet werden. Dies lässt sich durch zwei verschiedene Methoden erzielen, einerseits können die Switches mittels SNMP gesteuert werden, andererseits kann dies mittels vorgefertigter Scripte via Telnet realisiert werden. In beiden Fällen ist jedoch zu berücksichtigen, dass die verschiedenen Hersteller und Gerätetypen nicht immer einheitlich gesteuert werden können. Hier sind notfalls individuelle Anpassungen notwendig. Stand heute ist dies häufig die einzige Möglichkeit kurzfristig und ohne Neuanschaffungen solche Policies mittels gesteuerter Switchports zu realisieren.

Bewertung: herstellerunabhängig – relativ kostengünstig – sofort realisierbar

Integrierte Steuerung

Eine weitere Möglichkeit bietet die Durchsetzung von Policies durch eine integrierte Steuerung der Switchports. Dies bedeutet allerdings, dass im Vorfeld eine Reihe von Parametern festgelegt werden müssen. Beispielsweise ist festzulegen, welche Applikationen wann und in welcher Menge an welchem Switchport übertragen werden dürfen. Dies ist in Abhängigkeit vom jeweiligen Endgerät und Benutzern festzulegen. Die technische Realisierung ist in vielen Switchen bereits implementiert und könnte durchaus eingesetzt werden, jedoch trifft auch hierbei die Aussage zu, dass dies fast ausschließlich in einer homogenen Infrastruktur möglich ist. Notwendigerweise ist hier eine zentrale übergreifende Konfiguration notwendig, die alle erforderlichen Regeln an die Switches überträgt. Die lokale Konfiguration der Switche selbst entscheidet dann über den Verstoß gegen eine Policy. Unter Zuhilfenahme von weiteren Informationen (sFlow/NetFlow) könnten auch weitere Anomalien als Entscheidungskriterium dienen. Sicherlich ist dies eine wünschenswerte Möglichkeit unternehmensweite Policies durchzusetzen, die Realisierungsmöglichkeiten sind zurzeit allerdings stark beschränkt.

Bewertung: herstellerabhängig – aufwändig – flexibel

Fazit:

Die integrierte policy-basierte Steuerung von Switchports als einheitliche Implementierung auf heterogener Infrastruktur ist in absehbarer Zeit nicht zu erwarten.

Die momentan einzige Möglichkeit eine unternehmensweite heterogene Lösung zu implementieren kann nur mittels SNMP und Scripting erfolgen. Hier gibt es wirtschaftliche und technologisch sinnvolle Lösungen am Markt. Die Möglichkeit einer Kombination mit 802.1x ist gegeben und erscheint sogar ideal.

Schritt 4: Remediation

Der Prozess Remediation beinhaltet die Wiederherstellung der Konformität der unter Quarantäne gestellten Systeme. Dies bedeutet in der Regel, dass eine Infrastruktur zur Verfügung gestellt werden muss, die dafür sorgt, dass Endgeräte mit Softwareupdates und aktuellen Virensignaturen oder gar kompletten Softwarepaketen versorgt werden können. Nach erlangter Konformität muss das System automatisch dem zugeordneten VLAN zugeführt werden.

Dies sollte nach Möglichkeit fallspezifisch und benutzergeführt realisiert werden. In Abhängigkeit der vorliegenden Policy muss solch ein System idealerweise die Möglichkeit bieten einem Gastsystem temporär die Konformität zu verschaffen.

Es bieten sich unterschiedliche Lösungsmodelle an, ein Patentrezept existiert nicht. Manuelle Eingriffe sollten möglichst vermieden werden, da sonst der Helpdesk vermutlich überlastet wird. Automatismen können in der Regel nur mit Agenten auf den Endsystemen realisiert werden. Dies erfordert allerdings wiederum die Verteilung und Pflege der Agenten, sowie deren Konfiguration. Sollten auch Gastsysteme damit versorgt werden müssen, sind temporäre Agenten notwendig. Hierbei ist natürlich auf das notwendige Berechtigungskonzept zur Installation und Konfiguration der Gastsysteme zu achten. Eine vollständige und weitestgehend automatisierte Lösung kann dabei sehr kostspielig und aufwändig werden. Hierzu müsste in jedem Fall ein umfassendes Konzept aufgestellt werden, welches möglichst alle Fallbeispiele berücksichtigt.

Monitoring

Sind alle vorherigen Schritte durchlaufen und der Benutzer gelangt auf seine für ihn bestimmten Netzwerk-Ressourcen, ist das permanent oder zyklisch durchzuführende Monitoring der Endsysteme notwendig. Unabhängig davon, welche der hier beschriebenen Prozesse implementiert sind, müssen die durchgeführten Tests wiederholt werden. Jegliche nachträglich durchgeführte kritische Systemänderung muss auch weiterhin erkannt werden und sollte bei Verstoß gegen die Policy zu angemessenen Maßnahmen führen. Hierbei ist nicht zwingend das Durchlaufen aller Prozesse notwendig. Die einzelnen Maßnahmen können unabhängig voneinander und durchaus in sehr unterschiedlichen Zyklen erfolgen. Ein Portscan wird sicherlich nicht so häufig durchgeführt werden wie eine Überwachung der Adressparameter.

Über den Tellerrand hinaus…

…ist zu beachten, dass eine Reihe von bereits implementierten und im Unternehmen vielleicht schon lange und zuverlässig agierende Systeme ins gesamte Security-Konzept eingebunden werden können. Nennenswert wären da Systeme wie sFlow/netFlow, mit denen nicht nur Performance und Trends, sondern auch Anomalien im Netzwerk erkannt werden können. Solche Systeme agieren ggf. schon zur Anomalieerkennung (NADS) und können ebenfalls vollständig in ein NAC-Konzept eingebunden werden. Darüber hinaus bietet es sich an andere Sicherheitssysteme, wie Firewalls, Intrusion Detection und Viren- und Netzwerkscanner in ein übergreifendes Monitoring einzubinden, um hier eine Gesamtübersicht zur Verfügung zu stellen. Die Funktionalität von NAC ist für jedes andere System von Nutzen, da die Einzelsysteme nicht die Flexibilität und Vollständigkeit eines NAC-Konzeptes bieten.

Vorteile einer NAC-Lösung sind darüberhinaus die Verwendung der Lokalisierungsmöglichkeit von Endgeräten speziell in Bezug auf Voice over IP und WLAN-Komponenten. Die unternehmensweite Lokalisierung und Identifizierung dieser Geräte ist nicht nur aufgrund der potentiellen Angriffe gegen solche Systeme notwendig, sondern könnte hinsichtlich Notruf-Aktivierung eine zwingende Voraussetzung für den Einsatz solcher Systeme darstellen.

Zusammenfassend…

… sollte festgehalten werden, dass es nicht „die“ NAC-Lösung gibt, sondern eine ganze Reihe von Lösungen, die zu einer NAC-Lösung zusammengefasst werden. Welche Lösung die passende ist, ergibt sich letztlich aus den individuellen und gesetzlichen Anforderungen sowie aus der vorhandenen Infrastruktur und letztlich aus dem vorhandenen Budget. Bevor jedoch ein Projekt gestartet wird, ist es zwingend notwendig, die Ziele und Anforderungen zu definieren. Da solch ein Projekt schnell unübersichtlich werden kann, sollte in jedem Fall eine schrittweise Implementierung festgelegt werden. Die ausgesuchten Lösungen sollten zunächst in kleinen Umgebungen hinsichtlich der Funktion und Schnittstellen getestet werden, somit wird gleichzeitig transparent, wie hoch der Aufwand für die Installation, Betrieb und Wartung der Systeme ist. Ebenso können hier gleichzeitig die notwendigen Schnittstellen getestet werden. Mögliche Kostenfallen durch hohe ausgelagerte Aufwände können dadurch gleich erkannt werden. Darüber hinaus ist es von Vorteil, die technische Entwicklung der Hersteller und Produkte im Auge zu behalten, da möglicherweise die eine oder andere Anschaffung nur temporärer zu berücksichtigen ist. Zukünftig werden sicherlich zahlreiche Security-Features in die Infrastruktur (Switche/Router) integriert werden, was zumindest bei homogener Infrastruktur von Bedeutung ist.

Einordnung des IntraPROTECTOR in die vorhergehende Betrachtung

Abschließend möchten wir die Security Lösung IntraPROTECTOR in die vorhergegangene Betrachtung einordnen, um das vorhandene Leistungsspektrum des IntraPROTECTOR zu verdeutlichen. Natürlich sind nicht alle o.g. Funktionalitäten in der dargestellten Implementierungstiefe verfügbar, dies ist auch nicht unser Anspruch.

Unsere Motivation besteht vielmehr darin, Kunden, Anwendern und Integratoren ein möglichst umfassendes internes Sicherheitssystem zu einem kosten- und nutzenoptimierten Investitionsvolumen zu bieten.

Die zur Verfügung gestellten Schnittstellen ermöglichen darüber hinaus die Einbindung anderer Systeme und lassen somit sukzessive eine vollständige NAC-Lösung entstehen.

Allem voran bietet IntraPROTECTOR den Vorteil von Beginn an eine Identifizierung und Lokalisierung aller Geräte zu liefern.

Dies ist schließlich Voraussetzung eines jeden NAC-Projektes und Basis des zu erstellenden Konzeptes. Alle weiteren Schutzfunktionen können später bei Bedarf aktiviert werden.

Über COMCO AG:

Die COMCO AG mit Sitz in Dortmund ist ein marktführendes Software- und Systemhaus.

Das Unternehmen ist in die Geschäftsbereiche „Business Security Software“ und „Network Solution Provider“ gegliedert.

Der Unternehmensbereich „Business Security Software“ ist auf die Entwicklung von Security Lösungen zum Schutz unternehmensweiter Datennetze vor internen Angriffen fokussiert. Mit dem Geschäftsbereich „Network Solution Provider“ deckt die COMCO AG das gesamte Spektrum an Netzwerk Lösungen ab. Von der Beratung in der Planungsphase über die Implementierung bis zum Service und Support der gesamten IT-System-Umgebung reichen hier die Dienstleistungen. Darüber hinaus unterstützt COMCO ihre Kunden mit Netzwerk und Security Audits, Managed IT Services und Trainings.

Zum branchenübergreifenden Kundenkreis zählen renommierte Medienunternehmen, Banken, Versicherungen, Energieversorger, große Einzelhandelsunternehmen und Unternehmen aus dem Automotive-Bereich sowie Landes und Bundesbehörden.

Weitere Informationen

COMCO AG

Fallgatter 6

D-44369 Dortmund

Telefon: +49 (0) 231 47644 -0

Telefax: +49 (0) 231 47644 -299

info@comco.de

www.comco.de