Seminar: Netzwerksicherheit
NAP
Network Access Protection

Gennaro Piano

13. Juni 2013

Inhaltsverzeichnis

Glossary

FreeNac Eine Software basierend auf OpenSource. Es setzt anhand von MAC Adressen oder Ports, Clients in ein spezifisches VLAN.

NAP Abkürzung für Network Access Protection.

NAP Agent Dienst der auf dem Client läuft, ist die Schnittstelle von NAP.

NPS Network Policy Server, Netzwerkkomponente von Windows Server 2008, um Netzwerkzugriffsrichtlinien zu erstellen.

SHA System Health Validator; Dieser Dienst erfasst die einzelnen Sicherheitskriterien.

SoH Statement of Health; Resultat der Sicherheitskritieren.

SoHR Statement of Health Response; Enthält Informationen, ob der Client das Sicherheitskriterium bestanden hat.

SSoH System Statement of Health; Beinhaltet alle SoH und Informationen über das Betriebssytem.

SSoHR System Statement of Health Response; Enthält Zusammenfassung aller SoHR.

Abbildungsverzeichnis

1 Einleitung

1.1 Ausgangslage

Die KMU IT Management AG sucht seit längerem ein Produkt, welches infizierte Computer isoliert und somit keine Gefahr für andere Geräte darstellt. Vor drei Jahren wurde das Produkt FreeNAC evaluiert, jedoch entsprach dieses Produkt nicht den Vorstellungen der KMU IT Management AG. Ohne eine solche Lösung ist die KMU IT Management AG ständig dem Risiko ausgesetzt sich Würmer und Viren ins Netzwerk zu holen.

1.2 Projektbeschreibung

Dieses Projekt soll einen Einblick in das Network Access Protection von Microsoft geben. Es soll die Stärken sowie Schwächen von Network Access Protection aufzeigen. Anhand dieses Projekts wird die Geschäftsleitung entscheiden, ob Network Access Protection in der KMU IT Management AG eingeführt werden soll.

1.3 Ist Zustand

Das produktive LAN der KMU IT Management AG besteht aus 5 Clients und einem ESXi Server. Das Rechenzentrum der KMU IT Management AG befindet sich an einem anderen Standort und ist in einem anderen Netz. Die Verbindung zwischen dem internen Netzwerk und dem Rechenzentrum ist durch eine VPN Verbindung realisiert. Das interne Netzwerk sowie das Rechenzentrum sind durch Firewalls von Angriffen aus dem Internet geschützt. Die grössere Gefahr besteht aus dem LAN selbst. Es existiert keine Lösung um infizierte oder nicht genügend geschützte Clients, die sich mit dem LAN verbinden, zu identifizieren. Durch dieses Sicherheitsrisiko kann es passieren, das sich ein Wurm unbemerkt im LAN verbreitet. Es genügt diese Gefahr aus dem produktiven LAN zu entfernen, da sich Clients nur im produktiven LAN mit dem Netzwerk verbinden können. Somit kann sich ein infizierter Client nur im produktiven LAN befinden.

1.4 Erwartete Resultate

Dieser Bericht soll auf folgende Punkte eingehen:

- Funktionsweise von Network Access Protection
- Vorteile und Nachteile von Network Access Protection
- Vorstellung der fünf Network Access Protection Methoden
- Vergleich der fünf Network Access Protection Methoden
- Vergleich von Network Access Protection mit Konkurrenzprodukten
- Empfehlung

2 Network Access Protection

2.1 Was ist NAP

Network Access Protection ist ein Produkt das Microsoft ab Windows Server 2008 unter dem Network Policy Server (NPS) implementiert hat. Der Dienst NPS ersetzt den in Windows Server 2003 noch vorhandenen Internet Authentication Service. Network Access Protection verhindert, dass Clients die non-compliant[1] sind, das Firmennetz beschädigen können.

Definition von ungesund
Ungesunde Clients nennt man in der Fachsprache non-compliant. Das sind Clients, die den Sicherheitskriterien der Firma nicht entsprechen. In Windows 7 gibt es im Moment vier verschiedene Sicherheitskriterien auf die das Network Access Protection eingehen kann.

- Firewall vorhanden und aktiv
- Antivirus vorhanden, aktiv und auf dem neusten Stand
- Anti-SpyWare vorhanden, aktiv und auf dem neusten Stand
- Windows Updates aktiviert und alle Windows Updates installiert

Non-compliant Clients
Wenn das Network Access Protection einen Client bemerkt, der non-compliant ist, wird diesem Client nur limitierten Zugriff auf das Firmennetzwerk gegeben. Der limitierte Zugriff kann durch fünf verschiedene Methoden erstellt werden.

Limitierter Zugriff
Clients die limitierten Zugriff haben können nur Remediation Server im Netzwerk erreichen. Dies bedeutet das der Client abgeschottet ist und so gut wie keine Geräte im Netzwerk erreichen kann.

[1] Ungenügend geschützt

Remediation Server
Ein Remediation Server versucht die Sicherheitslücken eines Clients, der als non-compliant gekennzeichnet ist, zu schliessen. Bei einer NAP Implementation in der KMU IT Management AG gäbe es folgende Remediation Server:

- WSUS Server
- TrendMicro WFBS Server

Für die Firewall braucht es keinen Remediation Server, da bei den Clients die interne Windows Firewall benutzt wird. Die Windows Firewall schaltet sich selber ein, falls keine andere Firewall vorhanden ist.

2.2 Die fünf Methoden

Der limitierte Zugriff kann auf fünf verschiedenen Methoden geregelt werden, bei jeder Methode wird der Zugriff anders geregelt.

2.2.1 DHCP NAP Enforcement Methode

Die DHCP NAP Enforcement Methode benötigt mindestens einen DHCP Server. Der DHCP Server kann zugleich ein NPS Server sein, jedoch kann NPS auch auf einem separaten Server installiert sein. Bei dieser Methode regelt der DHCP Server den Zugriff aufs Netzwerk. Ein Client der non-compliant ist, erhält vom DHCP Server IP Parameter mit denen der Client nur auf die Remediations Server zugreifen kann. Ein Client der compliant ist, erhält die normalen IP Parameter, das bedeutet er hat Vollzugriff aufs Netz.

Diese Methode ist auf der nächsten Seite ausführlich erklärt, sie soll die Funktionsweise von NAP aufzeigen. Es ist die einfachste Methode zu implementieren und somit die Einfachste zu erklären. Die Erklärung der anderen Methoden geht bewusst nicht derart ins Detail, da der Hintergrund jeder Methode sehr ähnlich ist.

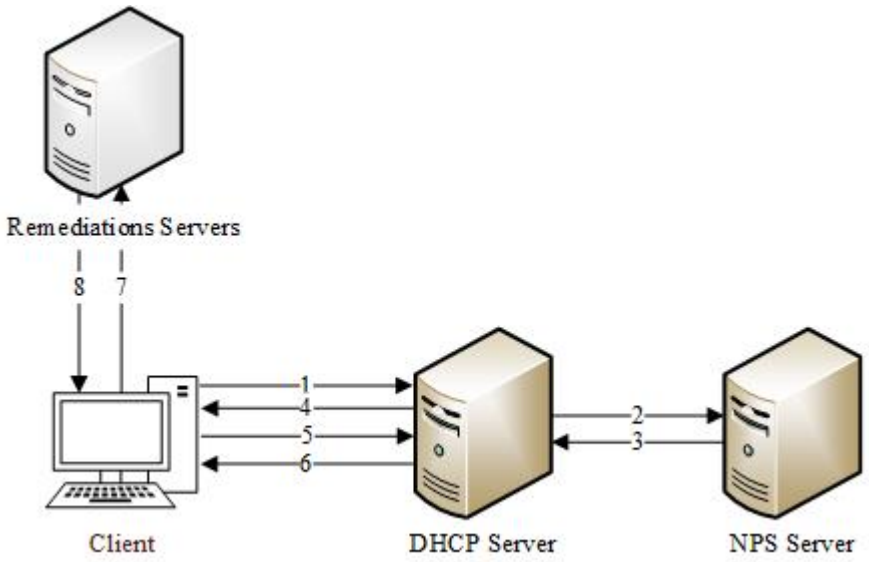


Abbildung 1: Vorgehen der DHCP NAP Enforcemenent Methode

Schritt 1
Bevor der Client einen DHCPDiscover macht, sammelt er mit Hilfe des System Health Agent, das SoH [2]. Das SoH beinhaltet Informationen über den Status der Sicherheitskriterien. Dieses SoH wird mit Hilfe der SHA[3] erstellt.

Ein SHA erfasst den Status eines Sicherheitskriteriums und publiziert es in einem SoH. Microsoft hat in Windows Vista und Windows 7 eine eigene SHA implementiert, welche mit dem Security Center kommuniziert und sich dadurch ein Bild des Sicherheitszustand des Clients machen kann. Die Microsoft SHA erstellt anhand des Status des Security Center ein SoH.

Das generierte SoH wird nun an den NAP Agent weitergeleitet, wessen Aufgabe es ist, alle SoHs zu sammeln und ein SSoH[4] zu erstellen. Das SSoH enthält Informationen des Betriebssystem und alle SoH's. Nun sendet der NAP Agent das SSoH an den DHCP NAP Enforcement Client.

[2]System of Health
[3]System Health Agent
[4]System Statement of Health

Was ist der DHCP NAP EC?
Jede Methode hat seinen eigenen NAP EC. Bei der DHCP Methode ist er eine Komponente des DHCP Client Dienst. Diese Komponente bekommt das SSoH, dadurch wird das SSoH in die DHCP Pakete implementiert. Das SSoH wird entweder zu den DHCPDiscover, DHCPRequest oder DHCPInform Pakete hinzugefügt.

Nun werden diese Pakete dem DHCP Server gesendet, welche vom DHCP Server Services empfangen werden. Der Dienst DHCP NAP Enforcement Server filtert das SSoH heraus. Der DHCP NAP Enforcement Server ist eine Komponente des DHCP Server Dienst.

Schritt 2
Das SSoH wird nun an den lokalen NPS Service weitergeleitet, welcher das SSoH über RADIUS an den NPS Server sendet. Der NPS Server empfängt das SSoH. Auf dem Server teilt der NAP Administration Server das SSoH in die einzelnen SoH's auf.

Schritt 3
Die SoH werden mit den Sicherheitskriterien des System Health Validator verglichen. Im Validator definiert man, welche Kriterien überprüft werden sollen. Nach der Prüfung der einzelnen SoH's erstellt der Validator für jedes SoH ein SoHR [5]. Nach dem alle SoH's geprüft worden sind, werden alle zu einem SSoHR [6] zusammengefügt. Das SSoHR wird dem DHCP Server zurückgesendet.

Schritt 4
Auf dem DHCP Server empfängt der lokale NPS Service das SSoHR. Dieser leitet es wieder an den DHCP NAP Enforcement Server weiter. Durch das SSoHR weiss der DHCP Server nun, welche IP Parameter der Client erhalten darf. Falls der Client compliant ist, erhält er die gewöhnlichen IP Parameter und hat somit Vollzugriff.

Falls der Client jedoch non-compliant ist, erhält er folgenden IP Parameter

Subnetzmaske:	255.255.255.255
Default Gateway:	keinen

Durch diese Parameter sieht der Client nur noch sich selbst.

Der DHCP Server sendet dem Client ein DHCPOffer mit den vorgeschlagenen IP Parameter und dem SSoHR.

[5] Statement of Health Response
[6] System Statement of Health Response

Schritt 5
Der DHCP Client sendet dem DHCP Server ein DHCPRequest, dass er die IP Parameter annimmt.

Schritt 6
Der DHCP Server sendet dem Client die IP Konfiguration und das SSoHR. Der DHCP NAP Enforcement Client leitet das SSoHR zu dem NAP Agent weiter. Dieser teilt das SSoHR in die entsprechenden SoHR auf und leitet es dem entsprechenden SHA zurück. Wenn der Client compliant ist, hat er Vollzugriff und beendet somit die Verbindung.

Schritt 7
Ein Client mit limitierten Zugriff versucht nun mit den Remediation Servers zu kommunizieren, um compliant zu werden. Ein Remediation Server kann beispielsweise ein WSUS Server sein, falls der Client nicht alle Updates installiert hat.

Wie kann der Client mit den Remediation Servers kommunizieren?
Ein Client der non-compliant ist, erhält nur eine eingeschränkte IP Konfiguration. Somit kann dieser nicht mit den Remediation Server kommunizieren, jedoch können auf dem DHCP Server statische Routen für Remediation Server erstellt werden. Diese statische Routen verteilt der DHCP Server nur an Clients die non-compliant sind. Somit kann der Client mit dem WSUS Server kommunizieren.

Schritt 8
Der WSUS Server sendet dem Client die fehlenden Updates. Der Client installiert die Updates und sendet dem DHCP Server das neue SSoH. Sobald der DHCP Server das SSoH empfangen hat, wiederholen sich die Schritte 2,3 und 6. Falls der Client nun compliant ist, erhält er eine neue IP Konfiguration, die ihm den Vollzugriff ermöglicht. Ansonsten bleibt die bestehende Konfiguration mit dem limitieren Zugriff.

2.2.2 IPSec NAP Enforcement Methode

Bei dieser Methode erhält der Client von Anfang an die normalen IP Parameter, jedoch benötigt er ein Zertifikat, welches ihm Zugriff ins sichere Netz ermöglicht. Dieses Zertifikat erhält der Client sobald er sich als compliant beweisen kann. Um ein Zertifikat zu erhalten kommuniziert der Client mit einem Health Registration Authority Server über HTTP oder HTTPS.

Der Client sendet dem HRA Server seinen momentanen Sicherheitszustand, dadurch signalisert der Client, dass er ein Zertifikat haben möchte. Der HRA Server leitet mittels RADIUS den Sicherheitszustand einem NAP Health Policy Server weiter. Dieser Server wertet den Sicherheitszustand aus.

Falls der Client compliant ist, sendet der NAP Health Policy Server dem HRA Server ein Zertifikat. Der HRA Server leitet das weiter zum Client. Durch dieses Zertifikat hat der Client Vollzugriff im Netzwerk. Falls der Client non-compliant ist, wird kein Zertifikat ausgestellt. Somit hat der Client nur limitierten Zugriff.

2.2.3 IEEE802.1x NAP Enforcement Methode

Die IEEE802.1x NAP Enforcement Methode benötigt mindestens einen 802.1x kompatiblen Switch und einen NPS Server. Diese Methode funktioniert mit VLANs. Clients, die den Status non-compliant haben, werden in ein Quarantänen VLAN transportiert. In diesem VLAN existieren nur Clients die non-compliant sind. Sobald der Client compliant ist, kommt er in ein VLAN welches Vollzugriff auf das Firmennetzwerk ermöglicht. In dieser Methode kommuniziert der NAP Client über ein 802.1x fähigen Switch mit dem NPS Server. Der 802.1x fähige Switch empfängt die Daten des Client und leitet sie weiter an den NPS Server beziehungsweise vom NPS Server zum Client. Er muss diese Daten weder verwalten noch ändern. Sobald er die RADIUS Access-Accept Nachricht vom NPS Server erhält, muss der Switch handeln.

Wenn der Client non-compliant ist, sendet der NPS Server dem Switch eine RADIUS Access-Accept Nachricht mit einem Zugriffsprofil, das den Zugriff des Clients auf das Quarantänen VLAN reduziert.

Wenn der Client compliant ist, sendet der NPS Server dem Switch eine RADIUS Access-Accept Nachricht ohne Zugriffsprofil, das ermöglicht dem Client Vollzugriff auf das Firmennetzwerk.

2.2.4 VPN NAP Enforcement Methode

Die VPN NAP Enforement Methode deckt den VPN Zugriff ab. Somit überprüft diese Methode die Clients, die von aussen über VPN auf das Firmennetz zugreifen wollen. In dieser Methode werden Remote Access Paket Filter benutzt, um den Clients die non-compliant sind, nur Zugriff im limitierten Netzwerk zu geben. Bei dieser Methode besteht die Kommunikation, um zu überprüfen ob der Client compliant ist, hauptsächlich zwischen VPN Client und NPS Server. Der VPN Server wird nur als Weiterleitung benötigt. Erst wenn der NPS Server dem VPN Server die RADIUS Access-Accept Nachricht sendet, muss der VPN Server handeln.

Wenn der Client non-compliant ist, sendet der NPS Server dem VPN Server eine RADIUS Access-Accept Nachricht die IP Paket Filter enthält, diese Filter ermöglichen dem Client nur limitierten Zugriff.

Wenn der Client compliant ist, sendet der NPS Server dem VPN Server eine RADIUS Access-Accept Nachricht ohne IP Paket Filter, das ermöglicht dem Client Vollzugriff auf das Firmennetzwerk.

2.2.5 TS Gateway NAP Enforcement Methode

Der TS Gateway ist ein Feature der Terminal Services, das Microsoft seit Windows Server 2008 eingeführt hat. Dieses Feature ermöglicht von aussen auf einen firmeninternen Terminal Server zuzugreifen. Dies wird mit einer RDP over HTTPS Verbindung hergestellt.

In dieser Methode wird den Clients, die non-compliant sind, den Zugriff auf den TS verweigert. Bei dieser Methode sendet der Client dem TS Gateway Server während der Benutzerauthentifizierung das System Statement of Health verschlüsselt, was bei dieser Methode SoH request blob heisst.

Der TS Gateway Server entschlüsselt nun den blob und sendet es über RADIUS an den NPS Server. Dieser entscheidet ob der Client compliant oder non-compliant ist und sendet dem TS Gateway Server ein SoH Response. Der TS Gateway Server leitet diese Informationen weiter zum TS Gateway Server RADIUS. Dieser entscheidet, ob der Client auf dem Terminal Server Zugriff haben soll. Diese Methode ist die einzige, die keine Auto-Remediation ermöglicht.

Hier nochmals die Architektur von Network Access Protection, dieses Mal einwenig detaillierter. Diese Bild wurde von der Technet-Seite von Microsoft übernommen.

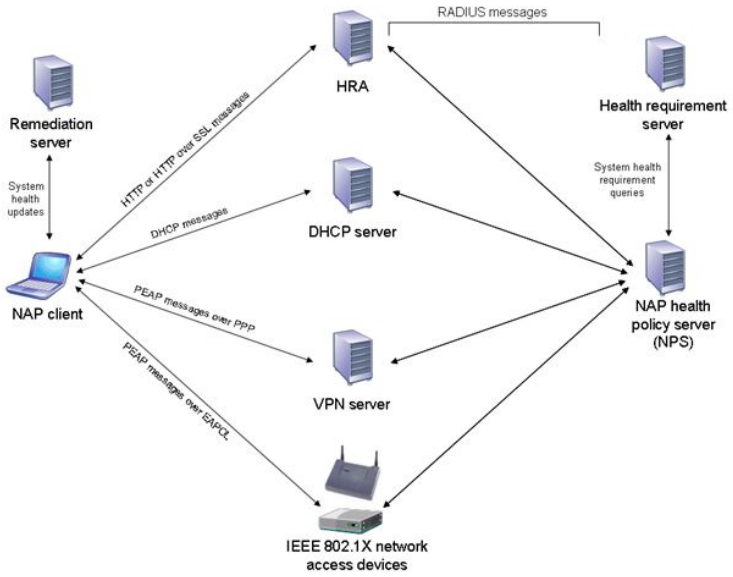


Abbildung 2: NAP Architektur allgemein; Quelle: technet.net

2.3 Auto Remediation

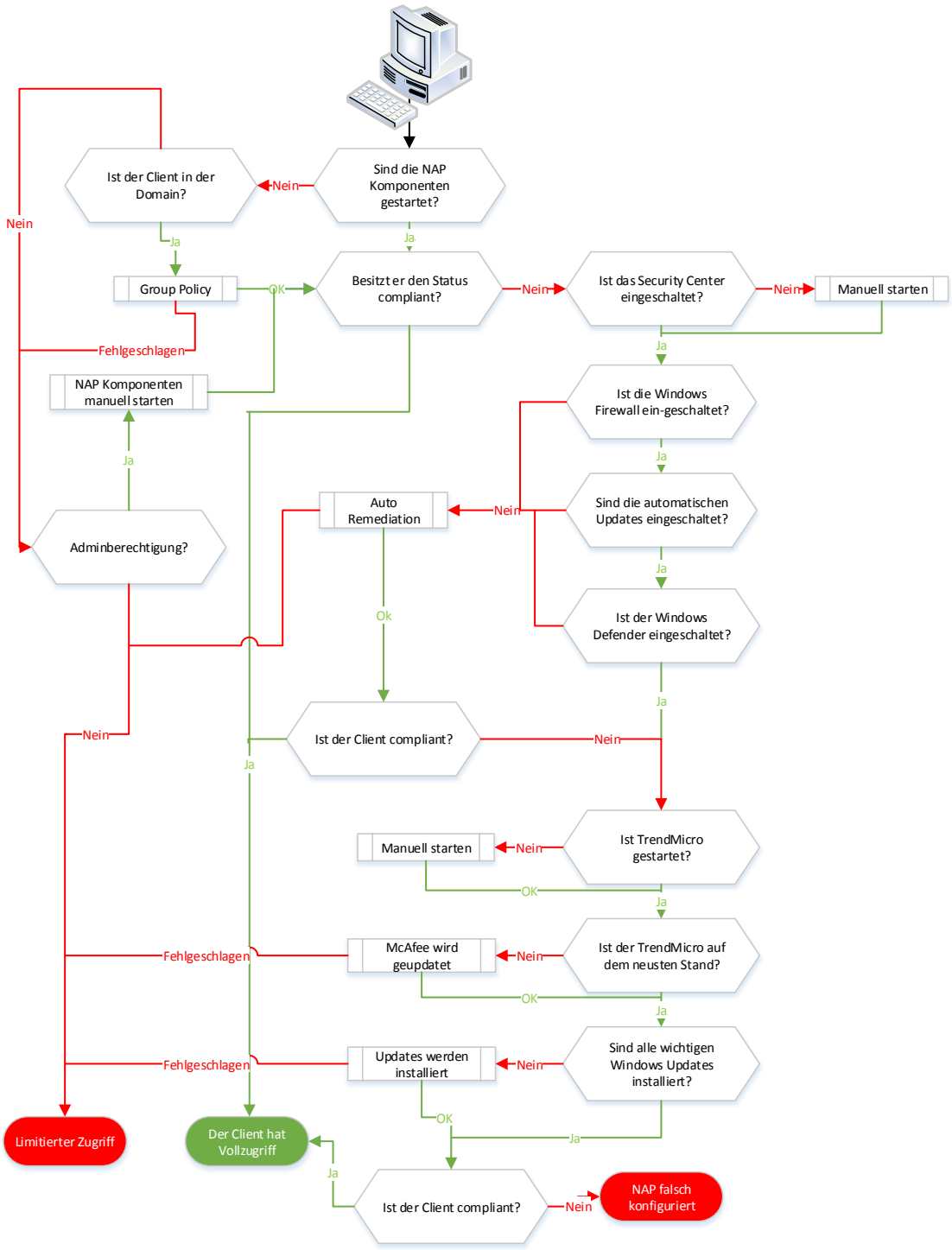
Die Auto Remediation ist eine Eigenschaft, die man auswählen kann. Mit Hilfe der Auto Remediation werden folgende Probleme automatisch behoben, ohne dass der User eingreifen muss.

- Windows Firewall wird automatisch eingeschaltet
- Windows Updates wird automatisch eingeschaltet
- Windows Defender wird automatisch eingeschaltet

Das automatische Herunterladen und Installieren der Windows Updates ist keine direkte Auto Remediation, da diese Option durch die Windows Update Einstellungen definiert wird. Aber da NAP die Einstellungen auf *Automatisches herunterladen und installieren von Windows Updates* ändert, kann diese Option als Auswirkung der Auto Remediation angesehen werden.

Bei Software von Dritthersteller (McAfee Antivirus, Comodo Firewall) kann NAP den Status der Software nicht automatisch ändern, da diese es nicht zulassen. Es kann sein das dies irgendwann möglich sein wird.

3 Ablauf einer NAP Abfrage



4 Vergleich

4.1 Anmerkung

Es hat sich herausgestellt das für die VPN NAP Enforcement Methode ein VPN Server von Microsoft benötigt wird. Die KMU IT Management AG besitzt keinen Microsoft VPN Server, somit fällt das Vergleichen der VPN NAP Enforcement Methode mit den anderen Methoden weg.

Die TS Gateway NAP Enforcement Methode fällt auch weg. Diese Methode macht nur mit dem Betrieb eines TS Gateway Servers Sinn. Die KMU IT Management AG besitzt keinen solchen Server und somit scheidet diese Methode aus.

4.2 Methodenvergleich

	DHCP	IPSec	802.1x
Enforcement Server	DHCP Server	HRA Server	802.1x Switch
Server vorhanden	Ja, mehrere	Nein	Ja
Manipulierbar	Ja, durch manuelle IP Werte	Nein	Abhängig von der Implementation
Internetzugriff	Nein	Ja	Ja
Abdeckungsgrad	100 %, solange DHCP auf allen Clients eingeschaltet ist	100 %, jeder Client benötigt ein Zertifikat	>100 %, falls ein Client an einem nicht kompatiblen 802.1x Switch verbunden ist, wird die Überprüfung umgangen.
Muss Domänenmitglied sein	Nein	Ja	Nein

4.3 Konkurrenzprodukte

Das populärste Konkurrenzprodukt von NAP ist das Network Access Control von Cisco. Dieses Produkt ist vergleichbar mit der 802.1x NAP Enforcement Methode. Es wurde entschieden das Einlesen in dieses Konkurrenzprodukt wegzulassen. Dieses Produkt funktioniert nur mit Cisco Produkten und da die KMU IT Management verschiedene Netzwerkgeräte im Betrieb hat, kann dieses Konkurrenzprodukt nicht implementiert werden.

5 Theoretische Umsetzung

Für die drei Methoden die verglichen wurden, wird aufgezeigt wie die Implementation der Methode in der Theorie aussehen wird. Dieses theoretische Implementation soll aufzeigen, was benötigt wird und wie gross der Aufwand einer allfälligen Implementation wäre.

5.1 Allgemein

Jede dieser Methoden benötigt einen NPS Server. Der NPS Server kann auf jeden beliebigen Windows Server installiert werden. Einzige Bedingung ist, dass der Server mindestens auf Windows Server 2008 laufen muss. Die Installation des NPS Server kann über den Server Manager installiert werden.

Nach der Installation des NPS Servers, muss der System Health Validator konfiguriert werden. Im System Health Validator wird bestimmt, welche Sicherheitseigenschaften des Clients überprüft werden soll. Danach kann man angeben, wann ein Client compliant ist und wann nicht.

Zum Schluss müssen alle Remediations Server angegeben werden und den Enforcement Server als RADIUS Client eintragen.

Auf den Clients muss der Dienst Network Access Protection auf Automatisch gesetzt werden und der benötigte Enforcement Client aktiviert werden. Dies kann über ein Group Policy Objekt automatisiert werden.

5.2 DHCP NAP Enforcement Methode

Der DHCP Server ist schon vorhanden und muss nicht mehr installiert werden, jedoch müssen gewisse Änderungen auf dem Server gemacht werden. Auf jedem DHCP Server des Unternehmens muss die NPS Rolle installiert werden. Im NPS wird der im vorherigen Kapitel installierte Server als RADIUS Server angegeben. Danach müssen in der DHCP Konfiguration die Remediation Server als statische Route in der Default Network Access Protection Class eingegeben werden. Die statischen Routen werden von Clients benötigt, die limitierten Zugriff haben.

5.3 802.1x NAP Enforcement Methode

Auf dem Switch müssen mindestens 3 VLANs konfiguriert sein. Das Standard VLAN, ein VLAN für Clients, die non-compliant sind und ein VLAN für Clients die compliant sind. Als Authentifizierungsserver muss der NPS Server angegeben werden. Auf Ports auf denen 802.1x aktiviert ist, sollten nur Clients angehängt sein. Für die Server ist es empfehlenswert, Ports ohne 802.1x Authentifizierung zu benutzen. Bei Inbetriebnahme dieser Methode dürfen sich nur 802.1x Switches im Netzwerk befinden, ansonsten könnte ein Client der non-compliant ist, plötzlich Vollzugriff erlangen.

5.4 IPSec NAP Enforcement Methode

Diese Methode ist sehr komplex einzubinden. Mangels Kenntnisse mit den Health Registration und den CA Root Services von Microsoft wurde auf eine genauere Beschreibung der Konfiguration verzichtet. Falls die Konfiguration dieser Methode das Interesse geweckt hat, kann man die benötigten Installationsschritte unter folgendem Link herunterladen.
`http://www.microsoft.com/en-us/download/details.aspx?id=12609`

Das untere Bild zeigt die Infrastruktur der IPSEC NAP Enforcement Methode auf, dies soll aufzeigen wie die IPSec Methode genau funktioniert.

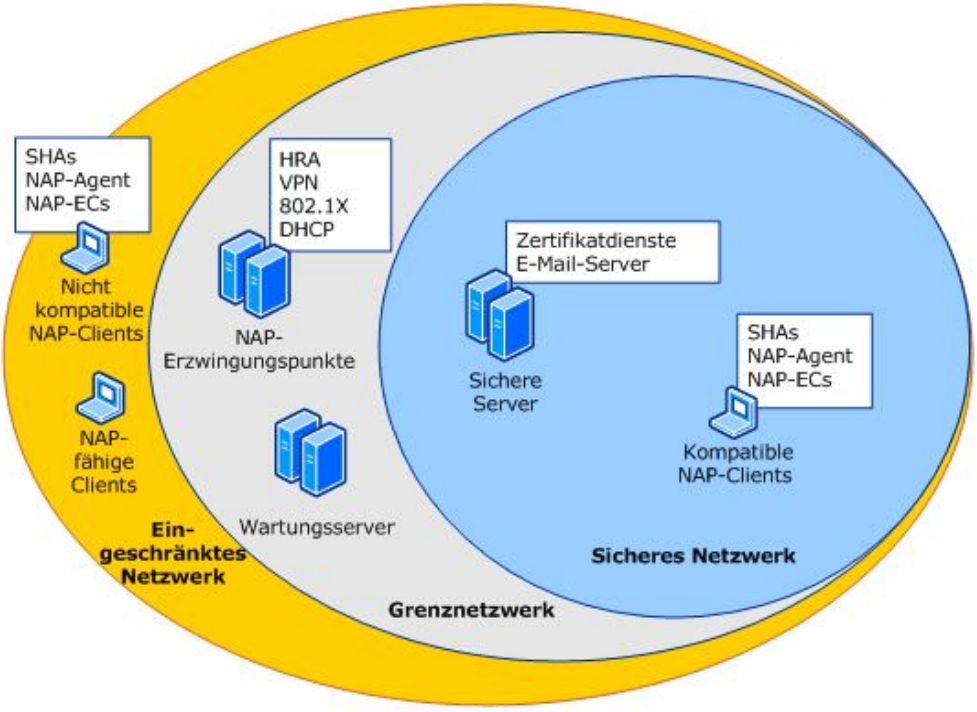


Abbildung 3: Architektur der IPSec Methode
Quelle: http://technet.microsoft.com/de-de/library/cc726008(v=ws.10).aspx

Im eingeschränkten Netzwerk befinden sich nicht zertifizierte Clients. Im Grenznetzwerk befinden sich Server, die von zertifizierten und nicht zertifizierten Clients benutzt werden können. In diesem Netzwerk befinden sich unter anderem die Remediation Server. Im sicheren Netzwerk befinden sich alle zertifizierte Clients und alle Server, die nur mit zertifizierten Clients kommunizieren dürfen.

6 Bewertung von Network Access Protection

6.1 Pro und Kontra

DHCP
Die DHCP NAP Enforcement Methode ist sehr einfach zu implementieren, jedoch bietet sie keinen Schutz vor Manipulierung. Falls der Client eine feste IP Adresse besitzt, benötigt er keinen DHCP Server. Dadurch wird der Sicherheitszustand des Clients nicht überprüft. Dieser Nachteil hat aber einen kleinen positiven Effekt. Ein Server oder ein Router, der keine Prüfung durchführen soll, kann durch eine manuelle IP Vergabe aussortiert werden. Clients, die limitierten Zugriff haben, können durch diese Methode nicht ins Internet. Dies ist ein weiterer Nachteil.

IPSec
Die IPSec NAP Enforcement Methode hat im Vergleich zu den anderen Methoden die kompliziertesteImplementation. Es muss ein Zertifikat erstellt werden und es braucht neben einem NPS Server und einem HRA Server noch einen CA Root Server. Clients, die sich nicht in der Domäne befinden, werden automatisch als non-compliant deklariert. Dies ist aus der Sicht der KMU IT Management AG ein Vorteil, jedoch aus Sicht unserer Kunden ein Nachteil. Verschiedene Kunden nehmen ihre privaten Notebooks mit um zu arbeiten. Dies wäre durch die IPSec Methode nicht mehr möglich. Die IPSec Methode ist was Sicherheit anbelangt die sicherste Methode, da der ganze Datenverkehr verschlüsselt ist und das Zertifikat nicht gefälscht oder kopiert werden kann.

802.1x
Die 802.1x NAP Enforcement Methode ist einfach zu implementieren und eine sehr sichere Methode. Um die Prüfung der Sicherheitsprüfung zu überspringen, muss man einen Hub oder Switch zwischen die Verbindung des 802.1x Switch und einem gesunden Client anhängen. Weil dieser Client compliant ist, ist der Port des Switches auf das offene VLAN gemappt, somit hätte jeder Client der sich mit den Hub verbindet Vollzugriff auf das Netzwerk. Das Eintreffen dieses Ereignisses ist sehr gering, da dies sehr auffällig ist. Wie schon erwähnt wird für diese Methode ein 802.1x Switch benötigt, dies ist als negativer Punkt zu nennen, da diese Switches nicht allgegenwärtig sind.

6.2 Empfehlung

Ich empfehle die 802.1x Methode, da die KMU IT Management AG im Besitz solcher Switches ist. Die IPSec Methode ist auch empfehlenswert, da es die sicherste Methode ist, jedoch ist der Aufbau her sehr komplex. Die DHCP Methode empfehle ich nicht, da sie relativ leicht umgangen werden kann und somit nicht wirklich zur Sicherheit des Unternehmens beitragen würde.

7 Anhang

7.1 Zeitaufwand

Arbeitsschritt	Schätzung in h	Benötigt in h
Planung	**15**	**19**
- Auswahl des Themas	3	2
- In EBS eingetragen	2	2
- Informationen sammeln	15	25
Realisierung	**35**	**54**
- Arbeit geschrieben	30	42
Präsentation	**10**	**?**
- Präsentation erstellen	8	?
- Präsentation vorbereiten	2	?
Total	**60**	**>71**

7.2 Review

Ich habe den Zeitaufwand für das Schreiben der Arbeit stark unterschätzt. Oft habe ich Zeit verloren, um gewisse Funktionen in Latex richtig zu benutzen. Auch das Einlesen in das Thema hat mich viel Zeit gekostet. Im Grossen und Ganzen sehe ich das Projekt aber als Erfolg an, da mir eine gute Beschreibung von Network Access Protection gelungen ist.

Literatur

[1] Network Policy and Access Services
http://technet.microsoft.com/en-us/network/bb545879.aspx

[2] Davies, J.G. and Northrup, T. and Northrup, A. (2008): *Windows Server 2008: Networking and Network Access Protection (NAP)*, Microsoft Press