INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Netzwerkzugriffsschutz

Der Zugriff auf das eigene Netzwerk sollte nur bestimmten Personen möglich sein. Zudem soll das Clientgerät aktuell und frei von schädlicher Software sein. Dieser INFONEWS zeigt, wie dies mit Windows Server 2008 gelöst werden kann und beantwortet dabei folgende Fragen:

- Was ist NAP/NAC?
- Wie kann damit das Netzwerk geschützt werden?
- Wie kann das Client-Gerät überprüft werden?

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Netzwerkzugriffsschutz

1.1 Einleitung

Immer häufiger wird es zur Gewohnheit, dass externe Berater und Betreuer ihr eigenes Gerät mitbringen und (meistens ungefragt) an das Firmennetzwerk anschliessen. Für den IT-Administrator ist es oft nicht möglich einzuschätzen, welche Geräte angeschlossen werden, in welchem Zustand sich diese befinden und was diese externen Personen im eigenen Netzwerk „anstellen". Daher ist es wichtig, den Zugriff so einzuschränken, dass sich nur erlaubte Geräte mit dem Netzwerk verbinden können. Weiter gilt es den Zustand des (erlaubten) Clientgerätes zu überprüfen. Die folgenden Fragen gilt es dabei zu klären:

- Verfügt dieses über aktuelle Patches?
- Ist der Virenscanner aktuell und aktiv?
- Läuft die lokale Firewall?

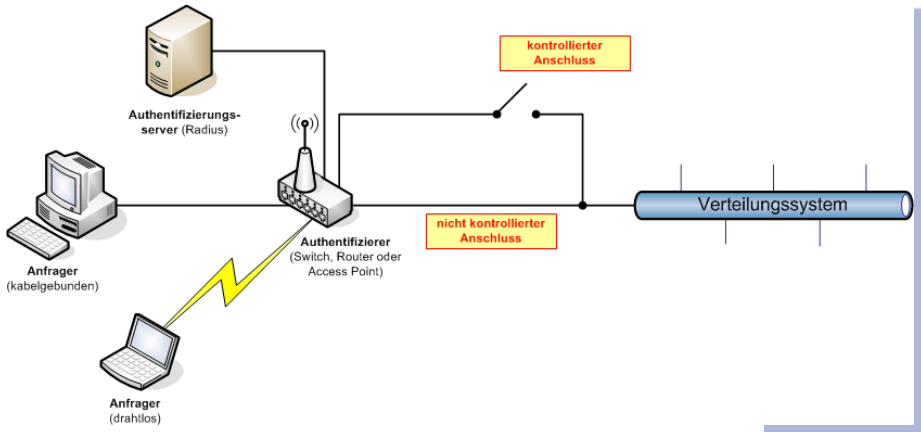
1.2 Netzwerkzugriffsschutz

Der Netzwerkzugriffsschutz kann schon seit längerem mit der Technik 802.1X gelöst werden. Die Steuerung wird in der Regel an einen entsprechenden Switch übergeben und nach erfolgter Authentifizierung kann das Netzwerk „betreten" werden.

1.2.1 Funktionsweise von 802.1X

Der IEEE-Standard 802.1X definiert, dass der Zugriff auf Ethernet-Netzwerke mit einer auf Anschlüssen (Ports) basierenden Netzwerkzugangskontrolle authentifiziert wird. Der Zugriff auf einen Anschluss kann verweigert werden, falls die Authentifizierung fehlschlägt. Dieser Standard wurde ursprünglich für Ethernet-Kabelnetzwerke entworfen, anschliessend an die Bedürfnisse drahtloser 802.11 Netzwerke weiter angepasst.

1.2.2 Elemente



- **Anschlusszugriffseinheit**
  Eine Anschlusszugriffseinheit (Port Access Entity, PAE), ist die logische Einheit, welche das IEEE 802.1X-Protokoll unterstützt. Ein PAE kann die Rolle des Authentifizierers, des Anfragers oder beide übernehmen.
- **Authentifizierer**
  Ein Authentifizierer ist ein LAN-Anschluss, der auf einer Authentifizierung besteht, bevor er den Zugriff auf Dienste zulässt, die über diesen Anschluss zugänglich sind. Bei drahtlosen Verbindungen ist der Authentifizierer der logische Anschluss des Access Points (AP), über den drahtlose Clients im Infrastrukturmodus Zugang zu anderen drahtlosen Clients und dem Kabelnetzwerk erhalten.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- **Anfrager**
  Der Anfrager (Supplicant) ist ein LAN-Anschluss, der Zugriff auf die Dienste wünscht, die unter Benutzung des Authentifizierers zugänglich sind. Bei drahtlosen Verbindungen ist der Anfrager der logische LAN-Anschluss auf einem Drahtlos-Netzwerkadapter, der Zugriff auf die anderen drahtlosen Clients und das Kabelnetzwerk fordert. Er muss sich dazu gegenüber dem Authentifizierer ausweisen.
- **Authentifizierungsserver**
  Zur Überprüfung der Anmeldeinformationen des Anfragers wendet sich der Authentifizierer an einen Authentifizierungsserver, der die Anmeldeinformationen des Anfragers im Auftrag des Authentifizierers überprüft und dann dem Authentifizierer mitteilt, ob der Anfrager für den Zugriff auf die Dienste des Authentifizierers autorisiert ist oder nicht. Der Authentifizierungsserver kann folgendes sein:

  a. Eine Komponente der Netzwerkkomponente. In diesem Fall muss die Netzwerkkomponente mit den Anmeldeinformationen der Benutzer konfiguriert werden, die den Anfragern entsprechen, von denen zulässige Verbindungsversuche zu erwarten sind.
  b. Eine separate Einheit. In diesem Fall leitet die Netzwerkkomponente die Anmeldeinformationen aus dem Verbindungsversuch an einen separaten Authentifizierungsserver weiter. Im Normalfall sendet eine Netzwerkkomponente mit dem RADIUS-Protokoll (Remote Authentication Dial-In User Service) einen Verbindungsanforderungsnachricht an einen RADIUS-Server.

1.2.3 Anschlussbasierte Zugriffskontrolle

Die anschlussbasierte Zugriffskontrolle des Authentifizierers definiert die folgenden beiden logischen Anschlussarten, die einem Zugriff auf das Kabel-Netzwerk über einen physischen LAN-Anschluss ermöglichen:

- **Unkontrollierter Anschluss**
  Der unkontrollierte Anschluss erlaubt einen unkontrollierten Datenaustausch zwischen dem Authentifizierer und anderen Geräten aus dem Netzwerk – unabhängig vom Autorisierungsstatus des Clients. Rahmen, die von unkontrollierten Clients verschickt werden, werden immer über den unkontrollierten Anschluss versendet.
- **Kontrollierter Anschluss**
  Der kontrollierte Anschluss erlaubt nur den Datenaustausch zwischen dem Client und dem Netzwerk, wenn der Client nach 802.1X autorisiert wurde. Vor der Authentifizierung ist der Schalter offen und es werden keine Rahmen zwischen dem drahtlosen Client und dem Kabel-Netzwerk weitergeleitet. Sobald sich der Client erfolgreich nach IEEE 802.1X authentifiziert wurde, wird der Schalter geschlossen und die Rahmen können zwischen dem Client und dem Netzwerk versendet werden.

1.2.4 EAP over LAN

Als Standardmechanismus für die Authentifizierung wurde für IEEE 802.1X das EAP (extensible Authentication Protocol) gewählt. EAP ist ein Authentifizierungsmechanismus auf Basis von PPP (Point-to-Point Protocol), das an den Einsatz in Punkt-zu-Punkt-LAN-Segmenten angepasst wurde. EAP-Nachrichten werden normalerweise als Nutzdaten in PPP-Rahmen verschickt. Damit EAP-Nachrichten über Ethernet- oder Drahtlos-LAN-Segmente verschickt

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

werden können, definiert der IEEE 802.1X-Standard eine einheitliche Kapselungsmethode für EAP-Nachrichten, die "EAP over LAN" oder "EAPOL" genannt wird.

1.3 DHCP

Das Ziel soll es sein, dass IP-Adressen nur an authentifizierte Geräte vergeben werden. Somit muss der DHCP Server mit in dieses Konzept eingebunden werden. Microsoft bietet diese Möglichkeit an.

1.4 VPN/ IPsec

Wenn nur verschlüsselte Verbindungen erlaubt sind, können Geräte, die über keinen Schlüssel verfügen (Pre-Shared Key oder Zertifikat), keine Verbindungen aufbauen. Oft ist der Aufwand relativ hoch, dies umzusetzen. Jedoch bietet Microsoft auch hier eine Möglichkeit an, dies mit IPsec zu lösen. Als Erleichterung können die IPsec Vorgaben via Gruppenrichtlinien (GPO) verteilt werden.

IPsec (Kurzform für IP Security) wurde 1998 entwickelt, um die Schwächen des Internetprotokolls (IP) zu beheben. Es stellt eine Sicherheitsarchitektur für die Kommunikation über IP-Netzwerke zur Verfügung. IPsec soll die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten. Daneben soll es vor so genannten Replay-Angriffen bzw. einer Replay-Attacke schützen – das heisst, ein Angreifer kann nicht durch Abspielen eines vorher mitgeschnittenen Dialogs die Gegenstelle zu einer wiederholten Aktion verleiten. Der RFC 2401 bildet das Hauptdokument zu IPsec. Er beschreibt die Architektur von IPsec. Darin werden weitere zu IPsec gehörende RFCs referenziert. Wesentliche Inhalte von IPsec sind das Authentication Header Protokoll (AH) und das Encapsulated Security Payload Protokoll (ESP) sowie das Internet Key Exchange Protokoll (IKE) zum Austausch der Schlüssel.

Im Gegensatz zu anderen Verschlüsselungsprotokollen wie etwa SSH arbeitet IPsec auf der Vermittlungsschicht (Schicht 3) des OSI-Referenzmodells.

1.4.1 Transport und Tunnel Mode

IPSec kennt zwei Betriebsmodi:

- **Transport Mode**
  Im Transport Mode wird IPSec zwischen zwei einzelnen Endsystemen aufgeschaltet. Beide beteiligten Systeme benötigen dazu einen IPSec Treiber.

- **Tunnel Mode**
  Ermöglicht sichere Übertragung zwischen zwei Netzwerken. Dabei werden nicht die Endgeräte selber mit IPSec ausgerüstet, sondern die Router, welche die beiden Netzwerke verbinden. Die Kommunikation wird nur auf der Strecke zwischen den beteiligten IPsec Routern verschlüsselt. Vor- und nach diesem Übertragungsstück erfolgt der Datenverkehr im "Klartext". Der Tunnel-Mode ist die für VPNs (Virtual Private Netzworks) übliche Betriebsart.

1.5 Cisco NAC

Cisco Network Admission Control (NAC) ist eine Sammlung von verschiedenen Technologien und Lösungen. Es ist stark an die Infrastruktur eines Cisco-Netzwerkes angelehnt und ermöglicht verschiedenen Endgeräten wie PCs, Servern und PDAs sich nach der Authentifizierungzu verbinden. Folgende Elemente werden benötigt: Cisco Trust

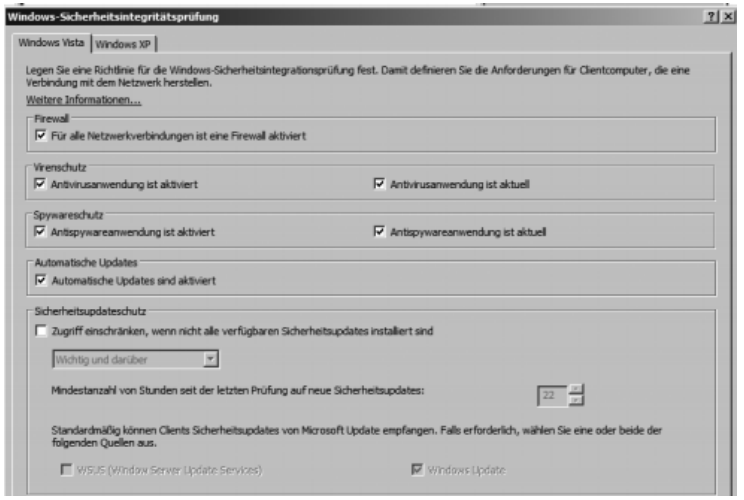
Agent, Cisco Security Agent für das Endgerät, Cisco Security Access Control Server für das Policy Management und Cisco Network Access Devices (Switches, Router) für die Netzwerkkontrolle. Unterstützt werden unter anderem VLANs, EAP/Radius, Switches, Router und über 75 Hersteller von Antiviren und Security-Lösungen.

2 Netzwerkzugriffsschutz unter Windows

Der Netzwerkzugriffsschutz (Network Access Protection, NAP) ist neu in Windows Server 2008. Als Client für diese Funktion wird Windows Vista oder Windows XP mit installiertem SP2 unterstützt. Der Client für NAP wird jedoch erst mit dem Service Pack 3 für Windows XP installiert. Damit NAP im Netzwerk eingesetzt werden kann, wird ein Richtlinienserver benötigt, über den die entsprechenden Richtlinien für NAP hinterlegt werden.

NAP kann aber nicht nur für Domänencomputer verwendet werden, sondern auch für Computer, die nicht Mitglied einer Domäne sind. Bei NAP kann der Netzwerkzugriff für Computer abhängig von deren Sicherheitseinstellungen, Patchstand und installierten Anwendungen gestattet oder verweigert bzw. beschränkt werden.

Im Gegensatz zu Serverdiensten wie die kostenlos erhältlichen Windows Server Update Services (WSUS) ist NAP nicht dafür zuständig, Patches zu installieren, sondern nur zu überprüfen, ob auf einem PC die entsprechenden Patches installiert sind. Entspricht ein Client nicht den Bedingungen für eine Einwahl, zum Beispiel durch einen installierten Virenscanner, installierte Patches oder sonstigen Sicherheitseinstellungen, wird diesem nur ein eingeschränkter Zugriff zum Netzwerk oder überhaupt kein Zugriff gewährt. Fremde Systeme, Zugriffe aus Internet-Cafés und unsichere Heimarbeitsplatze lassen sich so effizient vom Netzwerk ausschliessen. NAP ist dafür zuständig, nur jenen PCs den Zugriff auf das Netzwerk zu gewähren, die den Sicherheitsvorgaben des Unternehmens entsprechen.
Bei PCs mit Windows XP SP2 oder Windows Vista kann eine Windowssicherheitsintegritätsverifizierung durchgeführt werden, bei der konfiguriert ist, welche Bedingungen ein PC erfüllen muss. NAP ist damit sozusagen eine Weiterentwicklung der Network Access Quarantäne von Windows Server 2003. Microsoft stellt zudem eine API zur Verfügung, sodass auch Dritthersteller ihre Produkte in NAP integrieren können. So können Sie zum Beispiel auch diverse Antiviren-Hersteller in die Plattform eingebunden werden.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.1 Funktionsweise

Die NAP-Plattform baut auf verschiedenen Grund-Strukturen auf:

- Computer werden auf Basis von zentralen Richtlinien und der Windows-Sicherheitsintegritätsverifizierung eingeordnet.
- Computer, die den Richtlinien entsprechen, können ungestört im Netzwerk kommunizieren.
- Computer, die nicht den Richtlinien entsprechen, können bei der Kommunikation eingeschränkt werden oder an der Kommunikation gehindert werden.
- Computern, die nicht den Richtlinien entsprechen, können darüber hinaus Mechanismen zur Verfügung gestellt werden, um die Richtlinien einzuhalten. So können zum Beispiel Patches über einen WSUS installiert werden, sodass diese Computer zukünftig diesen Richtlinien entsprechen.
- Der Sicherheitszustand der Computer wird durch NAP dauerhaft und ständig sichergestellt.

Damit der Zugriffeines PCs überprüft werden kann, findet folgender Vorgang statt:

1. Ein Client will sich mit dem Netzwerk verbinden.
2. Als Nächstes generiert der Client ein Statement of Health. Der NAP-Client weiss, wie er das System untersuchen muss und kann einen Bericht erstellen, der an den Netzwerkrichtlinien-Server übergeben wird.
3. Dieser entscheidet auf Basis der zentralen Richtlinie, ob das Statement of Health gültig ist oder nicht.
4. Auf Basis dieses Ergebnisses wird eine Richtlinie verwendet, die den Zugriff gestattet oder nicht.

Somit kann für die NAP-Infrastruktur ein ungeschützter und ein geschützter Bereich unterscheiden werden. Im geschützten Bereich stehen zum Beispiel die Datei- oder Exchange-Server. Im ungeschützten Bereich könnte ein WSUS-Server oder der DHCP-Server stehen. Der ungeschützte Bereich ist von der NAP vollkommen unberücksichtigt. Wichtig ist in diesem Bereich die Art und Weise, wie der Zugriff zum Netzwerk stattfindet. Clients können sich per VPN einwählen, auf einen Terminal-Server Gateway zugreifen oder sich mit dem Netzwerk verbinden. Findet die Verbindung über das eigene Netzwerk statt, benötigt ein Client zunächst eine IP-Adresse von einem DHCP-Server. Dieser Zugriff sollte also gestattet werden. Nicht konforme Clients können sogar vom Beziehen einer DHCP-Adresse gehindert werden. Auch der Zugriff per WLAN kann über NAP gesteuert werden.

Die NAP-Infrastruktur basiert auf den drei Pfeilern:

- Systemintegritätsprüfungen (System Health Validators)
- Integritätsrichtlinien (Health Policies)
- Netzwerkrichtlinien (Network Policies)

2.2 Komponenten der NAP

NAP unterstützt verschiedene Funktionsweisen und die damit verbundenen Komponenten, um das Netzwerk zu schützen. Folgende Verbindungsvarianten können von NAP geschützt werden. Diese Komponenten werden von Microsoft auch als Enforcement Components bezeichnet.

IPsec-Kommunikation
Bei der Kommunikation mit IPsec, bekommen NAP-konforme Clients ein Zertifikat und können anschliessend

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

mit anderen IPSec-Computern kommunizieren. Entspricht ein Client nicht den Richtlinien, erhält er auch kein Zertifikat. Für das Ausstellen dieser Zertifikate ist der NAP-Server zuständig. Für diese Funktion wird nicht zwingend eine eigene PKI (Public Key-Infrastruktur) benötigt. Die Komponente in NAP, die dieses Zertifikat ausstellt, trägt die Bezeichnung Health Registration Authority (HRA). Bei den Zertifikaten handelt es sich um standardkonforme X.509-Zertifikate. Bei der NAP-geschützten IPSec-Kommunikation findet folgende Kommunikation statt. Diese Kommunikation findet analog auch bei den anderen Enforcement Components statt:

a) Der Client sendet seine Anforderung an die IPSec Enforcement Component. Der Client verwendet dazu entweder HTTP oder HTTPS (kann auch über die Gruppenrichtlinien definiert werden).
b) Diese sendet den Statement of Health des Clients (SoH) an die HRA.
c) Die HRA sendet die Anfrage an den Netzwerkrichtlinienserver (Network Policy Server, NPS).
d) Der NPS gibt den Status an den HRA zurück, ob der Client konform ist oder nicht und verweist den Client zusätzlich an die notwendigen Wartungsserver, zum Beispiel einen Server mit WSUS 3.0, von dem der Client aktuelle Patches beziehen kann.
e) Ist der Client NAP-konform, teilt die HRA ein Zertifikat zu.
f) Ist der Client nicht konform, erhält er kein Zertifikat, sondern die Anforderung sich mit dem Wartungsserver zu verbinden.
g) Der Client sendet eine Updateanforderung an den Wartungsserver, wenn er nicht NAP-konform ist.
h) Nach der Aktualisierung sendet der Client erneut seinen SoH an den HRA.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

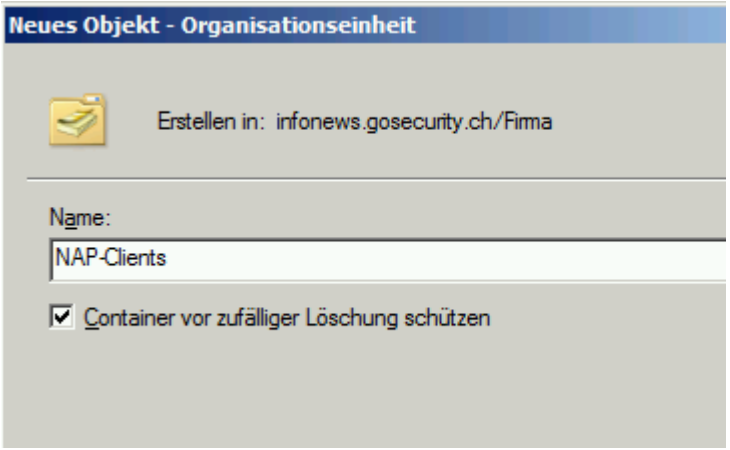
3 Beispiel - NAP mit DHCP

3.1 Einleitung

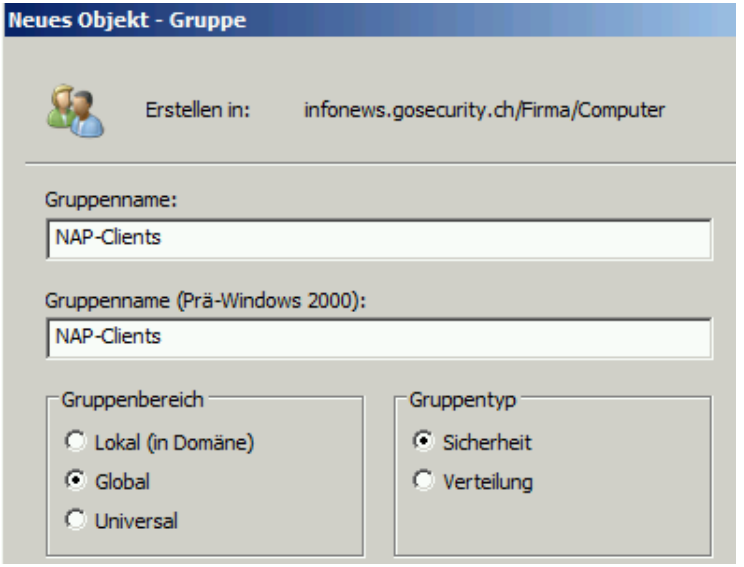
Für dieses Beispiel verwenden wir einen Windows Server 2008. Auf diesem Server werden vorbereitend die folgenden Rollen installiert:

- Active Directory- Domänendienste
- DNS (automatisch bei der Installation des ADs)
- DHCP

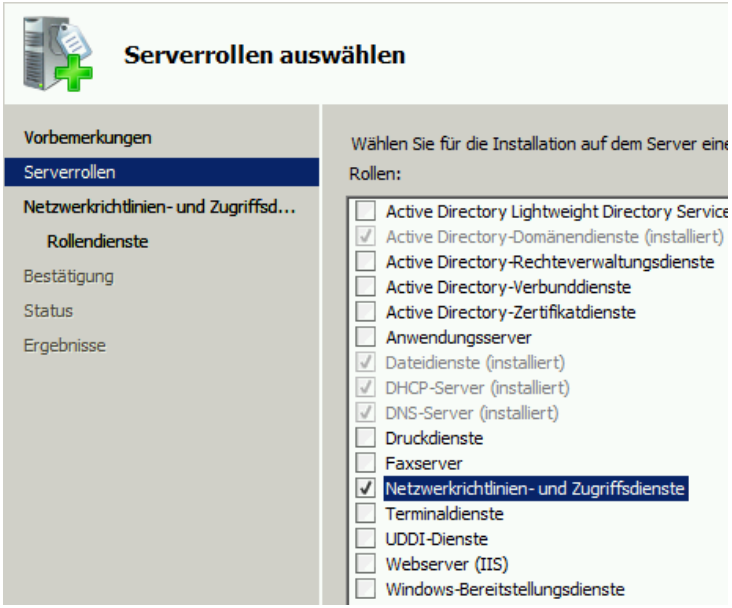
Als erster Schritt wird im Active Directory eine OU für die NAP Clients erstellt.



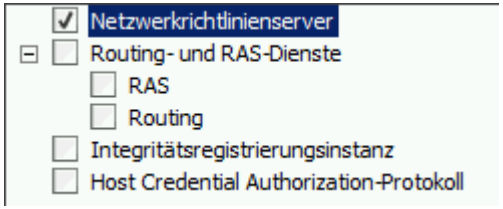
In der OU wird eine Gruppe für die NAP-Clients erstellt. In diese Gruppe werden alle Clients hinzugefügt, auf die die NAP-Einstellungen angewendet werden.



Danach wird die Rolle „Netzwerkrichtlinien- und Zugriffs-dienste“ hinzugefügt:



Benötigt wird der Netzwerkrichtlinienserver:

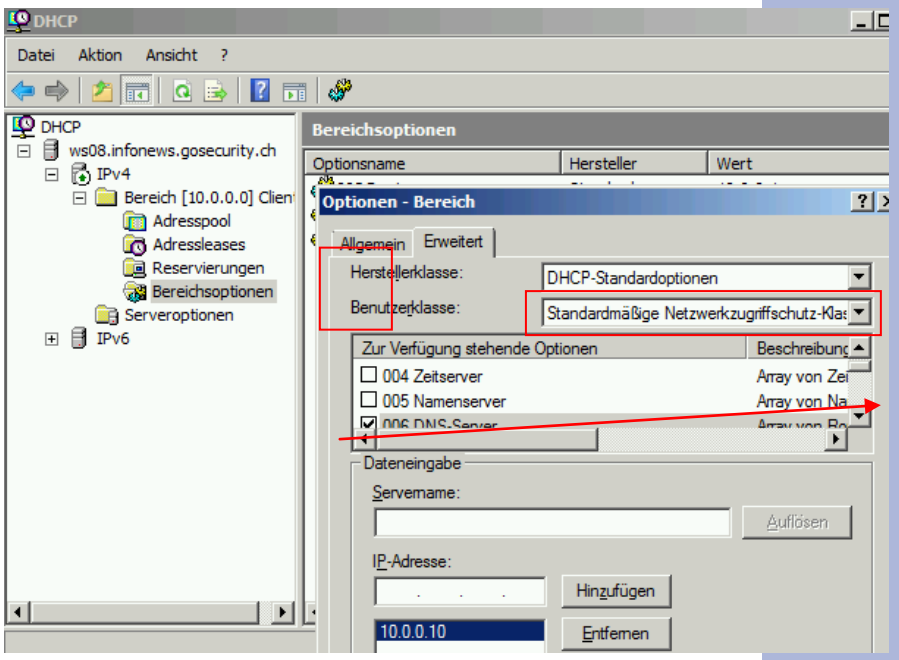


Danach sind drei Schritte notwendig:

- Konfiguration/Anpassen DHCP
- NAP-Policy erstellen
- Gruppenrichtlinie erstellen

3.2 DHCP-Anpassungen

Erfüllt ein Client die NAP-Einstellungen nicht, dann werden alternative DNS-Einstellungen verwendet. Diese finden sich im Register „Standardmässige Netzwerkzugriffsschutz-Klasse“. Hinzugefügt werden die beiden Optionen „006 DNS Server“ und „015 DNS-Domänenname“.

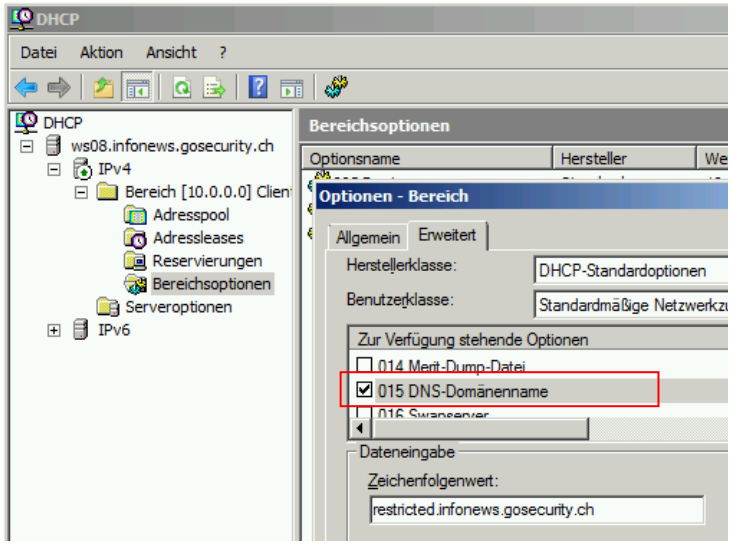


GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

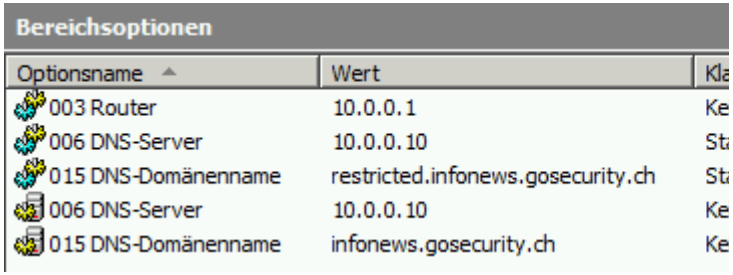
Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

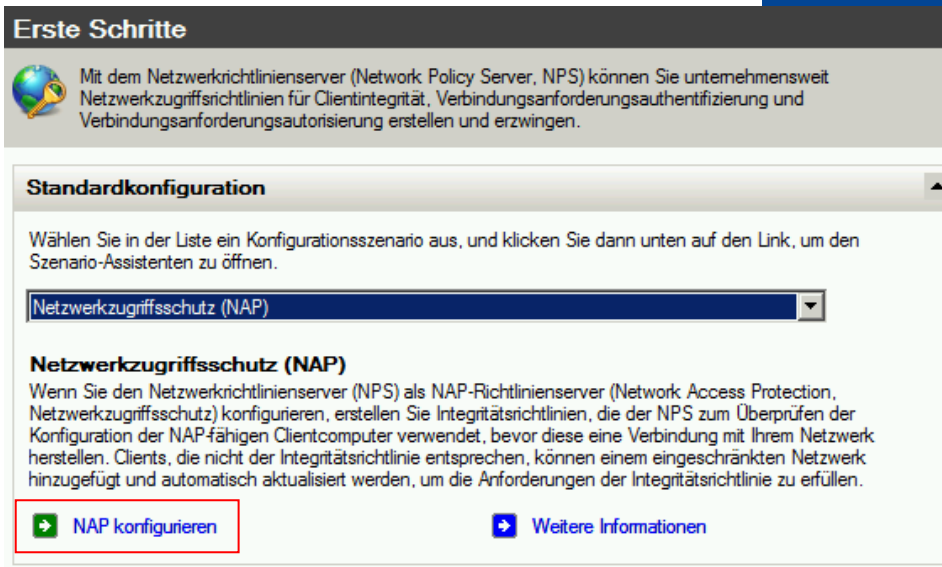


Am Schluss sehen die Einstellungen wie nachfolgend gezeigt aus:



3.3 NAP Konfiguration

Um eine Richtlinie gibt es zwei Möglichkeiten: manuell jede Einstellung vornehmen oder den Wizard ausführen. Für die ersten Schritte empfehlen wir den Wizard zu verwenden und anschliessend Anpassungen nach Bedarf vornehmen. Nachfolgend wird der Wizard gezeigt.



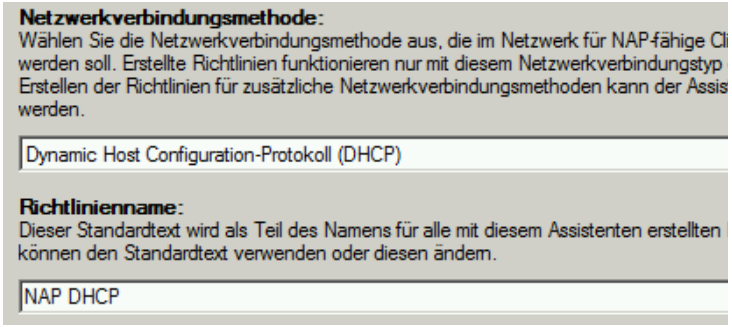
Für dieses Beispiel verwenden wir die Methode über den DHCP Server. Weitere Möglichkeiten, die zur Auswahl stehen:

Wir verwenden „Dynamic Host Configuration-Protokoll (DHCP)“. Der Richtlinienname „NAP DHCP“ belassen wir unverändert.

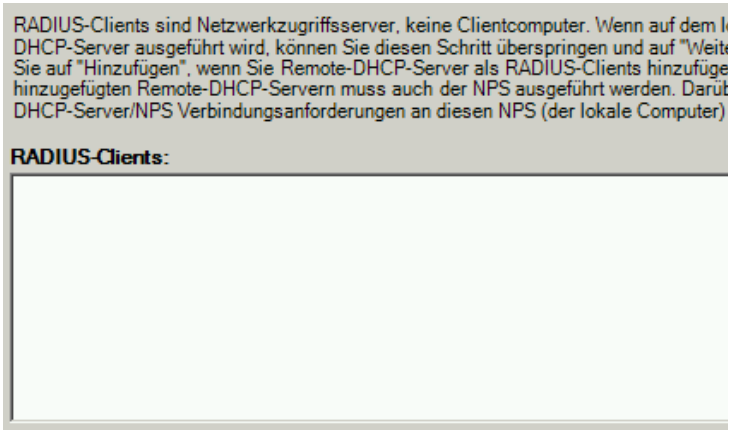
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

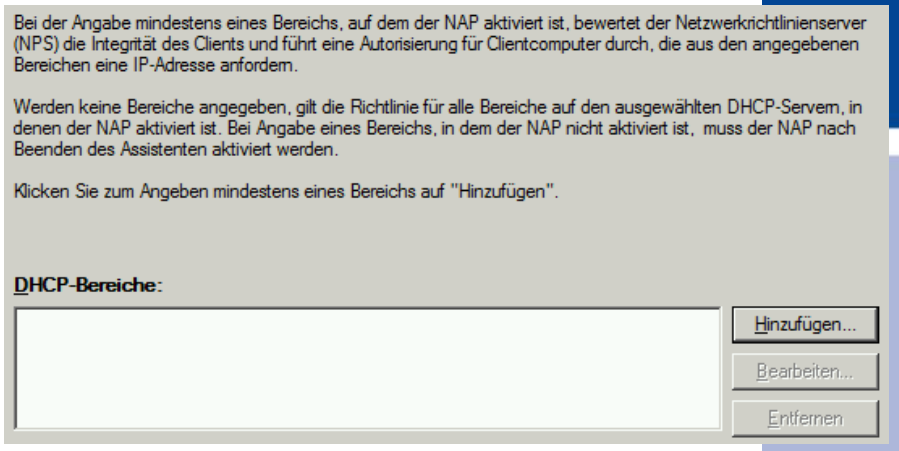
Telefon 052 320 91 20
Fax 052 320 91 21



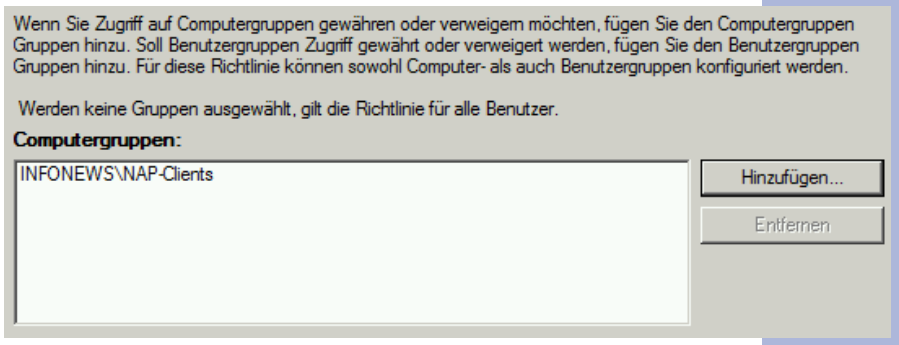
Da der NAP-Server auf dem Domain-Controller installiert wurde, muss hier kein RADIUS-Client angegeben werden (Client bezieht sich nicht auf Clientcomputer!)



Zusätzlich ist es möglich, nur auf einen bestimmten DHCP-Bereich zu wirken. Da wir für diese Übung den gesamten DHCP-Bereich verwenden (10.0.1.1 – 10.0.1.255), kann dieser Eingabebereich übergangen werden.

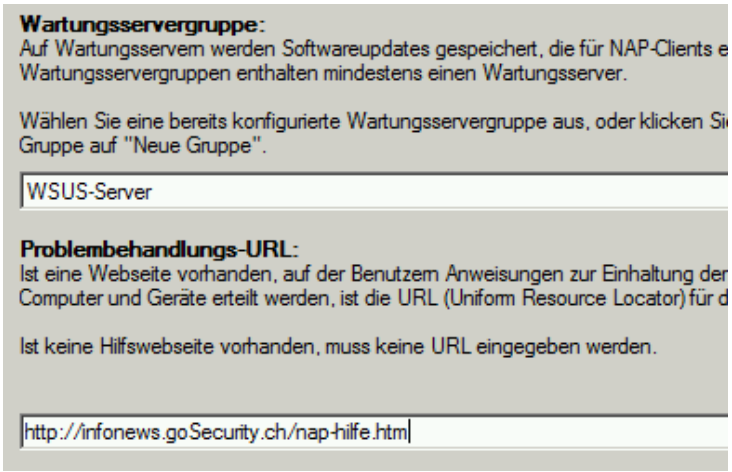


Das Regelwerk kann auf Clients oder Benutzer greifen. Wir verwenden unsere vorbereitete NAP-Clients Gruppe.

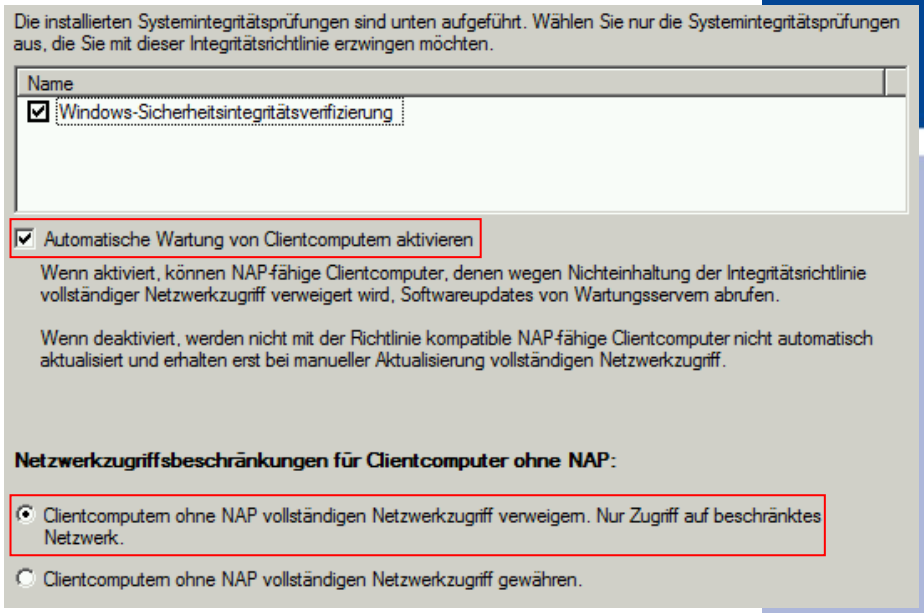


Als Wartungsserver definieren wir einen WSUS-Server. Hier sind weitere Server möglich, z.B. derjenige, der die Antivirenpattern verteilt. Auf diese Server darf ein Client zugreifen, wenn er die Bedingungen der Richtlinie nicht erfüllt.

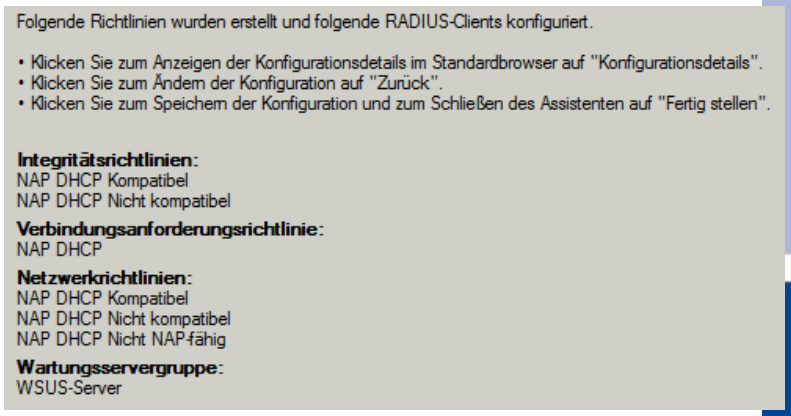
Weiter kann eine Hilfewebseite definiert werden.



Zum Schluss wird angegeben, ob der Client sich automatisch wartet und ob nicht NAP-Clients auf das Netzwerk zugreifen dürfen.



Die Zusammenfassung zeigt, welche Richtlinien automatisch erstellt werden. Diese können anschliessend angepasst werden.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

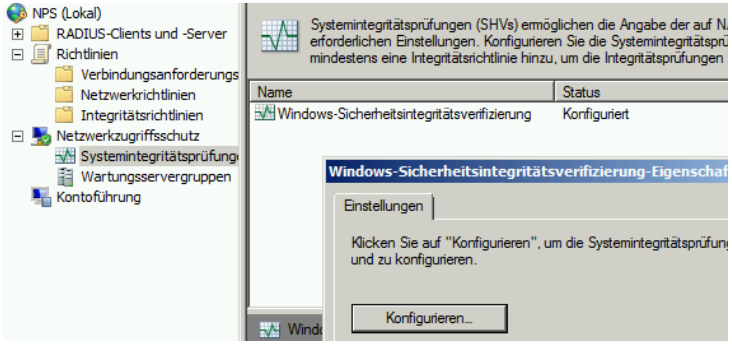
Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

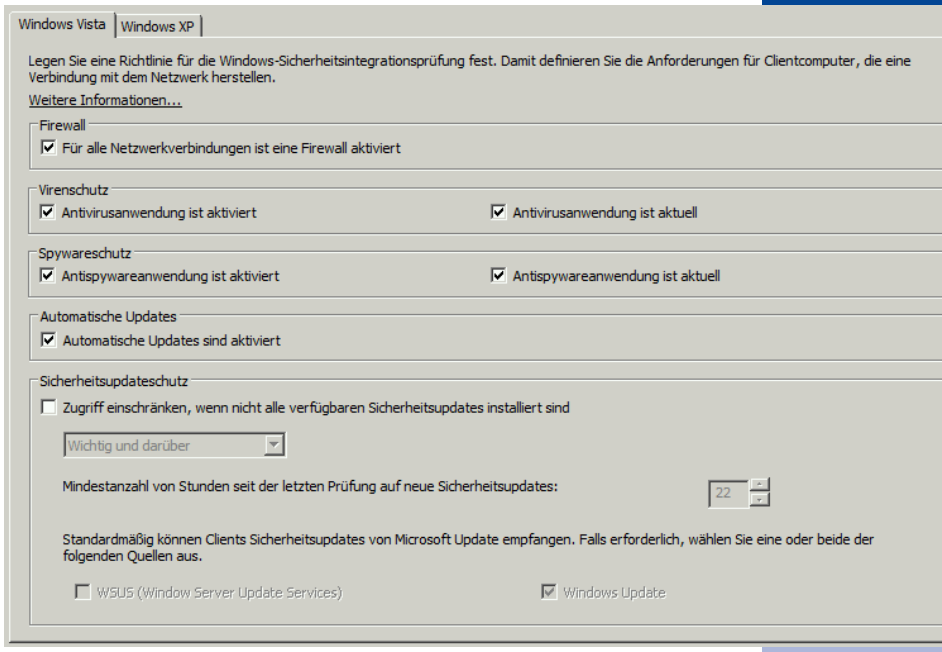
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Unter Netzwerkzugriffsschutz, Systemintegritätsprüfung kann die soeben erstellte Policy angeschaut werden:



Für Vista und XP stehen zwei getrennte Einstellungsmöglichkeiten zur Verfügung. Der Grund dafür ist, dass bei Vista weitere Sicherheitselemente dazu kamen. Untenstehend sehen Sie die möglichen Einstellungen:



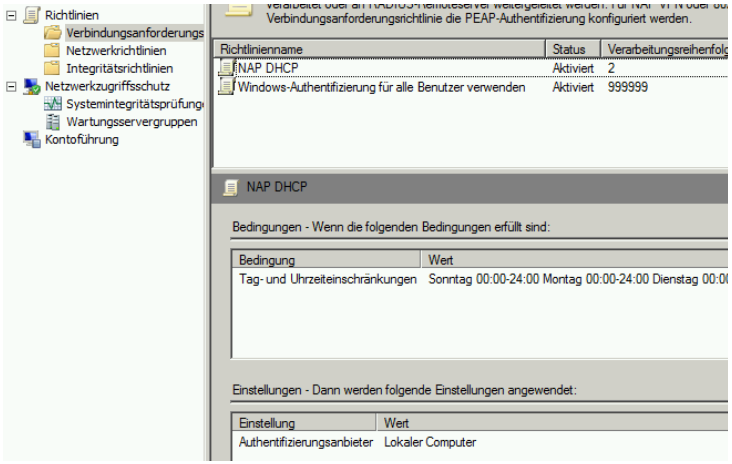
goSecurity.ch/infonews

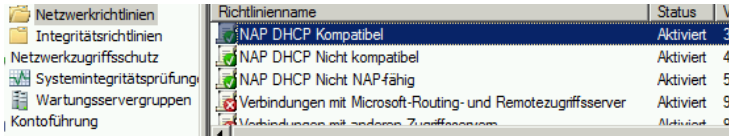
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

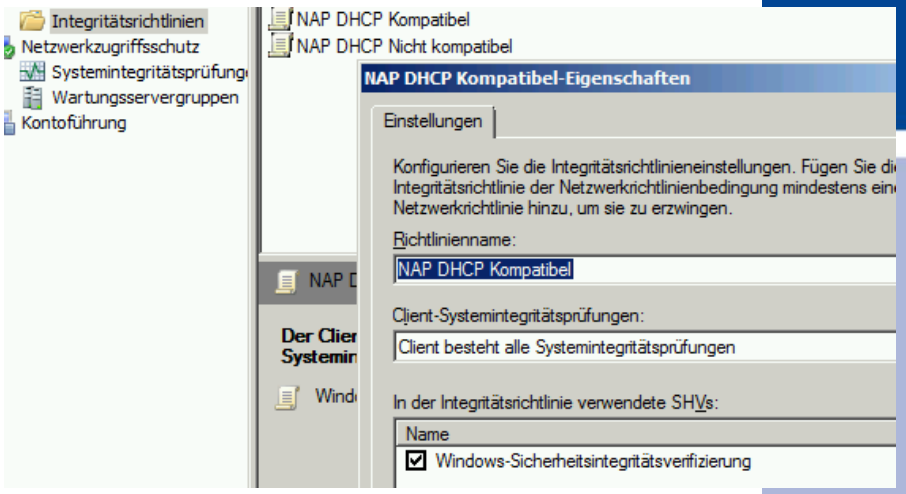
Unter Richtlinien sind die drei Stufen ersichtlich:

- Verbindungsanforderung (in unserem Fall DHCP)
- Netzwerkrichtlinien
- Integritätsrichtlinien

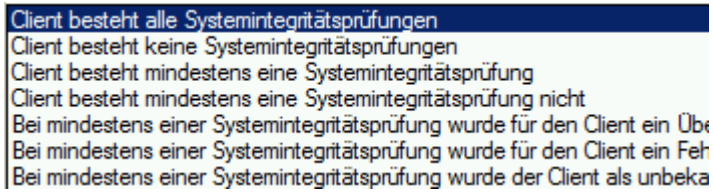




Unter Integritätsrichtlinien kann festgehalten werden, ob alle Prüfungen bestanden werden müssen oder nur Teile davon.

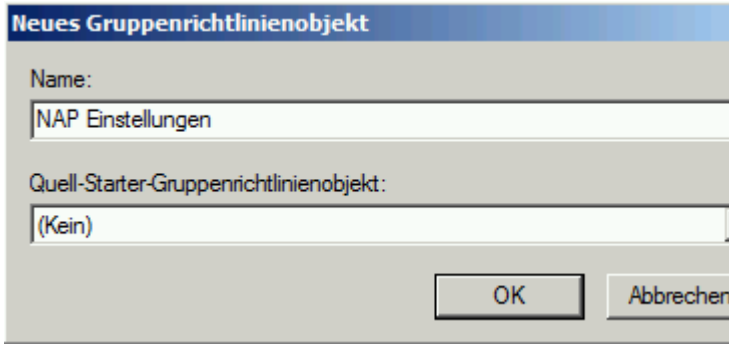


Folgende Möglichkeiten zur Client-Systemintegritätsprüfung stehen zur Verfügung:

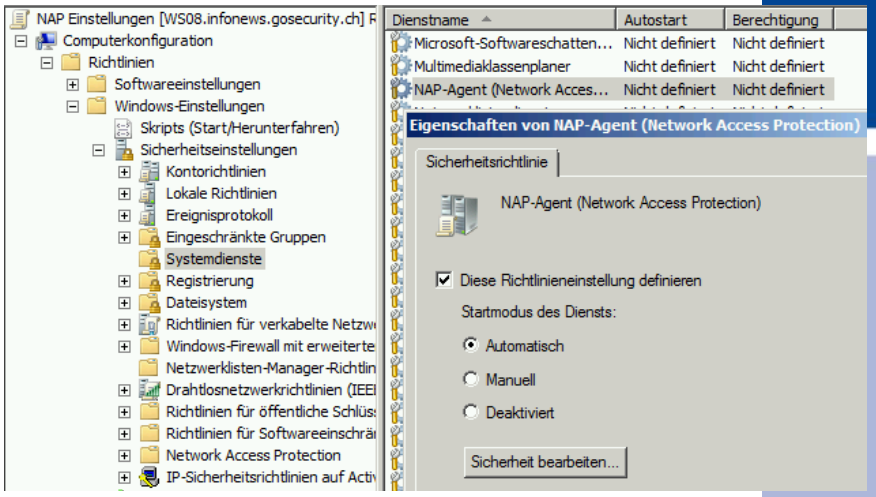


3.4 Gruppenrichtlinien

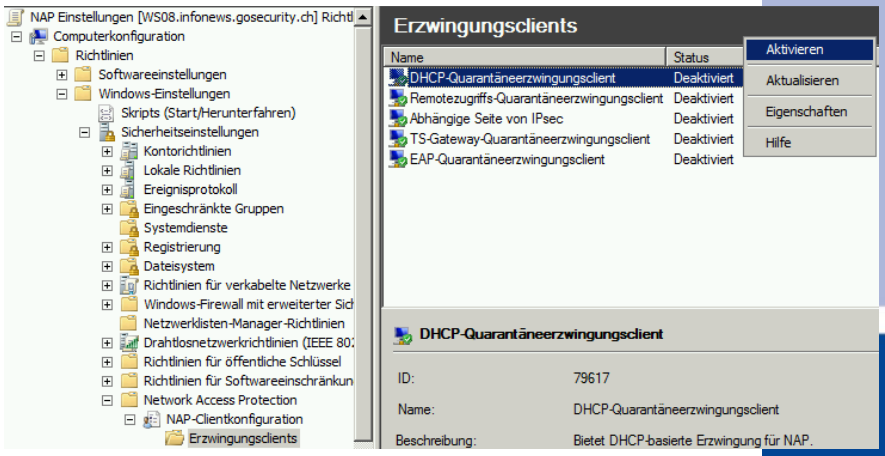
Für alle Clients werden nun die NAP-Einstellungen via Gruppenrichtlinien erzwungen. Dazu wird ein neues Gruppenrichtlinienobjekt erstellt.



Zuerst wird der Dienst „NAP-Agent" automatisch gestartet (Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Systemdienste).



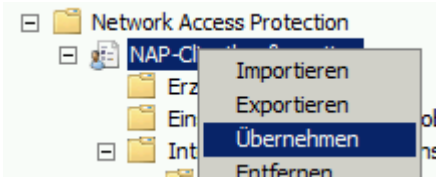
Weiter werden die DHCP Einstellungen erzwungen (Computerkonfiguration – Richtlinien – Windows-Einstellungen – Sicherheitseinstellungen – Network Access Protection – NAP-Clientkonfiguration – Erzwingungsclient – DHCP-Quarantäneerzwingungsclient)



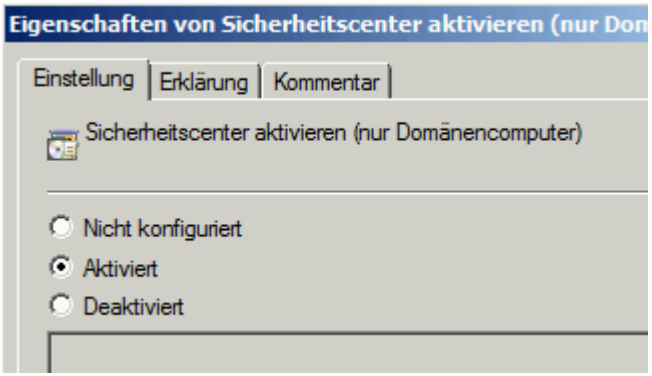
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

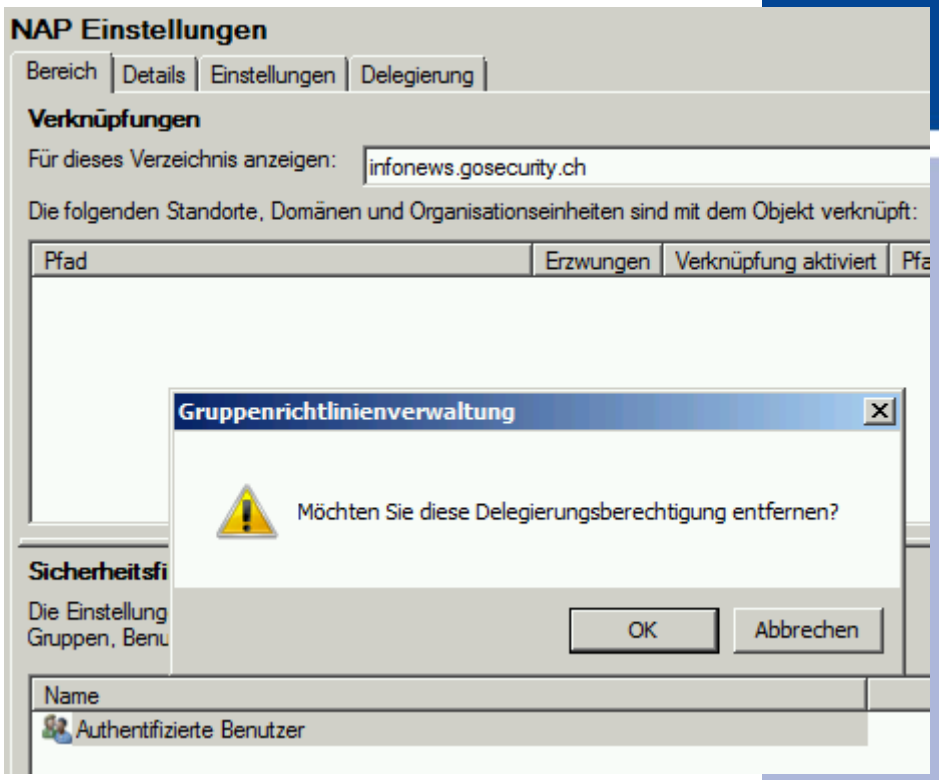
Damit die Einstellungen wirken, müssen diese nun übernommen werden

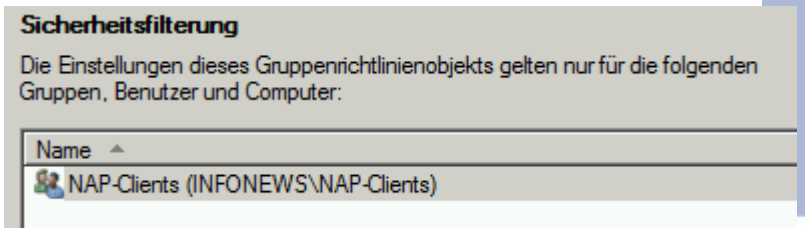


Nun gilt es unter Computerkonfiguration – Richtlinien – Administrative Vorlagen – Windows-Komponenten das Sicherheitscenter aktiviert werden.



Zu guter Letzt werden die Sicherheitseinstellungen angepasst. Dazu wird Gruppe „Authentifizierte Benutzer“ entfernt und die Gruppe „NAP-Clients“ hinzugefügt.





GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Zusammenfassung der Regeln:

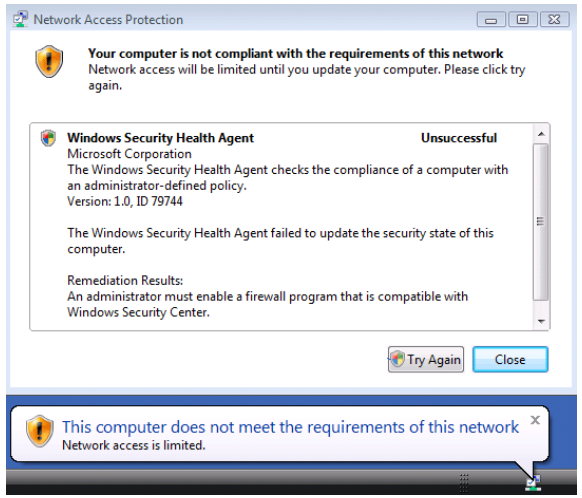
Computerkonfiguration (Aktiviert)		
Richtlinien		
Windows-Einstellungen		
Sicherheitseinstellungen		
Systemdienste		
NAP-Agent (Network Access Protection) (Startmodus: Automatisch)		
Berechtigungen Keine Berechtigungen angegeben		
Überwachung Keine Überwachung angegeben		
Netzwerkzugriffsschutz-Clientverwaltungseinstellungen		
Nachverfolgungseinstellungen		
Erzwingung Clienteinstellungen		
Komponente	**Einstellung**	
@%SystemRoot%\system32\dhcpqec.dll,-100	Aktiviert	
@%Systemroot%\system32\rasqec.dll,-200	Deaktiviert	
@%SystemRoot%\system32\napipsec.dll,-1	Deaktiviert	
@%SystemRoot%\system32\tsgqec.dll,-100	Deaktiviert	
@%SystemRoot%\system32\eapqec.dll,-100	Deaktiviert	
Einstellungen der Benutzerschnittstelle		
Einstellungen der Anforderungsrichtlinie für die Integritätsregistrierungsstelle		
Einstellungen für die vertrauenswürdige Servergruppe		
Administrative Vorlagen		
Richtliniendefinitionen (ADMX-Dateien) wurden aus dem lokalen Computer abgerufen.		
Windows-Komponenten/Sicherheitscenter		
Richtlinie	**Einstellung**	**Ko**
Sicherheitscenter aktivieren (nur Domänencomputer)	Aktiviert	
Zusätzliche Registrierungseinstellungen		

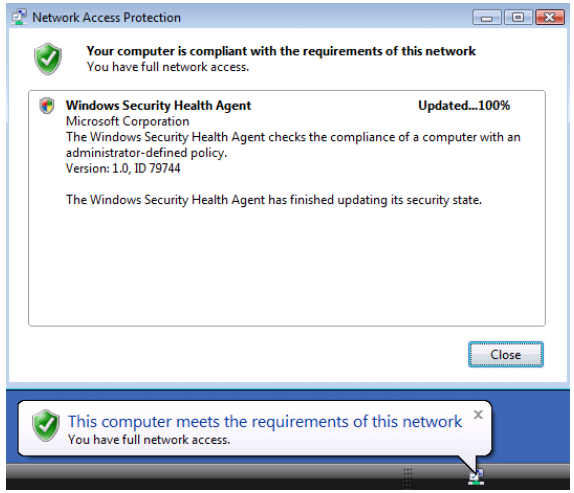
3.5 Quellen

- Microsoft:
  http://www.microsoft.com/windowsserver2008/en/us/nap-technical-resources.aspx
- Thomas Joos
  Microsoft Windows Server 2008 – Das Handbuch

3.6 Client

Die folgenden beiden Screenshots zeigen die Meldungen, ob ein Client die Anforderungen erfüllt oder nicht.





GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21