ERNW Newsletter 18 / August 2007

Liebe Partner, liebe Kollegen,

willkommen zur 18. Ausgabe des ERNW-Newsletters mit dem Thema:

Compliance mit Sophos NAC 3.0 aus Sicht des CISO - Ein dutzend Fragen und Antworten.

Version 1.0 vom 28. August 2007

von:
Friedwart Kuhn, fkuhn@ernw.de
Dror-John Röcher, droecher@ernw.de
Michael Thumann, mthumann@ernw.de

Der folgende Newsletter thematisiert Compliance aus dem Blickwinkel des Chief Information Security Officers (CISO) und analysiert, inwiefern Sophos NAC 3.0 in diesem Kontext ein sinnvolles Werkzeug sein kann.

INHALTSVERZEICHNIS

1 EINLEITUNG

Network Admission Control (NAC) nimmt seit zwei Jahren einen prominenten Platz in der Produktentwicklung und dem Marketing der Hersteller von Security Lösungen und Betriebssystemen ein. Auf Seiten der Hersteller von NAC-Lösungen ist der Begriff nicht einheitlich definiert[1] (anders zum Beispiel bei Antiviren-Software, wo eine allgemeine Übereinkunft über Funktion und Rolle existiert), und auf Seiten der Anwender herrscht Verwirrung, welchen Mehrwert NAC-Lösungen eigentlich bieten können und unter welchen Umständen von der Einführung von NAC abgeraten werden sollte. Die Security-Szene steht, aus ihrem Blickwinkel durchaus zu recht, NAC insgesamt skeptisch gegenüber[2]. Kurz gesagt – der Markt ist noch nicht definiert und NAC sucht seinen Platz. Der vorliegende ERNW-Newsletter soll einen Beitrag leisten, die Möglichkeiten einer spezifischen NAC-Lösung, Sophos NAC in der Version 3.0, auszuloten.

Eine weitere Entwicklung der letzten Jahre ist, dass die klassische IT-Security als Bestandteil einer risikobasierten Betrachtungsweise einer gesamtheitlichen Information Security begriffen wird und diese Information Security immer mehr organisatorisch statt technisch definiert wird. Treibender Faktor hinter dieser Entwicklung ist die Einführung immer neuer (teilweise gesetzlicher) Richtlinien. Die drei großen Richtlinien, die in diesem Zusammenhang die größte Aufmerksamkeit erhalten haben sind die ISO 27001[3], der Sarbanes-Oxley-Act (SOX)[4] und die Richtline „Neue Eigenkapitalanforderungen für Kreditinstitute“ (Basel II)[5]. Im Kern fordern diese Richtlinien, in durchaus unterschiedlicher Ausprägung, ein Risikomanagement der IT- und/oder operativen Risiken und definieren Anforderungen an die Transparenz von Bilanzen und die Revisionssicherheit.

In Deutschland sind neben dem allgegenwärtigen Bundesdatenschutzgesetz[6] (BDSG) der Grundschutzkatalog des Bundesamt für Sicherheit in der Informationstechnik (BSI) und die ebenfalls vom BSI publizierten Standards der 100er-Serie[7] von nicht zu unterschätzender Bedeutung. Insbesondere die erfolgte Anlehnung der BSI-Standards 100-1 und 100-3 an die korrespondierenden internationalen ISO-Normen ISO-27001 (Information Security Management System - Requirements) und ISO-27005 (Information Security Management System - Risk Management) hat zu einer „Wiederbelebung“ und Wertsteigerung des Grundschutzkatalogs beigetragen.

Die Notwendigkeit den vorgenannten Anforderungen im Unternehmen technisch und/oder organisatorisch zu genügen wird allgemein als „Compliance“ bezeichnet – was direkt zu den Fragen führt, wie sich Compliance umsetzen, der Grad der Compliance bewerten oder messen

---

[1] Die Hersteller sind sich nicht einmal einig, ob die Abkürzung NAC für „Network Admission Control“ oder „Network Access Control“ steht. Die Autoren benutzen durchgehend den umfassenderen Begriff „Network Admission Control“ um die Technologie im Allgemeinen zu bezeichnen. So über ein spezifisches Produkt gesprochen wird, wird die Bezeichnung des Herstellers übernommen.

[2] So hat Ofir Arkin schon auf der Blackhat 2006 in Amsterdam in einem bemerkenswerten Vortrag auf die allgemeinen Design-Schwächen von NAC-Lösungen hingewiesen, und die Autoren selbst haben ein Jahr später auf der Blackhat 2007 in Amsterdam zum ersten Mal praktisch demonstriert, wie sich eine spezifische NAC-Lösung, Cisco NAC, durch einen motivierten Angreifer komplett umgehen lässt.

[3] Auch wenn der Kürze wegen „nur“ von der ISO 27001 gesprochen wird, so wird sie natürlich als Fortführung der BS7799 verstanden und im Kontext der weiteren ISO-27000er-Serie Normen betrachtet.

[4] Die Auswirkungen von SOX auf Unternehmen in Deutschland, bzw. auf deutsche Unternehmen sind stark abhängig von der Branche und den Kunden des Unternehmens. Im Zuge dieses Newsletters wird auf eine weitere Betrachtung unter Gesichtspunkten der „SOX-Compliance“ verzichtet.

[5] http://www.bundesbank.de/download/volkswirtschaft/mba/2004/200409mba_baselII.pdf Ähnlich wie im SOX-Umfeld variieren die Auswirkungen der Richtlinie stark von Unternehmen zu Unternehmen. Allerdings ist zu erwarten, dass die Auswirkungen dieser Richtlinie tendenziell zunehmen werden.

[6] https://www.datenschutzzentrum.de/material/recht/bdsg.htm

[7] BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“ ist konzeptionell stark an die ISO 27001:2005 „Information Security Management Systems – Requirements“ angelehnt und kann als Basis für eine Zertifizierung nach ISO 27001 benutzt werden.

und den spezifischen Anforderungen entsprechend berichten lässt? Auch die Fragestellung, inwiefern sich Compliance in einer definierten Weise erzwingen lässt, ist für viele Umgebungen durchaus interessant. Viele Risikomanagement-Werkzeuge werben mit „Compliance Reporting“ auf Knopfdruck, und ohne diese Funktion lässt sich ein Risikomanagement-Werkzeug heute kaum noch verkaufen. Insbesondere die ISO 27001 fordert auch ganz konkret die Messung der Effektivität der eingesetzten Controls[8] - was im weiteren Sinn nichts anderes bedeutet, als den „Grad der Compliance“ zu messen.

Ein interessanter und durchaus vielversprechender Ansatz besteht in der Anwendung einer NAC-Lösung als technisch orientiertes Werkzeug zur Definition, Umsetzung und Kontrolle von Compliance aus Sicht des Chief Information Security Officers (CISO) eines Unternehmens. Genau dieses Szenario untersucht das vorliegende Whitepaper anhand einer spezifischen NAC-Lösung – namentlich Sophos NAC in der aktuellen Version 3.0 in Form von 12 Fragen und Antworten, die den CISO heutzutage typischerweise im täglichen Leben bewegen.

Der erste Teil geht dabei nochmals detailliert darauf ein, warum NAC in der Regel nicht als Security-Werkzeug eingesetzt werden sollte, bevor im zweiten Teil zunächst kurz auf die ISO 27001:2005 eingegangen wird und darauf aufbauend die 12 Fragen und Antworten angesprochen werden. Im Anhang ist eine ausführliche Installationsanleitung für Sophos NAC 3.0 enthalten, da die Original-Anleitung von Sophos in einigen Punkten mehrdeutig oder unvollständig ist.

[8] *Als „Control“ werden im Kontext der ISO-27000er-Normen allgemein Maßnahmen bezeichnet, die ein wohl-definiertes Ziel (s.g. Objectives) umsetzen sollen. Im Gegensatz zu den Maßnahmen des Grundschutzkatalogs werden die Controls in ISO 27001 bzw. 27002 generisch und nicht konkret bezeichnet.*

2 NETWORK ADMISSION CONTROL ALS SECURITY WERKZEUG?

2.1 Information Security

Ein funktionierender InfoSec-Security-Prozess besteht aus 3 Teilschritten[9]: *Definition*, *Umsetzung* und *Kontrolle*. Diese Kernpunkte beschäftigen sich im Unternehmensprozess „Information Security" mit sehr unterschiedlichen, aber aufeinander aufbauenden Fragestellungen.

Definition:

- Was soll wogegen geschützt werden?
- Warum ist etwas schützenswert?

Hier fließen neben internen (meist betriebswirtschaftlichen) Aspekten auch externe „Zwänge", wie etwa gesetzliche Anforderungen ein (z. B. Einhaltung des BDSG, Bilanzierung nach SOX für eine Notierung an der New Yorker Börse oder die Einhaltung der Richtlinien „Basel II" bzgl. Fremdfinanzierung von Krediten bei Geldinstituten).

Umsetzung:

- Welche Maßnahmen werden zum Schutz getroffen?
- Welche Maßnahmen werden nicht getroffen?
- Implementierung der gewählten Maßnahmen.

Die Umsetzung von Maßnahmen, bzw. die Entscheidung über die Umsetzung ist das, was im Allgemeinen unter dem Begriff „IT-Security" verstanden wird. Dazu gehört der Einsatz von technischen Werkzeugen wie Firewalls und Intrusion Detection-Systemen, aber auch organisatorische Werkzeuge wie Geheimhaltungserklärungen und Vertragsgestaltung mit externen Partnern sind Bestandteil eines gesamtheitlichen Information Security-Ansatzes. Auch das in diesem Newsletter diskutierte NAC-Beispiel, Sophos NAC 3.0, fällt in die Kategorie der technischen Maßnahmen.

Kontrolle:

- Greifen die Maßnahmen (noch)?
- Gewährleisten die getroffenen Maßnahmen die Erreichung der definierten Ziele?

Der Teilschritt „Kontrolle" stellt sicher, dass die definierten Ziele tatsächlich erreicht werden und die Maßnahmen effektiv sind.

Im Sinne dieses Information Security-Prozesses ist Compliance ein wesentlicher Bestandteil, zum einen innerhalb der Planung (Wie kann Information Security unter Einhaltung aller anzuwendenden Richtlinien umgesetzt werden? Welche technischen und organisatorischen Bestandteile müssen umgesetzt werden?) und zum anderen innerhalb der Kontrolle (Wie groß ist der Grad der Einhaltung der Richtlinien? Welche Verstöße gibt es?).

---

[9] *Ein Information Security Management System (ISMS) nach ISO 27001 basiert auf 4 Schritten „Plan, Do, Check, Act" (PDCA) – die Begründung dafür liegt unter anderem im strukturellen Abgleich der ISO 27001 mit den ISOs 9001 (Anforderungen an Qualitätsmanagementsysteme) und 14001 (Anforderungen an Umweltmanagementsysteme) siehe auch Abschnitt 3.1.*

2.2 Funktionsweise gängiger NAC-Lösungen

Die am Markt erhältlichen NAC-Lösungen bestehen üblicherweise aus den folgenden Komponenten:

- Data Collector: Der Data Collector ist meistens in Form eines Software Agenten implementiert, der auf Systemen installiert wird und Daten über die Konfiguration und den Zustand des Systems (z.B. Version des Betriebssystems, installierte Security Patches oder Aktualität der Virenschutz-Signaturen) an den Policy Server meldet.
- Policy Server: Der Policy Server ist eine Backend-Komponente, auf Anforderungen an die am Netzwerk teilnehmenden Systeme in der Form von definiert sind. Der Policy Server vergleicht die vom Data Collector gemeldeten Daten mit dem Soll-Zustand und entscheidet, ob ein System uneingeschränkt oder eingeschränkt am Netzwerk teilnehmen darf.
- Quarantäne- und Remediation Zone: Hierbei handelt es sich um ein dediziertes Netzwerksegment, dem Systeme zugeordnet werden, welche den definierten Anforderungen nicht genügen. Innerhalb dieses Netzwerkes befindet sich üblicherweise eine Komponente, der s. g. Remediation Server, mit dessen Hilfe ein System einen den Anforderungen genügenden Zustand erreichen kann. Diese Netzwerksegmente werden in der Regel mit Hilfe von Netzwerk Komponenten wie Switches (VLAN Konfiguration) und / oder Routern (Access-Listen) abgebildet.

Dieses Gesamtsystem kann (fälschlicherweise) als eine Art intelligente Firewall verstanden werden, die, basierend auf dem Zustand eines Systems, die Kommunikation mit wichtigen Unternehmensressourcen erlaubt oder verbietet - NAC wäre nach diesem Verständnis ein technisches Security-Werkzeug.

2.3 NAC als technisches Werkzeug

Üblicherweise sollen technische Maßnahmen, bzw. Werkzeuge in einem IT-Security-Prozess folgende Aufgaben zuverlässig und effektiv erfüllen:

- Verringerung der Eintrittswahrscheinlichkeit eines Schadens
- Minimierung der Auswirkung beim Eintreten eines Schadens
- Feststellen, dass ein Schaden eingetreten ist

Man kann NAC in die erste Kategorie (Verringerung der Eintrittswahrscheinlichkeit) einordnen, da etwa Systeme mit veralteten Antivirus-Signaturen nicht „ins Netz gelassen“ werden und dadurch die Wahrscheinlichkeit eines Wurm- oder Virusausbruchs im Netzwerk minimiert wird. Aber speziell die Zuverlässigkeit und Effektivität eines Werkzeugs, welches Entscheidungen an Hand von fremdgelieferten Informationen trifft, ist abhängig von der Vertrauenswürdigkeit der Informationsquelle und der Qualität der von der Quelle gelieferten Informationen. Klassische Firewalls sind ein Beispiel für diese Art der Informations-Qualitätssicherung: Der Firewall-Regelsatz (wer darf welche Ressourcen nutzen?) wird von definierten Personen (Firewall Administratoren) von definierten Management-Clients aus gepflegt, um sowohl die Qualität der Regeln als auch ihre Vertrauenswürdigkeit zu gewährleisten.

Der entscheidende Unterschied zwischen einer Firewall und NAC liegt genau in der fehlenden Qualitätssicherung der Informationen. Ziel von NAC ist es, ein nicht vertrauenswürdiges System zu bewerten – und dies geschieht, indem Informationen, die das nicht vertrauenswürdige System selber liefert, als Bewertungsgrundlage herangezogen werden. Dadurch wird dem System, das die Informationen liefert und das eigentlich nicht vertrauenswürdig ist, vertraut. Der immanente Widerspruch ist dabei offensichtlich. In letzter Konsequenz bedeutet dies, dass die vorgenannten Aufgaben eines technischen Security Werkzeugs von einer NAC-Lösung nicht hundertprozentig erfüllt werden können: denn weder kann ein möglicher Schaden in jedem Fall

erkannt, noch kann dessen Eintrittswahrscheinlichkeit immer verringert, bzw. die Auswirkungen minimiert werden. Alles hängt letztlich an der Vertrauenswürdigkeit des zu prüfenden Objekts.

2.4 Fazit

Unter einem streng technischen Gesichtspunkt ist NAC als technisches Werkzeug innerhalb des IT-Security-Teilschritts *Umsetzung* ungeeignet, da es die typischen Anforderungen an ein Security Werkzeug nicht hundertprozentig erfüllen kann. Typische Anwender sind allerdings nicht in der Lage den Zugangsschutz, den NAC Lösungen bieten, ohne Weiteres zu umgehen. Motivierte Angreifer werden durch NAC vor eine weitere, mit entsprechendem Know-How überwindbare, Hürde gestellt. Somit kann NAC unter praktischen Gesichtspunkten einen weiteren Beitrag zur Erhöhung der Security innerhalb einer Organisation bieten – sofern der ordnungsgemäße Betrieb durch die Organisation gewährleistet ist. Oder um es mit den Worten von Dan Kaminsky auf der Blackhat 2007 in Las Vegas, USA, zur formulieren: „Wenn ein Produkt nicht als Security Werkzeug konzipiert worden ist, dann wundern Sie sich nicht, wenn es auch nicht als Security Werkzeug funktioniert."

3 NETWORK ADMISSION CONTROL ALS COMPLIANCE-WERKZEUG

Im vorhergehenden Abschnitt wurde dargestellt, weshalb NAC die Erwartungen als technisches Security Werkzeug in der Regel nicht erfüllen kann. Daraus abzuleiten, dass NAC keinen Mehrwert innerhalb der Information Security bietet, wäre kurzsichtig. Ein interessanter und durchaus vielversprechender Ansatz ist der Einsatz von NAC als Compliance-Masurin-Werkzeug und/oder Compliance-Enforcement-Werkzeug. Dieser Ansatz wird am Beispiel Sophos NAC 3.0 und der ISO 27001, bzw. ISO 17799 diskutiert.

3.1 ISO 27001 & ISO 17799[10]

Die ISO 27001:2005, betitelt „Information technology - Security techniques - Information Security Management Systems - Requirements“, beschreibt Anforderungen an ein „ISMS“. Der strukturelle Aufbau eines ISMS ist dabei an den Aufbau von Qualitätsmanagement-Systemen angelehnt; dies wird insbesondere in der gewählten „Plan – Do – Check – Act“-Methodik sichtbar, die den Management-Kreislauf für jede Komponente beschreibt. Die generischen Anforderungen, die an das ISMS gestellt werden, sind in folgende Kategorien unterteilt [11]:

4.1 General requirements
4.2 Establishing and managing the ISMS
4.3 Documentation requirements
5 Management responsibility
5.1 Management commitment
5.2 Resource management
6 Internal ISMS audits
7 Management review of the ISMS
7.1 General
7.2 Review input
7.3 Review output
8 ISMS improvement
8.1 Continual improvement
8.2 Corrective action
8.3 Preventive action

[10] *Die ISO 17799:2005 wird im Lauf des Jahres 2007 als ISO 27002 in einer aktualisierten Version veröffentlicht werden. Aufgrund „alter Gepflogenheiten“ verwenden die Autoren noch die Bezeichnung ISO 17799.*
[11] *Die Nummern beziehen sich auf die entsprechenden Abschnittsnummern der ISO 27001.*

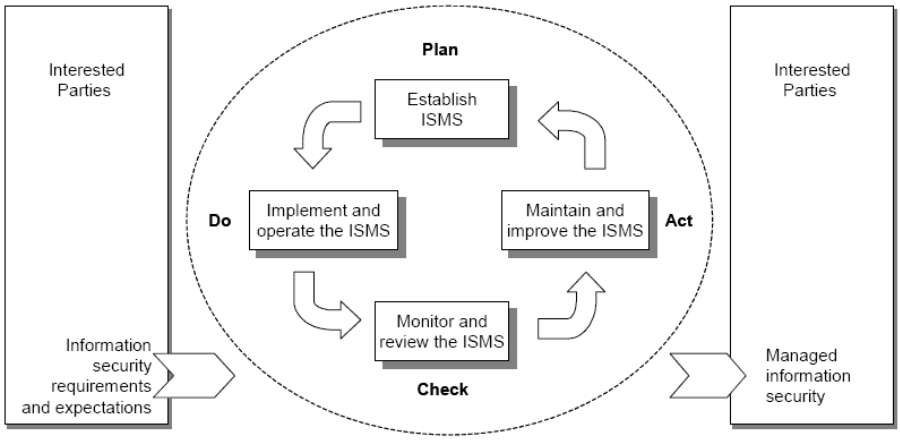


Abbildung 1 - Beispiel-PDCA Zyklus für das gesamte ISMS

Die in der ISO 27001 aufgestellten Anforderungen an ein ISMS werden durch Handlungsempfehlungen in ISO 17799:2005 „Information technology - Security techniques - Code of practice for information security management“ ergänzt. Diese Handlungsempfehlungen umfassen einen kategorisierten Maßnahmenkatalog, der als Vorschlag zur Umsetzung empfohlen wird und folgende Themengebiete beinhaltet [12]:

4 RISK ASSESSMENT AND TREATMENT
5 SECURITY POLICY
6 ORGANIZATION OF INFORMATION SECURITY
7 ASSET MANAGEMENT
8 HUMAN RESOURCES SECURITY
9 PHYSICAL AND ENVIRONMENTAL SECURITY
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT
11 ACCESS CONTROL
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
13 INFORMATION SECURITY INCIDENT MANAGEMENT
14 BUSINESS CONTINUITY MANAGEMENT
15 COMPLIANCE

Ähnlich wie Qualitätsmanagement-Systeme nach ISO 9001 zertifiziert werden können, können Information-Security-Management-Systeme nach ISO 27001 zertifiziert werden. Nach ISO 17799 kann aufgrund des Dokumenten-Charakters nicht zertifiziert werden. Im Kontext des vorliegenden Newsletter soll besonders auf die Abschnitte 15.1 (Compliance with legal requirements) und 15.2 (Compliance with security policies and standards, technical compliance“ hingewiesen werden. Die Zielsetzung für den Abschnitt 15.2 lautet:

> „Objective: To ensure compliance of systems with organizational security policies and standards.”

Die inhaltliche Nähe zu NAC-Lösungen liegt auf der Hand.

[12] *Die Nummern beziehen sich auf die Nummerierung der ISO 17799:2005*

4 DAS DUTZEND FRAGEN & ANTWORTEN – HILFE FÜR DEN CISO

4.1 Welche Anforderungen resultierend ISO 27001 bzw. ISO 17799 sind für den CISO relevant?

Als Hauptverantwortlicher der Information Security innerhalb einer Organisation sind fast alle Anforderungen aus der ISO 27001 für den CISO[13] direkt oder indirekt relevant – falls die Organisation basierend auf diesen Normen arbeitet oder falls die Organisation eine Zertifizierung nach ISO 27001 anstrebt. Aber auch wenn keine Zertifizierung angestrebt wird, kann ISO 27001 als Leitfaden sinnvoll eingesetzt werden. In erster Linie ist der CISO verantwortlich für den Aufbau und den Betrieb des ISMS – das Monitoring und die Prüfung liegen, je nach Aufstellung der Organisation, ggf. auch in der Verantwortlichkeit des CISO. Die in ISO 27001 im Abschnitt 5.1 thematisierte Anforderung „Management responsibilty" bildet die offensichtliche Ausnahme, da hier direkt das Top-Management einer Organisation in die Verantwortung genommen wird.

Die ISO 17799 definiert Handlungsempfehlungen im Kontext der Information Security – als Gesamtverantwortlicher für die Information Security sind auch diese Handlungsempfehlungen für den CISO direkt oder indirekt relevant.

Gleichzeitig bildet der CISO die Schnittstelle der Information Security zum Top-Management (woraus sich ergibt, dass er auf die Einhaltung der Anforderung „Management responsibility" der ISO 27001 durch das Management pochen kann/muss) und ist verantwortlich für das Reporting an den Vorstand. Als „Richtlinieninstanz" ist die „Sicherheitskultur" und ggf. auch die „Risiko-Kultur" einer Organisation maßgeblich durch den CISO geprägt.

4.2 Wie können diese Anforderungen organisatorisch umgesetzt werden?

Die organisatorische Umsetzung der Anforderungen geschieht durch (a) Inkraftsetzen von Policies, (b) Strukturierung von Prozessen und Verantwortlichkeiten und (c) Qualifizierung von Mitarbeitern.

Security Policies definieren den organisatorischen Rahmen der Information Security und finden ihr Abbild in den darauf aufbauenden Prozessdefinitionen. Die Mitarbeiter müssen qualifiziert sein, um den ihnen zugewiesenen Verantwortlichkeiten gerecht werden zu können.

Darüber hinaus ist die ISO 17799:2005 in der Definition der Anforderungen sehr generisch und häufig kann eine Anforderung sowohl technisch als auch organisatorisch erfüllt werden. Als Beispiel sei hier aus Abschnitt 10.1.4 *Separation of development, test, and operational facilities* zitiert:

> Control
> Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.
> Implementation guidance
> The level of separation between operational, test, and development environments that is necessary to prevent operational problems should be identified and appropriate controls implemented.

Ob die Trennung physisch (VLANs, eigene Netze) oder per Policy („Verbot der Übernahme von Produktivdaten in Testumgebungen" umgesetzt wird, ist eine Einzelfallentscheidung.

[13] *Ein interessanter Artikel zur Funktion des CISO wurde 2005 auf silicon.de veröffentlicht: http://www.silicon.de/enid/security_management/15462*

4.3 Wie können diese Anforderungen technisch umgesetzt werden?

Die Anforderungen der ISO 27001 an ein Information Security Management System sind in erster Linie organisatorischer Natur. Anders sieht es bei den Handlungsempfehlungen nach ISO 17799:2005 aus, da dort nicht das Management-System, sondern die Control-Objectives adressiert werden. Die Maßnahmen, die technisch adressiert und durch NAC-Lösungen erfasst werden können (entweder in der Form „Umsetzung durch NAC“ oder in der Form „Prüfung auf Compliance durch NAC“), sind zusammengefasst in der nachfolgenden Tabelle dargestellt:

Abschnitt	Kategorie	Control
10.1.2	Change Management	Changes to information processing facilities and systems should be controlled.
10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.
10.10.1	Audit Logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
10.10.2	Monitoring System Use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.
11.2.4	Review of user access rights	Management should review users’ access rights at regular intervals using a formal process.
11.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.
11.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
11.4.5	Segregation in networks	Groups of information services, users, and information systems should be segregated on networks.
11.4.6	Network Connection Control	For shared networks, especially those extending across the organization’s boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications
11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.
12.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.
12.5.1	Change control procedures	The implementation of changes should be controlled by the use of formal change control procedures.

15.2.1	Compliance with security policies and standards	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
15.2.2	Technical Compliance Checking	Information systems should be regularly checked for compliance with security implementation standards.

4.4 Welche angemessenen Metriken zur Messung des Compliance-Grads können definiert werden?

Security Metriken[14] sind zwar an sich kein neues Thema, allerdings wurden Metriken im Bereich der Information Security lange Zeit stiefmütterlich behandelt – obwohl sie eigentlich eine immanent wichtige Aufgabe innerhalb der Information Security wahrnehmen. Die beste den Autoren bekannte Definition von IT-Metriken geht auf Maizlitsh und Handler zurück[15]:

> "There are two fundamental types of metrics that must be considered before commencing with IT portfolio management: value delivery and process improvement. Value delivery consists of cost reduction, increase in revenue, increase in productivity, reduction of cycle time, and reduction in downside risk. Process improvement refers to improvements in the IT portfolio management process."

Eine "gute" Metrik zeichnet sich dadurch aus, dass sie

(a) konsistent gemessen wird und die Messung frei von subjektiven Einflüssen ist
(b) einfach, am besten automatisch, erfasst werden kann
(c) als Kardinal- oder Prozentzahl angegeben wird, nicht qualitativ als „hoch", „mittel oder „niedrig"
(d) kontextsensitiv und spezifisch ist, so dass sie als Entscheidungsgrundlage belastbar ist

Die ISO 27001 und die ISO 17799 verlangen immer, dass ein Control auch gemessen und berichtet wird – somit lassen sich aus den Controls des Abschnitts 4.3 direkt Metriken ableiten, die eine NAC Lösung prinzipiell erfassen kann – automatisch und kontinuierlich:

Abschnitt	Kategorie	Control	Metrik
10.1.2	Change Management	Changes to information processing facilities and systems should be controlled.	Wieviele Änderungen an Systemen wurden durchgeführt?
10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	Wieviele Systeme haben (k)einen aktuellen Virenschutz? Wieviele Virenvorfälle pro Monat? Wieviele nicht-löschbare Viren pro Monat?

[14] *Dem interessierten Leser sei an dieser Stelle das Buch "Security Metrics – Replacing Fear, Uncertainty and Doubt", von Andrew Jaquit, Addison-Wesley,2007, ISBN-10: 0321349989, wärmsten zur Lektüre empfohlen.*
[15] *B. Maizlitsh and R. Handler, IT Portfolio Management: Step by Step, John Wiley & Sons, 2005, ISBN 0471649848*

10.10.1	Audit Logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Wieviele sicherheitsrelevante Benutzer-Aktivitäten pro Benutzer oder Zeitraum?
11.2.4	Review of user access rights	Management should review users' access rights at regular intervals using a formal process.	Wieviele / welche Benutzer verfügen lokal über administrative/erhöhte Privilegien?
11.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.	Wieviele unautorisierte Zugriffsversuche auf bestimmte Ressourcen gibt es pro Zeitintervall?
11.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	Wieviele automatisch identifizierte Systeme greifen auf das Netzwerk zu? Wieviele nicht identifizierte Systeme greifen auf das Netzwerk zu?
11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should Be restricted and tightly controlled.	Welche System-Utilities werden wie oft benutzt?
12.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.	Wie viele nicht-autorisierte Softwarepakete sind installiert?
15.2.2	Technical Compliance Checking	Information systems should be regularly checked for compliance with security implementation standards.	Wie viele Verstösse gegen die Security Policy gibt es auf den Endsystemen?

4.5 Welchen Compliance-Anforderungen muss das Reporting genügen?

Das Reporting selbst sollte transparent, reproduzierbar und aussagekräftig sein und den Anforderungen einer internen Revision oder internen Audit-Abteilung, in Abhängigkeit von der Unternehmenspolicy auch einem externen Audit genügen. Die ISO 27001 bzw. die ISO 17799 definieren umfangreiches Reporting innerhalb der einzelnen Objectives, nicht jedoch als gesonderten Punkt. Eine Ausnahme bildet da Abschnitt 13.1 der ISO 17799 „Reporting Information Security Events and Wagnisses" – der allerdings auch thematisch einen Sonderfall darstellt und im Kontext dieses Newsletter nicht weiter betrachtet wird.

4.6 Wie kann mit non-compliant Systemen umgegangen werden?

Non-compliant Systeme lassen sich in 2 Kategorien unterteilen:

(a) Organisationseigene Systeme. Organisationseigene Systeme können entweder Systeme sein, die am Netzwerk teilnehmen aber systembedingt den Anforderungen nicht genügen können (auf Druckservern und TK-Anlagen kann üblicherweise keine Antiviren-Software installiert werden), oder aber es handelt sich um Systeme, auf denen die Prozesse, die Systeme compliant halten, versagt haben (etwa wenn aufgrund eines Fehlers die aktuellste Virensignatur-Datei nicht eingespielt werden konnte).

(b) Organisationsfremde Systeme: Notebooks von Besuchern und Consultants, die an das Organisationsnetzwerk angeschlossen werden, sind als fremde Systeme per se nicht vertrauenswürdig und sollten von der Security Policy immer als non compliant eingestuft werden.

Für die Behandlung von non-compliant Systemen stehen grundsätzlich folgende Optionen zur Verfügung:

(a) Beschränkung auf ein Gast-Netzwerk: Aus dem Gast-Netzwerk ist üblicherweise der Zugriff aufs Internet per http, https, und ftp möglich, aber der Zugriff auf Organisationsressourcen ist unterbunden.

(b) Beschränkung auf ein Remediation-Netzwerk: Dieser Ansatz macht nur für organisationsinterne Systeme Sinn. Einem System werden Werkzeuge zur Verfügung gestellt, um den Soll-Zustand zu erreichen. Ein Zugriff auf Organisationsressourcen ist nicht möglich, Zugriff auf das Internet auch nicht.

(c) Beschränkung auf ein Quarantäne Segment: Im Vergleich zum Remediation-Netzwerk bietet das Quarantäne-Netzwerk dem Benutzer keine Werkzeuge zur Herstellung des Soll-Zustands an. Es ist zwingend ein Eingreifen durch einen Administrator notwendig.

(d) No-Access: Der Zugang zum Netzwerk wird vollständig unterbunden.

(e) Limited Access: Definierte Organisationsressourcen (z.B. Email und Internet) sind verfügbar, alle weiteren Zugriffe (etwa Fileservices oder SAP) sind unterbunden.

(f) Full Access: Der Verstoß gegen die Policy wird festgestellt und geloggt, hat aber für den Benutzer keine weiteren Konsequenzen.

Für die Wahl der Behandlungsoptionen ist insbesondere die Fähigkeit der NAC-Lösung zwischen eigenen und fremden Systemen zu unterscheiden ausschlaggebend. Auch im Sinne des Compliance-Reporting spielt die Unterscheidung eine Rolle. Eine Aussage „Wir haben im Schnitt 5000 Zugriffe durch non-compliant Systeme im Monat“ relativiert sich schnell, wenn aus dem Bericht hervorgeht, dass 95% dieser Zugriffe durch fremde Systeme verursacht wurden (wobei sich dann andere Fragen eröffnen – warum gibt es so viele Zugriffe durch fremde Systeme? Sind die Zugriffe autorisiert? Durch wen? Warum?).

4.7 Welche Compliance-Anforderungen werden durch Sophos-NAC adressiert?

Auf einer generischen Ebene adressiert Sophos NAC die Compliance-Anforderungen, die in einer Sophos NAC-Policy definiert sind. Über eine Sophos NAC-Policy, bzw. über die dieser Policy zugeordneten Profile[16] lassen sich folgende Compliance-Anforderungen abhandeln:

- Compliance-Anforderungen in bezug auf das auf dem Client installierte Betriebssystem: Es kann Compliance hinsichtlich eines der folgenden Clientbetriebssysteme gefordert werden:
  - Windows Vista
  - Windows Server 2003
  - Windows XP

[16] *Eine Sophos NAC-Policy steuert den Zugriff auf die (Unternehmens-internen) Netzwerkressourcen über konfigurierbare Profile. Einer Sophos NAC-Policy kann, bzw. können eines oder mehrere Profile zugeordnet werden. Jedes Profil enthält dabei die Einstellungen, die bei einem Client auf Compliance überprüft werden sollen (Betriebssystem, Service Pack, Patchlevel etc.).*

  - Windows 2000
  - Windows 98 SE

- Compliance-Anforderungen in bezug auf das installierte Service Pack: Für ein bestimmtes Betriebssystem kann die Installation eines bestimmten Service Packs verlangt werden. So kann z. B. verlangt werden, dass Windows XP in dem Profil A Service Pack 2 aufweist, in dem Profil B dagegen Service Pack 1.

- Compliance-Anforderungen in bezug auf den Patchlevel des Betriebssystems: Für die unterstützten Betriebssysteme stehen derzeit über 600 Patches zur Evaluierung durch den auf dem Client installierten Agent bereit. So hätte etwa eine Policy, die MS03-26 verlangt haben würde, maßgeblich zu einer Eindämmung des Wurms W32/Blaster beitragen können. Die Patchdatenbank wird dabei kontinuierlich (von Sophos) erweitert.

- Compliance-Anforderungen in bezug auf Antivirus-Software[17]: Für Antivirus-Software kann Compliance hinsichtlich der folgenden Aspekte adressiert werden:
  - Ist eine Antivirus-Software installiert?
  - Läuft die Antivirus-Software auf dem Client?
  - Verfügt die Antivirus-Software über eine aktuelle Signatur?

- Compliance-Anforderungen in bezug auf Antispyware-Software: Für Antispyware-Software kann Compliance hinsichtlich der folgenden Aspekte behandelt werden:
  - Ist eine Antispyware-Software installiert?
  - Läuft die Antispyware-Software auf dem Client?
  - Besitzt die Antispyware-Software eine aktuelle Signatur?

- Compliance-Anforderungen in bezug auf Firewall-Software: Für Firewall-Software kann Compliance hinsichtlich der folgenden Aspekte überprüft werden:
  - Ist eine Firewall-Software installiert?
  - Läuft die Firewall-Software auf dem Client?

- Compliance-Anforderungen hinsichtlich weiterer installierter Software: Installierte Software, die nicht unter einer der vorgenannten Kategorien fällt, kann als compliant oder nicht compliant definiert werden. Sophos NAC gestattet es, manuell eine sehr granulare Definition von Anwendungen, Prozessen oder Registry-Schlüsseln vorzunehmen, die auf einem Client installiert sein müssen /laufen müssen, damit dieser Client als compliant zu gelten hat.

Darüber hinaus besteht die Möglichkeit der Priorisierung von Compliance-Anforderungen für Benutzer: Policies werden Benutzergruppen zugeordnet. Ein Benutzer kann mehreren Benutzergruppen angehören. Wenn für verschiedene Benutzergruppen verschiedene Policies definiert werden, kann in Active Directory-basierten Domänenumgebungen festgelegt werden, welche Policy dann für den Benutzer Priorität besitzt.

[17] *Sophos NAC kennt dabei derzeit über 350 verschieden Sicherheitsanwendungen wie Antivirus- und Antispyware-Programme, Firewall-, IDS- und weitere Sicherheitsanwendungen.*

4.8 Welche Endpunkte werden unterstützt? Wie kann mit nicht-unterstützen Systemen umgegangen werden?

Sophos NAC unterstützt die Evaluierung der (im vorausgehenden Abschnitt aufgeführten) Compliance-Kategorien für Endpunkte mit einem der folgenden Betriebssystemversionen[18]:

- Windows Vista
- Windows Server 2003
- Windows XP
- Windows 2000
- Windows 98 SE

Dabei gibt es zwei Möglichkeiten, die Compliance solcher Clients zu evaluieren: Entweder findet das Client-Assessment über einen für die genannten Betriebssysteme installierbaren Agent[19] statt, oder – für den Fall, dass kein Agent installiert werden kann oder kein Agent installiert werden soll oder darf[20] – findet das Assessment über den Browser statt. Bei dem Broswer muss es sich um den Internet Explorer handeln.[21]

Bisher nicht unterstützte Clients können immer noch generisch, und zwar auf einer „Ja“ /“Nein“-Basis behandelt werden: Einem nicht unterstützen Client kann der Zugang zum Organisations-LAN entweder gestattet oder verweigert werden kann. Eine Verweigerung (wie auch ein Gestatten) ist Policy-basiert (automatisiert) möglich[22]. Im Fall der Verweigerung kann der Endpunkt an ein dediziertes (von dem Organisations-LAN verschiedenes) Netzwerksegment verwiesen werden.[23] Dieses Segment kann ein Remediation- oder auch ein Quarantänesegment sein.

4.9 Lässt sich Compliance in Sophos NAC erzwingen?

Ja, Compliance lässt sich für unterstützte Clients erzwingen. Wird Compliance erzwungen, dann hat das für einen Client, der nicht compliant ist, eine von zwei Konsequenzen: Entweder der Client kann „compliant gemacht“ werden und erhält dann Zugang, oder er kann nicht „compliant gemacht“ werden und erhält dann keinen Zugang:

Ist ein unterstützter Client nicht compliant, dann lässt sich je nach Policy-Konfiguration festlegen, ob diesem Client der Zugang zum Organisations-LAN verweigert (oder gestattet) wird, oder ob der Client an ein dediziertes Netzwerksegment verwiesen wird, in dem Compliance zur Policy erreicht werden kann (Remediationsegment) oder in dem dem Client der Zugriff nur auf externe Ressourcen (etwa Internet und Maildienste) gewährt wird (Quarantänesegment). In dem s.g. Remediation-Netz können Remediation-Server stehen, die den Client etwa mit den notwendigen Antiviren-Signatur-Updates oder mit Betriebssystem-Patches versorgen[24]. Nach

---

[18] *Ab Frühjahr bis Mitte 2008 sollen laut Sophos auch Linux- und MAC OS-basierte Endpunkte unterstützt werden. Außerdem arbeitet Sophos an der Entwicklung eines Java-Clients.*

[19] *Der allgemeiner als „Data Collector bezeichnet wird (vgl. Abschnitt 2.2).*

[20] *Dies kann etwa bei s. g. VIPs oder auch einfach im Verbotsfall der Installation von Software auf Clients der Fall sein.*

[21] *Und zwar mindestens in der Version 5.0. Außerdem muss in dem Browser das Herunterladen und Ausführen von signierten Active X-Controls zusammen mit einigen weiteren Einstellungen konfiguriert sein (für Details siehe den Sophos NAC Agent User Guide).*

[22] *Wenn keine weiteren (technischen) Compliance- oder Riskmanagement-Werkzeuge für das Compliance-Assessment verwendet werden, dann sollten vor dem Gestatten des Zugangs unbedingt organisatorische Maßnahmen (wie etwa die Verpflichtung auf eine manuelle Überprüfung) stehen.*

[23] *Diese Zuweisung wird von dem Sophos NAC-DHCP-Enforcer (wenn der Client eine IP-Adresse über den DHCP-Server erhält) oder von dem Sophos NAC-RADIUS-Enforcer (wenn der Client etwa über 802.1x-Mechanismen auf das Organisations-LAN zugreift) durchgeführt.*

[24] *In Microsoft-Umgebungen ist etwa der WSUS-Server von Microsoft ein typisches Beispiel für einen Remediation-Server.*

dem Update des Clients findet dann eine erneute Prüfung des Clients auf Compliance statt.[25] Nach erfolgreich bestandener Überprüfung kann dem Client nun der Zugriff auf das Organisations-LAN gewährt werden. Nicht unterstützte Clients können immer an ein Remediation-Netz verwiesen werden (siehe vorausgehender Abschnitt).

4.10 Welche Schnittstellen zu anderen Compliance- oder Risk Management Werkzeugen existieren in Sophos NAC?

Sophos NAC bietet bisher eine Schnittstelle zu der Network Admission Control (NAC) -Lösung von Cisco und kann in solchen Umgebungen ohne großen Aufwand integriert werden. Diese Schnittstelle ist ein Plug-in für Endpunkte, um diese Endpunkte in eine möglicherweise schon bestehende NAC-Lösung von Cisco integrieren zu können:

Sophos NAC bietet für die Integration von unterstützten Clients ein s.g. Security-Posture-Plug-in an, dass es diesen Clients gestattet mit der auf diesen Clients (ebenfalls) installierten Endpunkt-Clientkomponente von Cisco – dem Cisco Trusted Agent (CTA) – zu kommunizieren. Der CTA auf dem Client kommuniziert seinerseits mit dem Cisco Secure ACS (Access Control Server). Dieser führt dann einen Vergleich der von dem Client übermittelten Daten mit der Cisco NAC-Policy durch[26]. Abhängig von der Policy-Konfiguration und dem Compliance-Level des Clients kann dem Client auch hier der Zugang zum Organisations-LAN gewährt oder verweigert werden, oder der Client kann an ein Remediation-Netz verwiesen werden.

Die Sophos NAC-Lösung kann darüber hinaus parallel zu ähnlichen Lösungen anderer Hersteller betrieben werden, die etwa ein weniger vollständiges Client-Compliance-Assessment bieten.[27]

4.11 Welche Reporting & Monitoring Möglichkeiten bietet Sophos NAC?

Sophos NAC bietet zahlreiche Reporting- und Monitoring-Funktionen für Compliance, Troubleshooting, Analyse und Audit. Dies beinhaltet die folgenden Kategorien:

- *Compliance Reports* enthalten sowohl eine High Level-Übersicht über den Compliance-Status aller Clients innerhalb eines bestimmten Zeitintervalls wie auch das Ergebnis der Compliance-Evaluation eines einzelnen Clients zu einem bestimmten Zeitpunkt. Die detaillierte Abfrage eines Clients ermöglicht die Anzeige der für diesen Client aufgrund der NAC-Policy geltenden Bedingungen, seiner Abweichungen gegenüber der Policy sowie aller Aktionen (z. B. Remediation), die aufgrund der Compliance-Bewertung des Clients auf diesem Client von Sophos NAC durch den Agent vorgenommen wurden.
- *Analysis Reports* zeigen Trends über definierte Zeiträume an und lassen damit Aussagen über die zeitliche Entwicklung zu. Diese Aussagen beziehen sich auf *Policies* und *Applications*, d. h. zum einen darauf, welche Policies auf welche Clients in einem bestimmten Zeitintervall angewendet wurden, zum anderen darauf, für welchen Client in Abhängigkeit von dessen Betriebssystem welche Service Packs, Patches, Registry-Einträge oder Anwendungen angewendet wurden.
- *Troubleshooting Reports* helfen bei der Aufspürung von sicherheitsrelevanten Vorfällen, die den Organisations-LAN-Zugang, die Compliance oder definierte Ausnahmen (von Compliance) auf Endpunkten betreffen. Dadurch dass es für jede Enforcement-Methode, für die Sitzung des Clients (Zeitdauer des durch Sophos NAC kontrollierten Netzzugangs) und für sein Assessment eine eigene Reporting-Kategorie gibt, ist eine profunde Analyse

---

[25] *Die Meldungen, die dem Benutzer dabei angezeigt werden, können vorkonfiguriert werden.*
[26] *Dazu muss der Cisco Secure ACS die von dem Security-Posture-Plugin ermittelten Daten interpretieren können. Dies wird durch den Import einer Datei erreicht, die für die Abbildung zwischen den Sophos NAC-Attributen und der Cisco NAC-Policy zuständig ist (detailliertere Information entnimmt man* Sophos NAC Agent User Guide*.*
[27] *Hierbei lässt sich z. B. an Microsofts künftige Network Access Protection (NAP)-Lösung denken, die voraussichtlich nur für Windows Server 2008, für Windows Vista- und Windows XP (SP3)-Clients zur Verfügung stehen wird.*

möglich. Diese kann sowohl bei der Fehlersuche als auch bei einer nachträglichen (etwa durch den Gesetzgeber oder die Revision geforderten) Analyse dienlich sein.

- *Audits* schließlich zeichnen bestimmte Ereignisse wie etwa Konfigurationsänderungen in Sophos NAC selbst auf, so dass es neben einer (üblichen) Reporting-Funktion der Sophos NAC-Umgebung auch ein Audit im engeren Sinn gibt (siehe dazu den nächsten Abschnitt).

4.12 Lässt sich die (technische) Definition und Konfiguration von Compliance von Sophos NAC unabhängig (z.B. durch die Revision) überwachen?

Ja: Sophos NAC-Einstellungen werden über das Web-Interface administriert. Die Administration findet rollenbasiert statt.[28] Unabhängig von der Rolle findet stets ein *Audit* (= Aufzeichnung) von bestimmten Ereignissen sowie Veränderungen der Konfiguration innerhalb von Sophos NAC statt[29]. Selbst die Rolle, die mit den höchsten Privilegien versehen ist (*System Administrator*), verfügt nicht über die Berechtigung, Audit-Einträge zu verändern. Damit ist eine von Sophos NAC unabhängige Überwachung der Compliance-Konfiguration(en), wie sie typischerweise von der Revision gefordert wird, möglich.[30]

---

[28] *Sophos NAC kennt die folgenden vier Administrations-Rollen:* System Administrator, Administrator, Help Desk *und* Guest.

[29] *Mögliche Audit-Kategorien in Sophos NAC sind u. a.: Konten-Verwaltung (in Sophos NAC), An- und Abmelden am Web-Interface und Profile- und Policy-Erstellungen.*

[30] *Audit-Einträge können zwar nicht über das Web-Interface verändert werden, sie könnten jedoch durch einem administrativen Account auf dem SQL-Server manipuliert werden. Daher muss der SQL-Server von einer von der* System Administrator*-Rolle verschiedenen Administrator-Rolle verwaltet werden. Diese Forderung deckt sich vollkommen mit einer elementaren Sicherheitsforderung, nämlich der der* Segregation of Duties *(Trennung von (Verwaltungs-) Zuständigkeiten). Der Forderung nach unabhängiger Überwachung – wie im übrigen auch der Forderung der Segregation of Duties – kommt die Möglichkeit zupass, neben Active Directory-intergrierten Konten auch Benutzerkonten von externen Datenbanken (etwa eines einzelnen nicht Domänenmitgliedsrechners) verwenden zu können.*

5 FAZIT

Die Anwendung von Sophos NAC als Compliance Monitoring und Reporting Werkzeug kann einen signifikanten Mehrwert für den typischen CISO darstellen. Dies gilt nicht nur in Bezug auf eine organisationseigene Security Policy, sondern auch ganz direkt in Bezug auf die ISO 27001 und die ISO 17799:2005. Analog der Vorgehensweise zur ISO 27001 können auch Anforderungen aus SOX, Basel II oder den BSI-Standards mit Sophos NAC erfüllt werden.

Der Mehrwert liegt dabei nicht so sehr auf dem direkten Gewinn an technischer IT-Security (dieser ist durchaus diskutierbar und in einigen Szenarien mag dieser Mehrwert den Compliance-Mehrwert auch in den Schatten stellen), sondern in den Möglichkeiten, die Sophos NAC zum Monitoring und zum Reporting bietet. Die Kombination von Metriken, Compliance-Anforderungen und Sophos NAC als Compliance-Reporting-Werkzeug entspricht nicht dem von NAC Herstellern üblicherweise beworbenen „Return of Security Invest“[31], sondern ist ein neuer und innovativer Ansatz. Dieser Ansatz kann nach Ansicht der Autoren durchaus dazu beitragen, dass NAC im allgemeinen und Sophos NAC im Besonderen seinen Platz auf dem Markt findet – es bleibt zu wünschen, dass Sophos in der Weiterentwicklung konsequent den Compliance-Ansatz in den Vordergrund stellt und nicht den „Yet-another-IT-Security-Tool“-Ansatz.

[31] *Ein Beispiel-Modell zur ROSI-Berechnung kann der geneigte Leser im Internet unter http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf finden.*

6 ANHANG – INSTALLATIONSANLEITUNG SOPHOS NAC 3.0

Dieser Abschnitt dokumentiert die Installation der Testumgebung und beschreibt grundlegende Konfigurationsszenarien.

6.1 Die Testumgebung

Die Testumgebung besteht aus den folgenden Systemen mit den folgenden Funktionen:

Funktion in der Infrastruktur	NAC-Rolle oder Funktion im Zusammenhang mit NAC	Hostname
Host für virtuelle Maschinen (VMware-VMs)		hdb-sophos-test-lab2
Domänencontroller	Enterprise-Authentifizierung	dc1pki
SQL-Datenbank	Sophos NAC-Datenbankserver	srv01
Anwendungsserver	Sophos NAC-Administrationsserver (Web-Interface)	srv02
Anwendungsserver	Sophos NAC-Policyserver	srv02
Anwendungsserver	Sophos NAC-Radius Enforcer	srv02
Anwendungsserver	Sophos NAC DHCP Enforcer	srv02
Zertifizierungsstelle (CA)	Zertifikatslieferant (z. B. für das Web-Interface	ca1.pki
Memberserver	Windows Server 2003-NAC-Client	srv03
Memberserver	Windows Server 2008-NAC-Client	srv08
Workstation	Windows XP Professional-NAC-Client	xp01
Workstation	Windows Vista Ultimate-NAC-Client	vista02

Alle Rechner sind Mitglied einer Domäne (*pki.org*), die durch den Domänencontroller (*dc1pki.pki.org*) begründet wird.

6.2 Voraussetzungen /Benötigte Umgebung für die Installation von Sophos-NAC

Sophos-NAC ist für Enterprise-Umgebungen und damit für die Integration in einen Verzeichnisdienst gedacht. Dieser Verzeichnisdienst kann ein ldap-basierter Verzeichnisdienst sein. Im Fall der vorliegenden Testumgebung ist der Verzeichnisdienst Active Directory. Für den Fall von Active Directory sind vor der Installation von Sophos-NAC die folgenden Microsoft-Komponenten bereitzustellen.

- Active Directory: dies kann Windows 2000 Server- oder Windows Server 2003-basiertes Active Directory sein.[32] Die Funktionsebenen haben keinerlei Auswirkungen auf Sophos NAC.
- Windows Server mit installiertem Microsoft SQL Server: Der SQL Server wird für die Sophos NAC-Datenbank benötigt. Die getestete Version von Sophos NAC benötigt SQL Server 2000.[33]

[32] *Theoretisch spricht nichts gegen ein Windows Server 2008-basiertes Active Directory, (wenn Windows Server 2008 auf den Markt kommt), da die Kernkomponenten von Sophos NAC nicht von speziellen Eigenschaften des Active Directory abhängen.*

- Windows Server mit installiertem Internet Authentication Service (IAS): Hier kann die IAS-Version von Windows Server 2003 verwendet werden. Sophos NAC benötigt für jeden RADIUS-Enforcement-Point und für jeden VPN-Enforcement-Point je eine IAS-Installation. Darüber hinaus wird eine IAS-Installation für das Web-Interface benötigt.
- Windows Server mit installiertem DHCP-Server: Wenn DHCP-Enforcement verwendet wird, benötigt Sophos NAC mindestens einen Windows 2000- oder einen Windows Server 2003-basierten DHCP-Server.
- Windows Clients für die Sophos NAC-Client-Komponente: Diese Clients können sein: Windows 98 SE, Windows 2000 (Server und Professional), Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008[34].
- Ein Zertifikat für die Web-Seite des Servers, auf dem das Web-Interface installiert wird.[35]

6.3 Installation von Sophos-NAC

6.3.1 Installation des Datenbankservers

Es empfiehlt sich, die Sophos NAC-Installation mit der Installation des Datenbankservers zu beginnen, da sowohl das Web-Interface als auch jede Enforcement-Server-Komponente auf den Datenbankserver zugreift.

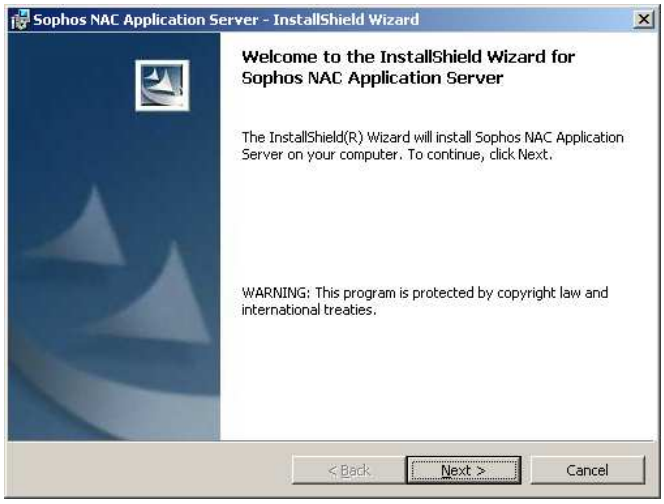
Voraussetzungen für die Installation den Datenbankservers:

- Microsoft SQL Server 2000 mit Service Pack 2
- Ein Dienstkonto, das für den Zugriff auf den Datenbankserver verwendet wird. Für dieses Dienstkonto haben die folgenden Bedingungen zu gelten:
  - Das Konto muss domänenweit gültig sein; es genügen die Berechtigungen eines gewöhnlichen Benutzers in der Domäne[36]
  - Das Konto benötigt das Privileg *Anmelden als Dienst*
  - Das Kennwort des Kontos sollte nicht ablaufen[37]

Wenn diese Voraussetzungen erfüllt sind, kann mit der Installation des Datenbankservers begonnen werden:

---

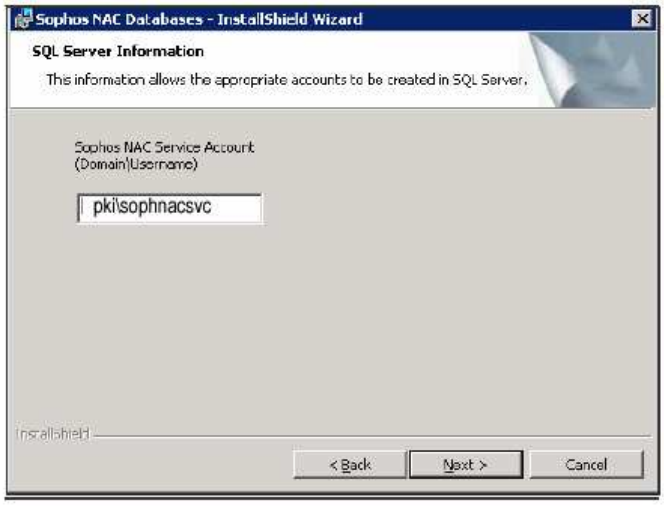
[33] *Laut Aussagen von Sophos wird derzeit an einer Version von Sophos NAC für SOL Server 2005 gearbeitet.*
[34] *Derzeit (August 2007) in der Beta 3 erhältlich.*
[35] *Wird ein Microsoft-basierter Web-Server verwendet, so lässt sich mit dem Tool selfss.exe, das Bestandteil des Resource Kits für den Microsoft Internet Information Server ist, ein Zertifikat für die Web-Seite des Web-Interfaces erstellen. In der vorliegenden Testumgebung wurde eine Windows-Zertifizierungsstelle zur Erstellung des Zertifikats verwendet. Eine eigene CA ist dazu jedoch nicht notwendig.*
[36] *D. h. das Konto kann Mitglied der Gruppe Domänen-Benutzer sein.*
[37] *Dafür kann ein hinreichend komplexes Kennwort (bis 128 Zeichen) gewählt werden.*



Ein Klick auf *Next* führt zu:

An dieser Stelle kann die Authentifizierungsmethode gegenüber dem SQL Server festgelegt werden. Bei der vorliegenden Teststellung mit der Integration in Active Directory wurde die (integrierte) Windows-Authentifizierung verwendet.

Ein Klick auf *Next* führt zu:



An dieser Stelle wird das vorher definierte Dienstkonto angegeben.

Ein Klick auf *Next* führt zur Installation des von Sophos verwendeten Aufsatzes für den SQL Server.

6.3.2 Installation eines Applikationsservers

Die Installation eines Applikationsserver ist Voraussetzung für eine der folgenden Enforcement-Server-Komponenten:

- 802.1x-Enforcement
- Enforcement für den Zugang über eine statische IP-Adresse
- DHCP-Enforcement

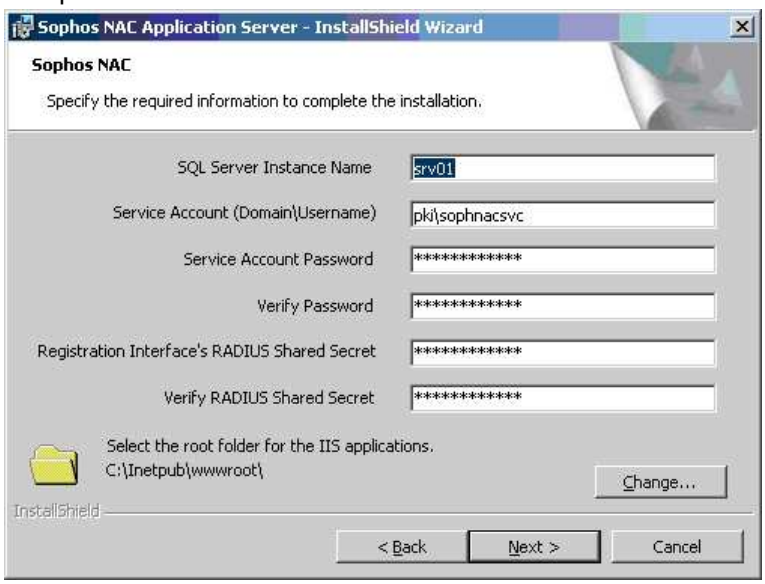
Die Applikationsserver-Topologie kann je nach Unternehmensanforderungen auf einen oder mehrere Applikationsserver verteilt werden. Wenn mehrere Applikationsserver verwendet werden sollen, dann ist darauf zu achten, dass diese hinsichtlich der zugrundeliegenden IAS-Konfiguration identisch sind (siehe dazu den *Sophos NAC Installation Guide*).

Voraussetzungen für die Installation eines Applikationsservers:

- Windows Server 2003 Service Pack 1 (oder höher)
- Microsoft .NET Framework 2.0
- Microsoft Web Service Enhancements (WSE) 3.0
- Microsoft Internet Information Services (IIS) mit aktivierter Unterstützung von ASP.NET
- Microsoft ASP.NET State Service
- Microsoft Message Queuing
- Microsoft Internet Authentication Services (IAS)
- Microsoft Data Access Components (MDAC)

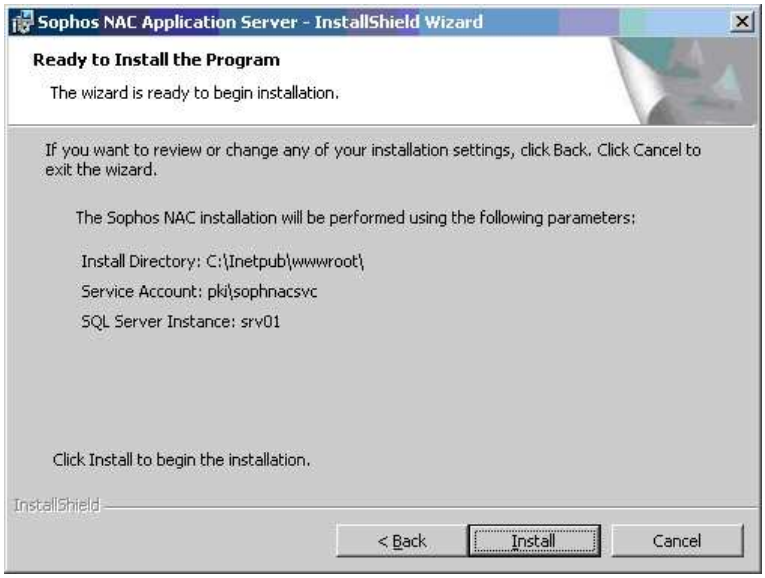
Sind diese Voraussetzungen erfüllt, dann kann die Installation gestartet werden:

Ein Klick auf *Next* sorgt für eine Überprüfung der in den Voraussetzungen genannten Komponenten:



Hier sind neben der Eingabe der Daten für den Zugriff auf den SQL-Datenbankserver die Eingabe eines sog. *Shared Secrets* und die Angabe des virtuellen Verzeichnisses für die Sophos NAC-Webseite notwendig. Das *Shared Secret* wird bei jeder Installation eines Applikationsservers verlangt und muss auf allen Applikationsservern identisch sein. Das virtuelle Verzeichnis für die Sophos NAC-Webseite sollte aus Sicherheitsgründen auf einem von *%Systemdrive%* verschiedenen Erfolgen.

Ein Klick auf *Next* führt zu einer zusammenfassenden Übersicht:



Ein weiterer Klick auf *Next* führt zur Installation des Sophos NAC-Applikationsservers.

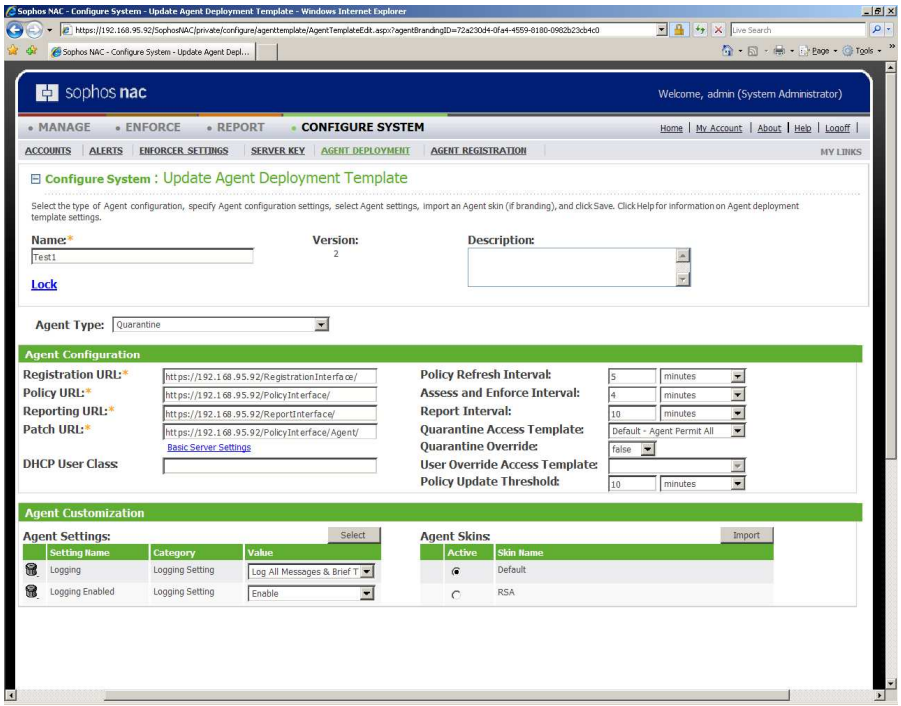
6.3.3 Installation und Konfiguration des Sophos NAC-Agents

Sophos NAC kennt zwei verschiedene Agent-Typen: einen fest installierbaren Agent und einen Web-Agent (der nur einen geeigneten Browser erfordert)[38].

6.3.3.1 Installierbarer Agent

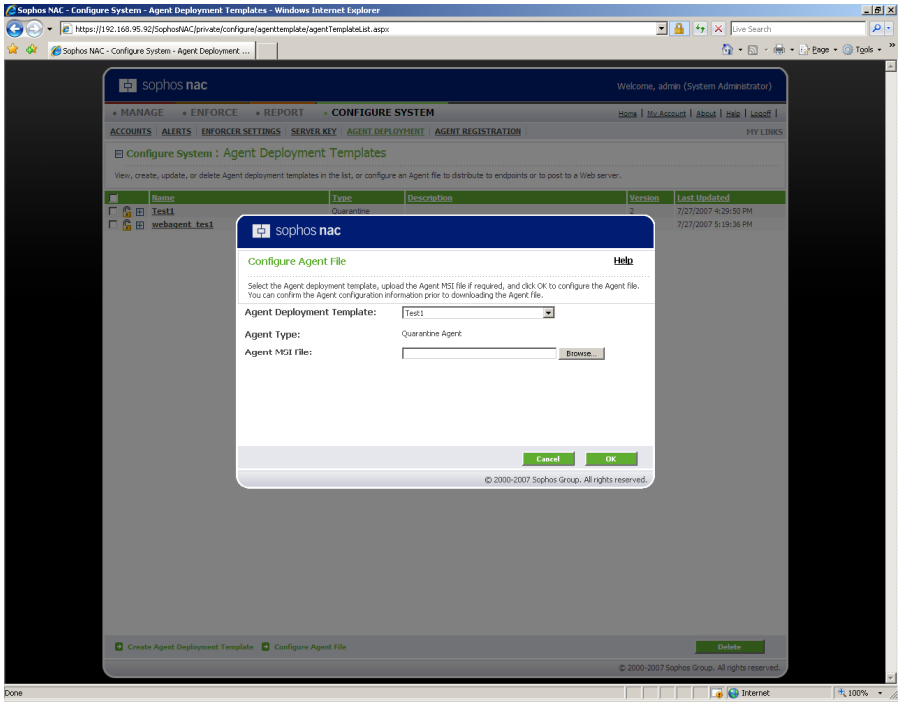
Installation und Konfiguration erfolgen in den folgenden Schritten:

1. Erstellung einer Vorlage für das Agent-Deployment über: Configure system -> Agent Deployment-> Create Agent Deployment Template: Dieses wird dann gespeichert.



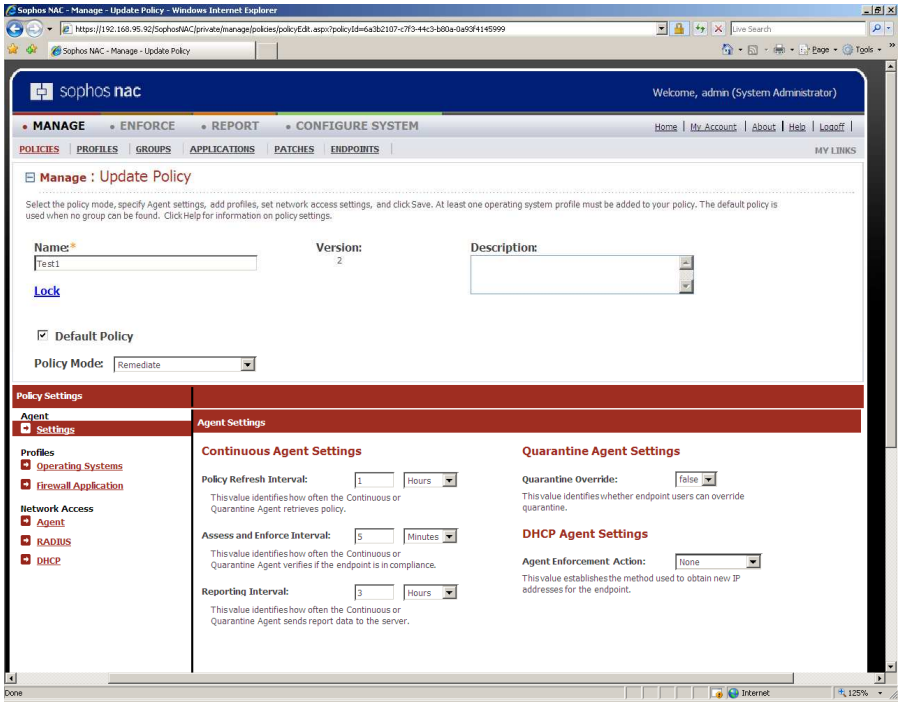
[38] *Den Internet Explorer in einer Version von mindestens 5.0.*

2. Auswahl und Konfiguration der Vorlage (dies erfolgt dann in den folgenden Schritten) über Configure System -> Agent Deployment -> Configure Agent File:

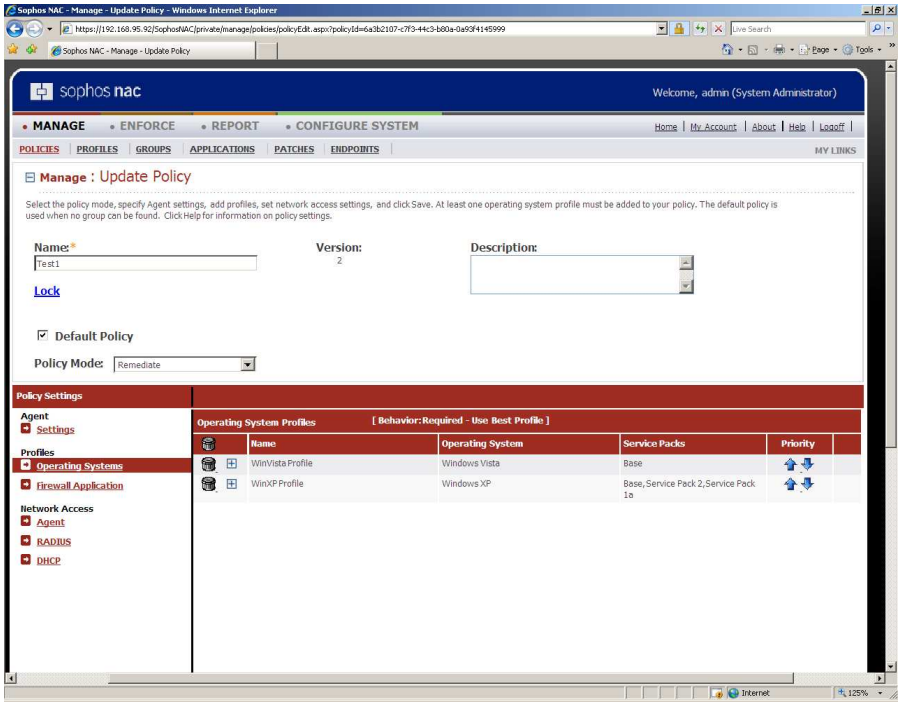


Die (in den nachfolgenden Schritten) konfigurierte Vorlage wird zusammen mit der Datei *Sophos NAC Agent NT.msi* zu einer *Name_der_Agent_Installations-Datei.msi*-Datei, die dann etwa per Gruppenrichtlinie auf die betreffenden Clients verteilt werden kann.

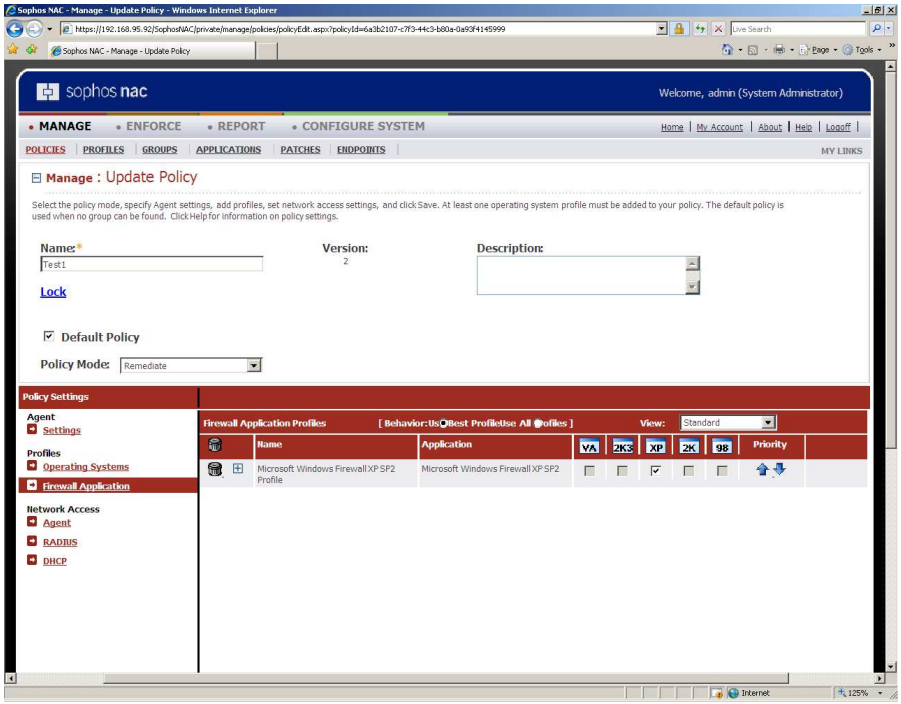
3. Erstellung einer Policy über: Manage -> Policies -> Create Policy: Dort wird mit den *Agent Settings* der erstellten Vorlage begonnen:



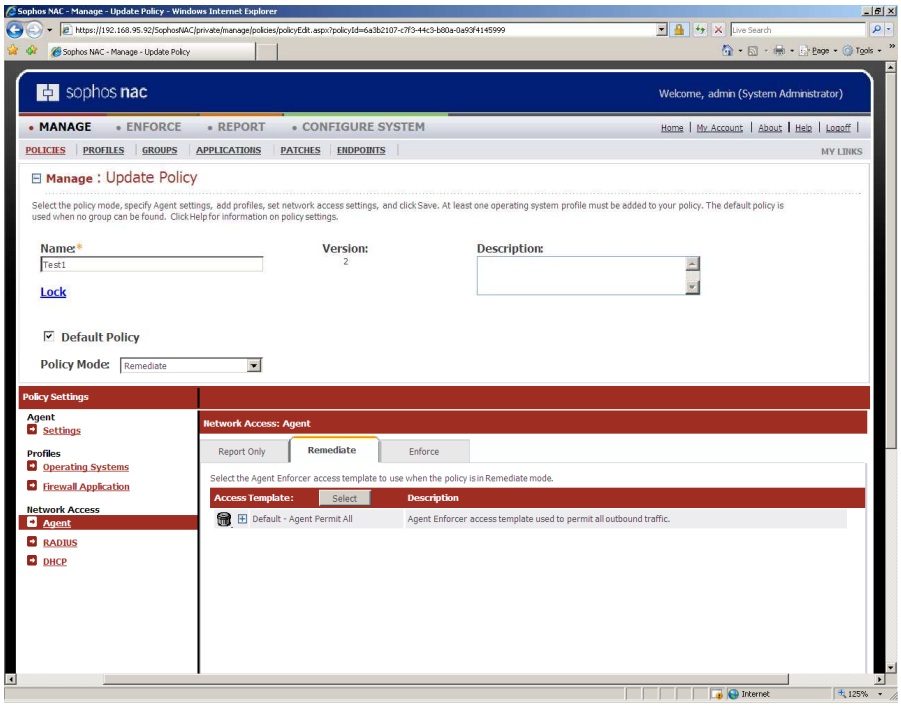
Anschließend wird das Profil für das diesem Profil zugeordnete Client-Betriebssystem konfiguriert:



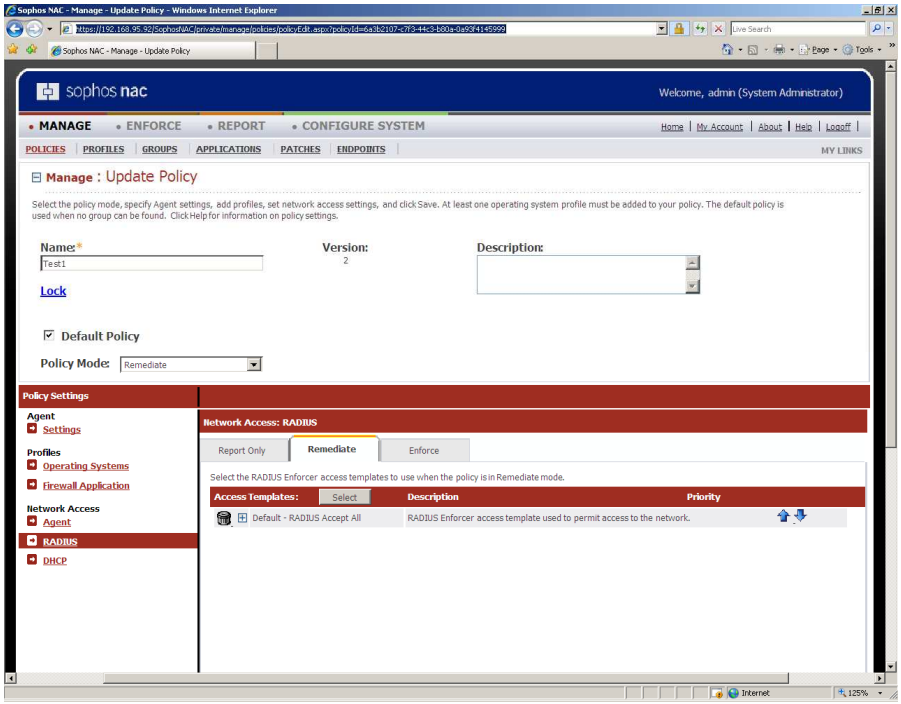
Bedingungen, ob eine und – falls ja, welche – Software-Firewall auf den Clients für dieses Profil verwendet werden soll:



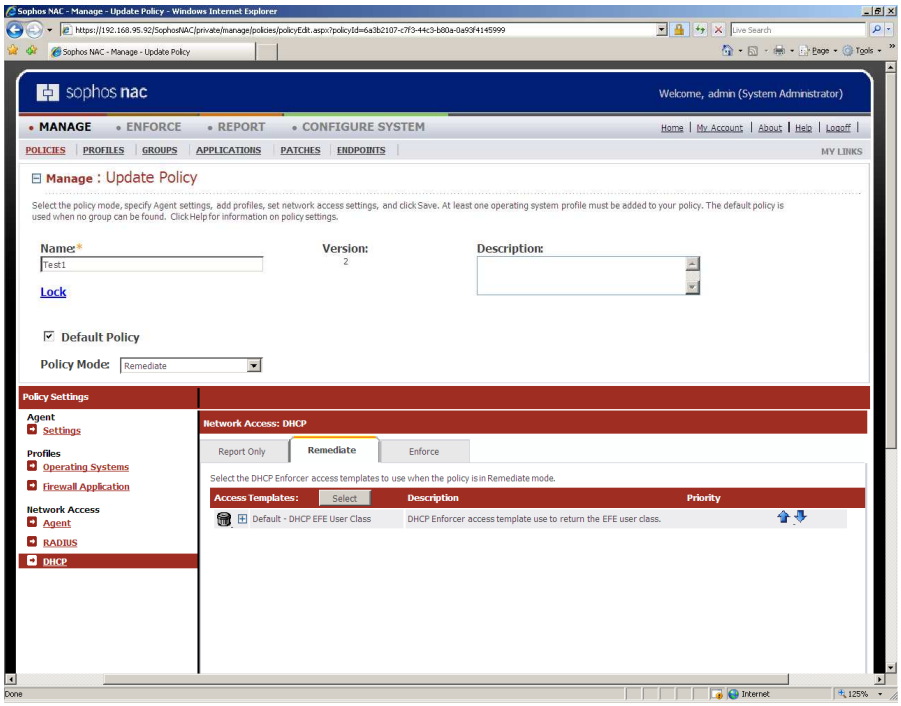
Auswahl der Agent-Enforcer-Vorlage für den Client:



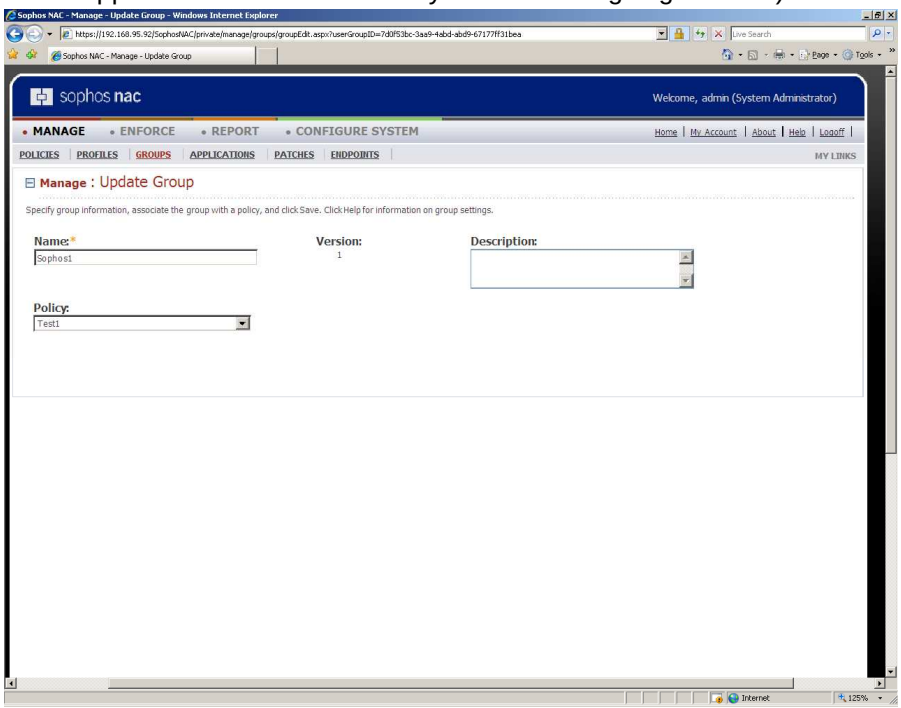
Auswahl der RADIUS-Enforcer-Vorlage für den Client:



Auswahl der DHCP-Enforcer-Vorlage für den Client:

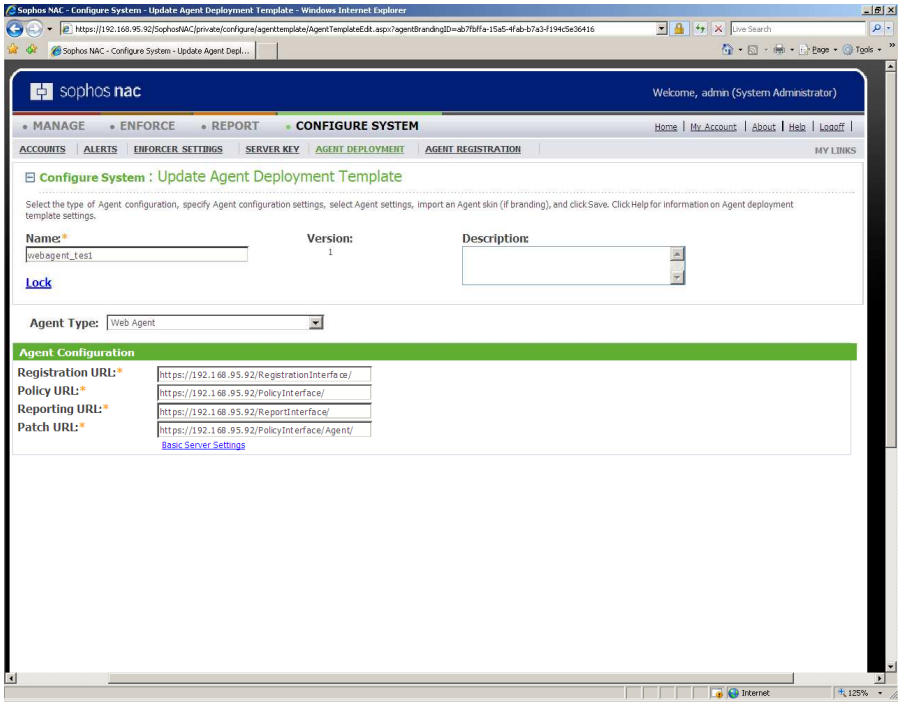


4. Zuordnung des erstellten Profils, bzw. der erstellten Vorlage zu einer Benutzergruppe (diese Gruppe muss im Active Directory existieren /angelegt werden):



6.3.3.2 Web-Agent

Die Konfiguration des Web-Agents beginnt analog:



und kann auch in Analogie konfiguriert werden. Die daraus entstehende Datei ist eine *.dat*-Datei (*WebAgentOpts.dat*), die dann auf dem Webserver (dies muss ein Windows Server 2003-basierter IIS sein) in einem geeigneten Verzeichnis abgelegt werden muss, und zwar über: Default Web Site -> WebAgent -> WebAgentOpts.dat.

Anschließend können dann die verschiedenen Enforcement-Szenarien konfiguriert werden.

Für weitergehende Informationen stehen die Autoren jederzeit gern zur Verfügung.

Mit freundlichen Grüßen,

[Friedwart Kuhn, Dror-John Röcher, Michael Thumann].

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de
info@ernw.de