

## **NAC an Endpoints:** Netzwerkkontrolle durch Geräte-Compliance

Lange Zeit gestaltete sich der Schutz von IT-Netzwerken relativ einfach, indem man Computer und Server mit einer Firewall umgab und den gesamten Datenverkehr über ein einziges Gateway leitete. Die Zunahme an mobilen Mitarbeitern, die zunehmende Geräteanzahl und -vielfalt sowie die hohe Anzahl der Externen, die Netzwerkzugang benötigen, haben jedoch zu einer Auflösung dieser Außenabgrenzung geführt. Da Zugangsanfragen mittlerweile von allen möglichen Personen und Orten kommen, entscheiden sich heutige Unternehmen oft für den Einsatz von NAC-Technologie (Network Access Control). Dieses White Paper beschäftigt sich mit der Bedeutung von NAC und der Art der Umsetzung an Endpoints, um maximalen Schutz zu gewährleisten.

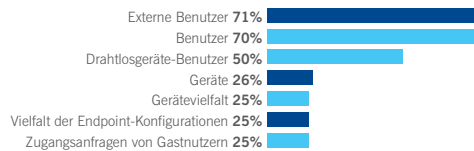
# NAC an Endpoints: Netzwerkkontrolle durch Geräte-Compliance

## Klassischer Netzwerkschutz

Netzwerkschutz gestaltete sich früher relativ einfach. Unternehmen umgaben ihre IT-Werte mit einer Firewall und begrenzten den ein- und ausgehenden Datenverkehr auf einen einzigen Zugangsweg. Mitarbeiter und Computer befanden sich meist vor Ort und ließen sich leicht mithilfe dieser festen Außengrenze vor Viren, Spyware und sonstiger Malware schützen. Dieser klassische Ansatz von Desktopcomputern im Büro und Firewall-geschützten Servern ist zunehmend überholt<sup>1</sup>.

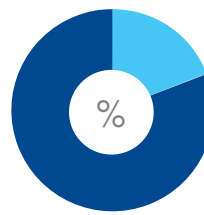
## Geschäftsumgebungen im Wandel

Mittlerweile haben sich Technologie und Arbeitspraktiken geändert, und zwar mit erheblichen Auswirkungen auf die IT-Abgrenzung nach außen. Auch Unternehmen erwarten ein zunehmendes Maß an Mobilität von ihren Mitarbeitern – die somit auf externen Netzwerkzugang angewiesen sind – und müssen ihrerseits die eigenen IT-Systeme für Subunternehmer und Gastbenutzer öffnen. Untersuchungen der Aberdeen Group<sup>2</sup> zeigen, dass Netzwerke eine wachsende Zahl an Geräten, Gerätetypen, Benutzern und Zugangsanfragen zu bewältigen haben (Abbildung 1). Dies führt zur Auflösung der Netzwerkabgrenzung und zu Sicherheitslücken.



Quelle: Aberdeen Group, 2007

Abbildung 1: In welchem Bereich nimmt die Netzwerknutzung bei Ihnen zu?



- 81 % der unternehmenseigenen Endpoint-Computer haben entweder keine Microsoft Sicherheits-Patches oder keine Endpoint-Sicherheitssoftware, oder die Client-Firewall ist deaktiviert.
- 19 % der unternehmenseigenen Endpoint-Computer sind vollständig geschützt.

Quelle: Sophos Endpoint Assessment Test, Juni 2008

Abbildung 2: Stellen Ihre Endpoint-Computer ein Sicherheitsrisiko dar?

Und diese Lücken sind gravierend. Bei der Frage, ob ihre Endpoint-Computer ein Sicherheitsrisiko darstellten<sup>3</sup>, wiesen viele Unternehmen erhebliche Mängel in Bezug auf wichtige und grundlegende Sicherheitsfunktionen auf (Abbildung 2). Diese Ergebnisse zeigen, dass IT-Teams den Netzwerkschutz verbessern und somit dafür sorgen müssen, dass sämtliche Endpoints den eigenen Sicherheitsbedürfnissen Rechnung tragen. Außerdem müssen sie die Einhaltung der Unternehmensrichtlinien durchsetzen.

## Wie lässt sich die Netzwerknutzung kontrollieren?

Unternehmen bedienen sich mehr und mehr der NAC-Technologie (Network Access Control), um die zunehmend variablen Außengrenzen ihrer IT-Systeme in den Griff zu bekommen. Neben den von Aberdeen bereitgestellten Zahlen haben Untersuchungen von Forrester ergeben, dass die Komplexität des Netzwerkzugangs eher noch steigen wird, da 63 Prozent der US-Unternehmen die Ausweitung der Laptop-Nutzung planen<sup>4</sup>. Somit werden sich die Netzwerk Grenzen weiter ausdehnen, um Mitarbeitern den Zugang von Flughäfen, Cafés und Zuhause aus zu ermöglichen.

NAC-Technologie erlangt zunehmende Bedeutung für den Schutz von Unternehmensnetzwerken, denn sie ermöglicht Unternehmen:

- Zu erkennen, wer den Zugang zum Netzwerk anfordert.
- Einzuschätzen, ob der betreffende Computer die richtigen Sicherheitsrichtlinien einhält.
- Den Zugang zu gewähren oder zu verweigern bzw. bis zur Compliance eine Quarantäne über Computer zu verhängen.
- Sicherzustellen, dass Benutzer nur diejenigen Bereiche des Netzwerks aufsuchen, die ihrer Rolle oder Aufgabe entsprechen.

### Wo muss die Kontrolle optimiert werden?

Im Zuge der Abkehr vom klassischen Firewall-Ansatz haben Sicherheitsanbieter eine Reihe von Hard- und Softwarelösungen ins Spiel gebracht, die sich mit der Frage beschäftigen, wo eigentlich die Zugangskontrolle erfolgen sollte. Derzeit stehen drei Einsatzvarianten zur Auswahl:

- Am Übertragungsweg
- Im Netzwerk
- Am Endpoint

#### NAC am Übertragungsweg

Dieser Ansatz sorgt für die Richtliniendurchsetzung auf dem Übertragungsweg der Daten und platziert die NAC-Appliance direkt zwischen Endpoint und Netzwerk. Zwischen Endpoint und Netzwerk werden Daten ausschließlich über die NAC-Appliance ausgetauscht. Obwohl die vom Endpoint gesendeten Daten überprüft werden, hat diese Art der Durchsetzung gewisse Nachteile.



*NAC sollte sich idealerweise auf der Endpoint-Ebene befinden, wo der Computer automatisch geprüft wird, bevor und während er mit dem Netzwerk verbunden ist.*



Zum einen muss an jedem physischen Standort – etwa an jedem Netzwerkzugangspunkt – eine NAC-Instanz angesiedelt sein, um vollständigen Schutz zu gewähren – aber das ist aufwendig und erfordert die Einbindung zusätzlicher Hardware. Zum anderen verlängert sich durch die direkt auf dem Übertragungsweg befindliche NAC-Anwendung die Verarbeitungszeit, wodurch die verfügbare Bandbreite eingeschränkt und die Netzwerkgeschwindigkeit gesenkt wird.

#### NAC im Netzwerk

Andere NAC-Appliances setzen außerhalb des Übertragungswegs an und überwachen den vorbeiziehenden Datenstrom neben der Strecke. Solche NAC-Appliances sind der Datenverbindung nachgeordnet und können Datenpakete erst prüfen, nachdem die Netzwerkverbindung hergestellt worden ist und der Datenverkehr eingesetzt hat. Die Appliances untersuchen normalerweise die gesendeten Daten auf abweichendes Verhalten, um Infizierungen festzustellen. Auch diese Variante erfordert erhebliche Investitionen in zusätzliche Hardware, da Geräte im gesamten Netzwerk installiert werden müssen.

#### NAC am Endpoint

Der effektivste Einsatz von NAC ist die Einbindung auf der Endpoint-Ebene, um sicherzustellen, dass der Computer automatisch geprüft wird, bevor und während er mit dem Netzwerk verbunden ist, egal zu welcher Uhrzeit. Ein wichtiger Aspekt ist, dass dies den Unternehmen ermöglicht, die Einhaltung der Sicherheitsrichtlinien selbst durch einzelne Endpoints sicherzustellen, bevor diese auf das Netzwerk zugreifen und (bei mangelnder Compliance) das Netzwerk schädigen.

Auf dieser Ebene ist NAC vollständig softwarebasiert. Somit wirkt sich NAC nicht auf die Verarbeitungsgeschwindigkeit des Netzwerks aus und lässt sich bequem auf sämtliche bestehende bzw. künftige Endpoint-Computer und -Geräte des Unternehmens ausdehnen.

Endpoint-NAC-Lösungen beruhen auf zentral festgelegten und verwalteten Sicherheitsrichtlinien, die Anfragen jeder Art bewältigen und die bequem zu aktualisieren sind.

Die Richtlinien für auf oder neben dem Übertragungsweg lokalisierte Appliances zu aktualisieren ist dagegen schwierig aufgrund der fragmentierten, über das Netzwerk verteilten Struktur, wobei die Hardware – die möglicherweise von verschiedenen Herstellern stammt – ihrerseits Richtlinien erfordert.

Eine NAC-Appliance am Gateway würde z.B. eine Richtlinie erfordern, um den Zugang mobiler Mitarbeiter zu regeln, während eine Appliance am WLAN-Switch eine Richtlinie für am Standort beschäftigte Mitarbeiter erfordern würde. Aktualisierungen der Gesamtrichtlinie eines Unternehmens müssten an jedem Punkt repliziert werden, um die Konsistenz für diejenigen Mitarbeiter zu gewährleisten, die sowohl intern als auch extern arbeiten. Mehrere Richtlinien zu aktualisieren ist zeitaufwendig und birgt die Gefahr, dass ein Punkt im Netzwerk übersehen wird, der so zu einem Sicherheitsrisiko oder einer Hürde für bestimmte Mitarbeiter werden kann.

NAC-Richtlinien lassen sich bedarfsgerecht gestalten und auch flexibel an veränderte Unternehmensanforderungen anpassen. Neue Personen, Gruppen oder Rollen lassen sich leicht hinzufügen, um einen durchgängig effizienten Betrieb sicherzustellen, wobei auch Überprüfungsabfragen der neuesten Sicherheitspatches festgelegt werden können.

### Compliance sicherstellen

NAC zum Herzstück des Endpoint-Schutzes zu machen ermöglicht IT-Administratoren, das nach Meinung vieler IT-Administratoren größte Netzwerkrisiko zu kontrollieren: die eigenen Mitarbeiter<sup>5</sup>.

Zu den unbeabsichtigten Folgen der Ausgabe von unternehmenseigenen Endpoints an Mitarbeiter zählen Konfigurationsveränderungen. Viele Unternehmen räumen dem einzelnen Benutzer Administratorrechte über die jeweils benutzten Geräte ein, um Helpdesk-Anfragen zu erleichtern und den Mitarbeitern eine gewisse Flexibilität zu gewähren. Im Laufe der Zeit ändern viele Benutzer dann die Gerätekonfiguration und entfernen sich allmählich so weit von den Sicherheitsrichtlinien des Unternehmens, dass das Gerät nicht mehr konform ist. Beispiele für Konfigurationsveränderungen sind das Deaktivieren von Firewalls und

die Installation von Instant Message-Software (IM). In beiden Fällen entstehen gravierende Sicherheitslücken.

NAC erkennt, ob sich die Konfiguration des Endpoint-Computers seit dem letzten Netzwerkzugriff verändert hat, und stellt den konformen Zustand wieder her, bevor der Zugang zum Netzwerk gewährt wird. So wird z.B. die Firewall automatisch wieder aktiviert und die IM-Software deaktiviert.

### Wer und was erfordert Zugriff?

Endpoint-basierte NAC-Technologie eignet sich für verwaltete und unverwaltete Geräte sowie für bekannte und unbekannte Benutzer.

#### Geräte- und Benutzerarten

- » **Verwaltete Geräte, die von einem bekannten Benutzer verwendet werden.** Hierbei handelt es sich um unternehmenseigene Computer, bei denen das Unternehmen bestimmen kann, welche Software installiert und welche Sicherheitsrichtlinien durchgesetzt werden.
- » **Unverwaltete Geräte, die von einem bekannten Benutzer verwendet werden.** Hierbei handelt es sich um einen Gastnutzer – normalerweise einen Subunternehmer –, der Netzwerkzugang über den eigenen Computer benötigt. Das Unternehmen ist nicht berechtigt, Software zu installieren, aber bestimmte Anwendungstypen (z.B. Anti-Virus) können ohne Angabe des Herstellers vorgegeben werden.
- » **Unverwaltetes Gerät, das von einem unbekanntem Benutzer verwendet wird.** Hierbei handelt es sich um eine Anfrage von Unbekannt, die eingeschränkt oder gesperrt wird.

#### Verwaltete Geräte

Unternehmen mit verwalteten Endpunkten installieren direkt im Gerät einen NAC Agent, der mit dem NAC-Richtlinienserver kommuniziert. Der Agent ist in der Lage, das Gerät auf die Sicherheitsrichtlinie des Unternehmens zu überprüfen und bei Änderung der Richtlinie Updates anzufordern.

Ist der Benutzer unterwegs und nicht mit dem Unternehmensnetzwerk verbunden, kann der NAC Agent über das Internet mit dem NAC-Richtlinienserver kommunizieren. Falls der Richtlinienserver nicht verfügbar ist, verwendet der Agent die auf der Festplatte des Geräts gespeicherte Richtlinie, um sicherzustellen, dass der Endpoint der Sicherheitsrichtlinie entspricht und geschützt ist, bis die Verbindung mit dem Netzwerk wieder möglich ist.

### Unverwaltete Geräte

Zunehmend benötigen auch betriebsfremde Personen Netzwerkzugang, z.B. Wirtschaftsprüfer, die Jahresprüfungen vornehmen, Subunternehmen, die an Projekten mitarbeiten, und Kunden, die Zugang über das Internet benötigen.

Das NAC-Verfahren bei unverwalteten Computern besteht darin, einen temporären Agent herunterzuladen, der das Gerät vor dem Verbindungsaufbau prüft. Dabei wird das Gerät auf folgende Merkmale überprüft:

- Art, Marke und Versionsnummer der ausgeführten Sicherheitsanwendung.
- Status der Betriebssystem-Patches.
- Zeitpunkt der letzten Malware-Prüfung.
- Status der Signaturdateien.

### Bequeme Umsetzung

Softwarebasierte NAC-Lösungen senken auch die Auswirkungen der Umsetzung, da sie phasenweise erfolgen kann. Im Unterschied zu NAC-Appliances, bei denen das Netzwerk teilweise für die Installation deaktiviert werden muss, ermöglicht der Einsatz von NAC-Software dem Unternehmen die Überprüfung der Endpoints und Sicherstellung der Compliance, ohne dass die IT-Infrastruktur in irgendeiner Form offline gehen muss.

Solche Implementierungen erfolgen in vier Phasen:

- Definieren.
- Überprüfen.
- Beheben.
- Durchsetzen.

### Definieren der Richtlinie

Bevor eine NAC-Lösung implementiert wird, muss das jeweilige Unternehmen festlegen, wie ein bestimmtes Benutzergerät genau konfiguriert sein muss, um Zugang zum Netzwerk zu erhalten. Dazu werden Richtlinien erstellt. IT-Teams können sicherstellen, dass bestimmte Anwendungen normalerweise nicht für den Geschäftsbetrieb verwendet werden, sodass z.B. Peer-to-Peer-Anwendungen weder installiert noch ausgeführt werden. Ferner können hiermit der Benutzertyp, die Gruppe oder Rolle festgelegt werden, denen bestimmte Zugangsrechte eingeräumt bzw. verweigert werden sollen. Eine Lösung könnte z.B. so eingerichtet sein, dass ein Mitglied des Vertriebsteams Zugang zum Vertriebsserver hat, nicht aber auf vertriebsfremde Server und Anwendungen, also z.B. nicht auf Daten des Personalwesens.

Mithilfe von Richtlinien lassen sich Zugangsanfragen anhand einer ganzen Reihe von Kriterien festlegen. Neben der Art des Geräts und des Benutzers könnte eine Richtlinie z.B. den Standort festlegen, von dem aus eine Anfrage kommen darf. So haben z.B. Geräte, die sich extern über VPN-Verbindung einwählen, andere Zugangsrechte als Geräte, die eine LAN-Verbindung verwenden.

### Überprüfen des Endpoints

NAC-Software kann zunächst auch im Modus „Nur melden“ implementiert werden. Dies ermöglicht Unternehmen eine netzwerkweite Übersicht, inwiefern die einzelnen Endpoints die Richtlinie einhalten, ohne das Tagesgeschäft zu unterbrechen. Die Lösung wird im Hintergrund ausgeführt, während der Endpoint ganz normal weiterarbeitet.

Anhand dieser Meldungen kann das IT-Team ermitteln, wie schwerwiegend das Compliance-Problem ist, und entsprechende Maßnahmen planen.

### Beheben des Problems

Viele Regelverstöße bei verwalteten Geräten lassen sich automatisch beheben, sodass sich der administrative Aufwand für das IT-Team reduziert und gleichzeitig volle Netzwerksicherheit gewährleistet ist.

So werden z.B. verwaltete Geräte, auf denen aktuelle Anti-Malware-Signaturen fehlen, die Firewalls deaktiviert sind, Betriebssystem- oder Anwendungssicherheits-Patches nicht auf dem neuesten Stand sind, vom NAC Agent aktualisiert. Die Aktualisierung erfolgt ohne Eingriff durch den Benutzer oder Administrator und senkt dadurch die Auswirkungen auf IT-Ressourcen und den Benutzer-Workflow.

Unverwaltete Geräte eignen sich normalerweise nicht für diese Art der Betreuung, da sie nicht der direkten Kontrolle des Unternehmens unterliegen. Hier werden Probleme dadurch behoben, dass der Benutzer eine Nachricht mit Anweisungen erhält, welche Maßnahmen zur Aktualisierung des betreffenden Endpoint-Computers zu ergreifen sind, um den Netzwerkzugang zu ermöglichen.

### Durchsetzen der Sicherheitsrichtlinie

Die letzte Phase der Implementierung betrifft unbekannte Endpoints, denen keine Netzwerkzugangsrechte zustehen. Solche Computer stellen ein klares Sicherheitsrisiko dar, und die NAC-Software reagiert, indem sie einfach den Zugang zum Netzwerk in Abstimmung mit der bestehenden Netzwerkinfrastruktur sperrt.

### Zusammenfassung

Die Abgrenzung von IT-Netzwerken nach außen wird immer fragwürdiger und schwieriger zu sichern. Dies liegt an der wachsenden Anzahl von Geräten und Zugangsmethoden, z.B. Mitarbeiter, die zu Hause oder unterwegs arbeiten, sowie Zugangsanfragen von Subunternehmern, Kunden und sonstigen Gastnutzern. Um zu steuern, wer und was sich in Ihr Netzwerk einwählt, entscheiden sich Unternehmen zunehmend für NAC, eine Lösung, die am besten auf der Endpoint-Ebene eingesetzt wird. Softwarebasierte NAC-Technologie ist hardwarebasierten Lösungen insofern überlegen, als dass sie alle bestehenden und später hinzukommenden Geräte mühelos abdeckt. Softwarebasierte NAC lässt sich zudem im gesamten Unternehmen einsetzen und bringt nur minimalen Aufwand für die Infrastruktur und die IT-Ressourcen mit sich.

---

## Sophos-Lösungen

Sophos bietet NAC-Lösungen zur Überprüfung und Kontrolle sämtlicher verwalteter und unverwalteter Computer an.

**Endpoint Security and Control** bietet Unternehmen grundlegende Kontrolle über den Sicherheitsstatus verwalteter und unverwalteter Computer.

**Sophos NAC Advanced** umfasst noch umfangreichere Richtliniendefinitionen und erweiterte Reporting-Funktionen.

## Quellen

1. *NAC for Dummies*, Wiley Publishing, Inc., 2008.
2. *Who's got the NAC? Best practices in protecting network access*. Aberdeen Group, Oktober 2007.
3. Sophos Endpoint Assessment Test, Mai 2008.
4. *Client Management 2.0*. Forrester, März 2007.
5. Sophos-Internetumfrage, September 2007.