



## **Aktuelle Studie von NetIQ weist auf die wachsende Bedeutung von Sicherheitsaspekten im Active-Directory-Management hin**

*NetIQ automatisiert proaktiv die Sicherheit und Verwaltung des Active Directory*

München – 28. August 2009 – Die erfolgreiche und effiziente Administration des Microsoft Active Directory zählt mit zu den wichtigsten Aufgaben von IT-Abteilungen. Die Ergebnisse einer aktuellen Studie von [NetIQ](#) verdeutlichen darüber hinaus die zentrale Bedeutung von Sicherheitsaspekten und zeigen eine Reihe von Herausforderungen auf, denen sich Administratoren bei der Absicherung von Active-Directory-Umgebungen stellen müssen. Angesichts des wachsenden Einsatzgebietes des Active Directory in Unternehmen bekommt die Absicherung der wertvollen Geschäftsressourcen im Active Directory eine zunehmende Dringlichkeit.

Von den 275 Unternehmen, die an der NetIQ-Studie teilgenommen haben, wurden das [Management von Gruppenrichtlinien](#), die [Pflege von Benutzerrechten](#) sowie die [Einhaltung von Compliance-Richtlinien](#) als die drei wichtigsten Herausforderungen im Bereich „Management“ und „Security“ des Active Directory genannt. So sehen 52 Prozent der Befragten die Durchsetzung von Richtlinien als eines der wichtigsten Themen an. 42 Prozent nannten die Nichteinhaltung von Compliance-Richtlinien und damit der Sicherheit als oberste Priorität. Zusätzlich betrachten 76 Prozent der Teilnehmer das Management des Active Directory als kritische oder wichtige Komponente ihrer entstehenden IAM-Strategien (Identity and Access Management).

Über die Hälfte der Befragten gab an, dass die Bedrohung durch unautorisierte Zugriffe und durch die Veränderung sensibler Daten IT-Abteilungen und Sicherheitsteams vor beträchtliche Schwierigkeiten stellt. Wenn Unternehmen Änderungen nicht feststellen können oder das Provisioning / Deprovisioning nicht flexibel verwalten können, multipliziert sich diese Bedrohung schnell um ein Mehrfaches. Um auf solche Risiken zu reagieren, müssen Unternehmen

entsprechende Richtlinien wirksam durchsetzen, Benutzerrechte einschränken und [unautorisierte Änderungen](#) im Active Directory – ob böswillig oder aus Versehen – kontrollieren.

Die Studie deckte außerdem folgende Fakten und Bedenken auf:

- 40 Prozent der Teilnehmer merken an, dass die Active-Directory-Ressourcen kaum mit den Unternehmensanforderungen Schritt halten können
- 85 Prozent geben an, dass ihre Active-Directory-Umgebungen allgemein durch IT-Teams verwaltet werden, bei 12 Prozent liegt diese Verantwortung direkt bei den Security-Teams und 3 Prozent greifen auf externe Anbieter zurück
- 49 Prozent sind der Meinung, dass die Informationssicherheit im Laufe der vergangenen drei Jahre zunehmend an Einfluss auf die Active-Directory-Richtlinien bzw. -Architektur gewonnen hat
- Lediglich 24 Prozent der Teilnehmer sind überzeugt, unautorisierte Veränderungen im Active Directory selbst feststellen zu können

Dies verdeutlicht, dass IT-Teams bei der Administration von Active Directory auf einen proaktiven Ansatz zurückgreifen sollten, um neue Anforderungen des Unternehmens sicher und effizient unterstützen zu können. Nur so wird ermöglicht, dass kritische und sensible Geschäftsinformationen so gespeichert werden, dass Unternehmen bei der Erfüllung ihrer Aufgaben unterstützt werden und gleichzeitig die Einhaltung von Unternehmensrichtlinien sowie branchenspezifischen Vorschriften gewährleistet ist.

Auf diese Weise können die Risiken reduziert werden, die in einem dynamischen Geschäftsumfeld herrschen. Um eine proaktive und sichere Administration von Active Directory sicherzustellen, sollten IT-Organisationen deshalb auf Lösungen zurückgreifen, mit denen die Sicherheit von Active Directory erhöht wird.

#### **Einhaltung der Compliance-Richtlinien und Kostenreduzierung:**

Um Unternehmen nicht nur zu helfen, Active Directory effizient abzusichern, sondern gleichzeitig auch die mit der Einhaltung von Compliance-Vorgaben verbundenen Kosten einzudämmen und somit letztlich eine bessere Ausrichtung an den geschäftlichen Zielsetzungen

des Unternehmens zu erreichen, bieten die Lösungen von NetIQ folgende Möglichkeiten und Vorteile:

- **Erkennung und Dokumentation von Änderungen in Active Directory:**

Mit NetIQs Lösungen für das Management von Active Directory können Änderungen in Active Directory in Echtzeit erkannt und klassifiziert werden, so dass Unternehmen schnell feststellen können, ob eine Änderung autorisiert ist oder nicht. Über individuelle Einstellungen können Alarme ausgelöst und Aktivitäten protokolliert und dokumentiert werden, so dass unbeabsichtigten Änderungen proaktiv entgegengewirkt wird.

- **Sichere Vergabe von Benutzerrechten:**

NetIQ-Lösungen ermöglichen eine regelbasierte und auch eine manuelle Vergabe von Benutzerrechten, wodurch die Arbeit von Administratoren erleichtert wird. Auf diese Weise kann festgelegt werden, dass Benutzer je nach Berechtigung bestimmte Aufgaben selbstständig erledigen können, wodurch die Inanspruchnahme von Help-Desk-Teams und anderen administrativen Mitarbeitern reduziert wird.

- **Erstellung von Berichten zu Benutzerrechten und Sicherheitskonfigurationen**

Mit den Active-Directory-Management-Lösungen von NetIQ können Unternehmen detaillierte Berichte generieren, mit denen dokumentiert wird, welche Mitarbeiter berechtigt sind, geschäftsprozessrelevante Änderungen vorzunehmen. Auf diese Weise kann die Anzahl von Benutzern, die unnötigerweise über uneingeschränkte Administrationsrechte verfügen, effektiv reduziert werden.

- **Automatisierung von IT-Prozessen für Active Directory**

Durch den Einsatz von NetIQ® Directory and Resource Administrator™ und die Nutzung der leistungsstarken Automatisierungsmöglichkeiten von NetIQ® Aegis® können routinemäßige Aufgaben im Zusammenhang mit der Administration von Active Directory automatisiert werden. Dies trägt zur Reduzierung des Risikos von Administratorfehlern, zu einer höheren Integrität der Daten und zur Minimierung der Gefahr einer Verunreinigung von Daten bei. IT-Teams sind so in der Lage, den veränderten Anforderungen des Unternehmens jederzeit kostengünstig gerecht zu werden.

**Zitat:**

„Das Active Directory spielt in Unternehmen eine zentrale Rolle und ohne Zweifel werden die Bedrohungen und Risiken auf diesem Gebiet zunehmen. Deshalb müssen IT-Organisationen ihr AD-Management neu definieren und Sicherheit und Compliance integrieren. Nur so können sie den Anforderungen des Unternehmens vollständig entsprechen“, erklärt Erin Avery, Manager of Product Marketing bei NetIQ. „Durch die Institutionalisierung und [Automatisierung von Sicherheit](#) und internen Kontrollfunktionen im Rahmen des täglichen Active-Directory-Managements werden IT-Organisationen die Kosten zur Sicherstellung der Compliance besser kontrollieren und letztlich die Ausrichtung an den Anforderungen des Unternehmens kontinuierlich verbessern können.“

**Über NetIQ**

NetIQ, ein Geschäftsbereich von Attachmate, ist ein weltweit führender Anbieter von Lösungen für das Systems und Security Management. Mehr als 12.000 Kunden in über 60 Ländern setzen NetIQ Lösungen ein, die IT-Organisationen unterstützen, IT Services im gesamten Unternehmen zu verbessern, Kosten messbar zu senken und gleichzeitig die Effizienz zu steigern. Das Portfolio von NetIQ umfasst IT Process Automation, Systems Management, Security Management, Configuration Audit, Configuration Control und Enterprise Administration sowie Lösungen für Unified Communications Management. Weitere Informationen finden Sie unter [www.netiq.de](http://www.netiq.de)

**Pressekontakte**

Lucy Turpin Communications GmbH  
Eva Hildebrandt und Katrin Hauck  
Prinzregentenstraße 79  
81675 München  
Tel.: (+49) (089) 41 77 61-14 / -15  
Attachmate [at] LucyTurpin.com

Attachmate Germany GmbH  
Nicole Dunkel  
Feringastrasse 11  
85774 Unterföhring  
Tel.: (+49) (089) 99 351-0  
[Nicole.Dunkel \[at\] Attachmate.com](mailto:Nicole.Dunkel@Attachmate.com)

*Copyright© 2009 NetIQ Corporation. All Rights Reserved. NetIQ, the NetIQ logo are trademarks or registered trademarks of NetIQ Corporation in the USA. All other trademarks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.*