

Zürich, 24. Januar 2007 – 14. at rete Event:

NAC - Network Access Control: Flexibilität und Schutz oder Aufwand und Fragezeichen?

NAC ist im Hype: Analysten prophezeien NAC eine goldene Zukunft; es gibt verschiedene Ansätze, das Thema anzugehen; und weit über 50 Hersteller versuchen, genau ihr NAC-Konzept und ihre NAC-Produkte der Kundschaft schmackhaft zu machen. at rete nahm das Thema genauer unter die Lupe.

Der 14. Kundenevent, diesmal im Hotel Zürichberg, war dem Thema NAC gewidmet, wobei at rete ihre Erfahrung aus verschiedenen aktuellen Kundenprojekten einfließen liess. Zuerst jedoch verabschiedete Toni Klee, CEO von at rete, Paolo Sebben, der viele Jahre als Director Sales & Marketing bei at rete tätig war und nun eine neue Herausforderung annehmen wird. Gleichzeitig nahm Klee die Gelegenheit wahr, Sebbens Nachfolger zu begrüssen, den 39-jährigen Michael Kaufmann.

Martin Strässler eröffnete den Hauptteil der Veranstaltung und stellte gleich zu Beginn fest, dass NAC prinzipiell ein Teil des Risikomanagements in einem Unternehmen ist. Es geht um IT Compliance und Security Policies sowie um die Kontrolle, wer zum Unternehmensnetzwerk und zu welchen Services Zutritt erhält. Im Juli hatte 2006 die Zeitschrift Network Computing in einer Umfrage die Business-Treiber für NAC ermittelt. Demzufolge sprachen sich 58% der Befragten für „Address Network Security Compliance“, 48% für „Enforce access control to specific network resources“ und 40% für „Provide controlled access for unmanaged users (partners, contractors)“ aus, wobei Mehrfachnennungen möglich waren.

Für eine Technologie im Hype ist es völlig normal, dass die diversen Hersteller verschiedene Lösungsansätze für NAC bieten – von Basic NAC mit einfacher Überprüfung der MAC-Adresse und Switch Enforcement bis hin zu Advanced NAC mit einer Client-Software für eine eingehende Überprüfung des Systems auf Patch-Level-Zustand, aktuelle Anti-Virus-Software und so weiter. Gemäss Strässler wird es noch 2-3 Jahre gehen, bis NAC sich als Grundschutz etabliert und demzufolge eine breite Akzeptanz erfährt. Es ist anzunehmen, dass sich dabei auch die Herstellerlandschaft selber auf ein paar wenige standard-basierte Lösungen reguliert.



Adrian Schmidlin ging als nächstes auf die entscheidenden Faktoren bei der Umsetzung von NAC ein und präsentierte die vorhandenen Lösungsansätze Switch-Integration, 802.1x und Client-Software.

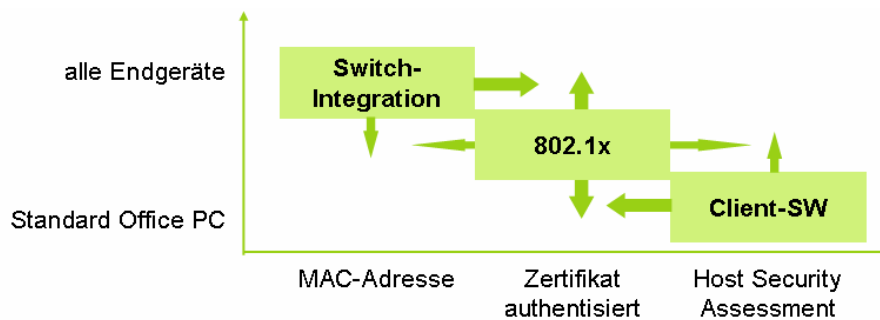


Abb. 1: NAC-Lösungsansätze

Entscheidend bei der Wahl des Ansatzes ist, dass definiert wird, welche Bedürfnisse mit einer NAC-Lösung erfüllt werden sollen. Anhand der folgenden Tabelle präsentierte Schmidlin im Überblick, welche Lösung sich wofür eignet:

Protection Pain Points (NWC Analytics, Poll)	Switch-Integration	802.1x	Client-SW (Agent)
Access to datacenter		✓	✓
Remote access			✓
Wireless LANs		✓	✓
Wired access to corporate LAN	✓	✓	
Branch office to corporate resources			✓
Guest access	✓	✓	
Contractor access	✓	✓	

Abb. 2: Business-Treiber

Basierend auf der Erfahrung aus verschiedenen at rete Kundenprojekten lassen sich die betrieblichen Aspekte wie folgt zusammenfassen:

Lösungen basierend auf der MAC-Adresse erlauben eine einfache Umsetzung betreffend Switch-Port-Management. Sie brauchen nur eine Inventarisierung der



MAC-Adressen und bieten den breitesten Grundschutz, wenn auch auf relativ tiefem Niveau. 802.1x-Lösungen haben im Gegensatz zu MAC-Lösungen besondere Anforderungen an die Switch-Hardware und die Endgeräte, indem sie einen höheren Aufwand im Switch-Port-Management bedingen, da sie nicht durchgängig realisierbar sind (z.B. müssen Legacy Systeme ohne 802.1x angeschlossen werden können). Dafür ist die Sicherheit höher als bei der MAC-Identifizierung, da typischerweise Zertifikate geprüft werden. Noch eine höhere Sicherheit versprechen die Client-Software-Lösungen, die jedoch meist nur für Windows-Systeme verfügbar sind. Mit einem Agent lässt sich auf den Endsystemen ein Host Assessment durchführen. Je nach Hersteller ist eine agentenbasierte Lösung ohne Switch-Integration realisierbar. Für alle Lösungen gilt, dass das Zertifikat- und Inventarmanagement einen moderaten Zusatzaufwand bedeutet.

Nach diesen Präsentationen kam der von vielen mit Spannung erwartete praktische Teil. at rete hatte in bewährter Weise einen RFP für ein virtuelles mittelgroßes Unternehmen mit ca. 820 Mitarbeitenden ausgearbeitet und verschiedenen Herstellern zugestellt. Cisco, United Security Provider und Juniper hatten eine schriftliche Offerte eingereicht und präsentierten ihr Angebot dem Publikum. Michel Chappuis von at rete hatte die eingegangenen Antworten vorab analysiert und präsentierte anschliessend den Anwesenden den Vergleich. Es kamen drei völlig unterschiedliche Lösungen mit erstaunlicherweise sehr ähnlichen Gesamtkosten zusammen.

Ein letzter Höhepunkt war die Präsentation von Christoph Graf, Leiter Abteilung Security bei SWITCH. Dieser zeigte, wie SWITCH, bereits lange bevor es den Begriff NAC überhaupt gab, eine auf VPN basierte Access-Control-Lösung für das akademische Umfeld geschaffen hatte und diese heute organisations- und auch grenzübergreifend auf Basis 802.1x eingesetzt wird. Dank diesem Service „Edu-roam“ haben heute unzählige Organisationen in über dreissig Ländern bei allen Partnerorganisationen automatisch Netzwerkzugriff.

Der Ausklang des Events fand diesmal im Zürcher Zoo statt mit einer Führung zum Thema Kommunikation im Tierreich, abgerundet mit einem Abendessen in der Masoala-Halle.

Michael Kaufmann, Tel. 044 266 55 55, Fax 044 266 55 88, E-Mail: info@atrete.ch

