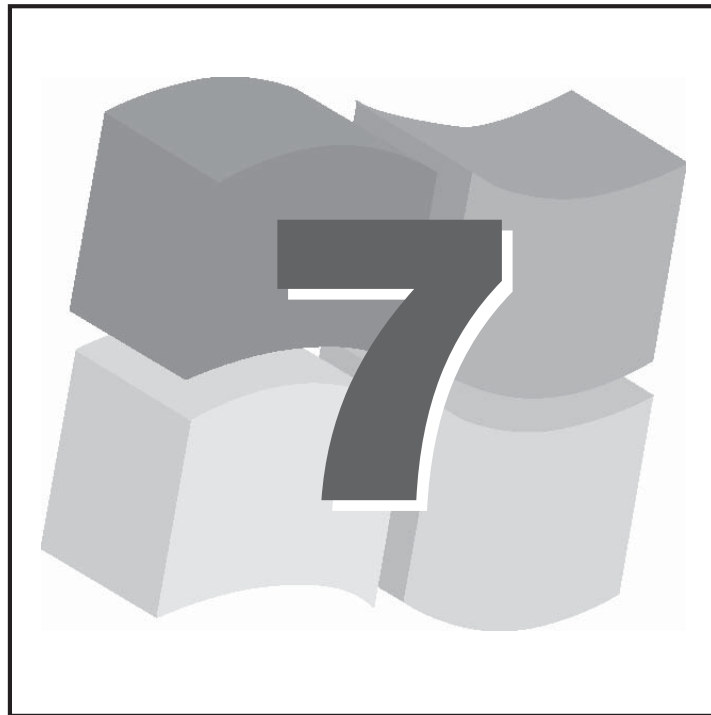


Erfordern Infrastruktur- Maßnahmen Windows 7?

von Dr. Frank Imhoff, Dominik Zöller



Nachdem sich während der Wirtschaftskrise viele Unternehmen große Zurückhaltung auferlegt haben, werden inzwischen wieder weitreichend Investitionen in Netzwerk- und Rechenzentrums-Infrastruktur geplant. Der Einsatz von IPv6, die Einführung von 802.1X, Unified Communications und Virtualisierung sowie der Ausbau des zentralen Managements sind Themen, die unsere Kunden derzeit intensiv bewegen.

Doch sind diese Aspekte ohne die Einführung neuer Server- und Client-Betriebssysteme überhaupt realisierbar? Und wie passt das am 22. Oktober 2009 erschienene Microsoft-Betriebssystem Windows 7, das aufgrund des geringen Marktanteils von Windows Vista als faktischer Nachfolger von Windows XP gelten kann, in dieses Bild?

Auf den ersten Blick stellt sich die Frage, was ein Client-Betriebssystem überhaupt mit Vernetzungsthemen wie IPv6, VPN etc. zu tun hat. Schließlich sind das Dinge, die teilweise schon lange diskutiert und andererseits lange schon genutzt werden. Windows 7 bietet gerade hier aber spannende Neuerungen, die möglicherweise zum Durchbruch führen.

Zweitthema

Erfordern Infrastruktur- Maßnahmen Windows 7?

Fortsetzung von Seite 1



Dr. Frank Imhoff ist Technischer Direktor der ComConsult Beratung und Planung GmbH. Er leitet dort den Bereich Applikationen. Unter seiner Verantwortung sind bereits zahllose Beratungsprojekte zu den Themen Voice, Unified Communications, Collaboration, Messaging, Mobilfunk etc. erfolgreich durchgeführt worden.



Dominik Zöllner ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich bereits auf moderne Kommunikationsnetze und Betriebssysteme. Zu seinen Spezialgebieten gehören jetzt u.a. die Konzeption und Ausschreibung professioneller Unified-Communications- und Kollaborations-Systeme sowie Microsoft-Lösungen.

IPv6-Fähigkeit

Das Thema IPv6 gärt seit nunmehr 14 Jahren in den Standardisierungsgremien dieser Welt. Lange schon ist klar, dass knapp 4,3 Milliarden IPv4 Adressen auf lange Sicht nicht den Bedarf einer vernetzten Welt decken können. Diese und weitere Unzulänglichkeiten von IPv4 in Puncto Erweiterbarkeit und Sicherheit führten zur Suche nach einer Alternative, welche man mit IPv6 theoretisch schon lange gefunden hat. Der nahezu unerschöpfliche Vorrat der 128 Bit langen IPv6 Adressen („das sind mehr, als es Sandkörner auf der Erde gibt“) ermöglicht es, jedem beliebigen Endgerät eine eigene, weltweit eindeutige Adresse zuzuweisen, ohne auf Krücken wie dynamische IP-Vergabe und Network Address Translation (NAT) zurückgreifen zu müssen. Gerade im Bereich der mobilen Endgeräte ist IPv6 daher äußerst attraktiv. Auch die erhöhte Sicherheit durch direkte Verankerung von IPsec im Protokoll lässt auf einen baldigen Durchbruch im Markt hoffen.

Doch eine Vielzahl von Problemen verhinderte bislang die Ablösung von IPv4. Anstelle einer kompatiblen Erweiterung des IPv4 Adressraums, führte die IETF mit IPv6 ein gänzlich neues Adressformat ein. Da viele Applikationen noch auf die Verwendung von IPv4 angewiesen sind, muss eine Koexistenz von beiden Protokollen über einen langen Zeitraum durch verschiedene Workarounds ermöglicht wer-

den. Inkompatible Endgeräte und Server müssen mithilfe von Gateways an IPv6-Netzbereiche angebunden werden. Ganze Netze, deren Umstellung auf IPv6 aus technischen oder wirtschaftlichen Gründen noch nicht möglich ist, müssen durch Tunnel überbrückt werden. Neue Endgeräte und Infrastrukturen müssen auf nicht absehbare Zeit die Nutzung beider Protokolle ermöglichen (Dual Stack).

Nicht erst seit dem gelungenem Aprilscherz der tagesschau.de-Redaktion ist das Thema IPv6 wieder auf dem sprichwörtlichen Tisch der Unternehmen. Die ARD titelte pünktlich zum 1. April diesen Jahres: „Alle IP-Adressen besetzt – ICANN schaltet Rootserver ab“ (<http://www.tagesschau.de/ausland/internet-abschaltung100.html>, zuletzt überprüft: 23.05.2010), und versetzte so einige Entscheider in helle Aufregung. Nicht auszu-denken, welche Folgen eine eintägige Abschaltung des gesamten Internet hätte. Das Chaos würde alle Vulkanausbrüche und Flugverbote problemlos in den Schatten stellen. Natürlich wird es – eben aufgrund der massiven logistischen und wirtschaftlichen Abhängigkeit – niemals eine geplante Totalabschaltung des Internet geben. Der Wandel muss sich schrittweise vollziehen. Mit der oben angesprochenen Koexistenz von IPv4 und IPv6.

Doch bei den Unternehmen setzt sich langsam aber sicher die Erkenntnis durch, dass ein Umstieg auf IPv6 nicht ewig auf

die lange Bank geschoben werden kann. Auch wenn lange Zeit ein Parallelbetrieb und die damit verbundenen Kosten in Kauf genommen werden müssen, so möchten doch die Wenigsten von einer plötzlichen Migrationswelle überrascht werden. Daher wird bei Investitionen in Applikationen und RZ-Infrastruktur zunehmend auf eine Aufwärtskompatibilität zu IPv6 geachtet, um Investitionssicherheit in Hinblick auf eine spätere Migration herzustellen.

Beim Dual Stack wird neben der IPv4-Adresse zusätzlich auch noch eine IPv6-Adresse zugewiesen. Ein Rechner kann dann über beide Protokolle unabhängig kommunizieren. Dieses Verfahren sollte der Regelfall sein, scheitert derzeit jedoch oft daran, dass einige Router auf dem Weg zum IPv6-Internet noch keine IPv6-Weiterleitung eingeschaltet haben oder unterstützen. Das hat vor allem in Heimnetzwerken oder bei direkt an das Internet angeschlossenen PCs zu Problemen geführt, da hier immer wieder Meldungen über fehlende Konnektivität etc. auftraten. Grund dafür ist die mangelnde Unterstützung von IPv6 durch die Zugangsserver des Internetproviders oder die Heimrouter. In Unternehmensnetzen sollte diesem Problem aber durch die Konfiguration der entsprechenden Router begegnet werden.

So ist es zu begrüßen, dass IPv6 nun endlich auch seinen festen Platz im Netzwerk-Stack von Windows gefunden hat. Bereits im Vorgänger Vista eingeführt, scheint

Erfordern Infrastruktur-Maßnahmen Windows 7?

der Dual Stack nun unter Windows 7 einen praxistauglichen Zustand erreicht zu haben. Auch bei den Server-Betriebssystemen der Produktreihe Windows Server 2008 gehört IPv6 zum Funktionsumfang. Den zukünftigen Stellenwert von IPv6 in der Windows Welt kann man an Microsofts Direct Access Konzept ablesen. Doch dazu später mehr. Bleibt die Feststellung, dass mit Windows 7 der Übergang zu IPv6 in greifbare Nähe rückt. Die Robustheit der Implementierung muss sich in zukünftigen Tests und der Praxis erst noch erweisen. Der Aufbau einer IPv6-basierten Infrastruktur setzt aber - falls Windows als Betriebssystem gesetzt ist - definitiv die Ablösung von XP durch Windows 7 voraus.

Wer aber immer noch XP in einer IPv6-Domäne betrieben muss, kann sich auch hier helfen: Mit „ipv6 install“ ist es möglich, bei Windows XP einen IPv6-Protokollstapel installieren. Ab Service Pack 1 hat dieser Protokollstapel „Production Quality“ und wird als Protokoll in den Netzwerkeigenschaften hinzugefügt. Ab Service Pack 2 kann IPv6 ebenfalls unter den Netzwerkeigenschaften hinzugefügt werden („Internet Protokoll Version 6“). Als DNS-Server können IPv6-Adressen mittels netsh eingetragen werden. In Bezug auf den Mobility-Support gilt für Windows XP ab Service Pack 1 das Gleiche wie für Windows Server 2003: „correspondent nodes“ sind verfügbar, „mobile nodes“ und „home agent nodes“ dagegen nicht. Im Rahmen des Mobile-IPv6-Technology-Preview-Programms sind allerdings entsprechende Erweiterungen verfügbar. Hat das System eine global routbare IPv4-Adresse, richtet Windows XP automatisch einen 6to4-Tunnel ein. Näheres ist unter <http://www.microsoft.com/germany/technology/datenbank/articles/600912.mspx> (zuletzt überprüft am 23.5.2010) zu finden.

Auf jeden Fall ist mit Windows 7 der Übergang in Richtung IPv6 ein weiteres Mal deutlich erleichtert worden. Derzeit sind aber lt. DE-CIX nicht mal 0,2 Prozent des über den größten deutschen Internet-Knoten abgewickelten Datenverkehrs IPv6-Pakete. Aufgrund des immensen chinesischen Wachstums und dem daraus folgenden Bedarfs an Internet-Adressen wird das aber sicherlich nicht mehr lange so bleiben. Nicht ohne Grund halte China Telecom bereits v6-Backbone-Netze für 120 Millionen Kunden vor. Hinzu kommen technische Entwicklungen wie Cloud Computing oder das „Internet of things“. Auch die deutsche Bundesregierung ist inzwischen auf dem Weg in Richtung IPv6. Das Bundesinnenministerium ist Mitglied im RIPE-NCC und hat bereits fünf Quintilli-

onen IP-Adressen (ein /26-Subnetz) für die öffentlichen Verwaltungen Deutschlands erhalten. Zudem starten in diesem Jahr zahlreiche Dual-Stack- und Migrationsprojekte in öffentlichen Verwaltungen.

Aber die Neuerungen von IPv6 umfassen nicht nur die Vergrößerung des verfügbaren Adressraums um den Faktor 296, sondern beispielsweise auch Vereinfachung und Verbesserung des Protokollrahmens. Das führt vor allem für Router zu einer schnelleren Verarbeitung der entsprechenden Pakete. Aber auch die zustandslose automatische Konfiguration von IPv6-Adressen, Mobile IP, Vereinfachung von Umnummerierung und Multihoming sowie die Implementierung von IPsec innerhalb des IPv6-Standards werden zu zahlreichen Neuerungen und Verbesserungen führen. Gerade aber auch die immer weiter um sich greifende IP-Telefonie und Videoübertragung wird durch die Unterstützung von Quality of Service und Multicast profitieren.

Quality of Service

Das Thema Quality of Service ist spätestens seit der zunehmenden Verbreitung von Voice- und Videodiensten immer wieder Anlass für Diskussionen. Während vor allem die Hersteller und Provider von VoIP-Lösungen den Einsatz QoS-Mechanismen sowohl für LANs als auch für WAN-Strecken fordern, vertritt ComConsult schon seit Jahren die Ansicht, dass im LAN-Bereich QoS weitgehend überflüssig ist. Was im WAN gut und sinnvoll ist, kann im LAN

wesentlich einfacher und billiger durch eine moderate und in den meisten Fällen ohnehin vorhandenes Overprovisioning erreicht werden.

Microsoft hat mit dem Einstieg in die Unified-Communications-Welt mit der Entwicklung eigener Voice- und Videocodes (RTAudio, RTVideo) für den Office Communications Server sogar den Versuch unternommen, auch im WAN auf QoS zu verzichten zu können. Dennoch erlauben Windows Vista und Windows 7 QoS-Einstellungen auf Betriebssystemebene. Neben dem DSCP-Wert kann die „Drosselungsrate“ konfiguriert werden. Hierüber lässt sich die Datenrate ausgehender Verbindungen gezielt begrenzen. Die Festlegung folgender Parameter kann per GPO zentralisiert erfolgen:

- Pfad/URL der Anwendung
- Quell- und Ziel-Adressen (IPv4 oder IPv6) oder Adresspräfixe
- Transport-Protokoll (TCP, UDP, beide)
- Quell- oder Zielports oder Portbereiche (TCP oder UDP)

Dies hat den Vorteil, dass Anwendungen nicht zwingend QoS-Aware sein müssen, um sich in ein QoS-Konzept zu integrieren. Da ist vor allem im Hinblick auf nicht QoS-fähige Applikationen sinnvoll, die über WAN-Strecken kommunizieren. Das ist beispielsweise immer dann der Fall, wenn der zugehörige Dienst im Zuge des Outsourcings als Hosted Solution angeboten wird oder die Applikation einer Außenstelle an die Zentrale angebunden werden

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Erfordern Infrastruktur-Maßnahmen Windows 7?

muss. Der mangelnde Nutzen für das LAN und die zunehmende QoS-Awareness von Applikationen reduzieren den Sinn dieses Windows 7 Merkmals aber ausschließlich auf das zentrale Management von applikationsbezogenen QoS-Parametern. Nicht mehr, aber auch nicht weniger. (siehe Abbildung 1)

Branch Cache

Eine weitere Möglichkeit mit Hilfe von Windows 7, unmittelbar Einfluss auf die Zugriffsgeschwindigkeit insbesondere für Außenstellen zu nehmen, ist der so genannte „Branch Cache“ – also ein Netzwerk-Cache für Zweigstellen. Damit werden von der Firmenzentrale abgerufene Inhalte zwischengespeichert, so dass sie ab dem zweiten Abruf der gesamten Außenstelle über das dortige LAN zur Verfügung stehen. Das ermöglicht vor allem den hoch performanten Zugriff auf Verzeichnisse, Zugriffsrechte oder Dateien, wenn eine häufige Nutzung derselben Inhalte innerhalb einer Außenstelle zu erwarten ist. Damit können also insbesondere Zugriffe auf zentrale Netz-Laufwerke erheblich beschleunigt werden, ohne die WAN-Anbindungen aufbohren zu müssen. Für häufige Nutzer von Netzlaufwerken ist das zweifelsohne eine erhebliche Erleichterung.

Selbstverständlich werden die Zugriffsrechte etc. auch weiterhin berücksichtigt. Bis auf die je nach Anwendungsfall stark verbesserte Performance ergibt sich für die Nutzer dadurch keine Änderung bei der Arbeit. In der Firmenzentrale benötigt Branch Cache zwingend Windows Server 2008 R2, am Arbeitsplatz eine Business-Version von Windows 7.

802.1X Unterstützung

Zur Absicherung von Unternehmensnetzen erfreut sich IEEE 802.1X einer immer größeren Beliebtheit. Mit 802.1X wird die Authentifizierung und Autorisierung von Clients direkt am Port des Access-Switches oder am Access Points des Wireless LAN ermöglicht. Hierzu authentisiert sich das Endgerät (Supplicant) beim Authenticator. Der Authenticator ist eine Netzwerk-Entität, die im Switch oder Access Point implementiert ist und die Zugangsdaten mit einem RADIUS-Server abgleicht. Erst nach erfolgreicher Authentifizierung erhält das Endgerät Zugriff auf das physikalische oder virtuelle Netzwerk (VLAN). (siehe Abbildung 2)

802.1X war bereits in Windows XP integriert, allerdings nur für WLANs. Für LANs nach IEEE 802.3 konnte 802.1X nur mit ei-

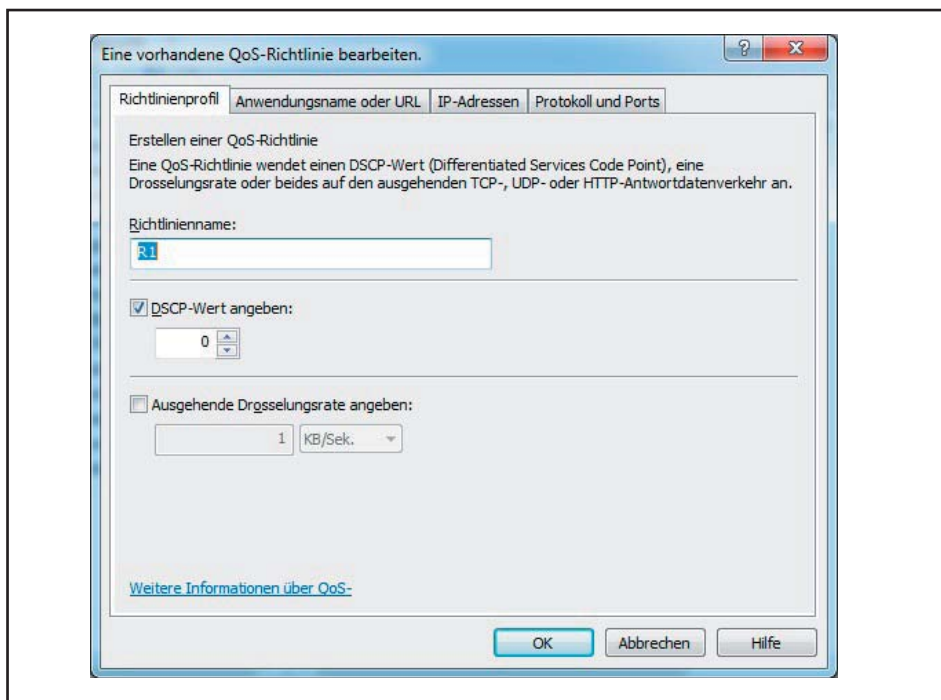


Abbildung 1: Konfiguration einer QoS-GPO

nigen unschönen Trickereien verwendet werden. Eine zentrale Administration der 802.1X Konfiguration war dennoch nicht möglich. Unter Windows 7 können die 802.1X Einstellungen nicht nur für WLAN,

sondern auch für kabelgebundene Netze konfiguriert werden. Dabei kann per GPO neben der generellen Verwendung von 802.1X erzwungen, sondern auch das Authentifizierungsverfahren und zugehörige

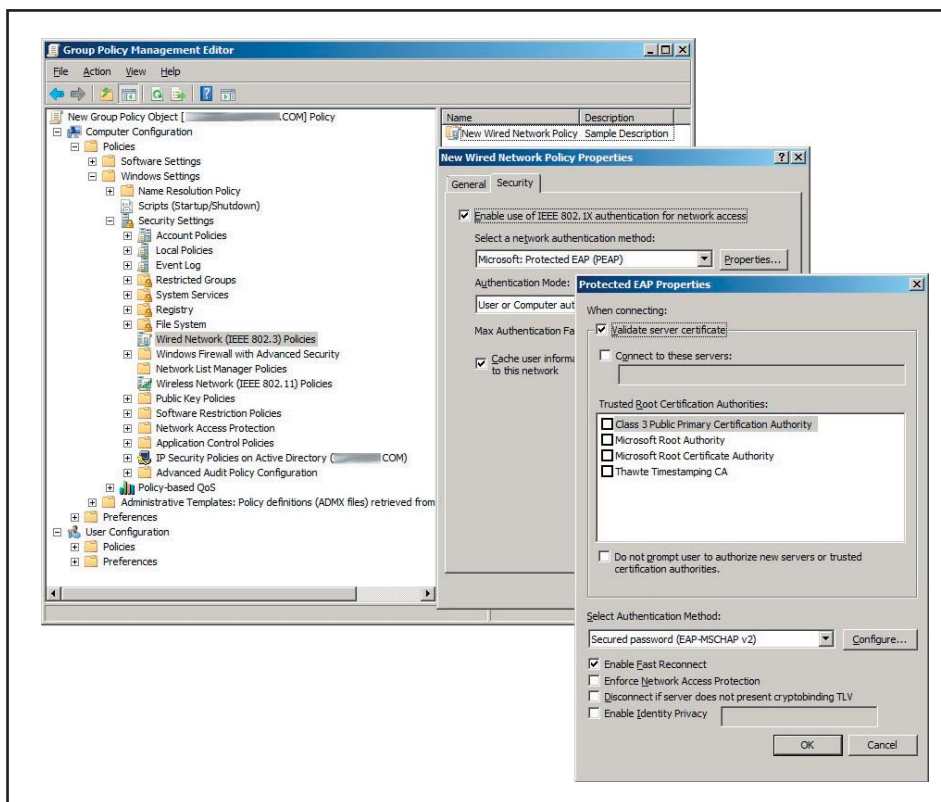


Abbildung 2: 802.1X Einstellungen

Erfordern Infrastruktur-Maßnahmen Windows 7?

Parameter, wie die Adresse des Authentifizierungsservers zentral administriert werden. Diese Möglichkeiten dürfte die Einführung von 802.1X in den meisten Unternehmen erheblich attraktiver machen als bisher schon.

Network Access Control

Noch einen Schritt weiter als 802.1X geht die so genannte Network Access Control (NAC) von Microsoft (vergleiche Abbildung 3). Sie ermöglicht den Schutz eines Netzwerks vor potentiell unsicheren Clients, indem die Einhaltung von Sicherheitsrichtlinien vor dem Netzzugriff überprüft wird. Diese Richtlinien können individuell auf die Infrastruktur und die verwendeten Applikationen des Unternehmens abgestimmt werden sowie unter anderem auch verschiedene Nutzergruppen berücksichtigen.

Bevor ein Client eine Verbindung zum Firmennetzwerk herstellt, überprüft der NAC-Agent (vergleiche Abbildung 4), ob auf dem Computer die erforderliche Software - z.B. Firewall, Patches, Virens Scanner - und Einstellungen vorhanden sind. Je nach „Gesundheit“ und Rechten des Clients

wird ihm dann der Zugang zu bestimmten Netzbereichen (vergleiche Abbildung 5) und Diensten gewährt oder verweigert. Werden Missstände festgestellt, so können diese automatisch behoben werden, indem beispielsweise der Zugriff auf ein Quarantäne-Netz gewährt und darüber Software- und Konfigurations-Updates eingespielt werden. Bis den Sicherheitsanforderungen entsprochen wird, erfolgt der Netzzugriff dann nur eingeschränkt oder wird komplett verweigert.

NAP ist Microsofts Implementierung des NAC-Konzepts. Die Umsetzung war bereits für Windows 2003 R2/Windows XP angedacht. Mit einiger Verspätung wurde unter Windows Vista erstmals ein NAP-Agent in das Betriebssystem integriert und in Verbindung mit Windows Server 2008 R2 kann eine NAP Infrastruktur aufgebaut werden. Insbesondere ist es empfehlenswert, NAP in Verbindung mit 802.1X und dynamischen VLANs einzusetzen. So kann eine verlässliche Identifikation der Clients gewährleistet werden. Durch NAP als unsicher identifizierte Clients können dann in einem VLAN mit eingeschränktem Zugriff separiert werden, während ande-

re VLANs den „gesunden“ Clients vorbehalten sind. NAP kann auch in Verbindung mit bestehenden VPN-Lösungen eingesetzt werden.

Direct Access

Mit Windows 7 Ultimate steht mobilen und auswärtigen Nutzern erstmals Direct Access (DA) zur Verfügung. Damit ist es möglich, unmittelbar sicheren Zugriff auf Firmenressourcen (Intranet, Datei-Freigaben, LOB-Systeme) zu ermöglichen. DA ist dabei deutlich mehr als eine bloße VPN-Lösung, sondern deren Ersatz. Denn anstelle einer Einwahl über einen VPN-Client bekommen Rechner automatisch Zugriff auf die Firmenrechner, sobald über das Internet Verbindung besteht. Der mobile Client ist damit auch vom Unternehmen aus erreichbar, beispielsweise für Updates oder Helpdesk-Support über Remote Desktop. Auch NAT-Anbindungen z.B. aus einem privaten Netzwerk heraus oder Client-Management-Konzepte (z.B. Intel vPro) können mit einer VPN-freien Anbindung wesentlich effizienter realisiert werden als bisher.

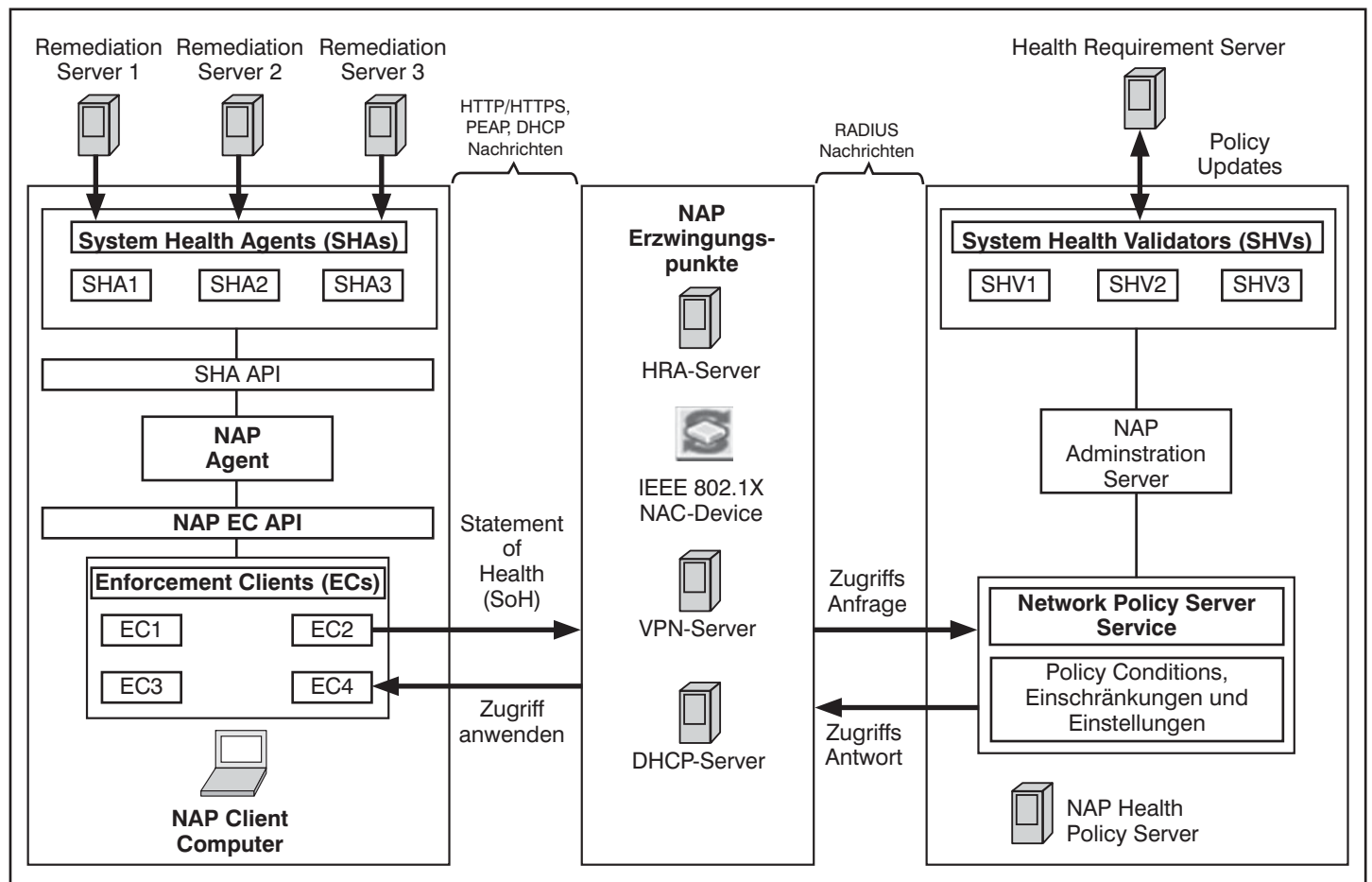


Abbildung 3: Interaktion der NAP-Komponenten

Erfordern Infrastruktur-Maßnahmen Windows 7?

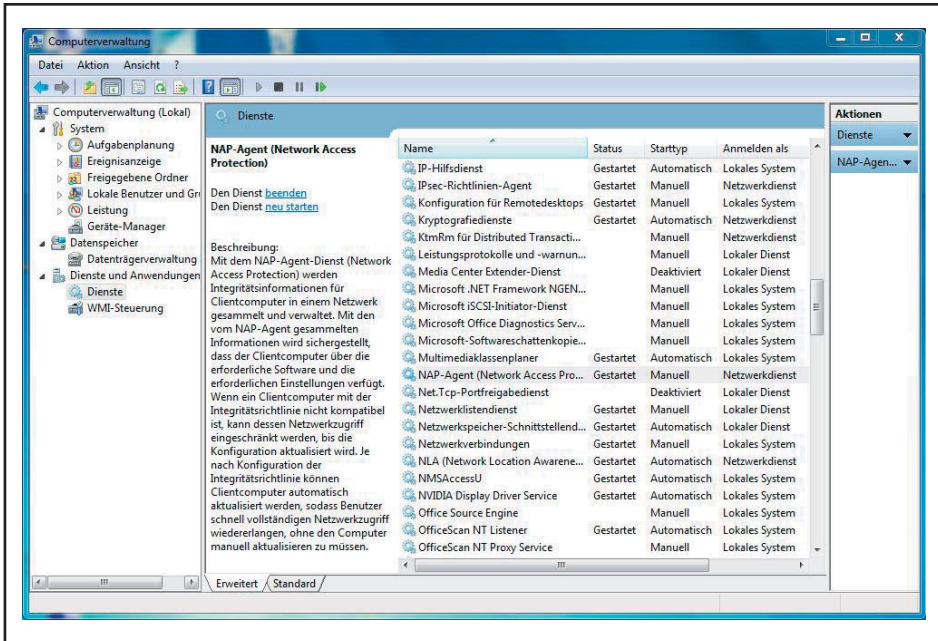


Abbildung 4: NAP-Agent

Um die Sicherheit auch ohne VPN zu gewährleisten, setzt Microsoft auf die in IPv6 enthaltenen IPsec-Mechanismen. Mithilfe eines Gateway-Servers auf Basis von Windows Server 2008 R2 wird die Authentifizierung und Autorisierung der mobilen Clients durchgeführt. Der Zugriff erfolgt transparent, also ohne Zutun des Anwenders, ohne manuelles „Einwählen“ in ein VPN oder Umleitung der normalen Internet-Zugriffe über das Unternehmensnetz. Bei bestehendem Internetzugriff wird das mobile Endgerät automatisch Teil des Unternehmensnetzes, ist also auch zu administrativen Zwecken vom Unternehmensnetz aus erreichbar. So können Wartungsarbeiten durchgeführt, Updates eingespielt und Gruppenrichtlinien angewendet werden, ohne dass ein mobiler Anwender in das Unternehmensnetz zurückkehren muss.

Wird Direct Access mit NAP kombiniert, müssen Direct-Access-Clients mit aktivem Netzwerkzugriffsschutz bei der ersten Verbindung mit dem Direct-Access-Server ein Integritätszertifikat für die Authentifizierung übermitteln. Dieses Integritätszertifikat enthält neben der Identität des Rechners auch die Zusicherung der Integrität des Systems. Damit ist beispielsweise sichergestellt, dass auf dem Rechner keine unzulässigen Applikationen installiert oder Virens Scanner auf dem neuesten Stand sind. Der Direct-Access-Client erhält das Integritätszertifikat erst, wenn Integritätsstatusinformationen vollständig an eine Integritätsregistrierungsstelle im Internet gesendet worden sind. Damit lässt sich unter anderem auch ein Unternehmensweiter Sicherheitsstand für mobile Mitarbeiter zeitnah durchsetzen. (siehe Abbildung 6)

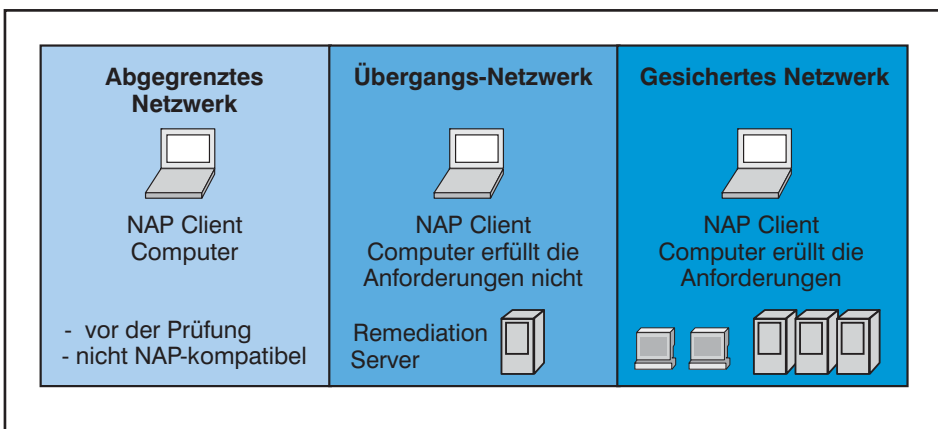


Abbildung 5: Netzwerkbereiche

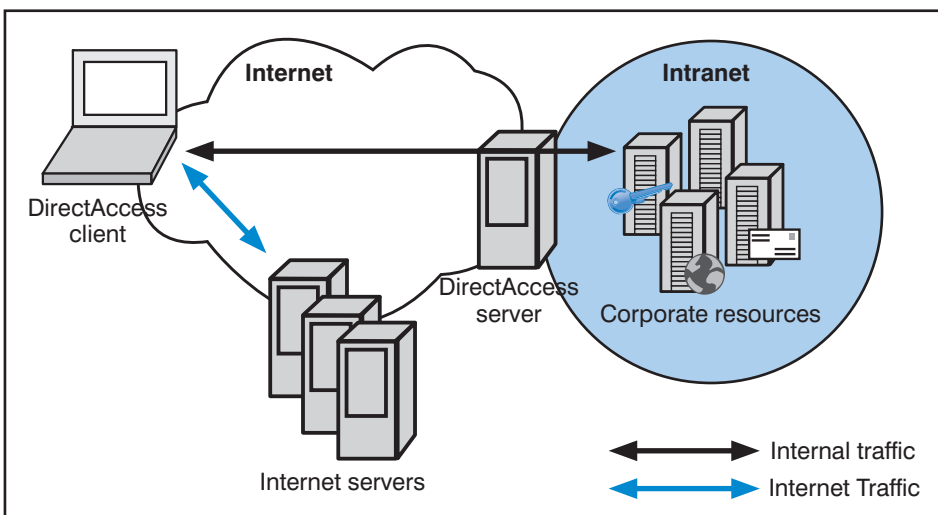


Abbildung 6: Direct Access mit IPv6 und IPsec

Um dieses Feature nutzen zu können, wird ein IPsec-over-IPv6 Tunnel zwischen dem Endgerät und dem jeweiligen Server aufgebaut. Für das Routing im Internet kann aus Kompatibilitätsgründen zu IPv4 „6to4“ (RFC 3056) oder „Teredo“ (RFC 4380) zum Einsatz kommen. Der IPv6-over-IPv4 Tunnel wird dabei im Unternehmensnetz terminiert, so dass die Adressierung der Server auf Basis von IPv6 stattfindet. Spätestens das macht eine IPv6-Infrastruktur im Unternehmensnetz notwendig. Server, die aus technischen Gründen nicht per IPv6 adressierbar sind, müssen über IPv6-Gateways angebunden werden.

Dass Microsoft hier auf IPv6 setzt, ist dem Umstand geschuldet, dass IPsec im IPv6-Standard verankert wurde und somit die Integrität und Ende-zu-Ende-Sicherheit für Dienst-Sessions gewährleistet werden kann. Zudem ist die eindeutige Adressierung von mobilen Endgeräten, unabhängig von eventuell dynamischen IPv4-

Erfordern Infrastruktur-Maßnahmen Windows 7?

Adressen, ein weiterer Pluspunkt.

Auch wenn das Tunneln von IPv6-Verbindungen momentan zusätzlichen Overhead erzeugt, ist der Einsatz von IPv6 hier doch sinnvoll und zukunftsweisend. Denn nach einer durchgängigen Umstellung der Netze auf IPv6 kann derzeit noch erforderlicher Kompatibilitätsballast abgeworfen werden. Falls also die Investition in IPv6-Infrastruktur geplant ist, macht der Einsatz von Direct Access Sinn. Die gezielte Freigabe von Diensten für die mobilen Clients, die Erreichbarkeit der Clients zu Wartungszwecken und der für den Benutzer transparente Zugriff auf das Unternehmensnetz sind nicht von der Hand zu weisende Vorteile. Ohne entsprechende IPv6-Migration können diese Vorteile allerdings nicht genutzt werden und es bleibt nur die Verwendung klassischer VPN-Lösungen.

Aber immerhin wurde auch für VPN-Nutzer noch eine kleine Verbesserung eingeführt: Windows 7 bietet erstmals VPN Reconnect, also das erneute Aufbauen des VPN-Tunnels ohne Zutun des Anwenders, falls dieser aufgrund fehlender Internet-Konnektivität getrennt wurde. Insofern ist Windows 7 auch ohne IPv6 für mobile Nutzer ein großer Fortschritt, so richtig komfortabel wird es aber erst mit IPv6. Dementsprechend ist auch hier mit einem Vorschub für die neue Adressierung und demzufolge mit deutlich mehr IPv6-Implementierungen in Unternehmen zu rechnen.

Übrigens lässt sich Direct Access aber auch von Clients nutzen, die nicht mit Windows 7 ausgestattet sind. Denn Dank der Standardisierung von Teredo ist es auch für andere Betriebssysteme wie beispielsweise Linux und Mac OS verfügbar. Die bekannteste Implementierung für Linux und Mac OS ist „Miredo“.

Doch die Nutzung von Teredo bringt auch Gefahren für die Unternehmen mit sich. Beispielsweise werden damit die Sicherheitsfunktionen NAT-basierter IPv4 Router ausgehebelt, denn die IPv6-Pakete werden in IPv4-basierte UDP-Nachrichten verpackt und damit transparent über IPv4-NAT-Komponenten und den UDP-Port 3544 übermittelt. Dadurch werden beispielsweise simple Paketfilter wirkungslos. Hinzu kommt, dass 6to4 oder Teredo die Clients u.U. zu nicht authentifizierten und weltweit erreichbaren IPv6-Gateways macht. Auf diese Weise ist dann auch ein unmittelbarer Zugriff auf die angeschlossenen IPv4-Netz-Komponenten denkbar.

Alternativen zu Windows 7

Die Neuerungen von Windows 7 sind

heutzutage für fast alle Unternehmen von Bedeutung: Verbesserter Zugriff von Außenstellen aus, einfacherer Zugriff von mobilen Clients, verbesserte Sicherheits- und Administrationsmerkmale und so weiter. Gleichzeitig steigt mit der Einführung von Windows 7 die Motivation, über neue Netzwerkstrukturen und Strukturen nachzudenken. Hier steht sicherlich IPv6 im Vordergrund. Aber auch andersherum wird ein Schuh draus. Denn nicht wenige Unternehmen müssen beispielsweise aufgrund der Einführung von Voice over IP oder Unified Communications eben mal kurz doppelt so viele IP-Adressen zur Verfügung stellen wie bisher. NAT und die Verwendung von reservierten Adressbereichen mögen hier zwar notfalls noch eine Zeit lang reichen, aber konsequent ist erst ein Umdenken in Richtung IPv6.

Ist die Entscheidung in Richtung IPv6 gefallen, ist ein Wechsel zu Windows 7 naheliegend. Betrachtet man Windows 7 aber mit der seit Vista gebotenen Skepsis, muss man sich natürlich auch die Frage nach möglichen Alternativen stellen.

Alternative 1: Alles bleibt wie es war

Windows XP (oder sogar Win2k?) verrichtet seine Dienste mehr oder weniger klaglos. Nach drei Servicepacks und etlichen Bug-Fixes haben Anwender wie Administratoren den Vista-Vorgänger liebgewonnen. Falls ein entsprechender Servicevertrag abgeschlossen wurde, kann der Betrieb im Status Quo noch bis maximal 2014 aufrecht erhalten werden.

Viele Unternehmen verfügen noch über keine IPv6-fähige Infrastruktur und die Umsetzung von 802.1X wurde bislang meist nur in höchst sicherheitskritischen Netzbereichen vorangetrieben. Zumeist begnügt man sich mit der auch unter XP verfügbaren Implementierung für WLAN-Clients.

Mobile Mitarbeiter werden über dedizierte VPN-Lösungen in das Unternehmensnetz eingebunden. Eine transparente Ende-zu-Ende Verschlüsselung der Dienst-Sessions à la Direct Access wird vielfach nur als Bonus wahrgenommen. Ein Wechsel des Betriebssystems ist von dieser Warte aus - zumindest für den Zeitraum der kommenden vier Jahre - nicht notwendig. Und dann wird ohnehin bereits Windows 8 verfügbar sein.

Alternative 2: Auf „Nummer sicher“ gehen

Die Entscheidung für ein neues Betriebssystem wurde vielerorts lang herausgezögert. Die alten Systeme sind

den heutigen Herausforderungen nicht mehr gewachsen, der Zeitpunkt für Neues ist gekommen. Aber da die Erfahrung mit XP gezeigt hat, dass ein neues Betriebssystem frühestens nach dem ersten Servicepack wirklich brauchbar ist, entscheidet man sich für den Mittelweg - die Umstellung auf Windows Vista.

Der Wechsel auf ein bereits seit Längerem etabliertes Betriebssystem kann vor unliebsamen Überraschungen schützen und Kosten sparen. Es kann bereits auf langjährige Erfahrungen in Administration und Anwendung zurückgegriffen werden, was den Umstieg deutlich erleichtert. Nachdem für Vista bereits SP2 vorliegt, ist jetzt der richtige Zeitpunkt, es im Unternehmen auszurollen. Das verschafft genügend Spielraum, um Erfahrungen rund um Windows 7 zu sammeln.

Aber älteren Rechnern sollte man diesen Schritt nicht mehr zumuten. Der Ressourcenbedarf von Vista ist atemberaubend. War der „alte“ Rechner unter XP subjektiv immer noch höchst performant ist er trotz Speicherweiterung nach der Umstellung auf Vista nicht selten eine lahme Krücke. Das trifft gleichermaßen natürlich auch auf Windows 7 zu.

Alternative 3: Neue Wege gehen

Wer sich kommerzieller Software-Produkte wie Microsoft Windows entledigen möchte, wird vielleicht mit dem Gedanken spielen, seine Desktops mit Linux auszustatten. Das Open-Source-Betriebssystem kann mit nunmehr 18-jähriger Geschichte als etabliert gelten und hatte gerade im preisbewussten SMB-Sektor, aber auch in den Rechenzentren der Enterprise-Welt einen festen Platz ergattert. Linux ist in vielerlei Hinsicht eine interessante - wenn auch keineswegs kostenlose - Alternative zu Microsofts Betriebssystemfamilie. Die Diskussion über das Für und Wider einer solchen Alternative ist jedoch nicht erschöpfend zu führen, schon gar nicht hier, im Rahmen dieses Artikels.

Betrachtet man die „Abstimmung mit den Füßen“, ist die Entscheidung bei den meisten Nutzern gefallen. Denn offensichtlich verkauft sich Windows 7 zwischenzeitlich aber besser als „geschnitten Brot“: Seit dem Verkaufsstart am 22. Oktober 2009 sind schon über 100 Millionen Lizenzen verkauft worden. Das ist selbst für Microsoft überraschend gewesen und hat zeitweise zu Lieferengpässen geführt. Windows 7 ist damit schon jetzt das mit Abstand erfolgreichste Betriebs-

Erfordern Infrastruktur-Maßnahmen Windows 7?

system überhaupt und innerhalb von nur sechs Monaten schon auf 10 Prozent aller PCs weltweit installiert.

Noch deutlicher wird der Erfolg im Vergleich zu Vista: Alleine in den letzten drei Monaten hat Microsoft seinen Umsatz mit Windows im Vergleich zum Vorjahr um 28 Prozent erhöht und damit fast 4,5 Milliarden US-Dollar umgesetzt. Allerdings ist diese Entwicklung angesichts der großen Schwächen von Vista sicherlich nicht überraschend. Viele Unternehmen haben lange, z.T. sogar sehr lange mit einem Umstieg gewartet, um sich nicht mit Vista herumärgern zu müssen. Aus heutiger Sicht war das sicherlich eine kluge Entscheidung. Welche Bedeutung Windows XP noch immer hat, wird mit einem Marktanteil von über 64 Prozent deutlich. Vista hat es gerade mal auf 10,2 Prozent gebracht. Da wird es noch einige Zeit dauern, bis Windows 7 an diese Marktanteile kommt.

Fazit

Während viele Features von Windows 7, wie z.B. VPN Reconnect, als marginal abgetan werden können, sind gerade im Bereich von Netzwerk- und Datensicherheit richtungsweisende Fortschritte erkennbar. Zwar wurden einige dieser Fähigkeiten schon mit Windows Vista eingeführt. Aufgrund der geringen Akzeptanz von Vista, welche nicht zuletzt auf schlechte Performance und unnötige Gängelung des Benutzers zurück zu führen ist, ist von einem Zwischenschritt über Vista allerdings dringend abzuraten. Mit einem regulären Ende des Mainstream Supports im April 2012 ist ein Verfallsdatum gesetzt, das – im Gegensatz zum beliebten XP – auch nicht mehr verlängert werden dürfte. Es muss also effektiv die Entscheidung zwischen dem – temporären – Verbleib bei Windows XP und der baldigen Migration zu Windows 7 getroffen werden. Hierbei ist Folgendes zu beachten:

1. Werden Applikationen eingesetzt, für die (noch) keine Windows 7 Unterstützung geboten wird und die nicht im XP Mode lauffähig sind, so kann keine Migration eingeleitet werden. Dies ist insbesondere der Fall, wenn das entsprechende Softwareprodukt nicht weiterentwickelt wird, aufgrund des spezifischen Einsatzgebiets kurzfristig aber kein adäquates Ersatzprodukt eingeführt werden kann. Hier muss eine Migration bis zum Ende eventuell bestehender Service- und Wartungsverträge und der Einführung eines Ersatzproduktes zurückgestellt werden.
2. Steht in naher Zukunft der Austausch

eines signifikanten Anteils von Client-Hardware an, so macht es Sinn, die Migration bis zu diesem Zeitpunkt zu verschieben. Die Performance profitiert von der besseren Unterstützung aktueller Hardware durch die gute Treiberbasis von Windows 7. Bei Neubeschaffungen von Hardware sollte auf Kompatibilität geprüft werden, auch wenn bei aktueller Hardware in den wenigstens Fällen mit Problemen zu rechnen ist. Insbesondere bei der Transition von 32-bit zu 64-bit Plattformen ist ein Umstieg auf Windows 7 ratsam, da die in die Jahre gekommene Architektur von Windows XP die gebotenen Performancevorteile nur unzureichend ausnutzt.

3. Sind Investitionen in die Netzwerk- und Serverinfrastruktur geplant, ist es sinnvoll, die Anforderungen in puncto Sicherheit, Dienstgüte und Erweiterbarkeit einer erneuten Prüfung zu unterziehen. Viele Technologien, die momentan Einzug in die Unternehmensnetze halten, wie z.B. IPv6 oder 802.1X, können ihre Vorzüge im Zusammenspiel mit Windows XP nicht entfalten. Auch die Einbindung mobi-

ler Mitarbeiter und die Ende-zu-Ende Sicherheit von Diensten kann durch eine Umstellung auf Windows Server 2008 und Windows 7 konsistenter gestaltet werden.

Im Falle nicht austauschbarer Spezial-Soft- und -Hardware kann eine Verzögerung der Migration zu Windows 7 also Sinn machen. Generell ist aber, in Hinblick auf die Investitionssicherheit der IT-Infrastruktur, ein baldiger Wechsel zu Windows 7 dringend zu empfehlen. Gerade im Zusammenspiel mit dem anstehenden Austausch von Client-Hardware und strukturellen Veränderungen im Unternehmensnetz, wie der Überarbeitung des Sicherheits- und Mobilitätskonzeptes, erscheint die Migration hochgradig sinnvoll.

Spätestens mit dem für das vierte Quartal 2010 zu erwartenden Service Pack 1 sollten erfahrungsgemäß die meisten Kinderkrankheiten behoben und eine reibungslose Migration möglich sein. Bei guter Migrationsvorbereitung können die Mitarbeiter so bald von einem stabilen und dem Stand der Technik entsprechenden Betriebssystem profitieren. Dann steht auch Investitionen in das Unternehmensnetz nichts mehr im Weg.

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>