ComConsult Research

# Der Netzwerk Insider

Januar 2006

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

## Ende der Hackerromantik - Kriminelle auf dem Vormarsch

**von Dipl.-Inform. Detlef Weidenhammer**

Obwohl Hacker in den letzten Jahren für eine Vielzahl von gravierenden Sicherheitsvorfällen mit Millionenschäden verantwortlich waren, haftet ihnen zuweilen noch immer ein romantisches Flair an. Dies dürfte sich bald ändern, denn zunehmend stellen sie ihre Fähigkeiten auch in den Dienst krimineller Organisationen. Gefährdet sind dadurch vorrangig Unternehmen aus den Bereichen eBusiness und Finanzdienstleistung, aber auch kritische Infrastrukturen müssen sich mit den zunehmenden Bedrohungen ernsthafter als bisher auseinander setzen.

Die ersten weltbekannten Hacker verbreiteten noch eine Art Cyberromantik und verfügten über so wohlklingende Namen wie Phiber Optik, Mafiaboy oder Agent Steal. Hacker sahen sich vorrangig als technisch Interessierte, denen es um die Lösung von Problemen und die Überwindung von Grenzen(!) ging. Man legte großen Wert auf die Abgrenzung zu sog. Crackern, die es sich im Gegensatz zu den Hackern zum Ziel machten, in fremde Systeme einzudringen und diese zu manipulieren. Die wohl gängigste Beschreibung zur Hackerkultur findet sich in „How to become a hacker“ von Eric Raymond (siehe http://www.catb.org/~esr/faqs/hacker-howto.html). Die Grenzen zwischen den WhiteHats (Hacker) und den BlackHats (Cracker) verschwammen aber sehr schnell und mittlerweile ist es mit der Romantik endgültig vorbei.

weiter auf Seite 21

Zweitthema

## Trennung von Benutzergruppen - Lösungen und ihre Folgen

**von Markus Schaub**

Spricht man heute über Sicherheit, so spricht man mit Sicherheit über zwei Themen: WLAN und etwas, was gerne mit dem schwammigen Begriff „Benutzertrennung“ tituliert wird. Seit dem WLAN-WEP Desaster stehen die Betreiber vieler Netze vor einem Dilemma: auf der einen Seite werden WLANs für Besprechungsräume, Kassensysteme, Scanner und vieles mehr gefordert, zum anderen soll die Sicherheit des Netzes natürlich nicht gefährdet werden. Dank mannigfacher Meldungen sowohl in der Fachpresse, vor allem aber auch in den alltäglichen Nachrichten, ist die Zugangssicherheit von ihrem Dornröschenschlaf geweckt ins Zentrum der Aufmerksamkeit vieler Manager gerückt worden. Und nun geht es nicht mehr um WLANs alleine, sondern um die Frage, wie generell ein Netzwerk gegen unberechtigte Zugriffe geschützt werden kann. Mit dem IEEE Standard 802.1X war schnell ein Mittel gefunden, das sich diese Forderung erfüllt. Aber 1X regelt nur das „Wer“ und „Wer-Nicht“, nicht jedoch das „Wie“ und das „Worauf“. Die (vorgebliche) Unsicherheit der WLANs stellte jedoch genau diese Anforderung: wer über ein WLAN zugreift, soll nur beschränkte Zugriffsrechte haben. Auch dafür wurden Konzepte entwickelt, die sich schnell auch auf andere Bereiche ausweiten lassen, wie kabelgebundene Netze und weitere Probleme wie die Umzugsproblematik. Ein jeder User soll gemäß seinem Netzwerkzugang immer und überall die notwendigen Zugriffsrechte bekommen, die für seine Arbeit wichtig und gemäß dem Netzwerkzugang angemessen sind.

weiter auf Seite 9

Top Veranstaltung

### Netzwerk-Redesign Forum 2006

auf Seite 4

Zum Geleit

### WiMax kontra IEEE 802.11n: hat WiMax wirklich eine Perspektive?

auf Seite 2

Report des Monats

### Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“

auf Seite 18

Zum Geleit

# WiMax kontra IEEE 802.11n: hat WiMax wirklich eine Perspektive?

Die Frage der Marktbedeutung und Investitionssicherheit zukünftiger Wireless-Technologien wurde auf dem Wireless-LAN-Forum im November intensiv diskutiert. Insbesondere der Wettbewerb zwischen WiMax und und dem neuen IEEE 802.11n-Standard stand dabei im Vordergrund. Aufgrund der höherwertigen Funktechnik wird dabei immer wieder über eine Ablösung der heutigen Wireless-Technologien durch völlig neue Technologien wie WiMax nach IEEE 802.16 spekuliert. Wäre dieses Risiko wirklich gegeben, dann müssten alle Investitionen in die heutige 802.11-Technik hoch riskant sein.

Aber wo stehen wir mit dem Vergleich dieser Technologien heute wirklich?

Auslöser der Zweifel an der Investitionssicherheit der heutigen 802.11-Technik sind die inhärenten Mängel dieser Technologie, die in der Tat sehr ernst zu nehmen sind:

- Zum einen sind dies Mängel im Standard, dort vor Allem das Medienzugangsverfahren und die Reduzierung auf 3 überschneidungsfreie 2,4GHz-Kanäle. Das Medienzugangsverfahren DCF verbraucht nicht nur die Hälfte der verfügbaren Bandbreite, es kann auch bei zu vielen Stationen pro Zelle kollabieren. Die Reduzierung auf maximal 3 überschneidungsfreie Kanäle macht ein flächendeckendes Design ohne Interferenzen nahezu unmöglich. In der Regel wird man bei intensiver Nutzung in der Fläche mit partiellen Störungen in einzelnen Zellen rechnen müssen
- Die heute verfügbaren Radioteile speziell für 802.11g sind schlicht schlecht. Sie strahlen stark in Nachbarkanäle und vernichten die mit der OFDM-Kodierung gewonnenen Vorteile gleich wieder (im Prinzip müsste OFDM dazu führen, dass man 4 Kanäle ohne große Verluste nutzen kann, dies ist aber bei Weitem nicht der Fall, unser Labor hat dazu umfangreiche Analysen ausgeführt, die 11g-Radios scheinen eindeutig schlechter zu sein als 11b Radios)
- Die Nutzung des 2,4 GHz-Bandes führt zu unabsehbaren und unkalkulierbaren Interferenzen mit anderen Nutzungsformen in diesem offenen Frequenzband. Insbesondere ist so keine Betriebssicherheit für die Zukunft gegeben, da niemand weiß, ob nicht morgen eine neue Anwendung im 2,4 GHz-Band entsteht
- Weder IEEE 801.11b noch 11g sind Backbone-Technologien, sie sind reine Client-Technologien. Insbesondere reichen die maximalen Sendeleistungen in der Regel nicht aus, um stabil größere Entfernungen zu überwinden (auch wenn die Sendeleistung auf einen eingeschränkten Abstrahlwinkel reduziert wird)

Diese Mängel sind nun seit Jahren bekannt und viele Anwender fühlen sich ob dieser Mängel auch in ihrer Investitionsentscheidung verunsichert. Da muss naturgemäß eine neue Wireless-Technologie wie WiMax wie die aufgehende Sonne am Horizont wirken. Die Kerneigenschaften von WiMax sind (für Details wird auf den Artikel von Dr. Kauffels im Netzwerk-Insider verwiesen, bei Bedarf anfordern):

- Hohe Reichweite
- Hohe Übertragungsrate
- Vermaschte Backbone-Infrastruktur mit sehr hoher Verfügbarkeit
- Deutlich besseres Medienzugangsverfahren
- Im Wesentlichen Nutzung reservierter Frequenzen

Bei der Betrachtung dieser Kerneigenschaften darf nicht übersehen werden, dass zurzeit noch keine wirklichen Serienprodukte verfügbar sind (vor Allem haben erste Pilotversuche weder die angestrebten Reichweiten noch die erhofften Bandbreiten erreicht). Und die Produkte, die verfügbar sind, sind reine Backbone-Produkte. Die unter 802.16e-genormte Client-Technologie, die sehr stark von Intel gepuscht wird, wird voraussichtlich nicht vor 2007 zur Verfügung stehen. So sind denn auch die heute typischen WiMax-Projekte Provider-Projekte, bei denen DSL-Konkurrenznetze auf Funkbasis errichtet werden. Dazu werden häufig nicht offene Frequenzen genutzt (3,5 GHz), die auch eine Zuweisung bzw. einen Kauf durch den Provider erfordern (in der Tat muss hier mit sehr hohen Kosten gerechnet werden). In der Regel wird damit eine vermaschte Infrastruktur aufgebaut, die Sichtkontaktfrei sehr stabil größere Flächen erschließen kann. Als Teilnehmer muss man sich dabei zurzeit eine Basisstation vorstellen, die ihrerseits den Übergang zu einer weiteren lokalen Infrastruktur schafft, typischerweise 802.11g zurzeit. Auch sind zurzeit keine seriösen Aussagen zu den Kosten einer WiMax-Infrastruktur möglich, man kann vermuten, dass der Client-Chip für Notebook PCs der Preisstruktur der heutigen 802.11-Netze entsprechen wird, aber die Kosten der Infrastruktur-Komponenten sind noch unklar.

Ist also die Erwartung, dass WiMax alle heutigen Funktechniken ablösen wird, real? Meiner Ansicht nach nein. Ich bin davon überzeugt, dass mit 95% Wahrscheinlichkeit WiMax auf Dauer eine Provider- bzw. Spezial-Technik für Sonderprojekte bleiben wird. Auf jeden Fall sehe ich die Nutzung primär im Backbone-Bereich. Mögliche Sonderprojekte könnten Transportsteuerungen in sehr großen Geländen wie Flughäfen oder Seehäfen sein. Hier könnte eine bessere und stabilere Flächenabdeckung mit einer parallel erhöhten Verfügbarkeit erreicht werden. Allerdings gibt es auch heute schon für 802.11 Produkte für den Logistik-Bereich mit sehr hohen Verfügbarkeitswerten (Beispiel Siemens).

Die Begründung für diese Annahme, dass WiMax die bisherigen Funktechniken nicht überrollen wird:

- Bei der Aufzählung der Nachteile von 802.11b/g wurde 802.11a/h nicht erwähnt. Es hat zwar das gleiche schlechte Medienzugangsverfahren, aber ansonsten deutliche Vorteile:
  - Deutlich bessere Ausleuchtung als 11b/g nach umfangreichen Messungen des ComConsult-Labors

WiMax kontra IEEE 802.11n: hat WiMax wirklich eine Perspektive?

  - Durch Sendeleistungen bis zu 1W gleichzeitig Eignung als Backbone-Technik, in der Praxis werden bereits große Backbones mit dieser 11a-Variante aufgebaut, gegenüber WiMax fehlt hier aber die Vermaschung und die Bandbreite liegt weit unter der von WiMax angestrebten Bandbreite
  - Höhere Zahl überschneidungsfreier Kanäle, so dass auch ein Flächendesign mit einer hohen Zellanzahl kein Problem ist
- Parallel entsteht mit 802.11n zur Zeit ein neuer Standard, der deutlich erhöhte Bandbreiten und Reichweiten mit sich bringt. Dieser Standard wird sehr stark vom Konsumer-Markt getrieben, der jetzt schon mehr als 50% des Marktes bestimmt und dessen Dominanz weiter zunehmen wird. Es muss damit gerechnet werden, dass 11n die Anforderungen des Konsumer-Marktes für die normalen Haushalte erfüllt. Damit ist vorerst für die Hersteller keine Motivation gegeben, gleich weiter am nächsten Standard zu arbeiten (die einzige Motivation wäre in der Tat, mit einem neuen Standard wieder neue Produkte verkaufen zu können, auch wenn diese vielleicht gar nicht benötigt werden). Aus heutiger Sicht spricht vieles dafür, dass IEEE 802.11n ein auf Jahre dominanter Wireless-Standard sein wird.

Die Konsequenzen werden sein:
- Konkurrenzlos niedrige Preise für den Client-Anschluss
- Ein Zusammenbrechen der Preise für Access-Points
- Die automatische Integration in immer mehr Typen von Endgeräten

IEEE 802.11n kann die normative Kraft des Faktischen werden. Risiken dabei sind:
- Die dabei eingesetzte MIMO-Technik hält nicht das, was sie theoretisch verspricht, speziell bezogen auf Stabilität und Reichweite. So überzeugen die bisher verfügbaren MIMO-Produkte, die allerdings nicht auf dem Standard 11n basieren, nicht wirklich. Trotzdem muss man davon ausgehen, dass mit Verfügbarkeit der ersten Standard-basierten Produkte diese Probleme gelöst werden
- IEEE 802.11n gestattet die Nutzung des 2,4GHz und des 5GHz-Bandes. Risiko ist, dass weiterhin die Hauptnutzung im 2,4GHz-Band erfolgt und der unbedingt notwendige Wechsel ins 5GHz-Band weiter verzögert wird. Es ist aber deutlich erkennbar, dass immer mehr Hersteller diesen Wechsel mit ihren Produkten vollziehen bzw. vollzogen haben (wobei leider zum Teil viel zu niedrige Sendeleistungen angeboten werden, was im Kern am eingesetzten Chip liegt, der leider sehr verbreitet ist)

Wie sieht nun meine persönliche Prognose aus:
1. Ich bin davon überzeugt, dass die IEEE 802.11n-Welle ab 2006 losläuft. Wenn die Hersteller sich nicht völlig zerstreiten, wird eine Verabschiedung des Standards möglich und Produkte werden schnell verfügbar sein. Das größte Risiko ist hier, dass der hohe Bedarfsdruck aus dem Konsumermarkt eine Welle von weiteren Pre-Standard-Produkten erzeugen könnte.
2. Die Hersteller haben den Wechsel ins 5 GHz-Band nun endlich vollzogen. Zumindest gibt es ein ausreichend großes Produktangebot attraktiver Hersteller, zu denen erfreulicherweise auch der deutsche Hersteller Lancom zählt.
3. Nach den bisher absehbaren Entwicklungen werden WiMax-Client-Produkte nach 802.16e einfach zu spät kommen. Sie werden technisch den bisherigen Wireless-Produkten überlegen sein, aber sie werden auf einen bereits teilweise gesättigten Client-Markt stoßen und in Summe über alle Kosten für lange Zeit auch deutlich teurer sein.
4. Auf der Providerebene bestehen in der möglichen WiMax-Akzeptanz weltweit erhebliche Unterschiede. Speziell in großflächigen Ländern mit eher dünner Besiedelung ist WiMax kostenmäßig nicht zu schlagen. Es ist keine Frage, dass es sich hier durchsetzen wird. Gerade aber in Europa und Deutschland hat WiMax mit der bereits existierenden UMTS-Infrastruktur eine erhebliche Konkurrenz. Vor Allem kann die Bereitschaft der großen Provider, hier eine zweite Parallelinfrastruktur aufzubauen, in Zweifel gezogen werden. Hier ist doch eher mit einer kontinuierlichen Verbesserung der UMTS-Leistung zu rechnen.

Im Kern bin ich davon überzeugt, dass WiMax für den Client-Bereich nur dann eine Chance hat, wenn sich 11n weiter verzögert und wenn 16e-Produkte von Anfang an sehr preiswert angeboten werden. Eigentlich hat 16e überhaupt nur eine Chance, weil Intel sich sehr stark engagiert und die Integration in die Notebook-Chipsets (Centrino) angekündigt hat. Aber es gilt der bekannte Spruch, wer zu spät kommt, den bestraft das Leben. Und es sieht so aus, dass WiMax für den Client-Bereich zu spät kommt.

In diesem Sinne sehe ich zurzeit keine Investitionsunsicherheit für Wireless-Produkte, wenn bestimmte Kriterien beachtet werden:
- Klare Orientierung am 5 GHz-Band
- Umsetzung einer zentralen Konfigurations-Lösung insbesondere zur schnellen Neukonfiguration der Kanalzuweisungen in den Zellen (ein dynamischer Kanalwechsel wie im Standard kann bei einer hohen Zelldichte nur sauber funktionieren, wenn er zwischen Nachbarzellen abgestimmt wird). Generell sollte man die Frage beantworten können, wie man sich einen Frequenzwechsel in den Zellen vorstellt, dessen Notwendigkeit sich beispielsweise durch ein Redesign mit neuen Zellen ergeben kann
- Zeitlich abgestimmter Wechsel von 11h nach 11n, d.h. jeder der zurzeit in 11h investiert, sollte klare Vorstellungen haben, wann 11n kommt und wann er seine Investitionen auf den neuen Standard umschwenkt. Gerade die bekannten und großen Hersteller können bei der Frage der Produkt-Verfügbarkeit wieder die bekannt träge Masse sein. Im Zweifelsfall sollte man sicht auf dynamischere Spezialanbieter konzentrieren
- Flächige Installationen müssen Voice-fähig sein (Zellüberlappung, L3-Handover)

Es darf dabei auch nicht übersehen werden, dass die meisten der großen Wireless-Projekte im Logistik- und Produktionsbereich stattfinden. Hier ist die Marktmacht von Intel nicht so entscheidend, da viele Spezial-Clients im Einsatz sind. Hier wird eher entscheidend sein, was Hersteller wie Symbol machen werden.

Fazit: keine Angst vor WiMax und die Zeit lieber für die Diskussion der Nutzbarkeit von Wireless-Switches in der 802.11-Technik nutzen. Diese können ab 100 Access-Points in einer zusammenhängenden Fläche deutliche Vorteile bieten. Allerdings erfordert die fehlende Standardisierung der Produkte erhebliche Kenntnisse in diesem sehr dynamischen Marktsegment. Auch gibt es ernstzunehmende Alternativen mit zentraler Konfiguration, die nicht auf einer Switchtechnik basieren (Lancom).

Dieses Thema wird ohne Frage zu intensiven Diskussionen auf dem Netzwerk-Redesign Forum 2006 führen. Wir werden diese mit aktuellen Studien und Projekterfahrungen, die wir zum Forum vorstellen, unterstützen.

Bis dahin

Ihr
Dr. Jürgen Suppan

Top-Kongress

# Netzwerk-Redesign Forum 2006

Die ComConsult Akademie veranstaltet vom 27. - 30. März das Netzwerk-Redesign Forum 2006.

Mit den wachsenden Anforderungen an Netzwerke hat sich das Design moderner Netzwerke immer weiter gewandelt. Im Wesentlichen basiert dieser Wandel auf 5 Kernfaktoren:

- Erhöhte Leistung in Kombination mit erhöhter Verfügbarkeit
- Vorbereitung auf IP-Telefonie (Voice-ready) und weitere neue IP-basierte Dienste
- Architektonische Integration von WLANs
- Sicherheit in mehreren Stufen auf Netzwerk-Ebene
- Vorbereitung auf Service-Management für ausgewählte Services

Nachdem Netzwerk-Produkte in den letzten Jahren im Kern immer ähnlicher wurden, laufen sie angesichts dieser Bedarfssituation wieder deutlich auseinander. Die Hersteller wählen zum Teil stark voneinander abweichende Lösungs- und Design-Ansätze.

Unsere Top-Veranstaltung des Jahres 2006 analysiert die aktuellsten Entwicklungen der Netzwerk-Technologien und bewertet Marktrends, Hersteller-Strategien und Produktentwicklungen. Wir blicken für Sie hinter die Kulissen, geben Erfahrungsberichte aus Top-aktuellen Projekten und bewerten die Praxis-Relevanz der neuesten Trends.

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Themen über den ganzen Tag intensiv evaluiert. Sie können zwischen folgenden Intensiv-Trainings wählen:

- SIP in der Analyse: auf dem Wege zur offenen IP-Telefonie?
- Wireless LAN in Produktion und Logistik
- Quality of Service

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

# Netzwerk-Redesign Forum 2006

Ich buche den Kongress
**Netzwerk-Redesign-Forum 2006**
vom 27.03. - 30.03.06 in Königswinter

**mit „Ein-Tages-Intensiv-Training“**
☐ SIP in der Analyse: auf dem Wege zur offenen IP-Telefonie?
☐ Wireless LAN in Produktion und Logistik
☐ Quality of Service
**zum Preis von € 2.190,- zzgl. MwSt.**

☐ **ohne „Ein-Tages-Intensiv-Training“**
**zum Preis von € 1.790,- zzgl. MwSt.**

☐ **mit Report**
„Netzwerkdesign-Wettbewerb 2005“
**zum Preis von nur € 210,- zzgl. MwSt.**

☐ **mit Report**
„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
**zum Preis von nur € 338,- zzgl. MwSt.**

☐ **ohne Report**

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.com**

| | |
|---|---|
| _____ Vorname | _____ Nachname |
| _____ Firma | _____ Abteilung |
| _____ Telefon | _____ Fax |
| _____ Straße | _____ PLZ,Ort |
| _____ eMail | _____ Unterschrift |

# Programmübersicht: Netzwerk-Redesign Froum 2006

## Montag, den 27.03.2006

**9:30 bis 12:00 Uhr**
**Top-Analyse unseres internationalen Labors: Internationale IT-Trends und Auswirkungen auf Netzwerke und Infrastrukturen**
- Neue IT-Architekturen und ihre Anforderungen
- Der Konsumer-Markt und seine Auswirkungen auf Client, Betriebssystem, Software
- Globalisierung und die Konsequenzen für Kommunikations-Architekturen
- Strategien ausgewählter Hersteller: Cisco, IBM, Microsoft, Siemens
- Moderne Technologien in der Trend-Analyse:
  - Speicher • Server/Datacenter
  - Intelligent Networks / Virtualisierung von Ressourcen im Netzwerk
  - IP-Telefonie • Kollaboration: Teamwork im Netzwerk
  - RFID, Architekturen und die Integrations-Aufgabe
  - Logistik-Anwendungen im Netzwerk
  - Aktuelle Netzwerk-Technologien und der Trend
  - Sicherheits-Architekturen für vernetzte Systeme
- Ausblick auf die internationale Entwicklung und die Konsequenzen für den deutschen Markt

*Dr. Jürgen Suppan, ComConsult Research*

**12:00 bis 12:30 Uhr**
**RFID - Ein Blick hinter die Technologie und auf die Anforderungen an das Netzwerk** *Dipl.-Ing. Frank Lange-Lietz, deconis gmbh*

**14:00 bis 15:30 Uhr**
**Wireless-Technologien - wohin geht der Weg? Investitionssicherheit im Wettstreit von IEEE 802.11n und WiMax**
- Aktuelle Wireless-Standards und ihre Vor- und Nachteile
- Konsumer- kontra Enterprise-Markt: wer bestimmt die Produkte
- IEEE 802.11n in der Analyse: Leistung und Grenzen eines neuen Standards
- WiMax: Vorteile der Wireless-Megatechnik
- IEEE 802.11n kontra WiMax: wohin geht der Weg
- Investitionssicherheit mit Wireless-Technologien: was ist zu tun?
- Wireless-Architekturen der Zukunft: die neue Wireless-Hierarchie
- Konsequenzen für die Zukunft: wie Netzwerke in 5 Jahren aussehen können
  - Campus-Design
  - Integration von Servern und Speicher
  - Distribution
  - Desktop-Bereich
- Fazit: Handlungsempfehlungen

*Dr. Franz-Joachim Kauffels, Unternehmensberater*

**16:00 bis 17:30 Uhr**
**Netzwerk-Redesign 2006:**
**Alternativen, Aufwand, Wirtschaftlichkeit**
- Gründe für ein Redesign
- Bewertung bestehender Netzwerke und Designs
- Neue Technologien und ihr Einfluss auf Design-Entscheidungen
- Optimierung von Konvergenz-Zeiten
- Leistungsspektrum moderner Switch-Produkte
- Grundsätzliche Design-Alternativen
- Campus-/Backbone-Design im Umfeld konvergenter Netzwerke
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide in der Nutzbarkeits-Analyse
- Fallbeispiele und Empfehlungen

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**10:30 - 11:00 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:30 - 16:00 Uhr Kaffeepause**
**ab 18:00 Uhr Happy Hour**

## Dienstag, den 28.03.2006

**9:00 bis 10:00 Uhr**
**Configuration Management Data Base CMDB:**
**Optimierung des Konfigurations-Managements von Netzwerken**
- CMDB als Basis zentralisierter Konfigurations-, Sicherheits- und Management-Architekturen
- ITIL und CMDB: vom Leitfaden zur Lösung
- Praktische Anforderungen
- Alternativen zur Umsetzung
- Automatisierung als logische Folge:
  - Spezialthema Automatisierung: Generierung aus einer CMDB
  - Spezialthema Sicherheit: Zugangspflege der Netzwerk-Plattform automatisiert mit Hilfe der CMDB
  - Spezialthema Management: Konfigurationspflege der Management-Plattform auf Basis der CMDB
- Kosten und Betrieb
- Bewertung und Ausblick

*Dipl.-Ing. Christian Roszak, ComConsult Kommunikationstechnik GmbH*

**10:00 bis 10:30 Uhr**
**Standardisierung und Technologie-Entwicklung:**
- Was passiert aktuell bei IEEE, was ist neu, wie relevant ist es?
- Positionen der Hersteller
- Aktuelle Standardisierungs-Arbeiten
  - 802.3an 10GBASE-T • 802.3aq 10GBASE-LRM
  - 802.3as Frame Extension • 802.3at Power oE Plus
  - 802.3ap Backpanel Ethernet
  - 802.3ar Congestion Management • Residential Ethernet
- Einschätzungen und Empfehlungen

*Dipl.-Ing. Thomas Schramm, Hirschmann GmbH*

**11:00 bis 11:45 Uhr**
**Anforderungen an die Netzwerk-Infrastruktur für 10 Gig-Ethernet und für zukünftige Anwendungen**
- Stand der Normierung
- Problematik bei der Umsetzung
- Empfehlungen

*Stefan Ries, Reichle & De-Massari AG*

**11:45 bis 12:30 Uhr**
**WAN-Planung und Optimierung**
- Neue WAN-Verfahren und ihre Bedeutung
- MPLS: Projekterfahrungen
- Applikationen und Datacenter im WAN
- Trends und Ausblick

*Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**14:00 bis 15:30 Uhr**
**Neue Wireless LAN-Technologien in der Analyse:**
**Projekterfahrungen**
- Controller-basierte Architekturen kontra traditionelles Access-Point-Design
- Herausforderung: zentralisierte Konfiguration
- Konsequenzen für das Distributions-System und die WLAN-Sicherheits-Infrastruktur
- Markt- und Produktsituation Wireless-Switching
- Mobilität und Sicherheit: wie aufwendig ist IEEE 802.11i
- Empfehlungen für erfolgreiche und investitionssichere Wireless-Projekte

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**16:00 bis 17:00 Uhr**
**Sicherheit im Netzwerk: Zugriffsschutz auf Benutzerebene**
- Bedrohungsanalyse
- Zugriffsschutz im Netzwerk: alternative Lösungsansätze
- Bestehende Standards und ihre Nutzbarkeit
- Potenziale und Grenzen gruppenbezogener Zugriffsrechte
- Praktische Umsetzung und Einsatzszenarien
- Behandlung von Problem-Geräten
- Prüfung der Patch-Level von Clients: Hersteller-Konzepte in der Bewertung
- Ausblick und Empfehlungen

*Markus Schaub, ComConsult Technologie Information GmbH*

**10:30 - 11:00 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:30 - 16:00 Uhr Kaffeepause**

# Programmübersicht: Netzwerk-Redesign Froum 2006

## Mittwoch, den 29.03.2006

**9:00 bis 10:00 Uhr**
**Projekterfahrungen zur IP-Telefonie**
- Vorgehensweise bei Ausschreibungen
- Applikationen und Sonderanwendungen in einer VoIP-Umgebung
- Voice-Tauglichkeit bestehender Netzwerke
- QoS-Konzeptionierung
- Welche QoS-Architektur ist zu empfehlen
- Integration und Trennung von Sprache und Daten im Netzwerk
- Ergebnisse aktueller Ausschreibungen

*Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**10:00 bis 11:00 Uhr**
**Business-Case IP-Telefonie**
- Typischer Projektablauf: was gehört zum typischen Voice-Projekt, wo liegen Stolpersteine, welcher Zeitablauf ist realistisch
- Traditionelle TK kontra IP-Telefonie: was zeigen aktuelle Projekterfahrungen
- Wirtschaftlichkeit: Ergebnisse aktueller TCO-Berechnungen, typische Amortisationszeiten
- Hosted IP-Telefonie: eine Alternative?
- Markt-Analyse: wo stehen wichtige Hersteller, welche Strategien verfolgen sie, wer ist für die nächsten Jahre am besten aufgestellt
- Sind offene, standardisierte Lösungen realisierbar?
- Zeitlicher Ausblick: was dominiert die nächsten 3 Jahre
- Empfehlungen für die erfolgreiche Projektdurchführung

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**11:30 bis 12:30 Uhr**
**Mobile Kommunikation**
- Anwendungsszenario mobile Kommunikation
- Herausforderung: zentrales Management der mobilen Endgeräte
- Aktuelle Standards: was sie leisten, was sie nicht leisten
- Trends und Ausblick

*Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH*

**14:00 bis 14:45 Uhr**
**Integration von Gefahren- und Meldetechnik in IP-Netzwerke**
- Videoüberwachung im Netzwerk: Trends und Produkte
- Gefahrenmeldetechnik im LAN: Probleme und Lösungen
- Trends und Ausblick

*Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH*

**15:15 bis 16:00 Uhr**
**Intrusion Prevention**

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**11:00 - 11:30 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**14:45 - 15:15 Uhr Kaffeepause**

## Donnerstag, den 30.03.2006 - Ein-Tages-Intensiv-Trainings/Workshops

**BITTE EIN GEWÜNSCHTES THEMA ANKREUZEN!!**

☐ **Intensiv-Training 1:**
**SIP in der Analyse:**
**auf dem Wege zur offenen IP-Telefonie?**
- Was leistet SIP, wie arbeitet es
- Welche Komponenten werden benötigt
- Wie sehen typische Produkte aus
- Ein Alltags-Szenario und seine Umsetzung mit SIP
- Variante 1: die offene Lösung
- Variante 2: SIP und die traditionellen Hersteller
- Ausblick

*Markus Schaub, ComConsult Technologie Information GmbH*

**Intensiv-Training 2:**
☐ **Wireless LAN in Produktion und Logistik**
- Anforderungen
- Wireless-Technologien und ihre Nutzbarkeit
- Roaming-/Handover
- Handhabung mobiler Teilnehmer
- Umsetzung hoher Verfügbarkeit und Redundanz
- Koexistenz und Integration unsicherer Teilnehmer und Teilnehmer alter Standards
- Beispiele und Projekterfahrungen
- Ausblick und Empfehlungen

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**Die Intensiv-Trainings starten alle parallel um 9:00 Uhr.**
**Bitte wählen Sie vorab einen der Intensiv-Trainings aus,**
**damit wir die weitere Organisation planen können. DANKE!**

☐ **Intensiv-Training 3:**
**Quality of Service**
- QoS-Ziele
- QoS-Anforderungen in Lokalen Netzwerken
- QoS-Mechanismen
  - Auf Ethernet-Ebene
  - Auf IP-Ebene
  - Über IP-Ebene
- Konzepte für den LAN-Ausbau im Hinblick auf QoS
  - Access-Bereich
  - Core-Bereich
  - Back-End-Bereich
- Sonderfall: QoS und IP-Telefonie
- Messungen in produktiven Netzwerken
  - Aufbau
  - Ergebnisse
- QoS im WAN
  - Architektur
  - Flankierende Maßnahmen
  - IP-Telefonie im WAN
- QoS im Wireless LAN
  - Einfluss der WLAN-Technologie
  - Kanalzugriff und Handover
  - IP-Telefonie
- Fazit und Empfehlungen

*Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**10:30 - 11:00 Uhr Kaffeepause**
**13:00 - 14:00 Uhr Mittagspause**
**15:30 Ende der Veranstaltung**

Der Veranstalter behält sich Änderungen im Programm vor!

IT-Sicherheits-Kongress

# IT-Sicherheits-Forum 2006

Die Comconsult Akademie veranstaltet vom 08. - 11. Mai das „IT-Sicherheits-Forum 2006“.

Das IT-Sicherheits-Forum 2006 wird auch in diesem Jahr wieder die gerade aktuellen Themen zu Bedrohungsszenarien der IT-Sicherheit und zu den wichtigsten Schutzmaßnahmen aufgreifen. Dabei wird ein äußerst großer Wert auf Praxisnähe gelegt, dies zeigt sich insbesondere bei den technisch orientierten Workshops und den Praxisvorträgen, die direkt anwendbare „Tipps & Tricks“ für den Tagesbetrieb weitergeben. Das Forum hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:

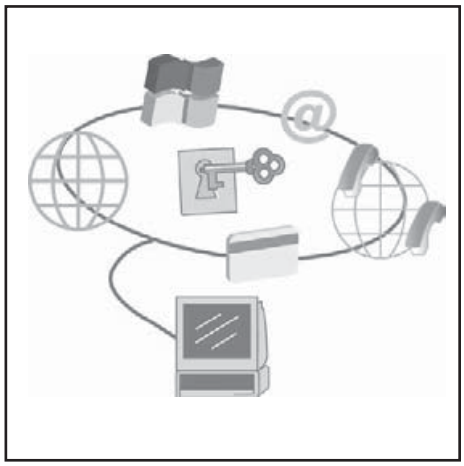
- Erfahrungen aus aktuellen Sicherheitsvorfällen und Aufzeigen absehbarer Trends
- Neue Entwicklungen bei Sicherheitstechnologie und Sicherheitsorganisation
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- Vertiefende Seminare und Tutorien

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2006 sind bisher vorgesehen:

Netzwerk-Redesign unter Sicherheitsaspekten
- Dezentralisierung der Netzgrenzen (deperimeterization)
- Überfällige Segmentierung des internen Netzes
- Identifikation und besonderer Schutz kritischer Systeme
- Anpassung von Identitäten, Zugriffskontrollen und Alarmierung

Gefahren durch zunehmende Kriminalisierung des Internets
- Industriespionage durch gezielte Spyware-Angriffe
- Massenattacken mit Phishing und Pharming
- Erpressungsversuche mit DDoS-Attacken



- Möglichkeiten des Identitätsdiebstahls

Application Security
- Neuartige Angriffe auf Webapplikationen
- Absehbares Gefahrenpotenzial bei Web-Services
- Sicherheit des SAP Enterprise Portals
- Schwachstellen bei Oracle DB

Best Practice Sessions (Praxistipps für typische Problembereiche)
- Sichere Konfiguration von Webbrowser und Webserver
- Aufbau einer sicheren Abwehr von Malware / Spyware
- Aufbau einer sicheren Adminumgebung
- Vorkehrungen für den sicheren Betrieb von mobilen Devices

Weiterhin sind folgende Themen vorgesehen:

Sicherheit bei Voice-over-IP
- Verwendete Technologien (SIP, H.323, proprietäre Protokolle)
- Schwachstellen und mögliche Angriffsszenarien
- Auswirkungen der Sicherheitsinfrastruktur auf die QoS bei VOIP
- Technische und organisatorische Schutzmaßnahmen

Sichere Nutzung von BlackBerry
- Analyse und Bewertung der Sicherheitsarchitektur
- Schutz der Übertragung, der Daten im Smartphone und des Mail-Servers
- Vorstellung zusätzlicher Schutzmaßnahmen
- Empfehlungen zum Einsatz von BlackBerry im Unternehmen

Schutz kritischer Infrastrukturen
- Ausfälle im Zusammenhang mit Fehlfunktionen der Informationstechnik
- Bedrohungen von SCADA-Systemen (Supervisory Control and Data Acquisition)
- BSI und seine Hilfsmittel zu KRITIS (Richtlinien, Sicherheitscheck)
- Grenzen der Zuständigkeit zwischen Unternehmen und Politik

Security Management
- Problem der fehlenden Sicherheitsstandards
- Lösungen zum Security Information Management (SIM)
- Event-Aggregation und Event-Correlation
- Probleme von SIM-Tools in stark heterogenen Netzen

Business Continuity Management
- Sicherung kritische Geschäftsprozesse bei Störungen oder Notfällen
- Best Practice Prozesse nach ITIL, BCI und DRII
- Vorgehensmodell: BIA, Strategie, Implementierung, Pläne, Tests
- Empfehlungen zum Tooleinsatz

Compliance / Risk Management
- Berücksichtigung staatlicher, industrieller und rechtlicher Vorgaben
- Informationssicherheit und Management von IT-Risiken
- Einschätzung der RM-Ansätze von BSI, ISO 17799 und IOS 13335
- Aufbau, Monitoring und Audit bei RM

Security Awareness und Governance
- Einbeziehung der IT-Prozesse in das interne Kontrollsystem
- Bekanntmachung und Durchsetzung einer SecPol im Konzernumfeld
- Durchführung einer Security Awareness-Kampagne

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat einen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier aller Erfahrung nach immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

IT-Sicherheits-Kongress

# 10% Frühbucherrabatt bis 15.02.06

## IT-Sicherheits-Forum 2006
### 08.05. - 11.05.06 in Bad Neuenahr

**4 Tage IT-Sicherheits-Forum 2006 mit „Tutorium“**
**zum Preis bei Buchung bis 15.02.06 von € 1.990,-**
**statt regulär € 2.190,- zzg. MwSt.**

**3 Tage IT-Sicherheits-Forum 2006 ohne „Tutorium“**
**zum Preis bei Buchung bis 15.02.06 von € 1.590,-**
**statt regulär € 1.790,- zzg. MwSt.**

**Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.**

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung
# IT-Sicherheits-Forum 2006

Ich buche den Kongress
**IT-Sicherheits-Forum 2006**
vom 08.05. - 11.05.06 in Bad Neuenahr

☐ **mit Tutorium am ersten Tag**
**zum Preis von nur € 1.990,- zzgl. MwSt.***

☐ **ohne Tutorium am ersten Tag**
**zum Preis von nur € 1.590,- zzgl. MwSt.***
***gültig bis 15.02.06**

☐ **mit Report**
„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
**zum Preis von nur € 338,- zzgl. MwSt.**

☐ **ohne Report**

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____bis_____06

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.com**

_____ Vorname

_____ Nachname

_____ Firma

_____ Abteilung

_____ Telefon

_____ Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

# Trennung von Benutzergruppen - Lösungen und ihre Folgen

Fortsetzung von Seite 1

Markus Schaub ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbreiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuster Hard- und Software aus dem Netzwerkumfeld.
Insbesondere verfügt er über langjährige Betriebs- und Praxiserfahrung mit CISCO-Routern und CISCO-Switch-Systemen. Er ist ComConsult Certified Network Engineer zertifiziert. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.

Im Folgenden werden verschiedene Lösungsansätze für eine Standortumgebung diskutiert, wie Sicherheitszonen voneinander getrennt werden können. Besonderes Augenmerk wird dabei auf die heute von vielen Herstellern angepriesene Möglichkeit gelegt, einzelnen Benutzern oder Benutzergruppen nach der Anmeldung am Netzwerk besondere Nutzungsrechte zuzuweisen. Es werden drei unterschiedliche Herstellerlösungen vorgestellt und auf ihre Vor- und Nachteile hin untersucht. Zunächst werden jedoch die generellen Designmöglichkeiten beschrieben.

### Designalternativen

Um Bereiche mit unterschiedlichen Sicherheitsanforderungen voneinander abtrennen zu können, gibt es verschiedene Ansätze, die im Folgenden näher betrachtet werden:

### Physikalische Trennung der Netzbereiche

Um verschiedene Benutzer und Bereiche voneinander zu trennen, gibt es eine Reihe von Möglichkeiten. Die extremste Form ist die physikalische Trennung der Welten voneinander: für jedes Netz werden dabei eigene Kabel und eigene Hardwarekomponenten eingesetzt (vgl. Abb. 1). Eine Kopplung der verschiedenen Sicherheitsbereiche erfolgt höchstens über dedizierte Firewalls. Gerade bei hohen Sicherheitsanforderungen bietet sich diese Variante an, beispielsweise für die Abtrennung des Produktionsnetzes oder der WLANs.

Unternehmen, die sich für ein solches Vorgehen entscheiden, tun dies für gewöhnlich in der Hoffnung, dadurch ein maximales Sicherheitsniveau zu erreichen: Fehler oder Viren im Bürobereich können nicht über das interne Netzwerk auf den Produktionsbereich übergreifen und der sprichwörtliche Hacker auf dem Parkplatz kann über das WLAN auch mit noch so guten Hackertools keinen Zugriff auf die Server erlangen.

Ein weiterer Vorteil ist die Übersichtlichkeit, die durch die klare Trennung entsteht: kein Pflegen ewig langer Listen, welcher Port auf welchem Switch warum welchem VLAN zugeordnet wurde, welches VLAN wo getrunkt ist und welche Funktion erfüllt, warum welcher Paketfilter welcher Usergruppe zugeordnet wurde und was sich hinter den IP Adressen verbirgt, etc.

Und ein dritter positiver Aspekt kann - bei entsprechendem Design des Backbones - der sein, dass man auf diese Weise auf Gebäude-übergreifende VLAN verzichten kann, wie sie für ein WLAN Handover in der Regel notwendig sind, da für die WLANs ein eigenes Backbone existiert. Somit kann das Büro-Backbone ausnahmslos als Layer 3 Backbone betrieben werden, was zum einen wiederum die Übersichtlichkeit erhöht und im Fehlerfall ein Troubleshooting erheblich vereinfacht, zum anderen können die Vorteile der Layer 3 Verfahren vollständig ausgespielt werden.

Nachteil dieser Vorgehensweise sind die höheren Kosten: physikalisch getrennte Netze bedeutet eben auch physikalisch getrennte Netzwerkkomponenten. Wenn beispielsweise nur wenige Access-Points auf einer Etage benötigt werden, kann man sich schon die Frage stellen, ob so viele ungenutzte Ports an dem Access-Switch, an dem die APs angeschlossen werden, nicht eine Verschwendung darstellen. Auch muss man zwei Backbones betreiben, wenn man das Konzept ganz durchziehen will.

Ein weiterer Nachteil ist, dass auf diese Weise zwar Sicherheitszonen verwirklicht werden können, wie die bereits genannten Beispiele LAN, WLAN und Produktionsbereich, es jedoch kaum hand zu haben ist, das Konzept auch „im Kleinen“ durchzuhalten, beispielsweise um verschiedene Abteilungen voneinander zu trennen.

### Trennung mittels VLANs

Eine kostentechnisch günstigere Möglichkeit ist es, die vorhandene Infrastruktur zu nutzen und die Bereiche virtuell mittels VLANs voneinander zu trennen (vgl. Abbildung 2). Hierbei werden die Sicherheitsbereiche auf VLANs abgebildet: bspw. können einzelne Etagen, Access Switches einen Sicherheitsbereich bilden, die WLANs bekommen ein eigenes, womöglich Gelände-übergreifendes VLAN und auch die Produktion bekommt eigene. Die Kopplung der VLANS kann, wie in Abbildung 2, durch Layer 3 Komponenten erfolgen und ggf. durch den Einsatz von Paketfiltern beschränkt werden, oder - bei höheren Anforderungen an die Sicherheit - durch Firewalls, analog zum Beispiel der physikalisch getrennten Netze.

Neben der Einsparung von zusätzlichen Hardware- und Verkabelungskosten gegenüber der physikalischen Trennung bietet diese Variante auch den Vorteil, dass sie einfach auf kleinere Bereiche ausgedehnt werden kann, wie beispielsweise Abteilungen oder unterschiedliche Produktionsstraßen.

Der vielleicht offensichtlichste Nachteil ist, dass diese Lösung schnell sehr unübersichtlich werden kann. Ohne eine gute Dokumentation der eingesetzten VLANs wird ein Betreiber schon bei wenigen VLANs schnell den Überblick verlieren. Insbesondere beim Troubleshooting kann das schnell zum Verhängnis werden.

Ein Nachteil aus Sicht der Sicherheit bildet die gemeinsam genutzte Hardware: ein

Angriff aus dem WLAN auf einen Access-Switch hat somit auch Auswirkungen auf die kabelgebundenen Netze. Und ein Fehler, wie beispielsweise ein Broadcaststurm oder ein fehlerhaft konfigurierter Spanning Tree, wirkt sich gleich auf alle Bereiche aus.

Zudem kann das Geländebackbone nicht mehr ausschließlich mittels Layer 3 betrieben werden, will man bspw. ein Handover für Mobiltelefone ermöglichen.

**Zugriffsrechte pro Benutzer**

Ist die physikalische Trennung das Extrem in Richtung Entkopplung der Netzebereiche, so bilden die heute vielfach propagierten, userbezogenen Zugriffsrechte das Extrem in Richtung Individualisierung und Konfigurationsaufwand.

Bei diesem Verfahren wird einem Switchport nach Anmeldung des Users/Clients über IEEE 802.1X ein Regelwerk mitgegeben, in dem definiert ist, welche Zugriffsrechte der User/Client besitzt. Im einfachsten Fall kann dies bedeuten, dass der Port einem VLAN zugeordnet wird, im schlimmsten Fall gibt es eine user-/clientbezogene Access-Liste, die genau regelt, was der Nutzer darf, und was nicht. Im Grunde handelt es sich hierbei nicht um eine weitere Designalternative zur physikalischen und virtuellen Trennung, sondern nur um eine besondere Spielart des virtuellen Konzepts, da sich der Aufbau des Netzes im Vergleich dazu nicht ändert, sondern nur die Methode, wie ein VLAN einem Port zugewiesen wird.

Die verschiedenen Lösungen, die heute auf dem Markt existieren, werden später noch im Einzelnen vorgestellt.

**Mischkonzept**

Betrachtet man die Vor- und Nachteile der virtuellen und der physikalischen Trennung, so scheinen beide zunächst in einem diametralen Widerspruch zu stehen. Jedoch ist es durchaus möglich, die beiden Lösungen miteinander zu verheiraten. Wie dies im Einzelnen aussieht, ist natürlich von den individuellen Anforderungen abhängig, jedoch kann das generelle Vorgehen dazu hier kurz vorgestellt werden:

Die Bereiche mit hohen Sicherheitsanforderungen werden physikalisch vom Rest des Netzes abgetrennt. Dies könnten zum Beispiel die Bereiche Produktion und WLAN sein. Es entstehen also drei physikalische Netze. Diese können intern nun wieder mit VLANs getrennt werden, wenn dies erforderlich ist. Im Büronetz werden beispielsweise die Etagen gegeneinander getrennt oder Abteilungen werden voneinander durch VLANs abgegrenzt.

Wenn man will, kann man jetzt sogar noch einen Schritt weiter gehen und für

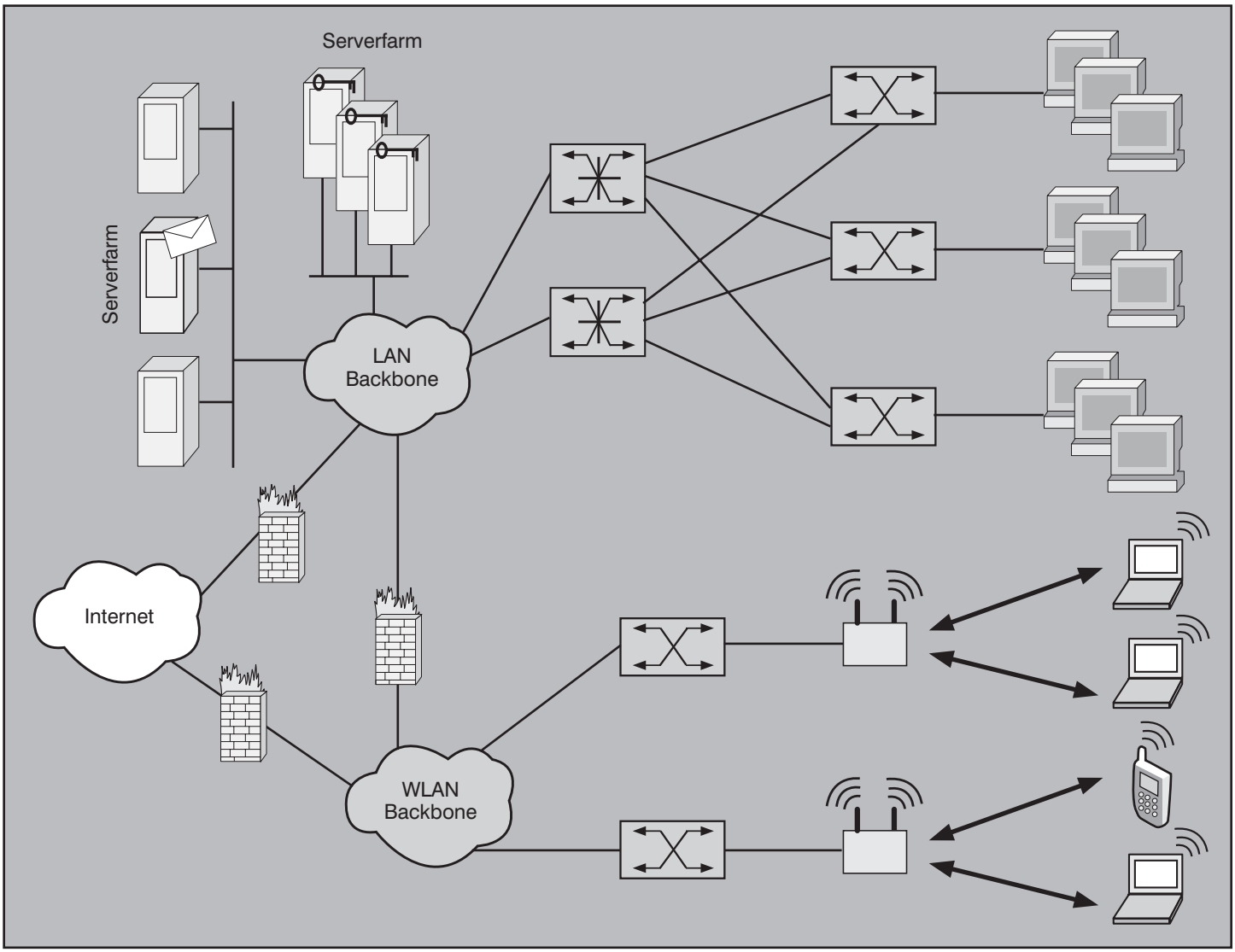



Abbildung 1: Physikalische Trennung der Sicherheitsbereiche

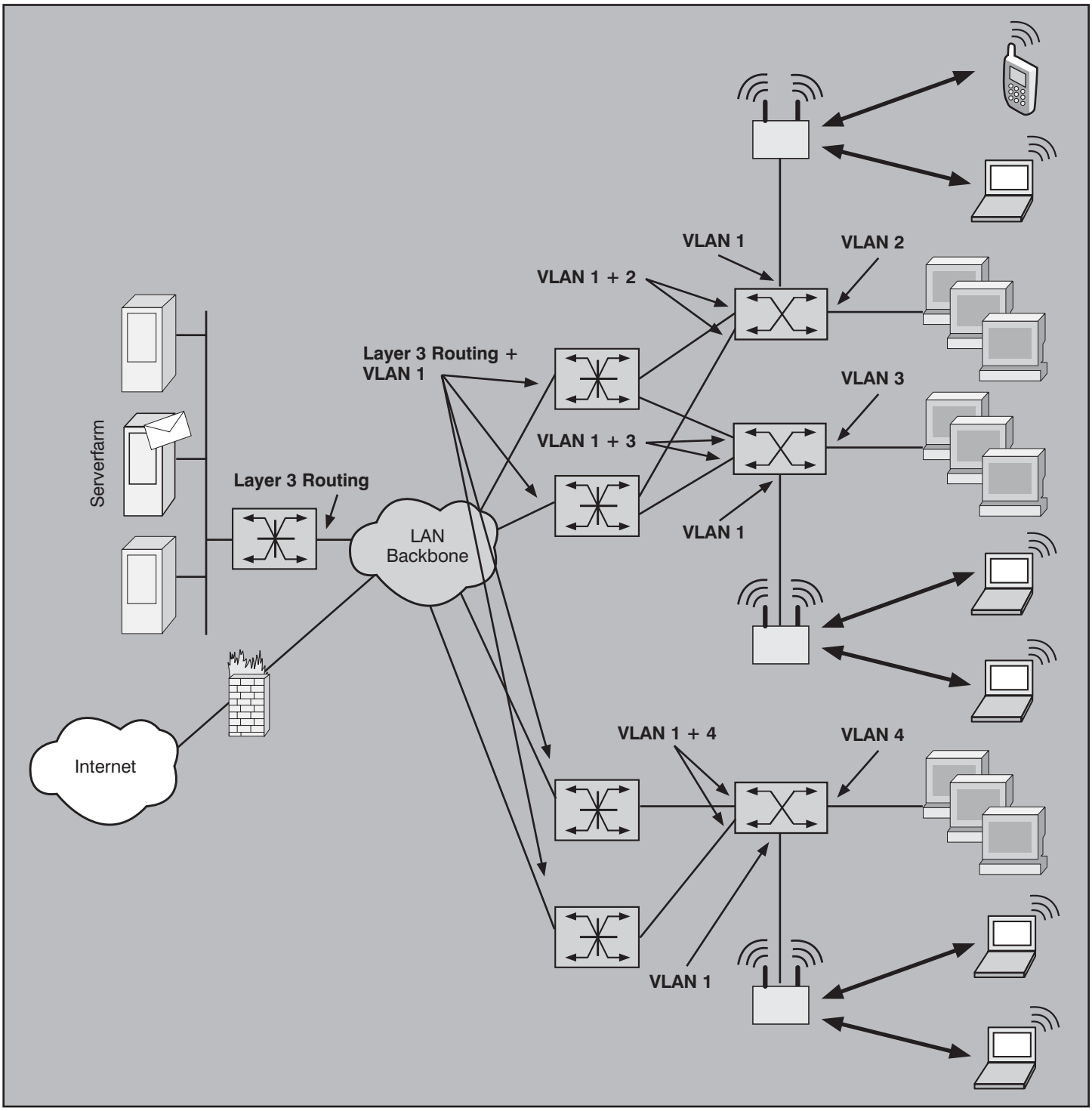



Abbildung 2: Virtuelle Trennung durch VLAN

bestimmte Bereiche userbezogene Zugriffsrechte definieren, beispielsweise im WLAN, um Gastzugänge für Gäste und externe Berater zu ermöglichen.

Vorteil von Mischkonzepten ist, dass es möglich ist, das Design auf die eigenen Sicherheitsbedürfnisse hin zu optimieren.

Der große Nachteil hingegen ist, dass sich fast alle Nachteile der zuvor vorgestellten Lösungen aufsummieren: die Kosten für getrennte Netze müssen getragen werden; innerhalb der Sicherheitsbereiche hat man mit den Problemen zu kämpfen, die VLANs mit sich bringen; das Troubleshooting kann äußerst komplex werden; ohne eine ausgezeichnete Dokumentation durchblickt man als Betreiber das eigene Konstrukt schon nach kürzester Zeit nicht mehr.

**Fazit: Designalternativen**

Jeder der vorgestellten Lösungen bringt ihre eigenen Vor- und Nachteile mit sich. Wie so häufig existiert kein allgemeingültiges Konzept, das sich immer anwenden

lassen würde. Für welche Variante man auch immer sich entscheiden mag, sollte man darauf achten, dass neben den Kosten und den Sicherheitsanforderungen auch der Betrieb berücksichtigt wird. Behält man nur die Sicherheitsaspekte im Auge oder begibt man sich gar auf den Pfad des Einsatzes aller technischen Möglichkeiten, kann der Schuss nach hinten los gehen: eine Konfiguration, die man nicht mehr überblickt, kann sehr schnell selbst zu einen Sicherheitsrisiko werden; sei es, weil unbeabsichtigt durch fehlerhafte Konfiguration Löcher in der Sicherheit existieren, oder sei es, dass der Versuch der Behebung eines Fehlerfalles durch die Komplexität der Lösungen zu einem Katastrophenfall wird.

**Grundkonzept: individualisierte Zugriffsrechte**

Wie bereits angesprochen, kam mit der Einführung von IEEE 802.1X schnell die Idee auf, die Userkennung zu benutzen, um die Zugriffsrechte zu individualisieren.

Dazu haben die Hersteller eigene Ansätze entwickelt, die im Folgenden vorgestellt werden:

Wie auch immer man das Verfahren nennen möchte, ob INA (Intelligent Network Access, Extreme), UPN (User Personalized Network, Enterasys), NAC (Network Admission Control, Cisco) oder sonstwie, bestimmte Grundzüge sind allen Verfahren gleich. Insbesondere im Endergebnis unterscheiden sie sich nicht mehr.

Schematisiert kann der Ablauf in allen Fällen wie folgt dargestellt werden:

1. User/Client meldet sich an der Netzwerkkomponente an und gibt dabei seine Identität preis, genutzt wird dazu IEEE 802.1X.

2. Die Zugangskomponente (Switch, WLAN-Access-Point) übermittelt die Zugangsdaten an einen RADIUS-Server zu Überprüfung.

3. Der RADIUS-Server überprüft die Zugangsdaten und sendet ein Accept oder Reject an die Zugangskomponente.

4. Bei einem Accept wird gemäß der Identität des Users/Clients für den Zugangsport eine Sicherheits-Policy aktiviert und der Zugang gewährt.

Die Unterschiede zwischen den in der Praxis existenten Lösungen ergeben sich aufgrund des vierten Schritts, der Zuweisung der Sicherheits-Policies. Hier gibt es zum einen unterschiedliche, propietäre Verfahren, wie die Policies auf die Zugangskomponente übertragen werden, zum anderen wird die Art der Policy von den Möglichkeiten der Zugangskomponente selbst bestimmt. Die unterschiedlichen Verfahren der Zuweisung werden im Folgenden noch detailliert erläutert.

Arten von Zugangspolicies sind aktuell zwei verbreitet:

1. Trennung auf Layer 2:
   Zuweisung eines VLAN/SSID
   Nach der Anmeldung wird dem Port ein VLAN zugewiesen. Eine weitere Filterung kann dann auf Basis der VLAN-ID durch Layer-3 Komponenten erfolgen. Im WLAN Bereich wird der Client nur zugelassen, wenn er sich zu einer bestimmten SSID assoziiert, andernfalls wird er abgelehnt. Die SSID kann dann durch den Access Point wiederum auf ein VLAN im kabelgebundenen Netz abgebildet werden.

2. Trennung auf Layer 3:
   Zuweisung einer Access-Liste
   Ist der Zugangsswitch Layer-3-fähig, kann anstatt mit einer reinen VLAN Zuweisung auch mit einer Layer-3-Access-Liste gearbeitet werden (vgl. Abbildung 3).

Das zweite Verfahren erhöht zwar die Flexibilität, da nicht mit verschiedenen VLANs gearbeitet wird, innerhalb derer alle User dieselben Rechte haben, sondern individuelle Regeln definiert werden können. Die Kosten aber, die man dafür zahlen muss, sind jedoch erheblich: hoher administrativer Aufwand, schnell unübersichtlich, höhere Kosten für Layer-3-fähige Access-Switches oder der „Schutz“ setzt erst am ersten Layer 3 Switch ein, an dem sich der User authentifiziert anstatt am Access-Switch. Grundsätzlich kann dies auch ein zentraler Switch wie der Gebäudezugangsswitch sein. Jedoch können dann alle Geräte, die vor demselben 1X-fähigen Switch angeschaltet sind, auch ohne sich anzumelden wechselseitig miteinander kommunizieren. Insbesondere Man-In-The-Middle Attacken auf Basis von DHCP oder ARP-Poisoning sind somit innerhalb dieser Bereiche auch durch Nutzer möglich, die keine Zugriffsberechtigungen haben.

Trotz der Nachteile wird das Konzept der Benutzertrennung zurzeit von einigen Herstellern stark propagiert. Aus diesem Grund werden später drei unterschiedliche Ansätze von Herstellern vorgestellt, wie die user-bezogenen Policies gepflegt und auf den Switch übertragen werden.

**Anforderungen an ein userbasiertes Zugangsverfahren**

- Zentrale Authentifizierung
  Die Einführung eines weiteren Servers, auf dem Authentifizierungsdaten gepflegt werden müssen, ist wenig prak-

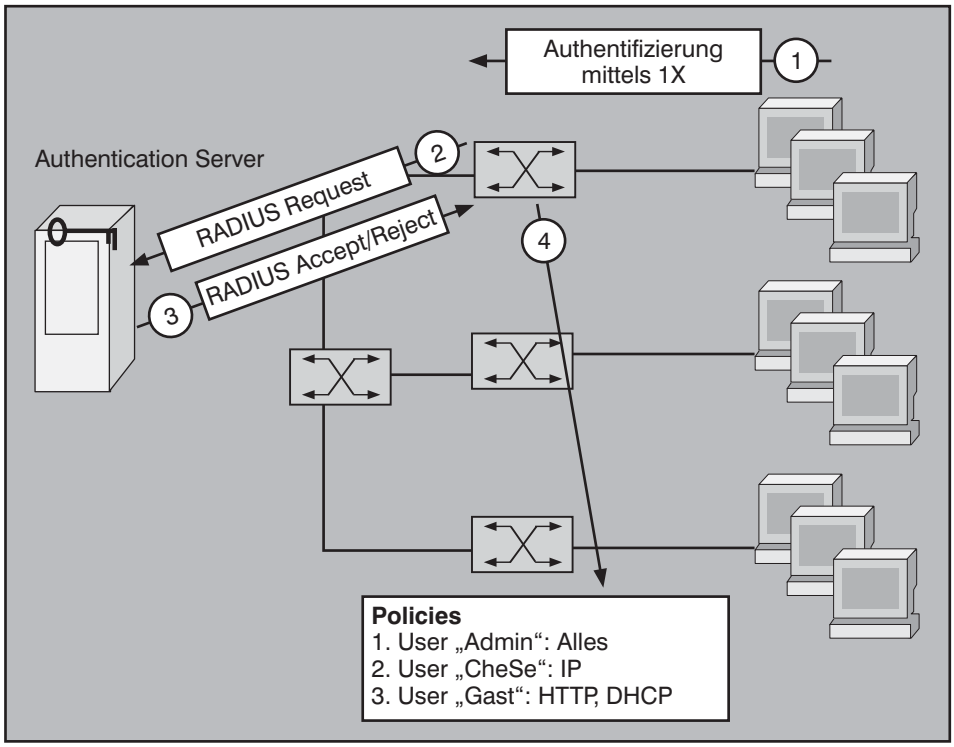



Abbildung 3: Schematischer Ablauf der Benutzertrennung

tikabel. Jegliche Lösung muss somit zumindest eine Schnittstelle für die Überprüfung der Daten gegen ein bereits bestehendes Authentifizierungssystem wie LDAP oder Active Directory (AD) zulassen.

- Unterscheidung des Zugangs
  Dem Authentifizierungs-Server muss es möglich sein, die Art des Zugangs (WLAN, Switch, Firewall, VPN-Gateway…) und den Zugangspunkt (Standort, Gebäude, Etage…) mit dem User, der sich anmelden will, zu korrelieren, bevor er eine Entscheidung trifft.

  Nicht jeder, der sich gültig an einem Netzwerk anmelden darf, darf das auf jede nur denkbare Art und Weise. Eine Sekretärin mit einem festen PC-Arbeitsplatz hat keinen Bedarf an einem WLAN-Access und noch weniger an einem WAN-Zugriff über VPN. Wohingegen im selben Unternehmen einem Vertriebsmitarbeiter durchaus Zugriff über VPN gewährt werden muss.

  Häufig spielt die Zugangsart auch für die Art der Authentifizierung eine Rolle: meldet sich ein Mitarbeiter beispielsweise über WLAN an, so ist für die Authentifizierung mittels 802.1X ein Maschinenzertifikat gewünscht, wohingegen die Anmeldung über VPN durch ein Einmalpasswort abgesichert wird.

  Auch kann die anschließende Policy von dem Zugangsweg abhängen: kann ein WLAN-Access-Point beispielsweise dem User nur in ein bestimmtes VLAN zuweisen, so ist es bei einem VPN-Gateway möglich mit Layer-3-Paketfiltern oder gar mit Proxies zu arbeiten.

- Gruppenberechtigungen
  Eine Konfiguration, die ausschließlich auf User-bezogene Profile setzt, ist schon bei kleinen Unternehmen nicht mehr handhabbar. Zu schnell verliert man den Überblick in einer Unzahl von Regel- und Filterwerken. Wenn man jetzt noch bedenkt, dass neben den einzelnen Usern auch noch die verschiedenen Zugangswege hinzukommen, so multipliziert die Anzahl der Profile schnell ins Unüberschaubare.

  Damit das Ganze überhaupt zu managen ist, muss eine Lösung so ausgelegt sein, dass vernünftige und übersichtliche Abstraktionen möglich sind. Wie Abbildung 4 zeigt kann aber auch ein solches Konzept schnell unübersichtlich werden. Ohne ein gut geplantes und sauber dokumentiertes Konzept ist auch diese Art von Lösung schnell nicht mehr zu verwalten.

**Wünschenswert**

- User- versus Maschinenauthentifizierung

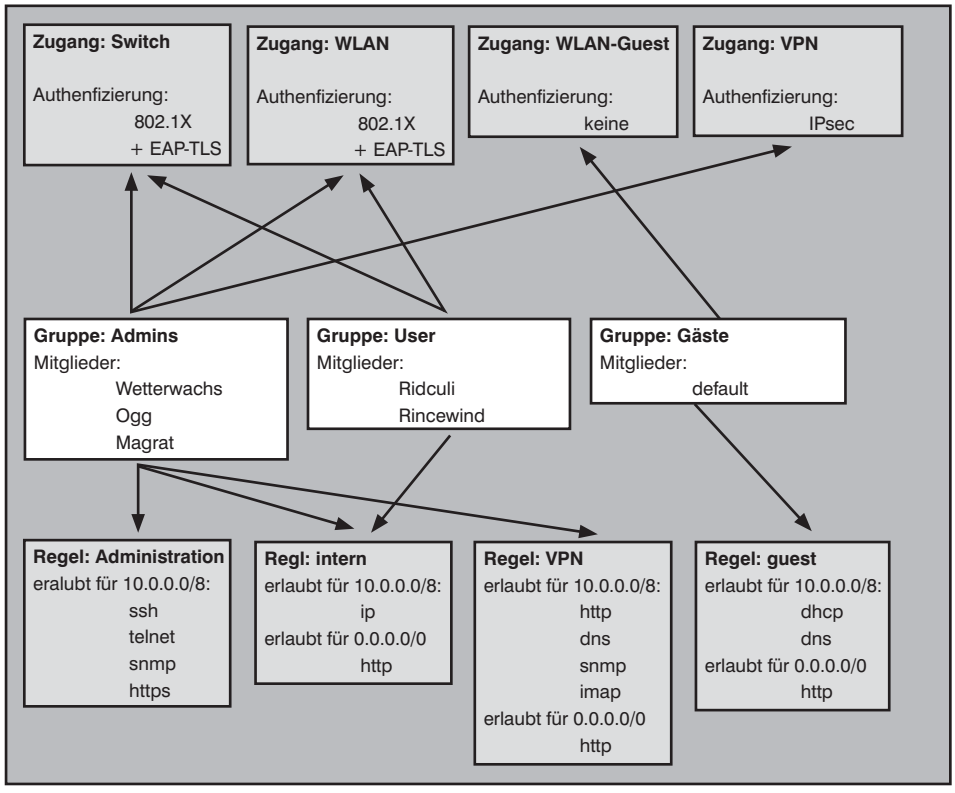



Abbildung 4: Beispiel eines gruppenbasierten Regelwerkes

Eine weitere Authentifizierung beim allmorgendlichen Anmelden werden die User wohl kaum akzeptieren. Soll heißen, die Authentifizierung gegen den Switch/Access-Point muss für den Benutzer transparent sein und nicht zu einer weiteren Authentifizierung führen, also erst am Switch und anschließend an der Domäne. Das Problem, das es dabei zu lösen gilt, ist, dass eine Domänenanmeldung erst möglich ist, wenn die Anmeldung am Switch bereits erfolgreich war, da erst nach der Freischaltung des Ports die IP-Konnektivität hergestellt werden kann. Nach einigen Experimenten mit verschiedenen Möglichkeiten von Seiten der Hersteller hat sich eine zertifikatsbasierte Maschinenauthentifizierung als aktuell gängigste Lösung durchgesetzt. Dabei authentifiziert sich das Gerät gegen den Netzzugangspunkt anhand eines Zertifikates.

Vorteil dieses Vorgehens ist, dass es problemlos so implementiert werden kann, dass ein reibungsloser Ablauf garantiert werden kann: erst meldet sich die Maschine am Switch an, der Port wird freigeschaltet und anschließend läuft der Bootvorgang mit DHCP und Domänenanmeldung wie gewohnt ab.

Der große Nachteil dabei ist, dass so nur überprüft wird, ob das Gerät zugangsberechtigt ist, nicht, ob der Benutzer davor auch wirklich auf das Netz zugreifen darf.

Alternativen zu diesem Vorgehen sind beispielsweise Smartcards, auf denen das benötigte Zertifikat dem PC über eine personengebundene Karte zur Verfügung gestellt wird. Eine weitere Möglichkeit ist die Änderung des Bootablaufs, indem erst die Anmeldemaske erscheint und die Userdaten abgefragt werden, bevor der Bootvorgang mit der IP Konfiguration bis zum Ende abläuft.

- Sicherstellung des Patchlevels
  Einige Hersteller werben damit, dass vor dem Zugang zum Netzwerk nicht nur die Authentifizierung überprüft, sondern auch sichergestellt wird, dass das sich anmeldende System ein „Mindest-Patch-Level“ besitzt. Dazu werden bei der Anmeldung zusätzlich die Release-Stände von sicherheitsrelevanter Software wie Betriebsystem und Virenscanner mit an den Switch übertragen. Ist das System in einem zu alten Zustand, wird es zunächst in eine Art Quarantäne gesteckt, d.h. es befindet sich in einem VLAN, in dem es zunächst keine Zugriffe auf weitere Netzwerkdienste

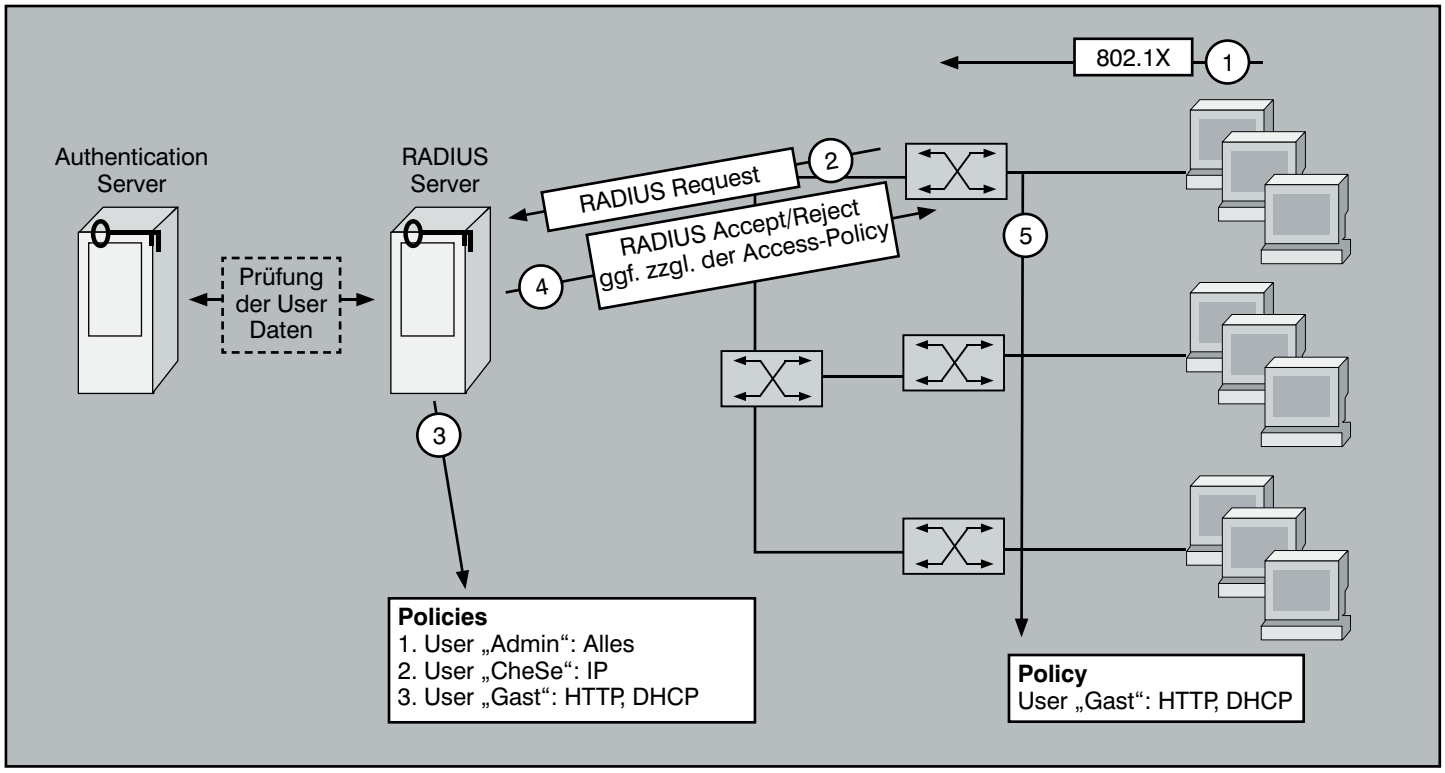



Abbildung 5: RADIUS-Server als zentrale Schnittstelle

hat, außer denen, die notwendig sind, die notwendigen Patches zu installieren. Anschließend muss sich der Benutzer neu anmelden.

**RADIUS-Server als zentrale Schaltstelle (NAC, Cisco)**

Die erste Möglichkeit Policies zu pflegen, ist dies zentral auf einem RADIUS-Server zu tun. Cisco geht beispielsweise mit seinem Access Control Server (ACS) diesen Weg.

Abbildung 5 zeigt schematisch das Vorgehen: im ersten Schritt meldet sich der Client über 1X an und übermittelt seine Zugangsdaten. Diese werden mittels RADIUS zum Server zur Prüfung weitergeleitet. Die Überprüfung der Daten selbst kann mittels eines weiteren Servers erfolgen, beispielsweise durch ein Active Directory. Ein doppeltes Pflegen der Authentifizierungsdaten ist somit nicht erforderlich. Kommt der Authentication-Server zu dem Schluss, dass der Client/User berechtigt ist, auf das Netz zuzugreifen, sendet er dem Zugangspunkt (e.g. dem Switch) ein Accept. In dem Accept steht die Policy, die für den User genutzt werden soll. Der Switch ordnet diese Policy nun dem Zugangsport des Clients zu.

Die Besonderheit dieser Vorgehensweise ist, dass die komplette Policy auf dem Authentication Server vorliegt und komplett an den Switch übertragen wird. Handelt es sich bei dem Switch beispielsweise um einen Layer 3 fähigen Access-Switch, so kann eine vollständige Access-Liste übertragen werden. Bei einem reinen Layer 2 Gerät würde man hingegen eine VLAN-ID übermitteln.

Da Access-Listen keine Standard-RADIUS-Parameter sind, nutzt Cisco die für solche

Fälle vorgesehenen Vendor-Extensions von RADIUS. Das bedeutet, dass generell jeder RADIUS-Server genutzt werden kann, der es erlaubt, Vendor-Extensions frei einzupflegen, was aktuell für die gängigen Server durchaus gilt.

Ist der RADIUS-Server nicht erreichbar, so können User/Clients sich nicht anmelden. Darum gilt - wie generell für den Einsatz von RADIUS -, dass der Server hochverfügbar sein muss und vorzugsweise redundant ausgelegt wird. Auch sollte man darauf achten, dass redundante Server nicht über denselben Weg durch das Netzwerk erreicht werden.

Pro
- Da für den Einsatz von 802.1X generell ein Authentication Server notwendig ist, wird für dieses Szenario keine zusätzliche Hard- oder Software benötigt.

- Da die verschiedenen Policies nicht in der Konfiguration abgelegt werden müssen, verbrauchen Sie auch keinen Speicherplatz im Konfigurations-Flash der Systeme. Da es sich unter Umständen um sehr viele oder sehr komplexe Regelwerke handeln kann, ist die Speichereinsparung mitunter erheblich.

Contra
- Generell kann zwar „jeder“ RADIUS-Server genutzt werden, die Anpassung der Regeln wird dann jedoch erstens sehr unübersichtlich und zweitens sehr kryptisch. Der hauseigene ACS hingegen ist so angepasst worden, dass er die eigenen Erweiterungen kennt und ihre Konfiguration vereinfacht wird. Deshalb wird sein Einsatz von Cisco auch dringend empfohlen.

### Offline Konfiguration von Benutzerrollen (UPN, Enterasys)

Einen anderen Weg geht die Firma Enterasys bei ihrem UPN, wie in Abbildung 6 dargestellt. Auch bei dieser Vorgehensweise meldet sich der Client via 1X bei dem Netzwerkzugang an und der leitet die Daten zur Überprüfung an einen Authentication Server. Dieser prüft die Daten und sendet ein Accept oder Reject an den Netzwerkzugang zurück. Im Falle eines Accepts wird ein weiterer Parameter übertragen: die Gruppenzugehörigkeit. Die Gruppe ist, anders als die Access-Liste bei Cisco, ein Standardparameter des RADIUS-Protokolles; Enterasys hat bewusst auf den Einsatz von proprietären Erweiterungen verzichtet.

Die Besonderheit dieser Lösung ist es, dass sämtliche Policies dem Switch bereits im Vorfeld bekannt sind und nicht online bei der Anmeldung vom Authentication Server übertragen werden müssen. Jeder Benutzergruppe wird eindeutig genau eine Regel zugeordnet, so dass der Switch nach dem Empfang eines Accepts anhand der übermittelten Gruppe die Regel dem entsprechenden Port zuordnen kann.

Zur Erstellung des Regelwerkes gibt es zwei Vorgehensweisen: erstens kann es mittels Konsole (CLI) in althergebrachter Weise erstellt und als Teil der Konfiguration abgespeichert werden. Zweitens gibt es einen Policy Server, auf dem die Policies mittels einer grafischen Oberfläche erstellt und auf alle notwendigen Komponenten übertragen werden können. Letztere Möglichkeit wird schnell zur Pflicht, da es sehr mühselig und fehleranfällig ist, einen größeren Satz von Filterregeln auf vie-

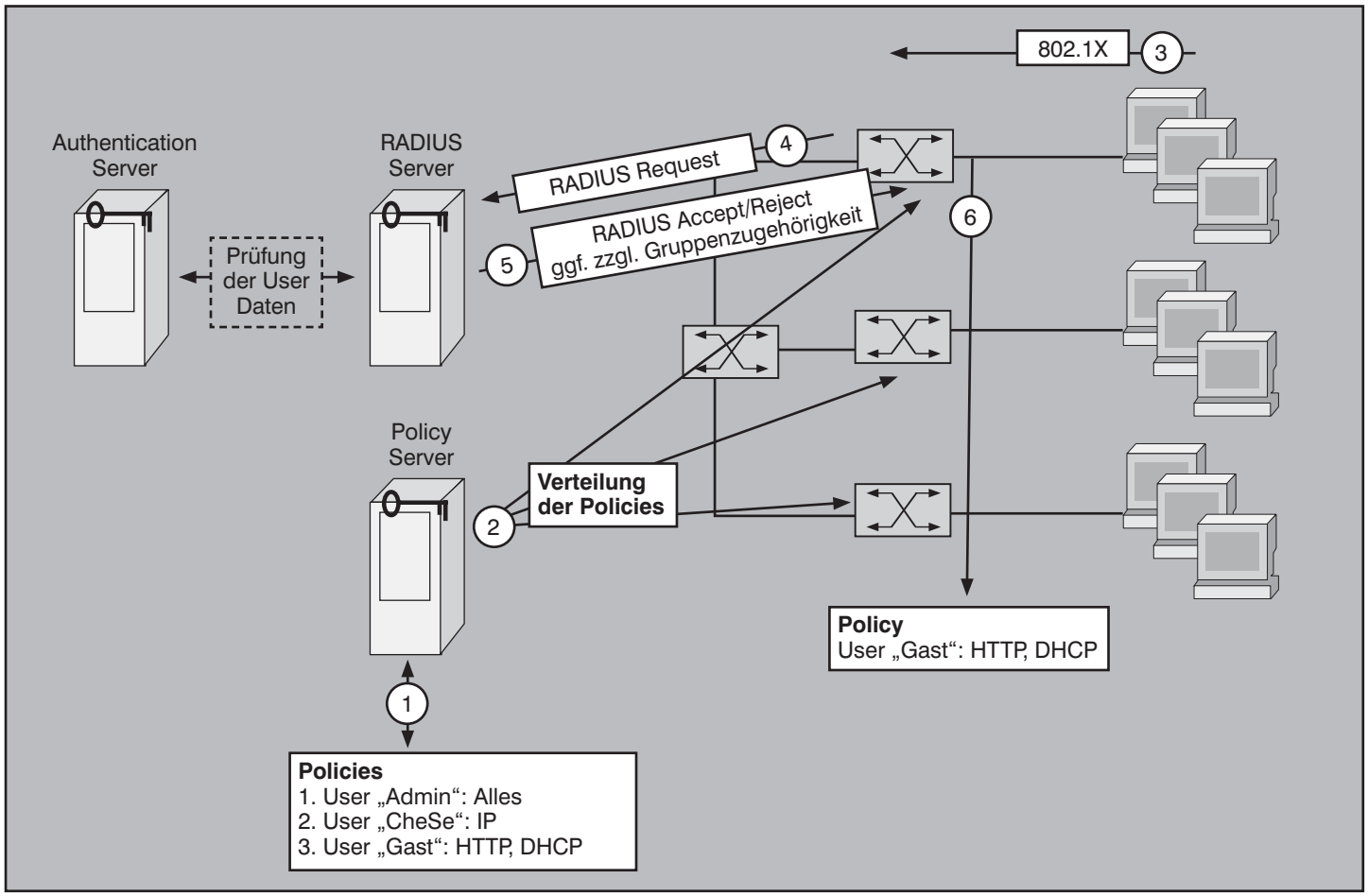



Abbildung 6: Offline Zuweisung der Benutzerrollen

len Geräten identisch zu halten. Der Policy Server ist jedoch nichts anderes als ein grafisches Tool, das dazu dient, die Regeln zu erstellen und zu verteilen. Anschließend werden sie von den Netzwerkkomponenten in die Konfiguration übernommen und ebenso behandelt, als wären sie manuell eingegeben worden.

Pro
- Da auf komplexe Erweiterungen des RADIUS-Protokolles verzichtet wird, ist generell jeder RADIUS-Server einsetzbar. Zudem muss bei einem Accept nur ein notwendiger Parameter, die Gruppe, mit übertragen werden, was die Konfiguration auf Seiten des Authentication Servers sehr überschaubar macht.

- An den Policy Server werden keinerlei Hochverfügbarkeitsansprüche gestellt, da er nur als Mittel zur Konfiguration der Netzkomponenten dient und danach bis zu einer Änderung des Regelwerkes nicht mehr gebraucht wird.

- Weil die Filterregeln in der Konfiguration abgelegt werden, sind sie auch nach einem Reboot eines Systemes noch da.

- In kleineren Netzen kann auf den Einsatz des kostenpflichtigen Policy Servers ganz verzichtet werden.

Contra
- Durch den Einsatz des Policy Servers bedingt, wird eine zusätzliche Software erforderlich und damit verbunden auch Lizenzkosten.

- Für eine umfangreiche Konfiguration von Regeln muss genug Speicherplatz zur Verfügung stehen.

### Online Konfiguration von Benutzerrollen (INA, Extreme)

Die Lösung von Extreme wirkt wie ein Mix aus den beiden Vorhergehenden, da auf der einen Seite sowohl ein RADIUS-Server wie auch ein Policy Server zum Einsatz kommen, auf der anderen Seite die Übertragung der kompletten Regeln jedoch online geschieht.

Das Verfahren ist in Abbildung 7 dargestellt.

Nach der Übertragung der Benutzer-/Clientdaten via 1X und RADIUS erfolgt auch hier die Zugangsbestätigung oder -ablehnung durch den Authentication Server. Im Falle eines Accepts jedoch wendet sich der Switch an einen Policy Server, um dort die Policy abzurufen und anschließend auf den Port zu mappen.

Pro
- Auch komplexe Filterwerke beeinflussen die Größe der Startup-Konfiguration nicht, da sie auf den Netzwerkkomponenten nicht abgespeichert werden müssen.

- Die Konfiguration des Authentication Servers bleibt übersichtlich, da wie bei der Enterasys-Lösung auf den Einsatz von Protokollerweiterungen verzichtet wird.

- Aus demselben Grund kann auch jeder beliebige RADIUS-Server genutzt werden.

Contra
- Da der Policy Server ständig erreichbar sein muss, muss er wie auch der RA-

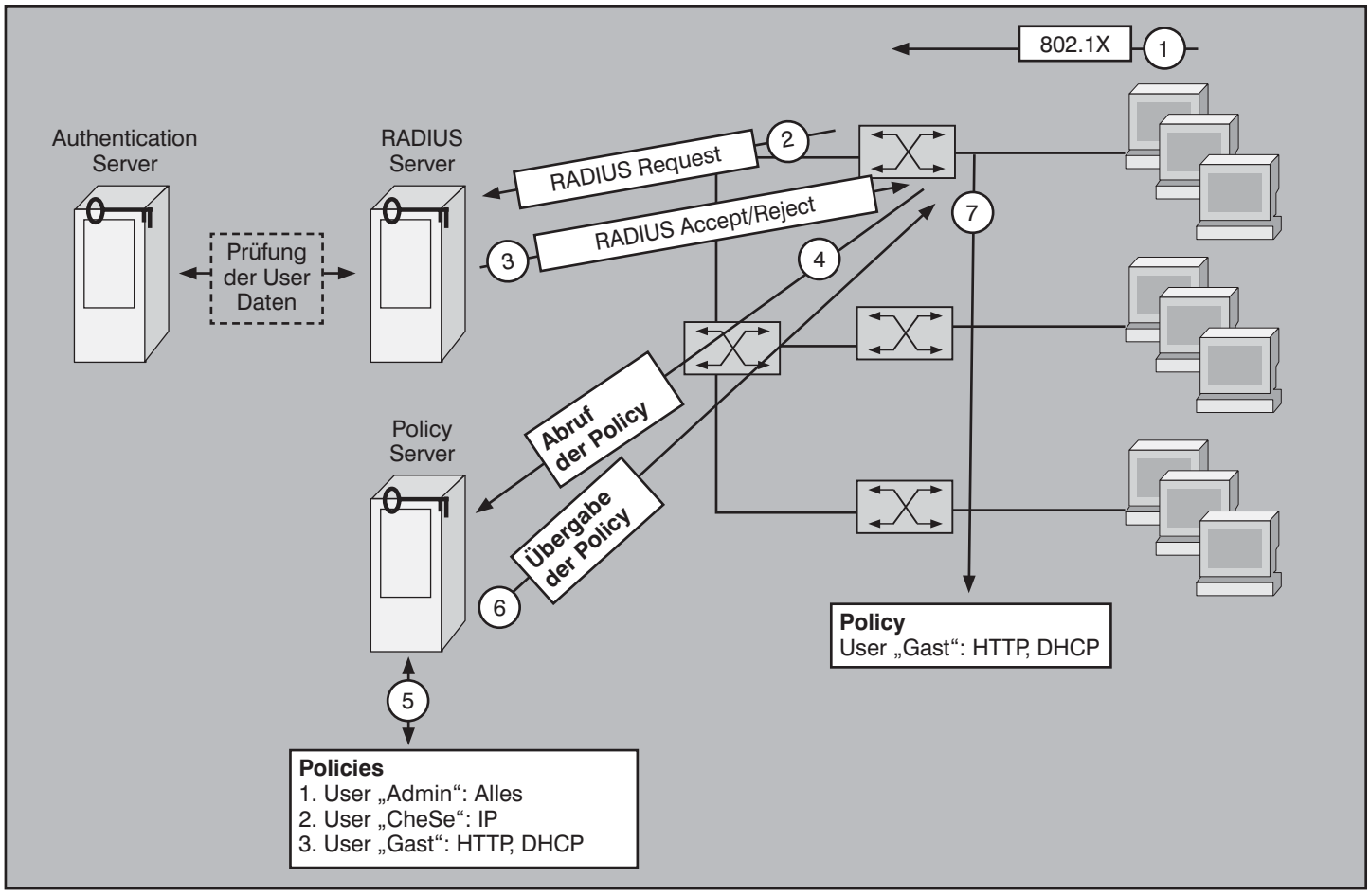



Abbildung 7: Online Zuweisung der Benutzerrollen

DIUS-Server hochverfügbar ausgelegt werden.

- Der Policy Server bedingt zusätzliche Lizenzkosten und ggf. auch zusätzliche Hardware.

**Fazit: individualisierte Zugriffsrechte**

Allen Verfahren gemeinsam ist, dass sie den bekannten Beschränkungen von 802.1X unterliegen, wie beispielsweise der ungelösten Fragen nach Druckeranschlüssen, alten Betriebsystemen oder spezieller Hardware, die nicht 1X fähig ist.

Die Kombination von 1X mit der Individualisierung der Zugriffsrechte bringt jedoch neue Nachteile:

Stellen 802.1X und RADIUS noch Standards dar, die herstellerübergreifend funktionieren sollten, so haben die Hersteller es geschafft, diese beim Einsatz von user-/clientbezogenen Zugriffsrechten so geschickt mit eigenen Funktionen zu verquicken, dass die Ergebnisse wieder proprietär sind. Sicher kann man in allen Fällen - grundsätzlich - einen beliebigen RADIUS-Server benutzen und zumindest bei Cisco und Enterasys ist die eigene Software (ACS, Policy Server) nicht zwingend notwendig, jedoch lassen sich die Lösungen nicht miteinander verheiraten, ohne dass man völlig den Überblick verliert. Wenn der Authentication Server auch noch Switch-bezogen unterscheiden muss, ob er eine Gruppe, ein VLAN oder eine Access-Liste übermitteln muss, kann von einer beherrschbaren Technik nicht mehr die Rede sein. Muss man oben drein auch noch mit verschiedenen Policy Servern arbeiten, hilft wahrscheinlich auch die beste Dokumentation nicht mehr aus, wenn sich irgendetwas ändert.

Kurz: will man INA, UPN oder NAC einsetzten, muss einem - Stand heute - klar sein, dass man den Hersteller zumindest für den Access Bereich heiratet, und zwar mit Ehevertrag und Gütertrennung: kommt es zur Scheidung, oder geht man auch „nur“ fremd, kann man sein Policy-Konzept vergessen.

Geht man jedoch diesen monogamen Weg, weil beispielsweise aus anderen Gründen ohnehin eine Ein-Hersteller-Politik betrieben wird, so sollte man das Konzept so schlicht wie möglich halten.

Wenn möglich:

- Nicht mit personalisierten Zugriffsrechten arbeiten, sondern nur mit gruppenbezogenen.
- Auf bereits bestehende Gruppen (bspw. im AD) zurückgreifen.
- Die Regeln für alle Swichtes identisch halten.
- Die Regeln für alle Access Point identisch halten.
- Die Regeln selbst einfach gestalten.

Kurz: wenn man eines dieser Konzepte einsetzten will oder muss, muss das KISS Konzept oberste Priorität haben.

**Abkürzungen**

| | |
|---|---|
| AP | Access Point |
| CLI | Command Line Interface |
| CS-ACS | (Cisco Secure ) Access Control Server |
| IEEE 802.1X | Port-Based Network Access Control |
| INA | Intelligent Network Access |
| KISS | Keep it Simple and Stupid |
| LAN | Local Area Network |
| NAC | Network Admission Control |
| RADIUS | Remote Access Dial-In User Service |
| SSID | Service Set-Identifier |
| UPN | User Personalized Network |
| VLAN | Virtual LAN |
| WLAN | Wireless LAN |

Report des Monats

# Neuerscheinung März 2006
# Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

Der IEEE-Standard 802.1X dominiert zunehmend die aktuellen Sicherheitslösungen für große Netzwerke. Für alle aktuellen Betriebssysteme existieren Lösungen sowohl auf der Client- als auch auf der Serverseite, praktisch alle neueren Switches und WLAN Access Points unterstützen den Standard, die führenden Hersteller von Netzwerkkomponenten bieten in der Regel sogar Komplettlösungen an, die durch spezielle Features ihrer Produkte ergänzt werden. Die Gründe für diese Entwicklung liegen auf der Hand: Die Anforderungen an Enterprise-Netzwerke wachsen ununterbrochen. Aktuelle Themen sind die Integration von Wireless-LAN-Funktechniken, von IP-Telefonie und der Einzug von Ethernet- und IP-basierten Protokollen in industrielle Umgebungen. Die Netze werden damit nicht nur größer, sondern wachsen auch zunehmend zusammen. Hinzu kommt die ungebrochene Bedrohung durch Viren, Würmer und Trojaner.

Daraus ergeben sich vermehrte und veränderte Sicherheitsansprüche:

- Für Besucher sollen Zugänge zum Internet oder speziellen Netzbereichen (Gastzugang) realisiert werden, ohne dass das produktive Netz kompromittiert wird.
- Es existieren ungeschützte Ethernetports in öffentlich zugänglichen Bereichen.


- Wireless LANs stellen per se „offene“ Zugangsport zum Netzwerk zur Verfügung - je nach Umgebung sogar von außerhalb des Betriebsgeländes.
- Endgeräte für IP-Telefonie benötigen spezielle Netzwerkressourcen wie Laufzeit und Jitter, die anderen Clients nicht zugestanden werden können.
- Die Verkehrsströme unterschiedlicher Benutzergruppen im Netzwerk mit eigenen Zugriffsrechten müssen getrennt werden.

Die traditionelle Benutzerauthentisierung an zentralen Servern im Kernbereich des Netzwerks kann diesen Anforderungen nicht genügen. Mit dem IEEE-Standard 802.1X ist aber der Rahmen für neue Sicherheitslösungen gesteckt, in dessen Mittelpunkt die Authentisierung von Benutzern und Endgeräten bereits an den Zugangskomponenten wie Switches oder Access Points steht.

Dieser neue Technologie-Report führt Sie umfassend in die folgenden Themen ein:

- die Grundlagen des Standards IEEE 802.1X,
- die Grundlagen der verwendeten Netzwerkprotokolle RADIUS, EAP, EAPoL,
- die wichtigsten EAP-Methoden, das damit erreichbare Sicherheitsniveau und die damit verbundenen Einschränkungen,
- Architekturen für verschiedene Lösungen mit 802.1X,
- Unterschiede im LAN und WLAN,
- Anforderungen an Produkte und verwendete EAP-Methoden, was geht und wie erreicht man es,
- Features und Unterschiede von gängigen Lösungen und Produkten.

Sie erhalten somit ein umfassendes Grundlagenwerk, das Sie bei der Auswahl und beim Aufbau einer 802.1X-basierende Sicherheitslösung unterstützt, auf die verborgenen Fallstricke dieses Frameworks aufmerksam macht und wesentliche Betriebsaspekte offen legt.

Fax-Antwort an ComConsult 02408/955-399

# Bestellung
# Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

☐ Ich bestelle den Report
**Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X**
(Preis € 398.-- zzgl. MwSt. und Versand)

Die Studie wird Anfang März ausgeliefert.

Bestellen Sie über unsere Web-Seite
**www.comconsult-research.de**

| | |
|---|---|
| Vorname | Nachname |
| Firma | Telefon/Fax |
| Straße | PLZ,Ort |
| eMail | Unterschrift |

Neues Seminar

# Planung und Betrieb mobiler Kommunikation

Die Comconsult Akademie veranstaltet vom 06. - 07. März erstmalig ihr neues Seminar “Planung und Betrieb mobiler Kommunikation“ in Düsseldorf/Kaarst.

Mobilität ist ein Schlüssel-Element moderner Betriebsabläufe. Dabei geht es weniger um die simple telefonische Erreichbarkeit. Es geht vielmehr um die Möglichkeit, unabhängig vom Aufenthaltsort und jederzeit auf ein Dienst-Spektrum zurückzugreifen, das dem Angebot im heimatlichen Büro entspricht. Dabei wird vermehrt neben allgemeinen Diensten wie Email, Kalender-, Aufgabenverwaltung und Intranet-Zugang die mobile Unterstützung der typischen Unternehmens-Applikationen gefordert.

Dieses Seminar analysiert die beim Betrieb von mobilen Teilnehmern und Geräten zu lösenden Aufgaben und gibt Empfehlungen zur optimalen Umsetzung. Auch die typischen Fallstricke werden benannt. Auf der Basis von vielen Beispielen wird die geeignete Handhabung der verschiedenen Technikbereiche erklärt. Dabei zeigt sich, dass Mobilität als Kernanforderung für konvergente Netze einen maßgeblichen Einfluss auf Architektur und Betrieb hat.

In diesem Seminar lernen Sie
- wie sich die Forderung nach Mobilität in konvergenten Netzen auf Netzarchitektur und Netzbetriebssystem auswirkt

- welche Besonderheiten bei den verschiedenen Betriebssystemen für PDAs und Smart Phones zu beachten sind
- ob ein Netzmanagement von mobilen Kleingeräten überhaupt möglich ist
- wie Synchronisation und Backup von PDA bzw. Smart Phone funktionieren, welche Standards hier eine Rolle spielen und welche Grenzen die Systeme der verschiedenen Hersteller haben
- welche Strategien zur Softwareverwaltung für mobile Clients sinnvoll sind und wie eine Software Release bzw. ein Patch ausgerollt werden kann
- wie die Daten auf mobilen Geräten geeignet abgesichert werden können, welche Möglichkeiten zur Verschlüsselung und zur Zugangskontrolle (Authentifizierung) bestehen

Themenschwerpunkte sind:
- Netzwerke, Betriebsysteme und Mobilität
- Systemverwaltung, Synchronisation und Backup mobiler Systeme
- Konzepte und Mechanismen zur Absicherung mobiler Systeme
- Mobile Anwendungen und die Auswirkungen auf die Infrastruktur

Durch das Seminar führt Dr. Frank Imhoff. Dr. Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## Planung und Betrieb mobiler Kommunikation

☐ Ich buche das Seminar
**Planung und Betrieb mobiler Kommunikation**
vom 06. - 07.03.06 in Düsseldorf/Kaarst
zum Preis von € 1.390,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____06

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.com**

| | |
|---|---|
| _____ Vorname | _____ Nachname |
| _____ Firma | _____ Telefon/Fax |
| _____ Straße | _____ PLZ,Ort |
| _____ eMail | _____ Unterschrift |

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

### Lokale Netze für Einsteiger - Intensiv Seminar, 06. - 10.02.06 in Aachen

Dieses 5-tägige Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Preis: € 2.290,- zzgl. MwSt.

### Wireless LANs: Planung, Produktauswahl, Installation, Trouble Shooting, 13. - 17.02.06 in Bonn

Dieses 5-Tages-Seminar identifiziert die herausragenden Gefahrenbereiche für Firewalls, Webserver, Clienten, Mailsysteme und Netzwerke und zeigt detailliert effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

### Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 13. - 17.02.06 in Bonn

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren. Preis: € 2.290,- zzgl. MwSt.

### TCP/IP und SNMP - Intensiv Seminar, 13.02-17.02.06 in Bonn

Dieses 5-tägige Seminar vermittelt systematisch die Grundlagen TCP/IP, beleuchtet Vor- und Nachteile und gibt wichtige Empfehlungen für den erfolgreichen Einsatz. Dies betrifft speziell auch die wichtigen IP-Infrastrukturdienste von der Adressierung über ARP bis zu DHCP, DNS, DDNS und NAT und die Management-Funktionalität SNMP. Preis: € 2.290,- zzgl. MwSt.

### Quality of Service - QoS, 14. - 15.02.06 in Köln

Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standards es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert. Preis: € 1.390,- zzgl. MwSt.

### Ethernet Technologien neuester Stand, 20. - 24.02.06 in Aachen

Dieses Seminar stellt die neuesten Ethernet- und Wireless-Varianten vor und zeigt, nach welchen Regeln und Auslegungsvorschriften diese zu konfigurieren sind. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, auch wichtige Betriebsfragen werden vorgestellt. Im Besonderen wird die Bedeutung der IP-Telefonie für die Gestaltung von Ethernet-LANs analysiert. Abgerundet wird das Seminar um wichtige Fragen des Trouble-Shootings. Preis: € 2.290,- zzgl. MwSt.

### Cisco Router erfolgreich einsetzen für Fortgeschrittene, 20. - 24.02.06 in Aachen

Dieses 5-tägige Intensiv-Seminar wendet sich an Fortgeschrittene und hilft das Potenzial von Cisco Routern optimal auszuschöpfen sowie typische Fehler in der Konfiguration zu vermeiden. Es beinhaltet aktive Konfigurations-Übungen mit Cisco 2600 Routern in Kleinstgruppen. Schwerpunkt in diesem Seminar sind Redundanzkonzepte auf Layer 3. Preis: € 2.350,- zzgl. MwSt.

### WAN-Planung für zentrale Dienste, 20. - 22.02.06 in Köln

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess. Preis: € 1.690,- zzgl. MwSt.

### Sicherheit im LAN mit IEEE 802.1X, 20. - 21.02.06 in Köln

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

### IP-Telefonie: Markt und Produkte in der Analyse, 20. - 22.02.06 in Aachen

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht. Hier setzt die 3-tägige Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt. Sie erfahren, was IP-Telefonie-Produkte leisten, worauf Sie bei der Auswahl achten müssen, wo Probleme liegen und welche Strategien ausgewählte Hersteller verfolgen. Preis: € 1.990,- zzgl. MwSt.

### Internetworking: optimales Netzwerk-Design mit Switching und Routing, 06. - 10.03.06 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt dem Einsteiger Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Preis: € 2.290,- zzgl. MwSt.

### IP-Telefonie: Vorbereitung, Migration, Management, 06. - 08.03.06 in Düsseldorf/Kaarst

Die Referenten dieses 3-tägigen Seminars vermitteln ihre jahrelangen Projekt-Erfahrungen bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld. Preis: € 1.690,- zzgl. MwSt.

Schwerpunktthema

# Ende der Hackerromantik - Kriminelle auf dem Vormarsch

Fortsetzung von Seite 1

Dipl.-Inform. Detlef Weidenhammer ist seit 1994 Geschäftsführer der GAI NetConsult GmbH und hat seitdem in einer Vielzahl von Projekten national und international agierende Unternehmen bei der Konzeption von Netzwerk- und Sicherheitslösungen unterstützt. Seine fachlichen Schwerpunkte liegen in den Bereichen IT Risk Management, Security-Auditing und Security Management. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen auch als Verfasser von Publikationen und als Referent bei Seminaren und Kongressen ein. Er leitet das jährlich stattfindende „IT-Sicherheits-Forum“ und ist Herausgeber der Fachpublikation „Security Journal“.

Das Aufspüren und Vermarkten von Schwachstellen, die für Attacken ausgenutzt werden können, ist inzwischen zu einem gut dotierten Job geworden. Einen wesentlichen Anteil daran haben gerade einige Unternehmen aus der Security-Branche. Diese versuchen entweder mit eigenem Personal (z.B. ISS) oder aber mit bezahlten externen Informationen (z.B. 3Com / TippingPoint) einen Wissensvorsprung vor der Konkurrenz zu gewinnen, den sie versuchen kommerziell auszuschlachten (zero-day knowledge). Ein ganz neuer Weg, die Kenntnis über Schwachstellen in Geld umzuwandeln, wurde unlängst bei eBay aufgezeigt. Bevor die Versteigerung einer Excel Schwachstelle zum Ende kommen konnte, wurde diese jedoch von der eBay-Aufsicht aus dem Verkehr gezogen. Der Anbieter zeigte dabei seinen Sinn für Humor, denn er setzte für erfolgreiche Bieter aus dem Hause Microsoft einen Discount von 10% aus. Eigentlich konsequent, da er damit den Erzeuger der Schwachstelle belohnt hätte.

Kaum abschätzbar sind indes die Aktivitäten von wirklich Kriminellen, egal ob Einzeltäter oder organisierte Kriminalität. Auf einschlägigen Internetseiten oder Foren ist beispielsweise Exploit-Code für eine bereits bekannte Sicherheitslücke für $100 - $500 zu kaufen, für eine bisher unbekannte Lücke steigt der Preis auf $1000 - $5000. Listen mit IP-Adressen infizierter Systeme, die beispielsweise für den Versand von Spam-Mails missbraucht werden können, sind bereits für $150 - $550 zu haben. Die Daten von etwa 1000 noch gültigen Kreditkarten können für einen Preis zwischen $500 und $5500 bezogen werden. Ein professioneller Hacker mit Erfahrung, der seine Dienste beispielsweise an Spammer oder zu Phishing-Zwecken verkauft, kommt durchaus auf ein Jahresgehalt von bis zu $200.000.

Das organisierte Verbrechen dehnt seine klassischen Betätigungsfelder wie Bestechung, Erpressung, Bedrohung und Betrug immer mehr in die virtuelle Welt aus. Die an sich unabhängigen Hacker werden entweder gut bezahlt oder durch Erpressung gezwungen, für Kriminelle tätig zu werden. Den gegenwärtigen Zustand des Internets kann man durchaus als kriminalisiert bezeichnen. Ständige Viren- und Trojaner-Attacken terrorisieren praktisch alle Internet-Anwender: Heimanwender, kleine und mittlere Unternehmen, Großunternehmen und staatliche Institutionen. Beispiele für die eingesetzten Techniken der Angreifer sind DDoS-Attacken, Phishing oder Pharming, die später näher vorgestellt werden. Solche massenhaft vorgetragenen Attacken dienen vorwiegend den folgenden Zielen:

- Diebstahl von Informationen für den Zugang zu Bankkonten
- Diebstahl von Kreditkarten-Nummern
- Netzwerk-Attacken mit nachfolgender Erpressung, damit die Attacken beendet werden (moderne Schutzgelderpressung)
- Aufbau von Trojaner-Proxy-Netzen und Zombie-Netzen (Botnets) für Spam-Versand (und kommerzielle Nutzung dieser Netze)
- Verbreitung von Programmen, die unerwünschte Reklame laden und installieren (Adware)

Diese Attacken werden durch ihre weltweite Verbreitung in aller Regel schnell bekannt und es können Gegenmaßnahmen eingeleitet werden. Eine wichtige Rolle spielen dabei die Antivirus-Hersteller, deren Produkte nach Auslieferung neuer Pattern die Störenfriede erkennen und eliminieren sollten. Deutlich schlechter sieht es mit der Erkennung aber bei gezielt vorgetragenen Angriffen („targeted attacks“) aus, die zunehmend für Aufsehen sorgen und ein hohes Gefahrenpotenzial beinhalten. Zielsetzungen sind:

- Sammeln vertraulicher Informationen (auch als Auftragsarbeit)
- Überwachen von Tastatureingaben mit Keyloggern
- Sammlung von kritischen Systeminformationen und Suche nach Netzwerk-Laufwerken
- Benutzen des infizierten Systems, um andere Systeme und Netzwerke zu attackieren
- Download von neuer Malware für weitere Angriffe
- Upload von ausgespähten Informationen und Dokumenten zu einem entfernten System

Das Auftreten solcher gezielten Attacken häufte sich in den letzten Monaten derart, dass sich das US-CERT gezwungen sah, eine (relativ unspezifische) Warnung herauszugeben: Targeted Trojan Email Attacks (Technical Cyber Security Alert TA05-189A). Eine Bewertung der wirklichen Tragweite der Tätigkeit moderner Cyber-Verbrecher ist noch ziemlich schwer. Die Zahl der Hacker und ähnlicher Gruppierungen geht wahrscheinlich in die Tausende, wovon Polizeiberichte praktisch aus allen computerisierten Ländern der Welt zeugen. In den vergangenen zwei Jahren wurden mehrere Dutzend Hacker und Hacker-Gruppen verhaftet, insgesamt einige hundert Personen. Dies hatte bislang jedoch keinen wesentlichen Einfluss auf die Anzahl neuer Viren und Trojaner. Nach einer Analyse des Marktforschungs-Unternehmens Computer Economics kassierten kriminelle Hacker und andere Cyberkriminelle im Jahre 2004 durch ihre Aktivitäten zirka 18 Milliarden US-Dollar steuerfrei mit einem Wachstum von 30 bis 40 % pro Jahr.

## Ende der Hackerromantik - Kriminelle auf dem Vormarsch

Die Internet-Kriminalität stellt auch nach Einschätzung des Bundeskriminalamtes eine immer größere Bedrohung dar. Die Behörde kündigte deshalb gerade für 2006 eine Erweiterung der neuen Abteilung „Internationale Koordinierung“ an, die sich der Früherkennung solcher Delikte widmen soll.

### Massenhaft vorgetragene Attacken

Attacken, die mit weltweiter Verbreitung und ungeachtet der Größe oder Reputation eines Unternehmens agieren, stellen seit Jahren ein hohes Ärgernis für private Nutzer und Unternehmen dar, trugen aber auch zu einem immensen Wachstum der Antivirus-Industrie bei. Obwohl deren Lösungen immer besser wurden, gibt es immer wieder neue Betätigungsfelder für Angreifer, deren wichtigste nachstehend vorgestellt werden.

### Malware (Viren, Würmer, …)

In 2005 verlangsamte sich das zweite Jahr in Folge das Wachstumstempo von Viren und Würmern. Eine Ausnahme bilden dabei sog. Netzwürmer, diese haben das Wachstumstempo nicht nur gehalten - sie verzeichnen das stärkste Wachstum überhaupt. Durch das Fehlen des Anwenders in der Verbreitungskette - Netzwürmer können sich selbständig verbreiten - ist das schnelle Wachstum erklärbar. Es konnte auch eine deutliche Zunahme der Professionalität der Angreifer beobachtet werden. Zunehmend werden sog. „Hybrid-Schädlinge“ entwickelt, die verschiedene Funktionen von einzelnen Malware-Arten vereinen. Die Viren dienen neuerdings vor allem kriminellen Absichten mit kommerziellem Hintergrund: Der Wurm MyDoom lancierte beispielsweise verschiedene Denial of Service-Attacken (DoS, z.B. gegen SCO.com, micro-soft.com, riaa.com und google.com). Bagle sowie MyDoom funktionierten infizierte Systeme auch zu SMTP-Servern um, so dass auf diesem Weg Spam-Mails versandt werden konnten. Die Virengruppen von Bagle, MyDoom und Korgo dienten vor allem dem Sammeln von Login-Informationen mit Key-Loggern, die Tastatureingaben aufzeichnen. Die Absicht dieser Schädlinge ist es, an Authentifizierungs-Daten für eBanking oder andere Finanzdienstleistungen zu kommen. MyDoom.A öffnete nach der Infektion beispielsweise auch eine Backdoor, über die sich das infizierte System fernsteuern oder zusätzlicher Schadenscode nachladen ließ.

Malware zielt aber immer weniger auf eine globale Ausbreitung ab, sondern versucht häufig, nur ein bestimmtes Netz zu befallen. Das Motiv für dieses Vorgehen liegt darin, eine Entdeckung durch Antivirus-Hersteller möglichst lange zu verhindern (was natürlich bei einer raschen globalen Ausbreitung nicht der Fall ist) und so mehr Zeit für das Sammeln von Daten zu gewinnen. Zudem wurde eine vermehrte Zusammenarbeit zwischen den einzelnen Virenschreibern zwecks Optimierung des finanziellen Gewinns beobachtet, was die Qualität der Schadprogramme in den letzten Monaten entscheidend ansteigen ließ. Mit „Sober.I“ tauchte der erste Wurm auf, der seine „Sprache“ dynamisch anpassen konnte. Er schaut dabei auf die E-Mail-Adresse des Empfängers. Endet diese zum Beispiel mit .de, wird ein deutscher Text eingeblendet.

Bereits in 2004 trat eine neue Form von Malware in Erscheinung, die unter dem Namen JS/Scob-A (bzw. Download.Ject und Toofer) Schlagzeilen machte. Bei diesem Vorfall wurde erstmals das Web selbst als Transportweg für Malware genutzt. Von Hackern veränderte Websites haben dabei ahnungslose Surfer mit Code infiziert, was nur durch Ausnutzung von Sicherheitslücken im Microsoft Internet Explorer und in bestimmten Webservern möglich war. Beim Aufruf einer infizierten Seite wurde der Browser des Benutzers auf eine russische Website umgeleitet, die eine Backdoor und ein Keylogging-Programm installierte. Das dabei installierte Programm wartete still im Hintergrund, bis es den Aufruf ganz bestimmter URLs (z.B. der einer Online-Bank) registrierte. Erst dann wurde das Keylogging-Programm aktiviert. Vertrauliche Daten wie Benutzernamen, Kennwörter und Kontonummern wurden direkt an das System der Hacker in Russland übermittelt. Anders als andere Angriffe in der jüngeren Vergangenheit, bei denen Malware erst in Folge einer Benutzerhandlung installiert wurden, z.B. durch Öffnen einer eMail, war hier keine Mitwirkung durch den Benutzer erforderlich.

**Einige Maßnahmen gegen Malware**

- Sensibilisierung der Nutzer verbunden mit periodischer Überprüfung
- Einsatz von mehrstufigen Antivirus-Produkten mit verschiedenen Engines
- Ausdehnen des Schutzes auch auf aktive Inhalte (ActiveX, Java, JS usw.)
- Blockieren von Executables und verdächtigen eMail-Attachments
- Ausschalten der Preview-Funktion bei eMail-Clients
- Einbeziehung auch mobiler Systeme in die Schutzvorkehrungen
- Zeitnahes Patchmanagement aller wichtigen Systeme
- Verfolgen aller Hinweise auf anomales Systemverhalten
- IP-Verkehrsanalysen zur Aufdeckung von ungewöhnlichen Datentransfers zu entfernten Systemen (z.B. über Port 80)

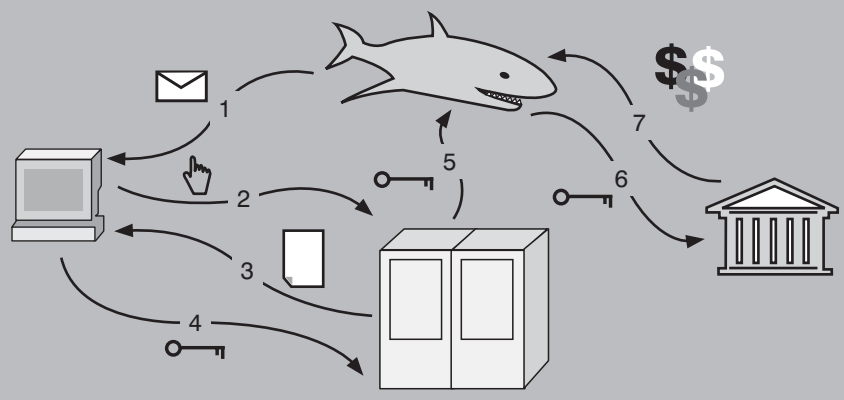
### Phishing und Pharming

Das Wort Phishing setzt sich aus den englischen Wörtern „Password“, „Harvesting“ und „Fishing“ zusammen. Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen eMails mit gefälschten Absenderadressen zustellen. In den eMails wird das Opfer beispielsweise darauf hingewiesen, dass seine Kontoinformationen und Zugangsdaten (z.B. Benutzernamen und Passwort) nicht mehr sicher oder aktuell sind und es diese unter dem in der eMail aufgeführten Link ändern soll. Der Link führt dann allerdings nicht auf die Originalseite des jeweiligen Dienstanbieters (z.B. der Bank), sondern auf eine vom Betrüger identisch aufgesetzte Webseite. Mit den erschlichenen Daten kann ein Betrüger im Namen des Opfers (Internet-Benutzer) beispielsweise Banküberweisungen tätigen oder Angebote bei einer Online-Versteigerung platzieren. (siehe Abbildung 1)

Phishing-Attacken sind seit etwa 2004 zu beobachten und zeigen seit Beginn 2005 ein deutliches Wachstum (siehe Abbildung 2). Unternehmen der Finanzdienstleistung sind dabei mit fast 90% der am stärksten heimgesuchte Bereich. Die Angreifer nutzen unterschiedlichste Techniken, um den Nutzern persönliche Daten oder Zugangscodes für Finanztransaktionen zu entlocken. Für Angriffe der Kategorie „Täuschung“ werden meist manipulierte eMails genutzt, um Nutzer auf nachgemachte Webseiten zu locken und sie zur Preisgabe ihrer Passwörter, PINs, TANs oder dergleichen zu bewegen. Durch die hohe Zahl der SPAM-artig versendeten eMails und viele leichtgläubige Nutzer werden auch heute immer noch Opfer gefunden.

Zukünftig noch deutlicher an Bedeutung gewinnen werden Angriffe der Kategorie „Malware Injection“, wobei mit unterschiedlichen Techniken (verseuch-

## Ende der Hackerromantik - Kriminelle auf dem Vormarsch




(1) Eine präparierte Information (z.B. eMail) erreicht den Nutzer
(2) Der Nutzer führt eine unvorsichtige Aktion aus und macht sich damit angreifbar (z.B. Öffnen eines Attachments, Anwahl eines Webservers)
(3) Der Nutzer wird (glaubhaft) zur Angabe vertraulicher Informationen aufgefordert
(4) Der Nutzer gibt die gewünschten Informationen preis
(5) Die Informationen werden vom Phishing-Server zum Angreifer weiter gegeben
(6) Die Informationen werden genutzt, um im Namen des Nutzers Aktionen auszuführen
(7) Der Angreifer kommt zum Erfolg (z.B. Geldtransaktion)

Abbildung 1: Ablauf einer Phishing-Attacke

te Downloads, Schwachstellen im Mailer, XSS usw.) Spionageprogramme direkt auf dem PC des Nutzers platziert werden und dort gezielt die gewünschten Informationen abgreifen. Dabei kommen Key- und Screenlogger genauso zum Einsatz wie Session Hijacking oder Web-Trojaner.

Ebenfalls deutlich im Ansteigen begriffen sind Angriffe der Kategorie „Pharming". Diese versuchen Nutzer ebenfalls auf manipulierte Kopien bekannter Webseiten zu leiten, benutzen dabei aber Techniken zur direkten Umlenkung von eigentlich korrekten Webrequests, z.B. durch DNS-Hijacking oder DNS-Poisoning. Das Grundprinzip funktioniert so, dass in ein DNS-Reply-Paket Extrainformation hineingeschmuggelt wird, die dann vom DNS-Server interpretiert werden. Dies erlaubt es dem Angreifer, falsche Informationen in den DNS-Cache eines DNS-Servers zu bringen. Anders als beim Phishing landet bei einem erfolgreichen Pharming-Angriff selbst ein Benutzer, der keinem Link in einer Phishing-Mail folgt und stattdessen die URL von Hand im Browser eingibt oder die Seite über einen Bookmark aufruft, auf der gefälschten Seite. Diese Seite sieht dann zwar wie die Originalseite aus, hat auch die entsprechende URL, wird aber auf dem Server des Angreifers gehostet. Während DNS-Spoofing bei den zumeist sicher konfigurierten DNS-Servern größerer Provider kaum droht, sind insbesondere kleinere, für die Namensauflösung in Firmennetzwerken zuständige, privat kontrollierte DNS-Server anfällig, so dass sich dieses Vorgehen insbesondere auch für Spionage-Aktivitäten (unbemerktes Umleiten der Nutzer eines Firmennetzwerks auf eine Seite, die Spionageprogramme verteilt) lohnt.

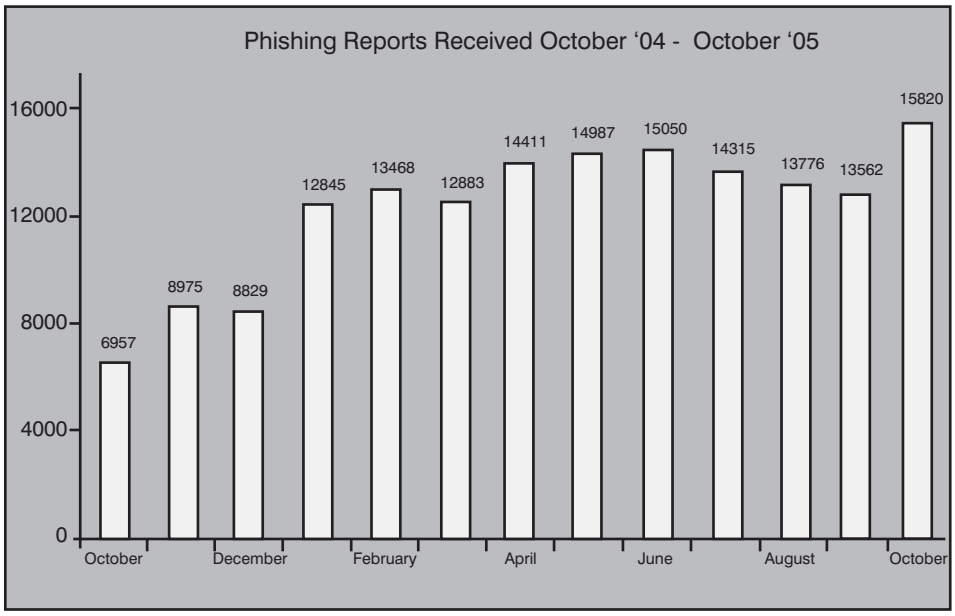



Abbildung 2: Starkes Anwachsen der Phishing Reports (Quelle: www.antiphishing.org)

Fallbeispiel: Wie das Internet Storm Center (ISC) im April 2005 bekannt gab, fanden im März und April mehrere gezielte Pharming-Attacken gegen DNS-Dienste statt. Insbesondere in Nord- und Südamerika waren schätzungsweise bis zu 1000 Firmen betroffen. Sämtliche Angestellten wurden so auf Websites geleitet, über die Spyware installiert werden konnte. Auch wenn in den beschriebenen Fällen keine Spionage betrieben wurde, könnte auf diese Weise schädlicher Code in ein Firmennetz eingeschleust werden, mit dem Daten, eMail-Verkehr, Passwörter und anderes mehr abgehört, gesammelt und anschließend an den Angreifer weitergeschickt werden können. (siehe Kasten „Maßnahmen gegen Phishing/Pharming")

**Bot-Netze / DDoS-Attacken**

Bot-Netze sind logische Computernetzwerke aus zuvor kompromittierten Systemen, die meist via Internet Relay Chat (IRC) kontrolliert werden, ohne dass die Besitzer dieser Systeme davon eine Ahnung hätten. Die Kompromittierung erfolgt meist durch das Ausnutzen einer ungepatchten Schwachstelle im Betriebssystem oder in einer Applikation (am häufigsten im Browser), schwache Passwörter sowie durch verseuchte eMail-Attachments. Nach der Infektion wird meist ein Programm installiert, mit dem anschließend Tastatureingaben aufgezeichnet, Passwörter mitgelesen oder verschiedene andere unerwünschte Tätigkeiten durchgeführt werden können. Vor allem aber kann ein auf diese Art kompromittierter Rechner von einem zentralen Server aus für verschiedene Aktionen ferngesteuert werden (siehe Abbildung 3). Im Falle eines abgestimmten Einsatzes sämtlicher, einem Bot-Netz angehöriger Rechner kann ein solches Bot-Netz beispielsweise für verteilte Denial-of-Service Angriffe (DDoS) missbraucht werden. Auf diese Weise kann die Band-

## Ende der Hackerromantik - Kriminelle auf dem Vormarsch

**Maßnahmen gegen Phishing / Pharming**
- Sensibilisierung der Nutzer verbunden mit periodischer Überprüfung
- Zeitnahes Patchmanagement aller wichtigen Systeme und Anwendungen
- Anlaufstelle für Phishing-Alarme schaffen
- Einsatz von mehrstufigen Antivirus-Produkten mit verschiedenen Engines
- Einsatz von Content-Gateways zum Filtern von bösartigen Webinhalten
- Einsatz von Tools gegen URL-Spoofing
- Einsatz von eMail-Authentisierung (oder sogar Verschlüsselung)
- Einsatz von Anti-Phishing Toolbars im Browser

breite, über die der angegriffene Server mit Datenpaketen bombardiert wird, massiv erhöht werden - gleichzeitig können auch Spuren verwischt werden, so dass die Herkunft der Attacke schwierig zu ermitteln sein wird. Das bisher größte beobachtete IRC-Botnetz hatte eine Größe von mehr als 100.000 Bots.

Die Erzeuger und Besitzer von Bot-Netzen verfolgen inzwischen in erster Linie kommerzielle Ziele. Dies kann die Zusammenarbeit mit Spam-Versendern sein, denen die Netze gegen Entgelt zur Verfügung gestellt werden. Ebenfalls bekannt geworden sind Vorfälle von Erpressung: Ein kurzer DDoS-Angriff, der die Infrastruktur des Opfers noch nicht vollständig zum Erliegen bringt, wird gefahren, um sich anschließend mit finanziellen Forderungen an das Unternehmen zu wenden. Andernfalls würde ein größerer, verheerender Angriff stattfinden. Die Dunkelziffer solcher Vorfälle dürfte beträchtlich sein, zumal ein betroffenes Unternehmen aus Image-Gründen damit kaum an die Öffentlichkeit oder die Behörden geht.

Fallbeispiel: In Großbritannien wurde der Fall des so genannten „Randex“ Bot-Nets bekannt, das von vier noch Minderjährigen betrieben wurde. Die Gruppe infizierte mit ihrem Computervirus „Randex“ tausende von Rechnern und installierte auf diesen ein Programm, welches über einen IRC-Channel Kontakt zu seinem Master aufnahm. Das Programm konnte nach CD-Keys von Spielen suchen, DDoS-Attacken gegen bestimmte Server starten oder unbemerkt beliebig weitere schädliche Software nachladen. Beispielsweise wurde ein SOCKS-Proxyserver auf die infizierten Maschinen nachgeladen, der den Einsatz des infizierten Systems zur Weiterleitung von Spam-Mails ermöglichte. Wie das amerikanische FBI ermitteln konnte, vermietete die Randex-Gruppe ihr Bot-Netz auch kommerziell. Offenbar bezahlte der CEO einer amerikanischen Firma, spezialisiert auf den Verkauf von Satelliten-Empfängern, der Gruppe Geld für einen DDoS-Angriff auf die Webseiten seiner Konkurrenz (z.B. rapidsatellite.com, weakness.com).

Die Gegenmaßnahmen entsprechen i.W. denen bei der Abwehr von Malware angeführten.

### Gezielte Attacken mit Spyware-Trojanern

Nach den aus der Vergangenheit bekannten und massenhaft vorgetragenen Angriffen mit Viren und Würmern ist zunehmend der Trend zur Verbreitung von Trojanern und Backdoor-Programmen zu bemerken (siehe Abbildung 4). Wöchentlich gibt es Dutzende neuer Varianten, die oft sehr unterschiedlich in Form und Funktion sind. Einige davon registrieren Tastenanschläge (Key Logging) und schicken die Daten per E-Mail an den Autor oder Lenker des Trojaners. Die aufwändigeren Vertreter übernehmen die komplette Kontrolle über den befallenen Rechner, wobei ganze Datenströme auf entfernten Servern abgelegt werden und weitere Befehle von diesen Servern empfangen werden können. Das Wachstumstempo ist nach wie vor sehr hoch und übersteigt das aller anderen Malware-Kategorien deutlich.

Gerade Vertreter dieser Kategorie ziehen in letzter Zeit auch verstärkt die Aufmerksamkeit seitens der kriminellen Cyber-Gemeinschaft auf sich. Kaspersky Labs deutet dies als „allmähliche Aktivitätsverlagerung der Cyberverbrecher“ und „intensive Kriminalisierung des Internets“. Dabei ist ein

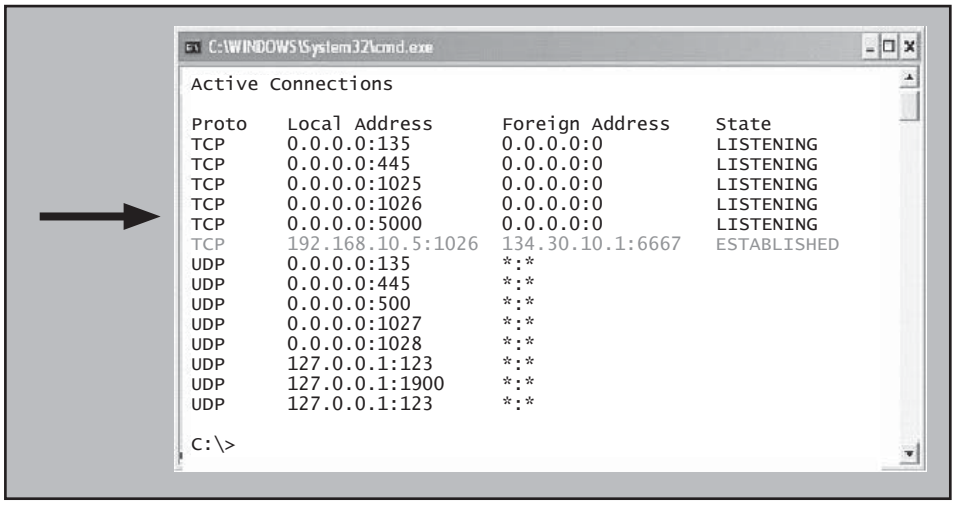



Abbildung 3: „netstat –an“ zeigt die Außenverbindung eines infizierten Systems

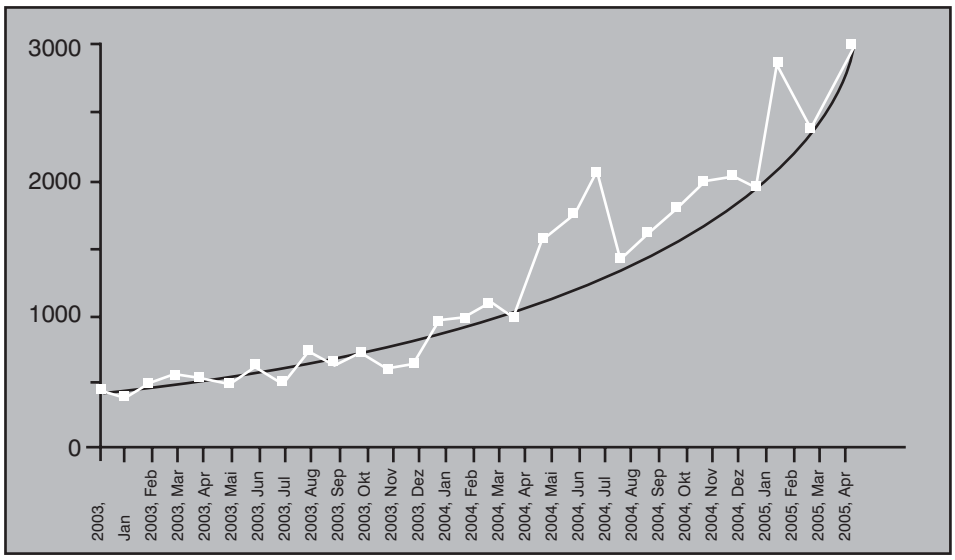



Abbildung 4: Wachsende Gefahr durch Trojaner (Quelle: Kaspersky Labs)

deutlicher Trend hin zu gezielten Aktionen („targeted attacks“) festzustellen. Anstatt eine möglichst große Verbreitung zu erzielen, setzen Angreifer auf eine gezielte Ausbreitung allein beim ausersehenen Opfer. Auf diese Weise können speziell auf das Ziel hin entwickelte Trojaner eingesetzt werden und es wird verhindert, dass Antivirus-Hersteller den Schädling frühzeitig entdecken und ihre Signaturen aktualisieren können – der Angreifer kann so unter Umständen über lange Zeiträume unbemerkt Daten sammeln. In den bekannt gewordenen Fällen wurden auch raffinierte Social Engineering Methoden angewandt, um die Zielumgebung auszuspähen und die Schädlinge auf einem System zu installieren.

Fallbeispiele: Wie im Juni 2005 durch das britische NISCC (National Infrastructure Security Coordination Centre) bekannt wurde, erfolgte seit Mitte 2003 eine Serie von gezielten Angriffen gegen mehr als 300 Regierungsstellen und Betreiber von Kritischen Infrastrukturen in Großbritannien. Die Angreifer hatten dabei in erster Linie Mitarbeiter mit Zugang zu sensiblen Daten im Visier. Angesprochen wurden diese mit Methoden des Social Engineering: Die Betreffzeile der eMail, mit der Trojaner eingeschleust wurden, enthielt oft Informationen, die für den Mitarbeiter von Interesse waren und bereits im Vorfeld aus seinem engsten Umfeld vom Angreifer recherchiert wurden. Die eMail selbst enthielt Links auf unscheinbare News-Webseiten oder Attachments, die nach News-Berichten aussahen.

Die zum Einsatz gekommenen Trojaner waren in der Lage, Passwörter zu sammeln, Screenshots anzufertigen, das Netzwerk zu scannen, die vollständige Kontrolle über das kompromittierte System zu übernehmen oder Dokumente ins Internet zu verschicken. Ziel der Angriffe war es, vertrauliche Informationen mit strategischem oder kommerziellem Wert zu sammeln. Bemerkenswert ist insbesondere, dass die eingesetzten Trojaner sonst nirgends auftauchten und daher keiner Antivirus-Software bekannt waren. So konnten die Schädlinge über Monate hinweg unbemerkt agieren.

Die Herkunft der Angriffe ist unklar, auch wenn sie ihren Ursprung im Fernen Osten haben dürfte, wie NISCC bekannt gab. Die raffinierte und gezielte Vorgehensweise lässt einen größeren, finanzkräftigen Akteur vermuten.

Ein anderer Aufsehen erregender Fall ereignete sich 2005 in Israel. Mit einem eigens entwickelten Trojaner wurden gleich mehrere große Unternehmen monatelang von Konkurrenten belauscht. Zu den Auftraggebern zählten nach Angaben der Ermittlungsbehörden unter anderem Mobilfunk-Provider, Satelliten-TV-Anbieter sowie ein Mineralwasserabfüller. Drei von den verdächtigten Unternehmen beauftragte Privatdetekteien hatten den Trojaner bei einem Hacker bestellt und in Umlauf gebracht. Verschickt wurde er getarnt auf unscheinbaren Werbe-CDs oder als Attachment von harmlos klingenden eMails. Einmal installiert, war das Programm kaum noch aufzufinden. Mit dem Trojaner ließ sich ein PC komplett fernsteuern. Wichtige Dokumente lud er direkt auf ferne FTP-Server hoch. Kein Antivirusprogramm hatte den digitalen Spion erkennen können.

Die Gegenmaßnahmen entsprechen i.W. denen bei der Abwehr von Malware angeführten. Es ist jedoch hervorzuheben, dass Antivirus-Produkte bei speziell erstellten Trojanern versagen werden. Deshalb ist besonderes Augenmerk auf die übrigen der genannten Aktivitäten zu legen.

**Attacken auf kritische Infrastrukturen**

Sind von den vorstehend genannten Angriffsformen und Fallbeispielen vorwiegend Unternehmen aus den Bereichen eBusiness und Finanzdienstleistung betroffen, so muss das Augenmerk zunehmend auch auf die Bedrohung von kritischen Infrastrukturen gerichtet werden.

Hauptgrund für die Zunahme der Befürchtungen ist wiederum die zunehmende Ausrichtung der Hacker auf finanziellen Gewinn. Werden diese Spezialisten erst einmal von Terroristen, Regierungen oder kriminellen Organisationen angeheuert, nimmt zumindest das Potenzial für einen erfolgreichen Angriff auf kritische Infrastrukturen massiv zu.

Unternehmen, Verwaltungen und private Haushalte sind von der ständigen Verfügbarkeit von Infrastrukturen beispielsweise zur Strom- oder Wasserversorgung stark abhängig. Viele dieser Infrastrukturen verwenden spezielle Prozessleitsysteme, auch SCADA-Systeme (Supervisory Control and Data Acquisition) genannt, zur Steuerung der verschiedenen Funktionen. Zur Vernetzung ihrer Komponenten nutzen diese Systeme heute immer häufiger die gleiche Technologie wie Computernetze. Die Hauptprobleme in der Sicherheit sind daher in den Bereichen der bisher weitgehend unverschlüsselten Daten- und Kommandoübermittlung, der Anbindung an öffentliche Netzwerke und in der fehlenden Standardisierung der Technologien zu suchen. Hat ein Angreifer Zugang zum Netz des Prozessleitsystems, kann er von „normalen“ Computersystemen her bekannte Angriffsmethoden nutzen, um die Funktionen des Systems zu beeinträchtigen.

## Ende der Hackerromantik - Kriminelle auf dem Vormarsch

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Nur wenn Kritische Infrastrukturen wie:
- Transport und Verkehr,
- Energie,
- Gefahrenstoffe,
- Informationstechnik und Telekommunikation,
- Finanz-, Geld und Versicherungswesen,
- Versorgung,
- Behörden, Verwaltung und Justiz,
- Sonstiges

ohne wesentliche Beeinträchtigungen verfügbar bzw. vor weit reichenden Schäden geschützt sind, können Staat und Wirtschaft uneingeschränkt ihre Aufgaben erfüllen. Im BSI werden insbesondere Störungen oder Ausfälle in Kritischen Infrastrukturen betrachtet, die im Zusammenhang mit (absichtlich herbeigeführten) Fehlfunktionen der Informationstechnik stehen. Kommt es in den genannten Infrastrukturen zu solchen Störungen oder Ausfällen, können durch eine Kettenreaktion weitere Störungen ausgelöst werden (so genannte Dominoeffekte), die unter Umständen eine Beeinträchtigung der Inneren Sicherheit in Deutschland zur Folge haben. Werden diese mit einer bestimmten Zielrichtung (z.B. Destabilisierung des Staates) herbeigeführt, können solche Vorfälle auch die äußere Sicherheit betreffen.

Abbildung 5: BSI-Definition kritischer Infrastrukturen

Das Gefahrenpotenzial ist groß, da bei vielen SCADA-Systemen aufgrund der besonderen Anforderungen die üblichen Sicherheitsmaßnahmen nicht immer angewandt werden können. Schutzmaßnahmen wie Netzwerkmonitore, IDS-Systeme und der Einsatz von Firewalls mit sehr restriktiven Regeln dürfen die Funktionalität der Prozessleitsysteme nicht beeinträchtigen. Bei der Entwicklung vieler SCADA-Komponenten ist außerdem der Aspekt der IT-Sicherheit nicht immer ausreichend berücksichtigt worden. Zudem wurden Sicherheitsmechanismen wie Authentifizierung und Verschlüsselung selten implementiert. Erschwerend kommt hinzu, dass die Unternehmen für die eingesetzten Prozessleitsysteme viel zu selten Risikoanalysen durchführen lassen.

Man muss wohl mit einer Zunahme von aus eMail herrührenden oder über Netzwerke direkt verteilten Schädlingen, DDoS-Attacken oder gezielten Einzelangriffen rechnen. Es ist aber wohl davon auszugehen, dass ein erfolgreicher Angriff auf solche Systeme ohne detailliertes Insiderwissen unrealistisch ist. Auch wenn es zwar möglich sein könnte, in solche Systeme einzudringen, erscheint es fast unmöglich, dramatische Effekte auf die Steuerung zu erzielen. Sollte dies doch gelingen, könnte zudem eine vorhandene automatische Steuerung rasch deaktiviert und die Versorgung manuell sichergestellt werden. Daher ist davon auszugehen, dass ein physischer Angriff auf absehbare Zeit hinaus viel größeren Erfolg verspricht. Die Möglichkeiten aber zumindest Erfolg versprechende Erpressungen durchzuführen, sind wohl schon heute gegeben.

Im Rahmen seiner KRITIS-Arbeit gibt das BSI den Unternehmen, die zu den sog. Kritischen Infrastrukturen zählen, konkrete Hilfsmittel an die Hand. Zwei dieser Hilfsmittel sind die vom BSI jüngst veröffentlichte Beispielrichtlinie „IT-Sicherheit im KRITIS-Unternehmen“ sowie „Audit-Materialien zum Standort-Kurzcheck in Kritischen Infrastrukturen“. (siehe http://www.bsi.bund.de/fachthem/kritis/hilfsmittel.htm)

CCNE

## ComConsult Certified Network Engineer

**Lokale Netze**
06.02. - 10.02.06 in Aachen
03.04. - 07.04.06 in D'dorf
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Stuttgart
04.12. - 08.12.06 in Aachen

**Internetworking**
06.03. - 10.03.06 in Aachen
08.05. - 12.05.06 in Bonn
11.09. - 15.09.06 in Aachen
13.11. - 17.11.06 in Aachen

**TCP/IP und SNMP**
13.02. - 17.02.06 in Bonn
15.05. - 19.05.06 in Stuttgart
25.09. - 29.09.06 in Köln
27.11. - 01.12.06 in Berlin

**Ethernet Technologien - neuester Stand**
20.02. - 24.02.06 in Aachen
29.05. - 02.06.06 in Aachen
25.09. - 29.09.06 in Aachen
27.11. - 01.12.06 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCTS

## ComConsult Certified Trouble Shooter

**Trouble Shooting in Lokalen Netzwerken - Grundlagen**
20.03. - 24.03.06 in Aachen
08.05. - 12.05.06 in Bad Neuenahr
04.09. - 08.09.06 in Aachen
06.11. - 10.11.06 in Aachen

**Trouble Shooting in geswitchten Ethernet-Umgebungen**
27.03. - 31.03.06 in Aachen
19.06. - 23.06.06 in Aachen
18.09. - 22.09.06 in Aachen
13.11. - 17.11.06 in Aachen

**Trouble Shooting für TCP/IP- und Windows-Umgebungen**
30.01. - 03.02.06 in Aachen
24.04. - 28.04.06 in Aachen
16.10. - 20.10.06 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCSE

## ComConsult Certified Security Expert

**Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung**
06.02. - 10.02.06 in Köln
15.05. - 19.05.06 in Stuttgart
11.09. - 15.09.06 in Bonn

**Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb**
20.03. - 22.03.06 in Bad Neuenahr
19.06. - 21.06.06 in Weimar
25.09. - 27.09.06 in Köln

**Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs**
03.04. - 07.04.06 in Aachen
26.06. - 30.06.06 in Aachen
23.10. - 27.10.06 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie