ComConsult Research

Der Netzwerk Insider

März 2007

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Welche neuen Gefahren kommen mit Web 2.0 auf uns zu?

von Björn Fröbe

Das Web 2.0 ist heutzutage in aller Munde. Die Hysterie um YouTube, MySpace, Google Maps und Co. weckt sogar Erinnerungen an die im Jahr 2001 geplatzte DotCom-Blase. Der vorliegende Artikel stellt einige Basistechnologien des Web 2.0 vor und beschreibt mögliche Gefährdungen, die diese Technologien mit sich bringen.

Eine genaue Definition was das „Web 2.0“ eigentlich ist, gibt es nicht. Der Begriff wurde von der O’Reilly Verlagsgruppe geprägt, die damit eine hauseigene Konferenzreihe (Web 2.0 Conference, erstmals durchgeführt im September 2004) umschreiben wollte. In einem Artikel von Tim O’Reilly

wurde erstmals folgende Mindmap erstellt, welche die Prinzipien des Web 2.0 umschreibt (siehe Abbildung 1).

Eine aus Sicht des Autors relativ gute Beschreibung des Web 2.0 ist „Read / Write“-Web. Typische Web 2.0 Elemente wie Blogs, Wikis und Social Bookmarking basieren auf der Mitarbeit des ursprünglichen nur konsumierenden Nutzers. Im Web 2.0 gibt es daher keine klare Abgrenzung mehr zwischen Anbietern und Konsumenten von Inhalten, da die Rollen beliebig vertauschbar sind.

weiter auf Seite 18

Zweitthema

NCCM als Erfolgsgarant für den Netzwerkbetrieb

von Ralf Horstmann, Sebastian Ahrens

In modernen IT-Infrastrukturen werden Störungen nicht mehr durch Komponentenausfälle verursacht, sondern hauptsächlich durch Fehlkonfigurationen. Durch den weit verbreiteten Einsatz von Netzwerkmanagementsystemen können Komplettausfälle schnell erkannt und rasch behoben werden. Fehlkonfigurationen der Komponenten dagegen sind nicht direkt identifizierbar und werden in den Managementsystemen erst durch ihre Auswirkungen sichtbar, nachdem Störungen aufgetreten sind. Eine umgehende Behebung dieser Störfälle ist nicht möglich, sondern erfordert eine zeit- und kostenaufwendige Analyse.

An dieser Stelle setzt Network Change and Configuration Managment (NCCM) an. Erstmals ist es möglich Fehlkonfigurationen durch gezielte Planung proaktiv zu verhindern, Konfigurationen zu überprüfen und automatische Maßnahmen zur Wiederherstellung des Soll-Zustands zu ergreifen. Die Prozesse des NCCM laufen weit unter der Wahrnehmungsschwelle von Netzwerk Management Systemen ab und stärken die Infrastruktur, das Rückgrat des modernen Unternehmens.

weiter auf Seite 11

Top Veranstaltung

ComConsult SIP-Forum 2007

auf Seite 4

Geleit

Offene TK-Lösungen: Aufregung im Markt

auf Seite 2

Report des Monats

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

auf Seite 16

Zum Geleit

Offene TK-Lösungen: Aufregung im Markt

Die Prognose von ComConsult-Research lautet seit einigen Wochen: spätestens 2008 wird der gesamte TK-Markt auf den offenen SIP-Standard umschwenken. Nun zeigt sich in den Projekten in Kombination mit dem Ergebnis unserer laufenden Testarbeiten, dass der Druck in diese Richtung noch viel größer ist als angenommen. Schon jetzt wird in vielen Projekten lebhaft diskutiert, in welchem Umfang man die „SIP-Fähigkeit“ zum KO-Kriterium der Ausschreibung macht. Cisco und Siemens reiben sich begeistert die Hände, zeigt dies doch, dass sie mit ihrer strategischen Linie richtig liegen. Auch die reibungslose Interaktion mit der kommenden Microsoft/Nortel-Lösung, die ebenfalls SIP-basiert ist, wird zunehmend ein Argument im Markt.

Diese Diskussion wirft eine Reihe von Fragen auf, die alles andere als trivial sind:

1) Was heißt hier offene TK-Lösung? Wann ist eine Lösung offen?
2) Warum offene TK-Lösung, wer hat davon welche Vorteile?
3) Inwieweit gefährdet die Offenheit die bestehende Herstellerwelt?
4) Welches Know how braucht der Betreiber dieser Welt, sind jetzt die IT-Gurus am Zuge und hat traditionelles TK-Wissen ausgedient?

Dabei treffen diese Fragen gar nicht den Kern der gerade ablaufenden Entwicklung, die alles überragende Kernfrage, die den gesamten Markt in Aufruhr hält, ist:

Wann muss man auf SIP-basierte Lösungen umschwenken, wie lange kann man noch an diesem Thema vorbei gehen und warten?

Damit hat sich die gesamte Fragestellung zu TK-Lösungen gedreht. Wir diskutieren nicht mehr, ob traditionelle TK oder IP-Telefonie, wir diskutieren über offene Lösungen. Damit löst IP-Telefonie einen Teil seines Versprechens ein. Im Endeffekt war und ist die Offenheit die zentrale Vision der IP-Telefonie.

Was macht ComConsult-Research, um diese Fragen für Sie zu beantworten:

1) Wir kündigen hiermit die Veröffentlichung unserer großen SIP-Studie an.

Diese wird im April erscheinen und sich mit dem Leistungsumfang von SIP und speziell der Frage der SIP-Compliance befassen. Mit Compliance ist dabei gemeint, welche Kriterien ein Produkt erfüllen muss, um wirklich als SIP-Produkt bewertet werden zu können. Immerhin behauptet jeder Hersteller, irgendwie SIP zu können. Nach unserem Verständnis trifft dies aber nur für einen sehr kleinen Teil der Produkte wirklich zu

2) Wir kündigen hiermit gleichzeitig eine große Sonderveranstaltung zu diesem Thema an, das ComConsult SIP-Forum 2007, das am 14. und 15. Mai in Frankfurt stattfinden wird. Cisco und Siemens stellen sich dabei offen der SIP-Diskussion, Alcatel wird den wichtigen Part der Analyse des SIP-Einflusses auf gehostete TK-Lösungen übernehmen. Und wir sind guter Hoffnung, dass auch die Anwenderseite gut vertreten sein wird

Wir werden uns sicher in den nächsten Wochen und Monaten noch intensiv mit den genannten Fragen auseinander setzen. An dieser Stelle schon einmal einige Anmerkungen.

Zum ersten würde ich gerne das Wort TK-Lösung loswerden, es trifft nicht mehr den Kern der zukünftigen Lösungen. Korrekt wäre es, von Realzeit-Kommunikation zu sprechen. Damit wird die gesamte Spannbreite von Sprache, Video und Kollaboration abgedeckt.

Wo liegt der Vorteil offener Realzeit-Kommunikations-Lösungen? Der hauptsächliche Mehrwert von offenen Lösungen liegt in der Gestaltbarkeit der Lösung. In diesem Bereich lassen sich nicht nur neue Funktionen schaffen sondern vor allem auch massiv Betriebskosten einsparen.

Insgesamt unterscheidet man folgende Bereiche der Gestaltung:

- Applikationen im Telefon: integrierte Browser gestatten die Ausführung von Web-Applikationen im Telefon. Über integrierte Funktions-API´s kann dabei auf Telefonie-Funktionen zugegriffen werden. Typische Anwendungen sind zentrale Telefonbücher oder Türöffner. Aber auch zusätzliche Funktionsmerkmale, die in der Grundausstattung nicht unterstützt werden, können umgesetzt werden

- Integration von externen Applikationen: umfangreiche API´s gestatten die Kombination mit Anwendungen auf dem lokalen PC und auf zentralen Servern. Gerade hier sind sowohl erhebliche Funktionszugewinne aber auch Betriebsoptimierungen erreichbar

- Nutzung von IT-Technik zum Betrieb: IP-Telefonie ist eine IT-Applikation. Entsprechend kann Standard-IT-Technik genutzt werden, um Backup-/Restore, Installation, Änderungen, Lastverteilung, Umschaltung im Falle eines Ausfalls und vieles andere mehr zu realisieren. Man ist nicht mehr auf individuelle Lösungen der TK-Hersteller angewiesen und kann sowieso vorhandene Prozeduren einsetzen

- Auf derselben Ebene liegt der Einsatz von Netzwerk- und System-Management-Tools. Als IT-Applikation IP-Telefonie weitgehend der Kontrolle und Steuerung traditioneller Management-Werkzeuge unterworfen werden. Lückenlose Eingliederung in vorhandene Operating-Strukturen, 24-Stunden Überwachung, Help-Desk-Integration werden dadurch deutlich erleichtert

- Die letzte Stufe jedes erfolgreichen IP-Telefonie-Projekts ist Automatisierung. Die Offenheit der Lösung ermöglicht Automatisierungsansätze, die vorher definitiv nicht möglich waren. Typisch ist eine effizientere Umsetzung von

Change-Management. Hier lassen sich zum Teil mehr als 50% der bisherigen Betriebskosten sparen.

Unsere bisherigen Labor-Arbeiten unterstreichen diese Sichtweise sehr. Wir sind selber überrascht, in welchem enormen Umfang sich offene Lösungen gestalten lassen. Tatsache ist, dass sich unser Denken über die Architektur von „TK-Lösungen" ändern muss. Die offene Technologie bringt einen völlig anderen Lösungsansatz mit sich:

- Basis der gesamten Architektur ist ein offenes Betriebssystem, dies wird vermutlich für die nächste Zeit Linux sein
- Auf diesem Betriebssystem wird ein zentrales Call-Routing/Registrar-System realisiert, das die Basis-Funktionsmerkmale der Lösung umsetzt. Das ist der Kern der Lösung
- Über offene API´s zu diesem Kern werden Applikationen mit dem Kern verknüpft, traditionell typisch sind Voice-Mail, IVR und ACD, in Zukunft werden Präsenz-Anwendungen und Kollaboration eine zunehmende Rolle spielen. In einer wirklich offenen Architektur eigentlich ja auch kein Problem
- Zentrales Merkmal der Offenheit ist, dass die einzelnen Applikationen nicht von einem Hersteller kommen müssen. Somit wächst der Druck auf alle Hersteller, ihre Applikationen zunehmend zu erweitern und zu verbessern. Wettbewerb ist nun einmal gut für den Anwender. Dies gilt auch für die Preisgestaltung. Standard-Applikationen werden in sehr kurzer Zeit völlig im Preis verfallen. Schon heute könnte Asterisk in mehr als 50% aller Projekte als IVR, Voice-Mail, UM und einfaches ACD-System die Kosten deutlich nach unten drücken.

Ist das der Untergang der traditionellen Hersteller? Die Antwort ist ein klares Nein. TK-Lösungen waren, sind und werden immer komplex sein. Mit dem Wandel zu weitergehenden Realzeit-Kommunikations-Lösungen wird sich das nicht ändern, im Gegenteil. Allerdings ergibt sich eine wesentliche Schwerpunkt-Verschiebung. Der zentrale Kern des Call-Routings verliert an Bedeutung, Stufe um Stufe wird dieser Bereich austauschbar sein (ist er eigentlich heute schon, siehe den SIP Express Router SER). Die Hersteller werden sich auf Anwendungen konzentrieren müssen. Und hier liegt so viel Potenzial, dass man eigentlich keine technischen Sorgen um die Zukunft der Hersteller haben muss.

Dies ist natürlich Theorie. In der Praxis bedeutet der Wandel, den wir hier erleben, einen Wechsel im Geschäftsmodell. Mit dem totalen Wechsel der Technik ändert sich der Bedarf an Entwicklung, an Vertrieb und an Support. Eine riesige Herausforderung, und es mag sein, dass dieser Herausforderung nicht jeder gewachsen sein wird. Allerdings haben die Hersteller Zeit. Weiterhin existiert eine erhebliche installierte Basis, die traditionelles Knowhow erfordert und weiterhin werden ja auch noch traditionelle Lösungen verkauft. Allerdings ist den wenigsten klar, wie schnell diese Verkäufe wegbrechen werden. Hier geben sich viele der trügerischen Illusion hin, dass es einen sanften Übergang geben wird. Dies sehen wir von ComConsult-Research nicht so. Der Umschwung auf offene Lösungen wird schnell und brutal erfolgen. Nach allen bekannten Mustern der Marktforschung befinden wir uns bereits über die Mitte von Phase 1 des typischen Life-Cycles hinaus. Dies deutet auf signifikante Verkaufsmengen in 2008 und einen totalen Umschwung im Sinne des Massenmarktes in 2009 hin.

Wie dramatisch ist diese Entwicklung für die Betreiber, ist deren traditionelles Knowhow nun nicht mehr gefragt, brauchen wir den Wechsel im Personal? Die Antwort ist ebenfalls ein klares Nein. Auch in Zukunft werden Realzeit-Kommunikations-Lösungen spezielle Elemente wie Rufnummerpläne, PSTN-Gateways, besondere Endgeräte usw haben. Hinzu kommt, dass die bisherigen Lösungen sehr komplex waren. Ich würde vermuten, dass jeder, der eine HiPath 4000 beherrscht, auch das Potenzial hat, die neue Welt ohne Probleme zu beherrschen. Allerdings ist ein Umdenken und eine Umschulung erforderlich. Die Nutzung der Vorteile einer offenen Kommunikationswelt kann nur erfolgen, wenn man die Elemente der offenen Welt wirklich beherrscht. Dazu gehören IP, Linux, XML usw. Es ist sicher sinnvoll, das „TK-Team" hier um Betriebssystem-Spezialisten anzureichern, die zum Beispiel die Themen Backup/Restore, Desaster-Recovery, Skalierbarkeit übernehmen. Das besondere an der notwendigen Weiterbildung ist aber, dass man sich hier Wissen aneignet, das weit über die TK-Welt hinaus von Bedeutung ist. Hier haben standardisierte Produkte und Technologien eben auch den Vorteil der Erweiterung der beruflichen Perspektiven.

Der traditionelle TK-Markt ist im Wandel. Dieser Wandel läuft viel schneller ab als viele angenommen haben. Jetzt ist die Zeit gekommen, in der sich Unternehmen dazu positionieren müssen. Wann und wie steigen Sie in diese Welt ein?

Noch einmal der Hinweis auf unseren Sonder-Kongress, der sich exklusiv diesem Thema widmet: das ComConsult SIP-Forum 2007, am 14. und 15. Mai in Frankfurt. Die Moderation werde ich übernehmen, Sie haben vielleicht diesem und einigen anderen Artikeln entnommen, dass ich mich momentan auf diesen Themenbereich konzentriere. Von daher freue ich mich, Sie in Frankfurt begrüßen zu können.

Ihr
Dr. Jürgen Suppan

Sonderveranstaltung

ComConsult SIP-Forum 2007

Die ComConsult Akademie veranstaltet vom 14. - 15.05.07 erstmalig ihr „ComConsult SIP-Forum 2007“ in Frankfurt.

Wenige Standards in der Geschichte der TK, der Netzwerke und der IT werden unsere Branche so verändern wie das Session Initiation Protocol SIP. Der Wechsel von Cisco und Siemens zu SIP mit dem CallManager 6 und der HiPath 8000 unterstreichen das genauso wie der Einstieg von Microsoft zusammen mit Nortel in diesen Markt.

Die Konsequenzen eines offenen Standards sind erheblich, auch wenn die Produkte von den traditionellen TK-Anbietern kommen:

- Ein zunehmendes Angebot offener Sprach- und Multimedia-Applikationen für ACD, IVR, UM und weitere Spezialanwendungen
- Freie Wahl von Endgeräten (abhängig von gewünschten Funktionsmerkmalen)
- Freie Wahl von Gateways
- Es entstehen standardisierte Entwicklungs-Umgebungen für Sonderlösungen: Cisco zeigt mit IPICS und der Integration von Funk, Sensoren, Sprache, Meldetechnik welchen gigantischen Umfang solche Lösungen haben können

In der näheren Analyse zeigen sich für nahezu alle Unternehmen die enormen Vorteile einer offenen Sprach- und Multimedia-Welt. Ein typisches Beispiel dafür ist Asterisk, der als offene Lösung nicht nur SIP-Telefonie implementiert sondern einen

umfassenden Baukasten für ACD, Queuing, Voice-Mail und Unified Messaging sowie für individuelle Entwicklungen bietet. Allein in der Ergänzung traditioneller TK-Lösungen durch Asterisk liegt ein hohes Potenzial an Funktionalität zu so geringen Kosten, dass alleine dieser Aspekt fast einer Revolution gleichkommt.

SIP ist ohne Frage eines der, wenn nicht das Megathema des Jahres 2007. Nach wie vor wird dabei insbesondere der Leistungsumfang von SIP weit unterschätzt. Auch so verbreitete Implementierungen wie Asterisk oder SER werden in ihrer Nutzbarkeit häufig falsch eingeschätzt.

Das ComConsult SIP-Forum 2007 ist unser Kongress des Jahres zum Thema des Jahres. Wir analysieren für Sie und stellen auf dem Forum vor:

- Die große SIP-Studie von ComConsult-Research wird vorgestellt
  - Was leistet SIP?
  - Was bedeutet Offenheit?
  - Wie offen sind die Lösungen der Hersteller?
- Wichtige Hersteller präsentieren ihre Strategie zu SIP:
  - Siemens erläutert Hintergründe und Zukunft der HiPath 8000
  - Cisco präsentiert wichtige Details zum Call Manager 6
  - Alcatel geht auf die Perspektiven eines offenen Standards im Zusammenhang mit gehosteten Lösungen ein
- Unser Labor präsentiert die Ergebnisse einer Reihe aktueller Untersuchungen
  - Wo steht Microsoft, wie tragfähig ist die Microsoft/Nortel-Lösung?
  - Wie lassen sich offene SIP-Lösungen um Applikationen von Drittherstellern ergänzen, was leisten Asterisk und co?
- Wir analysieren und präsentieren die Frage der Gestaltbarkeit zukünftiger Lösungen
  - Wie gestaltbar ist eine Linux-basierte TK-Installation?
- Wir berichten über laufende Projekte und die Sicht repräsentativer Anwender

Weitere Details zum Inhalt folgen in Kürze. Bedingt durch die Wahl eines zentralen Veranstaltungsortes in Frankfurt ist das Forum in der Teilnehmerzahl begrenzt, sichern Sie sich also rechtzeitig einen der begehrten Plätze.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-phase bis 31.03.2007

Anmeldung

ComConsult SIP-Forum 2007

Frühbucher-phase bis 31.03.2007

☐ Ich buche das
ComConsult SIP-Forum 2007
14.05. - 15.05.2007 in Frankfurt
zum Preis von € 1.590,-* zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

*gültig bis 31.03.07

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Aktueller Kongress

Netzwerk-Redesign Forum 2007

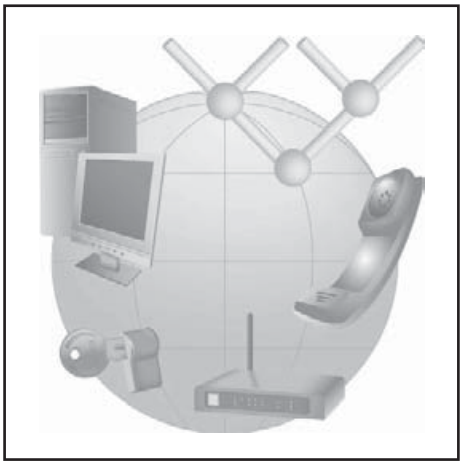
Die ComConsult Akademie veranstaltet vom 23. - 26.04.2007 ihren Kongress „Netzwerk-Redesign Forum 2007“ in Königswinter.

Wir stehen vor gravierenden Änderungen im Bereich der Netzwerk-Technologien und vor allem in den Applikations-Architekturen, die mit Netzwerken realisiert werden. Dies wird zu einem umfassenden Bedarf an Neukonfiguration über alle Layer des Referenzmodells führen.

Das Netzwerk-Redesign-Forum 2007 ist unsere zentrale Veranstaltung des Jahres 2007, die sich intensiv den Änderungen der Netzwerk-Technologien und dem damit verbundenen Einfluss auf das Design und den Betrieb der Netzwerke widmet.

ComConsult-Research hat eine große Markt- und Technologie-Analyse gestartet, die die Grundlage für das Netzwerk-Redesign-Forum 2007 bilden wird. Unter anderem werden wir auf folgende Entwicklungen eingehen:

- WAN-Konvergenz durch immer mehr Bandbreite
- Service-orientierte und Standort-neutrale Architekturen



- Von der Sprachkommunikation zur Kollaboration
- IP-Infrastrukturen im Wandel
- Sicherheits-Konzepte
- Quality of Service
- Wireless LAN: 11n und Mesh in der Analyse
- Auswahl neuer Netzwerk-Komponenten

Zögern Sie nicht und sichern Sie sich noch heute Ihren Platz auf der herausragendsten Veranstaltung diesen Jahres.

Am Donnerstag rundet das Netzwerk-Redesign Forum rundet sein Programm mit eintägigen Workshops ab. Diese sprechen hochaktuelle Themen an, die nicht in einem einstündigen Vortrag vermitteln werden können.

Bitte beachten Sie insbesondere auf den Workshop: Verkabelungstechnik: vom Kabel zum LWL-Multiplexer. Dieser Workshop hat den Charakter eines eigenen Mini-Kongresses. Sie werden auf den neuesten Stand zum Thema Verkabelung gebracht und gehen bei ausgewählten Themen, die sich in den letzten Monaten in den Projekten als wichtig dargestellt haben, in die Tiefe geführt.

Auch die beiden anderen Workshops zu SIP und Netzwerk-Sicherheit sprechen hochaktuelle Themen an und krönen die schon anspruchsvolle Veranstaltung mit einem weiteren Höhepunkt.

Die Moderation des Forums übernimmt Dr. Jürgen Suppan.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2007

Ich buche den Kongress
Netzwerk-Redesign Forum 2007

☐ vom 23.04. - 26.04.07 in Königswinter
inkl. Intensiv-Training am letzten Tag
☐ Thema 1: SIP
☐ Thema 2: Netzwerk-Sicherheit
☐ Thema 3: Verkabelungstechnik 2007
zum Preis von € 2.190,- zzgl. MwSt.

☐ vom 23.04. - 25.04.07 in Königswinter
ohne Intensiv-Training am letzten Tag
zum Preis von € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht Netzwerk-Redesign Forum 2007

Montag, den 23.04.2007

9:30 bis 11:00 Uhr

Zukünftige Entwicklung von Netzwerken und vernetzten Systemen in der Analyse - Studie unseres internationalen Labors in Christchurch

- Globale Trends in der Analyse
- Wohin treiben Apple, Cisco, IBM und Microsoft den Markt?
  - Zwischen Konsumer- und Enterprise-Geschäft
  - Kommunikation und Kollaboration
- Zukünftige IT-Architekturen und ihre Anforderungen an Netzwerke
  - Parallele versus hierarchische Systeme: wie real ist SOA
  - Sind Standort-neutrale Architekturen umsetzbar?
  - Was bedeuten hohe WAN-Bandbreiten?
- Konvergenz der Kommunikation in Lokalen Netzwerken
  - IP-Telefonie: auf dem Weg zu einem offenen Standard, Roadmap
  - Der Einfluss von IBM und Microsoft in der Analyse
  - Der Stellenwert von Open Source Software für Infrastrukturen
- Neue Anforderungen an IP-Infrastrukturen und das Design von Netzwerken
- Schlüsselthema Sicherheit
  - Was ist von der Cisco-Microsoft-Allianz zu halten?
- Empfehlungen

Dr. Jürgen Suppan, ComConsult Research

11:30 bis 12:30 Uhr

Das Session Initiation Protocol SIP und seine zukünftige Bedeutung in Netzwerken

- Die SIP-Grundidee
- Die Strategien von Avaya, Cisco, IBM, Microsoft, Siemens und die Folgen für den Markt
- SIP in der Praxis: wie sehen typische Lösungen aus?
- Compliance-Kriterien für offene Architekturen
- Wo stehen die Hersteller, wie offen sind die Produkte?
- SIP im Netzwerk: was bedeutet das?

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

14:00 bis 15:00 Uhr

Mesh-Netzwerke und die Struktur-Revolution: von WDS über IEEE 802.11s zu einem völlig neuen Konzept von Netzwerken

- Womit es harmlos begann: Wireless Distribution Services
- Der neue Distribution-Standard: IEEE 802.11s
- Auf dem Weg zur Revolution: weitergehende Maschenkonzepte
- Das Ziel: Universal Wireless Entity
- Diskussion: Anwendungsfälle und Bedarf
- Diskussion: Zeitskala

Dr. Franz-Joachim Kauffels, Unternehmensberater

15:30 bis 16:30 Uhr

Netzwerk-Redesign: Voice-Readiness und Quality of Service als Träger des Redesigns

- Migration zum Anschluss von Telefonen bei vorhandener Verkabelung
  - Anschlussmöglichkeiten PoE Switches, Power Hubs oder Steckernetzteilen
  - Telefon Switches
- Quality of Service im Redesign
  - Echtzeitdienste im LAN und ihre Anforderungen
  - Alternative Lösungsansätze
  - Generische Lösung versus QoS und benutzergruppen
  - Szenarien in der Diskussion
    - Überkapazität
    - Priorisierung
    - Bandbreiten-Limitierung
    - Einbindung der Access-Switches
- Wie umfangreich und aufwändig wird Einsatz und Betrieb von QoS bei
  - Streaming
  - Voice
  - Video
  - Produktionsumgebungen
  - Gebäudeautomatisierung
  - Überwachungs- und Zugangstechnik
- Monitoring von QoS und Einbindung ins Operating
- Wie kann der Nachweis von Qualität erfolgen
- Empfehlungen und Ausblick

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

16:30 bis 17:15 Uhr

Fixed Mobile Convergence: Realität oder Zukunftsmusik?

- Standards und Architekturen
- Erreichbarkeit unter einer Rufnummer und die technischen Konsequenzen
- Lösungen im Mobilfunknetz mit UMA und IMR
- PBX-basierte Lösungen
- WLAN-Integration
- Was leisten aktuelle Dual-Mode-Endgeräte mit WLAN-Adapter?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

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

Dienstag, den 24.04.2007 - Vormittag

9:00 bis 10:00 Uhr

Netztrennung

- Logische versus physikalische Netztrennung
- Warum Access Control Lists keine dauerhafte Lösung für die Sicherheit im LAN darstellen
- Kopplung zwischen getrennten Netzbereichen
- Virtual Routing als logische Konsequenz der VLAN-Trennung
- Ist MPLS im LAN eine praktikable Lösung? Für wen?
- Anforderungen an die Netzkomponenten

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

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause

10:00 bis 11:00 Uhr

IEEE 802.1X in der Analyse

- Ist IEEE 802.1X im gesamten Netz überhaupt praktikabel?
- Wo wird IEEE 802.1X wirklich gebraucht?
- Probleme beim Einsatz von 1X und IP-Telefonie
- VLAN-Zuordnung als Ergebnis der Authentifizierung
- Ist eine durchgängige Authentifizierungslösung im LAN und WLAN möglich? • Problematik Wake-on-LAN
- Welche Anforderungen müssen Authentifizierungsserver, Switches, IP-Telefone und Clients erfüllen, um in ein 1X-Konzept eingebunden zu werden?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:30 bis 12:30 Uhr

Network Access Control NAC in der Analyse

- Ziele
- Die Herausforderung: Integration von Netzwerk, Endgerät, Benutzer
- Framework-Architekturen im Vergleich
- Wer wird sich durchsetzen: die zentrale Rolle Microsofts
- Typische Probleme in der Umsetzung
- Ausblick und Empfehlungen

Dipl.-Ing. Markus Nispel, Enterasys Networks Deutschland GmbH

Programmübersicht Netzwerk-Redesign Forum 2007

Dienstag, den 24.04.2007 - Nachmittag

14:00 bis 15:30 Uhr
LAN-Designs 2007:
Vom Design zur Auswahl von Switch-Systemen

- LAN-Design 2007
  - Gigabit, 10 Gigabit: wo stehen wir
  - Anforderungen typischer Anwendungen
  - Trend bei Kosten und Produkten
  - Vollaktivierung kontra bedarfsorientierte Rangierung: was ist wirtschaftlicher?
- Auswahl der Übertragungskapazität / Bandbreite
- Mit oder ohne Stromversorgung gemäß IEEE 802.3af
- IP-Telefone und PCs kaskadieren?
- Attacken gegen den Switch und mögliche Schutzmaßnahmen
- Management-Integration

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

16:00 bis 17:00 Uhr
Industrial Ethernet

- Welche Wachstumsraten sind ind den nächsten Jahren im Industriebereich zu erwarten?
- Welche Netzstrukturen setzen sich in der Industrie durch: Stern, Ring, Linie?
- Wodurch unterscheiden sich die konzeptionellen Ansätze zwischen Büro- und Industriewelt?
- Warum ist die klassische 3-stufige Hierarchie häufig nicht geeignet?
- LWL vs. Kupfer in der Industrie
- Planungsbeispiele

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

15:30 - 16:00 Uhr Kaffeepause

Mittwoch, den 25.04.2007

9:00 bis 10:15 Uhr
IP-Redesign: IP-Infrastrukturen im Wandel

- Auswirkungen neuer „Anwendungen" im Netzwerk auf IP-Infrastrukturen
- IP-Telefonie und ihr Bedarf an IP-Adressen und -diensten
- IPv4 - jetzt doch ein Adressproblem?!
- Redesign des Adressraums: Konzepte
- IP-Dienste DNS und DHCP: akute Anforderungen und Lösungswege
- IP und Mobilität: Bedarf, Szenarien, Wege zur Lösung
- IPv6 - Status quo, möglicher Nutzen, IETF-Aktivitäten
- Was bedeutet IPv6-Readiness?
- Ausblick und Empfehlungen

Dipl.-Inform. Oliver Flüs,
ComConsult Beratung und Planung GmbH

10:15 bis 11:00 Uhr
WAN-Optimierung

- Anpassung von Applikationen an WAN-Bedingungen
- Einsatz von Traffic Optimizern
- QoS im WAN
- WAN-Bandbreitenmanagement bei Integration von Daten, Voice und Video im WAN

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

11:30 bis 11:50 Uhr
Hersteller-Präsentationen WAN-Optimizer

11:50 bis 12:35 Uhr
Trends in der WAN-Planung und Ausschreibung

- Multi- vs. Single-Providerlösungen
- Sinnvolle Kombination von MPLS und IPsec
- Governance-Problematik bei internationalen Konzernen
- WAN-Verschlüsselung: wann, wie, wo?
- Backup-Konzepte für WAN

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

11:00 - 11:30 Uhr Kaffeepause
12:35 - 14:00 Uhr Mittagspause
15:15 - 15:30 Uhr Kaffeepause

14:00 bis 15:15 Uhr
WLAN: Wohin geht der Weg?

- Leistungspektrum und Funktionsweise der Übertragungstechniken in IEEE 802.11n
- Strategien der Hersteller und Positionierung von IEEE 802.11n im Enterprise-Bereich
- Sonderrolle des 5-GHz-Bereichs
- Was werden IEEE 802.11k/r/v leisten?
- Evolution im Controller-basierten Design
- Planungs- und Migration zu IEEE 802.11n

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

15:30 bis 16:30 Uhr
Optimierung des Konfigurations-Managements von Netzwerken

- Reichen technologieorientierte Element-Manager wirklich aus, um Change Management durchzuführen?
- Ist die Geschwindigkeit von Konfigurations-Changes ausreichend, um eine geregelte Service-Erbringung sicher zu stellen?
- Ist die Zuverlässigkeit der Change-Durchführung ausreichend?
- Wo liegt das Potential, um das Risiko eines Service-Ausfalls zu minimieren?
- Werden Changes Kosten- und Zeitoptimiert durchgeführt?
- Sind die eingesetzten Methoden Berichts- und Audit-fähig?
- Skalieren die Verfahren hinreichend, um alle Netzwerk-Komponenten im Unternehmen zu erfassen?
- Ist die Reproduzierbarkeit von Changes im Netzwerk gewährleistet?
- Folgt die Change-Planung und Durchführung der definierten Unternehmensprozesse?
- Können alle Änderungen dokumentiert, gespeichert und präzise nachgewiesen werden?
- Werden gesetzliche Vorgaben im Rahmen von Nachweispflichten wirklich erfüllt?
- Welche Technologien werden abgedeckt, welche bilden Ausnahme in bestehenden Verfahren?
- Wie lässt sich NCCM in übergeordnete Workflow und Prozess-Steuerungswerkzeuge einbinden?

Ralf Horstmann,
ComConsult Kommunikationstechnik GmbH

Donnerstag, den 26.04.2007 - Ein-Tages-Intensiv-Trainings/Workshops - Beginn 9:00 Uhr (alle parallel)

Intensiv-Training 1: SIP in der Analyse

Dipl.-Inform. Petra Borowka,
Unternehmensberatung Netzwerke UBN

Intensiv-Training 2: Netzwerk-Sicherheit und IEEE 802.1X

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

Intensiv-Training 3: Verkabelungstechnik 2007 mit Spezialthema LWL-Multiplexer

Dipl.-Ing. Hartmut Kell, Dr. Frank Imhoff, Dr. Michael Wallbaum,
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!

Security-Kongress des Jahres

IT-Sicherheits-Forum 2007

Die ComConsult Akademie veranstaltet in Zusammarbeit mit der GAI NetConsult unter der fachlichen Leitung von Dipl.-Inform. Detlef Weidenhammer vom 07.05. - 10.05.07 ihren Kongress „IT-Sicherheits-Forum 2007“ in Königswinter.

Das Programm besteht aus Seminaren, Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und interaktiver Erarbeitung von Schutzszenarien. Das Forum verbindet damit in idealer Weise die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Als Schwerpunktthemen sind in diesem Jahr vorgesehen:

- Welche neuen Bedrohungen erwarten uns in 2007?
- Windows Vista unter Sicherheitsaspekten
- Content-Security: Umgang mit gefährlichen Inhalten

- Sicherheit in Automatisierungs- und Prozesskontrollsystemen (SCADA)

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 auch Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese in Vor- und Nachmittagssitzungen parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Die fachliche Leitung diese Kongresses übernimmt Detlef Weidenhammer. Er 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.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult
IT-Sicherheits-Forum 2007

☐ Ich buche den Kongress
ComConsult
IT-Sicherheits-Forum 2007
vom 07.05. - 10.05.07 in Königswinter
inkl. Tutorium am ersten Tag
(bitte wählen Sie ein Thema ------->)
(bitte wählen Sie zwei Workshops ------>)
zum Preis von € 2.190,- zzgl. MwSt.

☐ vom 08.05. - 10.05.07 in Königswinter
ohne Tutorium am ersten Tag
zum Preis von € 1.790,- zzgl. MwSt.
(bitte wählen Sie zwei Workshops ------>)

☐ mit Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“ zum Sonderpreis von nur € 338,-

Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

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

Tutoriumauswahl

☐ Thema 1

☐ Thema 2

☐ Thema 3

Workshopauswahl

vormittag	nachmittag
☐ Workshop 1	☐ Workshop 1
☐ Workshop 2	☐ Workshop 2
☐ Workshop 3	☐ Workshop 5
☐ Workshop 4	☐ Workshop 6

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht IT-Sicherheits-Forum 2007

Montag, 07.05.07 Tutorien - bitte wählen Sie ein Tutorium auf der Folgeseite aus!!

Alle Tutorien finden parallel statt und starten um 09:30 Uhr und enden gegen 17:30 Uhr

Tutorium 1: Prozessorientiertes IT-Sicherheitsmanagement mit ITIL

Interaktive Erarbeitung mit den Teilnehmern

- **IT-Sicherheitsmanagement im Unternehmen**
  - Ziel, Komponenten, Hindernisse, Nutzen?
- **ITIL: die Vorstellung**
  - Entstehung und Struktur
  - Prozesse im Überblick
- **Der Prozess ITIL Security Management**
- **IT-Sicherheitsmanagement in den ITIL-Kernprozessen**
- **ITIL-Sicherheitsmaßnahmen**
  - Darstellung der Maßnahmen in den Prozessteilen • Control • Plan • Implement • Evaluate • Maintenance • Report
- **Koexistenz mit anderen IT-Sicherheitskriterien**
  - IT-Grundschutz
  - ISO 17799 / ISO 27001
  - ISO 13335 • CoBIT

Christian Aust, .consecco

11:00 - 11:30 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Tutorium 2: Sicheres Netzwerk-Management

Live-Demos und Beispiele aus komplexen Umgebungen

- **SNMP**
  - Sicherheitsprobleme und Gegenmaßnahmen
- **SNMPv3**
  - Architektur und Konfiguration
  - Wann SNMPv3 eingesetzt werden muss und wann es nicht eingesetzt werden sollte
- **Device-Zugriff**
  - SSH vs. Telnet, Arbeit mit Jumphosts, das Problem Web-Interfaces, sicherer Konsolenzugriff
- **Sichere Konfigurations- und Image-Verwaltung**
  - Integritätsprüfung von Konfigs, wichtige Tools (RANCID et.al.)
- **Logging und Log-Auswertung**
  - Protokolle & Formate (BSD syslog, syslog-ng, Windows Eventlog), wichtige Tools
- **Revisionsanforderungen und rechtliche Aspekte**

Enno Rey, ERNW Netzwerke GmbH

Tutorium 3: Information Security Management

von A(udit) bis Z(ertifizierung)

- **Einführung**
  - Der Information-Security-Management-Prozess
  - Strategie, Konzeption, Umsetzung, Betrieb, Management
- **Standards**
  - ISO 27001
  - Grundschutzhandbuch
- **Security Policy**
  - Vorgaben, Umfang, Vorgehen bei Erstellung und Umsetzung
- **Risikoanalyse und Sicherheitskonzept**
  - Bestandsaufnahme, Schutzbedarfsfeststellung, Bedrohungsanalyse
- **Business Continuity Management & Emergency Response**
  - Notfallkonzept und -planung, Sicherheitsvorfälle
- **Umgang mit Sicherheitsvorfällen**
  - Management von Vorfällen, organisatorische Umsetzung, Business Continuity

Jörg Volker, Secorvo Security Consulting GmbH

Dienstag, 08.05.07

9:30 Uhr - 09:45 Uhr
Begrüßung / Übersicht

Detlef Weidenhammer, GAI NetConsult GmbH

9:45 Uhr - 10:30 Uhr
Vista unter Sicherheitsaspekten - Mehrwerte und Risiken?

- User Account Control (UAC) - eine gute Funktionalität, jedoch mit Schwachstellen?
- Bitlocker - tatsächlich eine Alternative im Bereich der Festplattenverschlüsselung?
- Gruppenrichtlinien - zentral Sicherheit verbreiten!
- Weitere „Kleinigkeiten“ wie driver signing, Netzwerk, Firewall und Defender, protected mode beim IE7

Michael van Laak, ComConsult Beratung und Planung GmbH

10:30 Uhr - 11:15 Uhr
Informationsdiebstahl durch Schadsoftware

- Funktionsweise und Infektionswege von Schadsoftware
- Vorbeugende Massnahmen
- Detektionsmechanismen
- Reaktionskonzepte

Tom Fischer, BFK GmbH

11:45 Uhr – 12:30 Uhr
Neue Gefahren aus der Sicht eines Antivirus-Herstellers

- Derzeitiger Stand der Bedrohungen
- Wie kann man sich vor „Targeted Attacks“ schützen?
- Umgang mit 0-day Exploits
- Wachsende Compliance-Anforderungen bei komplexeren Sicherheitsrisiken

Wolf-Dieter Jahn, mcAffee

12:30 Uhr - 13:00 Uhr
Podiumsdiskussion
„Neue Gefahren durch Malware“

14:30 Uhr - 15:15 Uhr
Netzzugangskontrolle und Desktop Integrity

- Port-basierte Zugangskontrolle mit IEEE 802.1X und EAP
- Rolle von Direcory Service und Identity Management
- Zuweisung von VLANs und ACLs über RADIUS
- Cisco NAC und Microsoft NAP in der Analyse
- Was ist von Trusted Network Connect (TNC) zu erwarten?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:15 Uhr - 16:00 Uhr
MPLS Sicherheit

- Sicherheitsaspekte beim Einsatz von MPLS (eigener Betrieb oder „Kauf eines VPN-Produkts“)
- Rahmenparameter und mögliche Sicherheitsmassnahmen
- neue (Ethernet-) Dienste und Sicherheitsprobleme
- Vorstellung einer Checkliste zur Bewertung

Enno Rey, ERNW Netzwerke GmbH

16:30 - 17:15 Uhr
Sicherheit sensibler Daten

- Bedrohungen für sensible Daten im Unternehmen
- Verschiedene Lösungsansätze
- Vor- und Nachteile der vorgestellten Lösungsansätze
- Handlungsempfehlungen

Stefan Strobel, cirosec GmbH

17:15 - 18:00 Uhr
Sicherheitsfaktor Mitarbeiter: Aufbau eines Personnel Security Lifecycles

- Bedeutung des Mitarbeiters für die IT-Sicherheit
- Steuerung, Motivation, Maßnahmen
- Bestandteile des Personnel Security Lifecycles
- Projektbeispiele

Christian Aust, .consecco

11:15 - 11:45 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Mittwoch, 09.05.07 Praxis-Workshops - bitte wählen Sie 2 Workshops auf der Folgeseite aus!!

9:00 Uhr - 12:30 Uhr

- **Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?**
- **Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen**
- **Workshop 3: Interne Compliance Audits**
- **Workshop 4: Rechtliche Aspekte der Mobile Security**

14:00 Uhr - 17:30 Uhr

- **Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?**
- **Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen**
- **Workshop 5: IT-Security Best Practice Top-10 Tips und Tricks in der Diskussion**
- **Workshop 6: Neues über VoIP-Sicherheit**

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause

Programmübersicht IT-Sicherheits-Forum 2007

Donnerstag, 10.05.07

9:00 Uhr - 10:00 Uhr

SCADA- und Automatisierungssysteme: Neue Bedrohungen durch fortschreitende Vernetzung

- Bedrohungen durch Konvergenz von Prozessleittechnik und klassischer IT
- ISMS-Ansatz für SCADA- und Automatisierungssysteme
- Richtlinienbeispiele, kommende Standards (IEC-62443, ISA SP99,..)
- Schutzmaßnahmen bei der Kopplung mit Office- und externen Netzen

Stephan Beirer, GAI NetConsult GmbH

10:00 Uhr - 11:00 Uhr

IT-Sicherheit in der Produktion: Der Status quo in deutschen Industrieunternehmen

- Schutzziele und Schadenspotenziale in der Produktion
- Die tatsächlichen Bedrohungen
- Der Sicherheitsstand heutiger Automatisierungssysteme
- Ausblick: Was muss getan werden, um den Zustand zu verbessern?

Ralph Langner, Langner Communications AG

11:30 Uhr - 12:30 Uhr

Bluetooth - Ein Risiko für das Unternehmen?

- Bluetooth Usage scenario
- Risiko für das Unternehmen? Mythen und Fakten
- Live -Demo einer Attacke
- Pin cracking

Thierry Zoller, n.runs AG

13:45 Uhr - 14:45 Uhr

Ermittlungsstrategien nach Systemeinbrüchen (IT-Forensik)

- Grundregeln und Abläufe bei der Ermittlung
- Analyseansätze für die Ermittlung
- Sicherstellung und Umgang mit Beweismitteln
- Werkzeuge für die Beweismittelsicherung und Analyse

Sebastian Krause, HiSolutions AG

14:45 Uhr - 15:45 Uhr

Notfallplanung unter dem Gesichtspunkt der Beschlagnahme

- Fälle von IT-Beschlagnahme in Unternehmen
- Rechtliches: Der Durchsuchungs- und Beschlagnahmebeschluss
- Integration in das Notfallkonzept (Merkblätter, technische Vorsorge, usw.)
- Folgen bei vorgenommener Beschlagnahme

Holm Diening, GAI NetConsult GmbH

15:45 Uhr - 16:00 Uhr

Zusammenfassung und Schlusswort

Detlef Weidenhammer, GAI NetConsult GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 13:45 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

Tutorien: Bitte kreuzen Sie *ein* Tutorium-Thema an!

1 **Tutorium 1: Prozessorientiertes IT-Sicherheitsmanagement mit ITIL - Interaktive Erarbeitung mit den Teilnehmern**

2 **Tutorium 2: Sicheres Netzwerk-Management - Live-Demos und Beispiele aus komplexen Umgebungen**

3 **Tutorium 3: Information Security Management von A(udit) bis Z(ertifizierung)**

Praxis-Workshops: Bitte kreuzen Sie *zwei* Workshops an (einen vormittags, einen nachmittags)

9:00 - 12:30 Uhr

1 **Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?**

- Freiheitsgrade in IEEE 802.1X: Wo unterscheiden sich die Hersteller?
- Was ändert sich bei Microsoft Vista, Longhorn hinsichtlich IEEE 802.1X?
- Herstellerkonzepte zur Prüfung der Desktop Integrity
- Migrationskonzepte für IEEE 802.1X
- Aufbau von Sicherheitszonen
- Umgang mit Geräten, die IEEE 802.1X nicht unterstützen
- Behandlung von Gastzugängen

Dr. Simon Hoff, ComConsult Beratung und Planung

2 **Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen**

- Einführung
- Buzzword Bingo: Ajax, RIA, Mashups und Co.
- Angriffe im Web 2.0 Umfeld
- Typische Sicherheitslücken in Ajax-Webanwendungen
- Cross-Site-Scripting 2.0
- Verfall der Same Origin Policy
- Javascript Malware
- Umgehen von DNS-Pinning
- Cross-Site-Request-Forging
- Zugriff auf das Intranet aus dem Internet
- Prüfung und Sicherung moderner Anwendungen
- Sind Ajax-Anwendungen über WAFs zu sichern?
- Wie verhalten sich klassische Web-Scanner bei Ajax-Anwendungen?

Björn Fröbe, GAI NetConsult

3 **Workshop 3: Interne Compliance Audits**

- Einführung • Arten von Audits
- Anwendungsgebiete von internen Audits
- Erfüllung gesetzlicher Auflagen • Interne Audits im Rahmen der ISO 27001/17799 • Erhebung von Security Metrics • Grundlagen
- Nachvollziehbarkeit, Vergleichbarkeit • RIDE und DRIVE Ansatz
- Vorgehensweisen • Erhebung durch Fragebögen
- Gestaltung und Auswertung der Fragebögen • Anwendungsgebiete
- Durchführung von Audits vor Ort
- Objektivitätsgrundsatz, Rolle des Auditors
- Erstellung eines Auditplans, Bestimmung von Stichproben
- Verfolgung von Audit-Trails • Audit-Bericht
- Fazit

Holm Diening, GAI NetConsult

4 **Workshop 4: Rechtliche Aspekte der Mobile Security**

- Datenschutz bei Smartphones und PDAs
- Schutz von Betriebsgeheimnissen • Verschlüsselungspflicht
- bei Speicherung auf mobilen Geräten? • bei E-Mail-Kommunikation auf mobilen Geräten? • Virenschutz auf mobilen Geräten
- Schutz gegen Bluejacking und Hacking von mobilen Geräten
- Aufbewahrungspflichten mobil gespeicherter Inhalte
- Neue Impressumspflichten bei SMS und Mail?
- Gefahren von mobilen Bezahlsystemen • Überwachungsmöglichkeiten
- des Inhalts mobiler Geräte • des Ortes mobiler Geräte

Ulrich Emmert, esb Rechtsanwälte

14:00 - 17:30 Uhr

1n **Workshop 1: Was leisten Herstellerlösungen zur Netzzugangskontrolle?**

2n **Workshop 2: (Un)sicherheit im Web 2.0 mit Live-Demos von Angriffen**

5 **Workshop 5: IT-Security Best Practice Top-10 Tips und Tricks in der Diskussion**

- Vorgesehene Themen sind: • Zentrale Lösungen zur Content-Security
- Durchführung von Security Audits • Aufbau einer Notfallplanung
- Aufbau einer ISMS-Lösung • Rechtsaspekte zur Archivierung von E-Mail
- Rechtsaspekte zu VoIP

Holm Diening, GAI NetConsult
Detlef Weidenhammer, GAI NetConsult
Ulrich Emmert, esb Rechtsanwälte

6 **Workshop 6: Neues über VoIP-Sicherheit**

- VoIP-Verschlüsselung: Erfahrungen und neueste Entwicklungen
- Probleme und Tücken beim Einsatz von IEEE 802.1X im Zusammenhang mit IP-Telefonen
- Für und Wider von logischer Netztrennung für VoIP im LAN
- Welche Kombinationen von VoIP-Sicherheitsmechanismen sind sinnvoll? Für wen?

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

Zweitthema

NCCM als Erfolgsgarant für den Netzwerkbetrieb

Fortsetzung von Seite 1

Ralf Horstmann ist seit mehr als 15 Jahren als IT Berater bei der ComConsult Kommunikationstechnik GmbH beschäftigt und heute in der Position des Abteilungsleiter IT Enterprise Management für die Planung und Umsetzung komplexer und hochintegrierter IT Enterprise Management Lösungen verantwortlich. Sein Aufgabenfeld umfasst von der fundierten herstellerneutralen Beratung über die Konzeptionierung bis zur Projektleitung und Implementierung ein breites Spektrum und bildet die Grundlage für die erfolgreiche Umsetzung vieler nationaler und internationaler IT Projekte.

Sebastian Ahrens ist Consultant für den Bereich IT Enterprise Management bei der ComConsult Kommunikationstechnik GmbH. Zu seinem Aufgabenbereich zählen die Analyse und Implementierung von Business-Service-Management, Netzwerk-Management sowie Change und Configuration Management Lösungen.

Das automatisierte NCCM unterstützt alle Unternehmen bei der Bewältigung der großen Herausforderungen aus den vier Bereichen Technik, Sicherheit, Unternehmen und Gesetzgebung. Aus technischer Sicht muss ein großes heterogenes Inventar von Netzwerkkomponenten verwaltet werden; der Netzbetrieb muss eine Datenkompromittierung verhindern und sicher durchgeführt werden. Aus unternehmerischer Sicht müssen Arbeitsabläufe automatisiert, standardisiert und gestrafft werden; aus rechtlicher Sicht müssen Unternehmen eine wachsende Zahl von Vorgaben, Richtlinien und Gesetzen einhalten, die weitgehende Auswirkungen auf den Infrastrukturbetrieb haben.

Change- und Configuration-Management der aktiven und managebaren Netwerkkomponenten ist deshalb für alle Unternehmen interessant, unabhängig davon in welcher Branche sie tätig sind oder in welcher aktuellen unternehmerischen Situation sie sich befinden.

Technische Anforderungen

Aktuell müssen vor allem große Unternehmen im Zuge der Internationalisierung oder bei Firmenzusammenschlüssen eine kaum überschaubare Menge an Netzwerkkomponenten unterschiedlichster Hersteller warten und betreiben. Verschiedene Hersteller-spezifische Werkzeuge erleichtern zwar die Administration und Verwaltung der herstellereigenen Komponenten, sie unterstützen Produkte anderer Hersteller aber nur begrenzt oder überhaupt nicht. Dadurch werden die Unternehmen gezwungen mehrere Werkzeuge einzusetzen oder die Verwaltung der Geräte manuell vorzunehmen.

Der Einsatz unterschiedlicher Software-Tools erleichtert dabei die Administration von Teilen der Infrastruktur, kann diese aber nie komplett abdecken und erfordert weitere manuelle Vorgehensweisen. Zudem lassen sich die Software-Produkte verschiedener Hersteller nicht untereinander integrieren, so dass Insellösungen bei der Verwaltung von Netzwerkkomponenten entstehen.

Der manuelle Verwaltungsansatz ist noch weniger Erfolg versprechend. Bei entsprechend großen Netzwerken muss ein Mitarbeiter allein für die Verwaltung der Komponenten abgestellt werden, um notwendige Updates, Konfigurationen oder Passwort-Wechsel durchzuführen. Der Einsatz von Skripten, die von den Mitarbeitern aus der Not erstellt wurden und die Effizienz steigern sollen, verschleiert die grundlegende Problematik und ist nicht zielführend. Die verwendeten Skripte sind nicht standardisiert, schlecht dokumentiert und müssen nach Änderungen in der Infrastruktur aufwendig angepasst werden. Im schlimmsten Fall findet in der IT-Abteilung kein Know-How-Transfer statt und sobald der zuständige Mitarbeiter seine Position wechselt, ist die hinterlassene Skript-Sammlung unbrauchbar.

Der potenzielle Schaden für die Unternehmen ist offensichtlich und Studien belegen mehr als 60% der Netzwerkausfälle oder Performanceprobleme sind auf Fehlkonfigurationen zurückzuführen (Enterprise Management Associates, 2005), die im manuellen Ansatz hauptsächlich durch die Mitarbeiter verursacht werden. Diese Schäden sind unnötig und werden durch ein konsequentes NCCM verhindert, das an dieser Stelle als zentrales, standardisiertes und vor allem herstellerunabhängiges Werkzeug einzusetzen ist.

Sicherheits Anforderungen

Bei steigender Vernetzung und immer größerer Abhängigkeit von der Unternehmens IT, müssen alle für kritische Geschäftspro-

zesse notwendigen Daten und die Zugänge zu diesen Informationen immer besser abgesichert werden. Unternehmens-Netzwerke sind immer häufiger ausgefeilten Angriffen ausgesetzt. Zero-Day Exploits, eine Flut von Trojanern, Würmern und Viren stellen eine zunehmende Bedrohung für IT Services dar, der Schaden kann verheerend sein.

Gegenmaßnahmen, wie die Isolation wichtiger Server und Datenbanken, scheitern häufig an den hohen manuellen Aufwänden die entstehen, wenn zur Schadensbegrenzung Netzwerk-Komponenten gezielt umkonfiguriert werden müssen. NCCM ermöglicht es, komplexe Notfallkonfigurationen vorzuhalten und diese automatisiert innerhalb von Minuten flächendeckend zum Einsatz zu bringen und so größeren Schaden abzuwenden.

Aber auch einfache sicherheitsrelevante Maßnahmen wie eine Passwort Alterung auf Netzwerk Komponenten lassen sich mit NCCM umsetzen. Viele Unternehmen schreiben den regelmäßigen Wechsel administrativer Passwörter vor, die Umsetzung scheitert häufig schlichtweg am erforderlichen hohen Arbeitsaufwand, so dass Passwörter selbst nach Jahren unverändert bleiben.

Die Möglichkeit, über NCCM proaktive Maßnahmen zur Steigerung der Unternehmenssicherheit zu implementieren, verhindert nicht nur finanziellen Schaden, sondern kommt dem Unternehmen auch in anderen Bereichen zugute und steigert das Vertrauen der Anwender in die IT.

Unternehmerische Anforderungen

Für das Unternehmen ergeben sich darüber hinaus noch viel weiter reichende Vorteile. Die laufende Ausrichtung der IT an Geschäftsprozesse erfordert Flexibilität, Schnelligkeit und Zuverlässigkeit bei der Administration. Neue Technologien, wie SOA und Webservices, setzen ein stabiles Netzwerk voraus, in dem Fehler in kürzester Zeit behoben werden können. NCCM Lösungen bieten hierfür entsprechende Automatismen an. So ist es möglich, Konfigurationen der Netzwerk-Komponenten zu überprüfen und Abweichungen von einem definierten Standard automatisiert zu korrigieren. Ist eine fehlerhafte Komponente identifiziert, kann in wenigen Sekunden aus der Historie eine lauffähige Konfiguration rekonstruiert werden. Erstmals werden IT-Abteilungen in die Lage versetzt das Rollout neuer Komponenten zu planen und sofort nach Einbindung in das Netzwerk eine vorgefertigte getestete Konfiguration einzuspielen.

Damit ist es möglich flexibel und schnell auf Änderungen im Unternehmen zu reagieren und ein Höchstmaß an Sicherheit bei der Umsetzung zu erreichen.

Rechtliche Anforderungen

Von außen werden zudem umfangreiche Anforderungen an die Unternehmen durch die Gesetzgeber gestellt. Basel-II, SOX, Solvency II und KonTraG sind bekannte Schlagworte, aber wie wirken sich die Gesetze und Verordnungen genau aus und für wen sind sie gültig?

Basel-II soll das Risiko der Kreditwirtschaft eindämmen und führt ein Rating für alle Kreditnehmer ein: sowohl Unternehmen, Staaten als auch Privatleute. Für das Rating werden nicht nur finanzielle Unternehmensdaten verwendet, sondern auch das operationelle Risiko bewertet. Die Spanne der Bewertungsfaktoren ist weit und fängt bei der Kompetenz der Mitarbeiter oder des Managements an. Für die Unternehmung unverzichtbare technische Einrichtungen liegen am anderen Ende der Bandbreite. Der nachweisbar sichere Betrieb einer Netzwerkinfrastruktur ist deshalb unbedingt positiv auf das Rating des jeweiligen Unternehmens anzurechnen. Diese durch Agenturen oder Banken durchgeführte Risikobewertung bestimmt entscheidend die Kreditwürdigkeit und den Zinssatz. Die aus EU Richtlinien entstandenen Regelungen werden spätestens seit dem 1. Januar 2007 europaweit angewendet.

Solvency-II regelt die Höhe des zurückzuhaltenden Kapitals von Versicherungsgesellschaften und ist in einem EU-Kommissionsprojekt entstanden. Für Deutschland ist die Umsetzung im Zeitraum 2008 bis 2010 geplant und fordert von den Versicherungen ein adäquates Risiko-management ein. Die IT-Abteilungen müssen dafür aktuelle Daten schnell und sicher liefern, um zuverlässige Reports und Statistiken zu erstellen. Die Sicherstellung der Datenkonsistenz und -integrität ist dabei ebenso unerlässlich, wie eine stabile und sichere Infrastruktur zur Datenlieferung.

Sarban-Oxley (SOX) ist ein US-amerikanisches Gesetz, in dem die Bilanzerstellung börsennotierter Unternehmen sowie deren Töchtergesellschaften im Ausland verbindlich geregelt wird. In Section 404, “Documenting and Evaluating Controls over Financial Reporting”, werden Unternehmen verpflichtet, die Unternehmensprozesse zu beschreiben in denen Zahlen für die Finanzberichterstattung entstehen. Diese Prozesse müssen mit Kontrollen hinterlegt werden, die das Risiko eines falschen Bilanzausweises minimieren sollen. Daraus ergibt sich in Konsequenz, dass die IT-Infrastruktur, in der Finanzdaten verarbeitet werden, so zu unterhalten ist, dass alle IT-Prozesse sowohl dokumentiert als auch nachweislich überprüfbar sind. Auch wenn ein Unternehmen selbst keine Tochtergesellschaft in den USA unterhält, können sich aufgrund von Geschäftsbeziehungen zu amerikanischen Partnern Nachweispflichten ergeben.

Ziel des **Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG**, seit Mai 1998 in Kraft) ist es, die Corporate Governance in deutschen Unternehmen zu verbessern. Das KonTraG ist kein eigenständiges Gesetz, sondern erweitert vorrangig sowohl das Akt-Gesetz als auch das HGB. Die Vorschrift, ein unternehmensweites Früherkennungssystem für Risiken einzuführen und zu betreiben, sowie Aussagen zur Risiken und Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen, ist Kern der Erweiterungen. Unternehmensleitungen und Vorstände werden nach § 91 Abs. 2 des AktG verpflichtet „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“.

Zusammenfassend fordern diese Gesetze und Vorschriften von allen Unternehmen ein geeignetes Risiko-Mangement und nachvollziehbare Prozesse zusammen mit überprüfbarer Dokumentation und Nachweispflichten. Der fundamentale Bestandteil aller Unternehmen und Basis aller IT Dienste ist die Netzwerkinfrastruktur mit ihren aktiven Komponenten, deren Verwaltung und Management über ein ausgereiftes NCCM gelöst werden muss. Auf die Kernfragen „Wer hat wann was gemacht?“, „Wer hat wen zu welchem Zeitpunkt dazu autorisiert?“ und „Wer hat wann die Änderung geprüft ?“ kann nur eine zentrale audit-fähige Verwaltung aller Komponenten die Antworten geben.

Funktionalität

Aus der Summe der aktuellen und zukünftigen Anforderungen haben die verschiedenen Hersteller im NCCM-Feld eine Vielzahl an Produkten und Lösungen entwickelt. In der grundlegenden Architektur sind die Produkte zwischen dem heterogenen Netzwerk und dem übergeordneten Netzwerkmanagement und Servicemanagement einzuordnen. (siehe Abbildung 1)

Gemeinsam sind grundlegende Funktionalitäten:

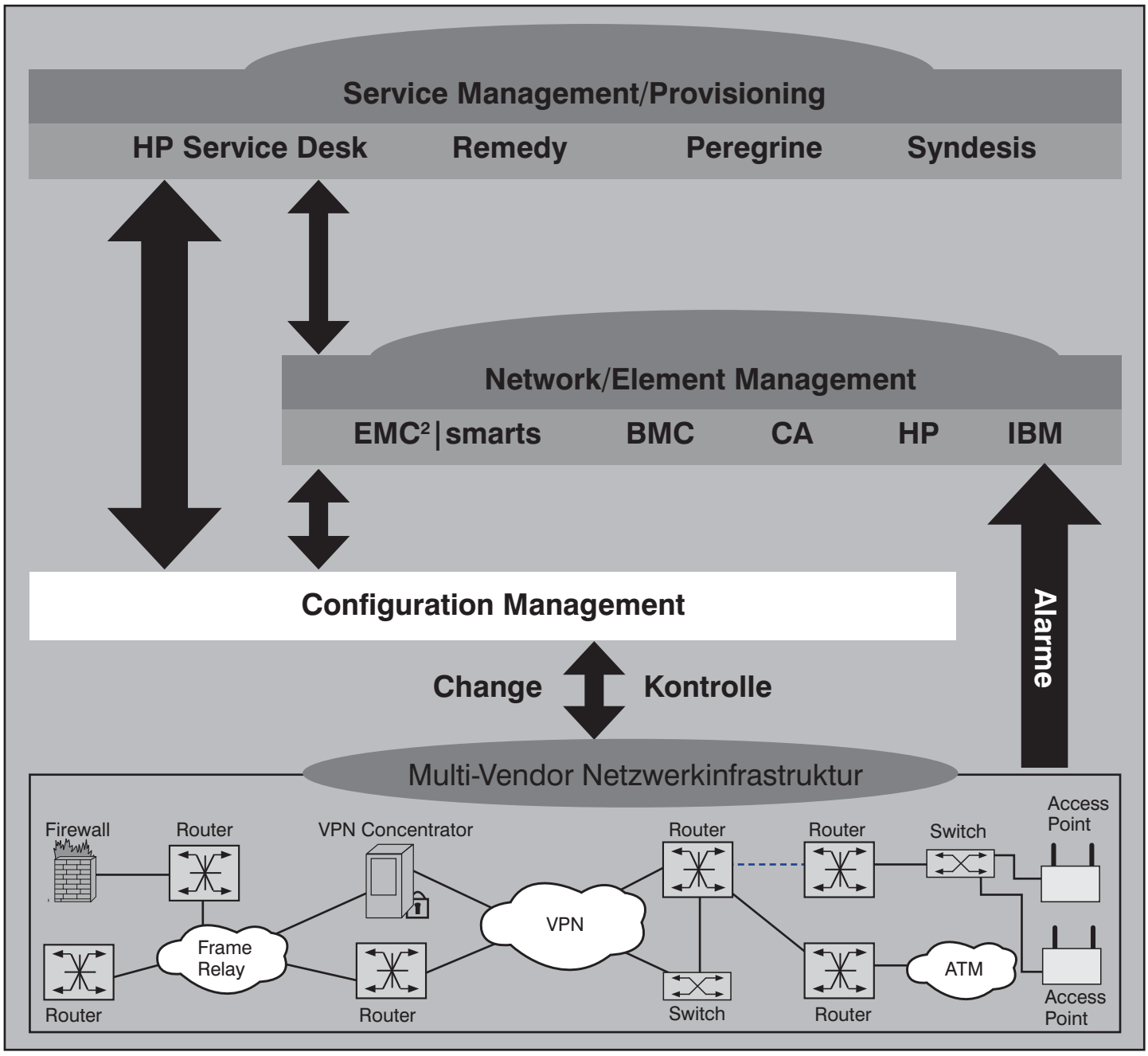


Abbildung 1: Einordnung in die Netzwerkinfrastruktur

- Hersteller-übergreifende Konfigurationsverwaltung und Historisierung der aktiven Netzwerkkomponenten
- Erkennung, Überwachung und Dokumentation von Konfigurationsänderungen im Netzwerk-Umfeld
- Erkennung der Abweichungen von Standard-Konfigurationen mit Dokumentation und Historisierung (baseline)
- Regelbasiertes, automatisiertes Erkennen von abweichenden Konfigurationen
- Historisierung von Änderungen
- Integration/Kopplung für die marktführenden System-Management-Werkzeuge (HP Openview, Tivoli NetView, Micromuse, EMC-Smarts etc.)
- Reporting-Funktion zur Nachweisbarkeit der Einhaltung gesetzlicher Richtlinien (compliance reports)

Zusätzliche Funktionen, die den Mehrwert eines NCCM-Produkts ausmachen, werden von den Herstellern unterschiedlich implementiert und sind nicht in jedem Produkt verfügbar:

- teilweise automatisches Zurücksetzen abweichender Konfigurationen (self healing, policy-based)
- Installation und Konfiguration von Neu-Geräten (zero touch install)
- Ausgefeilte Rechte-, Rollen- und Benutzerkonzepte, die Antworten auf die Fragen „wer?, was?, wann?“ geben
- Workflows mit Freigabekonzepten, Automation, Kalenderfunktionalität und Wartungsfenstern
- Automatische Verteilung von Änderungen (operatives Change-Management)
- Change-Planung und Testen der geplanten Konfigurationsänderungen
- Auto-Discovery der Netzwerkkomponenten

NCCM als Erfolgsgarant für den Netzwerkbetrieb

Für den produktiven Einsatz ist die Anzahl der unterstützten Netzwerkkomponenten grundlegendes Entscheidungskriterium. Einige Produkte unterstützen nur wenige große Hersteller, während andere Produkte auch zu Komponenten kleiner oder spezialisierter Hersteller kompatibel sind.

Werkzeuge

Werkzeuge für Network Change and Configuration Management (NCCM) gewinnen seit dem Jahr 2005 im professionellen Umfeld zunehmend an Bedeutung. Erste Firmen-Übernahmen fanden statt und Konsolidierungsbestrebungen nehmen zu. Laut einer aktuellen Studie der IDC wird der Markt der Netzwerk-Konfigurationsmanagement-Werkzeuge bis zum Jahr 2009 auf weltweit 1,12 Milliarden US-Dollar wachsen. Folgende Produkte sind in diesem Themenumfeld am Markt sichtbar:

- **Opsware Network Automation System**, Fa. Opsware
  Gegründet 1999 in Californien, USA. Im Jahr 2004 wurde die Fa. Rendition Networks mit dem Produkt TrueControl übernommen. Die Stärke des Network Automation System ist eindeutig die umfassende Reporting Funktion mit mehr als 60 vorgefertigten Reports über Compliance mit unterschiedlichen rechtlichen Vorgaben, über die vorhanden Komponenten und Betriebsabläufe.

- **Tripwire for Network Devices**,
  Fa. Tripwire
  Gegründet 1992 in Oregon, USA. Das Produkt ist ein Modul der Tripwire Enterprise/Server Plattform. Diese Plattform ist die Basis um Änderungen über die gesamte IT-Infrastruktur zu verfolgen. Sie ist modular erweiterbar, um benötigte Teilbereiche (wie Datenbanken, Betriebssyteme, Middleware, Applikationen) der Infrastruktur abzudecken. Schwerpunkt des Produktes ist es, Änderungen und Abweichungen von Konfigurationsrichtlinien zu erkennen, zu archivieren und Benachrichtigungen über die Änderungen abzusetzen.

- **DeviceAuthority,** Fa. AlterPoint
  Gegründet 2001 in Texas, USA. AlterPoint führt in seinem Produkt ein „Device Mediation Layer“ ein, um die Komplexität der einzelnen Netzwerkkomponenten abzufangen und die Verwaltung zu vereinheitlichen. Die Verbindung zwischen der Abstraktionsschicht und den einzelnen Komponenten wird über komponentenspezifische Treiber realisiert. Auf die Plattform kann von außen über ein auf Eclipse basierende Oberfläche oder über die Integration von Managementsystemen zugegriffen werden. Die Abstraktionsschicht ermöglicht die Einbindung fast jeder Netzwerkkomponente, unabhängig vom Hersteller.

  Alterpoint hat eine enge Zusammenarbeit mit Opnet (Produkt: IT Guru), deren Schwerpunkt die Planung und Simulation von kompletten Netzen ist. Neben dem kommerziellen Vertrieb sind Teile der Alterpoint-Lösung unter einer Opensource-Lizenz im Projekt „ZipTie“ veröffentlicht worden. Eine Erweiterung des Projektes und stärkere Anbindung an weitere Opensource-Produkte (Nagios, Snort und Putty) ist geplant.

- **Intelliden R-Series software suite**,
  Fa. Intelliden
  Gegründet 2000 in Colorado, USA. Itelliden wählt einen speziellen Ansatz, um die Verwaltung und den Zugriff auf Netzwerkkomponenten zu gewährleisten. Im Rahmen der Konfiguration werden die Netzwerkkomponenten in Modelle überführt. Alle Funktionen und Befehle der einzelnen Komponenten werden extrahiert und in ein XML-Format überführt, dass dem jeweiligen Modell zugeordnet wird. Durch diese Abstraktion werde alle Komponenten, unabhängig von herstellerspezifischen Befehlen, über eine einheitliche Syntax angesprochen. Zusätzlich bietet das Produkt ein sehr feinschichtiges Sicherheitskonzept, bei dem die Zugriffsverwaltung und das Rechtekonzept in vielen Details angepasst werden können.

  Im Jahr 2004 wurde die Fa. Gold Wire Technologies mit dem Produkt Gold Wire übernommen. Viele Kunden von Intelliden kommen aus dem Service Provider Umfeld.

- **VoyenceControl NG**, Fa. Voyence
  Gegründet 2000 in Texas, USA. Voyence zählt zu den Marktführern im NCCM-Umfeld und wird von vielen großen Systems Management Anbietern empfohlen. Das Produkt VoyenceControl NG konnte durch die umfassende Unterstützung einer Vielzahl von Komponenten und Herstellern, einem ausgereiften Workflow-Management und der automatischen Wiederherstellung einer den Richtlinien entsprechenden Konfiguration am Markt gewinnen. Viele Funktionen, die andere Hersteller bisher nur ansatzweise umsetzen konnten, werden in VoyenceControl NG zur Verfügung gestellt, so dass es zur Zeit das umfangreichste Produkt auf dem Markt darstellt.

  Hewlett Packard hat VoyenceControl als OEM-Version unter dem Namen „HP OpenView Network Configuration Manager“ integriert.

Die Marktdurchdringung dieser Werkzeuge wird von den Analysten von Gartner als zur Zeit <5% eingestuft, jedoch mit einer hohen Wachstumsrate prognostiziert.

Architektur

Der Zugriff auf die Netzwerkkomponenten

findet bei allen Herstellern über standardisierte Methoden wie SSH, Telnet, TFTP, HTTP, HTTPS statt. Abhängig von den durch die Komponente unterstützten Protokollen, wird üblicherweise die sicherste Übertragung gewählt. Auffälligerweise verwendet Opsware für die Speicherung von Konfigurations- und Komponentendaten unverschlüsselte FTP/TFTP-Server.

Die Zugangsdaten für die Komponenten können die Werkzeuge entweder selbst verwalten oder aus externen Datenbanken abrufen. Um neue oder geänderte Passwörter abzuspeichern ist entsprechend eine Schreibberechtigung auf den Daten notwendig.

Der Benutzerzugriff auf die NCCM-Produkte erfolgt bei fast allen Herstellern ausschließlich über Webtechnologien und dem Einsatz von Java-Clients. Nur AlterPoint und Opsware benötigen für den Zugriff eine lokale Installation des Clients. Zwar bietet auch AlterPoint ein Webinterface, dieses besitzt aber nur eine eingeschränkte Funktionalität.

Um in großen Umgebungen skalieren zu können, setzen die Hersteller auf verteilte Systeme, in denen spezielle Server den Zugriff auf die Komponenten und die Automatisierungsaufgaben übernehmen. Über einen zentralen Applikationsserver werden der Benutzerzugriff, die Administration und der Abgleich mit den verteilten Servern in der Infrastruktur durchgeführt. Dieses Konzept ermöglicht zudem über mehrere Netzsegmente und Firewalls ein ganzheitliches NCCM zu betreiben. Eine Ausnahme bildet Opsware, deren System an zentraler Stelle eingesetzt werden muss. (siehe Abbildung 2)

Fazit

Vor dem Hintergrund der aufgeführten äußeren Einflüsse und unternehmensinternen Anforderungen muss die Evaluierung aktueller Werkzeuge für das Change-Management für aktive Netzwerk-Komponenten in den Fokus der Netzwerkverantwortlichen rücken. Der Markt bietet heute ausgereifte Produkte, die durch einfache Implementierung, hohe Automation und Planungsmöglichkeiten bestechen. Die schnelle und sichere Umsetzung gesetzlicher Vorgaben und interne Optimierungen garantieren dabei einen schnellen ROI.

Aus strategischer Sicht kann im Bereich der bisher wenig einbezogenen aktiven Netzwerk-komponenten ein ITIL-konformes Change Management eingeführt werden, das in Kombination mit einer unternehmensweiten BSM-Strategie zu einem erheblichen Mehrwert führt.

Mit NCCM sind zum ersten Mal Werkzeuge mit einer Betriebsreife verfügbar, die ein aktives - im Sinne von „gezielte Überführung einer Infrastruktur von einem betrieblichen IST-Zustand in einen geplanten SOLL-Zustand“ - Change-Management in heterogenen Netzen erlauben. In den nächsten Entwicklungsstufen werden sich Fragen nach der Integration der NCCM-Werkzeuge in übergeordnete Change-Management-Prozess-Werkzeuge sowie der Informationsabgleich mit CMDB´s (Configuration Management Data Base) stellen. Ebenfalls noch offen ist die Art und Dichte der Integration mit aktiven Netzwerk-Management-Systemen klassischer Prägung wie HP OpenView o.ä.. Hier könnten sich durchaus Verschiebungen bis hin zur vollständigen Substitution ergeben, wenn man die Funktionsblöcke Status-Visualisierung und Konfigurationserkennung/ -verwaltung zwischen den „Building Blocks“ einer modernen BSM-Architektur (Business Service Management) umverteilt – hierzu mehr in einem späteren Folgeartikel zum Thema „Netzwerk-Management - Quo Vadis?“.

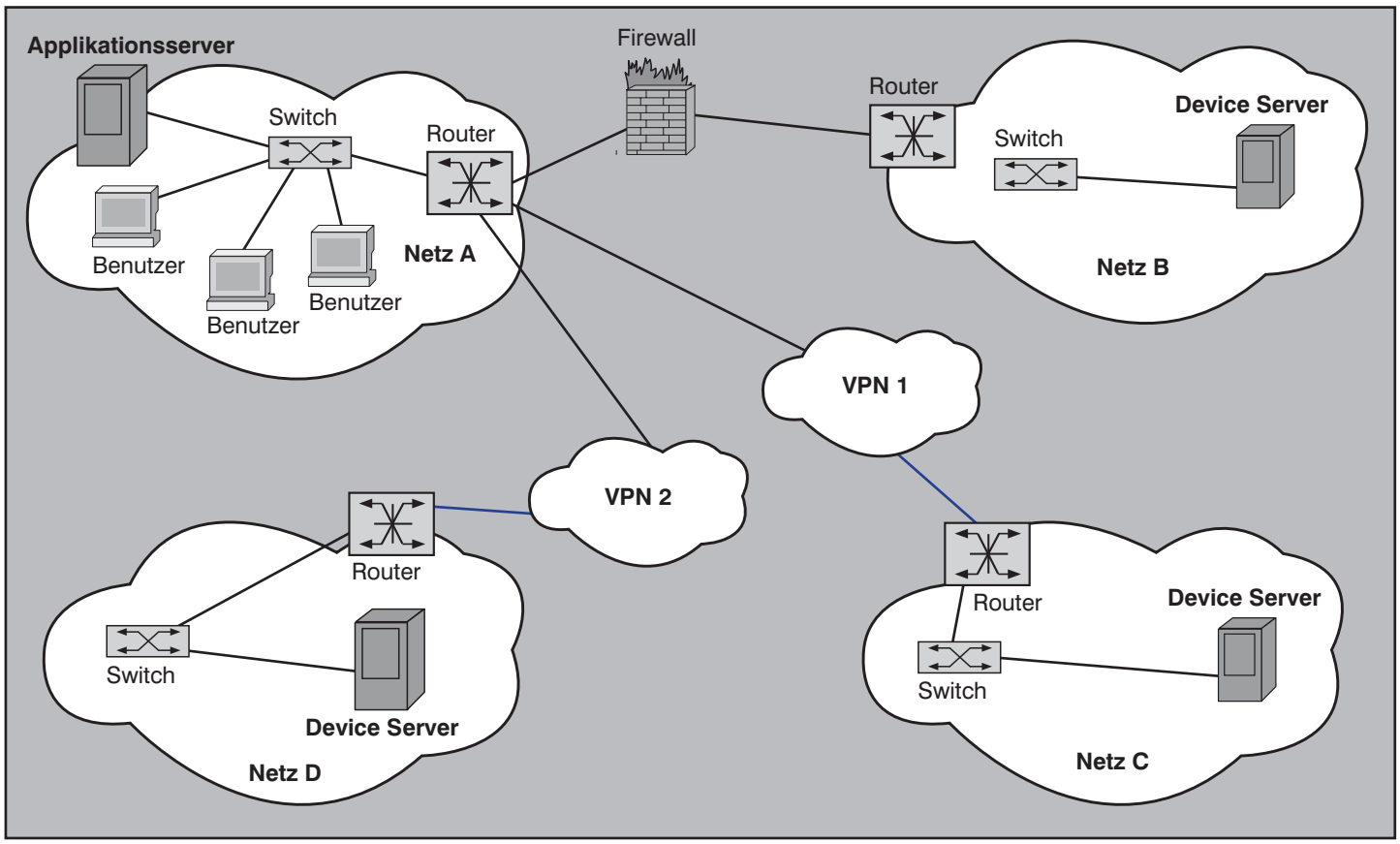


Abbildung 2: Verteilte Architektur der NCCM Werkzeuge

Report des Monats

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

Der komplett überarbeitete und neu aufgelegte Technologie-Report von ComConsult Research zeigt alle wichtigen Meilensteine bei Aufbau, Organisation und Betrieb einer VPN-Lösung. Die einzelnen Bausteine typischer Installationen werden anhand praxisnaher Vorgaben bewertet und ein umfangreiches Projekt- und Konfigurationsbeispiel detailliert besprochen. Insgesamt werden Sie somit in die Lage versetzt, Ihre eigene technisch und wirtschaftlich optimale VPN-Lösung zu entwerfen, in Ihr Gesamtkonzept einzubinden und zu betreiben. Lesen Sie im Folgenden einen Ausschnitt aus dieser Studie.

1.1 IPSec und das NAT-Problem

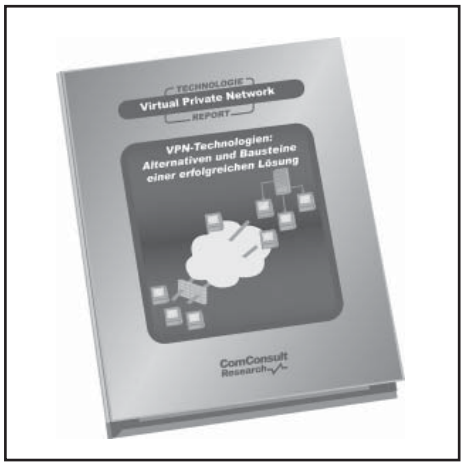
Der heute weit verbreitete Einsatz von NAT – hervorgerufen durch die Notwendigkeit, den knappen IPv4-Adressraum optimal zu nutzen, sowie aufgrund sicherheitstechnischer Vorteile bestimmter NAT-Varianten - hat beim Einsatz von VPN-Lösungen in der Vergangenheit meist für Probleme gesorgt, die erst seit Anfang 2005 durch standardisierte Mechanismen zumindest größtenteils behoben werden können. Dieses Kapitel behandelt Ursachen und Lösungsansätze dieses NAT-Problems.

1.1.1 Das NAT-Problem

Diverse Mechanismen von IPSec und NAT vertragen sich nicht miteinander. Insofern handelt es sich eigentlich nicht um ein NAT-Problem sondern um diverse NAT-Probleme. Wir wollen im Folgenden sukzessive diese Problembereiche untersuchen und beginnen bei dem offensichtlichen: dem Authentication Header.

Authentication Header

Der Authentication Header (AH) generiert eine kryptografische Prüfsumme über den Inhalt des IPSec-Pakets in Form eines Hashwerts, zu dessen Berechnung ein geheimer symmetrischer Schlüssel erforderlich ist. Dieser Hashwert umfasst alle im Paket befindlichen Daten mit Ausnahme des AH-Prüfsummenfelds und der nicht-statischen Informationen des IP-Headers. Da der Hashwert ohne Kenntnis des Schlüssels nicht gezielt gefälscht und der Schlüssel seinerseits aufgrund der Eigenschaften der Hash-Funktion nicht aus dem Hashwert zurückberechnet werden kann,



wird jegliche Manipulation am Datenpaket bei der Verifikation der Prüfsumme aufgedeckt und ein solches Paket vom Empfänger als ungültig verworfen. Der AH dient somit dem Erhalt der Integrität der übertragenen Datenpakete.

Unglücklicherweise basiert jedoch der NAT-Mechanismus bekanntermaßen genau auf einer gezielten Manipulation der IP-Adressen der Datenpakete: In der Regel wird die Absenderadresse durch eine andere Adresse ersetzt. Diese Manipulation wird vom AH äußerst wirksam unterbunden – er kann an dieser Stelle nicht zwischen erwünschten (NAT) und unerwünschten (IP-Spoofing) Manipulationen unterscheiden. Ein Einsatz des AH in NAT-Szenarien ist somit ausgeschlossen.

ESP und NAPT/PAT

Dies allein scheint nicht weiter dramatisch, wird doch der AH in vielen Szenarien gar nicht verwendet bzw. kann meist darauf verzichtet werden, da das zweite IPSec-Protokoll, ESP, ebenfalls eine - wenn auch nicht ganz so weit reichende - Integritätsprüfung beinhaltet. Doch leider löst auch der Verzicht auf den Authentication Header das NAT-Problem nicht, denn auch ESP (Encapsulating Security Payload) verursacht Probleme im Zusammenspiel mit NAT. Ein generelles Problem sind hier gemultiplexte NAT-Kommunikationsbeziehungen.

Multiplexing ist bei NAT dann vonnöten, wenn mehrere interne Adressen auf eine (oder wenige) externe Adresse abgebildet werden müssen - das Standard-Szenario etwa bei der Verwendung von DSL-Routern im SOHO-Bereich. Üblicherweise kommt hier NAPT (Network Address and Port Translation) zum Einsatz - dieser Mechanismus ist auch unter der Bezeichnung PAT (Port Address Translation) bekannt. NAPT/PAT multiplexen durch gezielte Manipulation des Client-Ports (bei UDP bzw. TCP) oder anderer aus Sicht des Empfängers frei wählbarer Parameter (z.B. ICMP-Identifier). Durch eine eindeutige Zuordnung der jeweiligen internen Adresse zu einem solchen Parameter lassen sich die Antwortpakete gezielt demultiplexen.

Unglücklicherweise verschlüsselt ESP den Teil des IP-Pakets, in dem sich diese manipulierbaren Parameter befinden. Somit ist eine sinnvolle Manipulation nicht mehr möglich und das Verfahren scheitert. Einzige Chance - für entsprechend ausgestattete NAT-Geräte - wäre eine Nutzung des IPSec-Headers zum Multiplexen. Hier steht allerdings lediglich der SPI (Security Parameter Index) zur Verfügung, der wegen der in ESP integrierten Integritätsprüfung nicht manipulierbar ist. Freilich bestünde grundsätzlich die Möglichkeit, den originalen ISP zu verwenden - immerhin ist die Wahrscheinlichkeit einer Kollision aufgrund der 32 Bit Länge des SPI extrem unwahrscheinlich - allerdings besteht hier ein grundsätzliches Problem: der SPI wird für jede der beiden Kommunikationsrichtungen zwischen den beteiligten Partnern separat vereinbart. Die Folge davon ist, dass zwischen dem SPI der gesendeten Pakete und dem der empfangenen nicht notwendigerweise eine Korrelation besteht. Anders ausgedrückt: der Empfänger eines Antwortpakets kann aus dem darin enthaltenen SPI nicht mit Sicherheit die korrekte Adressabbildung ermitteln, da dieser SPI mit dem zuvor gesendeten in keinem erkennbaren Zusammenhang stehen muss.

Daher ist diese Methode nicht allgemein verwendbar; es gibt allerdings Produkte (beispielsweise von Cisco Systems), die in der Lage sind, identische SPIs auf beiden Seiten der Kommunikationsbeziehung si-

cherzustellen, und somit ein NAPT/PAT ermöglichen, solange die VPN-Lösung homogen bleibt.

ESP im Transport-Modus
Es bliebe somit - wenn überhaupt - nur statisches NAT, d.h. die feste Zuordnung externer zu internen Adressen - ein Ansatz, der in den meisten Fällen an zu knapp bemessenem offiziellem Adressraum scheitern dürfte. Zudem ist auch der Einsatz von statischem NAT nicht unproblematisch: Schwierigkeiten treten zumindest dann auf, wenn ESP im Transport-Modus verwendet wird (dies ist beispielsweise bei der in Windows2000/2003 integrierten IPSec-VPN-Lösung der Fall). Ursächlich hierfür ist der Prüfsummenmechanismus in TCP (teilweise auch in UDP), der neben den Source- und Destination-Ports auch die jeweiligen IP-Adressen von Sender und Empfänger berücksichtigt. Ändert ein NAT-Gerät eine IP-Adresse, so muss der TCP-Header, konkret: das Prüfsummenfeld, entsprechend angepasst werden. Ohne ESP stellt dies kein Problem dar, mit ESP jedoch sehr wohl, da das Prüfsummenfeld verschlüsselt ist. Eine Korrektur ist somit nicht möglich – sie würde von der Integritätsprüfung von ESP sofort entdeckt werden – was dazu führt, dass die Prüfsummenverifikation beim Empfänger scheitert und dieser derartige Pakete verwirft.

Dieses Problem tritt allerdings nur im Transport-Modus auf: Im Tunnel-Modus bezieht sich die TCP-Prüfsumme auf den inneren IP-Header, während die Manipulation am äußeren, dem Tunnel-IP-Header vorgenommen wird. Da dieser auch von der ESP-Integritätsprüfung nicht erfasst wird, kann in diesem Fall statisches NAT eingesetzt werden.

IKE
Somit bliebe also ESP im Tunnel-Modus mit statischem NAT als mögliche Verfahrensweise, die in diversen DSL-Routern im Übrigen unter der Bezeichnung „IPSec-Pass-Through“ implementiert ist. Unglücklicherweise hat jedoch auch IKE Probleme mit NAT; hierfür gibt es gleich mehrere mögliche Ursachen:

- IKE verwendet, abhängig von Einsatzform und Implementierung, IP-Adressen zur Identifizierung der Kommunikationspartner. Diese befinden sich als Parameter innerhalb des IKE-Protokolls. Stimmen diese Parameter mit den tatsächlichen IP-Adressen nicht überein, so wird ein entsprechendes Paket meistens verworfen.

- IKE verwendet selbst ebenfalls SAs, um einen geschützten Kommunikationspfad („IKE-Tunnel“) für das Aushandeln der IPSec-SAs bereitzustellen. Die zugehörigen IKE-SAs bestehen in aller Regel recht lange, um beispielsweise ein regelmäßiges Rekeying (dabei werden in bestimmten Zeitabständen die Schlüssel für die ESP-Verschlüsselung neu vereinbart) mit größtmöglicher Effizienz zu gestalten. Demgegenüber sind die NAT-Timeouts für UDP, dem von IKE genutzten Transportschicht-Protokoll, in der Regel erheblich kürzer. Da über IKE nur bei Bedarf Informationen ausgetauscht werden, kommt es häufig zu langen Idle-Perioden, die dazu führen, dass das Adress-Mapping aus der NAT-Table gelöscht wird, was zur Unzustellbarkeit der betroffenen IKE-Pakete führt.

- Nicht alle IKE-Implementierungen akzeptieren Client-Ports, die vom Standard-Port (UDP 500) abweichen. Verändert ein NAT-Gerät den Source-Port eines abgehenden Pakets und der Empfänger akzeptiert nur den Port 500, so kommt keine Kommunikation zustande - die Aushandlung des IKE- und damit auch des IPSec-Tunnels scheitert.

Somit verbleibt oftmals nur die manuelle SA-Konfiguration, wenn NAT im Einsatz ist - ein Ansatz, der zumindest in umfangreicheren Szenarien absolut nicht praktikabel ist.

Lösungsansatz: Encapsulation
Das grundlegende Problem wurde natürlich schon vor geraumer Zeit erkannt und es existieren diverse Lösungen dafür, die jedoch allesamt proprietärer Natur sind. Allen derartigen Techniken ist gemeinsam, dass sie Encapsulation als Lösungsansatz verwenden, was nahe liegt, da sich damit - man sieht es beim ESP-Tunnel-Modus - einige Probleme quasi von selbst lösen.

Die meisten Hersteller generieren einen zusätzlichen UDP-Tunnel unter Verwendung verschiedenster Portnummern; eine etwas ausgefallenere Lösung bot die (mittlerweile strategisch durch die XSR-Router ersetzte) Aurorean-VPN-Lösung der Fa. Enterasys: Hier kam eine Verkapselung in HTTPS zum Einsatz, in der Hoffnung, auf dieser Basis aus vielen Netzwerken heraus ohne Anpassung einer etwaigen Firewall per VPN kommunizieren zu können. Dieser Ansatz wird im Übrigen auch von anderen Anbietern aufgegriffen, wenn auch nicht zur Behebung der NAT-Problematik: als Beispiel sei hier der so genannte Visitor Mode der Checkpoint VPN-1 genannt.

Schwerpunktthema

Welche neuen Gefahren kommen mit Web 2.0 auf uns zu?

Fortsetzung von Seite 1

Björn Fröbe arbeitet als Berater im Bereich IT-Sicherheit bei der GAI NetConsult. Sein Aufgabenfeld umfasst die Durchführung von Scan- und Penetrationstests, Einführung und Betrieb von Intrusion Detection Systemen, sowie die Konzeption sicherer Windows-Umgebungen.

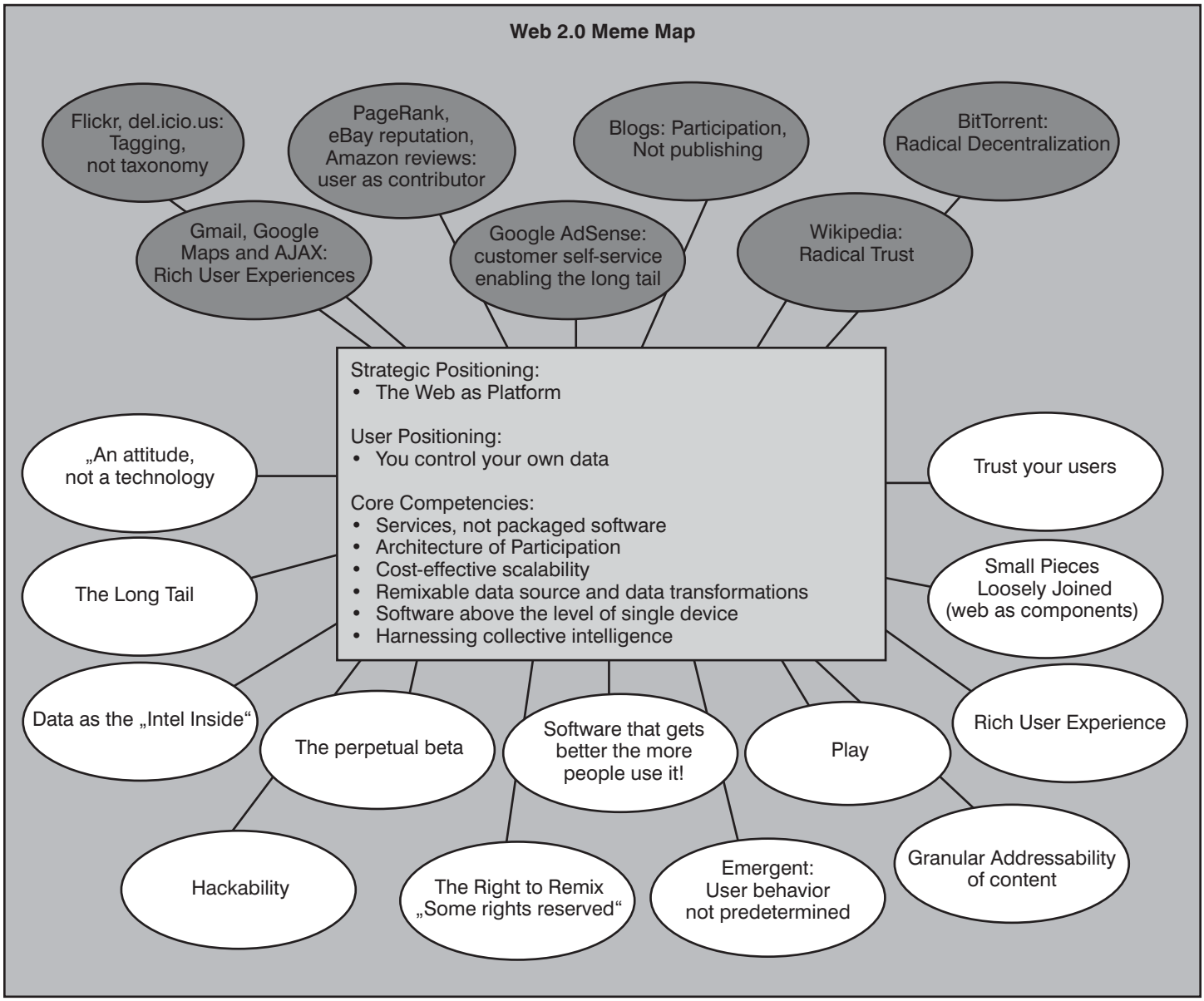


Abbildung 1: Prinzipien des Web 2.0

Welche neuen Gefahren kommen mit Web 2.0 auf uns zu?

Ajax
Im Zusammenhang mit Web 2.0 wird häufig der Name Ajax genannt, teilweise sogar als Synonym dafür. Von Wikipedia (welches ja auch in die Web 2.0 Welt einzuordnen ist) stammt folgende Definition von Ajax:

„Ajax ist ein Apronym für die Wortfolge Asynchronous JavaScript and XML. Es bezeichnet ein Konzept der asynchronen Datenübertragung zwischen einem Server und dem Browser, welches es ermöglicht, innerhalb einer HTML-Seite eine HTTP-Anfrage durchzuführen, ohne die Seite komplett neu laden zu müssen."

So ist also Ajax weder ein bestimmtes Produkt und auch keine (neue) Technologie, sondern ein Kunstwort, um das Zusammenspiel bereits vorhandener Komponenten zu beschreiben. Diese Wortschöpfung wird Jesse James Garret, dem Autor des Anfang 2005 veröffentlichten Aufsatzes „Ajax: A New Approach to Web Applications" [1], zugeschrieben. Angeblich auch nur deshalb, weil es ihm beim Schreiben zu umständlich war, die konkrete Kombination von lange bekannten Web-Technologien immer wieder neu zu formulieren.

Durch Kombination verschiedener bekannter Technologien und geschickte Verknüpfung von Client- und Server-Komponenten entstehen mit Ajax höchst interaktive Anwendungen, die den Eindruck vermitteln, als ob das Problem einer zustandslosen Web-Applikation behoben wurde. D.h. konkret, eine Ajax-Applikation kommuniziert auch ohne explizite Aktion des Benutzers mit dem Server. Vom Server empfangene Daten werden auch nicht zwangsläufig durch Refresh der ganzen Seite angezeigt, sondern können – abhängig von der hinterlegten Logik – auch nur zur Aktualisierung einzelner Elemente oder Abschnitte einer Seite führen. Eine Ajax-Anwendung basiert auf folgenden Web-Techniken:

- HTML (oder XHTML) und CSS, um das Aussehen einer Webseite beeinflussen zu können,
- Document Object Model zur Repräsentation von Daten bzw. Inhalten,
- JavaScript zur Programmierung lokaler Logik, Manipulation des Document Object Models und zur dynamischen Darstellung der Inhalte,
- XML als Datenaustauschformat,
- XSLT zur Datentransformation und Visualisierung,
- das XMLHttpRequest-Objekt, um Daten auf asynchroner Basis mit dem Webserver austauschen zu können.

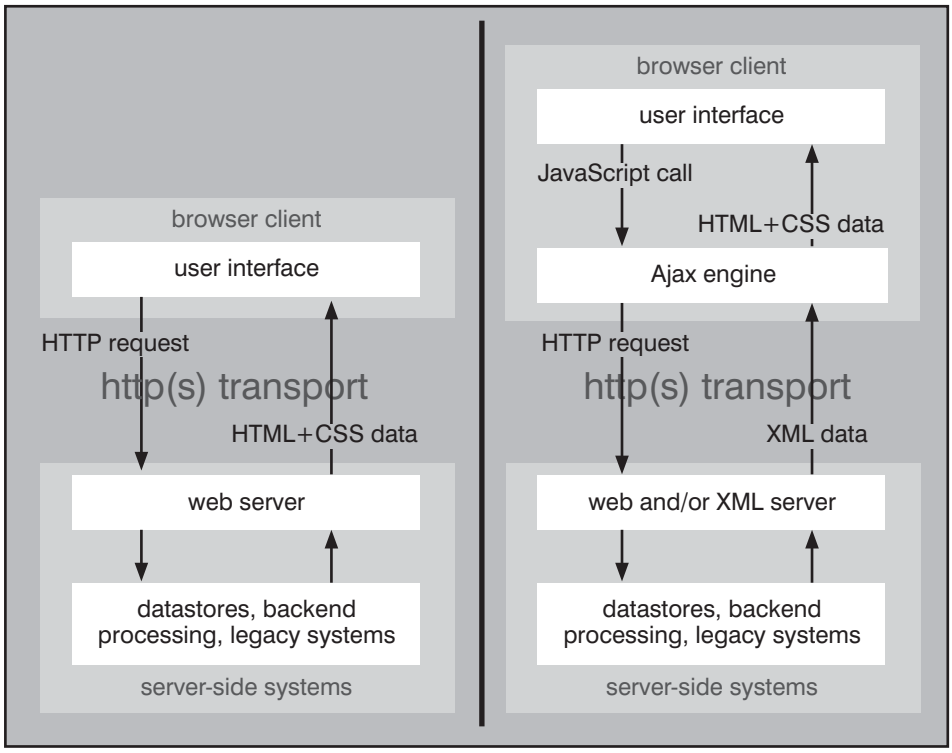


Abbildung 2: Das „klassische" Web-Applikations-Modells (links) und das „Ajax"-basierte Modell

Alle diese Elemente oder Basistechnologien sind bereits vorhanden gewesen und auch schon genutzt worden, bevor diese Kombination als AJAX bekannt wurde. Javascript wurde auch bisher schon hier und da in unterschiedlichem Umfang zur Erhöhen der Funktionalität auf Clientseite (Validierung von Feldinhalten, Prüfen von Abhängigkeiten oder Operationen in Datentabellen / Auswahlfeldern) genutzt - entweder in „Handarbeit" durch versierte Web-Entwickler oder automatisiert durch Nutzen von in Java gekapselten Javascript-Funktionen moderner J2EE-Entwicklungsumgebungen.

Neu ist die Kapselung der verwendeten Einzeltechnologien in einer separaten Komponente, eben der AJAX-Engine. Ebenso relativ neu und noch nicht allgemein bekannt sind die hierdurch möglichen Effekte in den mit Ajax erstellten Web-Applikationen, wie z.B. in den Ajax-„Muster"-Applikationen Outlook Web Access, Google Gmail und Google-Suggest. Mit Bezug auf den eingangs referenzierten Fachartikel [1] vom Ajax-Namensgeber sei nachfolgend die unterschiedliche Kommunikationsarchitektur „klassischer" und „Ajax"-basierter Web-Applikationen dargestellt.

In der Abbildung 2 wird die zentrale Instanz der Ajax-Engine im Browser des Clients deutlich, die fortan für die (asynchrone) Kommunikation mit dem Server über XMLHttpRequest und – falls erforderlich oder so vorgesehen – selbständig die Visualisierung / das Rendering durch dynamische Modifikation der relevanten Teile einer Seite zuständig ist. In diesem Falle wäre das Rendern von Web-Seiten durch den HTTP-Server überflüssig und die Kommunikation könnte auch direkt mit einem XML-Server erfolgen.

Wie aus der Abbildung 3 deutlich wird, laufen Aktionen des Benutzers und die Kommunikation der Ajax-Engine mit dem Server vollständig nebenläufig und asynchron ab. Der Benutzer bemerkt eine unmittelbare Reaktion der Ajax-Anwendung schon nach Eingabe einzelner Zeichen oder auch abhängig von anderen Ereignissen der hinterlegten Logik (z.B. Zeitsteuerung), ohne explizit eine Übertragung zum Server ausgelöst zu haben.

Sicherheitsrisiken für „Web 2.0" Applikationen

Zunächst einmal gelten für Ajax-Applikationen (mindestens) dieselben Sicherheitsrisiken wie für klassische Web-Applikationen, sicherer werden sie durch Ajax keinesfalls. Andererseits gibt es aber auch nur wenige wirklich spezifische Schwachstellen, die nur Web 2.0 Anwendungen betreffen würden.

Durch die Arbeitsweise von Ajax-Applikationen werden viele Aktionen der Anwen-

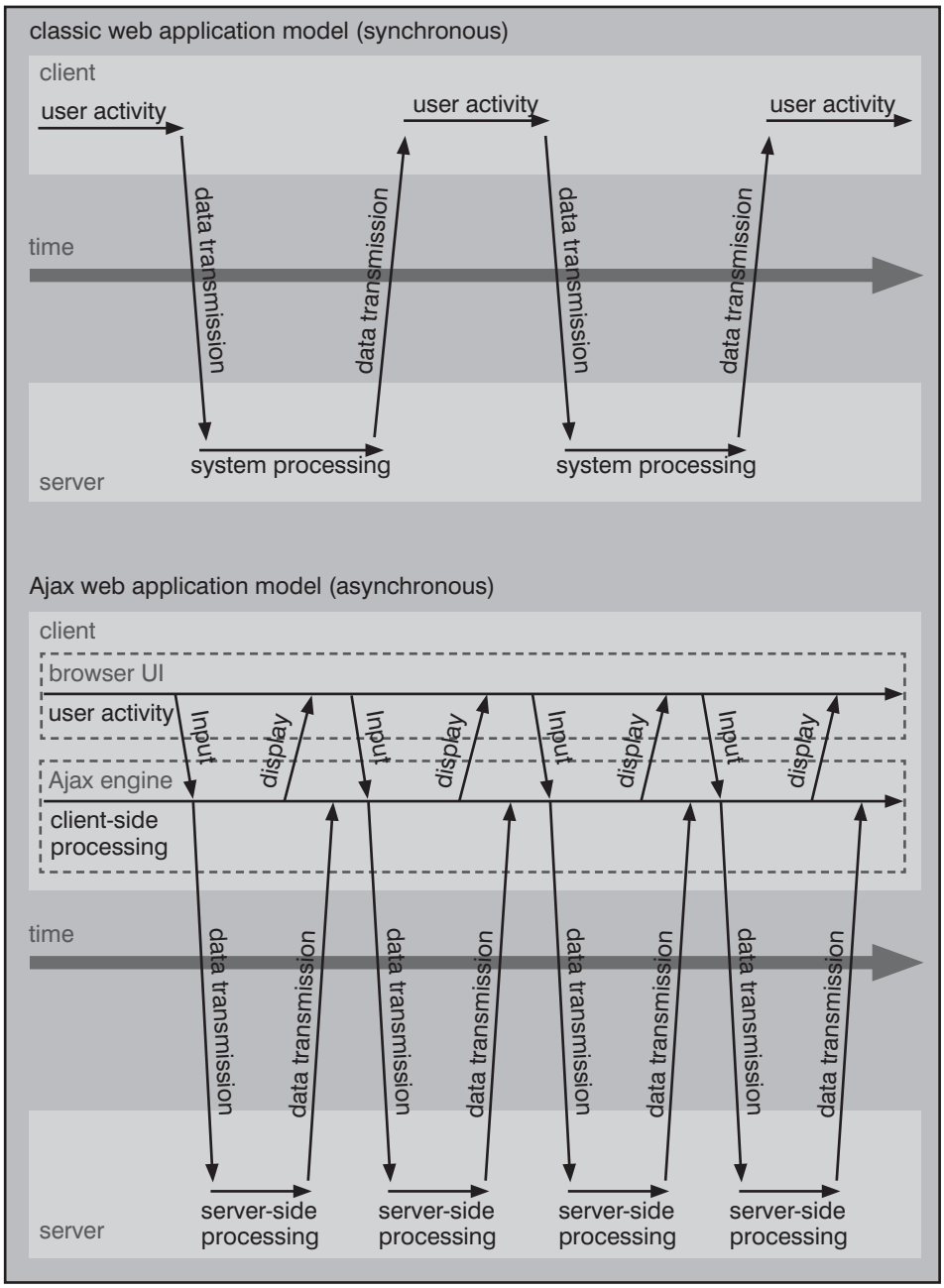


Abbildung 3: Asynchrones Kommunikationsverhalten mit dem Server

dung vor dem Nutzer versteckt. Insbesondere gibt es meist auch keine klassischen Eingabeformulare mehr, die erst bei einem Click auf „Submit“ die eingegebenen Daten übermitteln. Vielmehr ist ein konstanter Datenfluss zwischen Browser und Anwendung zu beobachten. Dies macht Schwachstellentests von Ajax-Applikationen aufwändig und erschwert häufig die Durchführung automatisierter Tests (was je nach Standpunkt positiv oder negativ bewertet werden kann).

Da der Anwender ja nicht mehr „sieht“, welche Daten zwischen Ajax Engine im Browser und Server ausgetauscht werden, neigen manche Entwickler allerdings dazu, Eingabevalidierungen schon am Client durchzuführen und den Eingaben der Ajax Engine zu vertrauen. Auch Fehler werden häufig nicht korrekt abgefangen, da Fehlermeldungen ja am Client nicht mehr gerendert werden.

Ein Beispiel hierfür wäre etwa die Seite „blinklist.com“, die man wohl auch zur Gruppe der Web 2.0 Anwendungen zählen kann. Blinklist ist eine der so genannten „Social Bookmarking“ Anwendungen, bei der jeder Nutzer Bookmarks ablegen, veröffentlichen und bewerten kann. Bei jedem Zugriff auf die Seite wird über das Javascript „blink.js“ die Anfrage „?Action=Userpage/Startpage/getmytag.ax.php“ ausgelöst. Als Antwort liefert der Server eine klassische MySQL-Fehlermeldung, was auf einen möglichen SQL-Injection Angriffsvektor hindeuten könnte. (siehe Abbildung 4)

Der normale Anwender bekommt diesen Fehler vermutlich nie zu Gesicht, da die Ajax-Engine die Meldung nicht in die HTML-Inhalte mit einbindet. Sichtbar gemacht wurde der Fehler mit der Firefox Erweiterung „Firebug“, welche die Analyse Javascript-intensiver Anwendungen erheblich vereinfacht.

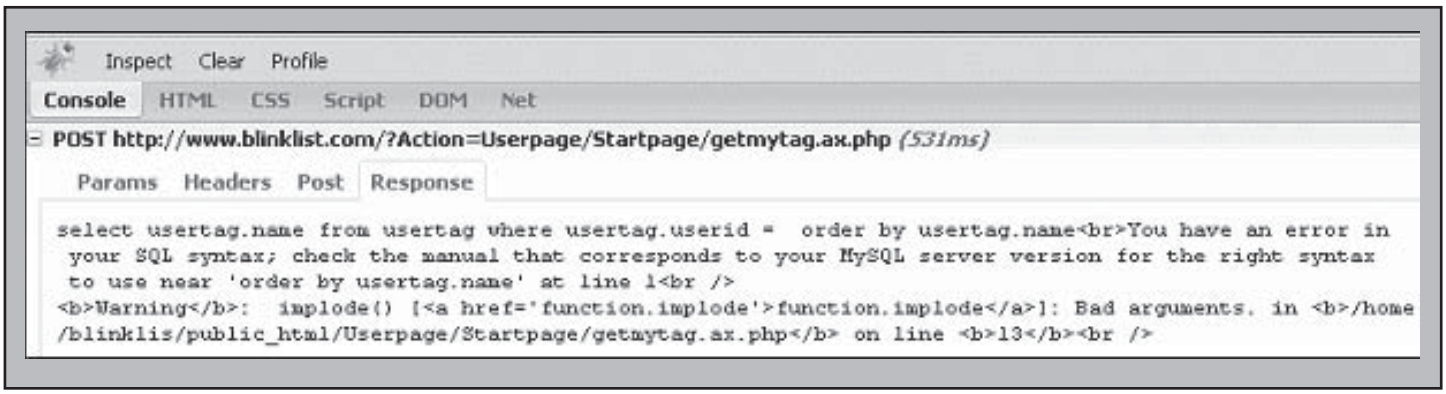


Abbildung 4: MySQL Fehlermeldung beim Zugriff auf www.blinklist.com

Welche neuen Gefahren kommen mit Web 2.0 auf uns zu?

Bedrohungen für Webclients durch Javascript

Eine der zentralen Komponenten des Web 2.0 ist Javascript. So steht z.B. das „J“ in AJAX für diese ursprünglich von Netscape entwickelte Scriptsprache. In den letzten Jahren sind immer wieder Sicherheitslücken in praktisch allen Implementierungen bekannt geworden. In diesem Abschnitt soll es aber weniger um echte Schwachstellen in Webbrowsern, als um die Grauzone zwischen der „normalen“ Verwendung von Javascript und einer Sicherheitslücke in der Implementierung gehen.

Im Zuge der sich rasant weiter entwickelnden Angriffsmethoden für Cross-Site-Scripting (XSS) Angriffe sind verschiedene Techniken entwickelt worden, Javascript für Aufgaben zu verwenden, für die es ursprünglich sicherlich nicht gedacht war. So beschäftigte sich z.B. bei der letztjährigen Blackhat-Konferenz in Las Vegas gleich eine ganze Vortragsreihe primär mit dem Thema Web Security im Allgemeinen und „Web 2.0“ Sicherheitsbedrohungen im Besonderen. Das Thema eines dieser Vorträge, nämlich „Hacking Intranet Websites from the Outside“ [2] von Jeremiah Grossmann gibt auch gleich einen Hinweis darauf, warum dieses Thema so interessant ist: Durch kreative Verwendung von Javascript kann der Browser des Anwenders als Eingangstor zum Unternehmensnetz verwendet werden. Ausgangspunkt für diese Bedrohung ist ein Javascript, welches vom Browser des Nutzers geladen wird. Um dies zu erreichen stehen einem Angreifer diverse Methoden zur Verfügung:

- Der Anwender wurde auf eine speziell für die Durchführung von Angriffen platzierte Webseite gelockt.
- Eine vom Anwender besuchte Webseite wurde kompromittiert und das Skript durch einen Angreifer dort platziert. Dies schließt auch indirekt besuchte Webserver, die z.B. für die Einblendung von Werbebannern verwendet werden, mit ein.
- Das Skript wurde über Cross-Site-Scripting (XSS) in eine vom Anwender besuchte Webseite eingebracht.

Ist das Skript des Angreifers im Browser des Anwenders aktiv, verfügt dieser über eine bidirektionale Kommunikationsverbindung in das Netz, in welchem sich der Anwender befindet. Diese Verbindung besteht so lange, wie der Anwender die betroffene Webseite im Browser geöffnet hat. Einige der Möglichkeiten, die sich dadurch bieten, werden im folgenden Abschnitt vorgestellt.

Der Javascript Portscanner

Die erste Aktion, die der Angreifer über den Browser des Nutzers durchführen möchte, könnte z.B. ein Portscan des internen Netzes sein. Grundsätzlich dürfte ein Portscan von Drittservern über Javascript aber nicht funktionieren. Warum? Weil es gegen die so genannte Same Origin Policy verstößt. Diese besagt, dass Inhalte der Webseite www.foo.com nicht auf Inhalte der Seite www.bar.com zugreifen dürfen. D.h. ein Script der Seite www.foo.com darf zwar eine Anfrage an www.bar.com senden, aber nicht auf die in der Antwort übermittelten Daten zugreifen. Der Portscanner würde also nie wissen, ob die Anfrage ihr Ziel erreicht hat oder nicht. Eine weitere Hürde, die im Intranetbereich überwunden werden muss ist die Frage der internen IP-Adressen. Diese sind ja in den allermeisten Fällen durch NAT verborgen.

Wie diverse funktionsfähige Implementierungen (z.B. [3] und [4]) beweisen, sind Portscanner auf Basis von Javascript aber dennoch möglich. Im Einzelnen funktionieren diese in etwa wie folgt:

- Über das Laden einer externen Komponente (z.B. ein Bild oder ein Skript) wird überprüft, ob ein Server existiert oder nicht. Hierfür werden die Javascript Funktion „onload“ und „onerror“ verwendet. Dies funktioniert, weil die im vorherigen Beispiel getroffene Aussage nicht ganz korrekt ist. Eine Unterscheidung zwischen „das Objekt wurde geladen“, „das Laden des Objekts hat einen Fehler verursacht“ und „das Objekt wurde nicht geladen“ ist durchaus möglich. Dauert es z.B. sehr lange, bis das „onerror“ getriggert wird, kann man davon ausgehen, dass der an“gepingte“ Host nicht aktiv ist.

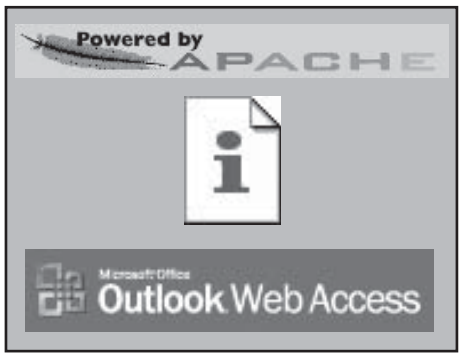


Abbildung 5: Icons, die zur Identifizierung von Webservern verwendet werden können

- Eingeschränkt ist sogar ein Fingerprinting der identifizierten Webserver und - anwendungen möglich. Hierfür können z.B. Anfragen nach häufig vorhandenen Bildern oder per Default vorhandenen Skripten genutzt werden (siehe Abbildung 5). Wird das Javascript „onerror“ in diesem Fall nicht ausgelöst, war die Anfrage erfolgreich.

Ende November letzten Jahres stellte Jeremiah Grossmann sogar eine Möglichkeit vor, zumindest HTTP-Pings ganz ohne Javascript, sondern nur unter Verwendung von Cascading Style Sheets (CSS) durchzuführen [5]. Die Technik basiert auf

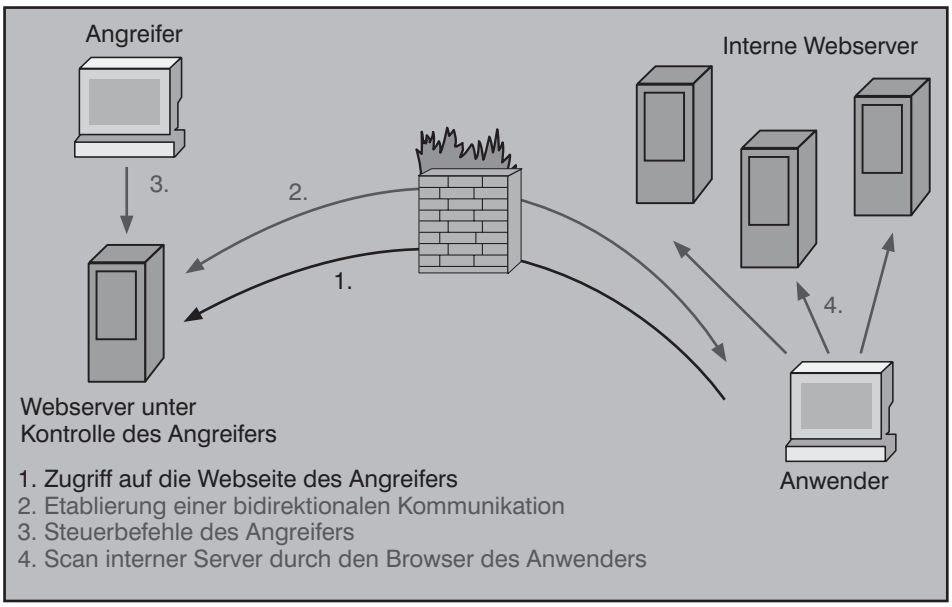


Abbildung 6: Ablauf eines Javascript Portscans

der CSS „Link"-Eigenschaft, über die Versucht wird, ein Stylesheet von einem internen Server nachzuladen. Über die Auswertung der Zeitdauer von Anfragen kann dann erkannt werden, ob eine IP-Adresse aktiv ist oder nicht.

Bleibt noch die Frage nach der internen IP-Adresse des Clients. Durch die alleinige Verwendung von Javascript ist es bisher nicht gelungen, diese auszulesen. Um die IP dennoch in Erfahrung zu bringen, kann man sich aber eines einfachen Java Applets bedienen. Durch Öffnen eines lokalen Sockets und nachfolgender Verbindung auf diesen Socket ist es möglich, die IP-Adresse des Clients auszulesen. Nachfolgend kann diese Information an einen externen Server übermittelt werden.

Auf diese Art und Weise lassen sich IP-Adressen, Webserver und –anwendungen im Intranet identifizieren. Die Frage ist, was bringen einem Angreifer diese Informationen? Hier kommt eine Angriffsform ins Spiel, die an sich schon recht alt ist, aber trotzdem nicht den Bekanntheitsgrad hat, der eigentlich angemessen wäre: Cross-Site-Request-Forging (XSRF). XSRF macht sich das implizite Vertrauensverhältnis zwischen einer Webseite und dem Browser des Anwenders zu nutze. Das vorangegangene Beispiel zeigte, dass ein Browser bei der Formulierung einer Anfrage nicht unterscheidet, ob diese auf eine URL innerhalb der jeweiligen Webseite verweist. Diese Tatsache wird bei XSRF-Angriffen ausgenutzt. Erlaubt eine identifizierte Intranet-Anwendung die Durchführung einer Aktion nur durch Angabe von URL-Parametern (also z.B. / sendmail.cgi?rcpt=hacker@example.org) kann durch Einbettung einer URL wie <img src="http://webmail.intranet/sendmail.cgi?rcpt=hacker@example.org"> in die von ihm stammende Webseite eine Aktion – in diesem Fall offensichtlich der Versand einer E-Mail – ausgelöst werden. Voraussetzung hierfür ist in den meisten Fällen natürlich, dass der Anwender zu diesem Zeitpunkt auch angemeldet ist. Die Frage, ob eine Anmeldung vorliegt oder nicht, lässt sich ggf. auch mit der für die Portscans verwendeten Methoden herausfinden, z.B. durch Laden einer URL innerhalb der Anwendung die nur für angemeldete Nutzer zugänglich ist. Gerade im Intranetbereich wird eine Authentisierung häufig durchgeführt, ohne dass der Anwender dies bemerken würde, z.B. durch Kerberos / NTLM oder Verwendung eines Single-Sign-On Cookies (z.B. den im Notes / Domino Umfeld häufig anzutreffenden LTPA-Token).

Handelt es sich bei der angegriffenen Anwendung um eine Standardkomponente wie z.B. einen Router oder einem Drucker kann auch versucht werden, mit Standardpasswörtern auf die Webschnittstelle zuzugreifen. In diesem Fall würden Nutzernamen und Passwort in die URL eingebettet werden, z.B. in der Form http://nutzername:passwort@ziel.intranet.

Welche Angriffe so durchgeführt werden, hängt letztlich von der Phantasie des Angreifers ab. (siehe Abbildung 6)

Historyklau mit CSS und Javascript

Die im vorangegangenen Abschnitt geschilderte kreative Form der Verwendung von Javascript lässt sich auch auf andere Art und Weise nutzen. Ein weiterer im Rahmen des genannten Vortrags demonstrierter Angriff ist das Auslesen der History eines Anwenders. Auch in diesem Fall erfolgt der Zugriff indirekt durch das Abfragen bestimmter Links. Der Browser wird also praktisch gefragt, warst du auf www.google.com? Dies funktioniert, weil der Browser besuchte Links anders einfärbt als noch nicht besuchte Links. (siehe Abbildung 7)

Um diese Problematik auszunutzen, werden über Javascript Links erzeugt und nachfolgend ausgelesen, um festzustellen ob diese Links durch den Browser blau (Seite nicht besucht) oder lila (Seite wurde besucht) eingefärbt wurden. Rsnake von ha.ckers.org hat ganz aktuell auch eine Technik vorgestellt, die das indirekte Auslesen der History auch ganz ohne Javascript und nur mit CSS ermöglicht [6].

SPI Dynamics zeigt in einem aktuellen Whitepaper [7], dass sich diese Technik nicht nur auf den Seitenbesuch an sich, sondern auch auf die komplette URL anwenden lässt. Auf diese Art und Weise können z.B. Sucheingaben bei Google ausgelesen werden, da der Suchstring ein Teil der URL ist. (siehe Abbildung 8)

Nun könnte man sich Fragen stellen, wie realistisch eine solche listenbasierte Abfrage ist, da ja die Liste mit den abzufragenden URLs an den Client übermittelt und dort das Skript zur eigentlichen Abfrage ausgeführt werden muss. SPI Dynamics gibt hierzu in dem referenzier-

Abbildung 7: Darstellung von besuchten und nicht besuchten Links

Abbildung 8: URL mit Suchworten bei Google

ten Whitepaper an, dass die Übermittlung und Auswertung einer über 46.000 Einträge umfassenden Liste insgesamt nur etwa fünf Sekunden gedauert hat, damit also durchaus realistisch ist. Auch wenn der indirekte Diebstahl der Browserhistorie vermutlich kein unmittelbares Risiko für eine IT-Infrastruktur darstellt, ist dieser zumindest aus Datenschutzgesichtspunkten äußert bedenklich. Auch für Phishing-„Anbieter" dürfte diese Technik sehr interessant sein, da so beim Besuch einer kontrollierten Webseite beispielsweise gleich mit abgefragt werden kann, welche Online-Banking Webseiten der Nutzer in der Vergangenheit besucht hat.

Ein Blick in die Mailinglisten-Historie zeigt, dass dieser Angriff bereits 2002 erstmalig erwähnt wurde (http://seclists.org/bugtraq/2002/Feb/0271.html), also nicht wirklich neu ist. Erschreckend ist eigentlich nur die Tatsache, dass eine über vier Jahre alte Angriffstechnik heute genauso gut funktioniert wie damals.

XSS-Toolkits

Mittlerweile existieren zumindest vier dem Autor bekannte Toolkits, die versuchen, die beschriebenen Angriffe unter einer Oberfläche zu vereinen. Verbundene Clients - also Anwender, die das Javascript des Angreifers eingebunden haben – werden dort meist als „Zombies" bezeichnet. (siehe Abbildung 9)

Teilweise enthalten die Toolkits auch noch weitere Nettigkeiten wie die Möglichkeit zum Auslesen der Zwischenablage (funktioniert nur bei Verwendung des Internet Explorers) oder einen Keylogger, der alle Nutzereingaben im Kontext der jeweiligen Webseite an den Angreifer übermittelt. Alle Toolkits verwenden AJAX-artige Techniken, um die Skriptausführung vor dem Anwender zu verstecken. Beispiele sind das gezeigte BeEF [8], oder die AttackAPI [9].

Javascript ist überall

Neben Webbrowsern verfügen mittlerweile auch viele andere typische Clientanwendungen über eine Javascript Engine. Dies sorgt für viele zusätzliche Angriffsvektoren zur Durchführung von Cross-Site-Scripting Angriffen. So verbreitete sich z.B. im Dezember 2006 ein XSS Wurm im Communityportal MySpace. MySpace erlaubt registrierten Nutzern die Integration eigener HTML- und Javascript-Inhalte sowie den Upload von Medienformaten wie Quicktime. Die Filterfunktionen von MySpace untersuchen zwar HTML und Javascript mehr oder weniger gut auf mögliche bösartige Funktionen, Filme im Quicktime-Format wurden jedoch in diese Prüfung nicht mit einbezogen. Ein Anwender, der ein befallenes Nutzerprofil betrachtete, wurde auf eine vorgetäuschte Anmeldemaske umgeleitet, nach der Authentisierung fügte sich der Wurm selbst in das Nutzerprofil ein und ersetzte alle Links innerhalb des Profils durch Links auf Phishing-Webseiten [10].

Ein weiteres von vielen als harmlos eingestuftes Dateiformat ist PDF. Zumindest der Adobe PDF Reader verfügt aber ebenfalls bereits seit vielen Jahren über eine Javascript-Implementierung. Im Dezember 2006 bzw. Januar 2007 wurden von den Italienern Stefano Di Paola, Giorgio Fedon und Elia Florio im Rahmen des CCC-Kongresses Cross-Site-Scripting Probleme in dieser Engine vorgestellt. Diese lassen sich sehr einfach ausnutzen, indem man an eine URL zu einem gültigen PDF-Dokument Scriptcode anhängt und einen Nutzer dazu verleitet, auf diesen Link zu klicken. Die URL könnte dann zum Beispiel folgende Form haben: http://example.com/document.pdf#FDF=javascript:alert('evil'). Folgt das Opfer dem Link, wird das PDF geöffnet und der eingeschleuste Scriptcode im DOM-Kontext des jewei-

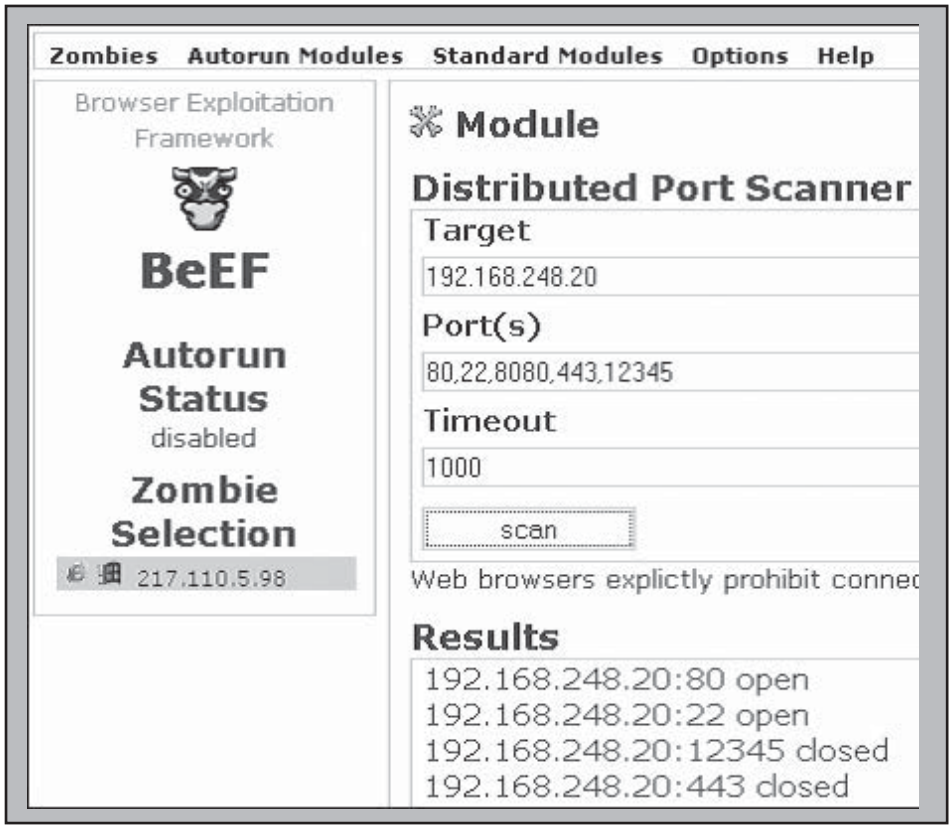


Abbildung 9: Screenshot BeEF

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<rss version="0.91">
<channel>
<title>GAI NetConsult GmbH</title>
<link>http://www.gai-netconsult.de</link>
<description>GAI NetConsult GmbH</description>
<language>de-de</language>
<copyright>GAI NetConsult GmbH</copyright>
<image>
<url>http://www.gai-netconsult.de/images/favicon.ico</url>
<title>GAI NetConsult GmbH</title>
<link>http://www.gai-netconsult.de</link>
</image>


<item>
<title>Security Journal Ausgabe 29</title>
```

Abbildung 10: Quelltext des Newsfeeds von www.gai-netconsult.de

ligen Webservers ausgeführt. Betroffen sind verschiedene Versionen des Adobe Browser-Plugins, abhängig vom verwendeten Webbrowser. Verbreitete Kombination, die von der Schwachstelle betroffen sind, wären z.B. Firefox mit dem Adobe Reader 7 oder der Internet Explorer mit dem Adobe Reader 6. Adobe hat diese spezielle Schwachstelle mit dem Adobe Reader 8 behoben. Dass das Angriffspotential für PDFs damit noch lange nicht erschöpft ist, zeigt aber ein aktueller Beitrag auf www.gnucitizen.org [11]. Der hinter dem Projekt stehende Petko Petkov hat hier fünf PDFs veröffentlicht, die z.B. automatisch URLs vom Typ „file://“ laden oder wiederum für generische Cross-Site-Scripting Angriffe genutzt werden könnten.

Bei der Risikobewertung von Dateitypen sollte daher immer berücksichtigt werden, ob diese die Integration von Skriptcode zulassen. Dies betrifft sowohl die Anwendungsseite (z.B. bei Upload-Funktionen), als auch die Clientseite (z.B. bei der Erstellung von dateityp-basierten Blocklisten).

Angriffe über News Feeds

Eine weitere dem Web 2.0 zugeordnete Funktionalität sind die bekannten RSS oder Atom News Feeds. Beide Formate basieren auf XML und ermöglichen den automatischen Download von Überschriften und ausgewählten Inhalten von Webseiten. Der Client kann in diesem Fall ein RSS Newsreader als Browserbestandteil oder ein externes Programm sein. Auch ein Webserver bzw. eine Webanwendung kann ein Client sein, z.B. um ein so genanntens Mash-Up – wieder ein Web 2.0 Begriff – aus mehreren Newsfeeds zu erzeugen. Clients sind mittlerweile in Standard-Softwarekomponenten wie z.B. dem Internet Explorer 7, Windows Vista und Firefox 2.x enthalten. (siehe Abbildung 10)

Die eigentlichen Feeds können wiederum HTML und Javascript beinhalten. Viele Newsreader stufen die bezogenen Inhalte als voll vertrauenswürdig ein und führen wenige bis keine zusätzlichen Prüfungen durch. In Kombination öffnet dies Tür und Tor für Angriffe wie Cross-Site-Scripting oder Cross-Site-Request-Forging. Zwar muss der Nutzer einen Feed immer noch selbst abonnieren, viele Anbieter von Newsfeeds erstellen diese aber wiederum aus Inhalten von Drittanbietern. Man sollte RSS News Feeds daher nicht mehr Vertrauen entgegenbringen, als den eigentlichen Webseiteninhalten. Genau dies ist aber zumindest bei vielen Feed-Clients bisher noch der Fall, wie ein Whitepaper von Rober Auger zu diesem Themenkomplex zeigt [12].

News Feeds schaffen daher einen weiteren Vektor für Angriffe auf Clients. Erschwerend kommt hinzu, dass Newsfeeds automatisch geladen werden, ohne dass der Nutzer auf eine bestimmte Seite zugreifen muss (vorausgesetzt, der Nutzer hat den Newsfeed einmal eingebunden).

Fazit

Aus Sicht des Autors bringt das Web 2.0 vor allen Dingen für die Webclients neue Gefährdungen mit sich. Die Verbreitung neuer Technologien wie RSS und die immer weitgehendere Integration von Skripting APIs in ehemals statische Dateiformate schafft neue Einfallstore, die in bisherigen Sicherheitsbewertungen vermutlich noch nicht betrachtet worden sind.

Durch das Abbröckeln der Same-Origin-Policy kann heutzutage auch bereits nur durch die Verwendung von Javascript und/oder Cascading Style Sheets und ohne Ausnutzung einer browserspezifischen Schwachstelle die Abgrenzung zwischen Inter- und Intranet ausgehebelt werden. Nimmt man alle beschriebenen Techniken zusammen, könnte der Browser eines Anwenders in einen Proxy zwischen einem Angreifer im Internet und webbasierten Intranetanwendungen verwandelt werden, ohne dafür eine spezielle Schwachstelle in dem Browser ausnutzen zu müssen. In einigen Fällen kann die Blockierung von Javascript Abhilfe schaffen, allerdings wurden wie beschrieben einige ehemals skriptbasierte Angriffe auf alternative Technologien wie CSS portiert. Letztlich obliegt es daher den Browserherstellern, sicherere Javascript und CSS-Implementierungen bereitzustellen.

Unsere diesbezüglichen Tests mit gateway-basierten Content-Scannern waren eher durchwachsen, bei der Kontrolle von Javascript scheinen hier noch erhebliche Defizite zu bestehen. Ggf. sollten Sie selbst einmal einige der referenzierten Tools ausprobieren, um die implementierten Sicherheitsmaßnahmen zu überprüfen.

Referenzen

[1] http://www.adaptivepath.com/publications/essays/archives/000385.php
[2] http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grossman.pdf
[3] http://www.spidynamics.com/spilabs/js-port-scan/
[4] http://www.gnucitizen.org/projects/attackapi/build/demos/PortScanner.htm
[5] http://jeremiahgrossman.blogspot.com/2006/11/browser-port-scanning-without.html
[6] http://ha.ckers.org/blog/20070228/steal-browser-history-without-javascript/
[7] http://www.spidynamics.com/assets/documents/JS_SearchQueryTheft.pdf
[8] http://www.bindshell.net/tools/beef/
[9] http://www.gnucitizen.org/projects/attackapi
[10] http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708
[11] http://www.gnucitizen.org/projects/pdf-strikes-back/
[12] http://www.spidynamics.com/assets/documents/HackingFeeds.pdf

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Grundlagen des Trouble Shooting in Lokalen Netzwerken, 12.03. - 16.03.07 in Aachen

Dieses Seminar vermittelt, welche Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind, wie man mit diesen Fehlersituationen analysiert und wie dabei methodisch vorgegangen wird, um in kürzester Zeit zu einem Ergebnis zu kommen.

Preis: € 2.490,- zzgl. MwSt.

IP-Telefonie: Vorbereitung, Migration, Management, 12.03. - 14.03.07 in Köln

Der Referent dieses 3-tägigen Seminars vermittelt seine jahrelange Projekt-Erfahrung bei der Nutzung und des Betriebs von IP-Telefonie sowie bei der Durchführung hochkomplexer Projekte in diesem Umfeld. Preis: € 1.690,- zzgl. MwSt.

Windows Vista - Tatsächlich Mehrwerte vorhanden?, 13.03.07 in Köln

Microsoft hat Ende November 2006 die finale Version von Windows Vista freigegeben und stellt diese auch für Unternehmenskunden zur Verfügung. Ende Januar 2007 kommt Vista dann in den Handel. Was haben Unternehmen von dieser neuen Version des führenden Betriebssystems zu halten? Schafft es Microsoft, mit der Etablierung von Vista die Basis für seine „people ready software“ zu legen? Welche Mehrwertpotentiale bietet Vista, insbesondere wenn man schon Windows XP im Unternehmen eingeführt hat? Competence Center Leiter Markus Holländer und Dipl.-Inform. Michael van Laak - die technisch Verantwortlichen der ComConsult Beratung und Planung GmbH zu dieser Thematik - erläutern diese Fragen in dem vorliegenden Seminar für Entscheider. Es werden insbesondere die Funktionen und Dienste betrachtet, die einen Mehrwert versprechen. Es ist vorgesehen, dass beide Spezialisten vor Ort sind.

Preis: € 990,- zzgl. MwSt.

Troubleshooting Windows Server 2003 Active Directory, 26.03. - 29.03.07 in Aachen

Dieses 4-tägige Seminar besteht aus einem Mix aus Know-How-Auffrischungen, Aufgaben, Live-Demonstrationen und Troubleshooting durch die Teilnehmer selber, so dass ein hoher Praxisgrad erreicht wird. Die Referenten kommen vom bekannten Competence Center Backoffice der ComConsult Beratung und Planung, das auf zahlreiche erfolgreiche nationale und internationale AD-Projekte im Bereich von ca. 300 bis zu 80.000 Benutzer/Computer zurück blicken kann. Preis: € 1.990,- zzgl. MwSt.

IP-Telefonie evaluieren, planen, betreiben, 16.04. - 18.04.07 in Neuss

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet. Preis: € 1.690,- zzgl. MwSt.

Lokale Netze für Einsteiger, 16.04. - 20.04.07 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.

Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen, 23.04. - 24.04.07 in Bonn

Sie erfahren in diesem 2-tägigen Seminar, welche typischen Ursachen den in den letzten Jahren festgestellten Störungen und Schäden in Netzwerken und DV-Installationen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können. Preis: € 1.390,- zzgl. MwSt.

Trouble Shooting in konvergenten Netzwerken, 23.04. - 27.04.07 in Aachen

Dieses Seminar vermittelt das notwendige Hintergrundwissen über die typischen Fehler, erklärt ihre Erscheinungsformen im laufenden Betrieb und trainiert systematisch ihre Diagnose und Beseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen.

Preis: € 2.490,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 23.04. - 24.04.07 in Bonn

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.

Trouble Shooting für TCP/IP- und Windows-Umgebungen, 07.05. - 11.05.07 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen in diesem Umfeld, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Preis: € 2.490,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 07.05.-08.05.07 in Bonn

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
16.04. - 20.04.07 in Aachen
25.06. - 29.06.07 in Aachen
15.10. - 19.10.07 in Aachen
03.12. - 07.12.07 in Aachen

Internetworking
07.05. - 11.05.07 in Aachen
17.09. - 21.09.07 in Aachen
10.12. - 14.12.07 in Aachen

TCP/IP und SNMP
21.05. - 25.05.07 in Aachen
15.10. - 19.10.07 in Berlin

Ethernet Netzwerke
21.05. - 23.05.07 in Aachen
10.09. - 12.09.07 in Aachen
26.11. - 28.11.07 in Aachen

Paketpreis für alle vier Seminare € 7.704.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--, Ethernet Netzwerke: € 1.690.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
12.03. - 16.03.07 in Aachen
11.06. - 15.06.07 in Aachen
03.09. - 07.09.07 in Aachen
12.11. - 16.11.07 in Aachen

Trouble Shooting in konvergenten Netzwerken
23.04. - 27.04.07 in Aachen
18.06. - 22.06.07 in Aachen
17.09. - 21.09.07 in Aachen
19.11. - 23.11.07 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
07.05. - 11.05.07 in Aachen
22.10. - 26.10.07 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
18.06. - 22.06.07 in Bonn
10.09. - 14.09.07 in Berlin

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
25.06. - 27.06.07 in Berlin
15.10. - 17.10.07 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
16.04. - 20.04.07 in Aachen
27.08. - 31.08.07 in Aachen
03.12. - 07.12.07 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 3234415

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