ComConsult Research

Der Netzwerk Insider

April 2007

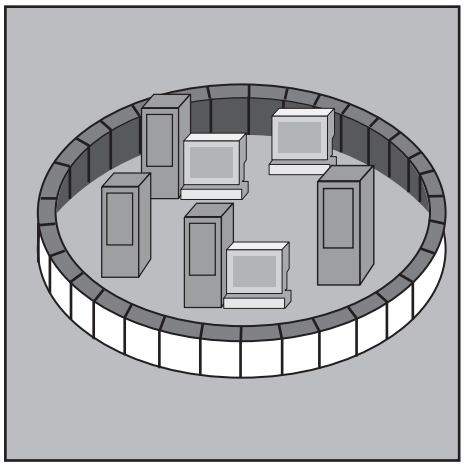
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Sicherheitsanalyse des Cisco NAC Framework

von Dror-John Röcher, Michael Thumann

Das Cisco „Network Admission Framework“ hat zum Ziel, den Zugang zum Netzwerk basierend auf der Einhaltung einer „Policy“ zu reglementieren. Dazu werden Clients einer Prüfung unterzogen und basierend auf dieser Prüfung wird der Zugang in verschiedenen Stufen gewährt. Cisco NAC ist eine relativ junge Technologie, die langsam an Bedeutung für den Markt gewinnt. Neben Cisco gibt es noch etliche andere Hersteller mit eigenen „Admission-Control“-Lösungen, die aber in diesem Artikel nicht näher beschrieben oder analysiert werden. Im ersten Teil wird ein kurzer Überblick über die Funktionsweise und wichtigen Bestandteile



des Cisco NAC Frameworks gegeben, der zweite, aufbauende Teil, enthält eine Sicherheitsanalyse des Cisco NAC Framework. Abschließend werden Maßnahmen zur Erhöhung des Sicherheitsniveaus in Cisco NAC diskutiert.

weiter auf Seite 22

Zweitthema

Virtuelle Poststellen - sichere E-Mail für alle?

von Dipl.-Inform. Andreas Meder

In der heutigen Zeit, da einerseits das schnelle und zuverlässige Austauschen von Informationen für die Geschäftsprozesse der meisten Unternehmen - zumindest vom Mittelstand an aufwärts - essentiell ist (Stichwort: Informationsgesellschaft) und andererseits diese Informationen vermehrt nur noch in elektronischer Form vorliegen - zumindest während der Entwurfsphase - besteht mehr denn je die Anforderung nach Möglichkeiten, diese Informationen, d.h. in aller Regel Dokumente respektive Daten, zwischen den eigenen Mitarbeitern und unternehmensfremden Anwendern auf sicherem Wege auszutauschen. Unter einem „sicheren Weg“ wird dabei allgemein eine Methode verstanden, die durch Einsatz kryptografischer Verfahren die Vertraulichkeit und Integrität der übermittelten Informationen hinreichend sicherstellt.

Zu den Nutzerkreisen eines solchen sicheren Dokumentenaustauschs gehören typischerweise neben Forschungs- und Entwicklungsgruppen insbesondere auch Anwender mit kaufmännischem oder juristischem Hintergrund.

weiter auf Seite 9

Top Veranstaltung

ComConsult SIP-Forum 2007

auf Seite 7

Geleit

SOA ist, wenn´s trotzdem läuft

auf Seite 2

Report des Monats

Voice-over-IP-Lösungen von Alcatel

auf Seite 18

Zum Geleit

SOA ist, wenn´s trotzdem läuft

Von einem globalen Trend, einem Hype, ist die Rede sobald man sich mit „Service Orientied Architectures“, kurz SOA, befasst. Die technische Grundidee ist so alt wie die Informatik, in der Vermischung mit organisatorischen Strukturen wird aus SOA die objekt-/modulorientierte „Balanced Scorecard“ der Neuzeit.

Zuerst einige Grundbegriffe, um die folgenden Ausführungen klarer zu machen:

1) Was ist SOA:
Versuch einer Definition

a. Service-Orientierung als das fundamentale Design-Prinzip

b. Kern-Geschäftsprozesse werden Top-Down herunter gebrochen auf ihren Service-Bedarf

c. Services werden granular und nicht redundant definiert (Beispiel: die Definition eines Kunden ist nur einmal im Unternehmen vorhanden und wird in allen Prozessen genutzt, es gibt keine unterschiedlichen Kundendatenbanken)

d. Services werden typischerweise in Domainen erbracht (Zuständigkeits-Bereichen), die ihre interne Struktur verbergen und Service-Schnittstellen zu anderen Domainen bieten. Unter einem Service wird dabei die Veränderung von Daten im Rahmen einer Funktion verstanden, Beispiel: neuen Kunden anlegen, Vertrag anlegen

e. Diese Domainen sind auch häufig räumlich, sprich systemtechnisch, verteilt und unterliegen getrennten Kontroll-Instanzen (OASIS Sichtweise der distributed ownership domains)

f. SOA-Dienste sind unabhängig von Herstellern, Plattformen, Entwicklungs-Technologien und Schnittstellen-Technologien. Alle Formen von Schnittstellen können Basis von SOA sein: RPC, DCOM, SOAP, WDSL. Im Markt wird SOA jedoch gedanklich häufig mit SOAP verknüpft

g. SOA erfordert eigene und spezielle Modellierungs-Technologien, zum Bespiel SOAD=Service Oriented Analysis and Design. Mit Sicherheit gibt es auch einen Toolbedarf, hier können im ersten Ansatz sicher die aus der Prozess-Optimierung/Beschreibung bekannten BPM-Tools zum Einsatz kommen (ARIS

als Beispiel). Sollte Ihnen das als sehr komplex erscheinen, dann sind Sie SOA gerade ein Stück näher gekommen. Auf jeden Fall hängen Business Process Management und SOA eng zusammen

Einen guten Zugang zu SOA bietet Wikepedia, von dort aus gibt es diverse Links zu wichtigen anderen Dokumenten und Organisationen

2) SOA und Standards:
das Chaos beginnt

SOA ist durch seine gedankliche Nähe zu Web-Technologien untrennbar mit der Vision der Nutzung offener Standards verbunden. Die Plattform- und Herstellerübergreifende Architektur der „Distributed Ownership Domains“ legt das mehr als nahe. Zurzeit befassen sich 56 Standardisierungs-Gremien mit SOA, die Zahl ist dabei sicher flexibel und steigend. Jeder möchte schließlich dabei gewesen sein. Von einem klaren Standard kann also nicht die Rede sein. Zumindest ist damit auch eine Hersteller- und Plattform-übergreifende Interoperabilität nicht sicher gestellt. Aber es besteht wohl die Chance, sich im technischen Kern auf einige Elementar-Standards beziehen zu können. Ein Unternehmen, das SOA machen will, muss also entsprechende eigene Rahmen-Standards festlegen. Auf jeden Fall ist zu beachten, dass die angesprochenen Standards sowohl neu bzw. häufig auch noch nicht fertig sind. Es besteht also zum Beispiel keinerlei Praxiserfahrung zur Frage der Skalierbarkeit derartiger Architekturen. Auch ist heute nicht absehbar, wie viele Änderungen es im Bereich Technologien innerhalb der nächsten Jahre noch geben wird.

Betrachtet man die Erfahrungen, die man in den letzten 20 Jahren mit derartigen Techniken und Organisationen gemacht hat, dann sollten eigentlich folgende Erkenntnisse gegeben sein:

1) Technische Erkenntnisse

a. Die Idee der Unternehmens-Datenmodelle war Ende der 80er Jahre ein Megathema. Auch wenn nun aus dem Datenmodell ein Service-Modell wird (was technisch dem Design der Zeit entspricht), ändert es nichts an der Komplexität des Vorhabens. Die Zahl der Unternehmen, die am Thema Unternehmens-Datenmodell gescheitert sind, ist sehr hoch. Sind Service-Modelle wirklich einfacher, insbesondere wenn sie granular und nicht-redundant sein sollen?

b. Verteilte Architekturen haben ohne Frage sowohl ihren Reiz als auch ihre Vorteile. Im Zeitalter der Web-Technologien ist man nur modern, wenn man verteilt ist. Aber seit der ersten Einführung Ende der 70er Jahre ist ihr Kernproblem in der Performance zu sehen. Beispiel: jeder, der in den letzten 10 Jahren versucht hat, SQL über WAN-Verbindungen zu betreiben, wird die Nutzlosigkeit dieses Bestrebens schnell eingesehen haben. Nun greift man mit SOA nicht mehr direkt auf Tabellen zu sondern auf Services, was den Interaktionsgrad (den Umfang des Ping-Pongs) deutlich reduziert (im Endeffekt die Kernidee von Java, Interpreter, aber bei einer deutlich optimierteren Befehlsstruktur). Aber die Grundidee, dass der Austausch von XML-Daten über HTTP in hohen Transaktionsraten performant sein soll, muss erst noch belegt werden. Eigentlich scheint diese Annahme wenig wahrscheinlich, da das Parsen von XML-Paketen einen hohen linearen Aufwand generiert, der sowohl Zeit kostet als auch zu einer permanent steigenden Last führt

2) Organisatorische Erkenntnisse

a. Die Idee, die Kernprozesse eines Unternehmens im Top-Down-Ansatz herunter zu brechen und auf eine nicht-redundante Service-Struktur abzubilden ist in der Theorie sicher gut. Mindestens vier Aspekte geben zu denken. Erstens setzt diese Idee voraus, dass ein Unternehmen seine Kernprozesse kennt und formal beschreiben kann. Dies ist in einigen Branchen durchaus üblich, in vielen aber nicht. Zweitens, dass diese mindestens so lange stabil sind, dass sich die Investition in SOA rentieren kann. Drittens, dass ein umfassender Ansatz über alle

Kernprozesse auf einen Schlag gewählt wird, weil sonst die Nicht-Redundanz der Services gar nicht gewährleistet werden kann. Viertens, dass die bestehende Organisation überhaupt willig ist, sich zu verändern. Ich möchte an dieser Stelle noch einmal an die Balanced Scorecard-Diskussion erinnern. Für alle Service-orientierten Unternehmen war und ist die Balanced Scorecard ein hervorragendes Instrument der Überarbeitung bestehender Kernprozesse. Im Vergleich zu SOA ist sie von geringer Komplexität. Nun hat sie sich nicht durchgesetzt, weil sie zu theoretisch und zu aufwendig war. Aha, aber warum soll denn SOA funktionieren, das demselben Grundgedanken folgt, nur ungleich aufwendiger ist?

b. Im Datenbankdesign hat sich gezeigt, dass das Ziel nicht-redundanter Datenstrukturen fast immer mit einem Performance-Desaster verbunden ist. Dementsprechend ist das Konzept der gezielten Denormalisierung zur Optimierung von Performance hier auch ein gelebter Standard. Analysiert man SOA-typische Umgebungen, so stellt man schnell fest, dass wesentliche Daten / Services in Applikationen verschiedener Hersteller vergraben liegen. Die Erwartung, dass diese sich auf ein gemeinsames Service- und Datenmodell einigen, kann als Null angesehen werden. Wie realistisch ist da das Ziel nicht-redundanter-Services? Technisch ist das nur mit einem Meta-Datenmodell zu lösen, das die notwendigen Daten und Services in einer Meta-Struktur (einer Service-Domain im SOA Sprachgebrauch) zusammen fasst und von dort als Service für die Unternehmens-Prozesse anbietet. Damit sind wir wieder beim Performance-Thema. Diese Art von Ansätzen mag bei Teilmengen von Daten funktionieren (Benutzerdatenverwaltung und Zentrales Login zum Beispiel), aber nicht bei Daten, auf die mit hohen Transaktionsraten zugegriffen wird. Liest man diverse Artikel aus aktuellen SOA-Projekten, insbesondere von den CEO´s und CTO´s verfasst, dann loben diese das Domainen-Modell, da hier die innere Struktur der Domainen verborgen bleibt. Das würde ich aus der Sicht eines CEO´s auch gerne so sehen, immerhin kann man damit alle wirklichen Probleme in die Domain-internen Bereich abschieben, muss sich damit nicht befassen (ist auch nicht die Aufgabe eines CEO´s/CTO´s) und kann als der große SOA-Held erscheinen. Aber woher kommt die Gewissheit, dass Domainen-intern die technischen Aufgaben wirklich gestemmt werden können? Liegt hier wirklich eine tragfähige Machbarkeits-Analyse vor? Skalierbarkeits- und Performance-Probleme liegen dermaßen auf der Hand, dass die Frage nach der Machbarkeit schon gestellt werden sollte.

Warum ist SOA also so ein Hype, wenn man die geschilderten Sichtweisen betrachtet? Nun zum einen ist SOA ein sehr schwammiger Begriff. Jeder, der die Botschaft transportieren möchte: ich bin modern, ich treibe mein Unternehmen voran, wir sind Service-orientiert, kann SOA in den Mund nehmen, wenn auch nur eine simple SOAP-Anwendung im Spiel ist. Von daher ist es auch kein Wunder, dass „Jeder“ SOA macht. Gerne wird hier auch der eigentlich organisatorische Ansatz geleugnet und SOA als technisches Thema behandelt.

Zum anderen ist SOA, wenn es wirklich vorangetrieben wird, ein Riesengeschäft für die IT-, Consulting- und Netzwerk-Industrie. „Richtige“ SOA-Projekte sind nicht klein, sie erreichen in den Großunternehmen schnell den Wert höherer zweistelliger Millionen-Beträge. Klar, dass hier auf der Seite der SOA-Industrie ein elementares Interesse daran besteht, diese Entwicklung zu forcieren.

Was ist nun aus diesen Ausführungen zu schließen? Alles in die Mülltonne und ignorieren? Sicher nicht. Die Optimierung von Kernprozessen und die Schaffung einer IT, die sich an den Kernprozessen und nicht an sich selbst orientiert, ist ohne Frage immer ein sinnvolles Ziel.

Aber: viele wirklich gute Entwicklungen der letzten 20 Jahre sind daran gescheitert, dass sie zum Hype gepuscht worden, unprofessionell und unüberlegt in die Unternehmen gedrückt wurden und dann logischerweise gescheitert sind. Dabei waren die Ideen in der Regel gut, die schlampige Umsetzung war das Problem. Wie viele Großunternehmen haben blind Verträge für System-Management in hohen zweistelligen Beträgen unterschrieben, ohne ein klares Ziel oder Konzept zu haben. Nachdem die Projekte dann naturgemäß gescheitert sind, war natürlich die „unreife“ Technik schuld. Dieses Schicksal sollte SOA wenn möglich erspart werden.

Dazu die Kernfragen:

1) Sind sie wirklich bereit, ihre Organisations-Strukturen völlig zu verändern, alte Zöpfe abzuschneiden, bestehende Führungspositionen zu eliminieren?
2) Sind sie wirklich bereit, erhebliche Summen in ihre Infrastrukturen zu investieren?
3) Sind Sie bereit Ihr IT-Personal signifikant auszubauen? SOA erfordert Personal in einem erheblichen Umfang. Und SOA ist kein Einmal-Aufwand. Die geschaffenen Strukturen bedürfen der permanenten Pflege. SOA erfordert den Kern-Informatiker (tatsächlich mal was, für das Informatiker wirklich ausgebildet worden sind), Sie müssten also schon bereit sein, eine erhebliche Anzahl an zusätzlichen Informatikern einzustellen. Ist nicht modern, machen Sie lieber mit externen Dienstleistern? Natürlich gerne, wir stehen alle bereit, aber externe Dienstleister sind in der Regel nur wirtschaftlich, wenn starke Einmal-Aufwände anstehen. SOA ist aber ein permanenter Aufwand.

OK, sie sind bereit? Sie sind SOA-willig und ich nur ein Nörgler. Wunderbar. Dann fangen wir doch mit einer Service-Modellierung von Teilnehmer-/Benutzerdaten in ihren Unternehmens-Netzen an. Dies ist kein Top-Down Ansatz, aber ist technisch prädestiniert für SOA, sozusagen der Muster-Anwendungsfall außerhalb der Kundendaten (Kunden,Verträge, Dienste sind die sonst übliche Ansatzform für SOA). Das Thema predigen alle Berater seit Jahren, weil es wirklich elementar ist. Sie brauchen das bestimmt, zum Beispiel für alle Sicherheits-Konzepte, für eine zentral gesteuerte Authentifizierung und für die immer weiter zunehmenden Kollaborations-Anwendungen, die von der Natur der Sache her Plattform-übergreifend sind.

Teilnehmer-/Benutzer sind u.a. in folgenden Systemen tätig

1) Daten-Netzwerken (1x-Autentifizierung)
2) Sprach-Netzwerken (IP-Telefonie)
3) Kollaborations-Netzwerken
4) Endgeräten
5) Servern
6) Applikationen
7) Sicherheits-Systemen

Wir brauchen dringend ein Hersteller-neutrales und Plattform-übergreifendes Konzept der Benutzer-Verwaltung. Die immer stärker werdende Diskussion um die Unified Clients für Kommunikations-Anwendungen macht das sehr deutlich. Wenn Sie sich nicht auf ewig einem Hersteller verschreiben wollen, brauchen Sie eine Hersteller- und Plattformneutrale Umsetzung von Teilnehmer-Datenbanken, Adressverzeichnissen, Gelben Seiten usw.

Zu komplex, können wir nicht leisten? Dies ist ein Bruchteil von SOA, im „Big-Picture“ ein Klecks. Vielleicht könnten wir damit schon mal anfangen.

Ihr
Dr. Jürgen Suppan

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

Änderungen im Programm behält sich der Veranstalter vor!

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

Das Programm entnehmen Sie bitte den Folgeseiten. 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

Anmeldung

ComConsult SIP-Forum 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

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

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

Programmübersicht ComConsult SIP-Forum 2007

Montag, den 14.05.2007

9:30 bis 10:30 Uhr

TK-Lösungen auf der Basis des SIP-Standards: was bedeutet das?

- Internationale Marktsituation heute
- Telefonie als IT-Applikation: was bedeutet das eigentlich?
- Traditionelle TK versus IP-Telefonie verus SIP: wo liegen die Vor- und Nachteile für den Anwender?
- Nutzungsbereiche von Offenheit und der Reifegrad:
  - Telefon
  - Telefon-Programmierung
  - Applikationen und Schnittstellen
  - Architektur
  - Betrieb
- Bewertung der Strategien ausgewählter Hersteller:
  - Wo steht Siemens und was ist das Ziel?
  - Cisco CallManager 6 und Unified Communication, was will Cisco wirklich?
  - Microsoft: warum Microsoft den Markt verändern wird?
  - welche Rolle spielt IBM?
- Bewertung der Gesamtsituation
  - Wie wird SIP den Herstellermarkt und die Positionen der Hersteller verändern?
  - Wo liegen Risiken und Fragezeichen?
  - Wo liegen Vor- und Nachteile für den Anwender
- Fazit: was sollte der Anwender heute tun?

Dr. Jürgen Suppan, ComConsult Research

10:30 bis 13:00 Uhr

Ergebnisse der SIP-Studie

- Die SIP-Grundidee
- SIP: Architektur und Protokoll im Überblick
- SIP in der Praxis: wie sehen typische Einsatz-Szenarien aus, wie sind sie redundant auslegbar
- Bedarf nach SIP-Compliance und Compliance-Kriterien

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

14:30 bis 15:30 Uhr

SIP: IP-basierende Echtzeitkommunikation bei DaimlerChrysler

Dipl.-Ing. Holger Lieb, DaimlerChrysler AG

16:00 bis 17:00 Uhr

Analyse: Telefonieren mit Microsoft: Wie weit wird Microsoft den Markt verändern?

- Microsofts Unified Communications Strategie
- Analyse: welche Auswirkung hat der Microsoft UC-Client auf die Branche?
- Übersicht über die Serverprodukte, d.h. Communications Server, Exchange Server und LiveMeeting
- Microsofts Office Communications Server 2007 als neue Kernkomponente
- Client-Software und ihre Integration mit anderen Produkten
- Standards, die von Microsoft unterstützt werden
- Strategische Allianzen und ihre Bedeutung
- Roadmap: wie sieht die Zeitachse aus, wann kommt Version 3?
- Kann MS eine traditionelle TK-Lösung ersetzen?

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr

Asterisk: Applikations-Server oder vollständige PBX-Lösung?

- Geschichte und Hintergrund
- Übersicht der grundlegenden Leistungsmerkmale
- Architektur und Erweiterungsmöglichkeiten
- Asterisk vs. SIPPING
- Distributionen und kommerzielle Lösungen
- Das Lizenzmodell und seine Auswirkungen
- Bedeutende Referenzinstallationen
- Unified Communications Lösungen mit Asterisk
- DUNDI und andere Mechanismen zur Sicherstellung der Verfügbarkeit
- Kostenvergleich mit Lösungen konventioneller Hersteller

Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 15.05.2007

9:00 bis 10:00 Uhr

Cisco Unified Communications Manager 6.0: Protokollphilosophie, SIP und Unified Communications

- Historie und Abgrenzung: CM 4/5/6
- Was bedeutet SIP aus der Sicht von Cisco
- Leistungsumfang im Vergleich zu SIPPING19
- Stellenwert von Skinny im CM6
- Offenheit der Architektur
  - Einbindbarkeit der Telefone anderer Anbieter
  - Nutzung von CISCO-Telefonen an SIP-Produkten anderer Hersteller
  - Integration von Applikationen von Drittherstellern
  - Nutzung von CISCO-Gateways in offenen SIP-Lösungen
- Unified Communication: Bedeutung und zukünftige Entwicklung
- Ausblick auf die weitere Roadmap

Daniel Gluch, Cisco Systems Deutschland

10:00 bis 11:00 Uhr

Die Siemens-Kommunikations-Strategie im Rahmen offener Standards

- Bedeutung von Software-Lösungen für den Markt
- Siemens Statement zu SIP
- HiPath 8000: Positionierung in der Siemens-Strategie
- Applikations-Architekturen
- Wie offen kann eine Lösung sein

Rudolf Bitzinger, Siemens AG

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

11:30 bis 12:30 Uhr

Sicherheit und SIP: was ist zu tun?

- Nutzung von SIP für die Signalisierung verschlüsselter Sprach-übertragung
- Verschlüsselung und Authentifizierung von SIP-Nachrichten
- Aufbau einer Vertrauenskette bei SIP-Signalisierung
- SIP und Firewalling
- Sicherheit bei externer SIP-Kommunikation ueber Trunks zu Provider-Netzen

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

14:00 bis 15:00 Uhr

Hosted-Services auf der Basis von SIP

- Bedeutung und Leistungsumfang von Hosted Services
- SIP als tragendes Element einer offenen Lösung
- Ausblick auf zukünftige Potenziale derartiger Lösungen

Dr. Jörg Fischer, Alcatel Deutschland GmbH

15:00 bis 16:00 Uhr

SIP: Brücke zwischen TK und TK-nahen Applikationen

- SIP als Voraussetzung für mehr Flexibilität und niedrigere Kosten
- Vorreiteranwendungen: Unified Messaging, CTI und Instant Messaging
- ACD, CRM, Voice Recording, Alarmserver, u.a. Applikationen
- Die Rolle von SIP bei der Fixed Mobile Konvergenz
- Telefone als generische Benutzerschnittstellen
- Hersteller und Lösungen

Dr. Frank Imhoff, Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH

Der Veranstalter behält sich Änderungen im Programm vor!

Zweitthema

Virtuelle Poststellen - sichere E-Mail für alle?

Fortsetzung von Seite 1

Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Man denke hier nur an den Erhalt eines erarbeiteten technologischen Vorsprungs während der gemeinsamen Entwicklungsarbeit über Standort- und mitunter sogar Unternehmensgrenzen hinweg oder an sensible Inhalte von Vertragstexten oder Angeboten. All dies soll verständlicherweise vor unbefugtem Zugriff möglichst sicher geschützt werden.

Derartige Informationen wurden früher in verschlossenem Umschlag der Post anvertraut - sofern man nicht aufgrund der besonderen Brisanz bestimmter Nachrichten auf Kuriere zurückgreifen musste. Die Rolle der Briefpost hat im Zeitalter des weltumspannenden Internets deren elektronisches Pendant übernommen. Allerdings bedarf es geeigneter Maßnahmen zum Schutz der Nachrichten während des Übermittlungsvorgangs: denn obwohl die Reisezeit elektronischer Post gegenüber der daher auch gern als „Snail Mail“ belächelten konventionellen Variante in aller Regel vernachlässigbar kurz ist, ist dennoch das Risiko eines Informationsabflusses an Unbefugte erheblich größer. Immerhin kennt die heute gebräuchliche E-Mail Technologie keinerlei informationstechnische Entsprechung des klassischen Briefumschlags, der konventionelle Briefpost vor neugierigen Blicken schützt und zumindest ein unbemerktes Lesen der Post erheblich erschwert; eine nicht durch Zusatzmaßnahmen geschützte E-Mail ist daher weit eher mit einer Postkarte vergleichbar, denn mit einem Brief. Und schlimmer noch: sogar Manipulationen am Inhalt der übermittelten Nachrichten sind prinzipiell mit Leichtigkeit möglich, ohne dass dieses dem Empfänger einer derart ihrer Integrität beraubten Botschaft unmittelbar auffallen kann.

Zum Glück lassen sich über zusätzliche Schutzmaßnahmen derartige Angriffe auf die Vertraulichkeit und Integrität von E-Mails wirksam verhindern: Kryptografie wird schon seit dem Altertum eingesetzt, um übermittelte Botschaften abzusichern und steht spätestens seit Mitte der 90er Jahre des vorigen Jahrhunderts auch Unternehmen, Behörden und sogar Privatpersonen zur Verfügung. Bis zu diesem Zeitpunkt erforderten speziell Lösungen zur E-Mail-Verschlüsselung enorme Rechenkapazitäten, die in der Regel nur Geheimdiensten oder allenfalls Großkonzernen oder Universitätsrechenzentren zur Verfügung standen. Die Ursache hierfür lag in den aufwändigen mathematischen Algorithmen, die bei sicheren (genauer: derzeit als sicher angesehenen) asymmetrischen Verschlüsselungsverfahren zum Einsatz kommen: die Geheimhaltung des privaten Pendants zu einem öffentlichen Schlüssel basiert auf der Verwendung so genannter „Einwegfunktionen mit Hintertür“ auf Basis sehr großer Primzahlen. Klassische Vertreter im Umfeld von Public Key Infrastructures (PKI) sind RSA - benannt nach seinen Entwicklern Rivest, Shamir und Adleman - , Diffie-Hellman oder El-Gamal.

Erst die Veröffentlichung von PGP (Pretty Good Privacy) durch Phil Zimmerman ermöglichte es auch mit Ressourcen, wie sie ein damals üblicher Arbeitsplatzrechner zur Verfügung stellte, komfortabel und sicher E-Mails zu verschlüsseln und zu signieren. PGP verwendete erstmals ein so genanntes Hybrid-Verfahren, bei dem die rechenintensiven Algorithmen nur zur Chiffrierung eines symmetrischen Schlüssels verwendet werden, nicht jedoch zur Verschlüsselung der gesamten Nachricht. Letztere wird stattdessen unter Verwendung des symmetrischen Schlüssels erheblich schneller ver- und natürlich auch entschlüsselt.

Das PGP-Problem

Leider hat PGP - und mit ihm alle vergleichbaren E-Mail-Verschlüsselungslösungen - einen nicht zu unterschätzenden Nachteil: es handelt sich dabei typischerweise um Einzelplatzlösungen für den E-Mail-Client des jeweiligen Anwenders. Grundsätzlich erfüllen alle diese Lösungen zwar die typischerweise spezifizierten Sicherheitsanforderungen, sofern hinreichend starke kryptografische Verfahren, d.h. insbesondere solche mit ausreichender Schlüssellänge, genutzt werden. Als problematisch hat sich jedoch der Betrieb solcher Lösungen in größeren Netzwerkumgebungen erwiesen. Aufgrund des Einzelplatzcharakters ist grundsätzlich eine mehr oder minder aufwendige Administration der jeweiligen Client-Installation erforderlich. Auch die Bereitstellung der notwendigen öffentlichen Schlüssel für alle an der jeweiligen Kommunikation Beteiligten generiert einen nicht zu unterschätzenden Overhead. Schließlich ist auch ein gewisses Augenmerk auf die Nutzer derartiger Lösungen zu richten: da heute der Einsatz von Verschlüsselung im Zusammenhang mit dem Austausch von E-Mails noch immer eher die Ausnahme als die Regel darstellt, stellt sich mangels regelmäßiger Nutzung bei vielen Anwendern die ansonsten hilfreiche Routine nicht oder stets nur phasenweise ein. Die Folge ist ein intensiver Betreuungsbedarf bei den meisten Nutzern hinsichtlich der Bedienung der jeweiligen Software.

Auch ist festzuhalten, dass insbesondere PGP zwar vor allem im Consumerbereich einen hohen Verbreitungsgrad erlangt hat, aber nicht den einzigen relevanten Standard für verschlüsselte E-Mail-Kommunikation darstellt. Insbesondere im Bereich des professionellen E-Mail-Einsatzes kommt häufig S/MIME (Secure Multip-

urpose Internet Mail Extensions) zur Anwendung. Die Inkompatibilität der beiden Standards führt dazu, dass ggfs. einer der beiden Kommunikationspartner ein zusätzliches Produkt neben seiner etablierten Standardlösung einsetzen muss. Auch dadurch steigt der Administrations- und Betreuungsaufwand - wenn auch in der Regel nicht auf beiden Seiten der Kommunikationsbeziehung.

Deutlich besser geeignet wäre hier eine Lösung mit zentralistischem Ansatz. Bei diesem Prinzip wird ein spezieller Server eingesetzt, der aus- und eingehende Mails bei Bedarf zentral einer Ver- bzw. Entschlüsselung unterwirft.

Basierend auf den mit gängigen Standalone-Lösungen gemachten meist eher negativen Erfahrungen sowie unter Berücksichtigung genereller Erwägungen - insbesondere hinsichtlich Sicherheit und Handhabbarkeit - lassen sich folgende grundsätzlichen Anforderungen an eine derartige Lösung formulieren:

- Die Lösung muss eine Verschlüsselung und Signatur nach dem aktuellen Stand der Technik bieten.
- Die Lösung muss zumindest zu den beiden am weitesten verbreiteten Standards für sicheren E-Mail-Verkehr, OpenPGP und S-MIME, kompatibel sein.
- Die Lösung sollte Optionen für den kontrollierten automatisierten Import von unterstützten Zertifikaten aus vorhandenen Client-Installationen bzw. empfangenen E-Mails bieten.
- Die Lösung muss ohne einen speziellen Client bzw. spezielle Client-Erweiterungen (Plug-Ins o.ä.) auskommen.
- Die Lösung sollte zur Vermeidung von Bedienfehlern weitestgehend automatisiert arbeiten, d.h. ohne bewusstes Zutun des jeweiligen Anwenders alle E-Mails, die als vertraulich eingestuft sind, der Verschlüsselung unterwerfen. Im Idealfall stellt sich die Lösung für den Anwender somit völlig transparent dar.
- Die Lösung sollte nach Möglichkeit auch für Umgebungen mit hoher Fluktuationsrate geeignet sein, da „vertrauliche Kommunikationsbeziehungen“ auch wechseln können und in solchen Fällen auch für neue Kommunikationsbeziehungen meist die Forderung nach schneller Verfügbarkeit der Verschlüsselungsoption gestellt werden wird.

Die Lösung: Virtuelle Poststellen

Einen besonders eleganten Weg zur Lösung der skizzierten Aufgabe bieten so genannte virtuelle Poststellen, die ein Mail-Gateway mit einem per Web-Browser nutzbaren Ablageserver nach folgendem Prinzip kombinieren:

- Das Mail-Gateway der virtuellen Poststelle untersucht jede ausgehende E-Mail dahingehend, ob diese zu verschlüsseln und/oder zu signieren ist. Falls nicht, wird die E-Mail unverändert weitergeleitet. Die Anweisung, ggfs. zu verschlüsseln bzw. zu signieren, kann sich dabei u.a. aus einer zentral einzurichtenden Richtlinie (z.B.: „Alle Nachrichten an Empfänger name@maildomain.de sind zu verschlüsseln!“) oder auch aus dem Inhalt der Nachricht, etwa der Betreffzeile, ergeben (z.B. gibt es Lösungen, die E-Mails verschlüsseln, wenn der Betreff mit einem bestimmten Schlüsselwort beginnt).
- Muss Verschlüsselung eingesetzt werden, prüft das Gateway, ob es im Besitz der notwendigen Schlüsselinformationen für den Empfänger ist. Falls ja, kann das Gateway die Mail geeignet verschlüsseln und der Empfänger die verschlüsselte Mail offensichtlich verarbeiten. Letzteres impliziert insbesondere das Vorhandensein eines entsprechenden Clients.
- Ist keine Schlüsselinformation vorhanden - sei es, weil der Empfänger keine E-Mail-Verschlüsselung einsetzt und daher verständlicherweise auch nicht im Besitz eines kompatiblen öffentlichen Schlüssels ist, oder weil mit diesem Empfänger bis dato noch keine Kommunikation stattgefunden hat - , so wird die Mail in ein Postfach eines zur Lösung gehörenden Web-Mailers umgeleitet; der Empfänger enthält eine entsprechende Benachrichtigung, dass in diesem Postfach eine Mail für ihn eingegangen ist.
- Der Zugriff auf das Web-Mail-Postfach erfolgt mittels Browser via HTTPS. Die Mail kann jetzt gelesen bzw. bei Bedarf auch auf den eigenen E-Mail-Client heruntergeladen werden.
- Über den Web-Mail-Zugang kann der Empfänger auch auf die empfangene Mail antworten bzw. aktiv Mails versenden.
- Umgekehrt werden alle ankommenden verschlüsselten E-Mails entschlüsselt und die Signaturen aller ankommenden signierten E-Mails auf Korrektheit überprüft.

Dieser Ansatz erfüllt die meisten der oben formulierten Anforderungen. Insbesondere ist die geforderte Transparenz für die Anwender gewährleistet. Auch sind alle auf diesem Wege ausgetauschten E-Mails auf dem gesamten Übertragungsweg geschützt.

Einzig verbleibendes Risiko ist die Möglichkeit, dass ein externer Kommunikationspartner vertrauliche E-Mails unverschlüsselt über den „normalen“ E-Mail-Weg sendet. Dies lässt sich auf technischem Wege kaum zuverlässig verhindern und muss daher anderweitig unterbunden werden, z.B. über entsprechende vertragliche Regelungen.

Der Markt in diesem Segment ist vergleichsweise überschaubar, zumindest in Deutschland: eine projektbezogene Recherche lieferte im Jahre 2006 folgende Anbieter kommerzieller Produkte:

- ICC: Julia Mail Office
- Utimaco: Secure E-Mail Gateway
- PGP: PGP Universal 500
- Zertificon: Secure Mail Gateway

Der grundlegende Funktionsumfang ist übrigens mittlerweile bei allen Produkten vergleichbar:

- Unterstützung von PGP zur E-Mail-Verschlüsselung
- Unterstützung von S/MIME zur E-Mail-Verschlüsselung
- Integrierter bzw. zurüstbarer Web-Mailer als Fallback-Option für Empfänger, die weder PGP noch S/MIME unterstützen

Insofern sollten alle benannten Lösungen grundsätzlich für eine konkrete Realisierung infrage kommen. Unterschiede sind freilich in Details der Handhabung und der Administration auszumachen. Diese fallen zwar in aller Regel nicht gravierend aus und sind häufig lediglich geeignet, einen von mehreren kostentechnisch vergleichbaren Kandidaten zu präferieren. Dennoch oder gerade deshalb sollte diesem Aspekt bei einer etwaigen Produktentscheidung die notwendige Aufmerksamkeit zuteil werden.

Zu den Fragestellungen, die in diesem Zusammenhang möglicherweise zu klären sein werden, gehören u.a. die nachfolgend aufgeführten:

Art und Schutz administrativer Zugriffe

Da auch die fortschrittlichste Virtuelle Poststelle bei aller Transparenz für den Anwender eines kontinuierlichen Managements durch einen Administrator bedarf, lohnt es sich, einen Blick auf die entsprechende Schnittstelle, sprich das Graphical User Interface, kurz GUI, zu werfen - sofern vorhanden und nicht stattdessen ein spartanisches Command Line Interface (CLI) herangezogen werden muss.

Von großem Vorteil ist es, wenn der administrative Zugriff via Web-Browser erfolgen kann: der landläufige Administrator sollte mit dieser Client-Software umgehen können und eine Installation ist nicht notwendig, so dass prinzipiell eine Administration von jedem beliebigen Büroarbeitsplatzrechner aus erfolgen kann. Diese Zugriffe müssen natürlich ausreichend gegen Mitlesen und/oder Manipulation geschützt sein; hierzu bietet sich z.B. die Nutzung von HTTPS an.

Schutz der Nachrichten auf dem Web-Mailer

Basis des Web-Mailers ist grundsätzlich eine Web-Server-Applikation, auf die von jedermann mindestens mittels HTTPS zugegriffen werden kann. Aufgrund dieser Konstellation und vor dem Hintergrund der Erfahrungen mit der Sicherheit von Web-Server-Implementierungen muss von einem nicht vernachlässigbaren Restrisiko ausgegangen werden, dass im Zuge eines Angriffs auf diese Web-Server-Applikation ein Datenzugriff durch Unbefugte möglich ist.

Insofern in jedem einzelnen Fall zu prüfen, ob erweiterte Anforderungen an die Absicherung der Postfachinhalte des Web-Mailers zu stellen sind. Ein denkbarer Ansatz könnte z.B. eine Verschlüsselung der Nachrichten sein. Zu beachten ist dabei, dass eine Verschlüsselung auf Betriebssystemebene oder darunter vermutlich keinen akzeptablen Schutz bietet, da unbefugte Zugriffe der beschriebenen Art möglicherweise unter Missbrauch der Identität berechtigter User bzw. Applikationen erfolgen.

Verhindern ungewollter Klartextkommunikation

Einige Lösungen (Beispiel: PGP) bieten beim erstmaligen Zugriff auf den Web-Mailer einen Auswahldialog, der es dem externen Mail-Empfänger ermöglicht, das zukünftige Verhalten des Mail Gateways zu beeinflussen. Steht als Option dabei u.a. auch der zukünftige Empfang von Klartext-Mails zur Verfügung, so ist zu prüfen, ob diese Option durch Setzen serverseitiger Parameter abschaltbar ist. Andernfalls könnte ein Empfänger versehentlich die Verschlüsselungsfunktion des Gateways für an ihn gerichtete Nachrichten außer Kraft setzen.

Kontrolle der Nutzerlizenzierung

Die oben erwähnten Produkte werden allesamt User-basiert lizenziert. Dabei ist nicht per se klar, welche internen User der Lizenzierung zugrunde zu legen sind. In der Regel dürfte es sich zwar um „aktive“ User handeln, d.h. solche, die die Funktion der virtuellen Poststelle nutzen, aber es sollte dennoch geprüft werden, wer durch das Gateway (bzw. den Anbieter) als „aktiver“ User angesehen wird. Es bestehen hier durchaus verschiedene Möglichkeiten:

- User, die als Sender verschlüsseln und/oder signieren
- User, an die eine empfangene verschlüsselte und/oder signierte E-Mail weitergeleitet wird
- User, die Mails mit externen Adressaten austauschen
- User, die prinzipiell die Möglichkeit haben, zu den bisher genannten zu gehören
- Beliebige Kombinationen davon

Um nicht plötzlich ungewollt gegen die Lizenzbedingungen zu verstoßen, sollte zusätzlich untersucht werden, ob und auf welche Weise die Lösung ein Controlling der Lizenzen unterstützt. Dabei sollte nicht vergessen werden, dass häufig aufgrund interner Fristen für Beschaffungen und Budgetplanung ein sich anbahnendes Überschreiten der Lizenz bereits sehr frühzeitig erkennbar sein muss; eine bloße Warnung (oder gar Einstellung der Funktion) im Moment der Lizenzüberschreitung wird daher in aller Regel nicht ausreichen.

Sicherheit der Implementierung

Die Implementierung der Virtuellen Poststelle sollte natürlich ausreichend sicher sein. Die Anforderungen an die diesbezügliche Robustheit des Systems entsprechen mindestens denen an andere öffentlich zugängliche Server in einer DMZ der Perimeter-Firewall am Übergang zum Internet.

Insofern müssen sowohl die eingesetzte Software der Virtuellen Poststelle selbst als auch das Basissystem gegen Angriffsversuche aus dem Internet hinreichend „gehärtet“ sein. Je nach Produkt sind dabei unterschiedliche Rahmenbedingungen zu berücksichtigen:

- Handelt es sich um eine reine Software-Lösung, die auf einem unterstützten Serverbetriebssystem installiert wird, so liegt die Vorbereitung/Härtung des Serverbetriebssystems in der Verantwortung des Installateurs. Bei Basisbetriebssystemen, für die intern kein oder nur unzureichendes Know-how vorhan-

den ist, empfiehlt es sich, die Installation einschließlich Systemhärtung als Dienstleistung im Zuge der Beschaffung einzukaufen.

- Handelt es sich um eine „Soft-Appliance“, d.h. eine Lösung, die auf einer unterstützten Hardware sowohl ein entsprechend zugeschnittenes Betriebssystem als auch die Software der Virtuellen Poststelle selbst mit einer einzigen Setup-Routine installiert, so muss die Systemhärtung vom Anbieter bei der Erstellung des Setup-Datenträgers vorgenommen werden. Eine manuelle „Nachhärtung“ ist zwar meistens theoretisch möglich – zumindest wenn es sich um Systeme auf Linux-Basis handelt – , aber aufgrund der unkalkulierbaren Auswirkungen auf die Funktion des Gesamtsystems nicht unbedingt zu empfehlen. Ggfs. sollte im Zuge der Beschaffung ein Sicherheitsscan des installierten Systems durchgeführt werden, um eine ausreichende Systemrobustheit sicherzustellen.

- Handelt es sich um eine Appliance, d.h. eine Komplettlösung, bei der der Anbieter von der Hardware, über die ggfs. proprietäre Firmware bis zur Software alle Komponenten des Gesamtsystems in betriebsbereitem Zustand ausliefert, so ist eine manuelle Nachhärtung in den meisten Fällen ausgeschlossen. Umso mehr ist darauf zu achten, dass das Gesamtsystem ausreichend robust ist. Auch in diesem Falle sollte daher ein Sicherheitsscan der Appliance im Rahmen des Beschaffungsvorgangs erwogen werden.

Ausfallsicherheit

Es muss bei der Planung einer Virtuellen Poststelle natürlich auch darüber nachgedacht und letztendlich entschieden werden, ob und in welchem Rahmen Störungen der E-Mail-Kommunikation toleriert werden können. Da E-Mail kein online-Medium ist, sind vorübergehende Ausfälle des Systems häufig akzeptabel, solange die jeweilige Ausfallzeit „überschaubar“ bleibt. Muss eine permanente Funktionsfähigkeit gewährleistet sein, kommt man um den Einsatz von Hochverfügbarkeitslösungen (Cluster o.ä.) nicht herum.

Einfacher (und in der Regel deutlich preiswerter) lässt sich ein derartiges System realisieren, wenn auf die Hochverfügbarkeit verzichtet werden kann. Es sollte in diesem Fall jedoch dafür Sorge getragen werden, dass vor allem zwei wesentliche Bedingungen erfüllt sind:

- Es muss sichergestellt sein, dass Hardware-Fehler innerhalb der zulässigen Ausfallzeit behoben werden können.

  Dies kann durch einen Wartungsvertrag mit entsprechenden Service Level Parametern erreicht werden. Dies ist ein Ansatz, der sich vor allem bei Verwendung von (Hard) Appliances empfiehlt.

  Alternativ kann ein zweites System bevorratet werden (Cold Standby). Dieser Ansatz hat den Vorteil, dass die Ausfallzeit in der Regel erheblich verkürzt werden kann, macht aber aufgrund der ansonsten zu erwartenden hohen Systemkosten nur bei Software-basierten Lösungen Sinn. In diesem Fall beschränken sich die Kosten auf die Bereitstellung der Basishardware, ggfs. inklusive Betriebssystem.

- Es muss sichergestellt sein, dass die vollständige Konfiguration innerhalb der Zeitspanne wiederhergestellt werden kann, die nach Wiederverfügbarkeit des Systems noch bis zur maximal tolerierbaren Ausfallzeit verbleibt.

  Hierzu bedarf es eines geeigneten Backup- und Restore-Konzepts. Dabei ist zu beachten, dass ggfs. auch alle E-Mail-Daten auf dem Webmailer wiederherstellbar sein müssen; insofern sind nur Konzepte tauglich, die eine sofortige Sicherung jeder Änderung am Datenbestand vorsehen.

  Im Zuge der Produktauswahl und –beschaffung sollte daher sorgfältig geprüft werden, inwieweit entsprechende Funktionen zur Datensicherung bzw. deren Unterstützung vorhanden sind.

Sprachen des Web-Mailers

Es sollte sorgfältig geprüft werden, welche Sprachen der Web-Mailer unterstützt. Sinnvollerweise sollten zumindest Deutsch als auch Englisch im Angebot sein; je nach erwarteter Klientel kann es aber sehr sinnvoll sein, wenn auch andere Sprachen verfügbar sind, insbesondere Spanisch, Französisch, etc.

Benachrichtigungstexte

Die Virtuelle Poststelle versendet bei Einsatz des Web-Mailers Benachrichtigungen: zumindest an den Empfänger der Mitteilung – immerhin muss dieser ja davon in Kenntnis gesetzt werden, dass er auf diesem Wege eine E-Mail erhalten hat – , aber ggfs. auch an den Absender. Im Einzelnen sollten die im Zuge der Nutzung des Web-Mailers erforderlichen Benachrichtigungen mindestens folgende Nachrichten bzw. Texte enthalten:

- Nachricht an den externen Empfänger, dass an ihn eine Mail per Web-Mailer ausgeliefert wurde – diese sollte aus den unterstützten Sprachen frei wählbar sein, nach Möglichkeit abhängig vom Empfänger.

- Nachricht an den internen Absender, dass seine Mail per Web-Mailer ausgeliefert wurde - dies ist essentiell, wenn er beim Erstzugriff des externen Empfängers auf sein Web-Mailer-Postfach mitwirken muss.

- Zusatzinformation in Mails an den internen Empfänger, dass diese über den Web-Mailer versandt wurden - dies ist interessant, damit der Empfänger auf einen Blick erkennen kann, ob sich sein Kommunikationspartner beim Versand der Botschaft des sicheren Weges bedient hat oder nicht.

Die jeweiligen Nachrichten bzw. Zusatzinformationen sollten hinsichtlich des textlichen Inhalts frei durch den Administrator konfigurierbar sein, nach Möglichkeit abhängig vom Empfänger - dadurch können insbesondere notwendige Erläuterungen und Hilfestellungen optimal auf die jeweiligen Bedürfnisse der Anwender zugeschnitten werden. Soweit durch das Produkt vorgegebene Texte zum Einsatz kommen, sollte die jeweilige Sprache im Rahmen der unterstützten Sprachen frei wählbar sein, nach Möglichkeit abhängig vom Empfänger. Die Texte sollten Informationen zum Ablauf der Nutzung beinhalten, um Support-Anfragen - insbesondere bei erstmaliger Nutzung - zu minimieren.

Kennwortübermittlung

Erhält ein externer Empfänger erstmals eine E-Mail über den Web-Mailer, so muss er nicht nur darüber und über die Verfahrensweise unterrichtet werden; ihm müssen auch auf akzeptabel sichere Art und Weise die Anmeldeinformationen für sein persönliches Postfach auf diesem Web-Mailer mitgeteilt werden.

Hierzu existieren im Detail unterschiedliche Verfahren in den verschiedenen Produkten; klar ist jedoch, dass eine Übermittlung in der Benachrichtigungs-Mail nicht in Frage kommt. In der Regel geht man den Weg, das Kennwort über den internen Anwender, der die zu schützende Nachricht gesendet hat, übergeben zu lassen. Demzufolge enthält die Benachrichtigung an den externen Empfänger z.B. den Hinweis, dass er sein Kennwort vom Absender der auslösenden E-Mail erhält - dabei wird, durchaus nicht zu Unrecht, unterstellt, dass letzterer dem Empfänger meist bekannt ist.

Zum weitergehenden Schutz wird die Login-Information noch geteilt übermittelt: z.B. ist der Login-Name in der Benachrichtigung enthalten, so dass er dem internen Absender nicht bekannt ist. Teilweise wird auch eine Hälfte des Kennworts per Mail und die andere Hälfte per Telefon vom internen Absender übergeben. Hier sollten die jeweiligen Konzepte geprüft und auf Akzeptabilität und Praktikabilität hin evaluiert werden.

Architekturen

Die Auswahl eines geeigneten Produktes ist eine Sache, die Implementierung und dabei insbesondere die Integration in die ja in den allermeisten Fällen bereits vorhandene E-Mail-Architektur eine andere. Nach Möglichkeit sollte der Einsatz einer virtuellen Poststelle keine einschneidenden Änderungen am grundlegenden E-Mail-Konzept erforderlich machen. Da kommt es gelegen, dass zumindest alle hier angesprochenen Produkte nach dem Prinzip des E-Mail-Relays arbeiten; sie lassen sich daher normalerweise sehr leicht als weiteres Element in die vorhandene Relay-Kette integrieren - lediglich das Mail-Forwarding ist ggfs. entsprechend anzupassen, damit alle Nachrichten an das jeweils korrekte Relay-System weitergegeben werden und sichergestellt ist, dass die virtuelle Poststelle dabei zwingend durchlaufen wird.

Im globalen Kontext ist dabei die Frage nicht uninteressant, ob die Verarbeitung von E-Mails einem zentralen oder einem dezentralen Ansatz folgt. Existieren (viele) dezentrale Mail-Systeme, die Botschaften von und zu externen Adressaten unmittelbar empfangen bzw. versenden, so steigt die Komplexität einer virtuellen Poststelle deutlich an: es muss mehrere Instanzen geben - eine je möglichem Mail-Pfad - und diese müssen sich untereinander hinsichtlich ihrer Konfiguration und ihres Datenbestands (insbesondere bezüglich der bekannten öffentlichen Schlüssel) abgleichen.

Typischweise wird der E-Mail-Verkehr über eine Relay-Kette, bestehend aus dem (internen) Mail-Server, Content Security Systemen (Anti Spam, Anti Virus) - meist in einer DMZ der Firewall realisiert - sowie einem (externen) Mail-Relay abgewickelt. Davon ausgehend ergibt sich die in Abbildung 1 dargestellte Architektur für eine Relay-Kette mit integrierter Virtueller Poststelle. Damit die Content Security Systeme (in Abbildung 1 ist ein Filter mit kombinierter Anti-Spam- und Virenschutzfunktion dargestellt - bei weiteren und/oder dedizierten Systemen verlängert sich die Relay-Kette entsprechend) auch von der Virtuellen Poststelle verschlüsselte E-Mails untersuchen können, muss die Virtuelle Poststelle in der Kette weiter „außen“ angesiedelt sein. Es bietet sich an, die Virtuelle Poststelle gleichzeitig als Mail-Relay zu verwenden - vorausgesetzt, die notwendige Systemrobustheit (s.o.) ist gewährleistet.

Ist letzteres nicht der Fall, kann natürlich jederzeit auch ein separates vorgelagertes Mail-Relay eingesetzt werden (s. Abbildung 2). Hierdurch wird das Risiko für die Virtuelle Poststelle reduziert, da ein direkter SMTP-Zugriff von außen auf die Virtuelle Poststelle nicht mehr erforderlich ist. Außerdem bietet ein dediziertes Mail-Relay verbesserte Flexibilität für zukünftige Anpassungen der E-Mail-Architektur: etwaige Änderungen an Spezialsystemen haben keine externen Auswirkungen mehr, da die externe SMTP-Schnittstelle stets konstant bleibt.

Übrigens empfiehlt es sich grundsätzlich, zumindest die Web-Mailer-Komponente der Virtuellen Poststelle auf einer separaten Plattform zu implementieren. Dies wird allgemein auch von den Herstellern der angegebenen Produkte so gesehen; bei Produkten auf Appliance-Basis gibt es demzufolge dann je ein System für die eigentliche Virtuelle Poststelle und eines für den Webmailer. Zusätzlich kann erwogen werden, das Web-Mailer-System in einer separaten DMZ zu positionieren.

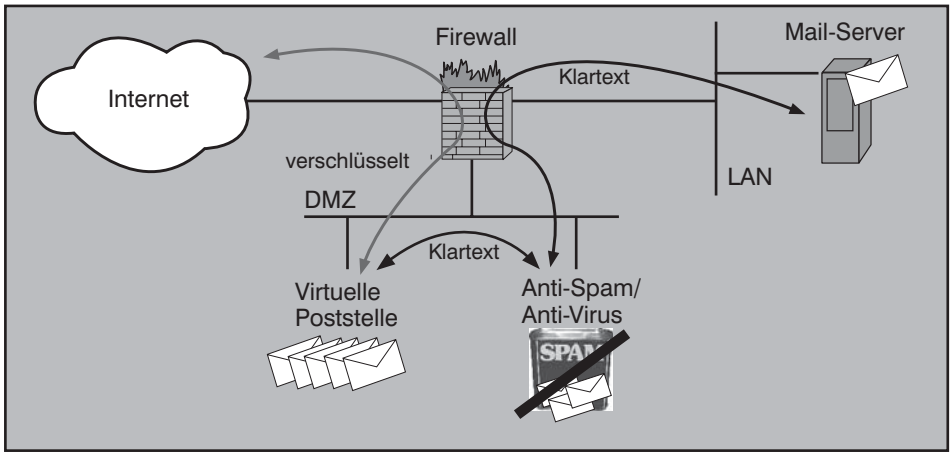


Abbildung 1: Typische Mail-Architektur mit virtueller Poststelle

Virtuelle Poststellen - sichere E-Mail für alle?

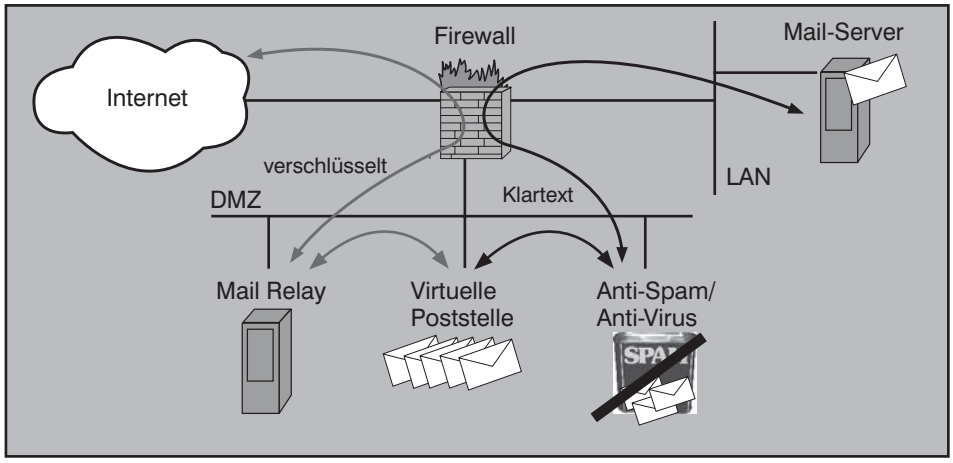


Abbildung 2: Variante mit vorgelagertem Mail-Relay

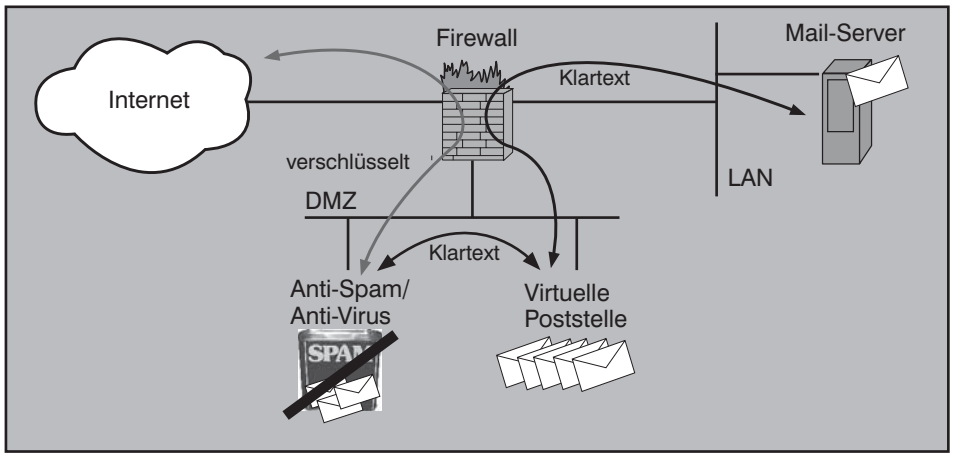


Abbildung 3: Alternative zur Nutzung spezieller Anti-Spam-Features

Allerdings verfügen manche Spam-Filter über spezielle Funktionen (z.B. Herabsetzung der „Annahmerate“ von E-Mails, die von offenkundig als Spam-verseucht anzusehenden Mail-Servern versendet werden), die nur dann genutzt werden können, wenn der Spam-Filter das äußerste Glied der Relay-Kette ist (s. Abbildung 1). Eine entsprechende Positionierung bedeutet dann aber zwangsläufig, dass eine weitergehende Content-Security durch den Spam-Filter für verschlüsselte Mails nicht geleistet werden kann. Doch keine Panik: unter Berücksichtigung der erweiterten Vertrauensstellung, die Kommunikationspartner genießen, mit denen verschlüsselt kommuniziert wird, kann diese Einschränkung der Schutzwirkung des Spam-Filters meist in Kauf genommen werden. Dies gilt insbesondere, wenn der interne Mail-Server über einen zusätzlichen eigenen Virenschutz verfügt.

Bedenken, dass womöglich infolge einer allgemeinen Veröffentlichung des öffentlichen Unternehmens-Schlüssels durch die Virtuelle Poststelle vermehrt verseuchte Mails unter dem Schutz der Verschlüsselung eindringen könnten, erscheinen dabei kaum gerechtfertigt, da eine derartige Veröffentlichung standardmäßig **nicht** stattfindet. Auch steht zu erwarten, dass insbesondere absichtliche Versender unerwünschter Mails aufgrund der jeweiligen Gesamtvolumina je Sendung von performancemindernden Verschlüsselungsoperationen in aller Regel Abstand nehmen werden, zumal der Einsatz von Verschlüsselung bereits auf entsprechende Sicherheitsmaßnahmen hinweist, die es nahe legen, eher andere, leichtere Opfer zu behelligen.

Soll trotz des insgesamt eher niedrig anzusehenden Risikos auch für verschlüsselte E-Mails ein erster Virenscan bereits innerhalb der DMZ erfolgen, so muss entweder ein kombiniertes Anti-Virus/Anti-Spam-System zweifach durchlaufen werden (siehe Abbildung 3) oder - falls eine derartige Konstellation aufgrund eventuell unzureichender Parametrierungsoptionen zu einem Loop führt - ein Einsatz dedizierter Systeme erfolgen, wobei dann die Anti-Virus-Funktion zwischen Virtueller Poststelle und internem Mail-Server installiert wird (siehe Abbildung 5).

Je nach Rahmenbedingungen können freilich auch noch andere Architekturen sinnvoll sein.

Für den Fall, dass eine für den Einsatz in der DMZ hinreichende Systemrobustheit nicht gegeben ist, - oder weil man generell ein System mit derart vergleichsweise sensibler Aufgabe nicht exponieren will - kann z.B. die Virtuelle Poststelle aus dem öffentlich zugänglichen in einen weniger exponierten Netzbereich verlagert werden; dieser kann u.U. auch das interne LAN sein. Bei diesem Ansatz muss jedoch der Web-Mailer auf ein separates System ausgelagert werden, da dieser in jedem Fall öffentlich zugänglich bleiben muss. Dieser bliebe dann zwar eine Schwachstelle im Gesamtsystem; bei einem angenommenen Ausfall infolge eines Angriffs von außen bliebe jedoch die eigentliche Virtuelle Poststelle, d.h. das Mail-Gateway, weiter einsatzfähig.

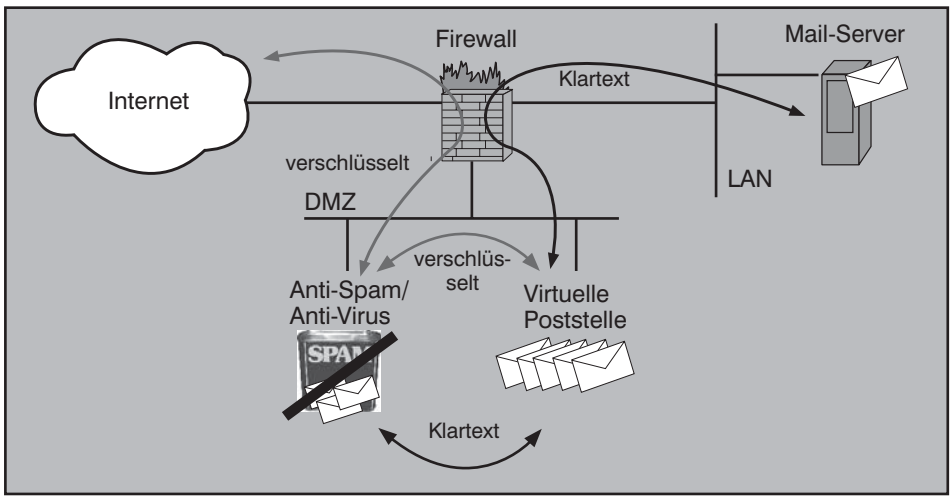


Abbildung 4: Zweifacher Durchlauf des Content Security Gateways

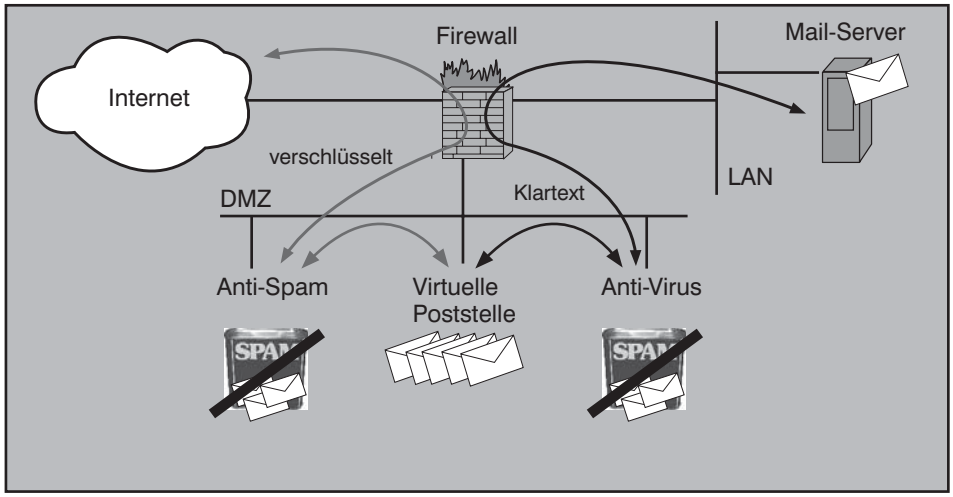


Abbildung 5: Zwei Content Security Gateways

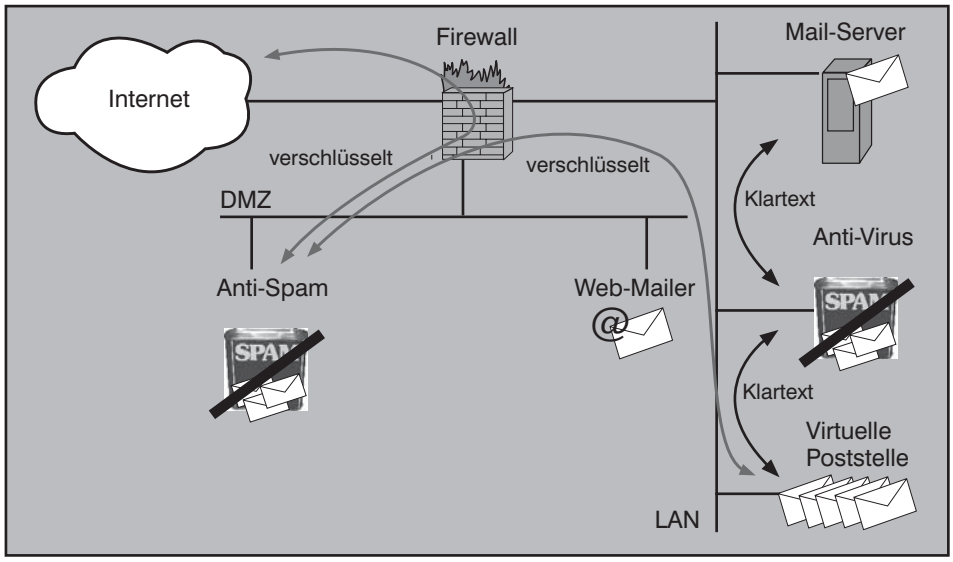


Abbildung 6: Virtuelle Poststelle im nichtöffentlichen Netzbereich

Nutzt man bei diesem Ansatz das Security Gateway als Mail-Relay, sollte jedoch auf den mehrfachen Durchlauf des Security Gateways (vgl. Abbildung 4) verzichtet und stattdessen in jedem Fall ein dediziertes zweites Gerät für den Virenscan eingesetzt werden (Abbildung 6). Steht ein dediziertes Mail-Relay ohne spezielle Content Security Funktion am vorderen Ende der Mail-Relay-Kette, kann hingegen wieder ein kombiniertes System zur Abwehr von Spam und Viren eingesetzt werden.

Migration

Neben der Integration der Virtuellen Poststelle in den E-Mail-Pfad müssen bei der Einführung einer solchen Lösung auch noch weitere Aspekte berücksichtigt werden. Dies gilt insbesondere dann, wenn in der Vergangenheit bereits Einzelplatzinstallationen von E-Mail-Verschlüsselungssoftware im Einsatz war.

Insbesondere müssen die betroffenen Mitarbeiter umfassend von den Möglichkeiten und Erfordernissen der neuen Lösung in Kenntnis gesetzt werden. Zwar erfolgt die Ver- und Entschlüsselung ebenso wie die Signatur bzw. deren Prüfung transparent und somit ohne unmittelbares Zutun der Nutzer. Immerhin müssen letztere aber auch sinnvoll mitwirken, damit die Virtuelle Poststelle ihre Arbeit sinnvoll tun kann. Zu dieser Mitwirkung gehört neben der schon angesprochenen Übermittlung des initialen Kennwortes des Web-Mail-Postfaches an betroffene externe Mail-Empfänger vor allem auch die Mithilfe bei der Definition der Richtlinie, nach der die Verschlüsselung gesteuert wird: damit ausgehende E-Mails bei Bedarf automatisch muss z.B. festgelegt werden, welche Adressaten ausschließlich (oder ggfs. bevorzugt) verschlüsselte Mails erhalten sollen. Sofern dies nicht unternehmensweit festgelegt ist, ist der Administrator der Virtuellen Poststelle hier auf Informationen durch die internen Mail-Nutzer angewiesen. Es empfiehlt sich im Übrigen, hierzu wie auch für einen eventuell notwendigen Nutzungsantrag standardisierte Formulare zu entwerfen und einzusetzen. Alle (potenziell) betroffenen Nutzer sollten darauf hingewiesen werden, dass ohne entsprechenden Antrag und Freigabe durch den zuständigen Vorgesetzten keine Nutzung der Virtuellen Poststelle möglich sein wird. Analog gilt, dass bei fehlerhaften oder unvollständigen Angaben im Formular eine korrekte Funktionalität aus Sicht des betroffenen Nutzers nicht gewährleistet ist.

Besondere Aufmerksamkeit ist denjenigen Mitarbeitern zu widmen, die in der Vergangenheit bereits Desktop-Lösung zur sicheren E-Mail-Kommunikation eingesetzt haben und nun sukzessive auf die Nut-

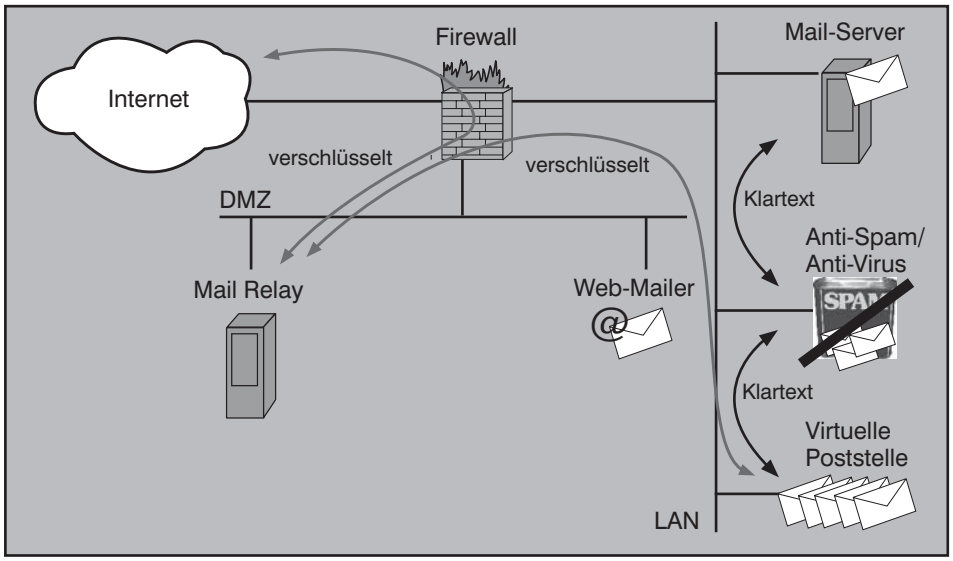


Abbildung 7: Virtuelle Poststelle im nichtöffentlichen Netzbereich mit separatem Mail-Relay

zung der Virtuellen Poststelle umzustellen sind. Eine Weiternutzung der bisherigen Lösung sollte dabei zumindest mittelfristig nur in begründeten Einzelfällen vorgesehen werden. Eine solche Begründung könnte etwa das Vorliegen entsprechender vertraglicher Regelungen sein, die explizit die bisherige Lösung zur Verwendung vorschreiben.

Daneben sollten auch Nutzungsbedingungen für den Web-Mailer formuliert und den externen Nutzern bekannt gegeben werden (z.B. über einen in der ersten Benachrichtigung enthaltenen Link auf die eigene Website oder über einen entsprechenden Text in der Benachrichtigung). In der Regel sollte mindestens auf folgende Punkte eingegangen werden:

- Weisen Sie darauf hin, dass das Postfach als Übergangslösung bis zum Aufbau einer zur Virtuellen Poststelle kompatiblen E-Mail-Verschlüsselungslösung beim externen Nutzer dient, nicht für eine dauerhafte Nutzung ausgelegt ist und daher keine Alternative zum Aufbau einer eigenen Lösung darstellt.

- Das Postfach ist typischerweise auch nicht als Ersatz oder Ergänzung für das eigene Postfach des externen Nutzers vorgesehen. Weisen Sie ihn daher sicherheitshalber darauf hin, dass demzufolge keinerlei Anspruch auf dauerhafte Vorhaltung oder garantierte Wiederherstellbarkeit von Nachrichten besteht, die in Postfächern des Web-Messengers abgelegt sind.

- Behalten Sie sich ausdrücklich vor, E-Mails nach einer bestimmten Verweildauer (z.B. von mehr als 3 Monaten) ohne Vorwarnung aus den Postfächern zu löschen.

- Das bei der Einrichtung eines neuen Postfachs vom System vergebene Benutzerkennwort sollte umgehend vom Nutzer durch ein anderes, nur ihm bekanntes ersetzt werden.

- Benutzerkennwörter müssen selbstverständlich geheim gehalten werden, d.h. sie sind sicher aufzubewahren und dürfen anderen Personen nicht zugänglich gemacht werden.

Neben diesen eher technischen bzw. organisatorischen Aspekten der Nutzung darf auch nicht vergessen werden, den externen Nutzer hinsichtlich seiner ggfs. sogar vertraglich fixierten Pflichten ins Gebet zu nehmen – meist wird dies Aufgabe des zugeordneten internen Nutzers sein. Auch eine Virtuelle Poststelle nämlich kann nicht sicherstellen, dass ein externer Absender ebenfalls einen sicheren Versandweg wählt - sei es seine lokale E-Mail-Verschlüsselungslösung oder den Web-Mailer. Zwar könnte die Virtuelle Poststelle unverschlüsselte E-Mails bestimmter Absender zurückweisen - zu diesem Zeitpunkt ist der potenzielle Schaden aber bereits angerichtet. Hier muss also durch entsprechende Aufklärung darauf hingearbeitet werden, dass keine Fehler vorkommen; dies gilt insbesondere für Nutzer des Web-Mailers, denen mangels lokaler Verschlüsselungsoption meist die Nutzung der sicheren Variante noch nicht in Fleisch und Blut übergegangen sein dürfte.

Zur Vermeidung von Fehlern in der Bedienung sowie im organisatorischen Ablauf – diesmal auf der internen Seite – ist übrigens generell ein vorgeschalteter Pilotbetrieb unbedingt zu empfehlen. In diesem Rahmen lassen sich eventuelle Defizite noch mit geringem bis vertretbarem Aufwand korrigieren. Für den Pilotbetrieb sollten tunlichst „problemresistente“ Anwender ausgesucht werden, da insbesondere zu Beginn noch mit technischen und organisatorischen Anlaufschwierigkeiten zu rechnen sein wird. Ein Produktiveinsatz in dieser Phase erscheint risikobehaftet und sollte nur in dringenden Fällen erwogen werden; betroffene Anwender sollten entsprechend intensiv betreut werden.

Zur Verifikation der grundlegenden Funktionalitäten sowie der korrekten Implementierung empfiehlt sich darüber hinaus ein intensiver Test im Vorfeld der Pilotphase. Hier können insbesondere auch Erkenntnisse gewonnen werden, die bei der Vervollständigung und Optimierung der für den Pilot- und späteren Regelbetrieb notwendigen Dokumente (Antragsformular, Benutzerinformation, Betriebshandbuch, etc.) nützlich sein können.

Um sicherzustellen, dass durch die Migration und insbesondere die ggfs. notwendige Deinstallation bereits vorhandener Desktop-basierter E-Mail-Verschlüsselungslösungen keine Beeinträchtigung der Kommunikationsfähigkeit bzw. des Datenbestands erfolgt, ist ein ausreichend dimensionierter Übergangszeitraum vorzusehen, innerhalb dessen eine Weiternutzung der Altlösung im Bedarfsfalle möglich ist.

Dieser Übergangszeitraum ist insbesondere auch zu nutzen, um – soweit möglich - weiterhin erforderliche Schlüssel und Zertifikate der Altlösung in die Virtuelle Poststelle zu importieren. Das genaue Prozedere des Imports ist dabei im Rahmen des oben empfohlenen Tests zu klären. Dazu sollte das gewählte Produkt nach Möglichkeit entsprechende Importfunktionen, z.B. für PGP-Keyring-Dateien, bieten. Für den Fall, dass vorhandene Schlüssel-Dateien importiert werden können, sollten diese jedoch durch die Anwender frühzeitig geeignet bereitgestellt werden. Eine praktikabel erscheinende Möglichkeit ist z.B. die Einrichtung eines speziellen Postfachs, an das die entsprechenden Dateien vom Anwender gesendet werden. Für

den Anwender sollte sinnvollerweise eine entsprechende Anleitung verfasst werden, die ihm das Auffinden der entsprechenden lokalen Dateien erleichtert.

Besonders wichtig ist der Übergangszeitraum mit Blick auf die in der Vergangenheit verschlüsselt ausgetauschten Nachrichten. Diese liegen im Mail-System stets nur in verschlüsselter Form vor. Nach einer vollständigen Deinstallation der bisherigen Verschlüsselungslösung ist eine Entschlüsselung derart geschützter Nachrichten in der Regel nicht mehr möglich! Daher müssen vor Entfernen der lokalen Installationen derartige Nachrichten - soweit nicht in der Vergangenheit bereits geschehen - in entschlüsselter Form gespeichert werden, sofern ein Bedarf an dauerhafter Zugriffsmöglichkeit besteht.

Um für den Fall, dass eine wichtige Nachricht tatsächlich nicht in entschlüsselter Form gespeichert worden sein sollte, auch in Zukunft eine Entschlüsselung sicherzustellen, kann erwogen werden, durch Sichern der privaten Schlüsselinformationen und der notwendigen Zugriffsinformationen (Passphrase oder ähnliches) eine Rekonstruktionsmöglichkeit für Notfälle zu schaffen; aufgrund des damit verbundenen Risikos und Aufwands erscheint jedoch die oben beschriebene Vorgehensweise grundsätzlich empfehlenswerter. Darüber hinaus birgt das Speichern der oben genannten sensiblen Informationen ein erhebliches Missbrauchspotenzial - insbesondere, wenn diese Keys womöglich auch zum Signieren und damit als Identitätsnachweis verwendet werden können.

Basierend auf den in zuvor diskutierten Aspekten bietet sich insgesamt beispielsweise folgender Migrationsablauf an:

1. Funktionaler Test der Lösung und Optimierung der Betriebsdokumente, insbesondere Antrag und Benutzerinformation
2. Festlegung der Pilotanwender, Information/Unterweisung, Ausfüllen der jeweiligen Anträge, Schlüssel-/Zertifikatsexport
3. Parametrierung der Virtuellen Poststelle auf Basis der Pilotanträge, Schlüssel-/Zertifikatsimport
4. Nutzung der Virtuellen Poststelle durch die Pilotanwender
5. Abschließende Optimierung der Betriebsdokumente
6. Information aller Anwender über die Umstellung, Verfügbarmachung der entsprechenden Dokumente
7. Beginn des vorläufigen Regelbetriebs
8. Festlegung Ende des Übergangszeitraums bis zur Deinstallation der Altlösung
9. Optimierung des Betriebs und Deinstallation Altlösung

Fazit

Grundsätzlich sind Virtuelle Poststellen eine sehr interessante Lösung zur Bereitstellung sicherer E-Mail-Kommunikation vor allem in umfangreichen Umgebungen. Zwar erfordert ihr Einsatz gewisse konzeptionelle und planerische Vorüberlegungen und eine sorgfältige Realisierung, insbesondere wenn eine Migration von bestehenden Desktop-Lösungen ansteht, das Resultat lässt aber diese Mühen hoffentlich vergessen. Immerhin gehören anschließend per elektronischer Postkarte jedermann unfreiwillig zugänglich gemachte Unternehmensgeheimnisse der Vergangenheit an - oder genießen zumindest Seltenheitswert…

Report des Monats

Voice-over-IP-Lösungen von Alcatel

Ergebnisse einer Technologie-Studie

Unser im letzten Jahr veröffentlichte Technologievergleich „Cisco versus Siemens: wer hat die bessere Lösung für IP-Telefonie“ gilt mittlerweile als führende Studie in diesem Bereich. Es wurde immer wieder die Bitte an uns herangetragen, doch weitere TK-Anlagen-Hersteller in den Vergleich einzubeziehen. Dieser Bitte kommen wir mit dem neusten Report von ComConsult Research nach.

Der Report analysiert die bestehenden TK-Lösungen von Alcatel und berücksichtigt dabei auch die erkennbare Weiterentwicklung der nächsten Jahre. Der Report bewertet nicht nur rein technische Elemente sondern gibt auch Einschätzungen zur Zukunftssicherheit der Produkte ab.

Im Anschluss haben wir für Sie eine kurze Leseprobe zusammengestellt:

4. Die Alcatel-Produktwelt für IP-Telefonie

Alcatel zählt seit vielen Jahren zu den europäischen Marktführern im klassi-schen TK-Bereich und ist insbesondere in Frankreich und der BRD zu den ersten fünf Herstellern bei klassischen TK-Lösungen für kommerzielle Unter-nehmen zu rechnen.

Die strategische Lösungslinie heißt OmniPCX. Alcatel hat die OmniPCX Office als separate Lösung für den Mittelstand, und seit 1996 die Flagschifflinie OmniPCX 4400. Nachdem zuerst im Jahr 2000 die OmniPCX Office in einen SoftSwitch auf Linux-Basis weiterentwickelt wurde, stellte Alcatel in 2003 auch die größere OmniPCX 4400 auf ein Linux-basiertes Konzept mit Call Control Agent und Media Gateways um. Seit dem heißt dieses System OmniPCX Enterprise.

Die OmniPCX Office wird als System mit zusätzlicher LAN-Funktionalität (wie später ausführlicher beschrieben wird) für den SME-Markt weiter vermarktet, obwohl die OmniPCX Enterprise in ihrer kleinsten Ausbaustufe auch für diesen Bereich einsetzbar ist.

4.1 Die OmniPCX Produktlinien

4.1.1 Die OmniPCX Enterprise

Unter dem Namen OmniPCX Enterprise vermarktet Alcatel eine dezentrale Hybrid-Architektur, bestehend aus Communicati-

on Servern / Softswitches (auch als Media Server oder Call Server bezeichnet), Media Gateways und Endgeräten (Hardware- oder Software-Telefone). Die einzelnen Komponenten sind seit Release v5.1 im Wesentlichen im Mix & Match vernetzt betreibbar. Die unterschiedliche Leistungsfähigkeit der Systemplattformen bringt gewisse Einschränkungen in der Funktionsweise und im Funktionsumfang mit sich. Daher ist es so, dass der Hersteller selber für bestimmte Anforderungen besondere Konfigurationen empfiehlt.

Die Kommunikation zwischen Communication Servern, Media Gateways und Endgeräten läuft über das proprietäre Protokoll ABC (Alcatel Business Communication). ABC basiert auf QSIG und ist eine Erweiterung der QSIG GF. Zwischen Endgerät und Media Gateway oder Communication Server läuft UA (User-Interface Alcatel), zwischen Media Gateways und Communication Servern läuft zusätzlich ABC-F (Alcatel Business Communication Telefon Features), ABC-R (Routing) und ABC-M (Management).

Eine Übersicht über Communication Server und Media Gateways zeigt Abbildung 4.1.

4.1.1.1 Server

Grundsätzlich kann ein Communication Server auf drei verschiedenen Hardware Plattformen betrieben werden:

- IP Rack Server als Einschub im CS-Slot eines IP Media Gateways (19“ Hardware auf Basis der OmniPCX Office, jetzt IPMG, wie unter Media Gateways beschrieben)
- IP Crystal Server als Einschub in einem Crystal IP Media Gateway 24“ modulare Chassis-Hardware auf Basis der früheren OmniPCX 4400, jetzt Crystal IP Media Gateway, wie unter Media Gateways beschrieben)
- IP Appliance Server als Software auf ei-

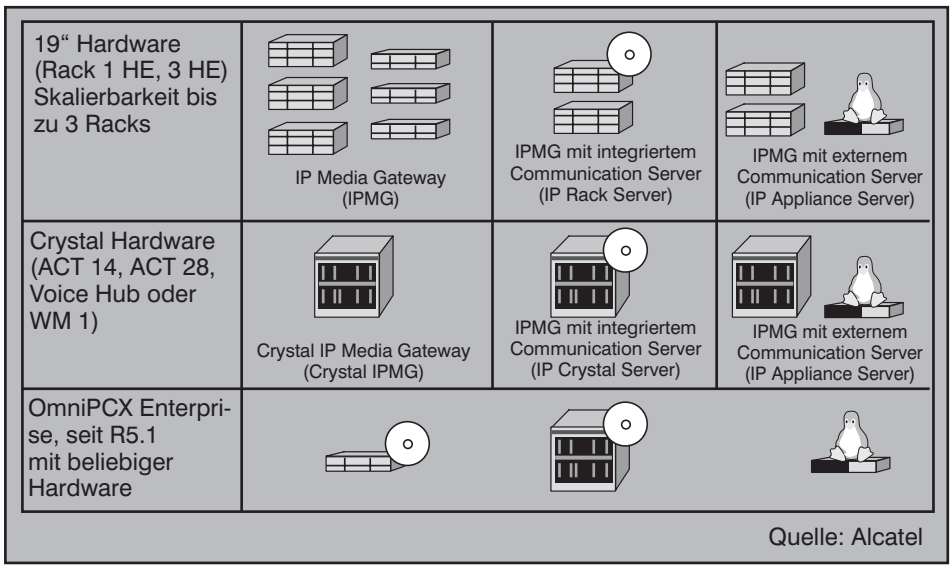


Abbildung 4.1: Hardware Plattformen der OmniPCX Enterprise

nem standalone Linux-Server (z.B. IBM Business Server, oder HP)

Das Betriebssystem ist Red Hat und Mandrake v7.2 Linux; das aktuelle OmniPCX Enterprise Software Release ist v6.0, für Mai 2005 ist das Release v6.1 angekündigt. Ein Communication Server (CS) kann bis zu 90 IP Media Gateways handhaben.

Der IP Rack Server (IP Rack CS) ist die kleinste Server-Ausbaustufe, wird in ein IP Media Gateway eingebaut und für Umgebungen mit bis zu 250 Anschlüssen (Benutzern) empfohlen. Seine Leistungsgrenze für den produktiven Betrieb liegt bei 6.000 BHCC und falls die angeschlossenen Benutzer keine allzu hohen Aktivitäten zeigen, kann eine Lizenzerweiterung auf 1000 Anschlüsse an einem Standort oder bis zu maximal 1500 VoIP Anschlüssen in WAN Umgebungen eingesetzt werden, die jedoch nicht die Leistungsgrenze von 6.000 BHCC erhöht und daher von Alcatel nicht empfohlen wird. Mit dem IP Rack Server sind bis zu 1000 Voice Mail Ports (Kanäle) möglich, müssen mehr parallele Voice-Mail Kanäle betrieben werden, so ist ein Crystal Gateway erforderlich. Ein Einsatzszenario zeigt Abbildung 4.2.

Zu den Einschränkungen für den Einsatz von IP Rack Servern und IP Rack MG gehört, dass sich diese Systemarchitektur vor allem für leistungsstarke DECT-Implementierungen nicht eignet. Für solche Implementierungen empfiehlt Alcatel den Einsatz von Crystal Media Gateways.

Falls Konferenzen mit Master / Meet-me Funktionalität (definierte Einwahlnummer, Moderator) und mehr als 29 Teilnehmern oder Casual Konferenzen (einfache, direkte Konferenzzusammenschaltung) mit mehr als 6 Teilnehmern erforderlich sind, müsste ein IP Rack Server zusammen mit einem Crystal Media Gateway eingesetzt werde; eine Konfiguration, die zwar als möglich, nicht jedoch empfohlen einzuordnen ist.

Bei komprimierten Verbindungen (spezielle TDM-Kompression, ab Version 6.1 nicht mehr unterstützt) standortweitem DECT oder speziellen Mehr-Standort-Verbindungen (z.B. über X.25-Ports, V.35 oder Multipoint Festverbindung zu mehreren benachbarten Systemen), ebenso bei umfangreicheren Konferenzen kann kein IP Rack Server eingesetzt werden.

Die 250 Teilnehmer an einem IP Rack Server sind eine praktische Grenze, die früher als „Express-Lösung“ bei minimaler TK-Funktionalität vermarktete Grenze von 500 Teilnehmern wird offiziell nicht weiter verfolgt. Für mehr als 250 Benutzer gibt es die beiden anderen, nachfolgend beschriebenen Servertypen.

Der IP Crystal Server ist als CS-Einschub für ein Crystal Media Gateway erhältlich. Er hat eine Leistungsgrenze von 150.000 BHCC, eine Lizenzgrenze von 5000 Teilnehmern und wird empfohlen, wenn eine höhere Media Gateway Funktionalität erforderlich ist: Über das Crystal Media Gateway werden diese erweiterten Funktionen wie standortweites DECT, Kompression, spezielle Mehr-Standort-Verbindungen (z.B. X.25-Ports, V.35 oder Multipoint Festverbindung zu mehreren benachbarten Systemen) und umfangreichere Konferenzen unterstützt. Das CS-Modul des IP Crystal Servers hat eine singuläre 10/100 Mbit Ethernet Schnittstelle zur Anschaltung an das IP Netzwerk.

Der IP Crystal Server kann als Backup Lösung durch Einbau zweier CS-Einschübe in ein Chassis gedoppelt werden.

Anstelle des IP Rack Servers oder IP Crystal Servers kann in jedem Fall auch der nachfolgend beschriebene hochwertige IP Appliance Server eingesetzt werden. Ein IP Appliance Server ist teurer als ein CS-Modul für die Crystal- oder die Rack-Architektur. Da aber, z.B. für den Anschluss analoger bzw. digitaler Teilnehmer und die Realsierung der Amtsanschaltungen, meistens Media Gateway-Chassis einer bestimmten Größe gebraucht werden, ist immer eine Rechnung erforderlich, welche Hardware tatsächlich das bessere Preis-Leistungsverhältnis aufweist. Ein IP Appliance Server in Kombination mit IP Media Gateways kann kostengünstiger sein als ein „embedded“ Crystal Server in Kombination mit Crystal Chassis. Ob in einer bestimmten Umgebung ein IP Rack Server oder ein IP Crystal Server eingesetzt wird, ist letztlich abhängig von den Media Gateway Anforderungen.

Der IP Appliance Server (IPAS) ist mit 300.000 BHCC die performanteste Serverlösung, die auch hinsichtlich Backup Konfigurationen die flexibelsten Möglichkeiten bietet. Bei allen größeren und Mehr-Standort-Konzepten, bei denen insbesondere die Standort-Verbindung rein über IP verläuft, wird der Einsatz von IP Appliance Servern empfohlen. Sie unterstützen auch ein standortübergreifend verteiltes Backup, in diesem Fall muss jedoch ein gemeinsames IP-Subnetz standortübergreifend definiert sein, da die Communication Server eine Layer-2 Verbindung zueinander benötigen. Für das Release v6.1 (Mai 2005) ist die Aufhebung dieser Beschränkung angekündigt, dann können zwei Communication Server auch in unterschiedlichen IP Subnetzen angebunden werden.

Liegt eine reinrassige IP-Welt vor, d.h. es gibt keinerlei Bedarf nach peripheren Baugruppen (PSTN-Trunks, analoge oder digitale Endgeräte etc.), so dass über die „TK-Anlage“ bzw. den Softswitch nur die Signalisierung zu den IP-Endgeräten läuft, so sind gar keine IP Media Gateways erforderlich, die Endgeräte können rein über einen Softswitch (Communications Server Appliance) betrieben werden, der sämtliche Signalisierungsströme handha-

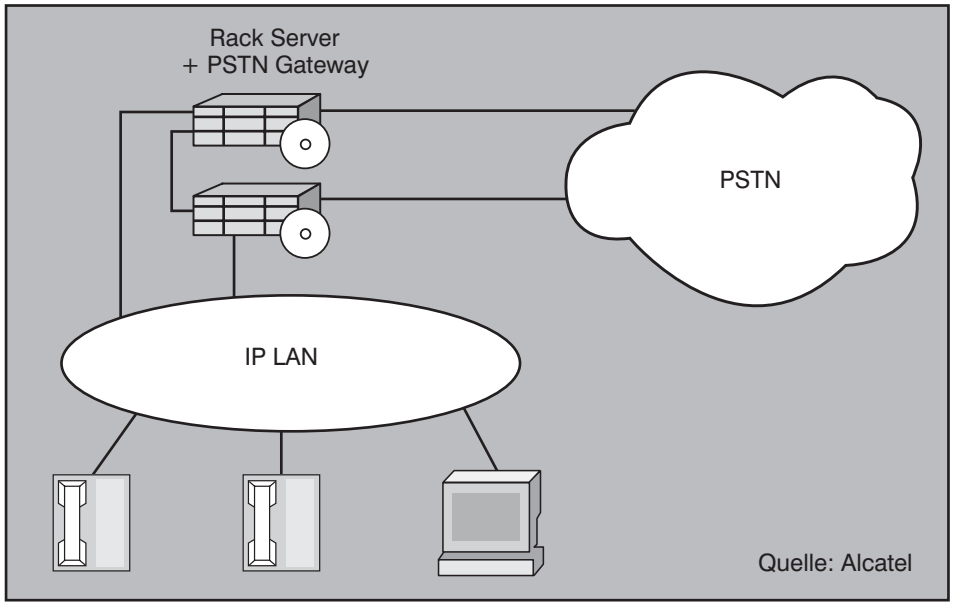


Abbildung 4.2: Einstandort-Lösung mit IP Rack Server

ben kann. Allerdings ist dieses Szenario ziemlich unwahrscheinlich, da zumindest ein PSTN-Zugang im Regelfall immer benötigt wird.

Da der Appliance Server ein reiner Softswitch ist, muss für eine non-IP Standortverbindung wie QSIG, ISDN, ABC über E1 etc. ebenso wie für die Anbindung aller non-IP Endgeräte wie analoge Telefone oder Faxgeräte ein separates Media Gateway eingesetzt werden (IP Media Gateway oder Crystal IP Media Gateway).

4.1.1.2 Media Gateways

Für die OmniPCX Enterprise gibt es zwei Media Gateway Typen:

- IP Media Gateway (IPMG, Rack Hardware)
- Crystal IP Media Gateway (ACT - Alcatel Crytsal Technology)

Beide Media Gateways haben intern eine TDM Architektur, da die Hardware auf klassischen Anlagen basiert. Das IP Rack MG hat eine passive Busstruktur. Das IP Crystal MG hat die Alcatel-typische vollvermaschte Matrix-Architektur („Kristall"), die einen blockierungsfreien Betrieb aller Einschubmodule in diesem System ermöglicht. Bis zu 90 Media Gateways können von einem Communication Server gesteuert werden.

4.1.1.2.1 IPMG (IP Media Gateway)

Das IPMG ist in 19" breiten Chassis-Modellen mit einem (RM1) oder drei (RM3) 19" Slots Bauhöhe verfügbar, wobei ein 19" Slot drei Modulslots aufnehmen kann.

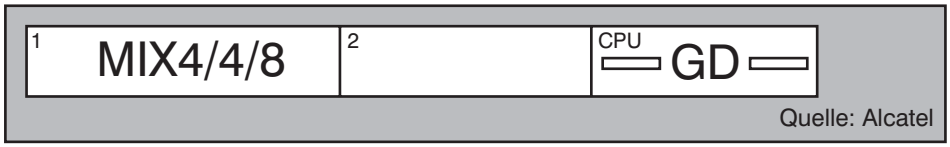


Abbildung 4.3: IPMG mit 1 Slot

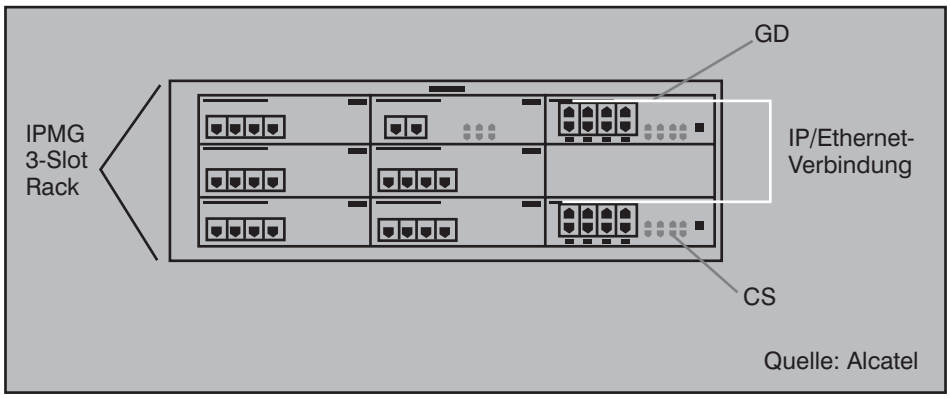


Abbildung 4.4: IPMG mit 3 Slots

In jedem Gateway muss mindestens ein GD oder CS-Steuermodul / CPU-Modul eingebaut werden, es können aber uch mehrere Steuermodule eingebaut werden.(siehe Abbildung 4.3 und Abbildung 4.4).

Es gibt folgende Steuermodule (CPU's):

- CS Communication Server
- GD Treiber zur Verwaltung von non-IP Endgeräten (24 Kanäle)
- GA Treiber zum Hinzufügen von optionalen Ressourcen wie DSP's, Kompressions-Chips (24 Kanäle)
- MEX CPU zum Anschluss von Erweiterungs-Racks mit HSL

Falls der Communication Server in das Gateway eingebaut ist, belegt er den untersten Slot rechts. Das CS-Modul hat 8 RJ-45 Ports, Port 1 wird zur LAN / GD-Anschaltung genutzt, Port 2 und 3 sind aktuell nicht genutzt, Port 4 ist ein V.24 Anschluss für die Console, Ports 5 bis 8 sind vier zusätzliche geswitchte Ethernet Ports.

Aktuelles Seminar

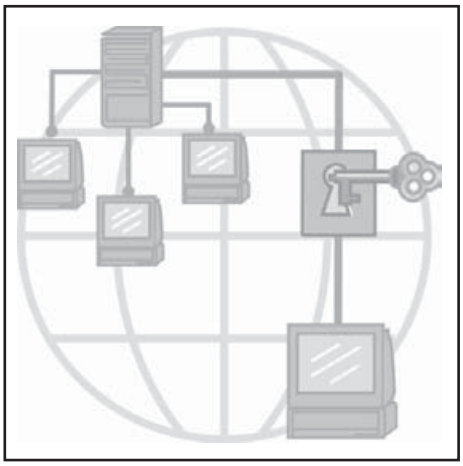
Erarbeitung und Umsetzung von Sicherheitskonzepten

Die ComConsult Akademie veranstaltet vom 25.06. - 29.06.07 ihr Seminar „Erarbeitung und Umsetzung von Sicherheitskonzepten“ in Berlin.

Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Anhand konkreter Projektbeispiele zeigt dieses Seminar auf, wie diese Aufgabenstellung von der Konzipierung über Ausschreibung, Abnahme und Betrieb bis hin zur Außerbetriebnahme der entsprechenden Systeme erfolgreich und wirtschaftlich bewältigt wird.

Auflagen zum Risikomanagement (Sarbanes-Oxley Act, Basel II oder FDA-Forderungen) und zum Datenschutz schließen eine „gelebte“ IT-Sicherheit als zwingenden Be-



standteil ein. Die konsequente Einhaltung solcher Anforderungen kann zudem signifikante Wettbewerbsvorteile schaffen.

Sicherheitskonzepte müssen also mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Anhand konkreter Projektbeispiele zeigt dieses Seminar auf, wie diese Aufgabenstellung von der Konzipierung über Ausschreibung, Abnahme und Betrieb bis hin zur Außerbetriebnahme der entsprechenden Systeme erfolgreich und wirtschaftlich bewältigt wird.
In diesem Seminar lernen Sie

- wie Sicherheitsstandards auf Ihre Bedürfnisse zugeschnitten angewendet werden können
- wie bedarfsgerechte Sicherheitsleitlinien und -konzepte entwickelt werden
- wie man Qualitäts- und Risikomanagement mit der IT-Sicherheit (ggf. sogar revisionsfest) verknüpft
- wie Sie in der Praxis Sicherheitslösungen konzipieren, planen, ausschreiben und betreiben

Referenten: Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff, Sven Ossendorf, Dipl.-Inform. Andreas Meder

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Erarbeitung und Umsetzung von Sicherheitskonzepten

☐ Ich buche das Seminar
Erarbeitung und Umsetzung von Sicherheitskonzepten
25.06. - 29.06.07 in Berlin
zum Preis von € 2.290,- 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

Schwerpunktthema

Sicherheitsanalyse des Cisco NAC Framework

Fortsetzung von Seite 1

Dror-John Röcher beschäftigt sich seit nun gut 10 Jahren mit Cisco-Themen, schwerpunktmäßig im Bereich Sicherheit von Enterprise Netzwerken und data-centers. Er ist als Senior Security Consultant für die ERNW GmbH europaweit tätig und hat diverse Whitepapers zu Security-Themen verfasst. Als Referent vermittelt er regelmäßig seine Erfahrungen auf Security-Veranstaltungen.

Michael Thuman ist einer der führenden Experten für Penetrationstests. Von ihm entwickelte Hacking-Tools, Advisories und zahlreiche Veröffentlichungen über Schwachstellen bei VPNs und verschiedenen Firewalls haben vielfach Sicherheitslücken frühzeitig aufgedeckt und massive Schäden verhindert. Auf der Basis von Penetrations-Tests und Audits entwickelt er wirksame Sicherheits-Konzepte für namhafte große und mittlere Netze. Michael Thuman ist Ko-Autor des Buches „Pen-Tests - Durch Risikoabschätzung IT-Sicherheit optimieren“ im Vieweg Verlag (2005).

1. Funktionsweise Cisco NAC Framework

Das Cisco NAC Framework[1] besteht aus vier verschiedenen Komponenten, deren Zusammenspiel eine Überprüfung des Clients und darauf aufbauend eine Reglementierung des Netzwerkzugangs für den geprüften Client ermöglichen soll. Einen Überblick über die Zusammenhänge der Komponenten ist in Abbildung 1 dargestellt.

- Die Client-Software: Damit NAC den Zustand eines Clients überprüfen kann, wird auf dem Client eine Applikation benötigt, die die notwendigen Informationen sammelt und überträgt. In der einfachsten Form ist diese Software der Cisco Trust Agent (CTA). Der CTA kommuniziert die sogenannten „Credentials“ via EAP[2] an einen Backend Policy-Server, den Cisco Secure ACS.

- Eine Netzwerk-Komponente (Network Access Device - NAD): Das NAD dient zum Einen als Kommunikationsvermittler zwischen dem Client und dem Cisco Secure ACS und zum Anderen ist es für die Umsetzung der Zugriffsbeschränkungen verantwortlich. Für die Kommunikationsvermittlung werden die EAP-Nachrichten vom Client als RADIUS-Nachrichten an den Cisco Secure ACS weitergeleitet. Router, Switche, Firewalls, VPN-Concentratoren und auch WLAN-APs können als NAD fungieren, solange sie aus dem Hause Cisco stammen und ein aktuelles Betriebssystem mit NAC-Feature-Unterstützung installiert haben.

- Der Cisco Secure ACS: Eine zentrale Stelle innerhalb des NAC-Frameworks nimmt der Cisco Secure ACS, Ciscos RADIUS-Server, ein. Er hat gleich mehrere Aufgaben:

  - Der ACS nimmt Client-Credentials vom NAD per RADIUS entgegen.

  - Der ACS überprüft die gelieferten Credentials gegen die definierte Policy.

  - Der ACS befragt ggf. Policy-Server von Drittherstellern, falls zusätzliche NAC-Applikationen[3] auf dem Client weitere Credentials geliefert haben.

  - Der ACS leitet aus der Policy und den kommunizierten Credentials die Zugangsbeschränkungen ab und kommuniziert diese an das NAD und den Client.

- Optionale Dritthersteller-Policy-Server: Falls zusätzliche NAC-Applikationen (AV, Patch-Management) eingesetzt werden, werden die zugehörigen Credentials entweder direkt vom ACS verarbeitet oder aber vom ACS an einen Dritthersteller-Policy-Server zur Evaluierung weitergeleitet. Diese externen Komponenten spielen in der vorliegenden Sicherheitsanalyse keine weitere Rolle und sind nur der Vollständigkeit halber aufgeführt.

1.1 Terminologie

Eine neue Technologie bringt fast zwangsläufig eine neue Terminologie mit sich, die an dieser Stelle vor einer tieferen technischen Betrachtung eingeführt werden soll.

Die Informationen, die der Client an den ACS übermittelt, werden Posture Credentials genannt, frei übersetzt etwa „Zustandsbeschreibung“. Dabei handelt es sich um Variablen-Wertepaare (Attribute-Value Pairs, AV-Pairs), welche Informationen zu Betriebssystem, Patchlevel, Anti-

[1] Die erste Anlaufstelle für Informationen rund um das Thema Cisco NAC ist (natürlich) die Website von Cisco zum Thema: http://www.cisco.com/go/nac
[2] EAP: Das Extensible Authentication Protocol ist ein Framework zur Authentifizierung und aktuell in RFC 3748 (http://rfc-editor.org/rfc/rfc3748.txt) beschrieben.
[3] Als „NAC-Applikation“ werden im Kontext dieses Artikels Applikationen bezeichnet, die ein Plug-In für das Cisco NAC-Framework mit sich bringen. TrendMicro Office Scan, eine Antiviren-Lösung, war zum Beispiel eine der ersten Applikationen, die ein Plug-In für Cisco NAC mit auf dem Client installiert hat.

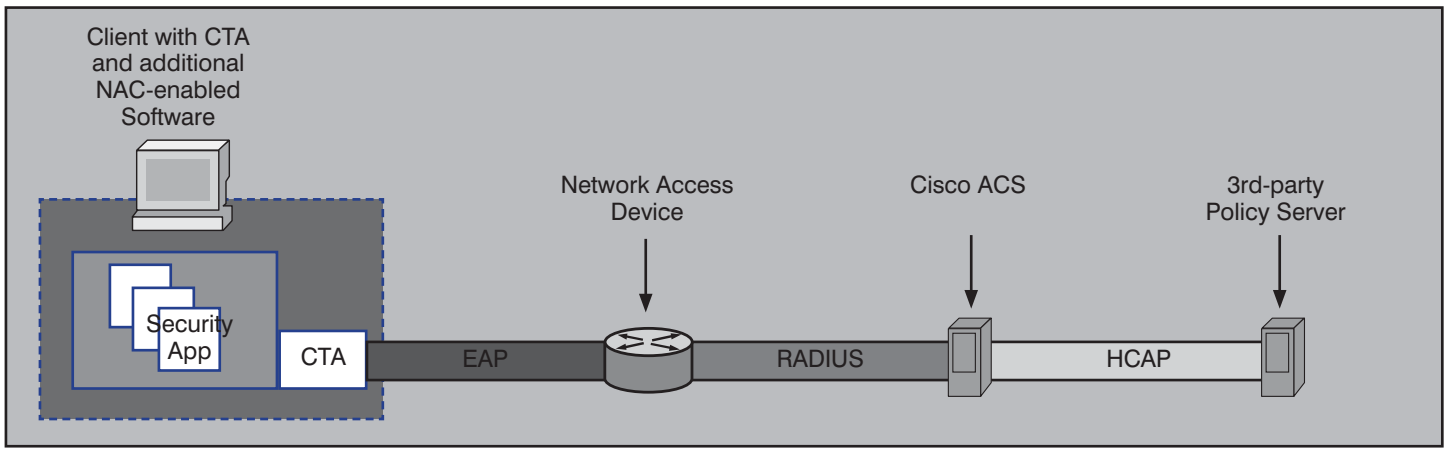


Abbildung 1: Komponenten im Cisco NAC Framework

Virus Definition usw. enthalten. Für jede NAC-Applikation, für die der CTA Posture Credentials liefert, wird ein Application Posture Token vom ACS ermittelt. Die Token haben definierte Namen und Bedeutungen:

- **Healthy:** Völlig konform mit der konfigurierten Policy für die Applikation.
- **Checkup:** Ausreichende aber nicht völlige Konformität mit der Policy, üblicherweise wird der Zugang nicht eingeschränkt, der Benutzer aber auf die Nicht-Konformität hingewiesen.
- **Transition:** Falls eine Überprüfung stattfindet, bevor alle Dienste des Clients gestartet sind oder während einer Überprüfung eines Agentless Clients[4], wird der Token Transition vergeben. Dieser Token hat einen temporären Charakter und temporäre Beschränkungen des Zugangs werden umgesetzt.
- **Quarantine:** Ungenügende Konformität mit der Policy, woraufhin der Netzwerkzugriff i.d.R. stark eingeschränkt wird, z.B. auf ein "Quarantäne-Segment", in welchem sich Update-Server für Anti-Virus und Patchmanagement befinden.
- **Infected:** Aktive Infektion des Clients mit Schadsoftware, darauf beruhend üblicherweise stärkste Beschränkung des Netzwerkzugangs bis hin zu kompletter Isolation des Clients.
- **"Unknown":** Wenn kein Token ermittelt werden kann oder der CTA nicht installiert ist, wird der generische Token Unknown vergeben. Basierend auf dem Token Unknown kann der Zugang zum Beispiel auf ein Gast-VLAN oder auf den Internet-Proxy beschränkt werden.

Nachdem für jede Applikation ein applikationsspezifischer APT abgeleitet wurde, wird ein systemspezifischer System Posture Token (SPT) ermittelt. Der SPT entspricht dem APT mit den niedrigsten Berechtigungen im Netzwerk. Der ACS übermittelt den SPT und die abgeleiteten Einschränkungen des Netzwerkzugriffs an das NAD, welches verantwortlich für die Umsetzung der Restriktionen ist. Der SPT, alle APTs und ein Hinweistext werden vom ACS an den Client übermittelt, der den Benutzer auf eventuelle Beschränkungen im Zugriff auf das Netzwerk hinweisen kann. Ggf. kann sich auch das Verhalten von Dritt-Applikationen durch den ermittelten APT ändern.

Cisco bietet drei verschiedene Varianten von NAC an, die auf verschiedene Zugriffswege ausgelegt sind und denen verschiedene Möglichkeiten der Zugangsbeschränkungen immanent sind.

1. Layer3-IP: Bei NAC-Layer3-IP werden die Zugangsbeschränkungen als IP-Access-Listen durch ein routendes Netzwerkgerät (Firewall, Router, VPN-Konzentrator) umgesetzt. Die Kommunikation des Clients mit dem NAD wird per „PEAP over UDP" auf UDP-Port 21862 abgewickelt.
2. Layer2-IP: NAC-Layer2-IP setzt die Zugangsbeschränkungen ebenfalls als IP-Access-Listen um, allerdings auf einem VLAN-Interface eines Switches. Auch hier findet die Kommunikation per "PEAP over UDP" statt.
3. Layer2-802.1X: Bei NAC-Layer2-802.1X kommen "klassische" 802.1X-Sicherheitsmechanismen auf einem Switch zur Umsetzung der Zugangsbeschränkungen zum Einsatz. Die Kommunikation findet nicht mehr über UDP statt, sondern wird direkt auf Layer2 mit EAP-FAST[5] abgewickelt. Dies ist die einzige Variante, in der
   - der Client authentifiziert wird, bevor er Zugang zum Netzwerk erhält.
   - komplette Isolation des Clients, auch vom lokalen Subnetz, erzielt werden kann.

NAC-Layer2-802.1X ist nicht nur die sicherste aller drei Varianten, sondern auch die aufwendigste, da eine funktionierende 802.1X Infrastruktur vorausgesetzt wird. Zusätzlich ist diese Variante aufgrund ihres Layer2-Ansatzes nicht immer möglich (so kann zum Beispiel beim Zugriff über ein VPN nur eine Layer3-Variante zum Einsatz kommen).

Tabelle 1 vergleicht die drei NAC Varianten bezüglich ihrer Eigenschaften und Einschränkungen.

Jede dieser Varianten bietet sich für verschiedene Szenarien an und die Varianten unterscheiden sich auch hinsichtlich der angebotenen Sicherheit deutlich voneinander (offensichtlich ist dies zum Beispiel

[4] Agentless Clients haben keinen CTA installiert oder der CTA weist eine Fehlfunktion auf. Diese Clients können in drei Kategorien unterteilt werden: (1) Legitime Systeme auf denen der CTA nicht installiert werden kann, z.B. Netzwerk-Drucker, (2) Unternehmensfremde Systeme, z.B. Gäste und Berater (3) legitime Systeme auf denen der CTA nicht korrekt funktioniert. Solche Systeme können entweder "whitelisted" werden (üblicherweise der Fall mit Systemen der ersten Kategorie), automatisch durch einen Schwachstellenscanner "auditiert" werden, oder es werden „Standard-Restriktionen", z.B. Gast-Zugang, angewendet.

[5] EAP-FAST wurde von Cisco als Nachfolger von LEAP entwickelt. Statt eines Zertifikats kommen sogenannte „Protected Authentication Credentials" (PAC) zum Einsatz. Dabei handelt es sich um client-spezifische, vom Server signierte pre-shared-keys.

Feature	NAC-L2-802.1X	NAC-L2-IP	NAC-L3-IP
Trigger	Data Link / Switchport	DHCP /ARP	geroutetes Paket
Machine ID	Ja	Nein	Nein
User ID	Ja	Nein	Nein
Posture	Ja	Ja	Ja
VLAN Assignment	Ja	Nein	Nein
URL Redirection	Ja	Ja	Ja
Downloadable ACLs	Cat 65k	Ja	Ja
Posture Status Queries	Nein	Ja	Ja
802.1X Posture Change	Ja	Nein	Nein

Tabelle 1: Vergleich einiger Eigenschaften der drei NAC Varianten

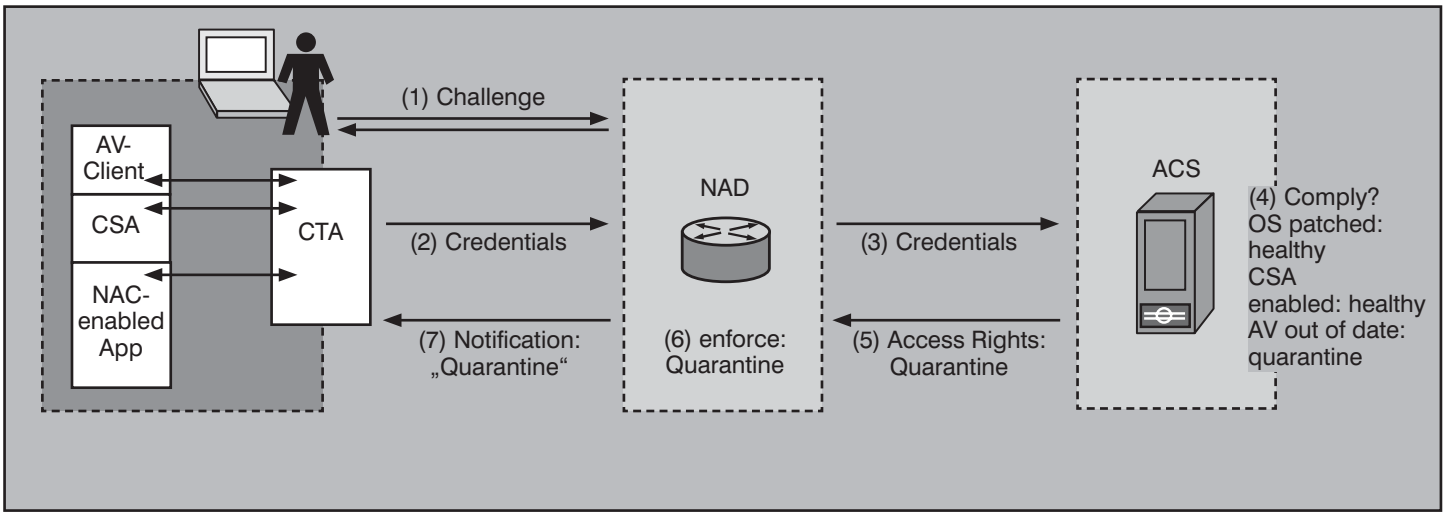


Abbildung 2: Kommunikationsablauf in Cisco NAC

durch die Abwesenheit einer Client-Authentifizierung in zwei der drei Varianten). Eine genauere Darstellung der Kommunikationsabläufe ist in Abbildung 2 abgebildet.

1.2 Technische Details

Nachdem die Technologie in groben Zügen skizziert wurde und die relevante Terminologie eingeführt wurde, ist es Zeit für einen genauere technische Betrachtung des Cisco NAC Frameworks.

1.2.1 Posture Credentials

Die vom Client an den ACS übermittelten Posture Credentials können in zwei Kategorien unterteilt werden. (1) Posture Credentials, die durch NAC-Applikationen (z.B. TrendMicro OfficeScan oder den CTA selbst) ermittelt wurden und (2) Posture Credentials, die über das enthaltene Scripting-Interface des CTA durch selbstentwickelte Scripte ermittelt wurden.

Die Posture Credentials werden als Variablen-Wertepaare übermittelt und die Daten-Typen sind fest definiert:

- Oktet-Array, Integer32, Unsigned32, String (UTF-8), IPv4 Adresse, IPv6 Adresse, Time (4 Oktette), Version (4-x-2 Oktette)

Nicht nur die Datentypen, sondern auch die Variablen-Bezeichnungen sind innerhalb einer logischen Struktur definiert, die sich aus der IANA SMI[6] Benamung, die auch in SNMP-MIBs Verwendung findet, ableitet. Die Bestandteile dieser Namensstruktur sind:

- Numerische Hersteller ID aus der IANA SMI Private Enterprise ID Assignments. Cisco, zum Beispiel, wurde die ID 9 zugewiesen, McAfee 1230 und Microsoft 311.
- Numerische Applikations-Typ ID (16 Bit Wert), definiert den Typ der Applikation. Die (von Cisco) definierten Werte sind in Tabelle 2 dargestellt.
- Numerische Attribute-ID, Attribute Name & Attribute-Datentyp

Tabelle 3 zeigt einen Überblick über die mit dem CTA (Version 2.0) ohne Installation weiterer NAC-Applikationen verfügbaren Posture Credentials.
Eine eindeutige Kennzeichnung eines spezifischen Posture Credentials ist somit gegeben; so definiert „9:1:8“ folgende Information: Hersteller: Cisco (9), Applikation: Posture Agent (1), Attribut: OS-Kernel (8) und basierend auf Tabelle 3 ergibt sich, dass die Information vom Daten-Typ „String“ ist (zum Beispiel Linux-2.6.4-8-i386-custom).

Wie schon erwähnt besitzt der CTA zwei unterschiedliche Schnittstellen, über die Posture Credentials an den CTA zur Übermittlung an den ACS übergeben werden können. Die erste ist für „reguläre“ NAC-Applikationen und stellt eine klassische (nicht offengelegte) Plug-In Schnittstelle dar und die zweite ist ein offengelegtes Scripting-Interface. Auch wenn beide letztendlich demselben Zweck dienen, so unterscheiden sie sich hinsichtlich ihrer Funktionalität nicht unerheblich.

Plug-Ins (in Windows-Versionen des CTA) werden durch DLLs realisiert, welche in “%CommonProgramFiles%\PostureAgent\Plugins” installiert und durch korrespondierende ini-Dateien konfiguriert werden. Die Installation des CTA 2.0 bringt per default folgende Plug-Ins mit:

- Host Posture Plug-In
- CTA Plug-In
- Scripting Plug-In

Das Scripting-Interface (clientseitig realisiert durch ctasi.exe und ctascriptPP.dll) kann benutzt werden, um weitere, nicht durch den CTA oder durch Plug-Ins abgedeckte Richtlinien, mit in den Überprüfungsprozess aufzunehmen. Die Konfiguration der im Script verfügbaren Posture Credentials erfolgt wieder durch ein ini-

[6] http://www.iana.org/assignments/enterprise-numbers

Applikations-Type ID	Applikations-Type Name	Anwendung
1	PA	Posture Agent (vom CTA mitinstalliertes Plug-In)
2	Host / OS	Host information (vom CTA mitinstalliertes Plug-In)
3	AV	Anti Virus
4	FW	Firwewall
5	HIPS	Host IPS
6	Audit	Audit
32768 - 65536		Reserviert für „loacal use“ - im Prinzip für selbstentwickelte Scripte und „private“ Erweiterungen.

Tabelle 2: Applikations-Typen

Applikations-Typ	Attribute ID	Attribute Name	Daten-Typ
Posture Agent	3 4 5 6 7 8 9	Agent-Name (PA-Name) Agent-Version OS-Type OS-Version User-Notification OS-Kernel OS-Kernel-Version	String Version String Version String String Version
Host	11 6 7 8	Machine-Posture-State Service Packs Hot Fixes Host-FQDN	1 - Booting, 2 - Running, 3 - Logged in String String String

Tabelle 3: Posture Credentials des CTA

File, welches syntaktisch identisch mit dem ini-File für Plug-Ins ist und welches das externe Script referenziert. Das Script muss die gesammelten Daten in einem definierten Format in eine Posture Data Datei schreiben und ctasi.exe aufrufen, welches die Datei parst und die extrahierten Posture Credentials an den ACS übermittelt.

Die Architektur des CTA (Abbildung 3) verdeutlicht die Zusammenhänge zwischen den verschiedenen Komponenten. Eine Kommunikationsschicht nimmt Posture Credentials (EAP-TLV) vom Broker entgegen und reicht diese weiter an Transportmodule, die von der NAC-Variante abhängig sind. Die Posture Plugin API und das Scripting Interface ermitteln Posture Credentials und übergeben diese mittels des Brokers an die Kommunikationsschicht.

1.2.2 Ein simples NAC-Layer3-IP Testsetup

Um ein besseres Verständnis der Funktionsweise und Zusammenhänge zu entwickeln, soll an dieser Stelle ein einfaches NAC-Layer-3-IP Testnetzwerk vorgestellt und die Konfiguration der beteiligten Komponenten dargestellt werden. In Abbildung 4 ist das Netzwerk in abstrahierter Form dargestellt. Der Cisco Secure ACS steht im NAC-geschützten Core, RAS-Benutzer können mittels einer VPN-Verbindung uneingeschränkt mit dem Office-Netzwerk kommunizieren, müssen allerdings einen NAC-Kontrollpunkt passieren, um auf Systeme im Core zugreifen zu können. Die Wahl der NAC-Variante für dieses Szenario ergibt sich von selbst; Layer2-802.1X kann nicht funktionieren, da die Clients nicht lokal an einen Switch konnektieren. Bei NAC-Layer2-IP wird der NAC-Vorgang per DHCP-Request oder ARP-Request getriggert – und offensichtlich wird das NAD von den RAS-Clients niemals einen ARP-Request oder DHCP-Request sehen. Somit bleibt nur noch NAC-Layer3-IP als mögliche Variante für dieses Szenario übrig. Dieses Testnetzwerk wurde mit vielen verschiedenen Policies getestet, um das Verhalten der Komponenten zu verstehen; exemplarisch ist in Abbildung 5 eine sehr einfache Admission-Policy wiedergegeben.

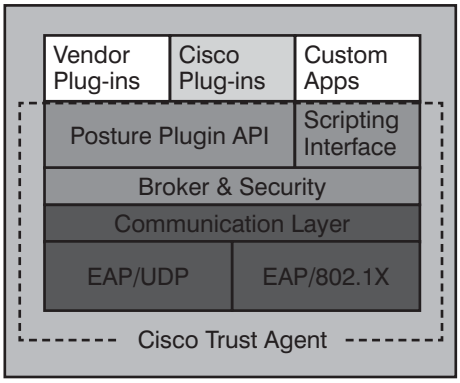


Abbildung 3: Architektur des CTA

Auf dem ACS können Benutzerbenachrichtigungen für jeden SPT konfiguriert werden.

Die Konfiguration des NAD (im beschriebenen Szenario wurde die Funktion des NAD von einem Cisco 3640 wahrgenommen) ist unaufwendig. Eine Admission Policy wird erstellt und an das externe Interface gebunden. Auf diesem Interface ist eine ACL als Paketfilter in Kraft, die außer dem EAPoU Verkehr keinen weiteren Verkehr in den NAC-geschützten Core des Netzwerkes passieren lässt. Falls auf dem ACS die SPTs mit dynamischen ACLs verknüpft sind, dann wird die auf dem NAD vorhandene ACL automatisch um die Einträge der dynamischen ACL erweitert. Zusätzlich wurde eine optionale Konfiguration für clientless Systeme vorgenommen. Diese Systeme werden gegen den ACS mit dem Benutzernamen clientless autorisiert und auf dem ACS ist dieser Benutzername mit einer eigenen (restriktiven) ACL konfiguriert, die automatisch für alle Systeme ohne funktionierenden CTA zur Anwendung kommt.

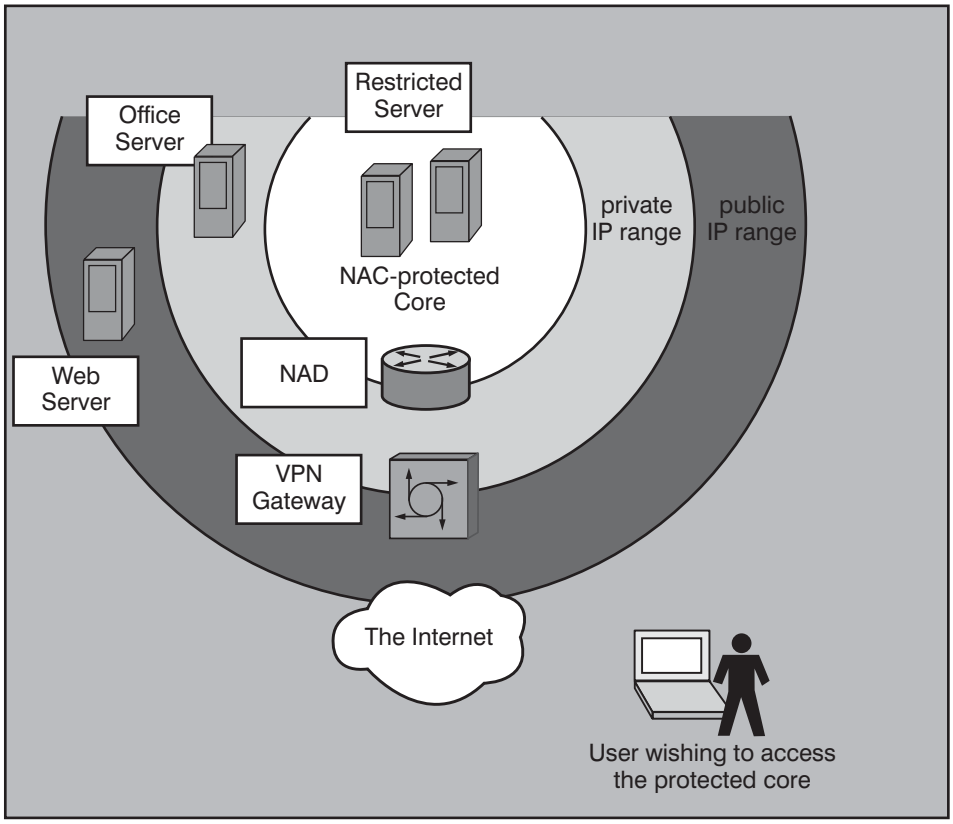


Abbildung 4: Einfaches NAC-L3 Setup

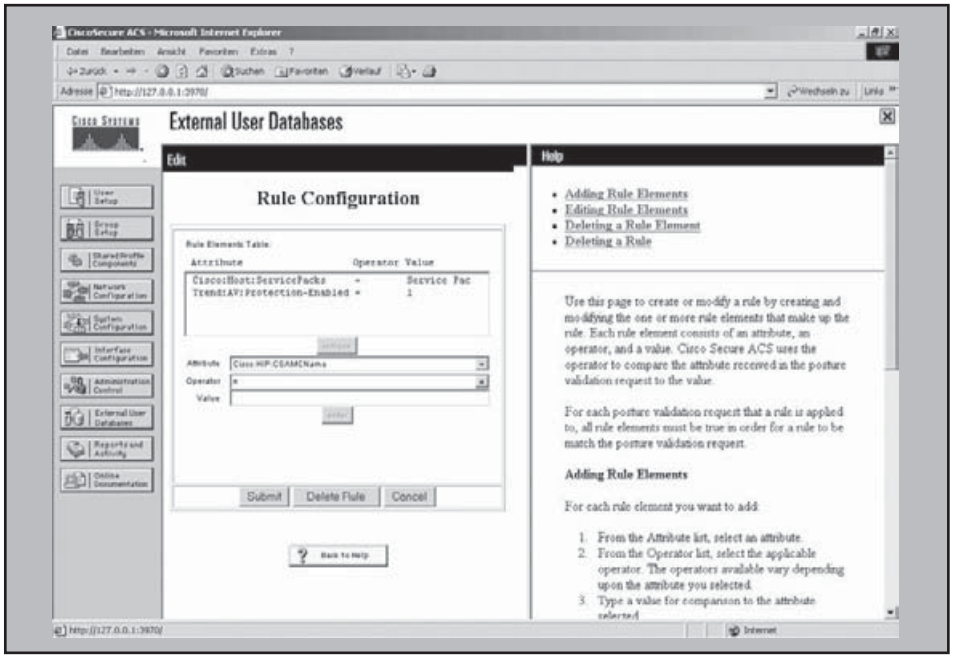


Abbildung 5: Eine exemplarische Policy zum Abfragen der Windows-Version und des Hostnamen. Beide Credentials sind für die Applikation PA (CTA). Der APT für PA ist healthy, falls das Client-Betriebssystem Windows XP Professional ist und der Client gleichzeitig den Hostnamen vm-xp-nocta ist. Falls einer der beiden Tests fehlschlägt, wird der APT für PA Quarantine.

Sobald IP-Pakete aus dem Office-Netzwerk Richtung Core durch den NAD geroutet werden, fängt die Admission Policy des NAD diese Pakete ab und sendet ein EAP-Hello zum Client um eine Kommunikation mit dem CTA zu etablieren. Nach erfolgreichem EAP-Handshake sendet der CTA seine Posture Credentials zum ACS, der aus der konfigurierten Policy die APTs und den SPT ermittelt und diese zuzüglich zu den ACLs an den Router bzw. an den Client kommuniziert. Abbildung 7 zeigt, dass der Client 192.168.67.34 ohne CTA als Clientless autorisiert wurde und der Client 192.168.67.24 per EAP den SPT healthy erhalten hat.

1.2.3 Kommunikationsfluss für NAC-Layer3-IP

NAC-Layer3-IP benutzt Protected EAP (PEAP) über UDP als Transport-Mechanismus zur Übermittlung der Posture Credentials. PEAP stellt zunächst einen sicheren[7] TLS-Tunnel zwischen dem Client und dem ACS her. Innerhalb des Tunnels kann der Client optional authentifiziert werden, was aber im Cisco NAC nicht geschieht. Abbildung 8 zeigt eine generische Abbildung des Kommunikationsflusses für NAC-Layer3-IP und Abbildung 10 zeigt den Kommunikationsfluss detaillierter inklusive der Informationen, die in jedem Paket übermittelt werden.

Cisco NAC-Layer3-IP und NAC-Layer2-IP benutzen PEAPv1 und EAP-TLV. Die PEAP-Kommunikation läuft in zwei Phasen ab. Phase 1 etabliert einen sicheren Tunnel per EAP-TLS und authentifiziert den Server mittels des Server-Zertifikats. Die zweite Phase beinhaltet eine optionale Client-Authentifizierung und den Austausch beliebiger Informationen – im Fall von Cisco NAC besteht diese beliebige Information aus den Posture Crendentials und Posture Notifications, die als EAP-TLV dargestellt werden.

[7] "Sicher" bedeutet in diesem Fall, dass der Client den ACSs per Server-Zertifikat authentifiziert und die Kommunikation innerhalb des Tunnels verschlüsselt stattfindet.

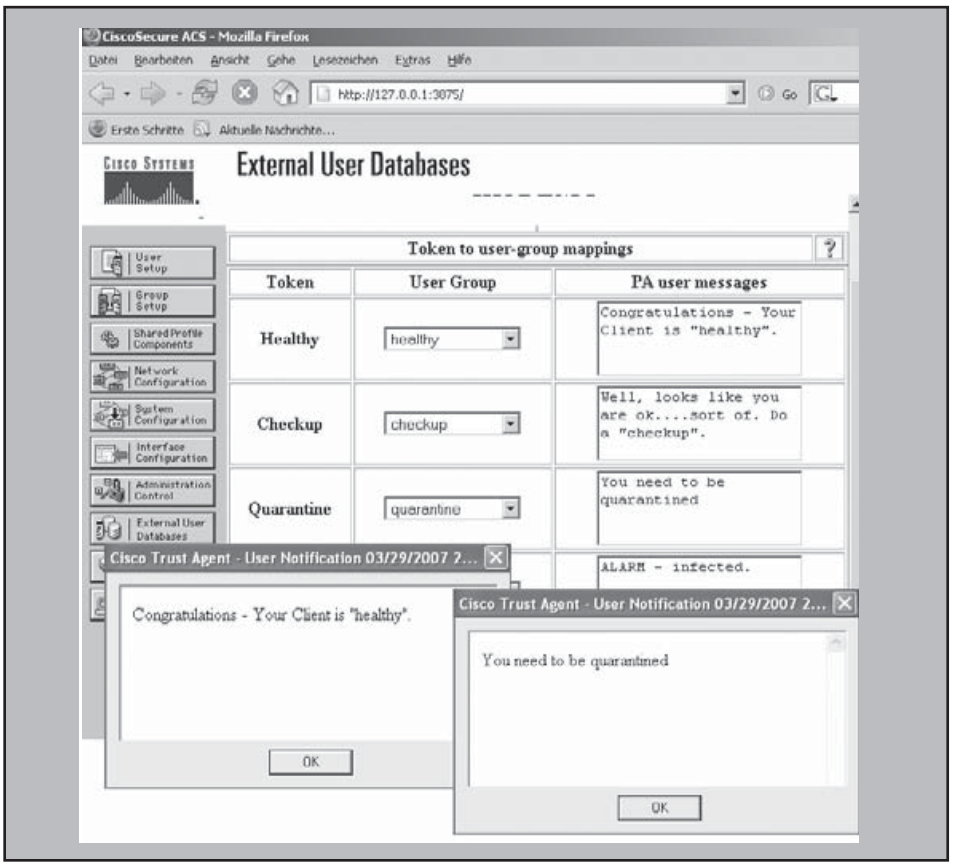


Abbildung 6: Konfiguration der Benutzerbenachrichtigung im ACS und korrespondierende Pop-Up-Fenster des CTA.

```
nad#
nad#
nad#show eou all
-----------------------------------------------------------------
Address         Interface       AuthType   Posture-Token Age(min)
-----------------------------------------------------------------
10.1.1.90       FastEthernet3/1 UNKNOWN    -------       0
192.168.81.70   FastEthernet3/1 EAP        healthy       0

nad#
```

Abbildung 7: Ergebnis von „show eou all" auf dem NAC-Router

2 Sicherheitsanalye

Im Vergleich der verschiedenen NAC Varianten bezüglich der immanenten Sicherheit, sind zumindest in zwei Aspekten große Unterschiede deutlich, die in der nachfolgenden Tabelle aufgeführt sind. (siehe Tabelle 4)

Eine gemeinsame Eigenschaft, bzw. ein gemeinsames Problem ist, dass der „Zustand" des Clients in allen Cisco NAC Varianten (und auch in den NAC Lösungen vieler anderer Hersteller) als Kriterium zur Ableitung des Zugriffslevels (oder auch der „Vertrauenswürdigkeit des Clients") herangezogen wird. Dieser „Zustand" des Clients wird ermittelt aus Informationen, die der (nicht vertrauenswürdige) Client selbst liefert – die Vertrauenswürdigkeit wird also abgeleitet aus Informationen die der nicht-vertrauenswürdiger Client selber liefert. Dieses Paradoxon erinnert frappierend an das philosophische Paradoxon des Epimenides. Der kretische Philosoph Epimenides stellte die Behauptung auf: „Alle Kreter sind Lügner".

Die nächste problematische Eigenschaft ist, dass zwei der drei Cisco NAC Varianten ohne intrinsische Client-Authentifizierung funktionieren, ja es nicht einmal die Möglichkeit gibt, eine Authentifizierung innerhalb des NAC-Frameworks zu benutzen. Die Identität des Clients wird von Cisco NAC nicht überprüft und es findet eine Autorisierung ohne Authentifizierung statt. Dies ist vergleichbar mit dem Vorzeigen einer gefälschten Polizeimarke an einer Zugangskontrolle ohne weitergehende Überprüfung der Identität des Vorzeigenden. Jeder, der eine gültig aussehende Marke hat, wird zum Zutritt autorisiert.

Entweder ist das Design von Cisco NAC fehlerbehaftet oder Cisco NAC wurde nicht als Sicherheits-Technologie entwickelt. An dieser Stelle sei ein Zitat der Cisco NAC Website[9] erlaubt. Unter dem Abschnitt „NAC business benefits" lautet der erste Eintrag: "dramatically improved security". Cisco betrachtet NAC also als Sicherheits-Technologie und so kommen die Autoren zu der Schlussfolgerung, dass das Design des CTA fehlerbehaftet ist.

Die aus der vorgenannten Schlussfolgerung abgeleitete Frage „kann das fehlerhafte Design durch einen Angreifer ausgenutzt werden?" liegt auf der Hand. Und wenn die Antwort auf die Frage „ja" lautet (und so lautet sie), dann lauten die nächsten Fragen „wie?", „unter welchen Umständen?" und „was kann ein Angreifer damit erreichen?". Der Aspekt, dass die Kommunikation mit dem lokalen Subnetz des Clients nicht eingeschränkt werde kann ist in diesem Kontext irrelevant und somit uninteressant. Das die Autorisierung über vom Client gelieferte Informationen ohne Authentifizierung des Clients stattfindet ist für einen Angreifer der interessantere Aspekt. Wenn es einem Angreifer gelingt zu kontrollieren, welche Informationen geliefert werden, oder wenn der Angreifer die zu liefernden Informationen selbst zu generieren vermag, dann kann dadurch ein unautorisierter Zugriff auf NAC-geschützte Netzwerke erlangt werden. Dieser Angriff wird im Folgenden als Posture Spoofing Attack bezeichnet.

2.1 Der Angreifer

Verschiedene Angriffs-Vektoren für den oben generisch beschrieben Posture Spoofing Angriff sind möglich. Welcher Angriffs-Vektor in einem konkreten Szenario möglich ist, hängt maßgeblich davon ab, ob der Angreifer ein Innentäter oder ein Externer ist.

Insider: Als Insider wird ein legitimer Benutzer eines NAC-geschützten Netzwerkes bezeichnet. Der Client des Insiders hat eine valide und funktionsfähige CTA-Installation und valide Benutzer/Maschinen-Daten zur Authentifizierung am Netz. Dies beinhaltet, dass auf dem Client des Insiders das Server-Zertifikat des ACS installiert ist und falls NAC-Layer2-802.1X benutzt wird der Client zusätzlich über ein valides PAC[10] verfügt. Die Motivation des

[9] http://www.cisco.com/go/nac
[10] PAC: Protected Authentication Credential. Eine Art signierter pre-shared-key, der in EAP-FAST zum Einsatz kommt.

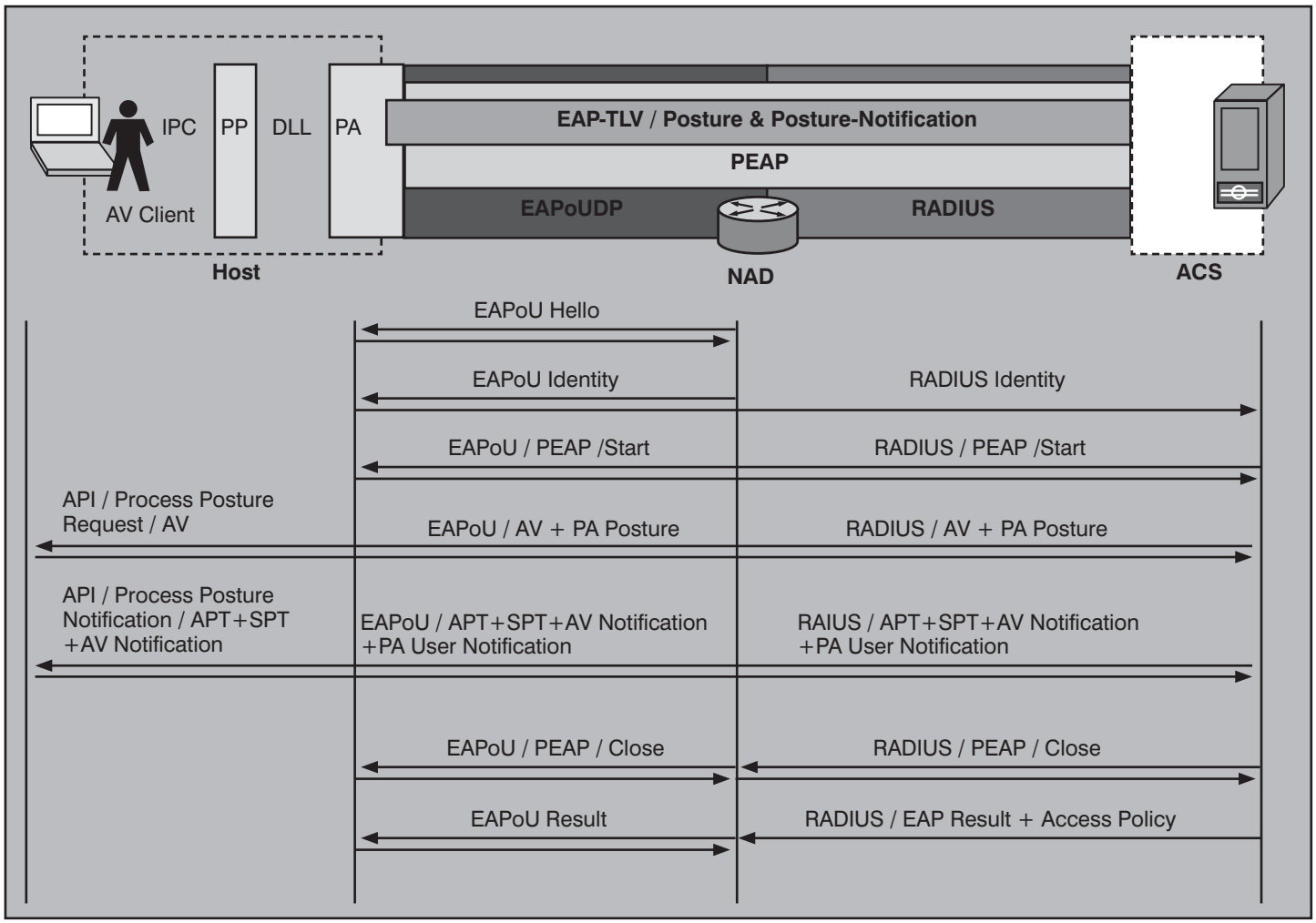


Abbildung 8: Generischer Kommunikationsfluss in NAC-Layer3-IP[8]

Insiders ist Zugriff auf das Netzwerk zu erhalten, obwohl sein Client nicht regelkonform ist (andere / keine Antiviren-Software, installierte Hackertools, die laut Policy verboten sind, etc.)

Outsider: Der Outsider ist kein legitimer Benutzer des NAC-geschützten Netzwerkes und versucht unautorisierten Zugriff zu erlangen. Ein Outsider verfügt nicht über gültige Login-Daten, hat kein valides PAC für NAC-Layer2-802.1X und ist auch nicht im Besitz des Server-Zertifikats des ACS.

Die logische Lokation des Angreifers bezüglich des Netzwerkes und der Typ des NAD (Router, Switch, etc) spielen keine große Rolle für den Angriff, da die relevante Kommunikation (EAPoU oder EAPo8021.x) immer erlaubt sein muss.

2.2 Die Angriffe

Folgende Angriffe gegen Cisco NAC sind, abhängig vom Angreifer und der eingesetzten NAC-Variante, möglich. (siehe Tabelle 5)

2.2.1 Austausch des CTA

Der einzige erfolgversprechende Angriff eines Outsiders besteht im Austausch des CTA durch einen selbstentwickelten NAC-Client, der die komplette Kommunikation nachbildet und beliebige, vom Angreifer ausgewählte, Posture Credentials übermittelt. Dieser Angriff ist möglich, da der ACS im Zuge der PEAP-Aushandlung dem Client das Server-Zertifikat übermittelt. Der CTA validiert dieses Zertifikat gegen das im Zertifikatsspeicher vorhandene Server-Zertifikat bevor die PEAP-Aushandlung weitergeführt wird. Ein alternativer NAC-Client müsste dieses Server-Zertifikat immer akzeptieren und das nicht offen gelegte Kommunikationsformat nachbilden.

2.2.2 DLL/Plug-In Austausch

Dem Insider steht neben dem kompletten Austausch des CTA auch der Austausch der Plug-In DLLs als Angriff gegen NAC zur Verfügung. Dabei werden die originalen Plug-Ins ersetzt durch Plug-Ins, die beliebige, vom Angreifer gewählte Posture Credentials übermitteln. Das Plug-In Interface des CTA ist zwar nicht offengelegt, allerdings kann die Funktionsweise durch Reverse-Engineering Methoden ermittelt werden. Der Aufwand ist im Vergleich mit der Entwicklung eines eigenen NAC-Clients sehr gering. Dieser Angriff konnte von den Autoren erfolgreich durchgeführt werden.

2.2.3 Manipulation des Scripting Interfaces

Ein weiterer Angriff, der dem Insider offen steht, ist der Missbrauch des Scripting-Interfaces des CTA. Dieser Angriff funktioniert ähnlich wie der Austausch von DLLs, allerdings ist nicht einmal die Programmierung einer DLL nötig, da das Scripting Interface mit beliebigen ausführbaren Programmen, also z.B. auch Batch-Dateien, zusammenarbeitet. Ein Angreifer kann über das Scripting Interface des CTA Posture Credentials an den ACS übermitteln. Laut Dokumentation sind diese Posture Credentials jedoch zwei Einschränkungen unterworfen. Zum einen muss die Vendor-ID immer Cisco sein und zum an-

[8] Ein Zitat aus "Implementing Network Admission Control Phase One Configuration and Deployment Guide" (erhältlich unter http://www.cisco.com) erhellt die Rolle des Routers innerhalb der Kommunikation: „Note that the router acts as a pass-through device at this point; it does not proxy any part of the PEAP session but merely reencapsulates the PEAP packets from UDP to RADIUS."

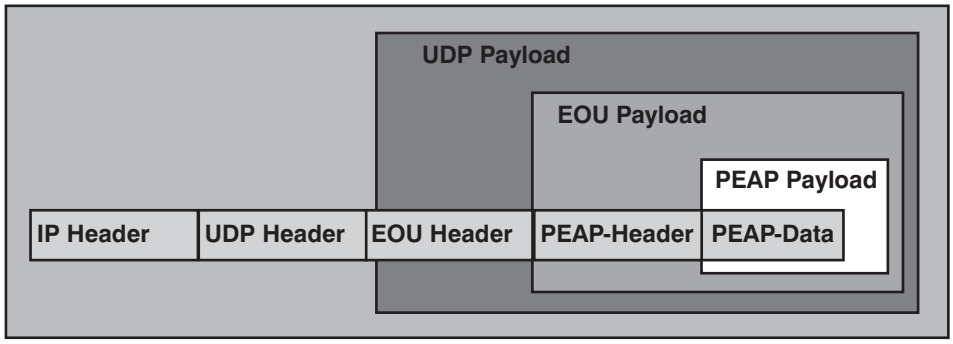


Abbildung 9: Generisches Frame Format

deren muss die Applikations-ID aus dem für Scripte reservierten, privaten Bereich stammen. Ein Script, welches das Posture Credential „McAfee Antivirus aktiviert“ liefert, ist demnach nicht möglich. In Tests mit dem CTA 2.0 konnte diese Einschränkung nicht verifiziert werden, ein erfolgreicher Angriff konnte aber noch nicht entwickelt werden.

3 Maßnahmen zur Verbesserung der Sicherheit

Die Frage, die sich aus der Sicherheitsanalyse ergibt, ist, wie eine sichere Variante des Cisco NAC Frameworks eingesetzt oder entwickelt werden kann. Da es sich bei den dargelegten Schwachstellen nicht um Programmierfehler, sondern um Designfehler handelt, kann ein einfaches Patchen seitens Cisco die Probleme nicht beheben.

3.1 Maßnahmen durch Cisco

Cisco kann das Design des NAC Frameworks verbessern um Angriffe durch Insider und Outsider zu verhindern. Einige denkbare Ansätze werden im Folgenden skizziert.

Code Signing: Durch Code Signing[12] der Plug-Ins und Überprüfung der Signatur der Plug-Ins durch den CTA würde die Ausführung von ausgetauschten DLLs verhindert werden. Signierter Code erhöht die Vertrauenswürdigkeit der Applikation und der durch die Applikation gelieferten Informationen massiv und sollte unserer Meinung nach für Applikationen im Sicherheitsumfeld eine Selbstverständlichkeit sein. Signierter Code könnte allerdings Angriffe durch einen selbstentwickelten, alternativen NAC-Client nicht verhindern.

Client	Authenticator
	<-- EAP-Request/Identity
EAP-Response/Identitiy (MyID) -->	
	<-- EAP-Request/EAP-Type=PEAP(PEAP Start, S bit set)
EAP-Response/EAP-Type=PEAP(TLS client_hello)-->	
<--EAP-Request/EAP-Type=PEAP(TLS server_hello, TLS certificate, [TLS server key_exchange,][TLS certificate_request,] TLS server_hello_done	
EAP-Response/EAP-Type=PEAP([TLS certificate,] TLS client_key_exchange, [TLS certificate_verify,] TLS change_cipher_spec, TLS finished) -->	
	<-- EAP-Request/EAP-Type=PEAP (TLS change_cipher_spec, TLS finished)
TLS tunnel established	
EAP-Response/EAP-Type=PEAP -->	
	<-- EAP-Request/Identity
EAP-Response/identity (MyID) -->	
	<-- EAP-Request/EAP-Type=X
EAP-Response/EAP-Type=X or NAK -->	
	<-- EAP-Reqeust/EAP-Type=X
EAP-Response/EAP-Type=X -->	
	<-- EAP-Success
Tunnel is decomissioned	

Abbildung 10: Detaillierte Darstellung der PEAPv1 Kommunikation

	NAC-Layer 3 IP	NAC Layer 2 IP	NAC Layer 2 802.1X
Client Authentifizierung	Keine intrinsische Authentifizierung des Clients. In VPN-Szenarien kann die Authentifizierung des Benutzers/des Clients am VPN als „Mitigating Control“ betrachtet werden.	Keine intrinsische Client Authentifizierung und keine Möglichkeit eine solche “on top” hinzuzufügen.	Client Authentifizierung per 802.1X.
Beschränkung der Kommunikation im lokalen Subnetz des Clients.	Keine Möglichkeit die Kommunikation des Clients im lokalen Subnetz durch NAC zu beschränken.	Keine Möglichkeit die Kommunikation des Clients im lokalen Subnetz durch NAC zu beschränken.	Zugriff auf das lokale Subnetz des Clients kann durch “Port Control” am Switch unterbunden werden.

Tabelle 4: Vergleich der immanenten Sicherheitsmechanismen der verschiedenen NAC Varianten

[12] Eine gute Einführung in die Thematik des “Code Signing” ist auf MSDN verfügbar: http://msdn.microsoft.com/workshop/security/authcode/intro_authenticode.asp

	Insider	Outsider
NAC-L2-802.1X	DLL/Plug-In Austausch Manipulation des Scripting Interface CTA Austausch[11]	Keine. Die immanente Client-Authentifizierung erzwingt zunächst einen erfolgreichen Angriff auf die Authentifizierung bevor ein Angriff auf NAC stattfinden kann. Aktuell sind keine Angriffe gegen EAP-FAST bekannt.
NAC-L2-IP	DLL/Plug-In Austausch Manipulation des Scripting Interface CTA Austausch	CTA Austausch
NACL-L3-IP	DLL/Plug-In Austausch Manipulation des Scripting Interface CTA Austausch	CTA Austausch

Tabelle 5: Angriffs-Vektoren für Posture Spoofing

Obligatorische Authentifizierung: Starke obligatorische Authentifizierung in allen NAC-Varianten würde Angriffe durch Outsider massiv erschweren. Aufgrund des Einsatzes von PEAP sollte die Einführung einer obligatorischen (oder im ersten Schritt zumindest optionalen) Authentifizierung nicht mit zu viel Aufwand durch Cisco verbunden sein, da PEAP Client-Authentifizierung als Option von Hause aus beinhaltet. Der einzige plausible Grund für das Weglassen der Authentifizierungsmöglichkeiten durch Cisco ist unserer Meinung nach „Business“. Die Einführung von Cisco NAC ist auch ohne den zusätzlichen Aufwand der Implementation einer zusätzlichen, bevorzugt zertifikatsbasierten, Authentifizierung für den Kunden enorm und die Autoren vermuten, dass Cisco diesen Aufwand nicht noch weiter in die Höhe treiben möchte, um potentielle Kunden nicht zu verschrecken.

3.2 Maßnahmen durch Ciscos NAC-Kunden

Die Sicherheit einer Cisco NAC Lösung hängt maßgeblich von der spezifischen Implementation in den Netzwerken und der ausgewählten NAC Variante ab.

Starke Authentifizierung: NAC-Layer2-802.1X sollte immer nach Möglichkeit die bevorzugte NAC-Variante sein, da die Autorisierung um eine 802.1X-basierte Authentifizierung mit EAP-FAST ergänzt wird und aktuell keine Angriffe gegen EAP-FAST bekannt sind. Falls NAC-Layer2-802.1X nicht möglich ist, sollte eine zusätzliche starke Authentifizierung implementiert werden, um Angriffe durch Outsider zu erschweren. Zum Beispiel sollte in RAS-VPN-Szenarien, in denen NAC-Layer3-IP die einzig mögliche NAC Variante ist, eine starke Authentifizierung am VPN durchgeführt werden.

Least Privilege: Alle Angriffe durch Insider weisen eine Gemeinsamkeit auf: Die Installation des CTA wird manipuliert. Entweder durch Austausch des CTA selbst, oder durch Austausch der Plug-In DLLs oder durch Hinzufügen von Scripten. Dieser Manipulation kann auf verschiedene Arten begegnet werden. Präventiv können strikte Zugriffsrechte der relevanten Dateien und Verzeichnisse umgesetzt werden, die eine Manipulation durch nicht-administrative Benutzer verhindert. Reaktiv bzw. detektiv könnten die relevanten Dateien und Verzeichnisse auf Veränderungen hin überwacht werden. Die letztgenannte Variante ist aufgrund ihres reaktiven Charakters die schlechtere Wahl gegenüber der präventiven Zugriffskontrolle. Weder eine Überwachung der Dateien und Verzeichnisse noch strikte Zugriffsrechte verhindern allerdings die Benutzung eines selbstentwickelten NAC-Clients. Dieser Bedrohung kann durch eine strenge Desktop-Firewall-Policy begegnet werden, die das Öffnen des UDP-Ports 28162 (EAPoU) auf den original Cisco CTA beschränkt. Dadurch wäre der alternative Client nicht mehr in der Lage per EAPoU mit dem ACS zu kommunizieren und die Autorisierung würde fehlschlagen.

Einsatz des CSA statt des CTA: Zusätzlich zum CTA bietet Cisco auch ein Host-IPS an, den Cisco Security Agent (CSA), der den CTA beinhaltet und ein eigenes CTA Plug-In mit sich bringt. Der CSA überwacht die Integrität des CTA und verhindert dadurch illegitime Veränderungen des CTA. Dadurch werden Angriffe durch Insider massiv erschwert.

[11] Falls 802.1x zum Einsatz kommt, müsste der selbstentwickelte Client zusätzlich als EAP-Supplicant mit EAP-FAST Unterstützung fungieren, was den Entwicklungsaufwand massiv in die Höhe treiben würde. Zusätzlich sind aktuell keine Angriffe gegen EAP-FAST bekannt. Deswegen wird dieser Angriff als eher theoretischer Natur betrachtet und hier nur der Vollständigkeit halber aufgeführt.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Internetworking: Optimales Netzwerkdesign mit Switching und Routing, 07.05. - 11.05.07 in Aachen

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

Troubleshooting Exchange Server 2003, 21.05. - 22.05.07 in Aachen

Dieses 2-tägige Seminar ruft bewährte Technologien der Exchange Server-Produkte nochmals bei den Teilnehmern in Erinnerung und zeigt anhand dieses Know-How effiziente Maßnahmen zur Sicherung, Reparatur und Wiederherstellung von Exchange-Daten auf. Des Weiteren werden die Möglichkeiten betrachtet, die Exchange Server 2003 mit integriertem Service Pack 2 bietet, um dem wachsenden Problem zu begegnen, welches durch die Flut unerwünschter Nachrichten entsteht. Preis: € 1.390,- zzgl. MwSt.

WAN-Planung für zentrale Dienste, 21.05. - 23.05.07 in Bonn

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess, dem auch dieses 3-tägige Seminar dienen soll. Preis: € 1.690,- zzgl. MwSt.

IP-Telefonie Projektbericht: Konzeption, Rollout und Betrieb einer IP-Telefonie-Lösung in der Praxis, 21.05. - 22.05.07 in Bonn

Dieses 2-tägige Seminar beschreibt die Planung, Installation und den Betrieb einer IP-Telefonie-Komplettlösung auf Basis vernetzter Cisco CallManager ergänzt um Zusatzprodukte. In einem Unternehmensnetz wurden bereits 50 der über 100 Standorte mit Systemen und über 15.000 IP-Telefonen ausgestattet. Die im Zusammenhang mit einem VoIP-Projekt stehenden, wesentlichen Aspekte werden in einem Mix aus Erfahrungsberichten und technischen Beiträgen betrachtet. Die beiden Referenten, die für den Betrieb des Sprach-Datennetzes und der Telefonie-Lösung verantwortlich sind, schließen mit diesem Seminar eine Lücke zwischen dem theoretischen Verständnis von VoIP und der praktischen Umsetzung und bieten einen umfassenden Einblick in eines der größten VoIP-Projekte in Deutschland. Preis: € 1.390,- zzgl. MwSt.

Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 21.05. - 25.05.07 in Aachen

Dieses 2-tägige Seminar beschreibt die Planung, Installation und den Betrieb einer IP-Telefonie-Komplettlösung auf Basis vernetzter Cisco CallManager ergänzt um Zusatzprodukte. In einem Unternehmensnetz wurden bereits 50 der über 100 Standorte mit Systemen und über 15.000 IP-Telefonen ausgestattet. Die im Zusammenhang mit einem VoIP-Projekt stehenden, wesentlichen Aspekte werden in einem Mix aus Erfahrungsberichten und technischen Beiträgen betrachtet. Die beiden Referenten, die für den Betrieb des Sprach-Datennetzes und der Telefonie-Lösung verantwortlich sind, schließen mit diesem Seminar eine Lücke zwischen dem theoretischen Verständnis von VoIP und der praktischen Umsetzung und bieten einen umfassenden Einblick in eines der größten VoIP-Projekte in Deutschland. Preis: € 2.290,- zzgl. MwSt.

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 21.05. - 23.05.07 in Bonn

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Preis: € 1.690,- zzgl. MwSt.

Ethernet-Netzwerke: Techniken, Einsatzgebiete und Betrieb, 21.05. - 23.05.07 in Aachen

Dieses Seminar stellt die aktuellen Ethernet-Themen vor und zeigt, wie etablierte und neue Techniken in bereits wohlbekannten und zukünftigen Anwendungsgebieten eingesetzt werden können. Zu den analysierten Sonderanwendungsgebieten gehören insbesondere VoIP, Gefahrenmeldetechniken, Industrienetze und Rechenzentrumsbereiche. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, Planungsregeln vorgestellt, Möglichkeiten und Grenzen von Quality of Service und Risiken durch Fehlentscheidungen bei der Technikauswahl aufgezeigt. Aufbau von Infrastrukturen, Fehlersuche und das allgegenwärtige Thema Sicherheit werden aus der Praxis moderner Ethernet-Netze beleuchtet. Preis: € 1.690,- zzgl. MwSt.

TCP/IP und SNMP, 21.05. - 25.05.07 in Aachen

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

Grundlagen des Trouble Shooting in Lokalen Netzwerken, 11.06. - 15.06.07 in Aachen

eses 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.

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
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: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
18.06. - 22.06.07 in Bonn
10.09. - 14.09.07 in Berlin

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheits-konzepten
25.06. - 29.06.07 in Berlin
15.10. - 19.10.07 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolg-reichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
27.08. - 31.08.07 in Aachen
03.12. - 07.12.07 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolg-reichen Lösung“ und und „Sicherheit in Wireless LANs“.
€ 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

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