ComConsult Research

Der Netzwerk Insider

April 2005

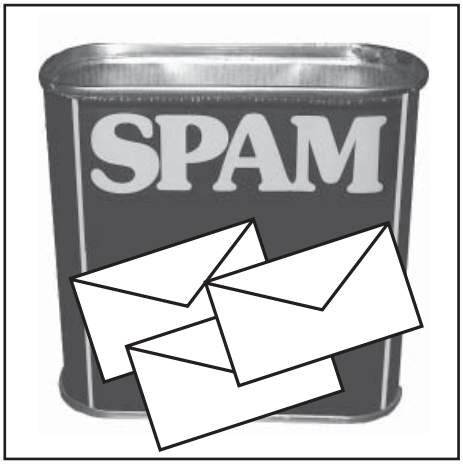
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

“Lovely spam! Wonderful spam!“ Was tut sich bei IETF?

von Markus Schaub

„Spam spam spam spam. Lovely spam! Wonderful spam! …“, sangen die Wikinger in Monty Pytons Flying Circus so laut, dass am Ende die anderen Gäste des Cafes nicht mehr zu verstehen waren. Zur Zeit gibt es viele Ansätze, SPAM und Phishing zu bekämpfen und auch - endlich könnte man aufseufzen - bei der IETF liegen Vorschläge namhafter Hersteller und Provider vor, ein weiteres Instrument im Kampf gegen die unerwünschten Mails zu standardisieren.



- Nur schwer verdauliche Kost -

Eigentlich war Dosenfleisch von Hormel Foods Inc. ursprünglich „Spiced Ham“ von den Wikingern gemeint, das später unter dem Markennamen Spam bekannt wurde. Das Bild passt jedoch so gut, dass sich der SPAM heute als Synonym für unerwünschte Massenmails genutzt wird. So amüsant vielleicht auch der Ursprung der Bezeichnung sein mag, so wenig amüsant ist allerdings auch die tägliche Werbeflut, die es einem fast schon unmöglich macht, die interessanten Emails in der Menge von Werbemüll auszumachen.

weiter auf Seite 22

Zweitthema

Praktische Umsetzung eines ISMS

von Holm Diening

Informationen und Informationsverarbeitung sind wesentlicher Bestandteil aller Geschäftsprozesse und gehören damit zu den Schlüsselfaktoren eines Unternehmenserfolges. Vergleichbar mit dem Qualitätsmanagement ist daher auch die Sicherheit der Informationsverarbeitung durch einen Managementprozess zu beobachten und zu steuern. „State of the art“ ist der Aufbau eines Information Security Management Systems (ISMS) nach dem British Standard 7799.

Dieser Artikel umfasst eine kurze Beschreibung des BS 7799 verbunden mit Hinweisen für den Aufbau eines solchen ISMS in größeren Unternehmen. Dabei soll der Fokus weniger auf dem generischen Ablauf eines solchen Projektes liegen, sondern sich vielmehr auf den Aufbau einer passenden Sicherheitsorganisation und Sicherheitsarchitektur konzentrieren. Zusätzlich wird die Möglichkeit der Nutzung des verbreiteten BSI-Grundschutzhandbuches zusammen mit BS 7799 aufgezeigt.

British Standard 7799

Die Entstehung des British Standard (BS) 7799 reicht zurück bis in das Jahr 1989. Die Abteilung CCSC (Commercial Computer Security Centre) des britischen Department of Trade and Industry (DTI) hatte die Aufgabe, einen “code of good security practice” zu erarbeiten.

weiter auf Seite 9

Top-Event

ComConsult IT-Sicherheits-Forum 2005

auf Seite 5

Zum Geleit

Für eine Zukunft der IP-Telefonie am Standort Deutschland

auf Seite 2

Report des Monats

Voice-over-IP-Lösungen von Alcatel

auf Seite 19

Zum Geleit

Für eine Zukunft der IP-Telefonie am Standort Deutschland

Im Gegensatz zu vielen anderen europäischen Regulierungsbehörden ist die RegTP offensichtlich nicht zu einer wirklichen Öffnung des Marktes für IP-Telefonie bereit. Die Konsequenzen dieser Haltung werden jetzt deutlich. So schätzt Arther D. Little, dass im Jahr 2007 in Frankreich ca. 60 Prozent der Bevölkerung IP-Telefonie nutzen werden, in Deutschland aber lediglich 10%. Für Japan geht man sogar von einer kurzfristigen Ablösung der traditionellen Telefonie durch IP-Telefonie aus.

Nun könnte man sagen, was soll es. Hauptsache die Preise für Sprachkommunikation sinken weiter, eigentlich ist ja auch egal womit wir telefonieren. Diese Sichtweise wäre mehr als kurzsichtig. Wir sprechen hier über einen immens großen Weltmarkt. In vielen Ländern ist IP-Telefonie längst Normalität.

Die Kernfrage der IP-Telefonie für Deutschland ist: wie viel von dem Weltmarkt werden deutsche Hersteller belegen können? Und hier ist nicht die Rede von den großen Anbietern a la Siemens sondern von dem Mittelstand, von dem dieses Land immer mehr lebt (immerhin kann ich mir von den Steuern, die so manches Großunternehmen zahlt noch nicht einmal eine Pizza kaufen). Und Unternehmen wie AVM zeigen, dass hier ein Markt ist, auf dem ein mittelständisches Unternehmen Erfolg haben kann.

Der richtige Zeitpunkt zum Einstieg ist jetzt.

IP-Telefonie ist im Umbruch zum SIP-Standard. Von daher werden die Karten für viele Firmen neu gemischt. Und gerade die Orientierung an SIP als Multimedia-Standard beinhaltet ein gewaltiges Potenzial. Viele Anwendungen, die in der Vergangenheit teuer, personalintensiv und schlecht nutzbar waren, werden mit SIP zum Mainstream. Beispiele dafür sind:

- Mehrpunkt-Sprachkonferenzen
- Mehrpunkt-Videokonferenzen
- Application-Sharing
- Kollaboration

Hier sind Ansatzpunkte für junge Unternehmen gegeben. Die Beispiele xten, Groove, WaveThree und viele andere mehr belegen dies. Auch für international tätige und spezialisierte Klein-Provi-

der ergeben sich wichtige neue Märkte (siehe Angebote wie sie heute von Viditel, SightSpeed, Convoq und ähnlich gelagerten Unternehmen im Web existieren). Hier kommt ein gewaltiger Markt auf uns zu. Wenn wir jetzt nicht auf diesen Markt reagieren, können wir uns ganz aus der IT-Entwicklung in Deutschland verabschieden (oder haben wir das nicht sowieso schon getan?).

Und jetzt kommt das Problem. Wer sich als Unternehmen in Deutschland für die Entwicklung von SIP-Produkten interessiert, der trifft auf einen künstlich klein gehaltenen lokalen Markt. Parallel kämpft man mit einem internationalen Wettbewerb, der in seinem Heimatmarkt deutlich bessere Bedingungen hat. Natürlich bietet gerade das Internet Anbietern von Software-Produkten eine perfekte Basis zu einer weltweiten Vermarktung, so dass für jedes auch deutsche Startup-Unternehmen das Ziel einer internationalen Vermarktung nur natürlich ist. Doch gerade für den Start sind optimale Standortbedingungen auf dem Heimatmarkt eine unverzichtbare Hilfe. Nur diese Umgebungsbedingungen garantieren die Verfügbarkeit von Kapital und lassen das Verhältnis von Risiko und Erfolgswahrscheinlichkeit für das Unternehmen tragbar erscheinen.

Oder lassen Sie uns die Frage anders herum stellen:

- Sie sind ein engagierter und gut ausgebildeter Netzwerk- und SIP-Spezialist, Sie sehen in diesem Markt eine Chance und wollen ein Unternehmen aufbauen
- Sie haben folgende Wahl:
  - Start in einem Heimatmarkt, der behindert wird, der sich deutlich langsamer als der Weltmarkt entwickelt, in dem keine ausreichenden Kapitalhilfen gegeben sind, in dem Sie durch völlig absurde Kreditvergaberegeln a la Basel II blockiert werden, in dem das bestehende Arbeitsrecht alle Pflichten auf ihre Seite legt, in dem Sie keine Kontakte zu den Großen der Branche haben
  - Start in den USA, mit vielen potenziellen gut ausgebildeten Mitarbeitern, wo Sie mitten im Geschehen sind, immer die neusten Informationen aus Ihrem Umfeld bekommen, wo Sie einen riesigen Heimatmarkt haben, einen deutlich leichteren Zugang zu Eigenkapital, den direkten Kontakt zu den Großen der Branche, wo Sie mitten in einem etablierten Beziehungsgeflecht stehen, das bereits an der Uni aufgebaut wird, wo ein flexibles Arbeitsrecht existiert
- Wie entscheiden Sie sich?

War der Schritt zu einer Unternehmensgründung im Ausland früher ein großer Schritt, so sprechen wir heute über einen Personenkreis von potenziellen Gründern, die mit hoher Wahrscheinlichkeit ein Jahr ihrer Gymnasialzeit und ein Jahr ihres Studiums im Ausland verbracht haben. Für diesen Personenkreis ist der Wechsel ins Ausland kein großer Schritt. Wenn wir diesem Personenkreis, der Deutschland in der Elektrotechnik und im Maschinenbau immerhin groß gemacht hat, im eigenen Land halten wollen, dann müssen wir klare, attraktive und nachhaltige Rahmenbedingungen schaffen.

So sehr nun die Interessen der deutschen Telekom zu beachten sind und so sehr die Telekom auch ein Anrecht auf eine faire Behandlung hat, so muss doch gleichzeitig an dieser Stelle festgestellt werden, dass es hier nicht um die Telekom sondern um den IT-Standort Deutschland geht. Wurde dieser bereits in den 80er

Für eine Zukunft der IP-Telefonie am Standort Deutschland

und 90er Jahren durch astronomische Steuersätze (ca. 70% für eine GmbH) blockiert, so wäre spätestens jetzt, da immer mehr Produktionsstandorte das Land verlassen, ein deutliches Umschwenken angesagt (in den letzten Jahren wurden über 20% aller deutschen Industriearbeitsplätze abgebaut). Wer nicht will, dass wir immer mehr zum reinen Vertriebsgebiet amerikanischer und asiatischer Produkte verkommen während gleichzeitig immer mehr deutsche Entwicklungen in die USA verlegt werden, der muss hier reagieren.

In diesem Zusammenhang ist das Verhalten der RegTP und der Bundesregierung ein Skandal. Um den Wert der noch durch den Bund gehaltenen Telekom-Aktien möglichst hoch zu halten, wird hier ein freier Wettbewerb bewusst verhindert. Zu welcher Heuchelei muss ein Politiker fähig sein, der einerseits die Situation des Standorts Deutschland beklagt und andererseits bewusst und mit voller Absicht einen wichtigen Zukunftsmarkt für Deutschland blockiert.

Für den Bereich IP-Telefonie müssen sofort Rahmenbedingungen geschaffen werden, die es für mittelständische Unternehmen attraktiv machen, in diesen Markt einzusteigen. Wir brauchen eine eigene starke IP-Telefonie-Industrie. Dazu gehört auch, dass gerade Unternehmen, die in diesem zukünftigen Weltmarkt tätig sein wollen, Eigenkapitalhilfen der KfW in einem dem Zielmarkt entsprechenden Ausmaß angeboten werden (ich spreche über einen 2-stelligen Millionenbetrag). Statt immer mehr Geld sinnlos und ohne jeden erkennbaren Effekt (außer gekauften Wählerstimmen) in den neuen Bundesländern zu vernichten, wäre hier ein Bereich gegeben, der einer wirklichen Förderung würdig wäre. Es wird Zeit, dass bei Subventionen verstärkt die Frage gestellt wird, wie viel man pro gezahltem Euro in welcher Zeit zurück erhält. Und während gleichzeitig Milliarden verschwendet werden, stehen für wirklich wichtige Entwicklungen mit herausragenden Chancen keine adäquaten Hilfen zur Verfügung. Statt dessen werden Unternehmen, die dann auch konsequenterweise ihre Aktivitäten ins Ausland verlegen als vaterlandslose Gesellen gebrandmarkt (wer hat denn eigentlich die heutigen europäischen Rahmenbedingungen geschaffen? Die Unternehmen, die nichts anderes tun als sich in einem vordefinierten Rahmen zu bewegen oder die Politiker, die frei von jeden nachvollziehbaren wirtschaftlichen Überlegungen eine EU-Erweiterung betreiben? Wer hat Herrn Schröder eigentlich davon abgehalten, vor der Aufnahme von 10 neuen Mitgliedern einen europäischen Mindeststeuersatz für die Körperschaftsteuer durchzusetzen? Er hat es doch weder versucht noch überhaupt diskutiert. Wenn es nicht erwünscht ist, dass sich Unternehmen frei im europäischen Rahmen bewegen und wenn alle, die dies tun, vaterlandslose Gesellen sind, warum hat man denn dann die EU in der heutigen Ausprägung geschaffen? Wozu hat man die europäische Niederlassungsfreiheit zu einem der höchsten bestehenden Rechtsgüter gemacht - man beachte die eindeutige Rechtssprechung des europäischen Gerichtshofes -, wenn man alle Unternehmen, die sich daran orientieren, beschimpft und verunglimpft?).

Die Mindestforderung für adäquate Standortbedingungen im Bereich IP-Telefonie sind:

- Sofortige Aufhebung der Bindung von DSL-Anschlüssen an Telefonanschlüsse
- Schaffung eines entbündelten Teilnehmerzugangs zu fairen Konditionen
- Übernahme der Grundhaltung der EU-Kommission: Themen wie Notruf und Security dürfen die Entwicklung dieser Technik nicht blockieren. Wir haben mündige Bürger, die selber für sich über diesen Punkt entscheiden können. Immerhin ist es ja auch erlaubt, keinen Telefonanschluss zu haben. Dann ist ein Notruf auch nicht möglich
- Aufbau universitärer Forschungszentren weit über das bestehende Ausmaß hinaus (heute sind zum Beispiel die Fraunhofer-Gesellschaften hier tätig) mit einer starken Anbindung an die Industrie

IP-Telefonie ist eine Chance für den Standort Deutschland. Gerade weil hier auch ein relativ leichter Zugang zu einem internationalen Markt besteht. Wenn wir noch ein paar Monate warten, ist dieser Markt belegt und ein Einstieg für kleinere Unternehmen nicht mehr sinnvoll. Von daher ist Eile geboten, die notwendigen Entscheidungen müssen in den nächsten Wochen fallen. Es kann nicht angehen, dass die übliche Trägheit von Provinzbürokraten und inkompetenten, heuchelnden Politikern wichtige Perspektiven für den Standort Deutschland vernichten. Wozu leisten wir uns eigentlich die teure Ausbildung von Diplom-Informatikern, wenn wir diesen jede Basis für eine spätere adäquate Berufsausübung entziehen?

Ihr
Dr. Jürgen Suppan

Neuer Report: Voice-over-IP-Lösungen von Alcatel

Unser im letzten Jahr veröffentlichter 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.

Dieser neuste Technologie-Report von ComConsult Research ist ein elementares Hilfsmittel für jede Evaluierung im IP-Telefonie-Markt, er stellt eine unschätzbare Einführung in die Produktpalette von Alcatel dar und ermöglicht in Verbindung mit dem Report „Cisco versus Siemens“ den direkten Vergleich mit den Produkten der beiden anderen Herstellern.

Autorin: Dipl.-Inform. Petra Borowka
Preis: € 398,- zzgl. MwSt. und Versand

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

Sonderveranstaltung
IP-Telefonie: Markt und Produkte in der Analyse

Vom 20.-22. Juni 2005 veranstaltet die ComConsult Akademie erstmalig ihre Sonderveranstaltung „IP-Telefonie: Markt und Produkte in der Analyse“ in Bonn.

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht:
- Hersteller haben ihre Strategien, Produkte und Ankündigungen mehrfach geändert
- Produkt-Architekturen sind komplex, insbesondere in redundanten Standort-übergreifenden Situationen
- Die gleiche Komplexität betrifft die Umsetzung von Sicherheits-Konzepten, die gerade bei IP-Telefonie elementar sind
- Neue Standards wie SIP verändern Produkte und ArchitekturenSDo
- Neue Funktionsbereiche wie Multipunkt-Audio und Video-Konferenzen, Kollaboration oder Präsenzbasierte Team-Funktionen erfordern die Kenntnis der zukünftigen Weiterentwicklung der Produkte

An dieser Stelle setzt diese hochaktuelle Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt.

Erfahren Sie:
- Was IP-Telefonie-Produkte leisten
- Worauf Sie bei der Auswahl achten müssen
- Wo typische Schwachstellen und Probleme liegen
- Welche Strategien ausgewählte Hersteller verfolgen
- Welche Erfahrungen ausgewählte Anwender gemacht haben

Die Veranstaltung besteht aus folgenden Teilen:
- Einführung in das Thema
- Anlagen-Architekturen, Funktionsmerkmale, Leistungsprofile
- Ergebnisse unserer großen Marktstudie
  - o Alcatel
  - o CISCO
  - o Siemens

In der Analyse und Bewertung, wer hat die beste Lösung für IP-Telefonie
- Vorstellung unseres Request for Information
- Stellungnahme und Präsentation der Hersteller
- Ausgwählte Anwender stellen ihre Erfahrungen mit IP-Telefonie-Installationen vor
  - o Wie erfolgte die Auswahl
  - o Wie hoch war der Konfigurationsaufwand
  - o Wie aufwendig ist der Betrieb
  - o Sind Erwartungen an Kostensenkung erfüllt worden
  - o Wie zufrieden sind die Anwender
- Ergänzt wird das Programm durch Detailanalysen:
  - o Die Zukunft der Siemens-Telefonie: was leistet die HiPath 8000
  - o IP-Telefonie und Sicherheit: Lösungsansätze und Alternativen

Wie Sie sehen, eine herausragende Veranstaltung, die Sie auf keinen Fall versäumen sollten, wenn Sie sich für IP-Telefonie interessieren. Die Veranstaltung steht unter der Leitung von Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke, unter deren Leitung auch die großen Marktanalysen über Alcatel, CISCO und Siemens entstanden sind. Als Teilnehmer an der Veranstaltung können Sie diese Markt-Analysen zu einem sehr attraktiven Sonderpreis erwerben.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IP-Telefonie:
Markt und Produkte in der Analyse

☐ Ich melde mich verbindlich an zur Sonderveranstaltung **“IP-Telefonie: Markt und Produkte in der Analyse“**
vom 20.-22.06.05 in Bonn
(Preis € 1.990.-- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich ein Hotelzimmer vom_____ bis_____05

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

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

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2005

Organisation und Technik der IT-Sicherheit mit Fachanalysen und Praxis-Workshops

Vom 06. - 09. Juni 2005 veranstaltet die ComConsult Akademie ihren Sicherheits-Kongress "ComConsult IT-Sicherheits-Forum 2005" in Königswinter.

Das Programm besteht aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen. Das Forum verbindet die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Der diesjährige Secuity-Kongress der ComConsult Akademie legt großen Wert auf Praxisnähe und bietet deshalb neben der notwendigen Behandlung ganz neuer Themen auch vielfältige Empfehlungen und direkt umsetzbare „Tipps und Tricks" für den Tagesbetrieb. Sie hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt.

An insgesamt vier Tagen werden angeboten:
- Aktuelle Übersicht zum Stand der Sicherheitsbedrohungen
- Trends und Marktentwicklungen bei Sicherheitstechnologien
- Behandlung wichtiger Bereiche der Sicherheitsorganisation
- Moderierte Produktvergleiche mit Live-Demos
- Vertiefende Tutorien und Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren mit folgenden Themen:
- Stand der IT-Sicherheit im Überblick - Secorvo College
- Sicherheit von Web-Applikationen Frank Breitschaft (GAI NetConsult)
- Praktische Einführung eines ISMS nach BS 7799 - Holm Diening (GAI NetConsult)

Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle fachliche Entwicklungen und Praxisbeispiele vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu speziellen Themen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2005 sind vorgesehen:

Endpoint Security - Dezentralisierung der Schutzmaßnahmen
- Notwendige Schutzfunktionen am Endpoint
- Anforderungen an das zentrale Management
- Endpoint Security Enforcement
- Cisco-NAC vs Microsoft-NAP

Identity Management
- IM und seine Bausteine (Directory Management, Provisioning, Access Management)
- Die Bedeutung von IM für die Sicherheitsinfrastruktur
- Wie kann man mit IM Kosten senken?
- Roadmap zur Einführung von IM

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

Sichere Nutzung von Webapplikationen
- Mit welchen Techniken werden Webapplikationen angegriffen?
- Vorstellung von Fallstudien und Erkenntnisse
- Sicherheitshinweise für Entwickler von Webapplikationen
- Sicherung von Webapplikationen mit Application Security Gateways

Was bringt die virtuelle Poststelle?
- Client- vs Server-basierte Mailverschlüsselung
- Signatur und Verschlüsselung durch zentrale Gateways (S/MIME, PGP)
- Zertifikats-Managements mit Benutzer-Domain- und Gruppenzertifikaten.
- Umsetzung von Anforderungen (BDSG, Grundschutzhandbuch BSI, BS 7799)

Sicherheitsaspekte bei Voice-over-IP
- Absehbare Bedrohungen gegen VOIP-Verbindungen
- Sicherheitsfeatures bei H.323 und SIP
- Auswirkungen der Sicherheitsinfrastruktur auf die QoS bei VOIP
- Wie kann man „Softphones" sicher betreiben?
- Physische Sicherheit in IT-Umgebun gen
- Haftungsrisiken für IT-Verantwortliche
- Sicherheit in der Bauausführung und Infrastruktur
- Sichere Ausführung von Energieversorgung, Zugangs- und Brandmeldetechnik
- Technische Sicherheit der IT-Komponenten

Schutz kritischer Datenbestände
- Disk- vs File-Encryption
- Schutz mobiler Daten: vom Notebook bis zum PDA
- wie umgehen mit „removable media"?
- Anforderungen an das zentrale Management

Aufbau eines ISMS nach BS 7799
- BS 7799 und Abgrenzung zum BSI-GSHB
- PDCA - die vier Phasen eines ISMS-Projektes
- Aufbau und Umsetzung in einer Konzernumgebung
- Welche Fehler sollte man unbedingt vermeiden

ComConsult IT-Sicherheitsforum 2005

Linux und Windows
- Ist Open Source sicherer als Closed Source?
- Kann Linux im Client -/ Server -Bereich empfohlen werden?
- Sind kombinierte Lösungen sinnvoll?

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

Weitere vorgesehene Themen
- VPN: IPsec vs SSL
- SAP-Security
- IT-Revision
- Forensische Untersuchungen

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

Moderator
Dipl.-Inform. Detlef Weidenhammer

ComConsult IT-Sicherheits-Forum 2005 06. - 09.06.2005 in Königswinter Frühbucher-Rabatt bis 15.04.2005

Teilnahmegebühr vom 06.06. - 09.06.05 inklusive Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.750,- (regulär € 1.990,-).

Teilnahmegebühr vom 07.06. - 09.06.05 ohne Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.480,- (regulär € 1.690,-).

Alle Preise zzgl. MwSt. Die Buchung innerhalb der Frühbucherphase ist verbindlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung ComConsult IT-Sicherheits-Forum 2005

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2005
vom 06.06. - 09.06.05 in Königswinter

mit Tutorium € 1.750,- zzgl. MwSt.*
☐ **Thema 1: Stand der IT-Sicherheit im Überblick**
☐ **Thema 2: Sicherheit von Webapplikationen**
☐ **Thema 3: Praktische Einführung eines ISMS nach BS 7799**

☐ **ohne Tutorium € 1.480,- zzgl. MwSt.***
***gültig bis 15.04.2005**

☐ Bitte reservieren Sie für mich ein Hotelzimmer vom_____bis_____05

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

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

Der Netzwerk-Insider Stellenmarkt

NEUER SERVICE!
Der Netzwerk-Insider Stellenmarkt

Der Netzwerk Insider zählt seit über 7 Jahren zu den führenden deutschen Technologie-Magazinen.

Die über 15.000 Stamm-Leser - davon mehr als ein Drittel in leitenden Positionen aus dem IT-Bereich und über 4.000 Netzwerk- und Server-Spezialisten - stammen aus den TOP 500 der deutschen Industrie und den deutschen Landes- und Bundesbehörden.

Mit der Februar-Ausgabe starteten wir den Netzwerk-Insider Stellenmarkt.

Für Ihre Personalsuche bieten wir:
- Perfekte Zielgruppenausrichtung
  - Netzwerk-Spezialisten/Innen
  - Server-Spezialisten/Innen
  - Web-Technologie-Spezialisten/Innen
  - Ebenso Führungskräfte aus diesen Bereichen
- Hohe Reichweite auf dem deutschen Markt
- Attraktive Preisgestaltung

Die genauen Mediadaten finden Sie auf unserer Homepage unter **www.comconsult-research.de** oder sprechen Sie uns an.

Ihre Stellenanzeige erscheint in der von Ihnen gewünschten Insider-Ausgabe sowie zwei Wochen später in einer Stellenmarkt-Sonderausgabe von Insider-Online. Parallel verröffentlichen wir Ihre Anzeige 4 Wochen auf unserer Homepage.

Auf Wunsch kann die Anzeige in der nächsten Insider-Ausgabe zu 50% des Preises wiederholt werden.

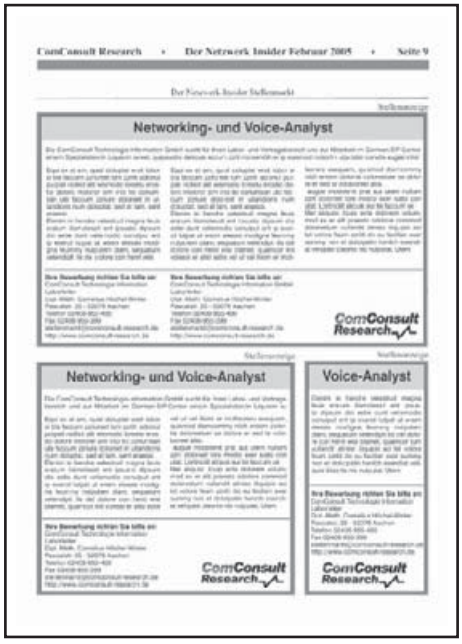
Bei Interesse schicken Sie Ihre Anfrage/Unterlagen an:
stellenmarkt@comconsult-research.de
oder rufen Sie einfach an:
Telefon: 02408-955 400
oder schicken Sie uns eine E-Mail an:
stellenmarkt@comconsult-research.de


ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Networking- und Voice-Analyst


ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Voice-Analyst

Sollten wir Interesse an einer Stellenanzeige in unserem Netzwerk-Insider geweckt haben, dann zögern Sie nicht sich mit uns in Verbindung zu setzen.

Ihre Ansprechpartnerinnen:
Christiane Zweipfennig
Stephanie Braun
Telefon: 02408-955 300

oder schicken Sie uns eine E-Mail an:
stellenmarkt@comconsult-research.de

☐ Ich bin an einer Anzeige im Netzwerk-Insider interessiert, bitte nehmen Sie zu mir Kontakt auf.

Vorname

Nachname

Firma

Straße

PLZ/Ort

Telefon

Fax

E-Mail

Inserieren Sie über unsere Web-Seite
www.comconsult-research.de

Der Netzwerk-Insider Stellenmarkt

Stellenanzeige

Networking- und Voice-Analyst

Die ComConsult Technologie-Information GmbH sucht für ihren Labor- und Vortragsbereich und zur Mitarbeit im German-SIP-Center eine/n Spezialisten/in

Leistungsprofil:
- Kenntnisse in Netzwerk-Technologien
- Kenntnisse in TCP/IP
- Kenntnisse in Sprachkommunikation
- Teamfähigkeit

Gegenstand der Arbeit sind folgende Tätigkeiten
- Installation und Betreuung der Labor-IP-Telefonie-Installationen
- Durchführung von Tests und Analysen
- Vorbereitung und Durchführung von Vorträgen und Seminaren

Sie sollten aufgeschlossen gegenüber neuen Technologien sein und den permanenten Weiterentwicklungen mit Spannung entgegen sehen. Die Stelle befindet sich am Standort Aachen.

Ihre Bewerbung richten Sie bitte an:
ComConsult
Technologie Information GmbH
Laborleiter
Dipl.-Math. Cornelius Höchel-Winter
Pascalstr. 25 - 52076 Aachen

Telefon 02408-955-400
Fax 02408-955-399
stellenmarkt@comconsult-research.de
http://www.comconsult-research.de

ComConsult Research

Stellenanzeige

Diplom-Ingenieur w|m bzw. Netzwerkmanager w|m

Nachrichtentechnik, Technische Informatik, Elektrotechnik

Innovationsfähigkeit und Know-how-Vorsprung bestimmen den Bosch Unternehmenserfolg. Meistern Sie zusammen mit uns neue Aufgaben durch Ihre Bereitschaft, ständig Neues zu lernen. Der Zentralbereich Informationsverarbeitung ist der Bosch-interne IT-Dienstleister, der die Geschäftsbereiche bei der Entwicklung ihrer Geschäftsprozesse unterstützt. Das Aufgabenspektrum umfasst neben der IT-Marktbeobachtung/-Beratung die Festlegung der IT-Architektur, die Entwicklung und den Betrieb von Anwendungen sowie den Betrieb der Infrastruktur wie Desktopsysteme, Computer-/Data Center, Kommunikationsnetze.
Ihre Aufgabe: ► Planung, Aufbau und Betrieb von Rechnernetzen (LAN) an unseren Standorten im Raum Stuttgart, Franken und Bühl ► Entwurf von LAN-Designs entsprechend unseren Standards ► Konfiguration und Inbetriebnahme von LAN-Komponenten ► Beseitigung von Störungen im LAN

Ihr Profil: ► Abgeschlossenes Ingenieurstudium (FH oder TH/Uni) im Bereich Nachrichtentechnik, Technische Informatik oder Elektro- und Informationstechnik bzw. ähnlicher Studiengang ► Kenntnisse in Ethernet, Routing und Switching; Netzwerkprotokollen; Netzwerkmanagement und -reporting; Komponenten des Herstellers Cisco; LAN-Verkabelung; Wireless LAN ► Erfahrungen im Betrieb von lokalen Netzen ► Selbständige, teamorientierte Arbeitsweise sowie ausgeprägte Kommunikationsfähigkeit ► Gute Englischkenntnisse ► Engagement über die normalen Arbeitszeiten hinaus

Jeder Erfolg hat seinen Anfang.
Bewerben Sie sich jetzt online unter www.bosch-career.de mit Angabe der Kennziffer 57212863.
Robert Bosch GmbH
Personalabteilung, Christina Hilz-Ettle
Postfach 30 02 20, 70442 Stuttgart

www.bosch-career.de

Zweitthema

Praktische Umsetzung eines ISMS

Fortsetzung von Seite 1

Holm Diening ist seit seinem Studium der Elektrotechnik als IT-Sicherheitsberater – zunächst selbständig, mittlerweile für die GAI NetConsult GmbH – tätig. Seine Schwerpunkte liegen im IT-Sicherheitsmanagement (ISO 17799), IT-Notfallmanagement (Business Continuity Management) und der Erstellung von organisatorischen und technischen Sicherheitsrichtlinien. Herr Diening hat umfangreiche Erfahrungen als Referent bei Sicherheitsschulungen und Security Awareness Trainings. Er besitzt die Zertifizierung als „Certified Information Systems Security Professional (CISSP)“ durch das (ISC)².
h.diening@gai-netconsult.de

Dieser wurde nach weiterer Überarbeitung als PD 0003 „A code of practice for information security management“ vom British Standards Institute (BSI, nicht zu verwechseln mit dem „Bundesamt für Sicherheit in der Informationstechnik“) heraus gegeben. Unter der Bezeichnung BS 7799 erfolgte die erste Veröffentlichung 1995. Der British Standard 7799 beinhaltet die in 127 Controls zusammengefassten „best practices“ für 10 Hauptbereiche der Informationssicherheit:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

Seit der Herausgabe des BS 7799-2:1998 ist der British Standard zweigeteilt: In einen „Code of Practice“ (Teil 1), der Richtlinien- und Empfehlungscharakter hat, und die „Specification with guidance for use“ (Teil 2), deren Inhalt die konkrete Umsetzung eines ISMS ist. Letzterer ist auch derjenige, der die Grundlage für eine eventuelle Zertifizierung nach BS 7799 bildet.

Aufgrund des internationalen Interesses wurde der British Standard 7799-1:1999 von der ISO als so genannter „Fast Track“, also in einem beschleunigten Verfahren, als ISO/IEC 17799:2000 adaptiert. Er ist inhaltlich identisch mit dem BS 7799-1:1999 und weist nur formale Anpassungen auf.

Die wohl wichtigste Neuerung ist aber die Überarbeitung des zweiten Teils, der als BS 7799-2:2002 veröffentlicht wurde. Wichtig vor allem deshalb, weil das Kernziel der Überarbeitung die Harmonisierung mit anderen Management-Standards wie der ISO 9001:2000 (Qualitätsmanagement) und der ISO 14001:1996 (Umweltmanagement) war. Der zweite Teil ist nun sowohl inhaltlich als auch strukturell konsistent mit diesen international anerkannten und vor allem auch bereits weitgehend implementierten Standards.

Wichtig ist die Neuerung aber auch deshalb, weil das PDCA (Plan-Do-Check-Act) Modell als Grundlage für den in sich geschlossenen Sicherheitsmanagement-Prozess eingeführt wurde. Er beschreibt die Elemente für die Entwicklung (Plan), die Einführung (Do) sowie die Revision (Check) und kontinuierliche Verbesserung (Act) eines ISMS.

Der British Standard 7799-2 bildet auch die Vorlage für die ISO 24743, die 2006 verabschiedet werden soll und dann ebenfalls, wie der Teil 1, internationale Gültigkeit hat. Sie soll im Wesentlichen dem britischen Original entsprechen.

Die derzeitige Revision der ISO/IEC 17799:2000 ist beinahe fertig gestellt. Die Veröffentlichung wird für Juni 2005 als ISO/IEC 17799:2005 erwartet. Die Änderungen ziehen eine entsprechende Anpassung des BS 7799-2:2002 nach sich. Dies betrifft insbesondere die Auflistung der Controls aus dem ersten Teil des Standards im Anhang des BS 7799-2. Der BS 7799-2:2005 wird dann zur selben Zeit veröffentlicht wie die ISO/IEC 7799:2005.

Abgrenzung zum IT-Grundschutzhandbuch

Der BS 7799 ist jedoch nicht der einzige Standard in der Information- und IT-Security. Gerade in Deutschland ist die Anwendung des IT-Grundschutzhandbuches (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik sehr verbreitet. Ein Vergleich beider Standards ist zwar möglich, wird aber zu keiner Bewertung im Sinne von „besser“ oder „schlechter“ führen, da bereits die Intention der Werke völlig verschieden ist. Die folgenden Bemerkungen sollen die wesentlichen Unterschiede zusammenfassen.

Zunächst ist das IT-Grundschutzhandbuch, wie der Name schon sagt, hauptsächlich IT-orientiert. Erklärtes Ziel ist die Erreichung eines angemessen Sicherheitsniveaus für Systeme niedrigen bis mittleren Schutzbedarfs. Es behandelt jedes Themengebiet als einen eigenen Baustein und bietet dazu einen Katalog von passenden Gefährdungen und Maßnahmen. Durch seinen modularen Aufbau und die regelmäßig erscheinenden Ergänzungslieferungen passt es sich der aktuell typischen IT-Situation in Behörden und Firmen an. Das Grundschutzhandbuch ist sehr praxisbezogen und adressiert beispielsweise auch konkrete Betriebssystemumgebungen oder Anwendungen. Die entsprechenden Module werden dabei nicht selten von den Herstellern selbst entworfen und gepflegt. Die Gestaltung als System von Bausteinen und auch die Unterstützung durch die Hersteller erleichtern die Umsetzung des Grundschutzhandbuches in der Praxis. Auf der anderen Seite verursacht dies leider aber auch die unterschiedliche Bearbeitungstiefe innerhalb der einzelnen Themengebiete.

Der BS 7799 richtet sich nicht an ein bestimmtes Sicherheitsniveau. Er ist auch nicht so stark IT-orientiert wie das Grundschutzhandbuch, sondern betrachtet Informationssicherheit ganzheitlich. Im Vordergrund des British Standard steht der

geschlossene Kreislauf des Sicherheitsmanagements, weniger die konkreten Maßnahmen der Umsetzung. Während beim BS 7799 eine klassische Risikoanalyse als Grundlage für die Auswahl der geeigneten Maßnahmen vorausgesetzt wird, sieht das Grundschutzhandbuch hierfür bereits vordefinierte Paarungen von Gefährdung und den entsprechenden Maßnahmen vor. Das GSHB hat damit gewissermaßen die Risikoanalyse für Standardfälle bereits durchgeführt und stellt die Ergebnisse als fertiges Handbuch zur Verfügung. Auch der BS enthält eine Liste von insgesamt 127 Controls, welche auf die Erreichung der Sicherheitsziele in den bereits genannten 10 Themengebieten ausgerichtet sind. Diese Controls sind jedoch generisch formuliert und enthalten keine konkreten Umsetzungsvorschriften. Produktbezogene Aussagen sind im BS an keiner Stelle enthalten.

Nicht zuletzt handelt es sich beim BS, vor allem nach der Adaptierung durch die ISO, um einen internationalen Standard, während das GSHB national ausgerichtet ist. Gerade für große Organisationen scheidet damit ein Einsatz des Grundschatzhandbuchs als führendes Dokument in der konzernweiten Information Security aus. Dies bedeutet aber keinesfalls, dass für die regionale Anwendung bei der Umsetzung das Gleiche gelten muss.

GSHB und BS sind also nicht als etwaige Entscheidungsalternativen zu betrachten, sondern vielmehr als in Teilen aufeinander aufbauende Dokumente, wobei der BS 7799 der führende und rahmenbildende Bestandteil sein sollte.

Hauptgründe für die Wahl des BS 7799 können sein:

- Er ist ein international anwendbarer und anerkannter Standard (Teil 1 auch formal durch die ISO), der keine Widersprüche zu regionalen Bestimmungen aufweist.
- Es existiert für den Teil 2 eine international anerkannte Zertifizierung, womit (ähnlich zur ISO 9001 „Qualitätsmanagement“) eine Vergleichbarkeit für das Sicherheitsmanagement in Unternehmen ermöglicht wird.
- Er führt eine weit reichende und übergeordnete Betrachtung der Informationssicherheit ein und beschränkt sich nicht nur auf die IT.
- Er enthält keine tiefer gehenden oder technischen Umsetzungsvorgaben, bestehende Konzepte können, sofern sie angemessen sind, integriert werden.
- Er fordert ausdrücklich die Berücksichtigung lokal geltender Gesetze und sonstiger Vereinbarungen (z.B. mit Kunden).
- Er harmoniert mit anderen internationalen Standards, die bereits in Unternehmen etabliert sind und kann von deren Umsetzung profitieren. Beispiel hierfür ist die ISO 9001:2000, die einen weitgehend gleichen strukturellen Aufbau hat wie BS 7799:2002. So lässt sich beispielsweise die „Lenkung von Dokumenten“ (4.2.3 [9001] bzw. 4.3.2 [7799]) sehr einfach adaptieren.
- Der IT-Prozess-Management-Standard „ITIL“ referenziert auf BS 7799-2.
- Der Nachweis für die Erfüllung der regulatorischen Anforderungen an die Informationssicherheit im Sarbanes-Oxley Act, im GmbHG oder im KonTraG wird durch die Einführung (und ggf. Zertifizierung) eines ISMS nach BS 7799-2 wesentlich erleichtert.
- Die Einführung eines international anerkannten ISMS hat möglicherweise Auswirkungen auf die Versicherungsprämien (IT-Haftpflicht, Betriebsunterbrechungsversicherung) und auf das Kredit-Rating (Senkung der operativen Risiken, Basel II).

Einführung eines ISMS-Projektes

Wer sich mit dem Gedanken trägt ein ISMS-Projekt ins Leben zu rufen, muss jedoch, noch bevor überhaupt mit der ersten Phase des ISMS begonnen werden kann, einige mögliche Stolpersteine aus dem Weg räumen. Etwa ein Drittel aller ISMS-Projekte werden während ihrer Einführungsphase abgebrochen, weil

- die Unterstützung des Managements nicht ausreicht und zum Beispiel durch eine Änderung der Prioritäten das Projekt verschoben wird.
- das Budget falsch kalkuliert wurde und ausgeschöpft ist.
- das eingesetzte Personal mit der Aufgabe überfordert ist.
- andere Abteilungen, außerhalb der IT, nicht einbezogen werden.

Unterstützung des Managements

Wichtigste Grundlage bei der Einführung eines ISMS ist die Unterstützung des, bezogen auf den Projektumfang, höheren Managements. Die Argumentation fällt leichter, wenn die Initiative, das Thema ISMS aufzugreifen, vom konzerneigenen Risikomanagement ausgeht. Hier kann auf bereits bestehende Verbindungen mit dem Top-Management zurückgegriffen werden. Da Information Security operationelle Risiken adressiert, ist die Zusammenarbeit mit dem Risikomanagement ohnehin obligatorisch.

In einer Präsentation sind dann vor allem folgende Aspekte wichtig:

- Operationelles Risiko „Informationsverarbeitung“ (eventuell Konsequenzen für das Rating darlegen)
- Trennung der Begriffe „IT-Security“ und „Information Security“, um die thematische Verknüpfung mit der IT-Abteilung zu lockern
- Zieldefinition: Einführung (und eventuell Zertifizierung) eines ISMS nach BS 7799
- Nutzen dieser Maßnahme klarstellen
- Prozessgedanken darstellen, eventuell durch Vergleiche mit dem Qualitätsmanagement
- Darstellung der benötigten Ressourcen und der formalen Befugnisse des Information Security Management Forums (Siehe weiter hinten im Text)

Kontinuierliches Budget sichern
Gerade die Budgetfrage kann auch noch in einer sehr späten Phase das gesamte Vorhaben scheitern lassen, nämlich dann, wenn das „Projekt“ der Einführung eines ISMS abgeschlossen ist und nun der „Prozess“ dieses ISMS zum Leben erweckt werden soll, aber die finanziellen Mittel nur für das „Projekt“ bereitgestellt wurden. Wichtig ist also von Anfang an zu verdeutlichen, dass ein neuer, kontinuierlicher Prozess, ähnlich dem Qualitätsmanagement, aufgebaut werden soll. Dieser Prozess benötigt für seine Initiierung, vor allem aber im laufenden Betrieb, ein entsprechendes Fundament an personellen und finanziellen Ressourcen.

Personalausstattung
Gerade die erstmalige Einführung eines ISMS erfordert neben einem hohen Personalaufwand auch ein sehr gutes Knowhow bei den Verantwortlichen. Die Unterstützung durch einen entsprechend erfahrenen externen Dienstleister ist daher angebracht. Ziel muss jedoch die Weiterführung des ISMS durch das eigene Personal sein. Dieses sollte daher in projektbegleitenden Workshops auf die späteren Aufgaben vorbereitet werden.

Die vier Phasen eines ISMS nach BS 7799

Mit der Version 2002 des zweiten Teils des BS 7799 wurde das PDCA (Plan-Do-Check-Act) Kreislaufmodell für die Abwicklung des kontinuierlichen Security Management Prozesses eingeführt. Die Phasen sind zwar aufeinander aufbauend, stellen jedoch keineswegs einen einzelnen Zustand dar, in dem sich das gesamte Projekt gerade befinden könnte. Alle Teile des Sicherheitskonzeptes können sich getrennt voneinander in unterschiedlichen Phasen dieses Modells befinden. In Abhängigkeit vom Entwicklungstempo bestimmter Technologien oder zum Beispiel der Natur eines Bedrohungsumfeldes werden einige Konzepte den Kreislauf mit einer höheren Frequenz durchlaufen als andere.

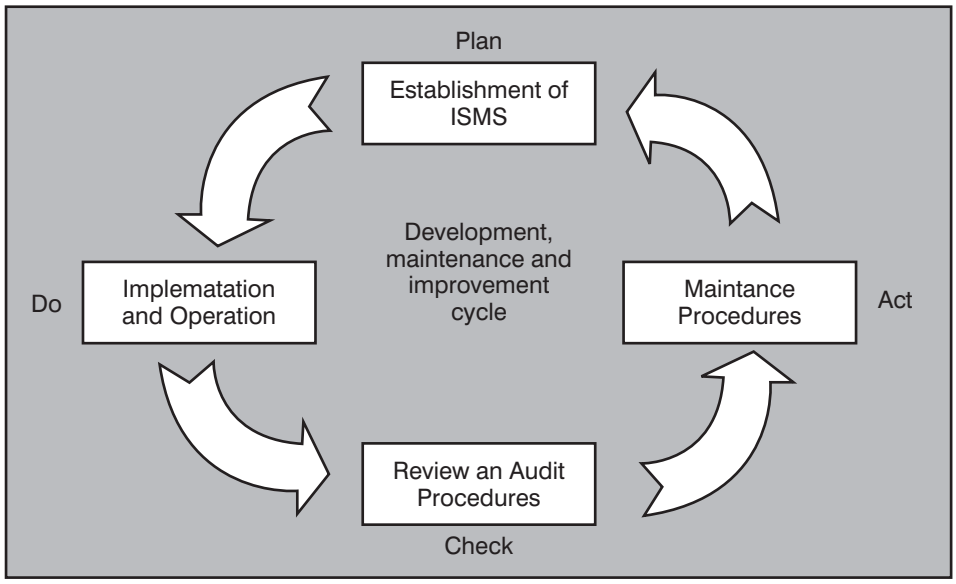


Abbildung 1: Die vier Phasen des ISMS

Die vier Phasen (siehe Abbildung 1) sind wie folgt zu charakterisieren:

Plan (ISMS Einführung):
Kerninhalt dieser Phase ist die Bestimmung der strategischen Sicherheitsziele, der Sicherheitspolitik sowie des Projektumfangs. Durch eine Analyse werden die Risiken identifiziert und bewertet, die innerhalb des definierten Projektumfangs liegen. Ergebnis ist dann ein Katalog, der die für die Behandlung der identifizierten Risiken geeigneten Kontrollmechanismen enthält. Der British Standard schreibt dabei keine spezielle Methode des Risk Assessment zur Anwendung vor.

Do (Implementierungsphase)
Die Implementierungsphase hat die Umsetzung der in der Planung definierten Kontrollmechanismen zum Inhalt. Der Entwurf der Sicherheitsarchitektur (Zusammenspiel aller Security Policies und den daraus abgeleiteten Standards und Guidelines) ist dabei ebenso wesentlicher Bestandteil wie der Aufbau der Sicherheitsorganisation, bei der Rollen und Verantwortlichkeiten im Sicherheitsprozess festgelegt werden. Nicht zuletzt erfolgt hier die tatsächliche organisatorische und technische Umsetzung der entwickelten Richtlinien und Standards.

Check (Überwachung und Überprüfung des ISMS)
Die „Check“ Phase begleitet eine Sicherheitskonzeption und das Sicherheitsmanagement selbst während des laufenden Betriebes. Hier wird die Übereinstimmung von Vorgabe und tatsächlicher Implementierung einer Revision unterzogen und gleichzeitig die Effektivität der getroffenen Maßnahmen in Bezug auf die formulierten Sicherheitsziele geprüft. Parallel dazu steht auch immer die Abstimmung der getroffenen Sicherheitsmaßnahmen mit der zu erreichenden Funktionalität eines Prozesses im Blickpunkt. Die Akzeptanz von Sicherheitsmaßnahmen hängt sowohl bei den Nutzern als auch beim Management davon ab, ob der reibungslose Ablauf eines Prozesses nicht durch zu starke Restriktionen behindert wird.

Act (Wartung und Verbesserung des ISMS)
Die Ergebnisse der Checkphase fließen permanent als Verbesserungen in das ISMS und die Sicherheitskonzepte ein. Die „Act“ Phase identifiziert und implementiert auch mögliche eingreifende oder präventive Maßnahmen, die sich aus der Analyse von Sicherheitsvorfällen oder Fehlfunktionen ergeben.

Wichtig für den Erfolg eines ISMS Projektes ist es, den Projektumfang zunächst nicht zu groß zu wählen, damit gerade bei den aufwändigeren Bestandteilen, zum Beispiel dem Risk Assessment, keine Dauerbaustellen entstehen, deren Ergebnisse bei Fertigstellung schon wieder veraltet sind. Bei großen Organisationen sollte daher zunächst das organisatorische Fundament des ISMS in der Muttergesellschaft realisiert werden. Kernthemen sind

hier die Formulierung der strategischen Sicherheitsziele und die Entwicklung einer konzernweit verbindlichen Sicherheitspolitik. Ebenso erfolgen hier die Etablierung der erforderlichen Managementprozesse und der zugrunde liegenden Sicherheitsorganisation sowie die Definition der Schnittstellen mit den Konzerngesellschaften. Diese Aufgaben werden durch das Information Security Management Forum übernommen, auf dessen Rolle hier noch einmal genauer eingegangen werden soll.

Die Gremien eines ISMS

Information Security spielt überall dort eine Rolle, wo Informationen in irgendeiner Form verarbeitet werden. Daher ist es nicht angebracht die Information Security dem IT- Bereich zuzuordnen, weil dieser lediglich das technische Fundament der Informationsverarbeitung bildet, die notwendigen Maßnahmen sich aber über die gesamte Breite des Unternehmens erstrecken. Zusätzlich besteht die Gefahr, dass die IT den dann entstehenden Zielkonflikt aus angestrebtem Sicherheitsniveau und der Bereitstellung von Funktionalität selbst ausfechten muss. Da die Leistungsfähigkeit einer IT jedoch zumeist weniger an der Security als an ihrem Beitrag für die Geschäftsprozesse gemessen wird, ist eine Vorentscheidung gegen die Umsetzung von Sicherheitsmaßnahmen absehbar.

Ähnlich dem Qualitätsmanagement eines Unternehmens ist das Information Security Management als eine Stabsstelle zu betrachten. Da es operative Risiken zum Gegenstand hat, sollte es mit dem Risikomanagement zusammenarbeiten. Die nachstehende Abbildung 2 verdeutlicht, welche Gremien nach ISO 17799:2000 empfohlen werden und wie diese positioniert sein könnte.

Zu den Aufgaben des Information Security Management Forums gehören:

- Genehmigung der Sicherheitsleitlinie und der Sicherheitsstrategie
- Festlegung der Risikoakzeptanzkurve (siehe Abbildung 3)
- Überwachung signifikanter Änderungen in der Bedrohungslage für Informationswerte
- Genehmigung wichtiger Initiativen zur Verbesserung der Informationssicherheit
- Überprüfung und Überwachung von bedeutsamen Sicherheitsvorfällen
- Ressourcenplanung
- Erfolgskontrolle und Benchmarking

Während das Information Security Management Forum des Konzerns im Wesentlichen für die Steuerung des ISMS selbst verantwortlich ist, fällt die konkrete Erfüllung von Aufgaben, wie zum Beispiel dem Erstellen von Sicherheitsrichtlinien, und die Koordination in den einzelnen Konzerngesellschaften dem Koordinationsforum zu:

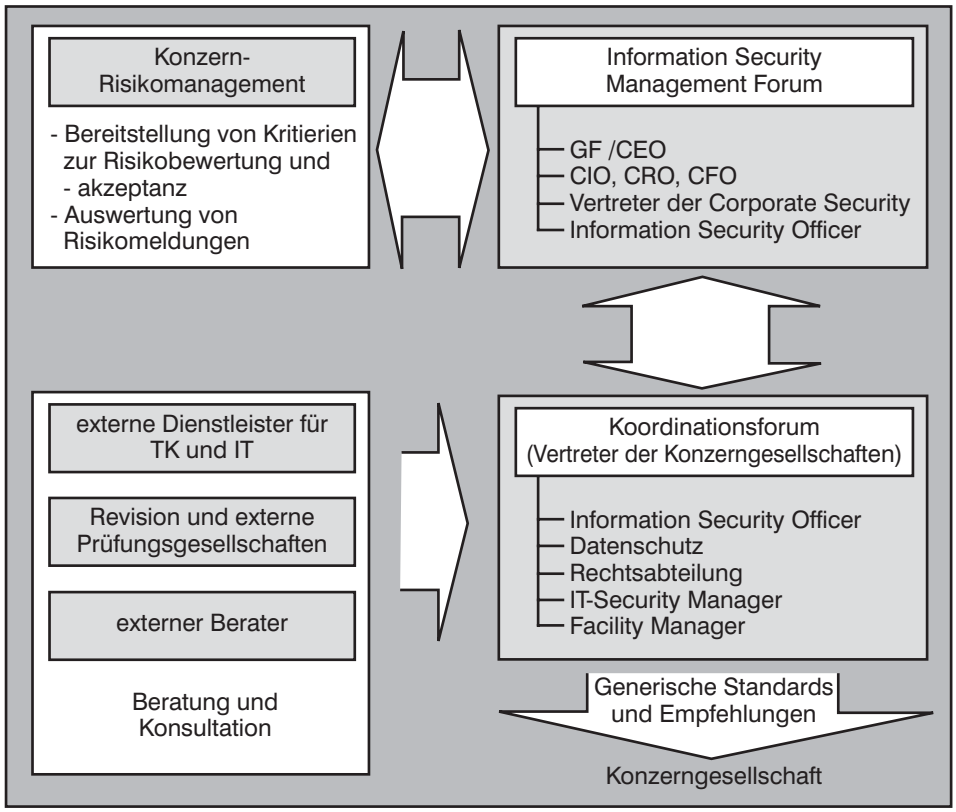


Abbildung 2: Aufbau und Positionierung der ISMS Foren

- Entwicklung der Sicherheitsorganisation (Rollen und Verantwortlichkeiten)
- Entwurf und Pflege von generischen Sicherheitsrichtlinien und Standards für die Konzerngesellschaften
- Herausgabe von Richtlinien für die Erarbeitung lokaler Sicherheitskonzepte
- Initiierung von Prüfungs- und Revisionsprozessen in den Konzerngesellschaften
- Entwurf von Security Awareness Programmen zur Schaffung einer Sicherheitskultur
- Analyse von Sicherheitsvorfällen

Das Koordinationsforum findet sein Pendant in den jeweiligen Konzerngesellschaften, z.B. als Information Security Team oder unter einer anderen Bezeichnung. Die Besetzung hängt hier sehr stark von deren Struktur und den lokalen Rahmenbedingungen ab. Hier kann eine Rolle spielen, ob die IT durch einen externen Dienstleister bereitgestellt wird oder nicht und ob zum Beispiel ein Datenschutzbeauftragter erforderlich ist.

Die Aufgaben können wie folgt umrissen werden:

- Konkretisierung der konzernweiten Richtlinien und Standards in lokale Sicherheitskonzepte
- technische und organisatorische Implementierung der Maßnahmen
- IT-Security Projekt-Controlling
- kontinuierliche Überprüfung der Wirksamkeit und eventuelle Anpassung der Maßnahmen
- Empfehlung von Verbesserungen an den generischen Standards
- regelmäßige Berichte über Sicherheitsvorfälle oder neue Risiken
- Durchführung von Schulungsmaßnahmen

Diese organisatorische Unterteilung hängt natürlich stark von der Größe der betrachteten Organisation ab, so dass die Aufgaben der verschiedenen Gremien auch zusammengefasst werden können.

Entwurf der Sicherheitskonzeption

Der Entwurf der generischen Sicherheitsrichtlinien und Standards im Koordinationsforum erfolgt mit Hilfe einer groben Risikoanalyse, die ausschließlich einer Top-Down Strategie folgt. Dabei werden in einem Managementworkshop zunächst die für die Geschäftsleitung elementaren

Bedrohungen für die Informationsverarbeitung identifiziert und qualitativ die damit verbundenen Risiken bestimmt.

Unter Bezugnahme auf die Sicherheitsziele erfolgt anschließend der Entwurf übergeordneter Richtlinien und Standards. Der British Standard sieht innerhalb des so genannten Risk Treatment Plan die Auswahl der geeigneten Controls zur Adressierung der identifizierten Risiken vor. Dabei ist man weder dazu verpflichtet alle 127 Controls umzusetzen, noch erhebt diese Auflistung einen Anspruch auf Vollständigkeit und kann durch eigene Kontrollmechanismen erweitert werden. Welche Controls letztendlich zur Anwendung gelangen, wird durch ein „Statement Of Applicability“ dokumentiert.

Für die Überführung der generischen Konzepte in die lokal in den Konzerngesellschaften geltende Fassung, muss das Information Security Management Forum auch einen Leitfaden für die Konkretisierung erarbeiten. Wichtiger Inhalt dieses Leitfadens ist unter anderem auch die Vorgabe einheitlicher Methoden für die Risikoanalyse, deren Granularität sowie der Risikoakzeptanzkurve (siehe Abb. 3).

Diese Kurve (oder auch tabellarische Matrix) gibt vor, welches Produkt aus Eintrittswahrscheinlichkeit und Schaden die Grenze zwischen tragbar und untragbar markiert.

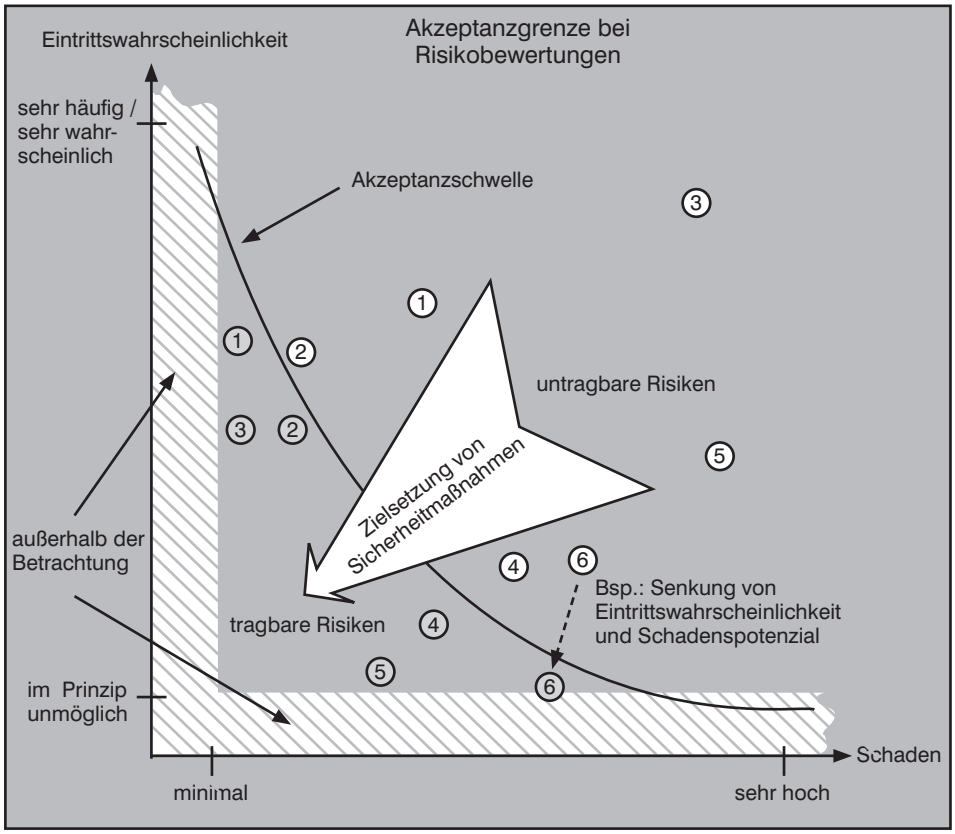


Abbildung 3: Abgrenzung zwischen tragbaren und untragbaren Risiken

Aufbau und Umsetzung in den Konzerngesellschaften

Wichtig ist, dass das Information Security Management die permanente Unterstützung des Topmanagements gegenüber den Konzerngesellschaften in Bezug auf die Umsetzung und Pflege des ISMS demonstriert. Gerade in der Einführungsphase muss verdeutlicht werden, dass die Reichweite der Information Security deutlich über die Grenzen der IT hinausgeht und dass bei der Gestaltung einer Sicherheitskultur alle Mitarbeiter ihre Rolle wahrnehmen müssen. Der Kickoff eines ISMS Projektes in den Konzerngesellschaften sollte daher auch das Interesse eines möglichst breiten Publikums erzeugen, damit sich alle Beteiligten auf die bevorstehenden Veränderungen einstellen können. Bei der Münchener Rückversicherung wurde hierfür zum Beispiel der provokante Projektname „@lcatraz“ gewählt. Natürlich erzeugt dieser Begriff Assoziationen, die mit dem Sinn eines ISMS nicht viel gemeinsam haben. Auf der anderen Seite wird dadurch aber in jedem Fall erreicht, dass man sich mit dem Thema Security auseinander setzt, egal ob mit einer negativen oder positiven Erwartungshaltung.

Je nach verfügbarer Personalkapazität muss bei ISMS-Projekten in den Konzerngesellschaften der Scope sehr genau abgegrenzt werden. Die hier aufwändigere Risikoanalyse, mit einem gemischten Top-Down und Botton-Up Ansatz, und auch die spätere Umsetzung der Maßnahmen können schnell die verfügbaren zeitlichen Ressourcen aufbrauchen. Zur Reduzierung des Projektumfanges sind folgende Merkmale als Abgrenzung sinnvoll zu verwenden:

- die Tiefe der Betrachtung (z.B. nur Anwendungen mit sehr hohem Schutzbedarf)
- prozessorientierte Einschränkungen (z.B. ausschließliche Betrachtung der Lagerhaltung)
- themenorientierte Einschränkungen (z.B. nur für das Identity Management)

Bei der Gestaltung der Teilprojekte muss natürlich darauf geachtet werden, dass sich nachfolgende ISMS-Projekte nahtlos anfügen lassen und dass die vom Konzern vorgegebenen Richtlinien und Standards ebenfalls entsprechend abzugrenzen sind. Gerade um dem letzten Aspekt gerecht zu werden, erscheint eine themenorientierte Einschränkung am sinnvollsten.

Erst hier, auf der Ebene dieser Teilprojekte, erfolgt die detaillierte Ausführung einer Risikoanalyse. Dazu wird zunächst die Erstellung des Inventars an Informationswerten und den dazugehörigen Applikationen und Systemen vorgenommen. Wichtig ist hierbei die Wahl einer geeigneten Gruppierung, um zusammenhängende Objekte möglichst einheitlich klassifizieren zu können. An dieser Stelle erfolgt auch die Zuordnung des jeweiligen Eigentümers für diese Objekte. Das Eigentümerkonzept ist fundamentaler Bestandteil eines ISMS, denn die Endverantwortung für die Zuweisung einer Klassifizierung und die Durchsetzung der damit verbundenen Sicherheitsmaßnahmen trägt der Eigentümer eines Objektes. Ist das Inventar erstellt kann die Zuordnung von Bedrohungen und der jeweiligen Eintrittswahrscheinlichkeit (möglichst anhand realer Schwachstellen) beginnen. Die sich hieraus ergebende Risikolandschaft ist die Grundlage für die Bildung von Prioritäten beim Entwurf von Sicherheitsmaßnahmen. Dieser Ablauf zeigt deutlich, dass der Scope für eine solche Art von Risikoanalyse nie zu groß gewählt werden darf, wenn das Projekt in überschaubarer Zeit abgeschlossen sein soll. Zusätzlich müssen auch die für die spätere Pflege notwendigen Ressourcen zur verfügbar sein.

Praktische Umsetzung eines ISMS

Natürlich sind in der Praxis bereits eigendynamisch technische und organisatorische Insellösungen in der IT-Security entstanden. Durch den Zukauf von Gesellschaften kann sich dann eine sehr farbenfrohe Landschaft an Sicherheitskonzepten innerhalb des Konzerns entwickeln. Diese lassen sich natürlich nicht einfach über den Haufen werfen. Vielmehr ist zu prüfen, wie eine sinnvolle Integration in das jetzt umzusetzende ISMS erfolgen kann und welche Ideen eventuell in die generischen Richtlinien und Standards auf Konzernebene einfließen können.

Die lokalen Sicherheitsanforderungen werden unter anderem durch die Berücksichtigung geltender Vorschriften, bestehender Vertragsbedingungen mit Dritten und den spezifischen Risiken der Konzerngesellschaft bestimmt (siehe Abbildung 4). Die konkrete Umsetzung der Konzernvorgaben in lokal geltende Konzepte und Prozesse gestaltet sich daher umso einfacher, je flexibler die generischen Vorgaben des Konzerns formuliert wurden.

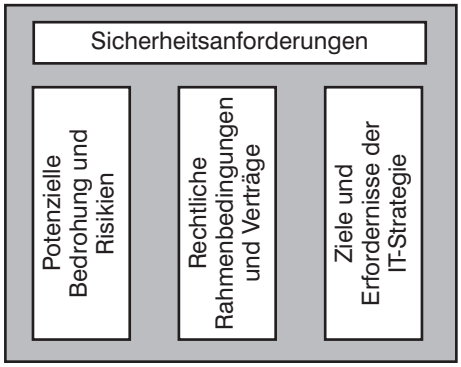


Abbildung 4: Ermittlung von Sicherheitsanforderungen

An dieser Stelle ist auch wieder der Einsatz des IT-Grundschutzhandbuchs mit seinen modular vorgegebenen Standard-Maßnahmen für Standard-Gefährdungen sinnvoll. Solange die Schutzbedarfsanalyse einen niedrigen bis mittleren Schutzbedarf für die entsprechenden Anwendungsgebiete ergibt, ist es ohne weiteres möglich, die Erstellung der lokalen Sicherheitskonzepte in der Konzerngesellschaft mit Bausteinen aus dem Grundschutzhandbuch zu vereinfachen. Erforderlich sind lediglich ein Konformitätsnachweis mit den Vorgaben des Konzerns und die Dokumentation der Anwendung des GSHB im „Statement of Applicability“ der regionalen Gesellschaft.

Dieses Beispiel zeigt, warum eine Trennung sinnvoll ist mit international und national, beziehungsweise konzernweit und regional gültigen Bestandteilen. Abgesehen davon vereinfacht diese Aufspaltung auch das Changemanagement der Dokumente, weil eine lokal geltende Richtlinie nicht bei jeder Änderung durch das Konzerngremium neu genehmigt werden muss. So kann auch später in jeder Konzerngesellschaft ein eigener Prozess, der auf die kontinuierliche Prüfung und Verbesserung der getroffenen Maßnahmen abzielt, regional etabliert werden. Die dadurch kürzeren Intervalle der Revision und die thematische Eingrenzung auf die jeweilige Gesellschaft erhöhen drastisch die Leistungsfähigkeit des ISMS.

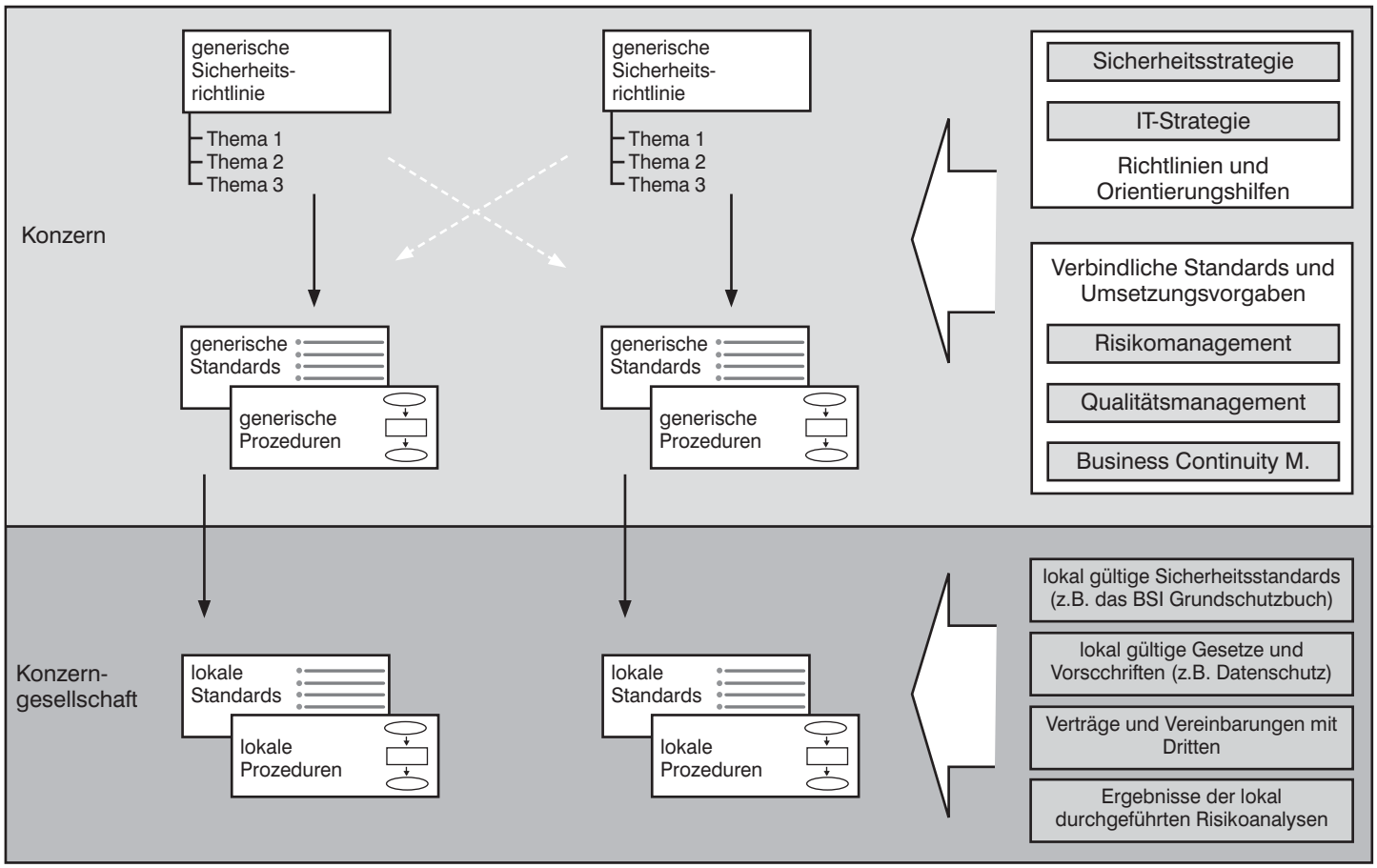


Abbildung 5: Zusammenhang zwischen konzernweit und regional gültigen Sicherheitsrichtlinien

1 Die Klassifikation muss dabei nicht unbedingt den herkömmlichen Anforderungen „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ folgen. Es ist jede Anforderung denkbar, anhand derer hinterher die Ausprägung einer Maßnahme abzuleiten ist. So sind zum Beispiel „Aufbewahrungspflicht“ oder „SOX-Relevanz“ ebenfalls mögliche Klassifizierungskriterien, für die sich hinterher Standardmaßnahmen ableiten lassen.

Abbildung 5 verdeutlicht sowohl die Entstehung der generischen Richtlinien und Standards auf der Konzernebene als auch deren Konkretisierung in den Gesellschaften.

Die übergeordneten Richtlinien auf der Ebene der Konzernspitze ergeben sich demnach aus der zuvor formulierten Sicherheitspolitik und der Sicherheitsstrategie sowie den Erfordernissen der konzernweiten IT-Strategie. Während diese Dokumente eine Art Leitlinie für die Sicherheitskonzeption bilden, fließen aus dem Risikomanagement, eventuell dem Qualitätsmanagement und dem Business Continuity Management klar definierte Vorgaben zur Umsetzung ein. Die lokale Interpretation der Vorgaben in der Konzerngesellschaft wird ihrerseits durch geltende Standards, Vorschriften, Verträge und natürlich Ergebnisse der Bestandsaufnahme und Risikoanalyse bestimmt.

Der Weg über die ISO 17799

Wie bereits erwähnt kann die Errichtung eines ISMS nach BS 7799 auf heftigen Widerstand stoßen, wenn es die Umordnung der gesamten Sicherheitsarchitektur erfordern würde. Letztendlich kommt man aber um einen Aufbau nach ISO 17799 / BS 7799-1 (referenziert im Anhang A des BS 7799-2) nicht herum. Wer sich also mit dem Gedanken trägt, ein ISMS nach BS 7799-2 aufzubauen, sollte eine schrittweise Umstellung seiner Sicherheitsarchitektur nach ISO 17799 in Erwägung ziehen. Hierzu werden in einer ersten Analyse die einzelnen Sicherheitskonzepte den Controls des Standards zugeordnet. Zumeist müssen dazu einige Konzepte auch inhaltlich aufgeteilt werden. Die Erfüllung bestimmter Controls wird nicht in Form von Sicherheitskonzepten sondern eher als allgemeine Unternehmensrichtlinien verwirklicht sein (z.B. „Klassifizierung von (Informations-)Werten“). Nachdem diese Zuordnung abgeschlossen ist, muss entschieden werden, wie man mit den entstehenden Lücken zum Standard verfahren möchte und welche zusätzlichen Controls zu benennen sind, um nicht zuordnungsfähige Sicherheitsmaßnahmen unterzubringen.

In Abhängigkeit vom Ergebnis dieser Analyse muss nun ein Konzept für die schrittweise Überführung der Sicherheitsarchitektur in eine ISO 17799 konforme Struktur erstellt werden. Dieses beinhaltet im Wesentlichen die Umbenennung von Dokumenten, die Zusammenführung von Inhalten aber meist auch die striktere Trennung zwischen Richtlinie und Umsetzung. Fingerspitzengefühl ist dabei für die Wahl des Zeitrahmens erforderlich. Gerade um Zeitdruck zu vermeiden ist die Durchführung eines solchen Umstellungsprojektes vor dem Beginn eines ISMS-Vorhabens sinnvoll. Dies gilt auch für die in der ISO 17799 definierten Managementgremien. Je frühzeitiger zumindest das Koordinationsforum seine Arbeit aufnimmt, desto eher kann mit der Erfüllung der periodisch wiederkehrenden Aufgaben im Sinne eines BS 7799 ISMS gerechnet werden.

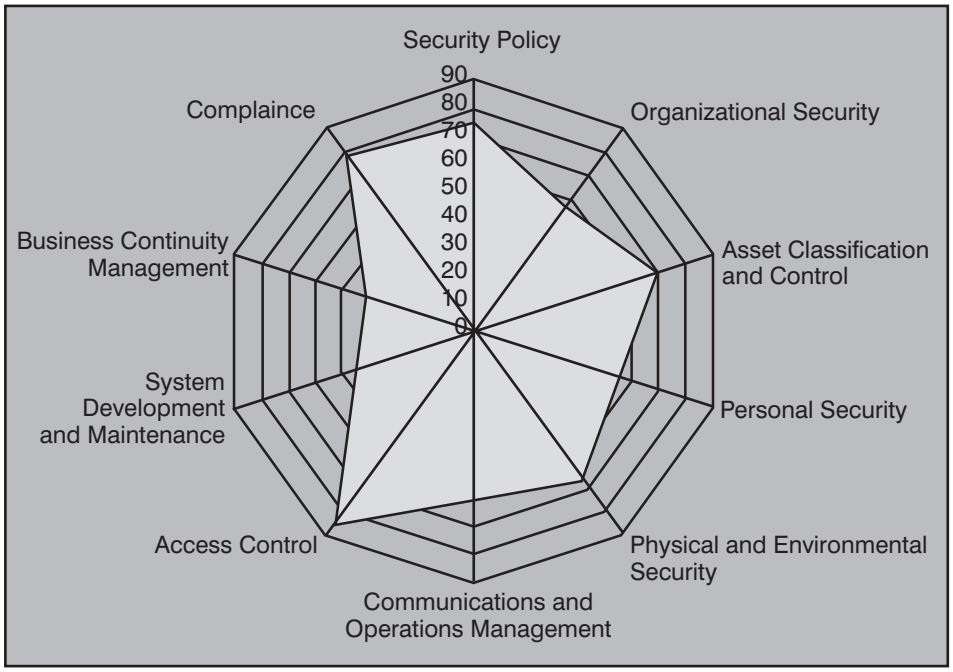


Abbildung 6: Bestimmung der Wirksamkeit von Sicherheitskonzepten durch Messung der Zielerreichung

Qualitätssicherung

Der British Standard 7799-2:2002 sieht explizit ein Management der Information Security vor und zielt damit auf deren kontinuierliche Verbesserung ab. In dieser und anderen Disziplinen ist der BS 7799:2002 gleich lautend und konsistent mit der ISO 9001:2000 und der ISO 14001:1996.

Um die geforderte Revision während der „Check“ Phase zu realisieren, sollte eine eigene Richtlinie das Intervall und den Umfang einer solchen Prüfung festlegen. Dabei wird die Wirksamkeit des Sicherheitskonzeptes anhand Zielerreichung in den 10 Themengebieten des BS 7799 gemessen (siehe Abbildung 6).

Idealerweise erfolgt die Durchführung auf der einen Seite durch die interne Revision der Gesellschaft und in größeren Abständen durch die Konzernrevision. Die Ergebnisse werden anschließend an das Information Security Management Team der jeweiligen Konzerngesellschaft bzw. der Konzernführung übermittelt. Die Wirksamkeit des ISMS an sich wird durch ein regelmäßiges (vorzugsweise jährliches) Management Review geprüft. Dieses führt das Information Security Management Team des Konzerns selbst durch. Prüfungen auf der Ebene des Konzerns dienen auch dem Benchmarking und damit einer Vergleichbarkeit der Sicherheitsstandards in den einzelnen Gesellschaften. Als methodischer Ansatz hierfür können Scoring-Verfahren wie die klassische Nutzwertanalyse gewählt werden.

Die Überwachung im laufenden Betrieb wird zum großen Teil durch technische Lösungen realisiert. Die Zusammenführung und Aufbereitung von Sicherheitsinformationen aus den IT-Systemen eines Unternehmens ist das Thema des Security Information Managements (SIM), welches nicht mit dem hier behandelten Information Security Management System verwechselt werden darf.

Alle diese Prozesse dienen der kontinuierlichen Überprüfung, ob die getroffenen Maßnahmen immer noch geeignet sind, die damit verfolgten Sicherheitsziele umzusetzen.

Sowohl die Ergebnisse aus der Check-Phase als auch die Meldungen über aktuelle Sicherheitsvorfälle (durch die Incident Response Teams) führen in der „Act“-Phase zur Anpassung der Sicherheitsarchitektur und zur Ergreifung von korrigierenden und vorbeugenden Maßnahmen. Die Maßnahmen in der „Act“-Phase können auch die wiederholte Durchführung einer Risikoanalyse für einen Teilbereich, das Redesign bestimmter Richtlinien oder Änderungen in der Sicherheitsorganisation zur Folge haben, womit wieder an die Planungsphase angeschlossen wird und der Kreis sich schließt.

Fazit

Mit dem British Standard 7799 (Teil 1 und 2) besitzt die Fachwelt eine international anerkannte und dennoch auf die regionalen Erfordernisse anpassungsfähige Umsetzungsrichtlinie für ein Information Security Management System. Weiterhin tragen seine Konsistenz mit bereits weitgehend in Unternehmen etablierten Managementsystemen wie z.B. der ISO 9001:2000 und die Möglichkeit einer Zertifizierung dazu bei, dass dieser Standard gerade für international aufgestellte Unternehmen sehr attraktiv ist. Dieser Artikel hat ebenfalls gezeigt, dass eine gleichzeitige Umsetzung von Teilen des Gundschutzhandbuches ebenfalls die Konformität mit dem BS 7799-2:2002 nicht gefährdet.

Literatur

BS 7799-2:2002, Information security management systems - Specification with guidance for use

ISO/IEC 17799:2000, Information technology – Code of practice for information security management

Völker, Jörg: BS 7799 – Von “Best Practice” zum Standard, in: DuD 2004, S. 102 ff.

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 2004

Holz, Karl-Heinz: Erfahrungen mit der Zertifizierung nach BS 7799, in DuD 2005, S. 10 ff.

Neuer Exklusiv-Report inklusive Seminar

Wireless LAN und Elektrosmog:
neue Erkenntnisse führen zu neuem Planungsansatz: Das TERW-Konzept

Neue europäische Studien belegen, dass es ein generelles gesundheitliches Risiko durch Einwirkung von Elektrosmog gibt. Die Ergebnisse dieser Studien gehen weit über die bisherigen Annahmen hinaus, so dass in den nächsten Monaten auch seitens der Betriebsräte und der Benutzer mit einer verstärkten Diskussion zu rechnen ist. Wir haben diese Studien analysiert und geben konkrete Empfehlungen für deren Handhabung.

Wireless LANs sind von dieser Diskussion stark betroffen, führen sie doch stufenweise zu einer flächendeckenden Belastung. Auch unter Berücksichtigung der Ergebnisse der neuen Studien ist ein Einsatz von WLANs generell möglich und sinnvoll. Allerdings sollten angemessene technische Grenzwerte berücksichtigt werden.

Angesichts der Dringlichkeit des Themas hat sich die ComConsult Research in Zusammenarbeit mit der ComConsult Akademie dazu entschlossen, Ihnen eine Sonderveranstaltung anzubieten. Diese ist mit dem Preis der Studie identisch, so dass Sie hier zum Preis der Studien quasi kostenfrei die Möglichkeit erhalten, sich vom Autor die Ergebnisse erläutern zu lassen und entsprechend zu diskutieren.

In einer topaktuellen Exklusivstudie haben wir für Sie untersucht:
- Welche Erkenntnisse lassen sich aus den neuen Studien ableiten
- Welche Grenzwerte sollten Sie in ihrer Planung von WLAN-Infrastrukturen berücksichtigen
- Was bedeutet das konkret für die Auslegung von Wireless-Funkzellen

Im Ergebnis kommt die Studie zu einem völlig neuen Planungsansatz für Wireless-Netzwerke, den wir als “Three Zone Electrosmog Reduced Wireless Networks, das TERW Zonen-Konzept” bezeichnet haben. Der Autor der Studie ist Dr. F.-J. Kauffels, der generell nicht im Verdacht steht, Gefahren durch Esmog über zu bewerten.

Interessant sind die Ergebnisse naturgemäß auch für den Bereich der Handy-Nutzung. Hier wird immer deutlicher, dass eine intensive Nutzung des Handys mit hohen gesundheitlichen Risiken verbunden ist. Unabhängig von der persönlichen Risiko-

Bewertung des Einzelnen stellen die Ergebnisse der neuen Studien Unternehmen vor ein immer größeres Problem. Gestatten sie ihren Mitarbeitern eine intensive Handy-Nutzung oder ist diese sogar untrennbar mit dem Job verbunden, besteht durchaus das Risiko einer zukünftigen Haftungssituation.

Auch hier setzt die neue Studie von ComConsult-Research mit dem neuen Planungsansatz an. Ein konsequenter Ersatz der GSM-Technik durch Voice-over-Wireless führt auch nach traditionellen Planungsansätzen zu einer massiven Senkung der Belastung. Wird dann auch noch der neue in der Studie ausgearbeitete TERW-Ansatz berücksichtigt, entsteht eine signifikante Reduktion der Belastung. Entsprechende Dual-Mode-Geräte, die sowohl GSM als auch VoWLAN unterstützen, kommen zur Zeit vermehrt auf den Markt. Sie haben allerdings den Nachteil, dass sie eine IP-Telefonie-Installation voraussetzen.

Inhaltsschwerpunkte sind:
Wireless World: Technologien und Potenziale
- Wireless World - Übersicht, Anwendungen
- WLANs: aktueller Stand
- IEEE 802.16 WiMAX
- IEEE 802.20

Neue Wireless-Technologien und Elektrosmog
- Wichtige aktuelle Studien und Empfehlungen
- Die NRBP-Empfehlungen, UK 2005
- EU-Aktivitäten
- Die REFLEX-Studie
- Zur Problematik von Grenzwerten

Planungsaspekte
- Einflussfaktoren
- Entwicklung der Campus-Netze
- Planungshilfen
- Ergebnisse der ComConsult Metastudie 2002
- RF-EMF-Belastung durch andere Kommunikationsdienste
- Weitere Verbesserungsmöglichkeiten durch neue WLAN-Konzepte
- Der Einfluss von WiMAX
- Zusammenfassende Planungsaspekte

Three Zone Electrosmog Reduced Wireless Networks: das TERW-Konzept
- Die TERW-Zonendefinition
- „Traditioneller“ Wireless Ansatz
- Drahtlose Voice Kommunikation heute
- TERW-Zonenplanung
- Infrastrukturfähige belastungsminimierte WLAN-Zellen
- Voice und WiMAX
- Kostenvergleich

Fazit

Motivation
Die neuen Kommunikationsmöglichkeiten durch WLANs und WiMAX sind wirtschaftlich und operationell ausgesprochen attraktiv und werden sich noch schneller als bisher ausbreiten. Weltweit rechnet man mit einem Wachstum von ca. 20% pro Jahr. Der eigentliche Durchbruch gegenüber bisherigen WLAN-Systemen geschieht durch die Möglichkeit der Bildung geschlossener Wireless Infrastrukturen im Rahmen einer Wireless Hierarchie. Die für ein individuelles Endgerät erzielbaren Datenraten liegen bei derartigen Lösungen weit höher als bei den bekannten Systemen, die auf GPRS oder UMTS basieren. Wegen der vergleichsweise geringen Reichweiten ist allerdings der Aufbau einer flächendeckenden Wireless Infrastruktur erforderlich. Diese wird innerhalb von Unternehmen und Organisationen die bisher kabelbasierten Lösungen mittelfristig verdrängen. Alle neuen Endgeräte werden in Weiterführung des mit der Centrino-Technologie entwickelten Grundgedankens standardmäßig mit Schaltkreisen ausgerüstet sein, die eine Einbindung in die Wireless-Infrastrukturen ermöglichen. Es

gibt eine Reihe von kommerziell ausgesprochen interessanten Kernanwendungen, die ausschließlich durch die neue Wireless Infrastruktur unterstützt werden können, wie z.B. die „funkenden Etiketten“ RFID, die die Logistik revolutionieren werden. Die allgemeingültigste Killer-Applikation ist „Voice over Wireless“ in Weiterführung der bisherigen VoIP-Entwicklungen. VoWLAN kann in Unternehmen und Organisationen GSM-Handys substituieren und insgesamt erhebliche Kostenvorteile mit sich bringen. Entsprechende Endgeräte werden schon Anfang 2005 vorgestellt.

Die Ausbreitung von Wireless-Infrastrukturen wirft die Frage nach der Belastung von Menschen durch die entstehenden elektromagnetischen radiofrequenten Felder (RF-EMF) auf.

Generell ist ein sensibler, vorsorgeorientierter Umgang mit diesen Fragestellungen nützlich und entspricht den Empfehlungen von WHO, EU-Kommission und anderen Institutionen. Es gibt nur wenige Aussagen zur Belastung durch WLAN-RF-EMF. Erschwerend bei der Erschließung der Thematik sind unterschiedliche Quantifizierungen in Radiotechnik und Dosimetrie. Neue Studien zeigen, dass die z.B. im Rahmen der CE-Zertifizierung vorgeschriebenen Grenzwerte für RF-EMF unter Umständen nicht ausreichend sind, um Wirkungen innerhalb menschlicher Körper mit Sicherheit völlig auszuschließen. Innerhalb der Studien ergeben sich jedoch auch Werte, bei denen keine Belastung mehr festzustellen ist. Dies ist jedoch kein endgültiges Kriterium, weil ein Negativbeweis aus theoretischen Gründen nicht möglich ist.

Die aktuelle WLAN-Technologiegeneration liegt hinsichtlich der RF-EMF Feldstärke und der durch sie entstehenden spezifischen Absorptionsrate im menschlichen Gewebe jedoch um Faktoren zwischen 1.000 und 100.000 unter den Grenzwerten, die entstehen, wenn man die neuen Studien berücksichtigt. Schon mit dieser Technologiegeneration ist eine Planung mit möglichst geringer persönlicher Belastung möglich und sinnvoll. Allerdings müssen die Kommunikationseinrichtungen von Hand einzeln kalibriert werden.
Neue Standards wie IEEE 802.11 h und n sowie IEEE 802.16 WiMAX ermöglichen eine hinsichtlich der RF-EMF-Belastung weiter optimierte und im Betrieb automatisch kalibrierende kabellose Infrastruktur.Die Optimierung der Belastung hinsichtlich minimal möglicher Werte setzt die Beachtung einiger wesentlicher, einfacher Grundregeln ganz früh im Designprozess voraus.Insgesamt sind mit den neuen Technologien Versorgungsstrukturen denkbar, deren Gesamtbelastung bei gleicher oder erweiterter Funktionalität weit unter der durch existierende kabellose Systeme wie GPRS, UMTS oder DECT liegt.
Das in der Studie eingeführte TERW-Designkonzept unterstützt die Planung funktional reichhaltiger und gleichzeitig besonders belastungsarmer drahtloser Infrastrukturen in einer frühen Stufe.
Eine Planung unter besonderer Berücksichtigung der Minimierung der persönlichen RF-EMF-Belastung führt zu einem System, welches, wenn überhaupt, nur marginale Mehrkosten gegenüber einem funktional äquivalenten Design, welches auf die Belastung keine Rücksicht nimmt, aufweist.
Eine Befolgung des TERW-Designkonzepts kann dazu beitragen, die durchschnittlichen jährlichen Kosten der drahtlosen Kommunikation eines Unternehmens oder einer Organisation auf etwa 20% der bisherigen Kosten zu drücken und gleichzeitig die RF-EMF-Belastung durchschnittlich um den Faktor 100 - 200 zu senken. Ein wesentliches Instrument in diesem Zusammenhang ist die Substitution von betriebsintern genutzten GSM-Handys durch VoWLAN-“Handys“ und die Einführung einer drahtlosen „Voice Ready“ Infrastruktur.

Da Elektrosmog völlig unabhängig von der - z.Zt. nicht mit Sicherheit endgültig abzuklärenden - Beantwortung der Frage, ob und ab welchen Grenzwerten er eine nachweisbar negative Auswirkung auf den menschlichen Organismus hat, für nichts weiter nutze ist, sollte man von Anfang an darauf hinwirken, ihn so weit wie möglich zu minimieren.

Autor und Referent
Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

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

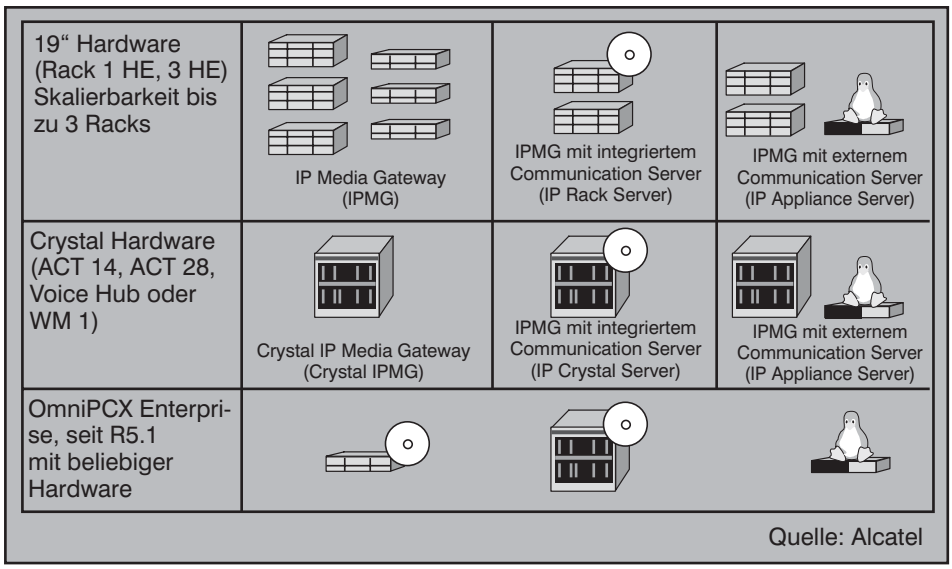


Abbildung 4.1: Hardware Plattformen der OmniPCX Enterprise

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.

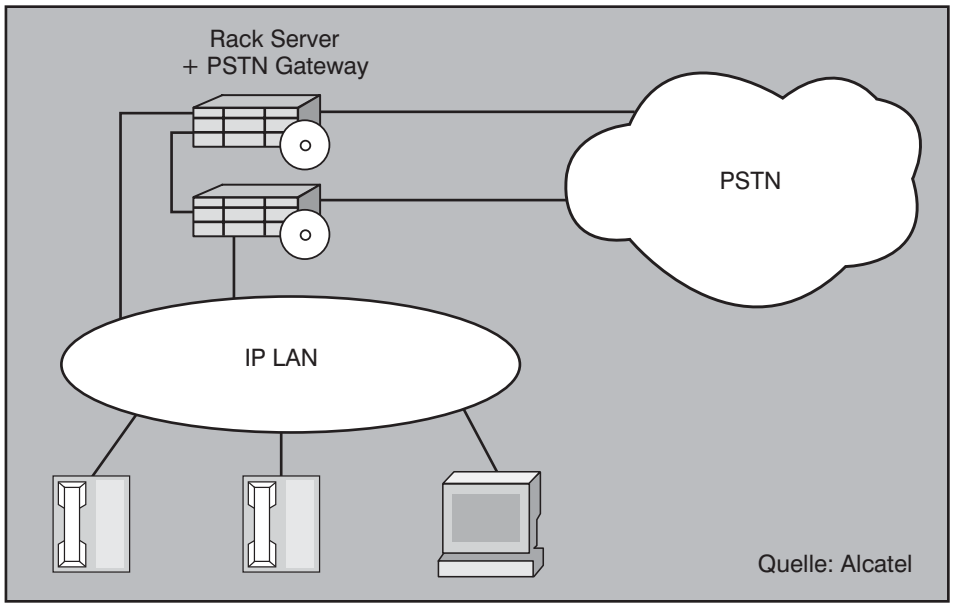


Abbildung 4.2: Einstandort-Lösung mit IP Rack Server

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-

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. In jedem Gateway muss mindestens ein

Abbildung 4.3: IPMG mit 1 Slot

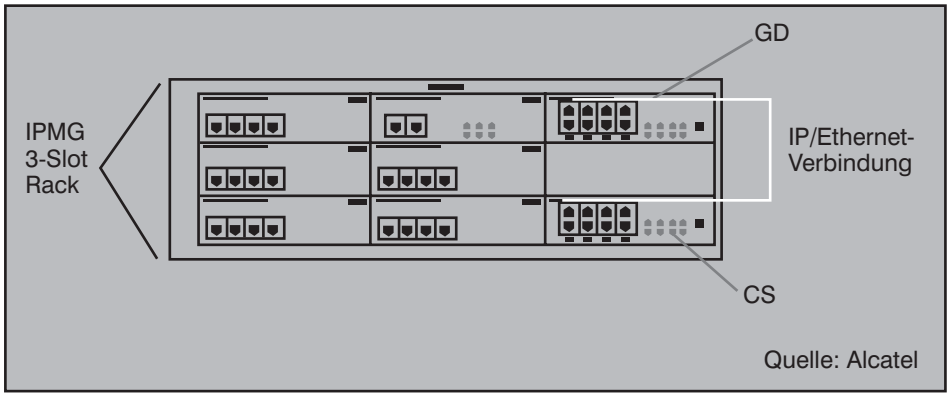


Abbildung 4.4: IPMG mit 3 Slots

GD oder CS-Steuermodul / CPU-Modul eingebaut werden, es können aber auch 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.

weiter lesen .... Download hier

Schwerpunktthema

“Lovely spam! Wonderful spam!“ - Was tut sich bei IETF?

Fortsetzung von Seite 1

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

Betriebs- und Volkswirtschaftler überschlagen sich aktuell darin Hochrechnungen aufzustellen, wie viel Zeit ein Mitarbeiter für das Aussortieren von Müllmails braucht und welcher finanzielle Schaden einer Firma dadurch entsteht. Da der Werbeschrott auch vor Geschäftsführungspostfächern nicht halt macht, haben Anbieter verschiedenster Dienste und Programme einen Markt erkannt: einige Email Clients werden mit SPAM-Filterfunktionen ausgeliefert, Plug-Ins werden für andere auf den Markt gebracht und (Vor-)Filterprogramme für Mailserver überschwemmen den Markt. Mailprovider werben mit SPAM-Schutz Funktionen, die mittlerweile sogar für die kostenlosen Email-Dienste fast obligatorisch geworden sind. Da aber auf der anderen Seite offensichtlich auch ein Markt existiert, wenden die Versender jener SPAM-mails alle möglichen Tricks an, um die Filterfunktionen zu unterlaufen. Mit anderen Worten: es herrscht Krieg, ein Krieg in dem aktuell die „Bösen“ zumeist vorne liegen.

Die Chancen stehen gut, dass auch bei einem John Chambers (Cisco), Bill Gates (Microsoft) und Terry Semel (Yahoo) jede Menge täglicher Werbemüll im Postfach landet und darum sind es dieses Mal eben nicht die „underdogs“, die startups und die Open-Sourceler alleine, die sich mit dem Thema beschäftigen und es angehen, sondern bei der Suche nach Lösungen haben eine Reihe von Alpha-Tieren die Bühne der Standardisierung betreten, die sich aktuell zu drei Gruppen formiert haben, mit unterschiedlichen Lösungsansätzen.

Im Folgenden werden die drei Lösungsansätze vorgestellt und auf ihre Vor- und Nachteile hin untersucht. Aktuell sind alle drei hier betrachteten Vorschläge im Draft-Stadium bei der IETF und noch existiert kein RFC. Trotzdem lohnt eine Betrachtung alleine schon deswegen, weil bereits Implementierungen existieren und zum Teil auch für den Markt bereits zur Verfügung gestellt werden.

Noch etwas anderes kommt hinzu, was die Situation für die Verteidiger der Postfächer nochmals verschärft hat: Phishing - der Versuch über scheinbar offizielle Mails ahnungslose Kunden auf bösartige Seiten zu locken, damit diese dort vertrauliche Daten eingeben: eBay und Banken werden besonders gerne als scheinbare Absender solcher Phishing Mails verwendet. Aktuell überprüfen Mailempfangsserver nicht, ob bei einer Mail, deren angeblicher Absender wirklich der ist, der er zu sein vorgibt. Die im weiteren vorgestellten Vorschläge zielen genau auf die Abwehr von Phishing-Mails und stellen keine generelle Lösung für SPAM dar.

Zwei Dinge vorweg bevor die drei Lösungen einzeln vorgestellt werden:

1. keine der drei Lösungen ist geeignet, das eigentliche Problem wirklich in den Griff zu bekommen, alle liefern nur eine weitere Entscheidungshilfe für spätere Programme zur Mailfilterung

2. alle basieren darauf, dass ein voll funktionstüchtiges und nicht korrumpiertes, weltweites DNS-System existiert.

Sender Policy Framework (SPF) / SenderID

Das Sender Policy Framework wurde im Sommer 2003 unter der Federführung von Meng Weng Wong ins Leben gerufen. Bereits im Dezember desselben Jahres gab es schon vereinzelte Installationen.

Mit Microsoft als Schwergewicht bei der Softwareentwicklung und mit Hotmail auch als Mail-Hoster und AOL als Online-Unternehmen mit mehreren Millionen Postfächern weltweit hat die SPF Technik zwei wesentliche Förderer gefunden. Da die Technik auch bei anderen Domänenanbietern rund um den Globus im Einsatz ist, können erste Erfahrungen in der Interoperabilität gesammelt werden. Laut Heise Meldung vom 02.03. diesen Jahres nutzen bereits eine dreiviertel Millionen Domains die SPF Technik. Laut eigenen Angaben setzt Microsofts Hotmail die SPF Prüfung bereits als ein Kriterium zur Kennzeichnung von SPAM; bei fast 25% der mittels SPF versandten Emails, die bei Hotmail eingegangen wären, hätte man ein Domain-Spoofing ausmachen können. Zwar sollen zunächst noch keine unauthorisierten Mails abgewiesen werden, aber authorisierte sollen bevorzugt behandelt werden und bei falschen Absendeadressen soll der „geschädigte“ Absender, der wahre Besitzer der Domäne, von dem Vorfall in Kenntnis gesetzt werden.

Sah es letztes Jahr noch so aus, als würde die Allianz zwischen AOL und Microsoft zerbrechen und die IETF dem Vorschlag wegen Patentfragen den Garaus machen, scheinen sich die Wogen geglättet zu haben. Jedoch hat die IETF aktuell vor der Standardisierung die Praxis gesetzt: die Herrn des Internets wollen zunächst Erfolge sehen. Aus diesem Grund existieren bislang nur Drafs keine RFCs, die zur Standardisierung vorgesehen sind. Wahrscheinlich sind auch die Erfolgsmeldungen von Microsoft vor diesem Hintergrund zu lesen; es ist fraglich, ob wirklich rund 20-25% gespoofte Mailadressen erkannt wurden, oder ob die entsprechenden Domain-Name-Server der angeblich gespooften Adressen nicht fehlerhafte Einträge enthielten.

“Lovely spam! Wonderful spam!“ - Was tut sich bei IETF?

Die Idee von SPF

Die Idee des SPF ist einfach und schnell skizziert, haarig wird es erst im Detail. Darum nur ein Überblick über das Verfahren, indem dann erst das klassische SPF und anschließend die Unterschiede von Version 2 zu Version 1 vorgestellt werden.

Wie in Abbildung 2 dargestellt wird zunächst eine Mail von einem Mail User Agenten (MUA = Mailclient-Software wie Outlook, Lotus Notes, Thunderbird etc.) an einen Mailserver weitergegeben. Ob und wie sichergestellt wird, dass der Mailclient die Berechtigung dazu hat, ist nicht Gegenstand des Verfahrens. Ebenso wenig wie die Kommunikation von Mailservern innerhalb eines Unternehmens, wenn mehr als einer existiert. SPF kommt erst im nächsten Schritt zur Anwendung, wenn ein Mailserver einer Domain mit dem einer anderen kommuniziert. In anderen Worten, wenn eine Mail von einem Provider/ Unternehmen an ein anderen/anderes zugestellt werden soll.

Schritt 1:

Der sendende Mail Transport Agent (MTA = Mailserver), im Fall dieser Zustellung ist er der Client, übermittelt während der Zustellung seine eigene Identität, d.h. seinen Domain-Namen, und, da SMTP auf Layer 3 über IP Übertragen wird, auch seine IP Adresse.

Schritt 2:

Der empfangende MTA (hier: der Server) fragt nun bei dem DNS Server der vorgeblichen Domain nach, ob und - wenn ja - wie eine Überprüfung des Senders erfolgen soll.

Schritt 3:

Der DNS Server liefert darauf die gewünschte Information, sofern die Domain am SPF teilnimmt, andernfalls schweigt er zu diesem Thema. Wichtig ist, dass der DNS Server kein „Ja“ oder „Nein“ zurückgibt, sondern eine Anweisung, wie die Authentizität zu überprüfen ist.

Ein solches Statement kann beispielsweise lauten: alle im DNS eingetragenen Mailserver (MX = Mail eXchanger) dürfen mails senden, sonst aber niemand.

Schritt 4:

Der Empfänger wertet die Antwort aus und besorgt sich, wenn nötig, weitere Informationen. Als Ergebnis liefert der Test einen Status zurück, also z.B. ob ein Test erfolgt ist, wenn ja: ob er positiv oder negativ verlaufen ist.

Im gerade gegebenen Beispiel fragt er den DNS Server erneut, diesmal nach den MX Servern und vergleicht deren IP Adressen mit der IP Adresse des Senders der Mail.

Das Ergebnis der Auswertung kann von weiteren Anti-Spammechanismen benutzt werden. SPF selbst definiert keine Reaktion auf die möglichen Ergebnisse der Prüfung.

Der wesentliche Unterschied zwischen der Version 1 und Version 2 liegt in der Frage, welche Domain für die Prüfung eigentlich genommen werden kann, denn bei der Übermittlung von Mails können viele Adressen und Domains an unterschiedlichen Stellen übermittelt werden, die durchaus voneinander abweichen können.

SPF Classic

Der neueste IETF Draft zum SPF ist vom Dezember 2004, ein RFC existiert zur Stunde noch nicht. Aktuell ist die classic Version die am weitesten verbreitete Variante.

Ablauf des SPF-Verfahrens

Der Versand von Emails wird durch das Verfahren nicht geändert. Es werden also keine neuen Zeilen in den Mailheader eingefügt, Änderungen an der Mail vorgenommen oder neue SMTP Befehle eingeführt. Die Überprüfung beginnt erst mit dem Empfang der Email und durchläuft folgende Schritte:

Schritt 1:
Ermitteln der Identität des Senders

Zur Überprüfung wird eine von zwei Identitäten herangezogen, die bei der

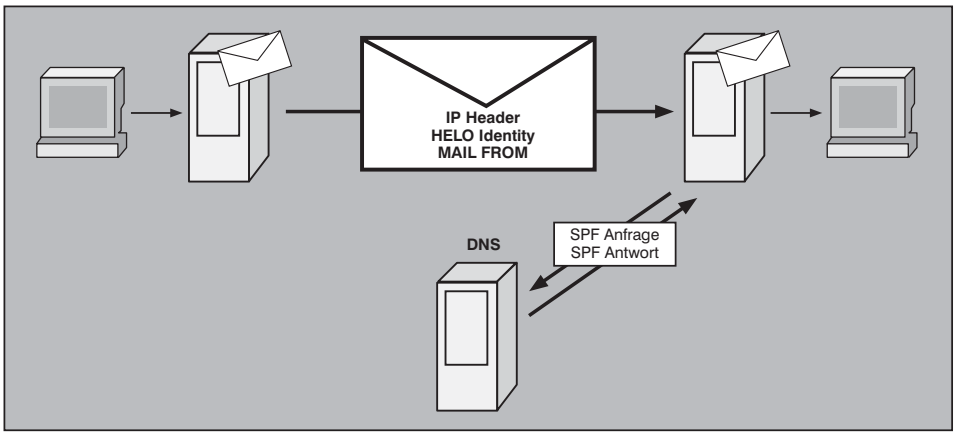


Abbildung 2: SPF Arbeitsweise

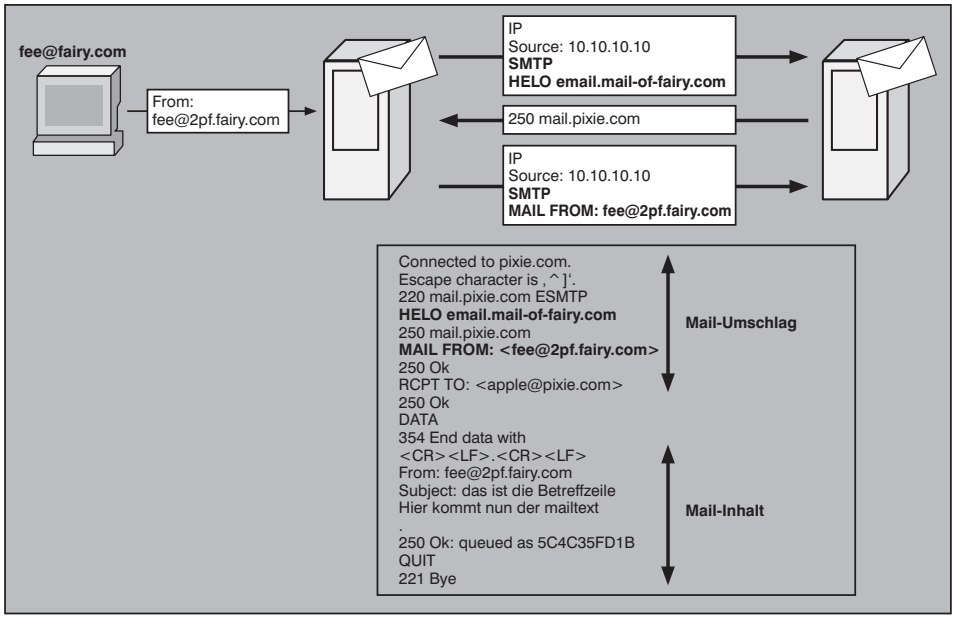


Abbildung 3: SMTP Klartext

Email-Übermittlung benutzt werden, bzw. benutzt werden können (siehe Abbildung 3).

- **HELO Identität**
  Während des Verbindungsaufbaus zwischen zwei Mailservern stellt sich der Sender noch vor der Übertragung der eigentlichen Email dem Empfänger mittels des HELO Kommandos vor. Moderne Mailserver können stattdessen auch das erweitertete SMTP EHLO Kommando benutzen.

  Korrekt konfigurierte Mailserver nutzen dafür ihren Full Qualified Domain Name (FQDN), also ihren eigenen DNS Namen. Grundsätzlich sind auch IP Adressen erlaubt, wenn kein FQDN existiert.

- **MAIL FROM Identität**
  Auch der MAIL FROM Befehl ist ein SMTP Befehl, der vor der eigentlichen Übertragung der Mail vom Sender an den Empfänger übermittelt wird. Häufig wird dieser Parameter auch der „reverse-path“ genannt, also der Pfad für eine Antwort. Dieser Parameter gibt nicht zwingend den ursprünglichen Sender der Mail wieder, auch wenn das häufig der Fall sein wird, sondern den Empfänger von Fehlermitteilungen und kann somit vom „From“ Parameter in der Mail abweichen.

Der Empfänger kann die HELO Identität testen. Ein „Fail“ bei der Überprüfung ist bindend und somit das Endergebnis. Je nach Konfiguration kann er jetzt bereits eine Fehlermeldung an den Sender zurückgeben und die Verbindung beenden. Kommt er nicht zu einem „Fail“, sondern irgendeinem anderen Ergebnis, so muss er die MAIL FROM Identität ebenfalls überprüfen.

Ein Vorteil der HELO und MAIL FROM Tests ist, dass sie sehr früh bei der Übermittlung der Mail erfolgen. Dadurch können Fehler noch während der Übermittlung an den Sender berichtet werden.

Grundsätzlich ist es auch möglich, ein sehr strenges Regelwerk zugrunde zu legen, was den Umgang mit SPAM angeht, so könnte man bereits nach der HELO / MAIL FROM Übermittlung die Kommunikation beenden und damit den Transfer unnötiger Daten in Form der eigentlichen Mail unterbinden. Von so einem strikten Vorgehen wird jedoch an dieser Stelle explizit abgeraten, solange das SPF Verfahren nicht allgemein verbreitet, wohldefiniert und wohlverstanden ist, würden sehr viele Mails fälschlicherweise abgelehnt werden.

Schritt 2:
Abfrage des SPF-Records im DNS
Der Standard definiert nicht, wie die IP Adresse des Senders gegen die Domain zu prüfen ist, das entscheidet vielmehr die sendende Domain selbst. Dazu wird vom Empfänger eine DNS Anfrage an den DNS Server der Domain gestellt. Die Antwort definiert die Art der Prüfung. Entsprechende Einträge müssen vom Sender im DNS für seine Domain vorgenommen werden. Grundsätzlich ist dafür ein neuer Resource Record (RR) vorgesehen, der „SPF“ Record. Damit möglichst schnell jedoch ein Betrieb des Frameworks gewährleistet werden kann, wird auch eine Variante spezifiziert, die auf den bereits im DNS vorhandenen TXT Record zurückgreift, so dass man nicht abwarten muss, bis die DNS Gruppe bei der IETF den neuen Typ spezifiziert hat und alle DNS Serverhersteller/-entwickler den neuen Typ auch implementiert haben. Sie sehen je ein Beispiel beider Varianten in Abbildung 4.

Zwar ist es kein Zwang, jedoch ratsam, wenn möglich beide Typen im DNS einzutragen. Versteht der Empfänger beide RRs, so wird er sich für den SPF Eintrag entscheiden. Auf alle Fälle ist es jedoch zwingend, dass beide Einträge völlig identisch sind. Bei den TXT Einträgen muss man bedenken, das grundsätzlich auch andere TXT Records existieren können. Daraus kann resultieren, dass die Datenmenge von TXT Antwortpaketen zu groß wird, als dass sie noch mittels UDP übertragen werden kann. Eine allgemeingültige Lösung für das Problem gibt es nicht, darum wird empfohlen, dass der Administrator die Einträge entsprechend kurz gestaltet.

Für jede Domain kann nur ein Eintrag eines jeden der beiden Typen generiert werden. Gibt es mehr, so führt das zu einem permanenten Fehler (PermError). Anders als Server Records (SRV) gelten SPF Records für die gesamte Domain und nicht für Subdomains; von dem Gebrauch von Wildcards bei den Domains (bspw: *.fairy.com) wird dringend abgeraten, auch wenn sie nicht verboten sind.

Liefert die erste Anfrage kein Ergebnis, so wird die Domain von links bis zum ersten Domainbegrenzer gekürzt. Meldet sich der Sender beispielsweise mit „mail.fairy.com“ und für diese Domain wird kein SPF Eintrag gefunden, so wird eine weitere Anfrage für „fairy.com“ ausgeführt. Dieses Vorgehen wird so lange wiederholt, bis entweder ein Eintrag gefunden wird oder keine Domain mehr über bleibt. In letzterem Fall geht der Empfänger dann davon aus, dass keine SPF Einträge vorhanden sind. Aktuell ist das also der Normalfall.

Ein SPF Eintrag wird von links nach rechts abgearbeitet bis ein Match gefunden wird; der erste Match zählt. Ausnahme sind „redirects“, die stets am Schluss erst bearbeitet werden. Wird kein passender Eintrag gefunden, liefert die Prüfung ein „neutral“ als Ergebnis zurück. Um das zu verhindern, sollten alle SPF Einträge entweder ein „redirect“ enthalten oder mit „-all“ enden (Erklärung der Einträge folgt).

Es werden zwei Varianten von Eintragstypen definiert: „Mechanisms“ und „Modifiers“.

Mechanismen sind die Entscheidungskriterien. Ihnen vorangestellt wird die Information, was bei Zutreffen des Kriteriums das Ergebnis der Prüfung ist. Definiert sind vier Möglichkeiten:

„+“	Pass
„-„	Fail
„~“	SoftFail
„?“	Neutral

Mögliche Mechanismen sind:

A
Der Host-Record des DNS. Löst einen Namen in eine IP Adresse auf. Liefert eine DNS Anfrage auf einen A Record mehrere IP Adressen, so werden alle geprüft.

MX
Der Empfänger prüft, ob der Mailserver, der ihm eine Email zustellt, für die entsprechende Domain als MX Server (Mails eXchanger) im DNS eingetragen ist.

PTR
Geprüft wird, ob zur IP Adresse des Senders ein reverse Lookup existiert und zur gegebenen Domain gehört. Dabei wird erst der Name rückwärts aufgelöst und dann vorwärts überprüft… warum einfach, wenn’s doch auch so schön kompliziert geht.
Da die PTR Methode für eine einzelne Überprüfung selbst im günstigsten Fall viele DNS-Anfragen generiert, sollte man direkt von ihr Abstand nehmen.

```
fairy.com.    IN    SPF    v=spf1 +mx  a:mail.fairy.de -all
fairy.com.    IN    TXT    v=spf1 +mx  a:mail.fairy.de -all
```

Abbildung 4: Beispiele für SPF Einträge im DNS

IP4 / IP6
Mit dem IP4 / IP6 Befehl können direkt IPv4 / IPv6 Adressen oder Netze spezifiziert werden.

all
Dieser Parameter trifft immer zu. Deshalb kann er sinnvoller Weise auch nur am Ende stehen, typischerweise wird er dort alles verneinen.
Beispiel `v=spf1 +mx -all`

exists
Der wohl komplexeste Mechanismus ist der exists Befehl, der nur in Zusammenhang mit einem komplexen Macroausdruck Sinn macht.

Über einen solchen Makrobefehl könnte bis auf Userebene eine Überprüfung der MAIL FROM Adresse realisiert werden.

include
Am einfachsten verständlich wird die Funktion des includes durch ein Beispiel: im MAIL FROM wird fee@fairy.com als Return-Path genannt. Defacto findet der Versand jedoch über den Mailserver der Domain „pixie.com“ statt. Dann kann eine SPF Anweisung für „fairy.com“ folgendermaßen aussehen. (siehe Abbildung 5)

Der Empfänger besorgt sich die SPF Daten der Domain „pixie.com“ und prüft, ob der Sender berechtigt ist, für diese Domains („pixie.com“) zuzustellen. Liefert die Prüfung ein „pass“ als Ergebnis, so ist auch das Ergebnis für die Domain „fairy.com“ ebenfalls „pass“, andernfalls wird weitergeprüft. Im Beispiel wäre das Ergebnis „fail“ wegen des „-all“ als letzte Anweisung. Es spricht jedoch nichts dagegen mehrere includes zu kombinieren, da nur geprüft wird, ob das Ergebnis „pass“ ist, alle anderen Ergebnisse der „Unterprüfung“ führen dazu, dass die originäre Prüfung weiter abläuft.

Zusammengefasst: eine Include Anweisung veranlasst den Empfänger dazu, den Sender der Mail bei einer anderen Domain auf Gültigkeit hin zu prüfen - nicht auf Ungültigkeit.

Sinn ist, die Verantwortung von einer Domain auf eine andere zu übertragen. Typische Anwendung hierbei wären WEB-Hoster. WEB-Hoster verwalten viele Domains für ihre Kunden jedoch häufig nur einige Mailserver, die zumeist zur Domain des WEB-Hosters selbst gehören. Damit bei einer Änderung der Mailserver nicht alle Kunden-

```
fairy.com.    IN    TXT    v=spf1 include:pixie.com -all
```

Abbildung 5: Beispiel mit include-Anweisung

DNS Einträge umgestellt werden müssen, wird bei den Kunden nur auf die Domain des Hosters verwiesen.

Neben den Mechanismen werden noch zwei Modifier spezifiziert:

redirect
Die Redirect Anweisung verweist auf eine andere Domain, die zur Prüfung herangezogen werden soll. Anders als der Include Befehlt, definiert der Redirect einen Ausstieg aus der aktuellen Prüfung und somit eine komplette Übergabe. Aus diesem Grund wird der Redirect Befehl auch immer als letztes ausgeführt, egal wo er in der SPF Anweisung auftaucht. Diesmal zählen nicht nur die positiven Ergebnisse sondern alle.

exp (Explanation)
Liefert die Prüfung ein „fail“ als Ergebnis, so wird, wenn angegeben, der Text hinter dem „exp“ Modifier an den Sender zurückgeliefert.

Schritt 3:
Der SPF-Test
Der Test liefert folgende Ergebnisse

None
Die entsprechende Domain nimmt am SPF nicht teil.

Neutral
Die DNS Antwort enthält den ausdrücklichen Hinweis, dass kein Statement bzgl. der Autorisation einer IP Adresse gegeben wird.

Pass
Der Test gilt als bestanden.

Fail
Das Ergebnis des Tests ist eindeutig negativ.

SoftFail
Die Domain des angeblichen Absenders übernimmt keine „Verantwortung” für den Absender, ist jedoch auch nicht gewillt ein eindeutiges Nein zu signalisieren.

TempError
Dieser Status wird zurück geliefert, wenn es sich um einen temporären Fehler handelt.

PermError
Ein PermError meint einen nicht zu behebenden Fehler.

Schritt 4:
Reaktion auf das Ergebnis
Aus den sieben verschiedenen Rückmeldungen ist ersichtlich, dass der Test selbst keine Aktion definiert, sondern nur eine Prüfung des Absenders vornimmt. Das Ergebnis kann für weitere Verarbeitungsroutinen genutzt werden. Unabhängig vom SPF-Test können weitere Mechanismen zu einer anderen Entscheidung gelangen, als die, die durch das Testergebnis impliziert ist. So kann beispielsweise eine Blacklist Mails verwerfen, obwohl sie den Status „Pass“ haben oder umgekehrt eine Whitelist Mails mit permanentem Fehler (PermError) akzeptieren. Das Ergebnis ist somit nur ein weiteres Entscheidungskriterium.

Einsatzszenarien

Jedes Verfahren muss sich einer Tauglichkeitsprüfung für Alltagssituationen unterziehen, wenn es zur Frage kommt, ob es eine Zukunft hat, oder eine von zahllosen Totgeburten ist, die in der Theorie gut klingen, aber in der Realität nicht funktionieren. Zu diesem Zweck eine Betrachtung von typischen Varianten der Email-Nutzung, ohne den Anspruch auf Vollständigkeit zu haben:

Standard Emailversand
Beim Standardversand von Emails erzeugt ein Mailclient eine Email, die er an seinen Mailserver weiterleitet, der zur selben Domain gehört. Der Mailserver übermittelt die Email an den Empfänger, der prüft, ob der Mailserver berechtigt ist, für die Domain Mails zuzustellen. Also, alles so wie bislang beschrieben. Ist der SPF Record korrekt angelegt, stellt diese Situation kein Problem dar. (siehe Abbildung 6)

Client und sendender MTA in unterschiedlichen Domains
Der Client und der sendende MTA gehören zu unterschiedlichen Domains. Beispielsweise bei einem Relaying durch einen Mailprovider: der User benutzt als Mailadresse „fee@fairy.com“, verfügt jedoch nicht über einen eigenen Mailserver, sondern nutzt den seines Providers „pixie.com“. Auch diese Situation führt beim klassischen SPF Verfahren nicht zwingend zu einer Konfliktsituation: wird die HELO Identität des sendenden Mailservers geprüft, ist die Domain ohnehin „pixie.com“, nicht „fairy.com“. Hat der Provider seinen eigenen Mailserver im SPF eingetragen, wird der SPF Test bestanden. Wird jedoch der MAIL FROM Eintrag geprüft, kann dort „fairy.com“ als Domain stehen. Der SPF Eintrag der Domain „fairy.com“ muss also den Mailserver seines Providers autorisieren. Dies kann zum Beispiel durch die Include Anweisung geschehen. (siehe Abbildung 7)

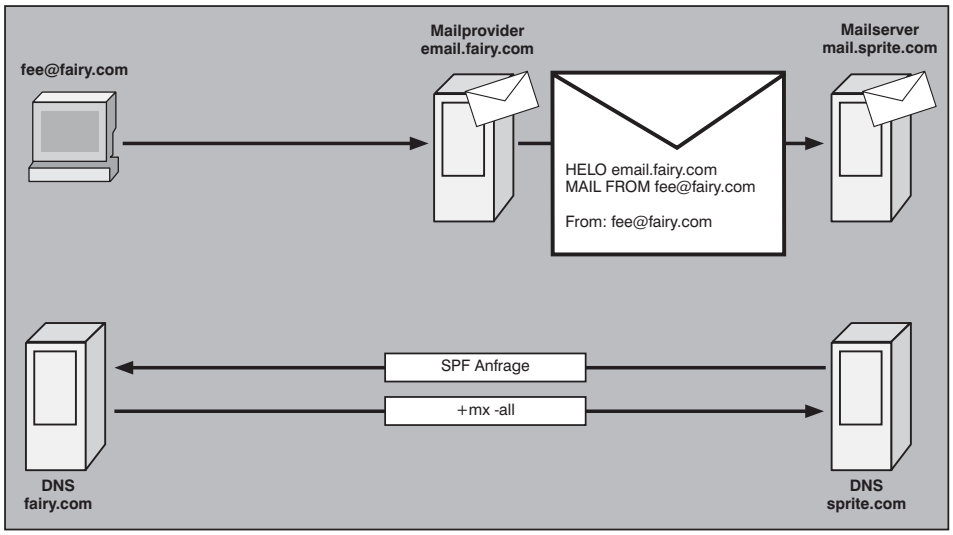


Abbildung 6: SPF bei Standardversand

Mailing-Listen
In diesem Fall wird eine Mail durch eine Mailing-Liste an viele Empfänger verteilt. Die RFCs 2821 und 1123 sehen vor, dass der Reverse-Path, also die für den klassischen SPF entscheidenden Einträge, auf die Domain der Mailingliste verweisen müssen: auf den Mailserver, der zur Mailingliste gehören. Somit stellt auch dieser Fall kein Problem dar.

In Abbildung 8 wird eine Email von fee@fairy.com an die Mailingliste liste@pixie.com geschickt. Der Mailserver der Mailingliste kann (muss aber nicht) nun eine SPF Prüfung durchführen, bevor er die Mail an die Mailingliste weiterleitet. Die Software der Mailingliste muss die Mail so bei ihrem Mailserver einliefern, dass als Return-Path (MAIL FROM beim klassischen SPF) eine Adresse aus der eigenen Domain angegeben wird. Faktisch ist der Sender, fee@fairy.com, ja auch gar nicht daran interessiert, zu erfahren, welche Mitglieder der Liste gerade im Urlaub sind bzw. welche Postfächer schon längst nicht mehr existieren. Auch in der Mail sollten entsprechende Einträge vorge-

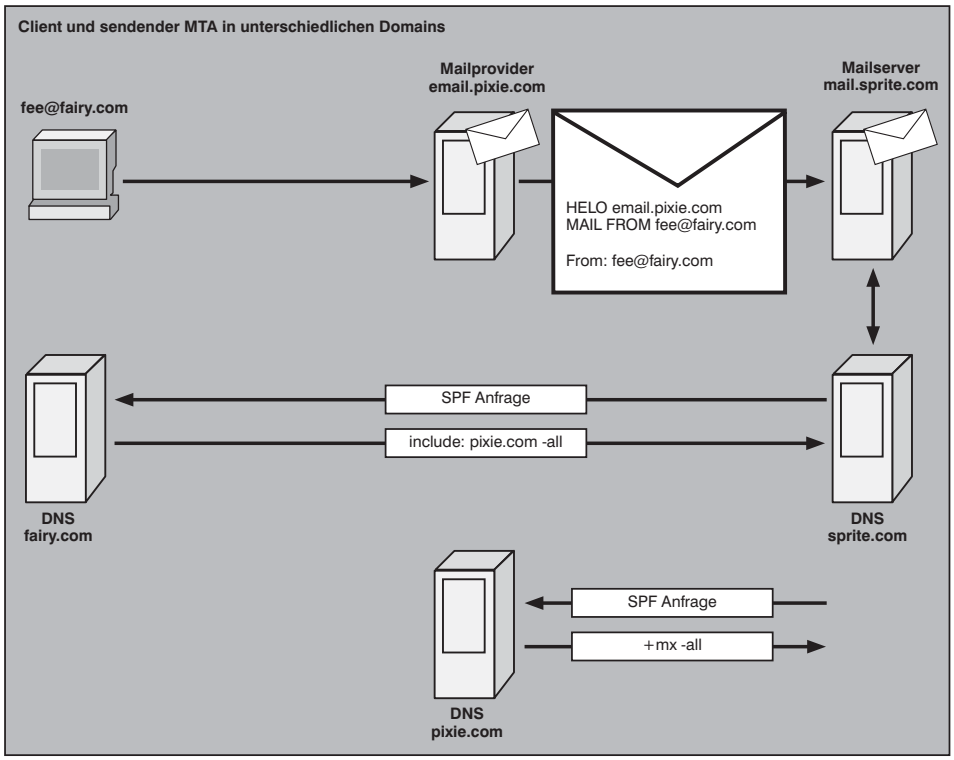


Abbildung 7: SPF für Domain-Hoster

nommen werden, wie im Beispiel das Resent-From.

Mail Service

Es gibt Anbieter, die Bulk-Mails für andere Firmen versenden, damit diese die entsprechende Infrastruktur nicht aufbauen müssen. Trotzdem sollen die Antworten auf solche Mails an den Auftraggeber zurückgehen, nicht an den Service-Provider. Die MAIL FROM Domain wird also von der des sendenden Mailservers abweichen. Eine Lösung, ist den Mailserver des Service-Providers in den eigenen SPF Eintrag zu integrieren. Damit gäbe man aber dem Anbieter die Möglichkeit beliebige Mail im eigenen Namen zu versenden, was ein großes Vertrauen voraussetzt. Somit kaum die gewünschte Lösung. Besser wäre, wenn der Return-Path, also die MAIL FROM auf eine Email-Adresse des Anbieters verweist und die FROM Adresse in der Mail auf eine Adresse des Auftraggebers. Die SPF Prüfung würde in diesem Fall gegen die Domain des Anbieters erfolgen. Resultat wäre, dass Bounces (Mails, die vom Empfänger nicht angenommen werden), an den Anbieter zurückgehen, jegliche Antworten jedoch an den Auftraggeber, da Client Programme die FROM oder RETURN-TO Einträge der Mail auswerten, nicht das MAIL FROM des Umschlags, den sie nie zu sehen bekommen. (siehe Abbildung 9 und 10)

Email Forwarding

Beim Forwarding wird eine Mail, die an Empfänger A geht, automatisch weitergeleitet an eine andere Empfangsadresse B, die sich in einer anderen Domain auf einem anderen Mailserver befindet. Gemeint ist hier ein echtes Forwarding, auf UNIX Systemen gerne durch die .forward Datei erreicht, nicht ein Alias für ein Postfach auf demselben Server. Beispiel: eine Email von fee@fairy.com an apple@pixie.com wird an den MTA von pixie.com zugestellt. Apple hat eine Weiterleitung definiert, die die Mail weiterleitet an ihr neues Postfach bei ihrem neuen Provider apple@sprite.com. Das Problem, das hierbei entsteht ist, dass der Return-Path weiterhin fee@fairy.com bleiben soll, denn schließlich möchte Fee darüber informiert werden, wenn die Mail nicht zugestellt werden kann. Folglich ist die HELO Identität bei der Zustellung an sprite.com zwar die Domain pixie.com jedoch die MAIL FROM Identität bleibt fee@fairy.com. Da die MAIL FROM gegenüber der HELO Identität Priorität beim SPF Test hat, schlägt die Überprüfung fehl, denn der Domain-Betreiber von fairy.com hat wohl kaum ein Interesse daran, die Mailserver der Domain pixie.com in seinen SPF Eintrag aufzunehmen und somit zu autorisieren.

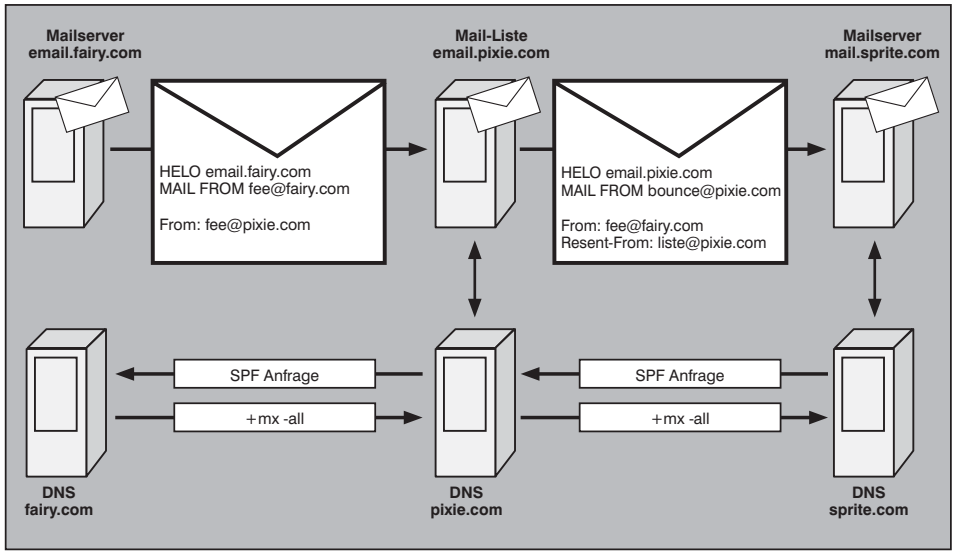


Abbildung 8: SPF bei Mailing-Listen

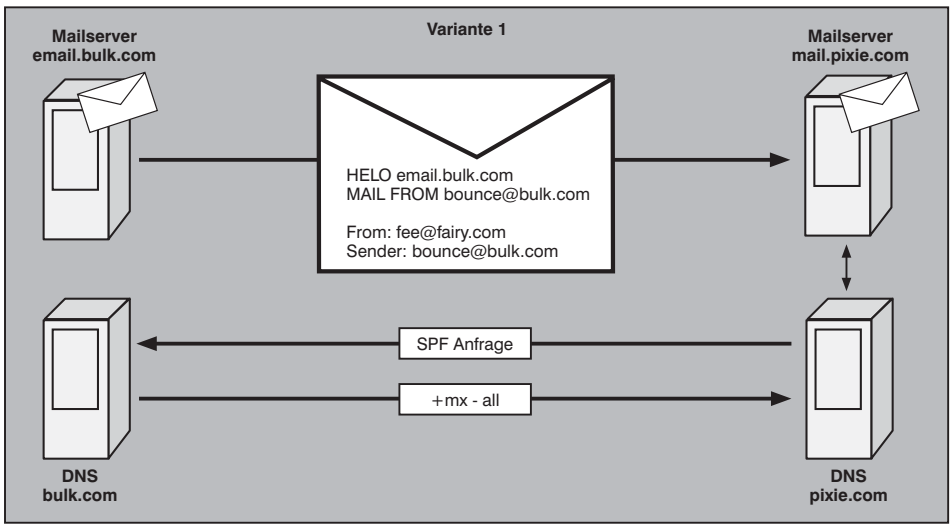


Abbildung 9: SPF bei Bulk-Mail-Providern (Variante 1)

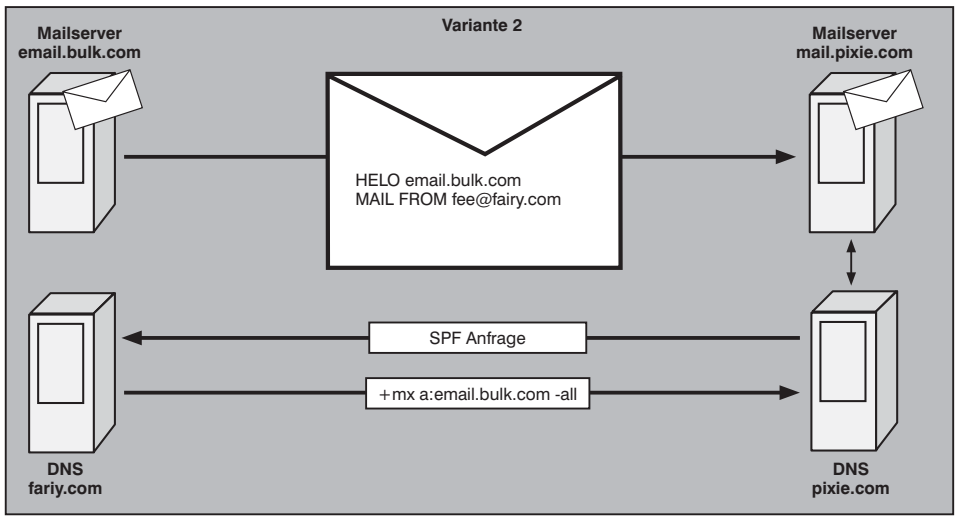


Abbildung 10: SPF bei Bulk-Mail-Providern (Variante 2)

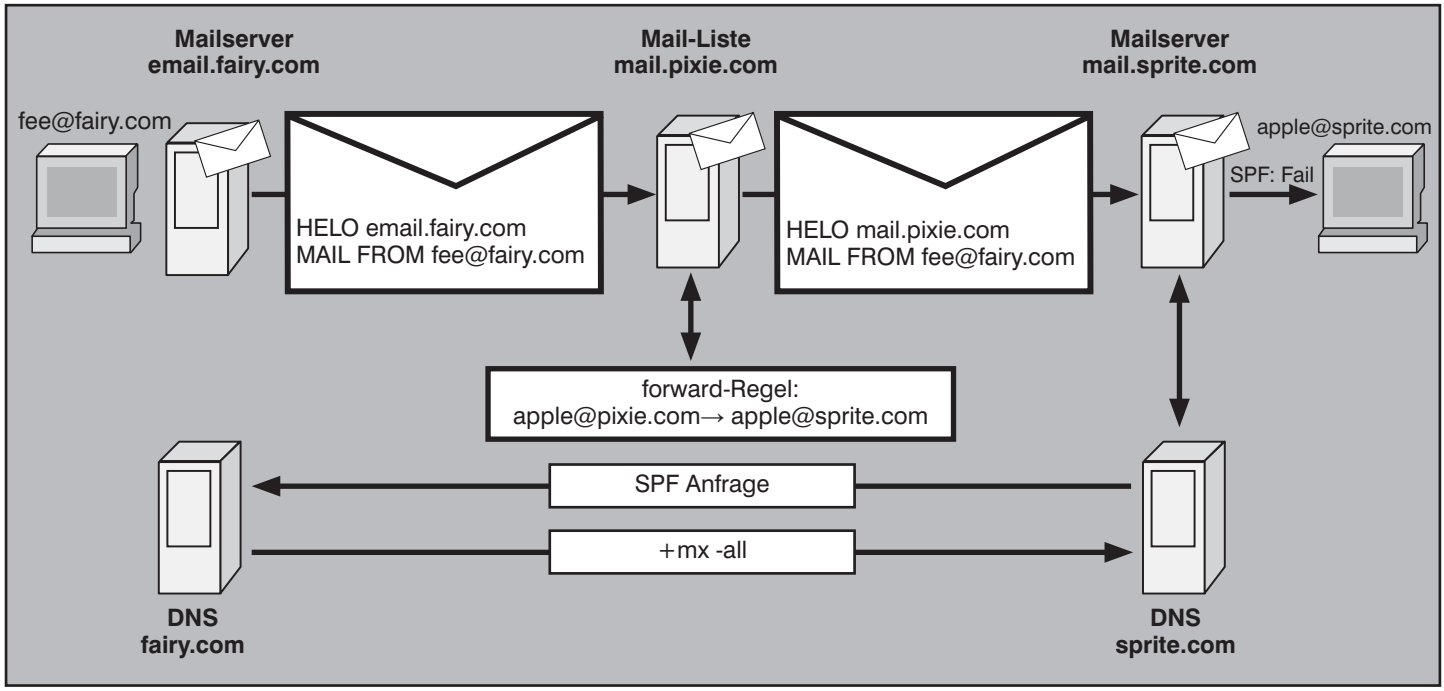


Abbildung 11: SPF beim Forwarding von Mails

Eine Lösung wäre, die IP Adressen der Mailserver von pixie.com in eine White-Liste bei der Domain sprite.de aufzunehmen, so dass der fehlgeschlagene SPF Test übersteuert wird. Allerdings hat das automatisch den Nachteil, dass alle Mails von pixie.com fortan gültig sind, nicht nur die weitergeleiteten.

Eine schöne Lösung für dieses Problem gibt es nicht. Letzten Endes läuft es darauf hinaus, dass in weiteren Tests das Fail des SPF durch eine andere Filterregel übersteuert werden muss. Es bleibt jedoch auf alle Fälle der Nachteil, dass der Empfänger, Apple, sich nicht mehr sicher sein kann, ob der Sender authentisch ist oder nicht. (siehe Abbildung 11)

Relay Gateways
Viele Internet Service Provider (ISP) bieten einen Relay Dienst für Mails an: für den Fall, dass der eigene Server nicht erreichbar ist, nehmen die Relay Gateways des Providers die Emails entgegen und senden sie an den eigentlichen Empfänger weiter, sobald dieser wieder erreichbar ist. Das Bild ähnelt dem eines Forwardings, jedoch mit dem entscheidenden Unterschied, dass das Relay-Gateway des Providers pixie.com für die gesamte Domain sprite.com agiert.

Auch hier schlägt der SPF-Test des Mailservers von sprite.com fehl, da der Server des ISPs nichts mit dem Sender zu tun hat. Jedoch bietet sich in diesem Fall folgende Möglichkeit an: der ISP, pixie.com, führt den SPF Test aus und die eigentliche Empfänger-Domain, sprite.com, trägt den oder die ISP Relay Server in so genannten White-Listen, also Listen mit IP Adressen, von denen generell Mails akzeptiert werden, unabhängig von anderen Testergebnissen. Da zwischen dem Provider und dem Empfänger ein größeres Vertrauensverhältnis bestehen sollte und nur wenige Server in die White-Liste einzupflegen sind, funktioniert das Verfahren. Beim Forwarding ist das Problem, dass es User-basiert ist und somit nicht unter der Kontrolle des Mailadministrators.

Damit das Relay-Gateway nicht zu einem generellen Schlupfloch wird, muss der Serviceprovider den Test durchführen, ansonsten wird das gesamte Framework ausgehebelt. Viele Spamer sind bereits heute dazu übergegangen, nicht die MX Eintrag mit der höchsten Priorität zu nutzen, sondern den mit der niedrigsten, in der Hoffnung, dass diese weniger aufwändig gewartet und gepflegt werden und somit geringere Sicherheitsbarrieren zu überwinden sind. Relay Gateways haben grundsätzlich die geringste Priorität, da sie nur benutzt werden sollen, wenn die eigentlichen Mailserver nicht erreichbar sind. (siehe Abbildung 12)

SenderID

Der SenderID Ansatz beruht auf dem Sender Policy Framework, ergänzt es jedoch um eine Authentifizierungsmöglichkeit anhand in der Mail vorkommenden Email-Adressen. Nachteil des klassischen SPF ist, dass es ausschließlich durch einen MTA abgewickelt werden kann, der noch über die notwendigen SMTP Informationen verfügt. Hier greift SPF Version 2, auch SenderID genannt.

PRA (Purported Responsible Address)
Definiert wird die Purported Responsible Address (PRA) – die vorgebliche Senderadresse. PRA spezifiziert einen Algorithmus, mittels dessen versucht wird, die Adresse aus dem Mailheader herauszufiltern, die am wahrscheinlichsten die Absendeadresse ist … oder zumindest die Adresse, die der Absender behauptet zu haben (engl.: purported = behauptet).

Dazu werden in folgender Reihenfolge

1. die Resent-Sender,
2. Resent-From,
3. Sender,
4. zuletzt (!) die From Adresse herangezogen.

Diese Adressen können dann analog zum klassischen SPF geprüft werden.

Der Test
Um die Erweiterung durch das SenderID Verfahren kompatibel zum SPF zu gestalten, wird die Version von 1 auf Version 2.0 gesetzt. Da auch beim SenderID Check eine Prüfung der MAIL FROM bzw. HELO Identitäten vorgenommen werden kann und diese von der PRA Identität abweichen können, muss der SPF Eintrag

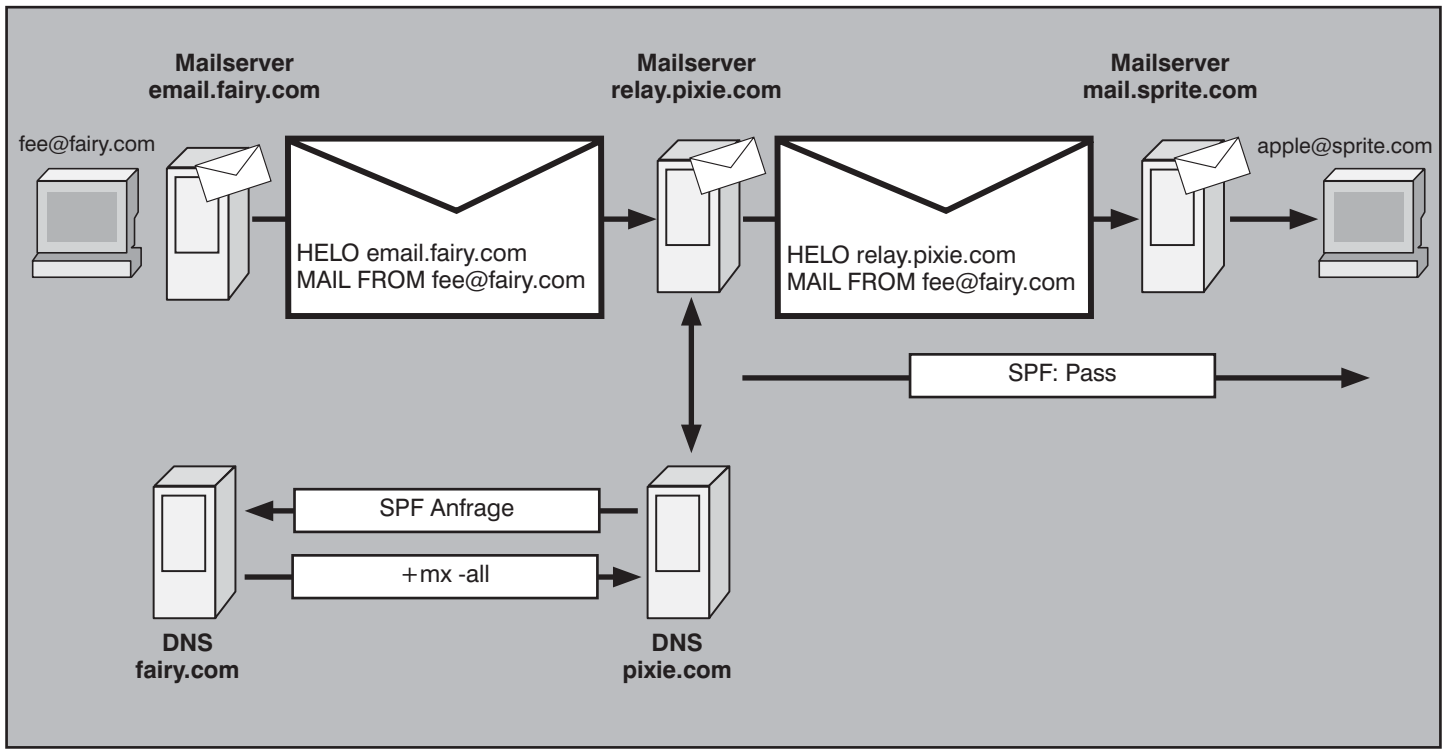


Abbildung 12: SPF beim Relaying von Mails

einen so genannten Scope enthalten, der angibt, ob sich die Prüfanweisung auf die PRA oder MAIL FROM/HELO Identität bezieht. Welche Prüfung vorgenommen wird, wenn für beide Scopes ein Eintrag vorliegt, entscheidet der Empfänger der Mail. Wie auch beim klassischen SPF darf nur ein Eintrag vorliegen, es spricht jedoch nichts dagegen sowohl einen für Version 1 wie auch Version 2 anzulegen, für den Fall, das der Empfänger nur Version 1 beherrscht. Auf diese Weise ist die Abwärtskompatibiltät sichergestellt. Der Rest funktioniert wie beim SPF.

Einsatzszenarien
Es werden die gleichen Einsatzszenarien durchgespielt wie auch beim SPF, auf eine Erläuterung der einzelnen Situationen kann somit verzichtet werden:

Standard Emailversand
Der einfache Emailversand ist ebenso unproblematisch wie beim SPF selbst.

Client und sendender MTA in unterschiedlichen Domains
In diesem Fall weichen die Domains des Mailservers und des Mailsenders mit Sicherheit voneinander ab. Eine Lösung ist, dass die Domain des Users eine Include Anweisung in Bezug auf die Domain des MTAs enthält. Diese Lösung eignet sich besonders für Web-Hoster, die einen Mailservice anbieten.

Ein Problem wird es jedoch, wenn ein Mail-Provider seinen Kunden erlaubt, Email-Adressen zu benutzen, die nicht dem Mail-Provider gehörten. Beispiel: Fee arbeitet gerne zu Hause, hat von dort aber über Internet aus Sicherheitsgründen keinen sendenden Zugriff auf einen Mailserver ihres Arbeitgebers „fairy.com“. Also nutzt sie den Server ihres Internetproviders „pixie.com“, verwendet als Absendeadresse jedoch ihre Firmen-Email fee@fairy.com. Jetzt schlägt SenderID zu: der Empfänger sieht als Absendeadresse eine IP Adresse der Domain „pixie.com“, als Absender jedoch „fairy.com“ und schon schlägt der Test fehl.

Lösungen für dieses Problem wären:

1. Die Server des Providers generell im SPF Eintrag von „fairy.com“ einzutragen. Woran bestimmt niemand bei „Fairy Ltd“ Interesse hat.

2. Der Provider ergänzt den Mailheader um einen „Resent-From“ oder einen „Sender“ Eintrag, in dem Beispielsweise die private Email-Adresse von Fee beim Provider eingetragen wird; also fee@pixie.com.

Mailing-Listen
Eben wegen der Mailing-Listen ist beim PRA den Sender-From- und Resent-From Adressen Priorität über dem From gewährt worden. Da viele Mailinglisten das From Feld nicht ändern können, kann durch das Einfügen zumindest eines dieser Einträge sichergestellt werden, dass der SenderID Test bestanden wird.

Mail Service
Wie bei den Mailing-Listen haben auch die Mail Service Provider für Bulk-Mails die Möglichkeit einen weiteren Eintrag in den Mailheader einzufügen, der Vorrang vor dem From Eintrag hat, den Sender Eintrag.

Relay Gateways
Die Relay Gateway Problematik bleibt dieselbe, die auch beim SPF vorliegt, mit denselben Lösungsansätzen.

Bemerkungen zur SenderID
Zu bemerken ist, dass bei der Auswahl der PRA zunächst die Adressen herangezogen werden, die sich auf den Antwort-Pfad beziehen und nicht die From Adresse. Letztere ist es jedoch, die man von seinem Email-Client her kennt, sprich die, die im Header der Mail zumeist angezeigt wird. Damit ist es aber möglich eine Email zu versenden, die als Return-Sender unglaublich@aberwahr.de eingetragen hat, wohingegen in From - und somit im Email-Programm des Users dargestellt - service@bank.de steht. Selbst wenn das From Feld herangezogen wird, wird nicht geprüft, was vor der Adresse steht:

"Lovely spam! Wonderful spam!" - Was tut sich bei IETF?

```
from: „service@bank.de“ <unglaublich@aberwahr.de>
```

würde von vielen Clients angezeigt als:

```
from: „service@bank.de“
```

Vorschlag zur Lösung der Erfinder von SenderID ist, die Clients dahingehend umzuschreiben, dass sie zumindest die zur Prüfung herangezogene Adresse zusätzlich zur From Adresse mit anzeigen.Außerdem ist zu beachten, dass nicht der Absender sondern dessen Domain geprüft wird.

Der SenderID Check wirkt zunächst so, als wäre er speziell für Clients entwickelt worden, die nachträglich einen SPF Test durchführen. Da sie keine Informationen über die SMTP Felder haben, müssen sie auf die Mailfelder zurückgreifen. Verwunderlich ist deshalb bei dem aktuellen Standard, dass nicht gefordert ist, dass MTAs die IP Adresse des Senders eintragen müssen. Grundsätzlich stehen in Email-Headern zwar auch alle MTAs, über die eine Mail gelaufen ist, verewigt, jedoch ist es häufig schwer, aus der Menge von Einträgen den Mailserver heraus zu filtern, der die Mail an die eigene Domain zugestellt hat. Hinzu kommt, dass das Verfahren in alle gängigen Email-Clients integriert werden müsste, um es nutzen zu können. Insofern bleibt die SenderID wohl für lange Zeit auf die MTAs beschränkt.

Bewertung der SPF Verfahren

Das klassische SPF ist eindeutig darauf ausgelegt, sendende Mailserver für ganze Domains zu autorisieren. Zwar ist es grundsätzlich möglich auch einzelne User/Absender zu überprüfen, jedoch ist das sehr aufwändig und würde sich ohnehin nur auf die MAIL FROM Adresse des Umschlags, nicht auf die From Adresse der Mail selbst beziehen. Das mag nicht unbedingt ein Nachteil sein, eine Einschränkung ist es jedoch auf jeden Fall.

Das SenderID Verfahren erweitert die Überprüfung auf Felder aus der Mail selbst. In der Praxis wird es jedoch wohl auf eine reine Domainenprüfung an den Grenz-MTAs beschränkt bleiben, wie auch das klassische Verfahren und somit wenig Mehrwert bringen, außer dass man Mails erkennen kann, die über offene Relay-Gateways gelaufen sind.

Vorteil beider Verfahren ist, dass die DNS Einträge im eigenen DNS Server gecached werden können und nicht für jede eintreffende Mail die gesamte Abfrage erneut laufen muss, wenn von der Sender-Domain vor kurzem erst eine Mail eingegangen ist.

Domainkeys

Wird der Druck groß genug, so bilden sich manchmal seltsame Verbindungen. Nicht nur in der Chemie, sondern auch bei Allianzen zur SPAM-Bekämpfung. So haben sich die beiden Konkurrenten Yahoo und Google für einen weiteren Vorschlag bei der IETF zur SPAM-Bekämpfung zusammengefunden, genannt: DomainKey.

Yahoo hat bereits im letzten Jahr den Einsatz von DomainKey für alle Kunden als Provider angekündigt. Damit wird, ähnlich wie bei SPF eine große Menge an Postfächern in die Waagschale geworfen, um dem Draft Nachdruck zu verleihen. Noch geht man aber nicht so weit, wie die Vertreter von SPF, die Technik auch aktiv, also beim Empfang, zum Einsatz zu bringen, doch ist es eher eine Frage der Zeit, bis auch das angekündigt wird.

Ebenso wie die SPF Lösung basiert auch die DomainKey Idee auf dem DNS und einer Überprüfung, ob der sendende Mailserver berechtigt ist, Mails für eine bestimmte Domain zuzustellen. Mit anderen Worten, das generelle Ziel ist identisch, jedoch unterscheiden sich beide Verfahren von der Umsetzung her fundamental. Zudem geht man bei dem von Yahoo eingebrachten Vorschlag einen Schritt weiter: neben der reinen Überprüfung des sendenden Servers wird auch die Integrität der Mail sichergestellt, also dass die Mail seit Verlassen des MTAs nicht geändert worden ist. Das dazu angewandte Verfahren erinnert stark an den Authetication Header (AH) bei IPsec.

Zunächst ist beim dem Verfahren nur die Authentifizierung und Integritätsprüfung auf Domain-Ebene spezifiziert worden, jedoch kündigt der Draft weitergehende Maßnahmen an, die auch den Zustellungspfad der Mail und eine Authentifizierung auf User-Ebene ermöglichen sollen.

Die Idee beim DomainKey Verfahren

Das Verfahren der DomainKey ist straight forward: keine großen Rückfrage-Aktionen beim DNS Server der sendenden Domain, in der Regel sollte eine einzelne Abfrage ausreichen und auch keine Wenn-Dann-Arie mit Redirects, Includes usw.

Eine Domain, die das Verfahren nutzen möchte, erzeugt zunächst ein kryptographisches, asymmetrisches Schlüsselpaar, also einen öffentlichen und einen privaten Schlüssel. Den öffentlichen Schlüssel stellt man der Welt über das DNS zur Verfügung, den privaten macht man seinem Boundary-MTA zugänglich. Das Versenden einer Mail läuft dann wie folgt:

1. Der sendende MTA muss sicherstellen, dass der Client/User berechtigt ist, den Mailservice in Anspruch zu nehmen. Die Frage, wie das geschieht, ist nicht die Sache dieses Standards. Dafür kann jedes beliebige Verfahren genutzt werden, das bereits im Einsatz ist oder noch entwickelt werden wird.

2. Bevor die Mail versendet wird, wird sie mit dem privaten Schlüssel signiert; d.h. sie wird nicht verschlüsselt, sondern es wird eine kryptographische Prüfsumme über alle unveränderlichen Teile der Email erzeugt und das Ergebnis wird mit dem privaten Schlüssel verschlüsselt und anschließend in den Header der Mail eingefügt.

3. Anschließend wird die Mail wie gewohnt zugestellt. (siehe Abbildung 13)

Ein Empfänger, der anhand des DomainKey prüfen will, ob die Mail von einem dazu berechtigten Server zugestellt und bei der Übertragung nicht verändert wurde, geht wie folgt vor:

1. Zunächst nimmt er die gesamte Mail entgegen. Eine vorzeitige Prüfung wie beim SPF Verfahren ist nicht möglich.

2. Er besorgt sich den öffentlichen Schlüssel von einem DNS Server der Domain des Absenders.

3. Der Empfänger erzeugt nun denselben Hash (Prüfsumme) wie der Sender, indem er alle unveränderlichen Teile der Mail darin einrechnet.

4. Zuletzt entschlüsselt er die Prüfsumme, die vom Sender im Header der Mail eingefügt wurde und vergleicht das Ergebnis mit seinem eigenen.

Da ein öffentlicher Schlüssel entschlüsselt, was der dazu passende geheime Schlüssel verschlüsselt hat, kann sich der Empfänger bei gleichem Ergebnis der Prüfsummen über zwei Dinge sicher sein: erstens, der Sender verfügt über den geheimen Schlüssel zu dem öffentlichen, den er selbst über DNS mitgeteilt bekommen hat und zweitens die Mail wurde nicht verändert, andernfalls wäre er nicht zum selben Ergebnis gekommen.

Soweit das Verfahren in Kurzform.

Versand einer signierten Email
Der Signatur Prozess des sendenden MTAs durchläuft fünf Phasen:

Schritt 1:
Identifikation der Absende-Domain

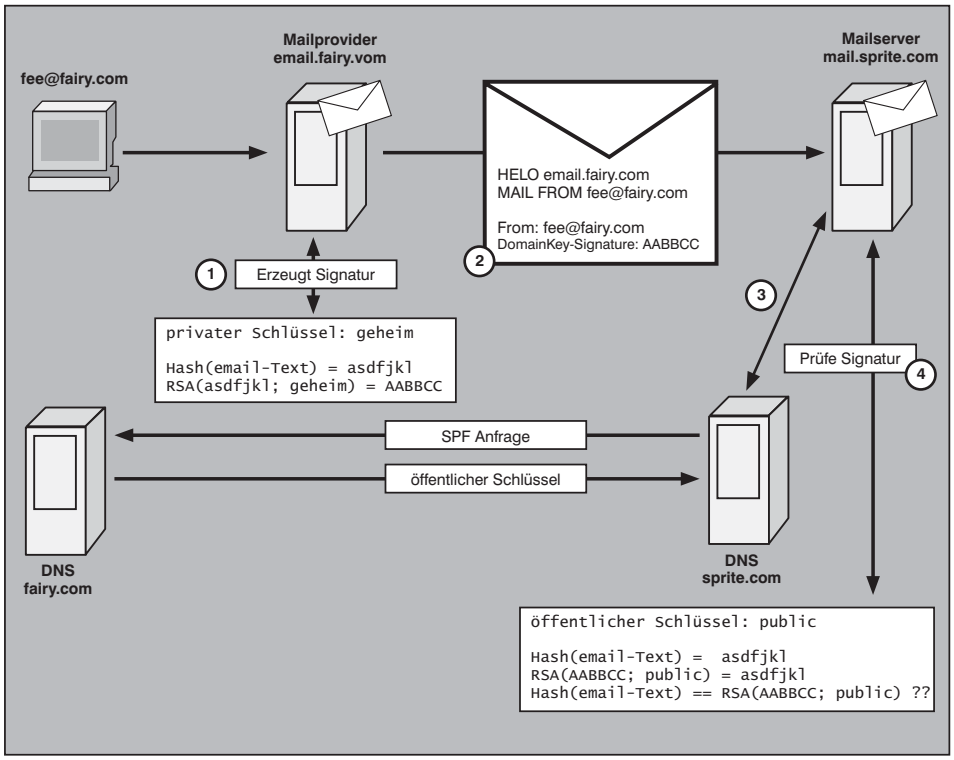


Abbildung 13: Generelle Vorgehensweise des DomainKey Verfahrens

Da beim DomainKey-Verfahren der eigentliche Inhalt der Mail und nicht der SMTP-Umschlag authentisiert und signiert wird, bezieht sich die Autorisierung auch auf die Adressen in der Mail. Aktuell kommen dafür zwei Einträge in Frage: die From- und die Sender Adresse.

Es werden drei mögliche Fälle unterschieden:
1. Es gibt sowohl eine From- wie auch eine Sender Adresse. In diesem Fall hat die Sender Adresse Vorrang gegenüber der From Adresse.

2. Es liegen nur Einträge für From vor. In diesem Fall ist die erste From Adresse zu nutzen.

3. Es liegt kein From in der Mail vor. Unabhängig davon, ob ein Sender angegeben ist oder nicht, findet keine Überprüfung statt.

Schritt 2:
Entscheidung, ob signiert werden muss
Auch bei der Entscheidung, ob signiert werden soll oder nicht, werden verschiedene Fälle unterschieden.

Der einfachste Fall, in dem ein Mailserver die Signierung nicht vornehmen kann, ist, wenn wer nicht über den entsprechenden privaten Schlüssel verfügt, der für den Absender genutzt werden müsste. Aber es gibt noch einen weiteren Grund: ist eine Mail bereits signiert, darf sie nicht erneut signiert werden. Auch ist es dem Mailserver verboten, eine bestehende Signatur in irgendeiner Art zu ändern oder gar zu löschen. Eine Ausnahme wird jedoch berücksichtigt: eine signierte Mail, deren Signatur sich auf die From Adresse bezieht und die nun auch einen Sender Eintrag enthält. Ein Beispiel dafür wären Mailinglisten.

Schritt 3:
Auswahl des zu benutzenden privaten Schlüssels
Bei der Auswahl des zu benutzenden privaten Schlüssels bleibt der Standardentwurf bestenfalls vage und legt das Verfahren dazu in die Hand des Administrators. Wie die Domain aus der Adresse zu extrahieren ist, wird nicht genau definiert. Die Gefahr, dass Sender und Empfänger zu einem anderen Ergebnis kommen, besteht nicht, wie später erläutert wird.

Schritt 4:
Berechnung der Signatur
Bevor die Signatur einer Mail berechnet wird, kann der Sender alle bereits aufgrund der From Adresse vorhandenen DomainKey-Signaturen aus der Mail entfernen, um Verwirrung beim Empfänger zu vermeiden. Normalerweise

sollte das jedoch nicht vorkommen, da es für gewöhnlich nur eine Instanz geben sollte, die eine Signierung vornehmen darf.

Zur Berechnung der Signatur wird die Mail zunächst kanonikalisiert. Diese Kanonikalisierung ist nur für die Berechnung der Signatur relevant, die Email, die später versendet wird, ist noch in ihrem ursprünglichen Zustand. Der Empfänger wird später bei der Überprüfung dieselbe Kanonikalisierung durchführen.

Das Problem, das es zu lösen gilt, ist, das Email auf ihrem Weg durch das Internet durchaus Änderungen unterliegen können, die sich auf Zeilenumbrüche und die Interpretation von so genannten „White-Spaces", nicht sichtbaren Steuerzeichen wie Tabulatoren, beziehen. In den meisten Fällen wird es dem Sender egal sein, wenn es „leichte" Änderungen bei der Zustellung gab, die sich auf eben jene White-Spaces beziehen, unter Umständen will man jedoch sicher gehen, dass die Mail völlig unverändert beim Empfänger ankommt. Um beide Varianten zu ermöglichen, werden zwei Formen der Kanonikalisierung spezifiziert: die „simple" und die „nofws" Variante.

Der „simple" Algorithmus geht wie folgt vor:

- Jede Zeile wird für die Signatur genutzt, von der ersten Header Zeile bis zur letzten der Mail.
- Zeilenbegrenzungen werden entfernt und ein CRLF ersetzt (notwendig, da verschiedene Betriebssysteme unterschiedliche Zeichenfolgen für einen Zeilenumbruch nutzen).
- Alle Leerzeilen am Ende einer Mail werden ignoriert.

Zusätzlich wird noch ein Parameter „h" definiert, mittels dessen angegeben kann, welche Zeilen des Headers für die Signatur genutzt werden sollen. Per Default werden alle Zeilen mit eingerechnet, mit dem Parameter kann die Auswahl eingeschränkt werden. Allerdings wirkt er sich nur auf die Header Zeilen nicht auf den Inhalt der Mail (Body) aus.

Der zweite Algorithmus, „nofws", ist etwas komplizierter, da auch unnötige Zeilenumbrüche im Header und Whitespaces entfernt werden:

- Jede Zeile wird für die Signatur genutzt.
- Zeilen des Email-Headers, die Zeilenumbrüche enthalten, werden zu einer Zeile zusammengefasst.
- Alle Whitespaces werden entfernt.
- Wie beim „simple" Verfahren werden jegliche Zeilenumbrüche durch ein CRLF ersetzt.
- Alle Leerzeilen am Ende der Mail werden ignoriert.

```
DomainKey-Signature: a=rsa-sha1; s=email; d=fairy.com;
q=dns; c=simple;b=AABBCC…;
```

Abbildung 14: Beispiel einer DomainKey Signatur

Auch beim „nofws"-Verfahren kann der „h" Parameter benutzt werden, um nur bestimmte Zeilen des Headers zu benutzten.

Das „simple" Verfahren ist somit das schärfere, da es keinerlei Änderungen zulässt, wohingegen beim „nofws"-Algorithmus durchaus Uminterpretationen von Whitespaces erlaubt sind. In beiden Fällen sind Änderungen am Text einer Email jedoch nicht zulässig und führen später zu einem Fehlschlagen der Signaturprüfung.

Schritt 5:
Einfügen der Signatur in die Mail

Die berechnete Signatur muss zuletzt noch in den Mailheader mit eingefügt werden. Dafür wird eine neue Header-Zeile „Domainkey-Signature" definiert, die selbst natürlich kein Bestandteil der Signatur sein kann, da sie zum Zeitpunkt der Berechnung noch nicht vorliegt. (siehe Abbildung 14)

Neben der eigentlichen Signatur können und müssen noch weitere Parameter in der Signatur einfließen, die zum Teil für die Überprüfung durch den Empfänger notwendig sind.

Empfang einer signierten Email

Der Ablauf beim Empfang einer Email und der Überprüfung der Signatur besteht aus drei Schritten:

1. Extraktion der zur Überprüfung notwendigen Daten aus der Email
2. Besorgen des öffentlichen Schlüssels
3. Überprüfen der Signatur

Sollte einer dieser Schritte fehlschlagen, so ist es Sache der Policy des Empfängers, wie darauf reagiert wird.

Schritt 1: Extraktion der zur Überprüfung notwendigen Daten aus der Email

Analog zur Erzeugung der Signatur wird die Sender/From Adresse aus der Email herausgefiltert, ebenso wie der Signatureintrag „Domainkey-Signature". Die Domain der Sendeadres-

se wird mit der Domain aus der Signatur verglichen.

Schritt 2: Besorgen des öffentlichen Schlüssels

Aus den Informationen in der „DomainKey-Signature“ wird eine DNS Abfrage generiert, um den öffentlichen Schlüssel des Senders zu erhalten.

Schritt 3: Überprüfen der Signatur

Die Überprüfung läuft völlig analog zur Erzeugung der Signatur.

Das Ergebnis des Tests wird in die Mail mittels des Eintrags „DomainKey-Status:“ eingepflegt und kann für weitere Tests verwendet werden oder durch den User-Client an den User weitergegeben werden.

Einpflegen der Keys im DNS

Anders als das SPF Verfahren, das einen eigenen DNS Resource Record vorsieht, verweisen die Erfinder des DomainKey-Verfahren auf einen (vielleicht) kommenden Standard der IETF, um einem Mailempfänger mitzuteilen, welche Policy ein Mailsender unterstützt. So lange ein solcher Standard jedoch nicht existiert, wird eine Zwischenlösung spezifiziert, die jedoch ausdrücklich als „Interim“ bezeichnet wird. Dafür wird der TXT Eintrag des DNS genutzt.

Zusätzlich zum öffentlichen Schlüssel selbst werden weitere Parameter definiert, die von der (vorgeblichen) Absende-Domain an die Empänger-Domain weitergegeben werden können. (siehe Abb. 15)

Eingetragen wird der Schlüssel für eine Domain unter folgender Domain. (siehe Abbildung 16)

Das Schlagwort „_domainkey.“ ist für die Übergangslösung als Subdomain definiert, in der der öffentliche Schlüssel gespeichert wird. Vor dem Schlagwort muss noch der so genannte Selector eingefügt werden. Wie in Abbildung 15 dargestellt, dient der Selector beispielsweise dazu, bestimmte Regionen bei internationalen Firmen spezifizieren zu können. Andere Anwendungen für den Selector sind der Einsatz mehrer MTAs, von denen jeder über einen eigenen privaten Schlüssel verfügt. Oder eine zeitliche Begrenzung der Gültigkeit, ohne durch DNS-Cacheserver in Probleme zu laufen.

Ein Beispiel für eine solche zeitliche Limitierung könnte so aussehen:

```
januar2005._domainkey.fairy.com   TXT    ...

februar2005._domainkey.fairy.com  TXT    ...
```

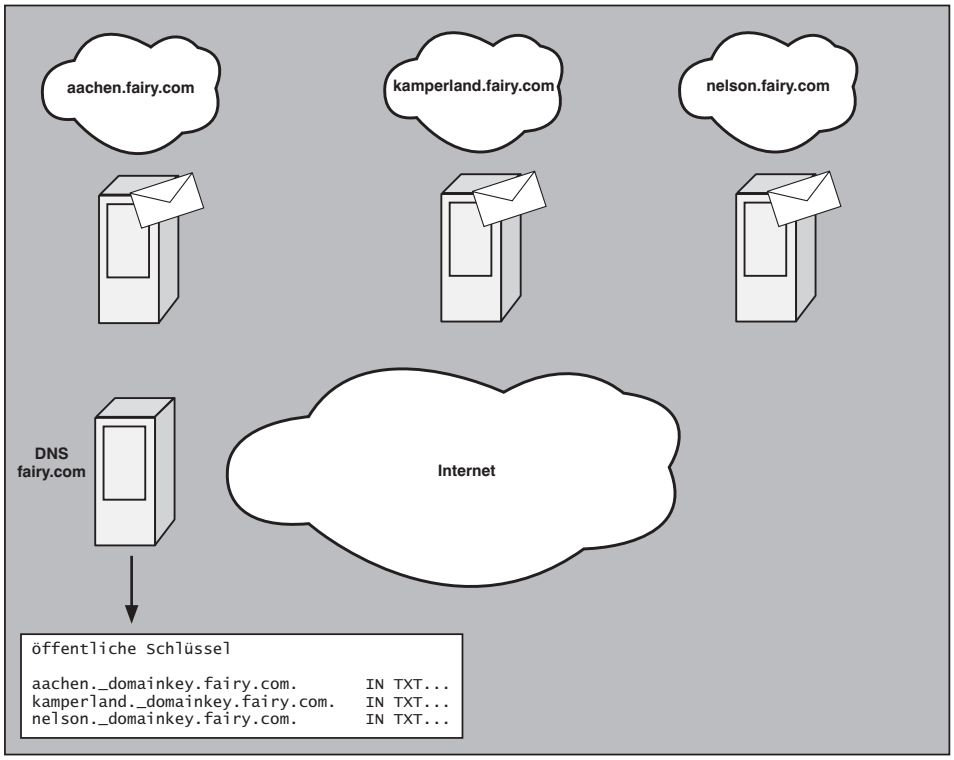


Abbildung 15: DomainKey - Anwendungsbeispiel für den Selector

```
selector._domainkey.domain. IN TXT “Schlüsse + Parameter”

Beispiel:
email._domainkey.fairy.com. IN TXT “k=rsa; p=AAAA…”
```

Abbildung 16: DNS Eintrag eines DomainKeys

Nach dem Monatswechsel nutzt der Sender den neuen Schlüssel. Da er den Selector in der Mail angeben muss, kann es nicht zu einem Problem mit den Cache-Servern kommen.

Einsatzszenarien

Standard Emailversand

Der Standardversand, Sender-Client und Mailserver befinden sich in derselben Domain, stellt natürlich kein Problem für das Verfahren dar.

Client und sendender MTA in unterschiedlichen Domains

In diesem Fall muss entweder der sendende Mailserver über einen geheimen Schlüssel für die Domain des Absenders verfügen oder der Client generiert selbst die Signatur, die dann von dem MTA des Mailproviders nicht mehr geändert werden darf.

Zwar ist es möglich, über einen entsprechenden Selector einen speziellen Schlüssel nur für den Provider zu generieren, der jederzeit zurückgezogen werden kann. Jedoch ist es sicherheitstechnisch immer problematisch, jemand „fremden“ einen gültigen geheimen Schlüssel anzuvertrauen. (siehe Abbildung 17)

Die zweite Variante setzt hingegen voraus, dass die Mailclients die Signatur beherrschen. Der h-Tag sollte dann gesetzt werden, so dass ggf. weitere Änderungen des Mailheaders durch den MTA nicht zu einem Fehler bei der Überprüfung führen. Solche weiteren Headerzeilen könnten beispielsweise durch Virenscanner auf dem Mailserver eingefügt werden.

Mailing-Listen

Mailinglisten, die weder Sender noch From Adresse ändern, sondern stattdessen mit Resent-From/Resent-Sender arbeiten, sind transparent für das Verfahren. Jedoch kann es durch die zusätzlichen Einträge im Header zu einem Fehlschlagen der Überprüfung beim Empfänger führen. Gegen die zusätzlichen Headerzeilen kann man

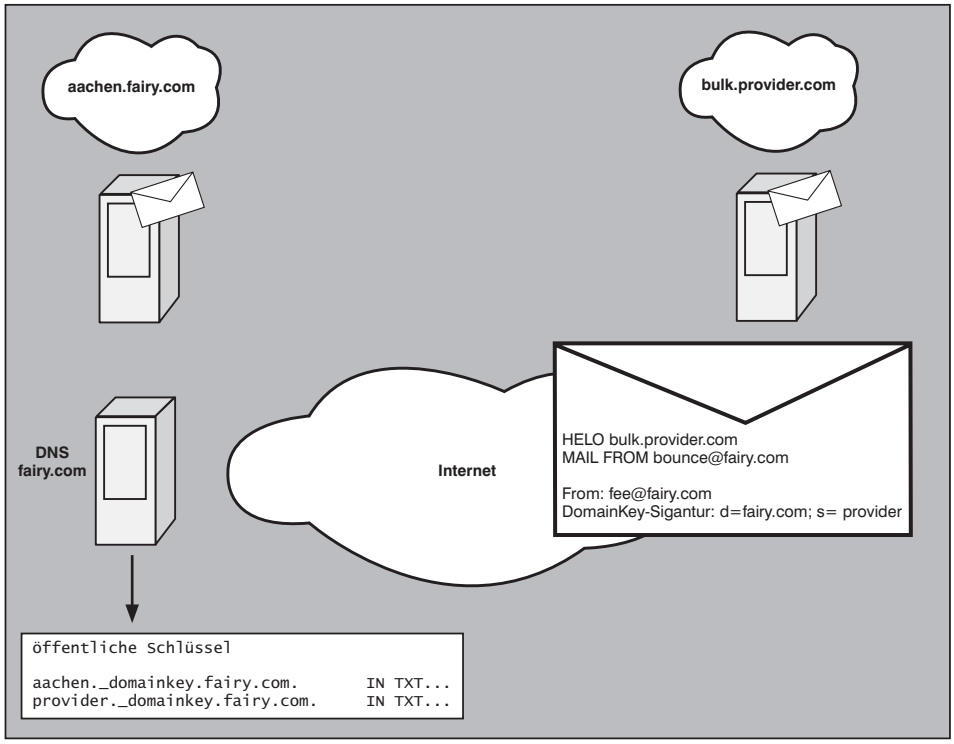


Abbildung 17: Domainkey - Bulk-Mail-Provider

zwar den h-Tag nutzen, so dass nur vom ursprünglichen Sender spezifizierte Zeilen genutzt werden, vielfach fügen Mailinglisten jedoch auch im Mailtext selbst Zeilen mit Hinweisen auf die Liste ein. Da diese zum Body der Mail gehören, fließen sie in jedem Fall in die Signaturberechnung durch den Empfänger ein.

Eine Lösung ist, dass die gesamte Signatur durch den Mailserver der Mailingliste erzeugt wird, dazu muss die Software der Mailingliste jedoch die Senderadresse setzten, da ansonsten die Domain des Absenders nicht zu der Domain des „DomainKey-Signature“ Eintrags passt.

Kurz: aktuell stellen viele Mailinglisten ein Problem dar, da Änderungen an der Software notwendig wären. Hier wären andere Konzepte durchdachter, die die Resent Einträge mit berücksichtigen. Doch vielleicht wird der DomainKey-Draft in den nächsten Versionen noch diesbezüglich angepasst.

Mail Service
Externe Service-Dienstleister für Bulk-Mails stellen für das Verfahren dasselbe Problem dar, wie der Fall, das Mailserver und Client unterschiedlichen Domains angehören. Die Lösungen sind somit analog.

Email Forwarding
Ein Forwarding von Mails stellt so lange kein Problem dar, wie der MTA, der das Forwarding weiterleitet, keine eigene Signatur einbaut. Die Software der MTAs sollte also so konfigurierbar sein, dass in diesem Fall auf ein Signieren verzichtet wird und die Mail „as is“ weitergeleitet wird.

Relay Gateways
Da beim Relaying weder die From- noch die Sender Adresse geändert werden, bleibt die Signatur gültig. Sie sind somit transparent für das DomainKey-Verfahren und stellen kein weiteres Problem dar.

Bewertung des Verfahrens
Das Verfahren wirkt schlichter als andere Verfahren wie SPF oder IIM. Für die DNS Abfragen ist das auch richtig, da eine einzelne Abfrage ausreicht und nicht weiter nachgefragt werden muss. Jedoch erhöht es die Prozessorlast der Mailserver des Senders wie auch des Empfängers in gleichem Maße. Die durch kryptographische Verfahren entstehende Last ist nicht zu unterschätzen, insbesondere asymmetrische Verfahren benötigen viele Prozessorzyklen. Mailserver sollten dementsprechend ausgestattet sein, oder es sollte mit mehreren gearbeitet werden.

Das Forwarding-, das Mailinglisten- und das Provider-Problem muss auf jeden Fall gelöst werden, bevor an einen flächendeckenden Einsatz zu denken ist.

Identified Internet Mail (IIM)

Domain-Hoster, Internet-Provider und Softwareentwickler haben sich bei den beiden bislang beschriebenen Vorschlägen zusammengetan, der letzte kommt von einer dritten, unerwarteten Seite: einem Netzwerk-Komponenten-Hersteller, Cisco. Bislang scheint Cisco mit seinem Vorschlag bei der IETF noch alleine da zu stehen, trotzdem ist der Vorschlag wert betrachtet zu werden. In seinen Grundsätzen ähnelt er dem Domainkey Entwurf sehr stark, geht jedoch von einer anderen Voraussetzung aus, als der Entwurf von Yahoo und Google: User-Keys werden nicht die Ausnahme sondern die Regel sein.

Als Hersteller für Netzwerkkomponenten für Firmen weiß Cisco um die Bedürfnisse seiner Kunden: mobile User und gestiegene Sicherheitsanforderungen. Vertriebsmitarbeiter schreiben Emails in Hotelzimmern ohne Zugriff auf ihren eigenen Mailserver zum Senden von Emails; Berater bekommen nur temporären und eingeschränkten Zugriff bei Kunden auf das Netz, um nur zwei Bespiele zu nennen. Damit werden mehr Schlüssel notwendig als bei der Voraussetzung, die bei dem Domainkey-Verfahren angenommen wurde. Ein separater Keyserver erhöht die Flexibilität der Konfiguration, aber auch den Pflegeaufwand, gleichzeitig reduziert es die Last der DNS Server. Damit hofft man ein Modell geschaffen zu haben, das besser skaliert.

Die Idee des Verfahrens
Die Idee ist der des Domainkey-Verfahrens recht ähnlich: auch beim IIM-Verfahren wird die Mail inklusive des Message-Bodies durch den Sender signiert und so gegen nachträgliche Änderungen geschützt. Ebenfalls identisch ist, dass dazu das DNS genutzt werden kann. Die Unterschiede liegen somit im Detail der Umsetzung.

Abbildung 18 zeigt das Vorgehen:

1. Zunächst signiert der Sender seine Mail. Ob das durch den Client oder den MTA geschieht, ist für den KRS Einsatz unerheblich. In den Signatureintrag kommen weitere Parameter, u. a. die Anweisung, die Signatur mittels DNS oder KRS zu überprüfen und auch den öffentlichen Schlüssel selbst.
2. Der Empfänger extrahiert die Signatur und den öffentlichen Schlüssel.
3. Darauf rechnet er die Signatur nach und prüft, ob er zum selben Ergebnis kommt.
4. Ist die Signatur korrekt, berechnet der Empfänger den Fingerprint des öffentlichen Schüssels.

Bis hierher ist die Vorgehensweise für DNS und KRS Überprüfung identisch. Beim DNS Verfahren geht es wie folgt weiter:

1. Der Fingerprint, der Eintrag „_krs.“ und die Absendedomain werden zu einer einzigen DNS Abfrage verbunden (Beispiel: „AAAA._krs.fairy.com“)
2. Existiert ein entsprechender Eintrag im DNS, so wird der Fingerprint je nach Konfiguration von der Senderdomain bestätigt oder abgelehnt.
3. Existiert kein Eintrag, so gilt der Test als nicht bestanden.

Hat der Sender hingegen KRS als Verfahren festgelegt, so geschieht folgendes:

1. Zunächst fragt der Empfänger den DNS Server des Absenders nach dem KRS.
2. Die Antwort enthält einen Link, unter dem der KRS zu erreichen ist.
3. Die KRS Abfrage selbst erfolgt dann über einen HTTP-Request beim KRS.

Handelt es sich bei dem Empfänger, der die Signatur überprüft, um einen MTA, so kann er das Ergebnis der IIM-Überprüfung in einem weiteren Eintrag im Mailheader vermerken, so dass er von weiteren Mechanismen zur SPAM-Bekämpfung als weiteres Indiz herangezogen werden kann.

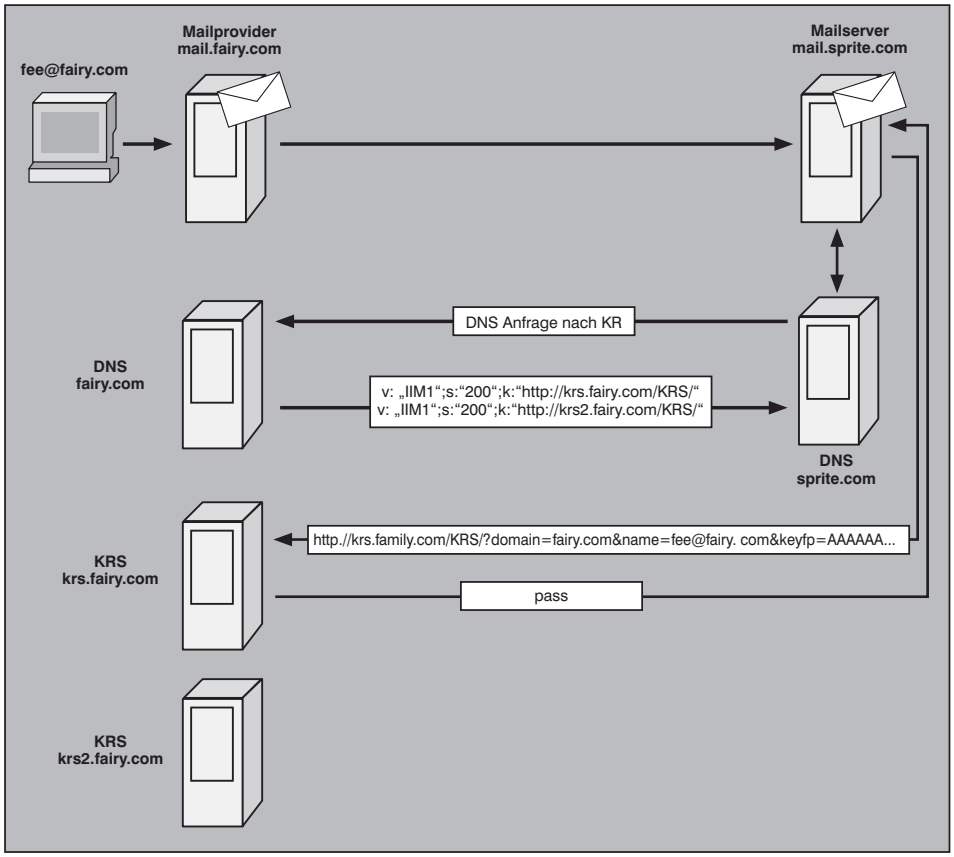


Abbildung 18: IIM - Überprüfung mittels KRS

Versand einer signierten Mail

Berechnung der Signatur

Die Erzeugung der Signatur ist ähnlich dem des DomainKey-Verfahrens. Der Unterschied besteht primär darin, dass die Header-Zeilen nicht in die Signatur mit einfließen, sondern nur die Parameter aus dem „IIM-SIG“-Eintrag. In diesen werden jedoch bestimmte Header-Zeilen hineinkopiert. Vorteil dieser Vorgehensweise ist, dass eine evtl. Änderung der Header-Zeilen beim Transport durch unterschiedliche Interpretation von Zeichensätzen oder einfügen von Leerzeichen/-zeilen keinen Effekt auf die Gültigkeit der Signatur haben.

Der Sender kann angeben, wie viele Zeichen er berücksichtigt hat. Auf diese Weise kann die Perfomance bei langen Mails verbessert werden. Zudem ist es so möglich, sicher zu stellen, dass später eingefügte Zeilen (bspw. von Mailinglisten als Footer) nicht berücksichtigt werden. Ein User-Client könnte nicht signierte und möglicherweise geänderte Zeilen optisch markieren und so den User informieren.

Auch das IIM-Verfahren unterscheidet zwischen denselben beiden Verfahren der Kanonikalisierung wie das DomainKey-Verfahren.

Einfügen des Signatur-Tags in die Mail

Die berechnete Signatur muss zuletzt noch in den Mailheader mit eingefügt werden. Dafür wird eine neue Header-Zeile „IIM-SIG“ definiert. (siehe Abbildung 19)

Neben der eigentlichen Signatur können und müssen noch weitere Parameter in der Signatur einfließen, die zum Teil für die Überprüfung durch den Empfänger notwendig sind.

Empfang einer signierten Mail

Berechnung der Signatur

Der Empfänger berechnet die Signatur analog zum Sender der Mail.

Überprüfung der Signatur

IIM bietet grundsätzlich die Möglichkeit, auch ohne einen speziellen KRS zu arbeiten und die Überprüfung mittels DNS vorzunehmen. Ob KRS oder DNS als Verfahren genutzt werden soll, weiß der Empfänger anhand des entsprechenden Eintrags in der IIM-SIG. Je nachdem welche der beiden Varianten zum Einsatz kommen, sieht sowohl die Frage an den DNS wie auch der Eintrag im DNS anders aus.

KRS

Cisco führt in seinem Vorschlag einen neuen Servertyp ein, den Key Registration Server (KRS). Auf diesem Server werden nicht die Schlüssel selbst hinterlegt, sondern nur die Fingerprints aller gültigen Schlüssel.

Der empfangende MTA weiß anhand des IIM-SIG Eintrags, dass die Prüfung via KRS zu erfolgen hat. Zunächst prüft er, ob er den entsprechenden Fingerprint noch im Cache hat und er noch gültig ist. So wird vermieden, dass unnötig viele Anfragen an den KRS Server gestellt werden. Ist dem nicht so, so fragt er den DNS Server, der sendenden Domain, welche KRS Server es gibt. Dafür wird ein neuer Resource Record im DNS eingeführt, der KR Record.

```
IIM-SIG: v:”1”; h:”email.fairy.com”; d:”fairy.com”;
  z:”home”; m:”krs”; t:”1234567890.654321”;
  x:”123456”; a:”rsa-sha1”; b:”plain:1234”; e:“Iw==;
  n:“zCND+…“; s:“Tg67i…“;
  c:“From: Fee 2Pf <fee@fairy.com>”;
  c:”Date: Wed, 23 Mar 2005 11:22:26 +0100 (MET)”;
  c:”Subject: RE: Reklamation des Wunsches“
```

Abbildung 19: Beispiel einer IIM-Signatur

Der DNS Eintrag enthält - in recht unübersichtlicher Form - eine Reihe von DNS Parametern und u. a. einen Hinweis auf eine URL, die der Empfänger benutzten soll, um den Fingerprint des Schlüssels aus der Signatur zu überprüfen. Nach Ermittlung der IP Adresse des Hosts, der zu der URL gehört, wird nun eine HTML-Abfrage generiert, die an den KRS gesendet wird.

Abbildung 21 zeigt die Form der Abfrage.

Der KRS Server überprüft daraufhin seine Datenbank und übermittelt ein „pass“ oder „fail“ zurück.

Abbildung 22 zeigt ein Beispiel, wie solch ein Eintrag aussehen könnte.

Vorteil eines speziellen Servers ist, dass die Beschränkungen, die durch DNS gegeben sind, durch das neue Verfahren aufgehoben werden. Wie das Beispiel zeigt, ist es möglich, selbst komplexe Organisationsstrukturen abzubilden oder einzelne Schlüssel zurückzuziehen.

Da der Schlüsselserver zu einem kritischen Punkt der Mailkommunikation wird, sollten mindestens zwei davon existieren, die möglichst räumlich voneinander getrennt sind. Analog zu den Nameservern des DNS. Anders als beim DNS ist jedoch aktuell kein Verfahren vorgesehen, wie die Informationen der verschiedenen KRS abgeglichen werden können, sondern es wird nur darauf hingewiesen, dass dies ein kritischer Punkt ist.

DNS

Für viele Domains dürfte der Einsatz eines KRS den Effekt haben, dass man mit Kanonen auf Spatzen schießt. Denn viele werden sich mit einem einzelnen Schlüssel für die gesamte Domain begnügen oder schlimmstenfalls noch für einige, wenige ausgesuchte User weitere Schlüssel benötigen. Aus diesem Grund sieht der Standardentwurf auch eine Überprüfung mittels DNS vor. (siehe Abbildung 23)

Im DNS Server wird für jeden Fingerprint ein eigener KR Eintrag angelegt, der wie in Abbildung 24 aussehen könnte.

Der Eintrag baut sich wie folgt auf: zunächst steht der Fingerprint (im Beispiel: AAAA) gefolgt von dem Kürzel „_krs“ und der Domain. Danach kommt der RR-Typ (KR). Anschließend eine Reihe von Parametern, die später noch erläutert werden.

Der Null-Key-Check

Die Frage ist jedoch, was passiert, wenn eine Mail überhaupt keinen IIM-SIG Eintrag enthält?

```
fairy.com.      IN KR 10 10 378
       „v:\“IIM1\“\;s:\“200\“\;k:\http://krs.fairy.com/KRS/\\;“
fairy.com.      IN KR 10 10 378
       „v:\“IIM1\“\;s:\“200\“\;k:\http://krs2.fairy.com/KRS/\\;“
```

Abbildung 20: DNS Eintrag für KRS

```
http://DNS-Response/?domain=domain&name=email-adresse&keyfp=fingerprint
Beispiel:
http://krs.fairy.com/KRS/?domain=fairy.com&name=fee@fairy.com&keyfp=AAAAAA…
```

Abbildung 21: KRS Abfrage mittels HTTP

```
#Auth   TTL             Adresse                 Service
#Key Fingerprint        Bemerkung

pass    86400           fee@hive.fairy.com      SMTP
AAAAAA…                 # Fee’s üblicher Schlüssel

pass    86400           fee@fairy.com           SMTP
AAAAAA…                 # Fee’s Schlüssel, wenn der MTA einen
                          Adress-Rewrite macht

pass    86400           elfe@fairy.com          SMTP
BBBBBB…                 # Der Schlüssel der Elfe auf ihrem PC

fail    86400           elfe@fairy.com          SMTP
CCCCCC…                 # Der Schlüssel der Elfe auf ihrem
                          verlorenen PDA

pass    86400           magier@fairy.com        SMTP
DDDDDD…                 # Des Magiers Schlüssel

pass    86400           magier@fairy.com        SMTP
AAAAAA…                 # Da der Magier der Assistent der Fee
                        ist, darf er auch ihren Schlüssel nutzen

pass    604800          *@fairy.com             SMTP
EEEEEE…                 # Der Schlüssel von Fairy, genutzt durch
                          einen MTA für die gesamte Domain

pass    86400           mystic@fairy.com        SMTP
*                       # Mystic kann jeden Schlüssel nutzen,
                          alle werden bestätigt => NICHT RATSAM
```

Abbildung 22: KRS Datenbank

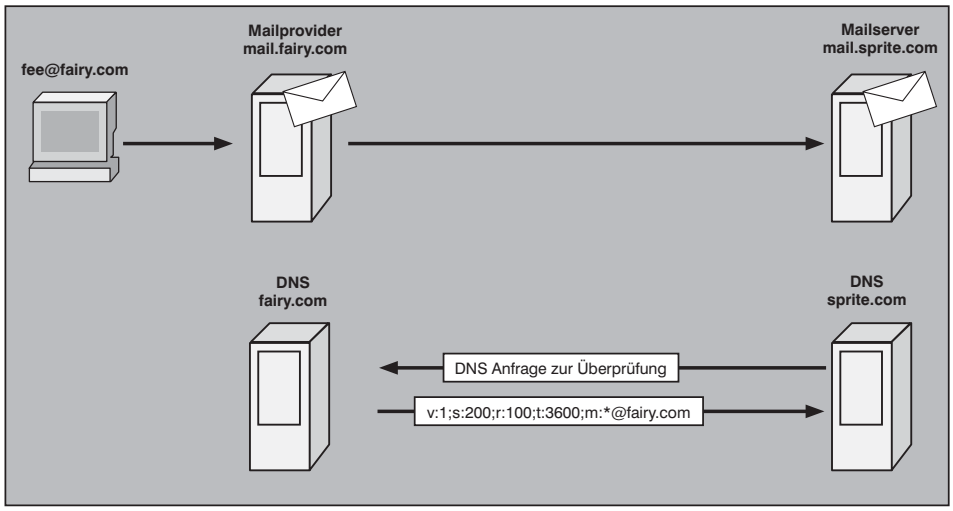


Abbildung 23: IIM - Überprüfung mittels DNS

In diesem Fall wird der Null-Key-Check durch den Empfänger ausgeführt:

Der Empfänger nutzt die From Adresse um die Domain zu ermitteln, von der die Mail angeblich stammt. Will ein Domain-Betreiber sicherstellen, dass nur signierte Mails in seinem Namen versandt werden dürfen, so muss er einen entsprechenden Eintrag in seinem DNS vornehmen, der wie in Abbildung 25 aussehen könnte.

Der Eintrag “a:fail” signalisiert dem Empfänger, dass die Domain grundsätzlich signiert. Weitere Einträge für gültige Fingerprints müssen natürlich vorgenommen werden.

Einfügen des Ergebnisses in den Mail-Header
Das Einfügen des Ergebnisses des Tests in Form eines „IIM-Verify“ Eintrags selbst ist dem MTA freigestellt. Jedoch muss ein empfangender MTA eine bereits vorhandene IIM-Verify Zeile löschen, wenn er selbst einen Test durchführt. Zwei Einträge dürfen nicht vorhanden sein. Ebenso muss ein Empfänger die Zeile entfernen, wenn er Mails von einer anderen Domain empfängt, unabhängig davon, ob er selbst plant einen Test durchzuführen oder nicht.

Einsatzszenarien

Standard Emailversand
Wie bei den anderen Mailverfahren auch, ist das IIM-Verfahren für einen Standard-emailversand von einem Sender zu einem Empfänger natürlich geeignet.

Client und sendender MTA in unterschiedlichen Domains
Das mobile User Problem besteht auch beim IIM-Verfahren. Eine Lösung wäre jedoch, mobilen User eigene Schlüssel zuzuweisen. Die Emailclients der User müssten in diesem Fall in der Lage sein, die Signatur selbst zu erzeugen, anstatt sie durch den Mailserver erzeugen zu lassen.

Mailing-Listen
Das Problem der Mailing-Listen trifft natürlich auch dieses Verfahren: unterschiedliches Verhalten je nach eingesetzter Software. Die Autoren unterscheiden zwei Fälle: Mailing-Listen, die nichts am Body oder an den signierten Headerzeilen ändern und solchen, die genau das tun.

Im ersten Fall kann die Signatur des ursprünglichen Senders unverändert bestehen bleiben. Jedoch ist es erlaubt, die Signatur zu ändern. Das wird insbesondere dann notwendig, wenn die Mailing-Liste einen Sender Eintrag im Header vornimmt, da dieser gegenüber dem From Eintrag Vorrang bei der Ermittlung der Sender-Domain besitzt.

```
AAAA._krs.fairy.com.                KR
      „v:\“1\“; s:\“200\“; r:\“100\“; t:\“3600\“; m:\*@fairy.com\““
```

Abbildung 24

```
fairy.com.    KR
    „v:\“1\“; s:\“200\“; a:\“fail\“; t:\“864000\“; m:\*@fairy.com\““
```

Abbildung 25

Im zweiten Fall hingegen muss die Mailing-Liste einen bereits vorhandenen IIM-Signatur Eintrag löschen, den Sender einfügen und die Signatur selbst neu berechnen.

Mail Service
Da das Verfahren eine sehr feine Strukturierung der Authentifzierungen zulässt, ist es für diesen Fall besonders geeignet: Ein Unternehmen kann für den externen Bulk-Mail-Provider eine oder mehrere Schlüsselpaare erzeugen und diesem zur Verfügung stellen. Die Schlüssel gelten jedoch nicht für die gesamte eigene Domain, sondern nur für einzelne Adressen. Die Einträge für diese Schlüssel nimmt man im eigenen DNS bzw. KRS vor und behält auf diese Weise auch die Kontrolle, da man Schlüssel selbst sehr einfach zurückziehen kann. (siehe Abbildung 26)

Email Forwarding
Email Forwarding stellt - wie beschrieben - häufig ein Problem dar. Im Falle des IIM-Verfahrens jedoch sollte ein Forwarding, dass die Mail nahezu unverändert weiterleitet, zu keinen Problemen führen, da der Mailbody sich nicht ändert und vom Mailheader nur die in der IIM-Signatur vermerkten Zeilen einfließen.

Relay Gateways
Da Relay Gateways keine Änderungen vornehmen, die für die Signatur von Bedeutung sind, stellen sie auch kein Problem dar.

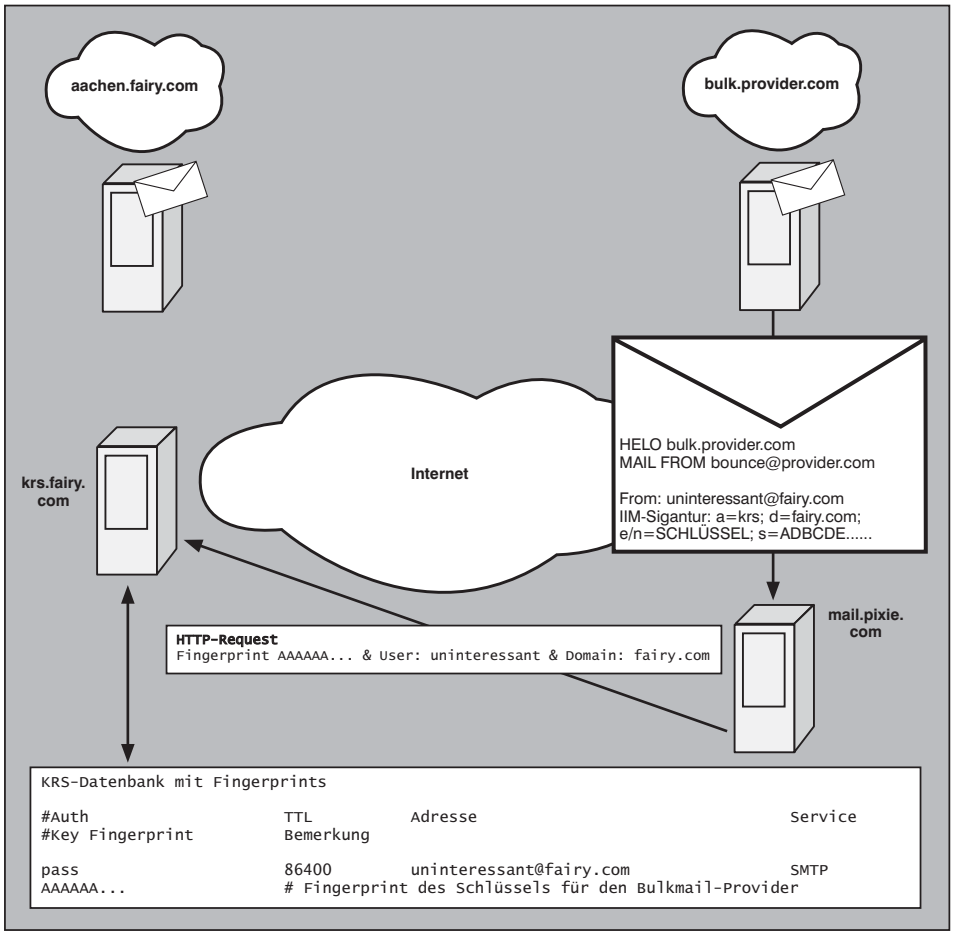


Abbildung 26: IIM - Bulk-Mail-Provider

Bewertung des Verfahrens

Das von Cisco eingebrachte Verfahren ist mit Sicherheit das flexibelste von den drei Vorschlägen, die aktuell diskutiert werden: sowohl Domain- wie auch Userschlüssel sind möglich und bei Einsatz eines KRS können sogar komplexe Strukturen verwirklicht werden.

Nachteile sind jedoch auch reichlich vorhanden:

- Ein neuer Servertyp, der KRS, wird eingeführt. Dieser muss zunächst noch entwickelt werden und sich in der Breite durchsetzen.
- Parallel dazu müssen Routinen für die MTAs und Clients eingeführt werden.
- Eine hohe Flexibilität steht meist auch für eine hohe Komplexität, was den Verwaltungsaufwand erhöht. Gerade bei der Abbildung komplexer Strukturen, wie sie durch IIM zugelassen werden, kann man sehr schnell die Übersicht verlieren. Mit anderen Worten, das KISS Prinzip wird durch das Verfahren nicht vorgegeben, sondern muss durch den Administrator verwirklicht werden.

In Anbetracht der Tatsache, dass Cisco mit dem Vorschlag alleine dasteht und anders als die beiden anderen Vorschläge auch nicht mit mehreren Millionen von Postfächern sein Verfahren mit Gewalt durchdrücken kann, wie Yahoo und Microsoft das mit ihren Verfahren machen, räumt der Autor diesem Verfahren die geringsten Chancen auf einen Erfolg ein.

Angriffsvarianten

Wie bei jeder neuen Technik gilt, dass nicht nur neue positive Möglichkeiten geschaffen werden, sondern auch neue Gefahren für Angriffe entstehen. Einige davon sind bei allen drei Verfahren gleich oder ähnlich, andere nur für eines oder zwei der Verfahren relevant. Einige Angriffsmöglichkeiten sind:

Denial of Service

Wie bei allen im Internet angebotenen Diensten ist keines der Verfahren immun gegen einen verteilten Denial of Service Angriff auf die DNS Server, von denen sie alle abhängen. Zwei Varianten sind dabei denkbar: einerseits der „typische“ DoS-Angriff, bei dem die Server mit unechten Anfragen überhäuft werden, bis sie die legitimen nicht mehr bearbeiten können; das kann durch in fremde Syteme eingeschleuste Software (Malware) wie Würmer oder Trojaner erfolgen. Eine andere Variante wäre ein indirekter Angriff: jemand verschickt eine sehr große Menge von Emails mit falschem Absender. Die Server der Domain, deren Absender in den Mails genutzt wird, bekommt nun eine große Menge von legitimen Anfragen, u. U. so viele, dass Anfragen zu Mails, die wirklich von ihm verschickt wurden, nicht mehr abgearbeitet werden. Für diese zweite Variante ist es noch nicht einmal notwendig, dass andere Systeme mit bösartiger Software infiziert werden, da es sich um eine Ausnutzung des Verfahrens selbst handelt.

Stall Taktik

Die Stall Taktik richtet sich nicht gegen eine Domain, sondern stellt einen Versuch dar, das Verfahren zu überlisten. Dazu sendet der Angreifer Mails, in denen er seine eigene Domain als Absender einträgt und stellt einen DNS (KRS) Server auf, der nur sehr langsam reagiert. Dadurch erhofft er sich, dass es bei den Empfängern zu einem Mailstau kommt, der seinerseits die Administratoren der Empfänger dazu veranlasst, den Mechanismus auszuschalten. Eine Lösung dafür wären Timeouts für die Requests.

Fehlerhafte Einträge

Gerne genutzt werden auch fehlerhafte Einträge, um Systeme zu kompromittieren. Die Implementation der Verfahren muss also sowohl vom DNS (KRS) Server wie auch vom Mailserver darauf vorbereitet sein, fehlerhafte Antworten/Fragen zu bearbeiten. Es wäre nicht das erste Mal, dass eine vergessene Syntax-Prüfung dazu führt, ein ganzes System lahm zu legen.

Besonderheiten bei DomainKey und IIM

Bereits existierendes Prüfungsergebnis

Ein Problem entsteht, wenn der Empfänger Mailserver keinen Test durchführt, der User-Client jedoch bereits auf das Verfahren reagiert und das Ergebnis an den User weitergibt. Dann kann ein Sender „einfach“ sowohl eine Signatur wie auch das Testergebnis in die Email einfügen und auf „ok“ setzen. Da der User-Client nicht entscheiden kann, wer den Status gesetzt hat, würde er dem Empfänger melden, dass die Signatur gültig ist.

Nutzung fremder Schlüssel

Ein Grundproblem beim Einsatz von asymmetrischen Verfahren ist der Schutz der privaten Schlüssel. Gelingt es einem Angreifer eine Kopie davon zu bekommen, kann er die Identität desjenigen annehmen, dessen Schlüssel er besitzt. Dieses Problem stellt sich für das IIM-Verfahren insbesondere, wenn mit User-Schlüsseln gearbeitet wird, die sich auf den Clienten befinden, da diese typischerweise nicht

dem gleichen Zugriffsschutz und der gleichen intensiven Kontrolle unterliegen, wie dies bei einem Server der Fall ist.

Möglich wäre zum Beispiel, dass ein Wurm sich bei einem Client einnistet und mittels des entsprechenden Mailclients mails verschickt. Je nach Implementation der Schlüsselverwaltung kann er sich selbst nun mittels korrekt signierter Mails verbreiten. Häufig werden Passphrasen, Mantras, genutzt, um private Schlüssel vor einem unberechtigten Zugriff zu schützen: bevor die Mail signiert wird, muss der User sein Mantra eingeben. Viele Enduser neigen jedoch dazu, sehr schwache Passphrasen zu benutzen, die sehr einfach zu erraten sind, was die Wirksamkeit eines solchen Schutzes in Frage stellt.

Auch könnte es einem Virus/Wurm gelingen, den Schlüssel zu kopieren und an seinen Programmierer zu senden.

Generell wäre es sinnvoller, alle Mails, auch die auf Userbasis, vom MTA signieren zu lassen, der über die entsprechenden Schlüssel verfügt und die Sicherstellung, dass ein User sendeberechtigt ist, anders sicherzustellen. Das Verfahren funktioniert natürlich nur, wenn es möglich ist, dass die User-Clienten immer ihren Server erreichen können. Zudem müssen dann weitere Mechanismen auf dem MTA sicherstellen, dass keine von einem Wurm infizierten Mails versendet werden.

Besonderheit SPF

Im Falle des Redirects ist die Möglichkeit für eine Denial-Of-Service Attacke (DoS) am offensichtlichsten, jedoch bieten auch andere Mechanismen diese Möglichkeit. Beispielhaft soll es in Abbildung 27 anhand des Redirects erklärt werden.

Ein Mailserver, der sich „email.fairy.com" nennt, sendet eine Email an die Domain „pixie.de". Der Mailserver extrahiert die Domain und erzeugt einen DNS-Request an seinen DNS Server und erhält als Antwort auf die Anfrage des SPF Records eine Hostprüfung (A) und einen Redirect. Darauf erzeugt er einen weiteren DNS Request an seinen DNS Server, um die Hostprüfung durchzuführen. Als Antwort darauf wird eine lange Liste mit IP Adressen zurückgegeben, die er alle mit der des sendenden Mailservers vergleichen muss. Da das zu keinem Ergebnis führt, folgt er nun dem Redirect und ermittelt via seinem eigenen DNS Server den SPF Record der Domain „sprite.com", der ebenfalls einen A Record und einen Redirect enthält. Auch dieser A Record wird aufgelöst und geprüft, führt zu keinem Ergebnis und der Redirect wird angewendet. Im Beispiel wird sogar ein Loop gebildet. In der Realität ist es vergleichsweise einfach, solche Loops aufzuspüren und als Abbruchkriterium in der Software zu implementieren. Schwieriger hingegen ist es, festzustellen, dass die Prüfung durch eine sehr lange Reihe von Redirects durchgereicht wird.

Die Gefahr, die von diesem Vorgehen ausgeht, ist, dass sowohl der Mailserver wie auch der DNS Server des Empfängers über ihre jeweilige Belastungsgrenze in DNS Anfragen und SPF Prüfungen verstrickt werden. Ähnliche Angriffe sind auch mit anderen Mechanismen möglich; so bietet sich beispielsweise der PTR Mechanismus mit seiner komplexen Mehrfachauflösung gerade dazu an, ebenso wie die Include Anweisung. Aus diesem Grund werden eine Reihe von Grenzwerten für die Mechanismen und Modifier definiert, die nicht überschritten werden dürfen.

Gesamtbewertung

Vorteile/Nachteile

So schön die Vorschläge zunächst auch einmal klingen, stellt sich doch die Frage: helfen sie uns der Spamflut Herr zu werden? Was hindert eigentlich einen SPAM-Versender daran, irgendwo auf dieser Welt eine Domäne zu reservieren, so wie sie es bereits heute tun, und dafür einen SPF Eintrag, Domainkey oder Public Key zu erzeugen, alles ordnungsgemäß im DNS einzutragen und dann Spams zu verschicken? Nichts hindert ihn!

Was hat es uns also gebracht? Sicher, **wir können nun beim Betreiber der Top-Level Domain erfahren, wer für die Domäne verantwortlich ist** und selbigen verklagen, da wir uns „sicher" sind, dass er es war, schließlich kam es „mit Sicherheit" von einem seiner Mailserver. Nun, das ist aber nichts neues, das können wir bereits heute. SPAM bringt dem Sender doch nur etwas, wenn er es schafft, mittels der Mail auch etwas zu verkaufen. Fast alle SPAM Mails enthalten Links entweder zu Domänen oder zu IP Adressen. In beiden Fällen lässt sich herausfinden, wer sich dahinter verbirgt. Also nichts Neues durch die neuen Techniken.

An dieser Stelle wird eingewendet, dass man jetzt genauer sagen kann, welche Mails von welchen Domänen man akzeptiert und welche nicht. Betrachten wir dieses Argument: wie häufig hat man mit Leuten zu tun, mit denen man bislang noch keinen Kontakt hatte, die Domäne also unbekannt ist? Wie oft „ändert" sich eine Domäne eines Bekannten, Zulieferers oder Kunden: gestern noch comconsult-akademie.de und heute schon comconsult-research.com. Der Pflegeaufwand für die Anpassung der Black-/White-Listen ist so groß wie früher.

Nächstes Argument: **Viren und Würmer können nun nicht mehr falsche Absender fingieren.** Stimmt, aber etliche Viren und Würmer haben das noch nie getan! Sie vermailen sich einfach vom Client aus, der gerade gestartet ist, mit der gül-

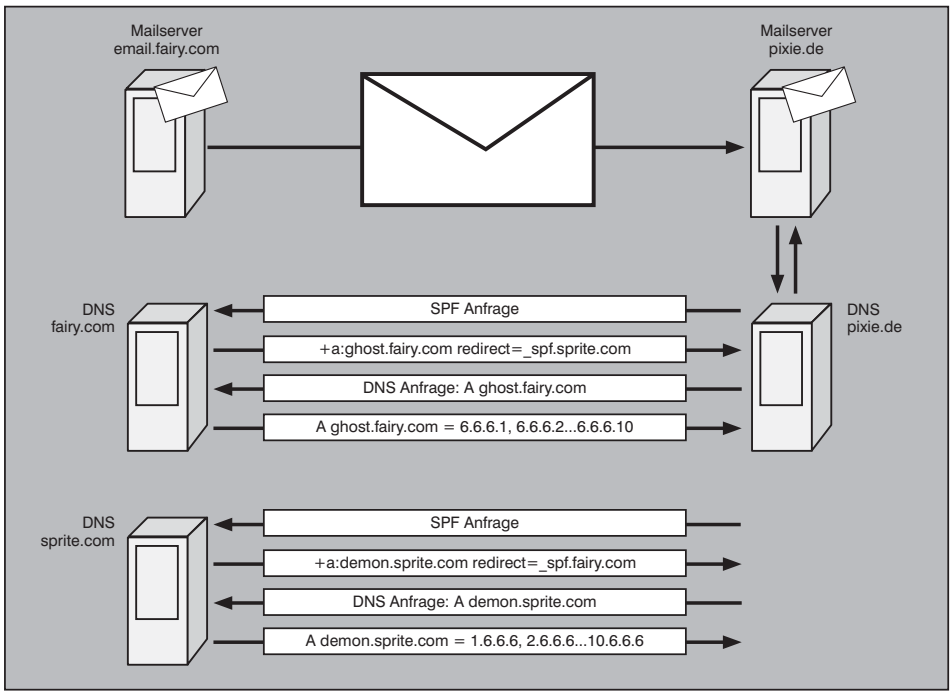


Abbildung 27: SPF - DoS-Attacke mittels redirect

tigen (!) Absendeadresse des aktuellen Benutzters.

Für die beiden auf Signaturen basierenden Vorschläge zusätzlich noch: **emails können nicht mehr verfälscht werden.** S/MIME und PGP sind schon lange im Einsatz, und mails, die einen Inhalt haben, der vor Verfälschungen sicher sein soll, können so geschützt werden.

Phishing-Attacken der heutigen Machart werden schwerer. Stimmt, signalisiert das Email Programm, dass der angebliche Absender mit dem wahren Absender nichts zu tun hat, werden viele wohl vorsichtiger sein, einfach ihre Kontodaten auf einer Seite einzutippen, die aussieht wie die ihrer Bank. Es besteht jedoch zu befürchten, dass die kriminelle Energie ebensolcher Subjekte (Krimineller) ausreichen wird, andere Wege aufzutun.

Fazit

Das SPF ist, verglichen mit den beiden anderen Verfahren, schon weit verbreitet. Viele Domainen-Anbieter und einige Email-Provider nutzen es bereits. Zumindest stellen sie ihren Kunden entsprechende DNS Einträge zur Verfügung oder nehmen sie gleich selbst vor. Auch bei der Software der MTAs und spezialisierter SPAM-Bekämpfungsapplikationen können Plug-Ins erworben werden, bzw. Zusatzprogramme installiert werden. Der Siegeszug des SPF wird wohl kaum aufzuhalten sein. Ob sich auch der jüngere Bruder, SenderID, durchsetzten wird, bleibt hingegen abzuwarten.

Auch dem Domainkey-Verfahren räumt der Autor realistische Chancen ein sich zu verbreiten. Das Verfahren ist verglichen mit dem Cisco-Vorschlag einfacher zu beherrschen und geht weiter als SPF, das gerade bei der Überprüfung der bei Clienten angezeigten Adressen schwere Mängel aufweist: es ist immer noch möglich, eine gefälschte From/Sender Adresse zu benutzen und trotzdem den SPF Test zu bestehen. Das wird durch die DomainKeys zwar nicht unmöglich, jedoch erschwert.

Doch auch das IIM sollte nicht leichtfertig unter den Tisch gekehrt werden. Die Entwickler des DomainKey-Verfahrens schreiben selbst, dass sie zunächst mit der einfachen Variante anfangen wollen und gedenken später Erweiterungen einzuführen, beispielsweise für Userautentifizierungen. Hier könnte die Stunde des IIM schlagen und eine große Anzahl von Ideen in das DomainKey-Verfahren in kompatibler Weise einfließen.

Allen Verfahren gemeinsam ist jedoch das Vertrauen auf ein funktionierendes und korrektes DNS, hieran kranken alle. Da sich hinter SPAM starke finanzielle Interessen verbergen, ist zu befürchten, dass die Angriffe auf das DNS zunehmen könnten. Einer weltweiten Einführung der schon lange existierenden Security Extensions des DNS sollte ein positiver Nebeneffekt der neuen SPAM-Schutz-Mechanismen sein.

Summa Sumarum:
Es wird kommen, es wird Arbeit machen, es wird wenig bis gar nichts bringen, höchsten im Bereich Phishing.

Frage ist: wird sich ein Standard durchsetzen, oder werden wir bald mehrere unterstützen müssen?

Abkürzungen

A	Eintrag im DNS, der einen Namen in eine IP Adresse umwandelt
AH	Authentication Header (Protokoll aus der IPsec-Suite, das die Sicherstellt, dass die übertragenen Daten nicht geändert wurden ohne die Daten selbst zu verschlüsseln)
CRLF	carriage return, line feed (Zeichenfolge, die das Zeilenende kennzeichnet)
DNS	Dynamic Name System
FQDN	Full Qualified Domain Name
IETF	Internet Engeneer Task Force
IIM	Identified Internet Mail (Ciscos Vorschlag zur Senderüberprüfung)
IP	Internet Protocol
IPsec	Sicherheitserweiterungen zum IP Protokoll
ISP	Internet Service Provider
KISS	Keep it simple and stupid
KRS	Key Registration Server (Server, der die öffentlichen Schlüssel zur Mailauthentifizierung beim IIM Verfahren verwaltet)
MDA	Mail Delivery Agent (Zustellfunktion vom empfangenden Mailserver an die Mailbox)
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent (Mailserverfunktion für den Versand und Emfang von Mails zuständig)
MUA	Mail User Agent (kurz: ein Mailprogramm)
MX	Mail Exchanger (DNS Eintrag, der die Mailempfänger einer Domain spezifiziert)
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PRA	Purported Responsible Address (vorgeblich verantwortliche Adresse)
PTR	Pointer Record (Rückwärsauflösung im DNS, löst eine IP Adresse zu einem Namen auf)
RFC	Request for Comment, Standarddokument der IETF
RR	Resource Record (Eintragstyp im DNS)
RSA	Rivest-Shamir-Adelman (asymmetrisches Verschlüsselungsverfahren, benannt nach seinen Erfindern)
S/MIME	Secure MIME
SHA	Secure Hash Algorithm (kryptographisches Hash-Verfahren)
SMTP	Simple Maile Transfer Protocol (Sendeprotokoll für Emails)
SPAM	eigentlich: Spaced Ham, heute als Ausdruck für unerwünschte Mails genutzt
SPF	Sender Policy Framework
TCP	Transport Control Protocol
TXT Record	Eintrag im DNS der nach DNS Standard Freitext enthalten kann, der nicht für das DNS selbst benötigt wird
UDP	User Datagram Protocol
URL	Uniform Resource Locator

CCNE

ComConsult Certified Network Engineer

Lokale Netze
25.04. - 29.04.05 in Aachen
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
14.11. - 18.11.05 in Bonn

Internetworking
06.06. - 10.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Ethernet Technologien - neuester Stand
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
11.04. - 15.04.05 in Aachen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
25.04. - 29.04.05 in Bonn
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
30.05. - 01.06.05 in Köln
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
18.04. - 22.04.05 in Aachen
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 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 5444632
Fax: 0064 3 5444237

German Hotline 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