Nationale Initiative für Internet- und Informations-Sicherheit

21. September 2010, Darmstadtium Darmstadt

Sichere elektronische
Kommunikation

Agenda Sichere elektronische Kommunikation

9:30 - 10:00	Registration
10:00 - 10:15	Begrüßung und Einführung in das Thema
10:15 - 11:00	E-Mail und dessen Sicherheit (Hr. Gärtner, NIFIS)
11:00 – 11:45	Lösung der Bundesregierung zur sicheren elektronischen Kommunikation (Dietrich, BMI)
11:45 - 12:30	Mittagspause (Imbiss und Diskussionsmöglichkeit, Raum „dynamicum“)
12:30 – 13:15	Rechtliche Implikation von De-Mail (Dr. Lapp, NIFIS)
13:15 – 14:00	De-Mail und Standards (Hr. Kammerer, regify AG)
14:00 - 14:45	De-Mail als Lösungsansatz für die sichere elektronische Kommunikation (Hr. Heyde, secunet)
14:45 - 15:00	Kaffeepause
15:00 - 15:45	Podiums-Diskussion mit MdB, NIFIS und den Tagesreferenten

Nationale Initiative für Internet- und Informations-Sicherheit

E-Mail und dessen Sicherheit, Bestandsaufnahme

Mathias Gärtner, NIFIS e.V.
Öffentlich bestellter und vereidigter Sachverständiger IT

Agenda

- E-Mail als Kommunikationsmittel
- Geschichte der E-Mail
- Wie funktioniert E-Mail
- E-Mail Probleme
- Lösungsansätze zur Sicherung
- Fazit

E-Mail als modernes Kommunikationsmittel

E-Mail als Kommunikationsmittel

- E-Mail löst den klassischen Brief als Offline-Kommunikationsmittel ab
- E-Mail ist einfach zu bedienen und kostengünstig
- Durch Zusätze wie z.B. Groupware kann E-Mail zu einem umfassenden Kommunikations- und Archivsystem werden

- E-Mail ist heute nicht mehr wegzudenken! Trend geht aber bei jungen Leuten weg von E-Mail, hin zu Social Network-Messages

Geschichte der E-Mail

Geschichte der E-Mail

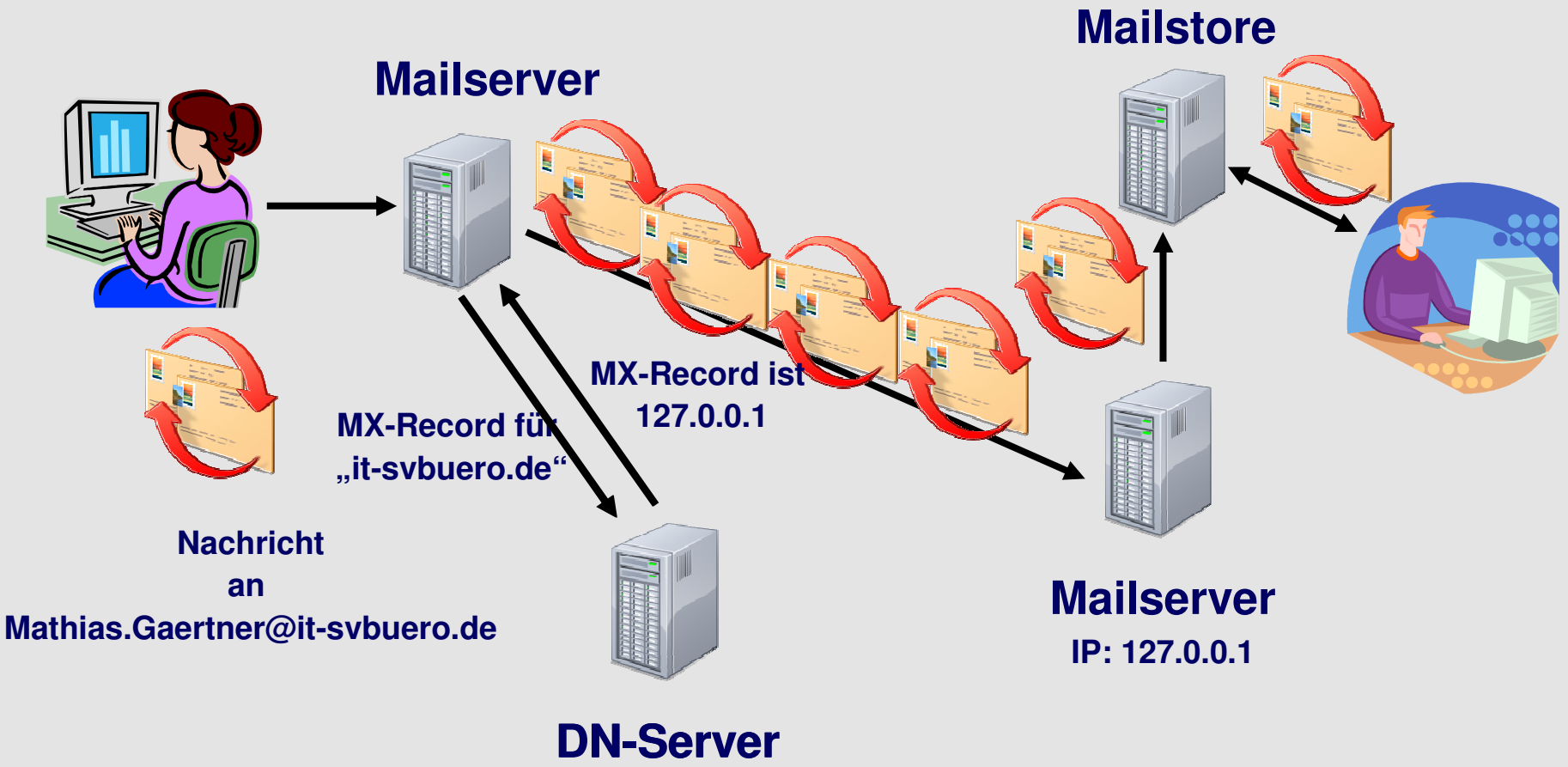
- Erste Textnachricht mit E-Mailadressformaten 1971
- Langsame Verbreitung, erste Standarisierung 1977, Protokoll SMTP (SimpleMailTransportProtocol) eingeführt
- Allgemeingültiger Standard 1982
- 1984 erste E-Mail in Deutschland
- Ca. 1,5 Milliarden E-Mail jährlich verschickt (immer noch per SMTP)
- Davon ca. 80% SPAM (unerwünschte Werbung)

Wie funktioniert E-Mail?

Wie funktioniert E-Mail

- E-Mail basiert auf einem Client-Server Prinzip
- Beteiligte Systeme:
  - E-Mail Storage-Server, auch POP-, IMAP-Server genannt
  - E-Mail Client (Thunderbird, Outlook, Webmail, …)
  - E-Mail Server (mind. einer)
  - Netzwerkinfrastruktur (Router, Switche, WLAN, Kabel, Verteiler usw.)
- DNS (Domain-Name-Server)
- SPAM- und Viren-Filter (optional)

E-Mailtechnik



E-Mail Probleme

E-Mail Probleme

- Neben technischen Probleme hauptsächlich:

- Identitätsproblem, wer hat die E-Mail gesendet
- Empfangsproblem, ist die E-Mail angekommen
- Sicherheitsproblem, wer kann mitlesen

Identität

- Jede E-Mail hat einen Absender. Sobald die E-Mail „unterwegs“ ist, ist dieser nicht ohne weiteres veränderbar
- Aber: Vor dem Absenden kann eine beliebige Adresse angegeben werden
- Über Headerdaten kann man den Weg zwar verfolgen, aber nur begrenzter Beweiswert

- -> Absender einer E-Mail bleibt unbekannt

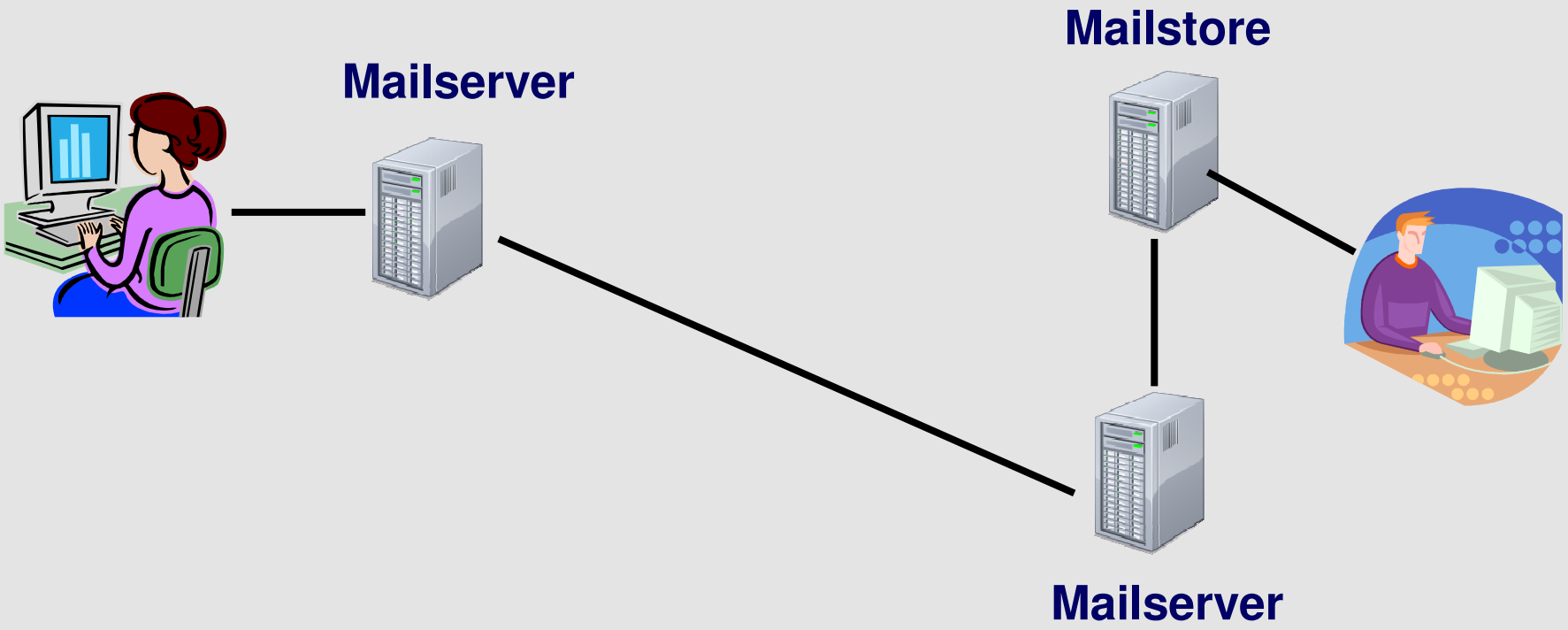
Empfangsbestätigung

- E-Mail kennt kein Einschreiben
- Es ist möglich eine Empfangsbestätigung anzufordern, wenn
  - Die E-Mail im Empfängerpostfach angekommen ist oder
  - Die E-Mail vom Benutzer (bzw. seinem E-Mailclient) aufgerufen wurde
- Eine Kenntnisnahme ist damit nicht garantiert
- Empfänger kann Empfangsbestätigungen verweigern (explizit oder implizit)
- -> Es gibt keine sichere Methode den Empfang bestätigt zu bekommen

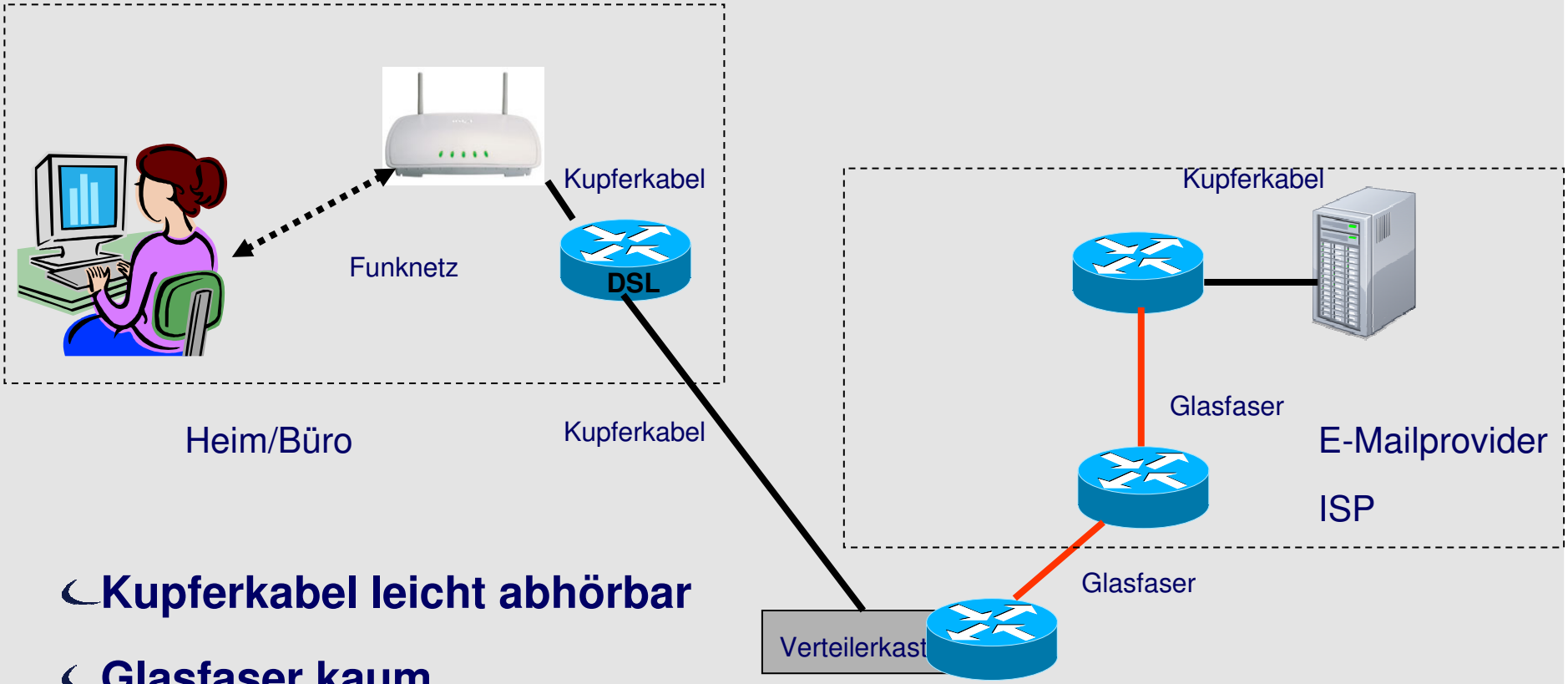
Sicherheit

- E-Mail ist generell unverschlüsselt und wird im Klartext übertragen (E-Mail als Postkarte)
- Vertraulichkeit ist daher nicht vorhanden
- Veränderungen des Inhalts jederzeit möglich (auch nachträglich beim Empfänger, z.B. mit Outlook!)
- Aber: Keine Sicherheitseinstufung OHNE Eintrittswahrscheinlichkeit sinnvoll

Sicherheit

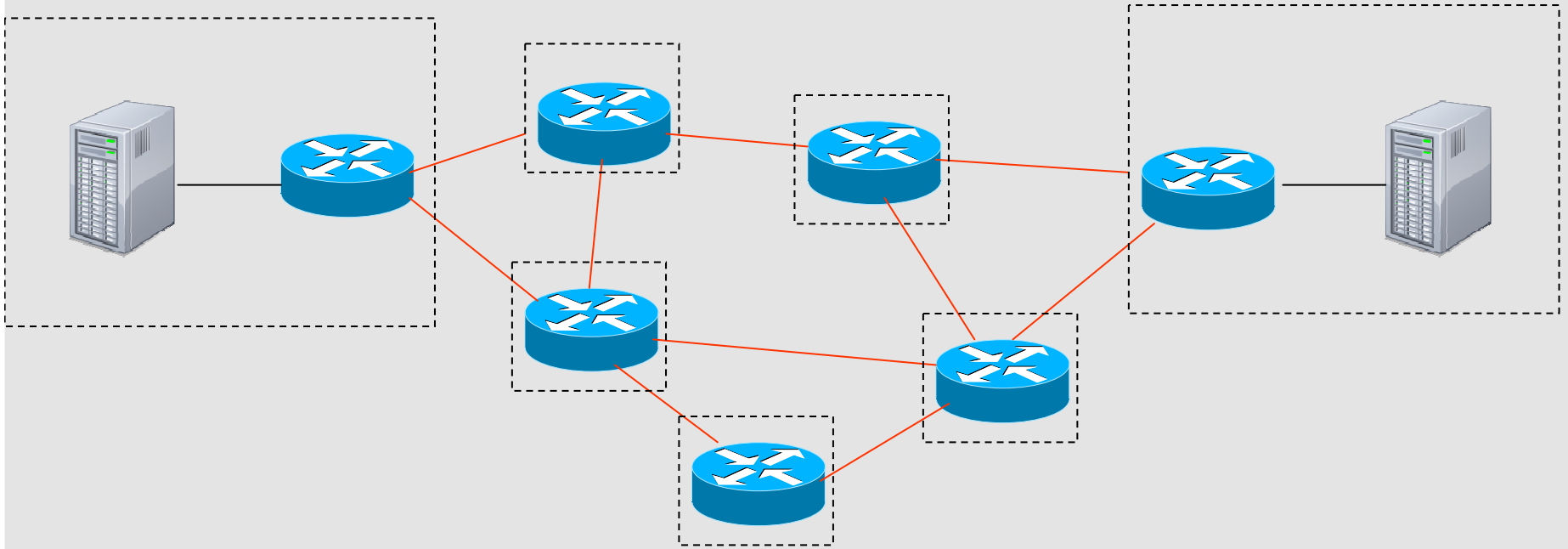


Sicherheit: Strecke zwischen Absender und 1. Server



- Kupferkabel leicht abhörbar
- Glasfaser kaum
- Providerbereich nach §109, I, Satz 2 TKG gesichert

Strecke zwischen den Mailservern



- Alle aktiven Geräte sind im gesicherten Bereich
- Glasfaserleitung im öffentlichen Raum
- Ggf. Verstärker im gesicherten, aber öffentlichen Raum

Sicherheit von E-Mail

- E-Mails grundsätzlich abhörbar
- Ohne extremen Aufwand nur bei dem/den Providern mit Insider-Hilfe möglich
- Öffentlich verlaufende Leitungen schwer abhörbar (Glasfaser)
- Beste Angriffspunkte:
  - Rechner des Absenders
  - E-Mailstore
  - E-Mailserver (kurzes Zeitfenster)
  - Kommunikationsinfrastruktur, nicht ohne Insiderzugriff
- **Trojaner oder Social Engineering das weitaus größere Risiko, die Infrastruktur nicht**

Lösungsansätze

Lösungsansatz Identität

- Nutzung von Signaturen auch für Standard-Email. Bei einer qualifizierten Signatur ist Absender hinreichend (§126a BGB) identifiziert

- Aber: Eher problematisch, da es kaum E-Mailclients mit gesicherter Schnittstelle zur Signaturkarte gibt
- Handhabung eher umständlich (Softwarewartung, zusätzliche Hardware)

Lösungsansatz Empfangsbestätigung

- KEINE bekannte bzw. funktionale

Lösungsansatz Sicherheit

- Einführung von Verschlüsselung
  - Mit PGP recht einfach
  - Mit Signaturkarten etwas aufwendiger
- Verschlüsselung löst NICHT das Trojanerproblem, nur die Sicherung des Transportweges und der ist nicht sehr unsicher
- Verschlüsselung funktioniert End-to-End, d.h. nur der Empfänger kann die E-Mail entschlüsseln
- Verschlüsselung löst auch das Integritätsproblem, Veränderungen ohne Auflösung der Verschlüsselung nicht möglich

Fazit

Zusammenfassung & Fazit

- Die Sicherheit von E-Mail ist besser als ihr Ruf
- Empfangsbekenntnis nicht vorhanden
- Identität des Absenders nur mit (erheblichen) Zusatzaufwand erreichbar
- Das verwendete SMTP-Protokoll adressiert KEINES der drei genannten Probleme

Vielen Dank für Ihre Aufmerksamkeit!

Mathias Gärtner
Tel: 069/40 80 93 70
E-Mail: Mathias.Gaertner@nifis.de

Weitere Informationen unter www.nifis.de