Überraschende Angriffsvektoren: Weit verbreitet, oft übersehen

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
http://www.redteam-pentesting.de

CeBIT 2009
CeBIT Open Source Forum
06. März 2009, Hannover

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Über diesen Vortrag

- Beispiele aus der Praxis
- Überraschende Schwachstellen resultierend aus falschen Annahmen
- Häufige Denkfehler:
  - „Das kann/macht doch keiner...“
  - „Da schützt uns doch...“
  - „Das kann ich besser...“
  - „Das ist ja einfach...“

„Das kann doch keiner“: DECT abhören

- ★ DECT-Telefone sind weit verbreitet
- ★ Abhören in der Praxis trivial (Hardwarekosten 20 Euro)
- ★ `http://www.dedected.org`

„Das kann doch keiner“: DECT abhören

DECT FORUM Statement:

The DECT Forum also states that it is a criminal act to eavesdrop telephone conversations. It is impossible to accidentally eavesdrop on telephone conversations and therefore the risk for users is very low. Only those with a clear criminal energy and intent and a sophisticated knowledge would be capable of eavesdropping.

(DECT Forum: http://www.dect.org/news.aspx?id=41)

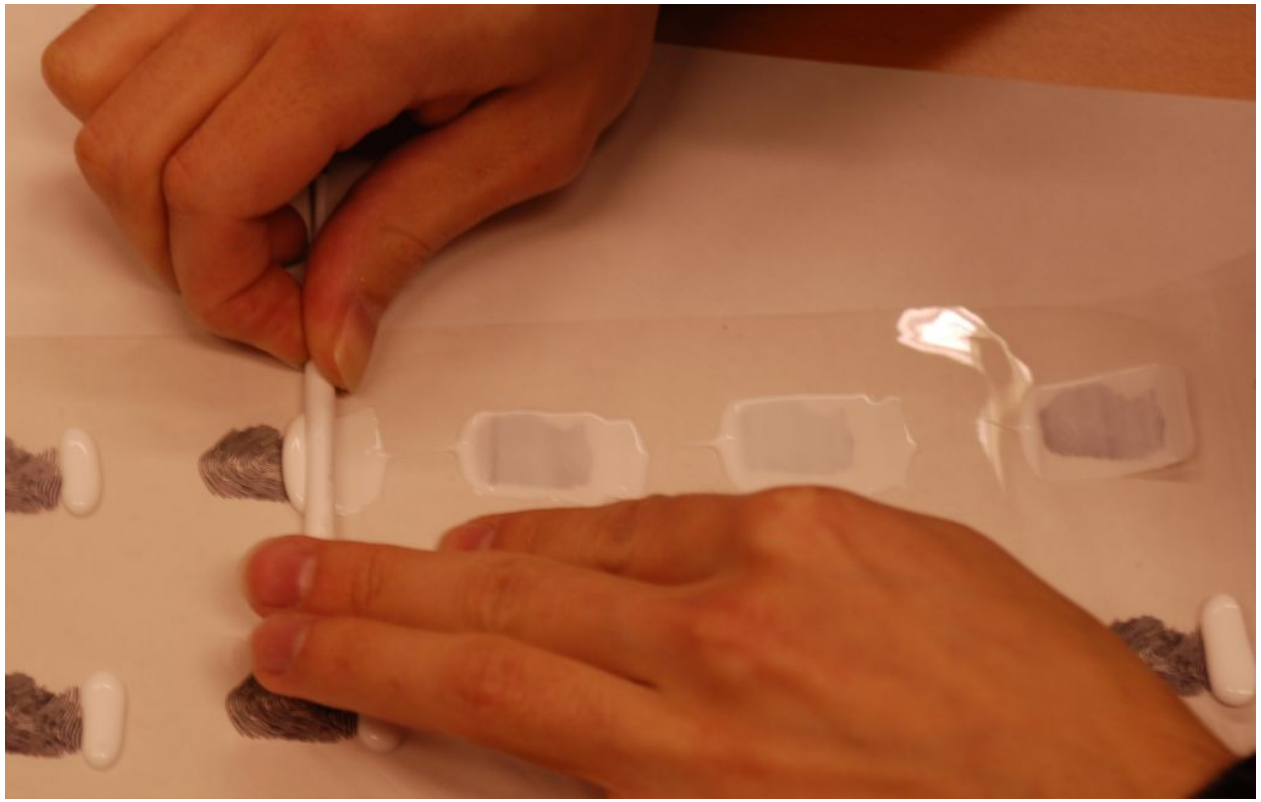
Definition Biometrie

Biometrie

[. . .] Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika.

(Wikipedia)

„Das kann doch keiner“: Fingerabdrücke



„Das kann doch keiner“: Fingerabdrücke

„Da schützt uns doch“: Policies

- ★ PC mit sensiblen Daten
- ★ Policy: Keine Kopien von Daten, kein Netzwerk, keine Schnittstellen für externe Geräte

„Da schützt uns doch“: Policies

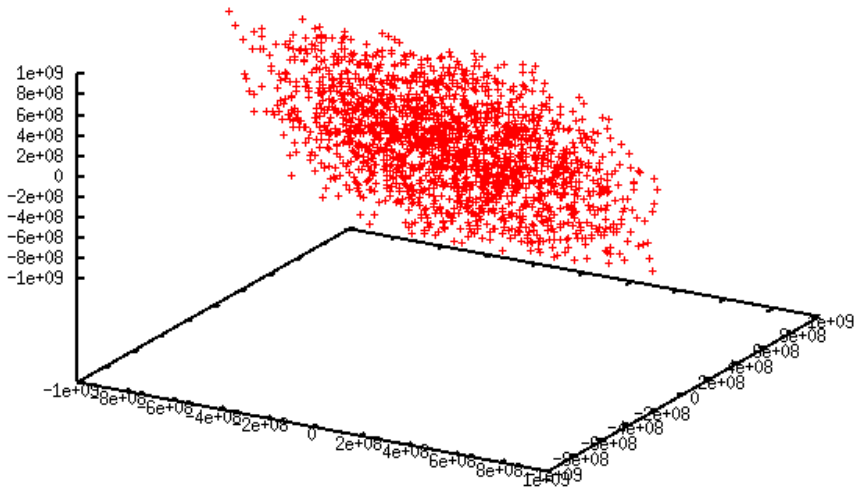
- ★ PC mit sensiblen Daten
- ★ Policy: Keine Kopien von Daten, kein Netzwerk, keine Schnittstellen für externe Geräte
  ⇒ Pentester benutzen Fotokamera für „Screenshots“
- ★ Lediglich ein anwesender Mitarbeiter im Raum ruft scherzhaft „Security“

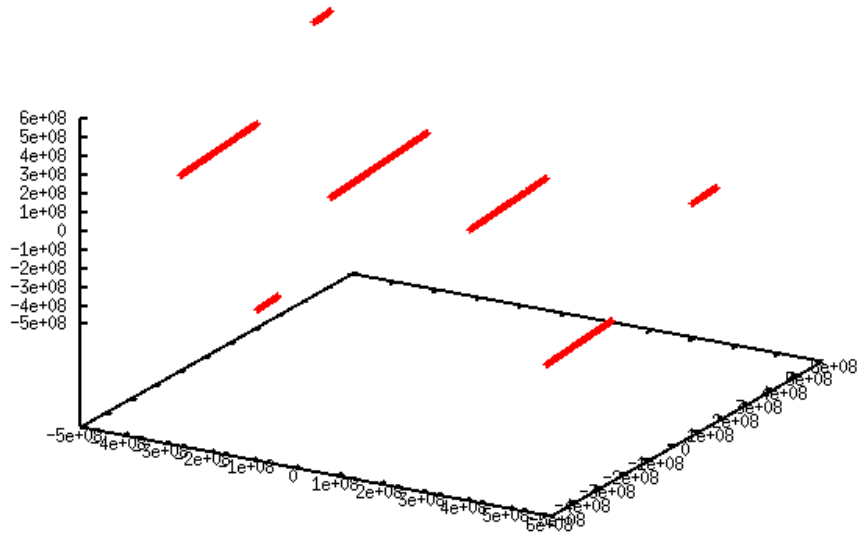
„Da schützt uns doch“: Add-On Security

„Da schützt uns doch“: Add-On Security

„Da schützt uns doch“: Skimming

„Das kann ich besser“: Zufall





„Das kann ich besser“: Passwortprüfung

Best Practice Passwortsicherheit

- ★ Passwörter nicht im Klartext speichern ⇒ Hash
- ★ Passwörter haben mindestens acht Zeichen

„Das kann ich besser“: Passwortprüfung

Best Practice Passwortsicherheit

- ★ Passwörter nicht im Klartext speichern ⇒ Hash
- ★ Passwörter haben mindestens acht Zeichen

Praxis Passwortsicherheit

Software speichert acht Zeichen des Hashes:

```
password = 381ca10f1a7ddf0c76e615e971ca0183
password =         1a7ddf0c
```

„Das kann ich besser“: Security by Obscurity

- ★ Propritäres Netzwerkgerät (Windows basierend)
- ★ Verschlüsselte Festplatte, Verschlüsselter Netzwerkverkehr. AES256.
- ★ Gerät bootet und arbeitet ohne Benutzerinteraktion

„Das kann ich besser“: Security by Obscurity

- ★ Propritäres Netzwerkgerät (Windows basierend)
- ★ Verschlüsselte Festplatte, Verschlüsselter Netzwerkverkehr. AES256.
- ★ Gerät bootet und arbeitet ohne Benutzerinteraktion

Frage: Wo sind die geheimen Schlüssel?

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.
- ★ Anschließend startet mehrmals das Programm `.reg.dat`

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.
- ★ Anschließend startet mehrmals das Programm `.reg.dat`
- ★ was de facto TrueCrypt ist

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.
- ★ Anschließend startet mehrmals das Programm `.reg.dat`
- ★ was de facto TrueCrypt ist
- ★ und verschiedene, kryptisch benannte Dateien (`8zui72rec.dat`, `8zui72tas.dat`, ...) mit einem 50-Zeichen-Passwort per Kommandozeile entschlüsselt

„Das kann ich besser“: Security by Obscurity

Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.
- ★ Anschließend startet mehrmals das Programm `.reg.dat`
- ★ was de facto TrueCrypt ist
- ★ und verschiedene, kryptisch benannte Dateien (`8zui72rec.dat`, `8zui72tas.dat`, ...) mit einem 50-Zeichen-Passwort per Kommandozeile entschlüsselt
- ★ Die Dateien enthalten die eigentliche Anwendung in dem Verzeichnis (`\.private\OS\Win32\bin\.plugins\lib\`)

„Das kann ich besser“: Security by Obscurity

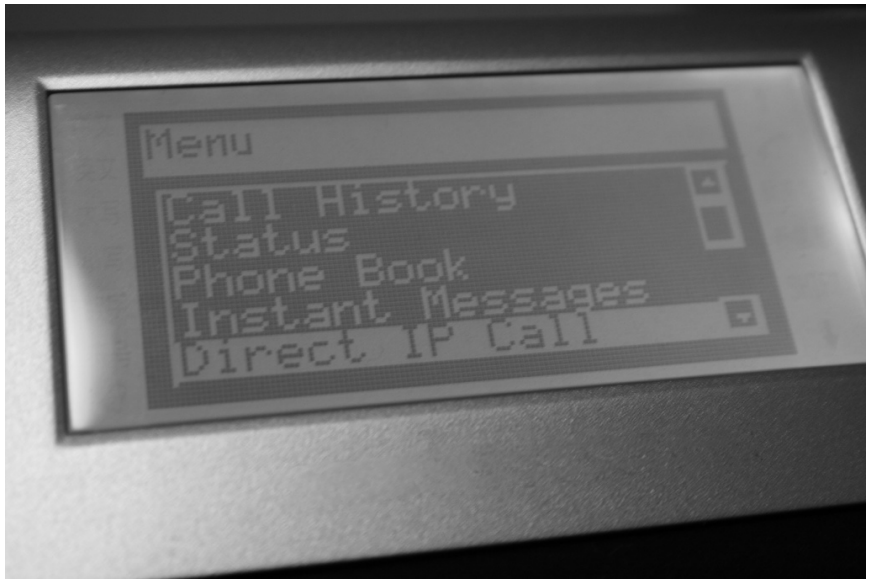
Der Boot Prozess:

- ★ Windows startet, startet `run1.exe`,
- ★ kopiert verschiedene verschleierte Dateien in `\cache`.
- ★ Anschließend startet mehrmals das Programm `.reg.dat`
- ★ was de facto TrueCrypt ist
- ★ und verschiedene, kryptisch benannte Dateien (`8zui72rec.dat`, `8zui72tas.dat`, ...) mit einem 50-Zeichen-Passwort per Kommandozeile entschlüsselt
- ★ Die Dateien enthalten die eigentliche Anwendung in dem Verzeichnis (`\.private\OS\Win32\bin\.plugins\lib\`)
- ★ Diese Anwendung enthält die gesuchten geheimen Schlüssel, die mittels Debugger schließlich extrahiert werden können

„Das ist ja einfach“

- ★ Soft- und Hardware ist heute sehr einfach in Betrieb zu nehmen
- ★ Die Sicherheit wird hierbei oft vergessen, noch geschürt von falschen „Tipps“ im Web

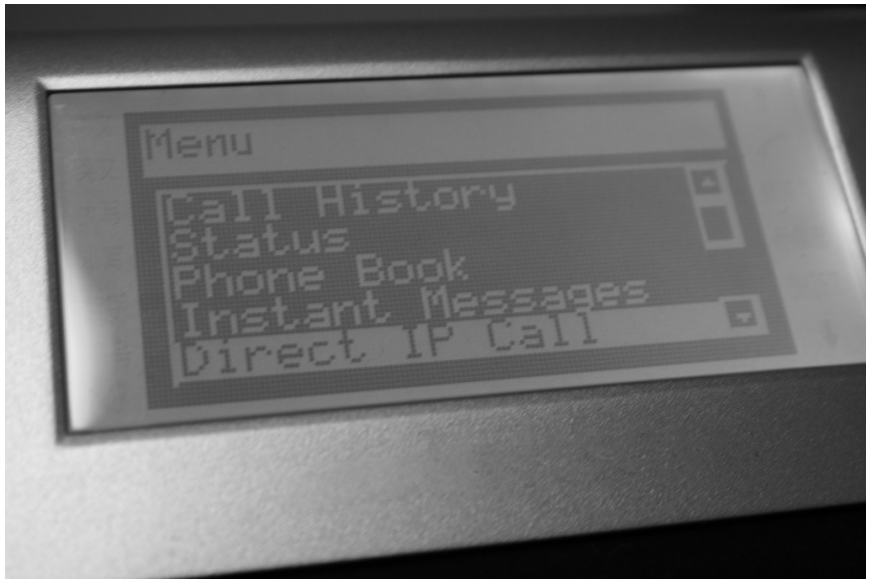
„Das ist ja einfach“: Voice over IP



 Jean-Etienne Poirrier

„Das ist ja einfach“: Voice over IP

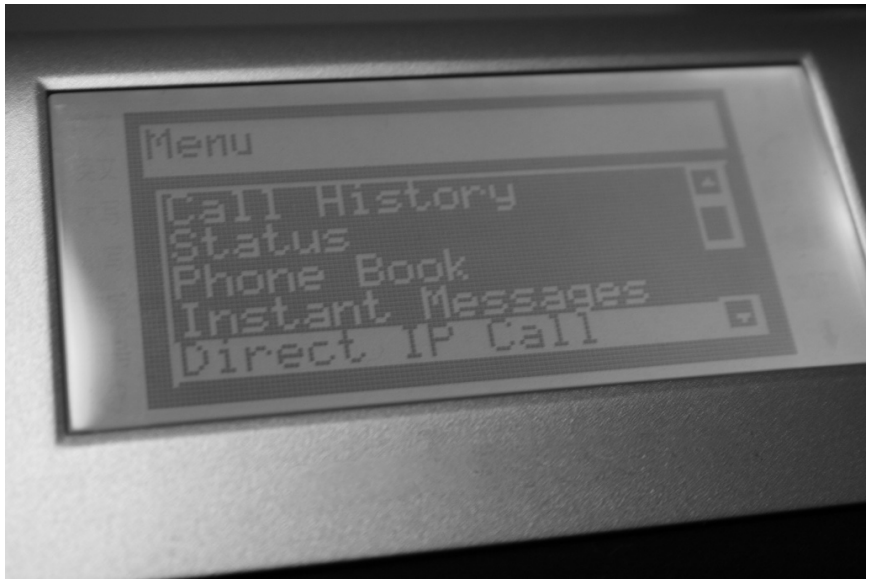
- ★ Abspielen von Audio-Dateien



 Jean-Etienne Poirrier

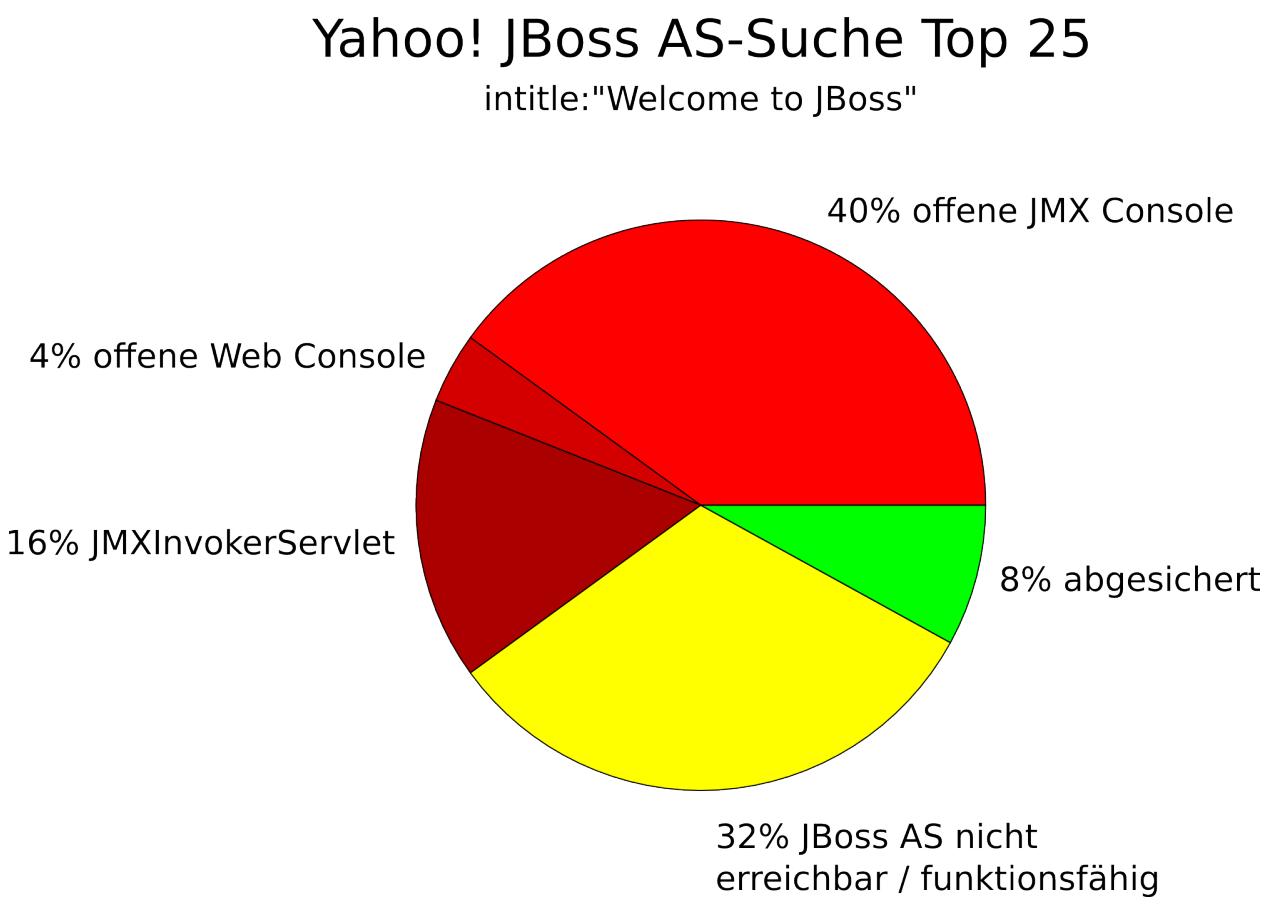
„Das ist ja einfach“: Voice over IP

- Abspielen von Audio-Dateien
- Fernsteuerung der Bedienelemente
  - Umleiten von Telefonaten
  - Abhören per Konferenzschaltung
  - Raumüberwachung



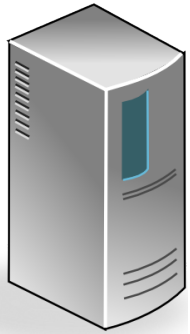
 Jean-Etienne Poirrier

„Das ist ja einfach“: JBoss AS



„Das ist ja einfach“: Authentifizierung

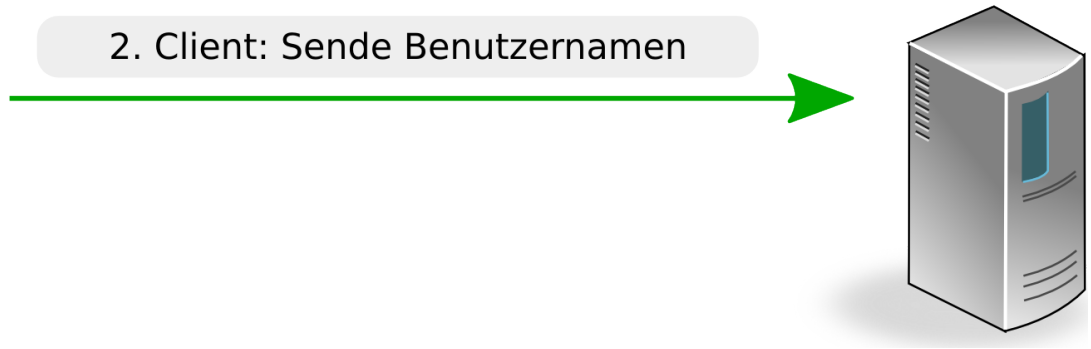
1. Client: Eingabe Name/Passwort



„Das ist ja einfach“: Authentifizierung

1. Client: Eingabe Name/Passwort

2. Client: Sende Benutzernamen

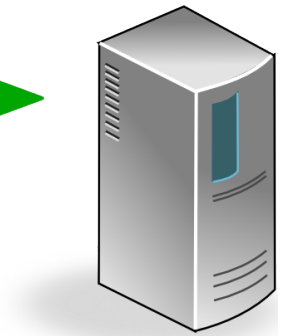


„Das ist ja einfach“: Authentifizierung

1. Client: Eingabe Name/Passwort

2. Client: Sende Benutzernamen

3. Server: Sende Passwort zum Namen



4. Client: Vergleiche Passwörter

Fazit

- ★ Viele Fehler basieren auf falschen Annahmen
- ★ Prüfen Sie immer kritisch, welche Annahmen für ein System (implizit) getroffen wurden

Fazit

- ★ Viele Fehler basieren auf falschen Annahmen
- ★ Prüfen Sie immer kritisch, welche Annahmen für ein System (implizit) getroffen wurden

$\Rightarrow$ Vermeiden Sie unangenehme Überraschungen!

Fragen?

Vielen Dank für Ihre Aufmerksamkeit