

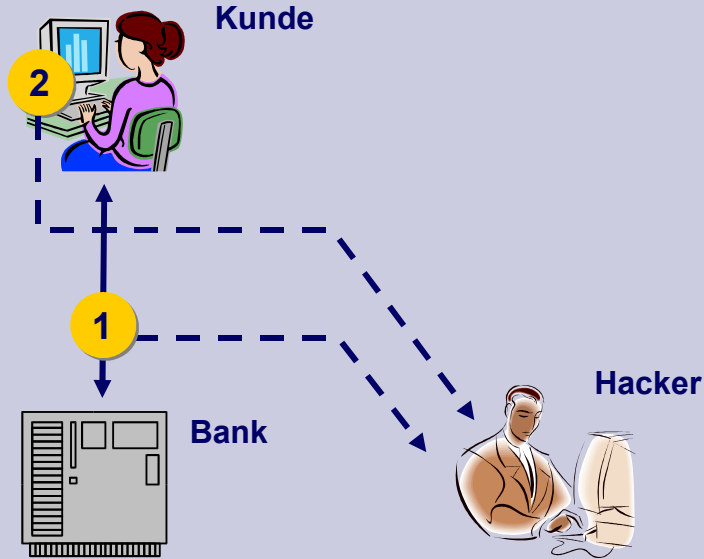


Neue Sicherheit in OnlineBanking-Anwendungen

Köln, 30. Juni 2005

- Phishing, Trojaner und Pharming
- Angreifbarkeit der Kunde-Bank-Kommunikation
- Maßnahmen gegen Hackerangriffe

Hacker-Angriffe: Relevante Varianten



1 Phishing: Hacker lockt Kunden mit Spam-Mail und gibt eigenen Rechner als Bank-Rechner aus

2 Angriff auf Kundenrechner:

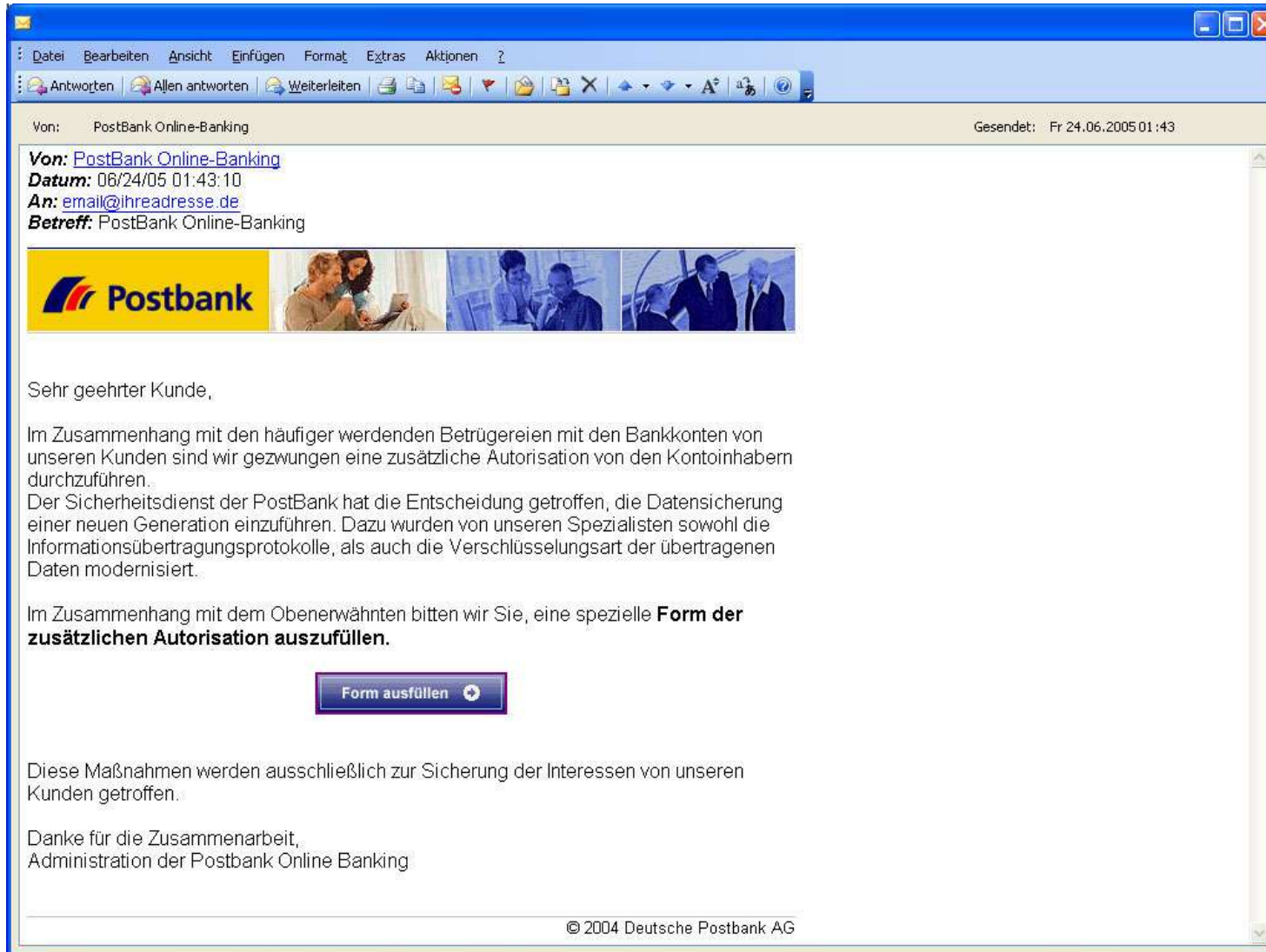
- Trojaner: Lesen Legitimationsdaten auf Kundenrechner aus
- Pharming: Ändert DNS-Eintrag auf Kundenrechner, so dass Zugriff unbemerkt auf Rechner des Hackers erfolgt

Auswirkungen Hacker-Angriffe

Imageverlust der Banken, die ausschließlich PIN/TAN-Banking-Anwendungen anbieten

Erheblicher finanzieller Schaden bei Kunden und Banken

Phishing-eMail im Namen der Postbank



[Sitemap](#)
[Kontakt](#)
[FAQ](#)
[Hilfe](#)

- ▶ Homepage
- Produkte & Preise
 - Service & Kredite
 - Anlegen & Sparen
 - Wertpapiere
 - Versichern & Vorsorgen
 - Baufinanzierung
 - Altersvorsorge
- Online-Services
- Mobile Services
- Vermögensberatung
- Markt & Research
- Presse
- Investor Relations
- Wir über uns
- Karriere

Deutsche Post World Net
 MAIL EXPRESS LOGISTICS FINANCE

Privatkunden

▶ Geschäftskunden

▶ Firmenkunden

Sehr geehrter Kunde,

Die PostBank macht sich Sorgen wegen der Sicherheit von unseren Kunden, darum entwickeln wir ständig neue Sicherheitsmethoden. In der letzten Zeit wurden die Diebstahlversuche der Geldmittel von den Bankkonten regelmäßiger geworden. Das System der Anwendung der TAN-Liste hat sich nicht in vollem Maße bewährt. Die Missetäter haben gelernt mit dieser Schutzart umzugehen. Wir haben äußerst aufmerksam jeden Geldmitteldiebstahlfall von den Konten untersucht und haben somit eine Kriterienliste der verdächtigen Operation zusammengestellt. Gegenwärtig haben wir ein neues elektronisches Schutzsystem, um den Zutritt zu den Bankkonten zu verhindern, das auf der Feststellung von diesen Kriterien basiert, entwickelt und es ist praktisch einsatzbereit. Wenn die Transaktion verdächtig scheint, stellt das System eine Geheimfrage. Wenn es darauf keine Antwort bekommt, so werden laufende Transaktion und Konto, von dem sie gemacht wurde, bis zur Klärung der Umstände blockiert.

Um das System funktionieren zu lassen, bitten wir Sie, die Form der zusätzlichen Autorisation auszufüllen (Achtung! Wir bitten Sie Login und Passwort von Ihrem elektronischen Konto anzugeben).

Name:

Familienname:

Telefon - Nr.:

Kontonummer: (Online-Banking)

PIN:

TAN:

(ACHTUNG! Verwenden Sie bitte zukünftig diese TAN nicht, das führt zur Blockierung vom Konto)

Geheimfrage:

Antwort auf die Geheimfrage:

[OK](#)

Vorsicht vor Betrügern!

Wichtiger Hinweis:
Vorsicht vor gefälschten **Postbank Sicherheits- und Service-eMails!**

So schützen Sie sich gegen Trojaner und erkennen Phishing-mails. Nutzen Sie die **mobile TAN**, die für Betrüger wertlos ist.

Postbank Newsletter

Infos, die sich lohnen!

Ja, ich abonniere kostenlos:

[Postbank Geldwert](#)

[Postbank AnlageWelt](#)

[Postbank Business update](#)

Anrede: Frau Herr

Vorname:

Name:

E-Mail*:

* erforderliche Angabe

[Datenschutz abschicken](#)

Postbank ist nationaler Förderer der FIFA WM 2006™

Ihre Zugangsdaten:

*
Anmeldename, Legitimations-ID
bzw. Konto-Nr.:

* BLZ:

* PIN:

* TAN1:

* TAN2:

Hiermit bestätige ich, dass ich die nachfolgenden Hinweise zur Kenntnis genommen habe und akzeptiere:

- ▶ Nutzungsbedingungen
- ▶ Sicherheitshinweis

- Phishing, Trojaner und Pharming

- **Angreifbarkeit der Kunde-Bank-Kommunikation**

- Maßnahmen gegen Hackerangriffe

Mangelnde Kenntnisse der Mechanismen im Internet

Falsche URL und keine "https"-Verbindung!

Die Postbank fordert Sie niemals dazu auf, auf einer Seite PIN und TAN gleichzeitig anzugeben!

Fehlendes Schloß-Symbol weist auf fehlendes Sicherheits-Zertifikat hin!

Womit Kunden und Banken bisher zu tun hatten

Komplette 1:1-Kopie von Bankseiten

Ähnliche URLs

Gefälschte eMail-Absenderadressen

Was die Zukunft bringen könnte

Gültige HTTPS-Zertifikate

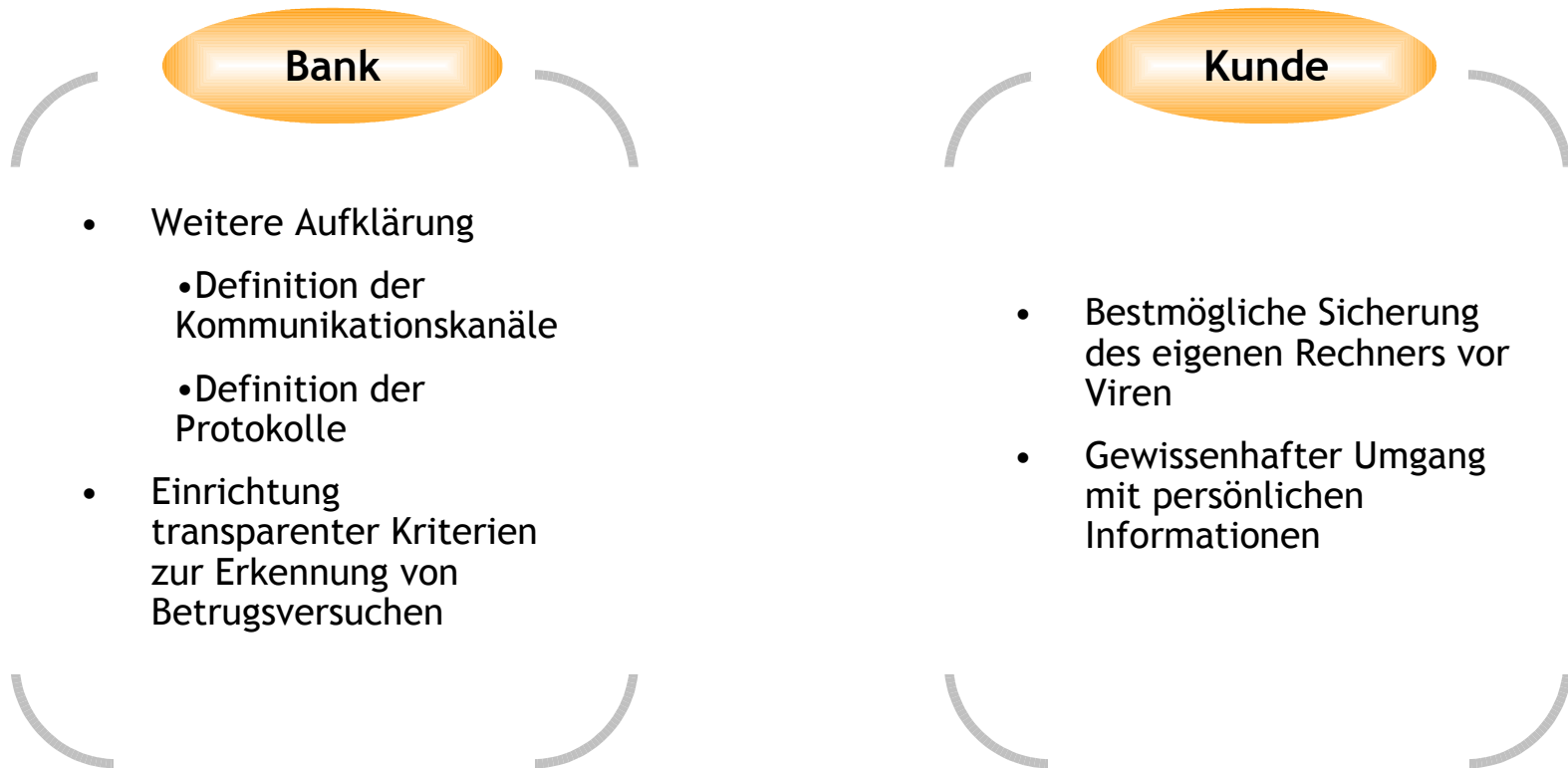
Ähnliche URLs

Intelligente Trojaner und Viren

Man-in-the-Middle-Attacks

- Phishing, Trojaner und Pharming
- Angreifbarkeit der Kunde-Bank-Kommunikation
- Maßnahmen gegen Hackerangriffe

Zusätzliche Sicherung der Kunde-Bank-Kommunikation



Zusätzliche Sicherung des PIN/TAN-Verfahrens

Zweckgebundene TANs

- Gebrauch einer TAN wird für einen bestimmten Zweck reserviert
- Die Kenntnis einer beliebigen TAN genügt i.d.R. nicht mehr, um einen beliebigen Auftrag anzulegen

Beispiele: Indiziertes TAN-Verfahren (iTAN), Mobile TAN-Verfahren (mTAN)

→ Simple Phishing-Attacken werden nicht mehr genügen, da eine beliebige TAN fast wertlos ist.

Alternative Kanäle

- Bank kommuniziert über einen zusätzlichen, schwer manipulierbaren Kanal mit dem Kunden
- Kunde kann über diesen Kanal verbindliche Informationen bei der Auftragsanlage erhalten

Beispiel: Mobile TAN-Verfahren (mTAN) mit zusätzlichem Versand der Auftragsdaten

→ Kunde kann sich vergewissern, dass die erhaltene mTAN für seinen Auftrag generiert wurde.

Indiziertes TAN-Verfahren

Funktionsweise

- Bank liefert dem Kunden TAN-Listen mit eindeutig gekennzeichneten TANs, z.B. laufende Nummern
- Bei der Anlage eines Auftrags wird eine TAN für diesen Auftrag reserviert und die Eingabe der TAN anhand der Kennzeichnung angefordert

Vorteile

- Hacker kann eine beliebig „gephischte“ TAN nicht verwenden
- Hacker weiß nicht, welche TANs bereits verbraucht sind
- Hacker weiß nicht, welche Kennzeichnungen an den TANs existieren

Nachteile

- Bankingsoftware und -protokolle (HBCI+, FinTS 4.0) unterstützen derartige Verfahren nicht
 - Bank bleibt über diese Kanäle angreifbar

Mobile TAN-Verfahren

Funktionsweise

- Bei der Anlage eines Auftrags wird eine mTAN für diesen Auftrag erzeugt und dem Kunde zusammen mit den Auftragsdaten per SMS auf sein Mobilfunktelefon zugestellt

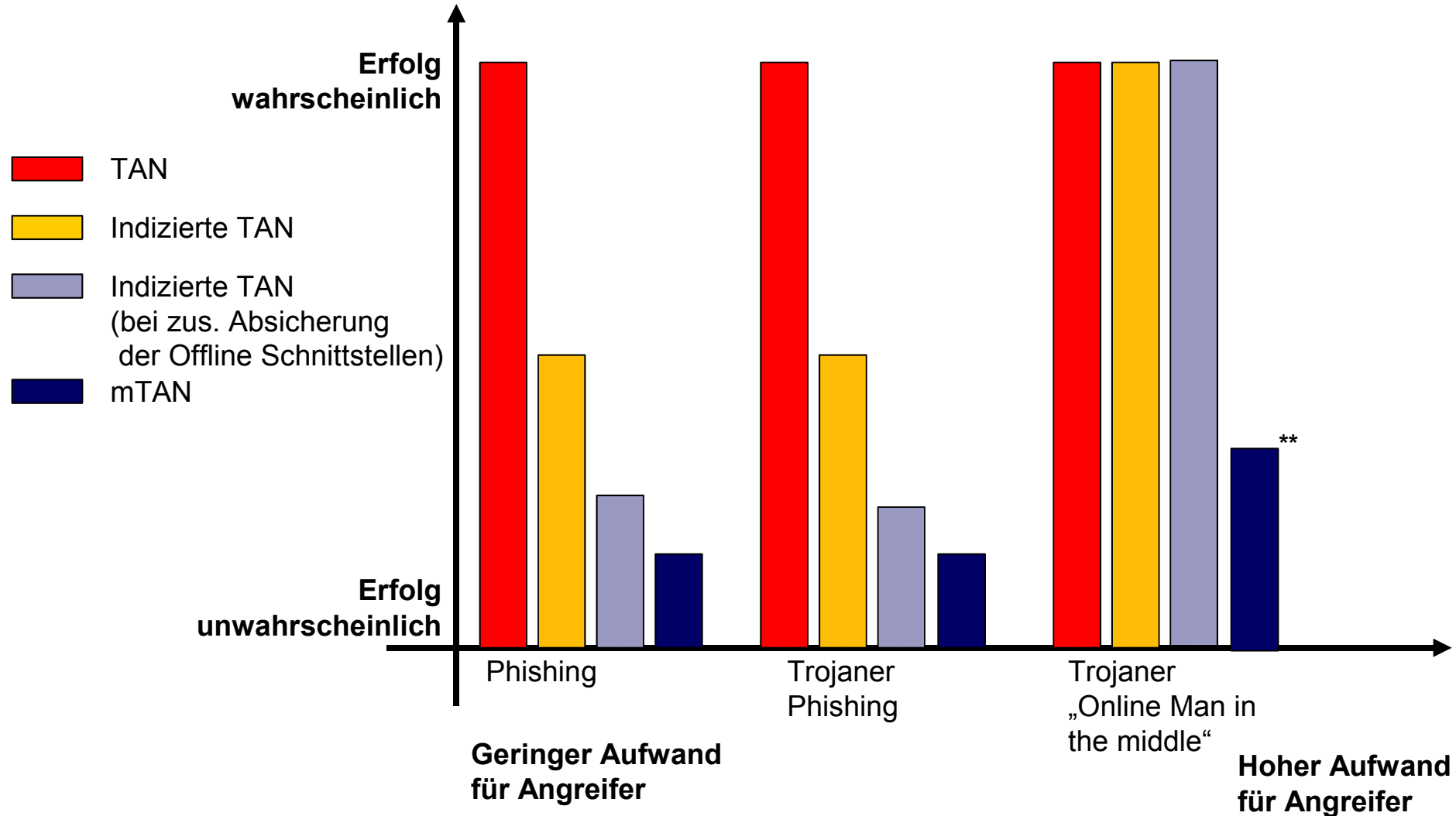
Vorteile

- Hacker kann den Kanal „Mobilfunk“ nur mit sehr hohem technischen Aufwand manipulieren
- Kunde kann in der SMS verifizieren, ob diese mTAN auch tatsächlich für seinen Auftrag gedacht ist
- Wirksames Mittel gegen Man-in-the-Middle-Attacken

Nachteile

- Bankingsoftware und -protokolle (HBCI+, FinTS 4.0) unterstützen derartige Verfahren nicht
 - Bank bleibt über diese Kanäle angreifbar
- Beim Versand entstehen zusätzliche Kosten

Erfolgswahrscheinlichkeit der unterschiedlichen Angriffsszenarien bei den aktuellen Sicherheitsverfahren



* Beurteilung durch Abteilung ISM

** Abhängig vom Kundenverhalten

Vielen Dank für Ihre Aufmerksamkeit

100world AG
Vordere Cramergasse 11
90478 Nürnberg

Tel.: 0911-4244-0
Fax: 0911-4244-100
info@100world.com
www.100world.com

Ihr Ansprechpartner
Timo Weber
timo.weber@100world.com