

# Sicherheit im Online Banking

Ein Vortrag der Sparkasse KölnBonn  
im Rahmen der Informationsveranstaltung „Internet im Handwerk“

Köln, den 02.11.2010

# Inhaltsverzeichnis

- Was heißt Sicherheit im elektronischen Zahlungsverkehr?
  - Datenschutz und -sicherheit
  - Beteiligte und Gefahren
- Schutzmaßnahmen im Online Banking
  - Maßnahmen der Bank
  - Maßnahmen des Nutzers
  - Was tun, wenn?
- Ausblick

# Was heißt Sicherheit im elektronischen Zahlungsverkehr?

- Datenschutz und -sicherheit
- Beteiligte und Gefahren

# Was heißt Sicherheit im elektronischen Zahlungsverkehr?

## Datenschutz und -sicherheit

### Vertraulichkeit der Daten

Die Daten bleiben vor Unbefugten abhörsicher und unbeobachtbar

### Integrität

Vollständige sowie unveränderte Übertragung der Daten

### Authentizität

Der Urheber/Absender ist eindeutig identifizierbar

### Verbindlichkeit

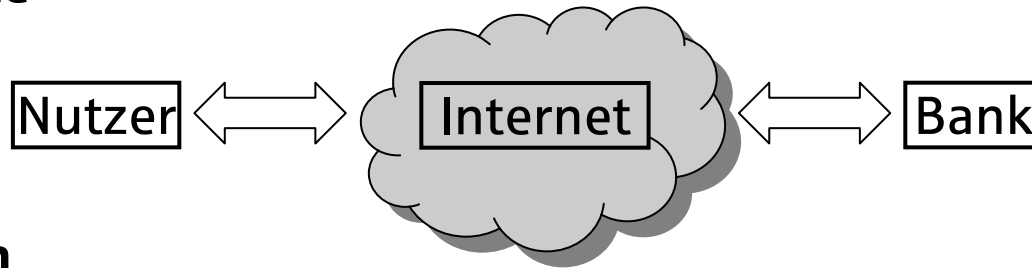
Die Urheberschaft und der Empfang der Daten sind nicht abstreitbar

### Verfügbarkeit

Die Nutzbarkeit der technischen Komponenten ist gewährleistet

# Was heißt Sicherheit im elektronischen Zahlungsverkehr?

## Beteiligte



## Gefahren

### Phishing

Der Versuch, Daten eines Internetnutzers durch E-Mails und gefälschte Webadressen zu bekommen

### Trojaner

Eine Schadsoftware, die ohne Wissen des Anwenders z.B. Informationen an Dritte weiter leitet

### Spoofing

Generell das Vortäuschen einer falschen Identität im Internet mit dem Ziel, Authentifizierungsverfahren zu umgehen

# Schutzmaßnahmen im Online Banking

- Maßnahmen der Bank
- Maßnahmen des Nutzers
- Was tun, wenn?

# Schutzmaßnahmen im Online Banking

## Maßnahmen der Bank

### Datenschutz

Verschlüsselung der Daten  
Firewallsystem  
Virenschutzsystem  
4-Augen-Prinzip  
Verbindliche Arbeitsanweisungen  
für Mitarbeiter

### Datensicherheit

IT-Sicherheitskonzept  
Redundante Auslegung aller  
Komponenten  
Mehrere Standorte  
Backup-Strategie  
Notfallplanung

### darüber hinaus

Bereitstellung mehrstufiger Zugangsdaten (Benutzername + Passwort  
bzw. PIN, iTAN, ChipTAN, smsTAN oder Chipkarte)  
Nachvollziehbarkeit der Kontobewegungen

# Schutzmaßnahmen im Online Banking

## Maßnahmen des Nutzers

### Aktualität der genutzten Systeme

- Virens Scanner / Firewall
- Betriebssystem
- Browser und weitere Anwendungen

# Schutzmaßnahmen im Online Banking

## Maßnahmen des Nutzers

### Verhalten des Anwenders

- manuelle Adresseingabe der Banking-Seiten
- keine Sicherheitsmedien abspeichern / weitergeben
- Sicherheitsmedien persönlich und getrennt aufbewahren
- sichere Kennwörter verwenden
- auf bestimmte Merkmale achten (Rechtschreibfehler)
- niemals PIN oder TAN telefonisch angeben
- niemals mehrere TANs gleichzeitig eingeben
- auf https-Verschlüsselung der Bankingseite achten
- Rechner vor unberechtigtem Zugriff schützen
- keine unbekannte Software installieren

# Schutzmaßnahmen im Online Banking

## Organisatorische Regelungen

- Arbeitsanweisung für Mitarbeiter
- IT Sicherheitskonzept
- Redundante Auslegung aller Komponenten
- Backup-Strategie
- Notfallplanung

## darüber hinaus

Banken werden E-Mails nie nutzen, um sicherheitsrelevante Informationen abzugleichen

# Schutzmaßnahmen im Online Banking

## Was tun, wenn?

- Bei Missbrauchsverdacht Zugangsdaten ändern oder sperren (im Internet-Banking oder durch 3x Passwortfehlingabe)
- Kontakt zur Bank aufnehmen
- Sicherheitsmailadresse der Banken für Phishing-Mails
- PC bereinigen

# Ausblick

## Ausblick

Sicherheitsverfahren werden regelmäßig weiterentwickelt

BTX => PIN/TAN => iTAN => ChipTAN / smsTAN => Signaturkarte => ...

Virenprogramme, Firewalls ... werden täglich aktualisiert

**Banken, Nutzer, Softwarehersteller ... alle sind für die Sicherheit der System mitverantwortlich ... gemeinsam werden sie immer sicherer**

Ihre weiteren Fragen beantworte ich gerne:



**Sparkasse  
KölnBonn**

**Björn Verheyen**  
Dipl.-Informatiker FH  
Referent

Electronic Banking  
Sparkasse KölnBonn  
Adolf-Grimme-Allee 1  
50829 Köln

Telefon 0221 226-58145  
Telefax 0221 212950  
bjoern.verheyen@  
sparkasse-koelnbonn.de