DEUTSCHE BUNDESBANK
EUROSYSTEM

SecuRe Pay: Praktische Auswirkungen für den Internet-Zahlungsverkehr

PaySys Breakfast-Meeting am 4. April 2014

Dirk Schrade, Deutsche Bundesbank

Gründe für das SecurePay-Forum

Sicherheit im Zahlungsverkehr

Handelsblatt

Finanzen | Unternehmen | Politik | Technologie | Auto | Meinung | Sport | Panorama

Industrie | Banken | Versicherungen | Handel + Dienstleister | IT + Medien | Mittelstand | Management | Beruf + Büro

ARTIKEL | KOMMENTIEREN

HACKERANGRIFF

10.01.2014, 18:28 Uhr

Datenverlust bei Target schlimmer als befürchtet

Bis zu 70 Millionen Kunden könnten vom Datendiebstahl beim Großhändler Target betroffen sein. Die Gefahr wächst stündlich. Die Hacker suchen jetzt im Internet Hilfe, um die Daten zu entschlüsseln.

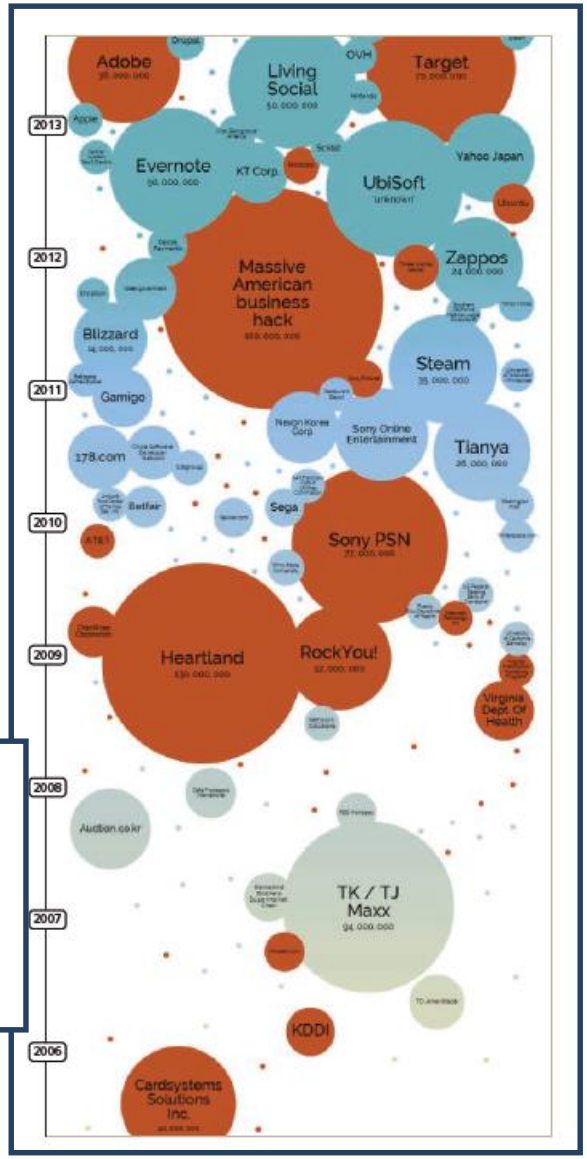
Target-Kunden in New York: Der Schaden durch einen riesigen Datendiebstahl ist noch nicht abzusehen. Aber die Gefahr wächst stündlich.
Quelle: Reuters

SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

HEARING ON

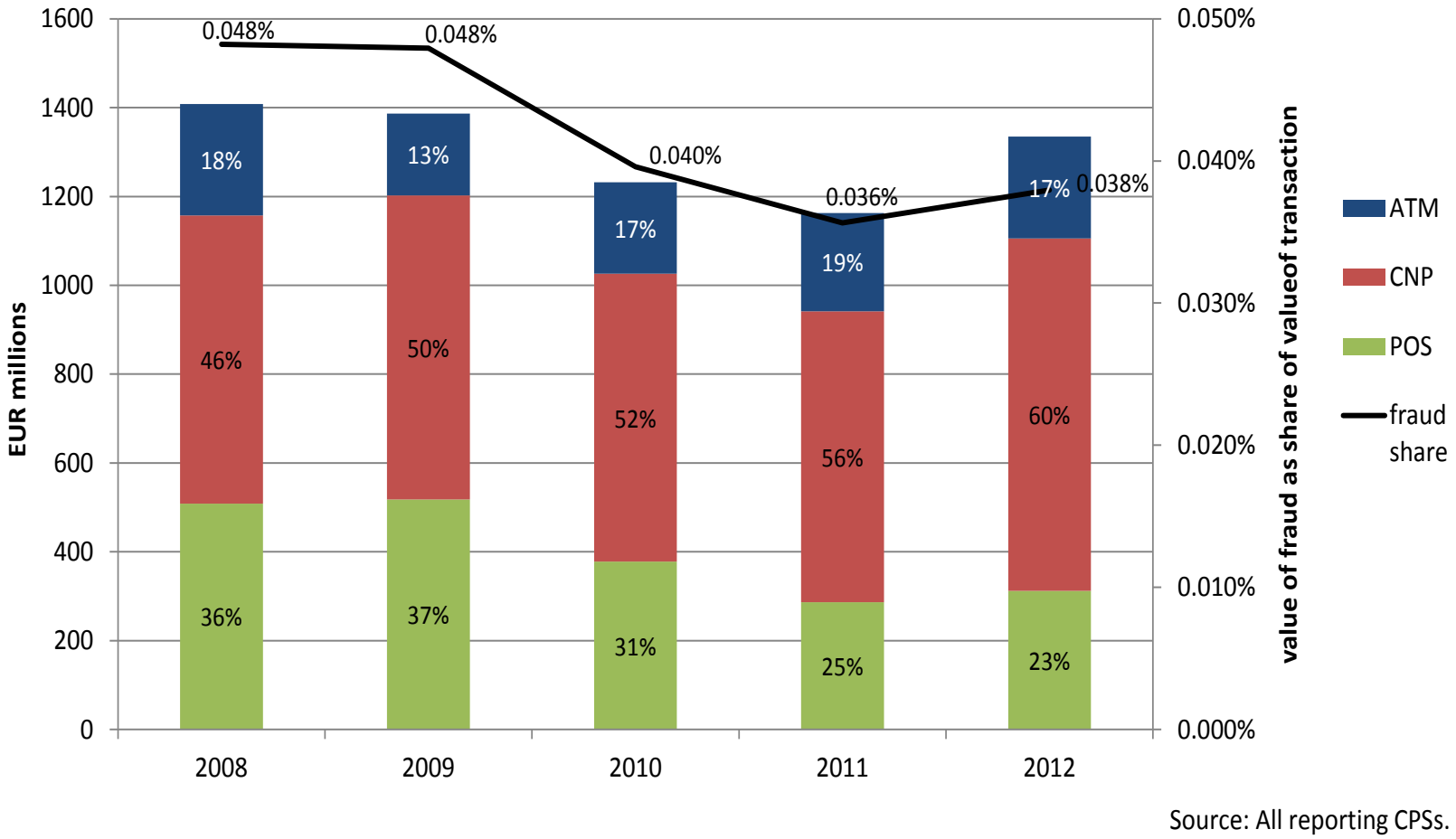
PROTECTING PERSONAL CONSUMER INFORMATION FROM CYBER ATTACKS

AND DATA BREACHES



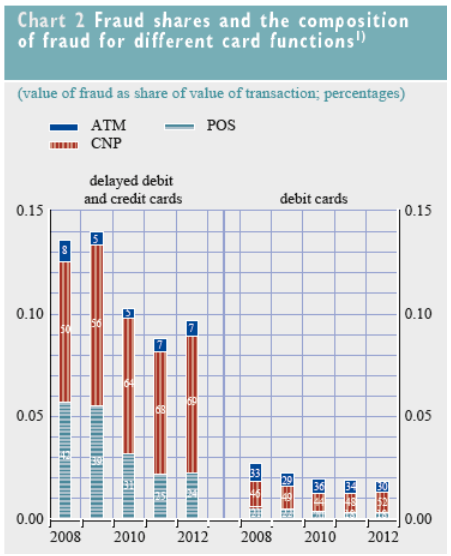
Quelle: Rand (National Security Research Division)

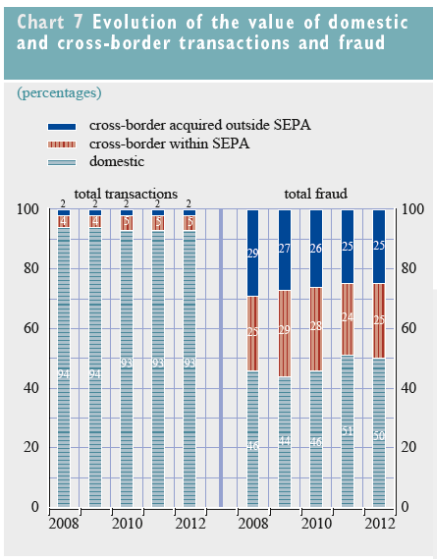
Entwicklung des Betrugs mit Zahlungskarten (1)

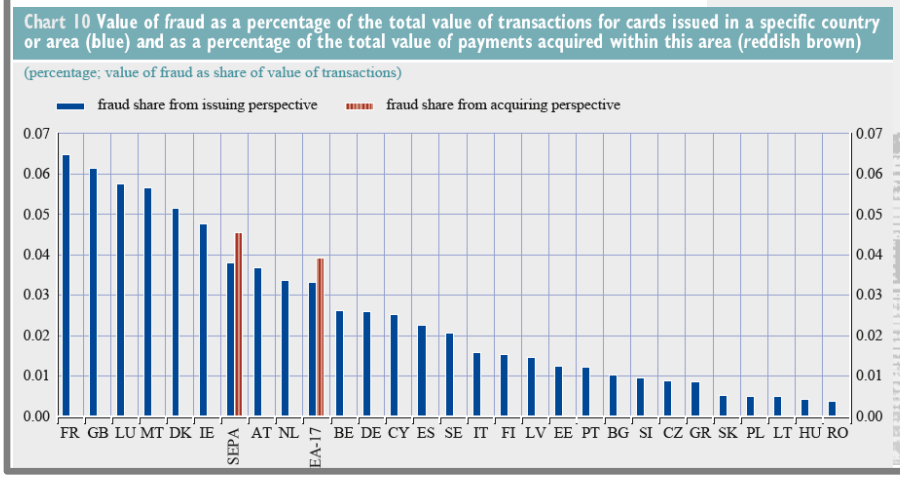


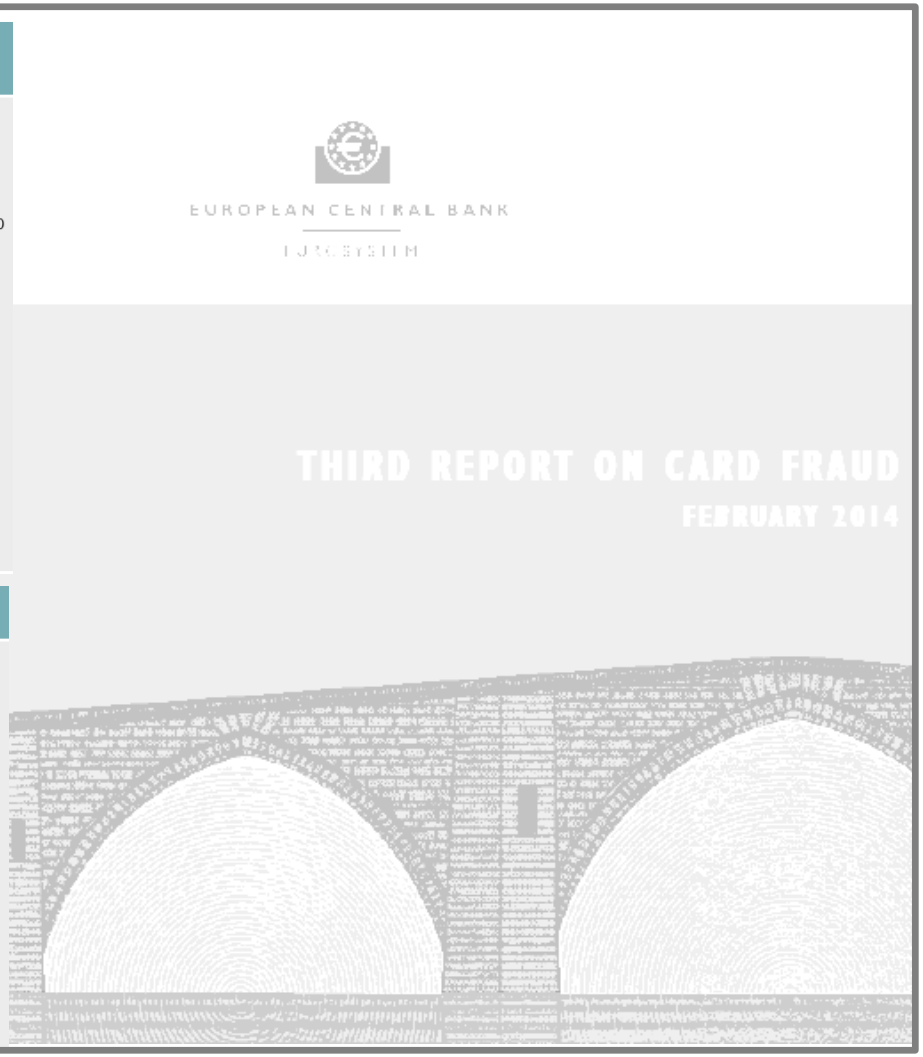
Quelle: Third Public report on card Fraud, EZB Januar 2014

Entwicklung des Betrugs mit Zahlungskarten (2)









Quelle: Third Public report on card Fraud, EZB Januar 2014

Zusammensetzung und Ziel

Freiwillige Kooperation

- Bankenaufseher und Zahlungsverkehrsüberwacher aus ganz Europa
- Vorsitz und Koordination durch EZB
- Beobachter von Europäischer Kommission und Europol

Ziel

- Identifizierung wesentlicher Schwachstellen
- Entwicklung von Empfehlungen als harmonisierte Mindestanforderungen
  - zur Erhöhung der Sicherheit im Massenzahlungsverkehr
  - zur Angleichung des Sicherheitsniveaus innerhalb Europas
- Generische Formulierung – keine Vorgabe konkreter technischer Lösungen
- Prinzip des „Comply or explain“

Implementierung

- Nationaler Rechtsrahmen (Aufsicht, Oversight)

Übersicht über die Arbeiten

	Entwicklung	Öffentliche Konsultation	Finalisierung	Veröffentlichung
Empfehlungen für die **Sicherheit von Internetzahlungen**	☑	☑	☑	☑
Empfehlungen für die **Sicherheit von Zugangsdiensten zum Zahlungskonto** – Zahlungsinitiierung, Kontoinformationsdienste	☑	☑	☑	
Empfehlungen für die Sicherheit von mobilen Zahlungen – Proximity / remote – NFC/QR-Codes, Apps, SMS…	☑	☑		
Informationsaustausch über schwerwiegende Sicherheitsvorfälle **zwischen europäischen Behörden**				

Empfehlungen für die Sicherheit von Internetzahlungen (1)

Anwendungsbereich

- **Kartenzahlungen** im Internet
  (einschließlich virtuelle Karten / Datenregistrierung in Wallets)
- Überweisungen im Internet (→ Onlinebanking)
- Erteilung und Änderung elektronischer Lastschriftmandate
- Transfer von E-Geld zwischen zwei E-Geld Konten über das Internet

Adressaten

- **Zahlungsdiensteanbieter** gemäß PSD und ***Governance Authorities*** von Zahlungssystemen
- **Online-Händler** → indirekt über PSPs und über sog. *best practices*

Umsetzung

- Bis zum 1. Februar 2015 – in DE mittels Rundschreiben der BaFin und Übernahme in den Eurosystem-Überwachungsrahmen

Konkretisierung im Assessment Guide

Empfehlungen für die Sicherheit von Internetzahlungen (2)

General control and security environment

- **Governance** – Implementation and regular review of a formal security policy
- Thorough **risk assessments**
- **Incident monitoring and reporting** – security incidents and security-related customer complaints; reporting to the management and the competent authorities (major payment security incidents)
- **Risk control and mitigation** – multiple layers of security defences
- **Traceability** of all transactions

Empfehlungen für die Sicherheit von Internetzahlungen (3)

Specific control and security measures

- **Initial customer identification** before access to the service and **information** about necessary requirements
- **Strong customer authentication** for initiation of payments and access to sensitive payment data
- **Enrolment for and provision of authentication tools and/or software delivered to the customer** in a secure manner
- Limits / rules for **log-in attempts, session time out and validity of authentication**
- Before final authorisation: **transaction monitoring**
- **Protection of sensitive payment data** when it is stored, processed or transmitted; encourage merchants not to store sensitive data

Empfehlungen für die Sicherheit von Internetzahlungen (4)

Specific control and security measures

Strong authentication

Knowledge	*password, code, PIN*
Ownership	*token, smart card, mobile*
Inherence	*fingerprint, iris*

- "Two-out-of-three"
- Mutually independence
- One element: non-reusable / not replicable / not being surreptitiously stolen via the internet

Exceptions

- Payments to trusted beneficiaries*
- Two accounts – same customer – same PSP*
- Low risk transactions
- Low value payments

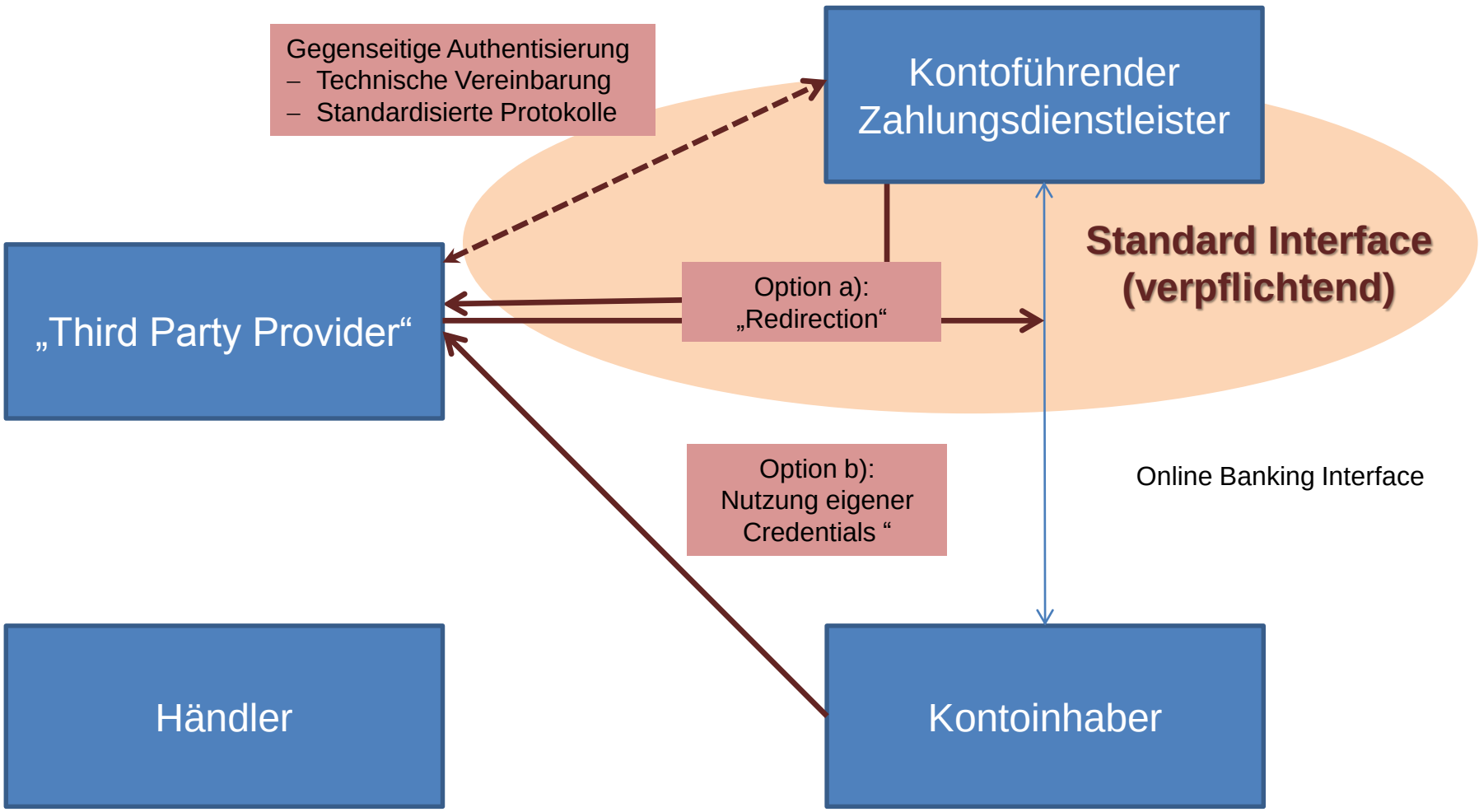
* Nicht anwendbar bei Kartentransaktionen

Empfehlungen für die Sicherheit von Internetzahlungen (5)

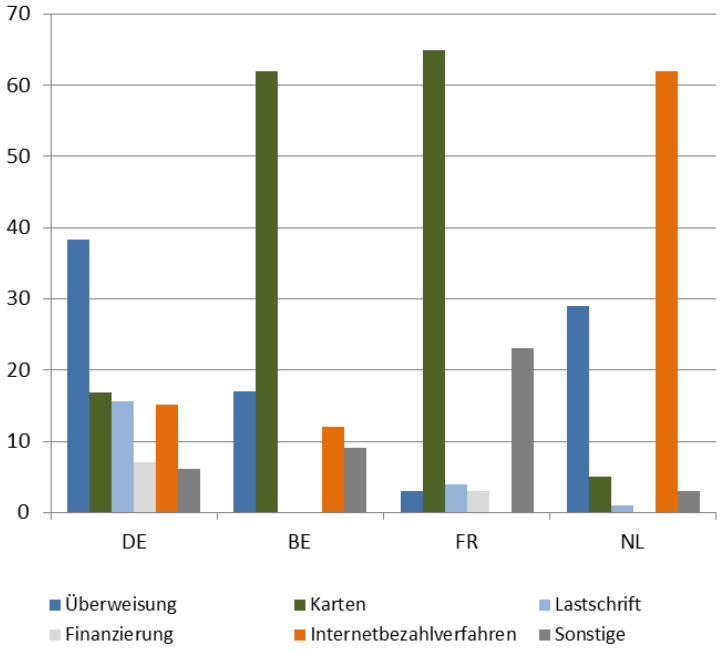
Customer awareness, education, communication

- **Customer education and communication** – assistance and guidance with regard to the secure use of the internet payment services; reassure customers of the authenticity of the messages received
- **Notifications, setting of limits** including options for customers for further risk limitation; alert and customer profile management services
- **Customer access to information on the status of payment initiation and execution**

Sicherheit von Zugangsdiensten zum Zahlungskonto



Folgen für den Internet-Zahlungsverkehr



Quelle: Steinbeis-Hochschule Berlin 2014

- **E-commerce bleibt „Wachstumsmarkt“**
- **Steigende Anforderungen an die Sicherheit im e-commerce**
- Trotz Harmonisierung:
  Keine „one-size / fits-all“-Lösung
- **Wirtschaftlichkeit wird schwieriger**
  - Höhere Sicherheit = höhere Kosten
  - Aber auch höheres Verbrauchervertrauen
  - Interchange-Regulierung
    (nicht Gegenstand des Secure Pay Forum!)
- **Komfortvorteile bei Lösungen mit einfacher Authentisierung**
- **Auswirkung auf Zugangsdienste zu Zahlungskonten / SDD im Internet unklar**

Quellen

Recommendations for the Security of Internet Payments, ECB, January 2013
http://www.ecb.int/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

Recommendations for the Security of Mobile Payments (draft for consultation), ECB, November 2013

https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

Assessment Guide for the Security of Internet Payments, ECB, January 2014

http://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201401en.pdf

Public Note on Payment Account Access Services, ECB, March 2014

https://www.ecb.europa.eu/pub/pdf/other/pubnote201403securitypaymentaccountaccessservicesen.pdf

Dirk Schrade
Deutsche Bundesbank

Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main
Deutschland
Email: Dirk.Schrade@bundesbank.de