Überblick zu den aktuellen Sicherheitsrisiken und Schwachstellen im IT-Bereich

Ivan Gudymenko
ivan.gudymenko@mailbox.tu-dresden.de
http://wwwpub.zih.tu-dresden.de/~igudym/

„Hacker Day"
Frankfurt, 27.11.2014

Agenda

- Aktuelle Bedrohungen und Trends: Überblick
- Kurses Demo: (Un)Sicherheit durch NFC
  - Kreditkartennumer mit NFC auslesen
- Vorschau auf die nächsten Vorträge

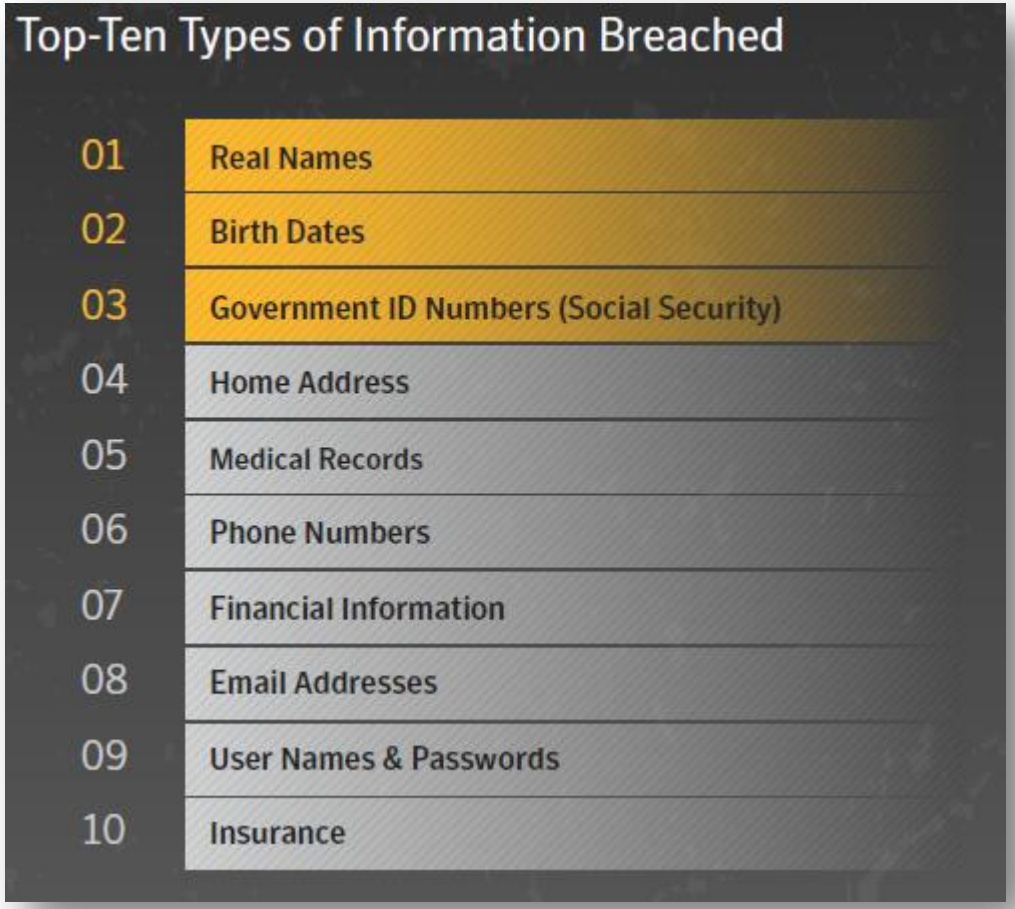
Wichtigste Trends im 2013

- 2013: das Jahr des „Mega Breach”
- Zunahme von gezielten Angriffen
- Zero-Day Vulnerabilities
- „Watering Holes“
- Ransomware („Strafe“ zahlen)
- Point of Sale Angriffe

[Quelle: Symantec Internet Security Threat Report 2014]

2013: das Jahr des Mega Breach

ca. 552 Mio. (!) Identities betroffen



im 2012 im 2013

[Quelle: Symantec Internet Security Threat Report 2014]

Sony Pictures komplett lahmgelegt

heise online > News > 2014 > KW 48 > Hacker legen Sony Pictures komplett lahm

25.11.2014 11:46 « Vorige | Nächste »

Hacker legen Sony Pictures komplett lahm

vorlesen / MP3-Download

Im Nachrichten-Forum Reddit hat ein Nutzer ein Foto eines gehackten Computers veröffentlicht. Dieser Nutzer, der inzwischen sein Konto gelöscht hat, hatte nach eigenen Angaben früher bei Sony Pictures gearbeitet – ältere Posts scheinen das zu bestätigen. Er will das Bild von einem Freund erhalten haben, der noch bei der Firma arbeitet. Weitere Nutzer beschrieben einer Zip-Datei, welche die Hacker ins Netz gestellt hatten. Diese soll Listen mit Dateien enthalten, die von den Hackern erbeutet wurden. Darunter sind augenscheinlich Finanzberichte, private Krypto-Schlüssel, interne Präsentationen und sogar Kopien von Pässen von Mitarbeitern.

Angreifer tauschten Android-App im Play Store aus

Die unbekannten Hacker sollen The Verge zufolge auch Twitter-Konten gekapert haben, die zu Sony Pictures gehören. Außerdem häufen sich Anzeichen, dass die Firma für kurze Zeit die Kontrolle über ihr Google-Play-Konto verloren hatte und jemand die App "Backup & Restore" gegen eine andere Version austauschte. Als System-App auf Sonys Xperia Handys kann man diese nicht entfernen. Die gehackte, möglicherweise bösartige App enthielt den Schriftzug "HeArT H4CK3R5" und wurde unter Umständen an einige Geräte als Update ausgeliefert. Sony hat die verdächtige App mittlerweile wieder entfernt.

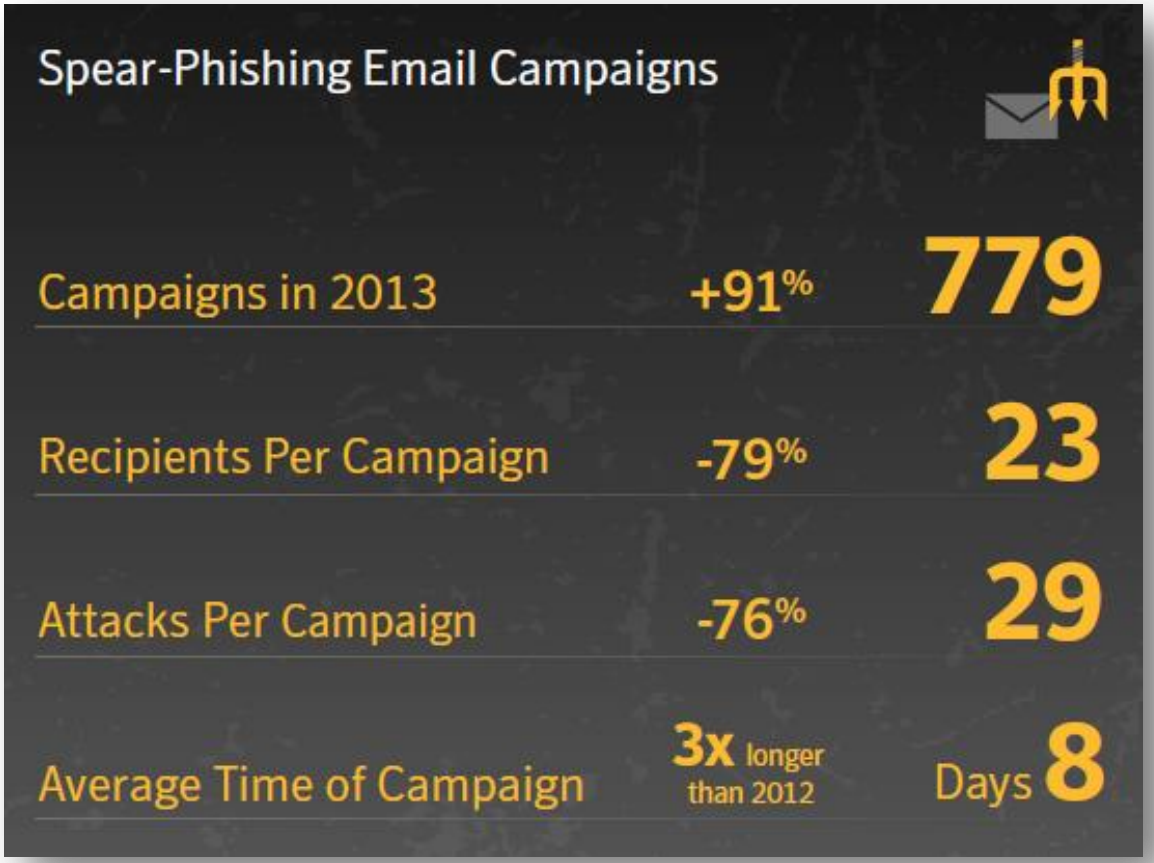
betroffen sein.

[Quelle: http://www.heise.de/newsticker/meldung/Hacker-legen-Sony-Pictures-komplett-lahm-2462889.html]

Zunahme von gezielten Angriffen

- Spear-Fishing: gestiegen um 93% im 2013
- U.a. durch verbessertes Social Engineering
- Angriffe über den längeren Zeitraum
  - „low and slow“ (~3 mal langsamer als im 2012)
  - weniger auffällig
- Dazu noch die „watering holes“ Angriffe (siehe weiter)

Zunahme von gezielten Angriffen (2)



[Quelle: Symantec Internet Security Threat Report 2014]

Zero-Day Vulnerabilities

- Entsteht durch die dem Vendor (noch) unbekannten Schwachstellen in Software
- Im 2013 mehr denn je:
  - Insgesamt 23 Vulnerabilities entdeckt
  - 77% von legitimen Webseiten betroffen
    - 1 von 8 kritisch
- Mehr Möglichkeiten für „Watering holes“ Angriffe (siehe weiter)

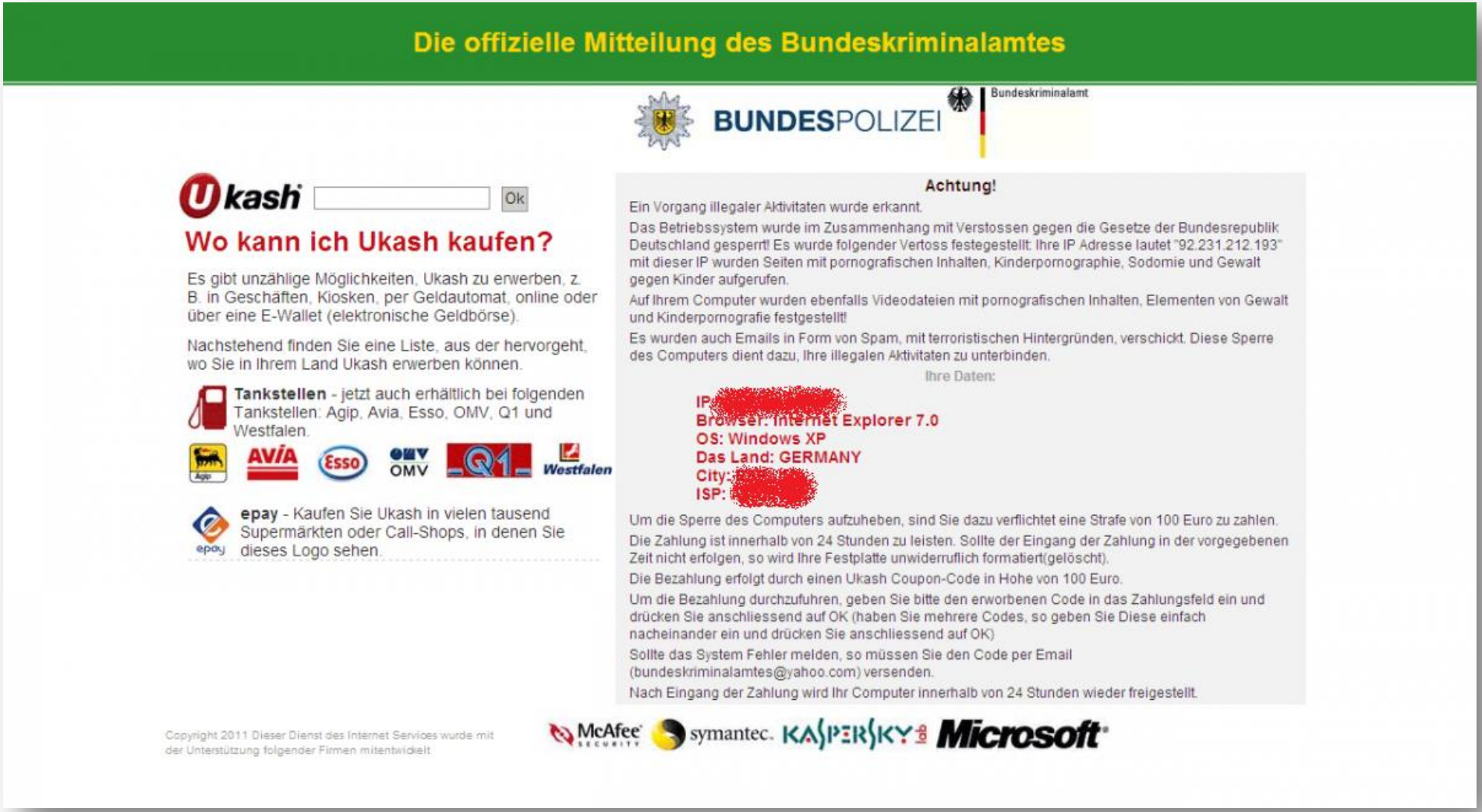
Watering Holes Angriffe

- Erstes mal dokumentiert im 2011
- Vorgehensweise:
  - Bestimmen welche ***legitime*** Webseiten das Opfer (häufig) besucht
  - Injektion vom bösartigen Code (Ausnutzung von Schwachstellen, u.a. auch Zero-Day)
  - Abwarten bis der Opferrechner infiziert wird
- Laut Symantec, 77% von gescannten Webseiten hatten Schwachstellen im 2013
  - 16% davon waren kritisch
    - Fazit: 1 von 8 Webpages sind unsicher!

Ransomware: Hintergrund

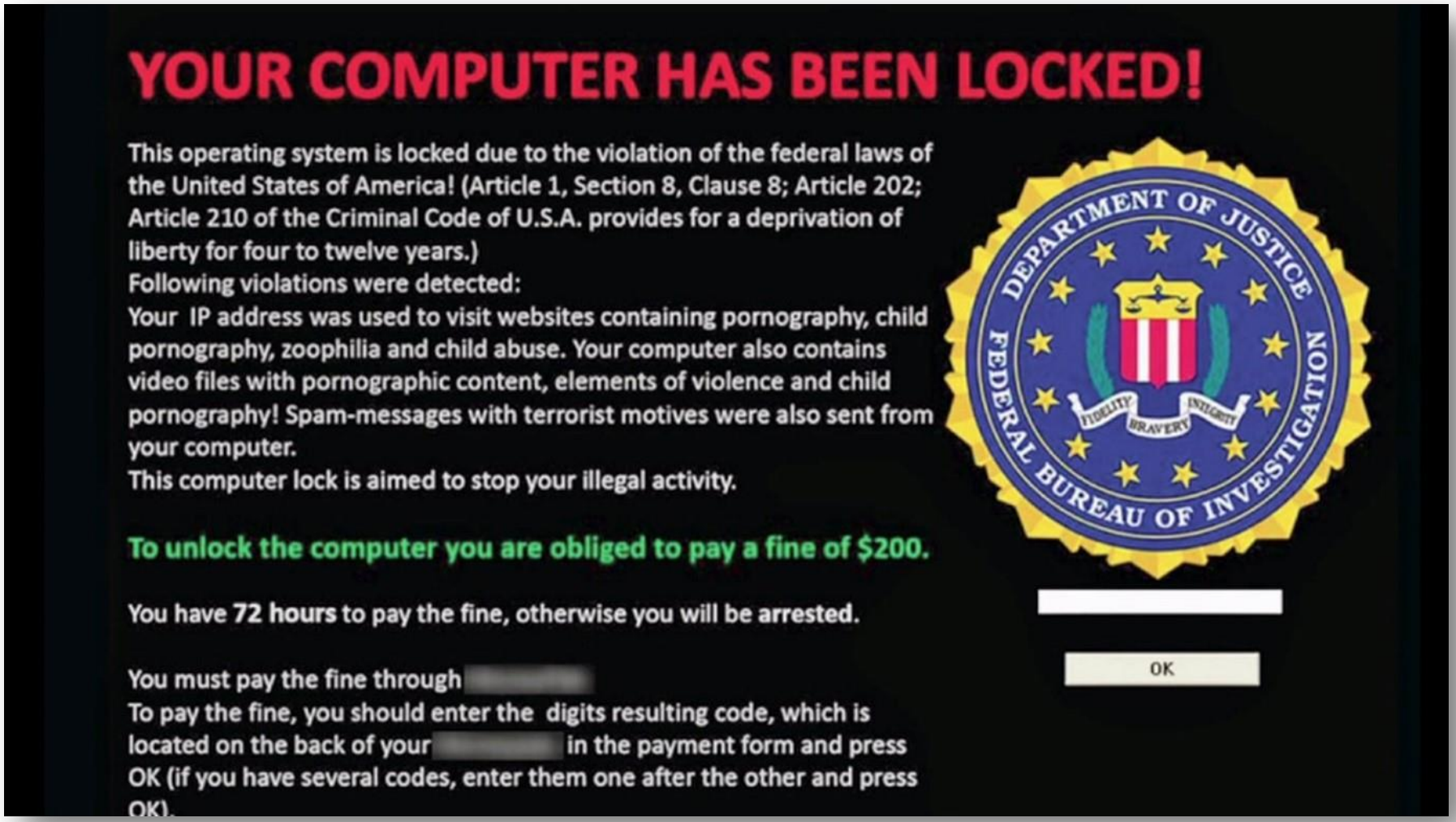
- „Cryptovirology“: geprägt im 1996 bei Adam Young and Moti Yung
- Hybride Verschlüsselung (kein “Reverse-Engineering” vom Schlüssel möglich)
- Hauptsächlich via E-Mail (bösartiger Anhang oder der Link in einer legitim aussehenden Business-Mail)

Ransomware — „Strafe“ zahlen: DE



[Quelle: http://www.homepage.eu/userdaten/0100221/709/download/anleitung_ransomware_loeschen_wheasel.pdf]

Ransomware — „Strafe“ zahlen: US



[Quelle: http://blog.kiandra.com.au/2013/11/cryptolocker-time-to-take-notice/]

Ransomware — „Strafe“ zahlen: PRISM

[Quelle: http://blog.kiandra.com.au/2013/11/cryptolocker-time-to-take-notice/]

Ransomware: Statistiken

- Beispiel: CryptoLocker
- Anzahl der Angriffe gestiegen um 500% (!) im 2013
- Hoch profitabel
  - ca. 3% der Betroffenen zahlen die „Strafe“
    - vielleicht hatte man doch etwas zu verbergen ☺

Point of Sale Angriffe

- 60% zahlen mit einer Kredit- oder Debitkarte
- Lukratives ziel für Angreifer

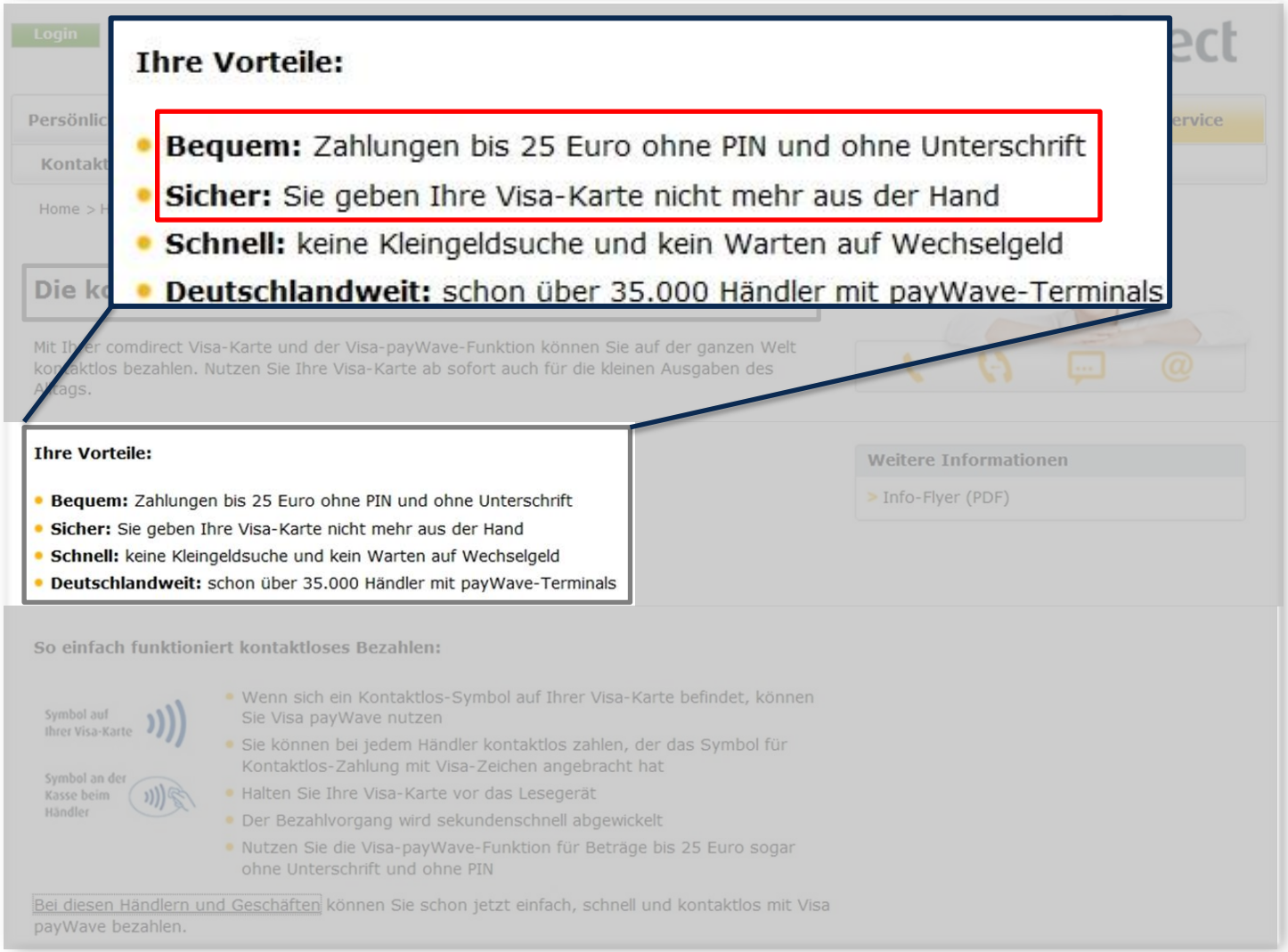
[Quelle: http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks]

Ein Kurzes Demo: Kreditartennumer über NFC auslesen

Case Study: VISA PayWave mit NFC

[Quelle: http://www.creditcardfinder.com.au/smart-cards-visa-paywave-and-mastercard-paypass.html]

PayWave von Comdirect



Kartennumer über NFC Auslesen

- Die Apps dafür sind frei verfügbar!
- Die ausgelesene Kartennummer kann missbraucht werden
  - wie etwa beim Online-Einkauf

Kartennumer über NFC Auslesen

02.07.2014 15:44 « Vorige | Nächste »

Betrug mit Online-Zugtickets: Bahn um hunderttausende Euro geprellt

vorlesen / MP3-Download

Die Online-Tickets wurden mit gestohlenen Kreditkartendaten bezahlt: Vier Verdächtige aus Hamburg sitzen wegen eines groß angelegten Betrugs in U-Haft. Der Schaden für die Deutsche Bahn ist hoch.

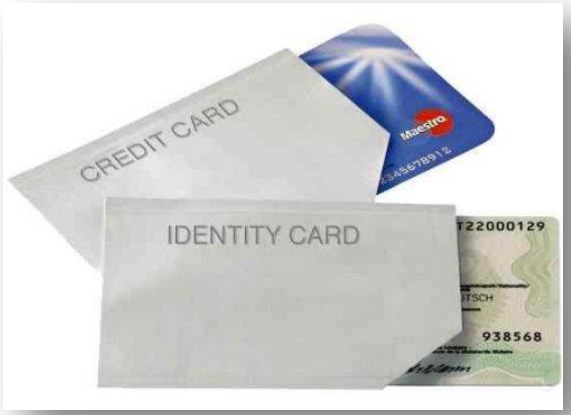
Vier junge Männer aus Hamburg sollen die Deutsche Bahn durch den Betrug mit Online-Tickets um rund 700.000 Euro geprellt haben. Die 18 bis 26 Jahre alten Verdächtigen sitzen wegen Verdachts des banden- und gewerbsmäßigen Computerbetrugs in Untersuchungshaft, wie der Sprecher der Hamburger Staatsanwaltschaft, Carsten Rinio, am Mittwoch sagte.

Kartennumer über NFC Auslesen

- Die Apps dafür sind frei verfügbar!
- Die ausgelesene Kartennummer kann missbraucht werden
  - wie etwa beim Online-Einkauf
  - ein Tracking-Merkmal
- Darüber hinaus, ein **Relay-Angriff** wäre möglich

Kartennumer Auslesen: Schutz?

- RFID-Schutzhülle
- bzw. Portmonee mit RFID-Blocker



Aktuelle Bedrohungen: Fazit

- 2013: das Jahr des „Mega Breach“
- Die Angriffe sind schlauer geworden
- Viele Webseiten sind immer noch angreifbar
- → Security IS INDEED a **Process**!

Vorschau auf die nächsten Vorträge

- (Un)Sicherheit zum anfassen: verschieden Live Hacking Demos
- Manipulierte USB-Sticks
  - Handy-Trojaner
  - SCADA-Security (Industrieanlagen)
- Hacking mit Schwerpunkt Mobile Security
  - Bösartige QR-Codes
- DDoS - Simulation eines DDoS-Angriffes

VIELEN DANK FÜR IHRE AUFMERSAMKEIT!

Haben Sie noch Fragen?

»Wissen schafft Brücken.«