bank-verlag Das Service-Unternehmen der privaten Banken

IT-Sicherheit von Online-Banking aus der Sicht der Banken

Symposium: Betrugsschutz beim Online-Banking

Gerd Rüter, Bank-Verlag GmbH
Gelsenkirchen, 26.04.2017

Der Bank-Verlag im Überblick

Gesellschafter:	Bundesverband deutscher Banken e.V.
Gründungsjahr:	1961
Standorte:	Köln, Frankfurt
Mitarbeiter:	ca. 200

Leistungsspektrum

- Produktion von Debit- & Kreditkarten – Datenservice & GU-Dienstleistungen für alle BdB-Banken
- Kopfstelle für die Autorisierung im Geldautomatensystem und von Debit-Karten-Zahlungen
- Betrieb des Key-Administration-Centers für die Deutsche Kreditwirtschaft
- Betrieb von eBanking-Portalen im Privat- und Firmenkundenbereich für mehr als 60 Banken
- Zentrale Authentifizierungsplattform mit allen gängigen Authentifizierungsverfahren
- Fraud-Management-Systeme zur Betrugserkennung bei Kartenzahlungen und in Online-Portalen

Sicherheitsaspekte beim Online-Banking 2017

- Angriffe auf das Online-Banking werden immer ausgefeilter und sind selbst durch aufmerksame Kunden oft nicht mehr zu erkennen

- Hohen Sicherheitsanforderungen der Regulierungsbehörden steht der Kundenwunsch nach uneingeschränkter, einfacher und mobiler Nutzung entgegen

- Durch Weiterentwicklung von Authentikationsverfahren allein lässt sich die Sicherheit des Online-Banking nicht mehr steigern

Übersichtsbild Online-Banking

Kunden- / Clientseite

- Zugriff über das Internet mittels Browser/App
- Nutzung verschiedener Endgeräte (PC, Tablet, Smartphone)

Kunde

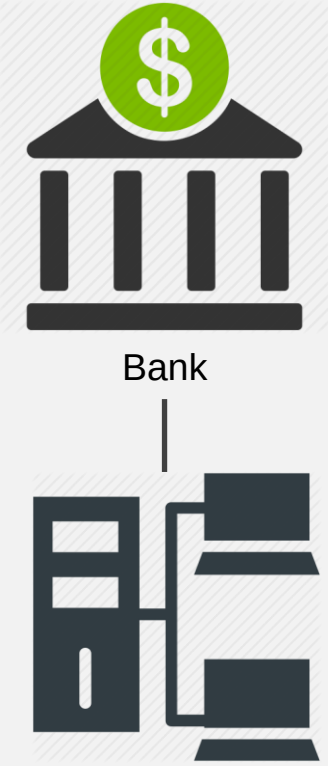
Internet

Angreifer

Online-Banking-Transaktionen

Bank- / Serverseite

- Betrieb in Rechenzentren der Bank oder bei externen Dienstleistern



Bank

Rechenzentrum

Regulatorische Anforderungen an Banken

MaRisk

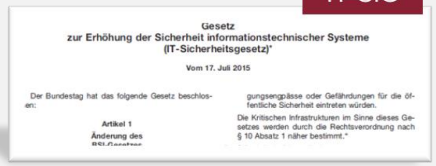
Mindestanforderungen an das Risikomanagement

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

BAIT

Bankaufsichtliche Anforderungen an die IT

IT-SiG



IT-Sicherheitsgesetz

Bundesamt für Sicherheit in der Informationstechnik

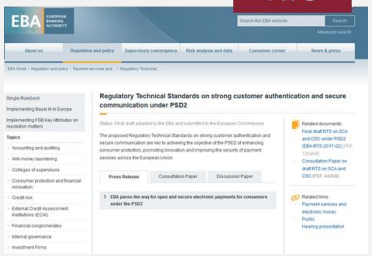
MaSI

Mindestanforderungen an die Sicherheit von Internetzahlungen

PSD II

Zahlungsdienste-Richtlinie

RTS



Technische Regulierungsstandards

EBA European Banking Authority

NIS

Richtlinie zur Netzwerk- und Informationssystemsicherheit

Europäische Kommission

Hohe Sicherheitsstandards der Bank-IT

Betrieb in gesicherter RZ-Umgebung

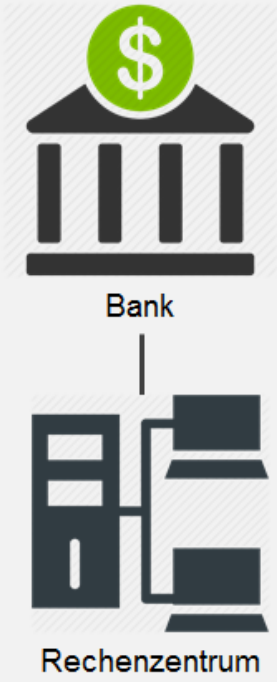
- mehrstufige Firewall-Infrastrukturen
- IDS/IPS-Systeme
- Härtung von Systemen
- Zutritts- und Zugriffsschutz

Definierte Prozesse

- Sicherheitsupdates
- Vier-Augen-Prinzip
- Incident-/Problem-Management

Regelmäßige Überprüfung des Sicherheitsniveaus

- Interne/externe Revisionen
- Zertifizierungen



Sicherheitsrisiken in Kundensystemen

Kundensysteme sind potentiell unsicher

- Veraltete Betriebssystemversionen
- Oft keine Virenscanner/Firewalls
- Viele verschiedene Anwendungsprogramme mit Sicherheitslücken
- Keine regelmäßige Installation von Sicherheitsupdates
- Leichtfertiger Umgang mit Passwörtern
- Geringe Kenntnisse über Bedrohungen

In der Regel richten sich Angriffe auf das Online-Banking gegen den Kunden und seine Infrastruktur!

Angriffsszenarien

Identitätsdiebstahl

- Links in Phishing-Mails leiten den Kunden auf gefälschte Bank-Seiten, auf denen er seine Logindaten eingeben soll.
- Durch den Einsatz von Schadsoftware (z.B. Keylogger) späht der Angreifer die Login-Daten des Kunden aus.

Fälschen von Transaktionen

- Mit Hilfe von Schadsoftware auf dem Kunden-PC manipuliert der Angreifer die Transaktion (z.B. durch Änderung des Zielkontos und des Betrags).

Social Engineering

- Durch eine überzeugende Story bringt der Angreifer den Kunden zur Durchführung einer Transaktion oder zur Herausgabe seiner Authentifikations-Daten.
- Hierzu können verschiedene Kanäle (z.B. E-Mail, Telefon) genutzt werden.
- Zusätzlich kann Schadsoftware eingesetzt werden (z.B. zur Einblendung manipulierter Umsatzanzeigen: „Rücküberweisungstrojaner“).

Trends

Angriffe werden immer ausgefeilter

- Phishing-Mails sind nicht mehr auf den ersten Blick zu erkennen
- Moderne Schadsoftware verwendet Konfigurationen, die durch die Angreifer flexibel nachgeladen werden können
- Reaktion auf neue Sicherheitsverfahren der Banken (z.B. 100TAN-Abfrage)
- Angriff auf 2-Kanal-Verfahren (z.B. SIM-Swap)

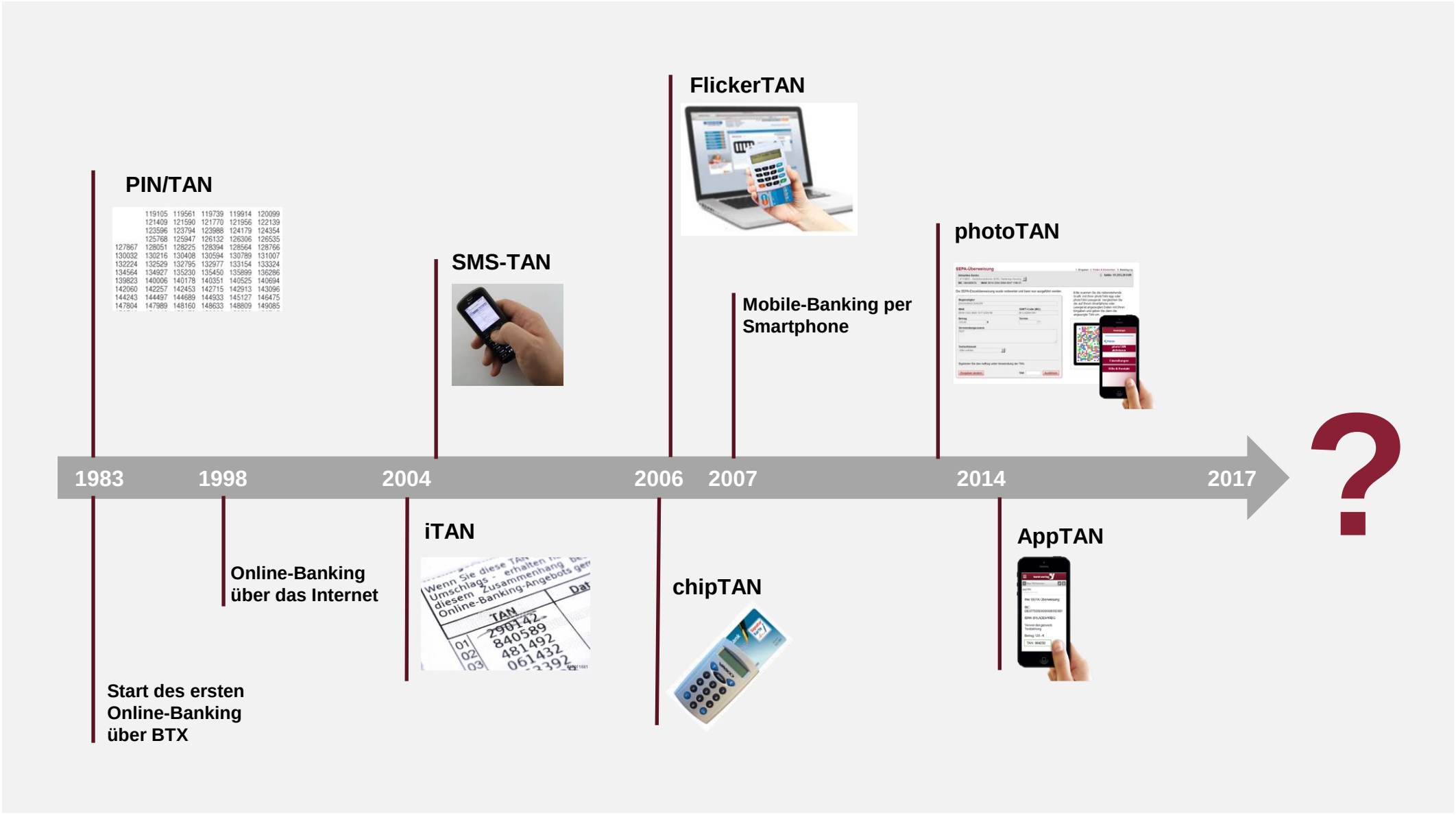
Arbeitsteiliges Vorgehen der Angreifer

- „Malware as a service“: Vom Schadsoftware-Baukasten zur Erzeugung eines eigenen Trojaners bis zum Zugriff auf Botnets zur Verteilung werden alle für einen Angriff erforderlichen „Dienstleistungen“ im Darknet angeboten
- Der eigentliche Angreifer benötigt nur noch wenig Know-How

Hohe Anzahl neuer Schadsoftware-Samples

- Geringe Erkennungsraten durch Virenscanner
- Vermehrt auch Schadsoftware für mobile Endgeräte

Entwicklung des Online-Bankings



Zielkonflikt bei Sicherheitsverfahren

Verbesserung der TAN-Verfahren als Reaktion auf wachsende Bedrohungen

- Prinzip der Kanaltrennung (Erfassung der Transaktion – Anzeige der TAN)
- Transaktionsbindung der TAN (Betrag, Zielkontonummer)
- Einsatz separater Hardware (Chipkarten, Leser)

Wunsch des Kunden nach möglichst einfachen Verfahren

- Zunehmende Nutzung von mobilen Endgeräten
- „One-Click“-Verfahren, Fingerprint

Lösungsansätze zur Erhöhung der Sicherheit

Einsatz von Betrugserkennungs-Systemen

- Analyse von Transaktionsdaten auf Auffälligkeiten (Betragshöhe, Zielkonten)
- Auswertung technischer Parameter (IP-Adresse/Geolocation, Device-Fingerprint, etc.)
- Analyse des http(s)-Datenstroms an der Firewall auf Auffälligkeiten, die auf eine Schadsoftware auf dem Kundenendgerät hindeuten
- Anzeichen, wie z.B. ein für ein Schadprogramm typisches „Klickverhalten“ (Velocity-Checks, etc.)

Einbindung der Authentikationsmedien in die Risikobetrachtung

- Prüfen der Integrität von Smartphones und Apps durch Härtung und serverseitige Überwachung
- Auswertung von Sensoren des Smartphones

Nutzung verhaltensbiometrischer Verfahren (z.B. Tippbiometrie)

- Für den Nutzer transparenter Sensor, keine zusätzliche Hardware erforderlich

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

Gerd Rüter

Bank-Verlag GmbH

Tel.: 0221/5490-422
Email: gerd.rueter@Bank-Verlag.de