Verbundvorhaben BOB

—

Bankseitige Schutzmechanismen

Gelsenkirchen, 26.04.2017

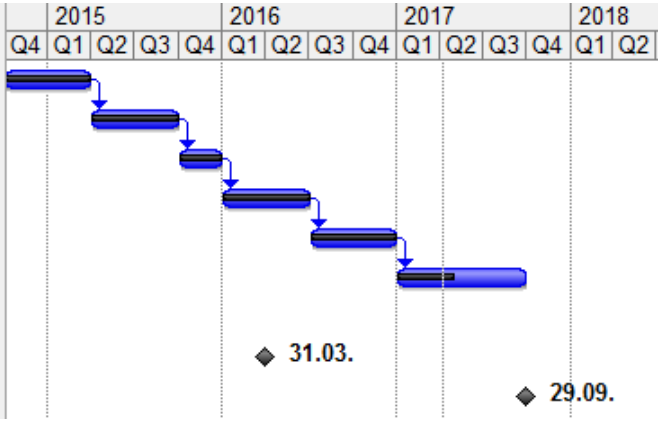
Fiducia & GAD

FIDUCIA GAD
ZUKUNFTSERFAHREN

Inhaltsverzeichnis

Arbeitspakete & Zeitplanung

Vorgangsname	Anfang
1.1.2 Ist-Analyse Betrugsfälle und Klassifizierung der Betrugsfälle in der Bank	Mi 01.10.14
1.4.3 Bezug von Sicherheitswerten zu Transaktionsdaten	Mi 01.04.15
2.1.2 Analyse Integration sicherer digitaler Identitäten in das Online Banking	Do 01.10.15
2.3.2 Bankenseitige Missbrauchsvermeidung	Fr 01.01.16
2.5.1 Analyse der Bewegungsabläufe bei Angriffen auf das Online-Banking	Mo 04.07.16
3.2 Evaluation und Demonstrator Angreifer-Wirtschaftlichkeit	Mo 02.01.17
Überprüfung der Meilensteine	Do 31.03.16
Projektabschluss	Fr 29.09.17



Status & Zwischenergebnisse 1/5

1.1.2 Ist-Analyse Betrugsfälle und Klassifizierung der Betrugsfälle in der Bank

- Die Betrugsfälle wurden klassifiziert nach Angriffsarten:
  - Klassisches Phishing
  - TAN-Diebe
  - Echtzeitmanipulationen
  - Social-Engineering
- Die Klassifizierung wurde abgeglichen mit den Untersuchungsergebnissen von if(is).
- **Fazit: Die Angriffsarten sind unabhängig von den Sicherheitsverfahren.**

Status & Zwischenergebnisse 2/5

1.4.3 Bezug von Sicherheitswerten zu Transaktionsdaten

- Aufgeschlüsselt nach Sicherheitsverfahren wurden für jeden Geschäftsvorfall mit Geldfluss die Transaktionsdaten beschrieben, an die die Sicherheitswerte in der Praxis gebunden sind.

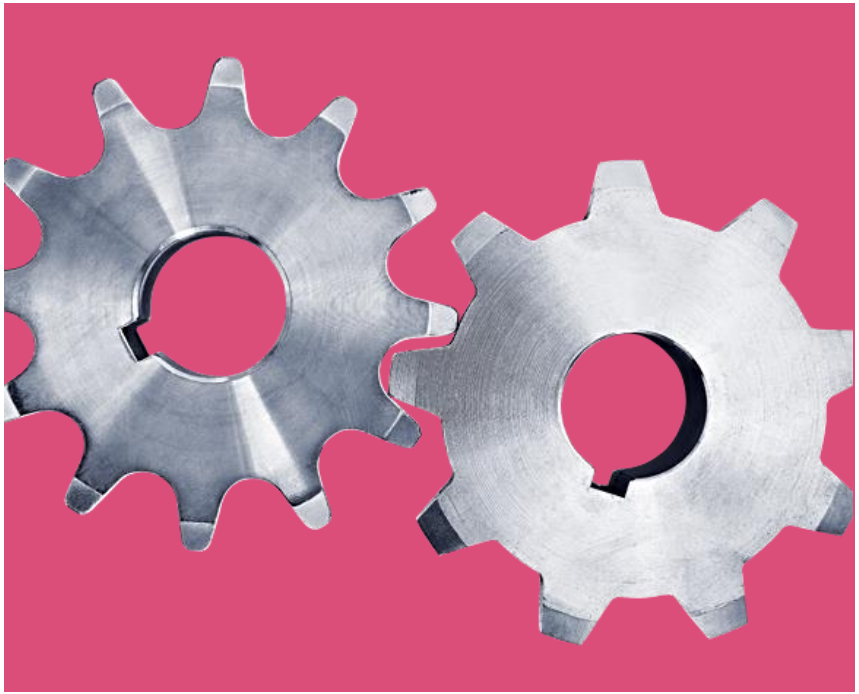
- Aufgeschlüsselt nach Sicherheitsverfahren wurden für jeden Geschäftsvorfall mit Geldfluss
  - die Daten beschrieben, die die Transaktion eindeutig definieren.
  - bewertet, welche Transaktionsänderungen möglich sind.

- **Fazit: Es ist kein Sicherheitsverfahren als besonders gefährdet einzustufen.**

Status & Zwischenergebnisse 3/5

2.1.2 Analyse Integration sicherer digitaler Identitäten in das Online Banking

- Gemäß Anforderungen aus der neuen Zahlungsdiensterichtlinie muss
  - die Authentifizierung durch zwei Faktoren (aus der Rubrik Wissen, Besitz, Sein) abgesichert sein. Dies gilt für eine Zahlung/Überweisung genauso wie für die Kontoinformation.
  - die Authentifizierung einer Zahlungstransaktion dynamisch mit dem Zahlungsvorgang (Zahlungsempfänger und Zahlungsbetrag) verlinkt sein.
- **Fazit: Eine bloße Identifizierung über die Nutzung der eID-Funktion des Personalausweises ist beim Online Banking bei einer Zahlung/Überweisung aus regulatorischer Sicht nicht ausreichend. Die Nutzung der eID-Funktion zur Identifizierung zum Zwecke der Kontoinformation ist zulässig.**
- **Hemmnis: Akzeptanz des Verbrauchers von „komplizierten“ Authentifizierungsmethoden.**



Status & Zwischenergebnisse 4/5

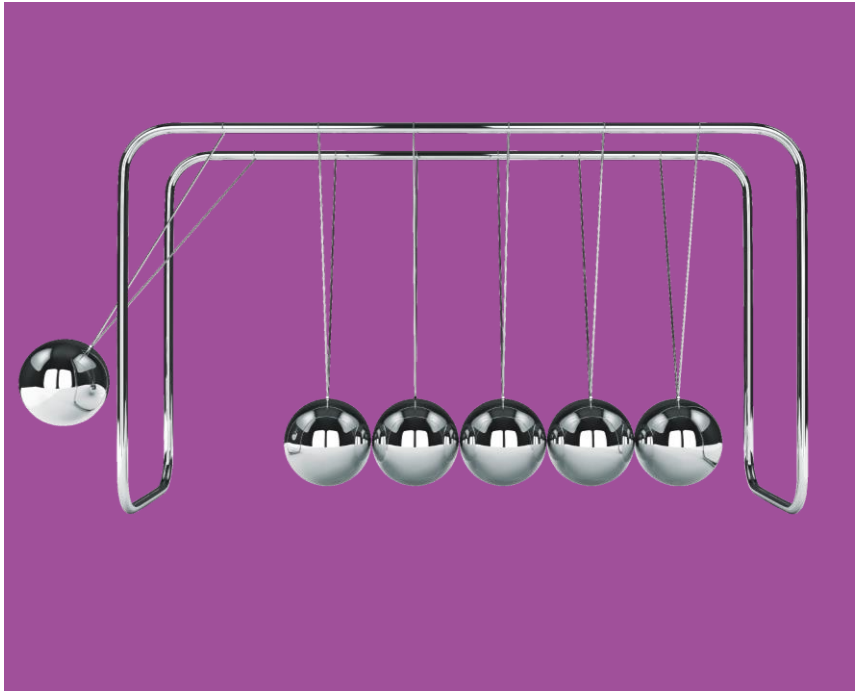
2.3.2 Bankenseitige Missbrauchsvermeidung

- Erkenntnisse aus Projekt
  - Die angewandten Authentifizierungsverfahren sind technisch und mathematisch sicher.
  - Der Kunde benötigt Information
    - zur Funktionsweise der Authentifizierungsverfahren.
    - zum Erkennen von Gefahren und Angriffen.
- Die bankenseitige Missbrauchsvermeidung muss insbesondere eine Hilfestellung für den Kunden beinhalten.
- Umgesetzte Maßnahmen sind u.a.:
  - Kundeninformation angepasst:
    - Sicherheitshinweise auf den Online Banking Webseiten direkt beim Login
  - Die Einführung einer neuen Generation von TAN-Lesern ist geplant
    - Neue schnellere Übertragungsart und damit Erhöhung der Nutzerakzeptanz
      ➔ höhere Vertrautheit schafft höhere Sicherheit
- Ziel der Maßnahmen ist eine verbesserte Aufklärung des Nutzers über
  - die Gefahren im Online Banking und den Schutz dagegen
  - die Anwendung der Sicherheitsverfahren

Status & Zwischenergebnisse 5/5

AP 2.5.1 Analyse der Bewegungsabläufe bei Angriffen auf das Online Banking

- Betrugsschutzsystem in agree21 eBanking aufgebaut.
- Erkenntnisse
  - Die Muster bei versuchten Angriffen unterliegen einem stetigen Wandel.
  - Die Abwehrmechanismen müssen ständig angepasst werden.
- Umgesetzte Maßnahme:
  - Funktion eines „Fraud Managers“ wurde ins Leben gerufen und personell ausgefüllt.



Ausblick

AP 3.2 Evaluation und Demonstrator Angreifer-Wirtschaftlichkeit

- Bearbeitung AP 3.2 läuft (seit Januar 2017)
- Idee: Erkennung von Banking-Webseiten-Manipulationen
- Hierfür sind gleichartige Skripte auf Client-Seite und auf Server-Seite zu erstellen.
- Stand der Bewertung:
  - Skript ist stark abhängig vom verwendeten Browser.
  - Die Erstellung ist aufwändig und fehleranfällig.
  - Auch die Wirtschaftlichkeit der Abwehr stößt an die Grenzen.

Dankeschön!

FIDUCIA GAD
ZUKUNFTSERFAHREN