Westfälische Hochschule

Wissen.
Was praktisch zählt.

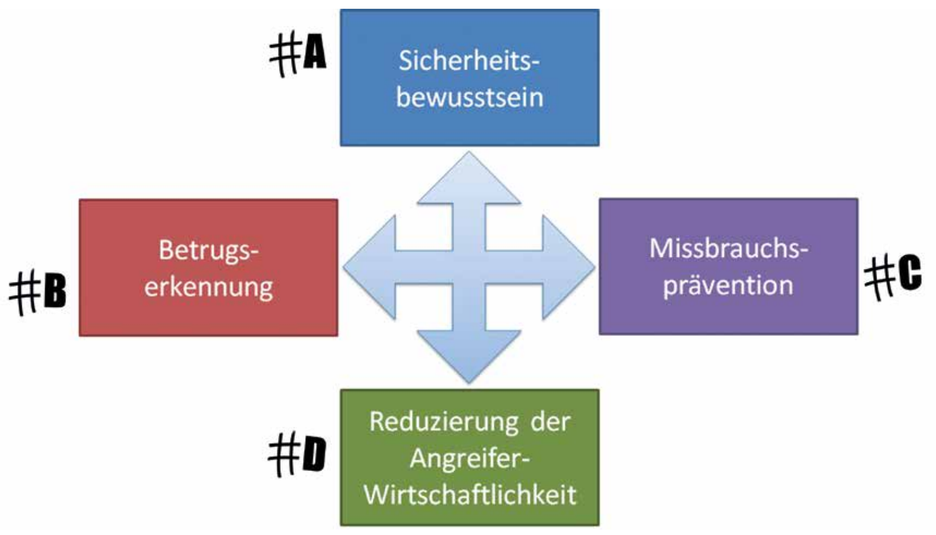
Betrugsschutz beim Online-Banking

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Autoren: Tobias Urban, René Riedel, Norbert Pohlmann

Ziele des Vorhabens

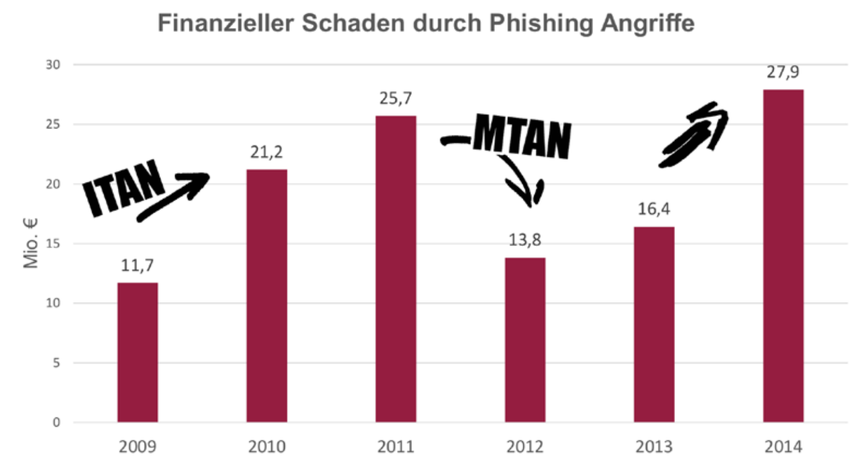
In dem Forschungsprojekt wird ein ganzheitlicher Ansatz zum Schutz des Online-Bankings erarbeitet. Neben technischen Maßnahmen, sollen auch gesellschaftliche Maßnahmen vorangetrieben werden. Die folgende Abbildung verdeutlicht die vier Säulen, die innerhalb des Projektes erarbeitet werden:



Erkenntnisse aus der Risikoanalyse bestehender Sicherheitsmechanismen sollen projektbegleitend aufbereitet und öffentlichkeitswirksam dargestellt werden (#A). Auf Seiten der Bank und der Nutzer sollen Mechanismen entwickelt werden, die Kriminaldelikte zeitnah aufdecken, unterbinden oder Rückabwicklungen ermöglichen (#B). Die bestehenden Authentisierungsverfahren sollen durch sicherere, wirtschaftliche und vom Nutzer akzeptierte Verfahren abgelöst werden (#C).

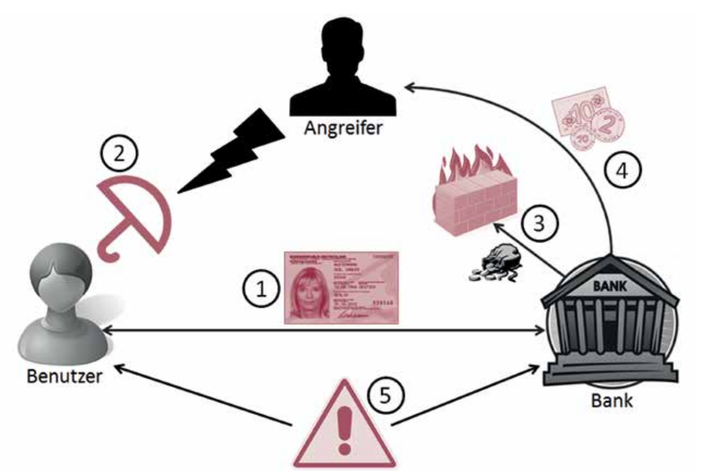
Problemstellung

Die Anzahl an Privatnutzern des Online-Bankings steigt. Allein im Jahr 2016 erledigten bereits 38 Millionen Deutsche (über 65% der 18- bis 49-jährigen) ihre Bankgeschäfte online.



Durch illegale Aktivitäten, wie etwa dem nicht autorisierten Zugriff auf Bankkonten (z.B. durch Phishing) oder der schadhaften Manipulation von Online-Überweisungen, entstehen den Banken und Endbenutzern immense Schäden. Die Abbildung verdeutlicht diesen Sachverhalt anhand von konkreten Daten aus dem „Bundeslagebild Cybercrime 2014“ vom Bundeskriminalamt.
Mit stetigem Trend entwickelt sich die Finanzkriminalität derzeit zu einer ernsten Gefahr. Betrüger zielen z.B. vermehrt darauf ab, Online-Banking auf den Smartphones der Nutzer zu missbrauchen. Ferner können vermeintlich sicherere Transaktionssysteme (z.B. mobile TAN) bereits von Angreifern umgangen werden.

Konzept des Forschungsprojektes



1. Nutzung von sicheren **digitalen Identitäten** beim Online-Banking.
2. Nutzerseitige Schutzmechanismen, wie z.B. die Erkennung von Banking-Trojanern.
3. Bankenseitige Schutzmechanismen, wie z.B. das Identifizieren und Blocken von betrügerischen Überweisungen.
4. Wirtschaftlichkeit des Angreifers durch die Streuung falscher Informationen stören.
5. Entwicklung eines **Alertsystems**, welches Banken und Benutzer direkt oder über Dritte (Medien, CERTs, etc.) vor akuten Gefahren warnt.

AVIRA · CISPA Center for IT-Security, Privacy and Accountability · FIDUCIA GAD ZUKUNFTSERFAHREN · if(is) internet-sicherheit. · TU berlin

Kontakt

Institutsleitung
Prof. Dr. (TU NN) Norbert Pohlmann
pohlmann@internet-sicherheit.de
Tel.: +49 209 9596 - 515

Tobias Urban, M.Sc.
urban@internet-sicherheit.de
Tel.: +49 209 9596 - 857

René Riedel, M.Sc.
riedel@internet-sicherheit.de
Tel.: +49 209 9596 - 816

Westfälische Hochschule
Fachbereich Informatik und Kommunikation
Institut für Internet-Sicherheit
www.internet-sicherheit.de