Westfälische Hochschule

Wissen.
Was praktisch zählt.

Du wurdest gewarnt!

Ein Alarmierungssystem im Online-Banking

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Autoren: Tobias Urban, René Riedel, Norbert Pohlmann

Problemstellung

Im modernen Bankgeschäft ist Online-Banking bereits seit vielen Jahren ein fundamentaler und richtungsweisender Bestandteil. Umso schwerwiegender ist die Tatsache, dass dieser Bereich immer noch häufig und erfolgreich von Betrügern mittels „Social Engineering“ angegriffen wird. Zu diesem Anlass stellen wir ein Alert-System für das Online-Banking vor, welches das Schutzniveau sowohl clientseitig, als auch serverseitig, erhöhen soll.

Konzeptionelle Umsetzung

Für die Umsetzung des Alert-Systems wird ein kontinuierliches Lagebild über die aktuelle Gefahrenlage beim Online-Banking erstellt. Hierzu nutzen und vergleichen wir unterschiedliche Algorithmen des maschinellen Lernens. Als Grundlage für die Berechnung werden unterschiedliche und freizugängliche Datenquellen genutzt, welche im direkten Zusammenhang zum Betrug im Online-Banking stehen.

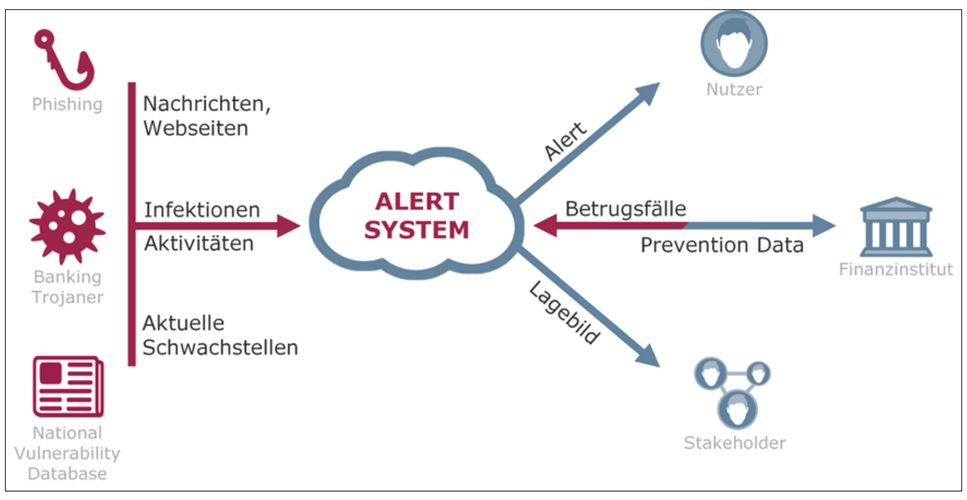

Abbildung 1: Konzept des Alert-Systems

Im Rahmen des Forschungsvorhabens wurden die folgenden mathematischen Modelle und Algorithmen betrachtet:

- Allgemeines lineares Modell
- k-Nearest Neighbor
- Support State Vector Machine (SVM)
- Künstliche neuronale Netze

Erste Ergebnisse

Wir überprüfen die Effektivität unseres Systems anhand von echten Betrugsfällen, die bei einer Bankengruppe aufgetreten sind und mit Hilfe von Malware-Statistiken eines großen Herstellers von Antiviren-Software.
Unsere ersten Ergebnisse zeigen, dass die verwendeten Verfahren dazu geeignet sind die Gefahrenlage im Online-Banking zu bestimmen. Hierfür ist in Abbildung 2 exemplarisch dargestellt, wie das Alert-System auf Basis der zur Verfügung stehenden Kennzahlen und der bekannten Betrugsfälle eine Einschätzung der Gefahrenlage beim Online-Banking vornimmt.

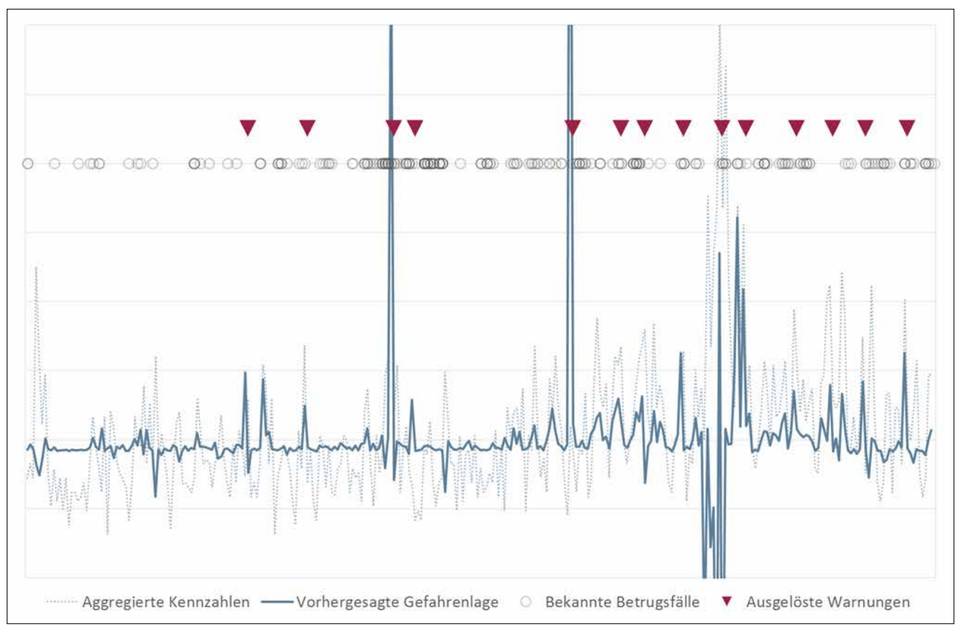

Abbildung 2: Beurteilung der Gefahrenlage auf Basis einer SVM

Alarmierung des Anwenders

Anwender können anhand des Lagebildes direkt auf die aktuelle Gefahrenlage aufmerksam gemacht und über aktuelle Angriffe aufgeklärt werden. So kann das Bewusstsein des Kunden punktuell erhöht und gängigen „Social Engineering“-Angriffen entgegen gewirkt werden.

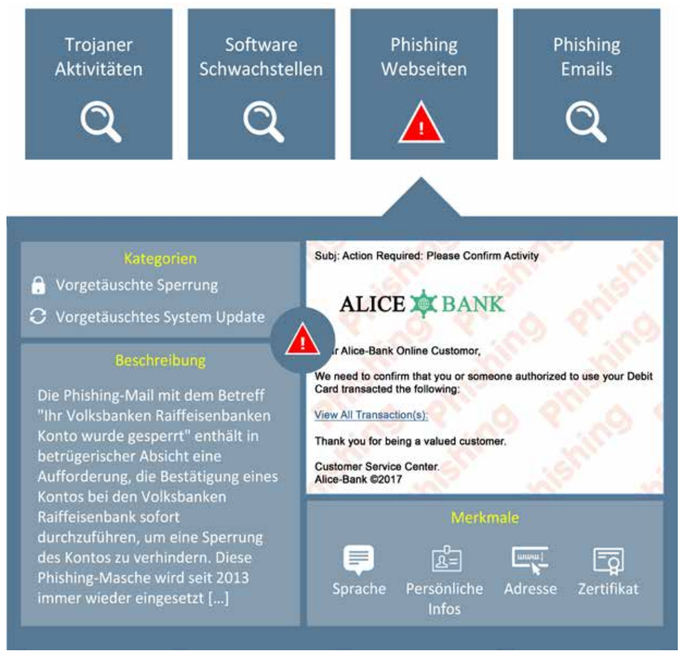

Abbildung 3: Exemplarische Darstellung einer Warnung beim Kunden

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

if(is) internet-sicherheit.