Du wurdest gewarnt!
Ein Alert-System im Online-Banking

Zusammenfassung

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 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. Hierfür wird durch das Alert-System ein kontinuierliches Lagebild über die aktuelle Gefahrenlage beim Online-Banking erstellt. Sollte vom System eine potentielle Gefahr bei der Verwendung von Online-Banking festgestellt werden, wird der Nutzer aktiv davor gewarnt. Diese Warnungen können unter anderem dafür verwendet werden, um den Nutzer gezielt und automatisiert auf aktuelle Angriffsmuster aufmerksam zu machen. Aus dieser Vorgehensweise resultiert der Vorteil, dass der Nutzer nur punktuell auf die Komplexitäten aktueller Angriffe aufmerksam gemacht wird und nicht pauschal mit einer Auflistung allen möglichen Angriffsszenarien konfrontiert wird. Das Alert-System ist erfolgsversprechend, da aktuell erfolgreiche Angriffe auf das Online-Banking lediglich durch *Social Engineering* Angriffe ein ‚Fehlerverhalten' des Nutzers provozieren.
Wir nutzen und vergleichen unterschiedliche *‚off-the-shelf'* Algorithmen des maschinellen Lernens, um die aktuelle Gefahrenlage zu berechnen. Als Grundlage für die Berechnung werden unterschiedliche und freizugängliche Datenquellen genutzt, welche im direkten Zusammenhang zum Betrug im Online-Banking stehen (z.B. bekannt gewordene Phishing-Seiten von Banken). Wir überprüfen die Effektivität unseres Systems anhand von echten Betrugsfällen, die bei einer Bankengruppe aufgetreten sind. Unsere ersten Ergebnisse zeigen, dass die verwendeten Verfahren dazu geeignet sind die Gefahrenlage im Online-Banking zu bestimmen.

1 Einführung

Online-Banking und Online-Transaktionen sind ein wichtiger Teil der modernen Informationsgesellschaft und werden in Zukunft noch weiter an Bedeutung gewinnen. Allein in dem Zeitraum zwischen 2006 und 2015 wuchs die Nutzung von Online-Banking in Europa von 25% auf 46% an [1]. Aufgrund des rasanten Wachstums von Anwendungen, die Micro-Transaktionen nutzen und der generellen Digitalisierung der Gesellschaft, wird dieser Bereich auch in Zukunft weiter wachsen [2]. Online-Banking Systeme werden heutzutage erfolgreich von Betrügern angegriffen (z.B. [3]). Laut offiziellen Angaben des Bundeskriminalamtes entstand allein 2015 in Deutschland, durch Betrug beim Online-Banking, ein Schaden von insgesamt 17,9 Millionen Euro [4]. Es kann davon ausgegangen werden, dass der Schaden der tatsächlich entsteht deutlich höher ist, da Finanzinstitute ihre Kunden meist direkt entschädigen [5], um negativer Presse vorzubeugen.

Ein Angreifer, der einen erfolgreichen Angriff auf einen Online-Banking Nutzer durchführen will, muss, aufgrund der aktuellen Sicherungsverfahren (z.B. smsTAN oder chipTAN [6]), immer über einen *Social Engineering* Angriff den Nutzer zu einem ‚Fehlverhalten' verleiten. *Social Engineering* Angriffe sind sehr schwierig auf technischer Seite zu bekämpfen, daher muss der Nutzer in das Sicherheitskonzept im Online-Banking aufgenommen werden.

Ein möglicher Angriff auf das smsTAN Verfahren [6] startet meist durch Manipulationen der Bank-Webseite oder durch den Besuch einer Phishing Seite. Anschließend wird der Nutzer von dem Angreifer aufgefordert seine Handynummer einzugeben, um diese zu ‚überprüfen'. An die angegebene Handynummer wird anschließend eine SMS versendet, welche den Nutzer auffordert ein „Sicherheitszertifikat" zu installieren. Dieses „Sicherheitszertifikat" infiziert das Smartphone des Nutzers mit mobile Malware, welche die SMS mit der TAN einer Transaktion stiehlt und so dem Angreifer die Möglichkeit gibt beliebige Transaktionen durchzuführen (siehe auch [3]).

Das Alert-System, das in diesem Dokument vorgestellt wird, soll den Nutzer warnen, wenn eine besonders hohe Gefahr vorliegt, dass dieser im Online-Banking angegriffen wird. So kann dem Nutzer mitgeteilt werden, welche Gefahr vorliegt und er kann über die Angriffstechnik aufgeklärt werden. Dem Nutzer wird so die Möglichkeit gegeben besser auf *Social Engineering* Angriffe zu reagieren und diese leichter zu erkennen. Ein Vorteil ist, dass Nutzer über Gefahren aufgeklärt werden, wenn diese anliegen. So wird die Wahrscheinlichkeit, dass der Angriff erfolgreich ist verringert. Des Weiteren können „Fraud Prevention Systeme" von Finanzinstituten von einer Übersicht zu der aktuellen Gefahrenlage profitieren, um die Aktionen der Nutzer besser bewerten zu können (z.B. bei einer hohen Gefahrenlage sind Überweisungen in das Ausland verdächtiger, als bei einer geringen Gefahrenlage). Banken gehören in Deutschland zu den Kritischen Infrastrukturen [7] und sind somit verpflichtet Lagebilder zu dem Zustand der Struktur zu erstellen [8]. Die Gefahrenlage, die von dem vorgestellten Alert-System bestimmt wird, liefert wertvolle Informationen für die Erstellung eines Lagebildes.
Die Hauptaugenmerke dieser Arbeit liegen auf den folgenden Punkten:

- Wir identifizieren die Kennzahlen, die für die Bestimmung der aktuellen Gefahrenlage ausschlaggebend sind (Kapitel 2). Dabei haben wir uns in erster Linie auf Kennzahlen konzertiert, die frei zugänglich sind.
- Wir bestimmen die Zeitpunkte an denen die Gefahrenlage besonders groß ist. Wir validieren die identifizierten Zeitpunkte anhand von echten Betrugsfällen, die bei einer deutschen Bank aufgetreten sind (Kapitel 3).
- Wir untersuchen die Reaktion von Nutzern auf unterschiedliche Warnungen (Kapitel 4)

Verwandte Arbeiten werden in Kapitel 6 vorgestellt.

2 Konzept

Dieses Kapitel beschreibt den konzeptionellen Aufbau des entwickelten Alert-Systems. Die Kennzahlen, die zur Beurteilung der aktuellen Gefahrenlage genutzt werden, sind in Abschnitt 2.1 beschrieben. Ebenfalls werden Metriken für die Gewichtung der Kennzahlen und der Effektivität des Alert-Systems (Abschnitt 2.2) vorgestellt.

2.1 Kennzahlen

Phishing ist im Online-Banking eine weit verbreitete Strategie, um beispielsweise Passwörter, Kreditkartendaten oder TAN-Nummern zu stehlen. Phishing bezeichnet dabei die Technik den Benutzer durch gefälschte E-Mails und Internetseiten dazu zu bewegen, seine geheimen Informationen dem Angreifer preiszugeben. Daher ist es für ein Alert-System wichtig, dass Informationen zu dem aktuellen Aufkommen von Phishing (SPAM) zu erhalten. Innerhalb des entwickelten Systems werden drei Quellen genutzt, die für Phishing Angriffe genutzt werden:

- **E-Mail:** Klassischerweise werden Phishing Angriffe über E-Mails durchgeführt. Die Angreifer versenden eine E-Mail, die einer echten Nachricht der Bank gleicht, um den Kunden zu täuschen. In dieser Arbeit werden SPAM Nachrichten verwendet, die in dem „SPAM Archive“ [9] zur Verfügung gestellt werden. In dem Beobachtungszeitraum (456 Tage) wurden insgesamt 670.622 SPAM Mails in dem Archive veröffentlicht. Anhand einer Stichwortsuche konnten 5.589 Mails identifiziert werden, die in direkter Verbindung zum Betrug beim Online-Banking stehen.
- **Foren / Soziale Netzwerke:** Phishing Angriffe werden zunehmend auf anderen Plattformen, wie z.B. in sozialen Netzwerken, Foren, oder Ähnlichem durchgeführt. Hier wird das Phishing z.B. über private Nachrichten oder öffentliche Posts durchgeführt. In dieser Arbeit werden SPAM Nachrichten genutzt, die auf den Webseiten des „Stackoverflow“-Netzwerkes erkannt werden [10]. Basierend auf einer Schlagwort-Suche wurden 1.904 Nachrichten identifiziert, die im direkten Zusammenhang mit dem Betrug im Online-Banking stehen.
- **Webseiten:** Zusätzlich wird auf Information zu aktuellen Phishing Webseiten zurückgegriffen. Als Quelle für Phishing Seiten werden alle Seiten verwendet, die von der Organisation PhishTank [11] veröffentlicht wurden. Insgesamt wurden anhand einer Klassifizierung von PhishTank und einer Schlagwortsuche 2.776 Phishing-Seiten für den Testzeitraum gefunden, die im direkten Zusammenhang zum Betrug beim Online-Banking stehen.

Die Kennzahlen mit Phishing-Bezug wurden zusammengefasst, um die Dimension der entwickelten Ansätze möglichst klein zu halten.

Wichtig für die Einschätzung der aktuellen Gefahrenlage beim Online-Banking ist die Aktivität von Banking-Trojanern. Da keine globale Sicht zu den Botnetzen verfügbar ist, müssen andere Indizien genutzt werden, um die Gefahr, die von einem Botnetz ausgeht, beurteilen zu können. Die Anzahl der Endgeräte, die mit einem Banking-Trojaner infiziert wurden, ist ein starker Indikator dafür, dass ein Nutzer sich mit einem Banking Trojaner infizieren könnte (es wird eine Kampagne zum Verteilen des Trojaners durchgeführt). In dieser Arbeit haben wir die erkannten Infektionen (insgesamt 23.184 in dem Testzeitraum) von Banking-Trojanern eines großen Herstellers von Antivirus Produkten genutzt.

Die Gefahr, dass sich Nutzer mit Schadsoftware infizieren, kann anhand aktueller Schwachstellen gemessen werden. Die Kennzahlen zu bekannten Schwachstellen werden aus der *National Vulnerability Database* [12] (kurz NVD) extrahiert. Die NVD wird von dem *National Institute of Standards and Technology* (kurz NIST) verwaltet und beinhaltet Informationen zu Software Schwachstellen, gewissen Fehlkonfigurationen und Metriken zu deren Einfluss. Von dem System werden nur Schwachstellen beachtet, die Remote ausgenutzt werden können, gängige Browser und Betriebssysteme betreffen und die es erlauben willkürlich beliebigen Code auszuführen. Es werden diese Schwachstellen in Betracht gezogen, da sie von einem Angreifer zur Infektion des Endgerätes ausgenutzt werden können. In dem Testzeitraum traten 875 solcher Schwachstellen auf.

Für die Kontrolle des Systems werden echte Betrugsfälle, die bei einer deutschen Bankgruppe aufgetreten sind, genutzt. Anhand dieser Betrugsfälle kann die Qualität der entwickelten Verfahren gemessen werden. In dem Testzeitraum lagen 459 Betrugsfälle vor. Abbildung 1 zeigt den konzeptionellen Aufbau des Alert-Systems.

Abbildung 1 - Konzept des Alert-Systems

2.2 Metrik zur Messung der Effektivität des Systems

Die Effektivität des Alert-Systems *S* wird in erster Linie anhand der Anzahl der korrekt identifizierten Betrugsfälle gemessen, die innerhalb eines Testzeitraums angefallen sind. Dieser Wert wird in Relation mit der Anzahl aller vorhandenen Betrugsfälle gesetzt. Im Kontext der Zielsetzung des Alert-Systems wäre diese Relation, ohne die Betrachtung einer Zeitkomponente, trügerisch, denn *S* würde zwar vor allen Betrugsfällen warnen, wenn alle *n* Tage ein Alert erstellt werden würde und ein Alert ebenfalls für *n* Tage gültig wäre. Sollte aber die Menge der aktiven Alerts in einem bestimmten Zeitraum zu groß werden, verliert *S* im Kontext der Zielsetzung an Effektivität, denn der Vorteil einer punktuellen Warnung vor einem Angriffsmuster wäre in diesem Zusammenhang nicht mehr gegeben. Es muss also eine Metrik gewählt werden, die zum einen alle Alerts *A* und die daraus resultierende „Alert-Zeit" *T* in Betracht zieht. Insgesamt ergibt sich aus diesen Überlegungen die in Formel 1 dargestellte Berechnungsvorschrift für die Ermittlung der Effektivität von *S*.

Sei Ω die Anzahl aller Betrugsfälle, die in dem gesamten Testzeitraum *T* aufgetreten sind. Des Weiteren sei T_{Alert} der Zeitraum zu dem Alerts aktiv sind (*n* Tage nach einem Alert) und *ω* die Anzahl der Betrugsfälle die in T_{Alert} liegen. Die Effektivität des Systems steigt also, wenn *ω* steigt oder T_{Alert} fällt (oder beides).

$$eff(S) := \frac{\omega/\Omega}{T_{Alert}/T} = \frac{\omega * T}{\Omega * T_{Alert}}$$

Formel 1 – Berechnung der Effektivität des Alert-Systems

3 Bestimmung der Alarmierungszeitpunkte

Zur genauen Bestimmung der Alert-Zeitpunkte werden die gesammelten Hinweise aller Kategorien nach Tagen sortiert. Für jeden Tag wird anschließend ein Maß bestimmt, das die aktuelle Gefahrenlage anhand der Hinweise, die für diesen Tag vorliegen, angibt.

3.1 Trainings- und Testset

Alle gesammelten Daten wurden in ein Trainingsset (das erste Drittel der Daten – 152 Tage) und ein Testset (die restlichen zwei Drittel der Daten – 304 Tage) aufgeteilt.

Zum Trainieren der unterschiedlichen Ansätze wurden die gesammelten Kennzahlen (siehe Kapitel 2.1) in Bezug zu den Betrugsfällen, die in den zehn Tagen nach dem Auftreten der Kenn-

zahl aufgetreten sind, gesetzt. Bei der Vorhersage handelt es sich also um ein Regressionsproblem. Aus den Hinweisen (Phishing, Malware, Schwachstellen) wird versucht vorherzusagen, wie viele Betrugsfälle in den folgenden *n* Tagen auftreten werden.

Bei allen entwickelten Verfahren wurde ein Grenzwert, ab dem eine Warnung ausgegeben wird, anhand des Trainingssets bestimmt. Dazu wurde jeder Ansatz zunächst mit dem Trainingsset trainiert und anschließend wurde der Grenzwert, anhand der vorhergesagten Werte, bestimmt. Dazu wurde das trainierte Verfahren nochmals auf das Trainingsset angewendet. Als Grenzwert wurden die Top 5% (insgesamt ca. 16 Alerts je Ansatz) der bestimmten Gefahrenwerte (Anzahl der vorhergesagten Betrugsfälle) genutzt.

3.2 Allgemeines Lineares Modell

Als Vergleichswert für die Verfahren wurde ein allgemeines Lineares Model der Form $\vec{y} := \boldsymbol{X}\vec{\beta} + \vec{\epsilon}$ mit $\mathbf{X}$ den unabhängigen Variablen (hier den Kennzahlen), $\vec{\beta}$ den Regressionskoeffizienten, der anhand des Traingssets bestimmt wurde, und $\vec{\epsilon}$ dem Störfaktor genutzt. Zur Optimierung des Models wurde „iteratively reweighted least squares“ (IRLS) verwendet. IRLS ist ein Standardverfahren, um die Maximum-Likelihood in einem allgemeinen linearen Model zu bestimmen. Als grundlegende Verteilung der Daten wurde die Poisson-Verteilung angenommen, da davon ausgegangen wird, dass die Betrugsfälle unabhängig voneinander in einem zeitlich begrenzten und räumlich getrennten Umfeld voneinander auftreten.

Abbildung 2 zeigt das Ergebnis des allgemeinen linearen Modells. Die rote Linie zeigt an dem jeweiligen Zeitpunkt (X-Achse) den berechneten und skalierten Gefahrenwert an. Die schwarze Line stellt die skalierten und aufaddierten Hinweise zu dem jeweiligen Zeitpunkt dar. Die Punkte stellen die tatsächlich stattgefundenen Betrugsfälle dar und die Dreiecke die Warnungen, die von dem System ausgegeben werden.

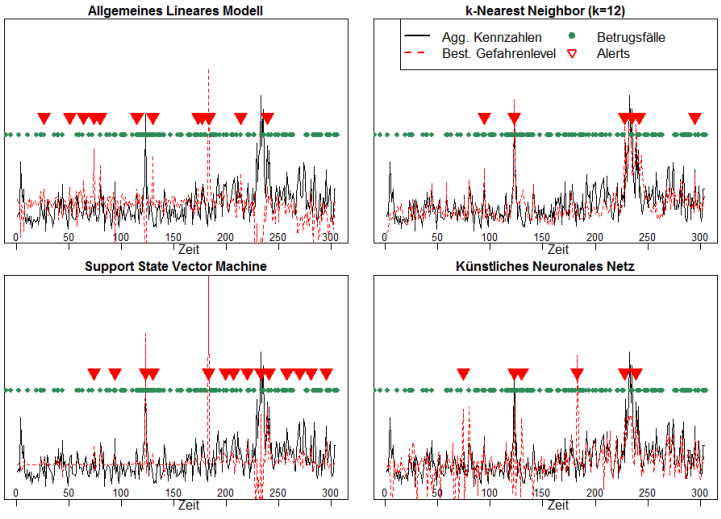

Abbildung 2 – Ergebnisse der vorgesellten Verfahren

3.3 k-Nearest Neighbor

Als erstes Verfahren wurde der *k-Nearest Neighbor* (k-NN) Algorithmus zur Bestimmung der Alert-Zeitpunkte verwendet.

Bei einer gegebenen Datenreihe (die aufaddierten Kennzahlen) kann der k-NN Wert für einen Datenpunkt als lokale Dichte der Datenreihe gesehen werden. Je größer der k-NN Wert ist, desto geringer ist die lokale Dichte und umso wahrscheinlicher ist es, dass es sich bei dem Punkt um einen Ausreißer handelt. Dieser „local outlier factor" ist verhältnismäßig simpel. Die Ergebnisse sind allerdings mit moderneren Verfahren vergleichbar [13]. Der Vorteil des k-NN Verfahrens ist, dass für jeden Datenpunkt ein Wert vorliegt, der angibt wie stark sich dieser von den Nachbarn unterscheidet.

Bei der Bestimmung der Ausreißer werden nur die *k* Datenwerte der Reihe verwendet, die *vor* dem zu untersuchendem Punkt liegen. Bei einem realistischen Einsatz des Systems liegen nur Messwerte aus der Vergangenheit vor, die zur Bewertung der Situation genutzt werden können. Aus diesem Grund beschränkt sich der Algorithmus nur auf die linken Nachbarn.

Zur Bestimmung des *k* wurden die Trainingsdaten verwendet. Dazu wurde *k* anhand der Funktion $eff(S)$ optimiert: $\max eff_k(S);\ \ k \in [1;20]$. Die Optimierung hat $k = 8$ als bestes k bestimmt. Abbildung 2 zeigt das Ergebnis des k-NN Ansatzes anhand der Testdaten. Wie zu erwarten, erkennt das k-NN Verfahren die Ausreißer in den Hinweisen (schwarze Linie).

3.4 Support State Vector Machine

Als weitere Technik wurde eine Support State Vector Machine (SVM) oder passender support vector regression (SVR) [14]) verwendet, um das geschilderte Regressionsproblem zu lösen. Die SVM wurde mittels des R-Pakets `e1071` [15] implementiert. Die verwendete SVM nutzt eine p*olynomielle* Kernel Funktion (ϕ) dritten Grades und führt eine ϵ-Regression durch. Zur Bestimmung des Models („model selection") wurden die Hyperparameter der SVM (cost und gama) mittels „grid search" optimiert.

Die Alerts, die von der SVM berechnet werden, sind in Abbildung 2 dargestellt. Einerseits ist anzumerken, dass die SVM Zeitpunkte, an denen augenscheinlich keine besondere Gefahr existiert (aggregierte Hinweise – schwarze Linie), als besonders gefährlich einstuft werden (z.B. ungefähr bei Zeitpunkt 175). Anderseits werden Zeitpunkte an denen augenscheinlich eine besondere Gefahr besteht, nicht direkt als gefährlich eingestuft (z.B. ungefähr bei Zeitpunkt 230). Beide Entscheidungen sind, aufgrund der auftretenden Schadensfälle, richtig.

3.5 Künstliche Neuronale Netze

Als letzter Ansatz wurde ein Künstliches Neuronales Netz (KNN) eingesetzt. Das Netz wurde als (3,3,1) Feed-Forward Netz (mittels des R Pakets `neuralnet` [16]) implementiert. Das heißt, dass jede Schicht nur mit der nächst höheren Schicht verbunden ist. 3 steht für die Anzahl der Input-Knoten, 3 für die Anzahl der Hidden-Knoten und 1 für die Anzahl der Output-Knoten. Das Netzwerk wurde mittels des RPROP Verfahren aufgebaut.

Das Ergebnis des KNN Ansatzes wird in Abbildung 2 dargestellt. Wie auch der SVM Ansatz erkennt das KNN die erhöhte Gefahrenlage nach Zeitpunkt 175. Allerdings erzeugt das KNN sehr viele Alerts zwischen Zeitpunkt 175 und 230. Dies führt dazu, dass die Effektivität des Systems mit 0,74 (siehe Abbildung 3) besser eingestuft wird als die Effektivität des SVM Ansatzes (T_{Alert} ist deutlich kleiner als bei dem SVM Ansatz).

3.6 Vergleich der Verfahren

Zur besseren Einschätzung der Qualität der entwickelten Verfahren werden diese mit zwei simplen Basiswerten verglichen. Für den ersten Basiswert werden Alerts zufällig platziert und deren Effektivität ($eff(S)$) wird gemessen. Diese Effektivität wurde über 100 Durchläufe gemessen und anschließend gemittelt. Als weiterer Vergleichswert werden 16 Alerts gleichmäßig auf den gesamten Testzeitraum aufgeteilt. Die Effektivität wird dann anhand dieser 16 Alerts gemessen.

Alle entwickelten Verfahren zeigen eine höhere Effektivität, für $n = 10$, als die verwendeten Basiswerte auf (siehe Abbildung 3). Wobei die Support State Vektor Machine und das neuronale Netz die besten Ergebnisse liefern.

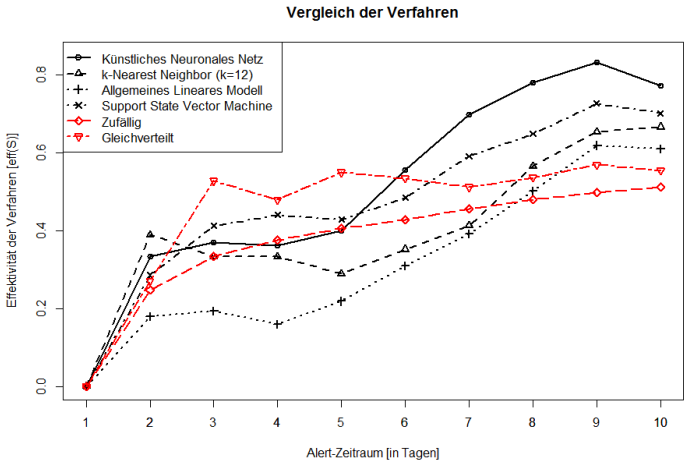

Abbildung 3 - Vergleich aller Verfahren

4 Nutzerstudie

Zum Thema „Nutzereinstellungen zu Alert-Systemen beim Online-Banking“ wurden im Zeitraum vom 02.03.17 bis 14.03.17 drei Fokusgruppendiskussionen mit insgesamt 15 Personen durchgeführt. Ziel war es einerseits von Nutzern die grundsätzliche Einstellung zum Einsatz von Alert-Systemen beim Online-Banking abzufragen. Andererseits wurden drei konkrete Design-Konzepte anhand von Screenshots mit den Teilnehmenden diskutiert und hierzu die Meinungen und Verbesserungsvorschläge abgefragt. Von den 15 Fokusgruppenteilnehmern waren neun weiblich und sechs männlich. Das Alter reichte von 23 bis 56 Jahre (M = 32.5, SD = 10.25). Die meisten Personen betreiben Online-Banking 1-4 Mal pro Monat vom eigenen Laptop bzw. PC aus und fühlen sich dabei „eher sicher“. Als Authentifizierungsverfahren werden am häufigsten TAN-Papierlisten und das smsTAN-Verfahren verwendet. Keiner der Teilnehmenden hat eigene Betrugserfahrungen gemacht.

In den drei Fokusgruppen wurden von den Teilnehmenden drei verschiedene Design-Konzepte von Alert-Systemen hinsichtlich möglicher Vor- und Nachteile sowie Verbesserungsvorschlägen zunächst jeweils in Kleingruppen und dann noch einmal im Plenum diskutiert. Hierbei handelte es sich einerseits um ein Ampel-System (siehe Abbildung 5) als kategoriale (siehe Abbildung 4, Links) und kontinuierliche Variante mit Prozentangaben (siehe Abbildung 4, Mitte). Anderseits wurde mit den Teilnehmenden ein Info-System mit aktueller Gefahrenmeldung (siehe Abbildung 4 , Rechts) diskutiert. Dieses bietet in der Detaildarstellung weitergehende

Beschreibungen und Erklärungen der (aktuellen) Gefahren beim Online-Banking (Abbildung 6).

Grundsätzlich positiv wird bei allen drei Systemen gewertet, dass diese beim Nutzer ein Bewusstsein für die Gefahren beim Online-Banking erzeugen und über die aktuelle Gefahrenlage informieren und damit zur Risikovermeidung beitragen. Die Nutzer wünschen sich, dass solch ein Alert-System von Seiten der Bank direkt bereits auf deren Startseite und nicht erst nach dem Einloggen in den persönlichen Account bereitgestellt wird.

Die beiden Ampel-Systeme (siehe Abbildung 4 und Abbildung 5, Links und Mitte) mit der Farbkodierung „ROT“ (hohe Gefahrenlage), „GELB“ (erhöhte Gefahrenlage) und „GRÜN“ (keine (besondere) Gefahren-lage) werden als leicht verständlich und übersichtlich eingeschätzt, gerade weil das mentale Model der Ampel-Farbkodierung allgemein bekannt ist. Jedoch merkten die Teilnehmenden bei beiden Systemen, anders als bei der Ampel im Straßenverkehr, eine gewisse Unsicherheit bezüglich des hieraus folgenden Nutzerverhaltens an. So wünschten sich die Teilnehmenden im Falle einer roten oder gelben Gefahrenmeldung eine konkrete Handlungsempfehlung, was nun als Nutzer von Online-Banking zu tun oder zu unterlassen ist. Mit Bezug zum Straßenverkehr stellten sich die Teilnehmenden zudem die Frage, ob ein „GRÜN“ nicht in diesem Fall eine falsche bzw. trügerische Sicherheit erzeugt, die es so nicht gibt, und in der Folge zu vermehrter Leichtgläubigkeit und Unachtsamkeit beim Online-Banking führt. Negativ wurde zu-dem bei beiden Varianten die englischen Fachbegriffe, wie z.B. Phishing oder Banking Mal-ware, gewertet, welche für den Laien unter Umständen unbekannt sind und auch nicht weiter erläutert werden.

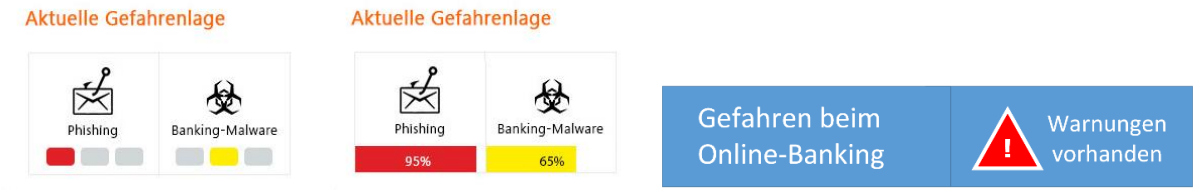

Abbildung 4 - Detaildarstellung der Gefahrenmeldung als kategoriales Ampel-System (Links), kontinuierliches Ampel-System (Mitte) und ein Info-System mit aktueller Gefahrenmeldung (Rechts)

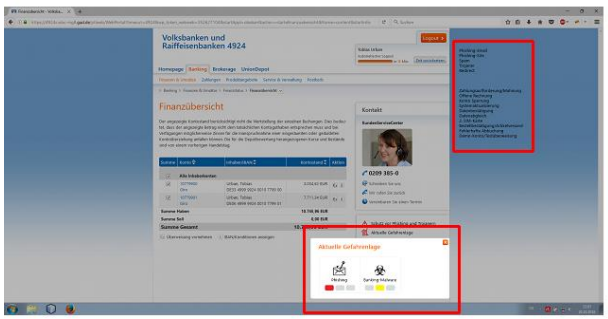

Abbildung 5 - Ampel-System auf der Online-Banking-Webseite nach dem Einloggen in den persönlichen Account

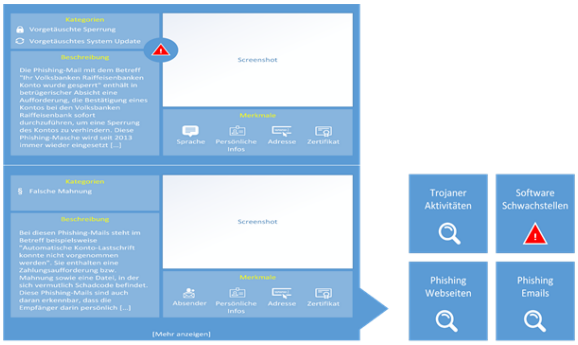

Abbildung 6 - Detaildarstellung des Info-Systems mit aktueller Gefahrenmeldung

Grundsätzlich wurde die kategoriale Ampel-Darstellung als positiver gewertet als die kontinuierliche Variante mit Prozentangaben. Gründe hierfür waren einerseits, dass Entstehung und Bedeutung der Prozentangaben für die Nutzer nicht nachvollziehbar waren. So fragten sich einige Teilnehmende, ob z.B. 50% für mehrere mittlere „Angriffe“ oder für wenige große steht. Andererseits wurde bemängelt, dass hierbei ein Gefühl von Genauigkeit erzeugt wird, welche so unter Umständen nicht existiert. Demzufolge wurde bei der Wahl zwischen beiden Varianten, die kategoriale Variante des Ampel-Systems ohne Prozentangaben bevorzugt. Jedoch wurde diese Version ebenfalls aufgrund der mangelnden Informationen über die Gefahren und die fehlenden Handlungsempfehlungen als kritisch angesehen. Zudem wird der Status „GRÜN“ als sehr problematisch gewertet, da dieser suggeriert, dass alles sicher ist und keine Gefahren existieren und der Nutzer unbedenklich agieren kann, was jedoch so beim Online-Banking nicht der Fall sein sollte.

Aufgrund der obengenannten Gründe wurde in allen drei Fokusgruppen das Info-System mit aktueller Gefahrenmeldung (Abbildung 6) am positivsten gewertet. Grundsätzlich weckt dieses System, wie die anderen beiden Ampel-Systeme auch, ein Bewusstsein für die Gefahren beim Online-Banking und trägt somit zur Risikovermeidung bei. Besonders positiv beurteilt wurden bei dieser Variante jedoch im Vergleich zu den anderen beiden Ampel-Systemen, dass zum einen eine generelle Informationsmöglichkeit über die „Gefahren beim Online-Banking“ gegeben wird und zum anderen ein konkreter und gut sichtbarer Warnhinweis in Form eines Warndreiecks über die aktuelle Gefahrenlage dargestellt ist. Sehr gelobt wurde in der Detailbeschreibung der Gefahr die Darstellung von Screenshots, z.B. um das Aussehen der konkreten Phishing Email zu erkennen. Diese Bildhaftigkeit hilft es Nutzern Angriffe besser zu identifizieren. Hilfreich wäre es hierbei auf diesen Screenshots etwaige Erkennungsmerkmale, z.B. Tippfehler in einer gefälschten URL, für die Nutzer speziell zu kennzeichnen, damit diese wissen, auf welche Merkmale besonders zu achten ist. Zudem wurde zunächst in ein bis zwei kurzen Sätzen eine generelle Beschreibung, worum es sich z.B. bei Phishing Emails handelt, gewünscht. Hiernach sollte dann eine Beschreibung der aktuellen Gefahr, z.B. Phishing Email als Mahnung, folgen. Danach sollten sich unter einer extra Zwischenüberschrift konkrete Handlungsempfehlungen, z.B. Löschen der Email, folgen. Bei diesem dreigliedrigen Vorgehen aus allgemeiner Gefahrenerklärung, Beschreibung der aktuellen Gefahr und konkreten Handlungsempfehlungen werden die Nutzer zunächst allgemein und speziell über die (aktuellen) Gefahren beim Online-Banking informiert und dann konkrete Verhaltensempfehlungen gegeben, um sich so besser zu schützen und aktiv zur Risikovermeidung beizutragen.

Generelle Fragen, welche sich die Teilnehmenden im Zusammenhang mit Alert-Systemen stellen, sind zum einen, ab welcher Gefahrenlage ein Warnhinweis bzw. ein Umschalten der Ampel

von „GRÜN“ auf „GELB“ oder „ROT“ erfolgt und wie häufig solche Statusmeldungen aktualisiert werden (z.B. stündlich oder wöchentlich). Auch wünschen sich die Nutzer, neben einer möglichst bildlichen Beschreibung der Gefahren, konkrete Handlungsempfehlungen für die jeweilige Bedrohung. Zum anderen fragen sich die Nutzer, ob sich mit dem Angebot der Warnung vor Gefahren beim Online-Banking auch die Verantwortung / Schadenshaftung auf den Nutzer überträgt und dann im Betrugsfall kein Schadensausgleich durch die Bank erfolgt.

Zusammenfassend ist festzuhalten, dass alle Teilnehmenden der drei Fokusgruppen ein auf ihrer Online-Banking-Seite bereitgestelltes Alert-System durchweg begrüßen würden. Als positiv wurde gewertet, dass damit ein Bewusstsein für die allgemeinen Gefahren beim Online-Banking erzeugt wird. Hinsichtlich der drei diskutierten Design-Konzepte wurde eindeutig das Info-System mit aktueller Gefahrenmeldung gegenüber den beiden Ampel-System-Varianten bevorzugt, da es mehr Informationen und Erklärungen für die Nutzer bereitstellt und weniger Unsicherheit bezüglich des aktuellen Gefahrengrades (z.B. Bedeutet „GRÜN“ sicher? Und was bedeuten „GELB“ oder „ROT“?) erzeugt. Grundsätzlich wichtig bei solch einem Alert-System sind den Nutzern sowohl allgemeine Erklärungen zu den verschiedenen Angriffsmöglichkeiten als auch die möglichst bildhafte Darstellung aktueller Gefahren, z.B. von sich aktuell im Umlauf befindlichen Phishing Emails. Zudem sollten neben der Gefahrenbeschreibung immer auch konkrete Handlungsempfehlungen für die Nutzer bereitgestellt werden, um diesen die aktive Risikovermeidung zu ermöglichen.

5 Fazit

Wir haben in dieser Arbeit gezeigt, dass mittels *‚off-the-shelf‘* Algorithmen die Gefahrenlage im Online-Banking effektiv bestimmt werden kann. Dabei haben wir fast ausschließlich freizugängliche Kennzahlen als Eingabedaten genutzt und unsere Ergebnisse mit echten Betrugsfällen einer Bankengruppe getestet. Eine Individualisierung der Algorithmen auf die gegebene Problemstellung und das Betrachten von bekannt gewordenen Betrugsfällen als Eingabe (nicht wie in dieser Arbeit lediglich als Vergleichswert) würde die Effektivität des Alert-System wahrscheinlich stark steigern. Unsere Erkenntnisse können zum einen genutzt werden, um die Awarness der Nutzer zu steigern und zum anderen, um Fraud Prevention Systeme von Finanzinstituten zu verbessern.

6 Verwandte Arbeiten

Alert-Systeme: Akhawe und Felt untersuchen in [17] wie Nutzer auf Warnmeldungen in den populären Webbrowsern Firefox und Google Chrome reagieren. Innerhalb der Nutzerstudie wurde das Verhalten von Nutzern bei über 25 Millionen Fehlernmeldungen im Browser analysiert. Die Ergebnisse zeigen, dass Warnmeldungen, z.B. bei unsicheren SSL-Verbindungen oder Webseiten die Malware verbreiten, ein effektiver Weg sein können Nutzer vor Angriffen zu schützen. Weniger als ein Viertel der Nutzer klickt die Warnungen weg, was zeigt, dass Warnungen einen gewaltigen Einfluss auf das Nutzungsverhalten im Web haben.

Eine frühere Nutzerstudie zu SSL-Warnungen im Webbrowser [18] hat aufgezeigt, dass das Desgin der Warnungen äußerst wichtig für die Effektivität dieser ist. Allerdings zeigen die Ergebnisse auch, dass Nutzer oft Warnungen ignorieren, weil Sie ein falsches Verständnis von den Gefahren haben. In der Nutzerstudie haben Nutzer angeben, dass sie denken dass Man-in-the-Middel Angriffe bei bekannten Seiten (z.B. der einer Bank) selten auftreten und daher SSL-Warnungen ignoriert werden können.

Phishing im Browser: Die Effektivität von „domain highlighting“ wird in einer Nutzerstudie von Lin et al. untersucht [19]. Domain highlighting ist ein Mechanismus, in modernen Webbrowsern, bei dem der Domainname hervorgehoben wird (z.B. fett gedruckt). Das Ziel ist Nutzer darauf aufmerksam werden, wenn Sie sich auf einer Phishing-Seite befinden. Innerhalb der Nutzerstudie wurde ermittelt, dass Domain highlighting nur einen geringen Schutz vor Phishing Angriffen bietet.

Eine demographische Analyse zur Anfälligkeit für Phishing Angriffe führen Shen et al. in [20] durch. Dabei zeigen Sie, dass jüngere Menschen anfälliger für Phishing Angriffe sind als ältere Menschen. Allerdings konnten durch Aufklärungen und Warnungen die Anfälligkeit für Phishing Angriffe, in der durchgeführten Nutzerstudie, um ca. 40% reduziert werden.

Mobile Phishing: Neben Webseiten werden ebenfalls Smartphone Apps vermehrt zum Ziel von Phishing Angriffen [21]. Hier werden Apps installiert, deren GUI der originalen App gleicht. So wird versucht sensible Daten des Nutzers zu stehlen. Als Gegenmaßnahmen zu diesen Angriffen wird in aktuellen Arbeiten die Personalisierung von Apps vorgeschlagen, um das Fälschen zu erschweren [22].

7 References

[1] Eurostat, the statistical office of the European Union, *Individuals using the internet for internet banking.* [Online] Available: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00099. Accessed on: Sep. 21 2016.

[2] M. Mäntymäki and J. Salo, “Why do teens spend real money in virtual worlds?: A consumption values and developmental psychology perspective on virtual consumption,” *International Journal of Information Management*, vol. 35, no. 1, pp. 124–134, 2015.

[3] S. Golovanov, D. Makrushin, and A. Monastyrsky, *Staying safe from virtual robbers.* [Online] Available: https://securelist.com/analysis/user-advice/58328/staying-safe-from-virtual-robbers/. Accessed on: Jun. 21 2016.

[4] Bundeskriminalamt, *Bundeslagebild Cybercrime 2015*, vol. 2015. Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.pdf?__blob=publicationFile&v=6. Accessed on: Jul. 25 2016.

[5] CosmosDirekt, *FinanzSchutz.* [Online] Available: https://www.cosmosdirekt.de/finanzschutz-allgemein/. Accessed on: Dec. 23 2016.

[6] Sparkassen-Finanzportal, *TAN-Verfahren: pushTAN, smsTAN, chipTAN.* [Online] Available: https://www.sparkasse.de/service/sicherheit-im-internet/tan-verfahren.html. Accessed on: Jan. 05 2017.

[7] Bundesamt für Sicherheit in der Informationstechnik, “KRITIS-Sektorstudie Finanz- und Versicherungswesen,” http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Finanzen_Versicherungen.pdf;jsessionid=07758D8AFA6F10955C1D076DA6F78CC7.1_cid330?__blob=publicationFile, 2015.

[8] Bundesministerium des Innern, “Schutz Kritischer Infrastrukturen Behörden – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden,” 2011.

[9] Bruce Guenter, *SPAM Archive.* [Online] Available: http://untroubled.org/spam/. Accessed on: Sep. 30 2016.

[10] Stack Exchange Inc, *SmokeDetector*. [Online] Available: https://metasmoke.erwaysoftware.com/search.json?body=financial. Accessed on: Jan. 09 2017.

[11] OpenDNS, *PhishTank | Join the fight against phishing.* [Online] Available: https://www.phishtank.com/. Accessed on: Sep. 30 2016.

[12] National Institute of Standards and Technology, *National Vulnerability Database.* [Online] Available: https://nvd.nist.gov/. Accessed on: May 02 2016.

[13] G. O. Campos *et al.*, "On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study," *Data Mining and Knowledge Discovery*, vol. 30, no. 4, pp. 891–927, http://dx.doi.org/10.1007/s10618-015-0444-8, 2016.

[14] Harris Drucker *et al.*, *Support Vector Regression Machines*.

[15] D. Meyer, E. Dimitriadou, K. Hornik, A. Weingessel, and F. Leisch, *e1071: Misc Functions of the Department of Statistics, Probability Theory Group (Formerly: E1071), TU Wien.* Available: https://CRAN.R-project.org/package=e1071.

[16] S. Fritsch, F. Guenther, and f. e. w. b. M. Suling, *neuralnet: Training of neural networks.* Available: https://CRAN.R-project.org/package=neuralnet.

[17] D. Akhawe and A. P. Felt, "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness," in *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C.: USENIX, 2013, pp. 257–272.

[18] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: An Empirical Study of SSL Warning Effectiveness," in *Proceedings of the 18th Conference on USENIX Security Symposium*, Berkeley, CA, USA: USENIX Association, 2009, pp. 399–416.

[19] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock, "Does domain highlighting help people identify phishing sites?," in *Conference proceedings and extended abstracts / the 29th Annual CHI Conference on Human Factors in Computing Systems: CHI 2011, Vancouver, BC, May 7 - 12, 2011*, New York, NY: ACM, 2011, p. 2075.

[20] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?," in *CHI 2010 - we are HCI: Conference proceedings and extended abstracts ; the 28th Annual CHI Conference on Human Factors in Computing Systems, April 10 - 15, 2010 in Atlanta, GA, USA*, New York, NY: ACM, 2010, p. 373.

[21] A. Vishwanath, "Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks," *Computers in Human Behavior*, vol. 63, pp. 198–207, 2016.

[22] C. Marforio, R. Jayaram Masti, C. Soriente, K. Kostiainen, and S. Čapkun, "Evaluation of Personalized Security Indicators as an Anti-Phishing Mechanism for Smartphone Applications," in *CHI 2016: #chi4good ; proceedings ; The 34rd Annual CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, May 07 - 12, 2016*, New York, NY: ACM, 2016, pp. 540–551.