Sei gewarnt! Vorhersage von Angriffen im Online-Banking

Tobias Urban[1], René Riedel[1], Christine Paulisch[2], Norbert Pohlmann[1]

[1]Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
{urban | riedel | pohlmann}@internet-sicherheit.de

[2]Institut für Psychologie und Arbeitswissenschaft
Technische Universität Berlin
{christine.paulisch}@mms.tu-berlin.de

Zusammenfassung

In diesem Artikel wird ein Alert-System für das Online-Banking vorgestellt, welches das Schutzniveau im Kontext von *Social-Engineering*-Angriffen sowohl clientseitig als auch serverseitig erhöhen soll. Hierfür wird durch das Alert-System ein kontinuierliches Lagebild über die aktuelle Gefahrenlage beim Online-Banking erstellt. Bei konkretem Bedarf wird der Nutzer punktuell vor aktuellen Betrugsmaschen gewarnt und zielgerichtet über Schutzvorkehrungen und Handlungsempfehlungen informiert.
Für die Berechnung der aktuellen Gefahrenlage wurden unterschiedliche *off-the-shelf*-Algorithmen des Maschinellen Lernens verwendet und miteinander verglichen. Die Effektivität des Alert-Systems wurde anhand von echten Betrugsfällen evaluiert, die bei einer Bankengruppe in Deutschland aufgetreten sind. Zusätzlich wurde die Usability des Systems in einer Nutzerstudie mit 50 Teilnehmern untersucht. Die ersten Ergebnisse zeigen, dass die verwendeten Verfahren dazu geeignet sind, die Gefahrenlage im Online-Banking zu beurteilen und dass ein solches Alert-System auf hohe Akzeptanz bei Nutzern stößt.

1 Einführung

Online-Banking und Online-Transaktionen sind ein wichtiger Teil der modernen Informationsgesellschaft und werden in Zukunft noch weiter an Bedeutung gewinnen. Allein zwischen 2006 und 2016 stieg die Nutzung von Online-Banking in Europa von 25% auf 49% an [1]. Aufgrund des Wachstums von Anwendungen die Micro-Transaktionen nutzen und der fortschreitenden Digitalisierung der Gesellschaft, wird dieser Bereich auch in Zukunft weiter wachsen [2].

Online-Banking Systeme werden heutzutage erfolgreich von Betrügern angegriffen (siehe z. B. [3]). Laut offiziellen Angaben des Bundeskriminalamtes entstand allein 2016 in Deutschland ein Schaden von insgesamt 8,7 Millionen Euro [4] im Zusammenhang mit Phishing im Online-Banking. Es kann davon ausgegangen werden, dass der tatsächlich entstandene Schaden deutlich höher ist, da die Dunkelziffer bei der Aufklärung von Cyberkriminalität generell hoch ist und Finanzinstitute ihre Kunden meist direkt entschädigen [5], um z. B. negativer Presse und dem damit verbundenen Reputationsschaden vorzubeugen.

P. Schartner · N.N (Hrsg.) · DACH Security YYYY · syssec (YYYY) pp-pp.

Aufgrund der aktuellen Sicherungsverfahren (z. B. smsTAN oder chipTAN [6]) muss der Online-Banking-Nutzer von einem Angreifer initial zu einem Fehlverhalten verleitet werden, damit ein erfolgreicher Angriff überhaupt erst möglich ist. Die Erkennung und Bekämpfung von *Social-Engineering*-Angriffen ist auf technischer Seite nur schwer zu realisieren. Aus diesem Grund muss der Nutzer in das Sicherheitskonzept des Online-Bankings eingebunden werden.

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 Abwehrmaßnahmen 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 real auftreten. So wird die Wahrscheinlichkeit, dass der Angriff erfolgreich ist, verringert. Des Weiteren können *Fraud-Prevention-Systeme* von Finanzinstituten von einer Übersicht zur aktuellen Gefahrenlage profitieren, um die Aktionen der Nutzer besser bewerten zu können, z. B. sind bei einer hohen Gefahrenlage Überweisungen ins Ausland verdächtiger, als bei einer geringen Gefahrenlage.

Banken gehören in Deutschland zu den kritischen Infrastrukturen [7] und sind somit verpflichtet, Lagebilder zum Zustand der Struktur zu erstellen [8]. Die Gefahrenlage, die von dem vorgestellten Alert-System bestimmt wird, liefert wertvolle Informationen für solche Lagebilder. Die Hauptaugenmerke dieser Arbeit liegen auf den folgenden Punkten:

- Es wurden wichtige Kennzahlen identifiziert, die für die Bestimmung der aktuellen Gefahrenlage ausschlaggebend sind (Kapitel 2).
- Es wurden die Zeitpunkte, an denen die Gefahrenlage besonders groß ist, bestimmt. Validiert wurden ebenso die identifizierten Zeitpunkte anhand echter Betrugsfälle, die bei einer deutschen Bank aufgetreten sind (Kapitel 3).
- In einer Nutzerstudie ($n = 50$) wurde die Nutzerfreundlichkeit, das Sicherheitsempfinden, das Nutzungsverhalten und die Akzeptanz des Systems untersucht (Kapitel 4).

Verwandte Arbeiten werden in Kapitel 6 vorgestellt.

2 Konzept

Im Folgenden wird der konzeptionelle Aufbau des entwickelten Alert-Systems erläutert. Es werden die ermittelten Kennzahlen (Abschnitt 2.1) sowie die Metrik zur Evaluierung des Alert-Systems beschrieben (Abschnitt 2.2).

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 z. B. durch gefälschte E-Mails und Internetseiten dazu zu bewegen, dem Angreifer seine geheimen Informationen preiszugeben. Daher ist es für das hier vorgestellte Alert-System wichtig, Informationen zum aktuellen Aufkommen von Phishing (Spam) zu erhalten. Aus den verwendeten Quellen werden nur Informationen extrahiert, die im direkten Zusammenhang mit Online-Banking stehen. Innerhalb des entwickelten *Alert-Systems* werden drei Quellen genutzt, die für Phishing-Angriffe relevant sind:

- **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 im „Spam Archive“ [9] zur Verfügung gestellt werden. Im Beobachtungszeitraum (456 Tage) wurden insgesamt 670.622 Spam-Mails im Archive veröffentlicht. Anhand einer Stichwortsuche konnten 5.589 relevante Mails identifiziert werden.

- **Foren / Soziale Netzwerke:** Phishing-Angriffe werden zunehmend auf anderen Plattformen, 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.
- **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 Kennzahlen mit Bezug zum Phishing wurden zusammengefasst, um die Dimension der entwickelten Ansätze möglichst klein zu halten.

Wichtig für die Einschätzung der aktuellen Gefahrenlage beim Online-Banking ist auch die Aktivität von Banking-Trojanern. Da keine globale Sicht zu den zugehörigen *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 sich ein Nutzer mit einem Banking-Trojaner infizieren könnte (z.B. wenn der Angreifer eine ‚Kampagne‘ zum Verteilen des Trojaners durchführt). In dieser Arbeit wurden die erkannten Infektionen (insgesamt 23.184 im Testzeitraum) von Banking-Trojanern durch einen großen Hersteller von Antivirus-Produkten genutzt.

Die Gefahr, dass sich Nutzer mit Schadsoftware infizieren, kann aber auch anhand aktueller Software-Schwachstellen gemessen werden. Die Kennzahlen zu bekannten Schwachstellen werden aus der *National Vulnerability Database* [12] (kurz NVD) extrahiert. Die NVD beinhaltet Informationen zu Software-Schwachstellen, Fehlkonfigurationen und Metriken zu deren Einfluss. Von dem entwickelten Alert-System werden nur Schwachstellen beachtet, die Remote ausgenutzt werden können, gängige Browser und Betriebssysteme betreffen und die es erlauben beliebigen Code auszuführen. In dem Testzeitraum traten 875 solcher Schwachstellen auf.

Für die Kontrolle des Alert-Systems werden Betrugsfälle, die bei einer deutschen Bankgruppe aufgetreten sind, genutzt. Anhand dieser Betrugsfälle kann die Effizienz der entwickelten Verfahren gemessen werden. In dem Testzeitraum lagen 459 Betrugsfälle vor. Abbildung 1 zeigt die genutzten Quellen und deren Verwendung in dem Aufbau des Alert-Systems.

2.2 Metrik zur Messung der Effektivität des Alert-Systems

Die Effektivität des Alert-Systems S wird in erster Linie anhand der Anzahl der korrekt identifizierten Betrugsfälle gemessen. Dieser Wert wird in Relation zur Anzahl aller vorhandenen Betrugsfälle gesetzt. Für die Zielsetzung des Alert-Systems wird zusätzlich eine Zeitkomponente zur Bestimmung der Effektivität hinzugefügt, damit die Menge der aktiven Alerts reguliert werden kann. Ohne die Zeitkomponente könnte beispielsweise die Menge der aktiven Alerts zu groß und somit der angestrebte Mehrwert durch eine punktuelle Warnung verringert werden. Es muss also eine Metrik gewählt werden, die 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.

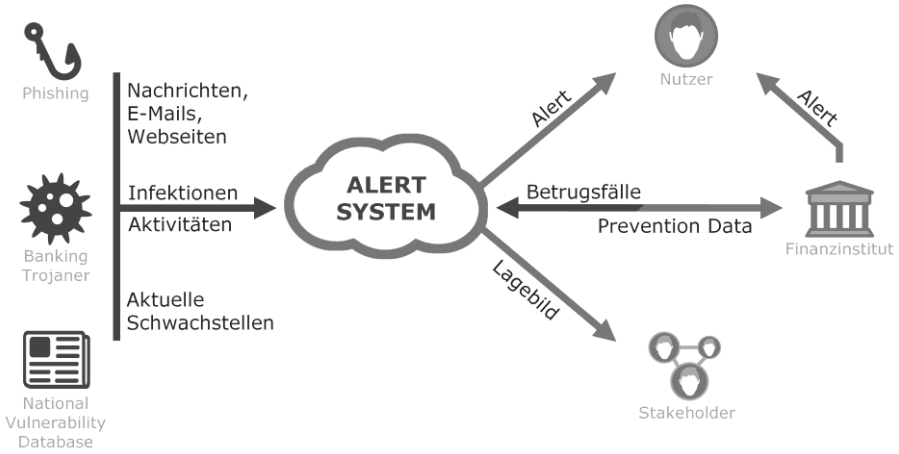

Abbildung 1 - Konzept des entwickelten Alert-Systems

Sei Ω die Anzahl aller Betrugsfälle, die im 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 Alert-Systems steigt demnach, wenn ω steigt oder T_{Alert} fällt (oder beides).

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

Formel 1 – Berechnungsvorschrift für die Effektivität des Alert-Systems

3 Bestimmung der Alarmierungszeitpunkte

Für die Bestimmung der Alert-Zeitpunkte werden die gesammelten Kennzahlen aller Kategorien zuerst nach Tagen sortiert. Anschließend wird mit Hilfe der betrachteten *off-the-shelf*-Algorithmen für jeden Tag ein Maß bestimmt, das die aktuelle Gefahrenlage beschreibt. In diesem Kapitel werden die verschiedenen Ansätze vorgestellt und die resultierenden Metriken der betrachteten Algorithmen miteinander verglichen.

3.1 Trainings- und Testset

Alle gesammelten Daten werden in ein Trainingsset (das erste Drittel der Daten – 152 Tage) und ein Testset (die restlichen zwei Drittel der Daten – 304 Tage) aufgeteilt, um die Vorhersagekraft der einzelnen Ansätze zu ermitteln und zu vergleichen.

Zum Trainieren der unterschiedlichen Ansätze werden die gesammelten in Bezug zu den Betrugsfällen, die in den zehn Tagen nach dem Auftreten der Kennzahl aufgetreten sind, gesetzt. Bei der Vorhersage handelt es sich also um ein Regressionsproblem. Anhand der vorliegenden Kennzahlen (Phishing, Malware und Schwachstellen) zum Zeitpunkt t wird versucht vorherzusagen, wie viele Betrugsfälle in den folgenden n Tagen auftreten werden.

Als Grenzwerte für das Ausgeben eines Alerts wurden die Top 5% (insgesamt ca. 16 Alerts je Ansatz) der bestimmten Gefahrenwerte (Anzahl der vorhergesagten Betrugsfälle) innerhalb des Trainingszeitraums genutzt. Der bestimmte Gefahrenwert der verschiedenen Ansätze kann ebenfalls für *Fraud-Prevention-Systeme* genutzt werden, um Transaktionen zu bewerten.

Als Vergleichswert für die Verfahren wurde ein allgemeines Lineares Model der Form $\vec{y} := \boldsymbol{X}\vec{\beta} + \vec{\epsilon}$ mit **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 die Methode *iteratively reweighted least squares* (IRLS) verwendet. IRLS bestimmt die Maximum-Likelihood in einem allgemeinen linearen Model.

3.2 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 Alert-Systems liegen nur Messwerte aus der Vergangenheit vor, die zur Bewertung der Situation genutzt werden können. Zur Bestimmung von *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 optimales *k* bestimmt.

3.3 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 verwendete SVM nutzt eine *polynomielle* 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.

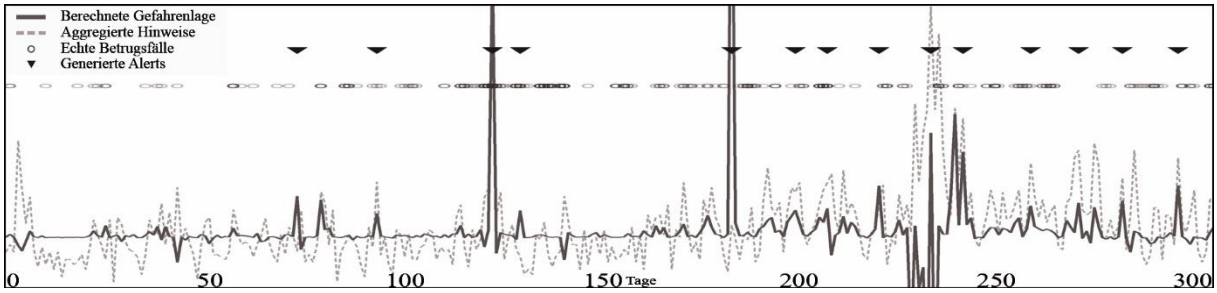

Abbildung 2 - Berechnete Gefahrenlage mittels Support State Vector Machine

3.4 Künstliche Neuronale Netze

Als letzter Ansatz wurde ein *Künstliches Neuronales Netz* (KNN) eingesetzt. Das Netz wurde als (3,3,1) Feed-Forward-Netz 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-Verfahrens aufgebaut. Das Ergebnis des KNN-Ansatzes wird Abbildung 3 dargestellt.

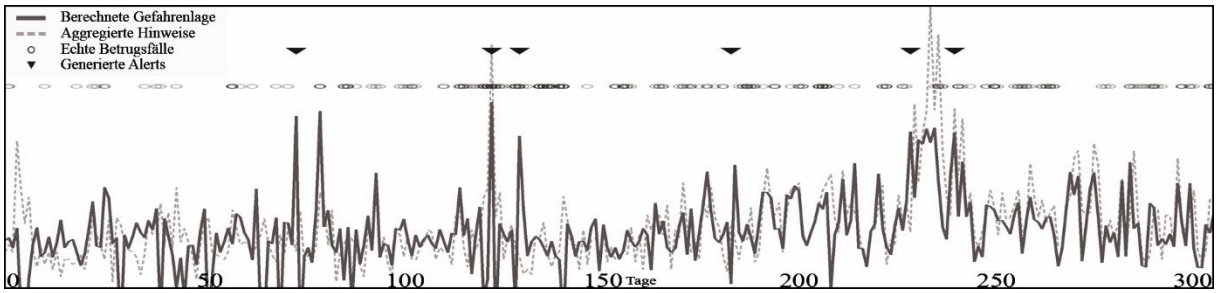

Abbildung 3 - Berechnete Gefahrenlage mittels Künstlicher Neuronaler Netze

3.5 Vergleich der Verfahren

Zur besseren Einschätzung der Qualität der entwickelten Verfahren werden diese mit zwei 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 (siehe Abbildung 4), wobei das *Neuronale Netz* die besten Ergebnisse liefert. Ebenfalls wird deutlich, dass ein Alarmierungszeitraum von mehr als sieben Tagen einen deutlichen Anstieg der Effizienz des Systems führt. Ides liegt auch daran, dass die verfahren mit einem Wert von $n = 10$ trainiert wurden.

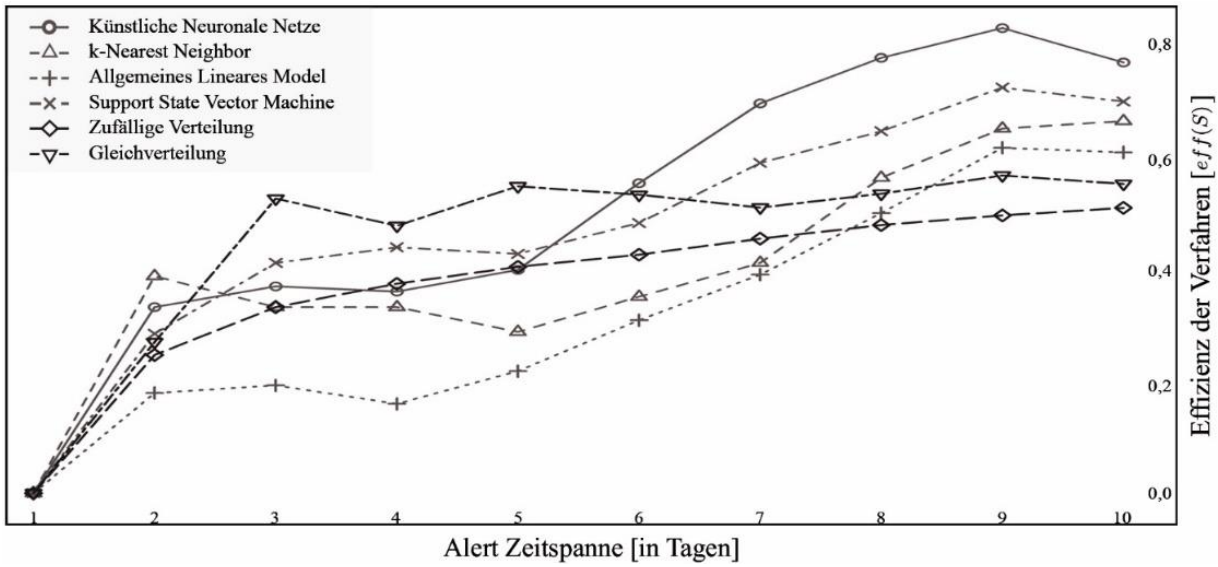

Abbildung 4 - Vergleich der Effizienz aller Verfahren

3.6 Diskussion

Das erzeugte *Neuronale Netz* hat im durchgeführten Vergleich die besten Ergebnisse geliefert, allerdings ist die Zeit für das Trainieren des Systems deutlich höher (ca. dreifach so hoch) als bei den anderen betrachteten Verfahren.

Zur weiteren Optimierung der Bestimmung der Gefahrenwerte können weitere Kennzahlen in Betracht gezogen werden (z. B. die Aktivitäten von Banking-Malware innerhalb von Botnetzen oder auf mobilen Endgeräten). Ebenfalls können die Schadensfälle selbst als Hinweise genutzt werden und nicht wie in dieser Arbeit nur als Kontrollwerte.

Die von uns genutzten Hinweise bezüglich Phishing können weitaus umfangreicher gesammelt werden. Es können beispielsweise weitere Soziale Netzwerke oder weitere Spam Honeypots als Hinweise genutzt werden. Bei einer größeren Menge an Hinweisen sollten jedoch modernere Ansätze der künstlichen Intelligenz („deep learning“) evaluiert werden. In dieser Arbeit wurden diese, aufgrund der limitierten Menge an Trainingsdaten, nicht betrachtet.

Die vom Alert-System bestimmte Gefahrenlage kann von einem Fraud-Prevention-System genutzt werden, um die Erkennung von bösartigen Transaktionen zu unterstützen. In Folge dessen könnte bei einem hohen Gefahrenwert und bei einer verdächtigen Transaktion das Autorisierungsverfahren dynamisch (z.B. mehr Sicherheit auf Kosten von weniger Benutzerfreundlichkeit oder umgekehrt) festgelegt werden. Somit kann das Alert-System gleichermaßen zum bankenseitigen und nutzerseitigen Schutz genutzt werden.

4 Nutzerstudie

Um eine ganzheitliche Sicht auf das Alert-System zu erhalten, sollte über die technische Umsetzung hinaus die Nutzerperspektive betrachtet werden. In diesem Kapitel werden die Ziele, die Durchführung und die Ergebnisse der Nutzerstudie vorgestellt. Vom Alert-System wurde sowohl eine Webseiten-Variante (Abbildung 6) als auch eine Smartphone-Variante untersucht. Das Alert-System wurde in der Studie auf der Login-Seite einer Bank präsentiert. Problematisch bei der Gestaltung der Alerts ist, dass ein Angreifer diese fälschen könnte. Daher muss die Alarmierung der Nutzer über einen überprüfbaren Kanal (z.B. signierte E-Mail) oder ein Kanal der von einem Angriff nicht Betroffen ist (z.B. Webseite bei einer Phishing-Welle) geschehen.

4.1 Untersuchungsziele

Ziel dieser Studie war es, dieses Alert-System hinsichtlich verschiedener Aspekte zu untersuchen. Betrachtet wurden die allgemeine *Nutzerfreundlichkeit* (z. B. Verständlichkeit), die *Vertrauenswürdigkeit*, die *Akzeptanz*, das potentielle *Nutzungsverhalten* sowie das *Sicherheitsgefühl* durch so ein Alert-System. Zudem ging es um die Frage, auf welchem Gerät (Webseite/PC vs. Smartphone) es von den Nutzern gegebenenfalls bevorzugt wird.

Eine Fragestellung bezüglich des Popup-Fensters war, welche der zwei Reiter-Reihenfolgen von den Nutzern präferiert wird. Die 1. Reihenfolge lautete: *Betrugsfälle | Was sind Trojaner? | Wie kann ich mich schützen?* Bei der 2. Reihenfolge (Abbildung 5) waren die ersten beiden Reiter umgekehrt: *Was sind Trojaner? | Betrugsfälle | Wie kann ich mich schützen?* Beim Reiter *Betrugsfälle* gab es ebenfalls zwei Möglichkeiten. Bei aktueller Gefahrenlage hieß der Reiter *Aktuelle Betrugsfälle* und enthielt ein Warndreieck. Ohne aktuelle Gefahrenlage wurden bei-

Abbildung 5 - 2. Reiter-Reihenfolge, ohne aktuelle Gefahrenlage

spielhalft Betrugsfälle aus der Vergangenheit aufgeführt und der Reiter mit *Bekannte Betrugsfälle* bezeichnet (Abbildung 6). Die Frage war, welche Reihenfolge bevorzugt wird, bei jeweils aktueller Gefahrenlage und ohne aktuelle Gefahrenlage.

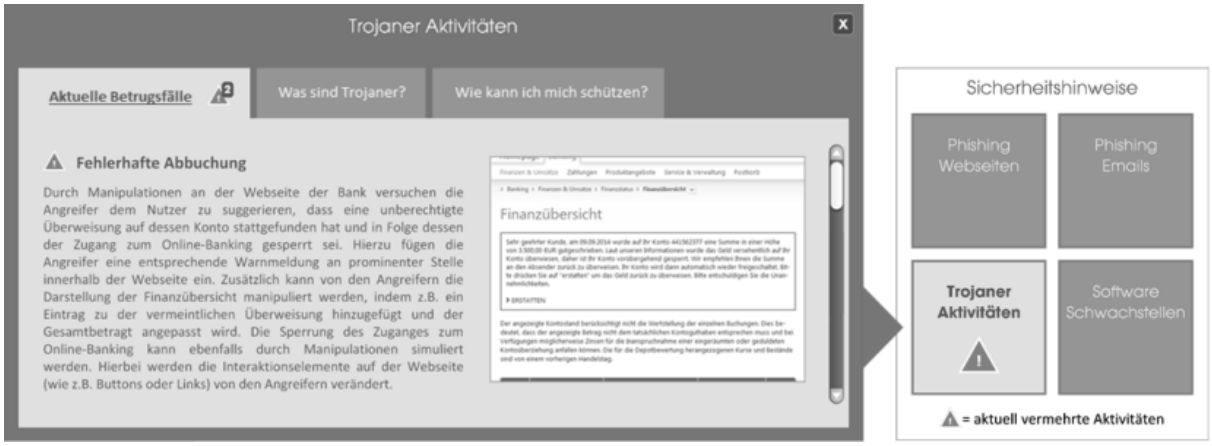

Abbildung 6 - Darstellung des Alert-Systems mit geöffnetem Popup-Fenster, 1. Reiter-Reihenfolge, mit aktueller Gefahrenlage (Warndreieck)

4.2 Versuchspersonenbeschreibung

Die Nutzerstudie wurde mit 50 Versuchspersonen (24 männlich, 26 weiblich) durchgeführt und die Personen möglichst altersrepräsentativ rekrutiert. Der Altersdurchschnitt lag bei 39,1 Jahren (sd = 12,6 Jahre), die Altersspanne bei 21 bis 67 Jahren. Es befanden sich 4% in Ausbildung und 40% im Studium. 30% waren Angestellte, 2% Beamte, 10% Selbstständige, 2% Hausfrauen/-männer, 6% ohne Arbeit und 4% sonstiges. Voraussetzung zur Teilnahme waren Erfahrungen im Umgang mit Online-Banking und Smartphones.

4.3 Durchführung

Die Nutzerstudie wurde im Juli und August 2017 durchgeführt. Die Versuchspersonen erhielten 10 Euro für ihre Teilnahme. Eine Sitzung dauerte etwa 45 Minuten. Zu Beginn wurden die Versuchsteilnehmer begrüßt und über den Versuchsablauf aufgeklärt. Anschließend wurde das Alert-System auf der Webseite auf einem PC-Bildschirm gezeigt, der Versuchsperson Fragen gestellt und sie gebeten, laut zu denken. Was die Reihenfolge der Reiter anging, wurden 25 Versuchspersonen die 1.Variante und 25 Versuchspersonen die 2.Variante gezeigt. Den Versuchspersonen wurden zwischendurch Fragebögen vorgelegt. Zum Schluss wurde die Smartphone-Variante des Alert-Systems gezeigt. Die Untersuchung endete mit einem demographischen Fragebogen. Während des Versuchs machte sich die Versuchsleiterin Notizen und das Gesagte wurde auf einem Diktiergerät aufgenommen.

4.4 Ergebnisse

Verständlichkeit: Den Versuchspersonen war klar, dass es sich bei dem Alert-System um ein Informationssystem handelt, das Sicherheitshinweise zum Online-Banking, bzw. zur Internetsicherheit bereitstellt. Erwartet wurde, dass nach einem Klick auf die Kacheln weitere Informationen erscheinen, etwa in Form eines Fensters oder in einem sich neu öffnenden Tab. Das Warndreieck wurde assoziiert mit einem wichtigen Hinweis, der die Aufmerksamkeit auf sich zieht. Die Darstellung des Fensters mit Reitern wurde als übersichtlich empfunden.

Bezeichnungen und Reihenfolge der Tabs: Die beiden Bezeichnungen *Was sind Trojaner?* und *Wie kann ich mich schützen?* wurden als verständlich angesehen. Der Unterschied zwischen *Aktuelle Betrugsfälle* und *Bekannte Betrugsfälle* war den Versuchspersonen meist klar. Jedoch wurde die Bezeichnung *Aktuelle Betrugsfälle* z. T. als nicht ganz passend empfunden. Bei der Reihenfolge der Reiter wurde von den Versuchspersonen tendenziell die jeweils im Versuch gesehene Reihenfolge-Variante (siehe Kapitel 4.1 und 4.3) als logisch und passend empfunden. Dies bezog sich sowohl auf den Zustand *aktuelle Gefahrenlage* (mit Warndreieck) und *keine aktuelle Gefahrenlage* (ohne Warndreieck).

Verbesserungsvorschläge: Auf einige Versuchspersonen wirkte die Farbgestaltung des Alert-Systems etwas unmodern. Einige empfanden die Darstellung des Kachelblocks wie einen Werbeblock. Einigen war nicht klar, ob sich die Warnmeldung auf den eigenen PC bezieht oder ob es sich um eine allgemeine Warnung handelt. Die Schriftgröße der Beschreibungstexte wurde teilweise als zu klein empfunden. Die Texte wurden teilweise als zu lang empfunden und enthielten zu viele Fachbegriffe. Gewünscht wurde, dass die Beispiel-Screenshots vergrößerbar sind und bei den *aktuellen Betrugsfällen* eine Datumsangabe erscheint.

Vertrauenswürdigkeit: 82% der Versuchsteilnehmer schätzen das Alert-System als vertrauenswürdig ein, wenn es von einer Bank bereitstellt wird. Auf die Frage, ob es noch vertrauenswürdigere Institutionen gibt, antworteten 56% „ja“, 40% mit „nein“ und 4% fanden beides gleich vertrauenswürdig. Als noch vertrauenswürdiger wurden beispielsweise Seiten der Bundesregierung, Universitäten, IT-Fachleute/Hacker oder auch große IT-Unternehmen eingeschätzt. Als Gründe wurden angegeben, dass diese Institutionen neutraler oder nicht kommerziell sind oder über ein größeres Expertentum verfügen.

Sicherheitsempfinden: Die Frage, wie sicher sie sich durch das Alert-System auf der Login-Seite fühlen würden, beantworteten die Versuchspersonen von „1 = sehr unsicher“ bis „5 = sehr sicher“ im Durchschnitt mit 3,6 (sd = 0,9). Das Sicherheitsgefühl sank, je mehr Warnungen, d.h. Warndreiecke, angezeigt wurden. Auf die Frage, welchen Einfluss das Alert-System auf ihr Sicherheitsgefühl hat, antworteten 42%, dass sie sich mit so einem Alert-System sicherer fühlen würden. 38% meinten, dass ihr Sicherheitsgefühl gleich bleibt, egal, ob ein Alert-System erscheint oder nicht. 20% gaben an sich mit dem Alert-System unsicherer zu fühlen.

Akzeptanz: Der Aussage „Ich kann mir sehr gut vorstellen, das Alert-System regelmäßig zu nutzen“ stimmten die Versuchspersonen von 1 = „stimme gar nicht zu“ bis 5 = „stimme voll“ durchschnittlich mit 3,5 zu (sd = 1,1) und der Aussage „Ich empfinde das Alert-System einfach zu nutzen“ mit 4,5 (sd = 0,7). Diese Aussagen stammen aus der *System Usabilty Scale* (SUS), welche in 10 Aussagen die subjektive Nutzerfreundlichkeit von Systemen erfasst. Insgesamt erzielte das Alert-System auf der *SUS*-Skala im Durchschnitt einen Wert von 4,3 (sd = 0,5).

Nutzungsverhalten: Wenn die Versuchspersonen das Alert-System zum ersten Mal sehen würden, würden sie alle Informationen kurz durchlesen, beim zweiten Mal würden sie nur noch die Warnhinweise lesen, sofern diese neu sind. Werden ein bis zwei Warnungen angezeigt, würden die Versuchspersonen die Informationen durchlesen und sich danach gegebenenfalls einloggen. Bei mehr als zwei Warnungen würden viele Versuchsteilnehmer aufmerksamer sein, sich nicht mehr einloggen oder gegebenenfalls die Bank kontaktieren.

Smartphone: 76% der Versuchspersonen würden das Alert-System nutzen, wenn sie Online-Banking auf dem Smartphone durchführen würden. Auf einer Skala von 1 = „sehr schlecht“ bis 5 = „sehr gut“ wurde das Alert-System auf dem Smartphone (m = 3,9 | sd = 1,1) gegenüber der Webseite (m = 4,0 | sd = 0,8) nicht signifikant besser bewertet (t(49) = 0,66 | p = 0,51). 42%

würden das Alert-System auf beiden Geräten, 42% lieber auf der Webseite, 12% lieber auf dem Smartphone und 4% würden das System gar nicht nutzen.

4.5 Diskussion

Die meisten Versuchsteilnehmer gaben an, ein Alert-System wie dieses nutzen zu wollen. Dabei würde das Alert-System tendenziell lieber auf der Webseite genutzt werden mit der Begründung, dass auf einem PC-Bildschirm mehr Platz zum Lesen sei und der lange Beschreibungstext zu viele Informationen für ein Smartphone-Display enthält. Hier könnte gegebenenfalls eine textlich gekürzte Variante helfen die Nutzerakzeptanz zu erhöhen.

Die mittleren Bewertungen beim Sicherheitsempfinden könnten daher rühren, dass den Versuchspersonen durch die Warnmeldungen bewusst wird, wie „gefährlich“ Online-Banking sein kann. Ohne ein solches Alert-System wäre die Gefahr für den Nutzer nicht so offensichtlich. Andere Studien zeigten, dass Nutzer oft über wenig Wissen bzgl. der Betrugsmaschen beim Online-Banking verfügen und daher eine Aufklärung empfohlen wird [15]. Das Weglassen eines Alert-Systems, damit keine Verunsicherung stattfindet, wäre keine sinnige Option.

Trotz der insgesamt guten Bewertung des Alert-Systems gab es vereinzelt Unklarheiten seitens der Versuchsteilnehmer und Änderungswünsche, welche vor allem die Darstellung und die Nutzerfreundlichkeit betrafen. Bei der Reihenfolge der Reiter konnte kein eindeutiger Favorit identifiziert werden, sodass die Reihenfolge irrelevant zu sein scheint.

Es handelte sich bei dieser Studie um einen Usability-Test zur Überprüfung der Nutzerfreundlichkeit des Systems. Nicht Gegenstand war es, zu beobachten, wie sich Nutzer im Alltag beim Online-Banking tatsächlich verhalten. Die Befragung fokussierte auf die grundsätzliche Meinung und Einstellung zu einem solchen Alert-System. Zwar gibt es Zusammenhänge zwischen Einstellung und Verhalten, jedoch können aufgrund der Studien-Ergebnisse keine kausalen Schlüsse von Einstellung auf tatsächliches oder zukünftiges Verhalten gezogen werden.

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-Systems wahrscheinlich stark steigern. Bei einer größeren Datenbasis ist davon auszugehen, dass die Algorithmen besser trainiert werden können und so die Gefahrenlage besser bestimmt werden kann. 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.

Da das Alert-System von den befragten Nutzern grundsätzlich positiv bewertet wurde, scheint es aussichtsreich, sich weiter mit solchen Alert-Systemen zu beschäftigen und sie auch in der Praxis zu testen. Das Feedback der Studienteilnehmer kann verwendet werden, um weitere Optimierungen vorzunehmen. Das vorgestellte Alert-System kann demnach noch ansprechender (Design) und verständlicher (Texte) gestaltet werden. In einem weiteren Schritt könnte eine verbesserte Variante auf einer echten Bank-Webseite zum Einsatz kommen. Hier könnte das

Nutzungsverhalten mit Webstatistiken überprüft werden, z. B. wie viele Webseiten-Besucher auf welchen Bereich des Alert-Systems klicken und wie sie auf Warnungen reagieren.

6 Verwandte Arbeiten

Alert-Systeme: Akhawe und Felt untersuchen in [16] 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 kann 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 [17] 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-Middle* 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 [18]. *Domain highlighting* ist ein Mechanismus, in Webbrowsern, bei dem der Domainname hervorgehoben wird (z. B. fett gedruckt). Ziel ist es Nutzer darauf aufmerksam zu machen, wenn Sie sich auf einer Phishing-Seite befinden. Innerhalb der Studie wurde ermittelt, dass *domain highlighting* einen geringen Schutz vor Phishing Angriffen bietet.

Eine demographische Analyse zur Anfälligkeit für Phishing Angriffe führen Shen et al. in [19] 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 [20]. 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 [21].

Danksagung

Diese Arbeit wurde von dem Bundesministerium für Bildung und Forschung (Förderkennzeichen: 13N13251 & 13N13252, BOB) und dem Ministeriums für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfahlen (Förderkennzeichen: 005-1703-0021, MEwM) unterstützt. Wir möchten ebenfalls Herrn D. Grafe für die Implementierung des Systems danken. Dank gebührt auch den anonymen Reviewern, die mit wertvollen Anregungen zu dieser Arbeit beigetragen haben.

7 Literaturverzeichnis

[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: Nov. 27 2017.

[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 2016.* Accessed on: Nov. 27 2017.

[5] CosmosDirekt, *FinanzSchutz.* [Online] Available: https://www.cosmosdirekt.de/finanz-schutz-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,” 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] V. M. I. A. Hartl and U. Schmuntzsch, “Fraud Protection for Online Banking,” in *Human Aspects of Information Security, Privacy, and Trust: 4th International Conference*, T. Tryfonas, Ed., Cham: Springer International Publishing, 2016, pp. 37–47.

[16] 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)*, 2013, pp. 257–272.

[17] 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*, 2009, pp. 399–416.

[18] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock, “Does domain highlighting help people identify phishing sites?,” in *Proceedings of the 29th Annual Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada, 2011, p. 2075.

[19] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?,” in *CHI 2010 the 28th Annual CHI Conference on Human Factors in Computing Systems, April 10 - 15, 2010 in Atlanta, GA, USA*, Atlanta, Georgia, USA, 2010, p. 373.

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

[21] 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*, Santa Clara, California, USA, 2016, pp. 540–551.