Tobias Hilt, Melanie Volkamer

Sensibilisierung für Phishing und andere betrügerische Nachrichten

Vergleich frei verfügbarer Angebote

Betrügerische Nachrichten wie Phishing-E-Mails stellen kein neues Phänomen dar. Dennoch ist diese Angriffsform immer noch sehr erfolgreich. Der Beitrag untersucht, ob und wie gut im Internet frei verfügbare Informationsangebote bei der Erkennung betrügerischer Nachrichten helfen können.

Hintergrund

Im Rahmen der Forschungsarbeiten der Forschungsgruppe SECUSO am KIT wurden Internetseiten aus verschiedenen Kontexten, die Informationen über betrügerische Nachrichten anbieten, auf ihre Eignung zur Sensibilisierung von Mitarbeiterinnen und Mitarbeitern insbesondere von kleinen und mittelgroßen Unternehmen (KMU) untersucht. Das Ergebnis zeigt, dass die Gefahren durch betrügerische Nachrichten und insbesondere solche mit gefährlichen Links zwar adressiert werden, aber die Informationen zur Erkennung von und zum Umgang mit betrügerischen Nachrichten, die auf den untersuchten Internetquellen zum Zeitpunkt der Untersuchung bereitgestellt werden, oft nicht ausreichend sind, um die Leser zu befähigen, betrügerische Nachrichten effektiv zu erkennen.

1 Betrügerische Nachrichten

Der Begriff „betrügerische Nachrichten“ ist sehr weit gefächert und umfasst die verschiedensten Kommunikationskanäle wie bspw. E-Mail-, SMS-, Messenger-Nachrichten oder Posts in sozialen Netzwerken. Bei dieser Angriffsform verschicken Betrüger Nachrichten, die oft auf den ersten Blick täuschend echt aussehende Nachahmungen offizieller Nachrichten sind, oder sie denken sich andere mehr oder weniger plausible Gründe aus, um die Empfänger dazu zu bringen, mit dem Absender oder Nachrichteninhalt wie vom Betrüger gewünscht zu interagieren.

Die „gewünschte“ Interaktion kann dabei darin bestehen sensible Informationen zurückzuschicken, (kostenpflichtige) Anrufe zu tätigen, Überweisungen zu tätigen, auf Links zu klicken und ggf. sich auf der anschließend erscheinenden sogenannten Phishing-Webseite anzumelden oder mitgeschickte Dateien zu öffnen. Ziel dieser Betrüger ist es, sich unmittelbar finanziell zu bereichern (z. B. durch kostenpflichtige Anrufe oder Geldtransaktionen), an sensible Informationen wie bspw. Zugangsdaten zu gelangen oder Schadsoftware zu verbreiten, um dann bspw. die Betroffenen entsprechend erpressen zu können oder sich durch die Ausfälle der IT-Systeme der Betroffenen einen anderen Vorteil zu verschaffen. Entsprechend groß kann das Ausmaß des Schadens sein, wenn eine betrügerische Nachricht nicht erkannt wird. Umso wichtiger ist es, dass Internetnutzer effektiv darüber informiert werden, woran sie solche Nachrichten erkennen.

2 Schulungsunterlagen von SECUSO

Die Digitalisierung stellt gerade kleine und mittelgroße Unternehmen (KMU), die keine eigenen Sicherheitsabteilungen besitzen, vor neue Herausforderungen. Um sich vor digitalen Betrügern und deren Angriffen zu schützen, ist die Sensibilisierung und Weiterbildung der Mitarbeiterinnen und Mitarbeiter von zentraler Bedeutung. Gerade Angriffe über betrügerische Nachrichten mit gefährlichen Links stellen hierbei eine enorme Bedrohung für die Sicherheit des Unternehmens dar.

Ziel des vom Bundesministerium für Wirtschaft und Energie geförderten Projekts KMU AWARE war es, die Mitarbeiterinnen

und Mitarbeiter von KMU in Deutschland verstärkt für die Gefahren beim Einsatz von IT zu sensibilisieren und ihnen aufzuzeigen, wie sie sich gegen ausgewählte Gefahren effektiv schützen können. Hierfür sollten an den realen Anforderungen in KMU orientierte Sensibilisierungs- und Schulungsmaterialien in einem iterativen Prozess entwickelt, evaluiert und verbessert werden. So wurde in einem aufwendigen Prozess mit Experten und Mitarbeiterinnen und Mitarbeitern von KMU auch eine Schulung zur Erkennung von betrügerischen Nachrichten entwickelt [2]. Folgende *vier Module* sind Bestandteile dieser Schulung:

- Einleitung zu betrügerischen Nachrichten
- allgemeine Informationen zu nicht-plausiblen betrügerischen Nachrichten mit gefährlichen Links bzw. mit gefährlichem Anhang
- plausible betrügerische Nachrichten mit gefährlichen Links und
- plausible betrügerische Nachrichten mit gefährlichen Anhängen.

Das *erste Modul* gibt einen Überblick darüber, dass Nachrichten unterschiedliche Arten von gefährlichen Inhalten beinhalten können und dass jede Art von Nachricht von den Betrügern genutzt wird (neben E-Mails auch z. B. Facebook Posts, WhatsApp- oder SMS-Nachrichten). Außerdem klärt das Modul darüber auf, dass jeder das Ziel dieser betrügerischen Nachrichten werden kann und was die Konsequenzen sein können, wenn man auf eine betrügerische Nachricht reagiert.

Das *zweite Modul* hilft, betrügerische Nachrichten zu identifizieren, indem es über Plausibilitätsüberprüfungen für eingehende Nachrichten informiert (z. B. können die E-Mail-Adresse des Absenders, die Sprache und der Inhalt der Nachricht auf Plausibilität geprüft werden).

Im *dritten Modul* werden betrügerische Nachrichten betrachtet, die auf den ersten Blick plausibel erscheinen, aber gefährliche Links enthalten. Das Modul erklärt, wie man überprüft, ob ein Link gefährlich ist und welche Tricks Betrüger verwenden, um diese Prüfung zu erschweren.

Das *vierte Modul* geht schließlich noch auf betrügerische Nachrichten ein, die auf den ersten Blick plausibel erscheinen, jedoch gefährliche Anhänge enthalten. Hierzu erklärt das Modul, wie man überprüfen kann, ob ein Anhang gefährlich ist oder nicht.

Nach iterativer Überarbeitung und Verbesserung der einzelnen Module wurde die Schulung in einer Benutzerstudie in drei KMU evaluiert [3]. Die Ergebnisse zeigen eine signifikante Verbesserung der Teilnehmer in der Erkennung von betrügerischen und legitimen Nachrichten. Die Erkennungsraten stiegen hierbei von 63,3% (bei betrügerischen Nachrichten) und 82,4% (bei legitimen Nachrichten) auf 84,3% (bei betrügerischen Nachrichten) und 87,1% (bei legitimen Nachrichten). Betrachtet man die Erkennungsraten von plausiblen und nicht-plausiblen betrügerischen Nachrichten getrennt, verbesserten sich die Erkennungsraten für nicht-plausible betrügerische Nachrichten von 71,1% auf 92%. Die Erkennung von plausiblen betrügerischen Nachrichten mit gefährlichen Links verbesserte sich von 48,6% auf 74,3% und die Erkennung von plausiblen betrügerischen Nachrichten mit schädlichen Anhängen verbesserte sich von 82% auf 94,4%. Die Ergebnisse zeigen, dass die Schulung maßgeblich zur Sicherheit in KMU beiträgt. Für diesen Erfolg leisten zwei Faktoren einen wesentlichen Beitrag: Der abgedeckte Inhalt und die Art sowie Verständlichkeit der Präsentation der Inhalte.

Im Folgenden wird der Frage nachgegangen, ob und inwieweit die für die Erkennung von betrügerischen Nachrichten hilfreichen Inhalte der Schulung bereits von anderen Angeboten aus dem Internet abgedeckt werden. Da es keine öffentlich verfügbaren Informationen darüber gibt, ob die Effektivität dieser Angebote bereits untersucht wurde, nehmen wir die Überschneidung mit den Inhalten unserer Schulung als Indikator für die Effektivität dieser Angebote. Auf diese Weise versuchen wir die Frage zu beantworten, ob die im Rahmen dieser Arbeit untersuchten Internetquellen mit ihren frei verfügbaren Angeboten den Lesern dabei helfen, betrügerische Nachrichten effektiv(er) zu erkennen.

3 Methodik

3.1 Kriterien

Die für die Untersuchung der betrachteten Internetangebote herangezogenen Kriterien lassen sich in drei Kategorien einteilen.

Format
Im ersten Schritt wurde das Format der bereitgestellten Informationen identifiziert, d. h. ob die Informationen als Text oder Video zur Verfügung gestellt werden. Anschließend wurde zuerst die Wortanzahl des Textes und, falls vorhanden, die Länge des Videos bestimmt. Für den Fall, dass ein Flyer zum Download mit weiterführenden Informationen angeboten wurde, wurde der Inhalt des Flyers analog zu den untersuchten Texten auf den Webseiten untersucht und als ergänzender Text betrachtet. Des Weiteren wurde die Verwendung von Beispielen dokumentiert. Hierbei werden die Anzahl und Art der Beispiele festgehalten. Folgende Arten werden unterschieden (und teilweise weiter untergliedert):

- **Erklärbeispiele**: Ein Bespiel wird verwendet, um einen Sachverhalt genauer zu erläutern. Hierbei wird unterschieden zwischen einem Beispiel (i.d.R. ein Bild) (a) einer betrügerischen Nachricht, (b) einer Phishing-URL oder (c) einer Phishing-Webseite.
- **Beispielnachrichten**: Hier werden tatsächlich verschickte betrügerischen Nachrichten eingebunden. Dies kann entweder (a) eine einzelne aktuelle betrügerische Nachricht sein oder (b) eine Liste älterer betrügerischer Nachrichten.

Inhalte Modul 1
Weitere Kriterien wurden aus Modul 1 der SECUSO Schulung abgeleitet:

- **Nachrichtenformat**: Hierbei wird unterschieden zwischen (a) Nennung von E-Mails, (b) Nennung von Formaten über das E-Mail Format hinaus (werden auch z. B. Kurznachrichten oder Messenger-Nachrichten genannt) sowie (c) Nennung von E-Mails und Erwähnen von weiteren Nachrichtenformaten, ohne näher auf ein konkretes Nachrichtenformat einzugehen.
- **Gefährliche Links**: Hier wird unterschieden zwischen Hinweisen, (a) dass die Gefahr darin besteht, dass Links zu Webseiten führen, auf denen man sensible Daten eingeben soll und (b), dass die Gefahr darin besteht, dass das Klicken auf Links dazu führen kann, dass (unbemerkt) Schadsoftware geladen wird, sowie (c) unspezifischen Hinweisen, dass Links gefährlich sind und man deswegen keinen Links in verdächtigen Nachrichten folgen sollte.

- **Gefährliche Anhänge**: Hier wird geprüft, ob überhaupt auf gefährliche Anhänge eingegangen wird oder dies nicht der Fall ist.
- **Aufforderung zu gefährlichen Aktionen**: Hier wird unterschieden, ob überhaupt auf konkrete gefährliche Aktionen eingegangen wird (d. h. einzelne gefährliche Aktionen konkret benannt werden) oder diese Themen nicht adressiert werden. Für den Fall, dass auf gefährliche Aktionen eingegangen wird, wird unterschieden zwischen Überweisung, kostenpflichtigen Anrufen bzw. dem Zurückschicken von sensiblen Informationen.

Inhalte Module 2, 3 und 4

Dieses Unterkapitel befasst sich mit den verschiedenen Regeln im Umgang mit möglichen betrügerischen Nachrichten. Entsprechende Regeln werden dem Leser in den Modulen 2, 3 und 4 der SECUSO-Schulung an die Hand gegeben, damit er schrittweise eingehende Nachrichten prüfen kann. Die Regeln werden im Folgenden kurz zusammengefasst, da bei der Untersuchung der im Internet verfügbaren kostenlosen Angebote geprüft wird, welche dieser Regeln jeweils abgedeckt werden:

- **Absender/Inhalt plausibel**: Prüfen Sie Inhalt und Absender jeder Nachricht auf Plausibilität.
- **URL identifizieren:** Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Link enthält, dann finden Sie heraus, welche Webadresse (sprich URL) tatsächlich hinter dem Link steckt.
- **Wer-Bereich identifizieren:** Wenn Sie die Webadresse hinter dem Link gefunden haben, identifizieren Sie als erstes den sogenannten Wer-Bereich (ggf. auch Domain genannt) der Webadresse.
- **Wer-Bereich überprüfen:** Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben, prüfen Sie, ob der Wer-Bereich einen Bezug zu dem (vermeintlichen) Absender oder Inhalt der Nachricht hat und korrekt geschrieben ist.
- **Weitere Infos einholen zum Link:** Wenn Sie den Wer-Bereich in der Webadresse identifiziert haben aber nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen.
- **Gefährliches Datei-Format:** Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Anhang enthält, dann prüfen Sie, ob dieser Anhang ein (sehr) gefährliches Dateiformat hat. Öffnen Sie den Anhang insbesondere im Fall von (sehr) gefährlichen Dateiformaten nur, wenn Sie diesen genauso von dem Absender erwarten.
- **Weitere Infos zum Anhang einholen:** Wenn der Anhang kein (sehr) gefährliches Dateiformat hat, aber Sie den Anhang nicht genauso vom Absender erwarten, dann sollten Sie weitere Informationen einholen.

3.2 Untersuchte Webseiten

Es wurden sowohl Webseiten von übergeordneten Instituten (Kriminalämter, Sicherheitsinstitute und Verbraucherzentralen) als auch von Anbietern diverser Internetdienste (Banken, E-Mail-Anbieter, Internetshops, Mobilfunkanbieter und soziale Netzwerkanbieter) untersucht. Um die Ergebnisse einzugrenzen wurden zwanzig Banken, die Verbraucherzentralen und Kriminalämter jeweils auf Landes- und Bundesebene, sieben Sicherheitsinstitute, zwanzig Internetshops (Webseiten mit Account- und Zahlungsinformationen), sechzehn Mobilfunk-Vertragsanbieter, zehn soziale Netzwerkanbieter und zehn E-Mail-Anbieter ausgewählt.

Die meisten der untersuchten Banken sind deutschlandweit tätig (z. B. DKB, Apobank, Deutsche Bank, PAX, Postbank und Commerzbank). Bei den Verbraucherzentralen und Kriminalämtern wurden die Webseiten auf Bundes- und Landesebene betrachtet. Hierbei ist wichtig zu erwähnen, dass aus dem Bereich der Verbraucherzentralen (neben dem Bund) nur drei weitere aufgenommen wurden, da die restlichen dreizehn lediglich auf die Seite des Bundes verweisen bzw. Inhalte von der Bundesseite kopieren.[1] Bei der Betrachtung der Kriminalämter wurden auf Grund fehlender Informationen ebenfalls nur zehn der sechzehn LKAs in die Untersuchung aufgenommen.[2] Die folgenden sieben Sicherheitsinstitute wurde wegen ihrer Bekanntheit ausgewählt: KlickSafe, BSI, BSIFB, CHIP, pc-Magazin, SecuPedia, Zentrum Digitalisierung Bayern. Die Auswahl der Internetshops, Mobilfunkanbieter, sozialen Netzwerke und E-Mail-Anbieter erfolgte über sogenannte Top-Listen, welche die in Deutschland verfügbaren Unternehmen gemäß ihrer Popularität (gemessen an der Anzahl der Besuche der jeweiligen Webseite) auflisten.

Die Analyse der Webseiten fand von März bis Mai 2019 statt.

4 Ergebnisse

Die Ergebnisse der Untersuchung zusammenfassende Tabelle ist auch als Online-Dokument verfügbar [1], zu denen die Autoren gerne Änderungswünsche entgegennehmen und diskutieren. Im Folgenden wird vor allem auf die Ergebnisse für die einzelnen Gruppen von Webseiten eingegangen. Die Ergebnisse für einzelne Webseiten sind in [1] nachzulesen.

4.1 Vergleich der Formate

Tabelle 1 | Ergebnis bzgl. der verwendeten Formate

Kürzel	# Worte	Video	Durchschnittl. Länge [Min]	Beispiel-nachrichten	Erklärungs-beispiele
Bank	532	25%	00:03:18	50%	35%
E-Mail Anbieter	602	0%		0%	33%
Internetshop	396	0%		8%	38%
Kriminalamt	499	0%		0%	9%
Mobilfunkanbieter	611	0%		0%	33%
Sicherheitsinstitut	622	29%	00:02:36	0%	57%
Soziales Netzwerk	280	0%		0%	40%
Verbraucherzentrale	408	0%		75%	75%
Gesamtergebnis	**499**	**10%**	**00:03:02**	**19%**	**36%**

Tabelle 1 gibt Aufschluss darüber, in welcher Form und Fülle die untersuchten Webseiten auf betrügerische Nachrichten und deren Erkennung hinweisen und bezieht sich somit auf die oben erläuterten Kriterien. So gibt die Spalte „# Worte“ an, wie viele Worte zur Aufklärung auf der Webseite durchschnittlich inkl. den hinterlegten Flyern verwendet wurden. „Video“ bezeichnet die prozentuale Anzahl der Webseiten, die ein Informationsvideo zur Thematik bereitstellen. Die Spalten „Erklärungsbeispiele“ und „Beispielnachrichten“ geben an, auf wie vielen Webseiten

1 Folgende Verbraucherzentralen (VZ) wurden nicht berücksichtigt: VZ Berlin, VZ Brandenburg, VZ Bremen, VZ Hessen, VZ NRW, VZ Rheinland-Pfalz, VZ Saarland, VZ Sachsen, VZ Sachsen-Anhalt, VZ Schleswig-Holstein und VZ Thüringen.

2 Folgende Kriminalämter wurden nicht berücksichtigt, da sie lediglich Inhalte von „polizeiberatung.de“ oder „kriminalpolizei.de“ kopierten oder darauf verweisen: LKA Baden-Württemberg, LKA Hessen, LKA Mecklenburg-Vorpommern, LKA Bremen, LKA Schleswig-Holstein, LKA Brandenburg, LKA Sachsen und LKA Saarland.

mindestens ein entsprechendes Beispiel verwendet wird. Informationen über die unterschiedlichen Arten von Erklärungsbeispielen finden sich in [1]. Zusammenfassend ist festzuhalten, dass durchschnittlich 499 Wörter verwendet werden und im Schnitt die Mobilfunkanbieter und die Sicherheitsinstitute die umfangreichsten Informationen zu Verfügung stellen.

4.2 Inhalte Modul 1

Tabelle 2 | Ergebnis bzgl. den adressierten Nachrichtenformaten

Kürzel	E-Mail	E-Mail + konkretes Format	E-Mail + unspezifisches Format	Unspezifisch
Bank	85%	15%	0%	0%
E-Mail Anbieter	67%	0%	33%	0%
Internetshop	100%	0%	0%	0%
Kriminalamt	91%	9%	0%	0%
Mobilfunkanbieter	100%	0%	0%	0%
Sicherheitsinstitut	100%	0%	0%	0%
Soziales Netzwerk	60%	0%	0%	40%
Verbraucherzentrale	100%	0%	0%	0%
Gesamtergebnis	**89%**	**6%**	**3%**	**3%**

Einen Überblick über die berücksichtigten Nachrichtenformate pro Webseiten-Kategorie gibt Tabelle 2. Bezüglich der Nachrichtenformate ist festzustellen, dass fast nur auf die Möglichkeit des Betrugs per E-Mail eingegangen wird (88,89%), andere Nachrichtenformate (Telefon, SMS, Messenger etc.) werden weitestgehend außer Acht gelassen. So gehen z. B. nur vier Webseiten auf betrügerische Nachrichten in Form von SMS ein. Andere Formate als E-Mails werden nur auf Webseiten von Banken, Kriminalämtern und E-Mail-Anbietern benannt.

Tabelle 3 | Ergebnis bzgl. der Arten von gefährlichen Inhalten

Kürzel	Link	Anhang	Aufforderung
Bank	100,00%	75,00%	85%
E-Mail Anbieter	100,00%	50,00%	67%
Internetshop	100,00%	69,23%	31%
Kriminalamt	100,00%	72,73%	55%
Mobilfunkanbieter	100,00%	50,00%	83%
Sicherheitsinstitut	100,00%	85,71%	57%
Soziales Netzwerk	100,00%	40,00%	20%
Verbraucherzentrale	100,00%	75,00%	50%
Gesamtergebnis	**100,00%**	**68,06%**	**60%**

Tabelle 3 kann entnommen werden, dass der Fokus auf betrügerischen Nachrichten (konkret: E-Mails) mit gefährlichen Links liegt. Dennoch weisen 68% der untersuchten Webseiten darauf hin, dass betrügerische Nachrichten Anhänge enthalten können, die auf keinen Fall geladen werden sollten, und 60% gehen auf andere Aktionen wie kostenpflichte Anrufe oder Überweisungen ein.

Tabelle 4 behandelt die bereitgestellten Informationen zu Links in betrügerischen Nachrichten. Immerhin weisen 68% der Webseiten darauf hin, dass die Links in gefährlichen Nachrichten Empfänger auf gefälschte Webseiten weiterleiten können – oft inklusive dem Hinweis, dass diese Webseiten täuschend echt aussehen und dass auf diesen sensiblen Daten eingegeben werden sollen. Nicht einmal ein Viertel der untersuchten Webseiten weist darauf hin, dass die Webadresse hinter dem Link bereits vor dem Klicken geprüft werden muss, da bereits beim Klicken Schadsoftware geladen werden könnte. Selbst bei den Sicherheitsinstituten ist es weniger als die Hälfte der betrachteten Webseiten. Erstaunlich ist auch, dass etwa ein Viertel der untersuchten Webseiten gar nicht weiter auf konkrete Arten möglicher Gefahren oder Konsequenzen eingehen, sondern nur ganz allgemein davon sprechen, dass sich Gefahren hinter Links verbergen können.

Tabelle 4 | Ergebnis bzgl. der Informationen zu potentiellen Gefahren, wenn auf einen Link geklickt wird

Kürzel	Webseite	Schadsoftware	Allgemein
Bank	80%	40%	30%
E-Mail Anbieter	100%	0%	0%
Internetshop	46%	15%	54%
Kriminalamt	55%	18%	18%
Mobilfunkanbieter	67%	17%	17%
Sicherheitsinstitut	71%	43%	29%
Soziales Netzwerk	60%	20%	20%
Verbraucherzentrale	75%	0%	0%
Gesamtergebnis	**68%**	**24%**	**26%**

Tabelle 5 | Ergebnis bzgl. der unterschiedlichen Aufforderungsformen im Kontext von gefährlichen Aktionen

Kürzel	Überweisung	Anruf	Zurück schreiben
Bank	45%	30%	80%
E-Mail Anbieter	17%	0%	67%
Internetshop	23%	0%	23%
Kriminalamt	45%	18%	36%
Mobilfunkanbieter	50%	17%	67%
Sicherheitsinstitut	14%	14%	43%
Soziales Netzwerk	0%	0%	20%
Verbraucherzentrale	50%	0%	50%
Gesamtergebnis	**33%**	**14%**	**51%**

Tabelle 5 stellt das Ergebnis für die Kategorie ‚Aufforderung zu gefährlichen Aktionen' dar. Negativ hervorzuheben ist, dass nur ein Drittel der Webseiten auf die Problematik mit den Überweisungen eingeht, obwohl dies der klassische Ansatz beim sogenannten *CEO Fraud* ist. Am ehesten wird noch auf den Fall eingegangen, dass sensible Informationen nicht zurückgeschickt werden sollen. Die Banken hingegen schneiden bei allen drei Angriffstypen (Überweisung, Anruf, Zurückschreiben) mit am besten ab. Definitiv Nachholbedarf besteht auch bei den Darstellungen auf Webseiten der Sozialen Netzwerke.

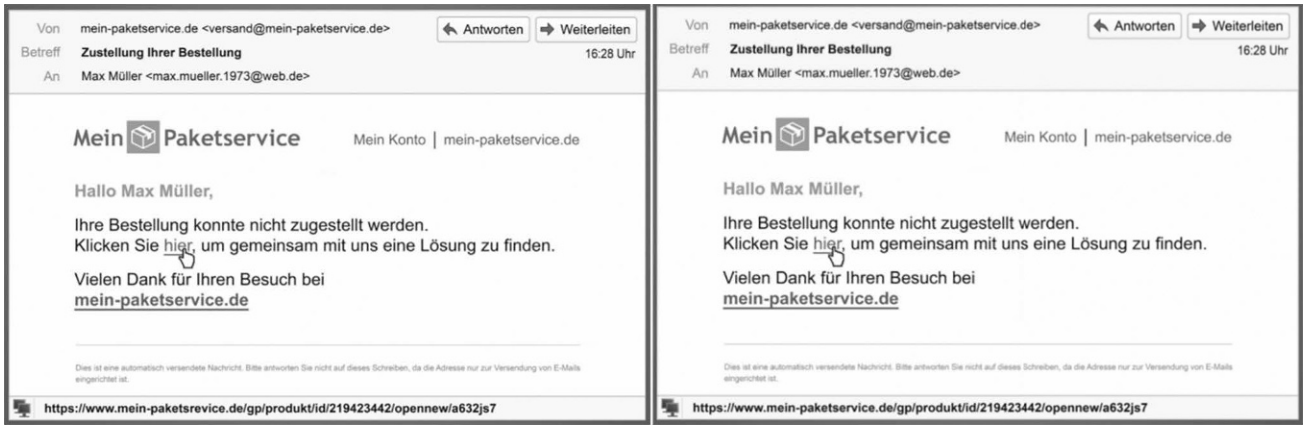
4.3 Inhalte Module 2, 3 und 4

Tabellen 6 und 7 geben Auskunft darüber, ob die betrachteten Webseiten auf die Regeln zur Erkennung von betrügerischen Nachrichten eingehen. 74% aller Webseiten weisen darauf hin, dass jede Nachricht zuerst auf Plausibilität überprüft werden

Tabelle 6 | Ergebnis bzgl. der Regeln zur Erkennung von betrügerischen Nachrichten (Teil 1)

Kürzel	Absender/Inhalt plausibel	URL identifizieren	WER-Bereich identifizieren	Weitere Informationen einholen
Bank	75%	30%	30%	30%
E-Mail Anbieter	67%	50%	17%	0%
Internetshop	77%	46%	23%	23%
Kriminalamt	64%	36%	18%	27%
Mobilfunkanbieter	83%	33%	33%	0%
Sicherheitsinstitut	86%	86%	43%	14%
Soziales Netzwerk	60%	40%	0%	0%
Verbraucherzentrale	75%	0%	0%	0%
Gesamtergebnis	**74%**	**40%**	**24%**	**18%**

Abbildung 1 | Links die Kopie einer echten Nachricht, in der die URL vor dem Versenden ausgetauscht wurde, und rechts die Originalnachricht



muss. Tabelle 6 zeigt, dass es großen Bedarf an Ergänzungen zu konkreten Handlungsempfehlungen gibt, wenn die Nachricht auf den ersten Blick plausibel aussieht: Nur 40% der untersuchten Webseiten weisen überhaupt darauf hin, dass es wichtig ist die URL hinter dem Link zu betrachten. Bei allen untersuchten Seiten der Verbraucherzentralen fehlt diese Information ganz. Der nächste Schritt, zu erklären, welcher Teil der URL relevant ist, wird nur von einem Viertel der Webseiten adressiert. Das Fehlen dieser Informationen würde bedeuten, dass die URL www.amazon.de.shopping-de.cc/login durchaus als legitime URL in einer E-Mail von Amazon angesehen werden kann. Weitere Details zur URL und verwendeter Angriffe in Bezug auf die URL werden von nahezu keiner Webseite adressiert.

Auch fehlen in 82% der Webseiten Informationen darüber, was getan werden kann, wenn man sich bei einer Nachricht unsicher ist.

Tabelle 7 gibt Auskunft darüber, welche Informationen die untersuchten Webseiten zu einem möglichen Anhang in einer betrügerischen Nachricht zur Verfügung stellen. Nur etwa ein

Tabelle 7 | Ergebnis bzgl. der Regeln zur Erkennung von betrügerischen Nachrichten (Teil 2)

Kürzel	Dateiformat	weitere Informationen einholen
Bank	20%	15%
E-Mail Anbieter	0%	0%
Internetshop	23%	0%
Kriminalamt	36%	18%
Mobilfunkanbieter	50%	0%
Sicherheitsinstitut	57%	14%
Soziales Netzwerk	0%	0%
Verbraucherzentrale	50%	0%
Gesamtergebnis	**28%**	**8%**

Viertel der untersuchten Webseiten weist darauf hin, dass zuerst das Dateiformat des Anhangs überprüft und nur 8% weisen darauf hin, dass bei Unsicherheit weitere Informationen eingeholt werden sollten.

Abgesehen von den defi nierten Kategorien wurden vereinzelt noch weitere Hinweise hinsichtlich der Erkennung von betrügerischen Nachrichten gegeben („auf Umlaute achten", „Mail-Header auslesen" und „nicht auf vermeintliche Gewinnspiele etc. reagieren").

5 Diskussion

Zusammenfassend lässt sich sagen, dass auf den untersuchten Informationsseiten insgesamt zu wenig auf die verschiedenen Aspekte von betrügerischen Nachrichten eingegangen wird und zu wenig klare Regeln zu deren Erkennung gegeben werden – insbesondere in Fällen, bei denen die Nachricht plausibel aussieht und nur der Link oder der Anhang ausgetauscht wurde (siehe Abbildung 1). Darüber hinaus fehlen klare Anweisungen, was getan werden kann, wenn man sich bei einer Nachricht unsicher ist, ob diese betrügerisch ist oder nicht.

Das Ergebnis der Untersuchung zeigt, dass Informationsangebote im Internet derzeit überwiegend nicht ausreichend sind, die Anfälligkeit von Unternehmen für Angriffe mittels betrügerischer Nachrichten und insbesondere für Phishing-Angriffe zu verringern. Wer sich informieren möchte, findet in vielen Fällen weder ausreichende Informationen noch klare Regeln, um sich effektiv gegen diese Art von Angriffen zu schützen.

Das Fehlen von klaren Regeln birgt die Gefahr der Frustration, da Leser zwar Informationen erhalten, aber nicht wissen, wie sie diese konkret anwenden sollen. Das Fehlen von Angriffsformen birgt die Gefahr, dass Leser die erhaltenen Informationen anwenden und damit sicher zu sein glauben (z. B. nur die Plausibilität des Absenders und des Inhalts überprüfen, nicht aber die Webadresse hinter dem Link oder das Dateiformat des Anhangs). Entsprechend essentiell ist es, dass die Informationsangebote entsprechend erweitert und konkretisiert werden.

Quellen

[1] Zusammenfassung der Ergebnisse der Untersuchung von Webseiten mit Informationen über betrügerische Nachrichten. Online-Ressource: https://www.secuso.org/dud-feb-2020-ergebnisse-in-google

[2] Forschungsgruppe SECUSO (Security, Usability, Society): *Schulungs- und Trainingskonzept zur Erkennung von betrügerischen Nachrichten inklusive Phishing-Nachrichten*. KIT. Link: https://secuso.aifb.kit.edu/betruegerische_nachrichten_erkennen.php

[3] Stephan Neumann, Benjamin Reinheimer, Melanie Volkamer: *Don't be Deceived: The Message Might be Fake*. In: 14th International Conference On Trust, Privacy & Security 2017. In: Digital Business (TrustBus), S. 199-214.