Short Paper: Business Chat ist verwirrt. Es hat sich vor Verwirrung selbst verletzt!

Moritz Gruber[1], Christian Höfig[1], Matteo Große-Kampmann[1], Tobias Urban[2], Norbert Pohlmann[3]

Abstract: In dieser Arbeit wird eine ganzheitliche Bedrohung für Business-Chat-Anwendungen aufgezeigt und bewertet: *Chishing* – Phishing über Business-Chats. Die Bedrohung hat ihren Ursprung in den Anfängen der heutigen vernetzten Welt und das zugrunde liegende Problem wird in seiner einfachsten Form als *Spoofing* bezeichnet. In vier von sechs Business-Chat-Tools, die in dieser Arbeit analysiert werden, ist es möglich, Anzeigenamen, Profilbilder und weitere persönliche Informationen erfolgreich zu fälschen. Dies stellt eine Bedrohung für Unternehmen dar, da es Insider-Bedrohungen Vorschub leistet und unter Umständen auch externen Entitäten dazu einlädt, sich als interne Mitarbeiterin auszugeben.

Keywords: Phishing; Chishing; Social Engineering; Business Chats

1 Einleitung

Seit den Anfängen des Internets haben Cyberkriminelle die Gelegenheit ergriffen Internetnutzer zu täuschen und sich so zu bereichern. Eine Möglichkeit, Verwirrung zu stiften, ist das sogenannte *Spoofing*. Spoofing beschreibt im Allgemeinen den Akt der Täuschung, indem versucht wird, eine gefälschte Entität so darzustellen, als sei sie das Original. Heutzutage wird der Begriff *Spoofing* für Angriffstechniken verwendet, bei denen Authentifizierungs- oder Identifizierungsverfahren umgangen werden und somit die Vertrauenswürdigkeit von Systemen nicht mehr sichergestellt werden kann, beispielsweise bei GPS- oder Gesichtserkennungssystemen [BKH16; Ti11]. *Spoofing* ist besonders kritisch, da die meisten Unterhaltungen im Internet heutzutage per E-Mail oder Chat stattfinden.

Diese Arbeit diskutiert eine Bedrohung für verschiedene Business-Chat-Programme. Es wird gezeigt, wie eine interne oder externe Angreiferin in verschiedenen Business-Chat-Anwendungen Identitäten fälschen kann. Analog zu *Phishing* über SMS, welches als *Smishing*[4] definiert wird, führten die Autoren die Wortschöpfung *Chishing* ein. Dieser Be-

[1] AWARE7 GmbH, Munscheidstraße 14, 45886 Gelsenkirchen, Deutschland, vorname@aware7.de
[2] Institut für Internet-Sicherheit – if(is), Westfälische Hochschule und secunet Security Networks AG, urban@internet-sicherheit.de
[3] Institut für Internet-Sicherheit – if(is), Westfälische Hochschule, Neidenburgerstraße 43, 45877 Gelsenkrichen, Deutschland, pohlmann@internet-sicherheit.de
[4] `https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html`

griff wurde durch die Autoren erstmalig in einem nicht zitierfähigen Preprint veröffentlicht[5]. Dieses Preprint sorgte bereits für eine kontroverse Diskussion in einem Online-Forum[6]. Nichtsdestotrotz ist der Begriff Chishing korrekt gewählt, da er Phishing über einen neuen Delivery-Vektor beschreibt. Gerade der Delivery-Vektor spielt bei der konkreten Beschreibung einer Bedrohung eine essentielle Rolle. Ähnlich wie bei Injection-Schwachstellen wie *SQL-*, *NoSQL-* oder *GraphQL-Injections* dient der im Namen der Schwachstelle enthaltene Delivery-Vektor der Abgrenzung und Präzisierung eines Angriffs. Zusammengefasst leistet der Artikel die folgenden Beiträge:

- Diese Arbeit zeigt auf, wie eine interne oder externe Angreiferin unter bestimmten Bedingungen in verschiedenen Business-Chat-Programmen Identitäten fälschen und somit eine Bedrohung für die Informationssicherheit darstellen kann.
- Die Bedrohung wird anhand einer relevanten Teilmenge der verfügbaren Anwendungen in diesem Bereich evaluiert.

2 Hintergrund

Traditionell hat die E-Mail eine wesentliche Rolle in der digitalen Kommunikation auf der ganzen Welt eingenommen [Cr82]. Heutzutage gewinnen aber auch andere Kommunikationskanäle an Bedeutung. Diese Arbeit konzentriert sich auf den Übermittlungsvektor Chat und befasst sich mit möglichen Schwierigkeiten und Bedrohungen, die sich aus dem *Spoofing* bestimmter Aspekte in diesen Chats ergeben.

Social Engineering: Social Engineering spielt in der heutigen Bedrohungslage eine bedeutende Rolle. Besonders kritisch bei dieser Bedrohung ist die Tatsache, dass es immer schwieriger wird, digitale Identitäten zwischen „beruflichem“ und „privatem“ Leben zu trennen [Br16]. Beim Social Engineering geht es der Angreiferin darum, ein Opfer erfolgreich von etwas zu überzeugen. Wenn hinter einem Social-Engineering-Szenario eine vertrauenswürdige Identität oder eine gefälschte Identität steht, können die Ergebnisse für die Informationssicherheit kritisch sein.

Phishing: Phishing wurde erstmals 1996 im Zusammenhang mit dem Diebstahl von America Online (AOL)-Konten verwendet [Ol04]. Falsche und betrügerische Nachrichten, die dem Opfer Geld versprechen, gehen bis ins 19. Jahrhundert zurück [Ne]. In der Computersicherheit beschreibt *Phishing* den Vorgang, bei dem sich eine Angreiferin als vertrauenswürdige Instanz ausgibt, um Benutzer dazu zu bringen, persönliche Daten preiszugeben oder über bösartige Anhänge oder Links Malware zu verbreiten [Pa15]. Dies kann per E-Mail, Chat oder über jedes andere Kommunikationsmedium geschehen. Solange es mindestens zwei Kommunikationspartner gibt, besteht immer eine gewisse Wahrscheinlichkeit, dass eine der beiden Personen böswillig handelt. *Phishing* wird von Angreifern immer wieder angewendet,

[5] https://www.researchgate.net/publication/355916867_Business_Chat_is_Confused_It_Hurt_Itself_in_its_Confusion_-_Chishing

[6] https://web.archive.org/web/20220111181830/https://www.reddit.com/r/cybersecurity/comments/qn9rv2/chishing_an_emerging_threat_for_business_chat/

weil es oft einfacher ist, Menschen auszunutzen – vor allem im Vergleich zu einem Einbruch in ein gehärtetes technisches System [FV18].

Spoofing: Spoofing ist eine weit verbreitete Bedrohung im Internet und beschreibt eine Technik bei welcher eine Angreiferin sich als eine vertrauenswürdige Entität ausgibt. Wenn eine Angreiferin sich als rechtmäßige Benutzerin des Systems ausgeben kann, versagen die Schutzmechanismen des Systems, da das System die Angreiferin als legitime Benutzerin einschätzt. Es wurden technische Gegenmaßnahmen eingeführt, um Spoofing-Angriffe zu verhindern, welche ihre Grenzen und Nebenwirkungen besitzen [Sh21].

3 Bedrohungsmodell

Dieser Abschnitt beschreibt die Bedrohungsmodelle, die für den Angriff berücksichtigt werden. Der Spoofing-Angriff gilt für die folgenden Angriffstypen.

Interne Angreiferin: Interne Angriffe gelten als große Bedrohung, da diese schwer zu erkennen sind [Pa21]. So kann eine interne Angreiferin, beispielsweise eine verärgerte Mitarbeiterin, das gesamte Unternehmen oder zumindest jeden, der am Unternehmens-Chat teilnimmt, angreifen. In dem Szenario dieser Arbeit kann die interne Angreiferin sich als beliebige andere Mitarbeitende ausgeben und in ihrem Namen Aktionen durchführen und Nachrichten verschicken.

Externe Angreiferin: Eine externe Angreiferin hingegen muss zunächst eine Einladung erhalten, damit ein Angriff erfolgreich sein kann. Die meisten Chat-Plattformen bieten die Möglichkeit, externe Personen in ihr Chat-System einzuladen. Dies stellt eine potenzielle Bedrohung dar, denn wenn eine externe Person ihren Namen im Chat ändern kann, eröffnet dies einen Phishing-Vektor. Die Auswirkungen des Phishing-Angriffs ändern sich jedoch, da die Angreiferin in diesem Experimenten nur Kontakte kontaktieren kann, die bestimmte Kommunikationsräume mit der Angreiferin teilen, und nicht die gesamte Belegschaft des Unternehmens.

4 Methodik

Der Schwerpunkt dieser Arbeit liegt auf der Analyse, welche geschäftlichen Chats es einer potenziellen internen und externen Angreiferin ermöglichen, Phishing-Nachrichten durch gezieltes Spoofing zu versenden. In diesem Kapitel wird zunächst erläutert, wie die untersuchten Business-Chats ausgewählt wurden. Anschließend wird definiert, welche Analyseschritte bei der Untersuchung der Anwendungen durchgeführt wurden.

4.1 Geprüfte Business-Chats

Insgesamt wurden in dieser Arbeit sechs verschiedene Business-Chat-Anwendungen untersucht. Hierbei handelt es sich um *Microsoft Teams*, *Element.io*, *Google Chat*, *Mattermost*,

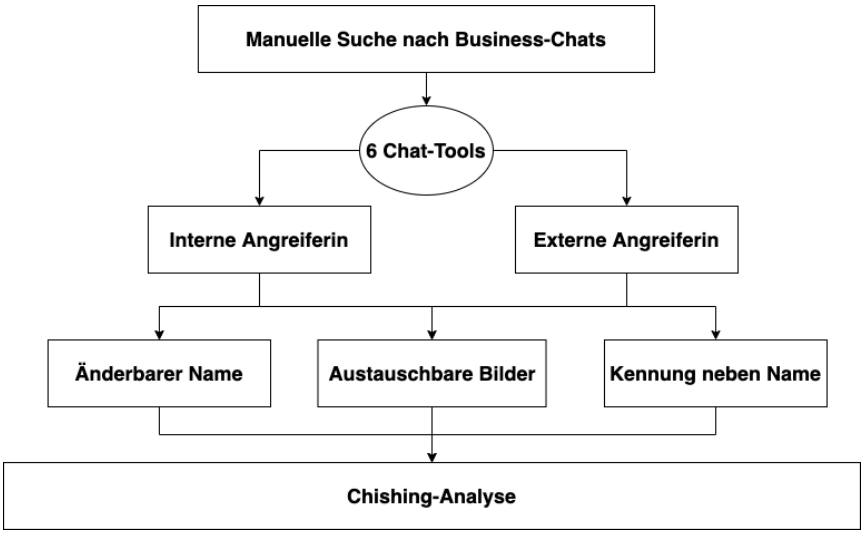

Abb. 1: Analyse-Pipeline zur Bewertung der Business-Chats

Slack und *WebEx Teams*. Mit Microsoft Teams und Slack wurden die Marktführer im Bereich Business Chat ausgewählt und um weitere vier Anwendungen ergänzt [Ke].

4.2 Analyse-Pipeline

Alle getesteten Anwendungen wurden wie in Abbildung 1 dargestellt untersucht. Zunächst wurde eine Benutzerin erstellt, die dem Angreifermodell entspricht. Dazu wurden für jede Business-Chat-Anwendung eine Gastbenutzerin und eine neue interne Benutzerin angelegt. Die folgenden Tests wurden anschließend mit diesen beiden Konten durchgeführt.

Zunächst wurde für jedes der beiden Konten geprüft, ob eine Benutzerin oder Gastbenutzerin den Namen ändern kann. Weiterhin wurde evaluiert, ob das Profilbild der Nutzerin für alle Anwendungen änderbar ist. Ziel dieser beiden Änderungen war es, das Profil einer anderen, bereits existierenden Benutzerin zu imitieren. Wenn der Name und das Profilbild einer Benutzerin geändert werden konnte, galt die Anwendung als fälschbar.

Es wurde außerdem die Anzahl der Klicks ausgewertet, die zur Identifizierung der Benutzerin erforderlich sind. Dadurch kann festgestellt werden, wie einfach es für das Opfer einer Chat-Phishing-Kampagne ist, die wahre Identität zu erkennen. Im Falle der externen Angreiferin wurde in diesem Schritt auch bewertet, wie eine Gastnutzerin identifiziert wurde.

Plattform	Externe Angreiferin möglich?	Interne Angreiferin möglich?
Microsoft Teams	Nein	Nein
Element.io	Nein	Nein
Google Chat	Ja	Ja
Mattermost	Ja	Ja
Slack	Ja	Ja
WebEx Teams	-	Ja

Tab. 1: Analysierte Plattformen und Ergebnisse

Plattform	Profilbild änderbar?	Benutzername änderbar?	Gast erkennbar?
Microsoft Teams	Ja	Nein	Ja
Element.io	Ja	Ja	Ja
Google Chat	Ja	Ja	Ja
Mattermost	Ja	Ja	Ja
Slack	Ja	Ja	Nein
WebEx Teams	Ja	Ja	Nein

Tab. 2: Übersicht, für welche Anwendungen Namens- und Profilbildänderungen möglich sind und ob eine Gastbenutzerin hervorgehoben wird

5 Ergebnisse

In Tabelle 1 sind die die Ergebnisse unserer Analyse für die sechs verschiedene Business-Chat-Tools dargestellt, bezüglich der Bedrohungsmodelle, die in Kapitel 3 definiert wurden. Insgesamt wurde festgestellt, dass es in allen Anwendungen möglich ist, das Profilbild ohne Überprüfung durch die Arbeitgeberin zu ändern und in den meisten der untersuchten Anwendungen den Anzeigenamen zu bearbeiten.

Wie in Tabelle 2 gezeigt, ist es in allen Business-Chats möglich, das Profilbild zu ändern. Der Name der eigenen Profils konnte in fünf von sechs der untersuchten Chat-Anwendungen geändert werden, was zu potenziellen *Chishing*-Angriffsvektoren führt. Bei zwei der Anwendungen ist es unter bestimmten Bedingungen nicht direkt möglich, eine externe von einer internen Angreiferin zu unterscheiden.

Abbildung 2 zeigt, dass Chat-Anwendungen identifiziert wurden, die der Benutzerin direkt die Identität (Benutzer-ID oder E-Mail-Adresse) der Angreiferin anzeigen. Bei Messengern wie *Slack* oder *WebEx* Teams muss das Opfer erst auf das Profil der Angreiferin klicken

und dann erneut klicken, um das vollständige Profil zu sehen (insgesamt zwei Klicks). In einer stressigen Situation stellt dies bereits ein erhebliches Hindernis bei der Erkennung dar. Geschäftliche Chat-Anwendungen wie *Google Chat* oder *Mattermost* zeigen der Nutzerin die Identität (E-Mail) der Angreiferin nach einem Klick auf das Profil (ein Klick) an. In

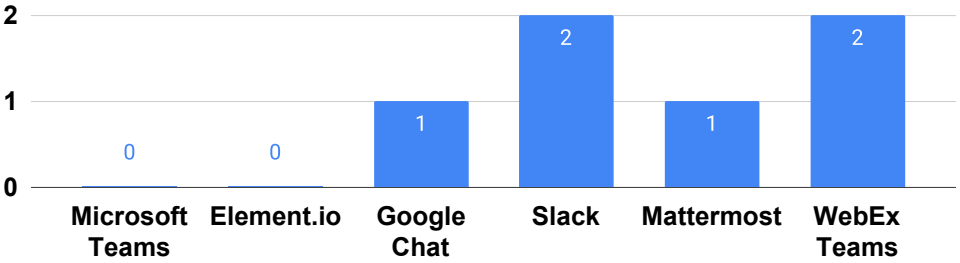

Abb. 2: Überblick über die Anzahl der Klicks, die erforderlich sind, um die Identität der Angreiferin aufzudecken

den folgenden Abschnitten werden die verschiedenen Auswirkungen und Bedrohungen beschrieben, welche die Ergebnisse für die jeweiligen Plattformen haben.

5.1 Microsoft Teams

Weder internes noch externes Spoofing ist bei Microsoft Teams möglich, wie in Tabelle 1 zu sehen ist. Bei MS Teams gehört eine Benutzerin immer zu einer Organisation, wobei Benutzerin und zugehörige Organisation von verschiedenen Administratoren verwaltet werden. Daher ist es nicht möglich, als normale Angestellte das eigene Profil zu bearbeiten. Somit ist das Bedrohungsmodell des Spoofing als interne und externe Angreiferin für Microsoft Teams hinfällig.

5.2 Element.io

Bei der Verwendung von *Element.io* als Business-Chat ist es nicht möglich, ein Profil so zu ändern, dass eine Angreiferin eine Benutzerin erfolgreich fälschen kann. Ändert eine Benutzerin ihren Namen, werden alle Mitglieder eines Kommunikationskanals benachrichtigt. Hinter dem Anzeigenamen wird außerdem immer eine eindeutige Kennzeichnung angezeigt, die für jede Benutzerin festgelegt wird und nicht geändert werden kann.

5.3 Google Chat

In Google Chat ist es relativ einfach, den angezeigten Namen zu ändern[7]. Dies ist sowohl für interne als auch für externe Angreifer möglich. Da Google Chat in Google Workplace eingebettet ist, führt die Umbenennung durch eine interne Angreiferin zu weiterer Verwirrung in anderen Google-Tools z. B. Google Kalender (Abbildung 4).

[7] `https://support.google.com/mail/answer/8158?hl=de`

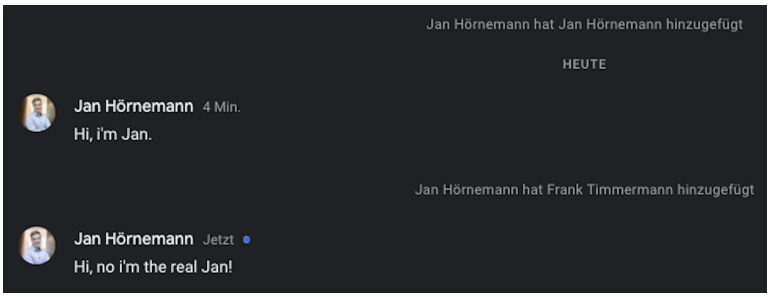

Abb. 3: Chishing-Angriff in der Google Chat-Webanwendung

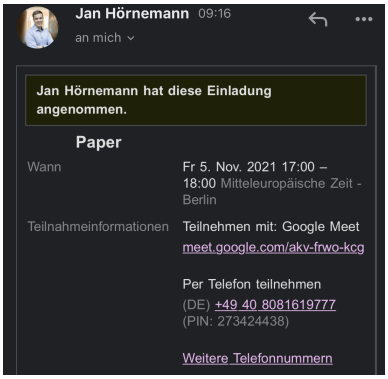

Abb. 4: Das gefälschte Konto nimmt Einladungen als jemand anderes an

Interne Angreiferin: Abbildung 3 zeigt, wie ein Chishing-Angriff in Google Chat aussehen könnte. Welches Profil des Benutzers Jan „echt“ ist, lässt sich erst erkennen, wenn sich die Nutzerin das Profil genauer ansieht und somit die unveränderbare E-Mail-Adresse angezeigt bekommt. Dies ermöglicht es internen Angreifern, eine legitime Benutzerin zu täuschen, was eine Bedrohung für Unternehmen darstellt. Das gleiche Problem besteht auch in der mobilen Version von Google Chat.

Auch beim Erstellen eines Meetings gibt es Probleme: Die E-Mail-Adresse der Benutzerin stimmt zwar nicht mit dem Namen überein, aber das wird leicht übersehen, da das Profilbild und der Anzeigename gut sichtbar sind.

Externe Angreiferin: Auch eine externe Angreiferin hat bei Google Chat mit einem Chishing-Angriff Erfolg. Ein oranger, visueller Marker in der oberen Ecke signalisiert, dass der Kanal mit einer Angreiferin geteilt wird.

5.4 Slack

Interne und externe Angreiferinnen können in Slack bestimmte Verhaltensweisen ausnutzen, um erfolgreich *Chishing*-Angriffe durchzuführen

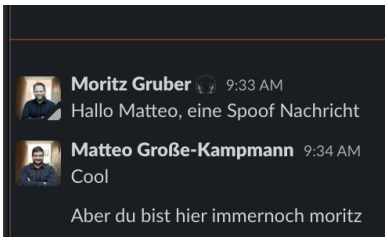

Abb. 5: Chishing in Slack - Bei dem gespooften Account handelt es sich um den Account „Moriz Gruber“

Interne Angreiferin: Als interne Angreiferin ist ein *Chishing*-Angriff umsetzbar. Wie in Abbildung 5 zu sehen ist, bemerkt die andere Person nicht, wer hinter dem Profil steckt. Selbst in der mobilen Version von Slack ist nicht erkennbar, dass es sich um einen möglichen Spoofing-Angriff handeln könnte. Der Benutzer „Matteo“ ist der legitime Benutzer und „Moritz“ ist eine gefälschte Identität von Mitarbeiter „Frank“. Dies ist jedoch für „Matteo“ in der Chat-Oberfläche nicht zu erkennen, sondern wird erst nach zwei Klicks auf den Profilbereich des gefälschten Moritz erkennbar.

Externe Angreiferin: Das externe Bedrohungsmodell kann auch in Slack umgesetzt werden. Selbst in einem Chat, in dem die echte Person und das gefälschte Profil miteinander kommunizieren, ist auf den ersten Blick kein Unterschied zu erkennen. Ein kleines graues Dreieck am unteren Rand des Profilbildes markiert eine Gast-Benutzerin.

5.5 Mattermost

Mattermost wurde als Open-Source-Alternative zu Slack entwickelt. Der Dienst ermöglicht Chats mit Einzelpersonen sowie in Gruppen. In Mattermost ist es möglich, die kompletten Benutzerdaten zu ändern und sich als eine andere Person auszugeben [8].

Interne Angreiferin: Eine interne Angreiferin kann Chishing in Mattermost durchführen. Innerhalb eines Chats ist nicht zu erkennen, dass die Gesprächspartnerin ein gefälschtes Profil sein könnte.

Externe Angreiferin: Eine externe Angreiferin kann in Mattermost auch erfolgreich ihr Profil fälschen, wenn diese zu einer geschlossenen Unterhaltung eingeladen wird. Eine normale Benutzerin kann sehen, dass die externe Angreiferin ein Gast ist, aber auch hier gibt es keine andere Möglichkeit zu erkennen, dass es sich nicht um das echte Profil handelt.

5.6 WebEx Teams

Wie bei anderen Chat-Tools, können auch bei WebEx Teams neue Chat-Bereiche innerhalb des Unternehmens erstellt oder privat mit anderen Mitarbeitern gechattet werden. Da WebEx Teams nicht die Funktion bietet, Gäste in Chaträume einzuladen, sondern nur 1:1-Gespräche zulässt, trifft das Bedrohungsmodell einer externen Angreiferin hier nicht zu.

[8] `https://docs.mattermost.com/messaging/manage-profile-settings.html?highlight=username`

Interne Angreiferin: Als interne Angreiferin war es möglich, das eigene Profil so zu bearbeiten, dass es wie ein gültiges Profil einer anderen Person aussieht [9]. In diesem Beispiel ist es fast unmöglich zu erkennen, wer das echte Profil hat und wer einen Spoofing-Angriff durchführt. Selbst in einem privaten Chat ist nicht erkennbar, ob es sich um ein gefälschtes Profil handelt. Es wird nur die Endung der E-Mail-Adresse angegeben, die aber nicht aussagekräftig genug ist, um eine Person genau zu identifizieren.

6 Fazit

Insgesamt kann festgestellt werden, dass *Chishing* in der Mehrheit der untersuchten Business-Chats nicht behandelt wird und unsere Forschungsarbeit der erste Versuch ist, diese aufkommende Bedrohung zu untersuchen. In fünf der sechs untersuchten Business-Chat-Anwendungen war es möglich, den Namen der Benutzerin nach Belieben für eine interne oder eingeladene, externe Angreiferin zu ändern. Dies stellt eine große Bedrohung für die sichere Nutzung von Chats im geschäftlichen Kontext dar. Insbesondere Chats dienen dem schnellen und permanenten Austausch von Informationen, was eine Angreiferin mit gefälschten Benutzernamen ausnutzen kann. Außerdem ist das Vertrauen in Chat-Nachrichten in der Regel höher als in E-Mails [BAB+21].

Um dieses Problem zu beheben, können Business-Chat-Anwendungen verschiedene Maßnahmen ergreifen. So wäre es zum Beispiel möglich, die Identität der Nutzerin neben dem Nutzernamen anzuzeigen, wie es Element.io implementiert hat. Eine andere Möglichkeit wäre, ähnlich wie bei Microsoft Teams, die Benutzer über die Administratorin daran zu hindern, deren Namen serverseitig ändern zu können. Insgesamt ist festzuhalten, dass neben den klassischen Phishing-Methoden *Chishing* ein weiteres großes Bedrohungspotenzial ermöglicht. Gerade in der modernen, Home-Office-getriebenen Büroumgebung müssen Aufklärungs- und Sensibilisierungskampagnen zum Schutz vor Chishing-Angriffen durchgeführt werden. Business-Chat-Plattformen müssen Maßnahmen ergreifen, um ihre Benutzer vor dieser Art von Angriffen zu schützen und Unternehmen sollten diese Bedrohung in ihrem Risikomanagementprozess diskutieren.

Literatur

[BAB+21] Blancaflor, E. B.; Alfonso, A. B.; Banganay, K. N. U. et al.: Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools. Proceedings of the International Conference on Industrial Engineering and Operations Management/, 2021.

[BKH16] Boulkenafet, Z.; Komulainen, J.; Hadid, A.: Face Spoofing Detection Using Colour Texture Analysis. IEEE Transactions on Information Forensics and Security 11/8, S. 1818–1830, 2016.

[Br16] Broadbent, S.: Intimacy at Work: How Digital Media Bring Private Life to the Workplace. Routledge, Walnut Creek, CA, 2016.

[9] `https://help.webex.com/en-US/article/nmig1kcb/Edit-your-Webex-Meetings-profile`

[Cr82] Crocker, D.: RFC#822: Standard for the format of ARPA Internet text messages, 1982.

[FV18] Ferreira, A.; Vieira-Marques, P.: Phishing Through Time: A Ten Year Story based on Abstracts. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy. ICISSP '18, INSTICC, SciTePress, Setúbal, Portugal, S. 225–232, 2018, ISBN: 978-989-758-282-0.

[Ke] Kent, D.: Slack vs Microsoft Teams 2021 – The Enterprise Messaging Wars Continue, Digital, https://web.archive.org/web/20220109224334/https://dispatch.m.io/enterprise-messaging-wars-slack-microsoft-teams/, Datum des letzten Abrufs: 28. Januar 2022.

[Ne] New York Times: An Old Swindle Revived, Print, https://web.archive.org/web/20201112040016/https://www.nytimes.com/1898/03/20/archives/an-old-swindle-revived-the-spanish-prisoner-and-buried-treasure.html, Datum des letzten Abrufs: 28. Januar 2022.

[Ol04] Ollmann, G.: The Phishing Guide–Understanding & Preventing Phishing Attacks. NGS Software Insight Security Research/, 2004.

[Pa15] Parsons, K.; McCormac, A.; Pattinson, M.; Butavicius, M.; Jerram, C.: The Design of Phishing Studies: The design of phishing studies: Challenges for researchers. Computers & Security 52/C, S. 194–206, 2015, ISSN: 0167-4048.

[Pa21] Padayachee, K.: A Theoretical Underpinning for Examining Insider Attacks Leveraging the Fraud Pentagon. In: International Symposium on Human Aspects of Information Security and Assurance. Springer, S. 179–188, 2021.

[Sh21] Shen, K.; Wang, C.; Guo, M.; Zheng, X.; Lu, C.; Liu, B.; Zhao, Y.; Hao, S.; Duan, H.; Pan, Q. et al.: Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks. In: 30th USENIX Security Symposium (USENIX Security 21). 2021.

[Ti11] Tippenhauer, N. O.; Pöpper, C.; Rasmussen, K. B.; Capkun, S.: On the Requirements for Successful GPS Spoofing Attacks. In: Proceedings of the 18th ACM conference on Computer and communications security. S. 75–86, 2011.