FERDINAND PORSCHE
FERN FH

Planung, Durchführung und Auswertung einer Phishing-Simulation im eigenen Unternehmen

Bachelorarbeit

eingereicht von: **Christian Blaschitz**
Matrikelnummer: 51841000

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades <einer/eines>

Bachelor of Arts in Business

Betreuung und Beurteilung: Dipl.-Ing. Thomas Györgyfalvay, BA MBA

Wiener Neustadt, November 2023

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Signiert von:	Christian Blaschitz
Datum:	14.11.2023 15:32:48

Dieses Dokument ist digital signiert!

Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

Seewalchen am Attersee, 14. November 2023

Unterschrift

Die Kapitel 2 bis 3 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 20.09.2023 als Bachelorarbeit 1 angenommen.

Kurzzusammenfassung: Planung, Durchführung und Auswertung einer Phishing-Simulation im eigenen Unternehmen

Das Ziel dieser Bachelorarbeit ist die Beantwortung der Forschungsfrage „Wieviel Prozent meiner Kolleginnen und Kollegen sind anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation?“. Im Rahmen der Arbeit wurden die wesentlichen Faktoren des Themas „Phishing“ betrachtet, um eine zielgerichtete Phishing-Simulation zu planen, durchzuführen und auszuwerten. Der Fokus lag, neben dem Inhalt der simulierten Phishing-E-Mails, auch auf der Wahl der passenden Angriffsmethode und dem idealen Zeitpunkt für den Versand. Die Inhalte bedienen die zwei Manipulationstechniken „Neugierde“ und „Druck“. Die passende Angriffsmethode lässt die Empfangenden glauben, sie würden eine legitime E-Mail lesen und eine legitime Webseite besuchen. Dafür kamen „Domain-Squatting“ und „Typo-Squatting“ zum Einsatz. Diese sind einfach umzusetzen, jedoch für Empfangende oft schwer zu erkennen. An Montagen und Freitagen sind Empfangende oftmals unaufmerksam, deshalb wurden diese Tage für die Zustellung der Phishing-E-Mails gewählt. Neben der Erstellung der Inhalte war auch die technische Umsetzung wichtig. Das Phishing-Framework „Gophish“ bietet alle Funktionen, die für diese Arbeit nötig waren. Es ermöglicht eine einfache Erstellung der Inhalte und bietet zudem gute Möglichkeiten für die Auswertung der Kampagnen.

Die Phishing-Simulation lief über einen Zeitraum von drei Wochen. In dieser Zeit haben zehn der achtundvierzig Empfangenden auf die simulierten Phishing-E-Mails reagiert und somit die Hypothese des Autors bestätigt.

Schlagwörter:

Phishing, Phishing-Simulation, Planung einer Phishing-Simulation, Durchführung einer Phishing-Simulation, Auswertung einer Phishing-Simulation, KMU Phishing-Simulation

Abstract: Planning, Executing and Evaluating a Phishing-Simulation in your own Company

The goal of this bachelor thesis is to answer the research question "What percentage of my colleagues are vulnerable to a self-performed email phishing simulation?". Within the scope of the thesis, the essential factors of the topic "phishing" were considered in order to plan, execute and evaluate a targeted phishing simulation. Besides defining the content of the simulated phishing emails, the choice of the appropriate attack method and the ideal time to send the mails was in focus. The content serves two manipulation techniques, "curiosity" and "pressure". The attack method makes recipients believe they are reading a legitimate email and visiting a legitimate website. Therefore, "domain squatting" and "typo squatting" were used. These are easy to implement, but often difficult for recipients to detect. On Mondays and Fridays, recipients are often inattentive, so these days were chosen for the delivery of the phishing emails. In addition to the creation of the content, the technical implementation was also important. The phishing framework "Gophish" offers all functions that were necessary for this work. It allows an easy creation of the content and offers good possibilities for the evaluation of the campaigns.

The phishing simulation ran over a period of three weeks. During this time, ten of the forty-eight recipients reacted to the simulated phishing emails, confirming the hypothesis of the author.

Keywords:

Phishing, Phishing-Simulation, Planing a Phishing-Simulation, Executing a Phishing-Simulation, Evaluating a Phishing-Simulation, SMB Phishing-Simulation

Inhaltsverzeichnis

1. Einleitung

Dieses Kapitel stellt den Eingangspunkt zu dieser wissenschaftlichen Arbeit dar. Es soll ein grundsätzliches Verständnis zur aktuellen Lage der IT-Sicherheit in KMU schaffen und die Zielsetzung dieser Thesis erklären.

1.1 Aktuelle Lage der IT-Sicherheit in KMU

Die aktuelle Lage der IT-Sicherheit in kleinen und mittleren Unternehmen (KMU) unterscheidet sich nicht grundlegend von derer großer Unternehmen. Es gibt jedoch ein paar Unterschiede und Eigenheiten, die berücksichtigt werden sollten. Der größte Unterschied zwischen KMU und großen Unternehmen ist, dass KMU in der Regel weniger Ressourcen zur Verfügung stehen, um die IT-Sicherheit zu verbessern. Es gibt nur selten die Mittel für spezialisierte IT-Fachkräfte und teure Sicherheitslösungen. Dies führt dazu, dass KMU häufig weniger gut geschützt sind als größere Unternehmen.

Der zunehmende Grad der Digitalisierung in produzierenden KMU sorgt zudem für eine verstärke Nutzung und Abhängigkeit von Informationstechnologien. War das Thema „Digitalisierung“ im Jahr 2016 für nur 25,8 Prozent der deutschen KMU von großer Bedeutung, waren es 2021 bereits 72,5 Prozent (Löher u. a. 2022). Viele KMU haben also erkannt, dass die Digitalisierung ihrer Geschäftsprozesse wichtig ist, um wettbewerbsfähig zu bleiben und die Effizienz zu verbessern. So wird die Digitalisierung immer mehr zum Gegenstand der Unternehmensstrategie. Diese birgt, neben den offensichtlichen Vorteilen, auch einige Gefahren und geht mit einer Vielzahl von zusätzlichen IT-Sicherheitsrisiken einher. Das führt seit Jahren zu einer weitreichenden Professionalisierung von Cybercrime. Der immer digitaler werdende Alltag der Unternehmen offenbart eine größere Angriffsfläche und führt zu Rekordumsätzen bei Angreifern. Laut der Allianz Versicherung überstieg die jährliche globale Schadenshöhe durch Cybercrime bereits im Jahr 2021 die 1-Billion-Dollar-Marke. Noch zwei Jahre zuvor war die Schadenshöhe rund 50 Prozent niedriger (Allianz 2021).

Auch haben sich, so das Ergebnis einer Umfrage der Allianz, „Cyber-Vorfälle“, wie in Abbildung 1 dargestellt, zum weltweiten Platz Eins der Geschäftsrisiken entwickelt. Im Jahr 2022 waren bereits 44 Prozent der Befragten der Meinung, dass „Cyber-Vorfälle“ das größte Geschäftsrisiko darstellen. Auch die mit 42 Prozent als zweitgrößtes

Geschäftsrisiko bewertete „Betriebsunterbrechung“ spielt eine große Rolle, da es durch Angriffe auf die IT-Infrastruktur nicht selten auch zu Betriebsunterbrechungen kommt (Allianz 2022). Für das Jahr 2023 zeigte diese jährlich durchgeführte Umfrage ein ähnliches Bild. Die Kategorie „Cybervorfälle“ ist noch auf Platz Eins, teilt sich diesen jedoch mit der „Betriebsunterbrechung“. Nur noch für 34 Prozent der Befragten stellen Cybervorfälle die größte Gefahr dar. Den größten Zuwachs konnten die Kategorie „Makroökonomische Entwicklungen“ (Gesamt 25 Prozent mit einem Plus von 11 Prozent im Vergleich zum Vorjahr) und die 2023 neu gelistete Kategorie „Energiekrise“ verzeichnen (Allianz 2023).

Abbildung 1 - Top 10 Geschäftsrisiken weltweit 2023. Quelle: (Allianz 2023)

Dies bestätigt auch Kaspersky und nennt Zahlen speziell von KMU. So würden 39 Prozent der befragten Unternehmen eine Cyberattacke als Krise definieren. In dieser

Umfrage ist dies jedoch nur das drittgrößte Risiko, hinter einem dramatischen Einbruch der Verkaufszahlen und einer Naturkatastrophe (Kaspersky 2022).

Ein brisanter Trend ist die laufende Erhöhung der Anzahl von Homeoffice-Arbeitsplätzen. War das Ausweichen ins Homeoffice anfangs eine akute Maßnahme gegen die COVID-19-Pandemie, ist dieses Arbeitsplatzmodell bei einigen Unternehmen beliebt geworden und nun gelebte Praxis. Der Erweiterung des Unternehmensnetzwerks durch Geräte im Homeoffice steht einer gestiegenen Anzahl an Angriffen auf ebendiese Komponenten gegenüber. Durch das erhöhte Risiko von Homeoffice-Arbeitsplätzen konnten im Jahr 2020 Schäden in der Höhe von 52,5 Milliarden Euro auf Angriffe auf Homeoffice-Arbeitsplätze zurückgeführt werden. 2019 lag die Summe dafür noch bei 21,5 Milliarden Euro. Die Schäden haben sich proportional zur Anzahl der Homeoffice-Nutzer entwickelt, was den deutlichen Anstieg der Anzahl und Schadenssummen der Angriffe erklärt (Engels 2021).

Eine positive Entwicklung hingegen gibt es bei den Einschätzungen von KMU, die Wichtigkeit von IT-Sicherheit betreffend. Die Initiative „Sicher-im-Netz“ führt jährliche Umfragen zum Thema IT-Sicherheit im Mittelstand durch. In deren Report aus dem Jahr 2021 wurde veröffentlicht, dass 86 Prozent der Befragten ihr Unternehmen als abhängig von der IT-Sicherheit sehen (Kellner 2021).

1.2 Arbeitsziel und methodische Vorgehensweise

Dieses Kapitel beschreibt das Ziel dieser Arbeit und zeigt die Methoden auf, die zur Beantwortung der Forschungsfrage und somit zum Erreichen des Arbeitsziels führen werden.

1.2.1 Arbeitsziel

Ziel der Arbeit ist es, herauszufinden, wieviel Prozent der Arbeitskolleg:innen des Autors anfällig auf eine von ihm geplante, durchgeführte und ausgewertete E-Mail-Phishing-Simulation sind.

Entscheidend für den Erfolg wird sein, dass die Inhalte und die Durchführung der Phishing-Simulation möglichst realistisch sind. Somit ist es ein Ziel, sowohl die Inhalte als auch die technische Umsetzung vergleichbar mit einem tatsächlichen, zielgerichteten Angriff zu machen.

1.2.2 Methodische Vorgehensweise

Um die Phishing-Simulation möglichst realistisch zu gestalten, gilt es herauszufinden, welche Inhalte aktuell in Phishing-Angriffen eingesetzt werden und welche von diesen die größte Gefahr darstellen. Die schwerwiegendste Gefahr stellen die Inhalte dar, auf die die Angegriffenen am wahrscheinlichsten reagieren.

Zur Feststellung der am besten geeigneten Inhalte werden aktuelle Reports und Beiträge ausgewertet. Dies wird einen Überblick über aktuelle Trends geben und bei der Auswahl von drei, für das Zielunternehmen am potenziell gefährlichsten, Inhalten helfen.

Ein nächster Punkt wird sein, herauszufinden, wie eine Phishing-Simulation technisch effizient und effektiv durchgeführt werden kann. Da sowohl die Durchführung als auch die Auswertung idealerweise auf nur einer Plattform durchgeführt werden können, bietet sich die Verwendung eines vollwertigen Phishing-Frameworks an. Dabei sollte bevorzugt auf eine Open-Source-Lösung zurückgegriffen werden, um etwaige Datenschutz-Risiken zu minimieren.

Für die technische Durchführung der Phishing-Simulation werden mehrere aktuell verfügbare Phishing-Frameworks evaluiert und gegebenenfalls getestet. Das für den Anwendungsfall am besten geeignete wird für die Durchführung ausgewählt.

Im zweiten Teil der Arbeit werden die aus dem ersten Teil gewonnenen Erkenntnisse umgesetzt. Zudem wird die technische Umsetzung stattfinden, sowie das gewählte Phishing-Framework installiert und so konfiguriert, dass eine Phishing-Simulation im Zielunternehmen durchgeführt werden kann. Dies beinhaltet auch die Registrierung etwaiger Domänen und die Konfiguration zusätzlich notwendiger Dienste. Das könnten zum Beispiel die Bereitstellung eines Webservers zur Darstellung der Phishing-Webseiten oder die Installation eines E-Mail-Servers zum Versand der Phishing-E-Mails sein.

Ist die technische Grundlange geschaffen, werden die zuvor identifizierten Inhalte erstellt und an das Zielunternehmen angepasst. Der Inhalt der Phishing-Mails geht aus der vorangegangenen Recherche hervor. Großes Augenmerk wird auf die Qualität, sowohl der Inhalte als auch der Umsetzung, gerichtet sein. Die Phishing-Simulation soll technisch und inhaltlich nicht von einer echten, zielgerichteten Attacke zu unterscheiden sein.

Nachdem die technische Umsetzung erfolgt ist und die Inhalte fertiggestellt sind, wird die Phishing-Simulation zu einem passenden Zeitpunkt durchgeführt. Um ein realistisches Ergebnis zu erzielen, werden nicht alle Phishing-Mails zeitgleich, sondern über den Zeitraum von mehreren Wochen ausgeschickt. Dabei wird darauf geachtet, dass nicht alle Empfänger:innen zeitgleich identische E-Mails erhalten, sondern eine möglichst breite Streuung der verschiedenen Inhalte angestrebt. Es muss jedenfalls

sichergestellt werden, dass am Ende der Simulation alle Teilnehmenden eine E-Mail mit je einem der drei zuvor definierten Inhalte erhalten haben.

Im Anschluss an die Durchführung der Phishing-Simulation wird diese ausgewertet. Dabei soll festgestellt werden, wieviel Prozent der Empfänger:innen die Phishing-E-Mails geöffnet haben und zudem, wieviel die darin enthaltenen Links angeklickt haben. Ebenso wird die Anzahl derer Empfänger:innen, die ihre Zugangsdaten preisgegeben haben, festgestellt. Die Auswertung wird es ermöglichen, die Forschungsfrage zu beantworten und somit die Hypothese dieser Arbeit zu bestätigen oder zu falsifizieren.

1.3 Forschungsfrage und Hypothese

Dieses Kapitel beinhaltet die Forschungsfrage dieser Arbeit und die darauf aufbauende Hypothese.

1.3.1 Forschungsfrage

Die konkrete Forschungsfrage, die es im Rahmen dieser Arbeit zu beantworten gilt, lautet:

> ***Wieviel Prozent meiner Kolleginnen und Kollegen sind anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation?***

1.3.2 Hypothese

Die Hypothese des Autors zur Forschungsfrage lautet:

> ***Mehr als 20 Prozent meiner Kolleginnen und Kollegen sind anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation.***

1.4 Aufbau der Arbeit

Die Einleitung dieser Arbeit gibt einen Überblick über die aktuelle Lage der IT-Sicherheit in KMU. Dies soll einen groben Ausblick auf die aktuellen Cyber-Gefahren und Trends schaffen. Weiters wird dort das Arbeitsziel und die methodische Vorgehensweise erläutert, sowie die Forschungsfrage samt der zugehörigen Hypothese des Autors beschrieben. Abgerundet wird das erste Kapitel durch diesen Überblick über den Aufbau der Arbeit und die Begriffsdefinitionen, in denen die verwendeten Fachausdrücke erklärt werden.

Im zweiten Kapitel wird näher auf das Thema „Phishing“ eingegangen. Da diese Cyber-Attacke der zentrale Gegenstand dieser Arbeit ist, wird das Thema sehr umfangreich

behandelt. Neben der Definition des Begriffs „Phishing“ gibt es einen Überblick über die aktuell gängigen Phishing-Methoden, sowie die Ziele und Motivation von Phishing-Attacken. Auch werden ausgewählte vergangene Phishing-Attacken vorgestellt, aktuelle Beispiele von Phishing-E-Mails beleuchtet sowie mögliche Maßnahmen zur Verhinderung von Phishing erklärt.

Kapitel drei wird den ersten Teil der Arbeit abschließen und neben dem aktuellen Stand der Technik, dem aktuellen Stand der Wissenschaft und dem konzeptionellen Lösungsvorgang auch eine Kurzvorstellung des Unternehmens, in dem die Phishing-Simulation durchgeführt wird, beinhalten. Beim aktuellen Stand der Technik wird auf die drei großen Themen dieser Arbeit eingegangen. So wird dort die Planung, die Durchführung und die Auswertung einer Phishing-Simulation im Detail behandelt. Der aktuelle Stand der Wissenschaft soll zeigen, welche anderen Ansätze es zur Beantwortung der Forschungsfrage schon gab.

Das Kapitel vier behandelt die Umsetzung der technischen Voraussetzungen des empirischen Teils dieser Arbeit. Darin wird auf die technischen Notwendigkeiten für die Durchführung einer Phishing-Simulation im Zielunternehmen eingegangen und die Installation des Phishing-Frameworks beschrieben.

Kapitel fünf zeigt, wie die Phishing-Kampagnen erstellt werden und wie diese aufgebaut sind. Darin wird präsentiert, wie die Phishing-Inhalte aussehen und welche Angriffsmethoden verwendet werden. Weiters beinhaltet dieses Kapitel Informationen über die Zusammensetzung der Adressat:innen-Gruppen und den Zeitplan für den Versand der Phishing-E-Mails

Das sechste Kapitel dieser Arbeit ist der Auswertung der Phishing-Simulation gewidmet.

Kapitel sieben stellt die Schlussfolgerung dieser wissenschaftlichen Arbeit dar. Darin wird die Forschungsfrage erneut erläutert und beantwortet. Dort findet sich auch die Bestätigung bzw. Falsifizierung der Hypothese des Autors.

Im abschließenden Kapitel acht findet sich eine Zusammenfassung der Arbeit und ein Ausblick. Die Zusammenfassung stellt die gewonnen Informationen und die verwendeten Methoden nochmal komprimiert dar. Der Ausblick zeigt neue Perspektiven für die Praxis und mögliche neue Forschungsansätze, die sich aus dieser Arbeit ergeben haben, auf.

2. Phishing

Die Grundlage für die Cyber-Attacke „Phishing“ ist das „Social Engineering“. Dies zielt darauf ab, den Menschen, als das vermeintlich schwächste Glied in der Cyber-Security-Kette (mmannika 2021), dahingehend zu manipulieren, dass sensible Informationen preisgegeben werden oder den Angreifenden Zugang zu geschützten Bereichen ermöglicht wird (Uebelacker und Quiel 2014).

2.1 Definition Phishing

Das Thema „Phishing“ ist ein sehr aktuelles und breit gestreutes. Auch ist es nicht nur relevant für Unternehmen und deren IT-Spezialisten, sondern etwas, das bei jeder und jedem im Alltag angekommen ist. Gerade, weil mittlerweile in vielen Bereichen des täglichen Lebens mit Phishing-Attacken zu rechnen ist, wurde es schnell ein recht komplexes und umfangreiches Thema. Das zeigt sich schon bei der Definition vom Begriff „Phishing“. Im Jahr 2014 erschien eine Arbeit, in der 113 einzigartige Definitionen untersucht wurden, um dem Ausdruck „Phishing“ eine einheitliche Definition zu geben. Das Ergebnis lautete: „Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target“ (Lastdrager 2014). Diese Definition ist sehr allgemein gehalten, jedoch noch gültig. In Anbetracht ihres Alters und der rasenden Entwicklung des Themas, sollten sich aber noch weitere Definitionen angesehen werden. Eine lautet: „The practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly“ (Webster 2023). Diese Definition beschreibt die aktuell gängige Praxis und betont, dass sich Phishing heute primär im Internet abspielt.

Erwähnt werden sollten jedoch auch Phishing-Methoden, die nicht darauf abzielen, die Angegriffenen zur Herausgabe von sensiblen Informationen zu bewegen. Wie erwähnt, kann es Angreifenden auch darum gehen, die Opfer dazu zu bringen, etwas zu machen, dass sie nicht machen sollten. Ein Beispiel dafür ist der „Business E-mail Compromise“. Dies ist eine Angriffsmethode, die darauf abzielt, die Angegriffenen zum Transfer von finanziellen Mitteln zu verleiten (Microsoft 2021).

Damit Phishing Erfolg hat, geben sich die Angreifenden während ihrer Attacken als legitime und den potenziellen Opfern bekannte Personen oder Organisationen aus und versuchen so, die Bekanntheit und das Vertrauen in die imitierte Instanz auszunutzen, um an ihr Ziel zu gelangen. (IBM 2022)

2.2 Phishing-Methoden

Es gibt verschiedene Methoden, mit denen Phishing-Attacken durchgeführt werden. Da jedoch immer der Mensch das Ziel einer Phishing-Attacke ist, muss dieser möglichst direkt erreicht werden. Dies geschieht in der Praxis heutzutage meist per E-Mail oder Kurznachrichten, manchmal auch noch telefonisch.

Die häufigste Phishing-Methode ist seit einigen Jahren das E-Mail-Phishing. Diese charakterisiert sich dadurch, dass eine Vielzahl von potenziellen Opfern eine E-Mail des Angreifers erhält. In dieser E-Mail findet sich meist ein Link zu einer Webseite, an der sich die Empfangenden der E-Mail anmelden und so dem Angreifenden ihre Zugangsdaten preisgeben sollen. Die gefälschte Webseite ist dem original nahezu ident. Bei diesen gefälschten Webseiten handelt es sich häufig um Online-Zahlungsdienstleister, Soziale Netzwerke oder E-Mail-Anbieter. Das E-Mail-Phishing ist deswegen so erfolgreich, weil bei gut gemachten Phishing-E-Mails sowohl der Inhalt dieser als auch die gefälschte Webseite auf den ersten Blick legitim aussehen und sich kaum vom Original unterscheiden. Zudem ist es verhältnismäßig einfach, an eine große Anzahl von gültigen E-Mail-Adressen zu gelangen. Dies macht das E-Mail-Phishing zu einer beliebten und lukrativen Methode, um an sensible und persönliche Daten zu gelangen. (Irwin 2023)

Eine weitere Methode des E-Mail-Phishings ist das Spear-Phishing. Zielt eine allgemeine Phishing-Attacke auf eine Vielzahl von potenziellen Opfern ab, so fokussiert sich das Spear-Phishing auf ein klar definiertes Ziel. Es kann sich auf eine einzelne Person oder eine Personengruppe beschränken. Dies ist eine zielgerichtete Attacke und muss vorab geplant werden. Finden die Angreifenden genug Informationen über ihr Opfer, können sie die Inhalte der Phishing-Attacke an dieses anpassen und eine maßgeschneiderte Attacke durchführen. Häufig wird versucht, sich als Lieferant oder Kunde des Angegriffenen auszugeben, um so Druck auszuüben und die Herausgabe von Informationen zu erreichen. Die Informationen gewinnen die Angreifenden häufig aus sozialen Medien und der Unternehmenswebseite. Zielt eine Spear-Phishing-Attacke auf ein Mitglied der Geschäftsleitung ab, wird diese Attacke „Whaling“ genannt. Ein solcher Angriff auf die Unternehmensspitze erlaubt es den Angreifenden, noch sensiblere und für diese Personenschicht spezifische Inhalte für die Spear-Phishing-Attacken zu verwenden. (Irwin 2023)

Eine weitere Form von Spear-Phishing ist der „Business E-Mail Compromise“, kurz BEC. Diese Angriffsmethode ist auch als „CEO-Fraud“ oder „Fake-President-Fraud“ bekannt. Dabei zielen die Angreifenden wieder auf ein Mitglied der Geschäftsleitung oder eine andere Schlüsselfigur eines Unternehmens ab. Beim BEC wollen sie diese aber nicht dazu verleiten, ihre Daten preiszugeben, sondern imitieren diese und täuschen so andere Mitarbeitende des Unternehmens. Die Angreifenden versuchen ihre Opfer so zur Überweisung von Geld zu verleiten. Diese Art der Attacke hat in der Vergangenheit

bereits zu massiven finanziellen Schäden bei Unternehmen geführt und wird immer häufiger beobachtet. (Proofpoint 2022)

Eine Phishing-Methode, die sich nicht der E-Mail-Technologie bedient, ist das „Vishing". Zusammengesetzt aus dem „V" für „Voice" und dem bekannten Begriff „Phishing", beschreibt es Angriffe, die über das Telefon durchgeführt werden. Dabei geben sich die Angreifenden gegenüber ihren Opfern meist als Mitarbeitende einer bekannten Organisation aus und üben massiven Druck auf diese aus. Ziel ist auch hier meist die Bekanntgabe von Daten oder Informationen, häufig liegt der Fokus zudem auf Kreditkartendaten. (Irwin 2023)

Eine weitere Methode ist das „Smishing". Dieser Begriff setzt sich aus dem Begriff SMS und dem geläufigen Begriff „Phishing" zusammen und beschreibt Phishing-Angriffe, die über Kurznachrichten am Smartphone empfangen werden. Inhaltlich orientiert sich diese Phishing-Attacke an der E-Mail- bzw. Spear-Phishing-Attacke. Die Kontrolle des Absenders und der Seriosität des Inhaltes ist am Smartphone umständlicher als auf dem Computer. Auch gibt es weniger Sicherheitsmechanismen, um die Inhalte von Kurznachrichten vor der Zustellung prüfen. Das und die Tatsache, dass mobile Endgeräte eine immer größere Rolle im Alltag spielen, macht diese Art der Attacke immer häufiger. (Irwin 2023)

2.3 Motive und Ziele von Phishing

Das E-Mail-Phishing ist eine sehr effektive Cyber-Attacke. Trotz der Tatsache, dass sie einfach verwirklichbar und kostengünstig ist, verspricht sie großen Erfolg, um an die gewünschten Informationen zu kommen. Durch die Wahl der geeigneten Phishing-Methode und der passenden Inhalte kann der Angriff an die Zielgruppe angepasst und so die Wahrscheinlichkeit für einen erfolgreichen Angriff gesteigert werden. Im Vergleich zu anderen Cyber-Attacken ist E-Mail-Phishing technisch einfach zu realisieren und für die Angreifenden auch ohne weitreichendes technisches Verständnis durchführbar. (Ahona 2022)

Obwohl das Bewusstsein für Phishing größer wird, ist es für viele Anwender:innen immer noch schwer, eine Phishing-Mail und die darin verlinkte Phishing-Seite von einer legitimen zu unterscheiden. Gerade, da das Internet laufend auch nicht-versierten Personen zugänglich gemacht wird, wächst die Zielgruppe und die Anzahl der potenziellen Opfer stetig (Erkkila 2011). Neben der technisch einfachen Umsetzung macht auch die schwierige Strafverfolgung das Versenden von Phishing-Mails sehr beliebt.

So breitgefächert die Möglichkeiten von Phishing sind, so sind es auch die Ziele. Diese können dabei in drei Kategorien unterteilt werden (McNeal 2022).

- Datendiebstahl – Daten sind in unserer Zeit ein wichtiges Gut. Gelangen sie in die falschen Hände, können diese weiterverkauft oder zur Erpressung verwendet werden.
- Identitätsdiebstahl – Wenn Angreifer an persönliche Daten der Angegriffenen gelangen, können diese online von ihnen imitiert werden. Diese gestohlenen Identitäten können für weitere kriminelle Handlungen genutzt oder an Dritte weiterverkauft werden.
- Finanzieller Diebstahl – Immer populärer werden die oben erwähnten BEC-Attacken, durch die Cyberkriminelle an große Geldbeträge gelangen können.

2.4 Erfolgreiche Phishing-Attacken

Die erste nennenswerte Phishing-Attacke hat im Jahr 1996 stattgefunden und zielte auf US-Amerikanische Nutzer:innen von America Online (AOL) ab. AOL war damals der führende Internetanbieter in den USA. Die Angreifenden generierten gefälschte Kreditkartendaten und registrierten sich damit für neue, kostenlose AOL-Test-Accounts. Aufgrund der gefälschten Kreditkartendaten waren diese nicht lange gültig. Sie konnten damit aber Zugriff auf das Internet bekommen, um dort automatisiert Chat-Nachrichten zu versenden, in denen sie sich als Administratoren von AOL ausgegeben haben. So wurde versucht, an die Zugangsdaten von legitimen Nutzer:innen zu gelangen, um diese dann weiterzuverkaufen oder für den eigenen Zugang zum Internet zu nutzen. (Rekouche 2011)

Ein bekannter Fall aus Österreich zeigt, dass es nicht immer nur um den Diebstahl von Zugangsdaten geht, sondern dass auch die Imitation einer Führungskraft, in diesem Fall des Geschäftsführers, weitreichende Folgen haben kann. Die Firma FACC, mit Sitz im oberösterreichischen Ried im Innkreis, ist „ein weltweit führendes Aerospace Unternehmen in Design, Entwicklung und Fertigung von fortschrittlichen Komponenten und -systemen für Luftfahrzeuge“ (FACC 2023). Zu Beginn des Jahres 2016 wurde bekannt, dass es Angreifern gelungen ist, sich 54 Millionen Euro vom Unternehmen überweisen zu lassen. Die Angreifenden gaben sich in E-Mails gegenüber der Unternehmens-Buchhaltung als Geschäftsführer aus und wiesen diese an, insgesamt 54 Millionen Euro in mehreren Überweisungen an ausländische Konten zu überweisen. Es ist gelungen, etwa 10 Millionen Euro wieder zurückzuholen – die Schadenshöhe von 42 Millionen Euro ist jedoch immer noch beträchtlich. Möglich wurde das durch eine erfolgreiche Spear-Phishing-Attacke auf die damalige Leiterin der Buchhaltung. (TrendMicro 2016)

Ein weiteres nennenswertes Beispiel für Phishing war die Fußball-Weltmeisterschaft im Jahr 2018 in Russland. Die weltweite Begeisterung für Fußball wurde dabei von einer Vielzahl an Cyberkriminellen ausgenutzt, um sich an der Reichweite der Veranstaltung

zu bereichern. So wurde bereits lange vor dem Anstoß des Eröffnungsspiels eine Flut an schadhaften E-Mails registriert. Darin ging es unter anderen um den Verkauf gefälschter Tickets, den Handel mit gefälschten Fanartikeln und das Anbieten von falschen Reise- und Unterkunftsangeboten. Neben diesen Methoden gab es auch einige Phishing-Versuche. So wurde den Angegriffenen in E-Mails, die den Anschein erweckten, sie würden direkt von der FIFA kommen, versprochen gratis Tickets zu bekommen. Hinter dem Link in der E-Mail befand sich eine Website, die einen aufforderte, persönliche Daten anzugeben. Im Rahmen der Fußball-Weltmeisterschaft 2018 gab es dadurch eine Vielzahl an Geschädigten. (Healy 2018)

2.5 Aktuelle Phishing-Angriffe

An dieser Stelle werden ein paar Beispiele von aktuellen Phishing-Inhalten präsentiert. Diese stammen unter anderem aus Portalen, die es sich zur Aufgabe gemacht haben, ihre Besucher:innen auf aktuelle Gefahren hinzuweisen.

Abbildung 2 zeigt eine E-Mail, die den Anschein erweckt vom Zahlungsdienstleister „PayPal“ zu stammen. Darin wird, hinter dem Deckmantel des Themas Datenschutzgrundverordnung, Druck auf die Empfangenden ausgeübt. Diese werden über einen in die E-Mail eingebetteten Link zur Bestätigung ihrer Zugangsdaten aufgefordert. In der E-Mail wird auch angedroht, dass das betroffene PayPal-Konto bei Nichtbestätigung der Daten gesperrt würde. (BSI o. J.)

Abbildung 2 - Angebliche E-Mail von PayPal. Quelle: (BSI o. J.)

Eine ähnliche Vorgehensweise konnte die Wirtschaftskammer Österreich beobachten und warnt auf der eigenen Webseite vor dieser Phishing-Attacke. Hierbei versenden Angreifer betrügerische E-Mails im Namen der Wirtschaftskammer und fordern die Empfangenden zur Aktualisierung ihrer persönlichen oder Unternehmensdaten auf. In Abbildung 3 ist der Inhalt einer solchen E-Mail ersichtlich. (Wirtschaftskammer Österreich 2023)

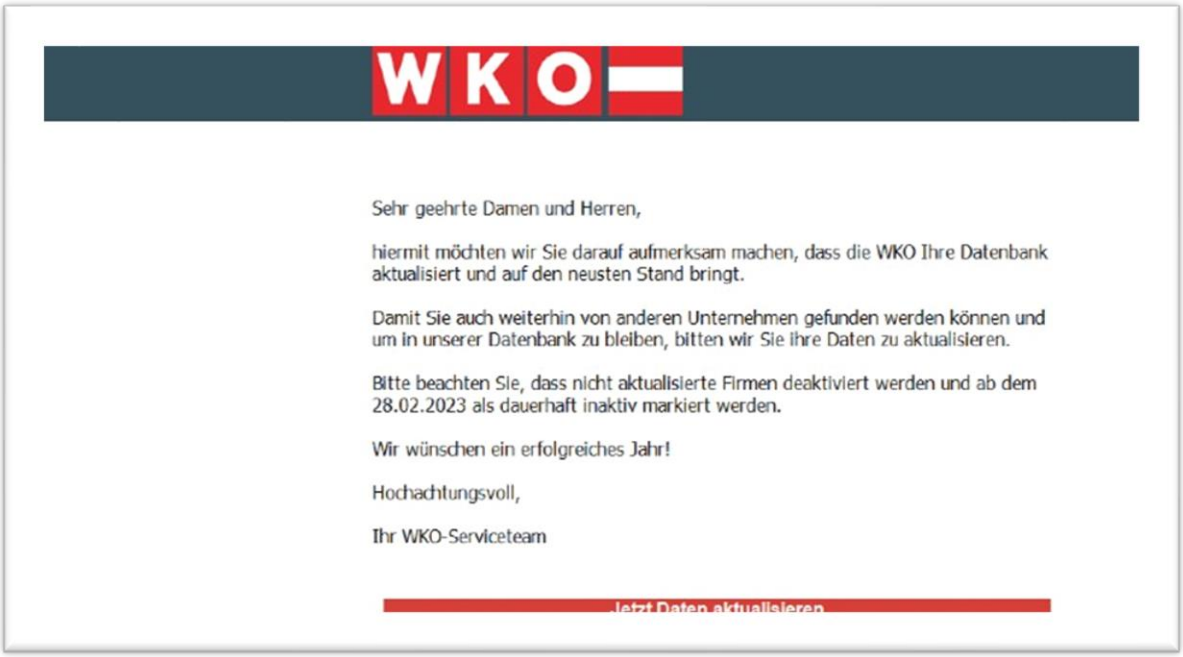

Abbildung 3 - Angebliche E-Mail der Wirtschaftskammer Österreich. Quelle: (Wirtschaftskammer Österreich 2023)

Eine weitere gängige Praxis beim Versand von Phishing-E-Mails ist das Vortäuschen von Gewinnen. Die in Abbildung 4 dargestellte Phishing-E-Mail suggeriert den Empfangenen, sie hätten einen Gutschein in der Höhe von 500 Euro für die deutsche Supermarktkette „EDEKA“ gewonnen. Wieder wird Druck ausgeübt, indem geschrieben wird, dass nur noch ein Tag zum Einlösen dieses Gutscheins Zeit ist und dass dieser ansonsten an einen anderen Teilnehmer des Gewinnspiels verlost wird. (Stahl 2023)

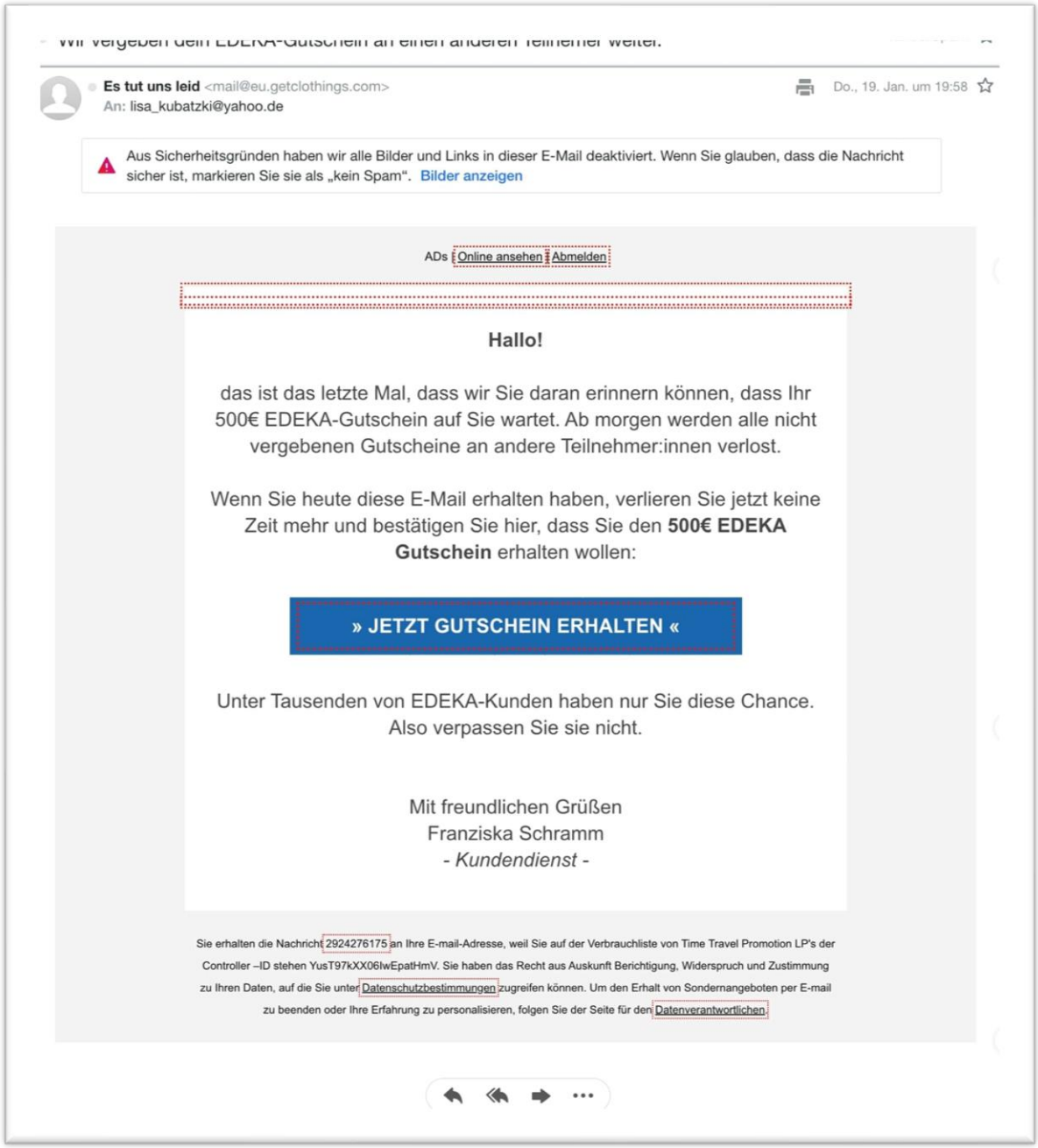

Abbildung 4 - Angeblicher Gewinnspiel-Gewinn. Quelle: (Stahl 2023)

Ein aktuelles Beispiel aus dem Unternehmen des Autors zeigt eine weitere Methode für Phishing-Attacken. Die E-Mail aus Abbildung 5 stammt von einem vermutlich gehackten E-Mail-Account eines legitimen Absenders aus derselben Branche, in der auch das Zielunternehmen tätig ist. Der Betreff suggeriert ein Angebot, die E-Mail selbst beinhaltet nur einen QR-Code mit dem Hinweis, diesem zu folgen. Sowohl der Absender als auch

die Signatur waren einwandfrei. Einzig die Tatsache, dass das Absenderunternehmen nicht bekannt war und die Vorgehensweise mit dem QR-Code sehr fragwürdig war, haben dazu geführt, dass die E-Mail an die interne IT zur Prüfung übermittelt wurde. Diese Überprüfung zeigte, dass sich hinter dem QR-Code eine Weiterleitung auf eine neuregistrierte .xyz-Toplevel-Domäne verbarg. Dort wurde eine Phishing-Seite präsentiert, die wie die mobile Anmeldung bei Microsoft 365 aussieht.

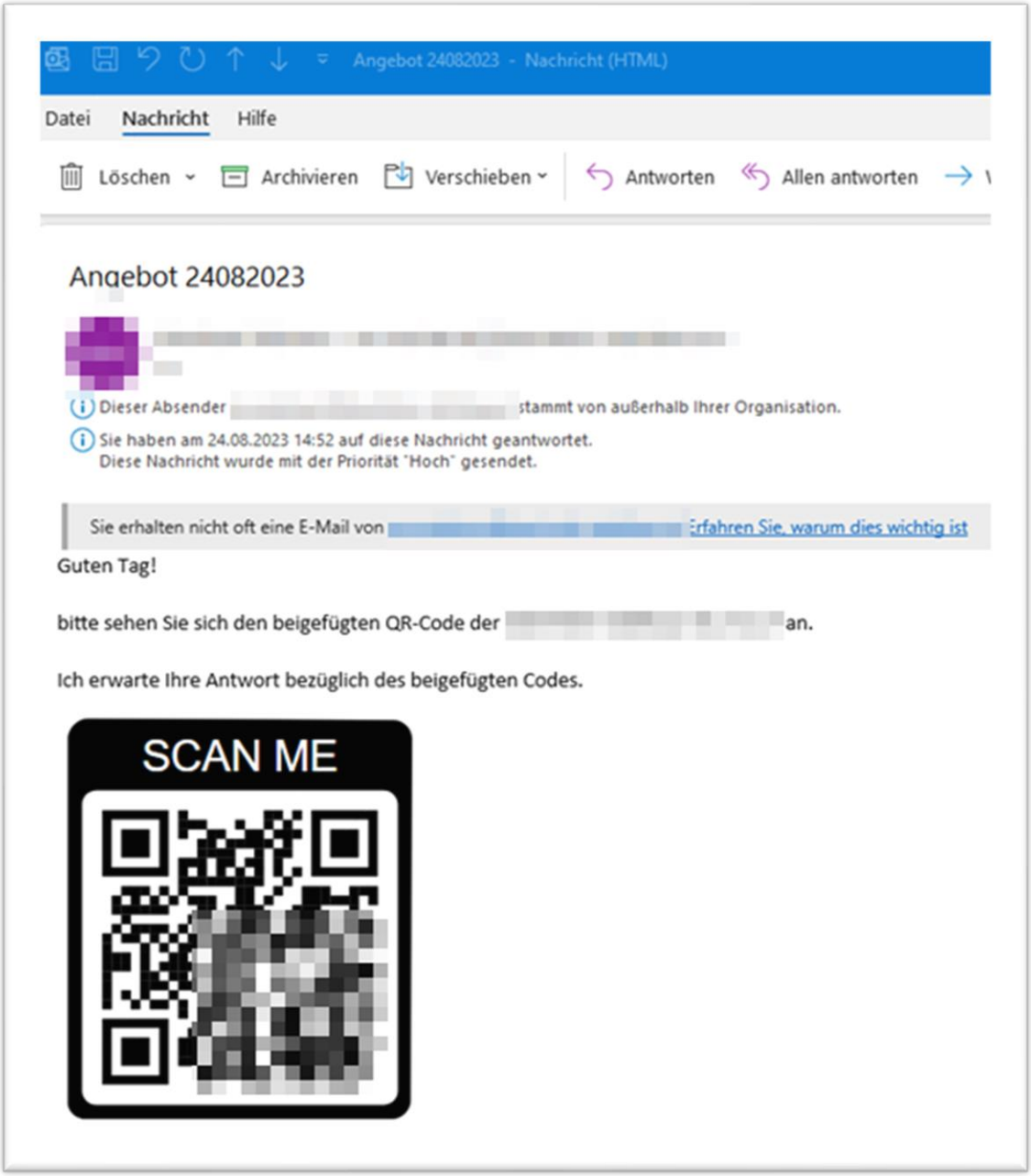

Abbildung 5 - Phishing-E-Mail. Quelle: Autor

2.6 Maßnahmen gegen Phishing

Der erste Schritt, um nicht zum Opfer von E-Mail-Phishing zu werden, ist es Phishing-Mails weitestgehend zu erkennen und zu löschen, bevor sie im Posteingang der Angegriffenen landen. Dazu gibt es eine Vielzahl von Anbietern für technische Möglichkeiten und Lösungen. Meist wird diese Funktionalität im Rahmen eines „E-Mail-Filters“ angeboten, der auch die Erkennung und Filterung von Spam-E-Mails erledigen soll. Auch wenn die möglichen Folgen einer zugestellten Phishing-E-Mail schwerwiegender sind als die einer Spam-E-Mail, vereint sie die Tatsachen, dass beide eine Art von ungewünschter Post sind und gleiche Merkmale aufweisen (Halgas, Agrafiotis, und Nurse 2020).

Eine zunehmend größere Rolle bei der Erkennung und der Abwehr von Spam- und Phishing-E-Mails spielen KI-Technologien. Durch maschinelles Lernen kann eine KI von bestehenden E-Mails lernen, den Inhalt und die Muster von unerwünschten oder gar schadhaften E-Mails von jenem Inhalt normaler E-Mails zu unterscheiden. Wurde eine Phishing-E-Mail also bereits als solche erkannt, kann diese Erkenntnis für die Prävention der weiteren Verteilung oder Zustellung dieses oder eines ähnlichen Inhaltes verwendet werden. (Mudiraj 2019)

Da es nicht reicht, sich lediglich auf die technischen Lösungen für diese Bedrohung zu beschränken, ist im Zusammenhang mit der Prävention gegen Phishing-Attacken immer wieder von „Awareness“ die Rede. Bewusstseinsbildung gegen Cyberangriffe spielt eine immer größer werdende Rolle in der Cyber-Security Verteidigung. Dies beginnt dabei, dass alle Anwender:innen die potenziellen Angriffsszenarien und auch deren mögliche Folgen kennen. Zum Bewusstsein zählt in diesem Kontext auch, dass erkannt wird, wer der wahre Absender einer E-Mail ist und wie festgestellt werden kann, ob die besuchte Webseite eine legitime ist.

Als Grundregel, um nicht Opfer von Phishing zu werden, nennt das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI): „Kein Kreditkarteninstitut und kein seriöser Anbieter fordert Sie per E-Mail auf, vertrauliche Zugangsdaten preiszugeben – auch nicht um der Sicherheit willen.“ (BSI o. J.). Weiters rät das BSI auf ihrer Infoseite gegen Phishing zu folgenden Verhaltensweisen:

- Die Adressleiste und der Verschlüsselungsstatus sollen im Browser kontrolliert werden, um so sicherzustellen, dass es sich um eine legitime Webseite handelt. Von der Eingabe von persönlichen Daten auf unverschlüsselten Webseiten wird abgeraten.
- Niemals sollte auf einen Link oder den Anhang in einer dubiosen oder verdächtigen E-Mail geklickt werden. Dies gilt auch für Downloadlinks. Es wird empfohlen, die Webseite des Anbieters direkt aufzurufen und von dort aus auf die Angebote zuzugreifen.

- Bestehen Zweifel an der Echtheit einer E-Mail oder Website, kann telefonisch Rücksprache mit der Stelle gehalten werden, an die die sensiblen Daten übermittelt werden sollen, um sich so Gewissheit zu verschaffen.
- Persönliche Daten sollen keinesfalls per E-Mail weitergegeben, sondern nur in der gewohnten Weise eingegeben werden. Als Beispiel wird hier die Bekanntgabe von Zahlungskarten-Details genannt, die eben nicht per E-Mail, sondern über die Online-Banking-Webseite geschehen soll.

Eine wirksame Methode, die die Folgen einer erfolgreichen Phishing-Attacke abschwächen kann, ist die Multi-Faktor-Authentifizierung (MFA). Diese verlangt für die erfolgreiche Durchführung eines Anmeldevorgangs zwei oder mehr verschiedene Authentifizierungsmethoden (CISA.gov 2022). Kommen nur zwei dieser Methoden zum Einsatz, kann auch von einer Zwei-Faktor-Authentifizierung (2FA) gesprochen werden. Die für MFA infrage kommenden Authentifizierungsmethoden werden in drei Kategorien eingeteilt (Stewart 2018):

Authentifizierungsmethode	**Beschreibung**
Etwas, das jemand weiß	Hierzu zählt alles, dass sich gemerkt, eingegeben und wiedergegeben werden kann. Beispiele: Kennwörter, PIN-Codes
Etwas, das jemand besitzt	Hierzu zählen physische Objekte, die zur Authentifizierung genutzt werden können. Beispiele: Schlüsselkarten, Smartphones, Smartcards, USB-Laufwerke und Token-Geräte.
Etwas, das jemand ist	Hierzu zählt jeder Teil des menschlichen Körpers, der für die Identifizierung genutzt werden kann. Beispiele: Fingerabdrücke, Handvenen, Gesichtserkennung, Iriserkennung und Stimmerkennung

Tabelle 1 – Authentifizierungsmethoden. Quelle: (Stewart 2018)

Der Einsatz von MFA reduziert die Gefahr, die von kompromittierten Zugangsdaten ausgeht. Kennwörter sind häufig das Ziel von Phishing-Attacken. Durch die Notwendigkeit von mehreren Authentifizierungsmethoden für die Anmeldung wird es Angreifenden schwer gemacht, etwaige erbeutete Daten dazu zu nutzen, weiteren Schaden anzurichten (CISA.gov 2022).

3. Grundlagen

Dieses Kapitel stellt die Basis für die Inhalte dieser Arbeit dar. Es ist die Grundlage für das technische und wissenschaftliche Verständnis des Themas und behandelt die theoretischen und konzeptionellen Ausgangspunkte.

3.1 Stand der Technik und Wissenschaft

Die Aussagekraft einer Phishing-Simulation hängt stark von ihrer Qualität ab. Das kritische Auseinandersetzen mit der aktuellen technischen und wissenschaftlichen Situation soll dafür Sorge tragen, dass die Simulation einem echten Angriff gleichkommt.

3.1.1 Planung einer Phishing-Simulation

Da in dieser Arbeit die Simulation einer realitätsnahen Phishing-Kampagne stattfinden soll, stellt die Planung einen wichtigen Part dar. Durch die Tatsache, dass der Autor im Zielunternehmen tätig ist, hat er einen Wissensvorsprung und verfügt teilweise über Informationen, die echten Angreifenden nicht ohne weiteres bekannt wären. Dies sind zum Beispiel Informationen über eingesetzte Software sowie bestehende Kunden und Lieferanten, die im Rahmen einer Phishing-Simulation imitiert werden könnten. Dabei handelt es sich jedoch um Informationen, die ein aufmerksamer und motivierter Angreifer erlangen könnte. Ungeachtet dessen gibt es einige grundlegende Dinge, die bei der Planung beachtet werden sollten.

Ein erster wichtiger Faktor für den Erfolg einer Phishing-Attacke ist der Betreff der E-Mail. SoSafe, ein Anbieter von Cyber Security Awareness Trainings, veröffentlicht jährlich die Trends, die die von ihnen durchgeführten Phishing-Simulationen aufzeigen. Darunter sind auch die Top-5 Phishing Betreffzeilen für das jeweilige Jahr (SoSafe 2023). Zu den Betreffzeilen gibt SoSafe auch an, welche Manipulationstechniken sie für den jeweiligen Betreff eingesetzt haben. Nachfolgend werden diese Daten zusammengefasst in Tabelle 1 dargestellt.

Betreffzeile	**Manipulationstechnik**
Auto beschädigt	Druck/Neugier
Teams-Einladung	Neugier
Fehler in der Gehaltsabrechnung	Druck/Neugier
Ihr Office Passwort läuft heute ab	Druck
Teams verpasste Chatnachricht	Druck/Neugier

Tabelle 2 - Top-5 Phishing Betreffzeilen und die eingesetzten Manipulationstechniken. Quelle: (SoSafe 2023)

Dies zeigt, dass es erfolgsversprechend ist, Druck auf die Empfangenden auszuüben oder deren Neugierde zu wecken. Abbildung 5 veranschaulicht, wie sich die Klickraten nach emotionalen Manipulationstechniken, vom Jahr 2022 zum Jahr 2023, entwickelt haben. Die Grafik zeigt für das Jahr 2023 ein sehr ausgewogenes Bild, bei dem keine Kategorie stark nach obenhin ausreißt. Lediglich der „finanzielle Anreiz“ scheint deutlich unterdurchschnittlich gut zu funktionieren.

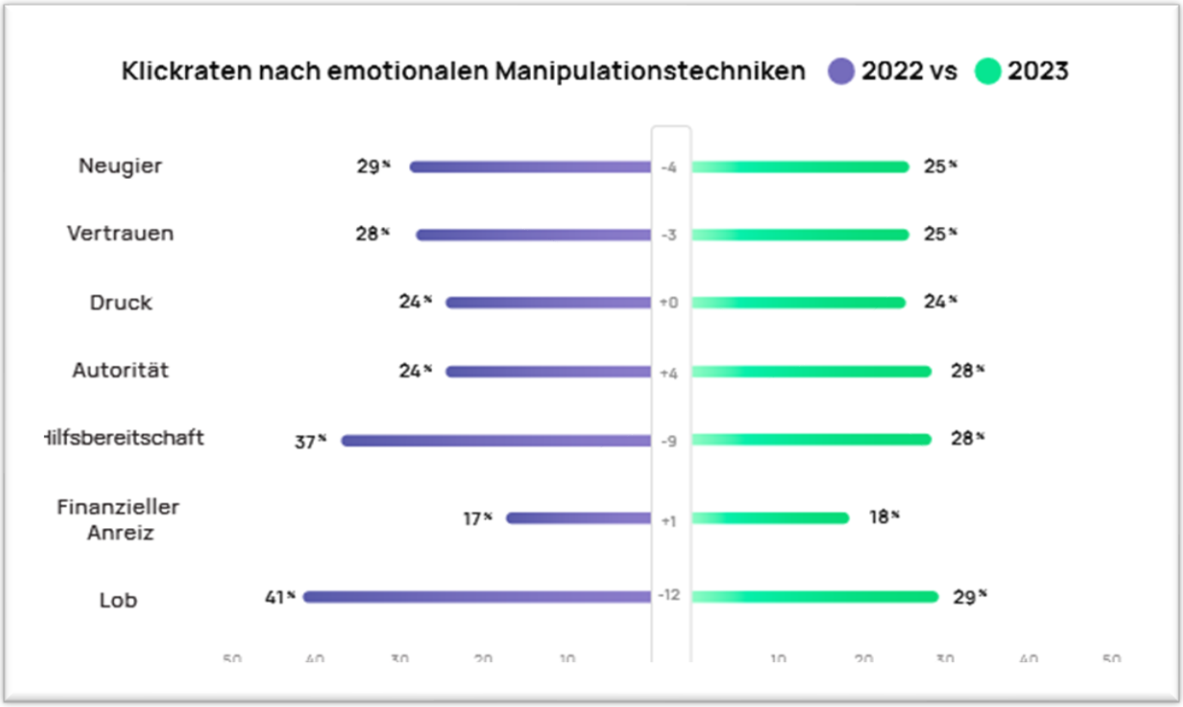

Abbildung 6 - Klickraten nach emotionalen Manipulationstechniken. Quelle: (SoSafe 2023)

Auch KnowBe4, ein weiterer Anbieter für Cybersecurity-Awareness-Trainings, listet in seinen „Top Phishing Email Subjects Globally“ für das erste Quartal 2023 (Sjouwerman 2023) vergleichbare Betreffzeilen. Diese zielen vorrangig auf die Manipulationstechniken Neugier und Druck ab. Da dieser Anbieter mehr US-amerikanische Kunden hat, sind darunter auch Einträge, die im Rahmen des Zielunternehmens dieser Arbeit wenig bis keine Relevanz haben.

Neben der Wahl der passenden Betreffzeile sind auch die Inhalte der Phishing-E-Mail und der Phishing-Webseite von entscheidender Bedeutung. Um herauszufinden, worauf bei der Phishing-E-Mail und Webseite zu achten ist, lohnt sich ein Blick auf Empfehlungen, woran Phishing-Inhalte erkannt werden können. So nennt Cofense die zehn häufigsten Zeichen einer Phishing-E-Mail (Cofense 2020) und listet folgende Merkmale:

- Ein ungewohnter Tonfall oder eine ungewohnte Begrüßung
- Grammatikalische und Rechtschreibfehler
- Inkonsistente E-Mail-Adressen, Links und Domänen
- Drohungen und vermittelter Druck
- Verdächtige E-Mail-Anhänge
- Anfragen von Personen, die nicht in deren üblichen Zuständigkeitsbereich passen
- Kurze Nachrichten ohne Kontext auf den Inhalt
- Antworten auf Konversationen, die der Empfänger nicht gestartet hat
- Nachfrage nach Zugangsdaten, Zahlungsdaten oder andere persönliche Details

Diese Merkmale lassen sich bei der Erstellung der Phishing-Inhalte im Rahmen dieser Arbeit vermutlich nicht gänzlich vermeiden, es wird jedoch versucht, weitestgehend darauf Rücksicht zu nehmen.

Auch der Zeitpunkt für den Versand von Phishing-E-Mails spielt eine Rolle für deren Erfolg. Laut (Badarau 2015), kommt es an den Wochentagen Freitag (38,5 Prozent) und Montag (30 Prozent) zum größten Aufkommen an Phishing-E-Mails. Ein Grund für den Versand am Freitag ist, dass Angreifende in ihren schadhaften E-Mails häufig Links verschicken, die zum Zeitpunkt des Versands noch nicht schadhaft sind. Erst wenn diese E-Mails die Sicherheitsmechanismen, wie beispielsweise einen E-Mail-Filter, passiert haben und in der Mailbox der Angegriffenen gelandet sind, werden die darin enthaltenen Links schadhaft gemacht. Dieser Vorgang funktioniert besser, wenn dafür mehrere Stunden bis Tage zur Verfügung stehen (Sjouwerman 2022). Für den Versand von Phishing-E-Mails am Montag spricht die Aussage von AtlasVPN. Dort wird berichtet, dass an Montagen 27 Prozent der Phishing-Angriffe auf höhere Angestellte durchgeführt werden. Begründet wird dies dadurch, dass Montage für viele die arbeitsreichsten und stressigsten Tage der Woche sind. Angreifende wollen sich das zu Nutze machen, indem sie darauf hoffen, dass ihre potenziellen Opfer unter diesen Umständen weniger sorgsam und aufmerksam agieren. (atlasVPN 2023).

Neben der Wahl des Zeitpunkts, der Betreffzeile und des Inhaltes, gilt es noch die konkrete Angriffsmethodik zu definieren. Es gibt eine Vielzahl an Möglichkeiten, Phishing-E-Mails zuzustellen und die Phishing-Webseiten darzustellen. In jedem Fall wird eine Absenderadresse und eine Webseiten-URL gebraucht, die die Empfangenden im Glauben lässt, legitimen Inhalt zu sehen. Eine häufig verwendete Methode für die Manipulation der potenziellen Phishing-Opfer ist das „Typosquatting“. Hierbei wird die zu imitierende Domäne geringfügig verändert, so dass sie auf den ersten Blick nicht vom Original zu unterscheiden ist. Angreifer finden und registrieren sich diese Domänen und können unter dessen Namen E-Mails verschicken und Webseiten bereitstellen

(Microsoft o. J.). Ein Beispiel für „Typosquatting“ wäre die legitime Domäne „musterfirma.at“, deren Typosquatting-Pendant „musterflrma.at“ lauten könnte.

Eine weitere Methode zur Irreführung ist das „Domainsquatting“. Dies hat seinen Namen und den Ursprung in der betrügerischen Registrierung von Domänen, mit dem Ziel diese gewinnbringend weiterzuverkaufen oder für andere gewinnorientierte Zwecke, wie das Darstellen von Werbung, zu verwenden (Hogue 2017). Heutzutage wird Domainsquatting aber auch häufig im Zusammenhang mit Phishing-Angriffen beobachtet. Die Angreifenden registrieren sich dabei Domänen, die dem imitierten Unternehmen zugeordnet sein könnten, dies jedoch nicht sind (Brad 2021). Angreifende könnten sich die Domäne „musterfirma-seewalchen.at“ registrieren, um den Eindruck zu erwecken, zum Unternehmen hinter „musterfirma.at“ zu gehören. Eine besondere Form des Domainsquatting ist das „Toplevel-Domainsquatting“. Hierbei werden die Domänen vom imitierten Unternehmen mit einer anderen Toplevel-Domäne registriert (Team 2021). Versuchten sich Angreifende beispielsweise als „musterfirma.at“ auszugeben, könnten sie sich die Domäne „musterfirma.com“ registrieren und für ihre Zwecke verwenden.

Die britische Universität Bath veröffentlichte einen Leitfaden, in dem auf den Entwurf einer Phishing-Simulation eingegangen wird (Crown 2017). Darin wird die Wichtigkeit von Phishing-Simulationen in Unternehmen deutlich gemacht und das Aufzeigen potenzieller Schwachstellen bei den Mitarbeitenden als einer der größten Vorteile genannt. Es sei auch wichtig, eine solche Simulation entsprechend zu planen. So wird sichergestellt, dass maximal von den Ergebnissen profitiert werden kann und diese auch über lange Zeit hinweg miteinander verglichen werden können.

Das erste Kapitel dieses Leitfadens rät dazu, die zu beantwortende Schlüsselfrage zu identifizieren. Dies setzt voraus, dass definiert wurde welche Rückschlüsse mit der Simulation gewonnen werden sollen. Dafür werden beispielhaft drei mögliche Schlüsselfragen genannt:

“Are some groups of employees more susceptible to phishing emails than others?”

Diese Frage zielt darauf ab, herauszufinden ob gewisse Personengruppen anfälliger für Phishing-Attacken sind als andere. Beantwortet werden kann diese Frage, indem die Empfangenden der Simulation in Gruppen aufteilt werden. Diese Gruppen könnten sich aufgrund der Anstellungsdauer, der Rollen, dem Freigabelevel oder dem Standort ergeben.

„Has employee susceptibility to phishing emails changed over time?”

Diese Fragestellung soll beantworten, wie sich der Erfolg der Phishing-Simulation über den Lauf der Zeit verändert hat. Dazu braucht es zumindest zwei vergleichbare Simulationen.

„Are employees more susceptible to certain types of threat?“

Damit soll aufgezeigt werden, ob es Phishing-Inhalte gibt, auf die Mitarbeitende häufiger reagieren. Dies kann sich auf mehrere Faktoren beziehen. So kann zum einen untersucht werden, ob vermehrt auf interne oder externe Phishing-E-Mails reagiert wird. Auch die Wahrscheinlichkeit des Erfolgs von verschiedenen Manipulationstechniken, wie Druck oder Neugierde, kann erfasst werden. Daraus lassen sich dann zu priorisierende Trainings-Inhalte und bewusstseinsbildende Maßnahmen ableiten.

Im zweiten Kapitel dieses Leitfadens geht es um den Entwurf der Phishing-Simulation. Dies setzt die vorangegangene Identifikation der zu beantwortenden Frage voraus und baut auf dieser auf. Daraus leiten sich Faktoren wie die Anzahl der verwendeten Phishing-E-Mails, wie breit die Inhalte gestreut werden sollten und wie groß die Stichprobengröße sein soll, ab.

Abschließend wird noch dazu geraten, nicht zu viele Fragen auf einmal beantworten zu wollen. Für die Beantwortung einer Frage braucht es eine möglichst hohe Stichprobengröße, die einem nicht unbegrenzt für Phishing-Simulationen zur Verfügung steht.

Welche Inhalte in Phishing-E-Mails attraktiver für die Empfangenden war, untersuchten (Siadati u. a. 2017) in einer Studie. Die Ergebnisse der Studie beziehen sich auf die Ergebnisse der Phishing-Simulation in einem mittelständischen US-amerikanischen Unternehmen. Neben der Erkenntnis, dass überzeugender Inhalt den Erfolg einer Phishing-E-Mail stark positiv beeinflusst, nannten sie auch die fünf effektivsten Themen. Sie empfehlen, dem Design der verwendeten Phishing-E-Mails große Bedeutung zukommen zu lassen, da es die Effektivität und die Effizienz der Simulation positiv beeinflusst. Wie in Abbildung 7 ersichtlich, waren die E-Mails mit den Themen Order, Complaints, Fax 1, Shipping und Fax 2 die, die am häufigsten dazu geführt haben, dass Empfangende den Links in der E-Mail gefolgt sind.

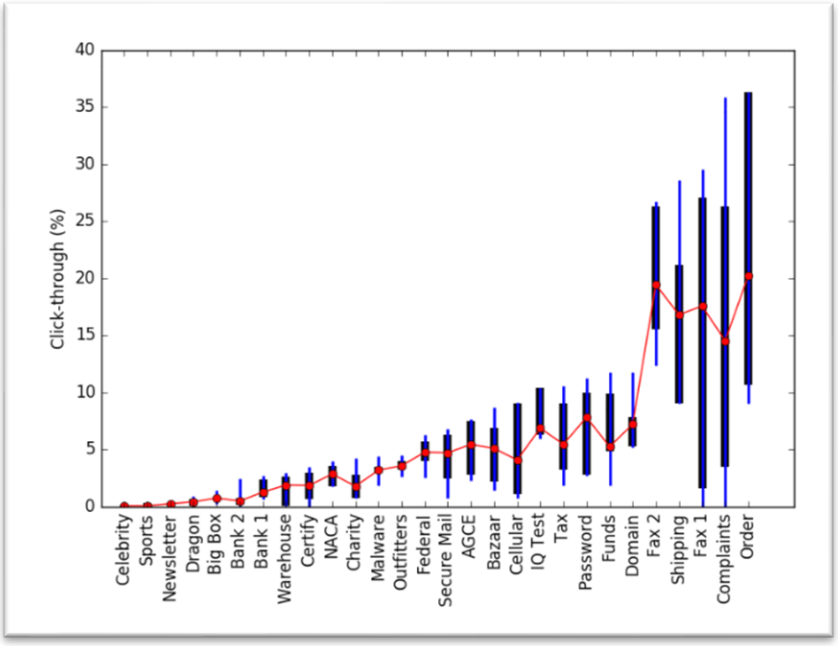

Abbildung 7 - Klickrate von 28 Phishing-E-Mails. Quelle: (Siadati u. a. 2017)

3.1.2 Durchführung einer Phishing-Simulation

Das Thema „Phishing-Simulationen“ hat heutzutage eine große Bedeutung, vor allem für größere Unternehmen haben sie häufig einen großen Stellenwert in der Cyber-Abwehrkette. Da die Nachfrage nach solchen Services dementsprechend groß ist, gibt es auch eine Vielzahl an Unternehmen, die diese Dienstleistung anbieten (RSA 2023). Die Phishing-Simulation im Rahmen dieser Arbeit ist selbstständig zu planen, durchzuführen und auszuwerten, daher kommt es nicht in Frage, dies über einen Dienstleister abzuwickeln.

Die Suche nach Phishing-Frameworks liefert einige Ergebnisse. Diese sind in zwei grundlegende Kategorien zu unterteilen. Ein großer Teil der gefundenen Frameworks ist darauf ausgerichtet, tatsächliche Angriffe durchzuführen. Dies macht sich dadurch bemerkbar, dass sie sehr ergebnisorientiert sind und der Diebstahl von Zugangsdaten und anderen Identitätsmerkmalen im Vordergrund steht.

Ein häufig referenzierter Vertreter dieser Kategorie ist „Zphisher“. Dabei handelt es sich um ein Open-Source Phishing-Framework, das in der Programmiersprache Python geschrieben wurde. Es arbeitet sehr ressourcenschonend und wird lediglich über die Kommandozeile bedient. Das Team hinter dem Werkzeug liefert Vorlagen für eine Vielzahl an Phishing-Seiten mit. Diese beschränken sich auf die Imitation von häufig besuchten Webseiten, wie soziale Netzwerke und Streaming Anbieter. Es besteht keine Möglichkeit, eigene Inhalte zu verwenden. Nachdem die Auswahl der Phishing-Webseite

getroffen wurde, gibt Zphisher einen Link aus, der an die potenziellen Opfer geschickt werden kann. Wie in Abbildung 6 ersichtlich, wird in der Kommandozeile angezeigt, ob jemand den Link aufgerufen hat. Zusätzlich werden die Zugangsdaten, die eingegeben wurden, angezeigt. (mohdshariq 2021).

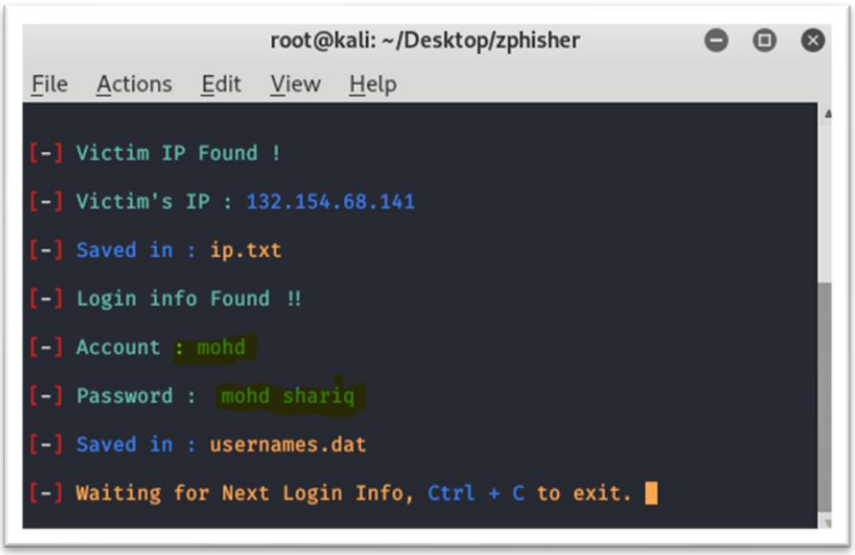

Abbildung 8 - Erfolgreiche Attacke mit Zphisher. Quelle: (mohdshariq 2021)

Die zweite Kategorie von Phishing-Frameworks besteht aus jenen, die sich tatsächlich auf die Durchführung von Phishing-Simulationen spezialisieren. Der Diebstahl von Zugangsdaten steht dort nicht im Fokus und das Erfassen dieser kann sogar deaktiviert werden. Dafür bieten diese Werkzeuge weitreichende Möglichkeiten, die Inhalte und den Ablauf von Phishing-Kampagnen zu planen und zur detaillierteren Auswertung der Ergebnisse. Zwei sehr populäre Vertreter dieser Kategorie sind die Produkte „Gophish“ und „SniperPhish“.

„Gophish“ ist ein für Phishing-Simulationen, in der Programmiersprache „Go“ entwickeltes, Open-Source Phishing-Framework. Es handelt sich dabei um eine Webanwendung, die auf dem lokalen Computer ausgeführt wird. Vom zentralen Dashboard aus können Phishing-E-Mail-Kampagnen erstellt werden. Dabei arbeitet das Programm mit „Sending-Profiles“ in denen der Mail-Server, die Absenderadresse und den Absendernamen definiert werden. Zudem wird ein „Email Template“ und eine „Landing-Page“ benötigt. Diese stellen den Inhalt der Phishing-E-Mail, beziehungsweise den Inhalt der Phishing-Website dar. Ein großer Vorteil ist die Möglichkeit, E-Mail- und Webseiten-Inhalte von bestehenden, legitimen Quellen importieren und anpassen zu können. Das macht die Erstellung dieser Inhalte sehr einfach, da keinerlei Programmierkenntnisse vorhanden sein müssen, um täuschend echte Phishing-Inhalte zu erstellen. Die Empfänger:innen lassen sich mittels eines CSV-Imports einfach in das

Portal übertragen und dort verwalten. Auch eine Aufteilung aller Empfangenen in einzelne Gruppen ist abbildbar. Bei der Erstellung einer Kampagne werden dann die zuvor erstellten Inhalte und Empfänger ausgewählt und der Zeitraum angegeben, in dem die Phishing-E-Mails zugestellt werden sollen. Die Definition von einem Zeitraum sorgt dafür, dass die E-Mails nicht alle zeitgleich, sondern gleichmäßig innerhalb eines bestimmten Zeitrahmens versandt werden. (Kladochnyi 2023).

Auch das zweite Produkt „SniperPhish“ ist ein auf Phishing-Simulationen ausgerichtetes Open-Source Phishing-Framework. Es handelt sich dabei um eine Webanwendung, die auf einem selbst bereitgestellten Webserver betrieben wird. Zentrale Komponente ist auch hier wieder ein Dashboard, von dem aus sehr detailliert konfigurierte Phishing-E-Mail-Kampagnen erstellt werden können. „SniperPhish“ arbeitet mit sogenannten „Web-Tracking-Codes“ und „E-Mail-Tracking Codes“. Diese verwendet es um nachzuvollziehen, welche Empfänger:innen eine E-Mail öffnen bzw. den darin enthaltenen Link angeklickt haben. Die Empfangenden können auch hier in Gruppen aufgeteilt werden, um sicherzustellen, dass nicht alle gleichzeitig dieselben Phishing-E-Mails erhalten (Zorz 2021).

3.1.3 Auswertung einer Phishing-Simulation

Zur Beantwortung der Forschungsfrage dieser Arbeit ist es nötig zu definieren, ab wann ein simulierter Phishing-Angriff als erfolgreich gewertet werden kann. Bei der Durchführung der Phishing-Simulation gibt es mehrere Werte, die dafür herangezogen werden können. In einem Blogbeitrag nennt unsecure.io (Lok 2022) vier Metriken für die Auswertung einer Phishing-Simulation. Der erste messbare Wert wäre das bloße Öffnen der simulierten Phishing-E-Mail. Festgestellt wird dies über das Einbinden eines Bildes oder einer anderen Ressource, die beim Öffnen der E-Mail von einer externen Quelle geladen wird. Da es beim Zugriff auf diese externen Ressourcen starke Unterschiede zwischen den verschiedenen E-Mail-Clients gibt, ist dies keine verlässliche Metrik. Auch ist das Öffnen einer Phishing-E-Mail noch nicht aussagekräftig genug, um den Erfolg daran zu messen.

Der zweite Schritt wäre das Anklicken des in der simulierten Phishing-E-Mail enthaltenen Links. Diese Metrik wird über die Besuchsstatistiken der in der E-Mail verlinkten Phishing-Webseite gemessen und ist sehr genau. Die auf Simulationen spezialisierten Phishing-Frameworks fügen in jede versandte E-Mail einen einzigartigen Link ein. Dieser ist somit immer einem Empfangenden zugewiesen und zeigt, wer den Link geöffnet und die Phishing-Webseite besucht hat.

Als dritter Schritt in dieser Phishing-Kette wird das Eingeben von Daten gewertet. Gibt einer der Angegriffenen persönliche Daten auf der Phishing-Webseite preis und übermittelt sie so den Angreifenden, hat dieser sein Ziel erreicht. Dies stellt das größte

Problem dar und würde zeigen, dass ein Angegriffener weder den Inhalt der Phishing-E-Mail noch die Phishing-Webseite als schadhaft erkannt hat.

Eine weitere Kennzahl ist die Anzahl der Meldungen einer simulierten Phishing-E-Mail. Als gemeldet gilt eine E-Mail, wenn Angegriffene den Phishing-Versuch als solchen erkennen und ihn an eine geeignete Stelle melden.

Aus diesen vier Werten leitet (Hoxhunt 2022) sich drei Möglichkeiten für die Bewertung des Erfolges einer Phishing-Simulation ab:

Der erste Indikator ist die „Fehlerrate pro Kampagne“. Sie gibt an, wie häufig die Angegriffenen unsichere Aktionen, im Zusammenhang mit der verschicken simulierten Phishing-E-Mail pro Kampagne, durchgeführt haben. Dazu zählen sowohl das Anklicken des Links, der sie auf die Phishing-Webseite bringt, als auch die Bekanntgabe von Daten.

Eine weitere Möglichkeit zur Bewertung des Erfolges einer Phishing-Simulation ist die „Erfolgsquote“. Als Gegenteil der Fehlerrate misst sie die Anzahl der Angegriffenen, die nicht auf die Phishing-E-Mail reagiert haben.

Die dritte Methode, die herangezogen werden kann, ist die Meldequote. Diese wird von der Anzahl der Meldung der simulierten Phishing-E-Mails gesteuert. Meldet ein Angegriffener den Phishing-Angriff, beispielsweise durch das Weiterleiten der E-Mail an ein gesondertes Postfach, zählt dieser Angriff als „gemeldet“. Die auf Simulationen ausgerichteten Phishing-Frameworks bieten diese Funktionalität automatisiert an. Dies benötigt aber einen definierten Prozess im Unternehmen und ein eigenes Postfach für E-Mails, die die Empfangenden melden sollen. Der Prozess würde vorsehen, dass die Empfangenen alle verdächtigen E-Mails zur internen Prüfung an ein dediziertes Postfach weiterleiten. Die Software zur Phishing-Simulation überwacht dieses Postfach und erkennt den Eingang von an Angegriffene versandte Phishing-E-Mails. Nach registriertem Eingang einer Phishing-E-Mail, wird der Phishing-Versuch automatisch auf „gemeldet“ gesetzt. Alternativ besteht die Möglichkeit, den Status „gemeldet“ pro versandter Phishing-E-Mail manuell zu vergeben.

3.2 Vorstellung des Unternehmens

Die im Rahmen dieser Arbeit durchgeführten Maßnahmen sollen vordergründig für das Unternehmen des Autors gültig sein. Da es bei der Vielzahl an produzierenden KMU jedoch sicherlich einige Parallelen gibt, wird diese Arbeit zumindest stellenweise auch Gültigkeit für andere Unternehmen haben. Unterschiede ergeben sich sicher bei der Wahl der Phishing-E-Mail-Inhalte. Auch wird es Unterschiede beim Zugang des Unternehmens zur Digitalisierung und dem Stand der IT-Awareness bei den MitarbeiterInnen geben.

Das für diese Arbeit herangezogene oberösterreichische Unternehmen ist seit den 1950er-Jahren am Markt. Seit der Unternehmensgründung hat sich der Geschäftsbereich verändert, dieser ist nun aber seit vielen Jahren stabil. Beim Referenzunternehmen handelt es sich um ein inhaberinnengeführtes Unternehmen im Bereich der Metallverarbeitung. Als Lohnfertiger für die Industrie wird eine Vielzahl an metallverarbeitenden Techniken und Vorgängen angeboten. Die Erfahrung und das breite Angebot an Dienstleistungen macht das Unternehmen zu einem wichtigen und meist langjährigen Partner von Industriebetrieben und Kraftfahrzeugherstellern. Als zentrales Mitglied der Supply-Chain der Kunden muss dementsprechend auch großer Wert auf die Qualität der internen Prozesse gelegt und das Ausfallrisiko minimiert werden.

Das Unternehmen hat nur einen Standort. An diesem findet sowohl die Produktion als auch die Verwaltung statt. Somit besteht die IT-Infrastruktur aus einer Mischung von Standard-IT-Komponenten wie Servern, Computern, Druckern und Peripherie, als auch verschiedenen Hardware-Komponenten im Maschinenpark. Diese teilen sich eine gemeinsame Netzwerk-Infrastruktur. Von den knapp unter einhundert Mitarbeitenden (Stand: Juli 2023) verfügt etwa die Hälfte über einen Computer-Zugang und einen E-Mail-Account. Eine gewisse Homogenität ist bei den Standard-IT-Komponenten einfacher zu erreichen als bei den branchenspezifischen Geräten und Anwendungen. Da Maschinen für die Metallverarbeitung häufig eine hohe Lebenszeit haben, sind durchaus ältere Technologien anzufinden. Diese stellen aus IT-Sicherheitssicht eine besondere Herausforderung dar.

Das ringförmig aufgebaute Netzwerk des Referenzunternehmens ist in verschiedene Subnetze unterteilt. Diese Unterteilung erlaubt es, die Kommunikation zwischen den einzelnen Subnetzen zu steuern und zu limitieren und ist eine Grundvoraussetzung für den sicheren Betrieb. Die Idee hinter der Trennung war, dass jedes Gerät so weit wie möglich eingeschränkt wird. Für jede so identifizierte Klasse wurde ein eigenes Netzwerksegment erstellt. Die Trennung und das Routing zwischen den einzelnen Netzwerksegmenten übernimmt ein Firewall-Cluster, bestehend aus zwei Firewalls.

Konzeptionell gibt es für jeden schützenswerten Bereich ein eigenes Subnetz. So werden Clients, Server, Drucker, Produktionsmaschinen verschiedener Hersteller, das Telefonsystem und das ERP-System jeweils voneinander getrennt.

Im Referenzunternehmen ist ein Cluster aus zwei physischen Servern mit einem geteilten Datenspeicher im Einsatz. Die gesamte Server-Infrastruktur basiert auf einer virtualisierten Umgebung. Diese ermöglicht es, die vorhandene Hardware und den vorhandenen Raum effizient zu nutzen, da nicht für jede Serverinstanz eine eigene Hardware angeschafft und betrieben werden muss. Die virtuellen Server teilen sich die physischen Ressourcen der Hypervisoren und sämtliche Daten befinden sich auf dem zentralen Datenspeicher. Die physischen Systeme sind so geplant und dimensioniert,

dass der Betrieb der Server-Infrastruktur auch beim Ausfall von einem der zwei Knoten weiter betrieben werden kann.

Seit 2021 gibt es im Unternehmen eine Plattform für IT-Sicherheit. Auf dieser selbst betriebenen und gepflegten Webanwendung werden regelmäßig Inhalte zum Thema IT-Sicherheit veröffentlicht. Die Mitarbeiter:innen arbeiten diese selbstständig durch und bestätigen ihr Wissen in einer abschließenden Wissensüberprüfung. Die Inhalte sind so gestaltet, dass sie in etwa 15 Minuten bearbeitet werden können. Die abschließende Wissensüberprüfung umfasst drei bis sechs Fragen aus dem Inhalt des Lernpakets. Die Plattform selbst ist eine Seite in Microsoft SharePoint 365, die Wissensüberprüfungen werden über ein Quiz in Microsoft Forms durchgeführt. Die Ergebnisse dieser Wissensüberprüfung werden in die drei Kategorien „OK“ (teilgenommen und ausreichend viele Punkte erreicht), „Nicht OK“ (teilgenommen aber nicht ausreichend viele Punkte erreicht) und „keine Antwort“ (nicht teilgenommen) unterteilt. Aktuell gibt es fünf Module, welche folgende Themen beinhalten:

- „E-Mail-Sicherheit – Unsichere Absender erkennen“ – Hier wird vermittelt, worauf bei E-Mail-Adressen zu achten ist.
- „E-Mail-Sicherheit – Links und Anhänge prüfen“ – Hier wird erklärt, wie Links und Dateianhänge überprüft werden können und so sichergestellt werden kann, dass diese nicht schadhaft sind.
- „Kennwortsicherheit“ – Dieses Modul erklärt, worauf bei der Wahl eines Kennworts zu achten ist.
- „Sicherer Umgang mit Daten und Informationen“ – Ein Überblick über das Thema Daten, Informationen, Datenschutz und die Speicherung sowie die Weitergabe von Daten.
- „Angriffsmethoden – eine Übersicht“ – In diesem Modul wird gezeigt, welche Angriffsmethoden im Kontext der Cyber-Security möglich sind, wie diese funktionieren und wie sie erkannt und verhindert werden können.

Die Auswertung dieser Wissensüberprüfungen zeigt sowohl bei der Teilnahme als auch bei den Ergebnissen ein überwiegend positives Ergebnis. Abbildung 9 zeigt die Anzahl der Teilnehmenden pro Modul, sowie die Anzahl der Ergebnisse in den jeweiligen Kategorien „OK“, „Nicht OK“ und „Keine Antwort“.

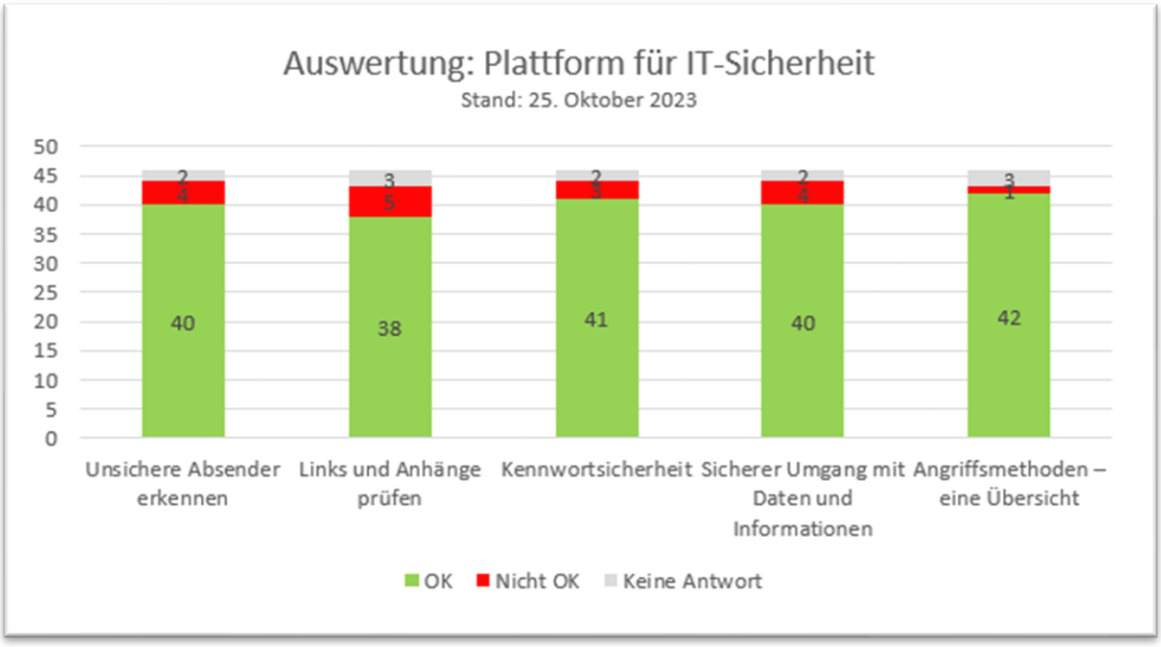

Abbildung 9 - Auswertung Plattform für IT-Sicherheit. Quelle: Autor

Neben diesen Lernpaketen gibt es auch laufend Informationen zu aktuellen Cyber-Risiken wie Phishing-Versuchen sowie zu anderen IT-Themen. Dies beinhaltet beispielsweise Infos per E-Mail bezüglich des „Data Privacy Day“ am 28. Januar, des „World Backup Day“ am 31. März oder auch des „Computer Security Day“ am 30. November, sowie regelmäßige Veröffentlichungen von Beiträgen in der Unternehmenszeitschrift.

3.3 Konzeptioneller Vorgehens- und Lösungsansatz

Um die Forschungsfrage zu beantworten, werden die zuvor gewonnen Erkenntnisse und Informationen zu den Themen Planung, Durchführung und Auswertung einer Phishing-Simulation zum Einsatz kommen.

In der Planungsphase werden die Inhalte für die simulierten Phishing-E-Mails gesammelt, sowie die einzelnen Kampagnen geplant. Dazu werden, soweit möglich, bestehende und legitime Inhalte verwendet und für die Zwecke der Arbeit aufbereitet. So wird sichergestellt, dass die Qualität der Inhalte der Phishing-Mails und Phishing-Webseiten möglichst glaubwürdig ist. Tabelle 3 gibt eine Übersicht über die umzusetzenden Inhalte. Sie beinhaltet den Betreff der Phishing-E-Mail und deren Inhalt. Zudem zeigt sie den Absender, inklusive der verwendeten technischen Methode, sowie die Empfängergruppen und den Zeitpunkt der Zustellung der jeweiligen Kampagnen.

Dabei kommen die zuvor als effektiv identifizierten Inhalte, Manipulationstechniken und technischen Methoden zum Einsatz.

Betreff: Auto beschädigt			
Inhalt	**Absender**	**Empfänger**	**Zeitpunkt**
Informationen über einen angeblichen Parkschaden am Unternehmensparkplatz mit einem Link zu angeblichen Bildern und weiteren Informationen.	Ein zentrales Unternehmenspostfach, mit einem Domain-Squatting-Absender	Alle Mitarbeitenden, simultan	Freitag, Vormittag
Betreff: Teams-Einladung			
Inhalt	**Absender**	**Empfänger**	**Zeitpunkt**
Einladung in ein Microsoft Teams-Team mit einem der Titel „Führungskräfte“, „Intern“ und „Weihnachtsfeier“ mit einem Link zum Beitreten.	Eine gefälschte Adresse von Microsoft mit einem Typo-Squatting-Absender	Alle Mitarbeitenden, in drei Gruppen aufgeteilt. Führungskräfte, neuere Mitarbeiter:innen und „Weihnachtsfeier“	Montag, Früh
Betreff: Fehler in der Gehalts-Abrechnung			
Inhalt	**Absender**	**Empfänger**	**Zeitpunkt**
Information über einen angeblichen Fehler in der Gehaltsabrechnung mit einem Link zum aktuellen Lohnzettel.	E-Mail-Adresse einer imaginären Steuerberatungskanzlei	Alle, in zwei Gruppen aufgeteilt (Physisch nahe Personen)	Freitag, Früh

Tabelle 3 - Geplante Kampagnen für die Phishing-Simulation. Quelle: Autor

In der Durchführungsphase werden das Phishing-Framework installiert, sowie die Kampagnen erstellt und auch durchgeführt. Mit „Gophish“ (https://getgophish.com) und „Sniperphish“ (https://sniperphish.com) konnten zwei Phishing-Frameworks, die sich für die Simulation von Attacken eignen, identifiziert werden. Beide bieten einen vergleichbaren und ebenbürtigen Funktionsumfang. Im Zuge der Arbeit wurden beide Tools evaluiert und getestet. Aufgrund der einfacheren Handhabe und des allgemeinen subjektiven Eindrucks fiel die Wahl auf das Programm „Gophish“. Für die praktische Umsetzung dieser Arbeit wird daher dieses Phishing-Framework zum Einsatz kommen. Es bietet alle Funktionen, die für die Durchführung und Auswertung der Phishing-Simulation von Nöten sind, in einer zentralen Lösung an und ist somit für den Zweck dieser Arbeit geeignet.

Die Software wird auf einem virtuellen Server im Unternehmen installiert und betrieben. Auch werden für den Versand der simulierten Phishing-E-Mails und zur Bereitstellung der simulierten Phishing-Webseiten interne Ressourcen des Zielunternehmens verwendet. Dies macht die Durchführung in vielerlei Hinsicht einfacher. Als große Vorteile sollten genannt werden, dass weder potenziell schadhafte Software im öffentlichen Raum des Internets betrieben werden muss, noch dass Daten und Informationen, die für die Auswertung nötig sind, das Unternehmen verlassen. Somit reduzieren sich sowohl die Kosten als auch die Gefahr, im Zuge der Durchführung der Simulation für einen echten Angreifer gehalten zu werden. Ein weiterer Vorteil der Verwendung von internen Ressourcen ist die Tatsache, dass keine Manipulation am E-Mail-Sicherheitssystem des Unternehmens passieren muss, damit die simulierten Phishing-E-Mails zugestellt werden können. Zudem hat dies monetäre Vorteile, da keine Kosten für einen E-Mail-Dienst, ein Webhosting für die Phishing-Webseiten oder zu registrierende Domänen anfallen.

Als Richtwert für die Bestätigung des Erfolges eines simulierten Phishing-Angriffs kommt im Rahmen dieser Arbeit der Ansatz der „Fehlerrate pro Kampagne“ zum Einsatz. Für die Beantwortung der Forschungsfrage bedeutet dies also, dass ein:e Kolleg:in als anfällig für eine selbst durchgeführte Phishing-Simulation gilt, wenn der Phishing-Link angeklickt wurde. Der Grund dafür ist, dass das Anklicken eines solchen Links bereits problematisch sein kann und eine aktive Interaktion mit dem Phishing-Versuch darstellt. Es macht auch deutlich, dass der Empfangende die schadhafte E-Mail nicht als solche erkennen konnte. Das bloße Öffnen der simulierten Phishing-E-Mail reicht dazu hingegen nicht aus, da dies im Zuge der Prüfung der E-Mail auf Legitimität notwendig sein kann. Jemanden erst nach der Eingabe von Zugangsdaten auf einer Phishing-Seite als anfällig für eine Phishing-Simulation zu erkennen, ist hingegen nicht relevant. Dies stellt bereits ein massives Sicherheitsproblem dar und es besteht die Gefahr, dass ein falscher Eindruck vom Sicherheitsniveau der Mitarbeitenden gewonnen wird, wenn zwar viele den Phishing-Link anklicken, jedoch nur wenige tatsächlich ihre Zugangsdaten eingeben.

4. Technische Umsetzung

Neben der Herstellung der Umgebung für den Betrieb des Phishing-Frameworks, gilt es weitere technische Voraussetzungen für die erfolgreiche Durchführung einer Phishing-Simulation zu schaffen. Ziel dieser Arbeit ist es herauszufinden, wie anfällig die Kolleg:innen des Autors auf Phishing-Angriffe sind, nicht wie resilient das Unternehmen gegenüber Phishing-Attacken ist. Darum müssen Maßnahmen getroffen werden, die den Versand und den Empfang von simulierten Phishing-E-Mails ermöglichen.

4.1 Voraussetzungen für die Phishing-Simulation

Da im Zielunternehmen großer Wert auf Cyber-Security gelegt wird, gibt es, neben den bewusstseinsbildenden Maßnahmen für Mitarbeitende, auch weitreichende technische Maßnahmen zum Schutz vor Phishing-E-Mails. Im Zuge der Evaluierung der Phishing-Frameworks ist aufgefallen, dass diese die Zustellung der simulierten Phishing-Nachrichten verhindern. Ein Teil der technischen Umsetzung hat sich damit auseinandergesetzt, den internen Versand von Phishing-E-Mails zuzulassen, damit die Simulation stattfinden kann. Dabei stand im Vordergrund, dass keine Sicherheitslücken entstehen, die echte Angriffe möglich oder einfacher machen könnten. Eine vollständige Deaktivierung aller für diesen Bereich relevanten Sicherheitsmechanismen stellte somit keine Option dar. Vielmehr galt es, eine möglichst genaue Definition von Ausnahmen für die jeweiligen Sicherheitsmechanismen zu finden. Auf diese wird in den folgenden Zeilen eingegangen.

Das Zielunternehmen benutzt einen Clouddienst von Microsoft für den E-Mail-Versand- und Empfang. Alle Mitarbeitenden haben ein „Microsoft 365 Business Premium“-Lizenzpaket. Dieses beinhaltet, neben der für die E-Mail-Funktion vorausgesetzten „Exchange-Online“-Lizenz, auch das Produkt „Microsoft Defender for Office 365“. Dieses bietet weitreichende Schutzmechanismen zum Schutz der E-Mail-Kommunikation, darunter auch Funktionen, die der Zustellung von Phishing-Nachrichten entgegenwirken.

Das erste Problem war, dass die testweise verschickten Phishing-E-Mails nicht zugestellt wurden oder im Junk-E-Mail-Ordner von Outlook landeten. Da dies bei professionellen Phishing-Attacken häufig nicht der Fall ist und diese im tatsächlichen Posteingang der Empfangenden landen, wurde dahingehend recherchiert. Es wurde klar, dass Microsoft für diesen Fall vorgebeugt hat und eine Funktion in Exchange-Online anbietet, die es erlaubt dedizierte Domänen, Absender-IP-Adressen und Simulations-Links zu erlauben. Für die Zustellung der simulierten Phishing-E-Mails im Rahmen dieser Arbeit, werden dort also die verwendeten Domänen und die IP-Adresse des verwendeten Postausgangsservers hinterlegt.

Diese Maßnahme hat dazu geführt, dass die selbst verschickten Phishing-E-Mails nun nichtmehr gänzlich blockiert wurden. Beim Versand von einer Domäne, die nicht der

Unternehmens-Domäne entsprach, landeten sie jedoch noch immer im Ordner „Junk-E-Mail“. Eine weitere Recherche zu der Thematik machte deutlich, dass auch die Richtlinie „Anti-Spam inbound policy“ des Produkts „Microsoft Defender for Office 365“ angepasst werden muss. Auch dort gibt es die Option, eine Liste der erlaubten Domänen und erlaubten Absender zu pflegen. Die im Rahmen der Phishing-Simulation verwendeten Domänen und Absender-E-Mail-Adressen werden also auch dort eingepflegt.

Mit diesen Schritten war es dann möglich, die simulierten Phishing-E-Mails direkt in die Posteingänge der Empfangenden zu verschicken.

Eine weitere Auffälligkeit gab es, da der Download von Bildern in E-Mails von unbekannten Absendern standardmäßig deaktiviert ist. Dies ist ein Sicherheitsfeature von Microsoft Outlook, das im Rahmen dieser Arbeit jedoch verhindert, dass die Anzeige des Status „E-Mail gelesen“ in der Auswertungsfunktion des Phishing-Frameworks korrekt funktioniert. Die technische Funktionsweise des Gelesen-Status in Gophish ist, dass in jede E-Mail-Nachricht ein einzigartiges Bild eingebunden wird. Wird dieses im E-Mail-Programm der Empfangenden dargestellt, wird es vom Phishing-Framework heruntergeladen. Merkt das Phishing-Framework, dass auf dieses Bild zugegriffen wird, markiert es die zugehörige Phishing-E-Mail als „gelesen“. Wenn der E-Mail-Client jedoch verhindert, dass das Bild heruntergeladen wird, findet dieser Vorgang nicht statt und der Status kann nicht auf „Gelesen“ gesetzt werden. Es gibt die Möglichkeit, den Download von Bildern von unbekannten Absendern zu erlauben. Im Rahmen dieser Arbeit wird davon aber nicht gebraucht gemacht. Da dies auch bei echten Phishing-E-Mails nicht der Fall ist, würde es den Eindruck der Empfangenden auf die simulierte Phishing-E-Mail manipulieren und somit einen Unterschied zur Realität darstellen. Dies hat jedoch zur Folge, dass der Status „gelesen“ in der Auswertung der Phishing-Simulation nicht korrekt sein wird. Da dieser jedoch keinen Einfluss auf die Beantwortung der Forschungsfrage hat, ist dies ein rein kosmetischer Mangel.

Da im Rahmen dieser Phishing-Simulation nur interne Ressourcen zum Einsatz kommen werden, stellt auch die Konfiguration der unternehmensinternen Namens-Server (DNS) einen nennenswerten Aufwand dar. Mit „Typo-Squatting“ und „Domain-Squatting“ kommen zwei Methoden zum Einsatz, die auf der Verwendung von speziellen Domänen-Namen basieren. Um diese Domänen für die Phishing-Simulation nutzen zu können, sie aber nicht kostenpflichtig registrieren zu müssen, werden sie auf den lokalen DNS-Servern des Unternehmens als neue Zonen registriert und verweisen auf die IP-Adresse, unter der das Phishing-Framework erreichbar ist. Dies ermöglicht es, den Empfangenden glaubwürdig vorzutäuschen, sie würden auf Ressourcen im Internet zugreifen, obwohl dies nicht der Fall ist.

4.2 Installation und Konfiguration des Phishing-Frameworks

Das Softwareprodukt „Gophish“ ist ohne Installation lauffähig. Somit beschränkt sich der Aufwand für die Inbetriebnahme des Phishing-Frameworks auf das Bereitstellen eines virtuellen Servers auf der Infrastruktur des Zielunternehmens und Anpassungen im Netzwerk. Im Rahmen dieser Arbeit wurde so ein virtueller Server mit Microsoft Windows Server 2022 in der Datacenter-Version bereitgestellt. Dieser verfügt über zwei virtuelle Prozessorkerne, acht Gigabyte Arbeitsspeicher und einer 90 Gigabyte großen virtuellen Festplatte. Dieser virtuelle Server ist in einem separaten Netzwerksegment untergebracht. Wie in Abbildung 10 ersichtlich, kommuniziert der Phishing-Server lediglich über TCP-Port 25 mit dem lokalen E-Mail-Gateway des Unternehmens und ist aus dem Client-Netzwerk über TCP-Port 80 zum Anzeigen der Phishing-Webseiten erreichbar.

Abbildung 10 - Netzwerkkonfiguration. Quelle: Autor

Der Zugriff auf das Phishing-Framework sowie die Verwaltung dessen passieren direkt am virtuellen Phishing-Server. Es war ein Ziel, dem Phishing-Framework nur die nötigste Konnektivität zu geben, um so mögliche Sicherheitsprobleme zu vermeiden.

Für den Betrieb von „Gophish“ ist dann nur noch der Download der aktuellen Version der Software aus dem GitHub-Repository des Programmierers und das Extrahieren dieses Archives notwendig. Das Phishing-Framework ist dann, ohne die Installation weiterer Abhängigkeiten, lauffähig und einsatzbereit. Die Software selbst läuft in der Kommandozeile.

Beim ersten Start der Software gibt die Kommandozeile des virtuellen Servers das Initialpasswort für die Anmeldung am Webinterface aus. Die Kommandozeile bleibt im Betrieb dauerhaft geöffnet und zeigt die Meldungen des integrierten Webservers an. Die Bedienung des Phishing-Framewoks findet dann im Webinterface statt.

Es gibt nur einen Konfigurationsschritt der notwendig ist, damit simulierte Phishing-E-Mails versendet werden können. Dabei handelt es sich um die Anlage eines sogenannten „Sending Profiles“. Darin wird konfiguriert, welcher Postausgangsserver verwendet wird und mit welchen Zugangsdaten auf diesen zugegriffen wird. Nach Eingabe der Verbindungsdaten besteht die Möglichkeit, diese Einstellungen zu testen, um so sicherzustellen, dass die Daten korrekt sind.

5. Erstellen der Phishing-Kampagnen

Wie aus den vorangegangenen Kapiteln der Arbeit hervorgeht, ist die Planung der Phishing-Simulation ein entscheidender Faktor für deren Erfolg. In diesem Teil der Arbeit wird im Detail auf die Planungsaspekte eingegangen.

5.1 Erstellen der Phishing-Inhalte

Im ersten Teil dieser Arbeit wurden die drei, für das Zielunternehmen potenziell gefährlichsten Phishing-Inhalte identifiziert. An dieser Stelle wird beschrieben, wie diese erstellt werden.

5.1.1 Inhalt 1 - Willkommensmeldung Microsoft 365

Im ersten Phishing-E-Mail geht es um die Willkommensmeldung einer Microsoft 365 Gruppe. Als Inhalt kommt die vom Autor angepasste Version einer legitimen Willkommensmeldung zum Einsatz. Um mehr auf die verschiedenen Positionen der Mitarbeitenden einzugehen, kommen drei Varianten dieser E-Mail, mit unterschiedlichen Betreffzeilen und Überschriften in der Nachricht, zum Einsatz:

- Sie sind der Gruppe „Weihnachtsfeier“ beigetreten
- Sie sind der Gruppe „Führungskräfte“ beigetreten
- Sie sind der Gruppe „Intern“ beigetreten

Erstellt wurde der Phishing-Inhalt durch die Import-Funktion im Phishing-Framework Gophish. Ausgangsmaterial war eine legitime Nachricht, die über die neuerlangte Zugehörigkeit zu einer Microsoft 365-Gruppe informiert. Zur optimalen Darstellung der Inhalte wurden die Bilder aus der originalen Nachricht heruntergeladen und der Phishing-Nachricht als Anhang hinzugefügt. Damit die Bilder im E-Mail-Programm der Empfangenden korrekt dargestellt werden, musste danach noch der Pfad im Quelltext der Nachricht angepasst werden.

Weiters wurden alle in der originalen Nachricht enthaltenen Links durch die Platzhalter-Links des Phishing-Frameworks ersetzt. Diese führen zu einer imitierten Microsoft 365 Anmelde-Seite.

In legitimen E-Mails dieser Art steht der jeweilige Gruppenname in der Absenderadresse. Dies ist technisch umsetzbar, wird jedoch nicht angewandt, da es zu Konflikten mit etwaigen, bereits existierenden und genutzten Inhalten kommen kann. Im Rahmen dieser Nachricht wird versucht, die Empfangenden glauben zu lassen, die Nachricht käme von Microsoft. Diese Glaubwürdigkeit soll in diesem Fall mittels der Methode „Domain- bzw. Typo-Squatting“ erreicht werden. Als Absender für diese Mail-Inhalte wird „noreply@microsoft356.com“ eingesetzt. In Abbildung 11 ist diese simulierte Phishing-

E-Mail ersichtlich. Diese wurde vorab zu Testzwecken an das Postfach des Autors verschickt.

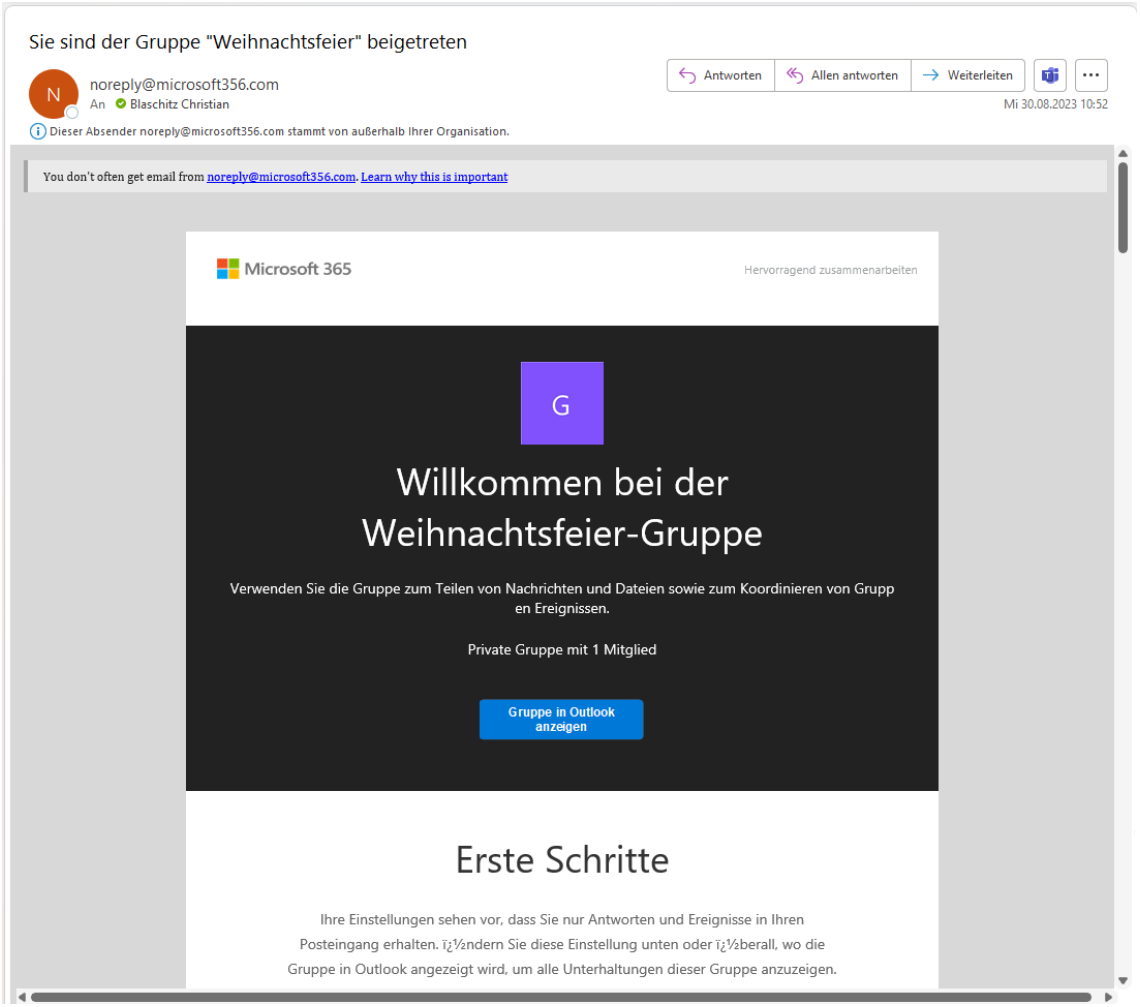

Abbildung 11 - Inhalt 1. Quelle: Autor

Alle Links in dieser Phishing-E-Mail führen zu einer gefälschten Anmeldeseite. Diese wurde der Anmeldeseite von Microsoft nachempfunden. Im Original kommt diese Seite bei Anmeldungen an Webanwendungen von Microsoft zum Einsatz. So beispielswiese auch bei der Anmeldung an Microsoft Teams oder Microsoft Outlook. Wie in Abbildung 12 ersichtlich, verlangt diese Phishing-Seite die E-Mail-Adresse, Telefonnummer oder den Skype-Benutzernamen zur Identifizierung des Benutzers und das zugehörige Kennwort für die Authentifizierung. Optisch ist die Phishing-Seite dem original sehr ähnlich, wenngleich es nicht möglich war, eine exakte Kopie davon zu erstellen. Diese Phishing-Seite wurde vom Autor mit Unterstützung von ChatGPT erstellt.

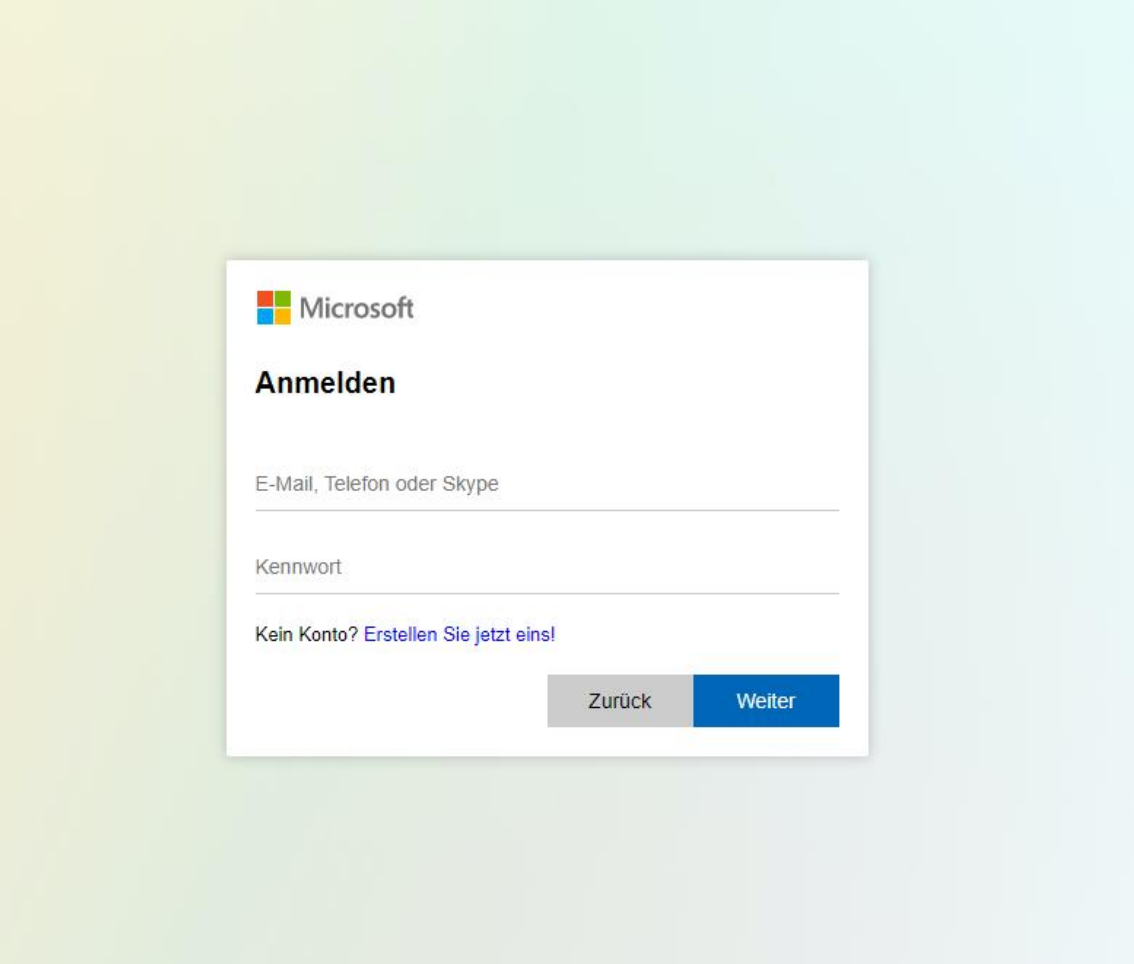

Abbildung 12 - Phishing-Seite. Quelle: Autor

5.1.2 Inhalt 2 – Auto beschädigt

Im zweiten Inhalt soll den Empfangenden glaubhaft gemacht werden, dass es am Parkplatz des Unternehmens zur Beschädigung mehrerer Fahrzeuge gekommen ist. In der Nachricht befindet sich ein Link zu angeblichen weiterführenden Informationen und Bildern. Dieser sieht aus, als würde er auf eine Freigabe in Microsoft Sharepoint bzw. Microsoft OneDrive verweisen. In Wahrheit führt auch dieser Link zu einer imitierten Microsoft 365 Anmelde-Seite. Die Nachricht wurde vom Autor dieser Arbeit selbst verfasst und bewusst simpel gehalten. Um Glaubwürdigkeit zu vermitteln, wurde auf die Methode Topleveldomain-Squatting zurückgegriffen. Anstatt der tatsächlichen .at-Domäne des Zielunternehmens, wird eine .com-Domäne verwendet. Die daraus resultierende Phishing-E-Mail ist in Abbildung 13 ersichtlich.

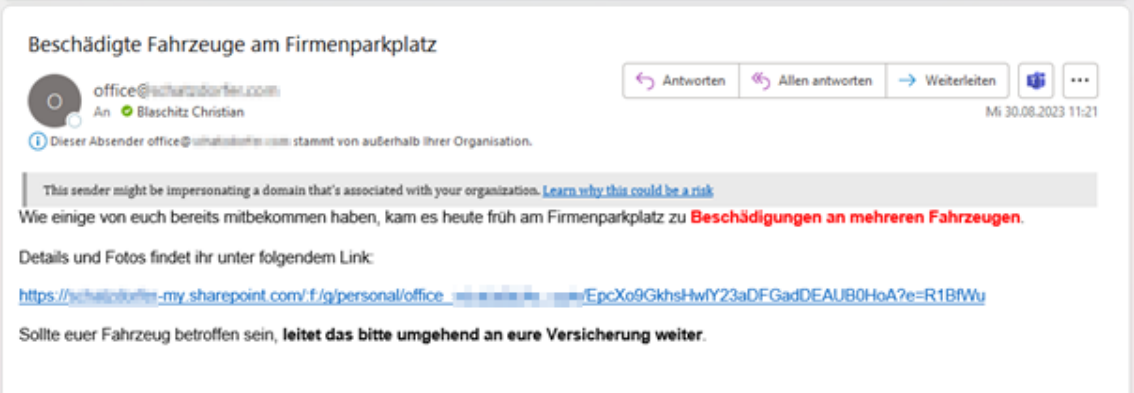

Abbildung 13 - Inhalt 2. Quelle: Autor

Auch der Link in dieser simulierten Phishing-E-Mail führt zur selben Microsoft-Anmeldeseite die in Abbildung 12 ersichtlich ist. Dies wäre also auch die Anmeldeseite die einen beim Zugriff auf einen legitimen Freigabe-Link auf eine Microsoft Sharepoint-Freigabe erwartet.

5.1.3 Inhalt 3 - Fehler in der Gehaltsabrechnung

Der dritte E-Mail-Inhalt der Phishing-Simulation versucht den Empfangenden glaubhaft zu machen, dass es einen Fehler bei ihrer Gehaltsabrechnung gab. Es wird in Aussicht gestellt, dass es aufgrund der Fehler zu Gehaltsnachzahlungen kommen kann. In der in Abbildung 13 dargestellten E-Mail wird dazu aufgefordert, die persönlichen Daten zu aktualisieren, um diese richtigzustellen. Dafür ist ein Link enthalten, der zu dem in Abbildung 14 dargestellten Formular führt. Darin ist der Name des Arbeitgebers, der eigene Name und das Geburtsdatum auszufüllen. Das Feld „Arbeitgeber“ ist dabei bereits mit dem Namen des Zielunternehmens vorausgefüllt. Zudem wird gefragt, ob das Beschäftigungsverhälts bereits länger als sechs Monate andauert. Auch gibt es die Möglichkeit, Fragen und Anmerkungen in ein Freitext-Feld zu schreiben. Besuchende der Seite werden noch darauf hingewiesen, dass sie im „nächsten Schritt“ erfahren würden, wie hoch ihre Rückzahlung sein wird. Diese Inhalte wurden vom Autor unter der Zuhilfenahme von ChatGPT erstellt.

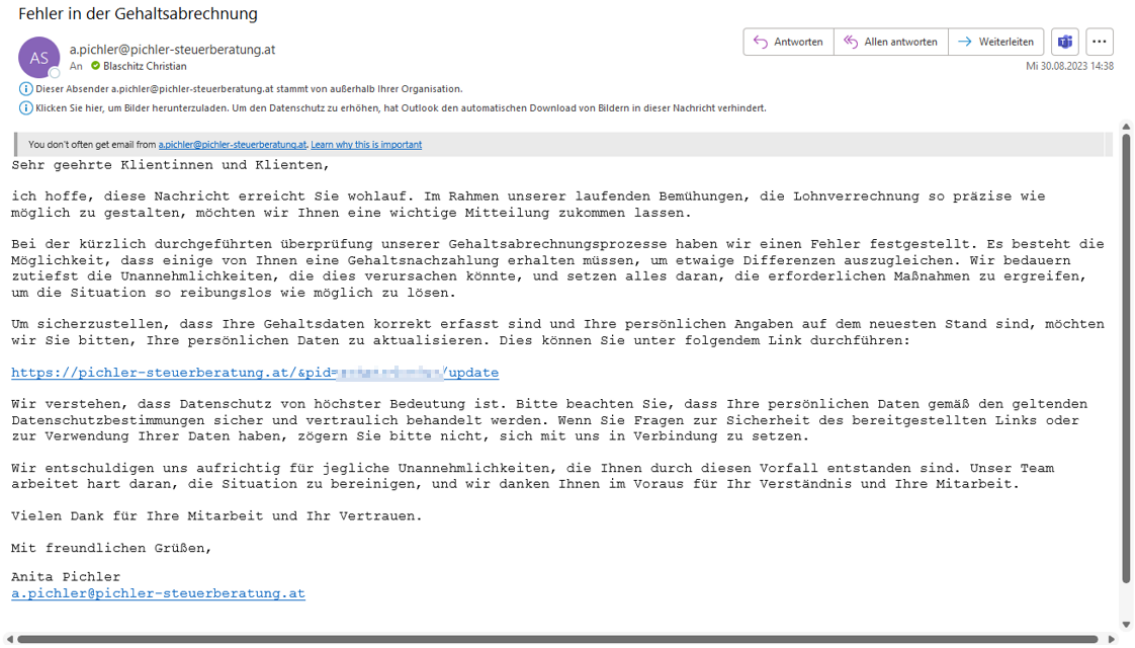

Abbildung 14 - Inhalt 3. Quelle: Autor

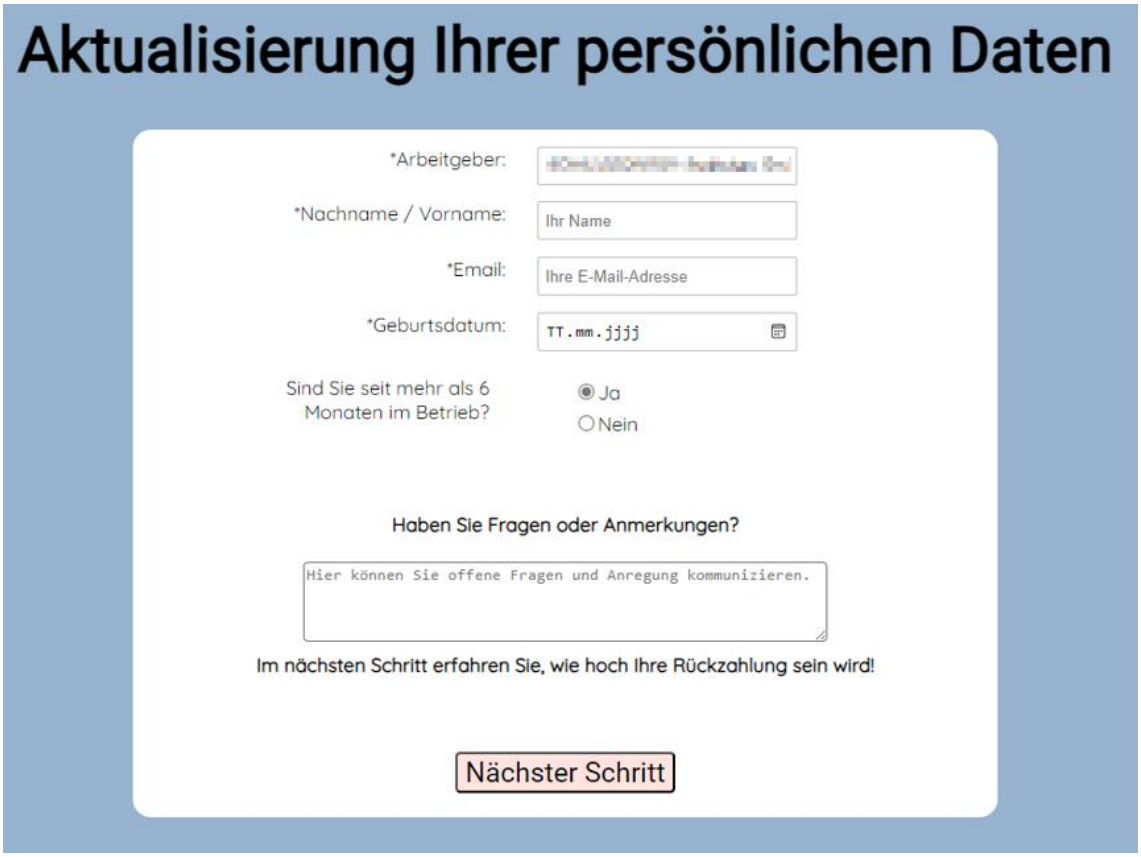

Abbildung 15 - Phishingseite für Inhalt 3. Quelle: Autor

5.2 Adressat:innen

In diesem Kapitel wird auf die Aufteilung der adressierten Personen eingegangen. Um die Anonymität der Empfangenden zu wahren, wird anstatt des Namens eine Nummer verwendet. Wie in Tabelle XYZ ersichtlich, erfolgt die Gliederung der Empfangenden nach den Attributen Abteilung und Position. Weiters ergeben sich aufgrund der Einteilung in verschiedene Empfängergruppen, aufgrund der Position im Unternehmen, der Dauer des Beschäftigungsverhältnisses und der physischen Nähe der Empfangenden zueinander eine weitere Einteilung in die, ebenfalls in Tabelle 4 ersichtlichen, Felder:

- Führungskraft (FK) – für die Geschäftsführenden und Abteilungsleiter.
- Neue Mitarbeitende (neue MA) – für Mitarbeitende, welche seit weniger als 12 Monaten im Unternehmen sind, oder in den letzten 12 Monaten ihren E-Mail-Zugang erhalten haben.
- Mehrjährige Mitarbeitende (MA) - für Mitarbeitende, die seit 12 oder mehr Monaten im Unternehmen beschäftigt sind.
- Ort1 und Ort2 – Alle Empfangenden werden, aufgrund ihrer physischen Position im Unternehmen, in zwei Gruppen aufgeteilt. Wenn sicher zwei oder mehr Empfangende ein Büro teilen, werden sie gleichmäßig auf die zwei Gruppen aufgeteilt. Besetzende von Einzelarbeitsplätzen sind in der Gruppe „Ort1“.

#	**Abteilung**	**Position**	**FK**	**neue MA**	**MA**	**Ort1**	**Ort2**
1	Produktion	Führungskraft	x				x
2	Produktion	Mitarbeiter:in			x	x	
3	Arbeitsvorbereitung	Mitarbeiter:in			x	x	
4	Produktion	Mitarbeiter:in			x	x	
5	Verwaltung	Mitarbeiter:in			x	x	
6	Geschäftsleitung	Geschäftsleitung	x				x
7	Vertrieb	Gruppenpostfach			x		x
8	Produktion	Führungskraft	x				x
9	Produktion	Mitarbeiter:in		x		x	
10	Lager / Logistik	Führungskraft	x			x	
11	Arbeitsvorbereitung	Mitarbeiter:in			x	x	
12	Produktion	Führungskraft	x				x
13	Verwaltung	Mitarbeiter:in		x		x	
14	Produktion	Mitarbeiter:in			x	x	
15	Produktion	Führungskraft	x			x	
16	Lager / Logistik	Mitarbeiter:in		x		x	

#	Abteilung	Position	FK	neue MA	MA	Ort1	Ort2
17	Verwaltung	Mitarbeiter:in			x		x
18	Produktion	Mitarbeiter:in			x	x	
19	Produktion	Führungskraft	x				x
20	Arbeitsvorbereitung	Mitarbeiter:in			x	x	
21	Verwaltung	Mitarbeiter:in			x	x	
22	Produktion	Mitarbeiter:in			x	x	
23	Verwaltung	Mitarbeiter:in			x		x
24	Verwaltung	Führungskraft	x			x	
25	Verwaltung	Mitarbeiter:in			x		x
26	Verwaltung	Führungskraft	x			x	
27	Arbeitsvorbereitung	Führungskraft	x				x
28	Produktion	Mitarbeiter:in			x	x	
29	Produktion	Mitarbeiter:in		x			x
30	Lager / Logistik	Mitarbeiter:in			x		x
31	Geschäftsleitung	Geschäftsleitung	x			x	
32	Geschäftsleitung	Geschäftsleitung	x			x	
33	Verwaltung	Führungskraft	x				x
34	Lager / Logistik	Gruppenpostfach			x	x	
35	Vertrieb	Führungskraft	x				x
36	Arbeitsvorbereitung	Führungskraft	x				x
37	Produktion	Mitarbeiter:in			x	x	
38	Verwaltung	Mitarbeiter:in			x		x
39	Lager / Logistik	Führungskraft	x				x
40	Produktion	Mitarbeiter:in			x	x	
41	Verwaltung	Mitarbeiter:in			x		x
42	Verwaltung	Mitarbeiter:in			x	x	
43	Lager / Logistik	Führungskraft	x				x
44	Verwaltung	Mitarbeiter:in			x	x	
45	Geschäftsleitung	Geschäftsleitung	x			x	
46	Vertrieb	Mitarbeiter:in			x	x	
47	Produktion	Mitarbeiter:in			x	x	
48	Produktion	Mitarbeiter:in			x	x	
49	Produktion	Mitarbeiter:in			x	x	
50	Produktion	Mitarbeiter:in		x		x	

Tabelle 4 - Adressat:innen. Quelle: Autor

5.3 Zeitplan für den Versand

Der Zeitpunkt der Zustellung kann entscheidend für den Erfolg einer Phishing-E-Mail sein. Darum wird auch großer Wert auf die Zeitplanung gelegt. Für die drei Phishing-Inhalte werden drei verschiedene Herangehensweisen gewählt.

Die erste simulierte Phishing-E-Mail wird die angebliche Teams-Einladung sein. Diese erreicht die drei Empfängergruppen am Montagvormittag. Das konkrete Datum dafür ist der 25. September 2023. Die Nachrichten werden im Zeitraum von 05:00 Uhr bis 09:00 Uhr zugestellt.

Als zweite simulierte Phishing-E-Mail wird die, des angeblichen Parkschadens am Firmenparkplatz versandt. Diese wird am 29. September 2023 um 10:15 Uhr an alle Empfangenden, also die Gruppe „Alle Benutzer“, gleichzeitig versendet.

In der dritten und somit letzten simulierten Phishing-E-Mail, die im Rahmen dieser Arbeit verschickt wird, geht es um einen angeblichen Fehler in der Gehalts-Abrechnung. Diese Nachricht wird in zwei zeitlichen Tranchen an alle Benutzer verschickt. Am 06. Oktober zwischen 06:00 Uhr und 09:00 Uhr wird die Gruppe „Ort1“ die E-Mail erhalten, am selben Tag, zwischen 09:30 Uhr und 12:00 Uhr die Gruppe „Ort2“.

6. Ergebnisse der Phishing-Simulation

Auf die Planung und die Durchführung der Phishing-Simulation folgt abschießend die Auswertung dieser. In diesem Teil der Arbeit werden die Ergebnisse der drei Phishing-Kampagnen präsentiert.

6.1 Ergebnisse Inhalt 1

Die erste Kampagne wurde in drei Teilen durchgeführt (vgl. Kapitel 5.1.1). Zur verbesserten Übersicht werden die Ergebnisse dieser drei Teile hier gesammelt dargestellt.

In Summe wurden in dieser Kampagne 50 simulierte Phishing-E-Mails verschickt. Fünf Empfangenden (zehn Prozent) haben den darin enthaltenen Link geöffnet und vier davon (80 Prozent) haben ihre Zugangsdaten preisgegeben.

Bei den IT-Ansprechpartnern des Unternehmens gab es keine Meldungen über einen Phishing-Versuch oder Rückfragen zu diesen Mails.

6.2 Ergebnisse Inhalt 2

Die E-Mails der zweiten Kampagne hat alle Empfangenden zur selben Zeit erreicht. In dieser Kampagne wurden auch wieder 50 simulierte Phishing-E-Mails verschickt. Vier der Empfangenden (Acht Prozent) haben auf den Phishing-Link geklickt, drei davon (75 Prozent) haben ihre Zugangsdaten preisgegeben.

Diese Phishing-E-Mail wurde von einem Mitglied der Geschäftsleitung als schadhaft erkannt und daraufhin gemeldet. Alle Empfangenden wurden im Zuge dessen darauf hingewiesen, diese E-Mail nicht zu öffnen. Diese Info erreichte die Empfangenden etwa drei Minuten nach der Zustellung der simulierten Phishing-E-Mail. Dieses Mitglied der Geschäftsleitung wusste über die Durchführung der Phishing-Simulation Bescheid. Da diese Meldung bereits drei Minuten nach der Zustellung erfolgte, ist davon auszugehen, dass mehr der Empfangenden auf diesen Inhalt reagiert hätten.

6.3 Ergebnisse Inhalt 3

Die E-Mails der dritten und letzten Phishing-Kampagne wurden in zwei Durchgängen verschickt. Zur verbesserten Übersicht werden die Ergebnisse dieser zwei Teile hier gesammelt dargestellt.

Auch in dieser Kampagne wurden in Summe wieder 50 simulierte Phishing-E-Mails verschickt. Einer der Empfangenden (Zwei Prozent) haben den Phishing-Link angeklickt. Es wurden jedoch keine Daten preisgegeben.

Diese Phishing-E-Mail wurde von einem Empfangenden als schadhaft erkannt und daraufhin gemeldet. Alle Empfangenden wurden im Zuge dessen darauf hingewiesen, diese E-Mail nicht zu öffnen. Aufgrund des zeitversetzten Versands der Phishing-E-Mail erreichte die Information über die Schadhaftigkeit die Empfangenden zwischen knapp einer Stunde nach- und 30 Minuten vor der Zustellung der simulierten Phishing-E-Mail. Der warnende Mitarbeiter wusste nicht über die Durchführung der Phishing-Simulation Bescheid.

6.4 Ergebnisse gesamt

Im Zuge dieser Arbeit wurden 150 simulierte Phishing-E-Mails versandt. Bei 140 (93,3 Prozent) wurde der Phishing-Link nicht angeklickt. Bei Zehn E-Mails (6,67 Prozent) wurde der Link angeklickt und in sieben Fällen (70 Prozent) wurden zudem auch noch Zugangsdaten preisgegeben. Dies wird in Abbildung 16 visualisiert dargestellt.

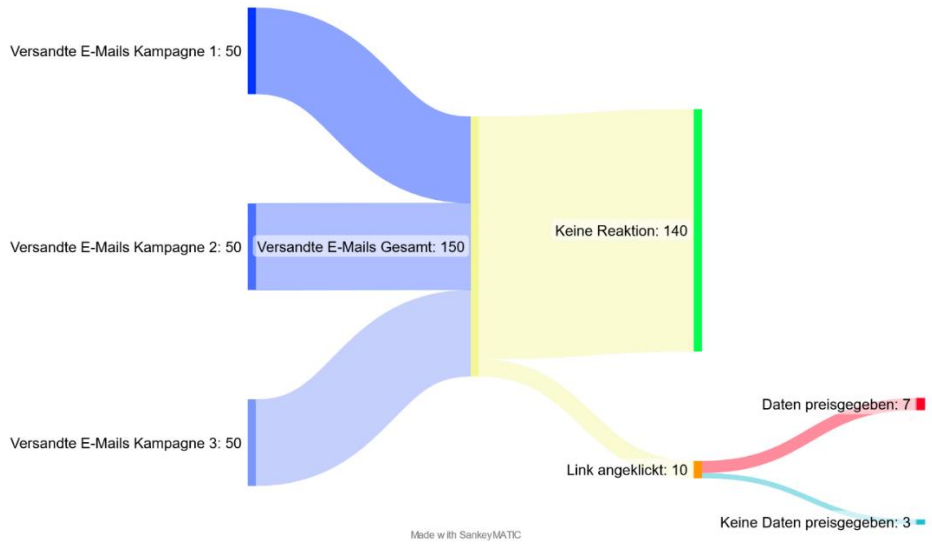

Abbildung 16 - Ergebnisse der Kampagnen. Quelle: Autor

Unter den 50 Empfangenden befanden sich auch zwei Gruppenpostfächer. Die Mitglieder dieser Gruppenpostfächer haben auch eine persönliche E-Mail-Adresse und die Phishing-Mails somit mehrfach erhalten. Da sich die Beantwortung der Forschungsfrage auf die Anzahl der Kolleginnen und Kollegen bezieht, werden die Gruppenpostfächer dort nicht berücksichtigt. Ein weiterer wichtiger Faktor ist, dass keiner der Empfangenden mehr als eine simulierte Phishing-E-Mails geöffnet hat.

Somit haben von den 48 empfangenden Personen also insgesamt zehn (20,83 Prozent) so auf die simulierten Phishing-E-Mails reagiert, dass sie als „anfällig für eine selbst durchgeführt Phishing-Simulation“ eingestuft werden müssen.

7. Schlussfolgerung

In diesem Kapitel werden die Ergebnisse der Untersuchung zusammengefasst und die Forschungsfrage beantwortet. Außerdem wird die Hypothese bewertet.

7.1 Beantwortung der Forschungsfrage

Die Forschungsfrage, die es im Rahmen dieser Arbeit zu beantworten gibt, lautet „Wieviel Prozent meiner Kolleginnen und Kollegen sind anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation?“.

In der vorangegangenen Auswertung der Phishing-Simulation ist ersichtlich, dass 20,83 Prozent der Kolleginnen und Kollegen anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation sind.

Die Tatsache, dass viele Empfangende zeitnah an die Zustellung der simulierten Phishing-E-Mails vor eben diesen gewarnt wurden, hat das Ergebnis der Phishing-Simulation sehr stark beeinflusst. Obwohl die Forschungsfrage dennoch beantwortet werden konnte, ist das Ergebnis nicht restlos zufriedenstellend. Zufriedenstellender und repräsentativer wäre es gewesen, wenn alleinig die persönliche Einschätzung der Empfangenden für deren Reaktion auf die simulierten Phishing-E-Mails verantwortlich gewesen wäre.

7.2 Bewertung der Hypothese

Die Hypothese des Autos lautete, dass mehr als 20 Prozent seiner Kolleginnen und Kollegen anfällig auf eine selbst durchgeführte E-Mail-Phishing-Simulation seien. Durch die Durchführung und Auswertung der Phishing-Simulation, konnte diese Hypothese bestätigt werden.

8. Zusammenfassung und Ausblick

Die Arbeit schließt mit einer Zusammenfassung und dem Ausblick ab. Hier wird nochmal deutlich gemacht, wie die Forschungsfrage lautete und welche Methoden zur Beantwortung dieser zum Einsatz kamen. Zudem gibt es einen Ausblick auf neue Perspektiven für die Praxis und mögliche neue Forschungsansätze, die sich aus dieser Arbeit ergeben.

8.1 Zusammenfassung

Die Beantwortung der Forschungsfrage sollte den aktuellen Zustand der Phishing-Cybersicherheit des Zielunternehmens veranschaulichen und zeigen, wieviel Prozent der Kolleginnen und Kollegen des Autors anfällig auf eine selbst geplante und durchgeführte Phishing-Kampagne sind.

Kapitel zwei setzt sich intensiv mit dem Thema Phishing auseinander und erklärt dieses umfassend. Darin wird deutlich, dass die Definition des Begriffes „Phishing“ nicht einfach ist. Frei übersetzt lautet diese, dass es beim Phishing darum geht, Internetbenutzer so zu täuschen, dass diese den Angreifenden persönliche und vertrauliche Informationen preisgeben. Das zweite Kapitel zeigt auch, dass es mannigfaltige Möglichkeiten gibt, um Opfer von Phishing zu werden (vgl. Kapitel 2.2). Neben den allgegenwärtigen Phishing-Methoden, die per Mail durchgeführt werden, werden auch immer häufiger Phishingversuche über das Telefon (Vishing) oder Kurzmitteilungen am Mobiltelefon (Smishing) verzeichnet. Da mobile Endgeräte eine immer größer werdende Rolle im täglichen Leben spielen, sind diese lukrative Ziele. Gerade auch, da es dort meist nicht einfach ist entsprechende technische Sicherheitsmechanismen zu etablieren. In diesem Teil der Arbeit wird auch erklärt, dass Phishing aufgrund der technischen Einfachheit und kostengünstigen Umsetzung eine sehr beliebte Art der Attacke ist, die immer häufiger wird. Als die primären Ziele der Angreifenden konnte der Datendiebstahl, der Identitätsdiebstahl und der finanzielle Diebstahl identifiziert werden. Diese werden dort auch anhand einiger Beispiele von echten Attacken dargestellt.

Wenn es um Phishing geht, muss auch die Vermeidung von Phishing-Attacken behandelt werden. So wird Kapitel zwei durch einen Überblick über mögliche Maßnahmen gegen Phishing abgerundet (vgl. Kapitel 2.6). Da Phishing allgegenwärtig ist, gibt es eine große Anzahl an technischen Produkten, die die Zustellung von Phishing-Mails verhindern sollen. Diese verwenden häufig auch maschinelle Lernfähigkeiten, die mit bestehenden Phishing-Inhalten trainiert werden, um neue Bedrohungen zu erkennen. Neben den technischen Lösungen für diese Art der Bedrohung, ist die Bewusstseinsbildung gegen Cyberangriffe sehr wichtig. Bewusstsein darüber, welche Bedrohungen es gibt und wie diese erkannt werden können. Dies ist bereits ein großes Thema für viele Unternehmen, die ihr Personal im Bereich der IT-Security schulen.

Der Aufbau der Kapitel dieser Arbeit dreht sich häufig um die drei Bereiche Planung-, Durchführung- und Auswertung einer Phishing-Kampagne. Ziel der Planung war es herauszufinden, welche Inhalte den größtmöglichen Erfolg versprechen. Nach der Durchsicht wissenschaftlicher und technischer Quellen konnten die vielversprechenden Manipulationstechniken identifiziert werden (vgl. Kapitel 3.1.1). So verspricht es den größten Erfolg, wenn über die Phishing-E-Mail Druck auf die Angegriffenen ausgeübt wird, oder deren Neugierde geweckt wird. Neben der Wahl der passenden Betreffzeile gibt es auch beim Gestalten des Inhaltes der Phishing-E-Mail und der Phishing-Website einiges zu beachten. Im Rahmen der Arbeit wurden dafür die häufigsten Zeichen einer Phishing-E-Mail ausgewertet (vgl. Kapitel 3.1.1) und bei der Erstellung der simulierten Inhalte weitestgehend vermieden. Als Inhalte für die Phishing-Simulation kamen eine Willkommensmeldung für eine Microsoft-Teams-Gruppe, eine E-Mail über einen angeblichen Schaden an geparkten Autos am Firmenparkplatz und einen angeblichen Fehler in der Gehaltsabrechnung zum Einsatz.

Weitere Faktoren, die großen Einfluss auf den Erfolg einer Phishing-Simulation haben, sind die Wahl der Angriffsmethodik und der Zeitpunkt für die Zustellung der simulierten Phishing-E-Mail. Die Angriffsmethodik beschreibt, welche Absender-E-Mail-Adresse für die Phishing-Kampagnen verwendet wird und auf welche Web-Adresse die Phishing-Links führen. Das diese legitim aussehen müssen, um die Angegriffenen täuschen zu können, kommen dafür meist die Methoden „Typosquatting“ und „Domainsquatting“ zum Einsatz. Dabei werden legitime Web-Adressen geringfügig verändert, so dass der Unterschied zur echten Adresse nicht einfach ersichtlich ist. Für die Umsetzung der Phishing-Simulation kamen je einmal Typosquatting, Topleveldomain-Squatting und die Domäne eines frei erfundenen Steuerberatungs-Unternehmens zum Einsatz.

Wie erwähnt, spielt auch der Zeitpunkt für die Zustellung der Phishing-E-Mails eine Rolle beim Erfolg einer Phishing-Simulation. Laut mehreren Quellen kommt es an Freitagen und Montagen zu einem erhöhten Aufkommen von Spam und Phishing-E-Mails. Dies begründet sich dadurch, dass Montage häufig die arbeitsreichsten Tage sind und die Aufmerksamkeit darunter leidet. Der Freitag hat sich etabliert, da viele Phishing-Links beim Zeitpunkt des Versandes noch nicht schadhaft sind, um E-Mail-Filter zu umgehen. Erst einige Stunden nach der Zustellung wird das Ziel des Links geändert und schadhaft gemacht. Die simulierten Phishing-E-Mails, die im Rahmen dieser Arbeit verschickt wurden, wurden Montag früh oder im Laufe des Freitags zugestellt.

Neben der Planung der Phishing-Simulation, wurde auch der professionellen Durchführung derer viel Aufmerksamkeit zuteil. Es galt, ein geeignetes Phishing-Framework zu finden, das die Anforderungen erfüllt und auch die spätere Auswertung einfach macht (vgl. Kapitel 3.1.2). Die Wahl fiel auf das Open-Source-Produkt „Gophish“. Dies wurde auf Ressourcen des Ziel-Unternehmens ausgeführt und für den Versand der simulierten Phishing-E-Mails wurde der interne E-Mail-Server verwendet. Somit war

sichergestellt, dass keine potenziell sensiblen Daten auf firmenfremden Ressourcen verarbeitet werden.

Nach der Planung und Durchführung ging es noch darum, die Simulation auszuwerten (vgl. Kapitel 6.4) und die Forschungsfrage zu beantworten (vgl. Kapitel 7.1). Insgesamt wurden 150 simulierte Phishing-E-Mails versandt, in zehn davon wurde der Link angeklickt und in insgesamt sieben Fällen wurden Daten preisgegeben. Insgesamt haben zehn von den achtundvierzig Empfangenden auf die Phishing-E-Mail reagiert. Das entspricht 20,83 Prozent. Die Durchführung der Simulation lief wie geplant, jedoch wurden die Empfangenden in zwei der drei durchgeführten Kampagnen von Mitarbeitenden zeitnah an die Zustellung der jeweiligen E-Mails darauf hingewiesen, dass es sich um eine Phishing-Nachricht handelt.

8.2 Ausblick

Die Durchführung der Phishing-Simulation wurde von der Unternehmensleitung des Zielunternehmens sehr positiv aufgefasst. Auch von den Mitarbeitenden gab es überwiegend positives Feedback auf diese Maßnahme. Es gibt bereits Pläne für zukünftige Kampagnen und sehr wahrscheinlich werden diese Simulationen auch in Zukunft regelmäßig stattfinden. Zur für diese Arbeit gewählten Vorgehensweise wird es jedoch einige Änderungen im Ablauf geben. So werden alle Mitglieder der Geschäftsleitung umfänglicher über die Inhalte und den Ablauf der Simulationen informiert. Auch werden die simulierten Phishing-E-Mails nicht mehr so stark konzentriert versendet, sondern über einen größeren Zeitraum hinweg verschickt. Diese zwei Änderungen sollen sicherstellen, dass die Empfangenden sich nicht gegenseitig auf die mögliche Schadhaftigkeit der E-Mails hinweisen können.

Für den praktischen Betrieb und die regelmäßige Durchführung ist auch anzudenken, auf die Phishing-Simulation eines Dienstleisters zurückzugreifen. Diese sind zwar allgemeiner und somit nicht auf das Zielunternehmen zugeschnitten, können wirtschaftlicher aber die bessere Wahl sein. Der zeitliche Aufwand, der hinter der selbstständigen Planung und Durchführung von Phishing-Simulationen steht, ist nicht außer Acht zu lassen. Auch reagieren diese Dienstleister oftmals auf aktuelle Phishing-Trends und berücksichtigen diese in ihren Kampagnen.

Aus dieser Arbeit ergeben sich einige mögliche weitere Forschungsansätze. So könnte untersucht werden, ob die regelmäßige Durchführung und Auswertung von Phishing-Simulationen einen Einfluss auf deren Erfolgsquote haben. Auch könnte erforscht werden, ob selbst geplante und durchgeführte Phishing-Simulationen einen größeren Erfolg haben als die automatisierten und eher allgemeinen Kampagnen eines Dienstleisters.

Literaturverzeichnis

Ahona, Rudra. 2022. „Warum ist Phishing so effektiv?“ 16. November 2022. https://powerdmarc.com/de/why-is-phishing-so-effective/.

Allianz. 2021. „Allianz Risk Barometer“.

———. 2022. „Allianz Risk Barometer“.

———. 2023. „Allianz Risk Barometer“.

atlasVPN. 2023. „You Are Most Likely to Get Phishing on Mondays“. 7. Juni 2023. https://atlasvpn.com/blog/you-are-most-likely-to-get-a-phishing-email-on-monday.

Badarau, Elena. 2015. „National Electronic Security and Electronics Risk Esimates in Economic Sphere“. 2015. https://irek.ase.md/xmlui/bitstream/handle/123456789/161/BadarauE-GribinceaA_ec_2015_1.pdf?sequence=1&isAllowed=y.

Brad. 2021. „Domain Squatting And Phishing: Everything You Need To Know - PhishProtection.Com“. 27. Juli 2021. https://www.phishprotection.com/phishing/domain-squatting-and-phishing.

BSI. o. J. „Aktuelle Beispiele für Phishing-Angriffe“. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen 7. August 2023a. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing.html?nn=132224.

———. o. J. „Wie schützt man sich gegen Phishing?“ Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen 7. August 2023b. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing.html?nn=132210.

CISA.gov. 2022. „Implementing Phishing-Resistant MFA“, Oktober.

Cofense. 2020. „10 Signs Of A Phishing Email | Cofense Email Security“. 23. März 2020. https://cofense.com/knowledge-center/signs-of-a-phishing-email/.

Crown. 2017. „phishing_simulations_guide.pdf“. Designing Phishing SImulations. 2017. https://www.npsa.gov.uk/system/files/documents/51/d7/phishing_simulations_guide.pdf.

Engels, Barbara. 2021. „IW-Kurzbericht 54/2021“, August.

Erkkila, Jussi-Pekka. 2011. „Why We Fall for Phishing“.

FACC. 2023. „Firmenwebseite“. 2023. https://www.facc.com/Company.

Halgas, Lukas, Ioannis Agrafiotis, und Jason R. C. Nurse. 2020. „Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)“. In , 11897:219–33. https://doi.org/10.1007/978-3-030-39303-8_17.

Healy, Colm. 2018. „World Cup-Themed Phishing Attacks Multiply“. Corrata. 3. Juli 2018. https://corrata.com/world-cup-themed-phishing-attacks-multiply/.

Hogue, RuthAnn. 2017. „What Is Domain Squatting and What Can You Do about It?“ GoDaddy Blog. 7. November 2017. https://www.godaddy.com/resources/skills/what-is-domain-squatting-and-what-can-you-do-about-it.

Hoxhunt. 2022. „The Guide to Cybersecurity Training Metrics - Hoxhunt“. 2022. https://www.hoxhunt.com/ebooks/the-guide-to-cybersecurity-training-metrics.

IBM. 2022. „Was ist Phishing?“ 2022. https://www.ibm.com/de-de/topics/phishing.

Irwin, Luke. 2023. „The 5 Most Common Types of Phishing Attack“. IT Governance Blog En. 31. Januar 2023. https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack.

Kaspersky. 2022. „Cyber-resilience during a crisis | Kaspersky official blog“. 2022. https://www.kaspersky.com/blog/smb-cyber-resilience-report-2022/.

Kellner, Michael. 2021. „Starke Partner für eine sichere Digitalisierung“.

Kladochnyi, Andrii. 2023. „How to Launch a Phishing Attack Using Gophish“. HackenProof Blog. 19. Januar 2023. https://hackenproof.com/blog/for-hackers/gophish-attack.

Lastdrager, Elmer Eh. 2014. „Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature“. *Crime Science* 3 (1): 9. https://doi.org/10.1186/s40163-014-0009-y.

Löher, Jonas, Siegrun Brink, Felix Becker, Annette Icks, Stefan Schneck, und Christian Schröder. 2022. „Digitalisierungsprozesse von KMU im Verarbeitenden Gewerbe - Folgebefragung“, Februar.

Lok. 2022. „How to Run an Effective Phishing Simulation?“ 28. Oktober 2022. https://blog.usecure.io/how-to-run-an-effective-phishing-test.

McNeal, Amy. 2022. „What Is the Goal Behind Phishing Emails?“ Graphus. 16. Dezember 2022. https://www.graphus.ai/blog/what-is-the-goal-behind-phishing-emails/.

Microsoft. 2021. „What Is Business Email Compromise (BEC)? | Microsoft Security“. 2021. https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec.

———. o. J. „What is typosquatting? - Microsoft Support“. Zugegriffen 9. August 2023. https://support.microsoft.com/en-gb/topic/what-is-typosquatting-54a18872-8459-4d47-b3e3-d84d9a362eb0.

mmannika. 2021. „Sicherheit darf kein Hindernis sein – Was ist ‚Usable Security & Privacy‘?“ *isits* (blog). 1. Juni 2021. https://www.is-its.org/it-security-blog/sicherheit-darf-kein-hindernis-sein-was-ist-usable-security-und-privacy.

mohdshariq. 2021. „Zphisher - Automated Phishing Tool in Kali Linux“. *GeeksforGeeks* (blog). 21. Mai 2021. https://www.geeksforgeeks.org/zphisher-automated-phishing-tool-in-kali-linux/.

Mudiraj, Nakkala Srinivas. 2019. „Detecting Phishing Using Machine Learning“. *International Journal of Trend in Scientific Research and Development* Volume-3 (Issue-4): 488–90. https://doi.org/10.31142/ijtsrd23755.

Proofpoint. 2022. „Was ist Business E-Mail Compromise (BEC)? | Proofpoint DE“. Proofpoint. 2. April 2022. https://www.proofpoint.com/de/threat-reference/business-email-compromise.

Rekouche, Koceilah. 2011. „Early Phishing“. arXiv. https://doi.org/10.48550/arXiv.1106.4692.

RSA. 2023. „Why Companies Should Use Phishing Simulations“. RSA Conference. 13. Juni 2023. http://www.rsaconference.com/library/blog/why-companies-should-use-phishing-simulations.

Siadati, Hossein, Sean Palka, Avi Siegel, und Damon McCoy. 2017. „Measuring the Effectiveness of Embedded Phishing Exercises“.

Sjouwerman, Stu. 2022. „What Is The Top Phishing Day Of The Week? And Why?“ 2022. https://blog.knowbe4.com/bid/252400/what-is-the-top-phishing-day-of-the-week-and-why.

———. 2023. „Q1 2023 Top-Clicked Phishing Report [INFOGRAPHIC]“. 9. Mai 2023. https://blog.knowbe4.com/q1-2023-top-clicked-phishing.

SoSafe. 2023. „SoSafe Human Risk Review 2023“.

Stahl, Tobias. 2023. „Die kreativsten Phishing- und Spam-E-Mail Beispiele 2023“. 31. Mai 2023. https://www.getresponse.com/de/blog/phishing-und-spam-email-beispiele.

Stewart, James Michael. 2018. „The Three Types of Multi-Factor Authentication(MFA)“. 26. Juni 2018. http://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/.

Team, ZeroFox. 2021. „How to Protect Against Domain Squatting“. ZeroFox. 21. Dezember 2021. https://www.zerofox.com/blog/protect-against-domain-squatting/.

TrendMicro. 2016. „Austrian Aeronautics Company Loses Over €42 Million to BEC Scam - Security News“. 26. Mai 2016. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/austrian-aeronautics-company-loses-42m-to-bec-scam.

Uebelacker, Sven, und Susanne Quiel. 2014. „The Social Engineering Personality Framework“. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 24–30. Vienna: IEEE. https://doi.org/10.1109/STAST.2014.12.

Webster, Merriam. 2023. „Definition of PHISHING“. 20. Juli 2023. https://www.merriam-webster.com/dictionary/phishing.

Wirtschaftskammer Österreich. 2023. „Erneut Phishing Mails im Namen der WKO im Umlauf“. 3. April 2023. https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/erneut-phishing-mails-im-namen-wko.html.

Zorz, Zeljka. 2021. „SniperPhish: An All-in-One Open-Source Phishing Toolkit“. *Help Net Security* (blog). 26. April 2021. https://www.helpnetsecurity.com/2021/04/26/sniperphish-phishing-toolkit/.

Abbildungsverzeichnis

Tabellenverzeichnis