Dirk Fox, Christian Titze

Phishing Awareness durch Gamification

Awareness-Kampagnen erfordern nicht nur eine differenzierte Zieldefinition, sondern auch eine aus dieser abgeleitete präzise Festlegung der zu vermittelnden Inhalte und die Konzeption eines geeigneten Trainings. Dabei kann der Einsatz moderner Vermittlungsmethoden wie „Gamification" und „Storytelling" helfen, die Akzeptanz und Attraktivität der Sensibilisierungsmaßnahmen deutlich zu erhöhen und so einen großen Teil der Belegschaft für die aktive Mitwirkung zu gewinnen. Dies wird am Beispiel einer Phishing-Awareness-Kampagne vorgestellt.

1 Hintergrund

Seit Anfang der 2000er Jahre ist die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in der IT- und Informationssicherheit ein Thema. Mit der Aufnahme in wichtige Informationssicherheitsmanagement-Standards wie den ISO 27002 (Überwachungsbereich „Human Ressource Security") und den BSI-Standard 200-2 ist die Mitarbeitersensibilisierung mittlerweile zudem wichtiger Prüfgegenstand bei Zertifizierungen. Bei der Umsetzung dieser Anforderung kommen je nach Unternehmensgröße, Branche und Budget jedoch sehr unterschiedliche Methoden und Medien zum Einsatz.

Nicht immer wird bei einer Awareness-Kampagne zunächst die Zielsetzung eindeutig definiert. Oft werden Maßnahmen, Methoden und Medien so „zusammengemischt", dass ein klarer inhaltlicher Fokus der Kampagne – wenn überhaupt – nur schwer zu erkennen ist. Viele Empfehlungen zur Durchführung von Awareness-Kampagnen verstärken diesen Trend, indem sie sich auf das organisatorische Vorgehen der Kampagne konzentrieren, aber die notwendige inhaltliche Fokussierung auf Kernrisiken und die Verknüpfung mit der übergreifenden Informationssicherheits-Strategie (insbesondere der Risikobewertung) nicht ausreichend berücksichtigen [1].

Dabei sollten die Kernrisiken, die vom Verhalten der Mitarbeiterinnen und Mitarbeiter beeinflusst werden, Inhalte und Methoden jeder Awareness-Maßnahme bestimmen. Natürlich kann man sich auf den Standpunkt stellen, dass jede Sensibilisierung besser ist als gar keine. Aber die Wirksamkeit der getroffenen Maßnahmen – eine in der Praxis ohnehin nur eingeschränkt verlässlich zu bestimmende Größe – lässt sich überhaupt nur dann untersuchen, wenn die intendierte Wirkung zuvor auch klar definiert wurde.

Noch wichtiger aber ist, dass bei Maßnahmen ohne durchdachte und sehr klare Zielsetzung und ohne inhaltlichen Fokus erhebliche „Streueffekte" auftreten: Die Maßnahmen erreichen vorrangig Mitarbeiterinnen und Mitarbeiter, die ohnehin bereits in hohem (oder zumindest ausreichendem) Maße für das Thema IT- und Informationssicherheit sensibilisiert sind, vermitteln Wissen, das den Mitarbeiterinnen und Mitarbeitern schon bekannt ist oder leiten die Aufmerksamkeit der Belegschaft auf Randthemen, die zwar auch wichtig sind, aber gar nicht den Kern der Gefährdungen ausmachen. In vielen Awareness-Kampagnen werden auch viele Inhalte vermittelt, die zwar im Zusammenhang mit IT- und Informationssicherheit interessant und deren Kenntnis bei den fachlich Verantwortlichen erwartet werden darf, die aber für die Mitarbeiterinnen und Mitarbeiter insgesamt bestenfalls von intellektuellem Interesse sind, für die tägliche Arbeit jedoch keinerlei Relevanz besitzen.

Umgekehrt formuliert: Eine möglichst präzise Definition der Zielsetzung verbessert die Auswahl der zu vermittelnden Inhalte und ermöglicht erst eine Bewertung der Eignung einzelner Maßnahmen zur Erreichung der gesetzten Ziele. Damit erfolgt der Einsatz der für die Awareness-Maßnahme investierten Personal- und Finanzmittel in der Regel wesentlich zielgerichteter.

1.1 Security Awareness

Sicherheitsbewusstsein (oder „Security Awareness") umfasst im Kern drei Dimensionen:

- **Haltung**: Die *Einsicht* in die Notwendigkeit sicherheitsbewussten Verhaltens und das *Verständnis* für die Bedeutung des eige-

Dirk Fox

ist Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

Christian Titze , M.Sc.,

ist Security Consultant bei der Secorvo Security Consulting GmbH. Seine Beratungsschwerpunkte liegen in den Bereichen Penetrationstests, Anwendungssicherheit und Security Awareness.
E-Mail: christian.titze@secorvo.de

nen Verhaltens im Zusammenhang mit konkreten Bedrohungen der IT-Sicherheit für die Sicherheit der Organisation bzw. des Unternehmens durch die *Vermeidung* oder *Abwehr* von Sicherheitsvorfällen und der dadurch möglichen Schädigung des Unternehmens oder der Organisation
- **Wissen**: *Kenntnis* aller für die Organisation oder das Unternehmen relevanten konkreten *Gefährdungen* und deren Erscheinungsformen, der *Erkennungsmerkmale*, der möglichen (ggf. auch technischen) *Konsequenzen* bei Eintritt der Gefährdung und des angemessenen Umgangs mit diesen (Vermeidung und Reaktion im Eintrittsfall)
- **Handeln**: *Einüben* des Erkennens und der adäquaten *Reaktion* auf konkrete Gefährdungen und Angriffsformen zur Vermeidung, Abwehr oder Schadensbegrenzung.

1.2 Security-Awareness-Kampagnen

In einer Security-Awareness-Kampagne sollten daher das für die Abwehr konkreter Bedrohungen erforderliche **Wissen vermittelt** und das angemessene **Reagieren praktisch trainiert** werden. Voraussetzung für die Bereitschaft, sich dieses Wissen anzueignen und das Handeln einzuüben, ist jedoch in jedem Fall die **persönliche Haltung** der Mitarbeiterinnen und Mitarbeiter. Diese lässt sich nur indirekt beeinflussen, z. B. durch klare Anforderungen und Regeln, deren Einhaltung auch eingefordert und durchgesetzt wird, und die insbesondere von Führungskräften auch vorgelebt werden.

Daher sind die Rolle und das Verhalten der Führungskräfte in einer Awareness-Kampagne meist erfolgsentscheidend, denn deren Verhalten ist für die meisten Mitarbeiterinnen und Mitarbeiter maßgeblich und verhaltensprägend. Die Führungskräfte müssen daher frühzeitig über die geplanten Maßnahmen und deren Zielsetzung informiert und möglichst mit einer aktiven Rolle in die Kampagne eingebunden werden. Besonders wirkungsvoll ist es, wenn eine zentrale Führungskraft als „Pate" der Kampagne gewonnen werden kann und diese gegenüber allen Mitarbeiterinnen und Mitarbeitern die Maßnahmen ankündigt und begründet.

Vor jeder Awareness-Kampagne ist zunächst zu betrachten, welchen Bedrohungen das Unternehmen oder die Organisation ausgesetzt ist, die durch ein fehlerhaftes oder unangemessenes Verhalten der Mitarbeiterinnen und Mitarbeiter zu konkreten Schäden führen können. Werden mehrere unterschiedliche Bedrohungsarten identifiziert, dann ist festzulegen, welche dieser Bedrohungen im Fokus der Kampagne stehen sollen. Auch eine Priorisierung der Bedrohungen ist zu empfehlen, damit die Maßnahmen entsprechend ausgestaltet werden können (beispielsweise hinsichtlich der Intensität oder Dauer der Beschäftigung mit dieser Bedrohungen im Rahmen der Kampagne).

Ist der inhaltliche Fokus der Awareness-Kampagne festgelegt, sind das in diesem Zusammenhang relevante Wissen und die konkreten Anforderungen an das Verhalten (oder etwaige Verhaltensänderungen) der Mitarbeiterinnen und Mitarbeiter zu präzisieren. Dabei ist darauf zu achten, dass die Wissensvermittlung sich auf die wesentlichen Inhalte beschränkt: Nur solche Inhalte sind relevant, die für das grundlegende Verständnis der Bedrohung, deren Erkennung sowie ein angemessenes Verhalten der Mitarbeiterinnen und Mitarbeiter erforderlich sind.

Die entscheidende Rolle, das belegen zahlreiche Untersuchungen, spielt jedoch das konkrete Training (siehe z. B. [2]). Kampagnen, die sich auf Schulungsvorträge, Plakate, Informationsbroschüren und Newsletter beschränken, vermitteln bestenfalls das erforderliche Wissen; in ihrer Wirkung bleiben sie deutlich hinter Kampagnen mit Trainingseinheiten zurück.

1.3 Phishing

Unter Phishing verstehen wir Angriffe, mit denen versucht wird, persönliche oder vertrauliche Daten von einer Person zu erhalten oder sie zu einer wie auch immer gearteten, sicherheitskritischen „Transaktion" zu bewegen.

Phishing-Angriffe gehören in die Angriffskategorie des „Social Engineering". Sie sind gewissermaßen „digitale Varianten" des bekannten Enkeltricks: Der Angreifer gibt sich als eine vertrauenswürdige Person aus und versucht, den Adressaten zu einem sicherheitskritischen Verhalten zu verleiten. Meist versendet der Angreifer beim Phishing eine E-Mail, mit der er den Empfänger oder die Empfängerin dazu zu bewegen versucht,
- auf einen mitgeschickten Link zu einer **gefälschten Webseite** zu klicken und auf dieser beispielsweise Zugangsdaten einzugeben,
- eine verlinkte **Schadsoftware** zu starten (bzw. zu installieren) oder
- eine **Transaktion** wie bspw. eine Überweisung auf ein bestimmtes Konto zu veranlassen.

Wie beim Enkeltrick versucht der Angreifer dabei, sein Ziel durch eine möglichst plausible „Geschichte" zu erreichen. Das kann wie beim so genannten „CEO-Fraud" so weit gehen, dass Mitarbeiter aus dem Rechnungswesen mit einer vermeintlich vom Vorstandsvorsitzenden oder Geschäftsführer stammenden E-Mail dazu gebracht werden, große Summen auf ein Auslandskonto zu überweisen.

Dadurch, dass das „Opfer" des Angriffs die Preisgabe der Daten selbst vornimmt oder eine Transaktion willentlich auslöst, lassen sich Mitarbeiterreaktionen auf Phishing-Angriffe meist nicht von „normalem" Verhalten unterscheiden. Daher lassen sie sich kaum durch technische Mittel erkennen und abwehren.[1]

Schutz vor Phishing bietet in den meisten Fällen nur die Erkennung durch den Empfänger und sein angemessenes Verhalten. Daher ist Phishing ein typisches Thema für Awareness-Kampagnen. In den vergangenen Jahren hat das Thema an Bedeutung gewonnen, da Phishing-Angriffe auf Unternehmen erheblich zugenommen haben. Nach einer aktuellen Studie der ENISA vom Oktober 2020 haben Phishing-Angriffe im Jahr 2019 Schäden in Höhe von mindestens 26,2 Mrd. € verursacht [3], und der jüngste Phishing Activity Trends Report der Anti-Phishing-Working-Group (APWG) vom November 2020 berichtet von einer Zunahme der Phishing-Angriffe zwischen August 2019 und August 2020 um mehr als 200%. Inzwischen werden monatlich rund 200.000 Phishing-Websites bekannt [4].

Phishing-Angriffe zielten zu Beginn zunächst auf Online-Banking-Zugänge angelsächsischer Länder und spielten daher einige Jahre im Unternehmensumfeld und insbesondere in Deutsch-

1 Sperrungen von Webseiten in Browsern, die unter „Phishing-Verdacht" stehen, greifen in der Regel erst nach einigen Stunden oder Tagen und auch nur dann, wenn der Betreiber der betroffenen Webseite (bspw. ein Online-Shop) solche Sperrungen veranlasst. Rechtzeitig erkannt werden sie häufig nur dann, wenn es sich um Massen-Phishing-Angriffe handelt; die sind jedoch meist vom Empfänger ohnehin leichter als gezielte Phishing-Angriffe (sog. „Spear Phishing") zu erkennen.

land keine nennenswerte Rolle. Sie waren hier zudem in der Regel leicht an der englischen Sprache oder an Fehlern im Text (Rechtschreibung, Wortwahl etc.) als Fälschung zu erkennen.

Inzwischen sind nicht nur die Erscheinungsformen von Phishing-Angriffen vielfältiger geworden, sondern es ist eine zunehmende Professionalisierung der Angreifer bzw. der Konstruktion der „Geschichten" hinter den Angriffen zu beobachten. Daher müssen heute alle Mitarbeiterinnen und Mitarbeiter eines Unternehmens oder einer Organisation damit rechnen, Adressat eines solchen Angriffs zu werden. Die Bedrohung durch Phishing ist inzwischen sehr ernst zu nehmen.

Den Angreifern spielt dabei in die Hände, dass über viele Unternehmen inzwischen zahlreiche Informationen, wie z. B. die Namen und Telefonnummern von Ansprechpartnern, im Internet oder in Social Networks zugänglich sind. Mit solchen Informationen lassen sich gezielte Phishing-E-Mails vertrauenswürdig gestalten.

Dabei wirkt sich erschwerend aus, dass – speziell in Deutschland – grammatikalische oder orthografische Fehler zum „gefühlten Erkennungsmerkmal" von Phishing-E-Mails geworden sind. Denn sprachliche Fehler sind kein generisches Merkmal einer Phishing-E-Mail: Ein Angreifer, der eine sprachlich einwandfreie Phishing-E-Mail versendet, hat daher eine große Chance, dass diese von deutschen Empfängern nicht auf Anhieb als Phishing-E-Mail eingeordnet wird.

Wer ein Unternehmen oder eine Organisation also gegen erfolgreiche Phishing-Angriffe wappnen möchte, muss die Mitarbeiterinnen und Mitarbeiter daher befähigen, auch in korrektem Deutsch verfasste Phishing-E-Mails äußerst plausiblen Inhalts zu erkennen. Dazu ist neben dem grundsätzlichen Verständnis vor allem ein intensives Training erforderlich.

2 Konzeption einer Phishing-Awareness-Kampagne

2.1 Zielsetzung

Eine Security-Awareness-Kampagne mit dem inhaltlichen Fokus auf Phishing-Angriffe muss das Ziel verfolgen,

- die **Erkennungsrate** eingehender Phishing-E-Mails bei den Mitarbeiterinnen und Mitarbeitern so zu steigern, dass die „**Klickrate**" auf in Phishing-E-Mails angegebene Links gegen Null geht,
- die **Melderate** bei erkannten Phishing-E-Mails nahe 100% zu steigern, damit im Falle konzertierter Phishing-Angriffe unverzüglich Gegenmaßnahmen zur Schadensbegrenzung (wie die Warnung aller Mitarbeiterinnen und Mitarbeiter oder die Sperrung von Domänen an der Firewall) ergriffen werden können, und
- die Mitarbeiterinnen und Mitarbeiter dazu zu bringen, dass sie, wenn sie sich unsicher sind, ob es sich bei einer E-Mail um Phishing handelt, sich bei internen Experten **rückversichern**, bevor sie auf die E-Mail reagieren.

Die Fortschritte und Erfolge eines Trainings können durch Messung der Klickrate und der Melderate (Zählung der eingehenden Meldungen) sogar gemessen und bewertet werden.

2.2 Inhalte

Die für das Verständnis der Bedrohung durch Phishing-E-Mails, eine hohe Erkennungsrate und die richtige Reaktion erforderlichen Inhalte sollten umfassen:

- das „**Geschäftsmodell**" von Angreifern an Beispielen (Gewinnung von Zugangsdaten, Überweisungen auf Auslandskonten, persönliche Daten, die wiederum Zugänge gewähren können oder deren Kenntnis als Nachweis von Vertrauenswürdigkeit gegenüber Dritten genutzt werden können),
- die **Methoden** der Angreifer (Vortäuschung einer vermeintlichen Vertrauenswürdigkeit im Kontext einer Geschichte, die zu einem üblicherweise als gefährlich bewertetem Verhalten verleitet),
- die **Erkennungsmerkmale** (formale Fehler, aber vor allem die Überprüfung des mitübersandten Links),
- den internen **Meldeweg** (Weiterleitung der E-Mail an ein internes CERT),
- die **Kontaktdaten** interner Experten, die in Zweifelsfällen befragt werden können,
- den **Eskalationsweg**, falls auf eine Phishing-E-Mail reagiert wurde.

Bei der Erläuterung des „Geschäftsmodells" der Angreifer sollten bevorzugt Beispiele aus der Branche der Organisation oder des Unternehmens gewählt werden. Auch Phishing-Angriffe auf Online-Banking, die Mitarbeiterinnen und Mitarbeiter privat betreffen könnten, sind geeignet, die Bedeutung und den Schaden, den erfolgreiche Phishing-Angriffe verursachen, zu veranschaulichen.

Auf die Methoden der Angreifer und die zu vermittelnden Erkennungsmerkmale soll etwas ausführlicher eingegangen werden, da sie im Fokus der inhaltlichen Vermittlung stehen.

Die Methoden der Angreifer

Nur wenige Menschen kämen auf die Idee, auf die direkte Anfrage einer ihnen fremden Person Zugangsdaten zu übermitteln oder Überweisungen auf ein angegebenes Konto zu tätigen. Daher ist Kernelement fast aller Phishing-Angriffe, dass der Angreifer mit einer plausiblen Geschichte versucht, eine „Ausnahmesituation" zu schaffen, in der die „üblichen" Gepflogenheiten nicht mehr gelten oder die es erforderlich machen, von Regeln abzuweichen.

Solche Ausnahmesituationen können beispielsweise sein:

- vorgetäuschte bzw. behauptete „Wartungsarbeiten" der IT, die die Preisgabe von Passwörtern oder den Download und die Aktivierung eines Programms erforderlich machen,
- eine Sonderbonifikation für alle Mitarbeiter oder strukturelle Änderungen im Unternehmen, deren Details erst nach Eingabe der persönlichen Credentials zugänglich sind,
- eine (vermeintliche) System-Fehlermeldung, z. B. aufgrund eines vollen Postfachs, die eine Aktion des Empfängers (wie den Klick auf einen Link zur Vergrößerung der In-Box o. ä.) erfordern,
- die (anscheinend) von einer Führungskraft zur Erledigung weitergeleitete E-Mail eines verärgerten Kunden, der in seiner E-Mail auf ein unter einem Link einsehbares Angebot oder ein anderes Dokument verweist, oder
- der Systemhinweis auf eine „verdächtige Anmeldung" am Konto, die durch Klicken auf einen Link bestätigt oder abgelehnt werden kann.

Allen diesen Fällen ist gemeinsam, dass sie zunächst von einer vertrauenswürdigen Person (Vorgesetzter, Vorstand, Personalabteilung) zu kommen scheinen und eine ungewöhnliche, aber dennoch hinreichend plausible Situation konstruieren, die entweder eine umgehende Reaktion erfordert oder den Empfänger so neugierig machen, dass die mit der Reaktion verbundene Regelverletzung (Preisgabe von Login-Daten, Klick auf einen unbekannten Link) möglicherweise nicht einmal bemerkt wird.

Besonders wichtig ist es daher, die Mitarbeiterinnen und Mitarbeiter dafür zu sensibilisieren, dass (Sicherheits-) Regeln auch im Ausnahmefall gelten und nicht durch Zeitdruck, eine Autorität oder ein „technisches Erfordernis" außer Kraft gesetzt werden dürfen.

Die Erkennungsmerkmale

Dieser inhaltliche Aspekt ist besonders wichtig und die Voraussetzung dafür, dass Mitarbeiterinnen und Mitarbeiter angemessen reagieren. Bei der Vermittlung der Erkennungsmerkmale ist darauf zu achten, dass zwar auf heute typische Indizien, die auf Phishing-E-Mails hinweisen können (wie der Verweis auf vermeintliche Gewinne, eine unbezahlte Rechnung oder Mahnung, die Behauptung einer Notlage, die Erzeugung von Zeitdruck oder der Hinweis auf Autoritäten, ungewöhnliche Uhrzeiten, Fehler in den rechtlichen Angaben oder der Adresse des Absenders), eingegangen wird, es aber vor allem auf das Kernelement einer Phishing-E-Mail ankommt: Den Anhang oder einen Link auf eine externe Webseite, der geöffnet oder ausgeführt bzw. die angeklickt werden soll.

Denn die Zahl der gezielten Phishing-Angriffe mit hoher Glaubwürdigkeit, bei denen z. B. auf eine tatsächlich stattgefundene Korrespondenz Bezug genommen oder Absenderdaten von existierenden oder ehemaligen Kollegen verwendet werden, steigt. Solche E-Mails sind an den bisher „üblichen" Merkmalen (Sprache, Uhrzeit etc.) nicht zu erkennen.

Das einzige, was vor solcherart gezielten Phishing-E-Mails schützt, ist, den angegebenen Link nicht anzuklicken oder einen Anhang nicht zu öffnen. Zwar unterstützen geeignet konfigurierte Office-Programme die Anwender heute bereits durch die Deaktivierung aktiver Elemente in Dokumenten; diese darf aber oft vom Benutzer aufgehoben werden.

Grundsätzlich sollte es auch leicht sein, einen externen Link zu erkennen, wenn man mit dem Aufbau einer URL vertraut ist. Allerdings versuchen Angreifer zunehmend, den in einer Phishing-E-Mail angegebenen Link zu verschleiern. Typische Methoden dafür sind

- die Anzeige eines unverdächtigen, existierenden Domain-Namens in einer HTML-E-Mail mit dahinter verborgenem Link auf die gefälschte Seite,
- die Registrierung der URL mit TLS-Zertifikat, sodass die Seite im Browser nicht als „unsicher" angezeigt wird (inzwischen etwa 80% [4]),
- die Reservierung und Verwendung von Domains, die den Namen der existierenden, vertrauenswürdigen Domäne mitverwenden (wie z. B. „bank-online.com" statt „bank.com"),
- die Verwendung von Domains, die einen regulären Domänennamen als Sub-Domäne beinhalten (wie „bank.de.cn"),
- die Verwendung von Domains, die eine leicht andere und auf den ersten Blick kaum unterscheidbare Schreibweise eines vertrauenswürdigen Domänennamens verwenden (wie „arnazon.de" statt „amazon.de"),
- den Link so lang zu wählen, dass die eigentliche Domäne auch bei einem „Mouseover" oder einer Übernahme des Links in die URL-Zeile des Browsers nicht vollständig angezeigt wird, also für den Benutzer nicht auf den ersten Blick als möglicherweise nicht vertrauenswürdig erkannt werden kann oder
- die Verwendung von Kurz-URLs als Alias, sodass die tatsächliche Domäne für den Empfänger der Phishing-E-Mail gar nicht erkennbar ist.

Im Kern ist dies aber dennoch die entscheidende Schwachstelle eines jeden Phishing-Angriffs: Letztlich muss eine vom Angreifer gefälschte Webseite angeklickt werden. Daher müssen Mitarbeiterinnen und Mitarbeitern vermittelt werden, welche Domänen vertrauenswürdig sind und in welchen Fällen sie misstrauisch werden sollten.

2.3 Voraussetzungen

Eine sehr wichtige generelle Voraussetzung für den Erfolg einer Awareness-Maßnahme ist, dass es definierte Prozesse, Richtlinien oder andere Vorgaben für das richtige Verhalten im Umgang mit einem bestimmten Risiko oder einer konkreten Bedrohung gibt.

So setzt die Sensibilisierung für Phishing-Angriffe voraus, dass es im Unternehmen auch einen Meldeweg für erkannte Phishing-Angriffe gibt, wie beispielsweise ein internes, leicht zu merkendes E-Mail-Postfach (phishing@...). Für Zweifelsfälle muss es intern eine verantwortliche Stelle geben, die zumindest zu den üblichen Bürozeiten bevorzugt telefonisch, aber auch per E-Mail erreichbar ist und Fragen zu möglichen Phishing-E-Mails beantwortet.

Außerdem sollte es im Intranet einen hervorgehobenen Bereich geben, in dem Warnmeldungen z. B. vor entdeckten aktuellen Phishing-Angriffen veröffentlicht werden, die von allen Mitarbeiterinnen und Mitarbeitern wahrgenommen und leicht gefunden werden. Schließlich benötigt das Unternehmen oder die Organisation für die Eskalation im Fall des Verdachts auf einen möglicherweise erfolgreichen Phishing-Angriff eine Hotline oder ein Postfach, über das möglichst rund um die Uhr eine Alarmierung erfolgen kann, auf die sofort reagiert wird.

Wenn diese Voraussetzungen nicht vor Beginn der Kampagne hergestellt werden und daher den Mitarbeiterinnen und Mitarbeitern keine ganz konkreten Handlungsoptionen angeboten und vermittelt werden können, kann die Wirkung der Sensibilisierungs-Maßnahmen vollständig verpuffen.

Außerdem kann eine Phishing-Kampagne zum Anlass genommen werden, die Erkennung von Phishing-E-Mails durch geeignete Konfigurationsänderungen oder Ergänzungen des E-Mail-Systems zu erleichtern. Dazu zählen beispielsweise die farbliche Markierung von externen E-Mails, die Einfügung einer Warnung in der Betreff-Zeile bei aus externen Domänen eingehenden E-Mails oder eine Popup-Warnung beim Aufruf externer Links aus einer E-Mail. Solche technischen Maßnahmen sind aber nur dann wirksam, wenn deren Zweck und die richtige Nutzung allen Mitarbeiterinnen und Mitarbeitern vermittelt werden. Denkbar ist auch im Zusammenhang mit der Kampagne Filterungen im E-Mail-Server einzuführen oder zu verschärfen, z. B. für externe E-Mails mit Anhängen, die aktive Komponenten enthalten können, die das Client-System nicht identifizieren kann (wie bspw. Word-Dokumente in älteren Formaten).

Schließlich ist es von besonderer Bedeutung vor Beginn der Kampagne für *interne* (Massen-)*E-Mails* zu regeln, dass diese kei-

ne Verweise auf externe Webseiten enthalten dürfen. Stattdessen sollten solche Links beispielsweise im Intranet publiziert und via E-Mail lediglich auf die (vertrauenswürdigen) Intranet-Seiten verwiesen werden. Anderenfalls werden die Erfolge der Awareness-Maßnahmen dadurch konterkariert, dass die Mitarbeiterinnen und Mitarbeiter daran gewöhnt werden, bei (vermeintlich) internen E-Mails eben doch auf die angegebenen externen Links zu klicken – und, schlimmstenfalls, auch Credentials darüber einzugeben. Leider werden inzwischen in vielen Unternehmen externe Dienstleister (z. B. für Online-Trainings) über Links in internen E-Mails bekannt gemacht, anstatt den Zugang über einen Link auf einer Intranetseite zu eröffnen.

Schließlich sollten interne Vorlagen keine aktiven Komponenten (wie z. B. Makros) enthalten, die die Nutzer dazu zwingen oder verleiten könnten, die Ausführung aktiver Komponenten im Office-Programm zu aktivieren.

2.4 Gamification als Trainings-Methode

Das zentrale Element bei einer Awareness-Kampagne mit dem Kernthema „Phishing" muss das Training sein. Herausfordernd ist dabei, dass die Mitarbeiterinnen und Mitarbeiter auf Phishing-E-Mails vorbereitet werden müssen, die immer ausgereifter und besser werden – und damit auch immer schwieriger zu erkennen sind.

Aus mehreren Gründen ist es jedoch nicht damit getan, beispielsweise von einem Dienstleister simulierte Phishing-E-Mails an alle Mitarbeiterinnen und Mitarbeiter schicken zu lassen und die entsprechenden Klickraten auszuwerten. Denn eine solche Maßnahme provoziert dreierlei:

- Mitarbeiterinnen und Mitarbeiter, die auf solche simulierten Phishing-E-Mails „hereinfallen", fühlen sich erfahrungsgemäß schnell „vorgeführt" – erst recht, wenn die E-Mails schwer zu erkennen sind. Ein solches (möglicherweise auch noch unangekündigtes) „Abprüfen" wird unterbewusst häufig als „Verrat" des Unternehmens an der Loyalität der Mitarbeiter verstanden und führt zur Ablehnung der Maßnahme.
- Schon die „Androhung" der Aussendung simulierter Phishing-E-Mails kann vor allem bei IT fernen Mitarbeiterinnen und Mitarbeiter Versagensängste auslösen.
- Insbesondere IT affine Mitarbeiterinnen und Mitarbeiter sind oft von ihrer eigenen Befähigung überzeugt, Phishing-E-Mails auf den ersten Blick zu erkennen. Sie neigen daher dazu, schwer zu erkennende simulierte Phishing-E-Mails mit dem Hinweis abzulehnen, dass diese ja nicht „realistisch" sind, da heutige Phishing-E-Mails viel einfacher zu erkennen seien.

Angst, Ablehnung und Verärgerung sind jedoch Reaktionen, die kontraproduktiv für einen wirksamen Lernprozess sind. Das Training sollte daher, um eine möglichst nachhaltige Wirkung zu erzielen, unter Bedingungen stattfinden, die ein Lernen fördern. Dazu zählen insbesondere die Konzentration auf den Lerngegenstand, das (vor allem emotionale) Wohlbefinden der Teilnehmerinnen und Teilnehmer und die Vermittlung wichtiger Grundkenntnisse (z. B. in Gestalt der wichtigsten Erkennungsmerkmale von Phishing-E-Mails) gleich zu Beginn des Trainings.

Das gelingt, wenn das Training in einer „Spielumgebung" erfolgt, die von Hierarchien und Erwartungshaltungen befreit ist. In dieser Umgebung können zusätzliche Lernanreize gesetzt werden wie z. B. das Ausloben von Preisen. Außerdem können die Lerninhalte in eine Geschichte eingebunden werden („Storytelling"), wodurch die Bereitschaft der Mitarbeiterinnen und Mitarbeiter zur „Konsumption" erheblich gesteigert werden kann. Zugleich sollte das Training idealerweise nicht in einer künstlichen Laborumgebung (wie einem Trainingskurs) stattfinden, sondern in derselben Umgebung erfolgen, in der die Mitarbeiterinnen und Mitarbeiter auch tatsächlich auf Phishing-E-Mails treffen: also im Arbeitsalltag und am Arbeitsplatz.

2.5 Das „Planspiel"

Wenn der Arbeitsalltag auf spielerische Weise zur Trainingsumgebung werden soll, bietet sich das Konzept eines Planspiels an: Durch die Simulation eines Phishing-Angriffs auf das gesamte Unternehmen kann das Training spielerisch in den Arbeitsalltag integriert werden.

Das „Setup": Eine Gruppe anonymer Angreifer kündigt z. B. per Video-Botschaft Phishing-Angriffe auf das Unternehmen an. Das Video wird im Intranet des Unternehmens veröffentlicht; daraufhin setzt die Unternehmensleitung zwei (fiktive) Mitarbeiter als Koordinatoren der Abwehr der Angriffe ein.

Diese beiden Mitarbeiter erhalten einen eigenen Intranet-Bereich mit einem Blog, in dem sie den Verlauf der Angriffe und die Erfolge der Abwehr dokumentieren und kommentieren. Ihre Aufgabe ist es, allen Kolleginnen und Kollegen die für die Abwehr des Angriffs erforderlichen Kenntnisse (tatsächliche Gefährdung, Methoden der Angreifer, Erkennungsmerkmale, Melde- und Eskalationswege) zu vermitteln, Tipps und Anregungen aus der Belegschaft aufzugreifen und, vor allem, die eingegangenen Phishing-E-Mails zu veröffentlichen und an diesen anschaulich die jeweiligen Erkennungsmerkmale zu erläutern.

Auch die Einführung technischer Hilfen im Laufe der Kampagne (wie ein „Phishing-Knopf" im E-Mail-Client für die sofortige Meldung einer als Phishing erkannten E-Mail oder ein farbiges „Warn-Banner" zur Markierung von externen E-Mails) sollte über diese beiden Koordinatoren angekündigt und erläutert werden.

Der Auftrag an die Mitarbeiterinnen und Mitarbeiter lautet, jede erkannte Phishing-E-Mail mit Angabe der Erkennungsmerkmale an das (ggf. neu eingerichtete) Postfach phishing@... des internen CERT weiterzuleiten.

Die Anzahl der (simulierten) Phishing-E-Mails, die an jeden Mitarbeiter verschickt wird, sollte auf wenige pro Woche begrenzt werden. Indem die Phishing-E-Mails an zufällige Stichproben der Belegschaft verschickt werden, können dennoch mehrere E-Mails pro Tag verschickt und im Blog ausgewertet werden: Auf diese Weise lernen die Mitarbeiterinnen und Mitarbeiter auch aus E-Mails, die sie selbst nicht erhalten haben.

Wichtig dabei: Werden auf den simulierten Angreifer-Webseiten Credentials abgefragt, sollte die Seite die Eingabe von Passwörtern verhindern: Es genügt, in dem Moment, in dem ein Passwort-Eingabefeld angeklickt wird, z. B. ein Erkennungssymbol der Hackergruppe anzuzeigen.

Mit weiteren Video-Botschaften der Angreifer kann die Kampagne im Verlauf angeheizt oder auch beendet werden.

2.6 Mengenmodell

Bei der Durchführung des Planspiels in einem deutschen Großunternehmen hat es sich gezeigt, dass der Versand von wöchentlich maximal zwei Phishing-E-Mails an jede Mitarbeiterin und

jeden Mitarbeiter ausreicht, um die Trainingsziele zu erreichen. Bewährt hat sich eine Kampagnendauer von rund fünf Wochen, sodass alle Mitarbeiterinnen und Mitarbeiter jeweils acht unterschiedliche Phishing-E-Mails erhielten. Täglich wurden 1-2 von insgesamt 30 simulierten Phishing-E-Mails über knapp fünf Wochen verschickt (in der Summe 120.000 E-Mails an rund 16.000 Mitarbeiterinnen und Mitarbeiter). Unter allen korrekt erkannten und an das CERT-Postfach weitergeleiteten E-Mails wurden je Phishing-E-Mail zehn Preise verlost.

2.7 Erfolgsmessung

Bei der Erfolgsmessung ist zu beachten, dass die Zählung der Klickrate anonym erfolgt. Viele Anbieter arbeiten mit pseudonymen Zählungen; die Klicks lassen sich daher prinzipiell auf einzelne Mitarbeiter zurückführen. Eine solche Zählung macht geeignete datenschutzrechtliche Vereinbarungen und die Mitwirkung des Betriebsrats bei der Ausgestaltung erforderlich – und birgt auch bei korrekter Gestaltung die Gefahr, dass die Mitarbeiterinnen und Mitarbeiter das Verfahren als „Kontrolle" empfinden.

Eine anonyme Zählung der Klickrate hat den Nachteil, dass Mehrfachklicks (beispielsweise um Kollegen die erhaltene simulierte Phishing-E-Mail vorzuführen oder von Mitarbeiterinnen und Mitarbeitern, die damit „experimentieren", um zu versuchen, das „Setting" des Spiels zu verändern) nicht festgestellt werden können, die Zählwerte also möglicherweise bei einzelnen E-Mails zu hoch ausfallen. Da allerdings die Schwankungen von E-Mail zu E-Mail ohnehin erheblich differieren können, sind die absoluten Zahlen ohnehin weniger wichtig als der „Trainingstrend", also der Rückgang der Klickraten insgesamt über den Verlauf des Trainings.

Generell gilt: Die Klickrate ist zwar ein Maß zur Bestimmung des Risikos (wie viele Mitarbeiterinnen und Mitarbeiter würden bei einem echten Phishing-Angriff ihre Credentials preisgeben?), aber es bleibt sehr ungenau, da die Klickrate – wie zu erwarten – in ganz erheblichem Maß davon abhängt, wie überzeugend die simulierte Phishing-E-Mail gestaltet wurde. So konnten im Projektverlauf Werte zwischen unter 5% und über 70% gemessen werden.

In jedem Fall aber ist es nicht zur Darstellung gegenüber den Mitarbeiterinnen und Mitarbeitern geeignet, da es ein negatives Maß ist: Es zeigt den Anteil an unerwünschtem Verhalten. Stattdessen solle bei der Auswertung einer Phishing-Kampagne immer die, im Übrigen auch eindeutig zu bestimmende, Melderate zur Bestimmung des Erfolgs herangezogen werden. Mit über 30.000 Einzelmeldungen wurde jede vierte Phishing-E-Mail nicht nur erkannt, sondern auch korrekt weitergeleitet. Erwartungsgemäß stieg die Melderate im Kampagnenverlauf. Ein leichter Rückgang in der fünften Trainingswoche signalisierte dafür eine beginnende „Ermüdung" der Teilnehmerinnen und Teilnehmer und wurde als Anlass genommen, die Kampagne ausklingen zu lassen.

Schließlich gibt es ein drittes Maß, das in einem Planspiel-Setup ausgewertet werden sollte: die Zugriffszahlen auf die Planspiel-Seiten. Mit rund 5.500 eindeutigen Seitenbesuchern und etwa 45.000 Seitenabrufen war die Seite während des knapp fünfwöchigen Kampagnenverlaufs die meistbesuchte Intranet-Seite des Unternehmens.

3 Fazit

Die Gestaltung einer Phishing-Awareness-Kampagne als Planspiel, in dem das Unternehmen über mehrere Wochen (simulierten) anonymen Angreifern ausgesetzt wird und die Verteidigung (Erkennung von Phishing-E-Mails) von einem Team aus (virtuellen) Mitarbeitern koordiniert wird, hat sich als sehr erfolgreiches Setup erwiesen. Die Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter konnte über einen fünfwöchigen Kampagnenverlauf auf einem konstant sehr hohen Niveau gehalten werden und führte zu einem signifikanten und nachweisbaren Trainingserfolg bei der Erkennung von Phishing-E-Mails.

Entscheidend waren dabei nicht nur der Gamification-Ansatz des Planspiels, sondern auch das „Storytelling"-Konzept der Vermittlung über einen Blog des „Verteidigungs-Teams". Hinzu kamen eine vorausgehende präzise Zieldefinition, die Konzentration auf wesentliche und relevante Vermittlungsinhalte sowie ein systematisch aufeinander aufbauendes Training, in dem die Erkennungsleistung der Mitarbeiterinnen und Mitarbeiter messbar verbessert werden konnte.

Nicht zuletzt wirkte sich die große Aufmerksamkeit, die die Kampagne mit diesem Setup erreichen konnte, auch positiv auf die Wahrnehmung der Informations- und IT-Sicherheit im Unternehmen insgesamt aus.

Literatur

[1] Isabella Santa: *The new users' guide: How to raise information security awareness*. ENISA, 29.11.2020.

[2] Giulio Schembre, Andreas Heinemann: *Zur Wirksamkeit von Security-Awareness-Maßnahmen*. In: P. Schartner, A. Baumann (Hrsg.): D•A•CH Security 2017, S. 13-23.

[3] Marco Barros Lourenço, Louis Marinos: *Phishing – ENISA Thread Landscape*. 20.10.2020

[4] APWG: *Phishing Activity Trends Report: 3rd Quarter 2020*. 24.11.2020.

[5] Werner Degenhardt, Andreas Amann, Jan Koppelmann, Frank Weidemann: *Schlaue Fische*. Awareness-Projekt der Landeshauptstadt Kiel. iX 5/2019, S. 78-83.