Phishing-Kampagnen zur Mitarbeiter-Awareness

Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch

12.05.2020

Autoren:

Prof. Dr. M. Volkamer (KIT, SECUSO, KASTEL)
Prof. Dr. M. A. Sasse (RUB, CASA)
Prof. Dr. F. Boehm (KIT, FIZ)

Phishing-Kampagnen zur Mitarbeiter Awareness

Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch

M. Volkamer, M.A. Sasse, F. Boehm
Version 1.0

Phishing-Angriffe sind kein neues Phänomen, aber sie sind nach wie vor eine große Gefahr für jede Institution (egal ob kleines oder großes, nationales oder internationales Unternehmen, Behörde, Verein oder Forschungseinrichtung)[1]. Phishing-Angriffe werden unterschiedlich definiert. Dem vorliegenden Beitrag liegt eine breite Definition des Phishings zugrunde. So ist nach unserem Verständnis das Ziel von Phishern,

- entweder die (digitale) Identität zu übernehmen, um darüber dem Opfer z. B. unmittelbar zu schaden oder die Identität zu nutzen, um weitere Angriffe durchzuführen,
- oder Schadsoftware zu installieren, um dann beispielsweise im Nachgang die Opfer zu erpressen: Es wird Geld – u.a. in Form von Kryptowährungen – gefordert, um wieder auf die eigenen Daten zugreifen zu können oder es wird gedroht, ansonsten die abgegriffenen, mitunter sensiblen Informationen zu veröffentlichen.

Es genügt, dass ein einzelner Angestellter einer Institution einem Phishing-Angriff Glauben schenkt. Dies kann unmittelbar massiven Schaden bei der Institution verursachen, oder der Angriff bildet den Startpunkt für weitere Angriffe, die massiven Schaden auslösen.

Um die Resistenz der Angestellten und damit einer Institution gegen Phishing-Angriffe zu erheben und/oder zu verbessern, überlegen Institutionen, eine sogenannte Phishing-Kampagne zu starten. Allgemein verstehen wir unter einer Phishing-Kampagne eine Aktivität in einer Institution, bei der Phishing-Nachrichten simuliert und entsprechend an die Angestellten verschickt werden. In diesem Artikel gehen wir auf unterschiedliche Ziele und Ausgestaltungsformen von Phishing-Kampagnen ein sowie auf potentielle Probleme und die Aussagekraft von Phishing-Kampagnen.

Da das Thema Phishing komplizierter ist als es auf den ersten Blick erscheint, gibt dieser Beitrag zunächst einen Überblick über die verschiedenen Facetten (Kapitel 1). In Kapitel 2 werden unterschiedliche Ziele von Phishing-Kampagnen vorgestellt, während Kapitel 3 auf

[1] Z. B. BSI-Lagebericht https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf

unterschiedliche Ausgestaltungsformen eingeht. In Kapitel 4 untersuchen wir Phishing-Kampagnen aus Security-Sicht, rechtlicher Sicht und aus der Perspektive Faktor Mensch (z. B. zur Frage, wie sich Angestellte fühlen, wenn sie Teil einer solchen Kampagne sind, und welche Auswirkungen es auf ihre Selbstwirksamkeit hat). In Kapitel 5 wird abschließend noch auf die Aussagekraft der bei Phishing-Kampagnen erhobenen Daten eingegangen.

1. Verschiedene Formen und Typen von Phishing-Nachrichten

Das Kapitel dient als Grundlage. Es wird definiert welche Angriffsform von Phishing-Nachrichten[2] es gibt.

Phishing-Nachrichten können über ***unterschiedliche Kanäle*** verschickt werden, sei es per E-Mail, über Nachrichten und/oder Posts in Social Media bzw. Social Networks, über Direktnachrichten in Messengers oder als SMS.

Die Inhalte von Phishing-Nachrichten können auf ***unterschiedliche Art gefährlich*** sein. Der Empfänger wird in einer Phishing-Nachricht i.d.R. aufgefordert, eine der folgenden Aktionen durchzuführen:

1. *sensible Daten* wie Zugangsdaten, schützenswerte Dokumente oder Kreditkartendaten *zurückzuschicken* (oder allgemein preiszugeben);
2. *Überweisungen oder Anrufe zu tätigen*, z. B. an vermeintliche Freunde oder Geschäftspartner (im Kontext des sogenannten CEO-Fraud bekannt geworden);
3. *Sicherheitsmaßnahmen abzuschalten oder zu umgehen,* z. B. den Virenschutz oder das Einspielen von Updates zu deaktivieren;
4. *gefährlichen Links zu folgen*, wobei diese Links
    i. entweder zu einer echt aussehenden aber betrügerischen Webseite führen, bei der sensible Daten wie die Anmeldedaten einzugeben sind
    ii. oder zu einer Webseite führen, die versucht, Schadsoftware auf den eigenen Geräten zu installieren und zu verbreiten (in dieser Konstellation kann schon der Klick auf den Link unmittelbar Schaden verursachen);
5. *gefährliche Anhänge zu öffnen*, wobei diese Anhänge Schadsoftware beinhalten oder wiederum gefährliche Links.

Phishing-Nachrichten sind dabei ***unterschiedlich einfach als solche zu erkennen***:

- *Sehr einfach zu erkennende* Phishing-Nachrichten enthalten dabei *massive Rechtschreib- und Grammatikfehler[3] und/oder Fehler in der Darstellung.*
- *Mittelschwer zu erkennende Phishing-Nachrichten* können inhaltlich und in ihrer Darstellung plausibel aussehen, aber von einem unplausiblen Absender kommen (z. B.

[2] Teilweise werden Phishing-Nachrichten auch als Spam bezeichnet. Spam umfasst jede Art von unerwünschten Nachrichten. Entsprechend gehören Phishing-Nachrichten zu Spam-Nachrichten; aber eben auch andere Nachrichten wie unerwünschte Werbung.

[3] Hierbei ist zu beachten, dass Nachrichten, die Rechtschreib- und Grammatikfehler enthalten, nicht zwangsläufig auf eine Phishing Nachricht hinweisen, sondern an den fehlenden Kenntnissen des Absenders liegen können.

Absender-E-Mail-Adresse[4] bzw. Absender-Telefonnummer). Ggf. wird nur der Name des Absenders einer E-Mail angezeigt und die Absender-Adresse ist erst sichtbar, wenn man den Namen mit der Maus berührt.

- *Schwer zu erkennende Phishing-Nachrichten* sind inhaltlich, von ihrer Darstellung und auch vom Absender plausibel. Entsprechend kann die Nachricht je nach Art der durch den Phisher gewünschten Aktion nur noch an der Konto- bzw. Telefonnummer, der URL hinter dem Link oder dem Anhang-Typ erkannt werden. Solche Nachrichten können verschickt werden, weil z. B. echte Nachrichteninhalte von großen Anbietern kopiert werden (sogenanntes Clone-Phishing), die E-Mail-Adresse gespooft (vorgetäuscht) wird, die Anrede entsprechend ersetzt wird und die entsprechende Information ausgetauscht wird.
- *Sehr schwer zu erkennende Phishing-Nachrichten* bilden eine weitere Steigerung im Schwierigkeitsgrad, nämlich wenn der Phisher bereits Zugriff auf einen E-Mail-Account hat und von dort bezugnehmend auf eine aktuelle E-Mail-Kommunikation plausibel klingende Phishing-Nachrichten verschickt. Bei dem E-Mail-Account handelt es sich meist um den einer Person (z. B. einem Kollegen, einer Kollegin oder allgemein eines anderen Angestellten der Institution). Es kann aber auch sein, dass es dem Phisher gelingt, Zugriff auf die E-Mail-Accounts von Diensteanbietern zu bekommen, um von dort die Phishing Nachrichten zu verschicken.

Phishing-Nachrichten gaukeln einen mehr oder weniger glaubhaften Grund vor, warum der Empfänger eine der oben genannten Aktionen durchführen soll. Dabei werden oft psychologische Tricks angewendet, z. B. wird Zeitdruck aufgebaut und/oder Sanktionen bzw. Gewinne angekündigt[5]. Diese haben einen Einfluss darauf, wie einfach die Phishing-Nachricht erkannt werden kann.

Angreifer können ***unterschiedliche Strategien*** verfolgen: Entweder versuchen Sie möglichst viele potentielle Opfer mit der gleichen Nachricht zu erreichen oder richten Ihre Nachricht ganz gezielt an eine konkrete Person:

- Beim *"klassischen" Phishing* schickt der Angreifer die gleiche Nachricht an alle ihm verfügbaren Empfänger (also nicht nur gezielt an eine Institution). Meist erfolgt die Anrede dann in der Form „Sehr geehrte Damen und Herren"/„Liebe Kundin, lieber Kunde". Die Nachricht wird höchstens dann personalisiert, wenn dies automatisiert erfolgen kann, z. B. weil versucht wird aus den Absender-Informationen (wie E-Mail-Adresse) den Namen abzuleiten oder weil neben der E-Mail-Adresse auch die Namen und ggf. das Geschlecht bekannt sind (z. B. weil auch diese Informationen auf Webseiten zur Verfügung stehen und automatisch ausgelesen werden können). Aus Sicht des Angreifers führt dieser Phishing-Angriff auch dann zum Erfolg, wenn nicht alle Empfänger auf die Nachricht reagieren, sondern nur einige wenige es tun, weil diese sich inhaltlich zum Zeitpunkt des Empfangens der Nachricht angesprochen fühlen – z.B. bei einer (Phishing-)Nachricht von Amazon einen Tag nach einer tatsächlichen Bestellung). Beim klassischen Phishing werden vorwiegend Phishing-Nachrichten mit gefährlichen Links und Anhängen verwendet, da diese besser in

[4] Dabei ist es wichtig, die Absender E-Mail-Adresse zu betrachten und nicht den Absender Namen, denn der lässt sich noch einfacher fälschen als die angezeigte Absender E-Mail-Adresse.

[5] Hierbei ist zu beachten, dass Nachrichten, die diese Attribute erfüllen, nicht zwangsläufig auf eine Phishing Nachricht hinweisen, sondern auch in echten Nachrichten vorkommen.

der Masse skalieren. Hierbei werden unterschiedlich einfach bzw. schwer zu erkennende Phishing-Nachrichten verwendet.

- *Spear-Phishing* schließlich ist eine Form von Phishing, bei der die Angreifer gezielt eine Institution oder sogar eine Person angreifen. Hierbei sammeln die Angreifer zunächst Informationen – entweder rein über die im Internet frei verfügbaren Informationen über die Institution (z. B. Kunden, Dienstleister, Kooperationspartner oder Newsletter) bzw. über die Belegschaft oder sogar zusätzlich über Telefonanrufe, weil jemand vor Ort sich weitere Informationen beschafft. Auf der Basis all dieser Informationen werden dann institutionsspezifische Phishing-Nachrichten (z. B. von einem Kunden, Dienstleister oder Kooperationspartner) verfasst. Spear-Phishing ist durch den Bezug zur Institution (und ggf. der eigenen Position und Funktion in der Institution) allgemein deutlich schwerer zu erkennen, als das klassische Phishing.

2. Ziele von Phishing-Kampagnen

Es können verschiedene konkrete Ziele für die Durchführung einer Phishing-Kampagne verfolgt werden. Dazu zählen vor allem die folgenden Ziele:

Ziel 1: Erhebung des ***Ist-Zustands in der Institution*** hinsichtlich der Resistenz gegen Phishing-Angriffe (ggf. inkl. des Meldens von entdeckten Phishing-Angriffen), z. B. um über die so nachgewiesene fehlende Resistenz mehr Budget für das Thema IT-/Informationssicherheit und/oder Datenschutz zu erhalten oder zu zeigen, dass eine entsprechende Security-Awareness-Kampagne und/oder Security-Schulung verpflichtend eingeführt werden sollte.

Ziel 2: Es wird versucht, die Phishing-Nachricht als sogenannten *Teachable Moment* zu nutzen. Hier wird angenommen, dass jemand, der auf eine (simulierte) Phishing Nachricht hereinfällt, unmittelbar danach besonders aufnahmefähig für Security-Awareness-Maßnahmen ist. Dazu bekommt diese Person genau in dem Moment, in dem sie potentiell Opfer geworden wäre, Informationen, wie Phishing-Nachrichten zu erkennen sind und wie diese zu melden sind. Die Informationen erhalten die Angestellten also nicht zu einem beliebigen Zeitpunkt – z. B. wenn die Security-Awareness-Maßnahme in Form einer Präsenzschulung oder eines web-based Trainings angeboten wird –, sondern nachdem man gerade eine (simulierte) Phishing-Nachricht nicht erkannt hat.
Hierbei können zwei Formen der Erhebung unterschieden werden:

a. ganz ohne die Anzahl der Personen zu zählen, die auf die Nachricht hereingefallen sind bzw. eine Nachricht gemeldet haben (also als ***reine Security-Awareness-Maßnahme***), oder
b. mit Erhebung der Anzahl der Personen, die auf die Nachricht hereingefallen sind bzw. eine Nachricht gemeldet haben, um (hoffentlich) zeigen zu können, dass die Kampagne das Schutzniveau der Institution erhöht hat (bzw. über die Zeit erhöht), sprich, um die ***Security-Awareness-Maßnahme zu evaluieren bzw. zu rechtfertigen***.

Ziel 3: **(Wissenschaftliche)** ***Evaluation einer (neu entwickelten) Security-Awareness-Maßnahme im Phishing-Kontext***, **die von der eigentlichen Phishing-Kampagne**

unabhängig[6] ist, und zwar durch Erhebung des Ist-Zustand vor und nach der Awareness Maßnahme. Die Kampagne dient hier ausschließlich dazu, die Maßnahme und nicht die Angestellten zu evaluieren. Entsprechend wäre es hier nicht notwendig, die Kampagne mit allen Angestellten durchzuführen. Dieses Ziel ist derzeit eher eins, das im wissenschaftlichen Kontext verfolgt wird.

Schließlich lässt sich noch ein weiteres, bedenkliches Ziel nennen: Phishing-Kampagnen können auch durchgeführt werden ohne Daten zu erheben, um später vorzugeben, als Institution "etwas" unternommen und vorgesorgt zu haben und im Schadensfall auf die Angestellten bzw. Angehörigen der Institution die Verantwortung abzuwälzen. Da hier das Ziel durch die Durchführung der Kampagne bereits erreicht wird und diese Einstellung als Ganzes sehr bedenklich ist, wird dieses Ziel in diesem Artikel nicht weiter betrachtet.

3. Ausgestaltungsformen von Phishing-Kampagnen

Bei einer Phishing-Kampagne werden unterschiedliche betrügerische Nachrichten über einen bestimmten Zeitraum an die Belegschaft der Institution geschickt. Solche Kampagnen können sehr unterschiedlich ausgestaltet werden. Die verschiedenen Ausgestaltungsformen werden im Folgenden vorgestellt:

Entsprechend der in Kapitel 1 aufgezeigten Facetten eines Phishing-Angriffs, können Phishing-Kampagnen unterschiedliche ***Nachrichtenkanäle***, unterschiedliche ***Arten gefährlicher Inhalte***, unterschiedliche ***Schwierigkeitsgrade von Phishing-Angriffen*** (mit oder ohne Einbindung von psychologischen Tricks) und unterschiedliche ***Strategien von Angreifern*** abdecken. Im Fall, dass hier Spear-Phishing-Angriffe adressiert werden, würde man von einer „Spear-Phishing-Kampagne" sprechen, sonst von einer „Phishing-Kampagne". Außerdem können auch unterschiedliche Arten des ***Inhalts einer Nachricht und des Absendertyps*** (z. B. kommt die Nachricht von einer Person oder Institution) abgedeckt werden. Darüber hinaus können Nachrichten mit oder ohne Bezug zu aktuellen Themen verschickt werden – was wiederum einen Einfluss auf den Schwierigkeitsgrad bei der Erkennung hat[7] [8].

Außerdem kann die Kampagne entweder durch ***institutionsinterne Personen oder durch externe Dritte,*** die von der Institution beauftragt werden, durchgeführt werden. Wenn externe Dritte beauftragt werden, gilt es zu unterscheiden, ob die Nachrichten von intern oder extern verschickt werden.

Phishing-Kampagnen unterscheiden sich hinsichtlich des ***Zeitraums der Durchführung*** und der ***Anzahl der Nachrichten,*** die während dieses Zeitraums (pro Angestelltem) verschickt

[6] Unabhängig meint hier, dass anders als bei dem vorherigen Punkt, die Security Awareness Maßnahme losgelöst von der Kampagne ist, z. B. in Form einer Präsenzschulung, eines Web-Based Trainings oder einfach einer neuen Dienstanweisung hinsichtlich der Meldung von Phishing-Nachrichten.

[7] Burns, Johnson, Caputo: Spear phishing in a barrel: Insights from a targeted phishing campaign. *in* Journal of Organizational Computing and Electronic Commerce 29(1):24-39

[8] Benenson, Gassmann, Landwirth: Unpacking Spear Phishing Susceptibility. Financial Cryptography Workshops 2017: 610-627

werden. Phishing-Kampagnen können so designt sein, dass die gleichen Nachrichten zum gleichen Zeitpunkt an die gesamte Belegschaft oder einen ausgewählten Teil der Belegschaft geschickt werden oder dass diese zwar die gleichen Nachrichten erhalten, dies aber zu unterschiedlichen Zeitpunkten. Denkbar wäre auch, dass jeder in der Belegschaft zu einem anderen Zeitpunkt auch eine andere Nachricht erhält. Wenn in einer Phishing-Kampagne mehrere Nachrichten verschickt werden, dann kann die Reihenfolge entweder zufällig sein, die Kampagne beginnt mit der am schwersten zu erkennenden Nachrichten oder mit der am einfachsten zu erkennenden Nachricht. Außerdem kann eine Phishing Kampagne so aufgebaut sein, dass der Schwierigkeitsgrad der nächsten Nachricht davon abhängt, ob die vorherige Phishing-Nachricht erkannt wurde oder nicht.

Schließlich gibt es verschiedene Möglichkeiten, ***um mit dem durch eine Phishing-Nachricht erzeugten Irrtum*** im Rahmen der Kampagne umzugehen:

- ein Hinweis zur tatsächlichen Situation mit oder ohne Erklärungen. Eine Erklärung kann dabei entweder aufführen, wie man zukünftig vermeiden kann, Phishing-Nachrichten Glauben zu schenken oder woran man hätte erkennen können, dass die aktuelle Nachricht eine Phishing-Nachricht ist;
- eine allgemeine Fehlermeldung, die es so aussehen lässt, als gäbe es ein allgemeines Problem, ohne dass klar wird, dass man auf eine simulierte Phishing-Nachricht reingefallen ist;
- das Opfer merkt nicht, dass es einer Phishing-Nachricht Glauben schenkt, z. B. weil es auf die tatsächliche Webseite weitergeleitet wird.

In den letzten beiden Fällen besteht die Möglichkeit, zu einem späteren Zeitpunkt alle oder die, die der Täuschung unterlegen sind, zu informieren, welche Phishing-Nachrichten verschickt wurden. Auch hier sind weitere Erklärungen denkbar.

Phishing-Kampagnen können ***mehr oder weniger prominent und mehr oder weniger detailliert angekündig***t werden, bis hin zu der Tatsache, dass nicht auszuschließen ist, dass es auch Kontexte gibt, in denen es gar keine Information an die Angestellten der Institution gibt.

Im Fall der *Erhebung* des Ist-Zustands (Ziel 1) und der Evaluation des Teachable Moments (Ziel 2 b) bzw. der Evaluation von (neu entwickelten) Security Awareness Maßnahmen (Ziel 3) ***würden unterschiedliche Werte betrachtet und entsprechend erhoben*** werden. Folgende Werte können betrachtet werden (einzeln oder in Kombination):

- die Anzahl der Personen, die je Phishing-Nachricht die entsprechende unerwünschte Aktion ausführen (z.B. auf den Link klicken/sensible Daten angeben/den Anhang öffnen);
- die Anzahl der Personen, die eine entdeckte Phishing-Nachricht melden/löschen;
- die Anzahl der Personen, die melden, dass sie der Täuschung in einer Phishing-Nachricht zum Opfer gefallen sind, nachdem sie es gemerkt haben;
- die Anzahl der Personen, die sich unsicher sind und nachfragen.

Das ***Reporten*** kann ebenfalls unterschiedlich detailliert erfolgen – u.a. bezogen auf alle Angestellten oder auf einzelne Gruppen, bzw. pro Phishing-Nachricht oder Nachrichtentyp.

4. Probleme und Stolpersteine von Phishing-Kampagnen

Zunächst gehen wir auf Gründe ein, die unabhängig von dem konkreten Ziel der Kampagne gegen die Durchführung einer Phishing-Kampagne sprechen. Dabei ist zu beachten, dass die Durchführung von Phishing-Kampagnen einen Einfluss auf die Vertrauens-/Sicherheits-/Fehlerkultur in der Institution hat, eine Reihe von Sicherheitsproblemen mit sich bringt und nicht einfach mit geltendem Recht vereinbar ist. Auf alle drei Aspekte wird im Folgenden genauer eingegangen.

4.1 Security

Zunächst ein allgemeiner Hinweis: Unterschiedliche Arten von Phishing-Nachrichten lassen sich unterschiedlich gut simulieren. Von den in Kapitel 1 genannten sind solche Phishing-Nachrichten eher schwieriger zu simulieren, die ihre Opfer dazu aufrufen, Überweisungen oder Anrufe zu tätigen sowie solche, die dazu aufrufen, Sicherheitsmaßnahmen abzuschalten oder zu umgehen. Denn die Nachricht selbst kann zwar noch einfach verschickt werden, aber es ist schwierig, nachzuvollziehen, ob jemand die Phishing-Nachricht für valide gehalten hat. Im Fall des Abschaltens der Sicherheitsmaßnahmen wird man aus Sicherheitsgründen von dieser Art der Phishing-Nachricht bei einer Kampagne ganz Abstand nehmen. Entsprechend sollte sich jeder, der in Erwägung zieht, eine solche Kampagne durchzuführen, auch überlegen, ob die in der Kampagne adressierten Phishing-Nachrichten überhaupt das größte Risiko für die Institution darstellen, oder eher die, die gar nicht abgedeckt werden.

Nun zu den Security-Problemen, die Phishing-Kampagnen verursachen:

Eine Reihe von Sicherheitsproblemen kann sich im Rahmen der Durchführung von Phishing-Kampagnen ergeben. Zunächst muss die ***Infrastruktur so konfiguriert sein, dass alle simulierten Phishing-Nachrichten durchgelassen werden*** und z. B. im Fall von E-Mails im Posteingang und nicht im Junk- oder Spam-Ordner landen. Andernfalls verfehlt die Kampagne ihr Ziel. Dies gilt insbesondere, wenn die Nachrichten von extern durch den Anbieter solcher Kampagnen verschickt werden. Eine Reihe von Fragen liegt auf der Hand: Wie soll etwa diese Änderung der Konfiguration erfolgen? Werden zunächst die Nachrichten für jeden Angestellten (wegen der möglichen persönlichen Anrede) festgelegt und dann genau diese gewhitelisted[9]? Oder ist es nur möglich, einzelne Absender zu whitelisten oder einzelne Bezeichnungen von Anhängen bzw. einzelne Domains/URLs[10]? Ist es technisch möglich, vor der eigentlichen

[9] Erfolgt das Whitelisting zu pauschal, dann können Phisher den gleichen Ansatz verfolgen und können sich sicher sein, dass ihre Phishing-Nachrichten beim Empfänger ankommen.

[10] Der Dienstleister für die Kampagne hat meist nur sehr begrenzt Wissen über die Infrastruktur und kann dadurch nur sehr pauschale Maßnahmen für die Möglichmachung der Phishing-Kampagnen vorschlagen. Entsprechend groß ist das Risiko, das Sicherheitsniveau der Security Prüfung allgemein herabzusetzen.

Security Prüfung von Nachrichten das Whitelisting anzuwenden[11]? Soll die Security Prüfung selbst angepasst werden[12]? *Hierbei besteht also die große Gefahr, dass zu offen konfiguriert wird und damit neue Sicherheitsrisiken entstehen, weil wirkliche Phishing-Nachrichten ebenfalls zugestellt werden, insbesondere solche, die die Phishing-Kampagne kopieren.* Entsprechend sinkt das Schutzniveau der Institution stark ab.

Bemerkungen: (1) Durch das Whitelisting wird nicht die Realität abgebildet und es würde folgende Information fehlen: Sind die Nachrichten aus der Phishing-Kampagne solche, die wirklich von den Angestellten erkannt werden müssten, weil die eingesetzte Security-Prüfung diese nicht erkennen würde? Oder sind in der Kampagne vor allem Nachrichten, die ohne Whitelisting nicht bei den Angestellten ankommen würden (was die Aussagekraft der Kampagne komplett in Frage stellt)? (2) Wenn das Argument ist, man verändere die Konfiguration doch gar nicht für die Phishing-Kampagne, dann muss dennoch klar sein, welche der Nachrichten aus der Phishing-Kampagne denn bei welchem Angestellten überhaupt ankam, weil sonst die Aussagekraft der Kampagne auch hierbei fraglich ist. Wenn das Argument weiter ist, dass trotz unveränderter Konfiguration nahezu alle Nachrichten bei den Angestellten ankommen, dann stellt sich die Frage, warum nicht erst einmal zentral die Security-Prüfung aus technischer Sicht verbessert wird, um das Sicherheitsrisiko hierüber massiv zu verringern, statt eine aufwendige Kampagne mit all ihren negativen Folgen durchzuführen. Hier ist es dringend anzuraten, erst einmal die Sicherheit des technischen Schutzes auf ein adäquates Level zu erhöhen, um die Last der Prüfung von Nachrichten bei den Angestellten so gering wie möglich zu halten. (3) Eine Änderung bzw. Absenkung der Security Prüfung könnte gegen Security-Richtlinien von Institutionen verstoßen und zu massiven Problemen bei Security Audits führen.

Darüber hinaus kann die ***Tatsache, dass eine Phishing-Kampagne durchgeführt wird, wiederum als Basis für einen Phishing-Angriff genutzt werden***. Beispielsweise könnte der Phisher sich als Kampagnen-Organisator ausgeben und an alle bekannten E-Mail-Adressen eine Phishing-E-Mail schreiben, die z.B. mit einem Link oder einem Anhang versehen ist, über den man sich dann angeblich über das eigene Abschneiden bei der Kampagne informieren kann. Diese Angriffe sind möglich, auch wenn die Angestellten nicht ausführlich im Vorfeld informiert wurden, da sich die Kampagne im Laufe der Zeit herumsprechen wird. Wenn die Kampagne durch externe Dienstleister durchgeführt wird, nennt der Anbieter die Institution ggf. als Kunde. Entsprechend gilt: Die Information, welche Kunden die Anbieter haben, auf Webseiten zu veröffentlichen, verringert das Schutzniveau für Ihre Institution stark – wobei sich die wenigsten Anbieter solcher Kampagnen dessen bewusst sind …

Bemerkung: Selbst wenn diese Information nicht öffentlich zugängig ist: In dem Moment, in dem ein Großteil der Institutionen solche Kampagnen fahren würden, wäre es für den Phisher einen Versuch wert, entsprechende E-Mails an die Angestellten zu schicken.

[11] Nach der Security Prüfung ist das Whitelisting nicht hilfreich, weil bei angemessenem Sicherheitsniveau der Security Prüfung würden die meisten Nachrichten aus der Phishing Kampagne abgeblockt werden und damit gar kein Risiko für die Institution bzw. die Angestellten darstellen.

[12] Wenn ein externer E-Mail-Dienstleister verwendet wird, ist diese Änderung unter Umständen gar nicht möglich.

Insbesondere für den Fall, dass die Angestellten über die Phishing-Kampagne informiert werden, entstehen die folgenden Security-Probleme:

In diesem Fall entstehen eine Reihe von Sicherheitsproblemen durch die Tatsache, dass sich die simulierten Phishing-Nachrichten für die Angestellten nicht von wirklichen Phishing-Nachrichten unterscheiden lassen. Wenn jemandem diese fehlende Ununterscheidbarkeit nicht bewusst ist, könnte diese Person aus unterschiedlichen Gründen mit einer als Phishing-Nachricht erkannten Nachricht interagieren (z. B. den Anhang öffnen, dem Link folgen, usw.): (1) aus Neugierde, wie die Phishing-Kampagne aufgebaut ist; (2) um mehr über das Thema zu erfahren, um auch schwerer zu entdeckende Phishing-Nachrichten zukünftig als solche identifizieren zu können; (3) um die Kampagne zu boykottieren, weil der Ansatz, die Angestellten "hinter das Licht zu führen", nicht gut geheißen wird. Da nicht ausgeschlossen werden kann, dass im Zeitraum der Kampagne auch wirkliche Phishing-Nachrichten die Angestellten erreichen, wird das ***Schutzniveau weiter herabgesenkt, weil es quasi als Einladung verstanden werden kann, mit Phishing-Nachrichten zu interagieren.*** Dieses Problem wird verschärft, wenn angekündigt wird, dass ein schlechtes Abschneiden bei der Kampagne keine arbeitsrechtlichen Konsequenzen hat. Hier stellt sich zunächst die Frage, wie man verständlich kommuniziert, dass es einerseits keine Konsequenzen hat, andererseits aber dennoch gefordert wird, dass jeder so gut wie möglich Phishing-Nachrichten erkennen und melden soll. Aus der fehlenden Ununterscheidbarkeit von echten und im Rahmen der Kampagne simulierten Phishing-Nachrichten folgt eine weitere Frage: Entfallen damit – während der Laufzeit der Kampagne oder allgemein – arbeitsrechtliche Konsequenzen, wenn mit Phishing-Nachrichten interagiert wird? Dies würde das Schutzniveau der Institution weiter herabsetzen, weil die Angestellten mit keiner unmittelbaren Konsequenz rechnen müssen.

Dieses Problem wird sogar noch verstärkt: Was passiert, wenn Angestellte nach dem Interagieren merken, dass es sich hierbei um einen wirklichen Phishing-Angriff handelt? Wird die Nachricht und/oder die Interaktion mit dieser jetzt noch gemeldet? Oder ist die ***Angst zu groß***, dass man jetzt (grob) fahrlässig gehandelt hat und mit entsprechenden (disziplinarischen) Konsequenzen rechnen muss? ***Das Nicht-Melden würde das Schutzniveau der Institution weiter senken,*** denn gerade das Melden spielt eine wichtige Rolle bei der Reduzierung des Schadens.

Ein weiteres Problem ergibt sich, wenn die fehlende Ununterscheidbarkeit nicht bewusst ist: Jemand könnte sich freuen, dass er eine ***"simulierte" Phishing-Nachricht*** selbst entdeckt hat, diese aber nicht meldet, weil sie ja ***bereits bekannt*** ist und dem Melde- und Rückfragewesen nur unnötig Arbeit generieren würde. ***Wenn es wirklich eine Phishing-Nachricht ist, würde diese nicht gemeldet werden, wodurch das Schutzniveau weiter herabgesenkt wird***, da die Filterregeln der Security Prüfung nicht entsprechend darauf eingestellt werden können oder andere Schutzmaßnahmen veranlasst werden können. Denn gerade das Melden spielt eine wichtige Rolle bei der Reduzierung des Schadens von Phishing-Nachrichten.

Eine weitere Situation in diesem Kontext, die das Schutzniveau herabsetzt, ist die Folgende: Jemand erkennt eine Phishing-Nachricht zunächst nicht und interagiert damit. Dann wird festgestellt, dass das wohl eine Phishing-Nachricht ist. Da aber ***angenommen wird, dass es Teil der Kampagne*** ist, ärgert man sich ggf. kurz, meldet dann aber nicht, weil davon ausgegangen wird, dass die Kampagne die Interaktion nach erfolgtem Irrtum ja bereits dokumentiert hat. Was aber, wenn dies gar keine Phishing-Nachricht war, die Teil der Kampagne ist? ***Auch hier führt ein Nicht-Melden dazu, dass das Schutzniveau herabgesetzt wird.***

Bemerkungen: (1) Es kann versucht werden, dieses Problem zu adressieren, weil im Vorfeld klar auf diese fehlende Ununterscheidbarkeit hingewiesen wird und kommuniziert wird, dass jede Art von Phishing-Nachrichten gemeldet werden muss – egal, wann man sie als solche entlarvt hat oder nicht. Ob eine solche Kommunikation erfolgreich ist oder sogar mehr verwirrt, sei dahingestellt. (2) In jedem Fall ist es vor dem Start einer Phishing-Kampagne wichtig, dass die Melde- und Rückfrageprozesse im Kontext von Phishing-Nachrichten klar geregelt, kommuniziert und im Arbeitsalltag umgesetzt werden. Hierzu zählt, wohin man sich wendet, wenn man bei einer Nachricht unsicher ist, wie man mit selbst erkannten Phishing-Nachrichten umgehen soll und wie man sich verhalten soll, wenn man doch auf eine Phishing-Nachricht hereingefallen ist.

Im Folgenden wird auch angenommen, dass Melde- und Rückfrageprozesse etabliert sind und im Vorfeld der Kampagne klar kommuniziert wurde, dass simulierte Phishing-Nachrichten sich nicht von Phishing-Nachrichten unterscheiden lassen und daher der Melde- und Rückfrageprozess immer anzuwenden ist.

Wenn die Melde- und Rückfrageprozesse richtig aufgesetzt und von den Angestellten richtig verstanden sind, dann wird eine Phishing-Kampagne dazu führen, dass mehr Meldungen getätigt werden und mehr Rückfragen gestellt werden. Außerdem werden die Situationen komplexer, denn (a) kann es nun Rückmeldungen zu simulierten und wirklichen Phishing-Nachrichten geben, (b) können rechtzeitig erkannte simulierte und wirkliche Phishing-Nachrichten gemeldet werden und (c) kann es Meldungen dazu geben, dass jemand auf einer simulierten und wirklichen Phishing-Nachricht aufgesessen ist. Entsprechend werden sich die Vorgaben zum Umgang erweitern. Je nach Ziel, welches mit der Phishing-Kampagne verfolgt wird, kommen Dokumentationsaufgaben hinzu. Wenn das Personal hinter dem Melde- und Rückfrageprozess nicht aufgestockt wird, bleibt in der Folge für jede Frage und jede Meldung weniger Zeit, damit auch für die Fragen und Meldungen echter Phishing-Nachrichten[13]. Dies führt bei Fragen zu längerer Wartezeit, was wiederum das Risiko erhöht, dass in der Zwischenzeit der Fragende doch mit der Nachricht agiert oder das Warten einen negativen Einfluss auf die Stimmung hat bzw. eine zweite Nachricht nicht mehr gemeldet wird, weil man ja bereits auf die letzte schon keine Reaktion erhalten hat. Dies führt beim Melden dazu, dass auch auf echte Phishing-Nachrichten langsamer reagiert werden kann. ***Insgesamt wird also***

[13] Burns, Johnson, Caputo: Spear phishing in a barrel: Insights from a targeted phishing campaign. *in* Journal of Organizational Computing and Electronic Commerce 29(1):24-39

auch hierdurch das Schutzniveau reduziert, weil das Melde- und Rückfragewesen dies nicht genauso gut stemmen kann wie ohne die zusätzlichen Phishing-Kampagne-Nachrichten.

Bemerkungen: (1) Natürlich kann versucht werden, das Problem zu lösen, wenn das Melde- und Rückfragewesen für die Zeit personell aufgestockt wird. Aber hierauf gehen die wenigsten Anbieter von Phishing-Kampagnen ein. Dies ist aber notwendig, da sonst ggf. die Kampagne abgebrochen werden muss, weil das Melde- und Rückfragewesen dies nicht stemmen kann. (2) Das erhöhte Aufkommen von Rückfragen wird auch dann auftreten, wenn es keine klaren Melde- und Rückfrageprozesse gibt, weil einfach Unsicherheit vorherrschen wird, wie man mit diesen Nachrichten und/oder Vorfällen umgehen soll.

Im Fall von Ziel 2 b (Nachweis, dass die Kombination aus Phishing-Kampagne und nachgelagerter Security Awarenessmaßnahme einen Effekt hat).

Damit genau der Effekt der Phishing-Kampagne gemessen werden kann, dürfen keine parallelen Security Awarenessmaßnahmen den Angestellten zur Verfügung gestellt werden. Im Fall, dass die Phishing-Kampagne ihr Ziel verfehlt, haben Sie auch Zeit verloren andere Security-Awarenessmaßnahmen anzuwenden. Damit das Ziel erreicht werden kann, sollte die Kampagne möglichst lange andauern, wenn nicht sogar dauerhaft laufen (die Angestellten werden immer wieder daran erinnert). Dies würde aber gleichzeitig das Schutzniveau dauerhaft herabsetzen.

Der Schwierigkeitsgrad der simulierten Phishing-Nachrichten kann ebenfalls einen negativen Einfluss auf die Sicherheit haben. Werden eher einfach zu erkennende verschickt, die man z. B. an der Sprache, dem Absender oder dem Datentyp des Anhangs erkennt, dann können Angestellte schnell davon ausgehen, dass sie nun wissen, wie man Phishing erkennt, aber dann die wirklich gut gemachten Nachrichten übersehen, weil sie gar nicht wissen, wie sie diese erkennen, weil in der Kampagne ja immer nur einfach zu erkennende genutzt wurden.

Zusammenfassend kann festgehalten werden, dass Phishing-Kampagnen das Schutzniveau der Institution während der Durchführung dieser Kampagnen massiv herabsetzen, insbesondere dann,

- wenn die Nachrichten von extern verschickt werden,
- wenn die Security Prüfung angepasst wird (und damit herabgesetzt wird),
- wenn keine klaren Melde- und Rückfrageprozesse in der Institution vorhanden sind,
- wenn die Phishing-Kampagne und die damit verbundenen Aufgaben und Erwartungen an die Angestellten nicht klar kommuniziert werden und
- wenn das Melde- und Rückfragewesen nicht entsprechend auf die Zusatzbelastung durch die Kampagne vorbereitet wird.

Es geht also um deutlich mehr als die Beauftragung eines Dritten, eine Kampagne durchzuführen bzw. einen eigenen Dienst aufzusetzen, um intern Phishing-Nachrichten zu verschicken.

Hinzu kommt, dass Phisher genau die Tatsache, dass Phishing-Kampagnen gefahren werden, nutzen können, um gezielte wirkliche Angriffe zu fahren.

4.2 Recht

Arbeitnehmerschutz und Datenschutz

Meistens (bei Ziel 1 und 2 b) aus Kapitel 3) geht es bei einer Phishing-Kampagne darum, eine Arbeitsleistung zu messen. Hieraus ergeben sich zunächst rechtliche Fragestellungen im Kontext des Arbeitnehmerschutzes und des Datenschutzes:

Aus rechtlicher Sicht ist es zunächst wichtig, dass Arbeitnehmer für schlechte Ergebnisse nicht sanktioniert werden. Ihnen sollen aus einem schlechten "Test"-Ergebnis also ***keine arbeitsrechtlichen Konsequenzen*** drohen. In diesem Zusammenhang stellt sich die Frage, wie kommuniziert wird, dass das eigene Test-Ergebnis keine arbeitsrechtlichen Konsequenzen zur Folge hat. Die Art der Kommunikation hängt eng mit dem in Kapitel 4.1 beschriebenen Problem der "Einladung", mit Phishing-Nachrichten zu interagieren, zusammen. ***Wie kann verständlich kommuniziert werden, dass es einerseits keine Konsequenzen hat, andererseits aber gefordert wird, dass jeder so gut wie möglich Phishing-Nachrichten erkennen und melden soll?*** Auch sollte geklärt sein, ob das Interagieren mit Phishing-Nachrichten außerhalb der Kampagne arbeitsrechtliche Konsequenzen hat und welche dies möglichweise sein könnten.

Um generell zu verhindern, dass die erhobenen Daten missbraucht werden und um die Sanktionsfreiheit zu gewährleisten, müssen ***Zugriffe des Arbeitgebers oder Dritter auf die Ergebnisse einzelner unterbunden werden***. Idealerweise würde dies durch eine vollständige Anonymisierung der Ergebnisse geschehen. Vollständig bedeutet hierbei, dass auch eine Zuordnung zu einzelnen Abteilungen oder Teams nicht möglich ist. Würden die Ergebnisse nicht vollständig anonymisiert, wären diejenigen Abteilungen bzw. Teams besonders exponiert, die insgesamt schlecht abschneiden, weil sie (a) im Sinne der Leistungskontrolle schlecht abschneiden und (b) weil diejenigen, die innerhalb des Teams besser als der Durchschnitt des Teams abgeschnitten haben, trotzdem eine schlechte Bewertung erhalten, da das Gesamtergebnis des Teams schlecht ist. Wie diese Anonymisierungsprozesse so zu gestalten sind, dass der Anbieter der Phishing-Kampagne zwar die Kontaktdaten aller Angestellten kennt und weiß, wem und wann welche Nachricht geschickt wurde, dass es ihm gleichzeitig aber nicht möglich ist, die Ergebnisse einzelnen Angestellten zuzuordnen, muss im Einzelfall genau geprüft werden. Durch die Bereitstellung der Kontaktdaten ist dies nicht trivial zu erreichen, sondern muss von demjenigen, der die Ergebnisse sammelt, erläutert werden. ***Eine vollständige Anonymisierung hätte allerdings den Nachteil, dass z. B. die Ergebnisse pro***

Person über den Zeitraum der Durchführung nicht miteinander in Beziehung gesetzt werden können, wodurch die Aussagekraft der Kampagne herabgesetzt wird.

Bemerkungen: (1) Prinzipiell wäre es denkbar, zur Erhöhung der Aussagekraft eine Pseudonymisierung statt einer Anonymisierung zu verwenden. Dann müsste aber gut begründet werden, warum dies notwendig ist und wie gewährleistet wird, dass der Link zw. Pseudonym und wirklicher Identität nicht hergestellt werden kann. Ob einzelne Vorschläge hierzu rechtlich vertretbar sind, wäre im Einzelfall zu beurteilen. (2) Darüber hinaus empfiehlt es sich, allgemeine Grundsätze der Datenverarbeitung sowie des Persönlichkeitsschutzes aufzustellen. In diesem Zusammenhang ist darauf einzugehen, welche Daten erhoben bzw. nicht erhoben werden. Insbesondere sollte darauf hingewiesen werden, dass die Gestaltung des Tests keine Rückschlüsse auf private Belange oder Interessen der betroffenen Arbeitnehmer zulässt. Außerdem ist in der Vereinbarung festzulegen, durch wen die Daten verarbeitet werden, welche technischen Sicherheitsvorkehrungen dort getroffen werden und wie lange die Daten gespeichert werden. Verträge sind im Fall eines externen Anbieters als Datenverarbeiter zwingend notwendig.

Spätestens wenn die Datenerhebung nur pseudonymisiert ist, ist ***die Beschäftigtenvertretung (Betriebs- oder Personalrat) aufgrund ihres Mitbestimmungsrechts*** zu beteiligen[14.] Auch bei reinen Schulungszwecken (Ziel 2 a) aus Kapitel 3) ist hinsichtlich der Modalitäten der Durchführung von Schulungen nach 98 Abs. 1 BetrVG der Betriebsrat mit einzubeziehen, entsprechende Regelungen existieren für Personalräte in den Landespersonalvertretungsgesetzten der Bundesländer. Betriebs- bzw. Personalrat sind u.a. bei der Festlegung des Zeitraums und der Auswahl der betroffenen Arbeitnehmer sowie im Hinblick auf die inhaltliche Festlegung und Ausgestaltung der Beurteilungsmerkmale zu beteiligen. Wichtig ist, dass die Einbindung rechtzeitig erfolgt, damit diese Gremien ausreichend Zeit haben, sich mit der Komplexität solcher Phishing-Kampagnen und den verschiedenen Auswirkungen auf Arbeitnehmer zu befassen.

Eine ***datenschutzrechtliche Einwilligung*** der Arbeitnehmer/Betroffenen könnte in Betracht gezogen werden. Allerdings wären diese dann unmittelbar und umfangreich über die Vorgehensweise unterrichtet. ***Dies würde sich zwar ggf. positiv auf das Vertrauensverhältnis auswirken (Kapitel 4.3). Allerdings wäre die Aussagekraft (Kapitel 5) der Phishing-Kampagne damit maximal in Frage gestellt und das Testergebnis wäre nur eingeschränkt nutzbar***. Hinzu kommen praktische Durchführungsprobleme, da Einwilligungen jederzeit widerrufen werden können.

Gem. Art. 88 Abs. 1 DS-GVO können auch Regelungen in Kollektivvereinbarungen, worunter nach Erwägungsgrund 155 auch Dienst-/Betriebsvereinbarungen fallen, zur Verarbeitung von personenbezogenen Beschäftigtendaten getroffen werden. Diese Norm des EU-Rechts ist durch § 26 Abs. 4 u. 1 BDSG ausgestaltet. Danach können ***Kollektivvereinbarungen grundsätzlich***

[14] Boehm/Hey/Ortner,"How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace", in European Journal of Law and Technology, Vol 7, No 1, 2016.

die Einwilligung der Arbeitnehmer/Betroffenen ersetzen bzw. eine taugliche Rechtsgrundlage darstellen. Diese dürfen allerdings das allgemeine Datenschutzniveau nicht wesentlich senken[15] und müssen in sich erforderlich und auch verhältnismäßig sein. Für öffentliche Stellen gelten die Landesdatenschutzgesetze, die ähnliche Regelungen vorsehen, allerdings in den Ländern unterschiedlich ausgestaltet sind. So benennt das LDSG-BW im Dienst- und Arbeitsverhältnis auch Kollektivvereinbarungen als Rechtsgrundlage; parallel erlaubt die Norm auch Datenverarbeitungen, die „zur Durchführung innerdienstlich planerischer, organisatorischer, personeller [oder] sozialer […] Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes“ erforderlich sind.[16] Das Berliner Datenschutzgesetz verweist hingegen auf die Regelung im BDSG.[17] Eine ausführliche Abwägung mit den Datenschutzinteressen der Angestellten ist in allen Fällen vorzunehmen.

In Bezug auf die Mitbestimmungsrechte genügt prinzipiell (in einfach gelagerten Fällen) eine formlose Absprache. Vorzugswürdig ist aber eine schriftliche ***Betriebsvereinbarung*** zwischen Arbeitgeber und dem Betriebsrat bzw. eine ***Dienstvereinbarung*** zwischen Arbeitgeber und Personalrat. ***Diese gewährleistet mehr Rechtssicherheit[18] und kann gleichzeitig als datenschutzrechtliche Erlaubnisnorm dienen***. Die Betriebs-/Dienstvereinbarung sollte inhaltlich klar formuliert sein und alle wesentlichen Phasen der Durchführung, eine Zusammenstellung der erhobenen Daten (inkl. des jeweiligen Zwecks i.S.d. DSGVO) und des Auswertungsverfahrens abdecken. Dabei sind die Bewertungskriterien ausdrücklich zu benennen. Entsprechend ist eine Information der Angestellten mindestens in Form der Verteilung der Betriebs-/Dienstvereinbarung erst einmal erforderlich. ***Während die Informationen aus den Betriebs-/Dienstvereinbarung dazu beitragen können, einzelne Security-Probleme aus dem vorherigen Kapitel zu adressieren, können die Informationen einen erheblichen Einfluss auf die externe Validität der Ergebnisse der Kampagne haben (siehe hierzu auch Kapitel 5).***

Unter der Annahme, dass die Betriebs-/Dienstvereinbarung rechtlich korrekt umgesetzt wird (aber nicht besonders prominent verteilt wurde, Zwecks Steigerung der Aussagekraft der Kampagne), stellt sich die Frage, wie gut sich eine solche Kampagne im Vorfeld bzw. spätestens, nachdem die erste Welle an Nachrichten verschickt wurde, vor den Angestellten geheim halten lässt. In jedem Fall fordert der Gesetzgeber, dass ***alle getesteten Personen transparent und umfassend aufgeklärt werden, nachdem die Kampagne durchgeführt wurde. Ihnen muss mitgeteilt werden, welche Daten erhoben wurden, zu welchem Zweck dies geschah und wer die verarbeitende Stelle ist. Außerdem sind die Betroffenen über ihre Rechte zu informieren.*** Zu fragen ist, wie sich die Geheimhaltung realisieren lässt, wenn die Kampagne fortlaufend über viele Jahre durchgeführt wird und welche Auswirkung diese Information aus einer ersten Kampagne für eine zweite Kampagne hat bzw. hätte.

---

[15] Umstritten: BeckOK DatenschutzR/Riesenhuber, 31. Ed. 1.2.2020, DS-GVO Art. 88 Rn. 67; *Taeger/Gabel/Zöll, 3. Aufl. 2019, DS-GVO Art. 88 Rn. 17*); Schrey/Kielkowski, "Die datenschutzrechtliche Betriebsvereinbarung in DSGVO und BDSG 2018 - Viel Lärm und Nichts? BB 2018, 629

[16] § 15 LDSG-BW, ähnlich auch: § 18 Abs. 1 S. 1 DSG NRW.

[17] § 18 BlnDSG.

[18] Wybitul, Neue Zeitschrift für Arbeitsrecht (NZA) 2017, 1488 ff. (1493).

Marken- und Urheberrecht

Darüber hinaus können sich rechtliche Grenzen aus dem Markenrecht ergeben. Im Rahmen der Frage, wie die Nachrichten gestaltet werden können und ob Clone-Phishing möglich ist, wenn dazu die Nachrichten inklusive der Logos der Anbieter (z.B. von SAP oder Paypal) verwendet werden sollten, ist klar zu unterscheiden, ob die komplette Kampagne rein unternehmensintern ***in der Infrastruktur der Institution abläuft (oder nicht)***. Unter Umständen muss keine Markenverletzung stattfinden, wenn Kampagnen rein unternehmensintern ablaufen und ohne dass ein eigener Geschäftszweck zum Ausdruck kommt, allerdings müssen dann auch alle ***Phishing-Webseiten nur institutsintern verfügbar sein***. Zusätzlich könnte auch zu fragen sein, ob der Nutzung solcher Logos z. B. nicht unternehmensweite Codes of Conducts entgegenstehen, wenn eine Marke, deren Ruf und das Vertrauen der Arbeitnehmer missbraucht werden. Darüber hinaus könnte – sofern überhaupt eine geistige Schöpfungshöhe bejaht werden kann – der urheberrechtliche Schutz solcher Logos in Betracht gezogen werden. All dies ist zu klären, wenn entsprechende Nachrichten verschickt werden sollen. ***Wenn keine Clone-Phishing-Nachrichten oder keine Nachrichten von bestimmten Anbietern verwendet werden können, dann schränkt diese die die Aussagekraft der Phishing-Kampagne ein, da es nicht möglich ist, die Art von Phishing Nachrichten zu verschicken, die sonst üblich sind.***

Zusammenfassend ist zu sagen, dass Personal- bzw. Betriebsrat in die Gestaltung einer Phishing-Kampagne mit einbezogen werden müssen und je nach Kommunikationskonzept für die Kampagne die entsprechenden Informationen dann bis zum Abschluss der Kampagne Geheimhalten müssen. Abhängig von der Größe der Institution oder der Teams kann eine anonyme Auswertung der Ergebnisse notwendig sein, um sicherzustellen, dass die Ergebnisse nicht einzelnen Arbeitnehmern zugeordnet werden können, bzw. es ist abzuklären, ob eine pseudonymisierte Auswertung arbeits- und datenschutzrechtlich ausreichend ist. Es ist zu klären, ob auf eine vorherige eingehende Information der Angestellten verzichtet werden kann. Dabei wirken sich umfangreiche und prominente platzierte Informationen negativ auf die Aussagekraft der Ergebnisse der Phishing-Kampagne aus. Wenig prominent platzierte Informationen können sich aber negativ auf das Vertrauen in die Institution auswirken und einzelne Security-Probleme verstärken.

Unabhängig davon ist sicherzustellen, dass ein schlechtes Abschneiden keine arbeitsrechtlichen Konsequenzen hat (was sich ggf. negativ auf das Schutzniveau der Institution während der Kampagne auswirken kann). Spätestens nach Beendigung der Kampagne sind die Angestellten umfänglich aufzuklären.

Insbesondere wenn die Kampagne nicht ausschließlich institutionsintern durchgeführt wird, sind außerdem Marken- und Urheberrechte im Fall von simulierten Phishing-Nachrichten von externen Anbietern zu prüfen. Im Fall einer Einschränkung, würden sich dies negativ auf die Aussagekraft der Phishing-Kampagne auswirken.

4.3 Faktor Mensch: Vertrauens- und Fehlerkultur

Security ist beim Endanwender in den meinen Institutionen kein besonders beliebtes Thema: Es gibt alle möglichen Security Policies. Von manchen hat man mal gehört, manche hat man vielleicht auch gelesen. Allerdings ist es fraglich, ob man auch diese richtig verstanden hat. Irgendwie weiß man, dass man sich nicht daran hält, weil sie bei den Arbeitsabläufen stören, gleichzeitig hat man ein schlechtes Gewissen deswegen, weil man sich nicht daran hält, zu wenig nachfragt usw. Eine Phishing-Kampagne trägt aus verschiedenen Gründen nicht zu einem besseren Image von Security in Institutionen bei:

Als Institution greift letztendlich die Leitung der Institution bei einer Phishing-Kampagne Ihre Angestellten an. Insbesondere im Fall, dass die Kampagne intern durchgeführt wird, greifen darüber hinaus die eine Gruppe von Angestellten (tendenziell aus der IT-Abteilung) alle anderen gewissermaßen an (im Worst Case außer der Institutionsleitung …). Je nach Gestaltung der Phishing-Nachrichten greifen sich alle Angestellten quasi auch untereinander an: Es ist i. d. R. für einen Angestellten nicht unterscheidbar, ob die erhaltene Nachricht Teil der Phishing-Kampagne ist, eine wirkliche Phishing-Nachricht ist oder der Kollege/die Kollegin die Nachricht auf Basis einer Nachricht, die er/sie selbst im Rahmen der Kampagne erhalten hat, geschrieben hat. Sobald gerade letztere Möglichkeit sich unter den Angestellten herumgesprochen hat, wird das Misstrauen untereinander steigen und bereits ***schwierige Beziehungen zwischen Angestellten werden weiter verschlechtert***. Dies wiederum führt zu einer verringerten Produktivität und im Worst-Case werden Mediationsgespräche notwendig.

Im Fall, dass die Kampagne ausführlich angekündigt ist, würden mehr Rückfragen gestellt werden an den potentiellen Absender, der im Fall von bereits schwierigen Beziehungen diese ggf. falsch interpretiert und so schneller neue Konflikte entstehen. Im Fall, dass die Kampagne nicht angekündigt wurde, die simulierte Phishing-Nachricht als Phishing-Nachricht erkannt wird und davon ausgegangen wird, dass der Kollege/die Kollegin einen „reinlegen“ möchte, führt zwangsläufig auch zu Konflikten. Entsprechend tragen Phishing-Kampagnen, bei denen auch Nachrichten von anderen Angestellten simuliert werden, ***negativ zum Betriebsklima und damit zur Vertrauenskultur in der Institution*** bei. Es ist naheliegend, dass Kollegen, die auf (schlecht gemachte) Phishing-Nachrichten hereinfallen, hierfür später sogar despektierlich behandelt werden könnten. Auch dies wirkt sich negativ auf das Betriebsklima aus.

Eine Phishing-Kampagne zu starten, ohne die Angestellten vorher entsprechend aufzuklären (d. h. zu erklären wie sie Phishing-Nachrichten erkennen können, wo sie sich melden sollen wenn sie unsicher sind, wie sie mit durch sie erkannten Phishing-Nachrichten umgehen sollten und wo sie sich melden sollen, wenn sie auf eine Phishing-Nachricht reingefallen sind), ist schlicht unfair. Entsprechend trägt eine Phishing-Kampagne ***nicht dazu bei, dass Angestellte Vertrauen in die Leitung der Institution haben,*** was wiederum aber wichtig wäre für die Security Compliance. Das Vertrauen wird insbesondere dann in Frage gestellt, wenn die Kampagne nicht offiziell und ausführlich angekündigt wird. Wenn dann festgestellt wird, dass eine entsprechende Kampagne gerade am Laufen ist, wird sich das schlecht auf die Selbstwirksamkeit auswirken: Die Angestellten merken, dass sie keine Kontrolle über die

Situation haben und reagieren schnell mit Resignation, sprich sie bemühen sich nicht einmal mehr, Phishing Nachrichten zu erkennen.

Wenn die Kampagne nicht offiziell angekündigt wird, aber über den „Flurfunk“ vereinzelt Informationen verteilt wurden, entstehen weitere Probleme, wenn im Vorfeld nicht unabhängig von der Kampagne klar kommuniziert wurde, wie die Melde- und Rückfrageprozesse sind: Angestellte sind sich unsicher, wie sie vorgehen sollen, wenn sie eine Phishing-Nachricht entdeckt haben oder darauf hereingefallen sind. Gilt für die simulierte Phishing der gleiche Meldeprozess? Wieso bekomme ich diese Nachricht und andere nicht? Wer weiß nun, dass ich dem Irrtum unterlegen bin? Was ist die Konsequenz davon? … ***Entsprechend werden Angestellte durch Phishing-Kampagnen verunsichert und fühlen sich kontrolliert. Beides wird sich negativ auf die Fehlerkultur auswirken.*** *Ein weiteres Problem des nicht offiziellen und ausführlichen Ankündigens besteht darin, dass sich dann schnell falsche Informationen verbreiten und die schwer wieder zu korrigieren sind.*

Wenn wirklich versucht werden soll, die Kampagne geheim zu halten, dann müsste das Melde- und Rückfragewesen angehalten werden, simulierte Phishing-Nachrichten genauso im Melde- und Rückfrageprozess zu behandeln. Dies führt nicht nur zu einem hohen Aufwand beim Melde- und Rückfragewesen, sondern bedeutet schlichtweg, dass Kollegen und Kolleginnen belogen werden müssen. Offensichtlich hat dies ***keinen positiven Einfluss auf die Vertrauenskultur zum Melde- und Rückfragewesen.*** Dies kann sich dann sogar wieder negativ auf das Schutzniveau auswirken, wenn die Konsequenz ist, dass man dort allgemein nicht mehr nachfragen möchte oder nichts mehr melden möchte, weil man diese Art des Umgangs nicht wünscht. Entsprechend haben Phishing-Kampagnen auch einen ***negativen Einfluss auf die Fehlerkultur in den Institutionen.***

Wenn die Phishing-Kampagne umfangreich angekündigt wird, werden die Angestellten viel mehr Nachrichten kritisch hinterfragen, sie werden bei dem Absender telefonisch nachfragen. Dies hat nicht nur einen negativen Einfluss auf das Betriebsklima, sondern kostet einfach auch Zeit. Wird den Angestellten im Rahmen der Ankündigung diese Zeit zugesprochen? Oder wird erwartet, dass die eigentliche Arbeit im Laufe der Kampagne genauso effektiv und effizient erledigt wird? Wird die Zeit den Angestellten nicht zugesprochen, wird der ***Druck auf die Angestellten erhöht, was sich ebenfalls negativ auf das Vertrauen in die Leitung der Institution auswirkt.*** Wenn die Zeit eingeräumt wird, dann muss akzeptiert werden, dass die Produktivität sinkt. Gleichzeitig steigt der Aufwand beim Melde- und Rückfragewesen.

Hinzu kommt, dass Angestellte übervorsichtig werden und legitime Nachrichten als Phishing-Nachrichten bewerten und so Aufgaben nicht bearbeiten. Dies führt einerseits zu Missverständnissen bis hin zu einem Schaden, weil z. B. Rechnungen nicht direkt bezahlt werden. Andererseits ist es wichtig, dass das Melde- und Rückfragewesen darauf vorbereitet ist und entsprechend zurückmeldet, wenn eine legitime Nachricht als Phishing-Nachricht von einem Angestellten klassifiziert wird. Falls Phishing-Nachrichten einfach nur gelöscht werden, steigt das Risiko durch übervorsichtiges Verhalten weiter an.

Der Schwierigkeitsgrad der simulierten Phishing-Nachrichten kann ebenfalls einen negativen Einfluss auf die Stimmung haben. Sind diese zu leicht, kann schnell der Eindruck entstehen, die Leitung der Institution denkt, man würde solche offensichtlichen Phishing-Nachrichten nicht als solche erkennen können. Bekommt man vom gleichen Typ Phishing-Nachricht eine zweite (nachdem man auf die erste von diesem Typ hereingefallen ist), entsteht schnell der Eindruck, dass die Leitung der Institution wohl denkt, man hätte es immer noch nicht verstanden. Auch dies wirkt sich ***nicht positiv auf das Vertrauen in die Leitung aus.***

Im Fall von Ziel 2 b (Nachweis, dass die Kombination aus Phishing-Kampagne und nachgelagerter Security Awarenessmaßnahme einen Effekt hat).

Rein aus Sicht der Phishing-Kampagne wäre es hierbei so, dass Angestellte nur an die Informationen aus der Security-Awarenessmaßnahme kommen, wenn sie einen Fehler gemacht haben. Dies führt leicht zu ***Irritationen und Verunsicherung. Es führt dazu, dass man, wenn man mehr wissen möchte (weil man denkt, man weiß nicht genug) mit Phishing-Nachrichten interagiert muss, was man ja wiederum eigentlich nicht tun soll.*** Dies hat eine negative Auswirkung auf die Selbstwirksamkeit der Angestellten[19] und reduziert das Schutzniveau.

Im Fall von Ziel 1 (Ist-Zustand erheben, um dann für eine nachgelagerte Security Awareness-Maßnahme zu motivieren) und Ziel 2 b).

Diese Fälle bringen ein weiteres Problem mit sich: Niemand findet es nett, wenn man auf seine eigenen Schwächen hingewiesen wird. Man fühlt sich danach erst einmal schlecht. Genau das ist es aber, was bei Phishing-Kampagnen passiert, wenn diese so gestaltet sind, dass man früher oder später erfährt, dass man auf Phishing-Nachrichten hereingefallen ist. Insbesondere sehr gut gemachte Phishing-Nachrichten werden mit hoher Wahrscheinlichkeit Opfer finden. Bei all diesen Angestellten ***wird zunächst ein negativer Effekt erzeugt.*** Es ist fraglich, ob und wie anschließend die Bereitschaft steigt, zu erfahren, wie man zukünftig Phishing-Nachrichten erkennen kann, denn es wurde mehrfach gezeigt, dass fehlende Selbstwirksamkeit einen negativen Einfluss auf das Security Verhalten hat[20].

Im Fall von Ziel 2 b gilt es insbesondere auch zu prüfen, ob die “Opfer” nicht vor Schock das Dokument oder die Webseite möglichst schnell schließen, damit keiner merkt, dass sie der Phishing-Nachricht zum Opfer gefallen sind. Entsprechend würden sie gar nicht merken, dass dort auch Informationen, wie man zukünftig Phishing-Nachrichten erkennen kann, hinterlegt sind.

[19] https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[20] https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Zusammenfassend ist zu sagen, dass Phishing-Kampagnen einen negativen Einfluss auf das Betriebsklima, die Vertrauens- und Fehlerkultur haben. Insbesondere das Vertrauensverhältnis zu der Leitung der Institution sowie das Melde- und Rückfragewesen wird verschlechtert. Auf simulierte Phishing-Nachrichten von Kollegen und Kolleginnen sollte ganz verzichtet werden. Angestellte werden durch Phishing-Kampagnen verunsichert und es wird i. d. R. ein Zeit- und Leistungsdruck aufgebaut. Inwieweit diese Probleme mit einer klaren und ausführlichen Information zu der Phishing-Kampagne entgegengewirkt werden kann, ist fraglich. Außerdem ist fraglich, ob das "Opfer werden" motiviert, sich weiter mit dem Thema zu beschäftigen bzw. ob die Opfer überhaupt die Security-Awareness-Information wahrnehmen.

In Kombination mit den Security Betrachtungen ist festzustellen, dass eine ausführliche Information im Vorfeld unabdingbar scheint, sowie, dass weder Phishing-Nachrichten von Angestellten simuliert werden sollten noch solche von externen Anbietern. Letzteres schränkt die Art der Phishing-Nachrichten enorm ein. Funktionierende Melde- und Rückfrageprozesse (mit einer inhaltlichen Erweiterung und personellen Aufstockung) sind genau wie das Einräumen von mehr Zeit zur Bearbeitung von Nachrichten eine Grundvoraussetzung – auch um Teile der genannten Sicherheitsprobleme zu adressieren. Entsprechend muss akzeptiert werden, dass die Produktivität der Angestellten sinkt.

Stehen all diese Nachteile im Verhältnis zu dem, was Anbieter von Phishing-Kampagnen versprechen?

5. Aussagekraft der erhobenen Daten

Sowohl zum Erreichen der Ziele 1, 2 b) und 3 werden Daten zur Evaluation erhoben. Zunächst ist zu sagen, dass die ***Validität durch die Informationen über die Phishing-Kampagne stark beeinflusst*** wird. Ein (Groß-)Teil der Angestellten wird skeptischer bei den entsprechenden Nachrichten sein als sonst üblich und eher als sonst nachfragen bzw. Kollegen und Kolleginnen informieren bzw. allgemein darüber reden, wenn sie eine Phishing-Nachricht entdeckt haben. Andere stehen dem Ansatz, Angestellte so „anzugreifen", derart abgeneigt gegenüber, dass sie absichtlich mit jeder Phishing-Nachricht interagieren. All dies gilt insbesondere, wenn die Zeitfenster für die Kampagnen kurz sind. Gleichzeitig wird durch kurze Kampagnen das

Sicherheitsrisiko nur für einen kurzen Zeitraum erhöht (siehe Kapitel 4.1). All diese Einflussfaktoren sollten mindestens als Limitation der Aussagekraft berücksichtigt werden[21].

Zum Erreichen der Ziele 1, 2b und 3 können verschiedene Datentypen – einzeln oder in Kombination – betrachtet werden:

- die Anzahl der Angestellten, die pro Phishing-Nachricht die entsprechende unerwünschte Aktion ausführen (z.B. auf den Link klicken/den Anhang öffnen). Diese gilt es dabei noch genauer zu definieren (z. B. bereits das Klicken auf einen Link oder erst das Eingeben von Zugangsdaten oder anderen sensiblen Daten[22]);
- die Anzahl der Angestellten, die eine entdeckte Phishing-Nachricht melden;
- die Anzahl der Angestellten, die melden, dass sie auf eine Phishing-Nachricht hereingefallen sind, nachdem sie die Täuschung festgestellt haben;
- die Anzahl der Angestellten, die sich mit Rückfragen zu Nachrichten melden.

Bei den letzten drei Ansätzen wird vorausgesetzt, dass es einen ***etablierten Melde- und Rückfrageprozess bereits vor dem Start der Phishing-Kampagne gibt.*** Dabei wäre es auch notwendig, dass der Prozess ein Melden von entdeckten Phishing-Nachrichten vorsieht und nicht ein Löschen. Sonst können Phishing-Nachrichten nicht von anderen Spam-Nachrichten oder sonstigen Nachrichten, die gelöscht werden, unterschieden werden. Teil des Melde- und Rückfrageprozesses muss es ebenfalls sein, dass auch solche Phishing-Nachrichten gemeldet werden müssen, von denen bereits bekannt ist, dass andere Angestellte (z. B. der Kollege/die Kollegin im gleichen Büro) diese bereits gemeldet haben.

Bemerkung: Es wird dringend angeraten, erst einmal den eigenen Melde- und Rückfrageprozess kritisch zu analysieren, bevor eine Phishing-Kampagne angedacht wird.

Für den Fall, dass Sie sich fragen, warum es nicht ausreicht, die Anzahl der Angestellten zu erfassen, die pro Phishing-Nachricht die entsprechende unerwünschte Aktion ausführen (z.B. auf den Link klicken/den Anhang öffnen), im Folgenden die Erklärungen:

Ein Nicht-Interagieren kann viele Gründe haben und kann daher nicht als eindeutiger Indikator interpretiert werden, dass die Nachricht als Phishing-Nachricht erkannt wurde: Die Nachricht wurde gar nicht gesehen, weil die Person in Urlaub oder krank war, keine Zeit hatte oder für sie nicht relevant war, weil die Person dort keinen Account hat; oder weil ein Kollege/eine Kollegin bereits auf diese Phishing-Nachricht aufmerksam gemacht hat. Letzteres bedeutet nicht, dass die entsprechenden Kollegen auch die Nachricht selbstständig als Phishing-Nachricht erkannt hätten. Es ist auch nicht möglich, den Angestellten zu sagen, dass sie andere Angestellte nicht informieren sollen, denn genau das ist es an sich, was man im Fall von wirklichen Phishing-Nachrichten möchte: nämlich, dass die Angestellten reagieren und anderen helfen, sich und die Institution zu schützen.

[21] Dies gilt insbesondere im Fall von Ziel 3. Jede andere Evaluation hätte ebenfalls Limitationen. Hier ist es ggf. sinnvoll, verschiedene Studienformen für die Evaluation zu nutzen.

[22] Letzteres stellt schnell ein weiteres Sicherheitsproblem dar. Denn diese sensiblen Daten dürfen nicht übertragen werden.

Letztlich müssten auch die False Positives gezählt werden, also Nachrichten, die legitim waren, die aber als Phishing-Angriff gemeldet wurden und daher erst einmal nicht bearbeitet wurden. Zugespitzt gesagt: Eine Phishing-Kampagne, die zwar zur Konsequenz hat, dass zuverlässig alle Phishing-Nachrichten erkannt werden, die aber auch zur Konsequenz hat, dass jede zweite legitime Nachricht gelöscht wird, weil man sie für eine Phishing-Nachricht hält, ist auch nicht zielführend.

Nun weiter zur Aussagekraft…

Die Aussagekraft hängt bei einer Phishing-Kampagne von den simulierten Phishing-Nachrichten ab. Es gilt: Umso leichter diese zu erkennen sind, umso "besser" sind die Ergebnisse. Extrem schwierig zu erkennende simulierte Phishing-Nachrichten würden von kaum jemanden als solche entdeckt. Eigentlich müssten die simulierten Phishing-Nachrichten solche aus wirklichen Angriffen abbilden (und damit eine Vielzahl unterschiedlicher), aber dafür müssten auch Nachrichten von Angestellten und externen Anbietern verwendet werden, was – wie in Kapitel 4 beschrieben – eine Reihe von Nachteilen hätte (u. a. auf das Vertrauensverhältnis zwischen Kollegen und Kolleginnen sowie, dass man ggf. markenrechtliche Aspekte prüfen müsste). ***Insgesamt gilt, dass die Aussagekraft immer in Bezug auf die simulierten Phishing-Nachrichten sowie in Bezug auf die Änderungen an der Infrastruktur zu sehen ist.***

Die Aussagekraft der erhobenen Daten hängt auch davon ab, ob bzw. inwieweit im Zeitraum der Erhebung andere Einflussfaktoren, z. B. Medienberichte, kontrolliert werden können.

Für den Fall, dass Ziel 2 b) verfolgt wird, ist außerdem Folgendes zu beachten:

Es müssten zusätzliche Daten erhoben werden. Für die Auswertung wäre es notwendig zu wissen, ob und wie lange eine Auseinandersetzung mit den nachgelagerten Security-Awareness-Inhalten erfolgt ist. Hierzu könnte die Datenerhebung nur pseudonymisiert erfolgen und nicht anonymisiert, was auf seine datenschutzrechtliche Zulässigkeit hin zu prüfen ist.

Zusammenfassend ist die Aussagekraft allgemein und insbesondere in konkreten Ausgestaltungsformen sehr umstritten. Gleichzeitig ist der Aufwand für eine Phishing-Kampagne, bei der die zusätzlichen Security-Probleme minimiert werden und die rechtskonform ist, extrem aufwendig. In jedem Fall bleiben die Probleme hinsichtlich des Vertrauensverhältnisses und der Selbstwirksamkeit, sowie die Arbeitszeit aller Mitarbeiter, die hierfür genutzt wird. Die Nachteile und Kosten (Zeit und Geld) wiegen die geringe Aussagekraft einer Kampagne nicht auf. Es wird daher empfohlen, Zeit und Geld in (1) eine Verbesserung der technischen Maßnahmen zu investieren. Außerdem sollten (2) geeignete Awareness-Maßnahmen den Angestellten nahebringen, welche Art von Phishing-Nachrichten sie trotz aller technischen Maßnahmen erreichen können und wie sie diese erkennen können. Schließlich sollte (3) der Melde- und Rückfrageprozesses verbessert werden. Dadurch ist der Aufwand für jeden einzelnen Angestellten vergleichbar gering und umsetzbar. Das Schutzniveau steigt ohne negative Auswirkungen auf Vertrauensverhältnisse und Selbstwirksamkeit.