Melanie Volkamer, Martina A. Sasse, Franziska Boehm

Phishing-Kampagnen zur Steigerung der Mitarbeiter-Awareness

Analyse aus verschiedenen Blickwinkeln – Security, Recht und Faktor Mensch

Phishing-Angriffe sind kein neues Phänomen, aber nach wie vor eine große Gefahr für jede Institution.[1] Um die Resistenz der Angestellten gegen Phishing-Angriffe zu erheben oder zu verbessern, führen zahlreiche Einrichtungen Phishing-Kampagnen durch, bei denen (simulierte) Phishing-Nachrichten an die Angestellten verschickt werden. Der Beitrag geht auf unterschiedliche Ziele und Ausgestaltungsformen von Phishing-Kampagnen ein und betrachtet potentielle Probleme und die Aussagekraft von Phishing-Kampagnen.[2]

Prof. Dr. Melanie Volkamer

ist Professorin am Karlsruher Institut für Technologie (KIT). Sie leitet dort die Forschungsgruppe Security, Usability, and Society (SECUSO) und ist PI des Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL).
E-Mail: melanie.volkamer@kit.edu

Prof. Dr. Martina A. Sasse

Leiterin des Lehrstuhls Human-Cent-red Security am Horst-Görtz-Institutfür IT-Sicherheit der Ruhr-Universität Bochum.
E-Mail: Martina.Sasse@ruhr-uni-bochum.de

Prof. Dr. Franziska Boehm

ist Bereichsleiterin für Immaterialgüterrechte in verteilten Informationsinfrastrukturen (IGR) bei FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur und Professorin am Karlsruher Institut für Technologie (KIT), Zentrum für angewandte Rechtswissenschaft (ZAR).
E-Mail: franziska.boehm@kit.edu

1 Ziele von Phishing-Kampagnen

Mit Phishing-Kampagnen werden unterschiedliche Ziele verfolgt. Dazu zählen vor allem die folgenden:

1. Erhebung des Ist-Zustands in der Institution hinsichtlich der Resistenz gegen Phishing-Angriffe (ggf. inklusive des Meldens von entdeckten Phishing-Angriffen), z. B. um über die so nachgewiesene fehlende Resistenz mehr Budget für das Thema IT-/Informationssicherheit oder Datenschutz zu erhalten oder um zu zeigen, dass eine entsprechende Security-Awareness-Kampagne oder Security-Schulung verpflichtend eingeführt werden sollte (Ziel 1).
2. Die Phishing-Nachrichten sollen als so genannter *Teachable Moment* genutzt werden (Ziel 2). 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 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 Personen zu zählen, die eine Nachricht nicht als Phishing-E-Mail erkannt bzw. eine Nachricht gemeldet haben (also als reine Security-Awareness-Maßnahme), oder

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

2 Eine Ausführlichere Diskussionen finden Sie unter: https://publikationen.bibliothek.kit.edu/1000119662

b) mit Erhebung der Anzahl der Personen, die eine Nachricht nicht als Phishing-E-Mail erkannt bzw. eine Nachricht gemeldet haben, um (hoffentlich) zeigen zu können, dass die Kampagne das Schutzniveau der Institution erhöht hat bzw. im Laufe der Zeit erhöht, also um die Security-Awareness-Maßnahme zu evaluieren bzw. zu rechtfertigen.

3. Evaluation einer (neu entwickelten) Security-Awareness-Maßnahme im Phishing-Kontext (Ziel 3), die von der eigentlichen Phishing-Kampagne unabhängig[3] ist, und zwar durch Erhebung des Ist-Zustands 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 wird eher im wissenschaftlichen Kontext verfolgt.

2 Design Space 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.

- Phishing-Kampagnen können 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 die Nachrichten unterschiedlichen Inhalts sein und mit verschiedenen Absendertypen verschickt werden (z. B. von einer einzelnen Person oder einer Institution).
- Darüber hinaus können Nachrichten Bezüge zu aktuellen Themen aufweisen, was wiederum einen Einfluss auf den Schwierigkeitsgrad der Erkennung hat[4 5].
- Schließlich kann die Kampagne von institutionsinternen Personen oder von externen Dritten, 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 weiter in der Länge des Durchführungszeitraums und der Anzahl der Nachrichten, die während dieses Zeitraums verschickt werden.
- Außerdem gibt es verschiedene Möglichkeiten, wie im Rahmen der Kampagne damit umgegangen wird, wenn Phishing-E-Mails nicht erkannt werden.
- Phishing-Kampagnen können mehr oder weniger prominent und mehr oder weniger ausführlich angekündigt werden, bis zu der extremen Form, in der die Angestellten der Institution überhaupt nicht informiert werden.

3 Unabhängig meint hier, dass die Security-Awareness-Maßnahme losgelöst von der Kampagne ist.

4 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

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

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) ist die Auswertung unterschiedlicher Indikatoren sinnvoll (siehe Abschnitt 4). Die Auswertung kann ebenfalls unterschiedlich detailliert erfolgen – z. B. bezogen auf alle Angestellten oder auf einzelne Gruppen bzw. pro Phishing-Nachricht oder -Nachrichtentyp.

3 Problemanalyse von Phishing-Kampagnen

Aus *Security-Sicht* können Phishing-Kampagnen das Schutzniveau der Institution während der Durchführung einer solchen Kampagne deutlich senken, wenn z. B.

- die Nachrichten von extern verschickt werden und die Nachrichten-Filterung an der Firewall angepasst wird, damit die Nachrichten nicht herausgefiltert werden, und
- die Phishing-Kampagne und die damit verbundenen Aufgaben und Erwartungen an die Angestellten nicht klar kommuniziert werden und
- keine klaren Melde- und Rückfrageprozesse in der Institution vorhanden sind.
- 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 durchgeführt werden, nutzen können, um gezielte reale Phishing-Angriffe vorzunehmen.

Aus *rechtlicher Sicht* ist zu berücksichtigen, dass Personal- bzw. Betriebsrat in die Gestaltung einer Phishing-Kampagne mit einbezogen werden müssen und – je nach Kommunikationskonzept – die internen Kenntnisse bis zum Abschluss der Kampagne geheim halten müssen. Abhängig von der Größe der Institution oder der Teams kann eine anonymisiert Auswertung der Indikatoren notwendig sein, um sicherzustellen, dass die Ergebnisse nicht einzelnen Arbeitnehmern zugeordnet werden können. Ggf. ist zu klären, ob eine pseudonymisierte Auswertung arbeits- und datenschutzrechtlich ausreichend ist.

Weiter ist zu prüfen, ob auf eine vorherige eingehende Information der Angestellten verzichtet werden kann. Dabei reduzieren umfangreiche und prominent platzierte Informationen die Aussagekraft der gemessenen Ergebnisse. Wenig prominent platzierte Informationen können sich aber negativ auf das Vertrauen der Arbeitnehmer in die Institution auswirken und einzelne Security-Probleme verstärken.

Unabhängig davon ist sicherzustellen, dass falsche Reaktionen auf die Phishing-Nachrichten nicht zu arbeitsrechtlichen Konsequenzen für die jeweiligen Arbeitnehmer führen (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 im Fall von simulierten Phishing-Nachrichten außerdem Marken- und Urheberrechte von externen Anbietern zu prüfen. Daraus folgende Einschränkungen hinsichtlich der Gestaltung der Nachrichten können sich negativ auf die Aussagekraft der gemessenen Ergebnisse der Phishing-Kampagne auswirken.

Neben den potentiellen Security-Problemen und den rechtlichen Herausforderungen können Phishing-Kampagnen auch einen *negativen Einfluss auf das Betriebsklima, die Vertrauens- und Fehlerkultur* haben. Insbesondere das Vertrauensverhältnis zur Leitung der Institution kann negativ beeinflusst werden. Auf simulierte Phishing-Nachrichten von Kollegen und Kolleginnen sollte ganz verzichtet, um das Vertrauensverhältnis zwischen Kollegen nicht zu gefährden. Angestellte werden durch Phishing-Kampagnen verunsichert und es wird in der Regel ein Zeit- und Leistungsdruck aufgebaut. Inwieweit diesen Problemen mit einer klaren und ausführlichen Information zur Phishing-Kampagne entgegengewirkt werden kann, ist fraglich. Außerdem ist fraglich, ob Mitarbeiter, die eine Phishing-Nachricht nicht erkennen und falsch reagieren, anschließend motiviert sind, sich weiter mit dem Thema zu beschäftigen bzw. die Security-Awareness-Informationen dazu überhaupt wahrnehmen.

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 auf die genannten Sicherheitsprobleme zu reagieren. Entsprechend muss akzeptiert werden, dass die Produktivität der Angestellten sinkt.

4 Analyse der Aussagekraft

Zum Erreichen der Ziele 1, 2 b) und 3 werden Daten zur Evaluation erhoben. Dabei wird die Validität der erhobenen Daten durch Art, Umfang und Wahrnehmung der Informationen über die Phishing-Kampagne stark beeinflusst. 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 eine Phishing-Nachricht entdeckt wird. 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. Diese Einflussfaktoren sollten mindestens als Beschränkungen der Aussagekraft berücksichtigt werden.[6]

Zur Prüfung, ob die Ziele 1, 2b und 3 erreicht wurden, können verschiedene Indikatoren – einzeln oder in Kombination – erhoben und ausgewertet werden:

6 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.

- die Anzahl der Personen je Phishing-Nachricht, die die entsprechende unerwünschte Aktion ausführen (z. B. auf einen Link klicken, sensible Daten angeben, einen Anhang öffnen; diese gilt es dabei noch genauer zu definieren: wird z. B. bereits das Klicken auf einen Link oder erst das Eingeben von Zugangsdaten oder anderen sensiblen Daten gewertet?[7]);
- die Anzahl der Personen, die eine entdeckte Phishing-Nachricht melden bzw. 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.

Die Erhebung der letzten drei Indikatoren setzt voraus, dass es bereits vor dem Start der Phishing-Kampagne einen etablierten Melde- und Rückfrageprozess 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 irrtümlich für Phishing-Nachrichten gehalten wurden, unterschieden werden. Teil des Melde- und Rückfrageprozesses muss es außerdem sein, dass auch solche Phishing-Nachrichten gemeldet werden müssen, von denen dem Empfänger bereits bekannt ist, dass andere Angestellte (z. B. ein Kollege oder eine Kollegin im gleichen Büro) diese bereits gemeldet haben.

Ein Nicht-Interagieren kann viele Gründe haben und kann daher nicht als eindeutiger Indikator interpretiert werden, dass die Nachricht als Phishing-Nachricht erkannt wurde:

- So wurde die Nachricht möglicherweise gar nicht gelesen, weil die Person in Urlaub oder krank war, keine Zeit hatte oder der Inhalt für sie nicht relevant war, weil die Person dort keinen Account hat;
- Ein Kollege oder eine Kollegin hat möglicherweise bereits auf diese Phishing-Nachricht aufmerksam gemacht. Letzteres bedeutet nicht, dass die betroffenen Kollegen die Nachricht auch selbstständig als Phishing-Nachricht erkannt hätten.[8]

Letztlich müssten auch die *False Positives* gezählt werden, also Nachrichten, die legitim waren, die aber als Phishing-Angriff gemeldet und daher erst einmal nicht bearbeitet wurden. Zugespitzt ausgedrückt: Eine Phishing-Kampagne, die zur Konsequenz hat, dass zuverlässig alle Phishing-Nachrichten erkannt werden, dass aber auch jede zweite legitime Nachricht gelöscht wird, weil sie für eine Phishing-Nachricht gehalten wird, kann der Produktivität und Reputation der Organsiation schaden.

Die Aussagekraft hängt bei einer Phishing-Kampagne von den simulierten Phishing-Nachrichten ab. Es gilt: Umso leichter diese zu erkennen sind, desto „besser" sind die Ergebnisse. Extrem schwierig zu erkennende simulierte Phishing-Nachrichten würden nur von wenigen Mitarbeitern als solche identifiziert. Idealerweise sollten simulierte Phishing-Nachrichten solchen aus wirklichen Angriffen ähneln, aber dafür müssten auch Nachrichten von Angestellten und externen Anbietern verwendet werden, was – wie in Abschnitt 3 ausgeführt – eine Reihe von Nachteilen hätte. Insgesamt gilt, dass die Aussagekraft sowohl von den simulierten Phishing-Nachrichten als auch von den Änderungen an der Infrastruktur abhängt.

5 Fazit

Die Aussagekraft von Phishing-Kampagnen ist allgemein und insbesondere in konkreten Ausgestaltungsformen sehr umstritten.[9] Gleichzeitig ist der Aufwand für eine Phishing-Kampagne, bei der die zusätzlichen Security-Probleme minimiert werden und die rechtskonform ausgestaltet ist, extrem aufwendig. In jedem Fall bleiben die Schwierigkeiten hinsichtlich des Vertrauensverhältnisses und der Selbstwirksamkeit sowie die Arbeitszeit aller Mitarbeiter, die hierfür aufgewendet wird, bestehen. Die Nachteile und Kosten (Zeit, Geld)) einer Kampagne, werden von der (geringen) Aussagekraft bzgl. des Sicherheitsbewusstseins nicht kompensiert. 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 Rückfrageprozess verbessert werden. Dadurch ist der Aufwand für jeden einzelnen Angestellten vergleichbar gering und umsetzbar. Das Schutzniveau steigt ohne negative Auswirkungen auf Vertrauensverhältnisse und Selbstwirksamkeit.

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

8 Es ist nicht sinnvoll, die Angestellten zu bitten, andere Angestellte nicht über eingegangene Phishing-Nachrichten zu informieren, denn genau dieses Verhalten ist das im Fall von wirklichen Phishing-Nachrichten gewünschte: dass die Angestellten reagieren und anderen helfen, sich und die Institution zu schützen.

9 https://www.ncsc.gov.uk/blog-post/im-gonna-stop-you-little-phishie