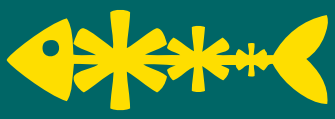

Stand: 28. Februar 2024

VORGEHENSMODELL

PhiSim 0.9

GENDERHINWEIS

Aus Gründen der leichteren Lesbarkeit wird in dem vorliegenden Dokument die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung jeglichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

VERSIONSHISTORIE

Datum	Version	Beschreibung	Bearbeiter
28.02.2024	0.9	1. Entwurf	Ronja Hönig Maik Neumann Georg Opitz Ullrich Prax Dirk Rostig

INHALTSVERZEICHNIS

VORWORT

Dieses Vorgehensmodell wurde im Anschluss an ein studentisches Projekt an der Hochschule Meißen (FH) und Fortbildungszentrum (HSF Meißen) erstellt. Das Thema lautete „Konzeption und Durchführung von Phishing-Simulationen am Beispiel der HSF Meißen“.

Die HSF Meißen ist zentrale Aus- und Fortbildungseinrichtung für den öffentlichen Dienst im Freistaat Sachsen. Im Dreiklang als Behörde im Geschäftsbereich des Staatsministeriums des Innern, Hochschule und staatseigenes Fortbildungszentrum nimmt sie eine besondere Rolle innerhalb der Staatsverwaltung ein und bietet einzigartige Möglichkeiten der Verknüpfung von Verwaltungspraxis, Aus- und Fortbildung sowie Forschung.

Die vier Studenten waren 2023/2024 im 6. Semester des Studiengangs Digitale Verwaltung an der HSF Meißen eingeschrieben. Bereits vor dem Studium sammelten sie Berufserfahrung in verschiedenen Wirtschaftsbereichen wie Softwareentwicklung, Marketing und Projektmanagement. Gemeinsam mit ihrem Projektbetreuer, dem Referent am Zentrum für Informationstechnologie der HSF Meißen entstand im Rahmen des Studiums diese auf praktische Informationssicherheit ausgerichtetes Projekt, welches in dieses Vorgehensmodell mündete.

EINLEITUNG

Dieses Vorgehensmodell bietet Leitlinien zu den Begriffen, Prozessen und Werkzeugen, die für eine erfolgreiche Durchführung einer Phishing-Simulation in der eigenen Organisation von Bedeutung sind und Auswirkung darauf haben.

Dieses Vorgehensmodell richtet sich an:

- Organisationen aller Arten und Größen, die mit externen und internen Faktoren und Einflüssen konfrontiert sind;
- Personen, die in Organisationen Werte schaffen und schützen, indem sie Risiken managen, Entscheidungen treffen, Ziele setzen und erreichen und die Leistung verbessern, insbesondere an
  - Führungskräfte bzw. Behördenleiter und Projektauftraggeber, damit sie die Grundsätze und die Praxis einer Phishing-Simulation besser verstehen sowie ihre Projektmanager, Kernteams und Projektteams angemessen unterstützen und anleiten können;
  - Projektmanager, Kernteams und Projektteams, damit diese eine gemeinsame Basis für den Vergleich ihres Vorgehens mit jenen anderer haben;

Informationssicherheit ist im Kontext der Digitalisierung aufgrund zunehmender und komplexer werdender Bedrohungen von entscheidender Bedeutung. Neben den technischen und organisatorischen Sicherheitsmaßnahmen spielt vor allem der „Faktor Mensch“ eine wichtige Rolle. Die Sensibilisierung von Mitarbeitenden für das Thema Informationssicherheit ist damit wesentlich. Mit diesem Vorgehensmodell wird gezeigt, wie eine Phishing-Simulation das Risikobewusstsein der Mitarbeitenden schärfen kann.

Dieses Vorgehensmodell soll den eigenen Einsatz von Phishing-Simulationen als Sensibilisierungsmaßnahme erleichtern.

1 ANWENDUNGSBEREICH

Dieses Vorgehensmodell legt Leitlinien für die Durchführung von Phishing-Simulationen fest und kann von Organisationen jeglicher Art, einschließlich staatlicher, privater oder gemeinschaftlicher Organisationen angewendet werden.

Dieses Vorgehensmodell bietet eine allgemeine Beschreibung der Begriffe, Prozesse und Werkzeuge, die für eine erfolgreiche Durchführung einer Phishing-Simulation in der eigenen Organisation als bewährte Praxis gelten.

2 NORMATIVE VERWEISUNG

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 9000:2015, *Quality management systems— Fundamentals and vocabulary*

DIN ISO 10006:2020-10, *Qualitätsmanagement – Leitfaden für Qualitätsmanagement in Projekten (ISO 10006:2017)*

3 BEGRIFFE UND DEFINITIONEN

Für die Anwendung dieses Vorgehensmodells gelten die folgenden Begriffe. Abbildung 1 zeigt deren Einordnung und die Zusammenhänge.

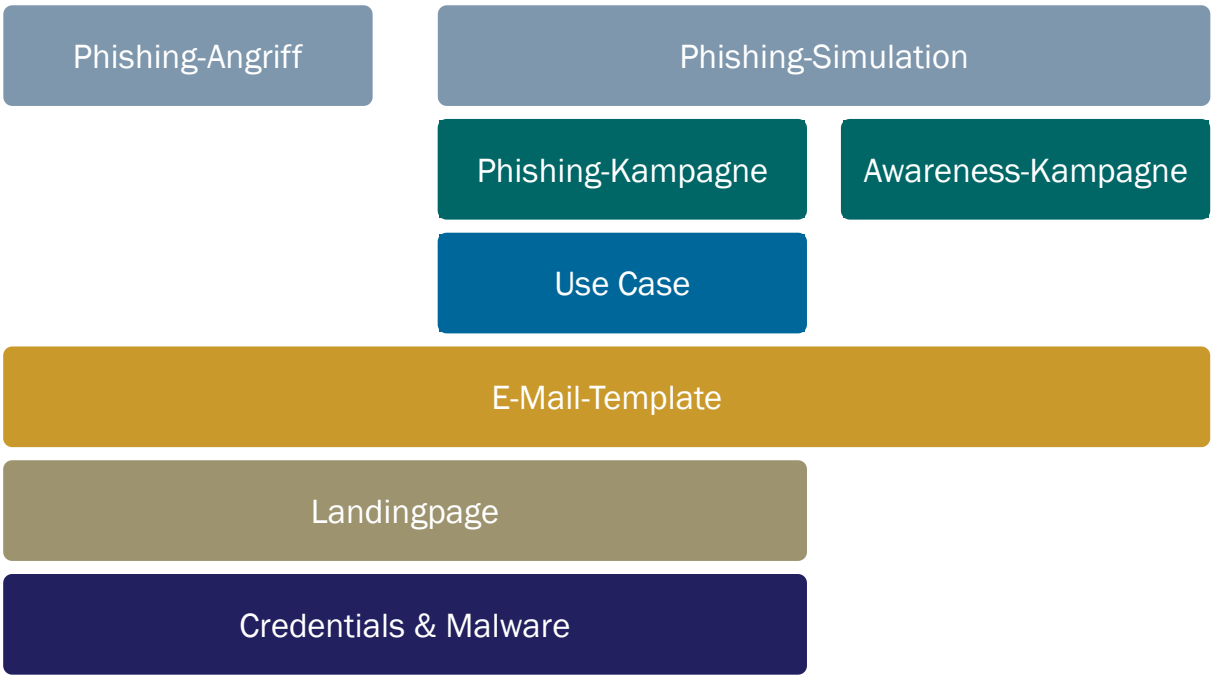

Abbildung 1: Einordnung und Zusammenhang der Begriffe

3.1 Awareness

Schaffung von Bewusstsein durch Sensibilisierungsmaßnahmen. Wird es als Kampagne durchgeführt, dann wird es auch als Awareness-Kampagne bezeichnet.

3.2 Credentials

Ein Berechtigungsnachweis, der einem System die Identität eines anderen Systems oder eines Benutzers/Betroffenen bestätigen soll. Die Identität muss dem verifizierenden System bekannt sein.

3.3 E-Mail-Template

Bestimmter Inhalt einer E-Mail, die im Rahmen einer Phishing- oder Awareness-Kampagne an einen bestimmten Nutzerkreis gesendet wird.

3.4 Landingpage

Die Seite, auf die der Betroffene gelockt wird, um seine Credentials einzugeben oder sein System mit Malware infiziert wird.

3.5 Malware

Malware ist schädliche Software, die auf IT-Systeme zugreift, um unerwünschte und schädliche Funktionen auszuführen, oft ohne das Wissen des Benutzers. Häufig werden Daten gestohlen oder Schaden angerichtet sowie Ressourcen des IT-Systems für schadhafte Handlungen genutzt.

3.6 Phishing

Phishing ist eine Form des Social Engineerings, bei der oftmals vertrauenswürdige Absender imitiert werden, um persönliche oder finanzielle Informationen zu erschleichen. Angreifer erlangen monetäre Vorteile oder verursachen Schäden, indem sie psychologische Täuschungsmethoden einsetzen. Es gibt verschiedene Formen des Phishings und der Wahl der zugrundeliegenden Methoden.

3.7 Phishing-Angriff

Böswilliger Angriff unter Zuhilfenahme sozio-technischer Systeme mit der Absicht, Credentials zu erlangen.

3.8 Phishing-Kampagne

Einzelne Kampagne mit bestimmten E-Mail-Template. Sie ist Bestandteil einer Phishing-Simulation.

3.9 Phishing-Simulation

Ein simulierter Phishing-Angriff zur Steigerung der Awareness.

3.10 Social Engineering

Ausnutzung menschlicher Schwächen, wie Hilfsbereitschaft oder Neugier, um unbefugten Zugang zu Informationen oder Systemen zu erlangen oder schädliche Handlungen durchzuführen. Der Betroffene handelt im Glauben, das Richtige getan zu haben.

3.11 Use Case

Szenario einer Phishing-Kampagne unter Nutzung von E-Mail-Templates.

4 PROJEKTPHASEN

Das Vorgehensmodell folgt vorrangig der Wasserfallmethode, da eine Phishing-Simulation sehr konstante Anforderungen aufweist. Die Phishing-Kampagnen hingegen können iterativ bearbeitet werden und folgen daher dem hybriden Projektmanagement-Ansatz.

Abbildung 2 zeigt die Zuordnung der einzelnen Aufgabenbündel und deren zeitliche Einordnung relativ zueinander. Zudem ist eine Unterteilung zwischen Phishing-Simulation und -Kampagne vorgenommen.

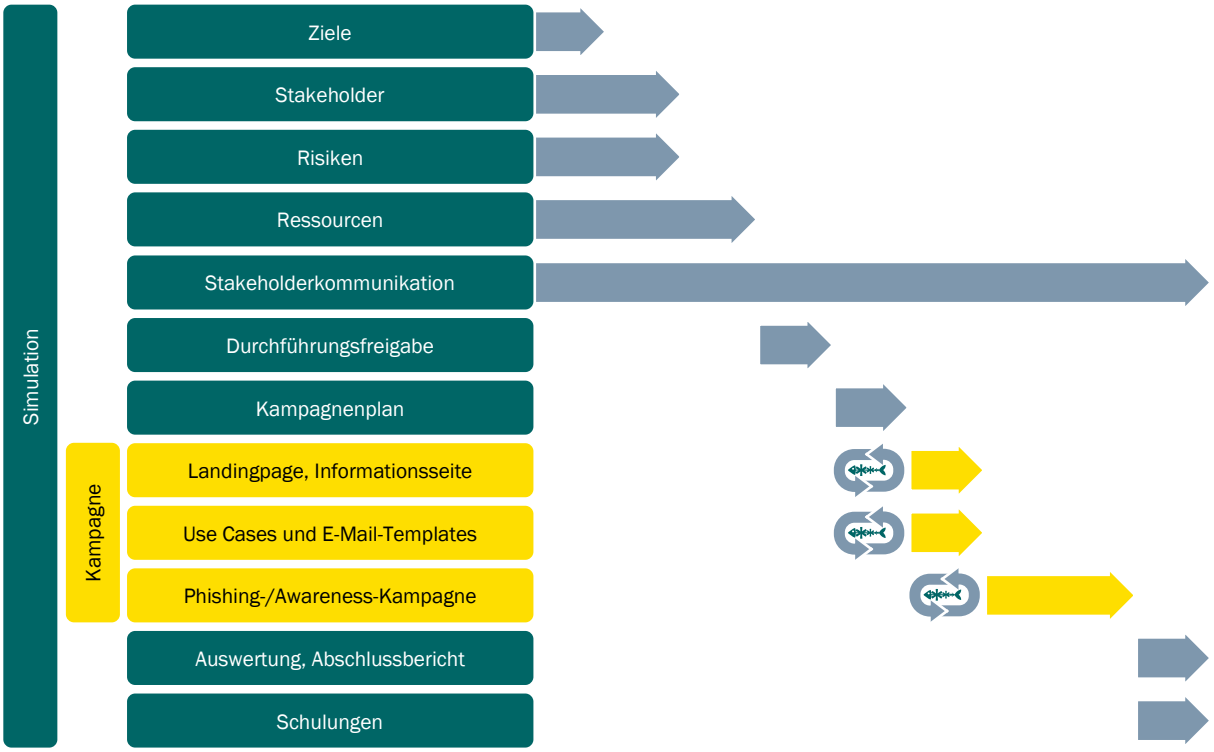

Abbildung 2: Einordnung und Zusammenspiel der Projektphasen

4.1 Projektstrukturplan

Abbildung 3 zeigt den Projektstrukturplan mit den jeweiligen Aufgabenpaketen.

Arbeitspaket 1 läuft parallel zu allen anderen Arbeitspaketen und muss iterativ und kontinuierlich durchgeführt werden. Es müssen Stakeholder involviert, Risiken betrachtet werden und allgemein eine sehr gute Kommunikation stattfinden.

Arbeitspaket 2 betrachtet die unterschiedlichen Ziele, welche die Phishing-Simulation erreichen soll. Dieses Arbeitspaket ist wichtig, um das Vorgehensmodell auf die organisationsspezifischen Bedürfnisse auszurichten und die eigenen Zielgruppen zu identifizieren.

Arbeitspaket 3 plant die gesamte Phishing-Simulation sowie einzelne Phishing-Kampagnen. Dieses Arbeitspaket stellt den größten Arbeitsaufwand dar. Dabei wird in die Detailplanung (Arbeitspaket 3.1), die inhaltliche Planung (Arbeitspaket 3.2) und die technische Planung (Arbeitspaket 3.3) unterschieden. Die Aufgaben der Arbeitspakete lassen sich wie folgt beschreiben:

- Arbeitspaket 3.1: Die benötigten Ressourcen sowie deren zeitliche Einordnung müssen geplant werden.

- Arbeitspaket 3.2: Use Cases sowie der Kampagnenplan müssen aufgestellt werden. Diese Planung hat Rückkopplungen auf die Zeitplanung. Ebenfalls muss eine Strategie für das Reaktionsmanagement erstellt werden, um Meldeketten nicht zu überlasten. Außerdem muss die Informationsseite gestaltet werden.

- Arbeitspaket 3.3: Evtl. Domain Names, Server, Datenbanken sowie E-Mail-Konten müssen angelegt und konfiguriert werden. Zudem muss sich um die Landingpage sowie das Cookie-Handlung gekümmert werden.

Arbeitspaket 4 für die Phishing-Simulation bzw. -Kampagnen durch. Die dafür notwendigen Hilfsmittel müssen erstellt werden.

Arbeitspaket 5 schließt das Projekt ab und wertet Ergebnisse aus und definiert evtl. Schulungsbedarf.

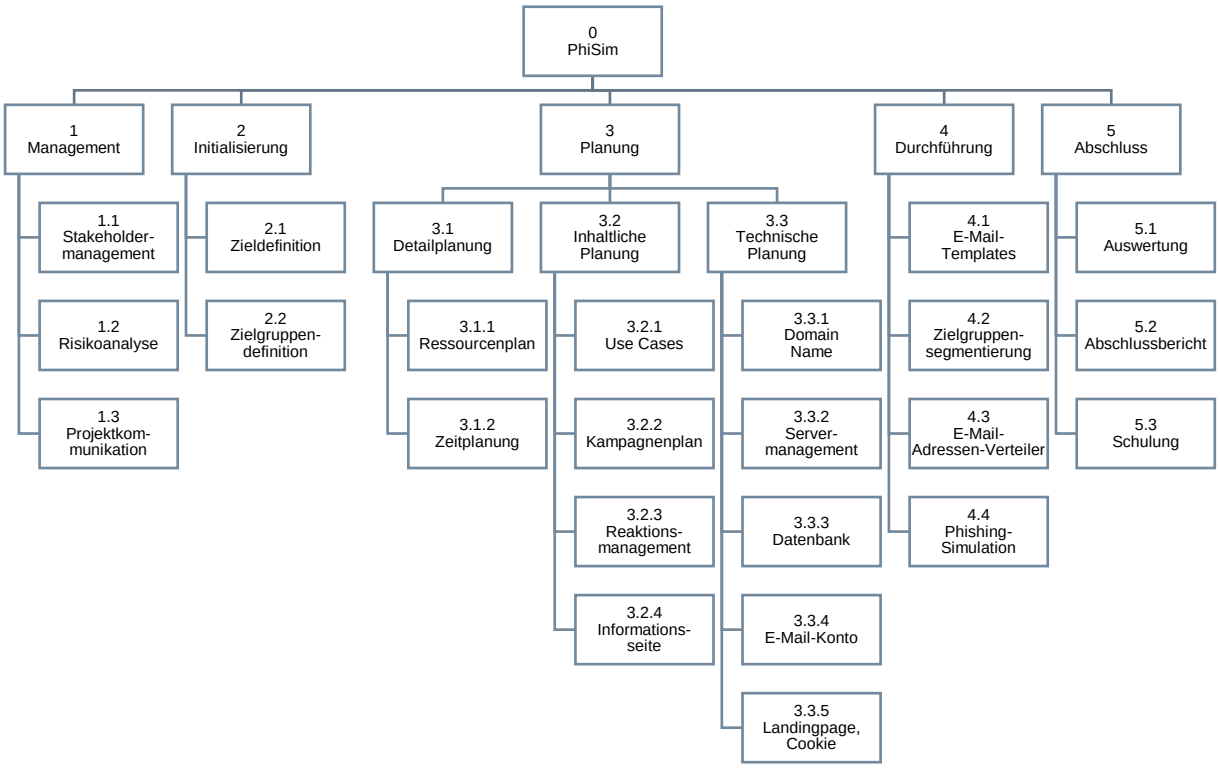

Abbildung 3: Einordnung der Arbeitspakete in den Projektstrukturplan

4.2 Meilensteine

Folgende Meilensteine (vgl. Abbildung 4) haben sich als hilfreich erwiesen. Die darin enthaltenen Aktivitäten sowie Methoden, Werkzeuge und Dokumente werden im Anschluss aufgeführt und beschrieben. Die fortlaufende Nummerierung gibt u. U. keine Reihenfolge an, sondern belegt nur die Vollständigkeit.

Nachfolgend werden die Aktivitäten beschrieben, die zur Erreichung der jeweiligen Meilensteine beitragen.

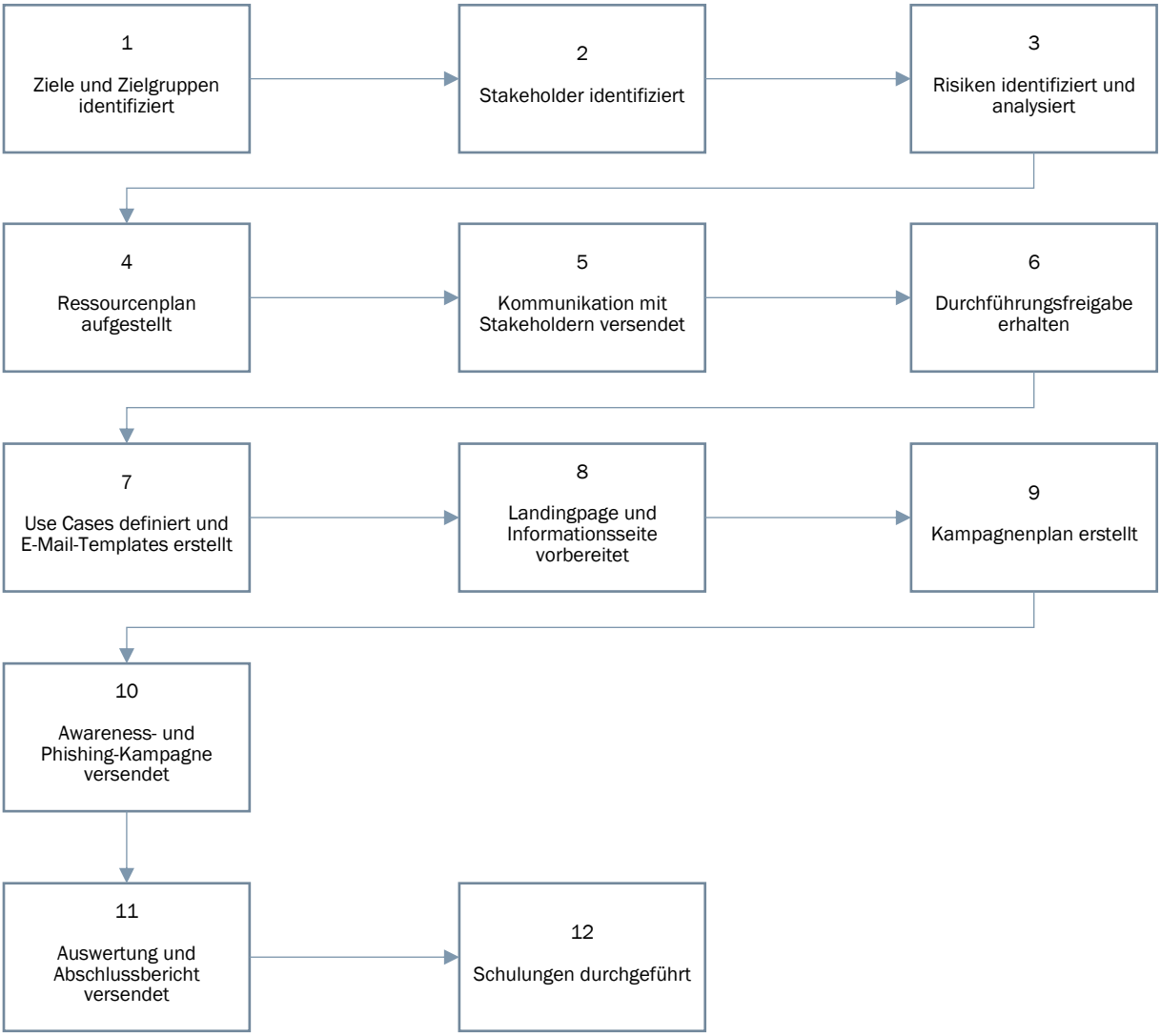

Abbildung 4: Meilensteine entlang des Vorgehensmodells

4.2.1 Ziele und Zielgruppen identifiziert

Zu Beginn des Projektes muss entschieden werden, an wen sich die Phishing-Simulation richten soll. Dabei können individuelle Teilgruppen oder die Gesamtorganisation als Ziel definiert werden. Eine Phishing-Simulation für alle Angehörigen der Organisation bietet sich an, um einen ersten Einblick in den aktuellen Sachstand bezüglich der Informationssicherheit bezüglich Phishings zu erhalten und eventuellen Schulungsbedarf zu identifizieren. Eine Durchführung an individuellen Teilgruppen bietet die Möglichkeit gezieltere Angriffe zu simulieren und spezifische Schulungsmaßnahmen umzusetzen. Außerdem muss entschieden werden, ob vorab Awareness-Maßnahmen durchgeführt werden oder ob auf diese verzichtet wird. In jedem Fall muss im Anschluss an die Phishing-Simulation eine Schulungsmaßnahme zur Verfügung gestellt werden, um die Betroffenen aufzuklären und nachhaltige Sensibilisierungseffekte zu erreichen. Andernfalls kann es bei den Betroffenen zu Frustration oder innerer Abwehrhaltung gegenüber der Organisation kommen. Ebenfalls muss anhand der Projektziele entschieden werden, mit welchen Use Cases gearbeitet werden soll, ob die Betroffenen mit persönlicher Anrede angeschrieben werden sollen und ob der Versand der Phishing-E-Mails gestaffelt oder komplett erfolgen soll.

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 2.1 und 2.2.

4.2.2 Stakeholder identifiziert

Die Stakeholder-Identifikation ist der Prozess, bei dem die verschiedenen Interessengruppen oder Beteiligten identifiziert werden, die von den Aktivitäten betroffen sind oder einen Einfluss darauf haben könnten. Stakeholder können eine Vielzahl von Gruppen umfassen: Kunden, Mitarbeiter, Lieferanten, Investoren, Interessenvertretungen und andere interessierte Parteien. Durch die Identifizierung und Analyse dieser Stakeholder können deren Interessen, Bedürfnisse, Erwartungen und potenzielle Auswirkungen auf die Aktivitäten besser verstanden und angemessen darauf reagiert werden. In einer Tabelle (vgl. Abbildung 5) sollen dabei die jeweiligen Stakeholder mit deren Einstellung und den persönlichen Erwartungen werden. Einfluss und Interesse werden abgeschätzt und in einer gewählten Skala von gering bis hoch festgelegt. Diese Einteilung wird anschließend in einer Vier-Felder-Matrix/Stakeholder-Matrix (vgl. Abbildung 6) eingetragen und deren Grundstrategie daraus abgeleitet.

1. Stakeholder mit hohem Einfluss und Interesse müssen eng begleitet werden (manage closely). Sie können das Projekt stark beeinflussen und sollten daher aktiv einbezogen werden.

2. Stakeholder mit niedrigem Einfluss, aber hohem Interesse sollten informiert bleiben (keep informed). So ist es möglich, evtl. Abwehrhaltungen aufzulösen und relevante Informationen für das Projekt zu erhalten.

3. Stakeholder mit hohem Einfluss, aber niedrigem Interesse müssen zufriedengestellt werden (keep statisfied). Diese müssen, mehr noch als andere Stakeholder, einer kontinuierlichen Risikobetrachtung unterzogen werden.

4. Stakeholder mit niedrigem Einfluss und Interesse müssen beobachtet werden. Sollten sich bei Ihnen Veränderungen ergeben, kann schnellstmöglich darauf reagiert werden.

Identifikation					Analyse		Grund-strategie
ID	Name	Einstellung	Persönliche Erwartungen, Ziele, Wünsche	Intern/ Extern	Einfluss	Interesse	
1	Stakeholder 1	positiv (+)	(+) Aspekt (+) Aspekt	intern	4,0	5,0	manage closely
5	Stakeholder 2	stark negativ (--)	(-) Aspekt	intern	4,5	3,0	manage closely
2	Stakeholder 3	neutral (o)	(-) Aspekt	extern	2,0	3,0	keep informed
7	Stakeholder 4	neutral, tendenziell negativ (o)	(+) Aspekt (-) Aspekt	intern	3,0	2,0	keep satisfied
...	...	...	...	...	...	...	...

Abbildung 5: Tabellarische Darstellung der Stakeholder-Identifikation

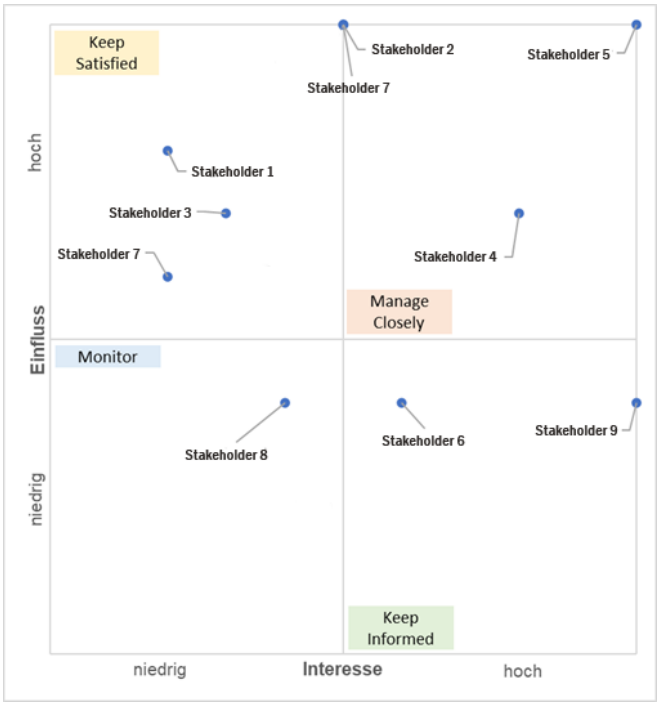

Abbildung 6: Grafische Darstellung der Stakeholder-Identifikation

ANMERKUNG Das betreffende Arbeitspaket ist PSP 1.1.

4.2.3 Risiken identifiziert und analysiert

Um eine erfolgreiche Projektdurchführung zu gewährleisten, müssen mögliche Projektrisiken vorab identifiziert, analysiert und bewertet werden, um im Anschluss entsprechende Gegenmaßnahmen zu entwickeln. Die Fehlermöglichkeits- und Einflussanalyse (FMEA) stellt dazu ein mögliches Werkzeug dar. Dabei werden identifizierte Risiken nach ihrer Auftretenswahrscheinlichkeit, Bedeutung und Entdeckungswahrscheinlichkeit auf eine Skala von 1 bis 10 bewertet. Aus deren Multiplikation ergibt sich die Risikoprioritätszahl (RPZ), welche eine Einteilung der möglichen Risiken in akzeptabel, mittel und hoch ermöglicht. Daraufhin kann das Projektteam eine Risikopriorisierung vornehmen und muss Gegenmaßnahmen zur Vorbeugung oder Reaktion auf eingetretene Risiken entwickeln und ggf. umsetzen.

Eine hilfreiche Matrix der Fehlermöglichkeits- und Einflussanalyse findet sich in Abbildung 16.

ANMERKUNG Das betreffende Arbeitspaket ist PSP 1.2.

4.2.4 Ressourcenplan aufgestellt

Der Ressourcenplan sollte ausweisen, welche Ressourcen benötigt und wann sie gemäß Meilensteinplan angefordert werden.

Die DIN ISO 10006:2020-10, beschreibt in 6.2.3 Zuweisung von Personal, dass das eingesetzte Personal die notwendige Kompetenz hinsichtlich Schulbildung, beruflicher Ausbildung, Fähigkeiten und Erfahrungen besitzen sollte (eine Definition von „Kompetenz“ ist in ISO 9000:2015, 3.10.4 als die „Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen“ beschrieben).

Die folgenden Personalressourcen können notwendig werden:

1. Projektleiter
2. Konzept-Verantwortlicher
3. IT-Verantwortlicher
4. Marketing- bzw. Personal-Mitarbeiter

Der Arbeitsaufwand beziffert sich auf diese Schätzwerte:

1.	organisatorische Belange:	8 Stunden
2.	konzeptionelle Belange:	40 Stunden
3.	technische Belange:	48 Stunden

Die folgenden Sachmittel sind notwendig:

1. ein Domain Name oder mehrere Domain Names
2. ein Webserver
3. ein Datenbankserver
4. ein E-Mail-Server
5. ein E-Mail-Konto

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 3.1.1., 3.3.1, 3.3.2, 3.3.3 und 3.3.4.

4.2.5 Kommunikation mit Stakeholdern versendet

Das Projekt sollte den Stakeholdern gegenüber in geeigneter Form kommuniziert werden. Dies kann z. B. per Post bzw. E-Mail erfolgen. Der Zweck dahinter ist das Abbauen von Bedenken und Ressentiments gegenüber dem Vorhaben.

Dieser Schritt beinhaltet unter anderem die kurze Vorstellung des Projektes in verständlicher Weise, das Nennen der Ziele, um den Stakeholdern den Nutzen des Projektes zu vermitteln, und das Erbitten der Durchführungsfreigabe bei relevanten Stakeholdern.

Es ist darauf zu achten, dass Stakeholder dem Projekt in der Regel sehr verhalten bis abwehrend gegenüberstehen.

ANMERKUNG Dieser Meilenstein ist Bestandteil des Arbeitspakets PSP 1.1 und 1.3.

4.2.6 Durchführungsfreigabe erhalten

Vor Beginn der Durchführung muss die Durchführungsfreigabe aller relevanten Stakeholder vorliegen. Die zu informierenden Stakeholder sind aus der Verantwortlichkeiten-Matrix/RACI-Matrix ersichtlich (vgl. Kapitel 5 Rollen und Verantwortlichkeiten).

ANMERKUNG Dieser Meilenstein ist Bestandteil des Arbeitspakets PSP 1.3.

4.2.7 Use Cases definiert und E-Mail-Templates erstellt

Vor der tatsächlichen Durchführung muss entschieden werden, welche Szenarien bei der Erstellung der Phishing-Kampagnen verwendet werden sollen. Dazu sollten Use Cases – organisationsspezifische Szenarien – entwickelt und auf dieser Grundlage anschließend die E-Mail-Templates verfasst werden.

Bei Erstellung dieser sollte auf einen authentischen Bezug geachtet werden, damit durch Betreff und Inhalt hohes Interesse beim Empfänger erwecken und ihn zum Klicken auf einen Link zu verleiten.

Auch für die Awareness-Maßnahme und das Reaktionsmanagement sollten E-Mail-Templates erstellt werden. Beispiele finden sich in Kapitel 6.1 E-Mail-Templates.

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 3.2.1, 3.2.3 und 4.1.

4.2.8 Kampagnenplan erstellt

Zur Durchführung der Phishing-Simulation muss ein Kampagnenplan erstellt werden, in welchem festgelegt wird, welche Zielgruppe an welchem Tag welche Phishing-E-Mail entsprechend der Use Cases erhalten soll. Dies dient der Planung entsprechender Ressourcen bei den beteiligten Akteuren. Dabei muss die Zielgruppensegmentierung beachtet werden. Sollte eine Awareness-Maßnahme geplant sein, sollte diese zirka 14 Tage vor der ersten Phishing-Kampagne versendet werden, um genügend Abstand zwischen Awareness und Angriff zu wahren und eine realitätsnahe Umgebung zu schaffen. Bei mehreren durchzuführenden Kampagnen sollte ein gewisser zeitlicher Abstand beachtet werden, um nachhaltige Effekte innerhalb der Angehörigen der Organisation aufzuzeigen.

Abbildung 7 zeigt einen exemplarischen Kampagnenplan mit fünf Testgruppen.

Datum	Use Case	Test-gruppe 1	Test-gruppe 2	Test-gruppe 3	Test-gruppe 4	Test-gruppe 5
Tag, Datum	Awareness-Schulung 1		A1			
Tag, Datum	Kampagne 1	P1	P2	P3		
Tag, Datum	Awareness-Schulung 2					A2
Tag, Datum	Kampagne 2	P4	P5			
Tag, Datum	Kampagne 3				P6	P7

Abbildung 7: Kampagnenplan und Themenzuordnung mit Phishing-Kampagnen

Anhand der Projektziele können sich verschiedene Fragestellungen ergeben (vgl. Abbildung 8), die mithilfe der einzelnen Kampagnen untersucht werden sollen. Dabei bieten sich beispielsweise folgende Fragestellungen an:

Kampagne	Fragestellung
P1	Wie hoch ist die Klickrate bei einer Phishing-Attacke ohne vorherige Awareness-Schulung?
P2	Wie unterscheidet sich Klickverhalten zu Testgruppe 1 nach einer Awareness-Schulung?
P3	Wie hoch ist die Klickrate bei einer Phishing-Attacke ohne vorherige Awareness-Schulung bei der Zielgruppe des berufsintegrierten Bachelorstudiengangs Allgemeine Verwaltung und des Masterstudiengangs Public Governance? Gibt es einen Unterschied beim Klickverhalten zwischen Berufstätigen und Studenten?
P4	Wie ändert sich das Klickverhalten nach einer ersten Phishing-Attacke?
P5	Wie ändert sich das Klickverhalten nach einer Schulung und ersten Phishing-Attacke?
P6	Wie verhält sich die Vergleichsgruppe, die bisher keine Awareness-Schulung oder Phishing-Attacke erhalten hat, im Vergleich zu den anderen Testgruppen?
P7	Wie verhält sich die Vergleichsgruppe, die zuvor eine Awareness-Schulung erhalten hat, aber noch keine Phishing-Attacke erlebt hat, im Vergleich zu den anderen Testgruppen?

Abbildung 8: Fragestellung der Kampagnen

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 3.2.2 und 4.2.

4.2.9 Landingpage und Informationsseite vorbereitet

Der Ordner „campaignData“ (vgl. 6.2.2 Projekt-Ordnerstruktur) enthält für jede einzelne Phishing-Kampagne die Landingpage und alle dafür notwendigen Ressourcen.

Die gewünschte Original-Seite muss dafür geklont werden. Dafür können je nach Zugänglichkeit der Landingpage auch öffentliche Tools, wie z. B. der Webdienst SaveWeb2ZIP, genutzt werden. Sämtliche Ressourcen (HTML, CSS, JavaScript, Bilder, Schriftarten) werden dafür heruntergeladen. Ein Vergleich der Original-Seite und der Landingpage muss dennoch erfolgen. Eventuelle Abweichungen sollten korrigiert werden, um die Ähnlichkeit zu maximieren.

1. Die Landingpage sollte in „index.php“ umbenannt werden. An ihr müssen einige Änderungen vorgenommen werden, damit sichergestellt ist, dass keine Anmeldedaten übermittelt werden können.

2. Die Attribute „action“ und „method“ des Anmeldeformulars dürfen keinen Wert mehr besitzen. Damit wird verhindert, dass Daten übermittelt werden. Dem input-Feld für den Benutzernamen und dem Passwort wird ein Attribut „onclick“ mit dem Wert „phisim_alert(); checkCookie(clickName)“ hinzugefügt. Damit werden JavaScript-Funktionen aufgerufen. (vgl. 6.2.9 Inhalt cookie_set.js, 6.2.12 Inhalt db_insert.js und 6.2.14 Inhalt phisim_alert.js)

3. Sollte die Landingpage über ein öffentliches Netz auch von organisationsfremden Personen aufgerufen werden können, ist eine Datenschutzerklärung (vgl. 6.3.1 Datenschutzerklärung) notwendig, welche auf der Landingpage verlinkt werden muss.

4. In Zeile 1 einer jeden Landingpage muss zusätzlich Code eingefügt werden. Das ist wichtig, weil hier Cookies gesetzt werden, was nur geschieht, wenn der HTTP-Header noch nicht beendet ist. Ein HTTP-Header wird beendet, sobald Inhalte übermittelt werden, die auf der Seite angezeigt wer-den (ACHTUNG: Dies gilt auch für HTML-Kommentare, die zwar nicht auf der Seite angezeigt wer-den, aber trotzdem Inhalt in diesem Sinne darstellen). (vgl. 6.2.6 PHP-Skript in Zeile 1 jeder Landingpage)

5. Im head-Bereich des HTML-Gerüsts muss Quellcode eingefügt werden. Dieser stellt JavaScript- und CSS-Ressourcen zur Verfügung. Diese werden benötigt, um mit den Cookies beim Klicken in der Anmeldemaske umzugehen und die erhobenen Daten in die Datenbank einzutragen. Ebenfalls werden Design-Anweisungen für eine Warnmeldung eingebunden. (vgl. 6.2.7 Includes für Cookies und der Datenbank in JavaScript sowie Design-Anweisungen für Warnmeldung)

6. Zusätzlich muss noch eine Informationsseite entworfen werden, die abstrakt oder spezifisch über Phishing informiert. Diese sollte auch im Hinweisfenster verlinkt sein, damit der Betroffene sich bei einem Klick in die Login-Maske weiter informieren kann.

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 3.2.2 und 3.3.5.

4.2.10 Awareness- und Phishing-Kampagne versendet

Der Versand einer Awareness-Kampagne ist optional.

Der Versand der E-Mails wird über die Seriendruckfunktion von Microsoft Word in Kombination mit Microsoft Outlook realisiert. Auf dem PC, welcher den Versand vornimmt, wird ein neues Profil mit dem entsprechenden E-Mail-Konto angelegt. Die E-Mail wird in Microsoft Word vorbereitet und kann mit einer Excel-Tabelle als Datengrundlage verknüpft werden, sodass die E-Mails anschließend mit Vor- und Nachnamen als persönliche Ansprache an die jeweiligen E-Mail-Adressen versendet werden können. Es kann auch eine andere Datenquelle genutzt werden. Außerdem muss keine persönliche Ansprache erfolgen, welche jedoch die Authentizität der E-Mail erhöht.

Weiterhin ist darauf zu achten, dass ein günstiger Versand-Zeitpunkt gewählt wird, damit interkollegiale Absprachen möglichst ausbleiben.

Ebenfalls sind interne Regelungen und technische Voraussetzungen für den E-Mail-Massenversand zu prüfen und zu beachten.

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 4.3 und 4.4.

4.2.11 Auswertung und Abschlussbericht versendet

Im Anschluss an die durchgeführte Phishing-Simulation muss eine Auswertung der Ergebnisse stattfinden. Dies kann je nach vorab definierten Zielen oder Kennzahlen differenzieren. Mögliche Auswertungsparameter können sein: E-Mails gelesen, Aufrufhäufigkeit des Phishing-Links, Eingabehäufigkeit Credentials, Melderate der Phishing-E-Mail, unterschiedliches Klickverhalten nach Zielgruppen, Klickraten im Zeitverlauf, etc.

Der Abschlussbericht stellt den formalen Abschluss des Projektes dar und dient der Zusammenfassung des Projektes und einer übersichtlichen Darstellung der Ergebnisse. Er kann weiterhin Handlungsempfehlungen für weitere Maßnahmen enthalten. Der Projektabschlussbericht wird nach Projektabschluss allen relevanten Stakeholdern zur Verfügung gestellt werden, um diese über den Projektverlauf und die Ergebnisse in Kenntnis zu setzen.

ANMERKUNG Die betreffenden Arbeitspakete sind PSP 5.1 und 5.2.

4.2.12 Schulungen durchgeführt

Je nach den Ergebnissen der Phishing-Simulation und der anfangs festgelegten Ziele muss entschieden werden, ob der Bedarf an Schulungen für die ganze Organisation oder nur für bestimmte Abteilungen besteht.

ANMERKUNG Das betreffende Arbeitspaket ist PSP 5.3.

5 ROLLEN UND VERANTWORTLICHKEITEN

Die jeweiligen Verantwortlichkeiten der Projektmitglieder und der Stakeholder können anhand einer Verantwortlichkeiten-Matrix bzw. RACI-Matrix ermittelt werden. „RACI" steht für die Begriffe Responsible, Accountable, Consulted und Informed.

Der Begriff „Responsible" legt den Verantwortlichen für eine spezifische Aufgabe oder Leistung fest. Es können weitere Personen für die Erfüllung hinzugezogen werden.

Der Begriff „Accountable" legt den Rechenschaftspflichtigen fest, der Rechenschaft für den Abschluss einer Aufgabe leistet. Diese Person kann Aufgaben an Angehörige der Gruppe „Responsible" delegieren und prüft anschließend die dabei entstandenen Ergebnisse.

Der Begriff „Consulted" umfasst die Rolle des Beraters. Diese Rolle umfasst Fachexperten oder Dritte, die nicht direkt an der Durchführung beteiligt sind.

Der Begriff „Informed" beschreibt die Rolle der Informierten. Diese werden bspw. über den Abschluss einer Aufgabe informiert, um Transparenz zu bewahren. Die Kommunikation erfolgt in der Regel einseitig.

Die Tabelle (vgl. Abbildung 9) ist ein Lösungsvorschlag für eine solche RACI-Matrix.

Aufgrund gesetzlicher Regelungen sind diverse Verantwortliche zwingend mit einzubeziehen. Dies betrifft den Datenschutzbeauftragten, den Beauftragten für Informationssicherheit oder Personalvertretungen (Betriebs- bzw. Personalrat). Zu beachten sind gesetzliche Reglungen nach der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, EU-DSGVO), Bundesdatenschutzgesetz (BDSG) bzw. Sächsischem Datenschutzdurchführungsgesetz (SächsDSDG), Bundespersonalvertretungsgesetz (BPersVG) bzw. Sächsisches Personalvertretungsgesetz (SächsPersVG) und weitere interne Dienst- oder Arbeitsanweisungen.

	Projektleitung	Konzept-Verantwortlicher	IT-Verantwortlicher	Auftraggeber	Organisationsleitung	Beauftragter für Informationssicherheit	Personalvertretung	IT-Koordination	Datenschutzbeauftragter	Computer Emergency Response Team (CERT)	weitere Interessenvertreter (Zielgruppen)
Ziele und Zielgruppen identifiziert	A	R		C							
Stakeholder identifiziert	R	C		A							
Risiken identifiziert und analysiert	A	R	R	C	C	C	C	C	C	I	C
Ressourcenplan aufgestellt	A	R	R	I							
Kommunikation mit Stakeholdern versendet	R/A	C	C	I	I	I	I	I	I	I	I
Durchführungsfreigabe erhalten	R	I	I	A							
Use Cases definiert und E-Mail-Templates erstellt	A	R		I							
Landingpage und Informationsseite vorbereitet	A	C	R						C		
Kampagnenplan erstellt	A	R	C	I			(I)	I		I	(I)
Awareness- und Phishing-Kampagne versendet	A		R					C		I	(I)
Auswertung Abschlussbericht versendet	R/A			I	I	I	I			(I)	(I)
Schulungen durchgeführt					A	R					

Abbildung 9: Beispiel für eine RACI-Matrix

6 METHODEN, WERKZEUGE UND DOKUMENTE

Nachfolgend werden verschiedene bewährte Methode, Werkzeuge und Dokumente zur Verfügung gestellt. Alle Dokumente dienen lediglich als Beispiel und müssen für den eigenen Gebrauch sowie die organisationsspezifischen Gegebenheiten und den Projektkontext angepasst werden.

6.1 E-Mail-Templates

Folgende E-Mail-Templates dienen als Beispiel für das Durchführen einer Phishing-Simulation. Einige Textpassagen müssen angepasst werden. Es können auch eigene Texte verfasst werden.

6.1.1 Reaktionsmanagement

Da Phishing eine ernstzunehmende Herausforderung ist, werden aufmerksame Teilnehmer der Simulation Phishing-E-Mails an die zuständige Stelle Ihrer Organisation melden. Die sogenannte Meldekette sollte bekannt sein. Dabei ist darauf zu achten, dass die Meldekette nicht überlastet wird, was aber durch eine ausgewählte Gruppengröße sowie eine zeitlich begrenzte Projektlaufzeit vermieden werden kann. Als Grundlage für das Reaktionsmanagement wird den Mitarbeitern des CERT dafür ein Standard-Text zur Verfügung gestellt, den sie aufmerksamen Teilnehmern als Antwort auf eine gemeldete Phishing-E-Mail senden können.

Abbildung 10 zeigt dabei ein mögliches Beispiel.

Sehr geehrte Damen und Herren,

vielen Dank für Ihren Hinweis auf eine im Umlauf befindliche Spam- und Phishing-E-Mail, die angeblich von <<E-Mail-Sender>> versendet wurde.

Mit Ihrer Meldung haben Sie genau richtig gehandelt und helfen so die Informationssicherheit in unserer Organisation zu erhöhen.

Die betreffende E-Mail wurde im Rahmen einer Phishing-Simulation mit Genehmigung und Wissen der Verantwortlichen verschickt und dient lediglich zu Sensibilisierungszwecken.

Es wurden keine persönlichen Daten erhoben und es lassen sich keine Rückschlüsse auf Ihre Person ziehen. Sie haben mit Ihrer Meldung an <<CERT>> richtig gehandelt. Ihre Meldung wird keinerlei persönliche Konsequenzen für Sie haben.

Nach Abschluss der Phishing-Simulation <<Datum>> werden deren Ergebnisse veröffentlicht und es werden weitere Hinweise zur Erhöhung der Informationssicherheit in unserer Organisation zur Verfügung gestellt.

Wir bedanken uns für Ihre Achtsamkeit und Ihre Mitwirkung.

Bitte informieren Sie keine weiteren Personen über diese Untersuchung, damit eine qualitativ aussagekräftige Untersuchung sichergestellt werden kann. Vielen Dank!

Wenn Sie mehr über Phishing im Allgemeinen sowie den Umgang damit in unserer Organisation erfahren wollen, können Sie sich auf dieser Seite weiter informieren.

Mit freundlichen Grüßen

<<Vorname>> <<Name>>

Abbildung 10: Vorlage für das Reaktionsmanagement

6.1.2 Awareness-Maßnahme

Diese E-Mail wird durch die zuständige Stelle für IT- und Informationssicherheit, verschickt, um die Authentizität und Plausibilität dieser „simulierten“ Informations-E-Mail zu bekräftigen. Dabei wird darauf hingewiesen, dass es in der letzten Zeit gehäuft zu Phishing-Angriffen in der Organisation gekommen ist und anhand welcher Merkmale, wie unbekanntem Absender oder falscher Schreibweisen von Namen und Webseiten, man Phishing-E-Mails allgemein erkennt.

Abbildung 11 zeigt dabei ein mögliches Beispiel.

ACHTUNG! Gehäufte Phishing-E-Mails in unserer Organisation

Sehr geehrte Damen und Herren,

in unserer Organisation sind in den letzten Wochen gehäuft Phishing-E-Mails gemeldet worden.
Bei diesen waren insbesondere Ihre persönlichen E-Mail-Adressen (max.mustermann@beispiel.de) betroffen.

Bitte seien Sie aufmerksam und achten Sie auf folgende Indikatoren:

- unbekannte Absender
- falsche Schreibweisen von Namen und Webseiten
- abweichende Absenderadressen
- Rechtschreibfehler im E-Mail-Text

Falls Ihnen eine E-Mail verdächtig vorkommt, melden Sie diese an das <<CERT>> (<<E-Mail-Adresse CERT>>)

Weitere Informationen zum Thema Phishing erhalten Sie auf der Webseite des BSI (Bundesamt für Sicherheit in der Informationstechnologie):
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html

Mit freundlichen Grüßen

<<Absender z. B. Beauftragter für Informationssicherheit>>

Abbildung 11: E-Mail-Templates der Awareness-Maßnahme und Phishing-Kampagnen

6.2 Codebeispiele, Konfiguration und Projektaufbau

6.2.1 Datenschema der Tabelle statistics

Um eine Auswertung der Phishing-Simulation vornehmen zu können, ist ein persistenter Speicher in Form einer relationalen Datenbank notwendig. Empfehlenswert ist eine MySQL- oder eine MariaDB-Datenbank.

Das Datenbankschema der benötigten Tabelle wird wie folgt definiert (vgl. Abbildung 12):

statistics					
id	person_id	campaign	actionType	clickTime	counterVal
INT	VARCHAR(40)	INT	VARCHAR(10)	DATETIME	INT
NOT NULL	NULL	NULL	NULL	NULL	NULL
PRIMARY					
AUTO_INCREMENT					

Abbildung 12: Datenschema der Tabelle „statistics"

Der Primärschlüssel „id“ wird selbstständig inkrementiert. Somit kann gewährleistet werden, dass die Daten innerhalb der Datenbank integer sind und nicht durch das Projektteam gelöscht wurden. Ein weiteres Augenmerk kann auf die Spalte „person_id“ gelegt werden, denn darin wird der Inhalt des „phisim“-Cookies abgespeichert. In der Spalte „campaign“ wird die jeweilige Kampagnennummer abgespeichert, sodass auch mehrere Phishing-Kampagnen parallel erfolgen können. Die Spalte „actionType“ speichert, ob ein Betroffener die Landingpage besucht hat oder ob er in die Login-Maske geklickt hat und damit versucht hat, sich anzumelden und Credentials einzugeben. Die Spalte „clickTime“ speichert den Zeitstempel der Eintragung auf dem Datenbankserver. Die Spalte counterVal“ liest den Inhalt des jeweiligen Coockies aus und speichert so die Anzahl der Versuche des jeweiligen actionTypes.

Um diese Tabelle zu erstellen, kann folgende SQL-Anweisung genutzt werden:

```
1 -- Create table „statistics“ with six columns
2 CREATE TABLE `statistics` (`id` INT NOT NULL AUTO_INCREMENT , `person_id` VAR-CHAR(40) NULL ,
3 `campaign` INT NULL , `actionType` VARCHAR(10) NULL , `clickTime` DATETIME NULL , `counter-Val`
4 INT NULL , PRIMARY KEY (`id`)) ENGINE = InnoDB;
```

6.2.2 Projekt-Ordnerstruktur

Die dem Projekt zugrundeliegende Ordnerstruktur richtet sich nach den folgenden Vorgaben. Dabei werden Konfigurationsdateien in einem nicht zugänglichen Ordner abgelegt und alle für die Phishing-Kampagne notwendigen Skripte in einen öffentlichen Ordner.

```
project
|
+---config
|       config_cookie.php
|       config_db.dev.php
|       config_db.php
|       config_db.prod.php
|
+---public
|   |   index.html
|   |
|   +---campaignData // data needed for the landingpage of a specific campaign
|   |
|   +---cookie
|   |       cookie_set.js
|   |       cookie_set.php
|   |
|   +---css
|   |       style.css // if needed
|   |       sweetalert2.min.css // external resource made internally
|   |
|   +---datenschutzerklaerung
|   |       datenschutzerklaerung.html
|   |
|   +---db
|   |       db_connect.php
|   |       db_insert.js
|   |       db_insert.php
|   |       db_insert_jquery.php
|   |
|   +---dist
|   |   \---img
|   |           logo.svg // if needed
|   |           header-img.png // image needed for the alert
|   |
|   +---info_site
|   |       info_site.html
|   |
|   +---js
|   |       phisim_alert.js
|   |
|   \---tools
|           main_script.php
|           multi_digit.php
|
|   .htaccess
```

Die folgende Tabelle (vgl. Abbildung 13) zeigt die Rechtevergabe auf dem Webserver, die sich hilfreich erwiesen hat.

Bereich	Verzeichnisberechtigung	Dateiberechtigung
config-Bereich	700	600
public-Bereich	755	644

Abbildung 13: Berechtigungen auf dem Webserver in der Oktalnotation

6.2.3 Inhalt config_cookie.php

Diese Datei konfiguriert die globale Lebensdauer eines Cookies für die gesamte Phishing-Simulation.

Zu beachten ist, dass, um eine leicht qualitative Auswertung der einzelnen Phishing-Kampagnen zu gewährleisten (auch im Hinblick auf evtl. Schulungsmaßnahmen zwischen den Kampagnen), dieses Cookie dazu dienen soll, Browser zu identifizieren, die ihre Cookies nicht löschen. Prämisse dabei ist, dass Personen ihren Standardbrowser verwenden und so eine Zuordnung der Kampagnen zu einer ID ermöglicht wird. Dabei können keinerlei Rückschlüsse auf eine natürliche Person gezogen werden. Sollte der gleiche Benutzer ein anderes Gerät oder einen anderen Browser benutzen, wird ein neues Cookie mit einer neuen ID gesetzt. Sollte der Cookie gelöscht werden, verhält es sich ebenso.

```
<?php

$config_cookie = array(
      'lifetime' => 90, // in days
)

?>
```

6.2.4 Inhalt config_db.php

Diese Dateien steuern den Datenbankzugriff. Da die Zugangsdaten für eine Datenbank zwischen Entwicklungssystem und Produktivsystem unterschiedlich sein können, wird die Server-Name-Variable ausgelesen und in Abhängigkeit des Rückgabewertes eine unterschiedliche Konfigurationsdatei geladen. So ist es möglich, die gleichen Skripte in der Entwicklungs- und der Produktivumgebung zu nutzen, ohne Daten anpassen zu müssen.

```
<?php

if ($_SERVER['SERVER_NAME'] === '<<FQDN>>') {
        include_once('config_db.prod.php');
} else if ($_SERVER['SERVER_NAME'] === 'localhost') {
        include_once('config_db.dev.php');
}

?>

<?php

$config_db = array(
        'dbHost' => '<<dbhost>>',
        'dbName' => '<<db>>',
        'dbUser' => '<<user>>',
        'dbPass' => '<<password>>',
        'dbPort' => '<<port>>',
        'dbCharset' => '<<charset>>',
        'dbEngine' => 'InnoDB',
)

?>
```

6.2.5 Inhalt config.php der einzelnen Phishing-Kampagne

Jeder einzelnen Phishing-Kampagne kann eine eigene Kampagnen-Nummer sowie ein Kampagnen-Name vergeben werden. Die hier konfigurierten Werte haben Einfluss auf die zu setzenden Cookies. Damit der Besucher der Landingpage nicht verwirrt wird, wenn der Warnhinweis erscheint, kann noch eine individuelle Nachricht passend zum verwendeten E-Mail-Template konfiguriert werden.

```
<?php

$config = array(
        'campaignNo' => 1,
        'campaignName' => 'phisim'
        'campaignMessage' => 'individual campaign message shown in alert'
)

?>
```

6.2.6 PHP-Skript in Zeile 1 jeder Landingpage

In Zeile 1 einer jeden Landingpage muss zusätzlich Code eingefügt werden. Das ist wichtig, weil hier Cookies gesetzt werden, was nur geschieht, wenn der HTTP-Header noch nicht beendet ist. Ein HTTP-Header wird beendet, sobald Inhalte übermittelt werden, die auf der Seite angezeigt werden (ACHTUNG: Dies gilt auch für HTML-Kommentare, die zwar nicht auf der Seite angezeigt wer-den, aber trotzdem Inhalt in diesem Sinne darstellen).

```
<?php

include("./config.php"); // config for campaign information

$campaignNo = $config['campaignNo'];
$campaignName = $config['campaignName'];
if (isset($config['campaignMessage']) && $config['campaignMessage'] !== "") {
        $campaignMessage = $config['campaignMessage'];
} else {
        $campaignMessage = "Die Inhalte der E-Mail sind frei erfunden und entsprechen nicht der
        Realität.";
}

include("../tools/main_script.php"); // all relevant functionallity for setting, reading, in-
crementing cookies and hand over to JavaScript

?>
```

6.2.7 Includes für Cookies und der Datenbank in JavaScript sowie Design-Anweisungen für Warnmeldung

Im HEAD-Bereich des HTML-Gerüsts muss Quellcode eingefügt werden. Dieser stellt JavaScript- und CSS-Ressourcen zur Verfügung. Diese werden benötigt, um mit den Cookies beim Klicken in der Anmeldemaske umzugehen und die erhobenen Daten in die Datenbank einzutragen. Ebenfalls werden Design-Anweisungen für eine Warnmeldung eingebunden.

```
1  <!-- PhiSim JavaScripts/jQuery and Alerts -->
2  <script src="dist/js/jquery.js "></script>
3  <script src="../js/phisim_alert.js"></script>
4  <script src="../cookie/cookie_set.js"></script>
5  <script src="../db/db_insert.js"></script>
6  <link rel="stylesheet" type="text/css" href="../css/sweetalert2.min.css">
```

6.2.8 Inhalt cookie_set.php

Dises PHP-Skript nutzt die PHP-Funktion „setcookie“. Dabei wird die globale Lebensdauer (vgl. 6.2.3 Inhalt config_cookie.php) verwendet. Die Funktion set_Cookie nimmt dabei zwei Parameter entgegen: den Namen und den Wert. Damit die Cookies von modernen Browsern akzeptiert werden, sind die optionalen Parameter „domain“, „secure“ und „httponly“ essenziell und dürfen nicht ohne Wertzuweisung sein, auch wenn diese „NULL“ ist.

```
1  <?php
2  function set_Cookie($name, $value) {
3
4          include("../../config/config_cookie.php");
5
6          setcookie(
7                  $name, // name
8                  $value, // value
9                  time() + (86400 * $config_cookie['lifetime']), // expire, 86400 = 1 day
10                 "/", // path
11                 NULL, // $_SERVER['HTTP_HOST'], // domain
12                 FALSE, // secure
13                 FALSE // httponly
14                 );
15
16         }
17
18 ?>
```

6.2.9 Inhalt cookie_set.js

Für das Setzen von Cookies in JavaScript muss zuerst geprüft werden, ob das Cookie schon gesetzt ist (Funktion „checkCookie“). Danach muss der Wert des Cookies ausgelesen werden (Funktion „getCookie“), um ihn weiter verwenden zu können und zum Abschluss muss das Cookie neu gesetzt werden (Funktion „setCookie“).

```
1  function checkCookie(cookieName) {
2
3          let cookie = getCookie(cookieName);
4          if (cookie != "") {
5                  let clickVal = getCookie(cookieName);
6                  clickVal++;
7                  setCookie(cookieName, clickVal, lifetime);
8          } else {
9                  setCookie(cookieName, clickVal, lifetime);
10         }
11
12 }
13
14 function getCookie(cookieName)
15
16         let cookieArr = document.cookie.split(";");
17         for (var i = 0; i < cookieArr.length; i++) {
18                 let cookiePair = cookieArr[i].split("=");
19                 if (cookieName == cookiePair[0].trim()) {
20                         return decodeURIComponent(cookiePair[1]);
21                 }
22         }
23         return null;
24
25 }
26
27 function setCookie(cookieName, cookieValue, cookieLifetime) {
28
29         let date = new Date();
30         date.setTime(date.getTime() + (cookieLifetime * 24 * 60 * 60 * 1000));
31         const expires = "expires=" + date.toUTCString();
32         document.cookie = cookieName + "=" + cookieValue + "; " + expires + "; path=/";
33
34 }
```

6.2.10 Inhalt db_connect.php

Dieses PHP-Skript stellt die Datenbankverbindung her. Die Konfigurationsdaten kommen aus der „config_db.php“ (vgl. 6.2.4 Inhalt config_db.php), welche in Entwicklungs- und Produktivumgebung unterschieden wird.

```php
<?php

function connectDB()
{
	include("../../config/config_db.php");

	// Create connection
	$conn = new mysqli($config_db['dbHost'], $config_db['dbUser'], $config_db['dbPass'],
	$config_db['dbName']);

	// Check connection
	if ($conn->connect_error) {
		die("Connection failed: " . $conn->connect_error);
	}

	return $conn;
}

?>
```

6.2.11 Inhalt db_insert.php

Dieses PHP-Skript ist verantwortlich für das Einfügen von Datensätzen in die Datenbank. Dabei werden Prepared Statements genutzt, um die Sicherheit der Phishing-Simulation zu erhöhen und SQL-Injektion zu unterbinden. Dabei wird der Zeitstempel nicht vom Webserver erstellt, sondern vom Datenbankserver selbst.

```php
<?php

function insertInto($person_id, $campaign, $actionType, $counterVal) {

	require_once("../db/db_connect.php"); // for connecting the db

	// prepare connection object
	$conn = connectDB();

	// prepare and bind
	$stmt = $conn->prepare("INSERT INTO statistics (person_id, campaign, actionType, click-
	Time, counterVal) VALUES (?, ?, ?, NOW(), ?)");
	$stmt->bind_param("sisi", $person_id, $campaign, $actionType, $counterVal);

	// execute prepared statement
	$stmt->execute();
	print $stmt->error; // to check errors

	// close db connection
	$stmt->close();
	$conn->close();

}

?>
```

6.2.12 Inhalt db_insert.js

Für das Einfügen von Datensätzen in die Datenbank aus JavaScript ist ein AJAX-Aufruf notwendig. Die Funktion wird ausgeführt, sobald ein Nutzer in die Anmeldemaske mit der HTML-ID „.form-control“ klickt. Dies muss individuell konfiguriert werden.

Klickt der Benutzer in die Anmeldemaske, werden Daten mit der POST-Methode an die URL gesendet. Der Zeitstempel, wird vom AJAX-Aufruf generiert und dient der Fehlersuche, da das Skript ebenfalls das Skript „db_insert.php“ (vgl. 6.2.11 Inhalt db_insert.php) nutzt. Dieses lässt den Zeitstempel durch den Datenbankserver setzen.

```
1  // AJAX call for inserting data into db
2  jQuery(document).ready(function () {
3          jQuery('.form-control').on('click', function () {
4
5          let date = new Date();
6          clickVal = getCookie(clickName);
7
8          jQuery.ajax({
9                  method: "POST",
10                 url: "../db/db_insert_jquery.php",
11                 dataType: "text",
12                 data: {
13                         personIdVal: personIdVal,
14                         campaignNo: campaignNo,
15                         actionType: 'click',
16                         clickTime: date.toISOString().slice(0, 19).replace('T', ' '),
17                         counterVal: clickVal
18                 }
19         });
20
21 });
22
23 });
```

6.2.13 Inhalt db_insert_jquery.php

Dieses PHP-Skript ist für die Entgegennahme der in JavaScript über den AJAX-Aufruf generierten Daten verantwortlich. Diese werden wieder an PHP-Variablen übergeben und anschließend mit der Funktion „insertInto“ (vgl. 6.2.11 Inhalt db_insert.php) in die Datenbank eingetragen.

```
1  <?php
2
3  require_once("db_insert.php");
4
5  $person_id = $_POST['personIdVal'];
6  $campaign = $_POST['campaignNo'];
7  $actionType = $_POST['actionType'];
8  $clickTime = $_POST['clickTime'];
9  $counterVal = $_POST['counterVal'];
10
11 insertInto($person_id, $campaign, $actionType, $counterVal);
12
13 ?>
```

6.2.14 Inhalt phisim_alert.js

Dieses PHP-Skript wird ausgeführt, sollte ein Benutzer in der Anmeldemaske Daten eingeben wollen. Grundsätzlich wird diese Meldung über ein externes JavaScript-Framework namens SweetAlert2 generiert, allerdings hätte die die Einbindung der Ressourcen aus externer Quelle ein erhebliches Sicherheitsrisiko bedeutetw, sodass die Warnmeldung nachgebaut werden muss. Die Styling-Anweisungen für die Warnmeldung befindet sich im Ordner css. (vgl. 6.2.2 Projekt-Ordnerstruktur)

Der Inhalt der Warnmeldung muss als HTML-Code komplett in im Skript erfolgen. Dieser muss noch an die individuellen Bedürfnisse angepasst werden.

Um die Warnmeldung wieder zu schließen ist die Funktion „removePhisimAlert“ zuständig. Danach wird noch die falsche Login-Maske entfernt und dem Betroffenen so noch einmal eindrücklich mitzuteilen, dass er auf einer Phishing-Landingpage gelandet ist.

Die jeweiligen DIV-Element-IDs müssen noch der jeweiligen Landingpage angepasst werden.

Ein Beispiel für eine Warnmeldung findet sich in Abbildung 14.

```
function phisim_alert() {

        // overlay
        var overlay = jQuery('<div id="phiSimAlert" class="swal2-container swal2-center swal2-
        grow-fullscreen    swal2-backdrop-show"    style="overflow-y:    auto;"><div    aria-la-
        belledby="swal2-title" aria-describedby="swal2-html-container"class="swal2-popup swal2-
        modal  swal2-icon-error  swal2-show"  tabindex="-1"  role="dialog"aria-live="assertive"
        aria-modal="true"    style="display:    grid;"><button    type="button"    class="swal2-
        close"style="display: none;" aria-label="Close this dialog">×</button><ul class="swal2-
        progress-steps" style="display: none;"></ul><div class="swal2-icon swal2-error swal2-
        icon-show" style="display: flex;"><span class="swal2-x-mark"><span class="swal2-x-mark-
        line-left"></span><span        class="swal2-x-mark-line-right"></span></span></div><img
        class="swal2-image"                          src="../dist/img/header-img.png"alt="<<Bild-
        beschreibung>>"style="width:    30rem;"><h2    class="swal2-title"    id="swal2-title"
        style="display: block;"><<Titel>></h2><div class="swal2-html-container" id="swal2-html-
        container" style="display: block;"><p style="font-size: 1.5em;"><<Untertitel>></p><br><p
        style="font-size:    1.2em;"><<Text>></p><br><p    style="font-size:    1.2em;"><b><span
        style="text-decoration:  underline;"><<fetter,  unterstrichener  Text>></span></b><b><a
        href="../info_site/info_site.html"      target="_blank">Seite      weiter      informi-
        eren</a></b>.</p><br><p style="font-size: 1.5em;">' + campaignMessage + '</p><br><p
        style="font-size: 1.2em;">Sollten Sie weitere Fragen haben, wenden Sie sich bitte an
        CERT    (<a    href="mailto:info@beispiel.de?subject=Fragen    zur    Phishing-Simula-
        tion">info@beispiel.de</a>).</p></div><input    id="swal2-input"    class="swal2-input"
        style="display: none;"><input type="file"class="swal2-file" style="display: none;"><div
        class="swal2-range"    style="display:    none;"><input    type="range"><output></out-
        put></div><select  id="swal2-select"  class="swal2-select"  style="display:  none;"></se-
        lect><div class="swal2-radio" style="display: none;"></div><label class="swal2-check-
        box"style="display:    none;"><input    type="checkbox"    id="swal2-checkbox"><span-
        class="swal2-label"></span></label><textarea   id="swal2-textarea"   class="swal2-tex-
        tarea"style="display:      none;"></textarea><div      class="swal2-validation-message"
        id="swal2-validation-message" style="display: none;"></div><div class="swal2-actions"
        style="display:      flex;"><div      class="swal2-loader"></div><button      type="but-
        ton"class="swal2-confirm  swal2-styled  swal2-default-outline"style="display:  inline-
        block;  background-color:  rgb(221,  107,  85);"  aria-label=""  onclick="removePhi-
        SimAlert()">Okay, ich habe es verstanden.</button><button type="button" class="swal2-
        deny swal2-styled" style="display: none;"aria-label="">No</button><button type="button"
        class="swal2-cancel  swal2-styled"style="display:  none;"  aria-label="">Cancel</but-
        ton></div><div  class="swal2-footer"  style="display:  block;"><<Projektteam>></div><div
        class="swal2-timer-progress-bar-container"><div        class="swal2-timer-progress-bar"
        style="display: none;"></div></div></div></div>');
        overlay.appendTo(document.body);

        // delete login area
        var box = document.getElementById('loginArea');
        box.innerHTML = '';
        var newDiv = document.createElement('div');

        newDiv.innerHTML = 'Zur richtigen Seite gehen: ' + '<a href="<<FQDN>>"><<FDQN>></a>';

        box.appendChild(newDiv);
        box.style.background = '#ff0000a3';

}

function removePhiSimAlert() {
        const element = document.getElementById("phiSimAlert");
        element.remove()
}
```

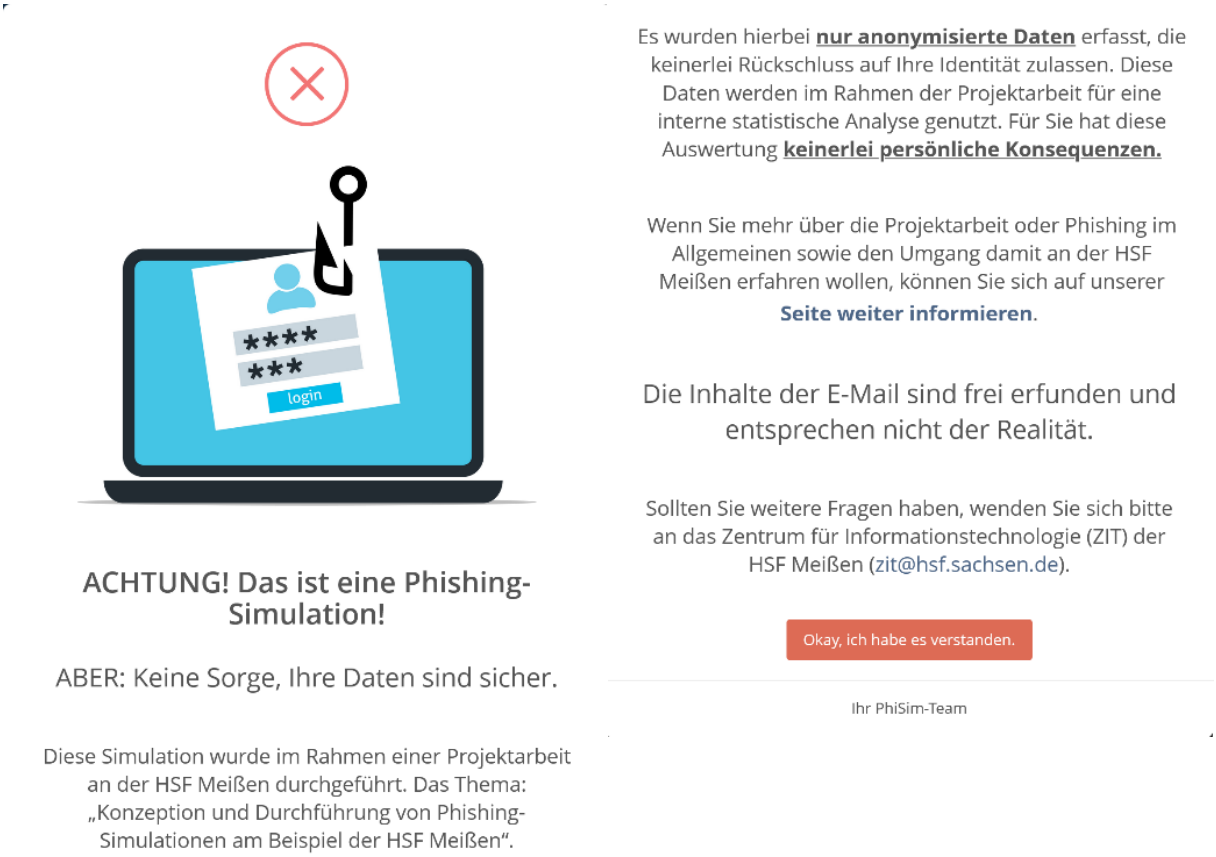

Abbildung 14: Warnhinweis beim Klick in die Anmeldemaske

6.2.15 Inhalt main_script.php

Das Hauptskript verbindet alle anderen Skripte miteinander und kümmert sich um die Abarbeitung der benötigten Funktionalität. Es werden die Namen der Cookies unter zu Hilfenahme der Funktion „multiDigitNumber“ generiert (vgl. 6.2.16 Inhalt multi_digit.php). Damit sind in Abhängigkeit des zweiten Parameters der Funktion beliebig viele Phishing-Kampagnen möglich, da die Kampagnennummer in eine mehrstellige Zahl umgewandelt wird.

Danach wird geprüft, ob das Cookie bereits gesetzt ist und setzen ihn ansonsten mit einem entsprechenden Wert. Dabei wird der Cookie-Name aus der „config.php“ (vgl. 6.2.5 Inhalt config.php der einzelnen Phishing-Kampagne) der jeweiligen Kampagne generiert. Das visitor-Cookie erhält zusätzlich noch die Kampagnen-Nr. sowie den Zusatz „_visit“. Das click-Cookie erhält ebenfalls zusätzlich noch die Kampagnen-Nr. sowie den Zusatz „_click“.

Die Bearbeitung des click-Cookies wird in JavaScript realisiert. Dafür müssen die PHP-Variablen an entsprechende JavaScript-Variablen übergeben werden.

Im Anschluss wird noch der Besuch des Benutzers in die Datenbank eingetragen.

Ein Struktogramm für das PHP-Skript findet sich in Abbildung 15.

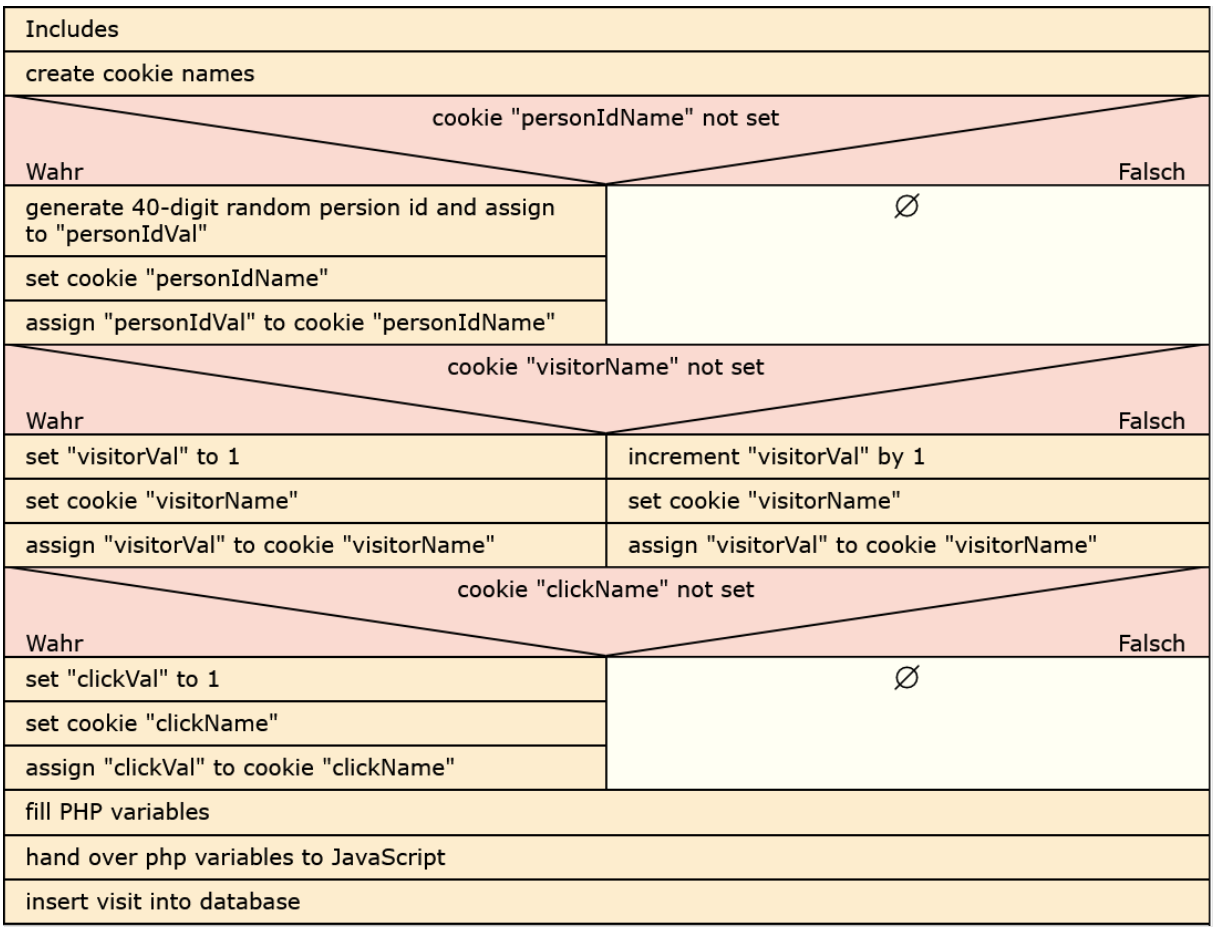

Abbildung 15: Struktogramm für main_script.php

```php
<?php

// requirements and includes
require_once("../cookie/cookie_set.php"); // for setting cookies
require_once("../db/db_insert.php"); // for insert values into the db
require_once("../tools/multi_digit.php"); // for changing campaign number into multi digit number
require_once("../../config/config_cookie.php"); // for cookie relevant specification

// campaign names
$personIdName = $campaignName;
$visitorName = $personIdName . "_camp" . multiDigitNumber($campaignNo, 2) . "_visit"; // format the campaign number into a two digit number with leading zero if necessary
$clickName = $personIdName . "_camp" . multiDigitNumber($campaignNo, 2) . "_click"; // format the campaign number into a two digit number with leading zero if necessary

// person_id
if (!isset($_COOKIE[$personIdName])) {

	$personIdVal = bin2hex(random_bytes(20)); // bin2hex doubles the amount of bytes => db has just VARCHAR(40)

	// setting cookies
	set_Cookie($personIdName, $personIdVal);

	// assigning the value to the cookie if it was in the header -> no refresh needed
	$_COOKIE[$personIdName] = $personIdVal;

}

// visitor
if (!isset($_COOKIE[$visitorName])) {

	$visitorVal = 1; // visited the first time

	// setting cookies
	set_Cookie($visitorName, $visitorVal);

	// assigning the value to the cookie if it was in the header -> no refresh needed
	$_COOKIE[$visitorName] = $visitorVal;

} else {

	$visitorVal = ++$_COOKIE[$visitorName];

	// setting cookies
	set_Cookie($visitorName, $visitorVal);

	// assigning the value to the cookie if it was in the header -> no refresh needed
	$_COOKIE[$visitorName] = $visitorVal;

}

// clicks
if (!isset($_COOKIE[$clickName])) {

	$clickVal = 0;

	// setting cookies
	set_Cookie($clickName, $clickVal);

	// assigning the value to the cookie if it was in the header -> no refresh needed
	$_COOKIE[$clickName] = $clickVal;

}

$personIdVal = $_COOKIE[$personIdName];
```

```
68  $visitorVal = $_COOKIE[$visitorName];;
69  $clickVal = $_COOKIE[$clickName];
70
71  ?>
72
73  <!-- script for handing over PHP variables to JavaScript -->
74  <script>
75
76  let clickName = "<?php echo $clickName; ?>";
77  let lifetime = "<?php echo $config_cookie['lifetime']; ?>";
78  let personIdName = "<?php echo $personIdName; ?>";
79  let personIdVal = "<?php echo $personIdVal; ?>";
80  let campaignNo = "<?php echo $campaignNo; ?>";
81  let clickVal = "<?php echo $clickVal; ?>";
82  let campaignMessage = "<?php echo $campaignMessage; ?>";
83
84  </script>
85
86  <?php
87
88  // insert into visitors
89  insertInto($personIdVal, $campaignNo, "visitor", $visitorVal);
90
91  ?>
```

6.2.16 Inhalt multi_digit.php

Dieses PHP-Skript dient der Transformation der Kampagnen-Nummer in eine mehrstellige Zahl. Der zweite Parameter gibt an, wie viele Stellen die Zahl haben soll. So wird bei der Übergabe einer „3“ z. B. aus „1“ eine „001“. Damit können zeitgleich eine Vielzahl von Phishing-Kampagnen durchgeführt wer-den und die Cookie-Namen werden in Abhängigkeit der Kampagnen-Nr. gewählt.

```
1   <?php
2
3   // change campaign number into a multidigit number
4   function multiDigitNumber($number, $digits)
5   {
6
7           return str_pad($number, $digits, '0', STR_PAD_LEFT);
8
9   }
10
11  ?>
```

6.3 Weitere Dokumente

6.3.1 Datenschutzerklärung

Diese Datenschutzerklärung stellt lediglich ein Beispiel für eine mögliche Datenschutzerklärung dar. Der genaue Einsatz muss mit allen Verantwortlichen abgestimmt und evtl. Maßnahmen getroffen werden. Sollte der Aufruf der Landingpage nicht über ein öffentliches Netz erfolgen, kann auf die Datenschutzerklärung verzichtet werden.

Datenschutzerklärung

1. Datenschutz auf einen Blick

Allgemeine Hinweise

Die folgenden Hinweise geben einen einfachen Überblick darüber, was mit Ihren personenbezogenen Daten passiert, wenn Sie diese Website besuchen. Personenbezogene Daten sind alle Daten, mit denen Sie persönlich identifiziert werden können. Ausführliche Informationen zum Thema Datenschutz entnehmen Sie unserer unter diesem Text aufgeführten Datenschutzerklärung.

<<Zweck und Ziel der Website>>

Nach Abschluss der Phishing-Simulation wird diese Seite offline gestellt (temporär begrenzten Betrieb).

Besondere Verantwortlichkeit

Da diese Website im Rahmen einer Phishing-Simulation erstellt und betrieben wird, ist auch die <<Organisation>> für deren Betrieb verantwortlich. Alle weiteren Informationen finden Sie unter der Datenschutzerklärungen der <<Organisation>> (ACHTUNG: externer Link).

Datenerfassung auf dieser Website

Wer ist verantwortlich für die Datenerfassung auf dieser Website?

Die Datenverarbeitung auf dieser Website erfolgt durch den Websitebetreiber. Dessen Kontaktdaten können Sie dem Abschnitt „Hinweis zur Verantwortlichen Stelle“ in dieser Datenschutzerklärung entnehmen.

Wie erfassen wir Ihre Daten?

Ihre Daten werden automatisch beim Besuch der Website durch unsere IT-Systeme erfasst. Das sind vor allem technische Daten (z. B. Internetbrowser, Betriebssystem oder Uhrzeit des Seitenaufrufs), aber auch Cookies (weitere Informationen dazu können Sie dem Abschnitt „Cookies“ in dieser Datenschutzerklärung entnehmen). Die Erfassung dieser Daten erfolgt automatisch, sobald Sie diese Website betreten.

Wofür nutzen wir Ihre Daten?

Ein Teil der Daten wird erhoben, um eine fehlerfreie Bereitstellung der Website zu gewährleisten. Andere Daten werden im Rahmen einer Phishing-Simulation der <<Organisation>> für eine interne statistische Analyse genutzt.

Welche Rechte haben Sie bezüglich Ihrer Daten?

Sie haben jederzeit das Recht, unentgeltlich Auskunft über Herkunft, Empfänger und Zweck Ihrer gespeicherten personenbezogenen Daten zu erhalten. Sie haben außerdem ein Recht, die Berichtigung oder Löschung dieser Daten zu verlangen. Wenn Sie eine Einwilligung zur Datenverarbeitung erteilt haben, können Sie diese Einwilligung jederzeit für die Zukunft widerrufen. Außerdem haben Sie das Recht, unter bestimmten Umständen die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen. Des Weiteren steht Ihnen ein Beschwerderecht bei der zuständigen Aufsichtsbehörde zu.

Hierzu sowie zu weiteren Fragen zum Thema Datenschutz können Sie sich jederzeit an uns wenden.

2. Hosting

Wir hosten die Inhalte unserer Website bei folgendem Anbieter: <<Anbieter>>

<<Anbieter Beschreibung und Kontaktmöglichkeit>

Die Verwendung von <<Anbieter>> erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Wir haben ein berechtigtes Interesse an einer möglichst zuverlässigen Darstellung unserer Website. Sofern eine entsprechende Einwilligung abgefragt wurde, erfolgt die Verarbeitung ausschließlich auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TTDSG, soweit die Einwilligung die Speicherung von Cookies oder den Zugriff auf Informationen im Endgerät des Nutzers (z. B. Device-Fingerprinting) im Sinne des TTDSG umfasst. Die Einwilligung ist jederzeit widerrufbar.

Auftragsverarbeitung

Wir haben einen Vertrag über Auftragsverarbeitung (AVV) zur Nutzung des oben genannten Dienstes geschlossen. Hierbei handelt es sich um einen datenschutzrechtlich vorgeschriebenen Vertrag, der gewährleistet, dass dieser die personenbezogenen Daten unserer Websitebesucher nur nach unseren Weisungen und unter Einhaltung der DSGVO verarbeitet.

3. Allgemeine Hinweise und Pflicht-informationen

Datenschutz

Die Betreiber dieser Seiten nehmen den Schutz Ihrer persönlichen Daten sehr ernst. Wir behandeln Ihre personenbezogenen Daten vertraulich und entsprechend den gesetzlichen Datenschutzvorschriften sowie dieser Datenschutzerklärung.

Wenn Sie diese Website benutzen, werden verschiedene personenbezogene Daten erhoben. Personenbezogene Daten sind Daten, mit denen Sie persönlich identifiziert werden können. Die vorliegende Datenschutzerklärung erläutert, welche Daten wir erheben und wofür wir sie nutzen. Sie erläutert auch, wie und zu welchem Zweck das geschieht.

Wir weisen darauf hin, dass die Datenübertragung im Internet (z. B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.

Hinweis zur verantwortlichen Stelle

Die verantwortliche Stelle für die Datenverarbeitung auf dieser Website ist:
<<Name>>
<<Straße & Hus-Nr.>>
<<PLZ Ort>>
Telefon: <<Telefon>>
E-Mail: <<E-Mail-Adresse>>

Verantwortliche Stelle ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten (z. B. Namen, E-Mail-Adressen o. Ä.) entscheidet.

Kontaktdaten des Datenschutzbeauftragten

Der Datenschutzbeauftragte des Verantwortlichen ist:
<<Name>>
<<Straße & Hus-Nr.>>
<<PLZ Ort>>
Telefon: <<Telefon>>
E-Mail: <<E-Mail-Adresse>>

Speicherdauer

Soweit innerhalb dieser Datenschutzerklärung keine speziellere Speicherdauer genannt wurde, verbleiben Ihre personenbezogenen Daten bei uns, bis der Zweck für die Datenverarbeitung entfällt. Wenn Sie ein berechtigtes Löschersuchen geltend machen oder eine Einwilligung zur Datenverarbeitung widerrufen, werden Ihre Daten gelöscht, sofern wir keine anderen rechtlich zulässigen Gründe für die Speicherung Ihrer personenbezogenen Daten haben (z. B. steuer- oder handelsrechtliche Aufbewahrungsfristen); im letztgenannten Fall erfolgt die Löschung nach Fortfall dieser Gründe.

Allgemeine Hinweise zu den Rechtsgrundlagen der Datenverarbeitung auf dieser Website

Sofern Sie in die Datenverarbeitung eingewilligt haben, verarbeiten wir Ihre personenbezogenen Daten auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO bzw. Art. 9 Abs. 2 lit. a DSGVO, sofern besondere Datenkategorien nach Art. 9 Abs. 1 DSGVO verarbeitet werden. Im Falle einer ausdrücklichen Einwilligung in die Übertragung personenbezogener Daten in Drittstaaten erfolgt die Datenverarbeitung außerdem auf Grundlage von Art. 49 Abs. 1 lit. a DSGVO. Sofern Sie in die Speicherung von Cookies oder in den Zugriff auf Informationen in Ihr Endgerät (z. B. via Device-Fingerprinting) eingewilligt haben, erfolgt die Datenverarbeitung zusätzlich auf Grundlage von § 25 Abs. 1 TTDSG. Die Einwilligung ist jederzeit widerrufbar. Sind Ihre Daten zur Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, verarbeiten wir Ihre Daten auf Grundlage des Art. 6 Abs. 1 lit. b DSGVO. Des Weiteren verarbeiten wir Ihre Daten, sofern diese zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind auf Grundlage von Art. 6 Abs. 1 lit. c DSGVO. Die Datenverarbeitung kann ferner auf Grundlage unseres berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO erfolgen. Über die jeweils im Einzelfall einschlägigen Rechtsgrundlagen wird in den folgenden Absätzen dieser Datenschutzerklärung informiert.

Empfänger von personenbezogenen Daten

Im Rahmen unserer Geschäftstätigkeit arbeiten wir mit verschiedenen externen Stellen zusammen. Dabei ist teilweise auch eine Übermittlung von personenbezogenen Daten an diese externen Stellen erforderlich. Wir geben personenbezogene Daten nur dann an externe Stellen weiter, wenn dies im Rahmen einer Vertragserfüllung erforderlich ist, wenn wir gesetzlich hierzu verpflichtet sind (z. B. Weitergabe von Daten an Steuerbehörden), wenn wir ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO an der Weitergabe haben oder wenn eine sonstige Rechtsgrundlage die Datenweitergabe erlaubt. Beim Einsatz von Auftragsverarbeitern geben wir personenbezogene Daten unserer Kunden nur auf Grundlage eines gültigen Vertrags über Auftragsverarbeitung weiter. Im Falle einer gemeinsamen Verarbeitung wird ein Vertrag über gemeinsame Verarbeitung geschlossen.

Drittland

Ihre Daten werden nicht in einem Drittland verarbeitet oder einem Dritten in einem Drittland übermittelt.

Widerruf Ihrer Einwilligung zur Datenverarbeitung

Viele Datenverarbeitungsvorgänge sind nur mit Ihrer ausdrücklichen Einwilligung möglich. Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

Widerspruchsrecht gegen die Datenerhebung in besonderen Fällen sowie gegen Direktwerbung (Art. 21 DSGVO)

WENN DIE DATENVERARBEITUNG AUF GRUNDLAGE VON ART. 6 ABS. 1 LIT. E ODER F DSGVO ERFOLGT, HABEN SIE JEDERZEIT DAS RECHT, AUS GRÜNDEN, DIE SICH AUS IHRER BESONDEREN SITUATION ERGEBEN, GEGEN DIE VERARBEITUNG IHRER PERSONENBEZOGENEN DATEN WIDERSPRUCH EINZULEGEN; DIES GILT AUCH FÜR EIN AUF DIESE BESTIMMUNGEN GESTÜTZTES PROFILING. DIE JEWEILIGE RECHTSGRUNDLAGE, AUF DENEN EINE VERARBEITUNG BERUHT, ENTNEHMEN SIE DIESER DATENSCHUTZERKLÄRUNG. WENN SIE WIDERSPRUCH EINLEGEN, WERDEN WIR IHRE BETROFFENEN PERSONENBEZOGENEN DATEN NICHT MEHR VERARBEITEN, ES SEI DENN, WIR KÖNNEN ZWINGENDE SCHUTZWÜRDIGE GRÜNDE FÜR DIE VERARBEITUNG NACHWEISEN, DIE IHRE INTERESSEN, RECHTE UND FREIHEITEN ÜBERWIEGEN ODER DIE VERARBEITUNG DIENT DER GELTENDMACHUNG, AUSÜBUNG ODER VERTEIDIGUNG VON RECHTSANSPRÜCHEN (WIDERSPRUCH NACH ART. 21 ABS. 1 DSGVO).

WERDEN IHRE PERSONENBEZOGENEN DATEN VERARBEITET, UM DIREKTWERBUNG ZU BETREIBEN, SO HABEN SIE DAS RECHT, JEDERZEIT WIDERSPRUCH GEGEN DIE VERARBEITUNG SIE BETREFFENDER PERSONENBEZOGENER DATEN ZUM ZWECKE DERARTIGER WERBUNG EINZULEGEN; DIES GILT AUCH FÜR DAS PROFILING, SOWEIT ES MIT SOLCHER DIREKTWERBUNG IN VERBINDUNG STEHT. WENN SIE WIDERSPRECHEN, WERDEN IHRE PERSONENBEZOGENEN DATEN ANSCHLIESSEND NICHT MEHR ZUM ZWECKE DER DIREKTWERBUNG VERWENDET (WIDERSPRUCH NACH ART. 21 ABS. 2 DSGVO).

Beschwerderecht bei der zuständigen Aufsichtsbehörde

Im Falle von Verstößen gegen die DSGVO steht den Betroffenen ein Beschwerderecht bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes zu. Das Beschwerderecht besteht unbeschadet anderweitiger verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe.

Recht auf Datenübertragbarkeit

Sie haben das Recht, Daten, die wir auf Grundlage Ihrer Einwilligung oder in Erfüllung eines Vertrags automatisiert verarbeiten, an sich oder an einen Dritten in einem gängigen, maschinenlesbaren Format aushändigen zu lassen. Sofern Sie die direkte Übertragung der Daten an einen anderen Verantwortlichen verlangen, erfolgt dies nur, soweit es technisch machbar ist.

Auskunft, Berichtigung und Löschung

Sie haben im Rahmen der geltenden gesetzlichen Bestimmungen jederzeit das Recht auf unentgeltliche Auskunft über Ihre gespeicherten personenbezogenen Daten, deren Herkunft und Empfänger und den Zweck der Datenverarbeitung und ggf. ein Recht auf Berichtigung oder Löschung dieser Daten. Hierzu sowie zu weiteren Fragen zum Thema personenbezogene Daten können Sie sich jederzeit an uns wenden.

Recht auf Einschränkung der Verarbeitung

Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen. Hierzu können Sie sich jederzeit an uns wenden. Das Recht auf Einschränkung der Verarbeitung besteht in folgenden Fällen:

- Wenn Sie die Richtigkeit Ihrer bei uns gespeicherten personenbezogenen Daten bestreiten, benötigen wir in der Regel Zeit, um dies zu überprüfen. Für die Dauer der Prüfung haben Sie das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen.
- Wenn die Verarbeitung Ihrer personenbezogenen Daten unrechtmäßig geschah/geschieht, können Sie statt der Löschung die Einschränkung der Datenverarbeitung verlangen.
- Wenn wir Ihre personenbezogenen Daten nicht mehr benötigen, Sie sie jedoch zur Ausübung, Verteidigung oder Geltendmachung von Rechtsansprüchen benötigen, haben Sie das Recht, statt der Löschung die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen.
- Wenn Sie einen Widerspruch nach Art. 21 Abs. 1 DSGVO eingelegt haben, muss eine Abwägung zwischen Ihren und unseren Interessen vorgenommen werden. Solange noch nicht feststeht, wessen Interessen überwiegen, haben Sie das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen.

Wenn Sie die Verarbeitung Ihrer personenbezogenen Daten eingeschränkt haben, dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Ihrer Einwilligung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Europäischen Union oder eines Mitgliedstaats verarbeitet werden.

4. Datenerfassung auf dieser Website

Cookies

Unsere Internetseiten verwenden so genannte „Cookies“. Cookies sind kleine Datenpakete und richten auf Ihrem Endgerät keinen Schaden an. Sie werden entweder vorübergehend für die Dauer einer Sitzung (Session-Cookies) oder dauerhaft (permanente Cookies) auf Ihrem Endgerät gespeichert. Session-Cookies werden nach Ende Ihres Besuchs automatisch gelöscht. Permanente Cookies bleiben auf Ihrem Endgerät gespeichert, bis Sie diese selbst löschen oder eine automatische Löschung durch Ihren Webbrowser erfolgt.

Cookies können von uns (First-Party-Cookies) oder von Drittunternehmen stammen (sog. Third-Party-Cookies). Third-Party-Cookies ermöglichen die Einbindung bestimmter Dienstleistungen von Drittunternehmen innerhalb von Webseiten. Die Websiten nutzen keinerlei Third-Party-Cookies.

Cookies haben verschiedene Funktionen. Zahlreiche Cookies sind technisch notwendig, da bestimmte Webseitenfunktionen ohne diese nicht funktionieren würden.

Sie können Ihren Browser so einstellen, dass Sie über das Setzen von Cookies informiert werden und Cookies nur im Einzelfall erlauben, die Annahme von Cookies für bestimmte Fälle oder generell ausschließen sowie das automatische Löschen der Cookies beim Schließen des Browsers aktivieren. Bei der Deaktivierung von Cookies kann die Funktionalität dieser Website eingeschränkt sein.

Welche Cookies und Dienste auf dieser Website eingesetzt werden, können Sie nachfolgender Aufstellung entnehmen.

phisim

Dieses Cookie ist eine zufällig generierte 40-stellige ID. Um eine leicht qualitative Auswertung der einzelnen Phishing-Kampagnen zu gewährleisten (auch im Hinblick auf evtl. Schulungsmaßnahmen zwischen den Kampagnen), soll dieses Cookie dazu dienen, Browser, die ihre Cookies nicht löschen, zu identifizieren. Prämisse dabei ist, dass Personen ihren Standardbrowser verwenden und so eine Zuordnung der Kampagnen zu einer ID ermöglicht wird. Dabei können keinerlei Rückschlüsse auf eine natürliche Person gemacht werden. Sollte der gleiche Benutzer ein anderes Gerät oder einen anderen Browser benutzen, wird ein neuer Cookie mit einer neuen ID gesetzt. Sollte der Cookie gelöscht werden, verhält es sich ebenso.

Es sind alle Besucher der Website von diesem Cookie betroffen. Das Cookie wird für 90 Tagen gespeichert.

phisim_campXX_visit

Dieses Cookie wird genutzt, um zu zählen, wie oft die Person, die durch das erstgenannte Cookie identifiziert wird, die Seite besucht hat. XX bezeichnet dabei die Nummer der aktuellen Kampagne. Der Wert des Cookies wird bei jedem Besuch um einen Wert inkrementiert. Sollte der gleiche Benutzer ein anderes Gerät oder einen anderen Browser benutzen, wird ein neues Cookie mit dem Initialwert des Cookies gesetzt. Sollte das Cookie gelöscht werden, verhält es sich ebenso.

Es sind alle Besucher der Website von diesem Cookie betroffen. Das Cookie wird für 90 Tagen gespeichert.

phisim_campXX_click

Dieses Cookie wird genutzt, um zu zählen, wie oft die Person, die durch das erstgenannte Cookie identifiziert wird, seine Login-Daten in die Login-Maske eingeben wollte. XX bezeichnet dabei die Nummer der aktuellen Kampagne. Der Wert des Cookies wird bei jedem Klick um einen Wert inkrementiert. Sollte der gleiche Benutzer ein anderes Gerät oder einen anderen Browser benutzen, wird ein neues Cookie mit dem Initialwert des Cookies gesetzt. Sollte der Cookie gelöscht werden, verhält es sich ebenso.

Es sind alle Besucher der Website von diesem Cookie betroffen. Das Cookie wird für 90 Tagen gespeichert.

Quelle: https://www.e-recht24.de

6.3.2 Fehlermöglichkeits- und Einflussanalyse

Die folgende Tabelle (Abbildung 16) stellt eine exemplarische Matrix für die Fehlermöglichkeits- und Einflussanalyse zur Verfügung. Je nach dem organisationsspezifischen Kontext kann können die entstehenden Risiken abweichen bzw. anders bewertet werden, sodass sich eine andere Matrix ergibt.

ID	Risikobeschreibung			Risikobewertung					Gegenmaßnahme
	Risiko	Kategorie	Ursache	Auftretenwahrscheinlichkeit	Bedeutung	Entdeckungswahrscheinlichkeit	Risiko-Prioritätszahl (RPZ)	Risiko	
				(Skala: 1 = gering, 10 = hoch)					
01	Keine Zustimmung durch entscheidungsbefugte Stakeholder	Durchführung/ Kommunikation	Bedenken, Unverständnis, rechtliche Rahmenbedingungen	7	10	3	210	hoch	zielgerichtete Kommunikation und Erklärung der technischen Realisierung
02	Anzeige durch einen Betroffenen	Durchführung	Unverständnis, Angst vor Datendiebstahl	2	7	10	140	hoch	Aufklärung über Projekt und Datensicherheit über Landingpage Awareness-E-Mail nach Phishing-Kampagne
03	Unzureichende Kommunikation mit Stakeholdern	Kommunikation	Fehlplanung, Missverständnisse, unzureichende, ungenaue Zeitplanung	3	9	4	108	hoch	Aufklärung über Kampagne, Fristsetzungen für Rückmeldungen
04	E-Mail wird als Spam identifiziert und nicht zugestellt	Durchführung	Markierung als Spam	10	10	1	100	hoch	Whitelisting des E-Mail-Absenders im MS365-Tennant bzw. in der Firewall
05	Vertrauensverlust der Mitarbeiter und Studenten der Organisation	Durchführung	Unverständnis, unzureichende Kommunikation	4	4	4	64	mittel	Aufklärung über Kampagne keine Erfassung der Credentials
06	Überlastung Meldekette	Durchführung	zu viele Meldungen der Benutzer an ZIT	3	5	3	45	akzeptabel	Vorlage für das Reaktionsmanagement für CERT wird bereitgestellt Aufklärung über Phishing-Simulation auf Informationsseite der Fake-Website
07	Keine Bereitstellung technischer Komponenten durch IT-Verantwortlichen oder -Koordination	Technik	keine Bereitstellung durch ZIT möglich	2	10	2	40	akzeptabel	Aufbau einer eigenen Server-Landschaft
08	E-Mail wird als Spam gemeldet ("Sie erhalten nicht oft E-Mails von diesem Absender")	Technik	Vorkonfiguration MS365-Tennant Mangelnde Kommunikation mit ZIT	8	4	1	32	akzeptabel	dieses Risiko wird akzeptiert und es werden keine Gegenmaßnahmen getroffen, um eine realitätsnahe Projektdurchführung zu gewährleisten
09	Schulungsmaßnahmen verfehlen Ziel	Durchführung	Schulungsmaßnahme zu schlecht konzipiert	4	2	4	32	akzeptabel	Schulungsmaßnahme überarbeiten Akzeptanz der Schulungsmaßnahme und Auswertung nach Kampagnenende
10	Vorzeitiges Bekanntwerden der Phishing-Simulation	Durchführung	Whistleblower	3	2	4	24	akzeptabel	Zielgruppensegmentierung
11	Webserver fällt aus	Technik	Stromausfall, defekte Hardware, Fehlkonfiguration	1	7	3	21	akzeptabel	Webserver absichern Backup

ID	Risikobeschreibung			Risikobewertung					Gegenmaßnahme
	Risiko	Kategorie	Ursache	Auftretenwahrscheinlichkeit (Skala: 1 = gering, 10 = hoch)	Bedeutung	Entdeckungswahrscheinlichkeit	Risiko-Prioritätszahl (RPZ)	Risiko	
12	Datenbankserver fällt aus	Technik	Stromausfall, Fehlkonfiguration, defekte Hardware	1	7	3	21	akzeptabel	Datenbankserver absichern Backup
13	Vorankündigung der Kampagnen erforderlich	Durchführung	Personalrat erwartet Vorankündigung der Phishing-Simulation	5	4	1	20	akzeptabel	Kommunikation der einschränkenden Aussagekraft bei Vorankündigung gegenüber Stakeholdern
14	Strafrechtliche Verfolgung durch die Staatsanwaltschaft	Durchführung	Anzeige durch einen Betroffenen	1	9	2	18	akzeptabel	Aufklärung über Kampagne keine Erfassung der Credentials
15	Unzureichende Kommunikation zwischen Projektteam	Kommunikation	vorzeitige Beendigung Studium, langfristige Krankheit, Fehlplanung, Unverständnis	1	7	2	14	akzeptabel	Kommunikationsstandards Weeklys Kanban-Board
16	Echte Login-Daten erhalten	Durchführung	Fehlkonfiguration	1	10	1	10	akzeptabel	entsprechende Konfiguration der Website keine Daten senden zu können
17	E-Mails werden durch Mail-Server nicht zugestellt	Durchführung	Stromausfall, Fehlkonfiguration, defekte Hardware	1	9	1	9	akzeptabel	Rücksprache mit Support Dienstleister, korrekte Konfiguration

Abbildung 16: Matrix der Fehlermöglichkeits- und Einflussanalyse

6.3.3 Stylesheet sweetalert2.min.css

Diese Datei ist Bestandteil eines externen Frameworks mit dem Namen SweetAlert2 (vgl. Github). Die neueste Version kann hier heruntergeladen werden: https://github.com/sweetalert2/sweetalert2/releases

Relevant ist nur die Datei „sweetalert2.min.css“.