gibb

Projektauftrag

FPM - Fake Phishing-Mail Service

Auftraggeber	Marc Aeby
Projektleiter	J. Storrer
Autor	J. Storrer
Klassifizierung	Intern
Status	Genehmigt

Änderungsverzeichnis

Datum	Version	Änderung	Autor
01.12.2023	0.1	Erster Draft	J. Storrer
12.12.2023	0.2	Diverse Änderungen	J. Storrer
14.12.2023	1.0	Final Dokument	J. Storrer

Inhaltsverzeichnis

1 Ausgangslage

In einem eher heiklen Unternehmen ist es wichtig, dass Mitarbeiter und Mitarbeiterinnen gegenüber SPAM, Phishing, Social Engineering usw. einen hohen Awareness-Level haben.

Um das Awareness-Level zu erhöhen, wurde bislang mit Newslettern und Tipps & Tricks versucht, die Benutzer zu sensibilisieren. In einer Umfrage, in der die Benutzer gefragt wurden, was sie sich wünschen, um im Bereich IT-Cybersecurity ein höheres Level an Awareness zu erreichen, wurde der Wunsch geäußert, die Mitarbeiter und Mitarbeiterinnen mit Fake-Phishing-Mails zu testen.

In diesem Projekt wird es darum gehen, eine geeignete Phishing-Software oder Plattform zu suchen, diese aufzubauen und mittels der vom Kunden definierten Prozesse eine interne Phishing-Attacke durchzuführen. Als Abschluss dienen Statistiken und Ergebnisse, sowie ein Awareness-Training und Newsletter, um die Cybersecurity Awareness der Mitarbeiterinnen und Mitarbeiter zu erhöhen.

Dieser Service kann beliebig erweitert und ausgereift werden, je nach der eingesetzten Plattform. Als Zusatz können noch PDF-Anhänge als zusätzliche Awareness-Tests angefügt werden.

Der grobe Ablauf wäre, dass die Benutzer eine FPM erhalten, wobei auswählbar ist, wie erkennbar der Fake ist (easy, medium, hard). Diese FPM werden nach dem Zufallsprinzip an verschiedene Mitarbeiter gesendet. So können Zeitabstände, Schwierigkeitsgrade und Häufigkeiten beliebig angepasst werden.

Eine solche FPM wird entweder einen Link mit Aufforderung zur Eingabe der Login-Daten auf einer Fake-Login-Webseite enthalten – oder wenn gewünscht ein manipuliertes PDF, welches sich auf dem Client dann einnistet.

Sobald der Benutzer fälschlicherweise seine Login-Daten auf der Fake-Login-Webseite aus der FPM eingegeben hat, wird er auf eine "OOPSIE"-Seite weitergeleitet, damit der Benutzer ein visuelles Bild für den Lerneffekt hat. Mit der Weiterleitung zum Awareness-Training werden die Mitarbeiter geschult, worauf zu achten ist und was unbedingt zu unterlassen wäre.

Wenn ein Benutzer ein PDF einer FPM herunterlädt, speichert oder öffnet, wird der Benutzer in einer separaten E-Mail darauf aufmerksam gemacht, dass dieses PDF infiziert ist. Ebenso werden hier die Links zum Awareness-Training hinterlegt.

Alle Benutzer, die die E-Mail an die IT richtig gemeldet haben – oder nach dem bekannten Prozess zur Meldung von auffälligen E-Mails – erhalten eine Bestätigungsemail, dass dies ein Test war. Ebenso könnten diese Mitarbeiterinnen und Mitarbeiter ebenfalls am Awareness-Training teilnehmen.

Als Abschluss des Fake-Phishing-Mail-Tests wird in einem Newsletter die Statistik und die Ergebnisse nach Analyse mit dem Kunden bereitgestellt, verarbeitet und dem Benutzer so zur Verfügung gestellt.

Dies ist ein einmaliger Prozess, der etwa ein halbes Jahr dauern wird (Bereitstellung, Konfiguration Plattform, Prozessdefinition mit Kunden, FPM-Versand und Ergebnisanalyse). Empfohlen wird dieser neue Service dann wiederholt, halbjährlich oder jährlich, erneut durchgeführt wird, um die Awareness beizubehalten oder neue Mitarbeiterinnen zu sensibilisieren.

Nachfolgend werden Fake-Phishing-Mails im Dokument **FPM** genannt.

2 Ziele

Folgende Projektziele müssen erreicht werden:

Nr.	Kategorie	Beschreibung	Messgrösse	Prio
1	*Technisches Ziel*	Versand von FPM an Mitarbeiter-Zufallgsgruppen	FPM's wurden an Zufallsgruppen gesendet	M
2	*Technisches Ziel*	Drei schwierigkeitsgrade der FPM (Erkennbarkeit ob Fake, easy – medium - hard)	Die Erkennbarkeit der drei Schwierigkeitslevels wurden definiert	M
3	*Technisches Ziel*	Plattform für Ergebnisse und Statistiken ist vorhanden	Auf einer Plattform können Statistiken und Ergebnisse der Klickraten angeschaut werden	2
4	*Technisches Ziel*	Plattform für Fake-Login-Pages existiert	Nach dem -fälschlicherweise- öffnen des FPM wird der User auf eine Fake Login Page weitergeleitet, um seine Logindaten abzufangen	1
5	*Technisches Ziel*	Plattform für Awareness-Training wurde bereitgestellt	Ein Awareness-Training wurde konzeptioniert und nach Bedürfnissen der Firma erstellt	2
6	*Betriebliches Ziel*	Sensibilisierung der User zur Angstnahme	Die User haben in persönlichen Gesprächen nur noch Respekt- & keine Angst mehr vom Internet. Die User werden achtsamer und wissen auf was sie schauen müssen. Klickrate auf zweite FPM deutlich geringer	M
7	*Betriebliches Ziel*	Schulen der User mit Umgang von Emails	Massgeschneidertes Awareness-Training für den Umgang mit Emails, auf was geachtet werden muss. Klickrate auf dritte FPM deutlich geringer.	1
8	*Lieferobjekt*	Awareness-Training auf Plattform vorhanden	Das massgeschneiderte Awareness-Training wurde mit der Firma definiert und konzeptioniert. Themengebiete und eventuelles Abschlussquiz wurde definiert	2

			und auf der Plattform angeboten.	
9	*Lieferobjekt*	Die 3lvl der FPM's wurden definiert	Es wurde mit dem Kunden besprochen und festgehalten, wie die Erkennbarkeitslevel der Emails sind und welche Fake Login Pages sie repräsentieren sollten.	M
10	*Lieferobjekt*	Statistiken & Ergebnisse werden auf einer Plattform angezeigt	Die Klickraten-Ergebnisse und die Statistik der drei FPMs kann auf einer Plattform eingesehen werden	2
11	*Lieferobjekt*	Newsletter mit Ergebnissen, Tipps & Tricks wurden an die Mitarbeiter versendet	Der Inhalt des Newsletters, Tipps & Tricks und den Ergebnissen wurden mit der Firma besprochen, konzeptioniert und bereitgestellt	1
12	*Leistungsziel*	User sind aufmerksamer, was Phishing-Mails betrifft	Die Klickrate vom ersten FPM zur dritten FPM muss in der Statistik 20% tiefer sein.	1
** Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief*				

Folgende Ziele sind die Vorgaben für die Phase Initialisierung:

Nr.	Kategorie	Beschreibung	Messgrösse	Prio
1	*Technisches Ziel*	Evaluierung FPM-Plattform	Eine Plattform für FPM wurde nach Vorgaben der Firma evaluiert und ist OpenSource	1
2	*Lieferobjekt*	Evaluation Backend FPM	Eine Plattform für FPM wurde nach Vorgaben der Firma evaluiert und ist OpenSource	1
3	*Lieferobjekt*	Grobkonzept Architektur	Das Grobkonzept der Architektur des Backendes, sowie dazugehörige Komponenten, besteht	2
4	*Lieferobjekt*	Serviceidee	Eine Serviceidee wurde visuell dargestellt	3
	Lieferobjekt	Definition der FPM-Levels	Die FPM-Level wurden definiert und dokumentiert	2
5	*Lieferobjekt*	Interne Festlegung und Abstimmung	Prüfung, ob Definition in Studie eingeflossen ist	1

		der Prozesse für interne Phishing-Attacken, wie Zeitabstände & Erkennbarkeitslevel		
6	*Lieferobjekt*	*Erstellung Kostenschätzung (Projektkosten und anschliessende Betriebskosten)*	Prüfen ob in Studie vorhanden ist	3
** Priorität: M = Muss / 1 = hoch, 2 = mittel, 3 = tief*				

3 Rahmenbedingungen

Rahmenbedingungen Phase Initialisierung

- Anwendung von HERMES Projektmethodik die auf das Projekt angepasst ist
- Wenn externe Berater in der Initialisierung eingesetzt werden, muss vorher das Einverständnis des Auftraggebers geholt werden

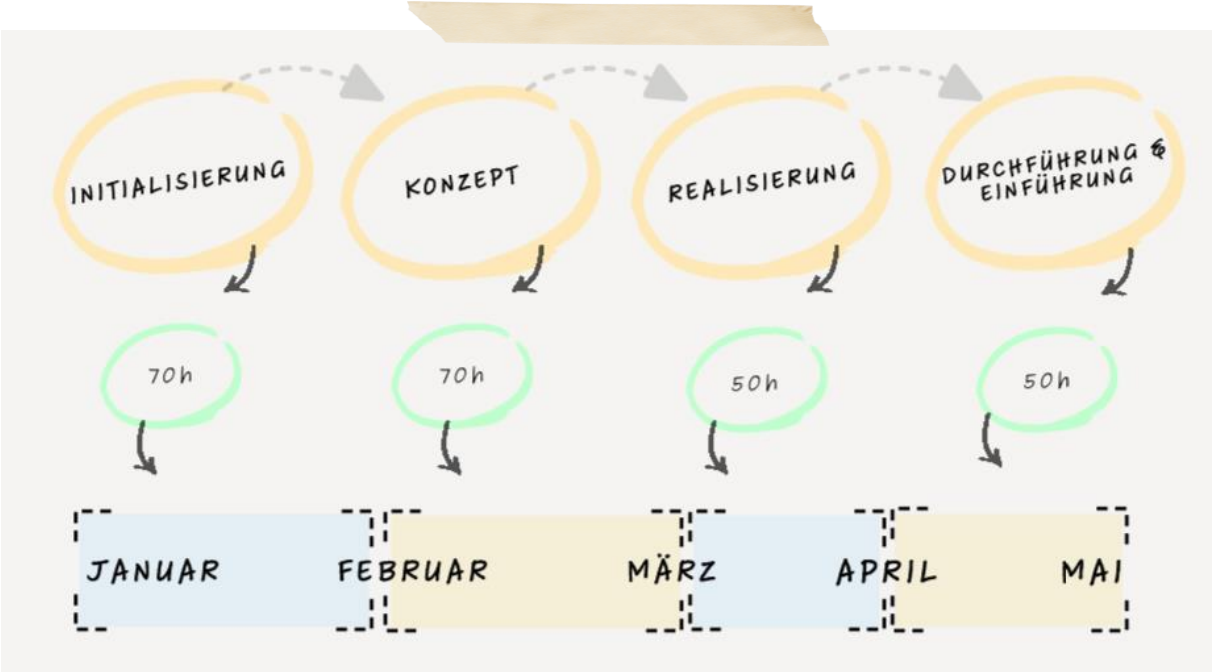
4 Ergebnisse und Termine

Folgende Ergebnisse werden in der Phase Initialisierung vom Projekt erstellt.

Nr	Ergebnis	Termin
1	*Studie*	06.02.2024
2	*Projektauftrag*	06.02.2024
3	*Projektplan*	06.02.2024

Aufwand

Geschätzter interner Personalaufwände in der Phase Initialisierung wird im untenstehenden groben Zeitplan als Grafik aufgezeigt. Diese Aufwände belaufen sich bei der Initialisierung auf ca. 70h



Kosten

Geschätzter interner Personalaufwand beläuft sich auf ca. 32‘000sFr. Der Aufwand wurde mit einem durchschnittlichen internen Ansatz von 170sFr berechnet.

(Material, externe Dienstleistungen, auch Aufwand mit internem Ansatz)

Phase	Geplant
Initialisierung	*CHF 11'900.-*

Ressourcen

Personalressourcen

Die Personalkosten belaufen sich auf Jessica Storrer und wird in der Initialisierung mit CHF 11'900.- gerechnet.

Sachmittel

Es werden keine Sachmittel wie Räume, IT-Infrastruktur, Spezifische Software, etc. benötigt die externen Kosten verursachen. Ein Notfall-Budget von CHF 1000.- ist jedoch eingeplant.

Die Sachmittel werden je nach Evaluation der Plattform in der späteren Dokumentation erläutert.

Kommunikation / Termine

Reporting während der Phase Initialisierung, Information Auftraggeber,

Information der Betroffenen Stellen und Stakeholder

Adressat der Information	Verantwortlich für die Kommunikation	Inhalt	Ziel	Mittel / Medium	Termin
Abteilungsleiter	*Auftraggeber Marc Aeby*	*Ziel und Planung der Projektinitialisierung*	*Die Abteilungen kennen den Auftrag an den Projektleiter*	*eMail*	*KW 6 2024*
Auftraggeber	*Projektleiter J. Storrer*	*Monatlicher Statusbericht*	*Vorschritt des Projekt an AG kommunizieren mit Aussagen zu Termin, Kosten*	*Status Report*	*Monatlich am 1. Arbeitstag im Monat*
Experte	*Experte Beat Loosli*	*Monatlicher Statusbericht*	*Vorschritt des Projekt an AG kommunizieren mit Aussagen zu Termin, Kosten*	*Status Report*	*Monatlich am 1. Arbeitstag im Monat*

5 Risiken

-

Nr.	Risiko-beschreibung	EW	AG	RZ	Massnahmen	Verantw.
	Unvorhergesehener Personalausfall	*2*	*2*	*4*	*Gesund Essen*	*jst*
	Evaluiertes tool nicht funktionsfähig	*2*	*2*	*4*	*Tool einkaufen*	*jst*
	Plattform nicht funktionsfähig	*2*	*2*	*4*	*Plattform extern geben*	*jst*
	Pandemie 2.0	*2*	*2*	*4*	*-*	*jst*

Legende: *EW=Eintretenswahrscheinlichkeit: 1 Niedrig / 2 Mittel / 3 Hoch;*
AG=Auswirkungsgrad: 1 Gering / 2 Mittel / 3 Gross;
RZ=Risikozahl: RZ = EW x AG