fake phishing mail service
&
cybersecurity awareness training

FPM & CAT

-PROJEJKTAUFTRAG-

Auftraggeber	Marc Aeby
Projektleiter	J. Storrer
Autor	J. Storrer
Dokument	ID2132_StorrerJessica_FPM&CAT_Projektauftrag_v1.docx
Klassifizierung	Intern
Status	Genehmigt

Änderungsverzeichnis

Datum	Version	Änderung	Autor
08.03.2024	0.1	Erster Draft	J. Storrer
08.03.2024	1.0	Fertigstellung	J. Storrer

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

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.

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 einen Link mit Aufforderung zur Eingabe der Login-Daten auf einer Fake-Login-Webseite enthalten.

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 Cybersecurity Awareness-Training werden die Mitarbeiter geschult, worauf zu achten ist und was unbedingt zu unterlassen wäre.

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). Empfoh-

len 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 und das Cybersecurity-Awareness-Training **CAT.**

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 und auf der Plattform angeboten.	2
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*				

Tabelle 1 - Projektziele

3. Projektorganisation

Im folgenden Kapitel wird die Organisation des Projektes aufgezeigt.

Der Service wird von der Firma «MJ Cybersecurity Services» angeboten. Der Kunde B&T dient als Pilotkunde.

3.1.1 Rollen

In dieser Übersicht sind die Schlüsselakteure der Projektorganisation aufgeführt, angefangen beim Auftraggeber und Projektleiter bis zum externen Experten. Die Tabelle bietet eine klare Darstellung der Verantwortlichkeiten und Zuständigkeiten der einzelnen Teammitglieder während des Projektablaufs.

Rolle in der Projektorganisation	Name	Kürzel	Funktion / Vertretene Organisationseinheit
Auftraggeber	*M. Aeby*	*mae*	*Leiter Diplomprozess*
Projektleiter	*J. Storrer*	*jst*	*Leiter IT MJ Cybersecurity Services*
Fachspeziallist / Engineer	*J. Storrer*	*jst*	*Fachspezialist und Engineer für Realisierung*
Experte ext.	*B. Loosli*	*blo*	*Experte für Diplomarbeitsbeurteilung*
Experte int.	*R. Maurer*	*rma*	*Von GIBB gestellter Experte für Diplomarbeitsbeurteilung*

Tabelle 2 - Rollen in der Projektorganisation

3.1.2 Organigramm

Folgend wird das Organigramm der Stamm- und Projektorganisation graphisch dargestellt.

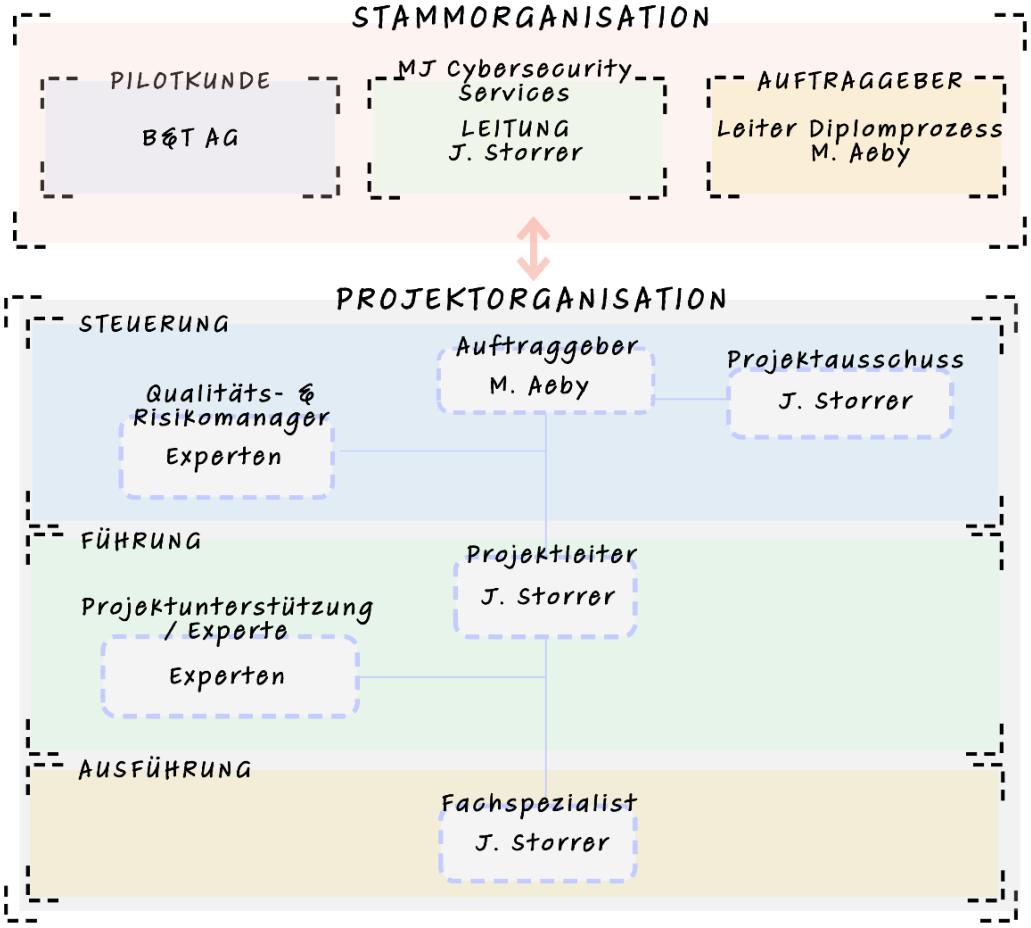

Abbildung 1 – Organigramm Stamm- & Projektorganisation

4. Lieferergebnisse

Im folgenden Kapitel werden die Lieferergebnisse dieses Projekts erläutert.

4.1 Overall

- ✓ Evaluation / Variantenentscheid: Plattformen für FPM und CAT wurden entschieden
- ✓ Serviceidee / Pricing: Eine Serviceidee und dessen Preise, sowie Factsheet wurde erstellt
- ✓ UseCases / Prozesse: Prozesse für FPM und CAT wurden definiert, Data-Sheets und Kundenblätter (Informationsgewinnung Kunde, Must-haves) wurden erstellt
- ✓ Test Cases: Test Cases für den FPM-Versand wurden anhand der erstellten Use-Cases erstellt

4.2 Lieferobjekte FPM

- ✓ Technisches Konzept/Aufbau: Mehrere Kunden betreubar, Multikundenfähiger Service, Parallel aufbaubar
- ✓ Konzepte FPM/FPL: Konzepte der Fake Phishing Mails und Fake Login Pages bestehen/wurden definiert
- ✓ Newsletter/Reporting: Newsletter und Klickratenreport per Ende FPM Service

4.3 Lieferobjekte CAT

- ✓ Trainings; Trainings wurden aufgesetzt, Themen definiert
- ✓ Tests & Quizzes; Div. Test & Quizzes wurden anhand der Trainings-Themen definiert und aufgesetzt
- ✓ Zusatzmaterial; Tipps & Tricks für den Alltag wurden aufgesetzt und bereitgestellt

5. Termine & Kommunikation

Folgend sind die unerlässlichen Termine des Projektes aufgelistet.

Datum / Uhrzeit ***(wenn keine Zeit, 23.58 Uhr)***	**Ereignis**	**Wo / Wie**
11.03.2024 – 14.00 Uhr:	1. Zwischenmeeting	Online, Teams
27.03.2024	Feedback Ermittlung Kundeninfos (Milestone)	Email
01.04.2024	Monatliches Update per Email	Email
08.04.2024 – 16.00 Uhr:	2. Zwischenmeeting	Online, Teams
10.04.2024	Feedback Test Emailkampagne (Milestone)	Email
17.04.2024	Feedback Start Durchführung (Milestone)	Email
01.05.2024	Monatliches Update per Email	Email
15.05.2024	Feedback Versand Newsletter & Report, off. FPM Abschluss (Milestone)	Email
27.05.2024 – 10.00 Uhr	Abschlussmeeting (B&T Vorort)	B&T AG, Tempelstrasse 6 3663 Thun
02.06.2024	Abgabe (Milestone)	Email, Hochladen, Binden

Tabelle 2 - Termine

6. Overview Serviceaufbau

In der folgenden Grafik wird aufgezeigt, wo sich die beiden Services angliedern, sowie wie die externen Parteien damit eingebunden sind und die Kundenbetreuung angegliedert ist.

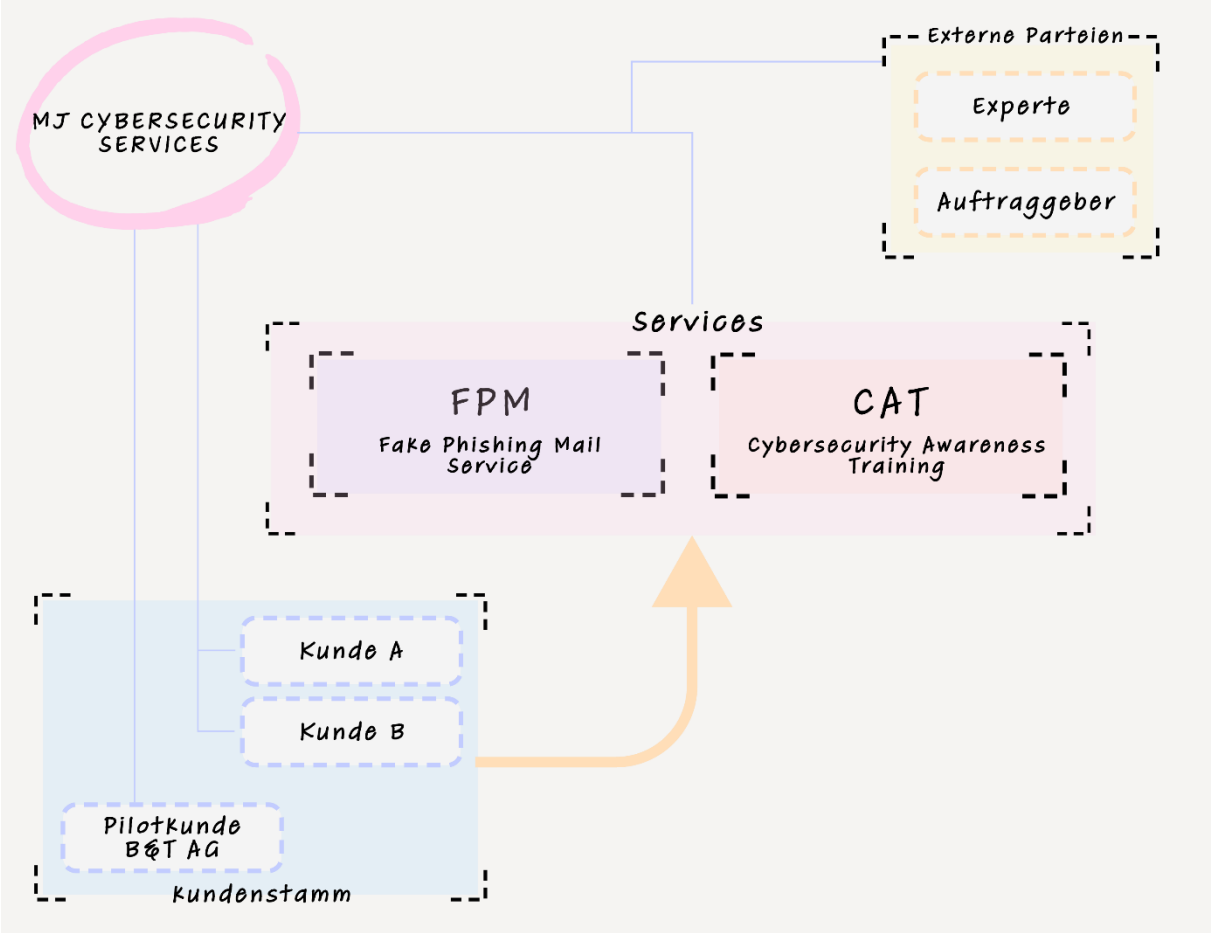

Abbildung 2 - Overview Serviceaufbau

6.1 Serviceidee

Die Serviceidee des FPM und CAT-Services wird anbei graphisch dargestellt. Der CAT-Service kann auch einzeln in Beanspruchung genommen werden, wobei der FPM-Service immer der CAT-Service mitbeinhaltet.

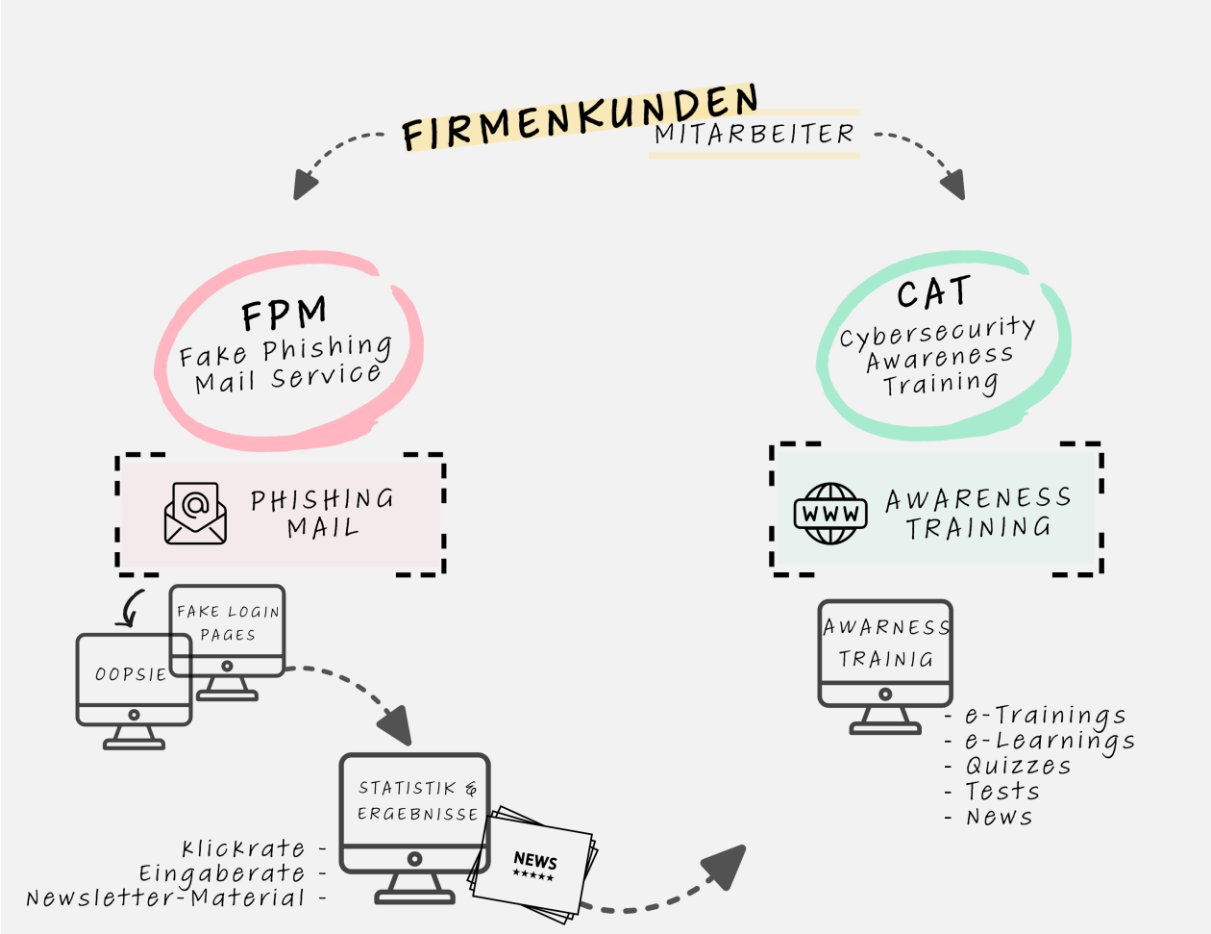

Abbildung 3 - Serviceidee

7. Ressourcen

Im folgenden Kapitel werden Ressource, wie Personal, Mittel, Infrastruktur, Notfall usw. für das Projekt dargestellt.

7.1 Personalressourcen

Folgend werden die Personalressourcen pro Phase und Monat dargestellt. Der Prozentsatz dient als Darstellung der Stunden, wie diese Prozentual aufgeteilt werden sollen.

Die Personalressourcen belaufen sich, wie dem Kapitel „Projektorganisation -> Rollen“ zu entnehmen ist auf folgenden Ressourcenkategorien:

- Projektmanager
- Fachspezialist/Engineer

Experten werden NICHT in den Ressoucenplan noch in den Prozentsatz eingerechnet und ist NICHT relevant für die Projektkostenrechnung und weitere Berechnungen.

Der genaue Projektplan wird hier aktualisiert und das Logbuch weitergeführt:

project_plan_v1_balken.xlsx

Die Personlressourcen werden in der nächsten Tabelle nach Projektphasen und Ressourcen aufgeschlüsselt. Innerhalb einem Monat werden die 100% verteilt. Da Projektmanaager und Fachspezialist ein und dieselbe Person ist, wird pro Monat die 100% Arbeit verteilt.

	Projektphasen				
Monat	**Initialisierung**	**Konzept**	**Realisierung**	**Durchführung**	**Abschluss**
FEB	Projektmanager (100%)				
MAR		Projektmanager (50%) Fachspezialist (20%)	Projektmanager (10%) Fachspezialist (20%)		
APR			Projektmanager (10%) Fachspezialist (70%)	Fachspezialist (20%)	
MAI				Projektmanager (20%) Fachspezialist (40%)	Projektmanager (40%)
JUN					Projektmanager (20%)

Tabelle 3 - Ressourcenplan, Personalressourcen

7.2 Geplante Stunden und Daten pro Phase

Folgend werden die Stunden pro Phase aufgegliedert. Da Projektmanager und Fachspezialist ein und dieselbe Person sind, werden die Stunden nicht pro Rolle aufgezeigt, sondern insgesamt.

Phase	**Von**	**Bis**	**Geplante Stunden**
INITIALISIERUNG	14.02.2024	08.03.2024	42
KONZEPT	08.03.2024	19.03.2024	70
REALISIERUNG	20.03.2024	10.04.2024	84
DURCHFÜHRUNG	17.04.2024	21.05.2024	25
ABSCHLUSS	22.05.2024	31.05.2024	20

Tabelle 4 - Geplante Stunden und Daten pro Phase

8. Risiken

Die genauen Beschreibungen der Risiken sind der Initialisierung zu entnehmen. Folgend wird die Risikobewertung pro Risiko aufgezeigt.

Nr	**Risiko**	**Eintretenswahrscheinlichkeit (EW):** *1 Niedrig / 2 Mittel / 3 Hoch*	**Auswirkungsgrad (AG):** *1 Gering / 2 Mittel / 3 Gross*	**Risikozahl (RZ):** *RZ = EW x AG*
1	Unvorhergesehener Personalausfall	2	3	6
2	Evaluiertes Tool nicht funktionsfähig	2	3	6
3	Pilotkunde fällt aus	1	2	2
4	Pandemie 2.0	2	1	2
5	Fehlinterpretation von Testergebnissen	2	2	4
6	Unbeabsichtigte Beeinträchtigung der Produktivität	3	1	3
7	Datenschutzverletzungen	1	3	3
8	Mangelnde Integration von Feedback	1	1	1
9	Technische Probleme mit der Phishing-Plattform	2	3	6
10	Schlecht aufgebaute CAT	2	2	4
11	Fehlende Anpassungsfähigkeit der Phishing-Platt-form	2	3	6
12	Technische Fehlfunktionen bei der Ausführung der Fake-Phishing-Mails (FPM)	2	3	6
13	Fehlendes techhnisches Know-How der Fachspezi-alisten	2	2	4

Tabelle 5 - Risikoanalyse und deren Bewertung

Punkte- & Farbaufschlüsselung der Risikoanlyse

Min. Punkte (RZ) pro Risiko = 1 („schwaches“ Risiko)

Max. Punkte (RZ) pro Risiko = 9 („starkes“ Risiko)

Farbcode	**Punkte**	**Massnahme**
Rot	7-9	Projektabbruch
Orange	4-6	Hilfe Beanspruchen (Experten)
Grün	1-3	Im Projektdokument dokumentieren

Tabelle 6 - Punkt- & Farbaufschlüsselung Risikobewertung

In jedem Fall wird versucht bei Ausfall oder Ereignisses eines der obengenannten Risiken das Projekt zu Ende zu stellen. Im WorstCase würde der Grundstein für einen tollen Service entstehen.

9. Abgrenzungen

Folgende Abgrenzungen sind nicht Teil des Projekts:

Infrastruktur: Die Infrastruktur, sowie Mailumgebung, muss bestehend sein.

100% Sicherheit: Es ist nicht garantiert, dass jede echte Phishing-Mail erkannt werden wird

Lernzeit Mitarbeiter: Es muss von der Firma vorgegeben werden wie lange die MA mit CAT verbringen dürfen, es liegt nicht in der Verantwortung von MJCS wieviel Zeitaufwand die Mitarbeiter auf Arbeitszeit aufwenden, es werden auch keine Statistiken/Logs darüber gesammelt, noch weitergegeben.

Abgrenzung zu echten Phishing-Angriffen: Das Projekt zielt darauf ab, die Awareness der Mitarbeiter zu stärken, indem kontrollierte und simulierende Fake-Phishing-Mails (FPM) verwendet werden. Es ist wichtig zu betonen, dass diese Aktionen ausschließlich zu Schulungszwecken durchgeführt werden und keine echten Bedrohungen darstellen.

Literaturverzeichnis

In arbeit..

Eidesstattliche Erklärung

Mit meiner Unterschrift erkläre ich, dass die vorliegende Arbeit selbständig und nur unter Verwendung der im Literaturverzeichnis aufgeführten Quellen erarbeitet worden ist. Die Stellen meiner Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, habe ich in jedem Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht. Die Angaben sind für jede einzelne Quelle als Fussnote mit Verweis auf die Quelle aufgeführt. Dasselbe gilt sinngemäss für Tabellen, Karten und Abbildungen, auch solche, die aus Internetquellen stammen.

Ort, Datum	Unterschrift