FPM & CAT
Fake Phishing Mail Service & Cybersecurity Awareness Training

Jessica Storrer

MJ CYBERSEUCRITY SERVICES

FPM

Fake
Phishing
Mail Service

Fake Phishing Mail Service für Sie und Ihre Mitarbeiter

CAT

Cybersecurity
Awareness
Training

Cybersecurity Awareness Training für Jedermann

MJ CYBERSECURITY SERVICES
Hüseli 10
CH-3663 Gurzelen

mjcybersecurity.com
mjcybersecurityteachable.com

KONTAKTFORMULAR
j.storrer@icloud.com

HFINF | Klasse 22b / Praktische Diplomarbeit 2024 | ID: 2132

Management Summary

Momentan sind überall Phishingmails, Phishingversuche, IT-Sercurtiy Zuhause oder am Arbeitsplatz in aller Munde, jedoch bei genauerem Hinhören wissen die Non-IT People nicht, wie mit den ganzen Digitalen Infos umzugehen. Diese aktuelle Situation streckt sich über jede Branche und Themengebiet und beschäftigt jeden, egal ob jung oder alt.

Benutzer der Digitalen Dienste werden mit Services, Awareness und Sicherheitsthemen zwar konfrontiert, jedoch scheint das noch lange nicht greifbar zu sein.

Ebenso wird festgestellt, dass es in Unternehmen eine erhebliche Bedrohung durch Phishing-Angriffe gibt. Mitarbeiter sind oft das schwächste Glied in der Sicherheitskette, da sie Phishing-Mails nicht immer erkennen und darauf hereinfallen.

Nach diversen Umfragen, Ganggesprächen und Chitchats mit Personen aller alters- und Interessensgruppen ergab sich die Idee für die beiden Services FPM & CAT.

FPM, der Fake Phishing-Mail Service, ist ein Service, welcher für Unternehmen Fake Phishing Mails mit Klickratenverfolgung für dessen Mitarbeiter anbietet. Es wurden drei FPM's konzipiert, von einfach – schwer. Jede Fake Email hat ebenso eine Fake Login Page, auf welcher der Empfänger aufgefordert wird, diese URL zu öffnen und fälschlicherweise seine Logindaten einzugeben. Jedes interagieren mit ebendiesen FPM's wird reportet.

Als Lerneffekt nach klicken oder öffnen des Links, wird der Benutzer darauf hingewiesen, dass dies grad eine Fake Phishing-Mail war und verweist den User auf CAT. Dies erfolgt personell und persönlich.

Wenn der Benutzer fälschlicherweise die Logindaten auf der Fake Login Page eingibt, wird dieser auf eine «Oopsie-Page» weitergeleitet, auf welcher der User interaktiv sieht, dass dies ein Test war und wird auf CAT weitergeleitet. Als Abschluss erhalten alle Teilnehmenden die Auflösung der Fake Phishing Mail, die Reports der Klickraten und wie die Emails zu identifizieren waren. Zudem wird ein Newsletter mit den neusten Erkenntnissen versendet.

CAT, das Cybersecurity Awareness Training dient nach Abschluss – oder während dem FPM -, oder für Privatpersonen als Online Cybersecurity Training. Das Online Kurs wurde auf die vier Hauptlerngruppen angepasst und ist mit interaktiven Lernelementen, Audios, Audioexkurse und Private Geschichten über Social-Engineering, Fallbeispiele, Höhrenverstehen, Suchbilder etc ausgestattet, sodass dieser kein 08/15 ist und jeden Teilnehmenden von Anfang an mitreisst.

mjcybersecurity.com / mjcybersecurity.teachable.com

fake phishing mail service
&
cybersecurity awareness training

FPM & CAT

-DIPLOMBERICHT-

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

Änderungsverzeichnis

Datum	Version	Änderung	Autor
10.05.2024	0.1	Erstellung Dokument	J. Storrer
14.05.2024	0.2	Initialisierung und Konzept	J. Storrer
15.05.2024	0.3	Durchführung	J. Storrer
16.05.2024	0.4	Abschluss, Anhänge	J. Storrer
18.05.2024	0.5	Finalisierung	J. Storrer
20.05.2024	0.6	Verfeinerungen, Abschluss	J. Storrer

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort, Einführung

Folgendes Dokument dient als Zusammenfassung des gesamten Projektes.

In diesem Diplombericht werden an diversen Stellen auf andere Dokumente / Anhänge gewiesen, welche das Thema detaillierter behandeln. Alle Anhänge werden im Kapitel „Anhänge“ aufgeführt, sowie im Text darauf verwiesen.

Zudem können alle Diplomarbeitsdokumente hier gedownloadet werden:

Downloads Diplomarbeit | MJCS (mjcybersecurity.com)

1. Phase Initialisierung

Folgend wird die Initialisierungsphase erläutert.

1.1 Ausgangslage

Momentan sind überall Phishingmails, Phishingversuche, IT-Sercurtiy Zuhause oder am Arbeitsplatz in aller Munde, jedoch bei genauerem hinhören wissen die Non-IT People nicht, wie mit den ganzen Digitalen Infos umzugehen.

Diese aktuelle Situation streckt sich über jede Branche und Themengebiet und beschäftigt jeden, egal ob jung oder alt.

Benutzer der Digitalen Dienste werden mit Services, Awareness und Sicherheitsthemen zwar konfrontiert, jedoch scheint das noch lange nicht greifbar zu sein.

Ebenso wird in der aktuellen Situation festgestellt, dass es in Unternehmen eine erhebliche Bedrohung durch Phishing-Angriffe gibt. Mitarbeiter sind oft das schwächste Glied in der Sicherheitskette, da sie Phishing-Mails nicht immer erkennen und darauf hereinfallen.

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 definierten Prozessen eine interne Phishing-Attacke durchzuführen. Als Abschluss dienen Statistiken und Ergebnisse, sowie ein Cybersecurity-Awareness Online-Training und Newsletter, um die Cybersecurity Awareness der Mitarbeiterinnen und Mitarbeiter zu erhöhen.

Der grobe Ablauf wäre, dass die Benutzer eine FPM – FakePhishingMail - erhalten.

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 CAT 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 der Fake Phishing Mail Kampagnen 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, 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 und das Cybersecurity-Awareness-Training CAT

1.2 Projektziele

Folgende Ziele wurden in der Initialisierung bestummen.

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

Die Ziele dienen dazu, die Anforderungen pro Service zu definieren.

1.3 Lieferergebnisse

Wie im Initialisierungsdokument erläutert werden folgende Lieferergebnisse von diesem Projekt verlangt. Pro Lieferergebnis sind die Nachschlagewerke angegeben.

Themengebiet	Lieferergebnisse	Verweis Dokument
Overall	Evaluation / Variantenentscheid: Plattformen für FPM und CAT wurden entschieden	ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf ID2132_StorrerJessica_FPM&CAT_Initialisierung_v1.pdf
	Serviceidee / Pricing: Eine Serviceidee und dessen Preise, sowie Factsheet wurde erstellt	ID2132_StorrerJessica_CAT_Konzept_v1. pdf ID2132_StorrerJessica_FPM_Konzept_v1. Pdf ID2132_CAT-Service-WhitePaper-MJCS_v1.pdf ID2132_FPM-Service-WhitePaper-MJCS_v1.pdf
	UseCases / Prozesse: Prozesse für FPM und CAT wurden definiert, Data-Sheets und Kundenblätter (Informationsgewinnung Kunde, Must-haves) wurden erstellt	ID2132_StorrerJessica_CAT_Konzept_v1. pdf ID2132_StorrerJessica_FPM_Konzept_v1. pdf
	Test Cases: Test Cases für den FPM-Versand wurden anhand der erstellten UseCases erstellt	ID2132_StorrerJessica_CAT_Testkonzept_v1.pdf ID2132_StorrerJessica_FPM_Testkonzept_v1.pdf ID2132_StorrerJessica_CAT_Testprotokollt_v1.pdf ID2132_StorrerJessica_FPM_Testprotokollt_v1.pdf
Lieferobjekte FPM	Technisches Konzept/Aufbau: Mehrere Kunden betreubar, Multikundenfähiger Service, Parallel aufbaubar	ID2132_StorrerJessica_FPM_Konzept_v1. pdf
	Konzepte FPM/FPL: Konzepte der Fake Phishing Mails und Fake Login Pages bestehen/wurden definiert	ID2132_StorrerJessica_FPM_Konzept_v1. Pdf
	Newsletter/Reporting: Newsletter und Klickratenreport per Ende FPM Service	ID2132_FPM_Abschluss_StorrerJessica_v1.pdf ID2132_FPM_Report_Kombiniert.pdf ID2132_AbschlussNewsletter_FPM.pdf

Lieferobjekte CAT	Trainings; Trainings wurden aufgesetzt, Themen definiert	ID2132_StorrerJessica_RealisierungDurchführung_CAT_v1.pdf ID2132_FPM&CAT_Abschluss_StorrerJessica_v01.docx
	Tests & Quizzes; Div. Test & Quizzes wurden anhand der Trainings-Themen definiert und aufgesetzt	ID2132_StorrerJessica_RealisierungDurchführung_CAT_v1 ID2132_FPM&CAT_Abschluss_StorrerJessica_v01.docx
	Zusatzmaterial; Tipps & Tricks für den Alltag wurden aufgesetzt und bereitgestellt	ID2132_StorrerJessica_RealisierungDurchführung_CAT_v1 ID2132_FPM&CAT_Abschluss_StorrerJessica_v01.docx

Tabelle 2 – Lieferergebnisse

1.4 Projektorganisation

Die Projektorganisation wurde wiefolgt aufgebaut.

1.4.1 Projektorganisation & 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 3 - Projektorganisation & Rollen

In der Stammorganisation von MJ Cybersecurity Services, welches die Firma darstellt, welche die Services anbietet, wird die Projektorganisation wie folgt dargestellt.

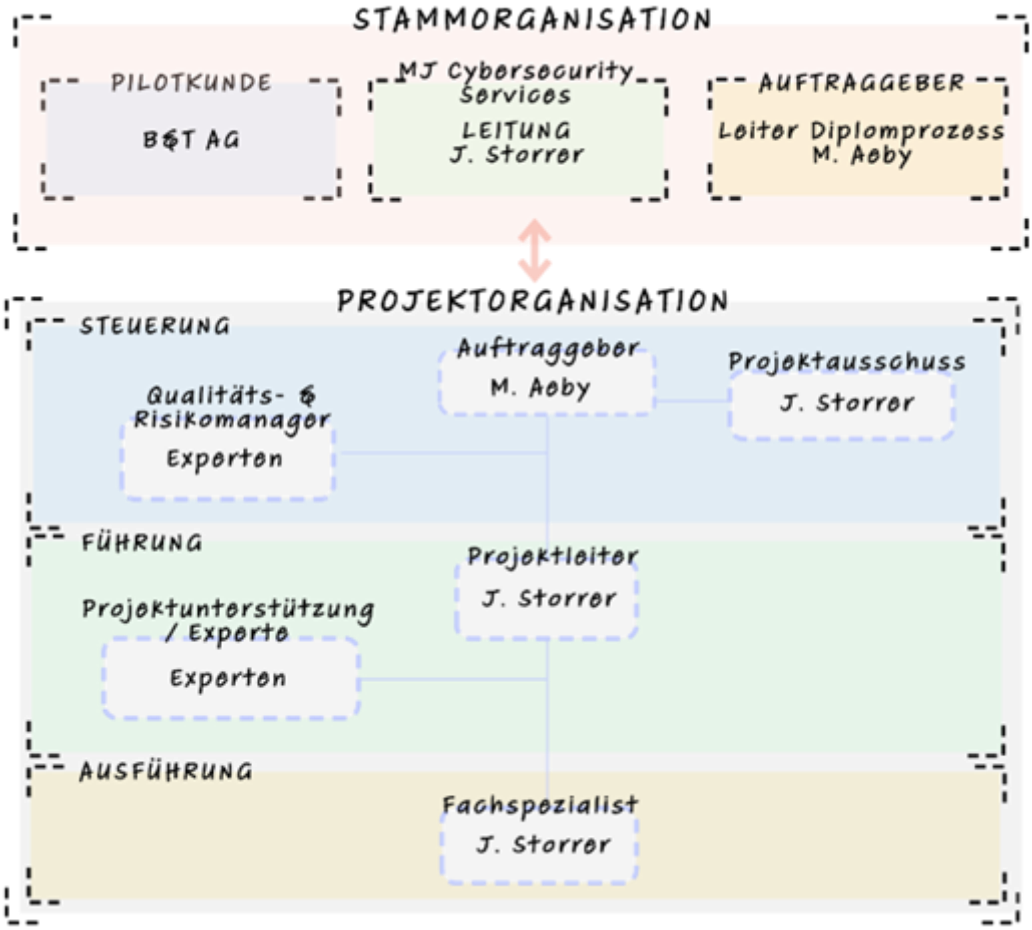


Abbildung 1 - Aufbau Stamm- & Projektorganisation

1.5 Projektplan

Der Projektplan wurde in Excel aufgesetzt und laufend mit den Stunden abgeglichen. Hier ist lediglich ein Auszug des Aussehens, der ganze Projektplan kann im folgenden Dokument unter der Mappe *„Projektplan_SOLLIST_Balken“* eingesehen werden. In Diesem Dokument werden nur die wichtigsten Dinge zusammengefasst.

ID2132_StorrerJessica_Projektplan_v01.xlsx

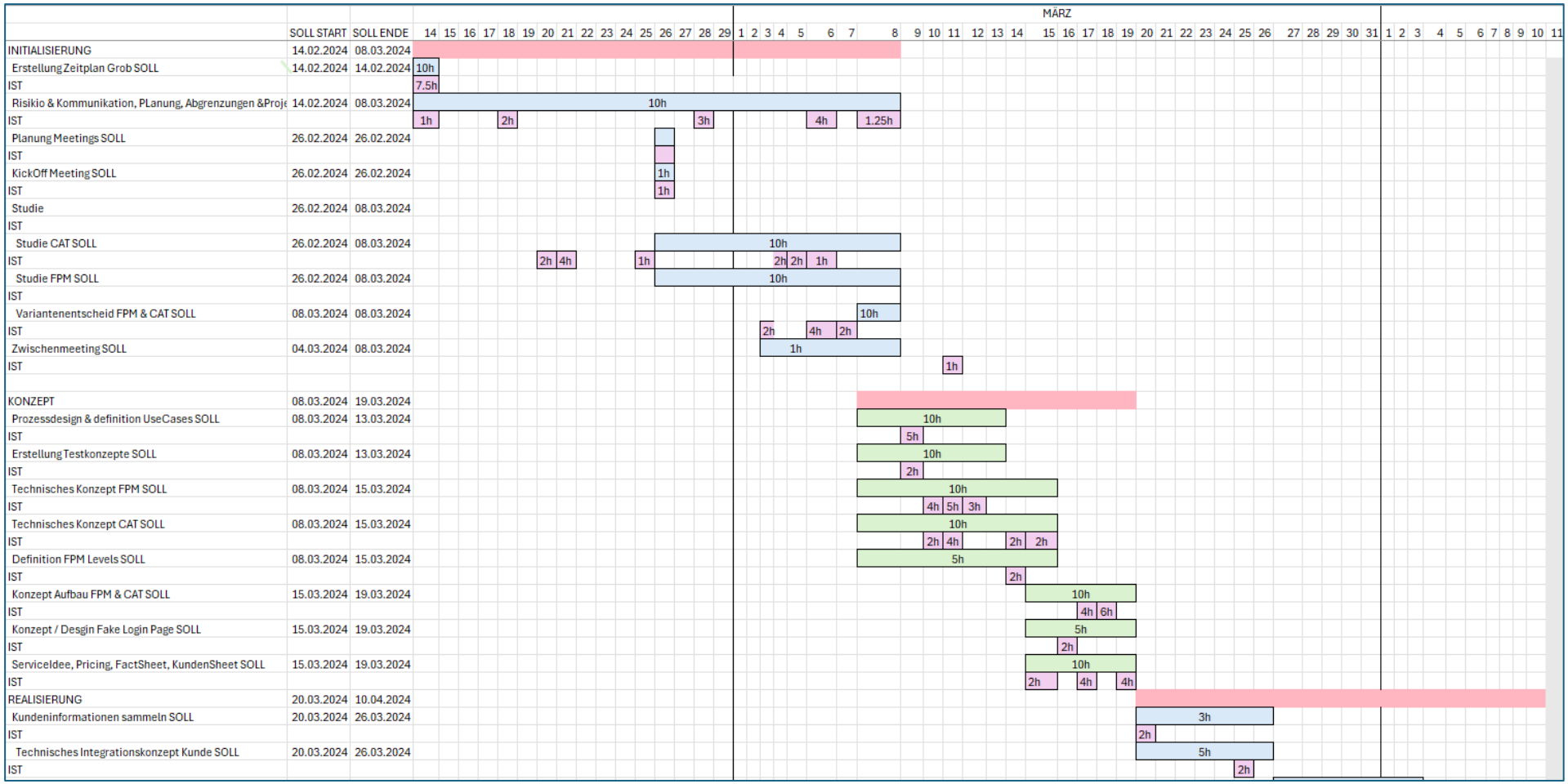


Abbildung 2 - Auszug Projektplan Mappe "Projektplan_SOLLIST_Balken"

Folgend werden die Differenzen SOLL/IST der Stunden der Phasen grafisch aufgezeigt.

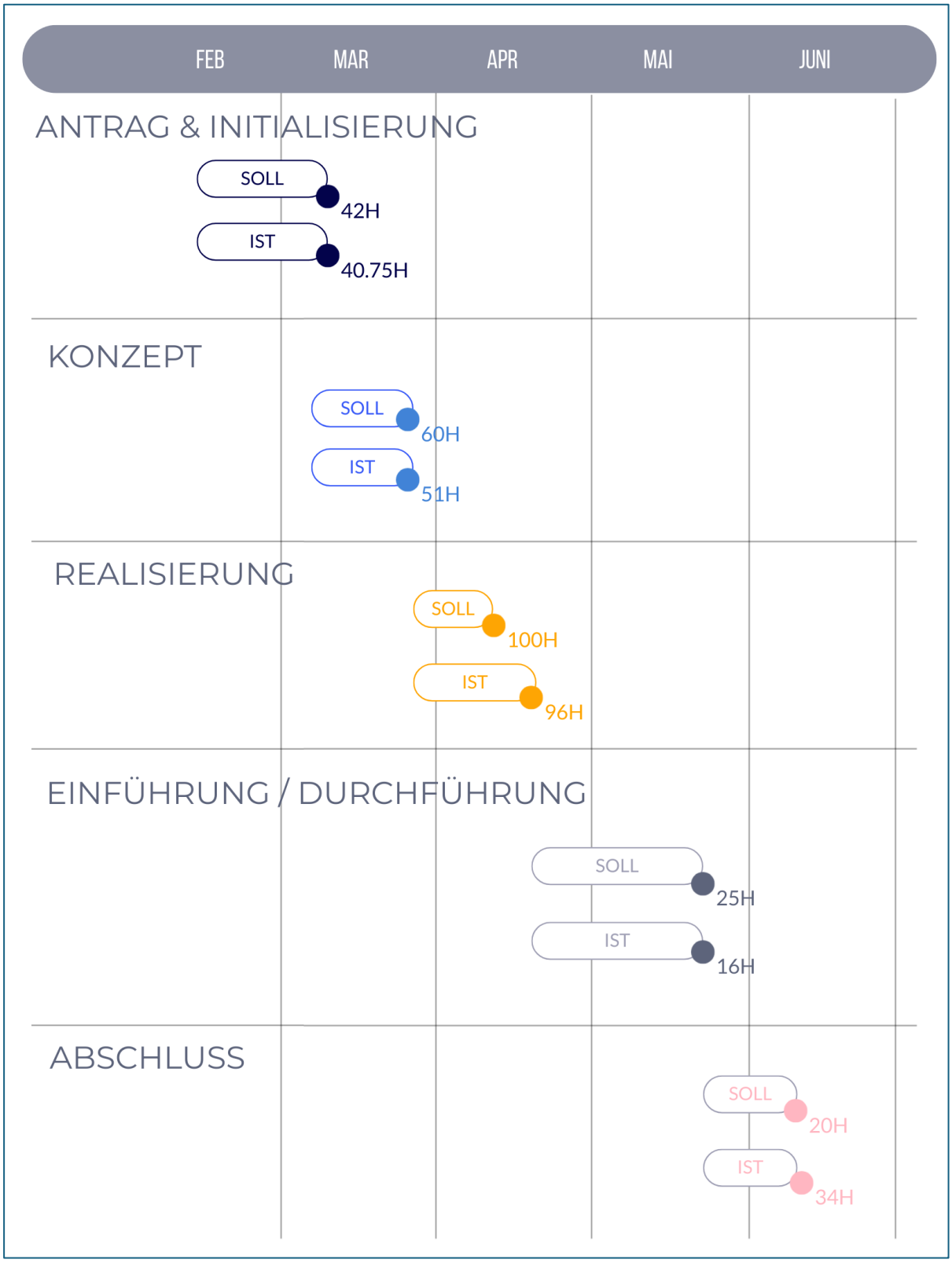


Abbildung 3 - Differenzen IST/SOLL Zeiten pro Phase

Wie in der Grafik zu sehen ist, wurden die geplanten Stunden und Zeiten hauptsächlich eingehalten. Das Projekt schrieb Zeiten & Daten pro Phasen vor, welche eingehalten werden müssen.

Die Tabelle zeigt die geplanten und tatsächlichen Zeiten für die verschiedenen Phasen des Projekts. Aufgrund privater Ereignisse wurde der zuvor geplante Buffer (10.04.2024 – 17.04.2024) gebraucht.

Phase	Von	Bis	Geplante Stunden
SOLL INITIALISIERUNG	14.02.2024	08.03.2024	42
IST INITIALISIERUNG	*14.02.2024*	*08.03.2024*	*40.75*
SOLL KONZEPT	08.03.2024	19.03.2024	60
IST KONZEPT	*08.03.2024*	*19.03.2024*	*51*
SOLL REALISIERUNG	20.03.2024	10.04.2024	100
IST REALISEIRUNG	*20.03.2024*	*17.04.2024*	*96*
SOLL DURCHFÜHRUNG	17.04.2024	21.05.2024	25
IST DURCHFÜHRUNG	*17.04.2024*	*21.05.2024*	*16*
SOLL ABSCHLUSS	22.05.2024	31.05.2024	20
IST ABSCHLUSS	*22.05.2024*	*31.05.2024*	*34*
SOLL Gesamt			247
IST Gesamt			*237.75*

Tabelle 4 - Daten & Zeiten pro Phase SOLL/IST

1.6 Ressourcenplan

Folgend werden die Ressourcen für das Projekt definiert

1.6.1 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.

	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%)

Die Personalressourcen 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.

1.7 Risiken

Im folgenden Kapitel sind die Risiken des Projektes aufgezeigt, die Risiken sind jeweils aufgegliedert in Ursachen, Auswirkungen und Massnahmen. Diese dienen als Grundlage zur Berechnung der Risikenbewertung.

Nr	Risiko	Ursache	Auswirkung	Massnahmen
1	Unvorhergesehener Personalausfall	Krankheit, Unfall oder andere unvorhersehbare Ereignisse führen zu einem Ausfall eines Schlüsselmitarbeiters	Verzögerungen im Projektverlauf, mangelnde Ressourcen und potenzielle Beeinträchtigung der Qualität	Gesunder Lifestyle
2	Evaluiertes Tool nicht funktionsfähig	Unvorhergesehene Probleme mit dem gewählten Evaluierungstool während der Implementierung	Verzögerungen bei der Durchführung und potenzielle Ineffektivität des gesamten Projekts	Sorgfältige Auswahl eines zuverlässigen Evaluierungstools, umfassende Tests vor dem Einsatz und Vorhaltung von Alternativen für den Fall von Ausfällen
3	Pilotkunde fällt aus	Der ausgewählte Pilotkunde zieht sich aus dem Projekt zurück oder kann seine Verpflichtungen nicht erfüllen	Mangelnde Möglichkeit zur Überprüfung der Wirksamkeit des Projekts unter realen Bedingungen	Klasse als Testkunden benützen (nach Absprache)
4	Pandemie 2.0	Wiederholung oder Verschärfung von Pandemiebedingungen, die die normale Geschäftstätigkeit beeinträchtigen	Einschränkungen bei der physischen Anwesenheit im Unternehmen, Verzögerungen und möglicherweise mangelnde Ressourcenverfügbarkeit	Entwicklung von Remote- Arbeitsplänen, verstärkte Nutzung digitaler Kommunikationsmittel und frühzeitige Implementierung von Notfallplänen für die Projektdurchführung
5	Fehlinterpretation von Testergebnissen	Unklare oder missverständliche Darstellung von Testergebnissen	Fehlende Erkennung von Schwachstellen und ineffektive Implementierung von Gegenmassnahmen	Klare und verständliche Präsentation der Testergebnisse, Schulung der Verantwortlichen für die Auswertung

6	Unbeabsichtigte Beeinträchtigung der Produktivität	Störende Auswirkungen des Tests auf den regulären Arbeitsablauf	Produktivitätsverluste und mögliche Frustration der Mitarbeiter	Sorgfältige Planung von Testzeiten, Kommunikation von Testphasen und Minimierung von Störungen
7	Datenschutzverletzungen	Unbeabsichtigte Offenlegung sensibler Informationen während des Phishing-Test	Vertrauensverlust der Mitarbeiter und mögliche rechtliche Konsequenzen	: Anonymisierung von Testdaten, klare Kommunikation über den Testprozess und Einhaltung von Datenschutzrichtlinien

8	Mangelnde Integration von Feedback	Fehlende Berücksichtigung von Mitarbeiter-Feedback und Vorschlägen	Versäumnis potenziell wichtiger Anpassungen für zukünftige Tests	Implementierung eines Feedback-Mechanismus, regelmässige Überprüfung von Rückmeldungen und Anpassung des Testansatzes
9	Technische Probleme mit der Phishing-Plattform	Funktionsstörungen oder Ausfälle der verwendeten Phishing- Software oder Plattform	Verzögerungen im Testablauf und möglicher Datenverlust	Regelmässige Wartung der Plattform, Implementierung von Backup- Mechanismen und schnelle Behebung von technischen Problemen
10	Schlecht aufgebaute CAT	Unklare Kommunikation über den pädagogischen Charakter des Trainings	Möglicher Widerstand oder geringe Beteiligung der Mitarbeiter am Schulungsprozess	Transparente Erklärung der Trainingsziele, Betonung des Lerncharakters und Einbindung von praxisrelevanten Beispielen
11	Fehlende Anpassungsfähigkeit der Phishing-Plattform	Einschränkungen oder Inkompatibilitäten der gewählten Phishing-Plattform	Schwierigkeiten bei der Anpassung der Plattform an spezifische Anforderungen oder Sicherheitsrichtlinien des Unternehmens	Sorgfältige Auswahl einer flexiblen Plattform, regelmässige Updates und Abstimmung mit den IT- Sicherheitsrichtlinien
12	Technische Fehlfunktionen bei der Ausführung der Fake-Phishing-Mails (FPM)	Unvorhergesehene technische Probleme, wie Serverausfälle, Firewallprobleme oder Programmfehler, während des Versands von FPM	Beeinträchtigung des Testablaufs, unerwünschte Auswirkungen auf IT-Systeme und potenzieller Abbruch des Projektes	Umfassende Tests und Überprüfungen der Plattform vor dem Einsatz, Implementierung von Backup-Mechanismen und schnelle Fehlerbehebung bei technischen Problemen

13	Fehlendes techhnisches Know-How der Fach-spezialisten	Mangelnde Kenntnisse der Fach-spezialisten in Bezug auf die Kon-figuration und den Einsatz von Phishing-Plattformen	Fehlfunktionen bei der Erstellung und Ausführung von FPM, subopti-male Anpassung an die Unterneh-mensbedürfnisse. Nicht funktionie-render Service	Gezielte Informationsbeschaffung und Workshops für die Fachspezia-listen, um sicherzustellen, dass sie über das notwendige technische Wissen für die effektive Umsetzung der FPM verfügen. Engere Zusammenarbeit mit IT- Exper-ten und externen Dienstleistern kann ebenfalls in Betracht gezogen werden

1.8 Risikoanalyse und Bewertung

Folgend werden die Risiken Bewertet und aufgeschlüsselt, wie bei welchem Wertepunkt gehandelt werden sollte.

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

Punkte- & Farbaufschlüsselung

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

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.

1.9 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.

1.10 Studie

Dies ist nur eine Zusammenfassung der Studie im Dokument *ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf*.

1.10.1 Aktuelle Situation

Momentan sind überall Phishingmails, Phishingversuche, IT-Sercurtiy Zuhause oder am Arbeitsplatz in aller Munde, jedoch bei genauerem Hinhören wissen die Non-IT People nicht, wie mit den ganzen Digitalen Infos umzugehen.

Diese aktuelle Sitation streckt sich über jede Branche und Themengebiet und beschäftigt jeden, egal ob jung oder alt.

Benutzer der Digitalen Dienste werden mit Services, Awareness und Sicherheitsthemen zwar konfrontiert, jedoch scheint das noch lange nicht greifbar zu sein.

Ebenso wird in der aktuellen Situation festgestellt, dass es in Unternehmen eine erhebliche Bedrohung durch Phishing-Angriffe gibt. Mitarbeiter sind oft das schwächste Glied in der Sicherheitskette, da sie Phishing-Mails nicht immer erkennen und darauf hereinfallen.

1.10.2 Lösungsansätze

Pflichtenheft und Anforderung werden im *Dokument ID2132_StorrerJessica_FPM&CAT_Studie_v1*.pdfgenau aufgegliedert.

Als Lösung für die in der Situation beschriebenen Probleme wurde der Aufbau der folgenden zwei Services angedacht.

Fake Phishing Mail (FPM) Service: Ein Service, der es Unternehmen ermöglicht, ihre Mitarbeiter mit simulierten Phishing-Mails zu testen und ihre Reaktionen zu überwachen.

Cybersecurity Awareness Training (CAT): Ein Training, das Mitarbeiter über die Gefahren von Phishing und anderen Cyberangriffen aufklärt und ihnen beibringt, wie sie diese erkennen und vermeiden können.

1.10.3 Funktionale & Nicht-Funktionale Anforderungen

Nach eingehenden Überlegungen werden folgende funktionalen Anforderungen für die Services ausgearbeitet. Hier werden die wichtigsten erläutert.

Empfang und Erkennung von FPMs: Mitarbeiter müssen FPMs empfangen und identifizieren können.

Interaktion mit FPMs: Benutzer sollen auf FPMs reagieren können, indem sie entweder die Falle erkennen und melden oder fälschlicherweise darauf eingehen.

AHA-Effekt nach fälschlicher Interaktion mit FPM:

Sobald die User mit der Email interagiert haben, werde diese persönlich Benachrichtigt und abgeholt für den AHA-Effekt. Das CAT-Training wird als Aufforderung gratis mittels Coupon angeboten.

Abschlussnewsletter & Report FPM:

Als Abschluss und zur Überprüfung was der FPM-Service gebracht hat, müssen detaillierte Reports über die FPM-Kampagnen erstellt werden können. Zudem, als weiterer AHA-Effekt, muss es für alle Mitarbeiter ein Abschluss- und Auflösungsnewsletter geben mit Auflösung der FPM und Aufforderung Teilnahme an CAT.

Teilnahme am CAT: Privat- & Unternehmensbenutzer müssen Zugang zum Awareness-Training haben und dieses absolvieren können. Für Firmenkunden mit FPM-Service gratis, für Privatpersonen zu einem erschwinglichen Preis

Zusatzinhalte, Interaktive Games & Quizzes, Digitale Downloads:

Wichtig war, dass das online Training einfach aufbaubar und für den User optisch und inhaltlich so ansprechbar ist, dass es kein 08/15 Kurs ist und der User von alleine am Ball bleibt.

Reporting und Feedback CAT: Benutzer sollen Feedback zu den Trainingsinhalten geben und verdächtige Aktivitäten melden können.

Sicherheit und Datenschutz: Die Plattform muss höchste Sicherheits- und Datenschutzstandards erfüllen.

Benutzerfreundlichkeit: Die Benutzeroberfläche muss intuitiv und einfach zu bedienen sein.

Mehrkundenfähig: Die Lösung muss mehrkundenfähig sein, um unterschiedliche Unternehmensgrössen und -anforderungen zu unterstützen.

Folgende Grafik zeigt das Zusammenspiel der Services und der auszuführenden Firma MJ Cybersecurity Services auf.

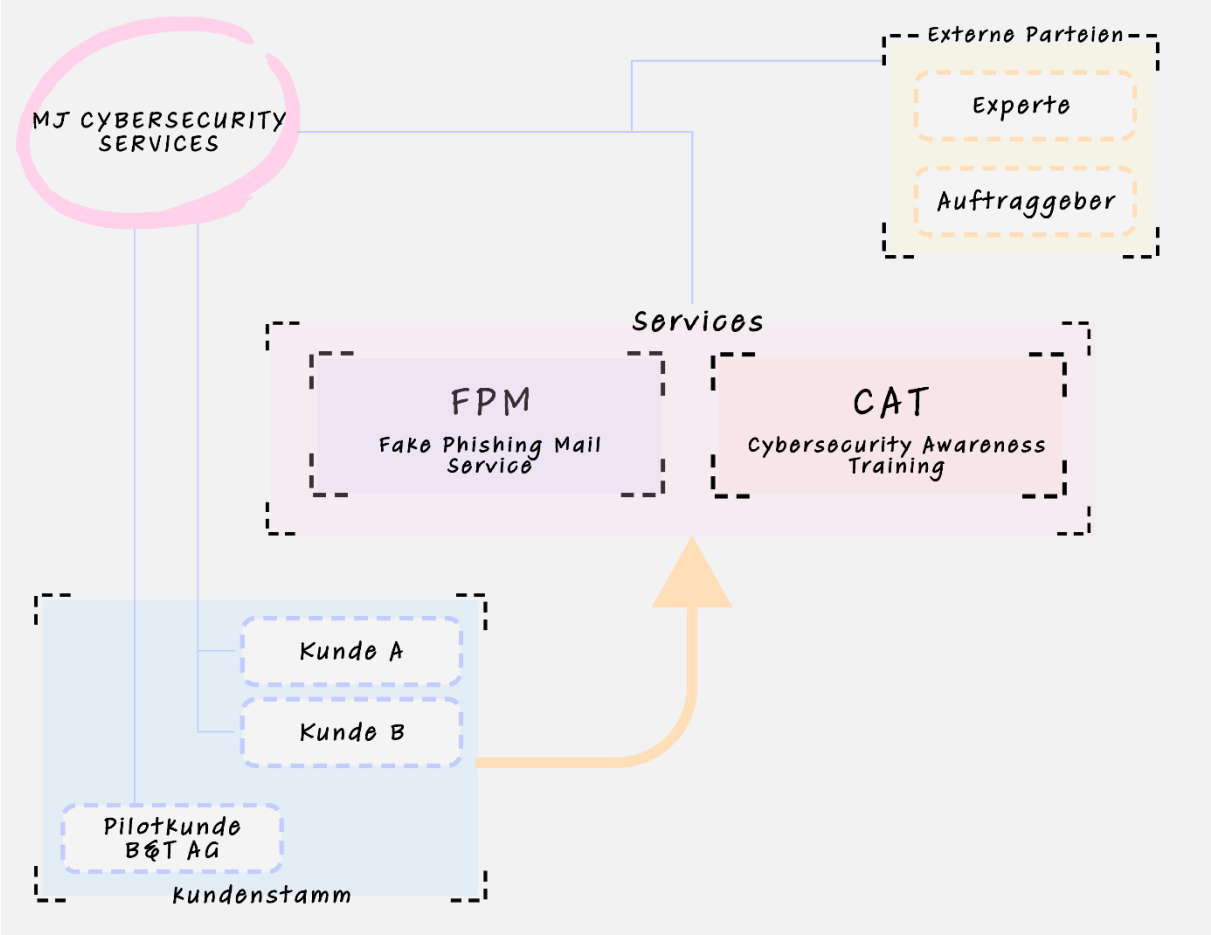


Abbildung 4 - Zusammenspiel Experte/Services/Kunden/MJCybersecurityServices

1.10.4 Erster Entwurf der Serviceldee

In der Folgenden Grafik wird der erste Entwurf der Serviceidee aufgezeigt.

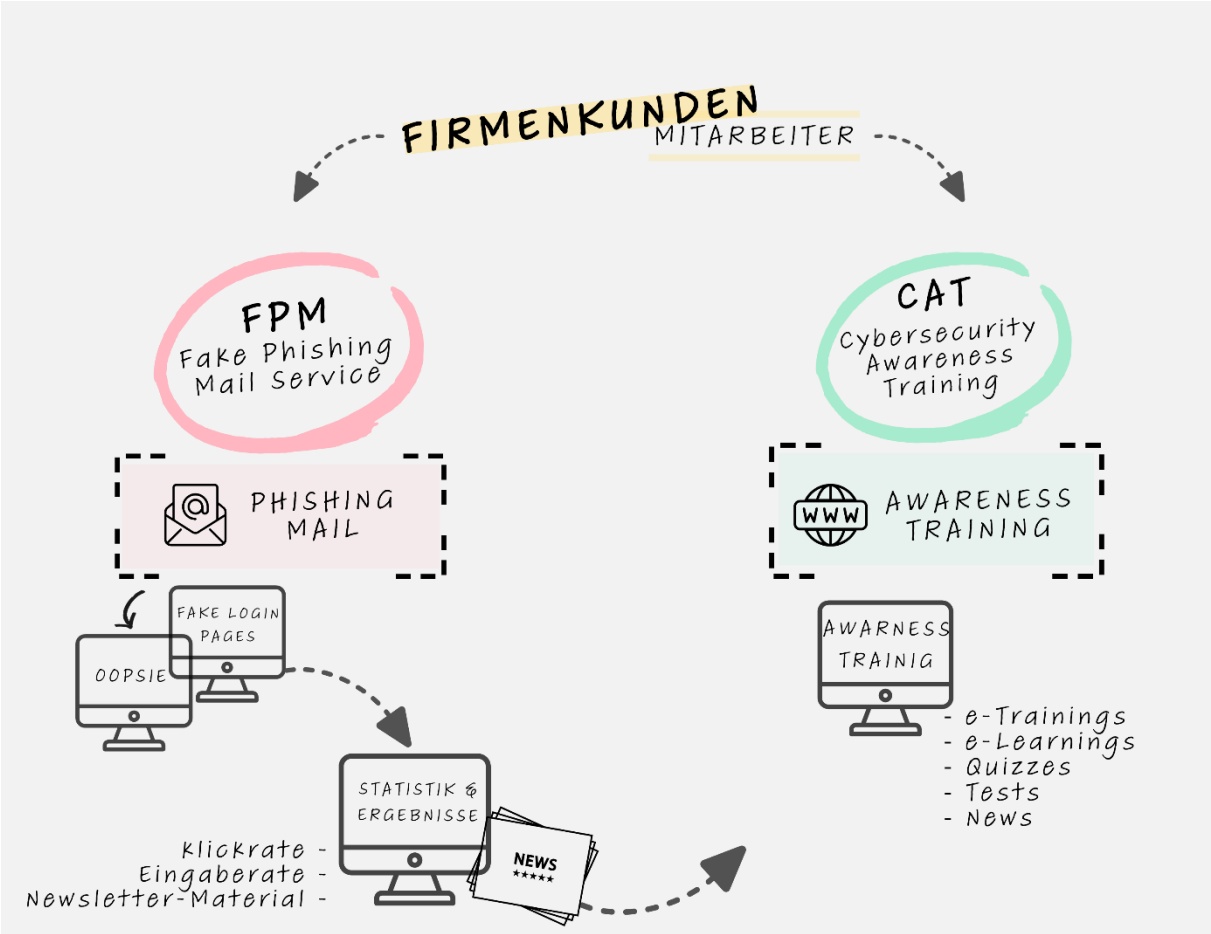


Abbildung 5 - Erster Entwurf der Serviceldee

1.11 Variantenentscheide für FPM&CAT

Der Variantenentscheid wurde in der Studie *ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf* genau dargestellt und bewertet. In diesem Teil der Dokumentation wird jeglich die aufgeschlüsselten Werte für den Entscheid dargestellt, dass eine Übersicht geschaffen werden kann, welche Varianten pro Service noch in Betracht gezogen wurden.

1.11.1 Variantenentscheid FPM-Tool

Bei entscheid welches Phishing Tool beim FPM-Service als Grundlage Dient, standen die folgenden drei Tools zur Auswahl.

GoPhish

KingFischer

PhishingFrenzy

In der Studie wurden die ***Anforderungen*** eruiert. Als Basis dessen wurde der Variantenentscheid gefällt.

Die Varianten kurz erklärt

GoPhish

Einfache Installation und Konfiguration.

Benutzerfreundliches Interface für Kampagnenmanagement.

Detaillierte Berichterstattung und Statistiken.

Unterstützung für die Erstellung von Fake-Login-Seiten.

Mehrkundenfähigkeit durch schnelle Installation und Export/Import von Kampagnendaten.

KingPhisher

Unterstützt sowohl E-Mail- als auch SMS-Phishing-Kampagnen.

Visuelle Kampagnen-Design-Tools und Template-Editor.

Detaillierte Kampagnenstatistiken.

Integration mit externen Tools.

PhishingFrenzy

Template-Management-System.

Detaillierte Statistiken und Erfolgsmessungen.

Automatisierung von Kampagnen.

In der Spalte Punkte gesamt ist das Endresultat der vergebenen Punkte im Entscheid angegeben. Alle Detailreicheren Informationen müssen in den Studien- & Initialisierungsdokumente nachgeschaut werden. *ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf*

Der Entscheid, welcher daraus zu führen ist, dass im Projekt „FPM as a Service“ das Produkt «GoPhish» als Phishing Tool eingesetzt werden wird.

Variante	Bezeichnung	Punkte gesamt
V1_FPM	*GoPhish*	*460*
V2_FPM	*KingFischer*	*354*
V3_ FPM	*PhishingFrenzy*	*363*

Diese wurden durch die folgenden Schlüssel ge- und bewertet:

Gewichtet wird Pro Anforderung pro Variante.
Gewertet wird folgendes:

Wie wichtig?	Wie wichtig ist es, dass das FPM-Tool die Anforderung erfüllt? Muss = 10 Kann = 5
Anforderung erfüllt?	Wird das Feature/Anforderung im Tool unterstützt? Wird die Anforderung vom Tool erfüllt? Ja = 1 Nein = 0
Wie einfach ist die Implementation der Anforderung?	Ist die Lösung der Anforderung schwierig zu implementieren? Sehr schwierig = 0 Sehr einfach = 10
Hilfestellung und Support (online-community, basierend auf vorhandenen Videos und Foren)	Ist die Online-Community (Foren, Dokumentationen, Videos, Anleitungen) gross vertreten? Keine Hilfestellung = 0 Viel Hilfestellung = 10

Die Summe aller gewerteten Anforderungen ergibt die Endsumme (Punktzahl) für die Variante. Die Variantensummen werden miteinander verglichen, sodass ein der Sieger mit am meisten Punkten aus dem Variantenentscheid hervorgeht.

1.11.2 Variantenentscheid CAT-Plattform

Bei entscheid Plattform für die Training als Grundlage dient, standen die folgenden drei Plattformen zur Auswahl.

Teachable

Moodle

Udemy for Business

In der Studie wurden die **Anforderungen** eruiert. Als Basis dessen wurde der Variantenentscheid gefällt.

Die Varianten kurz erklärt

Teachable

Einfache Drag-and-Drop-Schnittstelle zur Kursentwicklung.

Einbindung von Videos, Quizzen und interaktiven Elementen.

Fortschrittsverfolgung und Analysen.

KI-gesteuerte Kursgenerierung.

Moodle

Anpassbare Kursstrukturen und Lernmaterialien.

Foren und Gruppendiskussionen.

Überwachung des Lernfortschritts.

Open-Source-Plattform.

Udemy for Business

Grosse Auswahl an vorbereiteten Kursen.

Möglichkeit zur Erstellung eigener Schulungsinhalte.

Fortschrittsverfolgung und Zertifikate.

Teammanagementfunktionen.

In der Spalte Punkte gesamt ist das Endresultat der vergebenen Punkte im Entscheid angegeben. Alle Detailreicheren Informationen müssen in den Studien- & Initialisierungsdokumente nachgeschaut werden. ***ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf***

Der Entscheid, welcher daraus zu führen ist, dass im Projekt „CAT “ das Produkt «Teachable» als Awarenessschaffende Plattform eingesetzt werden wird.

Variante	Bezeichnung	Punkte
V1_CAT	*Teachable*	*158*
V2_CAT	*Moodle*	*155*
V3_ CAT	*Udemy for Business*	*153*

Gewichtet wird Pro Anforderung pro Variante.
Gewertet wird folgendes:

Wie wichtig?	Wie wichtig ist es, dass das FPM-Tool die Anforderung erfüllt? Muss = 10 Kann = 5
Anforderung erfüllt?	Wird das Feature/Anforderung im Tool unterstützt? Wird die Anforderung vom Tool erfüllt? Ja = 1 Nein = 0
Wie einfach ist die aktuellhaltung der Kursinhalten?	Das aktualisieren oder neu Erstellen von Kursinhalten sollte sich so einfach wie möglich halten Sehr schwierig = 0 Sehr einfach = 10
Kosten	Wären die Kosten im Notfallbudget vertretbar? Überschreitet Notfallbudget = 0 Niedrig (niedere hostingkosten) = 10

Die Summe aller gewerteten Anforderungen ergibt die Endsumme (Punktzahl) für die Variante. Die Variantensummen werden miteinander verglichen, sodass ein der Sieger mit am meisten Punkten aus dem Variantenentscheid hervorgeht.

Die Informationsbeschaffung, welche die Grundsteine für diesen Service darstellen, sind separat im Anhang im Dokument ***FPM_CAT_Studie_ID2132_StorrerJessica.docx*** dargestellt.

Es wurden unter anderem Interviews und diverse Umfragen durchgeführt, um zu schauen, ob diese Services überhaupt auf dem Markt gewünscht wären. Alles weiterführende ist dem oben genannten Dokument zu entnehmen.

1.12 Total Cost of Ownership

Im folgenden Abschnitt werden die Gesamtkosten des Projektes behandelt. Weiterführende Finanzdokumente können hier eingesehen werden. *ID2132_StorrerJessica_CAT_Konzept_v1.pdf & ID2132_StorrerJessica_FPM_Konzept_v1.pdf*

1.12.1 Projektkosten

Personalkosten: 160 CHF/Stunde

Geplante Stunden: 240 Stunden

Gesamte Personalkosten: 38.400 CHF

1.12.2 Zusätzliche Kosten:

Plattformkosten/Hosting: 800 CHF

Marketing/Werbung: 200 CHF

Notfallbudget: 1.000 CHF

1.12.3 Gesamtkosten:

Geplante Gesamtkosten: 38.400 CHF (Personalkosten) + 2.000 CHF (Plattform, Werbung, Notfallbudget) = 40.400 CHF

1.12.4 Jährliche Instandhaltungskosten:

Personalkosten für Aktualisierung und Wartung: 50 Stunden pro Quartal à 160 CHF/Stunde = 32.000 CHF/Jahr

Fixkosten (Plattformkosten/Hosting): 1.000 CHF/Jahr

Marketing/Werbung: 200 CHF/Jahr

Notfallbudget: 1.000 CHF/Jahr

1.12.5 Jährliche Gesamtkosten für Instandhaltung:

Gesamtkosten: 32.000 CHF + 1.000 CHF + 200 CHF + 1.000 CHF = 34.200 CHF/Jahr

Beispiel für eine Laufzeit von 5 Jahren:

Jahr 1:

Gesamtkosten: 40.400 CHF (Projektkosten) + 34.200 CHF (Instandhaltung) = 74.600 CHF

Jahr 2 bis Jahr 5:

Jährliche Instandhaltungskosten: 34.200 CHF/Jahr

Gesamtkosten für 4 Jahre: 34.200 CHF * 4 = 136.800 CHF

Gesamtkosten über 5 Jahre:

TCO: 74.600 CHF (Jahr 1) + 136.800 CHF (Jahr 2-5) = 211.400 CHF

1.12.6 Zusammenfassung:

Die Gesamtkosten für die Implementierung und Instandhaltung der Phishing- und Awareness-Training-Plattform über einen Zeitraum von 5 Jahren betragen etwa 211.400 CHF.

1.13 Informationsbeschaffung

Die Business Model Canvas für den Fake Phishing Mail Service (FPM) und das Cybersecurity Awareness Training (CAT) zeigen beide einen klaren Fokus auf die Erhöhung des IT-Sicherheitsbewusstseins in Unternehmen. Der FPM-Service konzentriert sich auf die Entwicklung und Implementierung von Phishing-Simulationen, die Erstellung von Fake-Login-Seiten und die Analyse der Ergebnisse. Hauptkunden sind mittelständische und große Unternehmen mit einem hohen Sicherheitsbedürfnis. Die Einnahmen werden durch Abonnementgebühren, einmalige Schulungsgebühren und Beratungsdienste generiert, während die Kosten hauptsächlich für die Entwicklung und Wartung der Plattform sowie die Personalkosten anfallen.

Das CAT-Service hingegen legt den Schwerpunkt auf die Entwicklung von Schulungsinhalten und die Durchführung von Online- und Präsenzschulungen. Es richtet sich an Unternehmen jeder Größe, die regelmäßige und anpassbare Schulungen benötigen, um Sicherheitsvorfälle zu reduzieren. Die Einnahmen stammen aus Abonnementgebühren für die Schulungsplattform, speziellen Schulungsgebühren und Zertifizierungseinnahmen. Die Kostenstruktur umfasst die Entwicklung und Wartung der Schulungsplattform, die Erstellung von Lernmaterialien und die Personalkosten für Schulungsexperten.

Die Umfragen in der Studie zeigten, dass die meisten Mitarbeiter unsicher im Umgang mit Phishing-Mails sind und einen hohen Bedarf an interaktiven und praxisnahen Schulungen haben. Es besteht ein großer Wunsch nach regelmäßigen Tests und Simulationen, um das Sicherheitsbewusstsein zu überprüfen und zu stärken. Das Feedback der Mitarbeiter betont die Wichtigkeit personalisierter Schulungen, die an den Arbeitsalltag angepasst sind, und zeigt die Notwendigkeit umfassender und kontinuierlicher Schulungsprogramme sowie regelmäßiger Phishing-Simulationen zur nachhaltigen Steigerung der IT-Sicherheit.

Zudem wurden für die beiden Services je ein Business-Model-Canvas erstellt, welche hier eingesehen werden können.

1.13.1 Business-Model-Canvas FPM

Das Business Model Canvas dient dazu rauszufinden, ob und wie der Service umgesetzt werden kann.

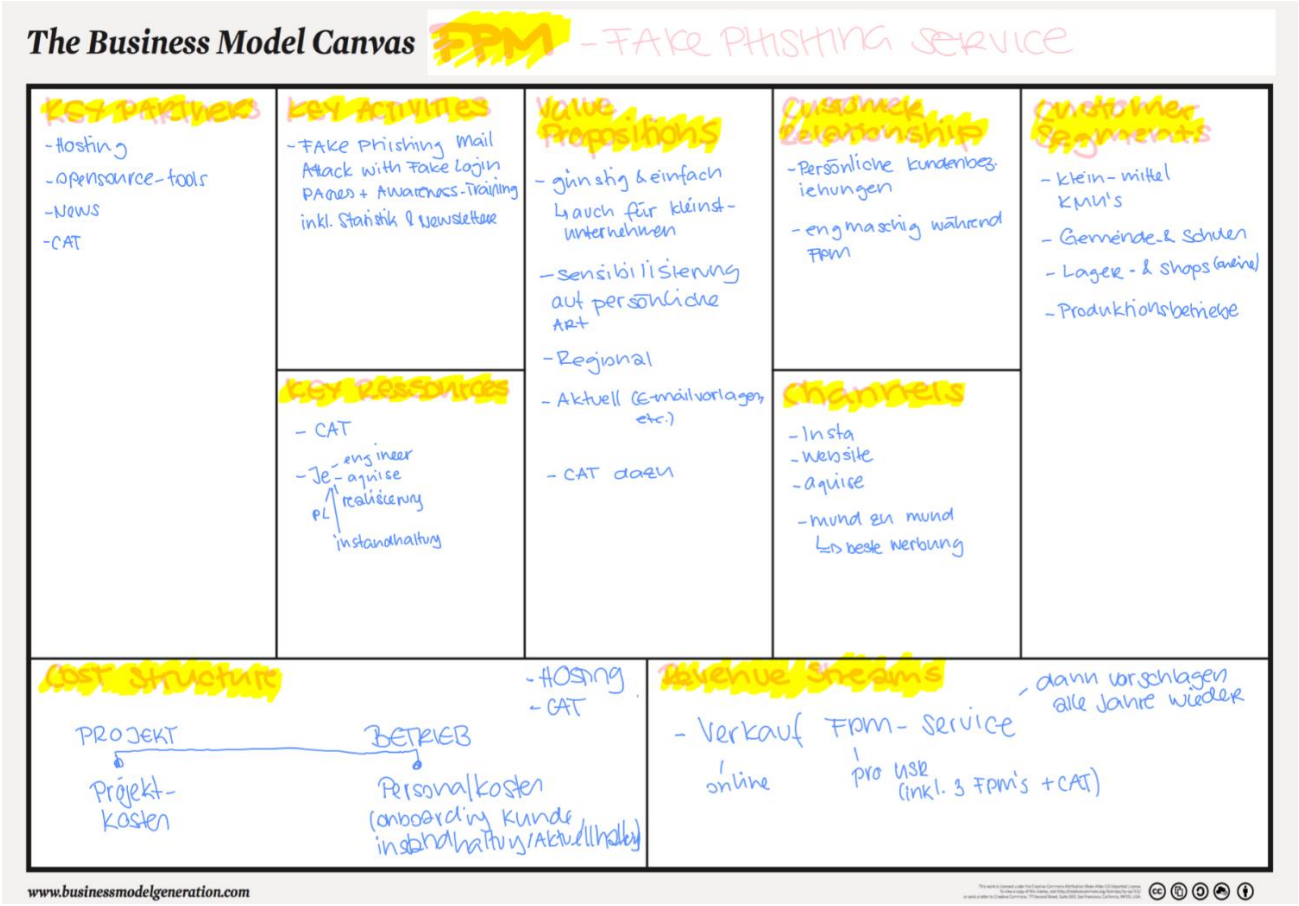


Abbildung 6 - Business Model Canvas FPM (im PDF zoombar)

1.13.2 Business-Model-Canvas CAT

Das Business Model Canvas dient dazu rauszufinden, ob und wie der Service umgesetzt werden kann.

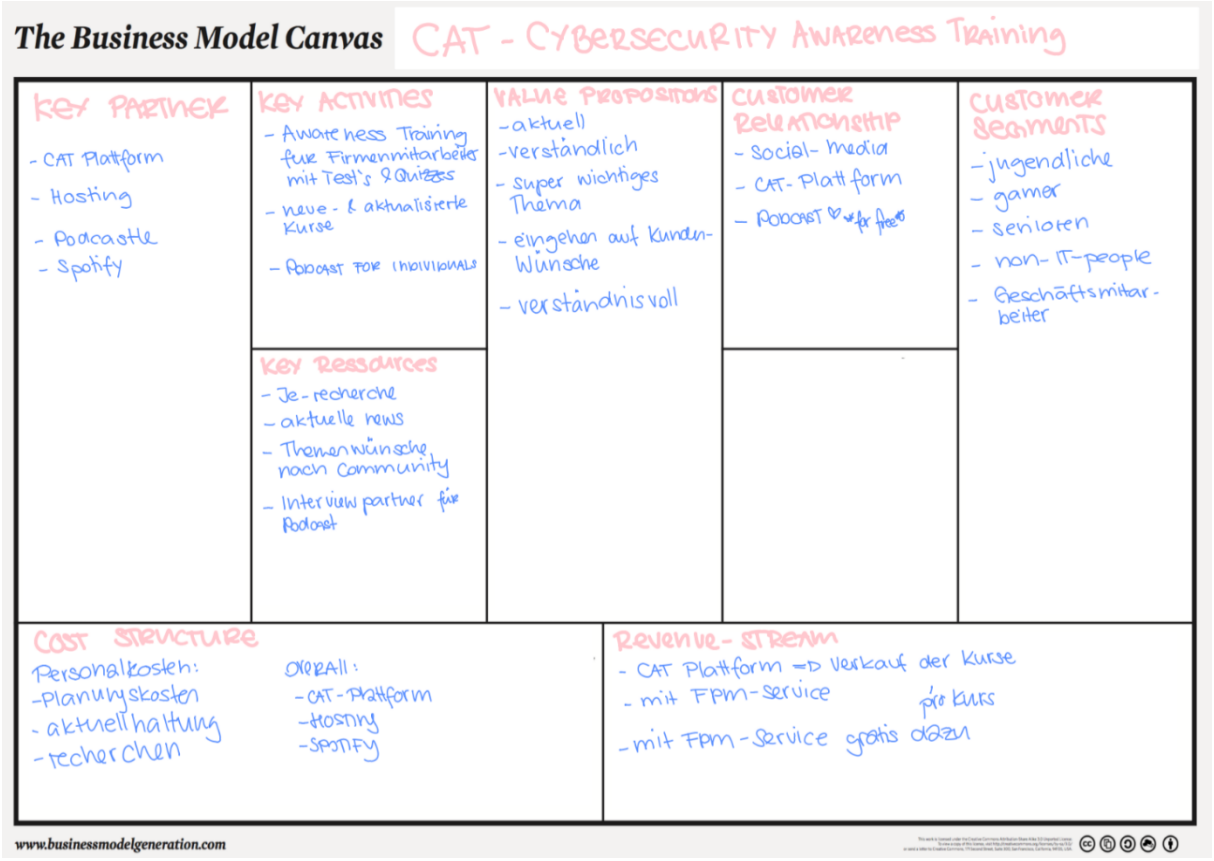


Abbildung 7 - Business Model Canvas CAT (im PDF zoombar)

2. Phase Konzept

Nachdem die Varianten entschieden wurden, konnte das folgende Konzept ausgearbeitet werden. In dieser Dokumentation geht es leglich über die Zusammenfassung der Phase Konzept. Alle Detailreicheren Informationen müssen in den Konzeptdokumenten nachgeschaut werden. Konzeptionelle Aussagen zur Lösung

2.1.1 Lösungsarchitektur

Die Lösung basiert auf einer dualen Architektur bestehend aus einem Fake Phishing Mail (FPM) Service und einem Cybersecurity Awareness Training (CAT). Der FPM-Service verwendet die Open-Source-Plattform GoPhish, die auf einer VM mit Ubuntu Server installiert wird. Der CAT-Service bietet interaktive und auf verschiedene Lerntypen abgestimmte Trainingsmodule an, die über die Plattform Teachable bereitgestellt werden.

2.1.2 Erklärung der technischen Umsetzung

Die technische Umsetzung des FPM-Services umfasst die Einrichtung einer VM, Installation und Konfiguration von GoPhish sowie die Erstellung von Phishing-Kampagnen mit angepassten E-Mail-Templates und Landing Pages. Um die Mehrkundenfähigkeit gewährleisten und die Sicherheit weiter gewährleisten zu können und zu verhindern, dass Kundendaten durcheinanderkommen, wird GoPhish bei jedem Kunden neu aufgebaut. Dank GoPhish’s einfache Installation und Konfiguration ermöglicht dies die Neuinstallation bei jedem Kunden. Dies dient auch der Sicherheit, da alles lokal beim Kunden läuft und alle Komponenten nach Ausführung wieder deinstalliert und gelöscht werden.

Wie GoPhish technisch aufgebaut ist, wir im Kapitel 2.2 „Design der Lösung“ erklärt

Der CAT-Service integriert verschiedene Lernmethoden und interaktive Elemente wie Minigames und Quizzes, die durch Teachable ermöglicht werden.

2.1.3 Tests

Tests werden sowohl funktional als auch nicht-funktional durchgeführt. Funktionale Tests überprüfen die korrekte Zustellung und Interaktion mit Phishing-E-Mails, während nicht-funktionale Tests die Sicherheit und Benutzerfreundlichkeit der Plattformen überprüfen. Testfälle sind detailliert dokumentiert und umfassen spezifische Szenarien wie das Öffnen von Phishing-E-Mails, Eingabe von Zugangsdaten und die Auswertung der Berichte.

ID2132_StorrerJessica_CAT_Testkonzept_v1.pdf & ID2132_StorrerJessica_FPM_Testkonzept_v1 & Testprokotolle

2.1.4 Security und Datenschutz

Sicherheitsmassnahmen umfassen die Nutzung von SSL-Zertifikaten, die Sicherstellung der Datenintegrität durch SQLLite-Datenbanken und die Implementierung von Datenschutzrichtlinien gemäss den geltenden gesetzlichen Vorschriften. Zugangsdaten und personenbezogene Daten werden verschlüsselt gespeichert und nur autorisierten Benutzern zugänglich gemacht

2.1.5 Aktualisierungen und LifeCycle

Für den Betrieb der Lösung müssen regelmässige Updates und Wartungen durchgeführt werden. Dies umfasst die Aktualisierung der GoPhish-Software, die Überwachung der Phishing-Kampagnen und die Anpassung der Trainingsinhalte im CAT-Service basierend auf Benutzerfeedback und neuen Bedrohungen.

2.2 Design der Lösung

Grob- und Detaildesign, Prozesse, Abläufe der beiden Services.

2.2.1 Grobdesign FPM

Das Grobdesign beinhaltet die Bereitstellung einer zentralen VM, auf der GoPhish installiert und konfiguriert wird. Diese VM dient als Host für die Phishing-Kampagnen. Parallel dazu wird die Teachable-Plattform genutzt, um die Trainingsmodule des CAT-Services bereitzustellen. Beide Systeme sind über ein Dashboard integriert, das eine zentrale Verwaltung und Überwachung ermöglicht. Die Lösung wird so gebaut werden, dass bei jedem Kunden der FPM-Server neu aufgesetzt, installiert und konfiguriert wird. Da GoPhish eine übersichtliche und relativ einfache Konfiguration hat, wird diese, um die Mehrkundenf$higkeit beizubehalten, bei jedem Kunden neu installiert und konfiguriert. Dies dient ebenso zur Sicherheit der Daten, dass diese nie bei einem anderen Kunden landen.

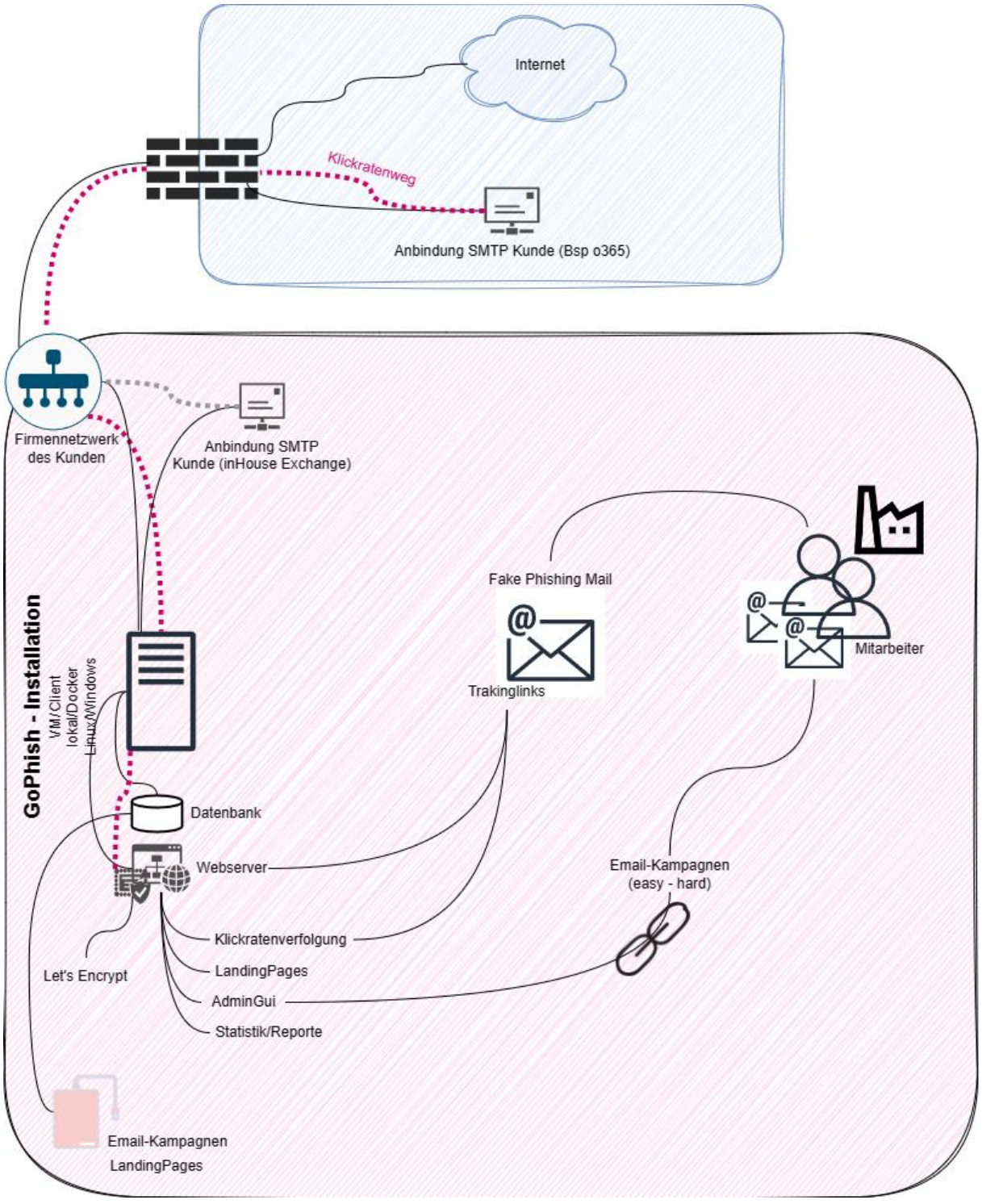


Abbildung 8 - Netzplan GoPhish

2.2.2 Detaildesign FPM

Das Detaildesign umfasst die spezifische Konfiguration der GoPhish-VM, einschliesslich der Netzwerkeinstellungen und der Anpassung der E-Mail-Templates und Landing Pages.

2.2.3 Technischer Aufbau GoPhish

GoPhish und seine Komponenten

Die Grundkonfigurationen der GoPhish-Plattform umfassen verschiedene Parameter, die in der config.json-Datei festgelegt werden müssen. Dazu gehören die IP-Adresse und der Port des Admin-Servers sowie des Phishing-Servers, die TLS-Einstellungen und die Pfade zu den SSL-Zertifikaten. Wichtig ist, dass die Datei nur vom richtigen Benutzer lesbar ist, da sie sensible Datenbankanmeldeinformationen enthält. Für die Phishing-Kampagnen werden drei Schwierigkeitsgrade angeboten, die über eine konfigurierbare Admin-Oberfläche verwaltet werden können. Es können Start- und Enddaten für den Versand von Phishing-Mails festgelegt sowie SMTP-Profile für den E-Mail-Versand definiert werden. Die Empfängergruppen können per CSV importiert werden, und die E-Mail-Templates müssen spezifische Platzhalter enthalten, um die Klickratenverfolgung zu ermöglichen.

Die Klickratenverfolgung erfolgt durch die Generierung eindeutiger IDs (rid-Parameter) für jeden Empfänger, die in der Datenbank gespeichert werden. Landing-Pages und E-Mail-Templates werden entsprechend verknüpft, um die Benutzerinteraktionen zu erfassen und Berichte zu erstellen. GoPhish bietet benutzerfreundliche Optionen zum Importieren von E-Mail-Templates und Landing-Pages sowie zur Verwaltung von SMTP-Profilen und Kampagnen. Die Plattform erleichtert zudem die Weiterleitung der Benutzer nach der Eingabe von Anmeldeinformationen und unterstützt detaillierte Konfigurationsmöglichkeiten für eine effektive Phishing-Simulation und das anschließende Reporting.

Detailgetreuere Erklärung sind dem Dokument *ID2132_StorrerJessica_FPM_Konzept_v1.pdf*, Kapitel4, zu entnehmen.

Für die Installation in der Realisierung existiert eine Installationscheckliste, welche hier eingesehen werden kann: *ID2132_StorrerJessica_FPM_ChecklisteInstallation_v01.pdf*

2.2.4 Kampagnen

GoPhish nennt die FPM's Kampagnen. Die Kampagnen bestehen aus folgenden Teilen:

Email Template

Das Emailtemplate wird das aussehen der eigentlichen FPM bestimmen und kann einfach per „Import Email" – eine der vielen Funktionen von GoPhish – realitätsgetreu importiert werden. In diesem Template werden dann die URL's und Platzhalter definiert. Das Email kann dann mithilfe der HTML-Ansicht noch genauer auf die Kunden angepasst werden. (Erklärt unter „Klickratenverfolgung") Ebenso kann hier die Absenderemailadresse frei angepasst werden.

Landing Page

Genau wie das Emailtemplate kann ebenso die Fake-Landing-Page – also die Page welche beim Klick im FPM geöffnet werden soll – definiert. Diese kann ebenso mithilfe von GoPhish importiert und angepasst werden. Für die authentität der Landing-Pages werden Domainzonen eingerichtet.

User & Groups

Die Users & Groups – also die zu angreifenden Emailadressen der Mitarbeiter – können als CSV in GoPhish in Gruppen hochgeladen werden. Diese werden dank dem Kundeninfoblatt vom Kunden bereitgestellt. Ebenso stellt GoPhish ein CSV-Template bereit, damit man weis, wie das CSV aussehend muss.

Sending Profile

Im Sending Profile wird der Absender definiert, welches die FPM's sendet. Hier reicht eine STMP-Adresse welche berechtigt ist zum senden. Da in den Emailteplates die Absenderadresse gefaket werden kann, kann mit seiner SMTP-Anbindung pro Kunde gearbeitet werden. Diese wird ebenso vom Kundeninfoblatt vom Kunden angefordert, sodass SPAM-Rules soweit als möglich umgehen werden können.

Klickratenverfolgung, URL's und Platzhalter

Die Klickratenverfolgung geschieht so, dass im Emailtemplate gewisse Platzhalter definiert werden müssen. Diese sind vordefiniert, anbei die welche in diesem Projekt gebraucht werden:

{{.URL}}

Dieser Platzhalter dient dazu, dass wenn der User auf die im Mail enthaltenen Link klickt, diese auch zur Richtigen Landing Page weitergeleitet wird. Dies wird in der Datenbank als RID-Parameter gespeichert und dient dann zur Klickratenverfolgung. (Zur veranschaulichung siehe Netzplan)

{{.Vorname}}

Dies dient dazu, den User im FPM persönlich ansprechen zu können. Dies nimmt dann dem Users' Vorname der anzugreifenden. Diese wird nach hochladen der UseCSV ebenso in der Datenbank gespeichert und abgelegt.

{{.Emailadress}}

Gleich wie beim Vornamen-Platzhalter dient diese dazu die FPM persönlicher zu gestaltet.

Die genaue Erläuterung wird im Dokument *ID2132_StorrerJessica_FPM_Konzept_v1.pdf* gefunden.

Emailkampagnen zusammenhänge (FPM-Kampagnen Zusammenhänge)

In der folgenden Grafik wird erläutert wie eine FPM-Kampagne mit den verschiedenen Konfigurationen zusammengestellt wird.

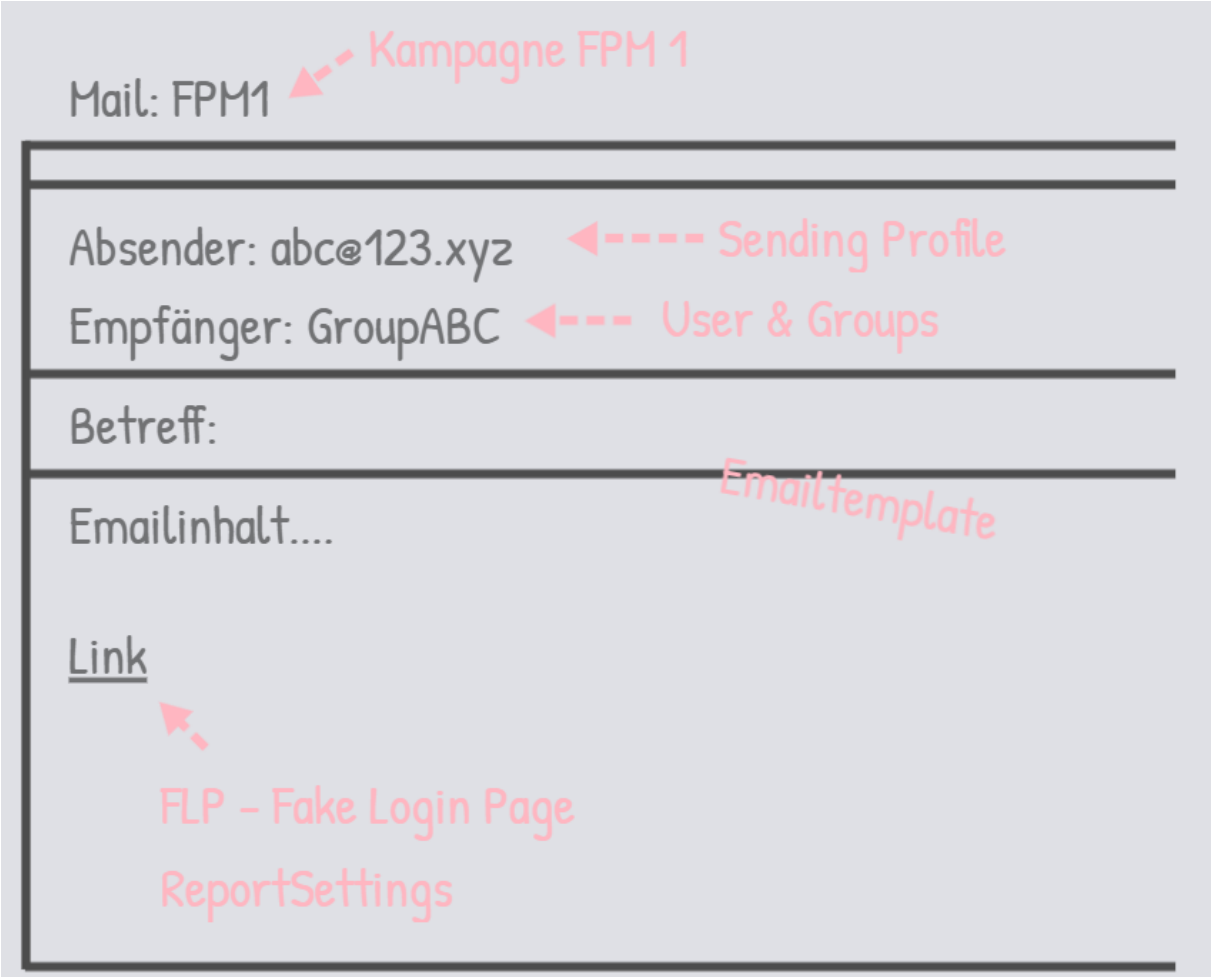


Abbildung 9 – Kampagnenzusammenhänge

Das Detailnetzkonzept, für wie die GoPhish Kampagnen verlinkt sind, sieht folgendermassen aus.

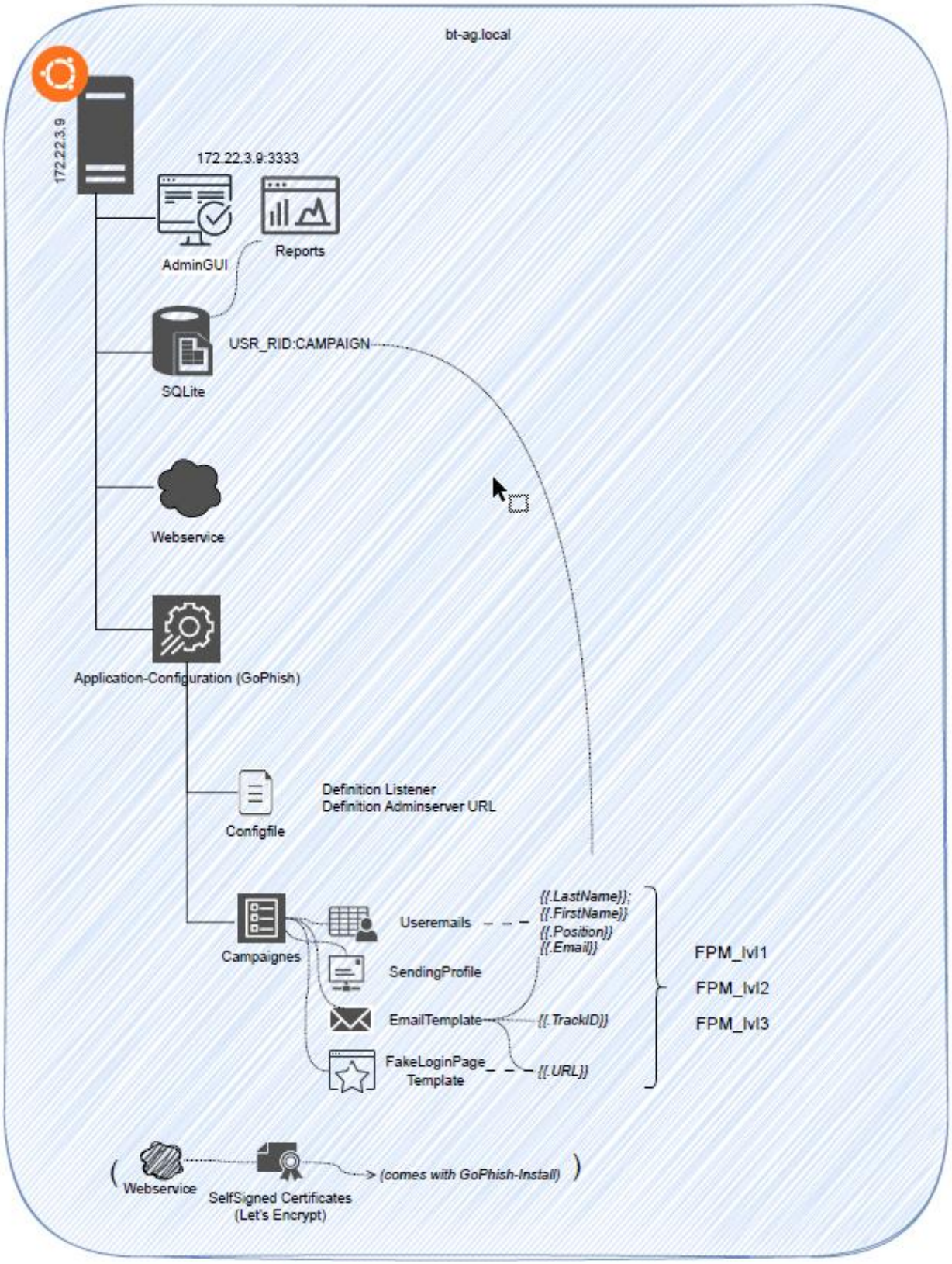
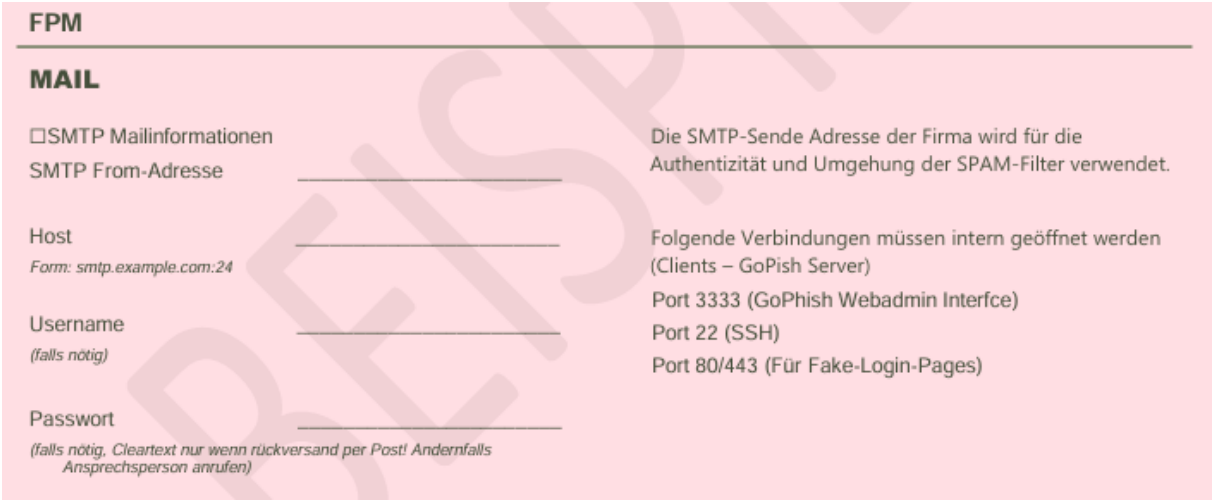


Abbildung 10 - Detailkonzept Netzwerkkomponenten/Konfiguration GoPhish

2.2.5 Kundeninfoblatt

Das Kundeninformationsblatt enthält die Infos für den Aufbau der VM/des Servers, sowie was der Kunde bereitstellen muss. Dies muss dem Kunden beim Onboarding angegeben werden, sodass der Kunde dies ausfüllen kann.

Das Kundeninfoblatt wird folgende Informationen enthalten:



FPM

MAIL

☐SMTP Mailinformationen

SMTP From-Adresse _____

Die SMTP-Sende Adresse der Firma wird für die Authentizität und Umgehung der SPAM-Filter verwendet.

Host _____

Form: smtp.example.com:24

Folgende Verbindungen müssen intern geöffnet werden (Clients – GoPish Server)

Port 3333 (GoPhish Webadmin Interfce)

Port 22 (SSH)

Port 80/443 (Für Fake-Login-Pages)

Username _____

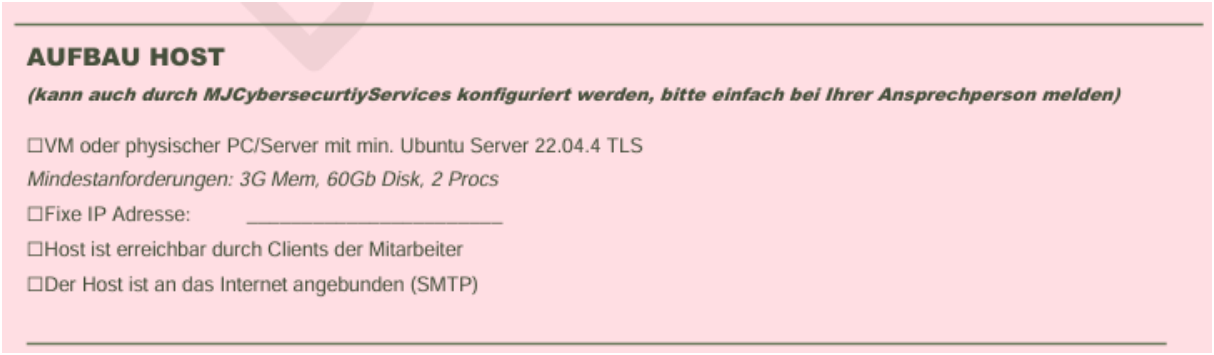
(falls nötig)

Passwort _____

(falls nötig, Cleartext nur wenn rückversand per Post! Andernfalls Ansprechsperson anrufen)

Abbildung 11 - Auszug Kundeninfoblatt

Wie im Konzept erarbeitet, wird die STMP Anbindung via Kunden-SMTP erfolgen, um die SPAM-Rules so weit als möglich zu umgehen. Zudem wird beschrieben, welche Ports und Verbindungen zum Server geöffnet werden müssen



AUFBAU HOST

(kann auch durch MJCybersecurtiyServices konfiguriert werden, bitte einfach bei Ihrer Ansprechperson melden)

☐VM oder physischer PC/Server mit min. Ubuntu Server 22.04.4 TLS

Mindestanforderungen: 3G Mem, 60Gb Disk, 2 Procs

☐Fixe IP Adresse: _____

☐Host ist erreichbar durch Clients der Mitarbeiter

☐Der Host ist an das Internet angebunden (SMTP)

Abbildung 12 - Auszug Kundeninfoblatt

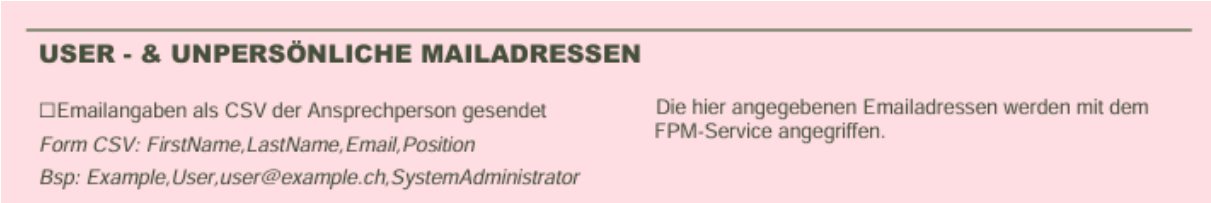


Abbildung 13 - Auszug Kundeninfoblatt

Des Weiteren kann der Kunde auf diesem Blatt noch die Kursauswahl einschränken, oder neue CAT-Kurse wünschen.

Das Kundeninfoblatt kann hier heruntergeladen werden: *ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v01.pdf*

2.2.6 Die drei Fake-Mails Konzept

Die Überlegungen welche die drei FPM's sein werden, wurde nach „schwierigkeit & erkennbarkeit" gewählt. *ID2132_StorrerJessica_FPM_Konzept_v1.pdf*

Die drei Fake Mails werden folgende sein:

FPM	Inhalt	Warum
FPM1 – Das Einfache	Galaxus-Geschenk	Hier wird von Galaxus ein Gratis-Geschenk angepriesen, dies sollte möglichst offensichtlich sein dass es SPAM ist.
FPM2 – Der Klassiker	O365 Passwort-Ablauf	Das Email des Passwort-Ablaufs von o365 sollte schon echt aussehen, aber mit ein paar Fehlern versehen.
FPM3 – Das gut Social Engineerte	Bugoutstore Geschenkgutschein	Als Dankeschön für die Treue der Mitarbeiter erhalten die Mitarbeiter einen Gutschein für dem Pilotkunden's neuen Store.

		Dieses wurde jedoch in der Realisierung noch auf ein besseres Thema geändert!

Tabelle 5 - Die drei Fake-Mails

2.2.7 Überwachung der FPMs und Handhabung Meldungen

Dank dem sehr übersichtlichen Admin-Panel von GoPhish kann dort jedes Email zu jedem User auf die Minute genau verfolgt werden. In den UseCases weiter in diesem Kapitel wird beschrieben, wie die User mit den UseCases umgehen werden können.

2.2.8 Grobdesign CAT

Für den CAT-Service werden die Trainingsmodule detailliert geplant und implementiert, wobei jede Woche einen spezifischen Fokus hat, wie z.B. Phishing-Erkennung, Social Engineering und IT-Sicherheit am Arbeitsplatz. Die Trainingsinhalte sind interaktiv und beinhalten Audiogeschichten, Minigames und Quizzes .

2.2.9 Detaildesign CAT

Dank der Studie, Informationsbeschaffung wie Umfragen etc, konnte eruiert werden, welche Theman in den Schulungen erarbeitet werden sollen.

Es werden drei Wochen Kurs aufgesetzt, welche in pro Tag max 15Minuten abgearbeitet werden können. Die Kurse müssen den vier Hauptlerntypen abgestimmt werden. Mehr dazu im CAT-Konzept. Zudem werden pro Kurs diverse Antwortkasten dem Teilnehmenden zur Verfügung gestellt, sodass Feedback und gelerntes aufgeschrieben werden kann.

Das Design der Kurse liegt ganz bei der Kreativität des Kurserstellenden.

Kunden, welche via FPM-Service auf CAT weitergeleitet werden, erhalten ein Coupon für Gratis-Zugang.

Folgend werden die Kurse und deren Themen Beschrieben, sowie welche Interkationen, Games, Downloads angeboten werden.

Kurs / Idee	Themen	Notizen	Quizzes, Minigames, etc
Kurs Woche 1	Phishing Mails: Erkennen & Handeln	Tipps und Trick über das Erkennen und Handeln von Phishing Mails	Phish or No-Phish, erkennen von FPM's Div. Interaktionen und Bilder. Ein Quizz über das gelernte muss vorhanden sein. -> Alles im Ermessen des Kurserstellers Diverse Antwortkasten für Feedback von den Teilzunehmenden.
Kurs Woche 2	Wissen wie der Hacker denkt: Ein Audioexkurs über Social Engineering	Hier sollen vier Geschichten über die vier Haupt-Social Engineering Themen erzählt werden. So bleiben diese dem Teilzunehmenden. (FOMO, Vertrauen & Authorität, Gegenseitigkeit & Norm der Gegenseitikeit, Emotionale Manipulation) Und Zusatz „Achtsamkeit“	Hier sollten vier Geschichten erzählt werden, schön ist noch ein Achtsamskeitszusatz, da die Achtsamkeit der erste Schritt zum Erkennen von SocialEngineering Hacks sind.
Kurs Woche 3	IT-Security am Arbeitsplatz	Hier sollten Themen wie der Umgang mit DeepL, ChatGPT, Google & co erläutert werden, sowie Daten verschleiert werden können. Passwort-Themen, etc	Mithilfe von Suchbildern, oder interaktive Fragen was zu IT-Security gehört, werden die Teilnehmer abgeholt und können interaktiv und visuell lernen. Ein Quizz über das gelernte muss vorhanden sein. Ein BigPicture in diversen Farben zum Download über die drei Wochen Kurs zum ausdrucken unf aufhängen.

Digitale Downloads	Social Meida Awareness Poster Big Pictures Was sind Phishing Mails?-Poster	Diverse Digitale Downloads zum Ausdrucken und Aufhängen. Diverse Antwortkasten für Feedback von den Teilzunehmenden.	

Tabelle 6 - Kurse & Inhalt

2.3 Prozesse und Abläufe FPM & CAT

Folgende werden die wichtigsten Prozesse und Abläufe erläutert. Alle Informationen können im *ID2132_StorrerJessica_FPM_Konzept_v1.pdf & ID2132_StorrerJessica_CAT_Konzept_v1.pdf* nachgelesen werden

2.3.1 FPM-Service UseCases

Beim FPM-Service gibt es zwei Arten von UseCases, welche ebenso als Prozesse angesehen werden können. Zum einen der Integrationsprozess eines Kunden und zum anderen die UseCases wie mit einer FPM umgegangen werden kann.

2.3.2 UseCase Integrationsprozess Kunde

In der folgenden Grafik wird der Integrationsprozess des Kundens dargestellt.
Voraussatzung dafür ist, dass Akuise & Vertragsabschluss vorhanden ist.

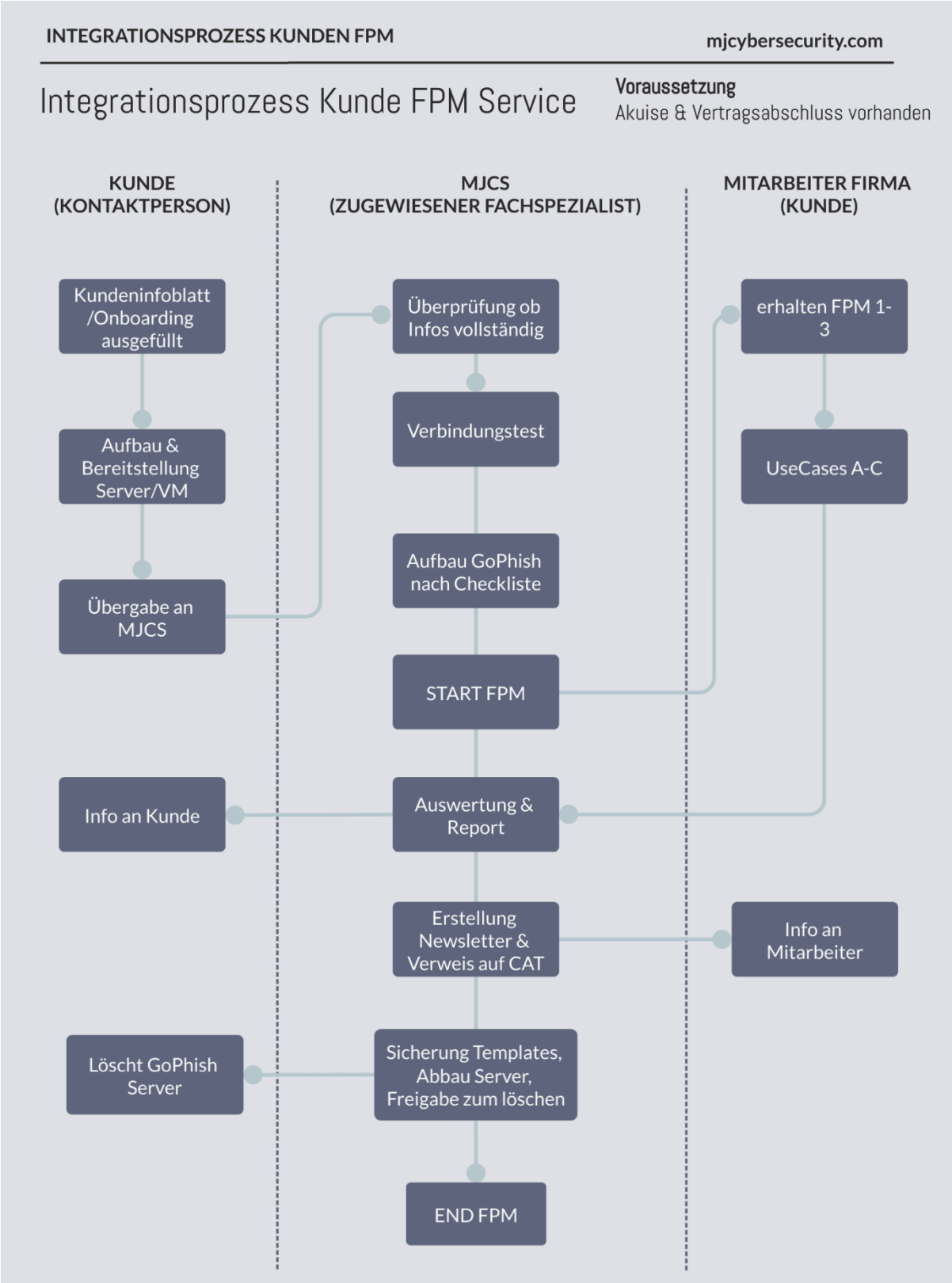


Abbildung 14 - Integrationsprozess Kunde FPM

2.3.3 UseCases FPM Interaktion und Meldung nach Kundenprozess

Folgende UseCases / Prozesse gelten bei Senden, Interaktion und Empfang der FPM’s.

UseCase A – Worst Case Szenario – Interaktion mit Link und Eingabe Credentials

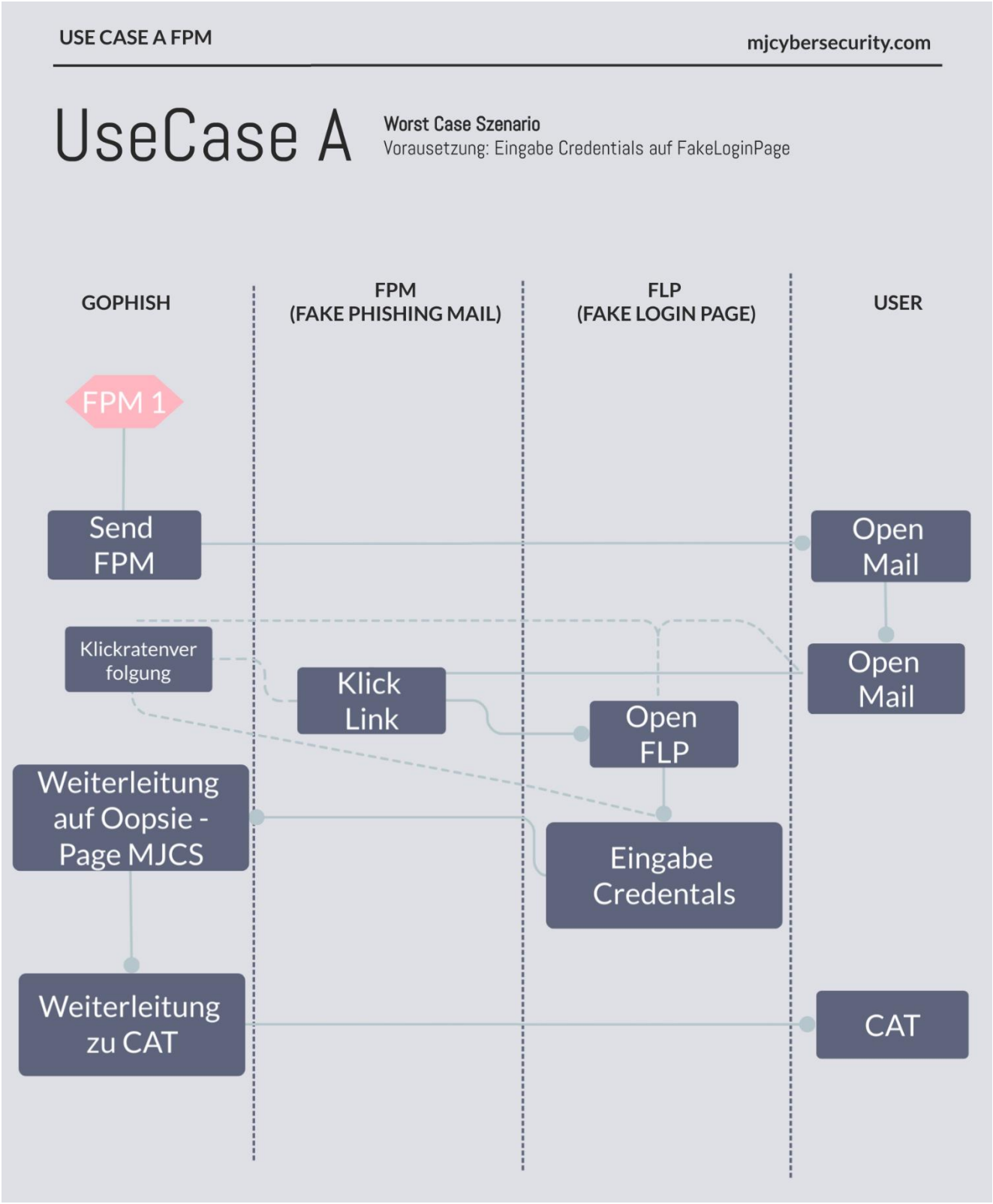


Abbildung 15 - FPM UseCase A WorstCase Szenario

UseCase B – User Klickt auf Link

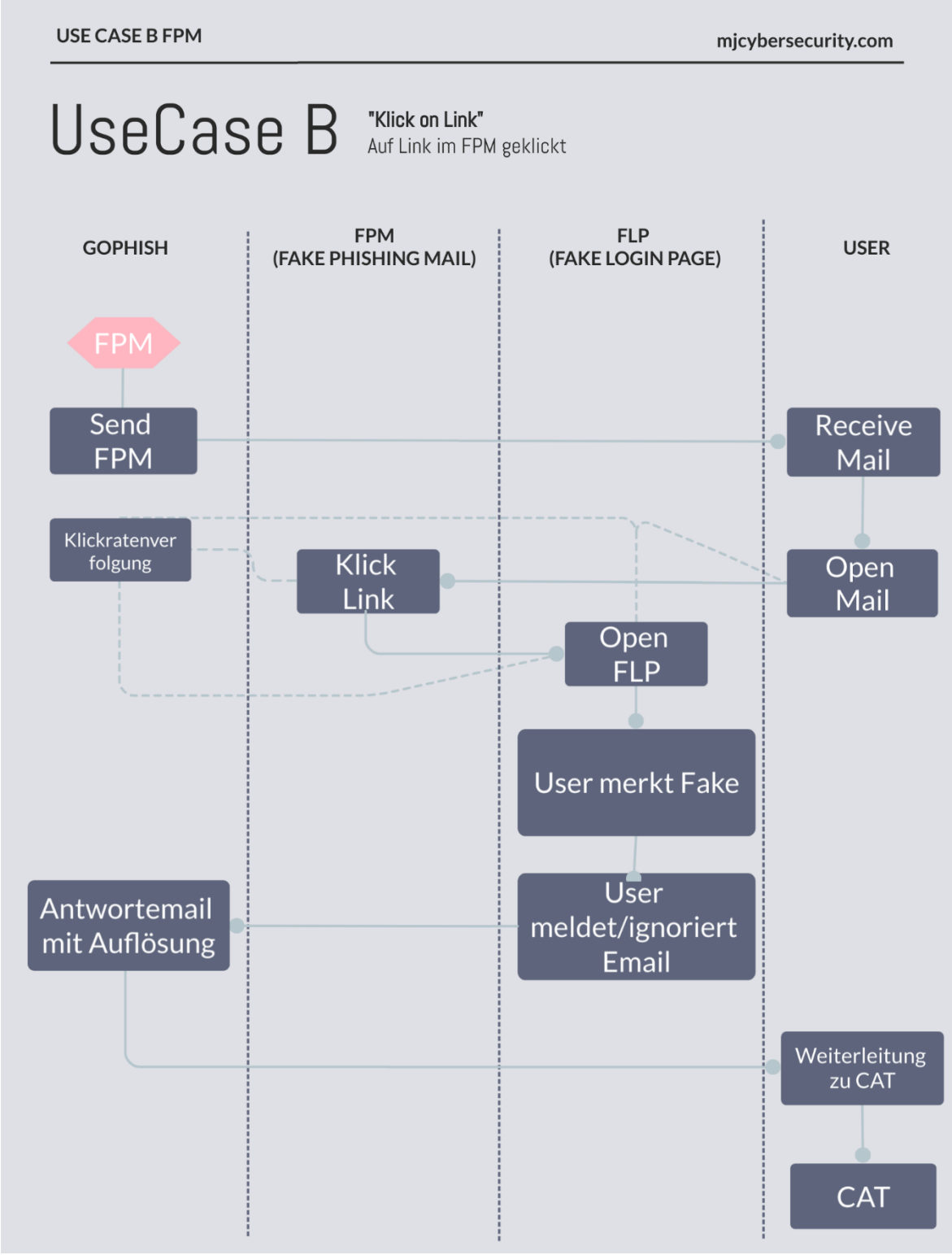


Abbildung 16 - FPM UseCase B User klickt auf Link

UseCase C – User Reportet / Löscht Email

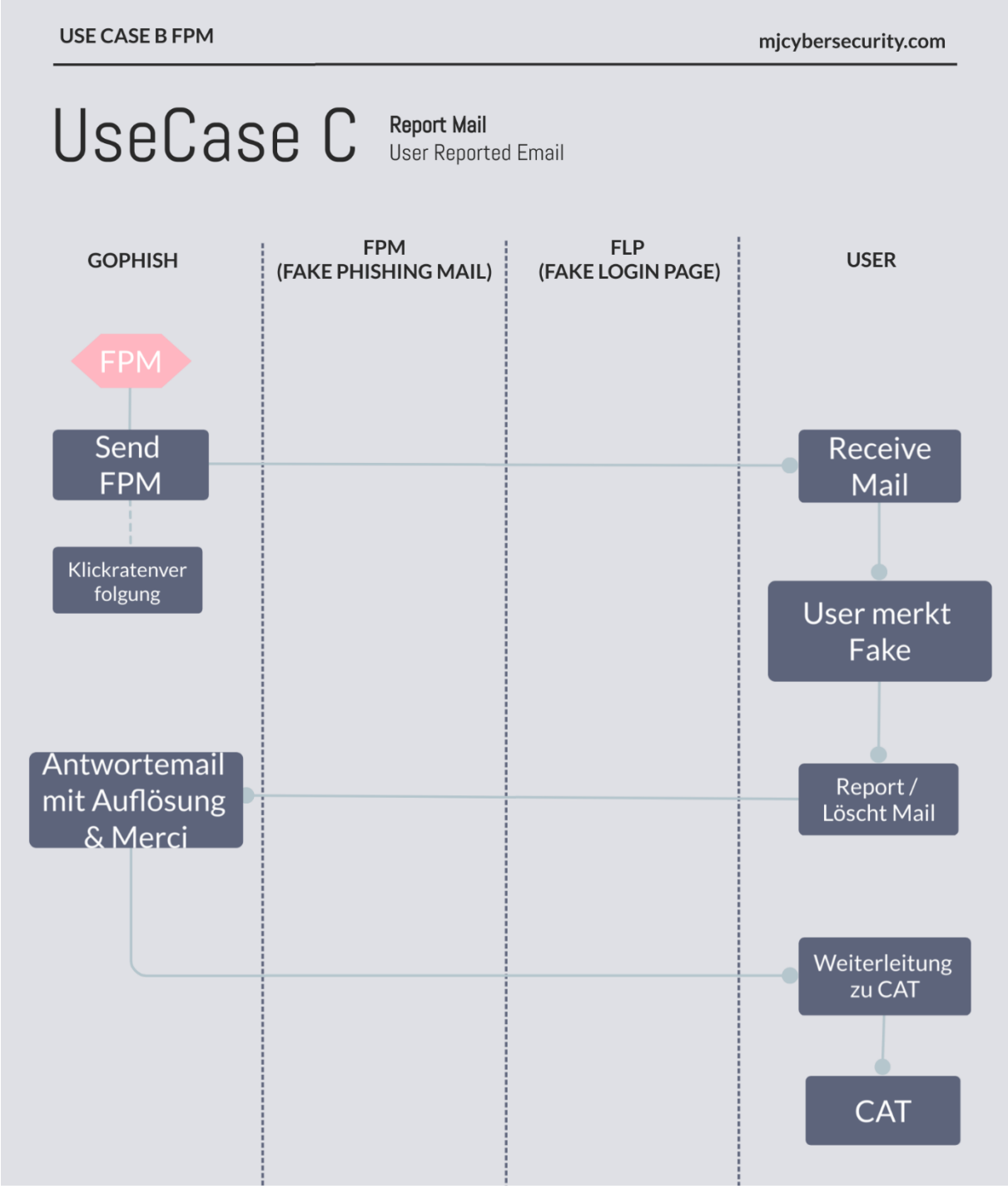


Abbildung 17 - FPM UseCase C Report / Delete Mail

2.3.4 UseCase CAT-Service

In der folgenden Grafik wird der UserCase des CAT-Services dargestellt.

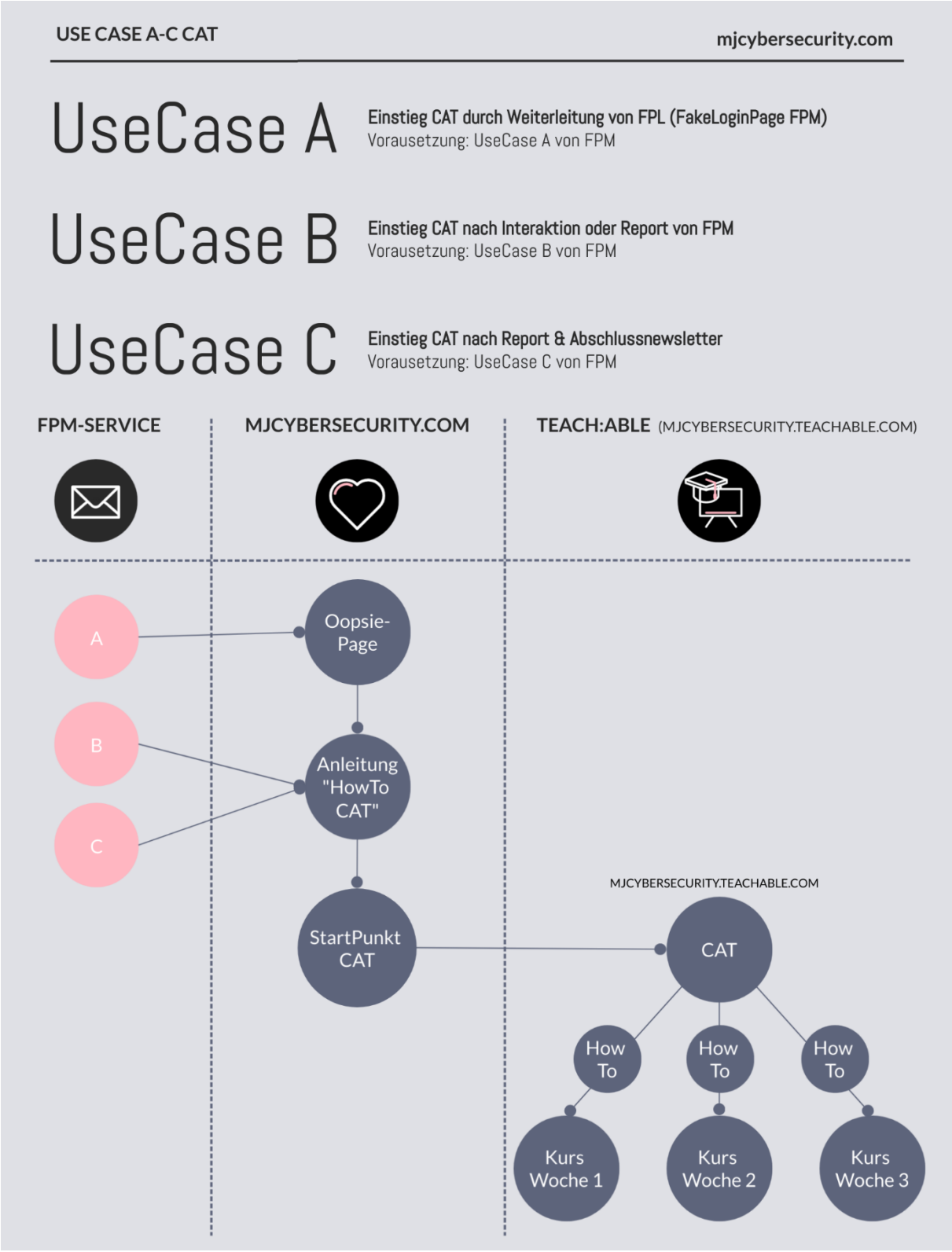


Abbildung 18 - UseCase A-C CAT

2.3.5 Transparenz und Nachvollziehbarkeit

Alle Zusammenhänge und Prozesse sind in den entsprechenden Dokumenten detailliert beschrieben. Dies umfasst die technischen Spezifikationen, die Testfälle und die Schulungskonzepte. Die Dokumente sind so strukturiert, dass sie eine klare Nachvollziehbarkeit und Transparenz der einzelnen Schritte und Entscheidungen bieten.

Diese Zusammenfassung fasst die wichtigsten Punkte der beiden Konzepte zusammen und zeigt die Implementierung und den Betrieb der Lösung auf. Die detaillierten Dokumente sind im Anhang enthalten und bieten eine umfassende Einsicht in die jeweiligen Bereiche.

3. Phase Realisierung

In den folgenden Kapiteln wird die Realisierung erläutert, diese wird pro Service (FPM&CAT) dokumentiert.

3.1 FPM Service

In diesem Kapitel wird die Realisierung des FPM-Services erläutert. Für Bilder und weitere Eindrücke oder Details kann dies im folgenden Dokument eingesehen werden.

ID2132_StorrerJessica_RealisierungDurchführung_FPM_v1.pdf

3.1.1 Installation und Grundkonfiguration GoPhish Server

Für die Installation des GoPhish Servers wurde eine Ubuntu-VW im Kundenfirmennetzwerk bereitgestellt. Auf ebendiesem wurde Ubuntu 22 installiert.

Für Specs der Ressourcen des Servers siehe Kundeninfoblatt: ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v1.pdf

Sobald der Server installier wurde, wurde GoPhish vom neusten Git-Repo heruntergeladen, entpackt und installiert. Sobald GoPhish installiert wurde, muss das Konfigurations-File mit folgenden Parametern angepasst werden:

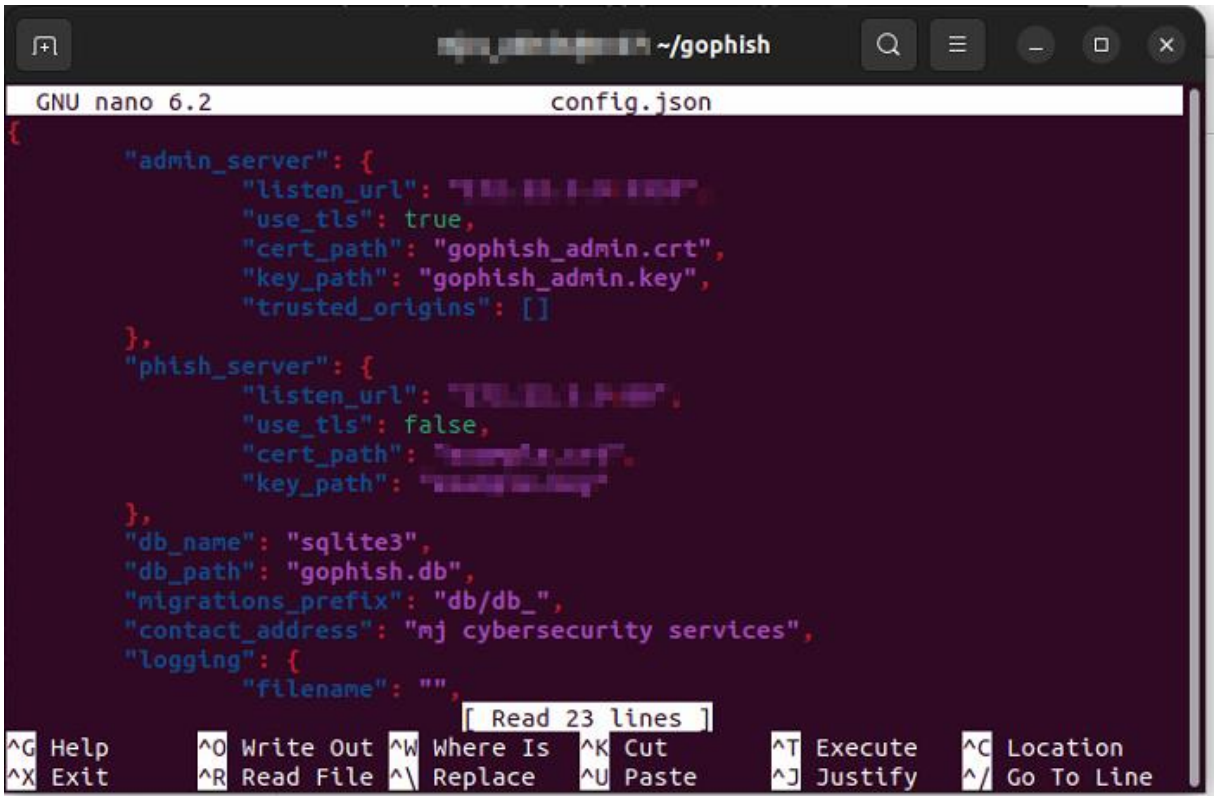


Abbildung 19 - Konfigurationsfile GoPhish

Nachdem Starten des neu installierten GoPhish Services ist die Applikation voll funktionsfähig und das Admin-Panel kann mittels [IP]:3333 aufgerufen werden.

3.1.2 Ausgearbeiteter Netzwerkplan

Im folgenden Netzplan sind alle Verbindungen von GoPhish, Domains, etc ersichtlich.

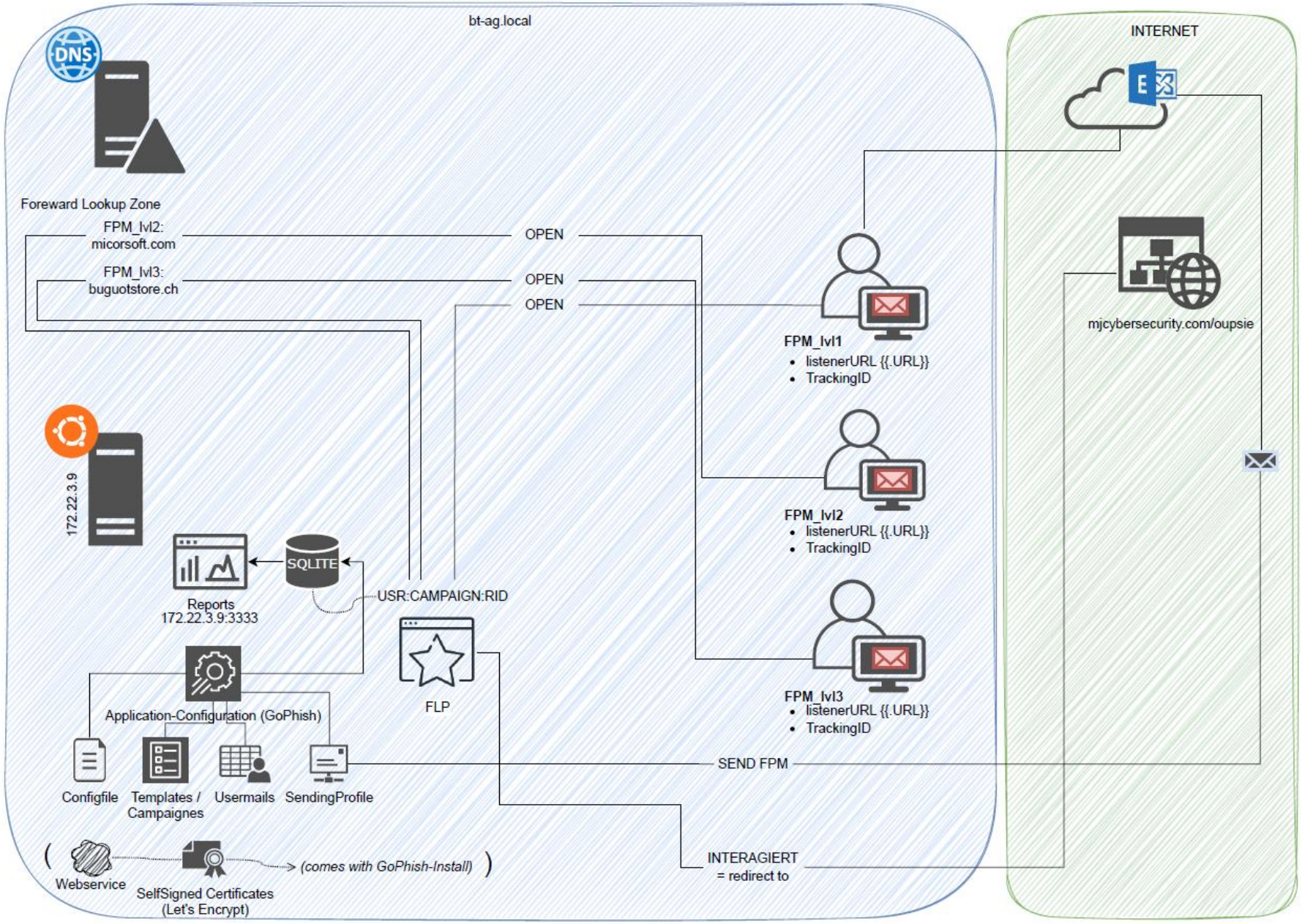

bt-ag.local
INTERNET
DNS
Foreward Lookup Zone
FPM_lvl2:
micorsoft.com
FPM_lvl3:
buguotstore.ch
OPEN
OPEN
OPEN
FPM_lvl1
listenerURL {{.URL}}
TrackingID
FPM_lvl2
listenerURL {{.URL}}
TrackingID
FPM_lvl3
listenerURL {{.URL}}
TrackingID
mjcybersecurity.com/oupsie
172.22.3.9
SQLITE
Reports
172.22.3.9:3333
USR:CAMPAIGN:RID
FLP
Application-Configuration (GoPhish)
Configfile
Templates /
Campaignes
Usermails
SendingProfile
SEND FPM
Webservice
SelfSigned Certificates
(Let's Encrypt)
(comes with GoPhish-Install)
INTERAGIERT
= redirect to

Abbildung 20 - Detaillierter Netzplan mit allen Komponenten

3.1.3 Erstellung und Durchführung der Phishing-Kampagnen

Die Erstellung von Emailtemplates, Landingpages und Kampagnen erfolgten nach Konzept. Die detailgetreue Realisierung kann im folgenden Dokument eingesehen werden.

ID2132_StorrerJessica_RealisierungDurchführung_FPM_v1.pdf

Die Emailkampagnen wurden wie folgt gesendet.

Kampagne	Start Kampagne	Ende Kampagne
FPM1 «Galaxus-Fake» Das einfache	17. April 2024	23. April 2024
FPM2 «Microsoft Passwortwechsel» Der Klassiker	22. April 2024	26. April 2024
FPM3 «QR-Code Fraud» Das Fiese	30. April 2024	1. Mai 2024
Versand Report & Newsletter	15. Mai 2024	

Tabelle 7 - Emailkampagnen

3.1.4 Konfiguration der Kampagnen

Die jeweiligen Konfigurationen werden gesichert, damit eine Bibliothek von Fake-Mails entstehen wird. Da aber die Emails und LoginPages schnelllebig sind und viel wechseln, müssen diese eventuell je nach FPM angepasst werden.

3.1.5 Marketing

E-Mail-Marketing, Social Media Kampagnen, Content Marketing und QR-Code Marketing.

3.1.6 Tatsächliche Kostenstruktur und Preisstrategie

Folgende Preisstrategie wurde ausgearbeitet:

Kosten FPM einmalig pro Emailadresse
Beinhaltet

- 1 Fake Phishing Mail Pro Emailadresse
- 3 Wochen eTraining CAT
- Abschlussnewsletter & Report

= CHF 24.80

Pro weiteres FPM = CHF 11.20

Beispiel Kunde mit 70 Emailadressen und 3 FPM‘s
Kunde wünscht 3 FPM’s für alle 70 Emailadressen:

70xCHF24.80 = **CHF 1736.-**

+

70*CHF11.20*2 = **CHF 1568.-**

Gesamtpreis für drei FPM, CAT, Abschlussnewsletter & Report für 70 Emailadressen
= **CHF 3‘304.-**

3.1.7 Tatsächlicher ROI & Break-Even

Folgend sind die Kosten die mit der Implementierung des FPM-Services und dem laufenden Betrieb verbunden sind aufgezeit.
Anders als in der Realisierung wird hier nun pro Emailadresse gerechnet. Siehe Musterbeispiel aus Kapitel 3.1.6 Dies macht mehr sinn, da die Kosten nicht abschrecken und so mehr Kunden angesprochen werden können.

Projektkosten

Personalkosten: 160 CHF/Stunde

Geplante Stunden: 240 Stunden

Gesamte Personalkosten: 38.400 CHF

Aufwandskosten pro Kunde:

Arbeitsaufwand: 15 Stunden pro Kunde zu CHF 160 pro Stunde = CHF 2'400

Einnahmen Pro Kunde

Angenommen Musterbeispiel aus 3.1.6 (Firma mit 70 Emailadressen, 3 FPM)

CHF 3304.-

Berechnung ROI

Nun wird die ROI-Berechnung durchgeführt.

$$\mathrm{ROI} = \left(\frac{\mathrm{Einnahmen} - \mathrm{Kosten}}{\mathrm{Kosten}}\right) \times 100$$

Der ROI beträgt etwa -51.77%. Dies bedeutet, dass die Kosten die Einnahmen pro Kunde derzeit um 51.77% übersteigen. Es entsteht also ein Verlust pro Kunde.

3.1.8 BreakEven

ID2132_StorrerJessica_RealisierungDurchführung_FPM_v1.pdf

Um den Break-Even-Punkt zu errechnen, bei dem die Einnahmen die Kosten decken, teilen wir die Gesamtkosten pro Quartal durch die Einnahmen pro Kunde:

$$\text{ROI} = \left(\frac{\text{Einnahmen} - \text{Kosten}}{\text{Kosten}}\right) \times 100$$

Um die Ausgaben zu decken, sind mindestens 3 Kunden pro Quartal (genauer gesagt, etwa 2.07 Kunden, aber da man keine Bruchteile von Kunden haben kann, runden wir auf die nächste ganze Zahl auf) benötigt. Hier wurde wieder das Musterbeispiel aus 1.4 genommen.

3.1.9 Schlussfolgerung

Der negative ROI deutet darauf hin, dass entweder die Kosten pro Kunde gesenkt oder die Preise erhöht werden müssen, um profitabel zu sein. Zusätzlich könnten die Einnahmen pro Kunde durch den Verkauf zusätzlicher Dienstleistungen oder durch eine effizientere Skalierung der Dienstleistungen (z.B. Verringerung des Zeitaufwands pro Kunde) gesteigert werden.

3.1.10 Massnahmen

Der niedrige ROI deutet darauf hin, dass die Aquise der Kunden gemacht werden muss, sowie der CAT-Service gepusht werden muss.

3.1.11 WhitePaper

Alle wichtigen Infos, wie Supportinformationen, Onboarding, Pricing und weiteres können im FactSheet / WhitePaper eingesehen werden.

ID2132_FPM-Service-Whitepaper-MJCS_v1.pdf

Dieses WhitePaper kann dem Kunden übergeben werden.

3.2 CAT Service:

Der CAT Service wurde mit Teachable aufgebaut. Eine intuitive Onlinelernplattform bei welchen mit Code Snippets eigene Interaktive Elemente hinzugefügt werden können.

Spannende Einblicke in den Kurs im Dokument Realisierung CAT im Kapitel Einblicke *ID2132_StorrerJessica_RealisierungDurchführung_CAT_v1.pdf*

3.2.1 Kursentwicklung und Plattformintegration

Erstellung von Kursinhalten in verschiedenen Formaten (Audio, Video, interaktive Quizzes).

Integration der Kurse in die Teachable-Plattform.

Regelmässige Aktualisierung und Erweiterung der Kursinhalte basierend auf Kundenfeedback und neuen Sicherheitsbedrohungen.

3.2.2 Über den Service

Für den CAT-Service umfasst die Entwicklung und Integration eines vollständigen Kursmoduls in die Teachable-Plattform. Dies beinhaltet die Erstellung von interaktiven Inhalten und die Implementierung von Feedbackmechanismen, um den Lernerfolg zu messen.

3.2.3 Webauftritte

Damit die Kunden immer einen zetralen Einstiegspunkt haben, wurde ein Webauftritt aufgebaut welcher hier eingesehen werden kann:

Start | Finclvr (mjcybersecurity.com)

Zudem wurde für die Teachable Online Lernplattform ebenso diverse Webauftritte erstellt, einzusehen unter:

Home | CAT - Cybersecurity Awareness Training by Je (teachable.com)

Teachable arbeitet mit Sales-Pages, diese werden pro Kurs angelegt.

3.2.4 Marketing

Als Marketingstrategie werden folgende Kampagnen erstellt:

E-Mail-Marketing: Versand von personalisierten Angeboten an bestehende Kunden des Fake Phishing Mail Services.

Social Media: Gezielte Kampagnen auf Plattformen wie LinkedIn für professionelles Publikum und Instagramm für Privatpersonen.

POST-Uetendorf: Wochen-Ausstellungsplatz mit Fact-Sheet und Bonus-Coupons wenn in der Geschäftsstelle gesehen.

Content Marketing: Regelmässige Blogbeiträge und Artikel, die die Wichtigkeit von Cybersecurity hervorheben und auf den Kurs aufmerksam machen. Zusatz wie der CAP – Cybersecurity Awareness Podcast.

QR-Code Marketing: Da der QR-Code Fraud steigt, werden QR-Code Kleber überall verteilt, eine Art Gerillia-Werbung, um die Leute Aufmerksam auf Fraud zu machen. Der QR Code führt zu QR | MJCS (mjcybersecurity.com) welche darauf Aufmerksam macht, dass QR Code Phishing am Steigen ist.

E-Mail-Marketing, Social Media Kampagnen, Content Marketing und QR-Code Marketing.

3.2.5 Tatsächliche ROI Berechnung und Break-Even-Analyse

Es wird von ***150 Kunden pro Quartal*** gerechnet, welche ***je CHF 25.- für einen Kurs*** bezahlen.

Plattform- & Kurserstellungskosten

Ausgaben

Plattform-, Hosting- & Marketingkosten: CHF 170 pro Monat für 4 Monate = CHF 680.-

Kurserstellung und -betrieb: CHF 160 pro Stunde für 15 Stunden = CHF 2'400.- pro Quartal

Gesamtkosten Plattform- & Kursgestaltung: CHF 680 + CHF 2'400 = CHF 3'080.-

Einnahmen

(Annahme von 150 Kunden im ersten Quartal)

Einnahmen pro Quartal: 150 Kunden * CHF 25 = CHF 3'750

3.2.6 ROI-Berechnung

Folgend wird mit der folgenden Formel die ROI-Berechung durchgeführt.

$$\mathrm{ROI} = \left(\frac{\mathrm{Einnahmen} - \mathrm{Kosten}}{\mathrm{Kosten}}\right) \times 100$$

Das bedeutet bei den Zahlen:

$$\mathrm{ROI} = \frac{3'750 - 3'080}{3'080} \times 100 = \frac{670}{3'080} \times 100 \approx 21.75\%$$

Wir nehmen die Einnahmen von CHF 3'750 und die Gesamtkosten von CHF 3'080 und berechnen den ROI.

Mit den Kosten ergibt sich ein ROI von etwa 21.75%. Der Service ist profitabel.

3.2.7 Break Even

Folgend wird der Break-Even auf Kundenanzahl ausgerechnet.

Bei wievielen Kunden sind die Servicekosten gedeckt?

$$\text{Anzahl der Kunden} = \frac{\text{Gesamtkosten}}{\text{Preis pro Kunde}}$$

Das bedeutet in Zahlen:

$$\text{Break-Even-Kundenanzahl} = \frac{\text{Gesamtkosten}}{\text{Preis pro Kunde}} = \frac{3'080}{25} \approx 123.2$$

Um die Kosten von CHF 3'080 zu decken, werden ungefähr 124 Kunden pro Quartal benötigt.

Der Service ist profitabel, doch eine weitere Steigerung der Rentabilität ist möglich, indem mehr Kunden gewonnen oder der Preis pro Kurs erhöht wird.

3.2.8 Tatsächliche Kostenstruktur und Preisstrategie

Damit die Kurskosten nicht abschreckend wirken für Privatpersonen, werden diese pro Kurs à CHF 25.- verkauft.

3.2.9 WhitePaper

Das WhitePaper mit allen Informationen über den Serivce kann hier eingesehen werden.

ID2132_CAT-Service-WhitePaper-MJCS_v1.pdf

3.3 Tests

Das Testkonzept und die Testprotokolle sind komplett in einem eigenen Dokument geführt und kann hier eingesehen werden.

ID2132_StorrerJessica_CAT_Testkonzept_v1.pdf & ID2132_StorrerJessica_PDF_Testkonzept_v1.pdf

ID2132_StorrerJessica_CAT_Testprotokoll.pdf & ID2132_StorrerJessica_CAT_Testprotokoll.pdf

3.3.1 Planung

Die Tests werden je Service von drei verschiedenen Personen getstet. Der FPM-Service wird vom Fachspezialist MJ Cybersecurtiy Services getestet und der CAT-Service von zwei unabhängigen Kollegen.

3.3.2 Testziele und Testobjekte

Folgend ist lediglich eine Zusammenfassung der Testziele, alles genauere kann den Testkonzepten entnommen werden

3.3.3 FPM Testziele

Sicherstellung, dass bestimmte Anforderungen, die welche im Vorgang getestet werden können, aus dem Pflichtenheft getestet wurden.

Bestätigung der Funktionalität des FPM Services

3.3.4 CAT Testziele

Sicherstellung, dass die Plattform bestimmte Anforderungen gemäss Pflichtenheft erfüllt und diese durch gezielte Tests verifiziert werden.

Bestätigung der Funktionalität des CAT-Services in verschiedenen Bereichen wie Benutzerfreundlichkeit, Inhaltsgestaltung, Sicherheit und Datenschutz.

3.3.5 Testobjekte FPM

Empfang von FPMs

Überprüfen, ob FPMs korrekt im Posteingang der Benutzer ankommen.

Testen der Zustellungszeit und -zuverlässigkeit.

Verifizieren der Anzeige und Lesbarkeit der FPMs in verschiedenen E-Mail-Clients.

Interaktion mit FPMs

Testen der Interaktionsmöglichkeiten mit der FPM, z.B. das Klicken auf Links.

Überprüfen der Funktionen, die nach der Interaktion ausgelöst werden, wie Warnmeldungen oder Weiterleitungen.

Überprüfen der Benutzererfahrung beim Interagieren mit verschiedenen Elementen einer FPM.

Konfiguration von FPM-Kampagnen

Prüfen der Benutzeroberfläche zur Erstellung und Verwaltung von FPM-Kampagnen.

Testen der Einstellmöglichkeiten für verschiedene FPM-Parameter wie Versandzeitpunkte, Zielgruppen und Inhalt.

Personalisierung von FPM-Inhalten

Testen der Funktionen zur Personalisierung von FPMs, um sie spezifisch auf den Empfänger abzustimmen.

Überprüfen der Anpassung von FPM-Inhalten basierend auf Benutzerdaten und Verhaltensmustern.

Reporting und Analyse

Testen des Reportings, um die Ergebnisse von FPM-Kampagnen zu analysieren.

Überprüfen der Berichte auf Nützlichkeit, Genauigkeit und umsetzbare Einsichten.

Testen der Exportfunktionen für Berichte und die Integration mit anderen Analysetools.

Benutzerfreundlichkeit und Design

Überprüfen der Benutzerfreundlichkeit der FPM-Plattform.

Testen der Zugänglichkeit und Verständlichkeit des User Interfaces für verschiedene Benutzerrollen.

3.3.6 Testobjekte CAT

Teilnahme und Zugang

Überprüfen, ob Benutzer sich erfolgreich am System anmelden und auf Kursübersichten zugreifen können.

Testen der Zugänglichkeit und Funktion von verschiedenen Trainingsmodulen und Schwierigkeitsgraden.

Sicherstellung des kostenlosen Zugangs zum CAT für Kunden des FPM-Services.

Interaktivität und Benutzerfreundlichkeit

Testen der Übersichtlichkeit und intuitiven Navigation durch den Kursaufbau auf der Plattform.

Überprüfen, ob der Kursaufbau als interessant und abwechslungsreich empfunden wird, um das Engagement und die Teilnahme der Benutzer zu fördern.

Inhaltsspezifische Funktionalitäten

Testen der Themen- und Kursauswahl sowie der Relevanz der Inhalte für spezifische Zielgruppen.

Überprüfung der Erstellung und Bereitstellung von Kursen und Quizzes durch Administratoren.

Sicherheit und Datenschutz

Überprüfen der Sicherheits- und Datenschutzstandards während des Anmeldeprozesses.

Sicherstellung, dass der Anmeldeprozess und die Plattform den Datenschutzbestimmungen und Compliance entsprechen.

Feedback und Personalisierung

Testen der Feedbackprozesse nach Kursabschluss und deren Benutzerfreundlichkeit.

Überprüfung der Kommunikation zur Zeitinvestition und der Anpassung von Kursinhalten auf Basis von Benutzerdaten.

Administration und Kosten

Überprüfung der Übersichtlichkeit des Backends für die Systemadministration.

Kontrolle der Kosten der CAT-Plattform im Vergleich zum Budget.

3.3.7 Testfälle und erwartete Ergebnisse

Die Erstellung der Testfälle im Konzept richtet sich an die erwarteten Ergebnisse der Tests.

3.3.8 Testprotokolle und Berichterstattung

Alle Tests haben wie erwartet funktioniert.

Die Dokumentation aller Ergebnisse können in den oben genannten Dokumenent nachgesehen werden.

4. Phase Durchführung/Abschluss

Folgend wird die Phase Durchführung und Abschluss erläutert.

4.1 Überwachung und Anpassung

Während der Kampagne muss auf dem Admin-Panel von GoPhish manuell die Kampagnen überwacht werden, dies dient dazu, dass die User je nach Interaktion persönlich angeschrieben werden und auf CAT Verwiesen werden. Dazu dienen diverse im Konzept vordefinierte Antwortemails.

4.1.1 Auswertung und Reporting FPM

Am Ende der Kampagnen wird mithilfe von GoPhish die Auswertung getätigt, dazu dient das Übersichtliche GUI von GoPhish.

Ausgewertet wird folgendes:

- GesamtZahl Email gesendet
    - Wieviele Emails wurden geöffnet
    - Wieviele haben im Email auf den Link geklickt
    - Wieviele haben Daten in die FakeLoginPage eingegeben
- Gründe warum geklickt wurde
- Wieviele Emails wurden reportet als SPAM
- Wieviele Emails wurden reportet, waren aber unsicher ob SPAM
- Wieviele Emails wurden direkt erkannt und gelöscht
- Fazit

Die Reports wurden pro FPM aufgebaut und können hier eingesehen werden.

ID2132_FPM_Report_Kombiniert.pdf

Erstellung detaillierter Berichte über die Ergebnisse der Phishing-Kampagnen, einschliesslich Klickraten und anderer relevanter Metriken.

4.1.2 Die Durchführung FPM

Folgend wird die Durchführung nach Schritten beschrieben.

- Kundeninformation einholen und Infrastruktur bereitstellen.
- Installation und Konfiguration der GoPhish-Plattform.
- Durchführung einer Testkampagne mit ausgewählten E-Mail-Adressen zur Überprüfung der Konfiguration und Funktionalität.
- Anpassung der Kampagnen basierend auf den Ergebnissen der Tests.
- Rollout der vollständigen Phishing-Kampagnen an alle definierten E-Mail-Adressen.
- Fortlaufende Überwachung und Anpassung der Kampagnen bei Bedarf.
- Erstellung und Verteilung der Abschlussberichte und Newsletter.
- Deinstallation der GoPhish-Plattform und Löschung aller Kundendaten .

4.2 Tatsächliche Kosten und Renditen FPM

4.2.1 Projektkosten

Personalkosten: 160 CHF/Stunde

Geplante Stunden: 240 Stunden

Gesamte Personalkosten: 38.400 CHF

Arbeitsaufwand: 15 Stunden pro Kunde von der Implementierung bis zum Abschluss zu CHF 160 pro Stunde = CHF 2'400

4.2.2 Einnahmen Pro Kunde

Angenommen Musterbeispiel aus 1.4 (Firma mit 70 Emailadressen, 3 FPM)

CHF 3304.-

4.2.3 Berechnung ROI

Nun wird die ROI-Berechnung durchgeführt.

$$\mathrm{ROI} = \left(\frac{\mathrm{Einnahmen} - \mathrm{Kosten}}{\mathrm{Kosten}}\right) \times 100$$

Der ROI beträgt etwa -51.77%. Dies bedeutet, dass die Kosten die Einnahmen pro Kunde derzeit um 51.77% übersteigen. Es entsteht also ein Verlust pro Kunde.

4.2.4 BreakEven

Um den Break-Even-Punkt zu errechnen, bei dem die Einnahmen die Kosten decken, teilen wir die Gesamtkosten pro Quartal durch die Einnahmen pro Kunde:

$$\text{ROI} = \left(\frac{\text{Einnahmen} - \text{Kosten}}{\text{Kosten}}\right) \times 100$$

Um die Ausgaben zu decken, sind mindestens 3 Kunden pro Quartal (genauer gesagt, etwa 2.07 Kunden, aber da man keine Bruchteile von Kunden haben kann, runden wir auf die nächste ganze Zahl auf) benötigt. Hier wurde wieder das Musterbeispiel aus 1.4 genommen.

4.2.5 Schlussfolgerung

Der negative ROI deutet darauf hin, dass entweder die Kosten pro Kunde gesenkt oder die Preise erhöht werden müssen, um profitabel zu sein. Zusätzlich könnten die Einnahmen pro Kunde durch den Verkauf zusätzlicher Dienstleistungen oder durch eine effizientere Skalierung der Dienstleistungen (z.B. Verringerung des Zeitaufwands pro Kunde) gesteigert werden.

4.2.6 Massnahmen

Der niedrige ROI deutet darauf hin, dass die Aquise der Kunden gemacht werden muss, sowie der CAT-Service gepusht werden muss.

4.3 Tatsächliche Kosten und Renditen CAT

Plattform- und Hostingkosten: CHF 680 pro Quartal.

Kurserstellung und -betrieb: CHF 2'400 pro Quartal (bei CHF 160 pro Stunde – ausgehend von 15h Pro Quartal) .

Zusätzliche Kosten für die Infrastruktur und Verwaltung der Phishing-Kampagnen: CHF 3'200 (für Onboarding und Implementation) .

4.3.1 Einnahmen

Einnahmen aus Kurslizenzen: CHF 3'750 pro Quartal (basierend auf 150 Kunden zu je CHF 25 pro Lizenz).

4.3.2 ROI-Berechnung

Einnahmen pro Quartal: CHF 3'750.

Gesamtkosten pro Quartal: CHF 3'080.

ROI: Etwa 21.75% .

4.3.3 Diskrepanz und Begründung

Die ursprüngliche Budgetplanung basierte auf optimistischen Schätzungen der Kundenanzahl und Einnahmen.

Tatsächliche Kosten fielen höher aus als geplant, insbesondere durch unvorhergesehene Aufwände in der Kurserstellung und Infrastrukturverwaltung.

Anpassungen im Preis pro Kurs und effiziente Marketingstrategien könnten helfen, die Diskrepanz zu verringern und die Rentabilität zu erhöhen .

4.4 Abschliessende wirtschaftliche Betrachtung der Arbeit

Folgende sind abschliessenden Worte über die wirtschaftliche Betrachtung

4.4.1 Abschliessende wirtschaftliche Betrachtung:

Der FPM-Service zeigt einen positiven ROI, jedoch sind Optimierungen erforderlich, um die Rentabilität weiter zu steigern.

Durch die regelmässige Aktualisierung der Phishing-Kampagnen und Schulungsinhalte kann eine kontinuierliche Verbesserung der Sicherheitsbewusstseins der Mitarbeiter erzielt werden.

Langfristig ist eine Steigerung der Kundenanzahl und eine mögliche Preisanpassung notwendig, um die Investitionen vollständig zu amortisieren und nachhaltige Gewinne zu erzielen

4.4.2 Unterschiede zwischen Konzept & Realisierung, Gedanken

Vergleich des Konzepts und der Realisierung des FPM- und CAT-Services

4.4.3 Entscheidende Unterschiede und Änderungen

Folgend werden die entscheidenden Unterschiede von Konzept und Realisierung aufgezeigt, owie einige Gedanken.

4.4.4 Konzept:

FPM-Service:

Ursprünglich wurden verschiedene Preismodelle erwogen, darunter eine Pauschale pro E-Mail-Adresse und Staffelpreise für Adressbundles.

Geplant war die Nutzung von GoPhish für die Phishing-Kampagnen mit detaillierter Konfiguration und personalisierten E-Mail-Templates.

CAT-Service:

Die Kursstruktur sah wöchentliche Module vor, die verschiedene Aspekte der IT-Sicherheit abdecken, wie Phishing, Social Engineering und allgemeine IT-Sicherheitspraktiken am Arbeitsplatz.

Der ROI wurde optimistisch auf Basis einer bestimmten Anzahl von Kunden pro Quartal berechnet, ohne Berücksichtigung der realen Marktbedingungen und tatsächlichen Arbeitsstunden.

4.4.5 Realisierung:

FPM-Service:

Die tatsächlichen Kosten pro Kunde waren höher als erwartet, was zu einem negativen ROI führte. Es wurden etwa 3 Kunden pro Quartal benötigt, um die Kosten zu decken, was höher war als ursprünglich kalkuliert.

Probleme wie die Quarantäne von E-Mails durch Exchange Online und die Nicht-Erreichbarkeit des GoPhish-Servers aus dem Home-Office mussten gelöst werden.

CAT-Service:

Der ROI war in der Realität niedriger als geplant, was auf höhere tatsächliche Kosten und geringere Kundenzahlen zurückzuführen war. Ohne die Berücksichtigung der Arbeitsstunden wäre der ROI jedoch deutlich positiver gewesen.

Die Schulungen wurden kontinuierlich angepasst und verbessert basierend auf Kundenfeedback, was zusätzliche Aufwände verursachte.

4.4.6 Entscheidende Unterschiede und Änderungen Finanzen: ROI und Break Even

Folgende entscheidene Unterschiede gab es in den Finanzen zwischen Konzept & Realisierung.

4.4.7 Konzept:

FPM-Service:

Ursprünglich erwarteter ROI: Positiv, basierend auf einer bestimmten Anzahl von Kunden und niedrigen Betriebskosten.

Break-Even: Kalkuliert auf Basis von angenommenen stabilen Einnahmen und niedrigen Implementierungskosten.

CAT-Service:

Geplanter ROI: Optimistisch berechnet basierend auf der Annahme von 150 Kunden pro Quartal und niedrigen Kurs- und Plattformkosten.

Break-Even: Erwartet bei etwa 31 Kunden pro Jahr ohne Berücksichtigung der Arbeitskosten.

4.4.8 Realisierung:

Kosten und ROI:

Konzept: Optimistische Schätzungen der Kundenanzahl und Einnahmen. Der ROI wurde basierend auf einer bestimmten Anzahl von Kunden pro Quartal berechnet.

Realisierung: Höhere tatsächliche Kosten durch unvorhergesehene Aufwände in der Kurserstellung und Infrastrukturverwaltung. Der tatsächliche ROI war niedriger als geplant, insbesondere bei Berücksichtigung der Arbeitsstunden.

4.5 Technische Herausforderungen:

Konzept: Geplant war die problemlose Nutzung von GoPhish und die einfache Integration in die bestehende IT-Infrastruktur.

Realisierung: Probleme wie die Quarantäne von E-Mails durch Exchange Online und die Nicht-Erreichbarkeit des GoPhish-Servers aus dem Home-Office mussten gelöst werden.

4.5.1 Finanzen: ROI und Break-Even

FPM-Service:

Tatsächlicher ROI: Etwa -51.77%, was einen Verlust bedeutet bei einem Kunden mit als Beispiel 70 Emailadressen und 3 FPM. Der Break-Even wird bei mindestens 3 Kunden pro Quartal erreicht.

4.5.2 Massnahmen zur Verbesserung

Senkung der Kosten pro Kunde und Erhöhung der Preise oder Anzahl der Kunden, um die Rentabilität zu steigern.

CAT-Service:

Tatsächlicher ROI: Deutlich niedriger als erwartet, -87.51% mit Berücksichtigung der Arbeitsstunden. Ohne diese Kosten wäre der ROI etwa 53.19% gewesen.

Break-Even: Erwartet bei etwa 124 Kunden pro QuartalArbeitskosten.

4.5.3 Ergebnisse der FPM-Kampagnen

Die Ergebnisse der letzten FPM-Kampagne zeigten, dass die meisten Mitarbeiter Phishing-Mails gut erkennen und entsprechend reagieren konnten. Die Berichte und Statistiken zeigten, dass viele Mitarbeiter entweder die Mails als Spam markierten oder an die IT-Abteilung weiterleiteten, was die Effektivität der Schulungen und Phishing-Simulationen unterstreicht .

Eine Besonderheit war der QR-Code-Phishing-Test, bei dem einige Mitarbeiter dennoch auf den QR-Code klickten, was auf einen Bereich hinweist, der weiter verbessert werden muss .

4.5.4 Zusammenfassung

Insgesamt zeigt der Vergleich zwischen Konzept und Realisierung, dass trotz sorgfältiger Planung einige unerwartete Herausforderungen und höhere Kosten aufgetreten sind. Die Anpassungen während der Realisierung, wie die Lösung von technischen Problemen und die kontinuierliche Verbesserung der Schulungsinhalte, waren entscheidend für den Erfolg des Projekts. Die wirtschaftliche Betrachtung und der ROI zeigen, dass die Projekte zwar potenziell profitabel sind, jedoch eine Anpassung der Preisstrategie und Effizienzsteigerungen erforderlich sind, um die Rentabilität langfristig sicherzustellen.

5. Schlussbetrachtung

Im folgenden Kapitel wird die Schlussbetrachtung über das gesamte Projekt gezogen.

5.1 Schlusskommentar zum Ergebnis der gesamten Arbeit

Meines Erachtens kann ich wohl Stolz sein, eine Firma plus zwei laufende Services mit allem drum und dran, wie Kosten, Marketing, Durchführung gemacht zu haben.

Nach vielen Überlegungen, auch in der Freizeit, wurde dies zu einem Herzensprojekt und zeigte mir, dass ich doch grosses Interesse in der Psyche des Menschen habe und im Designen diverser Sachen.

5.2 Persönlichen Beitrag der Lösung

Da ich unabhängig von allen arbeiten konnten, ist die gesamte Lösung ein persönlicher Beitrag. Dank der Implementation von einem OpenSource Tool und der Teachable Plattform, konnte ich dank der in den Tools vorhandenen Features mein persönlicher Touch und Design einfliessen lassen.

5.3 Wie geht es weiter mit dem Projekt

Das Projekt wird weitergeführt und die CAT Kurse noch feiner definiert für die Privatkunden. Der Service FPM werde ich ebenso anpreisen und versuchen die beiden Services wie bei Marketing beschrieben weiter anpreisen. Aber mehr als Sackgeld (;

Zusätzlich werde ich noch ein Träumli von mir erfüllen, und ein Kinderbuch mit Illustrationen über Cybersecurtiy erstellen und anbieten. (:

5.4 Persönliche Betrachtung

Ich weis gar nicht wo ich hier anfangen soll. Es war viel, ich habe viel „mimimi“ gemacht – aber wie ich jedem welchen ich „vollgegrännt“ habe gesagt habe, ich habe das gern gemacht. Sehr gerne sogar. Der Termindruck und die vielen Formellen Sachen welche man einhalten sollte fand ich hingegen nicht so toll, weil ich halt gerne einfach arbeiten wollte.

Da mir aber Design, Schreiben und gestaltet eher leicht fällt, machte ich das wirklich gerne. Bin aber auch sehr sehr sehr sehr froh, wenn ich abgegeben habe, die Präsentation vorbei ist

und bewertet wurde. Man grübelt dann doch immer wieder ob man alles so erwähnt hat, sodass das gegenüber es auch so versteht.

Eigentlich war dass das, wo ich schon immer machen wollte aber dachte „Ach für was, es wird ja eh nichts laufen". Jetzt ohne diesen Gedanken wars cool, dass ich endlich Zeit für das Aufbringen kann und habe so die Basis geschaffen um vor allem CAT & CAP weiterzubringen.

5.5 Dank

Der Dank gilt B&T AG, welche es mir ermöglich hat diese Diplomarbeit als Pilotkunde zu brauchen. Der Dank hierfür gilt auch für die erhaltenen Stunden, Freiheiten und gute Zusprüche.

Gerne möchte ich noch der „IQ-Lerngruppe" danken, welche die 2.5 Jahre einfach viel besser gemacht haben und echte Kollegen gefunden habe, welche einem mit Rat, Tat und Unterstützung zur Seite steht.

Weiter möchte ich *von herzen* meinem Partner danken, welchen ich „vollliieren" konnte, michbei ihm „ausgrännen" konnte und er mir immer mit Mut und Rat zur Seite stand. Danke.

Auch möchte ich mir selbst Danken, dass ich das so durchgezogen habe und mich in diesen zweieinhalb Jahren extrem weiterentwickeln konnte!

5.6 Ergänzungen

Trotz sorgfältiger Planung traten einige unerwartete Herausforderungen und höhere Kosten auf. Die kontinuierliche Verbesserung der Schulungsinhalte und die Lösung technischer Probleme waren entscheidend für den Erfolg des Projekts. Langfristig sind Anpassungen in der Preisstrategie und Effizienzsteigerungen erforderlich, um die Rentabilität zu gewährleisten.

Die detaillierten Berichte und Statistiken der letzten FPM-Kampagne zeigen, dass die Schulungen effektiv waren und die Mitarbeiter sensibilisiert wurden. Zukünftige Massnahmen sollten sich auf die Verbesserung der Sensibilisierung für weniger offensichtliche Phishing-Angriffe und die kontinuierliche Anpassung der Schulungsinhalte konzentrieren.

6. Authentizität & Urheberrecht

Mit meiner Unterschrift bestätige ich, die vorliegende Diplomarbeit selbstständig, ohne Hilfe Dritter und nur unter Benutzung der angegebenen Quellen ohne Copyright-Verletzung, erstellt zu haben.

Jessica Storrer – ID2132

Gurzelen, 20.05.2024

7. Anhang

Die Anhänge sind nach Phasen gegliedert. Hier kann alles gedownloadet werden:

Downloads Diplomarbeit | MJCS (mjcybersecurity.com)

Für die Gedruckte Version werden mehrere Dokumente zusammengefasst.

Die Mails und Codes sind unter GITHUB abgelegt:

estorj/MJCS: MJCS (github.com)

Phase	Dokument	Dokumentenname
PROJEKTANTRAG	Projektantrag	ID2132_StorrerJessica_Projektantrag_V1.pdf
INITIALISIERUNG	FPM&CAT Initialisierung	ID2132_StorrerJessica_FPM&CAT_Initialisierung_v1.pdf
	FPM&CAT Studie	ID2132_StorrerJessica_FPM&CAT_Studie_v1.pdf
	FPM&CAT Projektauftrag	ID2132_StorrerJessica_FPM&CAT_Projektauftrag_v1.pdf
KONZEPT	CAT Konzept	ID2132_StorrerJessica_CAT_Konzept_v1.pdf
	CAT Testkonzept	ID2132_StorrerJessica_CAT_Testkonzept_v1.pdf
	FPM Checkliste installation	ID2132_StorrerJessica_FPM_ChecklisteInstallation_v1.pdf
	FPM Mini DSG	ID2132_StorrerJessica_FPM_Datenschutzkonzept_fuer_interne_Phishing_Tests_v1.pdf
	FPM Konzept	ID2132_StorrerJessica_FPM_Konzept_v1.pdf
	FPM Testkonzept	ID2132_StorrerJessica_FPM_Testkonzept_v1.pdf
	FPM Kundeninfoblatt/ Onboarding	ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v01.pdf
REALISIERUNG & DURCHFÜHRUNG	CAT Realisierung	ID2132_StorrerJessica_RealisierungCAT_v1.pdf
	FPM Realisierung	ID2132_StorrerJessica_RealisierungFPM_v1.pdf
	CAT Testprotokoll	ID2132_StorrerJessica_CAT_Testprotokoll_v1.pdf
	FPM Testprotokoll	ID2132_StorrerJessica_FPM_Testprotokoll_v1.pdf
	WhitePaper/Fact Sheet CAT	CAT-Service-WhitePaper-MJCS_v01.pdf
	WhitePaper/Fact Sheet FPM	FPM-Service-Whitepaper-MJCS_v01.pdf
	Kundeninfoblatt	ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v01.pdf
ABSCHLUSS	Report FPM Kombiniert	FPM_Report_Kombiniert.pdf
	FPM&CAT Abschluss	ID2132_FPM&CAT_Abschluss_StorrerJessica_v1.pdf
DIPLOMBERICHT	FPM & CAT Diplombericht	ID2132_StorrerJessica_Diplombericht_v1.pdf
ZUSATZ	Projektplan	ID2132_StorrerJessica_Projektplan_v01.xlsx

	Arbeitsjournal	ID2132_StorrerJessica_Arbeitsjournal.pdf

Tabelle 8 - Alle Dokumente und Anhänge

Abkürzungsverzeichnis

Abkürzung	Bedeutung	Weitere Informationen
MJCS	MJ Cybersecurity Services	mjcybersecurity.com mjcybersecurity.teachable.com
FPM	Fake Phishing Mail	
CAT	Cybersecurity Awareness Training	
FLP	Fake Login Page	