fake phishing mail service
&
cybersecurity awareness training

FPM & CAT

-STUDIE-

Auftraggeber	Marc Aeby
Projektleiter	J. Storrer
Autor	J. Storrer
Dokument	ID2132_StorrerJessica_FPM&CAT_Studie_v1.docx
Klassifizierung	Intern
Status	Genehmigt

Änderungsverzeichnis

Datum	Version	Änderung	Autor
20.02.2024	0.1	Erster Draft	J. Storrer
21.02.2024	0.2	Pflichtenheft und Anforderungskata-loge	J. Storrer
25.02.2024	0.3	Lösungsvarianten	J. Storrer
06.03.2024	1.0	Final Dokument	J. Storrer

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Informationsbeschaffung

In diesem Teil der Studie wird die Informationsgewinnung der Services zusammengefasst. Die diversen Handnotizen werden als Anhang beigelegt.

1.1 The Business Model Canvas

Um eine bessere Übersicht und als MindMap wurden für die zwei Services ein Business Model Canvas erstellt, welche untenstehend eingesehen werden können. Vor allem ob es überhaupt Sinn machen wird und der Service in dieser Form wie es vorgestellt wurde auch machbar wäre.

1.1.1 FPM Business Model Canvas

Folgend das Business Model Canvas für den FPM-Service.

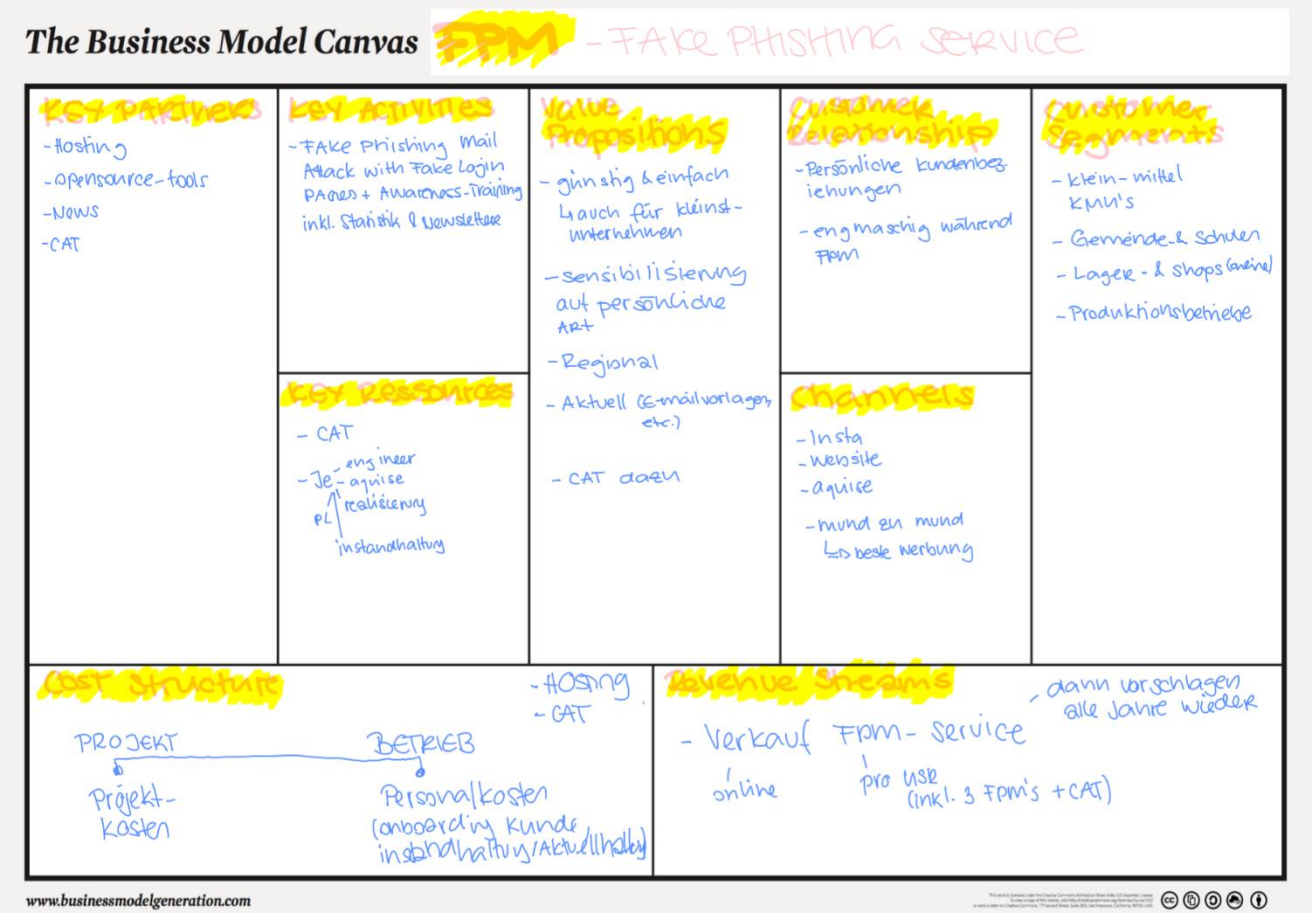

Abbildung 1 - The Business Model Canvas FPM

1.1.2 CAT Business Model Canvas

Nachstehend das Business Model Canvas für den CAT-Service

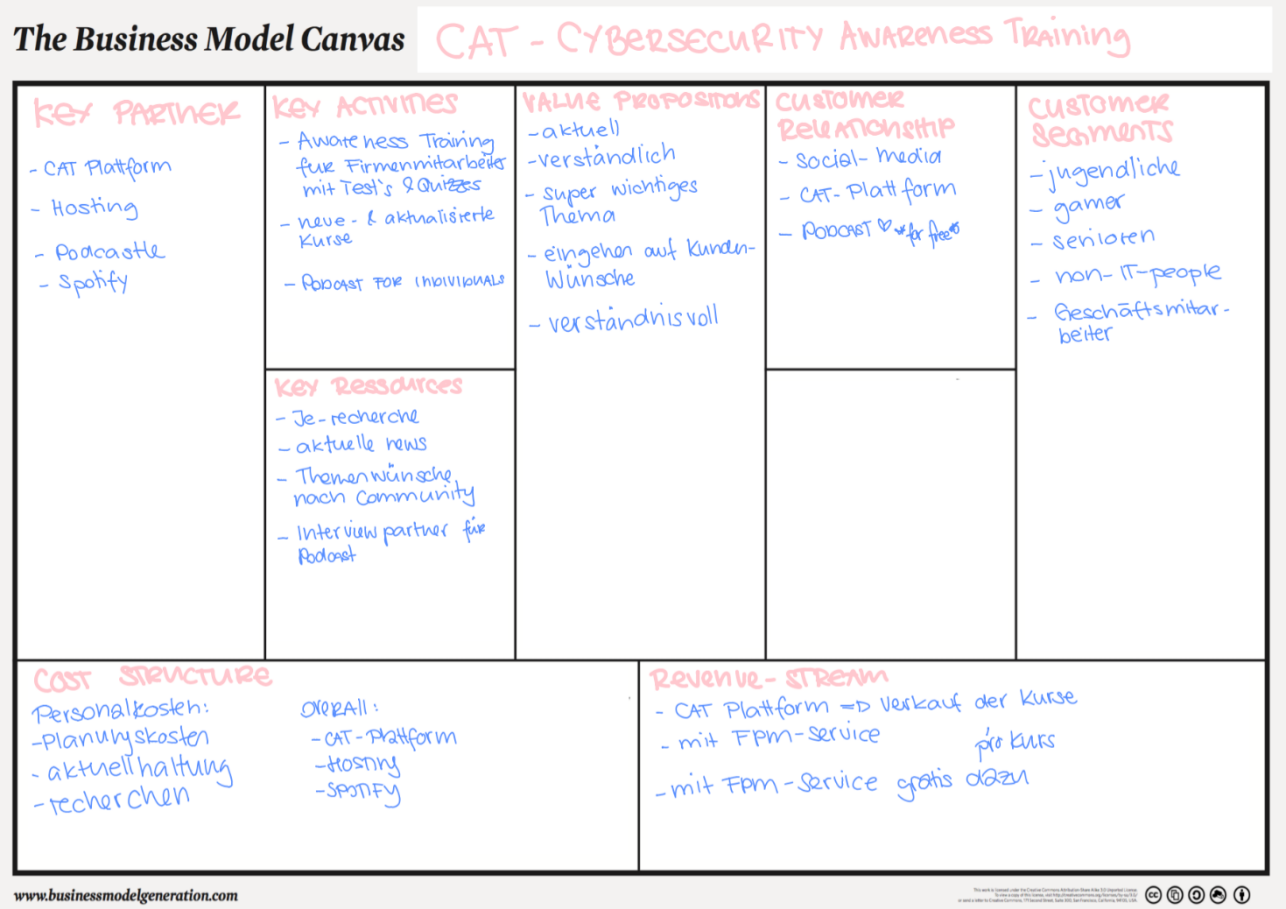

Abbildung 2 - The Business Model Canvas CAT

2. Pflichtenheft und Anforderungskataloge

Aus der dargelegten Ausgangslage und den definierten Zielen für das Projekt zur Erhöhung der Cybersecurity Awareness durch den Einsatz von Fake-Phishing-Mails (FPM) und einem Cybersecurity-Awareness-Training (CAT), ergibt sich folgender Katalog an funktionalen und nicht funktionalen Anforderungen. Dieser Katalog ist in drei Kategorien unterteilt: Anforderungen aus Benutzersicht, Systemadministration und Prozesse. Die einzelnen Anforderungen werden nach der Tabelle genauer beschrieben.

Diese Tabelle wird für Gewichtung, Evaluation und Entscheid der FPM- und CAT-Plattform als Grundlage dienen.

2.1 Pflichtenheft und Anforderungen FPM

Aus der dargelegten Ausgangslage und den definierten Zielen für das Projekt zur Erhöhung der Cybersecurity Awareness durch FPM (Fake Pshishing Mail), ergibt sich folgender Katalog an funktionalen und nicht funktionalen Anforderungen.

Dieser Katalog ist in drei Kategorien unterteilt:

Anforderungen aus Benutzersicht, an die Systemadministration und an Prozesse.

ID	Hauptkriterium	Subkriterium / Beschreibung	Funktional/nicht funktional	Art Muss/Kann	Beschreibung Abnahmekriterium	Anforderungen Benutzersicht/ Systemadministration/Prozesse	Testcase Nr.
FPM_A01	Empfang FPM	Empfang von FPMs	Funktional	Muss	Das FPM ist erfolgreich beim Postfach angekommen	*Benutzersicht*	*FPM_T01*
FPM_A02	Interaktion FPM	*Die Benutzer können mit dem FPM interagieren, Link öffnen*	Funktional	Muss	Der User kann der Fake Link im FPM öffnen	*Benutzersicht*	*FPM_T02*
FPM_A03	Interaktion FLP	Interaktion mit FLP, Credential-phishing	Funktional	Kann	Der User kann Credentials eingeben	*Benutzersicht*	*FPM_T03*
FPM_A04	Weiterleitung CAT	Teilnahme am CAT möglich nach erstem FPM (Direktes Weiterleiten, Link..)	Nicht Funktional	Muss	Der User wird nach öffnen des Links und Eingabe der Credentials, weitergeleitet auf CAT	*Benutzersicht*	*FPM_T04*
FPM_A05	Report nach Ende mit Auflösung	*Ein Report/Auflösung wird nach Beendung von FPM generiert*	x	Muss	Der User erhält der Report/Auflösung mit Newsletter	*Benutzersicht*	*FPM_T05*
FPM_A06	Konfiguration FPM	Die FPM können detailgetreu konfiguriert werden	Funktional	Muss	Die FPM wurden so echt wie möglich gestaltet	*Systemadministration*	*FPM_T06*

FPM_A07	FPM-Kampagnen	Es können mehrere Kampagnen gefahren werden damit verschiedene Schwierigkeitslevel (Erkennbarkeit FPM) designt werden können	Funktional	Kann	FPM-Levels Easy, Medium, Hard (Erkennbar ob FPM) ist realistisch umgesetzt	*Systemadministration*	*FPM_T07*
FPM_A08	Usermailgruppen für Kampagnen	Usermails können importiert und in Gruppen aufgeteilt werden	Funktional	Kann	Die Usermails der Kundenfirma können als ganzes importiert werden	*Systemadministration*	*FPM_T08*
FPM_A09	Versand FPM	Das FPM kann an diverse Usermailgruppen gesendet werden	Funktional	Muss	Damit es nicht zu offensichtlich ist, werden die FPM nicht allen gleichzeitig gesendet	*Systemadministration*	*FPM_T09*
FPM_A10	Exportmöglichkeit FPM	Die div. FPM und deren Konfiguration und Einstellungen können exportiert werden	Funktional	Muss	Die Konfigurationen der Kampagnen können exportiert werden, um diese als Vorlage für weitere Kunden zu verwenden	*Systemadministration*	*FPM_T10*
FPM_A11	FPM Tool	Einfach aufbaubares Tool, übersichtlich	Nicht funktional	Muss	Das Tool ist selbsterklärend aufgebaut	*Systemadministration*	*FPM_T11*
FPM_A12	FPM Tool	One-Klick Installation	Funktional	Kann	Die Installation kann mittels «weiter-weiter-ok» installiert werden, sodass bei jedem Kunden immer eine neue Installation erfolgen kann (auch Sicherheitstechnisch)	*Systemadministration*	*FPM_T12*

FPM_A13	Erstellung FLP	Erstellung und Verwaltung von Fake-Login-Seiten und deren Export (Designexport)	Funktional	Muss	FPLs können erstellt und detailgetreu nachgebaut werden	*Systemadministration*	*FPM_T13*
FPM_A14	Export FLP	Konfigurations-Export (Design) möglich	Funktional	Kann	Die Konfiguration (Design) kann für weitere Verwendung exportiert werden	*Systemadministration*	*FPM_T14*
FPM_A15	Klickratenüberwachung FPM	Klicks auf Links im FPM werden getrackt	Funktional	Muss	Die Klickraten werden für Analysezwecken aufbereitet	*Systemadministration*	*FPM_T15*
FPM_A16	Sicherheit und Datenschutz	Die Klickraten werden anonymisiert behandelt	Nicht funktional	Muss	Die Klickraten werden anonym behandelt	*Systemadministration*	*FPM_T16*
FPM_A17	Sicherheit und Datenschutz	Pro Kunde neu Installation	Nicht funktional	Kann	Um 0 Daten versehentlich von anderen Kunden mitgenommen werden, per USB geschehen	*Systemadministration*	*FPM_T17*
FPM_A18	Konfiguration SMTP	Die konfiguration wie SMTP usw muss einfach erfolgen können und am besten vom SMTP des Kunden, damit keine FPMs geblockt werden	Funktional	Muss	Die konfiguration wie SMTP usw muss einfach erfolgen können und am besten vom SMTP des Kunden, damit keine FPMs geblockt werden	*Systemadministration*	*FPM_T18*
	Kosten Plattform	Keine Kosten dank opensource	Nicht Funktional	Kann	Die Plattform darf keine Anschaffungs- oder Lizenzkosten beinhalten		
FPM_A19	Prozessdefinition interne FPM	Prozess wird mit Kunde (Zeitabspänne) definiert und festgelet	Nicht funktional	Muss	Prozess vom Kunden abgenommen	Prozesse	*FPM_T19*

FPM_A20	Reporting und Kommunikation Firmenintern	Kommunikation mit Ergebnissen	Nicht funktional	Muss	Der Prozess für die End-Kommunikation ist bestimmt	Prozesse	*FPM_T20*
FPM_A21	Reporting FPM	Reporting FPM an IT	Nicht funktional	Kann	Voraussetzung; Prozess ist klar für User – wurde Firmenintern schon definiert	Prozesse	*FPM_T21*
FPM_A22	Datenschutz und Compliance	Muss in DSG-Konzept von Firma leicht aufgenommen werden können	Funktional	Kann	Mittels DSG-Sheets und Checklisten kann die SW einfach im DSG und ITSM der Firma abgebildet werden	Prozesse	*FPM_T22*

Tabelle 1 - Anforderungskatalog FPM

2.2 Pflichtenheft & Anforderungen CAT

Aus der dargelegten Ausgangslage und den definierten Zielen für das Projekt zur Erhöhung der Cybersecurity Awareness durch CAT (Cybersecurity-Awareness-Training), ergibt sich folgender Katalog an funktionalen und nicht funktionalen Anforderungen.

Dieser Katalog ist in drei Kategorien unterteilt:

Anforderungen aus Benutzersicht, an die Systemadministration und an Prozesse.

ID	Hauptkriterium	Subkriterium/Beschreibung	Funktional/nicht funktional	Art Muss/Kann	Beschreibung Abnahmekriterium	Anforderungen Benutzersicht/ Systemadministration/Prozesse	Testcase Nr.
CAT_A01	Teilnahme CAT	Die Benutzer können am CAT Teilnehmen	Funktional	Muss	Der Benutzer kann am CAT Teilnehmen	*Benutzersicht*	*CAT_T01*
CAT_A02	Themenauswahl CAT	Auf der CAT Plattform können zwischen diversen Themengebieten ausgewählt werden	Funktional	Muss	Der Benutzer kann ein CAT-Thema auswählen	*Benutzersicht*	*CAT_T02*
CAT_A03	Themenauswahl CAT	Trainings sind auf Zielgruppe Mitarbeiter abgesehen	Nicht funktional	Muss	Die Trainings sind aktuell und für Zielgruppe Mitarbeiter Büro ausgerichtet	*Benutzersicht*	*CAT_T03*
CAT_A04	Div. Schwierigkeitslevel CAT	Die Trainings werden nach Schwierigkeitslevel angelegt	Nicht funktional	Kann	Die Trainings können von den Mitarbeiten von einfach bis Schwierig absolvieren	*Benutzersicht*	*CAT_T04*
CAT_A05	Kursaufbau CAT	Der Kursaufbau auf der Plattform muss übersichtlich sein	Funktional	Muss	Der Benutzer weis wo er welche Informationen/Kurse absolvieren kann	*Benutzersicht*	*CAT_T05*
CAT_A06	Ablauf CATs	Interessanter Aufbau, nicht e-Training like all	Funktional	Kann	Die Trainings wurden so aufgebaut, dass es nicht langweilig wird	*Benutzersicht*	*CAT_T06*

CAT_A07	Quizzes CAT	Quizzes für Check Lernprozess können besucht werden	Nicht funktional	Muss	Die Benutzer können Ihren Lernprozess anhand der Quizzes testen	*Benutzersicht*	*CAT_T07*
CAT_A08	CAT4Individuals	Kleiner Exkurs mit Tipps und Tricks für den Alltag als Privatperson	Nicht funktional	Kann	Tipps und Tricks für den Alltag für Privatgebrauch können angesehen werden	*Benutzersicht*	*CAT_T08*
CAT_A09	CAT4Individuals	Social Media Awareness wird für den Alltag angeboten (Einstieg Social Engineering)	Nicht funktional	Muss	Die Benutzer können einen Exkurs über Social Engineering und Social Media machen	*Benutzersicht*	*CAT_T09*
CAT_A10	Kosten CAT	Die Kunden welche den FPM-Service erworben haben, erhalten den CAT gratis. Individuals müssen für die Kurse bezahlen	Nicht funktional	Muss	Die Kunden welche den FPM Service erworben haben, erhalten den CAT gratis. Individuals müssen für die Kurse bezahlen		*CAT_T10*
CAT_A11	Bereitstellung CAT	Diverse Kurse müssen auf der Plattform erstellt werden können	Funktional	Muss	Es können diverse Kurse angelegt werden	*Systemadministration*	*CAT_T11*
CAT_A12	Bereitstellung CAT	Diverse Quizzes müssen auf der Plattform erstellt werden können	Funktional	Muss	Es können diverse Quizzes angelegt werden	*Systemadministration*	*CAT_T12*

CAT_A13	Backend CAT	Das Backend sollte übersichtlich aufgebaut sein	Nicht funktional	*Kann*	Der Aufbau des Backend ist übersichtlich, Zeit kann eingespart werden	*Systemadministration*	*CAT_T13*
CAT_A14	Kosten CAT	Die Kosten der CAT Plattform sollte sich unter CHF 250.- /6Mnt halten	Nicht funktional	Kann	Die Kosten der CAT Plattform belaufen sich innert einem halbenjahr weniger als CHF 250.-	*Systemadministration*	*CAT_T14*
CAT_A15	Rabatte CAT	Die Firmenuser müssen via Rabattcode gratis auf CAT zugreifen können	Nicht Funkational	Muss	Die Firmen welche den FPM Service gelöst haben, erhalten Gratis CAT Zugriff	*Systemadministration*	*CAT_T15*
CAT_A16	Sicherheit und Datenschutz CAT	Die Anmeldung ist der Plattform überlassen, dies wurde dem Kunden mitgeteilt	Nicht funktional	*Muss*	Die Anmeldung ist der Plattform überlassen, dies wurde dem Kunden mitgeteilt	*Systemadministration*	*CAT_T16*
CAT_A17	AI-Unterstützung CAT	Die Kurse und Quizzes können mithilfe von AI aufgebaut werden	Funktional	Kann	Die Kurse wurden unterstützungshalber mit AI Aufgebaut	*Systemadministration*	*CAT_T17*
CAT_A18	Schulungs- und Feedbackprozesse CAT	Es bestehen Feedbackprozesse über den Kursinhalt	Nicht funktional	Muss	Ein Prozess für Quartalsfeedback über die	Prozesse	*CAT_T18*

		(Kundenzufriedenheit)			CATs wurden definiert		
CAT_A19	Datenschutz und Compliance CAT	Die Anmeldung ist der Plattform überlassen, dies wurde dem Kunden mitgeteilt	Nicht funktional	Muss		Prozesse	*CAT_T19*
CAT_A20	Zeitinvestition, Lernepisoden FPM-Kunden	Die Teilnahmezeiten/Dauer per Mitarbeiter werden definiert	Nicht funktional	Kann	Die Mitarbeiter wurden darüber informiert, wieviel Zeit sie in CAT investieren sollen/dürfen	Prozesse	*CAT_T20*

Tabelle 2 - Anfoderungskatalog CAT

2.3 Anforderungen aus Benutzersicht

Empfang und Erkennung von FPMs: Benutzer müssen in der Lage sein, FPMs zu empfangen und je nach Schwierigkeitsgrad (easy, medium, hard) zu identifizieren.

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

Teilnahme am CAT: Benutzer müssen Zugang zum Awareness-Training haben und dieses absolvieren können, inklusive aller notwendigen Materialien und eventuellen Abschlusstests.

Feedback und Reporting: Benutzer sollen in der Lage sein, Feedback zu den Trainingsinhalten zu geben und verdächtige Aktivitäten effektiv zu melden.

2.4 Anforderungen an die Systemadministratoren

Konfiguration und Versand von FPMs: Die Administration muss in der Lage sein, FPM-Kampagnen zu konfigurieren, inklusive Zeitabstände, Schwierigkeitsgrade und Zielgruppen.

Erstellung und Verwaltung von Fake-Login-Seiten: Es muss möglich sein, verschiedene Fake-Login-Seiten zu erstellen und zu verwalten, die je nach FPM-Kampagne eingesetzt werden.

Überwachung und Analyse der Ergebnisse: Die Plattform muss Werkzeuge zur Überwachung und Analyse der Reaktionen der Benutzer auf die FPMs bieten, einschliesslich Klickraten und erfolgreicher Erkennungen.

Bereitstellung und Verwaltung des CAT: Die Systemadministration muss das Awareness-Training verwalten können, inklusive der Erstellung von Inhalten und der Überwachung der Teilnahme.

Sicherheit und Datenschutz: Das System muss höchste Sicherheits- und Datenschutzstandards erfüllen, um die Informationen der Benutzer und die Integrität des Tests zu gewährleisten.

2.5 Anforderungen an Prozesse

Prozessdefinition für interne Phishing-Attacken: Es müssen klare Prozesse für die Durchführung der FPM-Kampagnen, inklusive Zielsetzung, Durchführung und Nachbereitung, definiert sein.

Schulungs- und Feedbackprozesse: Es müssen Prozesse für die Schulung der Benutzer sowie für das Sammeln und Verarbeiten von Feedback existieren.

Reporting und Kommunikation: Es müssen Prozesse für das Reporting der Ergebnisse der Kampagnen sowie für die Kommunikation mit den Benutzern über Erfolge, Erkenntnisse und Verbesserungsmöglichkeiten etabliert werden.

Prozesse für die Aktualisierung und Wartung des Systems: Regelmässige Aktualisierungen und Wartungen des Systems müssen durchgeführt werden, um die Effektivität der Kampagnen und des Trainings zu gewährleisten.

Datenschutz und Compliance: Die Prozesse müssen die Einhaltung aller relevanten Datenschutzrichtlinien und Compliance-Anforderungen sicherstellen.

Zeitinvestition, Prozess Lernepisoden Kunden: Der Prozess für den Mitarbeiteraufwand für CAT muss definiert werden, um so sicherzustellen, dass nicht zu viel Zeit in das Learning verloren geht.

Dieser Katalog dient als Pflichtenheft und bildet die Grundlage für die Entwicklung, Implementierung und den Betrieb des Projekts zur Erhöhung der Cybersecurity Awareness durch den Einsatz von Fake-Phishing-Mails und Cybersecurity-Awareness-Training.

3. Lösungsvarianten FPM

Basierend auf den Anforderungen für das Projekt, das Fake-Phishing-Mails (FPM) und Cybersecurity-Awareness-Training umfasst, sind hier drei Open-Source-Tools, die am besten geeignet sind, um diese Anforderungen zu erfüllen. Diese Tools bieten umfangreiche Funktionen für die Erstellung, Durchführung und Analyse von Phishing-Simulationen und unterstützen die Erhöhung der Sicherheitsbewusstseinsbildung innerhalb einer Organisation.

3.1 Variantenübersicht FPM Plattforme

Drei Varianten wurden nach den Anforderungen des FPM-Services eruiert.

Variante	Bezeichnung
V1_FPM	*GoPhish*
V2_FPM	*KingPhisher*
V3_ FPM	*PhishingFrenzy*

Tabelle 3 - Variantenübersicht FPM

3.2 Variante V1 - GoPhish

Pro Varianten werden folgende Punkte beschrieben.

Kurzbeschreibung

GoPhish ist ein leistungsstarkes Open-Source-Phishing-Framework, das für Unternehmen und Sicherheitsteams entwickelt wurde, um effektive Phishing-Simulationen durchzuführen. Es ermöglicht die einfache Erstellung von Phishing-Kampagnen, Zielgruppenmanagement, sowie das Senden und Nachverfolgen von simulierten Phishing-E-Mails.Systemkontext (Soll)

Abbildung 3 - Logo "GoPhish"

3.2.1 Funktionen

- ✓ Benutzerfreundliches Interface für Kampagnenmanagement.
- ✓ Detaillierte Berichterstattung und Statistiken zur Erfassung der Benutzerinteraktionen.
- ✓ Anpassbare E-Mail-Vorlagen und Landing Pages für verschiedene Schwierigkeitsgrade.
- ✓ Unterstützung für die Erstellung von Fake-Login-Seiten zur Erfassung von Interaktionen.
- ✓ Phishlets für reelle WellKnown Fake Login Pages vorhanden (Templates)

3.2.2 Eignung

GoPhish erfüllt viele der technischen und prozessorientierten Anforderungen für das Projekt, insbesondere im Hinblick auf die Konfiguration und Durchführung von Phishing-Tests sowie die Analyse der Ergebnisse.

3.2.3 Produkt

Folgend wir beschrieben, wie die Implementation beim Kunden aussehen würde. Es wird alles lokal gewählt, sodass die Sicherheitsrisiken eingedämmt werden können, sowie möglichst keine neuen Poren (Porositys) geschafft werden.

Lediglich das Senden der Mails und die Verfolgung der Klickraten muss gegen aussen geöffnet sein. Am schönsten wäre es die Installation in einem separaten Netz mit separatem Port zu haben, um höchste Sicherheit gewährleisten zu können.

3.2.4 Globale Systemarchitektur

Nachfolgend wir die konzeptionelle Systemarchitektur beschrieben.

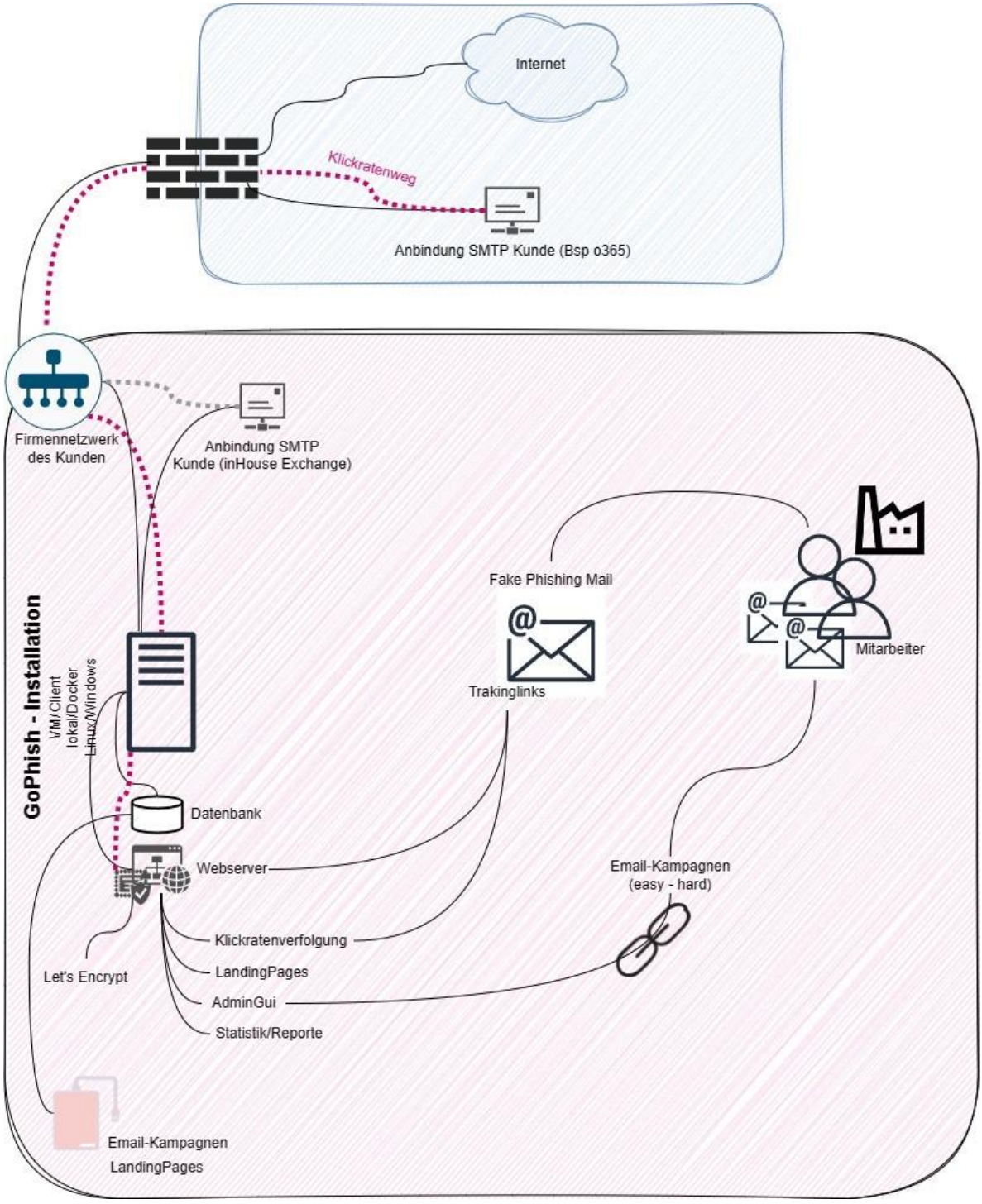

Abbildung 4 - FPM Systemarchitektur Grob "GoPhish"

3.2.5 Integration und Netzwerkplan (Konzeptuell)

Was oben graphisch dargestellt wurde, wird hier noch in Worten zusammengefasst.

Server:

GoPhish wird auf einem dedizierten Server innerhalb des Unternehmensnetzwerks oder in einer Cloud-Umgebung installiert. Dieser Server hostet die GoPhish-Webanwendung und die Datenbank, die die Kampagnendaten und Benutzerinteraktionen speichert.

SMTP-Konfiguration:

GoPhish benötigt Zugriff auf einen SMTP-Server, um Phishing-E-Mails zu versenden. Dies kann ein interner SMTP-Server des Unternehmens sein oder ein externer Dienst, der für diesen Zweck konfiguriert ist.

Landing Pages:

GoPhish ermöglicht die Erstellung von Fake-Landing-Pages, die auf demselben Server wie GoPhish gehostet werden. Wenn ein Benutzer auf einen Link in der Phishing-E-Mail klickt, wird er zu dieser gefälschten Seite weitergeleitet.

Statistik und Reporting:

GoPhish erfasst automatisch die Aktionen der Benutzer, wie das Öffnen von E-Mails und das Klicken auf Links. Diese Daten werden in der GoPhish-Webanwendung für detaillierte Berichte und Analysen verwendet.

Technische Umsetzung bei Klicks auf Fake-Mails:

Wenn ein Benutzer auf den Link in einer Phishing-Mail klickt, registriert GoPhish den Klick über einen Tracking-Link, der mit der Fake-Landing-Page verbunden ist. Die Interaktion wird in der Datenbank gespeichert und kann für die Auswertung der Kampagneneffektivität genutzt werden.

3.2.6 Mehrkundenfähigkeit

Schnelle Installation:

GoPhish bietet Installationsdateien für Windows, Mac und Linux, die eine einfache und schnelle Installation ermöglichen, an. Ein Docker-Container ist ebenfalls verfügbar, was die Bereitstellung auf verschiedenen Systemen erleichtert und standardisiert.

Konfigurationen speichern:

GoPhish unterstützt den Export und Import von Kampagnendaten, was die Wiederverwendung von Konfigurationen bei verschiedenen Kunden vereinfacht. Überlegen Sie, eine Bibliothek von E-Mail-Templates und Landing Pages anzulegen, die Sie für verschiedene Szenarien anpassen können.

Aufbauempfehlung:

Docker für die Bereitstellung, um eine konsistente Umgebung über verschiedene Kunden hinweg zu gewährleisten. Zentrale Bibliothek mit Templates und Landing Pages, die leicht angepasst werden können, um Zeit zu sparen und die Konsistenz zu wahren. Dokumentieren erfolgreicher Kampagnenkonfigurationen für eine schnelle Wiederholung bei neuen Kunden.

3.2.7 Zu Beachten

Im folgenden Kapitel werden die Knackpunkte der Anforderungen auf das Tool beleuchtet.

3.2.7.1 Klickratenlinkverfolgung

SMTP-Konfiguration:

Stellen Sie sicher, dass die SMTP-Konfiguration in Gophish korrekt ist. Dies umfasst die korrekte Angabe des SMTP-Servers, des Ports und der Authentifizierungsinformationen.

Firewall-Einstellungen:

Überprüfen Sie die Firewall-Einstellungen, um sicherzustellen, dass Gophish die erforderlichen Netzwerkverbindungen herstellen kann. Gophish muss möglicherweise ausgehende Verbindungen zum SMTP-Server sowie eingehende Verbindungen für die Web-Oberfläche zulassen.

E-Mail-Header und Tracking:

Gophish fügt Tracking-Informationen zu den versendeten Phishing-E-Mails hinzu, um Klicks zu erfassen. Stellen Sie sicher, dass diese Tracking-Informationen nicht durch Sicherheitsvorkehrungen (wie Spam-Filter) blockiert werden und dass die Empfänger die Bilder in den E-Mails laden können.

DNS-Auflösung:

Die DNS-Auflösung wird auf dem Server, auf dem Gophish ausgeführt wird, korrekt konfiguriert. Dies ist wichtig für die ordnungsgemässe Verarbeitung von Links in den Phishing-E-Mails.

SSL-Zertifikat:

Für «echte» Fake Login Pages wird ein Zertifikat von Let’s encrypt benötigt.

3.2.7.2 SMTP-Mailversand

In GoPhish können Absender (From-Adresse) für die Phishing-E-Mails konfiguriert werden. Das bedeutet, dass beliebige Absender angeben werden können, welche in den gefälschten E-Mails erscheinen. Diese Adresse kann so angepasst werden, dass sie den Anschein erweckt, von einer vertrauenswürdigen Quelle oder einer internen Abteilung zu stammen. Es ist wichtig zu beachten, dass dies Teil der Simulationsübung ist und darauf abzielt, wie gut die Mitarbeiter auf potenziell gefälschte E-Mails reagieren.

3.2.7.3 HTTPS für GoPhish FLP

HTTPS und Zertifikate:

Für eine realistische Phishing-Website ist es möglich, ein HTTPS-Zertifikat zu verwenden, um die Website als sicher erscheinen zu lassen. Ein SSL/TLS-Zertifikat ist jedoch erforderlich, um eine sichere Verbindung herzustellen und das "https://" in der URL anzuzeigen.

Selbstsignierte Zertifikate:

In einigen Fällen können Phishing-Akteure selbstsignierte Zertifikate verwenden, um den Eindruck einer sicheren Verbindung zu erwecken. Beachten Sie jedoch, dass moderne Browser oft Warnungen anzeigen, wenn sie auf eine Website mit einem selbstsignierten Zertifikat zugreifen.

Gültige Zertifikate:

Um einen noch realistischeren Eindruck zu erwecken und Warnungen zu vermeiden, könnten Angreifer ein gültiges Zertifikat verwenden. Diese könnten von Zertifizierungsstellen (CAs) ausgestellt werden. Beachten Sie, dass es illegal und eine schwerwiegende Verletzung der Sicherheit ist, echte Zertifikate ohne Zustimmung des Eigentümers zu verwenden.

Gophish und HTTPS:

Gophish unterstützt die Verwendung von HTTPS für die Web-Oberfläche, um eine sichere Verbindung zwischen dem Benutzer und dem Gophish-Server herzustellen. Dies hat jedoch nichts mit den erstellten Phishing-Seiten zu tun. Sie müssen das SSL/TLS-Zertifikat direkt auf der Phishing-Website konfigurieren

3.2.8 Informationssicherheit und Datenschutz

Gophish zeichnet in der Standardeinstellung tatsächlich keine Benutzeranmeldeinformationen (Credentials) auf, sondern erfasst nur, dass ein Klick auf den Phishing-Link erfolgt ist. Dies geschieht aus Gründen der Privatsphäre und Sicherheit, um den unbefugten Zugriff auf tatsächliche Anmeldeinformationen zu verhindern.

3.2.9 Voraussetzungen, Abhängigkeiten, Abgrenzungen

Voraussetzung ist eine Netzwerkinfrastruktur des Kunden, bei welchem ein Server (am liebsten Virtuell) bereitgestellt werden kann. Firewallregeln müssen durch dir Firma erstellt und gewartet werden können. Eine SMTP-Senderemail ist vorhanden. Useremailgruppen werden bereitgestellt. Die DNS-Einstellungen der Domains und Webservices werden von der Firma verwaltet und nach Absprache hinzugefügt.

3.3 Variante V2 - KingPhisher

Pro Varianten werden folgende Punkte beschrieben

3.3.1 Kurzbeschreibung

King Phisher ist ein weiteres umfassendes Tool für Phishing-Kampagnen, das es ermöglicht, fortschrittliche Phishing-Angriffe zu simulieren, um das Bewusstsein für Cybersecurity zu schärfen.

Abbildung 5 - Logo "KingPhisher"

3.3.2 Funktionen

- ✓ Unterstützt sowohl E-Mail-Phishing-Kampagnen als auch SMS-Phishing.
- ✓ Visuelle Kampagnen-Design-Tools und Template-Editor.
- ✓ Detaillierte Kampagnenstatistiken für eine gründliche Analyse.
- ✓ Integration mit externen Tools für erweiterte Flexibilität.

3.3.3 Eignung

King Phisher eignet sich besonders gut für Unternehmen, die eine flexible und erweiterbare Lösung für Phishing-Tests suchen, die über reine E-Mail-Kampagnen hinausgeht.

3.3.4 **Produkt**

Folgend wir beschrieben, wie die Implementation beim Kunden aussehen würde.

Es wird alles lokal gewählt, sodass die Sicherheitsrisiken eingedämmt werden können, sowie möglichst keine neuen Poren (Porositys) geschafft werden.

Lediglich das Senden der Mails und die Verfolgung der Klickraten muss gegen aussen geöffnet sein.

Am schönsten wäre es die Installation in einem separaten Netz mit separatem Port zu haben, um höchste Sicherheit gewährleisten zu können.

3.3.5 Gobale Systemarchitektur

Nachfolgend wir die konzeptionelle Systemarchitektur beschrieben.

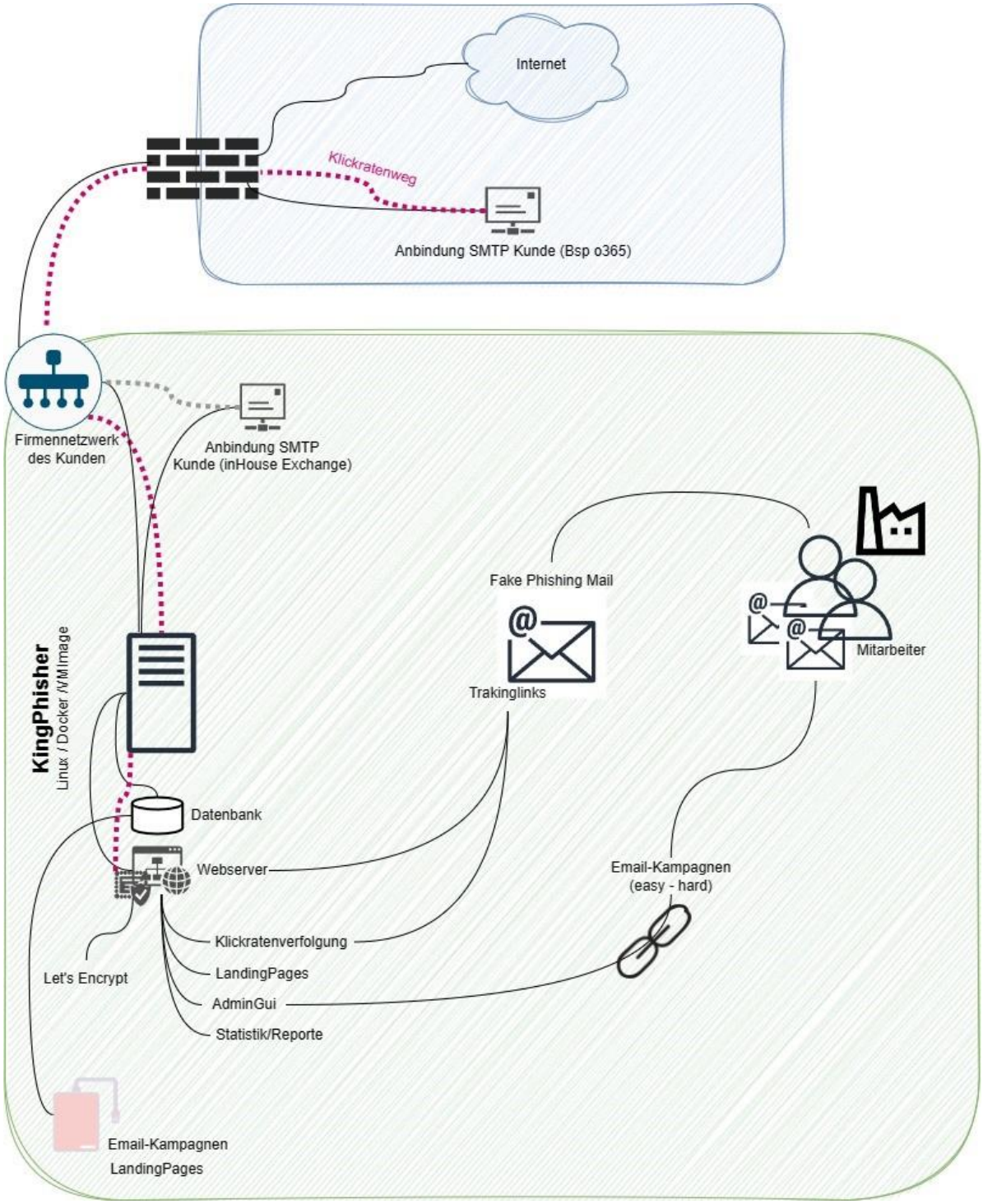

Abbildung 6 - Globale Systemarchitektur "KingPhisher"

3.3.6 Integration und Netzwerkplan (Konzeptuell)

Server:

King Phisher wird auf einem Server installiert, der entweder im Unternehmensnetzwerk oder in einer geeigneten Cloud-Umgebung platziert ist. Dieser Server dient als zentrale Plattform für das Versenden von Phishing-E-Mails und das Hosting von Landing Pages.

SMTP-Server:

Ähnlich wie GoPhish benötigt King Phisher Zugang zu einem SMTP-Server, um die Phishing-E-Mails zu versenden.

Landing Pages:

Benutzerdefinierte Landing Pages werden auf dem King Phisher Server gehostet. Diese Seiten können speziell gestaltet werden, um die Ziele der Phishing-Kampagne zu unterstützen.

Statistik und Reporting:

King Phisher verfügt über detaillierte Tracking-Funktionen, um das Benutzerverhalten wie das Öffnen von E-Mails und das Klicken auf Links zu verfolgen.

Technische Umsetzung bei Klicks auf Fake-Mails:

King Phisher verwendet speziell gestaltete URLs in den Phishing-E-Mails, um Benutzerinteraktionen zu verfolgen. Wenn ein Empfänger auf einen Link klickt, wird dieser Klick vom King Phisher Server registriert, und der Benutzer wird zur vordefinierten Landing Page weitergeleitet.

3.3.7 Mehrkundenfähigkeit

Schnelle Installation:

King Phisher erfordert etwas mehr Konfigurationsaufwand als GoPhish, unterstützt aber Skripte für eine automatisierte Installation auf Linux-Systemen. Eine Virtual Machine Image oder Docker-Option ist für eine schnelle Einrichtung ideal.

Konfigurationen speichern:

Ähnlich wie GoPhish können Sie bei King Phisher Kampagneneinstellungen und Templates für den wiederholten Gebrauch speichern. Nutzen Sie die Möglichkeit, Kampagnenvorlagen zu exportieren, um sie bei anderen Kundenprojekten zu verwenden.

Aufbauempfehlung:

Automatisierungsskripte oder Docker für eine standardisierte Installation. Sammlung von vordefinierten Templates und Phishing-Szenarien, die schnell an spezifische Kundenanforderungen angepasst werden können. Reporting-Funktionen von King Phisher, um spezifische Kundenberichte zu generieren und zu speichern.

3.3.8 Informationssicherheit und Datenschutz

Die Klickratenverfolgung wird anonymisiert behandelt, und es werden keine Credentials abgefangen.

3.3.9 Voraussetzungen, Abhängigkeiten, Abgrenzungen

Voraussetzung ist eine Netzwerkinfrastruktur des Kunden, bei welchem ein Server (am liebsten Virtuell) bereitgestellt werden kann. Firewallregeln müssen durch dir Firma erstellt und gewartet werden können. Eine SMTP-Senderemail ist vorhanden. Useremailgruppen werden bereitgestellt. Die DNS-Einstellungen der Domains und Webservices werden von der Firma verwaltet und nach Absprache hinzugefügt.

3.4 Variante V3 – PhishingFrenzy

Pro Varianten werden folgende Punkte beschrieben.

3.4.1 Kurzbeschreibung

Phishing Frenzy ist eine Open-Source-Software, die für die Durchführung von E-Mail-Phishing-Kampagnen entwickelt wurde. Sie ermöglicht es, personalisierte Phishing-Angriffe zu entwerfen, durchzuführen und deren Erfolg zu messen, um die Sicherheitsbewusstseins-bildung innerhalb einer Organisation zu erhöhen.

Phishing Frenzy: SSL Support on Rails 4 with Syntax Highlighting - Pentest Geek

Abbildung 7 - Logo "PhishingFrenzy"

3.4.2 Funktionen

- ✓ Template-Management-System zur Erstellung und Verwaltung von Phishing-E-Mails und Landing Pages.
- ✓ Detaillierte Statistiken und Erfolgsmessungen, um die Reaktionen der Benutzer auf Phishing-Versuche zu verfolgen.
- ✓ Automatisierung von Kampagnen für eine effiziente Durchführung von Tests.
- ✓ Flexibles Kampagnenmanagement ermöglicht die Anpassung an spezifische Schu-lungsziele und -bedürfnisse.

3.4.3 Eignung

Phishing Frenzy ist besonders geeignet für Organisationen, die eine vielseitige und anpassbare Lösung suchen, um umfangreiche Phishing-Simulationen durchzuführen und detaillierte Rückmeldungen über die Wirksamkeit ihrer Schulungsprogramme zu erhalten.

3.4.4 Produkt oder IT-System

Folgend wir beschrieben, wie die Implementation beim Kunden aussehen würde.

Es wird alles lokal gewählt, sodass die Sicherheitsrisiken eingedämmt werden können, sowie möglichst keine neuen Poren (Porositys) geschafft werden.

Lediglich das Senden der Mails und die Verfolgung der Klickraten muss gegen aussen geöffnet sein.

Am schönsten wäre es die Installation in einem separaten Netz mit separatem Port zu haben, um höchste Sicherheit gewährleisten zu können.

3.4.5 Globale Systemarchitektur

Nachfolgend wir die konzeptionelle Systemarchitektur beschrieben.

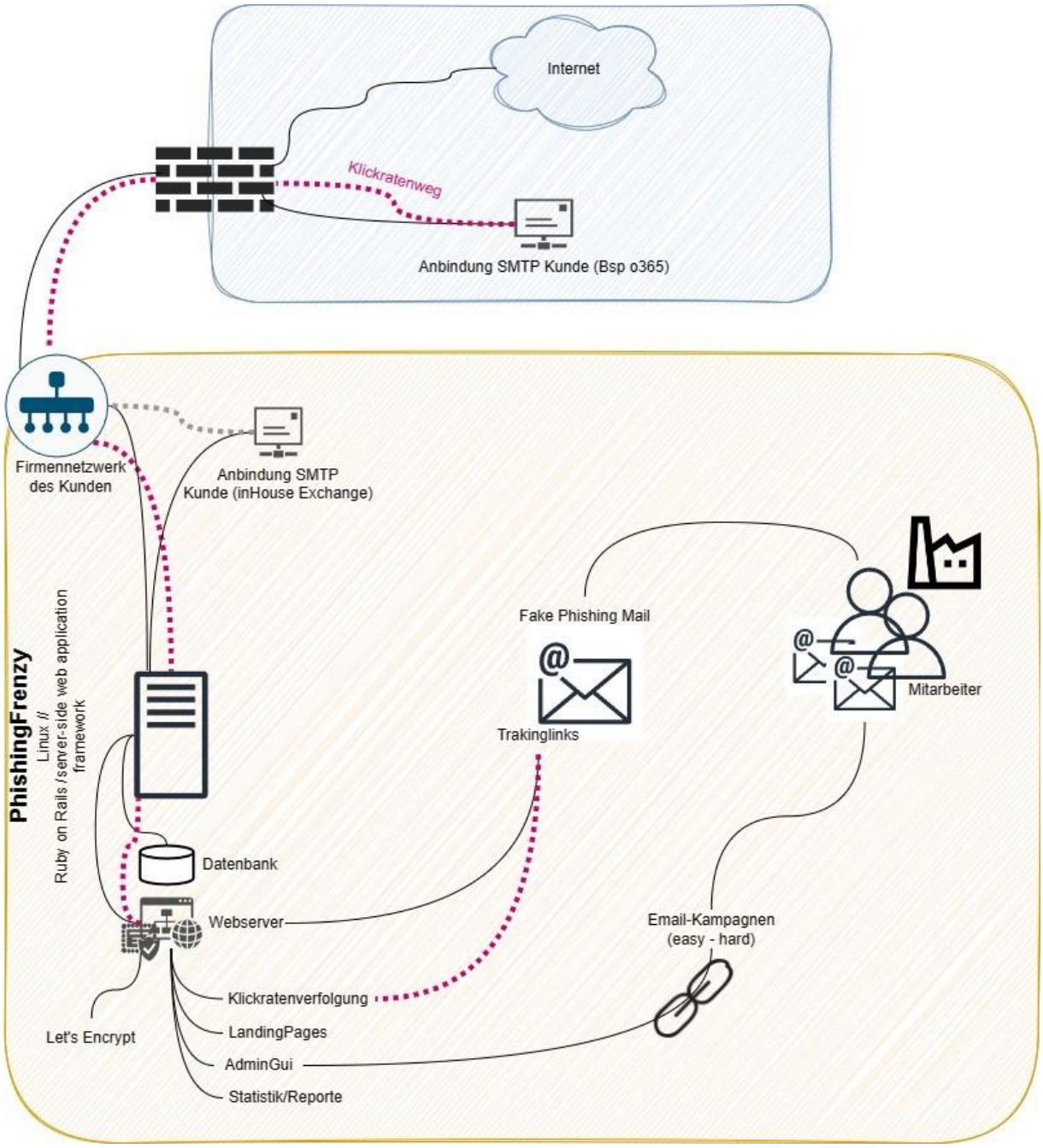

Abbildung 8 - Globale Systemarchitektur "PhishingFrenzy"

3.4.6 Integration und Netzwerkplan (Konzeptuell)

Server:

Phishing Frenzy erfordert die Installation auf einem Linux-Server, der entweder im lokalen Netzwerk oder in einer Cloud-Infrastruktur betrieben wird. Dieser Server wird für das Versenden von Phishing-E-Mails und das Hosting der Webseiten verwendet.

SMTP-Konfiguration:

Für das Versenden von Phishing-E-Mails muss Phishing Frenzy mit einem SMTP-Server verbunden sein. Dies kann ein unternehmenseigener SMTP-Server oder ein externer Dienst sein.

Landing Pages und Email Templates:

Phishing Frenzy ermöglicht die Gestaltung von Email-Templates und das Hosting von Landing Pages auf demselben Server, um eine realistische Phishing-Umgebung zu schaffen.

Statistik und Reporting:

Die Plattform bietet umfassende Möglichkeiten zur Erfassung und Analyse von Benutzerinteraktionen, einschliesslich Klicks und Eingaben auf den Landing Pages.

Technische Umsetzung bei Klicks auf Fake-Mails:

Phishing Frenzy nutzt Tracking-Techniken, um die Interaktionen der Benutzer mit den Phishing-E-Mails zu verfolgen. Ein Klick auf einen Link in der Phishing-Mail wird erfasst, indem der Benutzer über einen Tracking-Link zur gefälschten Landing Page weitergeleitet wird, wo weitere Aktionen analysiert werden können.

3.4.7 Mehrkundenfähigkeit

Schnelle Installation:

Phishing Frenzy ist für die Verwendung auf Ruby on Rails ausgelegt und erfordert daher eine spezifische Umgebung. Eine vorbereitete Virtual Machine (VM) oder die Nutzung von Containertechnologie wie Docker kann die Einrichtung beschleunigen.

Konfigurationen speichern:

Phishing Frenzy ermöglicht die Verwaltung von Templates und Kampagnen über seine Web-Oberfläche. Die Wiederverwendung von Kampagneneinstellungen und Templates ist durch die interne Verwaltung der Plattform vereinfacht.

Aufbauempfehlung:

VM oder Docker, um Phishing Frenzy schnell und konsistent auszurollen.

Bibliothek von Angriffsvorlagen auf, die für verschiedene Kunden und Kampagnen angepasst werden können.

Strategie für das Kampagnenmanagement, um den Überblick über verschiedene Kundenumgebungen zu behalten und effizient Berichte zu erstellen.

3.4.8 Informationssicherheit und Datenschutz

Die Klickratenverfolgung wird anonymisiert behandelt, und es werden keine Credentials abgefangen.

3.4.9 Voraussetzungen, Abhängigkeiten, Abgrenzungen

Voraussetzung ist eine Netzwerkinfrastruktur des Kunden, bei welchem ein Server (am liebsten Virtuell) bereitgestellt werden kann. Firewallregeln müssen durch dir Firma erstellt und gewartet werden können. Eine SMTP-Senderemail ist vorhanden. Useremailgruppen werden bereitgestellt. Die DNS-Einstellungen der Domains und Webservices werden von der Firma verwaltet und nach Absprache hinzugefügt.

4. Lösungsvarianten CAT

Basierend auf den Anforderungen für das Projekt, das Fake-Phishing-Mails (FPM) und Cybersecurity-Awareness-Training umfasst, sind hier drei Open-Source-Tools, die am besten geeignet sind, um diese Anforderungen zu erfüllen. Diese Tools bieten umfangreiche Funktionen für die Erstellung, Durchführung und Analyse von Phishing-Simulationen und unterstützen die Erhöhung der Sicherheitsbewusstseinsbildung innerhalb einer Organisation.

Für die Durchführung von Cybersecurity-Awareness-Trainings (CAT) gibt es verschiedene Plattformen, die sowohl kommerzielle als auch Open-Source-Optionen umfassen. In diesem Kapitel werden drei Plattformen erläutert, welche sich für die Entwicklung und Bereitstellung von Cyversecurity-Awareness-Training eignen.

4.1 Variantenübersicht

Folgend sind die drei Varianten aufgelistet.

Variante	Bezeichnung
CAT_V1	*Teachable*
CAT_V2	*Moodle*
CAT_V3	*Udemy for Business*

Tabelle 4 - Variantenübersicht CAT

4.2 Variante 1 "Teachable"

Die erste Variante behandelt Teachable.

Abbildung 9 - Logo "Teachable"

4.2.1 Kurzbeschrieb

Teachable ist eine moderne E-Learning-Plattform, die sich durch ihre benutzerfreundliche Oberfläche und umfangreichen Funktionen auszeichnet. Sie ist besonders auf technische Schulungen und Kurse spezialisiert, bietet jedoch auch vielseitige Möglichkeiten für andere Bildungsbereiche. Sie ermöglicht die Erstellung und Bereitstellung von Cybersecurity Awareness-Trainings für Firmen und bietet sowohl kostenlose Zugänge für Unternehmensmitarbeiter als auch kostenpflichtige Optionen für Einzelpersonen.

4.2.2 Funktionen

- ✓ Einfache Drag-and-Drop-Schnittstelle zur Kursentwicklung.
- ✓ Möglichkeit zur Einbindung von Videos, Quizzen und interaktiven Elementen.
- ✓ Integrationen mit externen Tools und Diensten.
- ✓ KI-Gesteuerte Kursgenerierung
- ✓ Live-Webinare und Aufzeichnungen
- ✓ Fortschrittsverfolgung und Analysen
- ✓ Kollaborative Lernumgebungen
- ✓ Integrierte Coding-Sandbox
- ✓ Benutzerfreundliche Oberfläche für einfache Navigation.
- ✓ Anpassbare Lernmodule für Cybersecurity Awareness.
- ✓ Interaktive Diskussionsforen.

4.2.3 Eignung

Geeignet für Unternehmen, die eine einfache und benutzerfreundliche Plattform für Cybersecurity Awareness-Trainings suchen. Besonders ansprechend für kleine und mittelständische Unternehmen.

4.2.4 Produkt

Das Produkt Teachable bietet eine Cloud-basierte E-Learning-Lösung, die speziell auf die Bedürfnisse von Unternehmen zugeschnitten ist. Neben der Erstellung von massgeschneiderten Trainings ermöglicht es auch die einfache Verwaltung von Nutzerzugriffen und Fortschrittsverfolgung.

4.2.5 Globale Übersicht

Teachable bietet eine übersichtliche Darstellung aller verfügbaren Kurse mit detaillierten Beschreibungen. Die Plattform ermöglicht eine einfache Navigation und einen klaren Überblick über den Fortschritt der Teilnehmer in den einzelnen Kursen.

4.2.6 Integration beim Kunden

Teachable ermöglicht eine nahtlose Integration in bestehende Systeme des Unternehmens, einschliesslich Single Sign-On (SSO) und API-Integrationen. Dies gewährleistet eine reibungslose Implementierung der Trainings in die vorhandene IT-Infrastruktur.

4.2.7 Mehrkundenfähigkeit

Teachable ist mehrkundenfähig und ermöglicht es Unternehmen, separate Schulungsumgebungen für verschiedene Kunden, Abteilungen oder Tochtergesellschaften zu erstellen. Dies erleichtert die Verwaltung und Anpassung der Trainings für unterschiedliche Anforderungen.

4.2.8 Zu beachten:

Folgendes ist zu beachten

4.2.8.1 Coupons notwendig

Die Integration von Coupons ist notwendig, um sicherzustellen, dass Mitarbeiter der Kunden welche auch den FPM-Service gekauft haben, kostenfreien Zugang zu den Trainings erhalten. Unternehmen können Coupons verwalten und individuelle Nutzer können diese bei Bedarf für kostenpflichtige Kurse verwenden.

4.2.9 Informationssicherheit und Datenschutz

Teachable verwendet verschlüsselte Verbindungen und sichere Protokolle, um die Vertraulichkeit der Daten zu gewährleisten. Es werden auch Compliance-Standards eingehalten, um die Sicherheit der Informationen zu gewährleisten.

4.2.10 Voraussetzungen, Abgrenzungen

Voraussetzungen: Stabile Internetverbindung für den Zugriff auf die Plattform, unterstützte Browser.

Abgrenzungen: Die Effektivität der Cybersecurity Awareness-Trainings hängt auch von den Teilnehmern ab, von deren Motivation und Lernfähigkeit. Dazu ist zu beachten, dass jede Person anders lernfähig ist und lernt.

4.2.11 Kosten

Teachable bietet verschiedene Preismodelle an. Die Kosten hängen von den Funktionen, der Anzahl der aktiven Schüler und anderen Faktoren ab. Untenstehend sind die grundlegenden Pläne für Teachable (Stand März 2024):

Basic Plan: Dieser Plan beginnt bei rund $39 pro Monat (bei jährlicher Zahlung) und bietet grundlegende Funktionen für die Erstellung und den Verkauf von Kursen.

Pro Plan: Der Pro Plan beginnt bei rund $119 pro Monat (bei jährlicher Zahlung) und bietet erweiterte Funktionen wie unbegrenzte Schüler, Quizze, Zertifikate und mehr.

Diese Pläne unterscheiden sich unteranderem in:

Pro Plan: Dieser Plan richtet sich an grössere Unternehmen und bietet Funktionen wie Gruppenunterricht, fortgeschrittene Berichterstattung und einen dedizierten Erfolgsspezialisten. Die Kosten sind massgeschneidert und müssen direkt bei Teachable angefragt werden.

Transaktionsgebühren: Beim Basic-Plan erhebt Teachable eine Transaktionsgebühr für jeden Kursverkauf, während der Business-Plan normalerweise eine geringere oder keine Transaktionsgebühr hat.

Anzahl der Admin-Nutzer: Der Business-Plan erlaubt in der Regel mehrere Admin-Nutzer, was nützlich ist, wenn mehrere Personen an der Verwaltung des Kurses beteiligt sind.

Unbegrenzte Anzahl von Teilnehmern: Während der Basic-Plan eine Obergrenze für die Anzahl der aktiven Teilnehmer pro Kurs hat, erlaubt der Business-Plan normalerweise eine unbegrenzte Anzahl.

Gruppenunterricht: Der Business-Plan bietet oft die Möglichkeit, Gruppenunterricht zu geben, was bedeutet, dass Sie Ihren Kurs an ganze Teams oder Organisationen verkaufen können.

Fortgeschrittene Berichterstattung: Der Business-Plan bietet normalerweise erweiterte Berichterstattungsfunktionen, um detaillierte Einblicke in den Fortschritt und das Verhalten der Schüler zu erhalten.

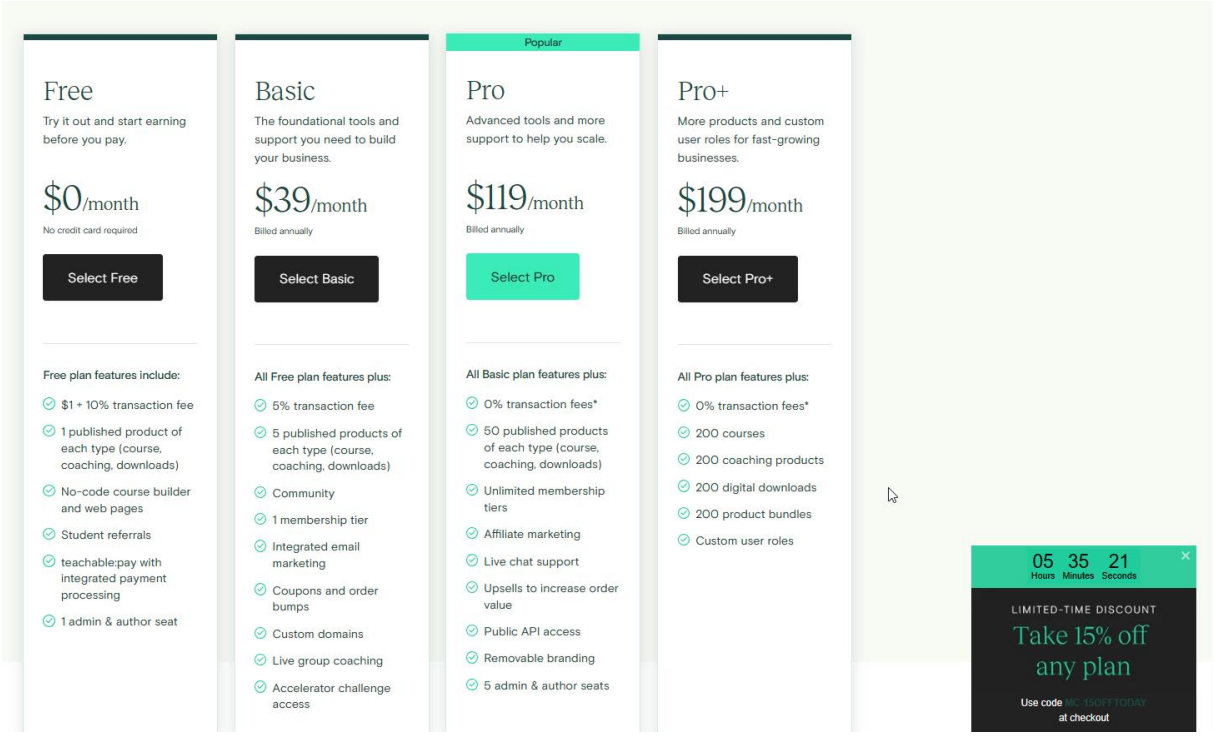

Abbildung 10 - Preisplan Teachable MAR 2024

In diesem Fall müsste die Basic variante genommen werden.

Jährliche Kosten; CHF 468.-

4.3 Variante 2 "Moodle"

Folgend wird die Variante Moodle näher erläutert.

Abbildung 11 - Logo "Moodle"

4.3.1 Kurzbeschrieb

Moodle ist eine weit verbreitete Open-Source-Lernplattform, die sich durch ihre Anpassbarkeit und Vielseitigkeit auszeichnet. Hier können massgeschneiderte Trainings für Firmen erstellt werden. Der Zugang ist für Unternehmensmitarbeiter kostenlos, während individuelle Nutzer kostenpflichtige Optionen nutzen können.

4.3.2 Funktionen

- ✓ Anpassbare Kursstrukturen und Lernmaterialien.
- ✓ Foren und Gruppendiskussionen für den Austausch von Erfahrungen.
- ✓ Überwachung des Lernfortschritts und Leistungsbewertungen.
- ✓ Integration von Multimedia-Elementen für ein multimediales Lernerlebnis.

4.3.3 Eignung

Ideal für Unternehmen, die eine hochgradig anpassbare Plattform mit umfassenden Funktionen für die Schulung ihrer Mitarbeiter im Bereich Cybersicherheit suchen. Geeignet für Unternehmen jeder Grösse.

4.3.4 Produkt

Moodle stellt eine Open-Source-Plattform dar, die Unternehmen die Möglichkeit gibt, individuelle Lerninhalte zu erstellen und zu verwalten. Es bietet eine flexible und anpassbare Umgebung für die Durchführung von Trainings sowie die Integration von externen Tools und Ressourcen an.

4.3.5 Globale Übersicht mit Kursen usw

Moodle präsentiert eine umfassende Übersicht über alle erstellten Kurse, Module und Lernmaterialien. Hier können Unternehmen globale Statistiken zum Lernfortschritt und zur Absolvierung der Trainings einsehen.

4.3.6 Integration beim Kunden

Moodle bietet umfassende Integrationsmöglichkeiten, einschliesslich der Integration von LDAP und anderen Authentifizierungsmethoden. Unternehmen können die Plattform problemlos in ihre bestehenden Systeme einbinden und die Lernumgebung anpassen. Um Moodle zu verwenden, muss die Software heruntergeladen und auf einem Server installiert werden. Moodle ist eine Open-Source-Lernplattform, die von den Nutzern selbst gehostet werden kann. Der Kunde müsste dafür ein Web- und Datenbankserver einrichten.

4.3.7 Mehrkundenfähigkeit

Die Mehrkundenfähigkeit von Moodle ermöglicht es Unternehmen, verschiedene Lernumgebungen für unterschiedliche Abteilungen oder externe Partner einrichten zu lassen. Jeder Kunde kann eine massgeschneiderte Schulungsumgebung für ihre spezifischen Anforderungen haben.

4.3.8 Informationssicherheit und Datenschutz

Hier liegt der Datenschutz, sowie die Informationssicherheit beim Kunden. Die Umgebung kann auch dediziert, ohne Internet, gehostet werden. (Intranet..)

4.3.9 Voraussetzungen, Abhängigkeiten, Abgrenzungen

Interne/Eigene Infrastruktur, Server und Webserver müssten vom Kunden gegeben werden. Die Kurse können so nicht einfach geupdated/erneuert werden. Die Effektivität der Cybersecurity Awareness-Trainings hängt auch von den Teilnehmern ab, von deren Motivation und Lernfähigkeit. Dazu ist zu beachten, dass jede Person anders lernfähig ist und lernt.

4.3.10 Kosten

Moodle ist eine Open-Source-Plattform, und die Kosten für Moodle können stark variieren. Die Software selbst ist kostenlos, aber es gibt Kosten für Hosting, Wartung und möglicherweise die Integration von Erweiterungen oder individuellen Anpassungen.

Die Hosting-Kosten hängen davon ab, ob Sie sich für eine Selbsthosting-Lösung entscheiden oder einen Hosting-Provider nutzen. Es gibt auch Unternehmen, die gehostete Moodle-

Lösungen anbieten, und die Kosten können je nach den Funktionen und der Anzahl der Benutzer variieren

4.4 Variante 3 "Udemy for Business"

Folgend wird die Variante Udemy for Business erläutert.

Abbildung 12 - Logo "Udemy business"

4.4.1 Kurzbeschrieb

Udemy for Business bietet eine umfassende Plattform für die Bereitstellung von Trainings für Unternehmen. Mitarbeitende haben kostenfreien Zugang, während individuelle Nutzer für den Zugriff auf die Schulungen bezahlen können. Die Plattform zeichnet sich durch ihre breite Nutzerbasis und innovative Lehrmethoden aus.

4.4.2 Funktionen

- ✓ Grosse Auswahl an vorbereiteten Kursen zu Cybersecurity Awareness.
- ✓ Möglichkeit zur Erstellung eigener Schulungsinhalte.
- ✓ Fortschrittsverfolgung und Zertifikate für abgeschlossene Kurse.
- ✓ Teammanagementfunktionen für die Unternehmensadministration.

4.4.3 Eignung

Eignet sich gut für die, welche eine breite Palette von vorgefertigten Kursen wünschen und die Möglichkeit haben möchten, eigene Schulungsinhalte zu integrieren. Skaliert gut für grosse Unternehmen.

4.4.4 Produkt

Udemy for Business ist eine umfassende Schulungsplattform, die eine breite Auswahl an vorbereiteten Kursen zu Cybersecurity Awareness bietet. Es können auch interne Schulungen erstellt und verwaltet werden. Die Plattform zeichnet sich durch ihre globale Reichweite und Vielfalt an Lerninhalten aus.

4.4.5 Globale Übersicht

Die Plattform bietet eine globale Übersicht über alle verfügbaren Kurse, sowohl interne als auch externe. Unternehmen haben Zugriff auf umfangreiche Statistiken und Analysen, um den Fortschritt der Mitarbeiter im Bereich Cybersecurity Awareness zu verfolgen.

4.4.6 Integration beim Kunden

Udemy for Business ermöglicht Integrationen in führende Unternehmensplattformen und Learning Management Systems (LMS). Diese Flexibilität erleichtert die Implementierung von Trainings in bestehende Unternehmensstrukturen.

4.4.7 Mehrkundenfähigkeit

Udemy for Business ist auf die Bedürfnisse von Unternehmen jeder Grösse ausgelegt und bietet eine skalierbare Lösung. Die Plattform unterstützt mehrere Kundenprofile und ermöglicht es, Schulungsumgebungen für unterschiedliche Kunden zu erstellen.

4.4.8 Informationssicherheit und Datenschutz

Udemy setzt verschiedene Sicherheitsmassnahmen ein, um die Plattform und die darauf gespeicherten Daten zu schützen. Dazu gehört unter anderem 2FA.

4.4.9 Voraussetzungen, Abhängigkeiten, Abgrenzungen

Voraussetzungen: Stabile Internetverbindung für den Zugriff auf die Plattform, unterstützte Browser.

Abgrenzungen: Die Effektivität der Cybersecurity Awareness-Trainings hängt auch von den Teilnehmern ab, von deren Motivation und Lernfähigkeit. Dazu ist zu beachten, dass jede Person anders lernfähig ist und lernt.

4.4.10 Kosten

Udemy ist eine Plattform, auf der Instruktoren Kurse erstellen und verkaufen können. Udemy behält eine Provision von den Kursverkäufen ein. Instrukteure können ihre Kurse zu einem von Udemy festgelegten Preis verkaufen, und Udemy behält einen Prozentsatz, normalerweise 30%, des Verkaufspreises ein. Der Rest geht an den Instrukteur.

5. Variantenbewertung FPM

Folgend werden die Anforderungen anhand der Features der Varianten bewertet. Bewertungskriterien, Gewichtung und Schlüssel sind in den nachfolgenden Kapiteln ersichtlich.

5.1 Bewertungskriterien, Gewichtung und Schlüssel

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.

Summe der Bewertung (obere Tabelle) = Sieger FPM-TOOL

5.2 Variantenbewertung FPM

Folgend werden die Gewichtungen für die Varianten per Anforderung verteilt. Die Gewichtung / Bewertung wird im oberen Kapitel vorgestellt.

5.2.1 Variantenbewertung V1_CAT - «Teachable»

Folgend die Variantenbewertung für die OpenSource Lösung «GoPhish»

ID	Subkriterium / Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5)	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die Implementation der Anforderung? (Schwierig = 0 / Einfach = 10)	Hilfestellung und Support (online-community, basierend auf vorhandenen Videos und Foren) (keine Hilfestellung = 0 / Viel Hilfestellung = 10)
V1_FPM – «GoPhish»					
FPM_A01	Empfang von FPMs	10	1	7	10
FPM_A02	*Die Benutzer können mit dem FPM interagieren, Link öffnen*	10	1	5	9
FPM_A03	Interaktion mit FLP, Credential-phishing	5	1	4	7
FPM_A04	Teilnahme am CAT möglich nach erstem FPM (Direktes Weiterleiten, Link..)	10	1	8	8
FPM_A05	*Ein Report/Auflösung wird nach Beendung von FPM generiert*	10	1	4	5
FPM_A06	Die FPM können detailgetreu konfiguriert werden	10	1	6	9
FPM_A07	Es können mehrere Kampagnen gefahren werden damit verschiedene Schwierigkeitslevel (Erkennbarkeit FPM) designt werden können	5	1	8	7

FPM_A08	Usermails können importiert und in Gruppen aufgeteilt werden	5	1	10	10
FPM_A09	Das FPM kann an diverse Usermailgruppen gesendet werden	10	1	8	10
FPM_A10	Die div. FPM und deren Konfiguration und Einstellungen können exportiert werden	10	1	8	9
FPM_A11	Einfach aufbaubares Tool, übersichtlich	10	1	10	10
FPM_A12	One-Klick Installation	5	1	10	10
FPM_A13	Erstellung und Verwaltung von Fake-Login-Seiten und deren Export (Designexport)	10	1	7	9
FPM_A14	Konfigurations-Export (Design) möglich	5	1	8	9
FPM_A15	Klicks auf Links im FPM werden getrackt	10	1	5	7
FPM_A16	Die Klickraten werden anonymisiert behandelt	10	1	9	8
FPM_A17	Pro Kunde neu Installation	5	1	10	10
FPM_A18	Die Konfiguration wie SMTP usw muss einfach erfolgen können und am besten vom SMTP des Kunden, damit keine FPMs geblockt werden	10	1	8	10
Summe:		150	18	135	157
					Summe V1_FPM: 460

5.2.2 Variantenbewertung V2_FPM - «KingFischer»

Folgend die Variantenbewertung für die OpenSource Lösung «KingFischer»

ID	Subkriterium / Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5)	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die Implementation der Anforderung? (Schwierig = 0 / Einfach = 10)	Hilfestellung und Support (online-community, basierend auf vorhandenen Videos und Foren) (keine Hilfestellung = 0 / Viel Hilfestellung = 10)
V2_FPM – «KingFischer»					
FPM_A01	Empfang von FPMs	10	1	5	6
FPM_A02	*Die Benutzer können mit dem FPM interagieren, Link öffnen*	10	1	5	6
FPM_A03	Interaktion mit FLP, Credential-phishing	5	1	5	5
FPM_A04	Teilnahme am CAT möglich nach erstem FPM (Direktes Weiterleiten, Link..)	10	1	7	6
FPM_A05	*Ein Report/Auflösung wird nach Beendung von FPM generiert*	10	1	5	4
FPM_A06	Die FPM können detailgetreu konfiguriert werden	10	1	4	5
FPM_A07	Es können mehrere Kampagnen gefahren werden damit verschiedene Schwierigkeitslevel (Erkennbarkeit FPM) designt werden können	5	1	8	7
FPM_A08	Usermails können importiert und in Gruppen aufgeteilt werden	5	1	7	7
FPM_A09	Das FPM kann an diverse Usermailgruppen gesendet werden	10	1	8	7
FPM_A10	Die div. FPM und deren Konfiguration und Einstellungen können exportiert werden	10	1	3	5
FPM_A11	Einfach aufbaubares Tool, übersichtlich	10	1	4	6
FPM_A12	One-Klick Installation	5	1	0	4

FPM_A13	Erstellung und Verwaltung von Fake-Login-Seiten und deren Export (Designexport)	10	1	5	4
FPM_A14	Konfigurations-Export (Design) möglich	5	1	4	4
FPM_A15	Klicks auf Links im FPM werden getrackt	10	1	3	4
FPM_A16	Die Klickraten werden anonymisiert behandelt	10	1	7	6
FPM_A17	Pro Kunde neu Installation	5	1	6	6
FPM_A18	Die Konfiguration wie SMTP usw muss einfach erfolgen können und am besten vom SMTP des Kunden, damit keine FPMs geblockt werden	10	1	4	4
Summe:		150	18	90	100
					Summe V1_FPM: 354

5.2.3 Variantenbewertung V3_FPM - «PhishingFrenzy»

Folgend die Variantenbewertung für die OpenSource Lösung «PhishingFrenzy»

ID	Subkriterium / Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5)	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die Implementation der Anforderung? (Schwierig = 0 / Einfach = 10)	Hilfestellung und Support (online-community, basierend auf vorhandenen Videos und Foren) (keine Hilfestellung = 0 / Viel Hilfestellung = 10)
V3_FPM – «PhishingFrenzy»					
FPM_A01	Empfang von FPMs	10	1	3	6
FPM_A02	*Die Benutzer können mit dem FPM interagieren, Link öffnen*	10	1	5	6
FPM_A03	Interaktion mit FLP, Credential-phishing	5	1	4	5
FPM_A04	Teilnahme am CAT möglich nach erstem FPM (Direktes Weiterleiten, Link..)	10	1	7	7
FPM_A05	*Ein Report/Auflösung wird nach Beendung von FPM generiert*	10	1	4	5
FPM_A06	Die FPM können detailgetreu konfiguriert werden	10	1	6	5
FPM_A07	Es können mehrere Kampagnen gefahren werden damit verschiedene Schwierigkeitslevel (Erkennbarkeit FPM) designt werden können	5	1	7	7
FPM_A08	Usermails können importiert und in Gruppen aufgeteilt werden	5	1	9	7
FPM_A09	Das FPM kann an diverse Usermailgruppen gesendet werden	10	1	8	7
FPM_A10	Die div. FPM und deren Konfiguration und Einstellungen können exportiert werden	10	1	4	7

FPM_A11	Einfach aufbaubares Tool, übersicht-lich	10	1	4	7
FPM_A12	One-Klick Installation	5	1	0	5
FPM_A13	Erstellung und Verwaltung von Fake-Login-Seiten und deren Export (De-signexport)	10	1	5	5
FPM_A14	Konfigurations-Export (Design) möglich	5	1	4	5
FPM_A15	Klicks auf Links im FPM werden getrackt	10	1	3	5
FPM_A16	Die Klickraten werden anonymisiert behandelt	10	1	7	6
FPM_A17	Pro Kunde neu Installation	5	1	6	6
FPM_A18	Die Konfiguration wie SMTP usw muss einfach erfolgen können und am besten vom SMTP des Kunden, damit keine FPMs ge-blockt werden	10	1	4	4
Summe:		150	18	90	105
					Summe V1_FPM: 363

5.3 Variantenentscheid FPM

Folgend sind die Summen, welcher dem obigen Kapitel entnommen werden können, hinterlegt. Als Sieger geht eindeutig GoPhish hervor, dies unter anderem wegen seiner einfachen Integration und Bedienung.

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

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

6. Variantenbewertung CAT

Folgend werden die Anforderungen anhand der Features der Varianten bewertet. Bewertungskriterien, Gewichtung und Schlüssel sind in den nachfolgenden Kapiteln ersichtlich.

6.1 Bewertungskriterien, Gewichtung und Schlüssel

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

Abbildung 13 - Bewertungskriterien CAT

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.

6.2 Variantenbewertung CAT

Untenstehend werden die zuvor definierten Punkte vergeben.

6.2.1 Variantenbewertung V1_CAT - «Teachable»

Die Variantenbewertung wird mitfolgenden Punkte pro Anforderung bewertet:

ID	Subkriterium/Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die aktuellhaltung der Kursinhalten? (Schwierig = 0 / Einfach = 10)	Kosten (Überschreitet Notfallbudget = 0 / Niedrig = 10)
V1_CAT – «Teachable»					
CAT_A01	Die Benutzer können am CAT Teilnehmen	10	1	9	4
CAT_A02	Auf der CAT Plattform können zwischen diversen Themengebieten ausgewählt werden	10	1		
CAT_A03	Trainings sind auf Zielgruppe Mitarbeiter abgesehen	10	1		
CAT_A04	Die Trainings werden nach Schwierigkeitslevel angelegt	5	1		
CAT_A05	Der Kursaufbau auf der Plattform muss übersichtlich sein	10	1		
CAT_A06	Interessanter Aufbau, nicht e-Training like all	5	1		
CAT_A07	Quizzes für Check Lernprozess können besucht werden	10	1		
CAT_A08	Kleiner Exkurs mit Tipps und Tricks für den Alltag als Privatperson	5	1		

CAT_A09	Die Kunden welche den FPM-Service erworben haben, erhalten den CAT gratis. Individuals müssen für die Kurse bezahlen	10	1		
CAT_A10	Diverse Kurse müssen auf der Plattform erstellt werden können	10	1		
CAT_A11	Diverse Quizzes müssen auf der Plattform erstellt werden können	10	1		
CAT_A12	Das Backend sollte übersichtlich aufgebaut sein	*5*	*1*		
CAT_A13	Die Kosten der CAT Plattform sollte sich unter CHF 250.- /6Mnt halten	5	0		
CAT_A14	Die Firmenuser müssen via Rabattcode gratis auf CAT zugreifen können	10	1		
CAT_A15	Die Kurse und Quizzes können mithilfe von AI aufgebaut werden	5	1		
CAT_A16	Es bestehen Feedbackprozesse über den Kursinhalt (Kundenzufriedenheit)	10	1		
CAT_A17	Die Teilnahmezeiten/Dauer per Mitarbeiter werden definiert	5	1		
Summe:		130	16	8	4
Summe V1_CAT: 158					

6.2.2 Variantenbewertung V2_CAT - «Moodle»

Die Variantenbewertung wird mitfolgenden Punkte pro Anforderung bewertet:

ID	Subkriterium/Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die aktuellhaltung der Kursinhalten? (Schwierig = 0 / Einfach = 10)	Kosten (Überschreitet Notfallbudget = 0 / Niedrig = 10)
V2_CAT – «Moodle»					
CAT_A01	Die Benutzer können am CAT Teilnehmen	10	1	3	8
CAT_A02	Auf der CAT Plattform können zwischen diversen Themengebieten ausgewählt werden	10	1		
CAT_A03	Trainings sind auf Zielgruppe Mitarbeiter abgesehen	10	1		
CAT_A04	Die Trainings werden nach Schwierigkeitslevel angelegt	5	1		
CAT_A05	Der Kursaufbau auf der Plattform muss übersichtlich sein	10	1		
CAT_A06	Interessanter Aufbau, nicht e-Training like all	5	0		
CAT_A07	Quizzes für Check Lernprozess können besucht werden	10	1		
CAT_A08	Kleiner Exkurs mit Tipps und Tricks für den Alltag als Privatperson	5	1		
CAT_A09	Die Kunden welche den FPM-Service erworben haben, erhalten den CAT gratis.	10	1		

	Individuals müssen für die Kurse bezahlen				
CAT_A10	Diverse Kurse müssen auf der Plattform erstellt werden können	10	1		
CAT_A11	Diverse Quizzes müssen auf der Plattform erstellt werden können	10	1		
CAT_A12	Das Backend sollte übersichtlich aufgebaut sein	*5*	*0*		
CAT_A13	Die Kosten der CAT Plattform sollte sich unter CHF 250.- /6Mnt halten	5	1		
CAT_A14	Die Firmenuser müssen via Rabattcode gratis auf CAT zugreifen können	10	1		
CAT_A15	Die Kurse und Quizzes können mithilfe von AI aufgebaut werden	5	0		
CAT_A16	Es bestehen Feedbackprozesse über den Kursinhalt (Kundenzufriedenheit)	10	1		
CAT_A17	Die Teilnahmezeiten/Dauer per Mitarbeiter werden definiert	5	1		
Summe:		130	14	3	8
					Summe V2_CAT: 155

6.2.3 Variantenbewertung V3_CAT - «Udemy for Business»

Die Variantenbewertung wird mitfolgenden Punkte pro Anforderung bewertet:

ID	Subkriterium/Beschreibung	Wie wichtig? (Muss = 10 / Kann = 5	Anforderung erfüllt? (Ja = 1 / Nein = 0)	Wie einfach ist die aktuellhaltung der Kursinhalten? (Schwierig = 0 / Einfach = 10)	Kosten (Überschreitet Notfallbudget = 0 / Niedrig = 10)
V3_CAT – «Udemy for Business»					
CAT_A01	Die Benutzer können am CAT Teilnehmen	10	1	6	3
CAT_A02	Auf der CAT Plattform können zwischen diversen Themengebieten ausgewählt werden	10	1		
CAT_A03	Trainings sind auf Zielgruppe Mitarbeiter abgesehen	10	1		
CAT_A04	Die Trainings werden nach Schwierigkeitslevel angelegt	5	1		
CAT_A05	Der Kursaufbau auf der Plattform muss übersichtlich sein	10	1		
CAT_A06	Interessanter Aufbau, nicht e-Training like all	5	0		
CAT_A07	Quizzes für Check Lernprozess können besucht werden	10	1		
CAT_A08	Kleiner Exkurs mit Tipps und Tricks für den Alltag als Privatperson	5	1		
CAT_A09	Die Kunden welche den FPM-Service erworben haben, erhalten den CAT gratis.	10	1		

	Individuals müssen für die Kurse bezahlen				
CAT_A10	Diverse Kurse müssen auf der Plattform erstellt werden können	10	1		
CAT_A11	Diverse Quizzes müssen auf der Plattform erstellt werden können	10	1		
CAT_A12	Das Backend sollte übersichtlich aufgebaut sein	*5*	*0*		
CAT_A13	Die Kosten der CAT Plattform sollte sich unter CHF 250.- /6Mnt halten	5	1		
CAT_A14	Die Firmenuser müssen via Rabattcode gratis auf CAT zugreifen können	10	1		
CAT_A15	Die Kurse und Quizzes können mithilfe von AI aufgebaut werden	5	0		
CAT_A16	Es bestehen Feedbackprozesse über den Kursinhalt (Kundenzufriedenheit)	10	1		
CAT_A17	Die Teilnahmezeiten/Dauer per Mitarbeiter werden definiert	5	1		
Summe:		130	14	6	3
					Summe V2_CAT: 153

6.3 Variantenentscheid CAT

Nachfolgend ist der Gewinner in der folgenden Tabelle ersichtlich. Die Punkte wurde aus den hervorgehenden Tabellen die Summen entommen.

Tabelle 5 - Variantenentscheid CAT

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

Folgend sind die Summen, welcher dem obigen Kapitel entnommen werden können, hinterlegt. Als Sieger geht eindeutig GoPhish hervor, dies unter anderem wegen seiner einfachen Integration und Bedienung.

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

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