fake phishing mail service

FPM

-KONZEPT-

Auftraggeber	Marc Aeby
Projektleiter	J. Storrer
Autor	J. Storrer
Dokument	ID2132_StorrerJessica_FPM _Konzept_v01.docx
Klassifizierung	Intern
Status	Genehmigt

Änderungsverzeichnis

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

Inhaltsverzeichnis

Inhaltsverzeichnis 1
Abbildungsverzeichnis 3
Tabellenverzeichnis 4
1. Lieferergebnisse 5
1.1 Overall 5
1.2 Lieferobjekte FPM 5
1.3 Lieferobjekte CAT 5
2. Usecases/Userstorys und Prozesse FPM 6
2.1.1 UseCase / Prozessdefinition A «Worst case Szenario» 6
2.1.2 UseCase / Prozessdefinition B „Klick on Link“ 8
2.1.3 UseCase Prozessdefinition C 10
3. Aufbau VM 12
3.1 Settings 12
3.2 Webserver 12
4. Aufbau GoPhish 13
4.1 Über die Kundenimplementation 14
4.2 Installation 14
4.3 Grundkonfiguration 14
4.3.1 Genauere Beschreibung der Werte 15
4.3.2 SSL Zertifikate 16
4.3.3 SQLLite 16
4.4 Kampagnen 16
4.5 User & Groups 18
4.6 Email-Templates 19
4.7 Landing-Pages 21
4.8 Sending Profiles 22
4.9 Listener / Klickratenverfolgung 24
4.10 Die Zusammenhänge der Kampagne 24
5. Definition FPM & FPL 1 easy – 2 medium - 3 hard (Kampagnen) 26
5.1 Definition FPM, FPL - level easy – Das Auffällige 27
5.1.1 Idee Galaxus-Gutschein 27
5.1.2 Email-Template 28
5.1.3 Landing-Page 28
5.1.4 Sending-Profile 29
5.1.5 Kampagne 29
5.1.6 Antwort-Vorlage für Report an IT 29
5.1.7 Klickratenverfolgung 30
5.2 Definition FPM, FPL - level medium – Der Klassiker 31
5.2.1 Idee “Abgelaufene o365 Anmeldung” 31
5.2.2 Email-Template 31
5.2.3 Landing-Page 32
5.2.4 Sending-Profile 32
5.2.5 Kampagne 32
5.2.6 Antowort-Vorlage für Report an IT 33
5.2.7 Klickratenverfolgung 33
5.3 Definition FPM, FPL - level hard 34
5.3.1 Idee “Bugoutstore-Gutschein” 34
5.3.2 Email-Template 34
5.3.3 Landing-Page 35
5.3.4 Sending-Profile 35
5.3.5 Kampagne 35
5.3.6 Antwort-Vorlage für Report an IT 36
5.3.7 Klickratenverfolgung 36
6. Mehrkundenfähigkeit 37
6.1 Speichern von Templates und LandingPages 37
6.2 Integration beim Kunden / Integrationsprozess 38
6.2.1 Integrationsprozess 38
7. Reporting & Statistiken 40
7.1 Wie das Reporting Funktioniert 40

7.2 Dashboard 40
7.2.1 Zusatz: GoReport 40
7.3 Überwachung während Service 41
7.4 Newsletter und Report an Firma 41
7.4.1 Inhalt Report 41
7.4.2 Inhalt Newsletter 42
8. Kundeninformationsblatt 43
9. Checkliste Installation 44
10. Datenschutzgesetz Konzept und Infos 45
11. Testkonzepte nach Anforderungen 46
12. Pricing 47
12.1 Pricing FPM 47
12.1.1 Allgemeine Preisstrategie 47
12.1.2 Preisstruktur Pauschale Lizenzmodell 47
12.1.3 Wirtschaftliche Überlegungen / Break Even 48
12.1.4 Fazit 49
Literaturverzeichnis 50
Eidesstattliche Erklärung 51

Abbildungsverzeichnis

Abbildung 1 - UseCase A FPM 7
Abbildung 2 - UseCase B FPM 9
Abbildung 3 - UseCase C FPM 11
Abbildung 4 - Übersicht Konfigurationen GoPhish 13
Abbildung 5 - GoPhish Kampagne (Bild aus Testinstallation) 17
Abbildung 6 - User&Gruppenimport GoPhish (Screenshot aus Testinstallation) 19
Abbildung 7 - EmailTemplate FPM GoPhish (Screenshot aus Testinstallation) 20
Abbildung 8 - URL Eingabe in MailTemplate 21
Abbildung 9 - LandingPage FPL GoPhish (Screenshot aus Testinstallation) 22
Abbildung 10 - Sending-Profile SMTP-Informationen (Screenshot aus Testinstallation) 23
Abbildung 11 - SendingProfile EmailHeaders 23
Abbildung 12 - Zusammenhänge Aufbau Kampagne 25
Abbildung 13 - Zusammenhänge Templates & Kampagne 27
Abbildung 14 - Integrationsprozess Kunde 39

Tabellenverzeichnis

Tabelle 1 - Mindestanfoderungen VM 12
Tabelle 2 - Grundkonfiguration GoPhish config.json 15
Tabelle 3 - Level easy – «Das Auffällige» EmailTemplate Page Konfiguration 28
Tabelle 4 - Level easy – «Das Auffällige» Landing Page Konfiguration 28
Tabelle 5 - Level easy – «Das Auffälige» Kampagne Konfiguration 29
Tabelle 6 - Level medium – «Der Klassiker» EmailTemplate Konfiguration 31
Tabelle 7 - Level Medium – «Der Klassiker» Landing Page Konfiguration 32
Tabelle 8 - Level medium – «Der Klassiker» Kampagne Konfiguration 32
Tabelle 9 - Level hard – «Das gut Social-Engineerte»EmailTemplate Konfiguration 34
Tabelle 10 - Level hard – «Das gut Social-Engineerte» Landing Page Konfiguration 35
Tabelle 11 - Level hard – «Das gut Social-Engineerte» Kampagnen Konfiguration 35
Tabelle 12 - BreakEven analyse im ersten Jahr im Lizenzmodell 48

1. Lieferergebnisse

Im folgenden Kapitel werden die Lieferergebnisse dieses Projekts erläutert.

Die GELB hinterlegten Lieferergebnisse sind im Konzept zu bearbeiten. (Die GRÜN hinterlegten sind bereit erledigt, ROSA muss noch graphisch dargestellt werden, GRAU bezieht sich auf eine andere Phase)

1.1 Overall

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

1.2 Lieferobjekte FPM

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

1.3 Lieferobjekte CAT

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

2. Usecases/Userstorys und Prozesse FPM

Folgende werden die verschiedenen UseCases und Prozesses des FPM-Services aufgezeigt.

2.1.1 UseCase / Prozessdefinition A «Worst case Szenario»

Der Usecase A des FPM Prozesses ist «WorstCase Szenario» - der User gibt auf der FakeLogin Page fälschlicherweise die Credentials ein.

GoPhisch merkt das und versendet eine Email mit der Auflösung dass dies Fake war und verweist auf CAT.

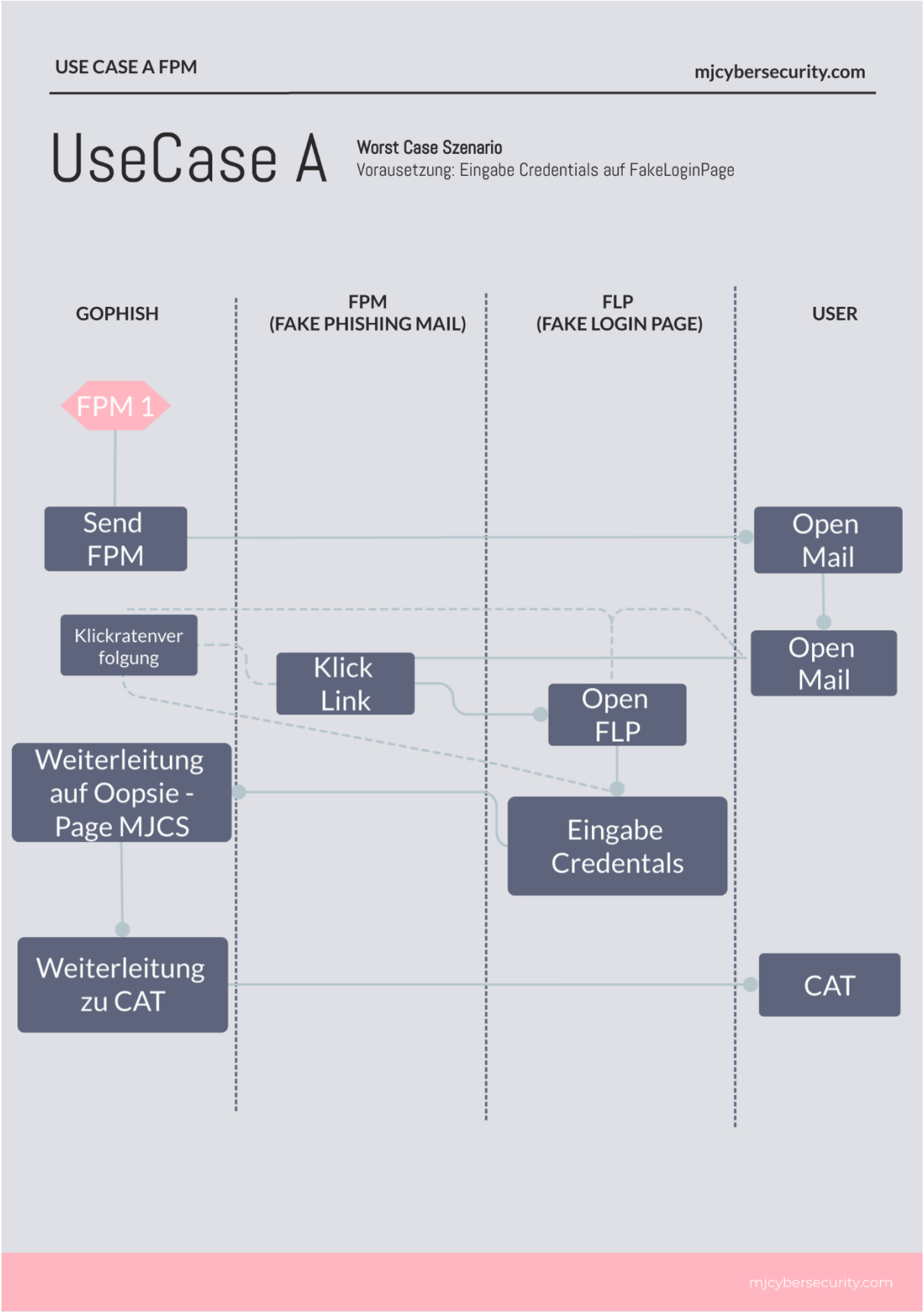

Abbildung 1 - UseCase A FPM

2.1.2 UseCase / Prozessdefinition B „Klick on Link“

Im UseCase B Szenrario, Klickt der User auf den Link, merkt dann jedoch, dass es fake ist und reportet die Email der internen IT der Firma.

GoPhish merkt den Klick auf den Link und versendet hier ebenso eine Email mit der Auflösung und den Verweis an CAT. Der Report ist je nach Firma unterschiedlich. Beim Pilotkunden werden die Emails an die IT weitergeleitet. Hierdurch kann die IT mit der Auflösungsemail und CAT-Verlinkung diesen Usern Antworten. Wenn auf GoPhish ein Klick verzeichnet wurde, wird dieser durch die ***Manuelle Überprüfung der Kampagne*** (AdminPanel GoPhish) durch den Mitarbeiter erkannt und kann so persönlich dem Mitarbeiter antworten, auflösen und auf CAT weiterleiten.

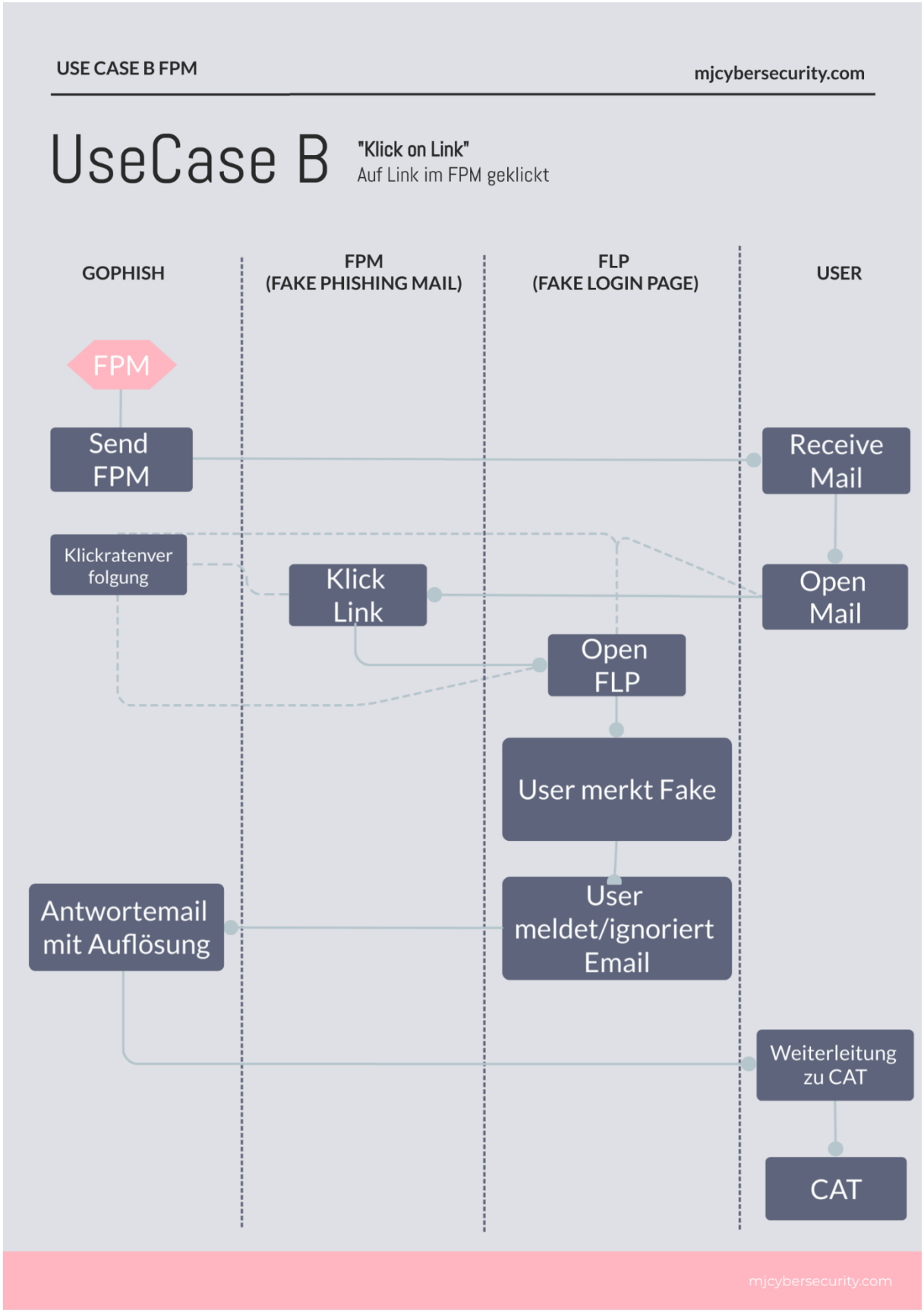

Abbildung 2 - UseCase B FPM

2.1.3 UseCase Prozessdefinition C

Im UseCase C merkt der Mitarbeiter sofort, dass die FPM fake ist und reportet dies der internen IT der Firma. Hier bedankt sich dann die IT und versendet eine Email mit Verweis auf CAT.

Der Report ist je nach Firma unterschiedlich. Beim Pilotkunden werden die Emails an die IT weitergeleitet. Hierdurch kann die IT mit der Auflösungsemail und CAT-Verlinkung diesen Usern Antworten.

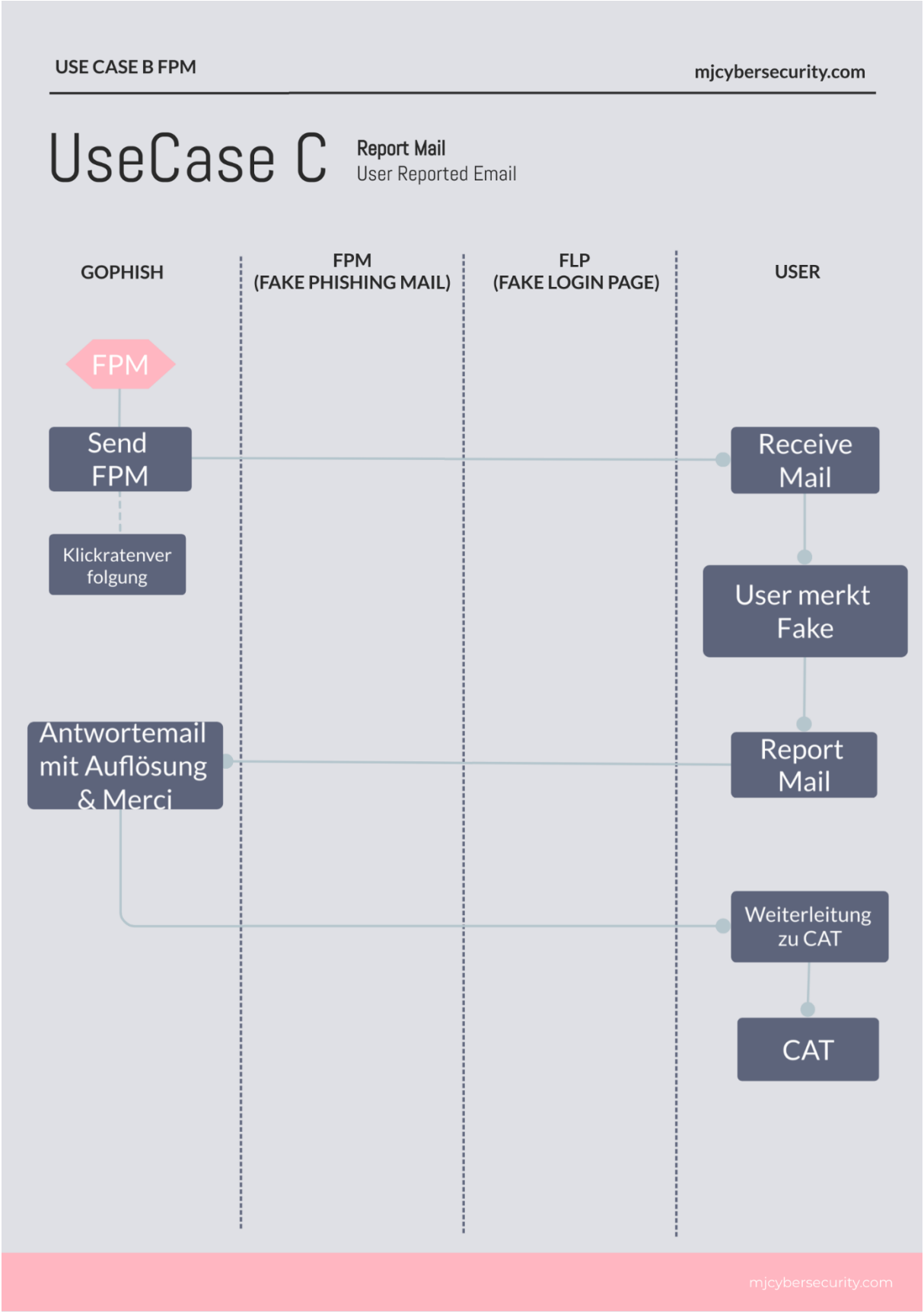

Abbildung 3 - UseCase C FPM

3. Aufbau VM

Im folgenden Kapitel wird der Aufbau der VM, sowie deren Webservice und der Aufbau von GoPhish konzeptionell erläutert.

Da eine Anforderung an FPM „OpenSource“ ist, wird die VM mit Ubuntu Server (min. 22.04.4 TLS) als Basis verwendet. Für alle weiteren Einstellungen dienen die unteren Kapitel

3.1 Settings

Folgende Mindestanforderungen muss die VW haben. Dies Mindestanforderungen kann entweder vom Kunden bereitgestellt werden, oder MJ Cybersecurity Services wird diese Aufbauen. (Wenn vom Kunden gewünscht, kann die Installation ebenso auf einem physischen Gerät konfiguriert werden)

Mindestanforderungen VM		
Memory	8GB	
Disk	60GB	
Kernels	2	
Interfaces	1, fixe IP Adresse muss vergeben werden	
Erreichbarkeit durch Clients	Im selben Netz wie die Userclients	
Erreichbarkeit Internet (für SMTP Send)	Maschine hat Internetanbindung	
Betriebssystem	Ubuntu Server, min. 22.04.4 TLS	
AdminUser	Passwort muss bei Übergabe an MJ Cybersecurity Services bekannt gegeben werden	

Tabelle 1 - Mindestanfoderungen VM

Anhand der oben in der Tabelle genannten Informationen muss die VM für die weiteren Installationen bereit sein.

3.2 Webserver

GoPhish erstellt bei Installation selbständig einen Webserver.

Zusatz: GoPhish mit Domain ansprechbar machen.

4. Aufbau GoPhish

Im folgenden Kapitel wird der Aufbau von GoPhish so erläutert, wie er in der Realisierung umzusetzen ist. Die genauen Konzeptionellen Angaben werden im Kapitel 5 erläutert. Im Kapitel 4 sind die Allgemeinen Konfigurationsmöglichkeiten als Hilfestellung Dokumentiert.

Im folgenden Bild sind die Zusammenhänge der verschiedenen Konfigurationszusammenhänge von GoPhish zur Visualisierung graphisch dargestellt.

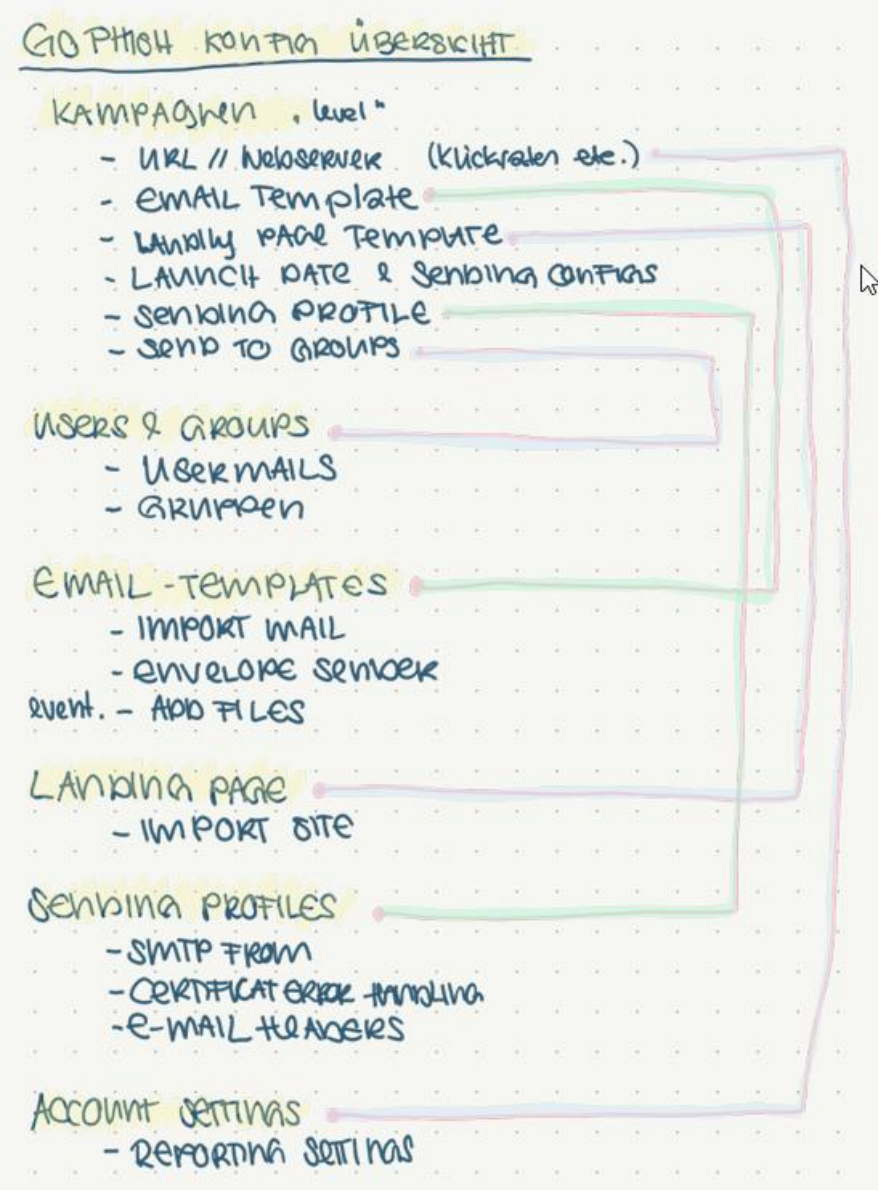

Abbildung 4 - Übersicht Konfigurationen GoPhish

4.1 Über die Kundenimplementation

Gophish wird bei Kunden in der Umgebung auf einer VM auf Ubuntu Server aufgesetzt. Gophish installiert Datenbank (SQLLite) und einen Webserver automatisch mit.

Der GoPhish Server ist im selben Netzwerk wie deren Client und ist am SMTP des Kunden angebunden.

Des Weiteren bietet gophish das Versenden von fake phishing Mails an. diese werden an die Firmenmitarbeiter gesendet. die Emails enthalten fake-Landing-pages - ebenfalls auf GoPhisch konfigurierbar. wenn die User das mail öffnen oder der link darin, wird das in der Datenbank gespeichert, um so einen Klickratenreport machen zu können, welchen GoPhish ebenso anbietet

Die Klickratenverfolgung wird in der Datenbank abgespeichert. in der Datenbank wird ebenso ein RID-Parameter für die LandingPages in Verknüpfung mit User abgebildet, sodass GoPhish weiss, welche Landing page zu welcher E-Mail gehört

4.2 Installation

Die Installation erfolgt einfach via install-command, wie von Ubuntu gewöhnt. Dazu wird folgendes Abbild verwendet: **`github.com/gophish/gophish`**

Alle Informationen, sowie Anleitungen sind hier zu finden, ebenso wurden die Informationen über GoPhish ebenso dieser Dokumentation entnommen:

Installation | Gophish User Guide (getgophish.com)

4.3 Grundkonfiguration

Folgende Grundkonfigurationen sind im config.json zu konfigurieren.

Wert	Value	Beschreibung
admin_server.listen_url	[FixeIP_GoPhishVM]:3333	IP/Port of gophish admin server
admin_server.use_tls	false	Use TLS for admin server?
admin_server.cert_path	*Wird dank der Versionen 0.3+ von GoPhish selber hinterlegt*	Path to SSL Cert
admin_server.key_path	*Wird dank der Versionen 0.3+ von GoPhish selber hinterlegt*	Path to SSL Private Key
admin_server.trusted_origins	*[]*	Comma separated list of trusted origins
phish_server.listen_url	[FixeIP_GoPhishVM]:80	IP/Port of the phishing server - this is where landing pages are hosted.

Tabelle 2 - Grundkonfiguration GoPhish config.json

Diese Tabelle wurde der Dokumentation vom im Kapitel 4.1 erwähnten Onlinedokument entnommen, und auf die Installationen für diesen Service angepasst.

Vorsicht: Da die config.json-Datei Datenbankanmeldeinformationen enthält, muss sichergestellt werden, dass sie nur vom richtigen Benutzer lesbar ist.

4.3.1 Genauere Beschreibung der Werte

Folgend werden die Werte der des Konfigurationsfile näher beschrieben, wie das bei diesem Service umgesetzt werden muss.

admin_server.listen_url

Um den Admin-Server ebenfalls über das Internet, und so für die Clients, zugänglich zu machen, muss der Eintrag für admin_server.listen_url in [FixeIP_GoPhishVM]:3333 geändert werden.

admin_server.use_tls

Da die Installation pro Kunde immer neu erfolgt und in deren lokalen Netzwerk ist, wird dies in dieser Installation nicht benötigt.

admin_server.key_path & admin_server.cert_path

Wird dank der Versionen 0.3+ von GoPhish selber hinterlegt

admin_server.trusted_origins

Die Option phish_server.trusted_origins ermöglicht es Adressen hinzuzufügen, von denen eingehende Verbindungen erwartet werden. Dies ist hilfreich in Fällen, in denen die TLS-Terminierung durch einen Lastenausgleich oberhalb der Anwendung, anstatt durch die Anwendung selbst, gehandhabt wird. Da die Installation pro Kunde immer neu erfolgt und in deren lokalen Netzwerk ist, wird dies in dieser Installation nicht benötigt.

phish_server.listen_url

Diese Einstellung dient dem Klickratenreport. Dieser hört sich die Verbindungen auf die gegebene IP-Adresse an und schreibt so die Klicks, welche er durch die Email und Emaillinks aufgenommen hat für das Reporting in die unten beschriebene Datenbank.

4.3.2 SSL Zertifikate

GoPhish erstellt ab Version 0.3 Self-Signed Zertifikate. Diese werden in den korrekten Pfaden hinterlegt

4.3.3 SQLLite

SQLLite wird als Standarddatenbank von GoPhish gerade mitgeliefert. Die Datenbank speichert die Templates, sowie jede Klickverfolgung mittels Kampagnen- und UserID und dient so ebenso als Reportingquelle. Zielseiten werden in der Datenbank gespeichert. Gophish generiert eine einzigartige ID (den sogenannten rid-Parameter) für jeden Empfänger in einer Kampagne und verwendet diese ID, um die korrekte Zielseite dynamisch zu laden.

Das direkte Durchsuchen zum Gophish-Listener ohne Angabe eines rid-Parameters führt zur Anzeige einer generischen 404-Seite.

4.4 Kampagnen

Die Kampagne ist das Herzstück von GoPhish. Im FPM-Service werden drei Kampagnen angeboten, je nach erkennbarkeitslevel von dem FPM. Diese sind im Kapitel 5. Genauer definiert.

Die Kampagne dient als zentrales Werkzeug von GoPhish, mit welchen die Fake-Attacken gestartet werden. In der Kampagne fliessen alle zuvor definierten (weiter unten beschrieben in diesem Kapitel) zusammen.

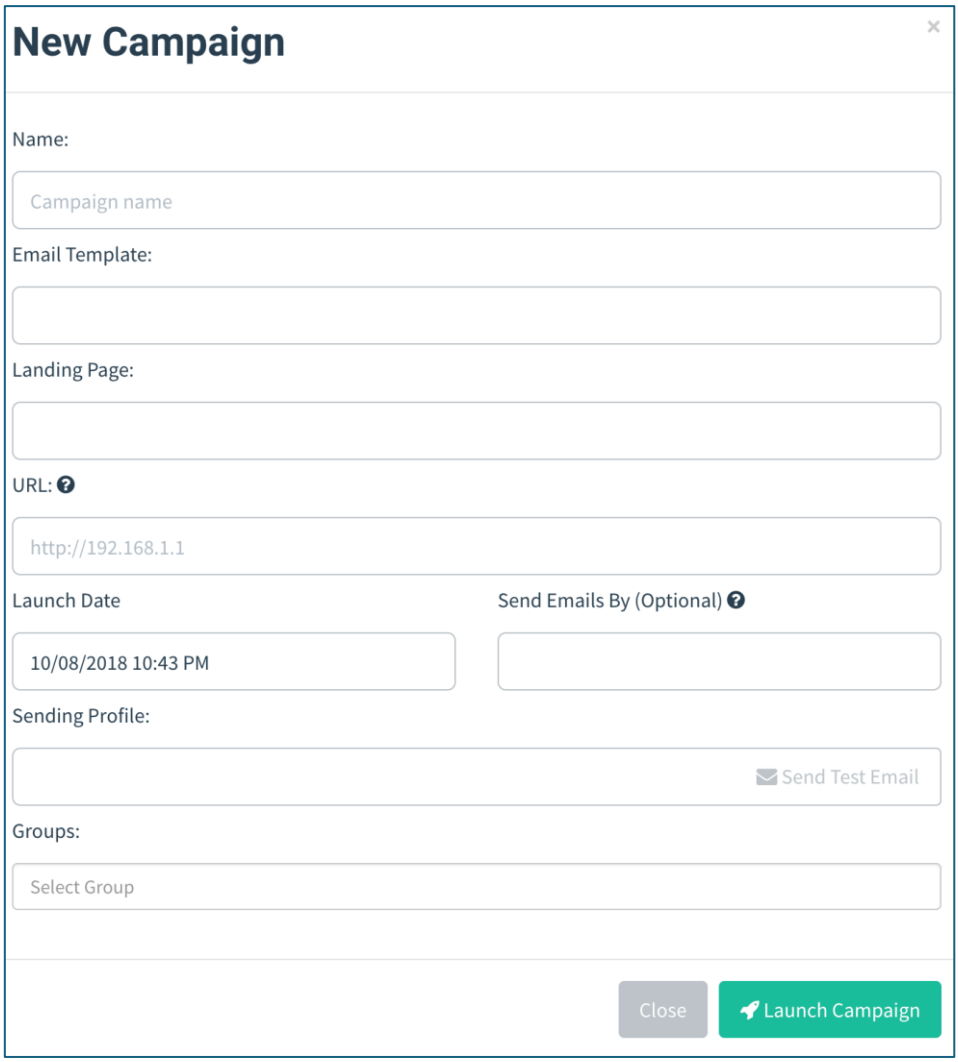

Abbildung 5 - GoPhish Kampagne (Bild aus Testinstallation)

In der Kampagne werden die im Kapitel 4.5 – 4.7 Konfigurationen hinterlegt.

Launchdate & Send Emails by (optional)

Dank der *Launchdate & Send Emails by (optional)* kann die Planung einer Kampagne im Voraus konfiguriert werden. Dabei gibt es zwei wichtige Felder zu beachten: das Startdatum und das Datum, bis zu dem die E-Mails versendet werden sollen.

Das Startdatum ist der Zeitpunkt, zu dem Gophish mit dem Versenden von E-Mails beginnen soll. Das SendEmailsBy der Endzeitpunkt. GoPhish sendet die Emails dann verteilt im Zeitraum der Kampagne.

SendingProfile (Kundeninfos)

Das SendigProfile, also die Absender SMTP Adresse über welchen die FPM's versendet werden, sind dem Kundeninfoblatt zu entnehmen. Dies wird so konzeptioniert, sodass möglichst viele SPAM-Filter umgehen werden können.

Um E-Mails zu versenden, muss in Gophish SMTP-Relay-Daten konfiguriert werden, die als "Sende-Profile" bezeichnet werden. Diese werden beim OnBoarding des Kunden via Kundeninfoblatt abgeholt.

Es ist wichtig sicherzustellen, dass die "Von"-Adresse ein gültiges E-Mail-Adressformat hat.

Das Sending-Profile wird einmalig eingerichtet.

Send to Groups

Die sendingGroups definiert auch, welche Gruppen von Empfängern in die Kampagne einbezogen werden sollen. Definition Users & Groups. Siehe dazu die Konfigurationskonzepte im Kapitel 5.

4.5 User & Groups

In diesem Konfigurationsschritt können die Mitarbeiteremails angegeben werden. Diese können per CSV als Bulk-Import hochgeladen werden. GoPhish bietet dazu eine CSV-Vorlage an. Die Kundenfirma muss dieses CSV liefern, wie im Kundeninfoblatt beschrieben.

Dank der *„Launchdate & Send Emails by (optional)“* konfigurationsmöglichkeit der Kampagne, müssen die Emails nicht Gruppiert werden, auch da die FPM nicht nach Mitarbeitergruppen/Rollen verteilt werden, sondern allgemeiner Natur gehalten werden.

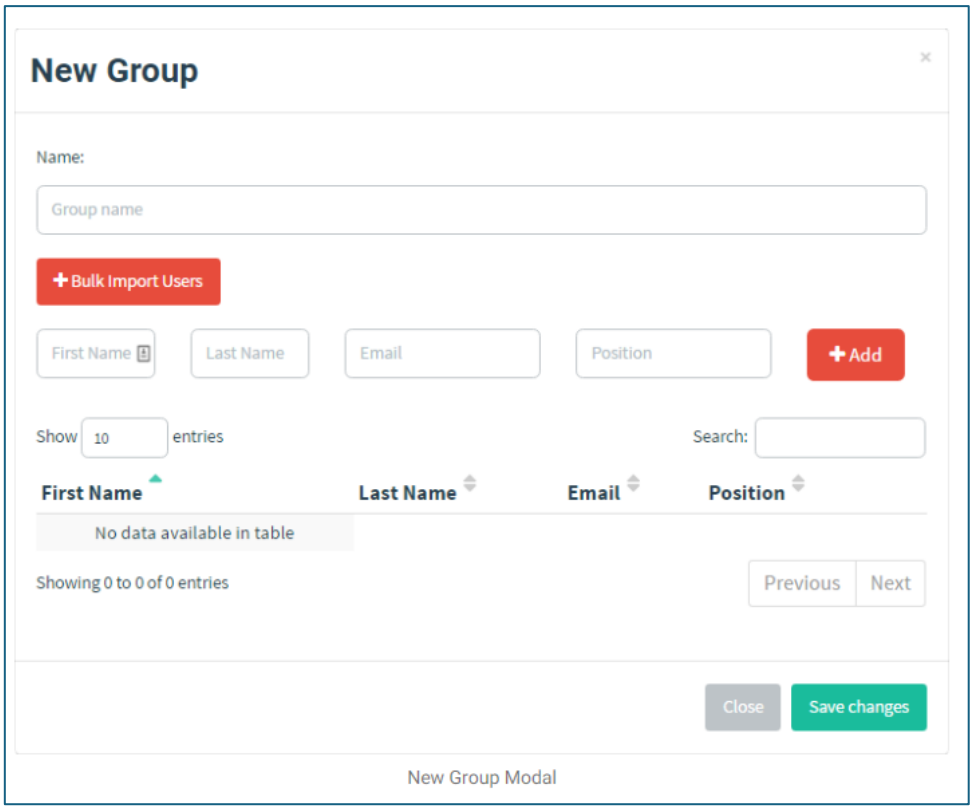

Abbildung 6 - User&Gruppenimport GoPhish (Screenshot aus Testinstallation)

Zur Konfiguration dient die oben abgebildetes GUI.

4.6 Email-Templates

Die Email-Templates sind die wirklichen Fake-Phishing Mails. Wie die aussehen und konfiguriert werden, wird im Kapitel 5 beschreibend erklärt.

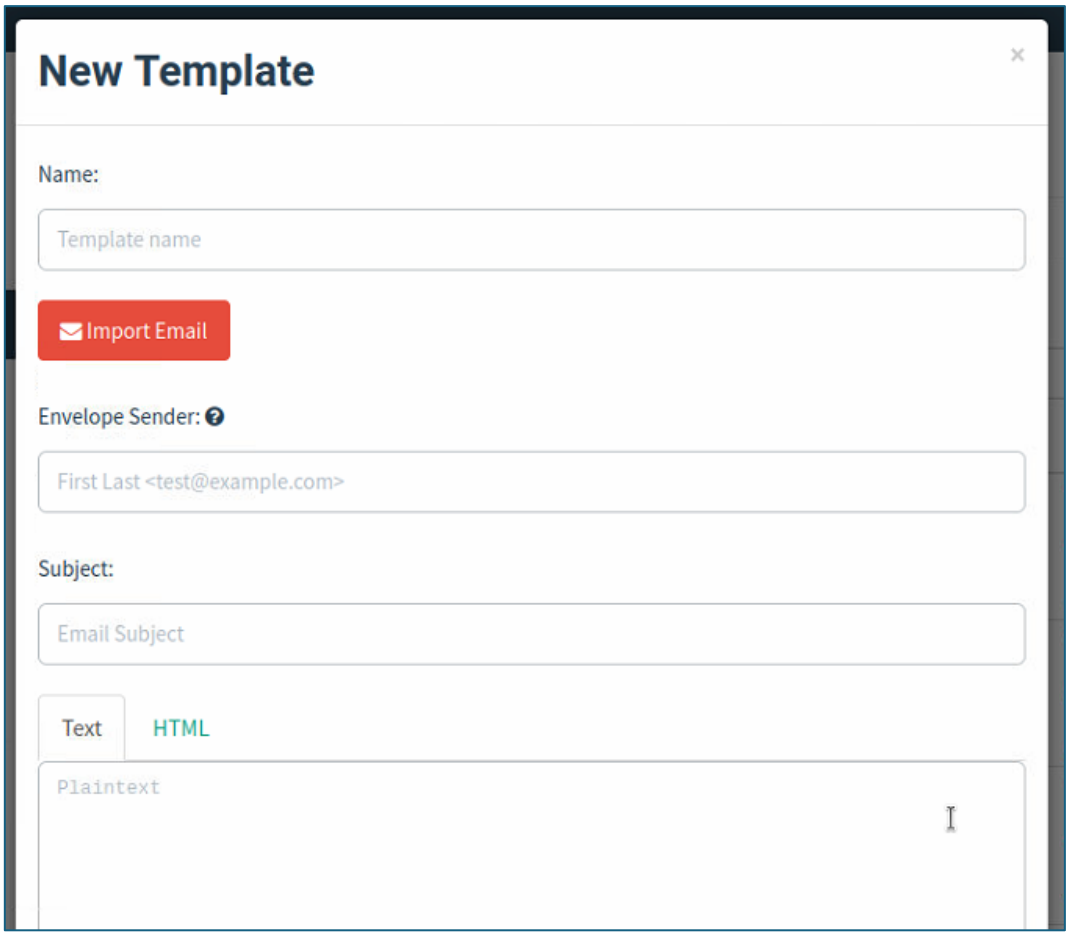

Abbildung 7 - EmailTemplate FPM GoPhish (Screenshot aus Testinstallation)

Da GoPhish wirklich ein sehr Userfreundliches Programm ist, kann direkt eine Email importiert werden. Diese werden im Kapitel 5 definiert. Damit der Link in der FPM zur richtigen Loginpage – sowie zur Klickratenverfolgung dient – muss als Link der Parameter {{.URL}} eingegeben werden. Diese werden durch den RID-Wert für die Klickratenverfolgung je User und Landingpage gespeichert.

Wichtiger Punkt ist der Envelope-Sender, hier kann die Absenderadresse welche für den Empfänger zu sehen ist, eingegeben werden. Wie diese Templates aussehen werden, wird im Kapitel 5 definiert.

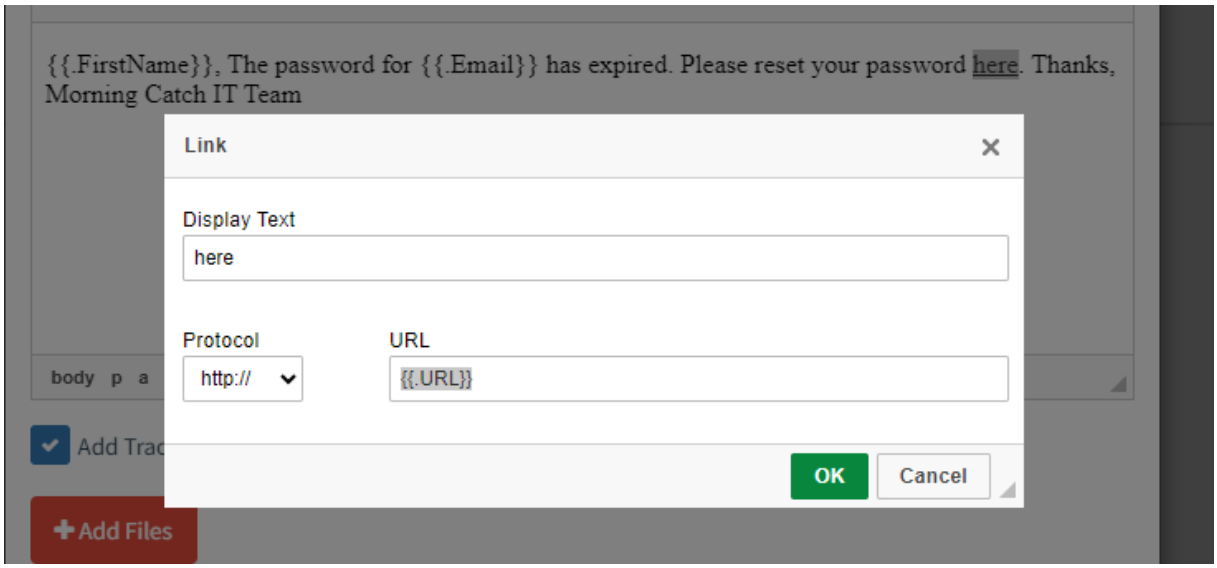

Abbildung 8 - URL Eingabe in MailTemplate

Ausserdem wird hier die Klickratenverfolgung definiert – dank dem Platzhalter im Link.

{{.URL}} definiert mithilfe der Datenbank und dem darin pro User zugewiesenen RID-Parameter die LandingPage (welche in der Kampagne miteinander „verknüpft“ werden). Damit wird die Klickratenverfolgung abgedeckt. Wie das genau funktioniert ist im Kapitel 4.8 beschrieben.

4.7 Landing-Pages

Die Landing-Pages dienen für das Credential-Phishing der User, um zu sehen, ob diese Ihre Daten in einem Fremden Link eingegeben werden. Jeder Klick auf diese LandingPages werden in der Datenbank gespeichert. Landingpages werden in der Datenbank gespeichert. Gophish generiert für jeden Empfänger in einer Kampagne eine eindeutige ID (genannt der rid-Parameter) und verwendet diese ID, um die richtige Landingpage dynamisch zu laden. Wenn direkt zum Gophish-Listener gebrowst wird, ohne einen rid-Parameter anzugeben, wird eine generische 404-Seite angezeigt. Wie das genau funktioniert ist im Kapitel 4.8 beschrieben.

Landingpages sind die tatsächlichen HTML-Seiten, die Benutzern zurückgegeben werden, wenn sie auf die Phishing-Links klicken, die sie erhalten.

Landingpages unterstützen Vorlagen, das Erfassen von Anmeldeinformationen und die Weiterleitung von Benutzern auf eine andere Website, nachdem sie ihre Anmeldeinformationen eingereicht haben.

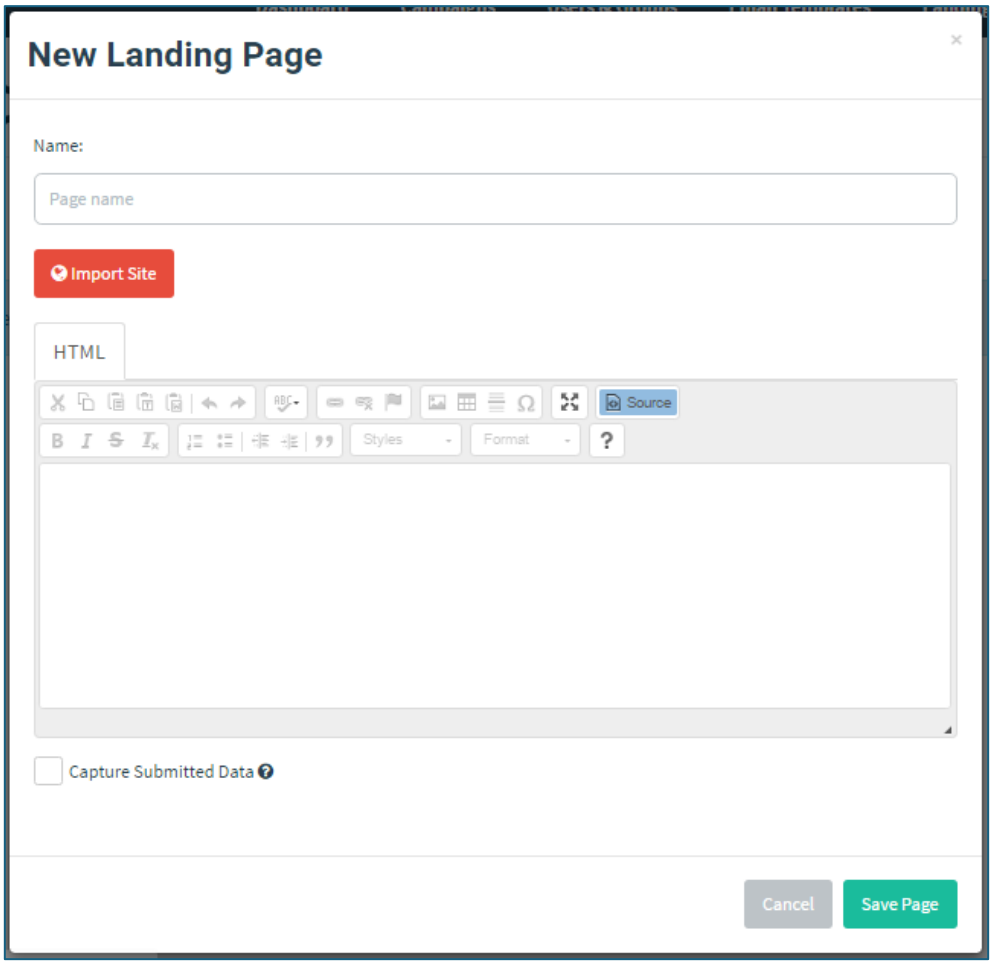

Abbildung 9 - LandingPage FPL GoPhish (Screenshot aus Testinstallation)

Ebenso wie bei dem EmailTemplate, kann hier eine ganze Seite detailgetreu importiert werden. Die Konfiguration dieser wird im Kapitel 5 erläutert.

Gophish erleichtert die Weiterleitung von Benutzern, nachdem sie Anmeldeinformationen eingereicht haben. Um Benutzer umzuleiten, wird die URL zu CAT in das Textfeld "Weiterleiten nach:" eingegeben, das nach Auswahl des Kontrollkästchens "Capture Submitted Data" angezeigt wird. Ebenso dient dies für die Klickratenverfolgung und der spätere Report. Mehr dazu im Kapitel 4.8

4.8 Sending Profiles

Die Sending Profiles dienen als SMTP-Sender. Jeder Emailausgang aus GoPhish wird über diese Verbindung gehen. Dank der Internen SMTP Anbindung beim Kunden, sollte auch der SPAM-Filter umgangen werden, sodass alle Emails ankommen sollten.

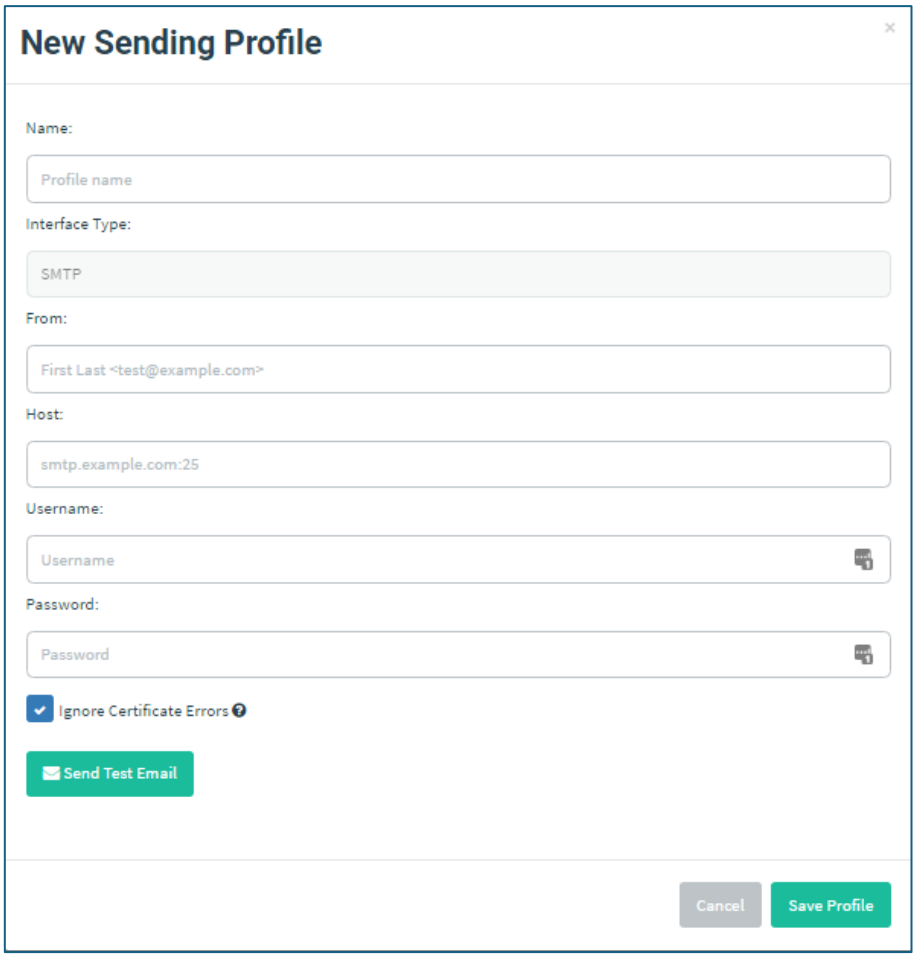

Abbildung 10 - Sending-Profile SMTP-Informationen (Screenshot aus Testinstallation)

Hier werden die Angaben des SMTP des Kundes verwendet, welche mit dem Kundeninfoblatt abgeholt werden.

Abbildung 11 - SendingProfile EmailHeaders

Neu wurden von GoPhish ebenso EmailHeaders definiert, die wie in den Email-Template zu sehende {{.URL}} definiert wird, für die Klickratenverfolgung. Mehr dazu im folgenden Kapitel 4.8.

4.9 Listener / Klickratenverfolgung

Folgend wird erläutert, wie die Klickratenverfolgung funktioniert.

LandingPage:

Jeder Klick auf diese LandingPages werden in der Datenbank gespeichert. Landingpages werden in der Datenbank gespeichert. Gophish generiert für jeden Empfänger in einer Kampagne eine eindeutige ID (genannt der rid-Parameter) und verwendet diese ID, um die richtige Landingpage dynamisch zu laden. Wenn direkt zum Gophish-Listener gebrowst wird, ohne einen rid-Parameter anzugeben, wird eine generische 404-Seite angezeigt.

"Capture Submitted Data" dient ebenso für die Klickratenverfolgung und der spätere Report.

Emailtemplate:

{{.URL}} definiert mithilfe der Datenbank und dem darin pro User zugewiesenen RID-Parameter die LandingPage (welche in der Kampagne miteinander „verknüpft“ werden). Damit wird die Klickratenverfolgung abgedeckt.

Sending-Profiles EmailHeaders:

Neu wurden von GoPhish ebenso EmailHeaders definiert, die wie in den Email-Template zu sehende {{.URL}} definiert wird, für die Klickratenverfolgung.

4.10 Die Zusammenhänge der Kampagne

In der folgenden Grafik wird erläutert, welches Template wo in der Emailkampagne greift.

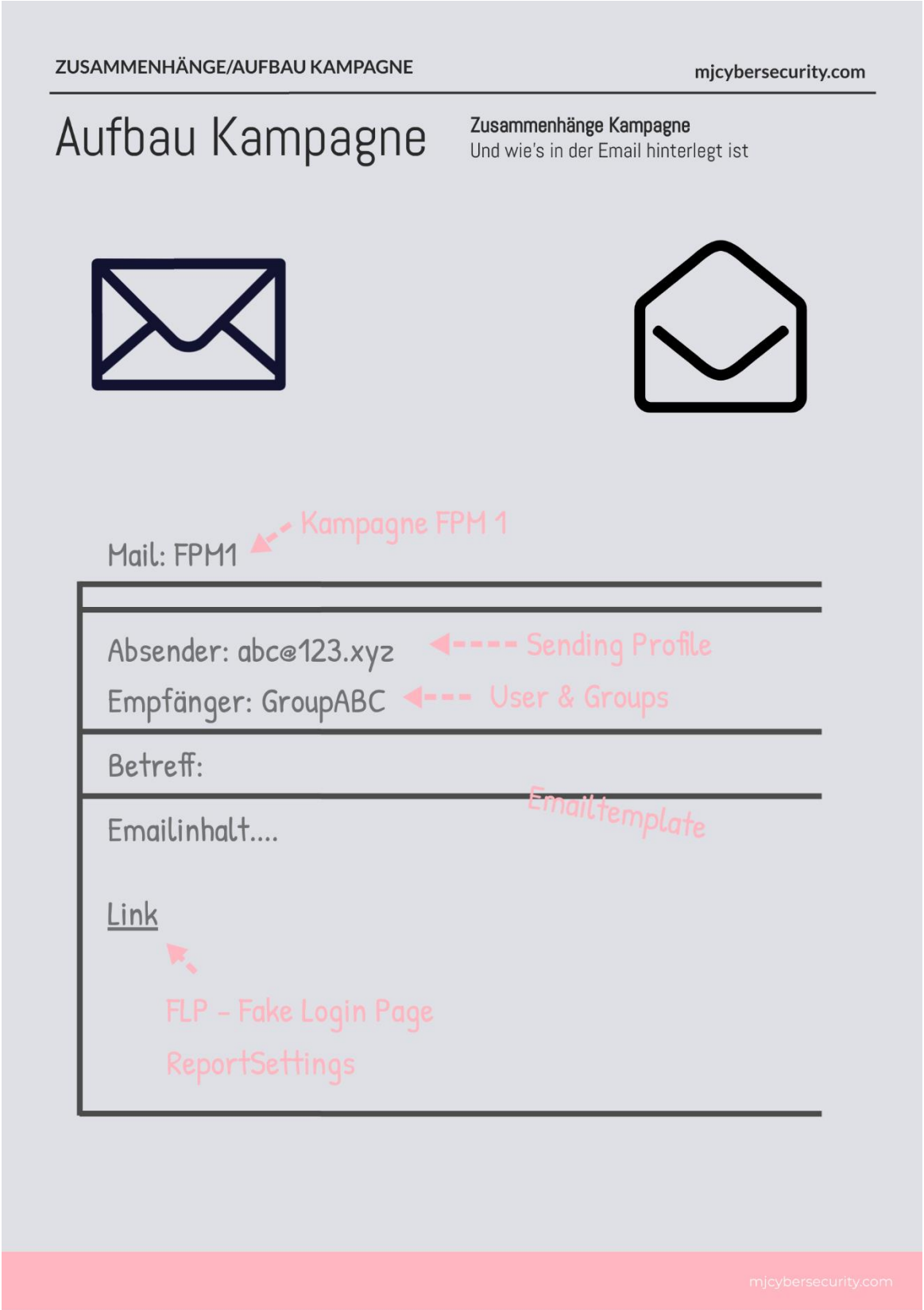

Abbildung 12 - Zusammenhänge Aufbau Kampagne

5. Definition FPM & FPL 1 easy – 2 medium - 3 hard (Kampagnen)

In diesem Dokument werden die spezifischen Definitionen für die Anforderungen der FPM und FPL definiert.

Diese werden für den erwähnten Pilotkunden B&T AG definiert.

Folgende Konfigurationen müssen getätigt werden:

- ***Drei Email Templates***
    - *Das Auffällige – level easy*
    - *Der Klassiker – level medium*
    - *Das gut Social-Engineerte – level hard*
- **Drei dazu passende Landing-Pages**
- **Drei dazu passende Email-Templates**
- **Die drei Kampagnen und die Definition der Sendezeiträume**

Zudem wird für jede Kampagne eine Emailvorlage definiert, falls ein Mitarbeiter das Fake erkennt und der IT meldet.

Folgend wird graphisch dargestellt, welche Templates wo beim FPM greifen:

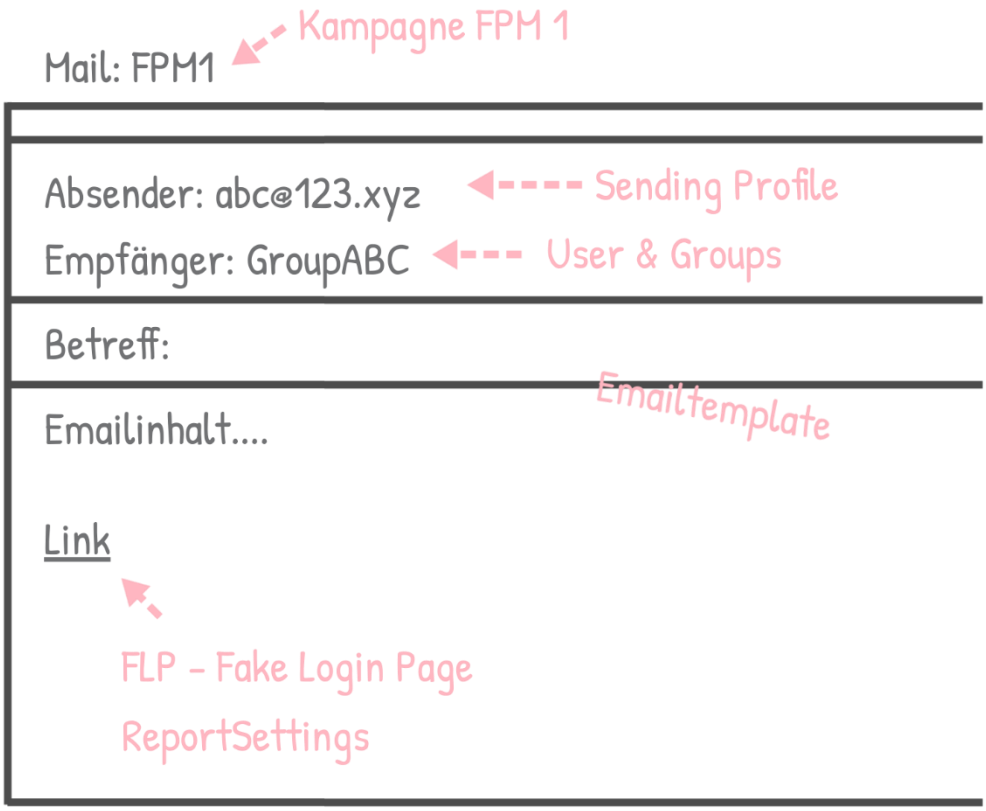

Abbildung 13 - Zusammenhänge Templates & Kampagne

5.1 Definition FPM, FPL - level easy – Das Auffällige

Die erste FPM welche die Mitarbeiter der Pilotkunden erhalten werden, sollten einfach zu halten und sehr leicht erkennbar sein. Folgend sind die Konfigurationen für die Kampagne der FPM «level easy» definiert.

5.1.1 Idee Galaxus-Gutschein

Level Easy - Das Auffällige

Die erste FPM sollte möglichst einfach gehalten, und sehr leicht erkennbar sein. Die Idee ist, dass ein Fake-Geschenkgutschein von Galaxus für die Treue der Firma und deren Mitarbeiter angeboten wird. Die Auffälligsten Merkmale wie das sofort handeln, die Fehler in der Rechtschreibung, sowie die Auffällige IP-Adresse der Landingpage und ein komischer Absender, sollten berücksichtigt werden.

5.1.2 Email-Template

In der folgenden Tabelle sind die Konfigurationen für das FPM-Template level easy definiert:

Level easy – «Das Auffällige»	
Name	FPM_Level_Easy
Envelope Sender	hallo@gls123.ch
Subject	Ein grosses Merci!
Emailtext	Hallo! Erstmals danke für Deine Treue!! Du hast nun 5 Stunden Zeit Dein Geschenkgutschein zu Einlösung! Klicke auf den Link und melde Dich an um Dir den Gutschein zu sichern! Du hast nur 5 Stunden Zeit! Klicke hier! -> Verlinken mit: {{.URL}} Wir hoffen sehr auf weitere treue von Dir! Galaxus Team
Vorlage Email	[Aktuelle Email suchen]
Anpassung Link	{{.URL}}

Tabelle 3 - Level easy – «Das Auffällige» EmailTemplate Page Konfiguration

5.1.3 Landing-Page

Die Landing-Page wird das Login von Galaxus.ch. Folgende Parameter müssen konfiguriert werden.

Level easy – «Das Auffällige»	
Name	FPL_Level_Easy
Import Site Template Link	Galaxus Login (digitecgalaxus.ch)
Capturing Submitted Data	Yes
Weiterleiten nach	https://www.mjcybersecurity.com/OOPSIE

Tabelle 4 - Level easy – «Das Auffällige» Landing Page Konfiguration

Gophish erleichtert die Weiterleitung von Benutzern, nachdem sie Anmeldeinformationen eingereicht haben. Um Benutzer umzuleiten, wird die URL zu CAT in das Textfeld "Weiterleiten

nach:" eingegeben, das nach Auswahl des Kontrollkästchens "Capture Submitted Data" angezeigt wird.

5.1.4 Sending-Profile

Um E-Mails zu versenden, muss in Gophish SMTP-Relay-Daten konfiguriert werden, die als "Sende-Profile" bezeichnet werden. Diese werden beim OnBoarding des Kunden via Kundeninfoblatt abgeholt.

5.1.5 Kampagne

Folgende Parameter müssen für diese Kampagne übernommen werden:

Level easy «Der Auffällige»	
Name	Level_Easy
EmailTemplate	FPM_Level_Easy (Auswahl)
LandingPage	FPL_Level_Easy (Auswahl)
URL	http://[IP_vonGoPhishServer]
LaunchDate	[Datum Launch]
SendEmails By	[Datum EndeLaunch] (so werden die Emails in diesem Zeitraum verteilt gesendet) *Daten abhängig Sendezeiträume, werden in Realisierung/Vor Durchführung definiert*
SendingProfile	[SendingProfil] (Auswahl)
Groups	[EmailGruppe_All] (Auswahl)

Tabelle 5 - Level easy – «Das Auffälige» Kampagne Konfiguration

5.1.6 Antwort-Vorlage für Report an IT

Folgende Emailantwort kann als Vorlage genutzt werden wenn ein User die FPM reported. Um den persönlichen Draht zu den Usern zu behalten, bezw. Aufzubauen, werden die Emails persönlich versendet.

Liebe [Name]

Bravo! Das war eine Fake-Phishingmail test!

Merci vielmals fürs melden – du hast richtig reagiert. Wenn Du noch mehr Tipps, Tricks und Wissen zu Phishing-Mails und deren Geschichten und Impact, IT-Security am Arbeitsplatz aneignen möchtest oder lernen möchtest, wie Du der Arbeitgeber so gut wie möglich mithilfst zu schützen oder schon nur wissen möchtest, wieso SocialeEngineering zu erkennen so wichtig ist, bitte ich Dich doch am Folgenden dreiwwöchigen Kurs teilzunehmen!

Wie das geht ist hier beschrieben: (ja – hier darfst Du draufklicken (;)

KURS | MJCS (mjcybersecurity.com)

Danke!

5.1.7 Klickratenverfolgung

Email Report Settings dank dem {{.URL}} im EmailTemplate.

5.2 Definition FPM, FPL - level medium – Der Klassiker

In diesem Kapitel wird definiert, wie das FPM level Medium für den Piliotkunden B&T AG konfiguriert sein muss.

5.2.1 Idee “Abgelaufene o365 Anmeldung”

Level Medium - Der Klassiker

Die zweite FPM sollte ein wenig schwieriger erkennbar sein, deswegen wird in dieser Mail die o365 Neuanmeldung empfohlen. Hier wird das Erkennungsmerkmal die falsche/verdächtige URL und der verdächtige Absender sein. Die Schwierigkeit hier für die User wird sein, dass sie sich eventuell sicher fühlen, wenn sie direkt per Namen angesprochen werden.

5.2.2 Email-Template

In der folgenden Tabelle sind die Konfigurationen für das FPM-Template level medium definiert:

Level Medium – «Der Klassiker»	
TemplateName	FPM_Level_Medium
Envelope Sender	O365.anmeldungen@office.ch
Subject	Neuanmeldung bei O365 erforderlich!
Emailtext	Hallo [Vorname] → *Verlinken mit {{Name von User}}* Deine Anmeldung auf o365 muss erneuert werden. Bitte melde Dich mit folgendem Link wieder an: Neu Anmelden -> *Verlinken mit: {{.URL}}* Beste Grüsse Microsoft
Vorlage Email	[Aktuelle Email suchen]
Anpassung Link	{{.URL}}

Tabelle 6 - Level medium – «Der Klassiker» EmailTemplate Konfiguration

5.2.3 Landing-Page

Die Landing-Page wird das Login von Galaxus.ch.

Level Medium – «Der Klassiker»	
Templatename	FPL_Level_Medium
Import Site Template Link	Bei Ihrem Konto anmelden (microsoftonline.com)
Capturing Submitted Data	Yes
Weiterleiten nach	https://www.mjcybersecurity.com/OOPSIE

Tabelle 7 - Level Medium – «Der Klassiker» Landing Page Konfiguration

Gophish erleichtert die Weiterleitung von Benutzern, nachdem sie Anmeldeinformationen eingereicht haben. Um Benutzer umzuleiten, wird die URL zu CAT in das Textfeld "Weiterleiten nach:" eingegeben, das nach Auswahl des Kontrollkästchens "Capture Submitted Data" angezeigt wird.

5.2.4 Sending-Profile

Um E-Mails zu versenden, muss in Gophish SMTP-Relay-Daten konfiguriert werden, die als "Sende-Profile" bezeichnet werden. Diese werden beim OnBoarding des Kunden via Kundeninfoblatt abgeholt.

5.2.5 Kampagne

Folgend kann nun die Kampagne nach untenstehender Tabelle konfiguriert werden.

Level medium «Der Klassiker»	
Name	Level_Medium
EmailTemplate	FPM_Level_Medium (Auswahl)
LandingPage	FPL_Level_Medium (Auswahl)
URL	http://[IP_vonGoPhishServer]
LaunchDate	[Datum Launch]
SendEmails By	[Datum EndeLaunch] (so werden die Emails in diesem Zeitraum verteilt gesendet) *Daten abhängig Sendezeiträume, werden in Realisierung/Vor Durchführung definiert*
SendingProfile	[SendingProfil] (Auswahl)
Groups	[EmailGruppe_All] (Auswahl)

Tabelle 8 - Level medium – «Der Klassiker» Kampagne Konfiguration

5.2.6 Antowort-Vorlage für Report an IT

Folgende Emailantwort kann als Vorlage genutzt werden wenn ein User die FPM reported. Um den persönlichen Draht zu den Usern zu behalten, bezw. Aufzubauen, werden die Emails persönlich versendet.

Liebe [Name]

Bravo! Das war eine Fake-Phishingmail test!

Merci vielmals fürs melden – du hast richtig reagiert. Wenn Du noch mehr Tipps, Tricks und Wissen zu Phishing-Mails und deren Geschichten und Impact, IT-Security am Arbeitsplatz aneignen möchtest oder lernen möchtest, wie Du der Arbeitgeber so gut wie möglich mithilfst zu schützen oder schon nur wissen möchtest, wieso SocialeEngineering zu erkennen so wichtig ist, bitte ich Dich doch am Folgenden dreiwwöchigen Kurs teilzunehmen!

Wie das geht ist hier beschrieben: (ja – hier darfst Du draufklicken (;)

KURS | MJCS (mjcybersecurity.com)

Danke!

5.2.7 Klickratenverfolgung

Email Report Settings im EmailTemplate dank dem {{.URL}}

5.3 Definition FPM, FPL - level hard

Das level Hard FPL wird als «gut Social-Engineert» angeschaut. Es wird angenommen, dass der Attackierende weiss, dass ein neuer Shop eröffnet worden ist. Er gibt sich als Finanzleiter aus und wirbt als Dankeschön für die Mitarbeit einen Gutschein an.

5.3.1 Idee “Bugoutstore-Gutschein”

Level Hard - Das gut Social-Engineerte

Das letzte Email ist eher schwer zu erkennen, auch hier ist der reine Augenmerk bei der Domain der Landing-Page und bei der unschönen Signatur und der Emailadresse, welche nur der Original ähnelt. In diesem FPM wird ein gut Social-Engineertes Ereignis genützt. Die B&T AG hat vor kurzem einen zweiten, neuen Shop «Bugoutstore» eröffnet. In dieser FPM werden Gutscheine für den Bugoutstore als Dankeschön angepriesen.

5.3.2 Email-Template

In der folgenden Tabelle sind die Konfigurationen für das FPM-Template level hard definiert:

Level hard – «Das gut Social-Engineerte»	
Name	FPM_Level_Hard
Envelope Sender	Andreas.solllberger@btag.ch
Subject	Ein grosses Merci!
Emailtext	Hallo! Danke für Deine Mitarbeit! Wenn Du Dich auf der Seite hier anmeldest, bekommst Du einen CHF 50.- Rabatt auf Deine nächste Bestellung beim neu eröffneten Bugoutstore! Neu Anmelden -> *Verlinken mit: {{.URL}}* Beste Grüsse B&T AG
Import Email Vorlage Email	Emailvorlage B&T ➔ Signatur auf «unschön» ändern
Anpassung Link	{{.URL}}

Tabelle 9 - Level hard – «Das gut Social-Engineerte»EmailTemplate Konfiguration

5.3.3 Landing-Page

Level hard «Das gut Social-Engineerte»	
Templatename	FPL_level_hard
Import Site Template Link	Bug Out Store → *Anmeldeseite generieren lassen*
Capturing Submitted Data	Yes
Weiterleiten nach	https://www.mjcybersecurity.com/OOPSIE

Tabelle 10 - Level hard – «Das gut Social-Engineerte» Landing Page Konfiguration

Gophish erleichtert die Weiterleitung von Benutzern, nachdem sie Anmeldeinformationen eingereicht haben. Um Benutzer umzuleiten, wird die URL zu CAT in das Textfeld "Weiterleiten nach:" eingegeben, das nach Auswahl des Kontrollkästchens "Capture Submitted Data" angezeigt wird.

5.3.4 Sending-Profile

Um E-Mails zu versenden, muss in Gophish SMTP-Relay-Daten konfiguriert werden, die als "Sende-Profile" bezeichnet werden. Diese werden beim OnBoarding des Kunden via Kundeninfoblatt abgeholt.

5.3.5 Kampagne

Folgende Parameter können nun in der Kampage ausgefüllt werden.

Level medium «Der Klassiker»	
Name	Level_Hard
EmailTemplate	FPM_Level_Hard (Auswahl)
LandingPage	FPL_Level_Hard (Auswahl)
URL	http://[IP_vonGoPhishServer]
LaunchDate	[Datum Launch]
SendEmails By	[Datum EndeLaunch] (so werden die Emails in diesem Zeitraum verteilt gesendet) *Daten abhängig Sendezeiträume, werden in Realisierung/Vor Durchführung definiert*
SendingProfile	[SendingProfil] (Auswahl)
Groups	[EmailGruppe_All] (Auswahl)

Tabelle 11 - Level hard – «Das gut Social-Engineerte» Kampagnen Konfiguration

5.3.6 Antwort-Vorlage für Report an IT

Folgende Emailantwort kann als Vorlage genutzt werden wenn ein User die FPM reported. Um den persönlichen Draht zu den Usern zu behalten, bezw. Aufzubauen, werden die Emails persönlich versendet.

Liebe [Name]

Bravo! Das war eine Fake-Phishingmail test!

Merci vielmals fürs melden – du hast richtig reagiert. Wenn Du noch mehr Tipps, Tricks und Wissen zu Phishing-Mails und deren Geschichten und Impact, IT-Security am Arbeitsplatz aneignen möchtest oder lernen möchtest, wie Du der Arbeitgeber so gut wie möglich mithilfst zu schützen oder schon nur wissen möchtest, wieso SocialeEngineering zu erkennen so wichtig ist, bitte ich Dich doch am Folgenden dreiwwöchigen Kurs teilzunehmen!

Wie das geht ist hier beschrieben: (ja – hier darfst Du draufklicken (;)

KURS | MJCS (mjcybersecurity.com)

Danke!

5.3.7 Klickratenverfolgung

Email Report Settings im EmailTemplate dank dem {{.URL}}

6. Mehrkundenfähigkeit

Die Mehrkundenfähigkeit gestaltet sich hier anders als beim CAT-Services.

Datenschutz- und Echtheitstechnisch- sowie Einfacher und Wartbarer wird es bei jedem Kunden neu aufgebaut. Dazu wird noch eine Checkliste, siehe Kapitel 10, erstellt, was wann installiert werden muss und dient als Installationsgrundlage/Anleitung für den Aufbau bei einem neuen Kunden. Die Templates, welche nicht Firmenbezogen sind (beim Pilotkunden B&TAG also das level easy und level hard) werden separat exportiert und in einer Bibliothek gespeichert. Siehe Kapitel 7.1

Die Schätzung wird Installation und Konfiguration pro Neukunde – *Voraussetzung: Kundeninfoblatt vorhanden und verifiziert vom Kunden* – 6 Stunden beanspruchen.

Ein weiterer Vorteil dazu ist, dass der Server nach Fertigstellung des FPM-Services komplett abgebaut werden kann – ***und so Ressourcen und umweltschonend ist.***

6.1 Speichern von Templates und LandingPages

Die Templates (FPL und FPM) von level easy und medium werden exportiert und gesichert in einer Cloud gelagert, sodass diese – falls der Kunde dieselben Vorlagen wünscht – eine Bibliothek von Templates entsteht.

Nachteil: Emails, Websites etc sind sehr schnelllebig, aufpassen bei Wiederverwendung ob Websitenaussehen noch aktuell ist.

6.2 Integration beim Kunden / Integrationsprozess

Im folgenden Kapitel wird der Integrationsprozess von Anfang bis Abschluss vom FPM Service definiert.

6.2.1 Integrationsprozess

In der folgenden Grafik wird aufgezeigt, wie der Kunde mit MJCS die GoPhish-Umgebung aufbaut, die FPM-Kampagnen sendet, sowie der Abbau der GoPhish Umgebung aus Sicherheitsgründen.

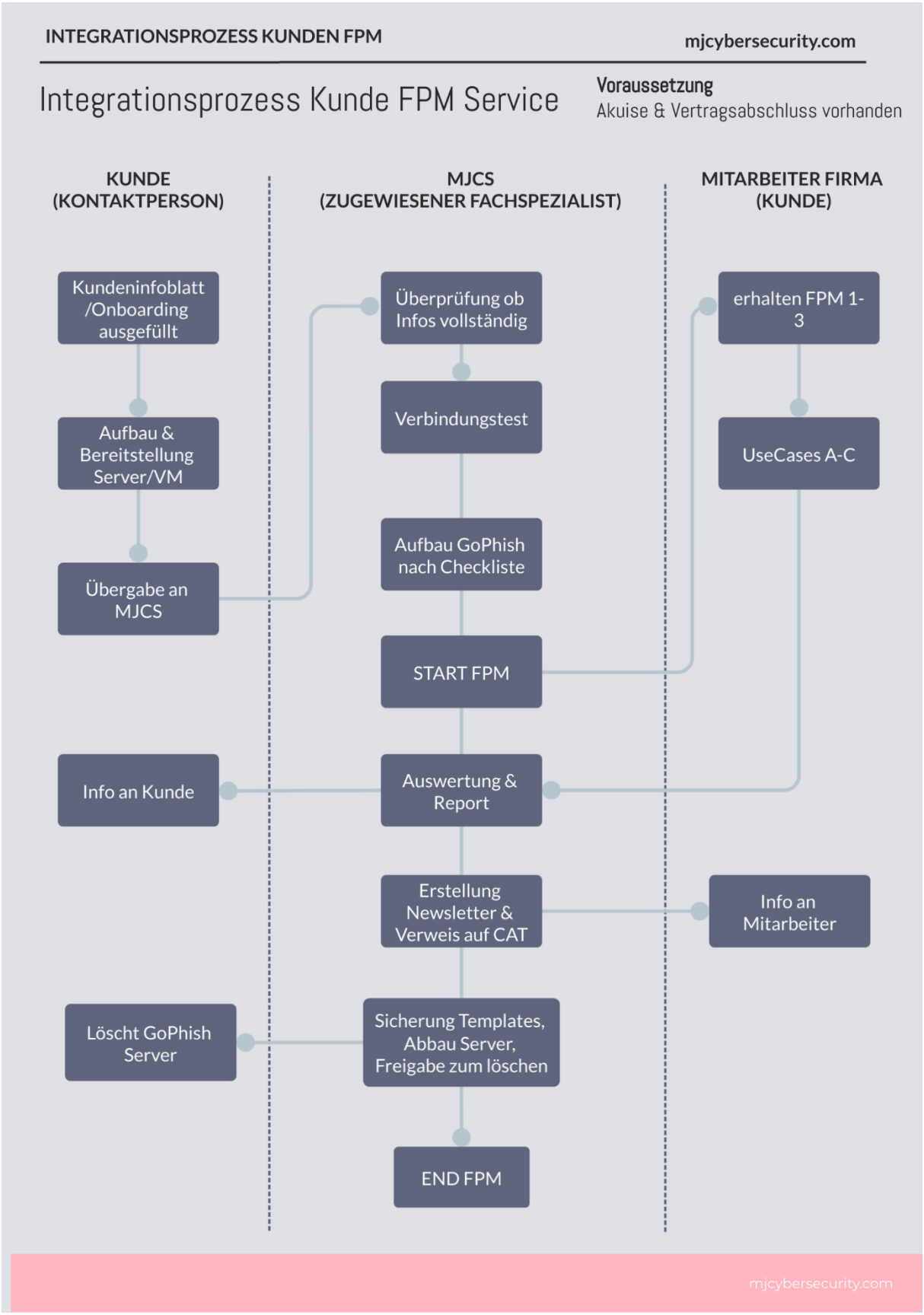

Abbildung 14 - Integrationsprozess Kunde

7. Reporting & Statistiken

Berichterstattung ist ein wichtiger Bestandteil jeder Gophish-Kampagne. Folgend wird der minimale Output für die GL und die Mitarbeiter der Firma deklariert.

Wenn eine Kampagne gestartet wurde, wird automatisch eine Ergebnisseite der Kampagne erstellt. Auf der Ergebnisseite sind Übersichtsinformationen zum Status der Kampagne sowie detaillierte Ergebnisse für jedes Ziel einzusehen.

Die Reporte können exportiert und für einen Newsletter verwendet werden.

Gophish erleichtert das Anzeigen der Kampagnenergebnisse in einem Zeitachsenformat.

Im Ergebnisbereich wird angezeigt, was ein Kampagnenempfänger getan hat, wie das Öffnen der E-Mail, das Klicken auf den Link oder der Versuch, Daten von der Landingpage zu übermitteln.

Gophish zeichnet auch Informationen über das Gerät auf, das den Link geklickt oder Daten übermittelt hat. Diese Daten werden aus der Benutzer-Agent-Zeichenfolge des Browsers analysiert. Das Betriebssystem und die Browser-Version werden unterhalb der Ereignisdetails angezeigt.

7.1 Wie das Reporting Funktioniert

Jede von Gophish versendete E-Mail enthält einen Link, der auf die für die Kampagne konfigurierte Zielseite zeigt. Diese URL sieht wie folgt aus:

http://]phish_server]/?rid=1234567

Die Zusammenhänge werden im Kapitel 4.8 genauer erklärt.

7.2 Dashboard

Das Dashboard von Gophish bietet einen schnellen Überblick über die Ergebnisse einer bestimmten Kampagne. Neben der Anzeige der Ergebnisse im Dashboard gibt es die Möglichkeit, die Rohdaten aus Gophish zu in CSV zu exportieren. Diese CSV-Dateien können dann mit anderen Programmen wie Excel oder Google Sheets weiterverarbeitet werden.

7.2.1 Zusatz: GoReport

Falls Zeit ist, kann mit GoReport ein Report erstellt werden: GitHub - chrismaddalena/Goreport: A Python script to collect campaign data from Gophish and generate a report

Da jedoch GoPhish schon ein sehr gutes Reporting hat, wird die verbliebene Zeit auf den CAT Service und dessen Kunden gelegt.

7.3 Überwachung während Service

Die Kampagnenresultate werden visuell in GoPhish dargestellt, jedes Email wird angezeigt und es wird Minutengenau folgendes getrackt:

- Email gesendet
- Email geöffnet
- Link angeklickt / interagiert mit Email
- Eingabe Credentials auf Fake Login Page (Passwortspeicherung wird nicht ausgewählt!)

Um die Kundenbindung, sowie der Aha-Effekt für die Mitarbeiter zu stärken, wird die Kampagne manuell Täglich überprüft. Durch die Graphishe Oberfläche für die Kampagnenüberprüfung in der Admin-Konsole (WebGUI) werden die Mitarbeiter, welche mit der Email interagiert haben, mit den zuvor definierten Antwortemails auf Ihren Fehler aufmerksam gemacht. Zudem wird er zu CAT weitergeleitet.

7.4 Newsletter und Report an Firma

Nach Beendung der Kampagnen wird der Firma einen Report zugestellt und den Mitarbeiter ein Newsletter mit den Ergebnissen. Der Report enthält diverse Facts über die verschiedenen Kampagnen, diese werden ebenso den Usern der Firma als Newsletter und Auflösung zugesendet.

7.4.1 Inhalt Report

Folgende Facts wird der Report enthalten

- Anzahl gesendete Emails
- Anzahl geöffneter Emails
- Anzahl geklickter Links
- Anzahl eingegebener Daten auf FakeLoginPage
- Gründe warum so wenig/so viel mit den Links interagiert wurde
- Reported Emails der Mitarbeiter
    - Anzahl Meldungen welche sich sicher waren dass es Phishing/SPAM ist
    - Anzahl Meldungen welche wegen Unsicherheit ob Phishing/SPAM die FPM reported hat
    - Anzahl direkt gelöschtren Mails

- Fazit

7.4.2 Inhalt Newsletter

Folgende Themen werden im Newsletter behandelt

- Aussehen der verschiedenen FPM's -> Was war auffällig? Wo waren die Unterschiede zu echten Emails?
- Auflösung des FPM Services
- Weiterleitung und Erklärungen zu CAT (Coupon, 15‘ pro Tag, etc)
- Fazit FPM Service

8. Kundeninformationsblatt

Das Kundeninformationsblatt enthält die Daten der Kunden, ohnewelche GoPhish nicht aufgebaut werden kann.

Dokument: *ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v1.pdf*

Dieses ist im *ID2132_StorrerJessica_FPM_Onboarding&Kundeninfos_v1.pdf* und wird zu Beginn des Services, direkt nach Vertragsabschluss, dem Kunden zur Ausfüllung vorgelegt.

Das Kundeninformationsblatt enthält die Infos für den Aufbau der VM/des Servers, sowie was der Kunde bereitstellen muss. Ein Clientzugang im Netzwerk des Kundens ist unerlässlich für Tests.

9. Checkliste Installation

Folgende Checkliste muss bei jedem Kunden abgearbeitet werden.

Dieses ist im Dokument *ID2132_StorrerJessica_FPM_ChecklisteInstallation_v1.pdf*

10. Datenschutzgesetz Konzept und Infos

Um es dem Kunden mit der Revision und dessen DSG-Gesetzes einfacher zu gestalten, ist im Anhang ein generisches Datenschutzkonzept für diesen Service definiert. Dieser kann angepasst und dem Kunden für Ihre Dokumentation abgelegt werden.

ID2132_StorrerJessica_FPM_Datenschutzkonzept_fuer_interne_Phishing_Tests_v1.pdf

11. Testkonzepte nach Anforderungen

Im folgenden Dokument können die Testkonzepte nach den Anforderungen des FPM-Services eingesehen werden.

ID2132_StorrerJessica_FPM_Testkonzept_v1.pdf

Das Testkonzept dient als Vorlage für die Tests und Testprotokolle in der Realisierung.

12. Pricing

Man beachte, dass hier noch der CAT einbegriffen wird.

Das Pricing wird pro Emailadresse verrechnet, welche die Firma testen will. Dazu gehören auch unpersönliche/shared Postfächer. Das FactSheet zeigt der lang währende Benefit für die Firmenkunden.

In der Realisierung wird das Pricing nochmals angeschaut, verglichen und eventuell abgeändert, um etwaige, unerwartete Änderungen berücksichtigen zu können.

12.1 Pricing FPM

Der folgende Dokumentationsteil beschäftigt sich mit den preislichen Aspekten des Firmenpostmanagements (FPM). Hierbei wird der Einbezug des CAT (Cost Allocation Tool) berücksichtigt, um eine transparente und gerechte Preisgestaltung zu gewährleisten.

12.1.1 Allgemeine Preisstrategie

Die erste Idee wäre: Das Pricing wird pro E-Mail-Adresse berechnet, die eine Firma testen möchte. Dies umfasst sowohl persönliche als auch unpersönliche/shared Postfächer.

Im Zuge der Umsetzung wird das Pricing einer detaillierten Prüfung unterzogen, um es gegebenenfalls anzupassen und unerwartete Veränderungen zu berücksichtigen. Die definitive Preisstrategie wird somit in der Realisierung getätigt.

Eine andere Preisstrategie ist eine Pauschale pro Emailadressenanzahl. Diese Strategie wird hier weiter verfolgt.

12.1.2 Preisstruktur Pauschale Lizenzmodell

Angenommen von einem Preis pro Emailadresse CHF 180.-

Als Pauschale werden Emailadressenanzahl in Bundels zusammengefasst und ein Mittelwert bis untere Mitte für ebendiese berechnet.

Dies würde folgendermassen aussehen:

- **Lizenzversion A** (2 - 20 Adressen): **CHF 3'400.-**

  Gewinn pro Kunde: CHF 200.-

- **Lizenzversion B** (21 - 55 Adressen): **CHF 6'200.-**

  Gewinn pro Kunde: CHF 3'000.-

- **Lizenzversion C** (56 - 110 Adressen): **CHF 14'000.-**

Gewinn pro Kunde: CHF 10'800.-

- **Lizenzversion D** (111 - 145 Adressen): **CHF 22'800.-**

  Gewinn pro Kunde: CHF 19'600.-

- **Lizenzversion E** (146 - 200 Adressen): **CHF 32'400.-**

  Gewinn pro Kunde: CHF 29'200.-

- Pauschale für Grossbetriebe ab 200+ Emailadressen auf Anfrage

Es muss beachtet werden, dass der CAT-Service (3 Woche eTraining) zu diesen Preisen dazugehört.

12.1.3 Wirtschaftliche Überlegungen / Break Even

Folgend werden die Wirtschaftlichen Überlegungen durch den Break Even berechnet.

BreakEven Analyse für das erste Jahr, die Projektkosten belaufen sich auf die Stunden der Realisierung des Fachspezialisten à CHF 160.-/Stunde. Der Stundensatz für das Onboarding und die Implementierung beträgt CHF 160.-. Für KMUs bis zu 200 E-Mail-Adressen wird eine geschätzte Zeit von 20 Stunden angesetzt, was Fixkosten von CHF 3'200.- entspricht.

Annahme erstes Jahr

Lizenzversion	Anzahl verkaufte Lizenzen (Kundennzahl)	Total Einnahmen in CHF	Fixkosten in CHF (Ausgaben Implementierung CHF3200.- * Anzahl verkauft)	Gewinn in CHF (Total Einnahmen - Fixkosten)
A	0	-	-	-
B	2	12‘400.-	6‘400.-	6‘000.-
C	4	56‘000.-	12‘800.-	43‘200.-
D	0	-	-	-
E	0	-	-	-
				49‘200.-

Tabelle 12 - BreakEven analyse im ersten Jahr im Lizenzmodell

Im zweiten und dritten Jahr werden Einnahmen und Fixkosten weiterhin auf Basis der verkauften Lizenzen und der durch CAT unbeeinflussten Kosten berechnet, um eine klare Sicht auf die Wirtschaftlichkeit zu gewährleisten.

Nachvollziehbarkeit:

*CHF 160.- Stundenansatz * Geschätzte Zeit Onboarding und Implementation Kunde (von der Installation bis zum Abschlussreport, KMU's bis 200 Emailadressen): 20h* = CHF 3'200.- Fixkosten

12.1.4 Fazit

Die Preise sehen auf den ersten Blick sehr hoch aus, es muss jedoch bedacht werden, dass pro User ein eTraining Cybersecurity Awareness Training CAT (3 Wochen) mit dabei ist, sowie drei FPM's und den Report und Newsletter, nebst zusätzlichen Digitale Downloads. Dank dem einfachen GoPhish Aufbau kann die Anzahl Stunden der Installation gering gehalten werden, und mit Erstellung Report- und Newsletter die geplanten Stunden nicht überschritten werden.

Literaturverzeichnis

https://docs.getgophish.com/user-guide

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