fake phishing mail service
&
cybersecurity awareness training

FPM

-REALISIERUNG & DURCH-FÜHRUNG-

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

Änderungsverzeichnis

Datum	Version	Änderung	Autor
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

Abbildungsverzeichnis

Tabellenverzeichnis

1. Marketing

Da der FPM-Service einen umfassenden Dienst zur Simulation von Phishing-Angriffen mit dem Ziel, die Cybersicherheitskompetenz der Mitarbeiter zu erhöhen und Unternehmen vor realen Bedrohungen zu schützen anbietet,

1.1 Zielgruppe

Unser primärer Fokus liegt auf mittelständischen bis grossen Unternehmen in Branchen, die häufig Ziel von Cyberangriffen sind, wie Finanzdienstleistungen, Gesundheitswesen und Regierungsbehörden.

1.2 Unique Selling Proposition (USP)

FPM ist personell, günstig und den Kundenwünschen erweiterbar. Aktuelle Fake-Mail Templates und personalisierbar. Regional, herzlich und integer.

1.3 Marketingkanäle:

Digitales Marketing – mjcybersecurity.com: Google Ads und SEO-optimierte Inhalte, die auf Keywords wie „Phishing-Simulation“, „Cybersicherheitstraining“ und „Mitarbeiterschulung für Sicherheit“ abzielen.

Social Media Marketing – @CAP_by_Je & @justjethings (reichweite): Regelmässige Beiträge und Anzeigen auf Plattformen wie Instagram, die auf IT-Sicherheitsleiter und Entscheidungsträger ausgerichtet sind.

E-Mail-Marketing: Versand von Informationsmaterial und Fallstudien an eine sorgfältig zusammengestellte Liste von Entscheidungsträgern in den Zielbranchen.

Per Post Marketing: Damit die potentiellen Kunden nicht schon in der ersten Email von mir auf einen Link klicken müssen, werden die Fact-Sheets und Werbe-Poster per Post an die potentiellen Firmenkunden versandt

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

Ausstellen in der Post-Filiale Uetendorf: Um möglichst noch mehr Kunden ansprechen zu können, werden die Poster/Fact Sheets für drei Wochen in der Postfiliale Uetendorf ausgestellt. Die Kosten dafür werden von MJ MOTORSPORT gesponsert.

1.4 Verkaufsstrategie

Für den FPM-Service wird ein fixer, einmaliger Betrag pro Emailadresse und FPM geplant.

Falls der Kunde mehr als ein FPM wünscht, werden diese zusätzlich – günstiger – verrechnet.

Anders als in der Realisierung wird hier nun pro Emailadresse gerechnet. Dies macht mehr sinn, da die Kosten nicht abschrecken und so mehr Kunden angesprochen werden können.

Beispiel:

Folgend sind die Kosten für eine Musterfirma mit 70 Emailadressen berechnet.

Kosten FPM *einmalig*

Beinhaltet

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

= CHF 24.80

Pro weiteres FPM **= CHF 11.20**

Kunde wünscht 3 FPM's für alle 70 Emailadressen:

70xCHF24.80 = CHF 1736.-

+

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

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

1.5 Kundenfeedback und Produktanpassung:

Regelmässige Kundenbefragungen zur Verbesserung des Services. Anpassung der Phishing-Szenarien basierend auf den neuesten Cyber-Bedrohungen und Feedback der Kunden.

Im Newsletter Mitarbeiter-Mood Abfragen durchführen.

1.6 Erfolgsmessung:

Kundenbindung: Analyse der Verlängerungsraten von Abonnements, um die langfristige Zufriedenheit und das Engagement der Kunden zu bewerten. Rezessionen preisgeben.

Mitarbeiterkompetenz/Reports: Vorher-Nachher-Analyse der Phishing-Erkennungsraten bei Mitarbeitern als direktes Mass für den Erfolg unserer Schulungen.

2. ROI

Folgend wird die ROI-Berechnung für den FPM-Service durchgeführt.

2.1 Kostenstruktur

Folgend sind die Kosten die mit der Implementierung des FPM-Services und dem laufenden Betrieb verbunden sind aufgezeit.

Anders als in der Realisierung wird hier nun pro Emailadresse gerechnet. Siehe Musterbeispiel aus Kapitel 1.4. Dies macht mehr sinn, da die Kosten nicht abschrecken und so mehr Kunden angesprochen werden können.

2.1.1 Aufwandskosten pro Kunde

Projektkosten

Personalkosten: 160 CHF/Stunde

Geplante Stunden: 240 Stunden

Gesamte Personalkosten: 38.400 CHF

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

2.1.2 Einnahmen Pro Kunde

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

CHF 3304.-

2.1.3 Berechnung ROI

Nun wird die ROI-Berechnung durchgeführt.

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

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

2.1.4 BreakEven

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

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

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

2.1.5 Schlussfolgerung

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

2.1.6 Massnahmen

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

3. MINI-BUSINESS CASE

Ein Mini-Business-Case für den FPM-Service wird hier aufgelistet.

3.1 Problemstellung

Trotz engagierter Bemühungen, das Bewusstsein der Mitarbeiter durch Newsletter und Sicherheitstipps zu schärfen, bleibt die Notwendigkeit akut, die Reaktionsfähigkeit auf Phishing-Angriffe signifikant zu verbessern. Viele Mitarbeiter erkennen nach wie vor nicht alle Phishing-Versuche rechtzeitig, was das Risiko für Sicherheitsverletzungen im Unternehmen erhöht.

3.2 Lösungsansatz

Um dieses Problem zu adressieren, schlagen wir die regelmässige Durchführung von realistischen Phishing-Tests vor. Diese Fake-Phishing-Mails (FPM) sind darauf ausgelegt, den Mitarbeitern praktische Erfahrungen im Erkennen und adäquaten Reagieren auf tatsächliche Bedrohungen zu vermitteln. Durch diese gezielten Simulationen werden die kritischen Fähigkeiten geschärft, die für die Erkennung und Abwehr von Cyberangriffen notwendig sind.

3.3 Kosten

Die Implementierung dieser Lösung beinhaltet verschiedene Kostenfaktoren:

Lizenzkosten für die Nutzung einer spezialisierten Phishing-Testplattform.

Aufwand für die Konfiguration und fortlaufende Verwaltung der Phishing-Tests.

Entwicklung und Durchführung von Schulungsmaterialien zur Unterstützung der Lernprozesse der Mitarbeiter.

3.4 Nutzen

Die Investition in solche Phishing-Tests bringt mehrere Vorteile mit sich:

Reduzierung der Sicherheitsvorfälle: Durch verbesserte Reaktionen der Mitarbeiter auf Phishing-Versuche wird die Anzahl erfolgreicher Cyberangriffe signifikant verringert.

Messbare Steigerung der Cybersecurity-Awareness: Die regelmässigen Tests ermöglichen eine kontinuierliche Bewertung und Stärkung des Sicherheitsbewusstseins im Unternehmen.

Verringerung potenzieller Kosten durch Cyber-Angriffe: Indem weniger Sicherheitsvorfälle auftreten, spart das Unternehmen erheblich bei den Ausgaben, die normalerweise für die Behebung von Sicherheitsverletzungen anfallen würden.

Empfehlung

Um ein anhaltend hohes Niveau an Cybersecurity-Awareness zu gewährleisten, empfehlen wir die kontinuierliche und regelmässige Wiederholung der Phishing-Tests. Dies fördert nicht nur die Wachsamkeit der Mitarbeiter, sondern passt auch die Schulungsmassnahmen an die sich ständig weiterentwickelnden Bedrohungen an. Die regelmässige Auffrischung des erworbenen Wissens ist entscheidend, um die Wirksamkeit der Cybersecurity-Massnahmen dauerhaft zu sichern.

4. FACT SHEET

Anbei das Fact Sheet für den Service FPM. Als WhitePaper für den Kunden mit allen Infos ist hier zu finden.

DOWNLOADS | MJCS (mjcybersecurity.com)

4.1 Kurze Beschreibung des Services

MJ Cybersecurity Services bietet ein innovatives Phishing-Awareness-Training an, das Unternehmen dabei unterstützt, die Reaktionsfähigkeit ihrer Mitarbeiter auf Phishing-Versuche zu verbessern. Durch den Einsatz von Fake-Phishing-Mails (FPM) werden Mitarbeiter geschult, betrügerische E-Mails effektiv zu erkennen und darauf zu reagieren, wodurch das Risiko von Sicherheitsverletzungen signifikant reduziert wird.

4.2 Zielgruppe

Der Service richtet sich an alle Unternehmen, die das Bewusstsein und die Sicherheitskompetenzen ihrer Mitarbeiter erhöhen möchten, insbesondere in Branchen mit hohem Risiko für Cyberangriffe.

4.3 Service-Eigenschaften

4.3.1 Verfügbarkeit

Geschäftszeiten von 08:00 Uhr bis 15:00 Uhr für FPM.

4.3.2 Service Level Agreements (SLAs)

99% Verfügbarkeit während der Geschäftszeiten.

Reaktionszeit von maximal 24 Stunden bei technischen Anfragen.

4.3.3 Sicherheitsmerkmale und Compliance

Einsatz von verschlüsselten Datenübertragungen.

Einhaltung von DSG für den Schutz persönlicher Daten.

4.3.4 Technische Details

Plattformen und Technologien

Verwendung der GoPhish-Plattform für die Durchführung von Phishing-Tests.

Integration

Nahtlose Integration mit Microsoft Exchange Online für den E-Mail-Versand.

4.3.5 Kundenanforderungen

Der Kunde stellt einen Server bereit, der die vorgegebenen Voraussetzungen (im Kundeninfoblatt vorhanden) erfüllt

Internetverbindung und Zugang zu internen Netzwerken.

MJ Cybersecurity übernimmt Installation und Konfiguration des Services.

4.3.6 Kosten und Preismodell

Kostenstruktur

- Einmalige Gebühr pro E-Mail-Adresse für FPM: CHF 24.80.
- Reduzierte Preise für zusätzliche FPMs: CHF 11.20.

Kosten FPM *einmalig*

Beinhaltet

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

= CHF 24.80

Pro weiteres FPM **= CHF 11.20**

Rabatte

Mengenrabatte für Bestellungen über 100 E-Mail-Adressen.

4.3.7 Support- und Kontaktinformationen

Verfügbarkeit

Support von 08:00 bis 15:00 Uhr für FPM und bis 18:00 Uhr für eTraining CAT.

Eskalationsprozeduren

Eskalation an die Inhaberin J. Storrer per E-Mail oder Telefon.

4.3.8 Nutzungsstatistiken und Performance-Indikatoren

Pilotprojekt

Das Pilotprojekt zeigt eine Steigerung der Phishing-Fallraten um 8% innerhalb der ersten sechs Monate vom ersten zum dritten FPM. Das Level Hard FPM wurde in 10% nicht als Phish erkannt und lernet somit dazu.
Lernrate = 100% derjenigen der geklickt haben

4.3.9 Zugriff und Berechtigungen

Informationen über den Zugang

Adminzugang ist exklusiv für MJ Cybersecurity und die IT-Abteilung des Kunden.

4.3.10 Implementierungs- und Migrationsdetails

Implementierungsschritte

Detaillierte Schritte sind dem Kundeninfoblatt zu Entnehmen.

Dokumentation der Schulungsressourcen

Alle Dokumentationen zu den Schulungsressourcen sind auf mjcybersecurity.com

Verfügbare Ressourcen

Umfangreiche Handbücher, Anleitungen und Online-Ressourcen auf mjcybersecurity.com.

Regelmässige Schulungen und Workshops, siehe Fact Sheet zum CAT-Service.

4.3.11 Zukünftige Entwicklungen und Updates

Updates

Quartalsweise Aktualisierung von E-Mail-Templates und Schulungskursen.

Anpassungen und Erweiterungen basierend auf Kundenfeedback.

Release-Zyklus

Server wird nach Durchführung dem Service abgebaut, alle Kundendaten gelöscht, nur der Kurs bleibt bestehen.

Abschluss

Nach jedem Training wird ein detaillierter Newsletter und ein genauer Report erstellt, um die Effektivität der Schulung zu messen um alle Mitarbeiter abzuholen um awareness zu schaffen.

4.4 Checkliste Installation

Anbei ist die Checkliste für die Installation. So kann gewährleistet werden, dass nichts vergessen gegangen wird.

ID2132_StorrerJessica_FPM_ChecklisteInstallation_v1.pdf

5. AUSFÜHRUNG // LÖSUNG

Nach erhlalt der Kundeninformationen kann mit dem Kunden ein Datum festgelegt werden für die Installation. Dafür empfiehlt sich 6h beim Kunden einzuplanen. Folgende wird der Aufbau, Installation und Konfiguration während der Ausführung – bauen der Lösung FPM Service - beim Pilotkunden B&T AG.

Nach Erhalt der Kundeninformationen wird ein Termin für die Installation festgelegt. Hierfür sollten etwa 6 Stunden beim Kunden eingeplant werden. Der Aufbau, die Installation und Konfiguration des FPM-Services erfolgen beim Pilotkunden B&T AG.

Die Installation wird nach der Checkliste Installation (Kapitel 4.4) – erarbeitet in der Konzeptphase – erledigt und in diesem Dokument ausdokumentiert.

6. Installation & Konfiguration Server „Ubuntu 22.04.4“

Eine VW wurde beim Pilotbetrieb aufgebaut und mit den Minimalanforderungen für Ubuntu Server 22.04.4 TLS. Anbindung per Trunk (Verbindung zu Clients und Internet möglich). Das Ubuntu wurde von der Offiziellen Ubuntu-Website gedownloadet. Für jede installation wird immer die neuste Version heruntergeladen.

Konfiguration Ubuntu

Adminuser wird aufgesetzt und eine fixe IP – nach Kundenblatt – wird vergeben.

6.1 Tests Verbindungen/open Ports

Mittels einem Client im selben Netzwerk wird versucht per Ping der eben erstellte Server zu erreichen.

7. Installation GoPhish

Für die Installation des GoPhish Servers wird wieder jedesmal die neue GoPhish-Version von GitHub heruntergeladen und mit Go Get installiert.

(Anleitung: Installation | Gophish User Guide (getgophish.com))

sudo apt install gccgo

go get github.com/gophish/gophish

Das File wird kompiliert und mit ./goPhish ausgeführt.

In der Ersten ausführung wird ein Admin-PW für den Admin-Zugang aufgezeigt.

Dieses muss bei der ersten Anmeldung auf der Admin-Oberfläche geändert werden.

Danach wird das Konfigurationsfile von GoPhish angepasst.

Folgend ein Bild der Beschreibung der verschiedenen einzutragenden Konfigurationsdaten.

Bemerkung: Onlineanleitung ist ein wenig veraltet, in der neuen GoPhish-Version werden die Zertifikate und Pfade selber erstellt und im Konfigurationsfile definiert.

Key	Value (Default)	Description
admin_server.listen_url	127.0.0.1:3333	IP/Port of gophish admin server
admin_server.use_tls	false	Use TLS for admin server?
admin_server.cert_path	example.crt	Path to SSL Cert
admin_server.key_path	example.key	Path to SSL Private Key
admin_server.trusted_origins	[]	Comma separated list of trusted origins
phish_server.listen_url	0.0.0.0:80	IP/Port of the phishing server - this is where landing pages are hosted.

Abbildung 1 - Konfigfile Description (old) from GetGoPhish.com

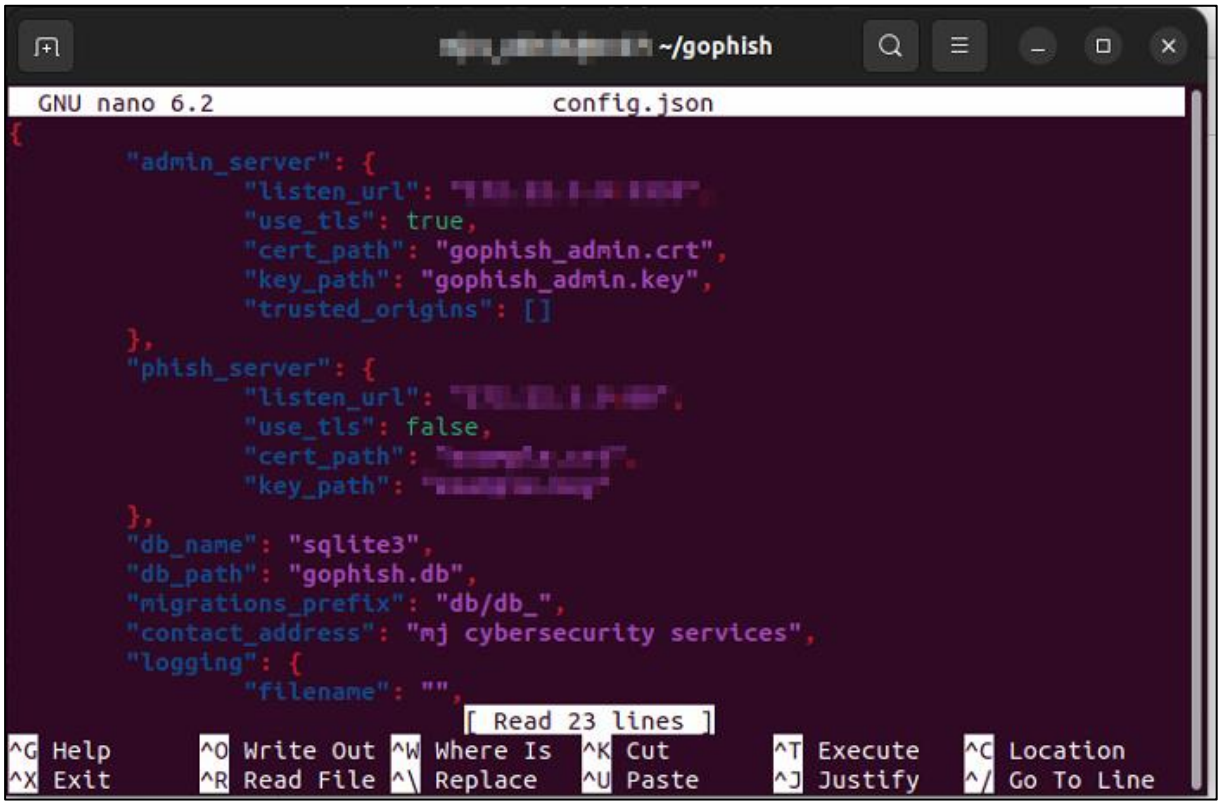


Abbildung 2 - ConfigurationFile GoPhish

7.1 Testen der Verbindungen

Da die Installtion und Konfiguration so einfach sind, kann nun mit dem Client via IP:3333 auf das Admin-Portal von GoPhish zugegriffen werden.

7.2 Übersicht

Auf der Untenstehenden Grafik wird die Systemübersicht von GoPhish beim Pilotkunden B&T AG dargestellt. Die Umgebung läuft auf einer Virtuellen Umgebung, welche hier aus Sicherheitsgründen nicht abgebildet werden kann. Dazu dient jedoch die Grafik untenstehend, welche ebenso verständlich genug sein wird.

Abgebildet wird der Sendeprozess des GoPhish Servers. In jeder FPM wird eine TrackingID hinterlegt, sowie der URL-Platzhalter. Ersteres dient dazu, ein DB Eintrag zu machen auf welcher User, Kampagne, FPM und FLP abgebildet werden. Mithilde des URL-Parameters kann das Tracking zum jeweiligen User nachverfolgt werden. Pro User wird ein RID-Eintrag in die Datenbank geschrieben, mit der Zugehörigen Kampagne, FPM und FPL zum jeweiligen User. So kann die TrackingID der geklickte Link verfolgen.

Um die zweiten beiden Emails authentischer zu gestalten, wurde auf dem Internen DNS der Firme – ein weiterer Vorteil einer internen Installation – zwei Zonen und A-Records erichtet, welche zum GoPhish Server zeigen. In den zwei letzten GoPhish Kampagnen werden dann statt die IP der GoPhish Maschine die jeweilige Fake-Domain hinterlegt.

Die Ports welche offen sein müssen sind 80/443 für die FakeLoginPages, 22 für SSH und 3333 für das AdminPortal.

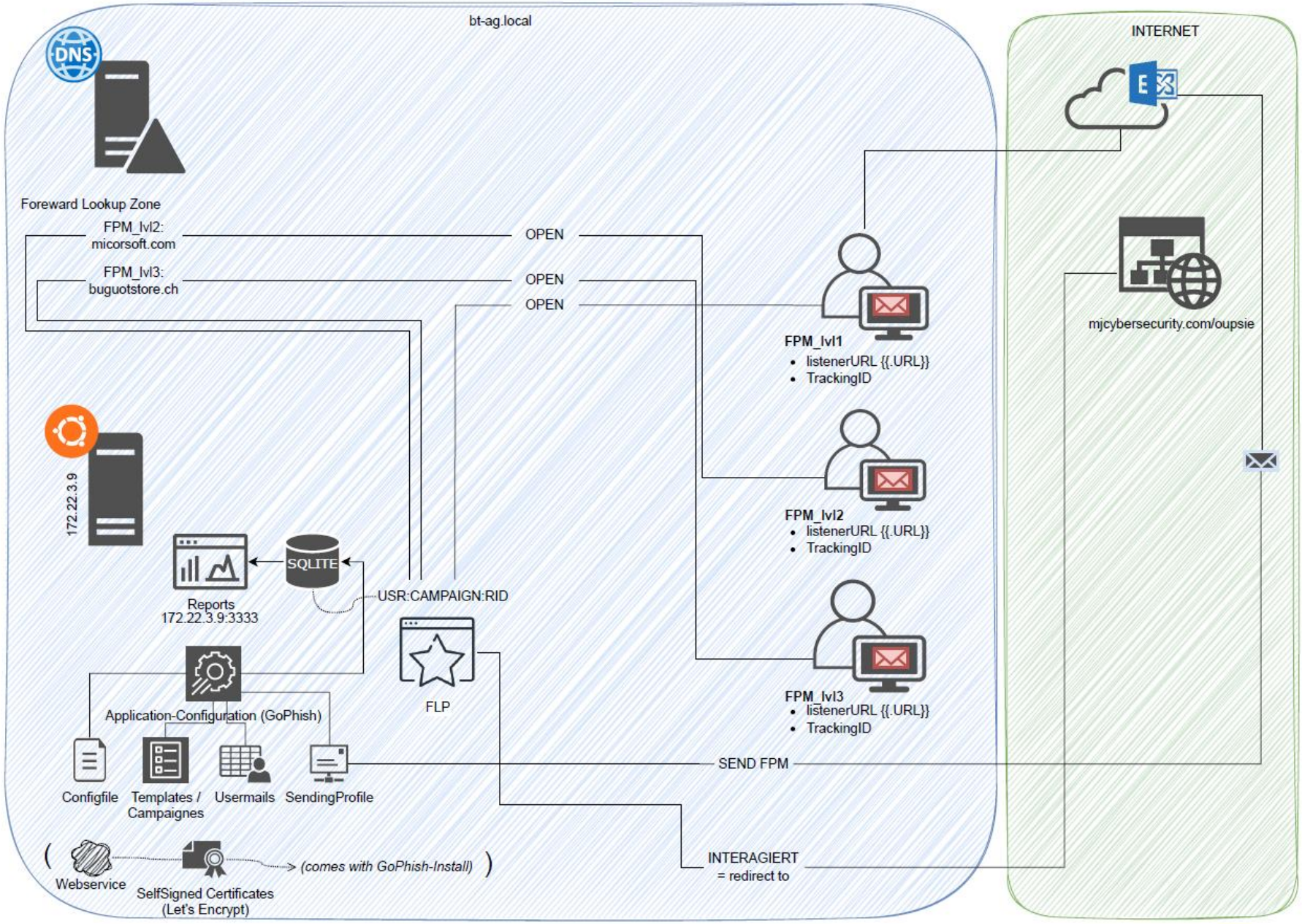
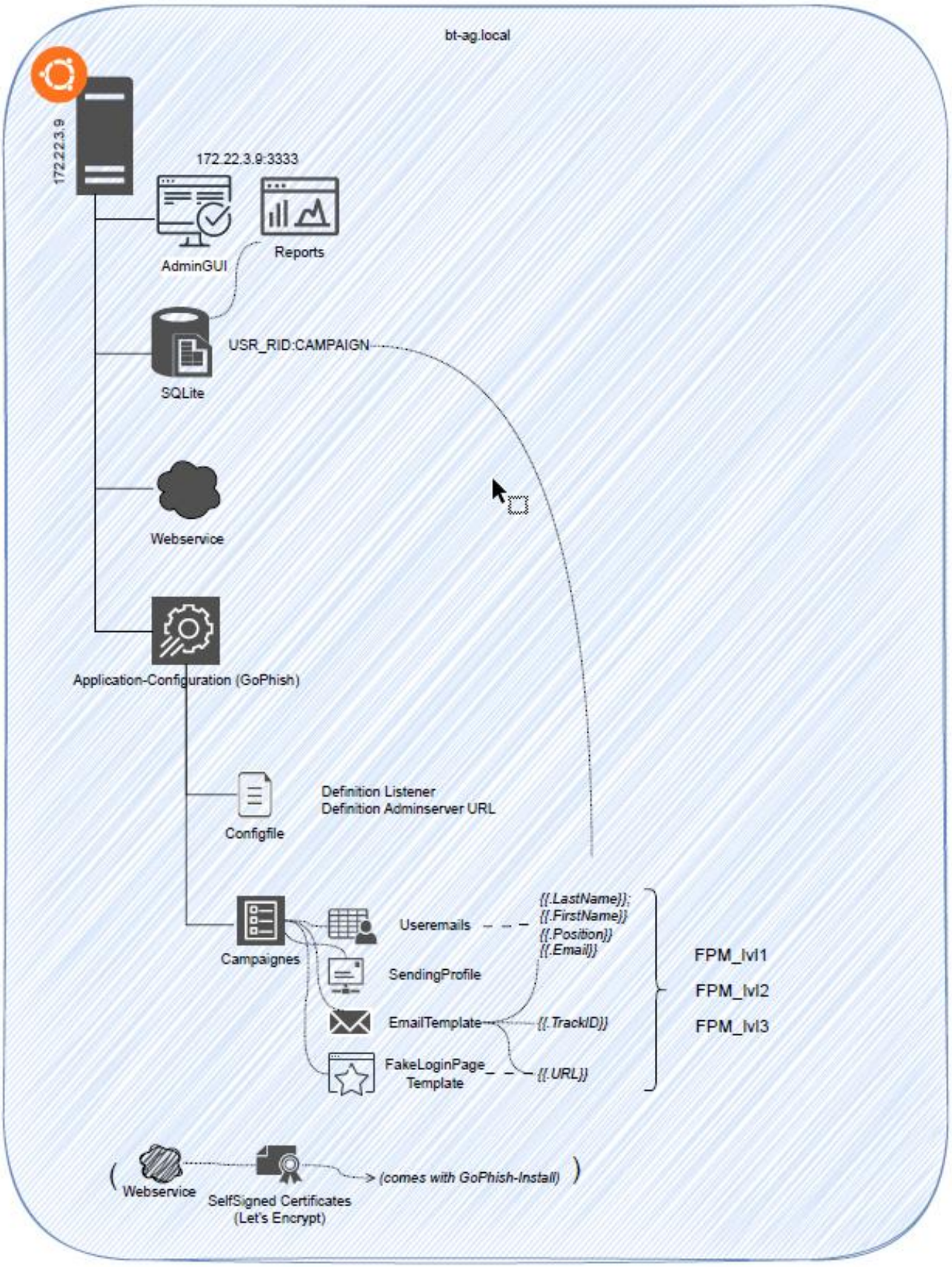

bt-ag.local
INTERNET
DNS
Foreward Lookup Zone
FPM_lvl2:
micorsoft.com
FPM_lvl3:
buguotstore.ch
OPEN
OPEN
OPEN
FPM_lvl1
• listenerURL {{.URL}}
• TrackingID
FPM_lvl2
• listenerURL {{.URL}}
• TrackingID
FPM_lvl3
• listenerURL {{.URL}}
• TrackingID
mjcybersecurity.com/oupsie
172.22.3.9
SQLITE
Reports
172.22.3.9:3333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

Abbildung 3 - Übersicht GoPhish in Kundenumgebung

Bei der Konfiguration verwendet Gophish üblicherweise den Port 3333 für die Admin-Schnittstelle. Dieser Port wird genutzt, um über einen Webbrowser auf das Gophish-Administrationspanel zuzugreifen. Der Port für den Phishing-Server, der in E-Mails für Links verwendet wird, ist hingegen standardmässig auf Port 80 eingestellt. Im Konfig-File wird der Listener definiert, welcher im normalfall die IP der GoPhish-Maschine ist und auf Port 80 oder 443 hört. Dies wird dann bei neustart des Services, odr des Servers, automatisch eingelesen und in die installation/konfiguration von GoPhish genommen.

Die in den Geschwungenen schleifen sind Parameter, welche in den FPM zur authentizität genutzt werden können. Diese sind abbilde der User in der Datenbank. Alle User welche hochgeladen werden und als Usermails dienen, werden nach CSV in der Datenbank gespeichert. Anhand diesen werden die Platzhalter gestaltet.

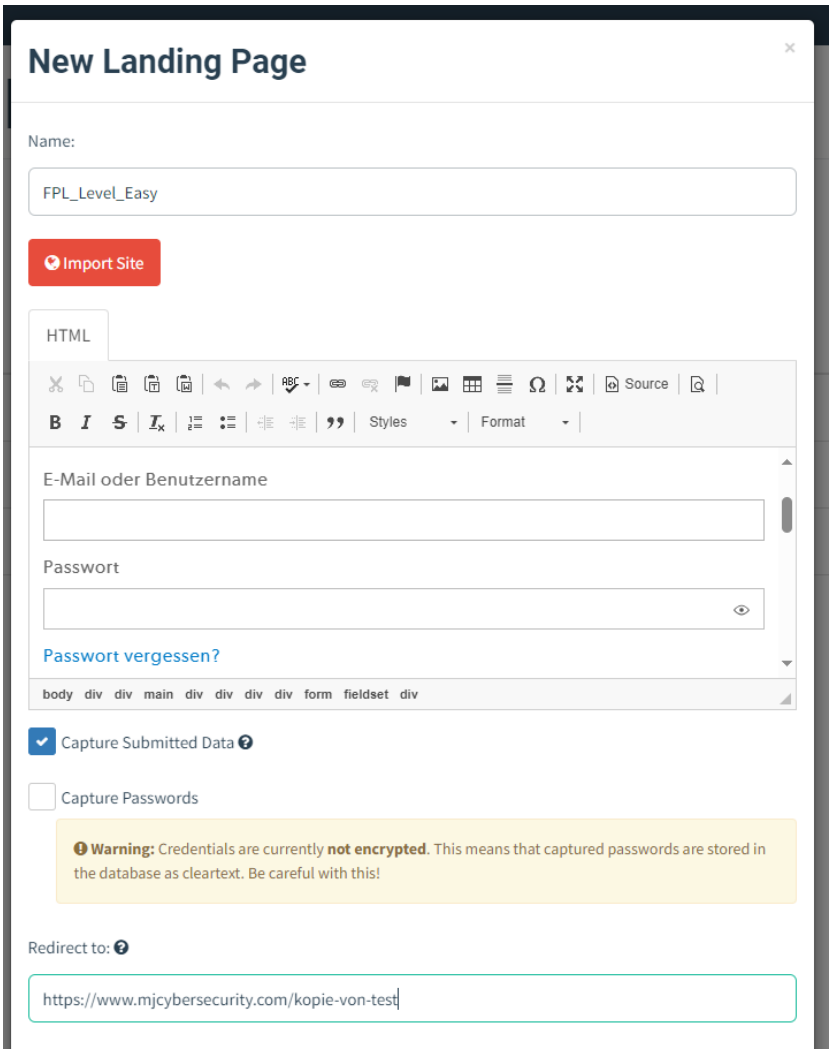

bt-ag.local
172.22.3.9
172.22.3.9:3333
AdminGUI
Reports
SQLite
USR_RID:CAMPAIGN
Webservice
Application-Configuration (GoPhish)
Configfile
Definition Listener
Definition Adminserver URL
Campaignes
Useremails
SendingProfile
EmailTemplate
FakeLoginPage_
Template
{{.LastName}},
{{.FirstName}}
{{.Position}}
{{.Email}}
{{.TrackID}}
{{.URL}}
FPM_lvl1
FPM_lvl2
FPM_lvl3
Webservice
SelfSigned Certificates
(Let's Encrypt)
(comes with GoPhish-Install)

7.3 Konfiguration FPM1

Folgend wird die erste Kampagne realisiert. Wie den vorhergehenden Dokumenten beschrieben, besteht eine Kampagne immer aus

- Mail Template, Absender, Platzhalter
- LoginPage (LandingPage) Template, Klickratenverfolgung AN
- User&Groups
- Redirects & Domains
- Kampagnestart & End

Kampagne	Schritte
FPM-Template	1) Galaxus Email kopieren (Source) nehmen und Anpassen 2) Absenderadresse auf etwas auffälliges, weil einfachste FPM  3) URL und Name mit Platzhalter anpassen Name = {{.Firstname}} → Nimmt der Vorname (definiert im CSV) URL für «Klicke Hier» = {{.URL}} → Nimmt automatisch dann die richtige Landing-Page  4) Anpassen des Emails mit rechtschreibefehlern und Grafik-Fehlern 5) TEST-Kampagne erstellen und sich selber senden für Test des Aussehens und Funktionen

FLP-Template	1) Kopieren der Galaxus-Login-Page (Import Site) 2) Capture Submitted Data 
User & Groups	Für dieses Beispiel wurden alle Emailadressen des Kunden genommen, ebenso unpersönliche Mailadressen wie zBsp. «Info@..» Ent
Domains & Redirects	Für das “einfache” Phishing wird keine DNS-Zone/»Domain» erstellt, da dieses Email am auffälligsten sein sollte.
Kampagne	1) Erstellung neuer Kampagne und Namensauswahl ebendieser 2) Die Zuvor definierten Templates hinterlegen 3) URL = in diesem Falle, da keine Domain eingerichtet wurde für dieses

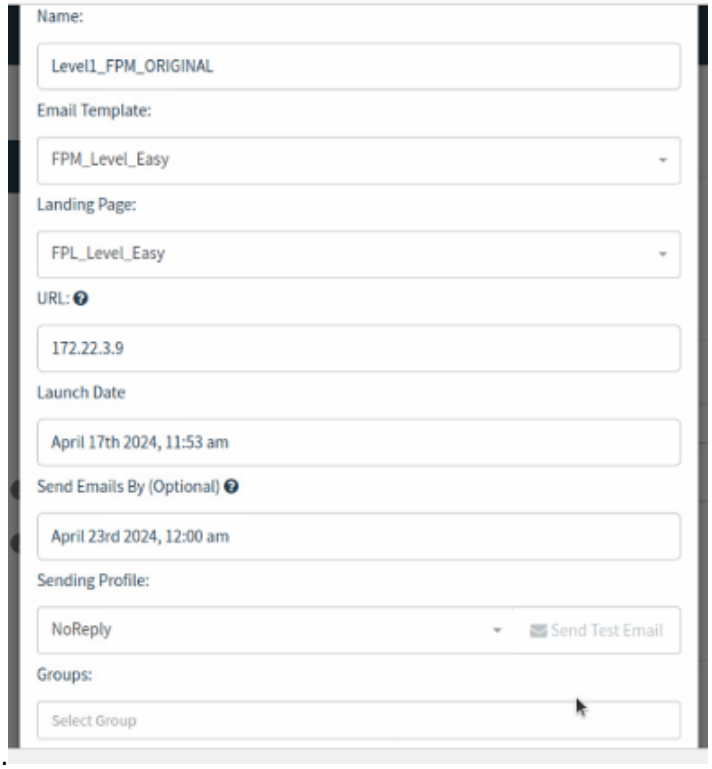
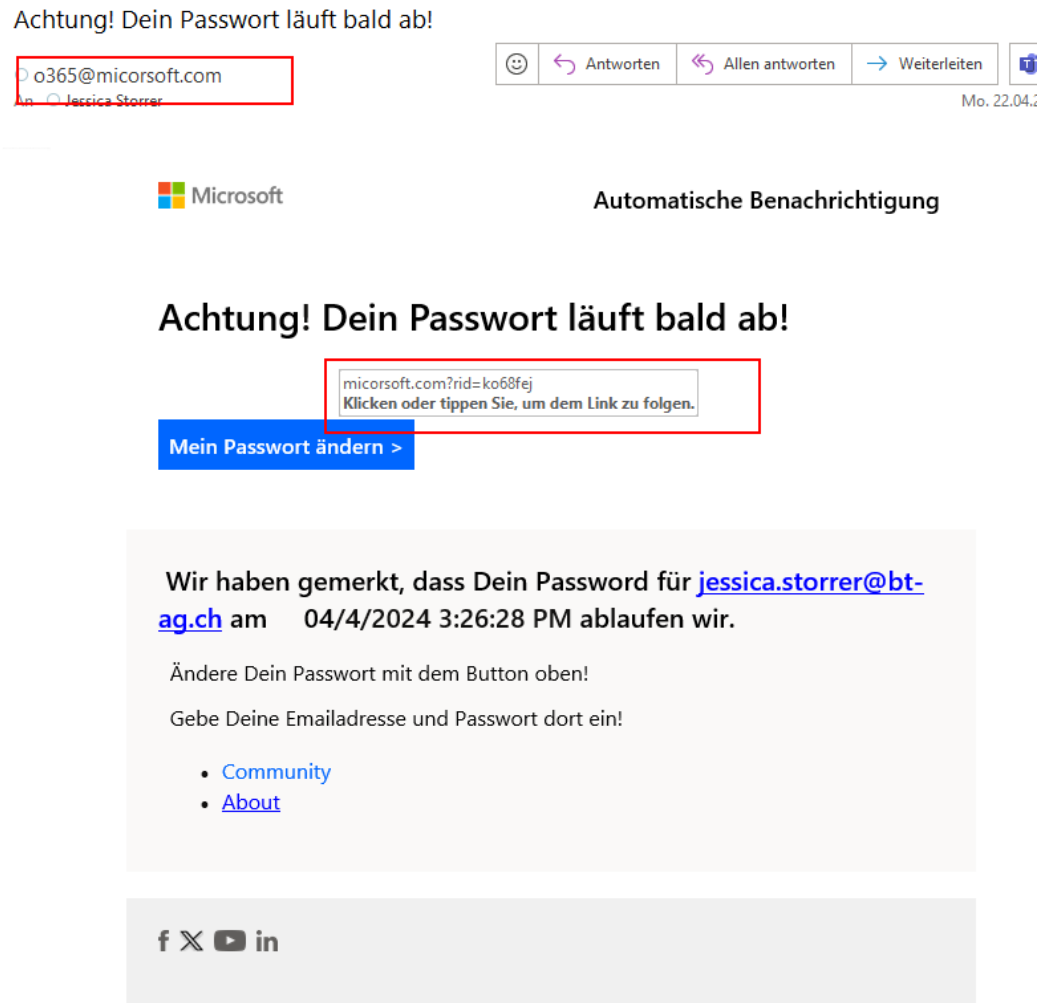
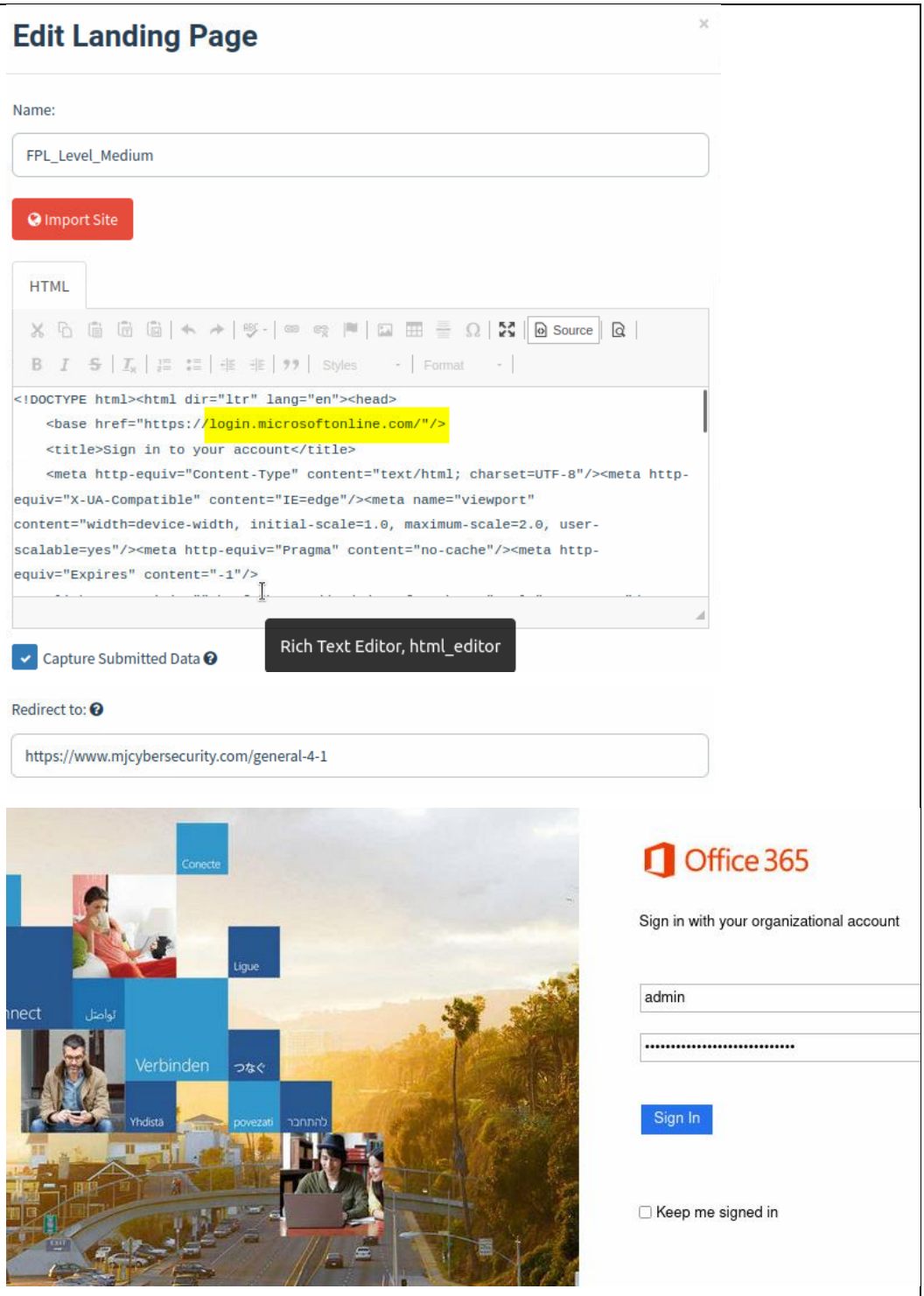
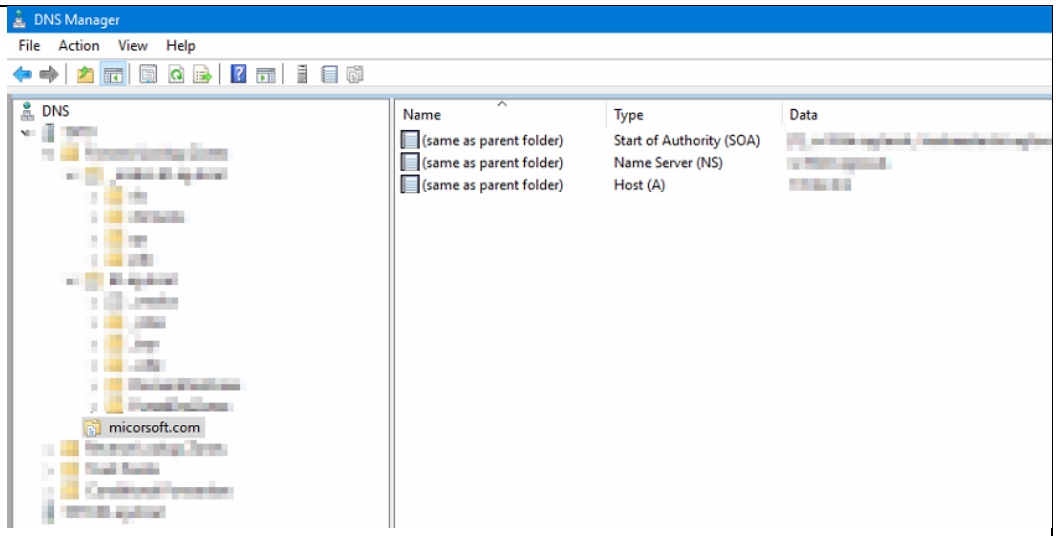
	FPM, wird hier die IP des GoPhishs Server angegeben 

Tabelle 1 - Konfiguration FPM1

7.4 Konfiguration FPM2

Kampagne	Kampage #2 FPM2
FPM-Template	
FLP-Template	1) Import alte o365 Login Seite (die neue hat eine automatische Überprüfung drin, ob der Account besteht oder wo der zugehörig ist, welche im html nicht ausgeschalten werden kann) 2) Capture Submitted Data und redirect to Oopsie Page nach Logineingabe

	
User & Groups	Nur persönliche Emails, CSV angepasst
Domains &	Micorsoft.com -> miCORsoft // miCROsoft

Redirects	 DNS Manager File Action View Help DNS micorsoft.com Name Type Data (same as parent folder) Start of Authority (SOA) (same as parent folder) Name Server (NS) (same as parent folder) Host (A)

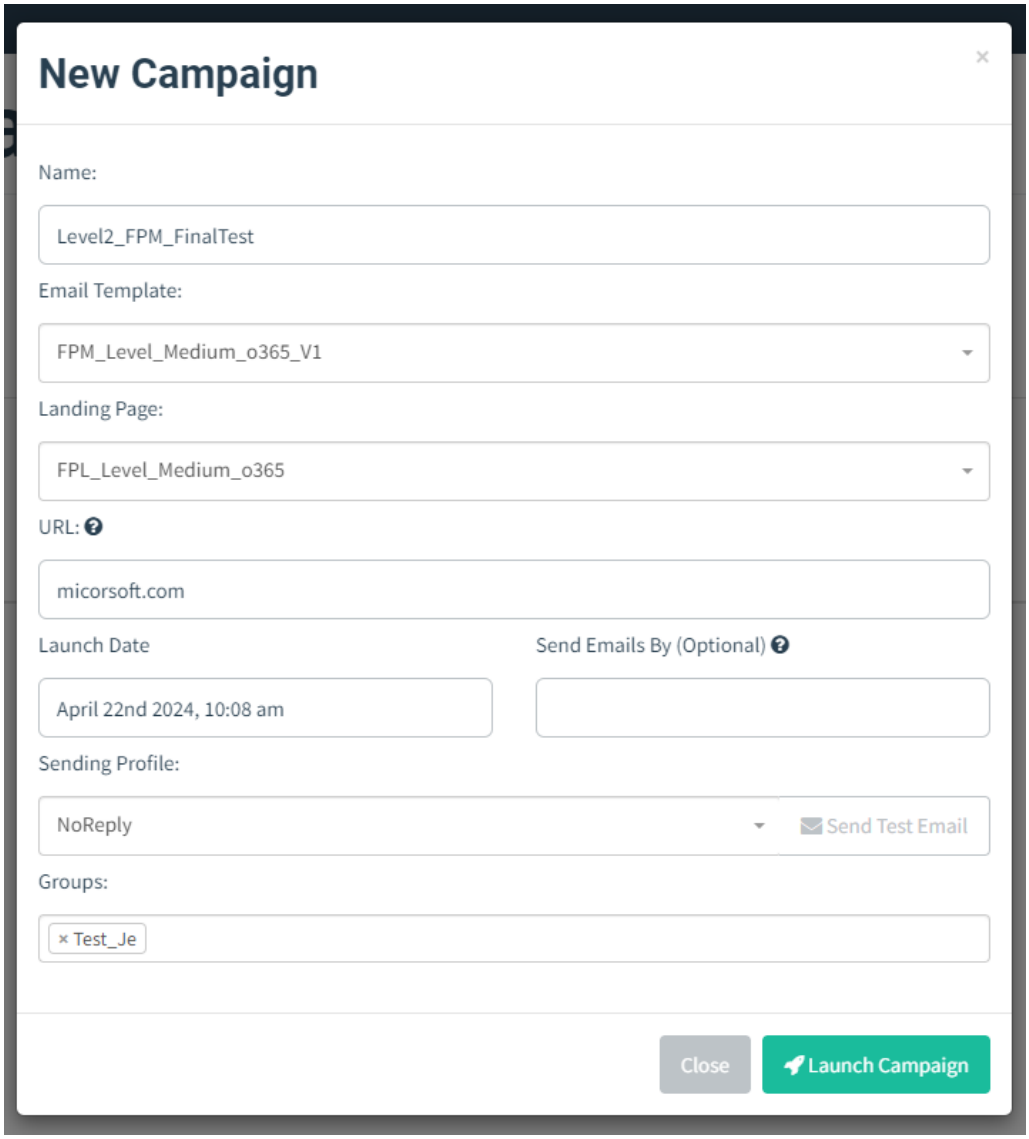
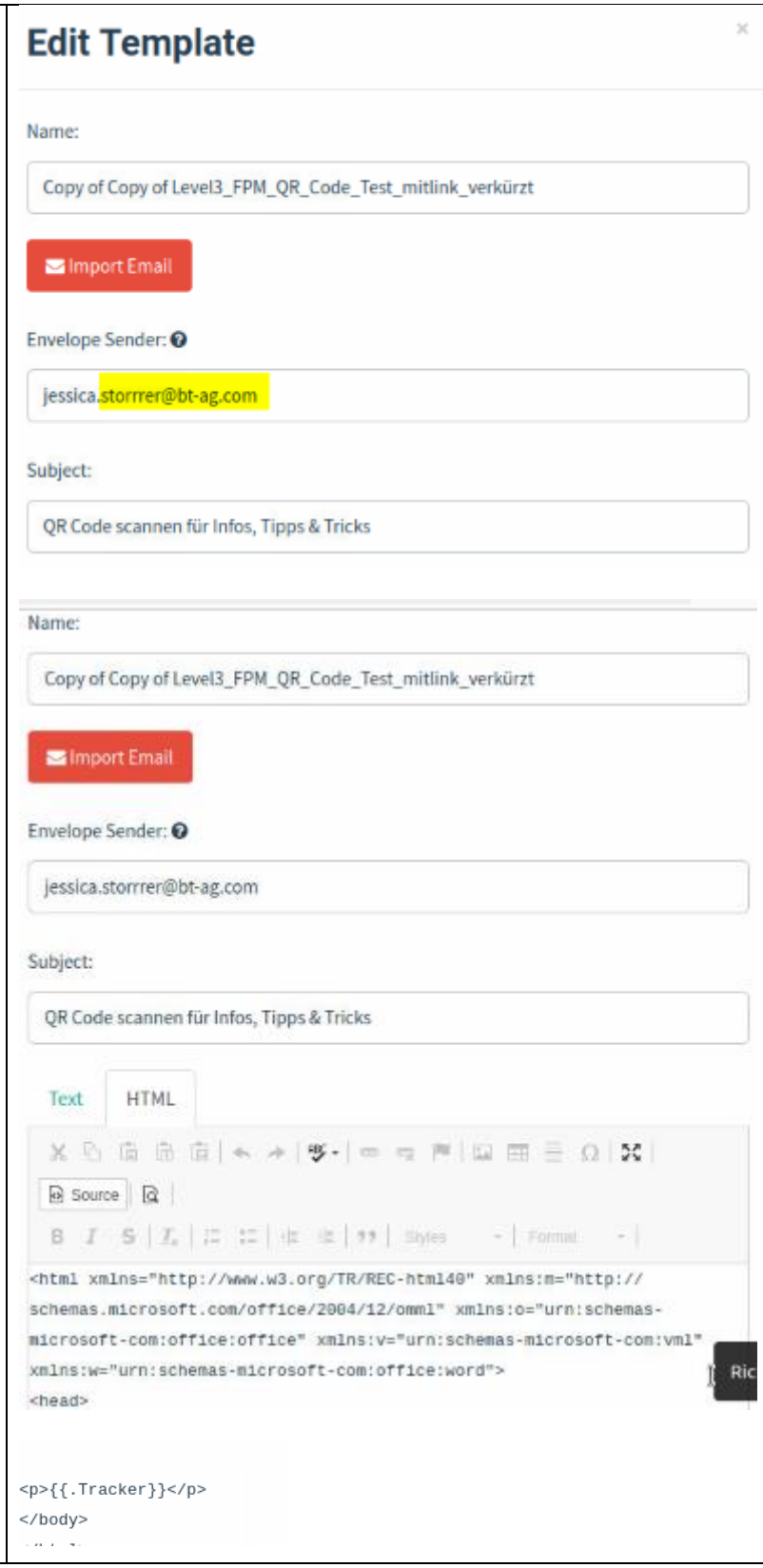
Kampagne	

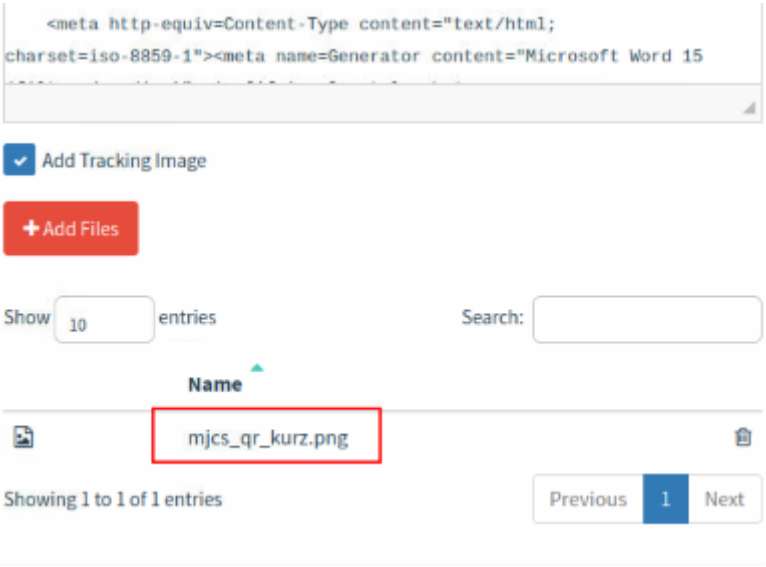
Tabelle 2 - Konfiguration FPM2

7.5 Konfiguration FPM3

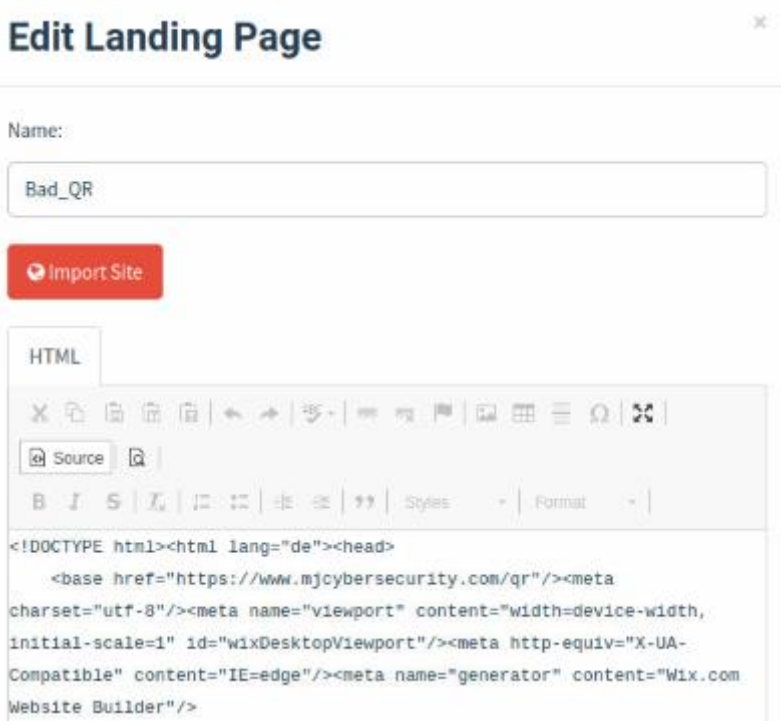
Kampagne	QR Code Fraud
FPM-Template	1) Vorgehen wie bei FPM1&2


Edit Template
Name:
Copy of Copy of Level3_FPM_QR_Code_Test_mitlink_verkürzt
Import Email
Envelope Sender:
jessica.storrer@bt-ag.com
Subject:
QR Code scannen für Infos, Tipps & Tricks
Name:
Copy of Copy of Level3_FPM_QR_Code_Test_mitlink_verkürzt
Import Email
Envelope Sender:
jessica.storrer@bt-ag.com
Subject:
QR Code scannen für Infos, Tipps & Tricks
Text
HTML
Source
<html xmlns="http://www.w3.org/TR/REC-html40" xmlns:m="http://
schemas.microsoft.com/office/2004/12/omml" xmlns:o="urn:schemas-
microsoft-com:office:office" xmlns:v="urn:schemas-microsoft-com:vml"
xmlns:w="urn:schemas-microsoft-com:office:word">
<head>
{{.Tracker}}
</body>

<table>
<tr>
<td></td>
<td>
<span style="font-size:10.0pt;font-family:"Verdana",sans-serif;color:blac
doch den unteren QR Code für weitere Tipps & Tricks! Oder klicke hier:&n
span>



Hier wird noch der QR-PNG hinzugefügt und im Quelltext so ergänzt.
</td>
</tr>
<tr>
<td>FLP-Template</td>
<td>
QR-Code Fraud von mjcybersecurity.com kopiert



</td>
</tr>
</table>

	
User & Groups	Hier werden wieder alle, also auch die unpersönlichen Emailadressen, angeschrieben.
Domains & Redirects	Mjcybersec.ch

8. Durchführung

Das genaue aussehen der Emails und Templates sind im Dokument Abschluss/Report ersichtlich.

8.1 Termine FPM Service

Folgend sind die Termine der verschiedenen FPM's ersichtlich. GoPhish sendet zwischen den Daten die Emails automatisch gestaffelt. Zudem wird danach der Newsletter und Report vorbereitet, welche circa zehn Arbeitstage nach dem letzten FPM zur Auflösung des FPM Services gegenüber den Mitarbeiter an Alle versendet werden.

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

Tabelle 3 - Termine FPM Service (Durchführung)

Zu empfehlen für eine nächste Servicedurchführung sind längere Abstände zwischen den FPM's, oder mehrere gleichzeitig und dann später noch eines. Leider geling dies in diesem Projekt aufgrund der kurz gegebenen Zeitspanne nicht.

8.2 Kampagnenübersicht

Sobald eine Kampagne gestartet wurde, wird dies im GoPhish Admin-Panel graphish hinterlegt. Der folgende, «detaillierte», Auszug ist von der ersten Kampagne, die anderen Bilder dienen rein als Beweis für den Versand, Start und Abschluss der Kampagnen.

Kampagne FPM1

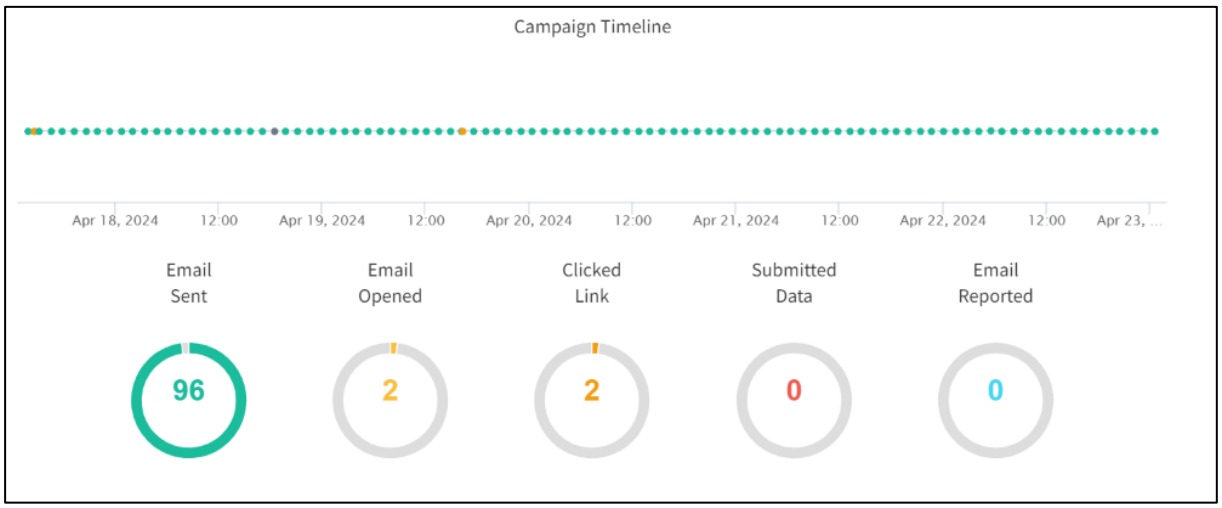


Abbildung 5 - FPM-Kampagne 1 Übersicht

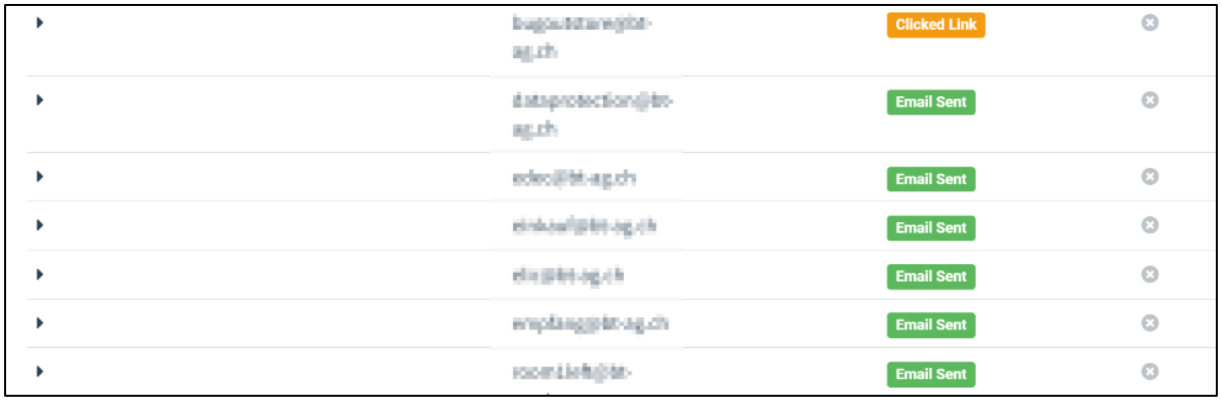


Abbildung 6 - FPM-Kampagne 1 Übersicht Detailliert 1

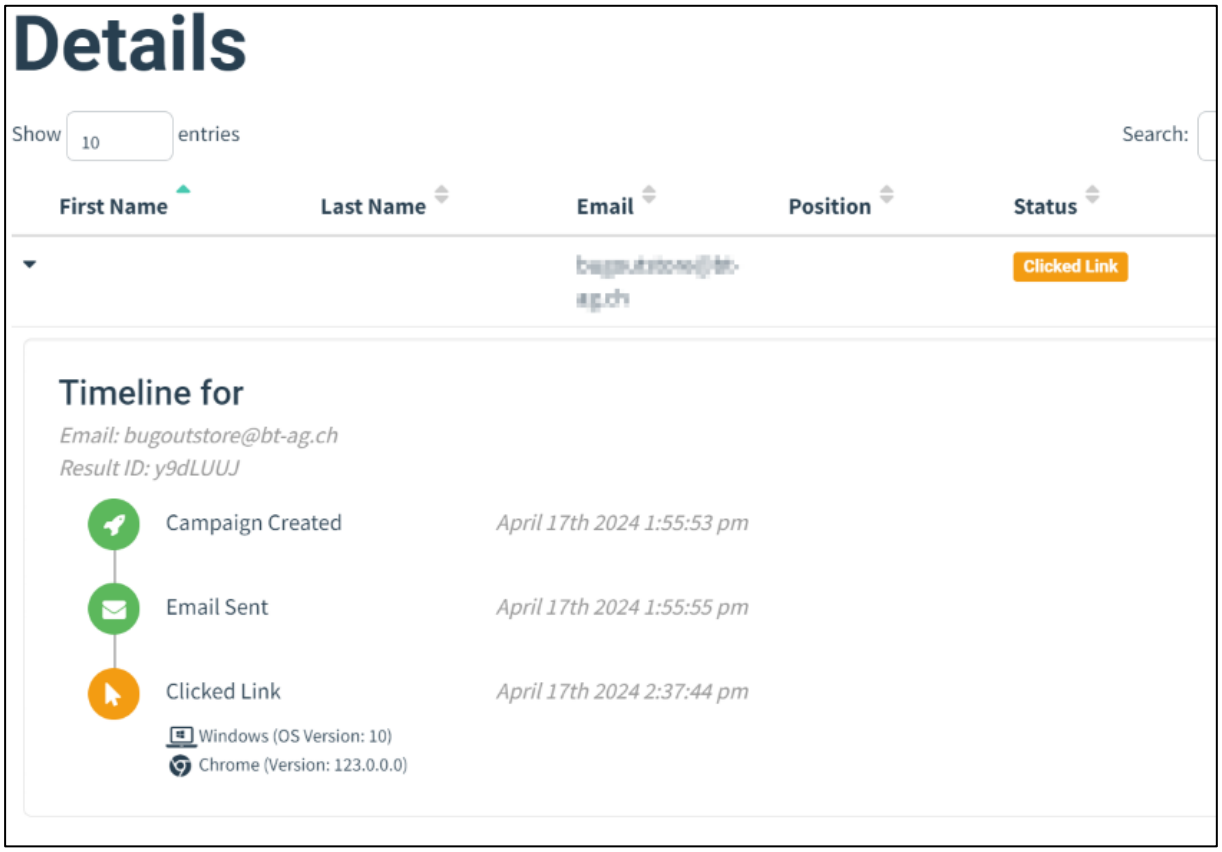


Abbildung 7 - FPM-Kampagne 1 Übersicht Detailliert 2

Kampagne FPM2

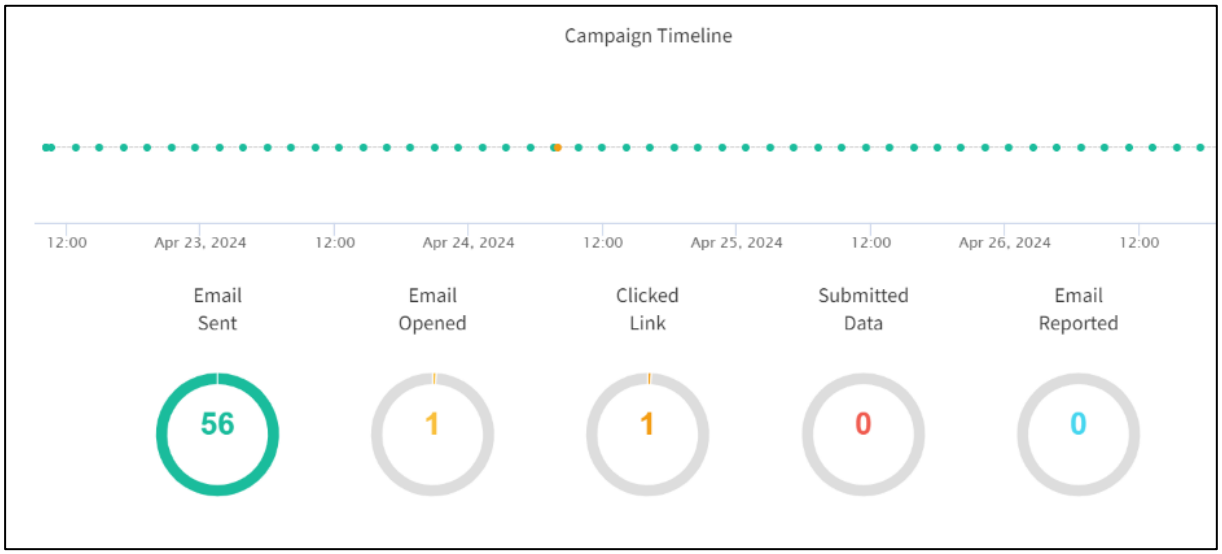


Abbildung 8 - FPM-Kampagne 2 Übersicht

Kampagne FPM3

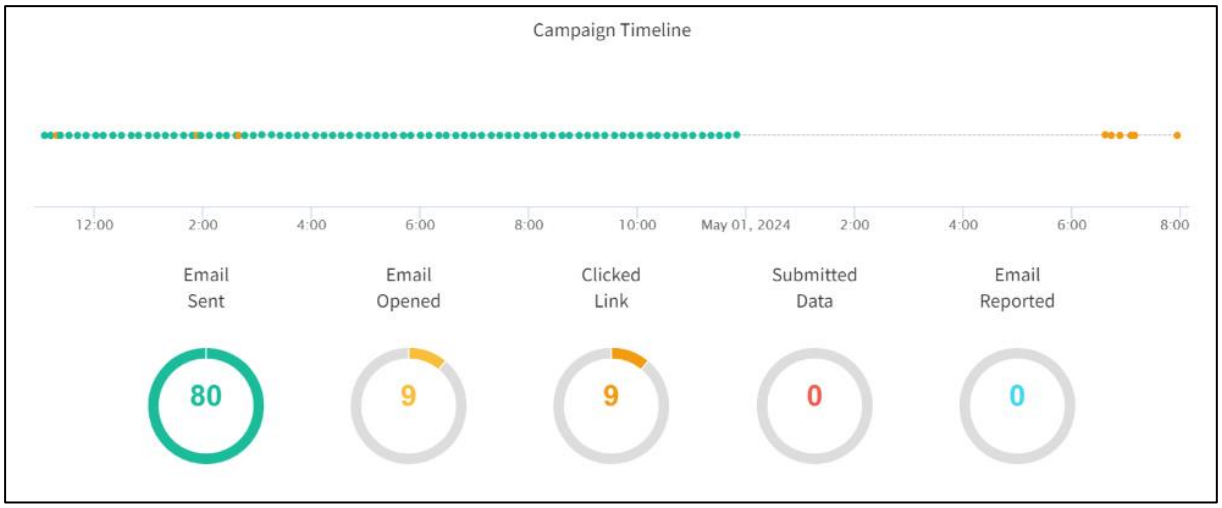


Abbildung 9 - FPM-Kampagne 3 Übersicht

8.3 Überwachung der Kampagne

Regelmässiges, manuelles Überwachen der Kampagen zur Überprüfung, ob der Service noch am laufen ist. Dies kann ebenso als Script eingebunden werden, welches die Domain mittels einem einfachen Ping schaut, ob der GoPhish Server und deren erstellten Domains noch ansprechbar sind. Falls nicht, könnte dieses Script via Emailalarming Alarm geben, dass der Service nicht mehr ansprechbar ist.

8.4 Überprüfung der Kampagne

Während den einzelnen Kampagnen wurden die Klickraten überprüft. Sobald eine interaktion mit dem Fake Mail geschehen ist wird der User persönlich angeschrieben. Der Persönliche Aspekt stärkt nochmals das Aha-Erlebnis und so kann auf jeden User persönlich eingegangen werden. Die Personen werden ermahnt und erhalten Zugang zu CAT.

Diejenigen Personen welche die mail als Verdächtig oder Phishing gemeldet haben, erhalten ebenso eine Persönliche Dankensemail für die Aufmerksamkeit. Ebendiese User erhalten ebenso Zugriff auf CAT.

Report und Abschluss werden in einem Separaten Dokument dokumentiert.

8.5 Antwortemails

Folgend sind ein paar der Antwortemails hinterlegt, diese können wiederverwendet und abgeändert werden.

8.6 Mögliche Probleme / Aufgetretene Probleme

Folgend sind die zu erwartenden Probleme und die aufgetrenenen Probleme Dokumentiert.

8.6.1 Mögliche Probleme und deren Lösung

Folgend sind mögliche Probleme und deren möglichen Lösungen dargestellt

Exchange Online schiebt die Emails in Quarantäne

Regel erstellen in der Exchange Online Quarantäne Verwaltung

Verbindung zu GoPhish Server nicht vorhanden

Allgemeine Verbindungen und Netzwerke prüfen, Firewallrules, GoPhish-Service restart.

8.6.2 Aufgetretene Probleme

Exchange Online schiebt die Emails in Quarantäne

Obwohl der Absender eigentlich vom SMTP des Kunden kam und bei den Tests mit einer Email auch nie ein Problem gab, landete beim ersten FPM die Email in der Exchange-Online Quarantäne. Dank dem Adminzugang konnte eine Regel gesetzt werden, damit der Exchange Online die Absenderadresse nicht mehr als SPAM erkennt und die Emails freigibt.

Verbindung zu GoPhish Server nicht vorhanden

Es kam vor, dass der GoPhish Server (AdminKonsole) nicht vom Client verfügbar gewesen ist. Dies war aber nur der Fall, als aus dem HomeOffice gearbeitet wurde. Da dies nicht immer der Fall war, sind VPN/FW-Rules auszuschliessen. Da das Suchen des Problemes länger gedauert hätte als es Verfügbar war, wurde dieses Problem ignoriert.

9. Bibliotheken

Um die FakeEmailtemplates und FakeLoginPages für andere Kunden brauchen zu können, werden die Quelltexte derer, sowie die Emails selber, in einer GitHub Bibliothek gespeichert.

Diese müssen jedoch pro Kunden angepasst werden.

Alle Bibliotheken sind öffentlich, bis die Notenbewertung durch ist. Danach werden diese auf privat gesetzt.

9.1 Emailtemplates / Emails

In der folgenden Bilbliothek werden die Emailtemplates gespeichert.

https://github.com/estorj/MJCS.git

9.2 Login Pages

In der folgenden Bibliothek werden die Login-Page Quelltexte gespeichert.

https://github.com/estorj/MJCS.git

10. Testprotokolle

Das Testprotokoll ist in folgendem Dokument zu finden.

ID2132_StorrerJessica_FPM_Testprotokoll.pdf

11. Abschlussworte Realisierung

Die Realisierung beinhaltete das Aufsetzen und Installieren eines Ubuntu Servers, sowie das installieren von GoPhish auf ebendiesem.

Nachdem installieren der GoPhish Applikation konnte dank dem konfigurieren des Konfiguration-Files der GoPhish Server von aussen her angesprochen werden.

Mithilfe des Admin-Panels können die ganzen Parameter wie Sendeprofile, Emailtemplates, LoginPages und Usergruppen mittels einem GUI zu FPM-Kampagnen zusammengeführt werden.

Dank den anpassbaren Platzhaltern wie {{.URL}} oder {{.Vorname}} können die Emailtemplates personalisiert werden.

Das Admin-Panel beherbergt ebenso die Kampagnen Resultate und werden graphisch dargestellt und aufgezeichnet, welcher User wann geklickt hat.

Persönliches Fazit:

Die Realisierung lief besser als gedacht, es musste nur eine SPAM-Umgehungs-Rule erstellt werden beim ersten FPM, danach gingen die Mails ohne Probleme durch.

Das Anpassen der Fake Mails und das Anpassen der Fake Login Pages gestaltete sich als sehr einfach und effizient. Alles in allem war die Realisierung des GoPhish Services sehr schnell durch.

Literaturverzeichnis

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