22. BERNER TAGUNG «SICHERHEITSASPEKTE BEI IT-BESCHAFFUNGEN»

«ÜBERPRÜFEN DER SECURITY AWARENESS ODER WIE BE-PHISHED MAN MEHRERE TAUSEND BENUTZER» -

DOMINIQUE BRACK - T-SYSTEMS SCHWEIZ AG

FISCHERS FRITZ FISCHT FRISCHE FISCHE – PHISHER PHISHEN PINS UND TANS!

WAS IST PHISHING?

Beim Phishing handelt es sich um Cyberattacken, bei denen der Täter mit Hilfe gefälschter E-Mails, SMS oder Websites versucht, vertrauliche Zugangs- und Identifikationsdaten von Internetnutzern zu erlangen. Phisher verursachen mehr als 90 Prozent aller gezielten Angriffe im Internet. Dabei bedienen sich die Phisher raffinierter Methoden und nutzen die erbeuteten Daten für unterschiedliche Zwecke.

TARNUNG

Getarnt als seriöse Bank oder Firma

TÄUSCHUNG

E-Mails im HTML-Format verweisen auf einen „offiziellen“ Link dahinter versteckt sich dann ein ganz anderer Link.

VERSCHLEIERUNG

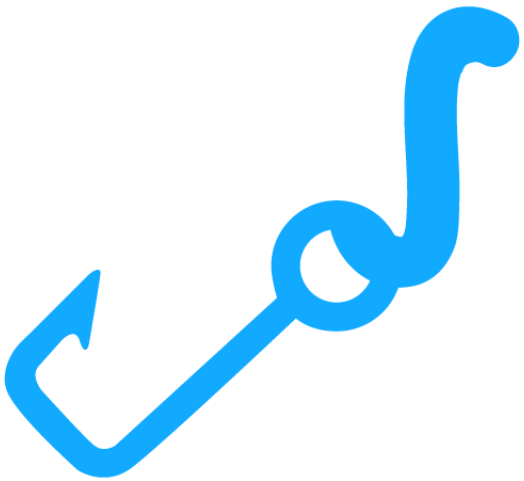
Die Phishing-Mails sind so gestaltet, dass sie den originalen E-Mails täuschend ähnlich sind.

FALLE

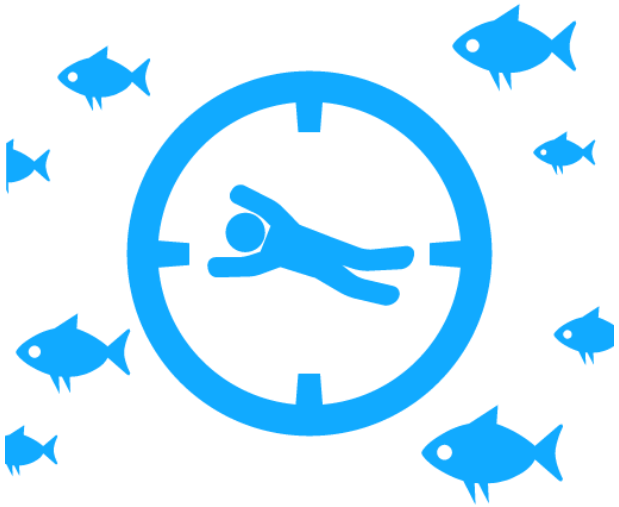
Gefälschte Login-Seite des Angreifers dem Opfer wird eine scheinbar sichere Umgebung vorgetäuscht.

T · · Systems ·

PHISHING – EIN TEIL VON SOCIAL ENGINEERING



Phishing



Spear Phishing

Whaling

T · · Systems ·

SECURITY AWARENESS

Das stärkste Glied in der Kette ist der

Mensch!

Wenn die Technik versagt bleibt nur noch der Mensch.

Ansonsten wird’s der CISO richten mit Awareness Schulungen.

T · · Systems ·

BEISPIELE

REPLY

Steuerverwaltung ESTV

Today 19:05

Fragen zu der Einkommensteuererklarung Ihre Rufnummer ist nicht erreichbar

To: info@807am.com

ESTV Dokument_34540_18_10_2017.doc (~660 KB)

Sehr geherte Frau Brack , sehr geherter Herr Brack.

Ich bin Patrick Wegmann, ich bin Steuerprüfer in Ihrem Bezirk.

Es haben sich ..... ergeben einige Fragen zu Ihrer Steuererklärung

Dieses Dokument enthält die Liste von Fragen zu Ihrer Einkommensteuererklärung und meine Telefonnummer.

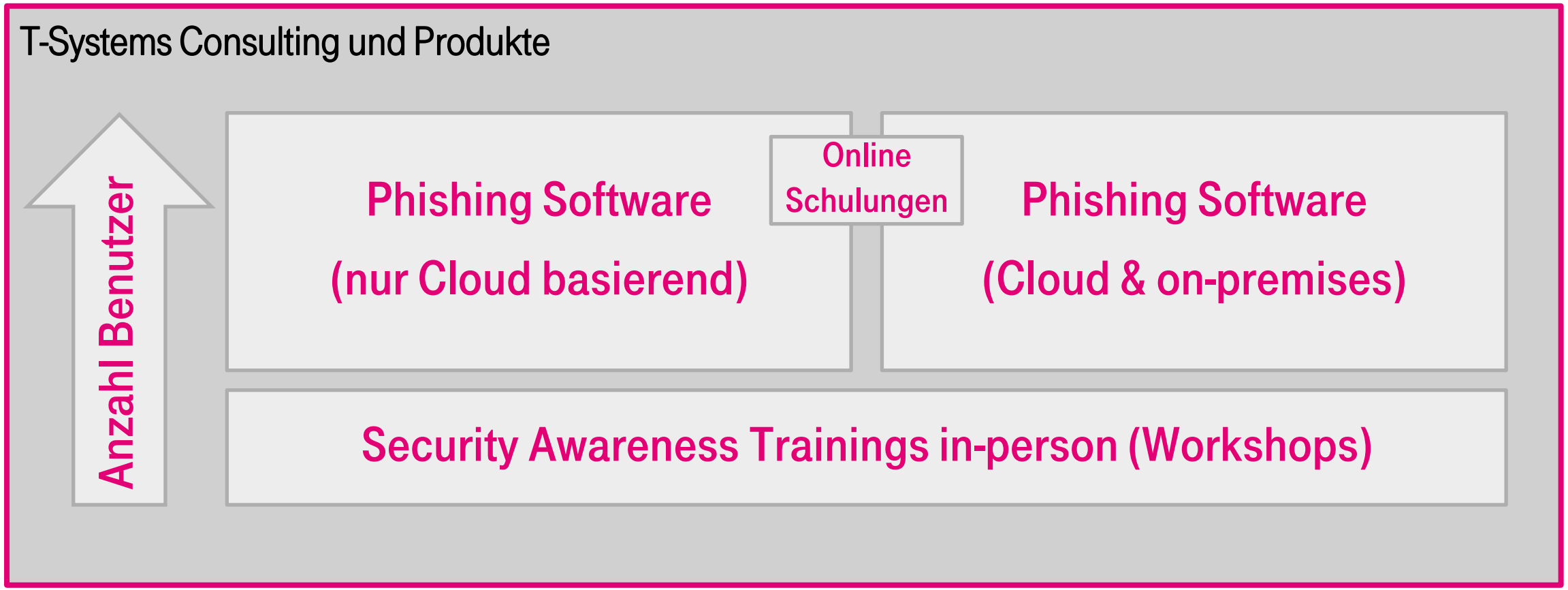
Mit freundlichen Grüssen
Patrick Wegmann

Eidgenössische Steuerverwaltung ESTV

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

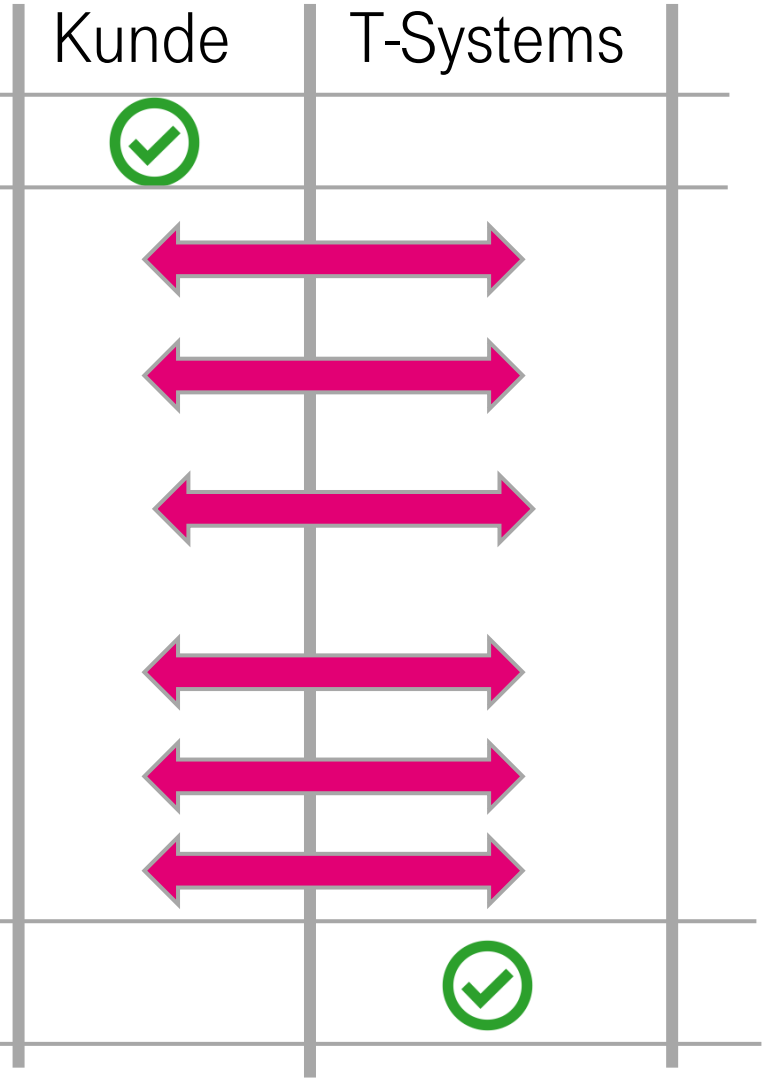
T · · Systems ·

SECURITY AWARENESS UND PHISHING SERVICES



T · · Systems ·

AUFBAU EINER KAMPAGNE



- Nur Software Lizenz

- Erstellen des Phishing Templates oder Payloads
- Professionelles Tracking der Phishing Emails und der Schulungsmodule
- Detailliertes Reporting und Auswertung der Kampagnen
- Planung, Steuerung und Koordination der Kampagne (interne Security etc.)
- Import der Benutzer
- Konfiguration der Plattform

- Projekt komplett Outgesourced

Beim Security Awareness (Phishing) Angebot gibt es verschiedene Möglichkeiten der Zusammenarbeit. Der Kunde kann nur das Produkt beziehen oder aber T-Systems managend alles aus einer Hand.

T · · Systems ·

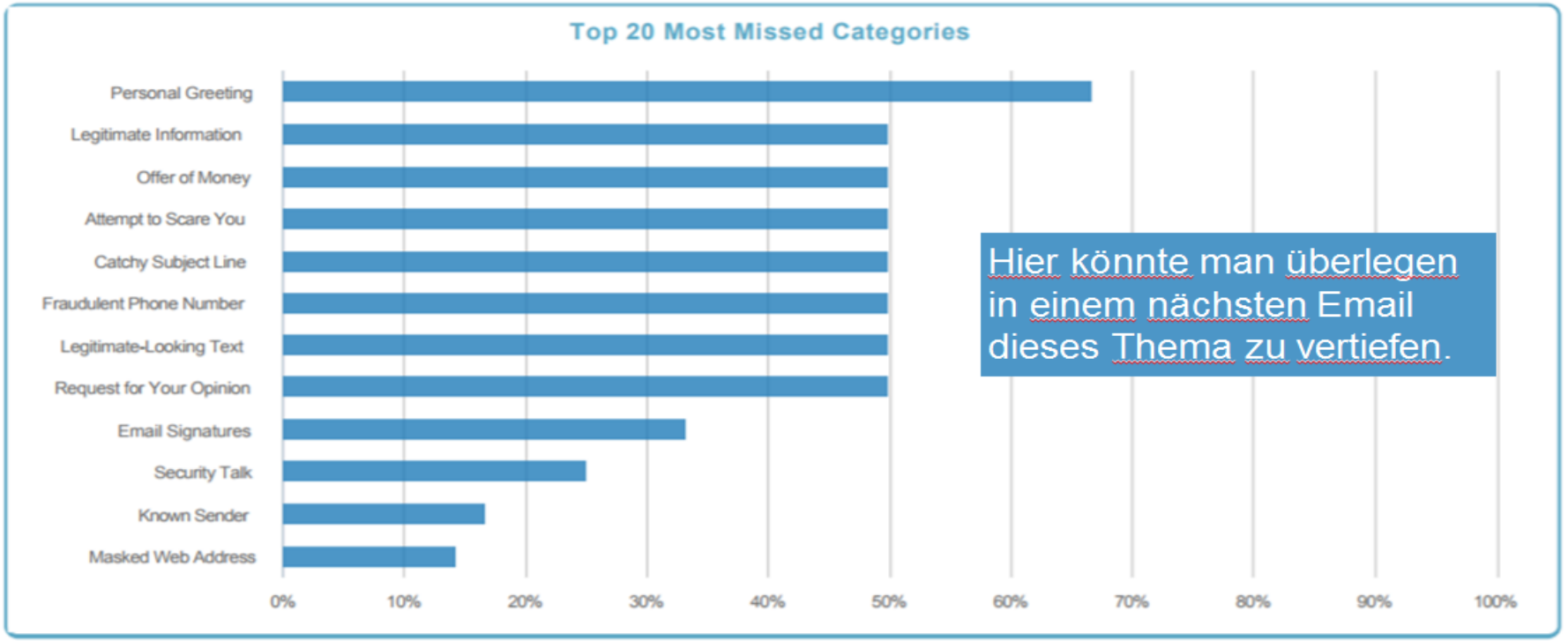
REPORTING BEISPIELE AUS DEN «PHISHING» TOOLS

Report Training

Summary

# of Categories	Average % Incorrect	Average % Correct	Total Incorrect Responses	Total Correct Responses	# of Modules
24	20,55%	79,45%	15	58	1

Visualization



T · · Systems ·

REPORTING BEISPIELE AUS DEN «PHISHING» TOOLS

Stats - Überprüfung XING/ LinkedIn Profil Einträge

Show me the numbers

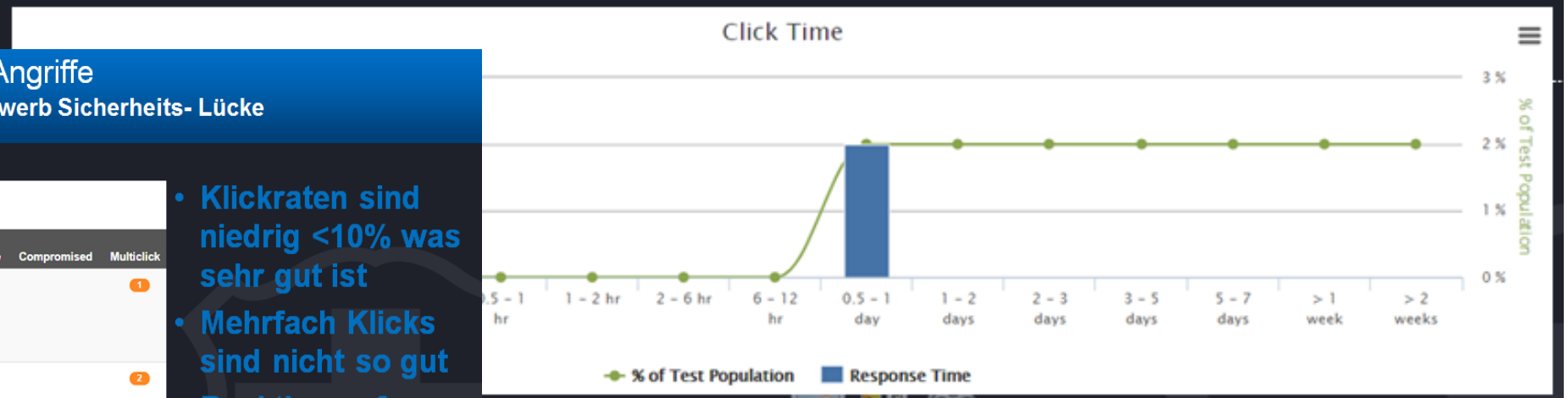
Auswertung der Phishing Angriffe

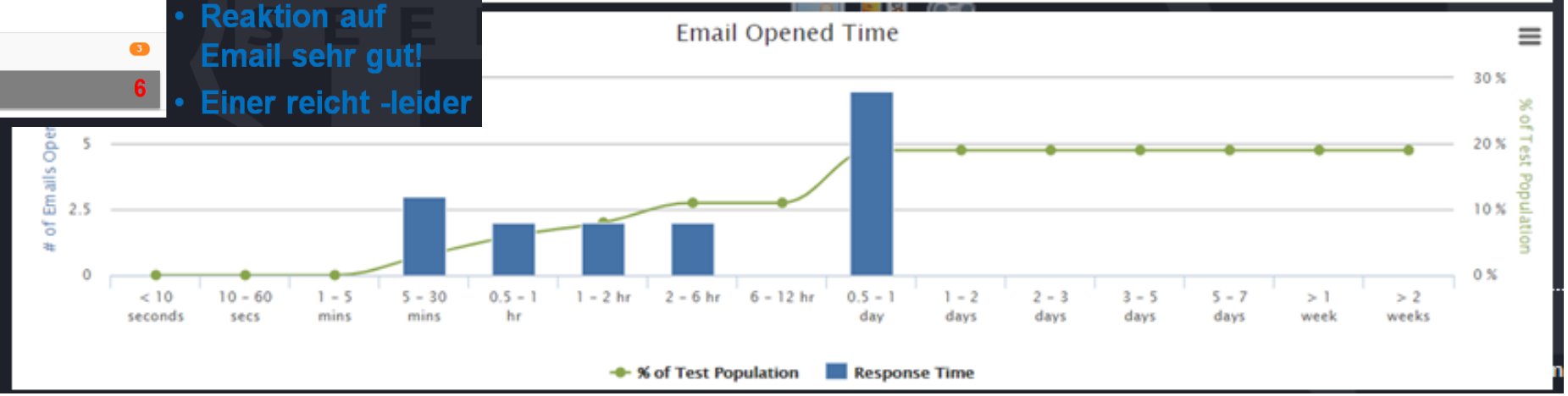
3 Templates: Immobilien, Wettbewerb Sicherheits- Lücke

All Email Campaign History 3

Title	Sent	Opened	Clicked	Vulnerable	Compromised	Multiclick
Überprüfung XING/ LinkedIn Profil Einträge **From:** Marc Wydler	81	16	2	0		1
Swisscom Outsourcing **From:** Swisscom	41	7	5	3		2
Mitarbeiterangebot Immobilien **From:** Siro Roesch	39	21	6	6		3
		44	13			6

- Klickraten sind niedrig <10% was sehr gut ist
- Mehrfach Klicks sind nicht so gut
- Reaktion auf Email sehr gut!
- Einer reicht -leider

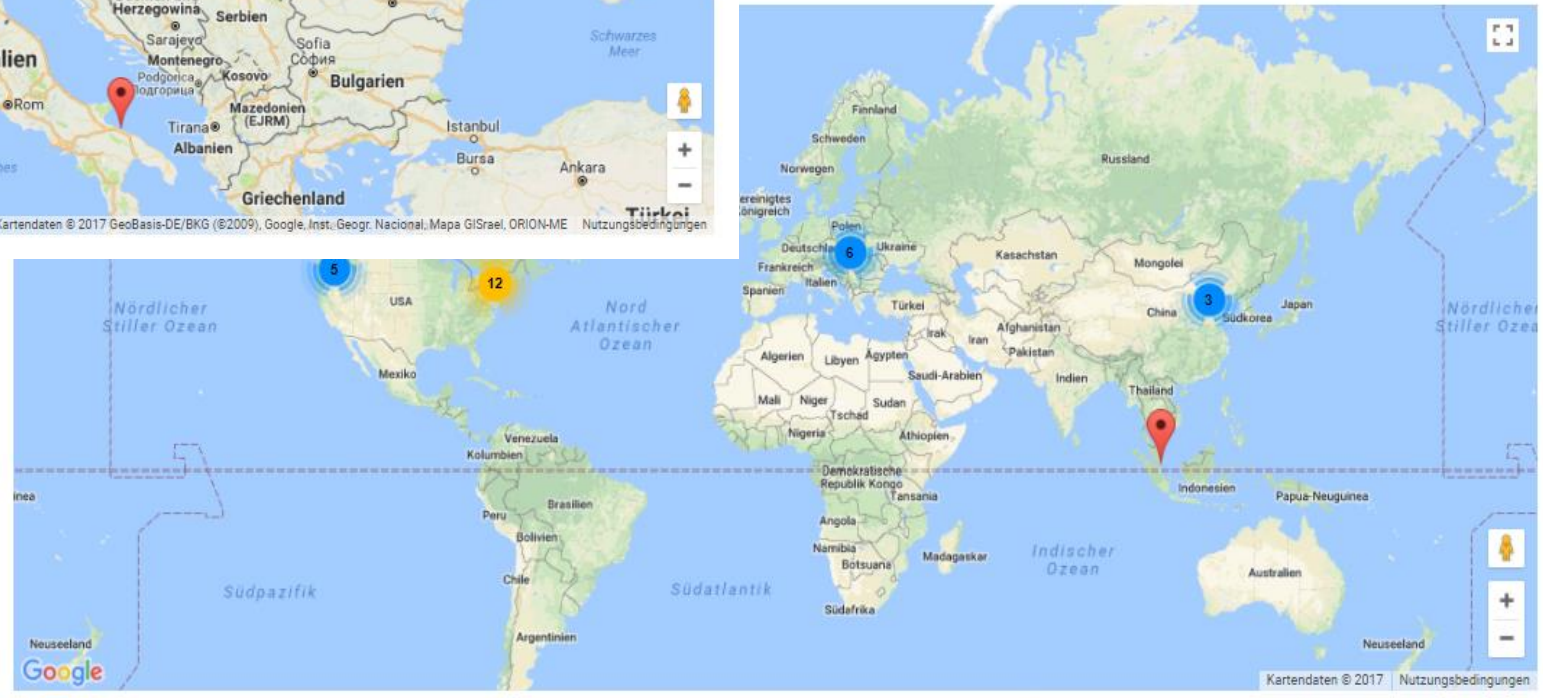




T · · Systems ·

REPORTING BEISPIELE AUS DEN «PHISHING» TOOLS

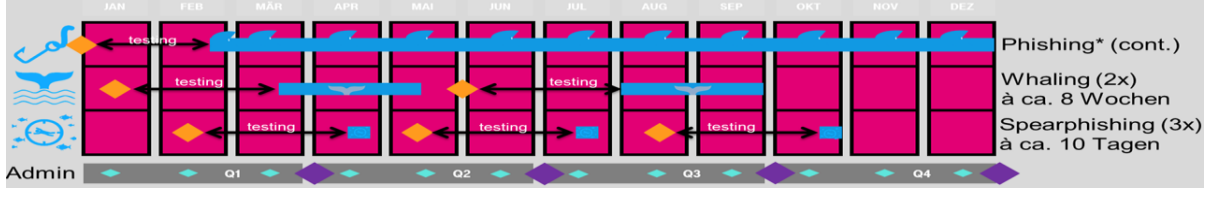
Campaign Overview | Endpoints | Users | Geographic Distribution | Notes



T · · Systems ·

ERFAHRUNGEN UND RISIKEN BEI «PHISHING» VORHABEN

Risiko	Klein/ Mittel/ Hoch	Massnahmen	Restrisiko
Daten Leck	Mittel	Daten werden verschlüsselt zur Verfügung gestellt. Eine sichere Einlieferung ist so möglich. Trennung Betrieb/ Projekt bei T-Systems. RBAC Modell für die Applikation. Ev. Manueller Prozess. Nur Daten einliefern die auch benötigt werden.	Klein
Verunsicherte Benutzer	Hoch	Verweis auf die Auflösungsseite. Flankierende Massnahmen – Intranet. CISO Infomail.	Mittel
Auslösen von Alarmsystemen (IDS/ IDPS)	Hoch	Langsames Herantasten an die verkraftbare Grenze für das Mailing. Erstellen von Testemails vor der Kampagne. Selbsttest der Phishing Applikation.	Mittel
Generieren von Support Tickets – Kostenfolgen	Mittel	Eruieren der Betriebsverantwortung der Kunden Infrastruktur und Absprache mit den Betreibern.	Klein
SLA Verletzungen	Klein	Eruieren der Betriebsverantwortung der Kunden Infrastruktur und Absprache mit den Betreibern.	Klein
Weiterleitung der Phishing Emails (Privat)	Hoch	Generische Benutzerinformation oder Publikation des Quartalsreports.	Mittel
Versand an falsche Adressaten	Klein	Definition von Benutzergruppen. Vieraugenprinzip bei der Erstellung der Kampagnen. Sign-off beim Management	Klein
Bulk Versand – Sturm	Klein	Definition von Benutzergruppen. Vieraugenprinzip bei der Erstellung der Kampagnen.	Klein
Vertrauensverlust in Email	Mittel	Generelle Benutzerinformationen. Intranet News. Gestaltung der Phishing Emails. Maturitätsprinzip.	Klein



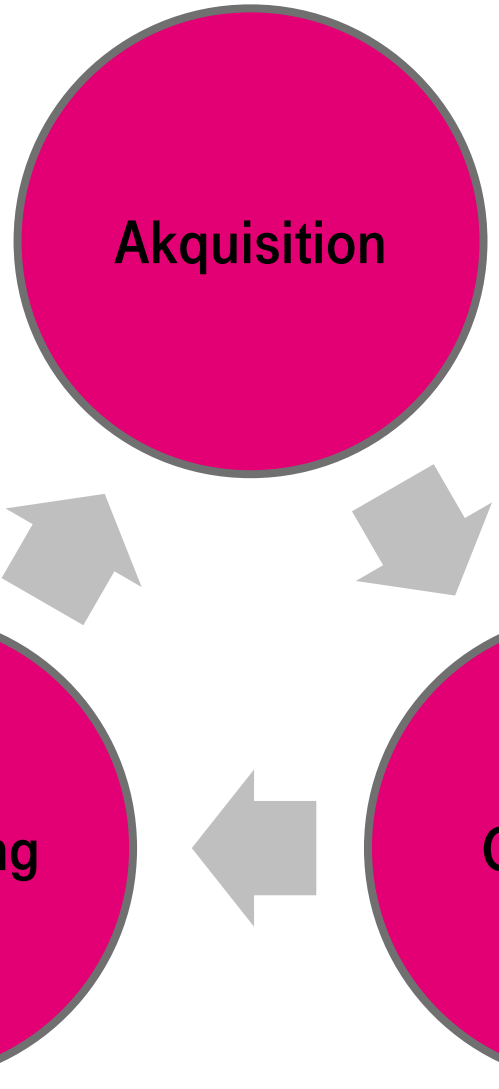
DIE WAHL EINES GEEIGNETEN PARTNERS

Jeder machts! (auch das VBS).

Es gehört zur Basis Ausbildung seine Mitarbeiter an Awareness Schulungen Teilhaben zu lassen.

T · · Systems ·

LEBENSZYKLUS



Nicht den Vorgaben entsprechend:

- Cloud Software
- Daten im Ausland
- Persönliche Daten
- Verschlüsselung
- Archivierung

Misskonfiguration/ no Security:

- Data Leakage
- Keine Verschlüsselung
- Kein ISDS/ Policies
- Bearbeitungsregelment
- DSG/ GDPR

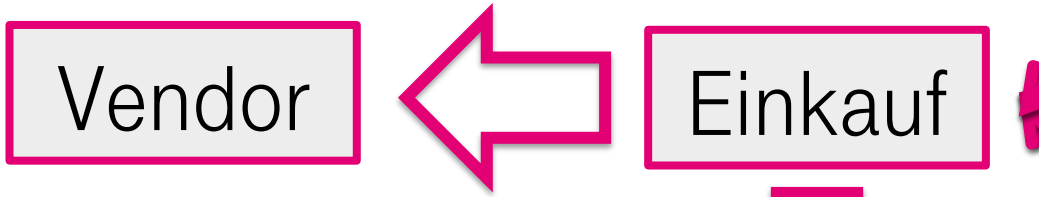
Archivierung:

- Wiping
- Archivierung
- Aufbewahrungspflicht
- eWaste

T · · Systems ·

Alles einmal nach vorne

LEBENSZYKLUS



CISO
IT-SiBe
CIO
Risk Management
Compliance
Governance

Nicht den Vorgaben entsprechend:
- Cloud Software
- Daten im Ausland
- Persönliche Daten
- Verschlüsselung
- Archivierung

Misskonfiguration/ no Security:
- Data Leakage
- Keine Verschlüsselung
- Kein ISDS/ Policies
- Bearbeitungsregelment
- DSG/ GDPR

Archivierung:
- Wiping
- Archivierung
- Aufbewahrungspflicht
- eWaste

T · · Systems ·

WIR SIND FÜR SIE DA

T · · Systems ·

DANKE

10 GEBOTE ZUM SCHUTZ VOR PHISHING

1. Bestätigen Sie niemals Kontonummern, Passwörter oder andere geheime Daten nach einer Mail-Aufforderung! Seriöse Institute oder Firmen würden ein solches Vorgehen aus Sicherheitsgründen nie wählen.

2. Falls ein Online-Bezahldienst oder Online-Shop (z.B. PayPal, Amazon oder eBay) Sie zur Aktualisierung Ihrer Daten auffordert, geben Sie dessen Webadresse manuell in die Adresszeile Ihres Browsers ein – und nicht über einen E-Mail-Link.

3. Überprüfen Sie den Sicherheitsstatus von Webseiten, auf denen Sie persönliche Informationen eingeben! HTTPS ist keine Garantie für die Echtheit einer Website. Prüfen Sie das Sicherheitszertifikat der Website durch Anklicken des Schlosssymbols in der Statuszeile des Browsers.

4. Wenn Sie eine E-Mail von einem unbekannten Absender erhalten, öffnen Sie nicht bedenkenlos darin enthaltene Links, Formulare oder Anhänge.

5. Bei auffälligen Mails von vertrauten Adressaten (z.B. Ihrer Bank) setzen Sie sich telefonisch mit Ihrem Ansprechpartner in Verbindung und lassen Sie sich die Richtigkeit der Mail bestätigen.

6. Sicherheitslücken in Programmen, insbesondere in Browsern, können von Datenfischern ausgenutzt werden. Aktualisieren Sie die Browser-Software regelmäßig und installieren Sie aktuelle Sicherheits-Updates.

7. Setzen Sie aktuelle Anti-Virenprogramme und Firewalls ein und verwenden Sie Webfilter. Markieren Sie unerwünschte E-Mails als Spam!

8. Verwenden Sie unterschiedliche Passwörter für Ihre Accounts.

9. Wenn Sie befürchten, dass Sie einem Phishing-Angriff zum Opfer gefallen sind, verständigen Sie umgehend Ihre Bank oder Ihren Geschäftspartner und sperren Sie den betroffenen Account.

10. Das Vertrauen in die „Unfehlbarkeit“ der Technik kann der Türöffner für einen Phishing-Angriff sein. Ein „gesundes Misstrauen“ schützt davor, den Phishern ins Netz zu gehen!

T · · Systems ·