

Warum viele Awareness-Aktivitäten heute schwach sind und wo KI helfen kann.

Palo Stacho @ it-sa 2024

[CYBERDISE-AWARENESS.COM](https://www.cyberdise-awareness.com)



Wer ist dieser Typ, der über 'sinnlose' Dinge redet?

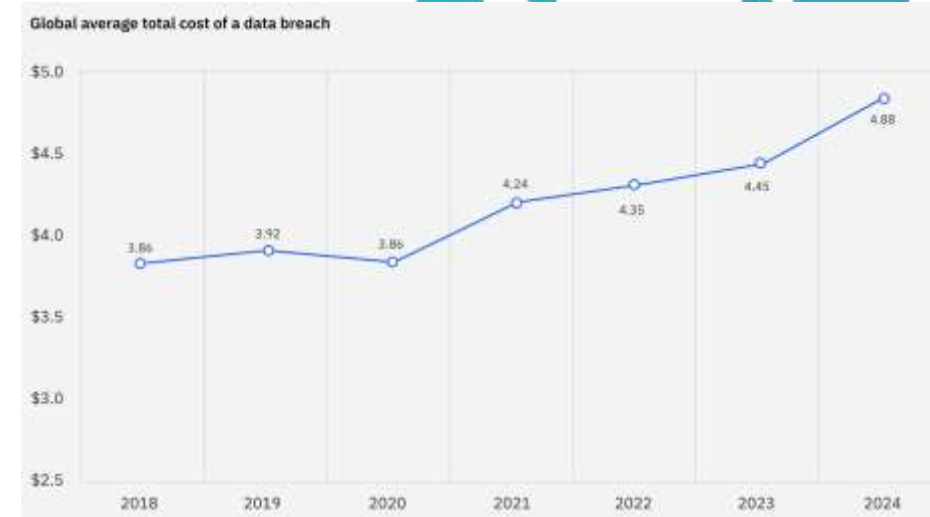
Palo Stacho

- Cybersecurity-Awareness-Berater seit 10 Jahren.
- Das ist bereits meine zweite Awareness-Firma!



40 Jahre Cybersicherheit, und es wird nicht wirklich besser!

- 47 % aller erfolgreichen Angriffe sind immer noch auf unvorsichtige Mitarbeiter zurückzuführen [1]
 - insbesondere Phishing [2].
 - Kein signifikanter Rückgang in den letzten Jahren [3].
- Durchschnittliche Kosten eines Sicherheitsvorfalls bis zu 4,88 Mio. USD [4]
- Kosten sind in den letzten 5 Jahren um 20 % gestiegen [5]
- KI wird in großem Umfang bei diesen Angriffen eingesetzt [6]



[1] Analysis of the IBM Cost of Data Breach Report 2024, Figure 7: Cases that can be attributed to a lack of employee awareness amount to 16% compromised/stolen credentials, 15% phishing, 10% Business Email Compromise and 06% social engineering. Means that 47% of all attacks target inexperienced, gullible or careless employees.

[2] IBM Cost of Data Breach Report S.13

[3] ebenda, S.13

[4] ebenda, Figure 7

[5] ebenda, Figure 1

[6] ebenda, page 4 & Figure 26

Stellen Sie sich vor, was passieren würde...

...wenn diese KI-basierten Angriffe gegen
unsere Nutzer immer effizienter werden

ODER

was passieren könnte,

wenn unsere Nutzer falsch geschult werden...



CYBERDISE



Gute Cybersecurity- Awareness hilft!



CYBERDISE



...und warum?

Um meine
Mitarbeiter klüger,
wachsamer zu machen
und mein Unternehmen
sicherer!



CYBERDISE



KI-basierte Fakes / Phishing-Angriffe: Was bedeutet das für mich?

KI ermöglicht es Kriminellen,

- mehr personalisierte Phishing-Angriffe zu erstellen...
- ...nein, viel bessere Phishing-Angriffe
- um neue Angriffsvektoren auszunutzen

- und diese massenhaft anzuwenden



Die Angreifer nutzen künstliche Intelligenz
bereits heute

Nutzen auch Sie die KI für
Schulungen und
Angriffssimulationen



CYBERDISE



Ein kurzes Framing: Was ist Cybersecurity-Awareness?

Das ist mein Verständnis davon:

Anpassbare Inhalte und Vorlagen für die Durchführung von Awareness-Programmen

Cybersecurity
LLM

Awareness
Trainings

Phishing &
Smishing
Exercises

«Phish
Button»
+Analyse



Let's get back to the topic

Warum sind die meisten Awareness-Maßnahmen heutzutage nicht besonders smart?

Phishing &
Smishing
Exercises

Awareness
Trainings

«Phish
Button»



Was macht eine gute Phishing-Übung aus?

Sie basiert auf einem realistischen Szenario!

- Im Kontext meines Unternehmens oder meiner Marke
 - Verwendet eine gefälschte Domain, die mein Unternehmen betrifft
 - „Vernünftiger / Plausibler“ Nachrichteninhalt
-
- Doch immer noch als Phishing (simuliert) erkennbar
 - An die Fähigkeiten des Nutzers angepasst
 - Keine einmalige Aktion



Aber ich stoße auf Phishing-Übungen, die...

Ohne Unternehmenskontext sind

- Meist nicht konkret mit dem Unternehmen oder der Marke verbunden
- Nutzen nicht verwandte Standarddomains
- Stehen nicht im Zusammenhang mit dem Unternehmen
- Haben eine eher geringe Qualität des Nachrichteninhalts
- Als Phishing von Weitem erkennbar
- An die Fähigkeiten der wenig erfahrenen Nutzer angepasst
- Keine einmalige Aktion sind (gut!)



Und was macht einen guten Schulungskurs aus?

- Unterhaltsam
- Abwechslungsreich (auch im Stil!)
- Messbar
- An den Unternehmenskontext angepasst
 - Ich bin hüte mich vor Kursen, die nur zu 90 % passend sind
 - Beinhaltet unternehmensspezifische Fragen
 - Wiedererkennung durch Farben, Schriftarten und Logos
- Nicht zu lang (+/- 5 Minuten)
- An die Fähigkeiten des Nutzers angepasst
- Keine einmalige Aktion



Und was macht einen guten Schulungskurs aus?

Und...

...als CISO vermittele ich zuerst meine eigenen Richtlinien!



Aber ich stoße auf Kurse, die sind

- nicht wirklich unterhaltsam
- nicht wirklich abwechslungsreich
- oft nicht messbar
- nicht an den Unternehmenskontext angepasst
- fast immer zu lang (über 5 Minuten)
- kaum an die Fähigkeiten des Nutzers angepasst
- meist keine einmalige Aktion (gut!)



Und ich habe noch nie den Fall gesehen

Wo der CISO zuerst seine eigenen Richtlinien vermittelt!

Sind Sie jemand, welcher das tut, dann sagen Sie es mir bitte!



Urteilen Sie selbst,
wo Sie stehen



...und zuletzt

Es gibt wissenschaftliche Beweise dafür, dass eLearnings nicht wirklich effektiv sind.



- Mitarbeiteraktionen stellen ein größeres Cyber Risiko dar als Hacks.
- **Traditionelle Schulungen verfehlen die Verhaltensänderung bei Risiken.**
- Maßgeschneiderte Ansätze verbessern die Risikodiagnose und -resilienz.
- Frühe Tests verbinden Einstellungen mit Risikoverhalten und zeigen das Potenzial der Tools.
- Phishing-Tests bewerten Risiken effektiv und sollten genutzt werden.

<https://www.mdpi.com/2227-9091/12/7/116>



CYBERDISE

Cyber Risks – Risks 07/24.pdf

Article
Towards Diagnosing and Mitigating Behavioral Cyber Risks


Carlo Pugnetti ^{1,*}, Albena Björck ², Reto Schönauer ³ and Carlos Casán ⁴

¹ Institute of Financial Services Zug IFZ, Lucerne School of Business, Sauerstoff 1, 63434 Rotkreuz, Switzerland
² ZHAW School of Management and Law, Zurich University of Applied Sciences, St.-Georgen-Platz 2, 8400 Winterthur, Switzerland; albena.bjorck@zhaw.ch
³ Schweizer Mobiliar Versicherungsgesellschaft AG, Bundesgasse 35, 3001 Bern, Switzerland; reto.schoenaue@mob.ch
⁴ Kessler & Co AG, Furchstrasse 95, 8002 Zurich, Switzerland; carlos.casan@kessler.ch

* Correspondence: carlo.pugnetti@bsl.ch

Abstract: A company's cyber defenses are based on a secure infrastructure and risk-aware behavior by employees. With rising cyber threats and normative training efforts showing limited impact, raising cyber risk awareness is emerging as a challenging effort. The review of the extant literature on awareness diagnosis shows interdisciplinary but mainly theoretical approaches to understanding attitudes and influencing risk behavior. We propose and test a novel methodology to combine and operationalize two tools, deep metaphor interviews and the IDEA risk communication model, to apply them for the first time in the context of behavioral cyber vulnerabilities. The results show a link between diagnosed attitudes and effective risk behavior in a real-life organizational setting, indicating the potential for an expanded diagnostic effort. We propose to develop a broader diagnostic and intervention set to improve cyber awareness and a toolset to support the business practice of cyber risk management.


Keywords: risk; cybersecurity; cyber risk; risk behavior; risk communication; risk mitigation

 **check for updates**

Citation: Pugnetti, Carlo; Björck, Albena; Schönauer, Reto; Casán, Carlos. 2024. Towards Diagnosing and Mitigating Behavioral Cyber Risks. *Risks* 12: 116. <https://doi.org/10.3390/risks12070116>

Academic Editor: Koyulsof Jung

Received: 6 April 2024
Revised: 21 June 2024
Accepted: 2 July 2024
Published: 19 July 2024



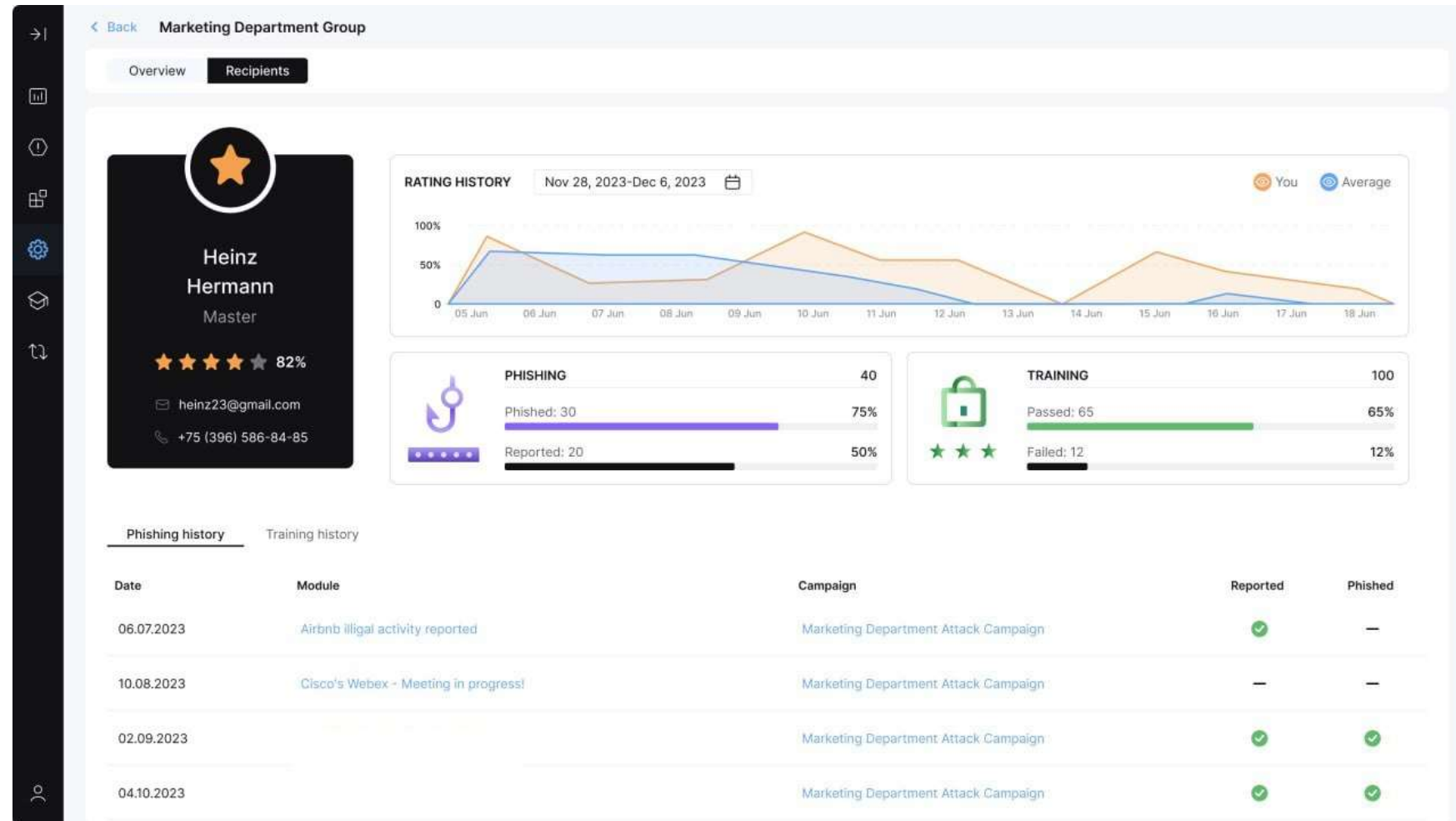
Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cyber risks, defined as risks affecting information technology assets and threatening the confidentiality, availability, and integrity of information and entire information systems (Bisener et al. 2015), pose a significant and growing threat. Cybercrimes already cost the world at least USD 6 trillion in 2021 and could lead to over USD 10 trillion worth of annual damages by 2025 (Morgan 2020). The continuous and increasing dependence on IT systems, and the surge in digitalization and the associated increase in the home office and hybrid work schedules, give attackers new opportunities to steal company data, smuggle malware into company networks, and steal money from companies using social engineering methods. While relatively new, cyber risks are among the top risks for every company—independent of size and industry (WEP 2022). The discussion of these risks in the public sphere and in the academic literature is driven primarily by technological development, individual and organizational vulnerabilities, and regulatory pressures. Academic research on the perception of cyber risks has spanned psychological, cultural, and human aspects, but cyber risk investigation remains challenging: First, with the rapid technological development and penetration of activities, new threats emerge constantly making the phenomenon highly dynamic, and any risk information and needed precautions need to be updated much faster and more often than other risks. Second, the cybercriminals and their networks remain anonymous, and a thorough investigation, if any, is not made public. Third, the technical sophistication and complexity of the topic prevent the involvement of larger stakeholder groups and the public in a wider risk discussion (Xu et al. 2021). Human error often leads to a cyber incident. For example, in the UK, 90% of cyber data breaches were caused by user errors in 2019 (CybSafe 2020). Recent

Risks 2024, 12, 116. <https://doi.org/10.3390/risks12070116> <https://www.mdpi.com/journal/risks>

Wo kann KI helfen?



Cyberdis Learning Management System and Cybersecurity Chatbot

CYBERDISE

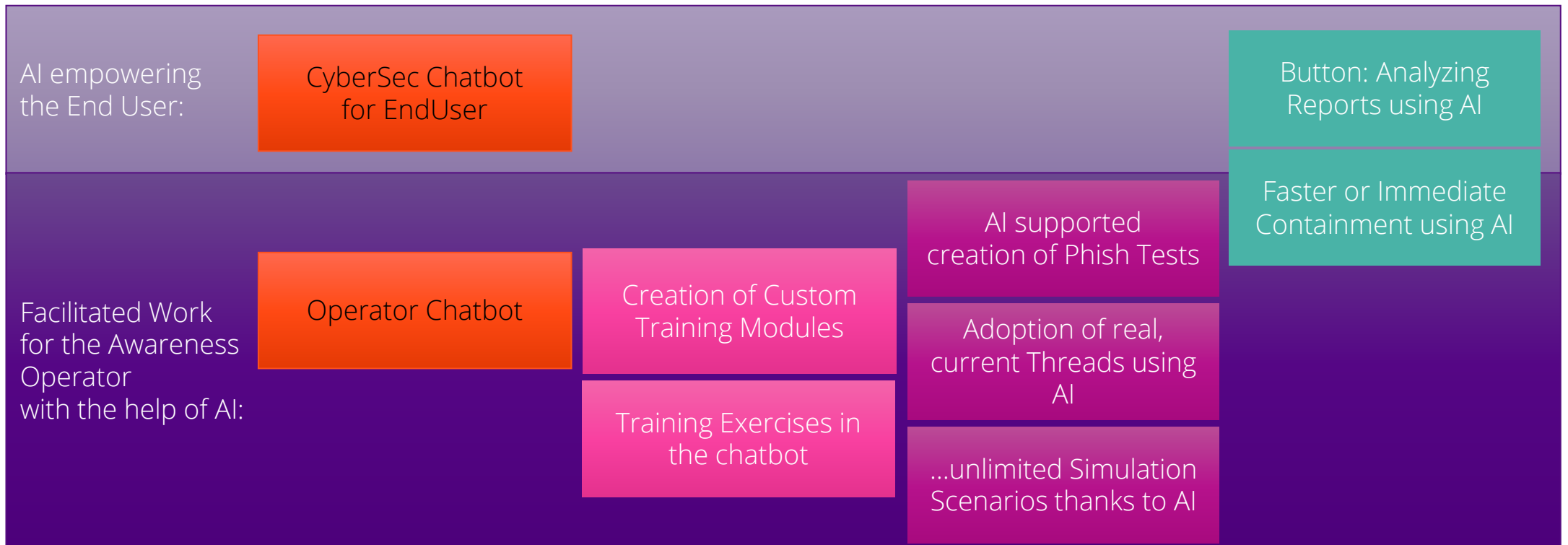


KI-Funktionen innerhalb einer Awareness Lösung

Erleichterung bei verschiedenen Ebenen und in mehreren Bereichen

- **Cybersecurity-Chatbot, Trainings im Chatbot integriert**
- **KI-generierte Spear-Phishing-Nachrichten und Landingpages**

Mehr dazu unten:



“Als wir die Schwachstellen der Awareness Branche erkannten, haben wir beschlossen, es mit einem neuen Produkt und Services deutlich besser zu machen!”

Palo Stacho, Geschäftsführer und Gründer



Besuchen Sie uns in
Halle 6 - Stand 6-246
und erhalten Sie einen
20 % it-sa
Rabattgutschein
für Cyberdise
(Software und
Dienstleistungen)

A screenshot of a chat application interface. On the left, there is a sidebar with a '+ New Chat' button and several chat history items, including 'welches sind die ...', 'was sind die schritte zur...', 'what basic awareness tr...', 'most effective phishing ...', 'What are the phases in a...', and 'was sind die schritte zur...'. The main chat area is titled 'Query' and contains a list of 34 numbered steps for a phishing simulation. At the bottom, there is a text input field with the text 'was sind die schritte zur perfekten Phishing Simulation?' and a blue send button.

Query

+ New Chat

welches sind die ...

was sind die schritte zur...

what basic awareness tr...

most effective phishing ...

What are the phases in a...

was sind die schritte zur...

2. Ziele festlegen

3. Vorheriges Training verstehen

4. Analyse und Verständnis für die aktuelle Internetnutzung der Mitarbeiter

5. Infrastruktur verstehen

6. Entscheiden, wo die Simulation(en) gehostet werden sollen

7. Technische Aspekte aus der Sicht des Benutzers verstehen

8. Erstmalige Kommunikation

9. Benutzer in die Lage versetzen, verdächtige E-Mails zu identifizieren und zu melden

10. Soll das Training zuerst durchgeführt werden?

11. Richtige Menge und Häufigkeit auswählen

12. Die richtige Gruppe von Personen auswählen

13. Über den Datenschutz nachdenken

14. Technische Anforderungen für den Webinhalt ausarbeiten

15. Die Grenzen des Angriffs oder der Trainingsszenarien kennen

16. Den richtigen Szenariotyp auswählen und ein wenig böse werden

17. Soll es echt aussehen oder nicht?

18. Eigener Kontext zum Szenario hinzufügen

19. Die richtige E-Mail-Absenderdomäne auswählen

20. Entscheiden, was passieren soll, wenn Benutzer auf die Angriffssimulationen reagieren

21. Entscheiden, was passieren soll, wenn der Benutzer direkt auf die Phishing-Domäne zugreift

22. Den richtigen Angriffstyp auswählen

23. Über die Verwendung von Marken Dritter in einem Angriff entscheiden

24. Ob und wann zur E-Learning-Einladung im Falle eines erfolgreichen Angriffs eingeladen werden soll

25. Nachfolgendes Follow-up-Training

26. Disziplinarmaßnahmen für den wiederholten Fall definieren

27. Testläufe

28. Entscheiden, wann eine Awareness-Kampagne geplant werden soll

29. Kampagne starten und überwachen

30. Berichterstattung

31. Nachfolgende Kommunikation

32. Belohnungen und Anreize definieren

33. Die nächsten Schritte definieren

34. Von vorne beginnen

was sind die schritte zur perfekten Phishing Simulation?

Laden Sie hier die Präsentation und
die Studie herunter:



CYBERDISE

cyberdise-awareness.com

Vielen Dank! palo.stacho@cyberdise.io

