



Phishing Trainings im Kontext – Praxisbeispiel der Swisscom (Schweiz) AG

Marcus Beyer, Security Awareness Officer bei Swisscom Group Security



Ein falscher Klick

...



Eine dringliche Mail

...



Ein unachtsamer Moment

...



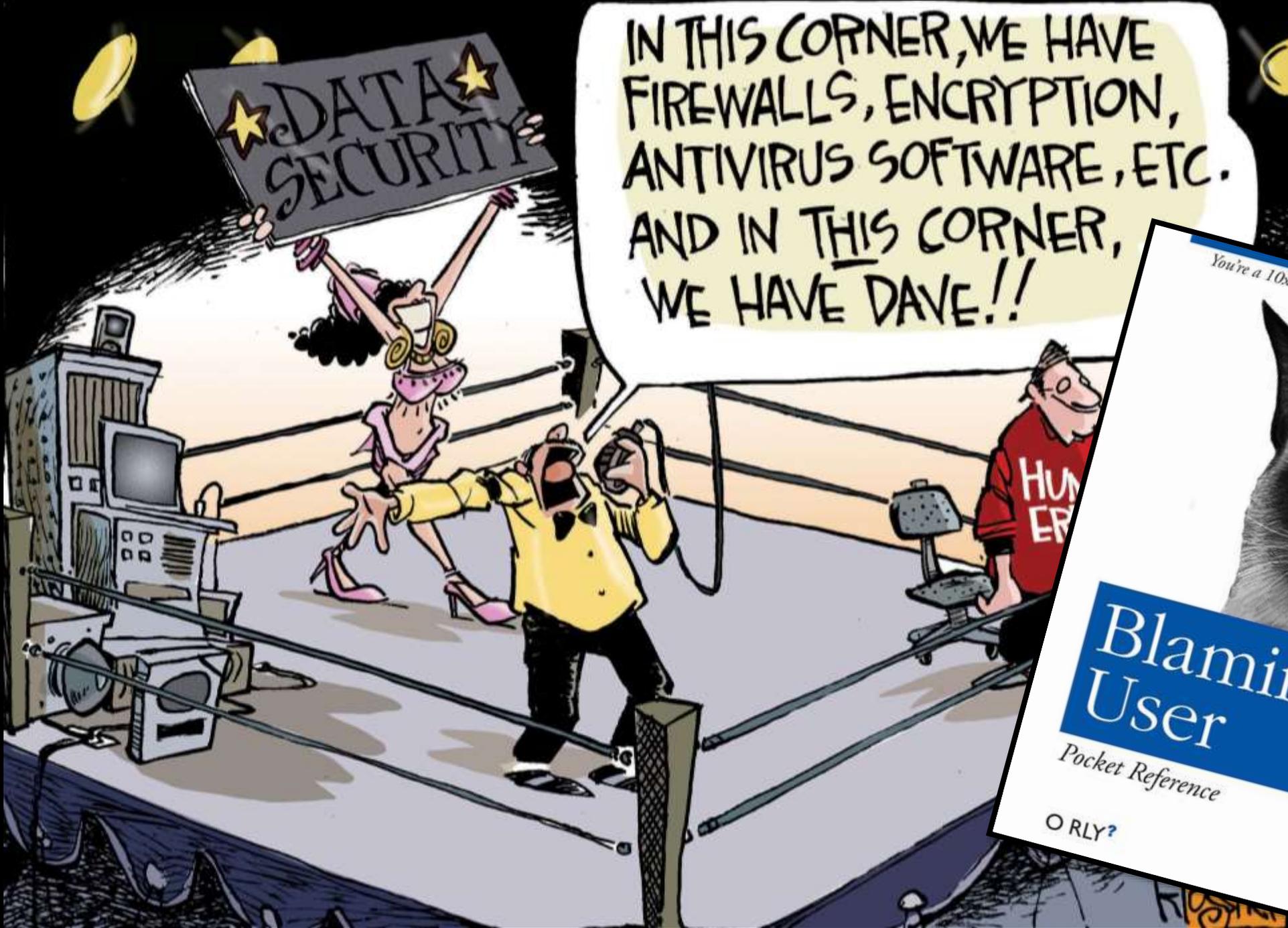
82%

aller IT-Sicherheitsvorfälle
sind auf das menschliche
Fehlverhalten zurückzuführen.

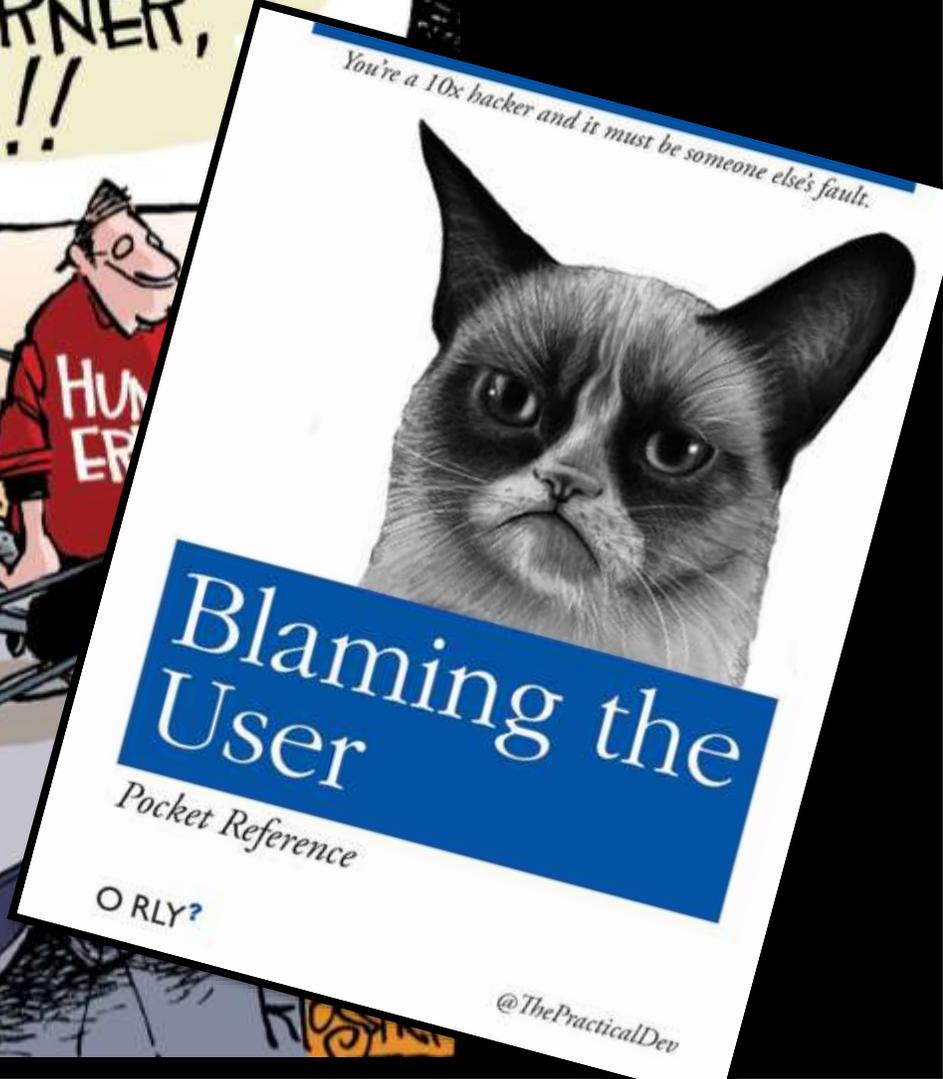


Alle machen Phishing Traininings – und ihr?





Marcus Beyer, Swisscom (Schweiz) AG, ITSA 2024, CI - Public





Wie das Hoxhunt System zur Verhaltensänderung funktioniert?





Marcus Beyer, Swisscom (Schweiz) AG, ITSA 2024, C1 - Public

Das richtige Mindset.



I hacked Swisscom and all I got was this lousy sticker.



Angebote für die interne Security Community



Wertschätzung



Interessante und "andere" obligatorische Schulungsformate



Gamification

Immersive Erlebnisse schaffen

Human Centred Security



Nah an den "Lebenswelten"



Security positiv beleben

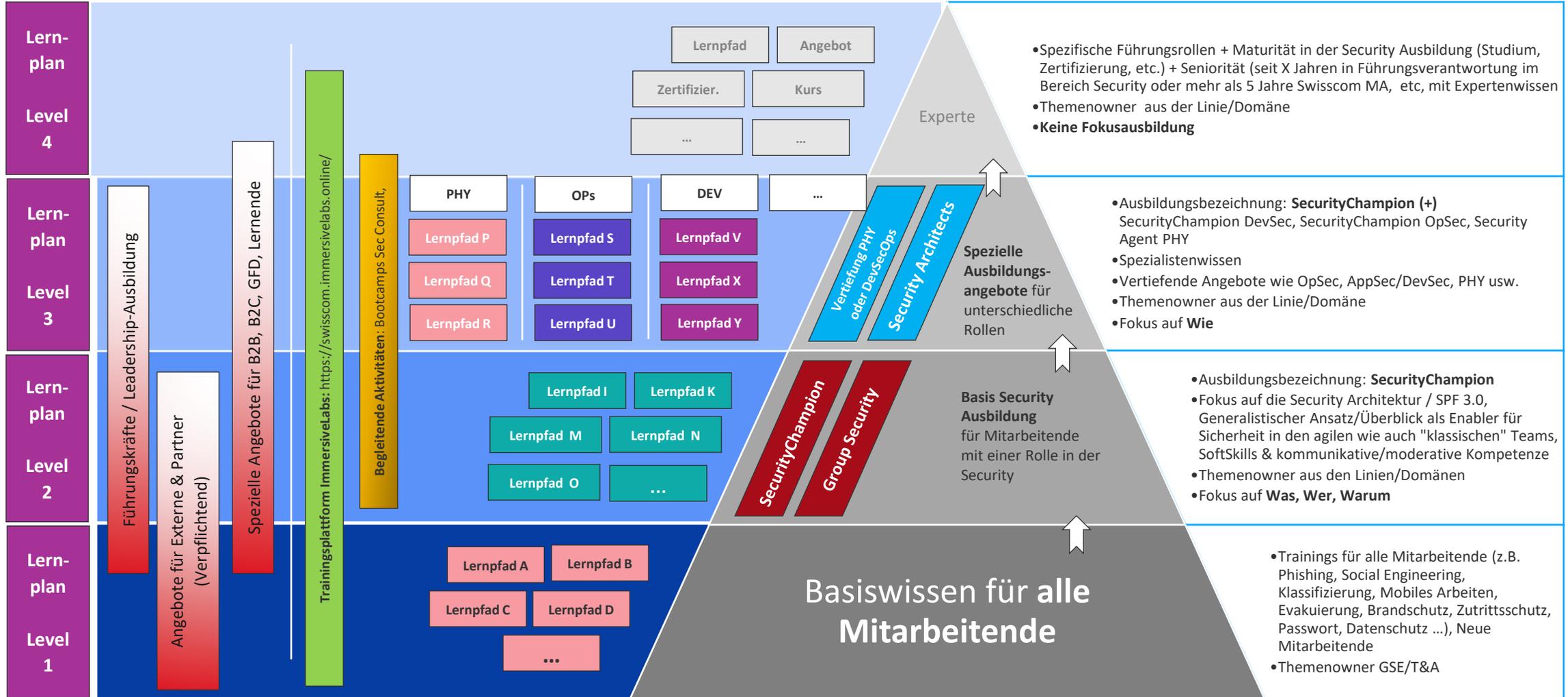


Führungskräfte trainieren und involvieren





Struktur Security Ausbildung- und Trainingsprogramm: Gesamtübersicht SecurityPeaks

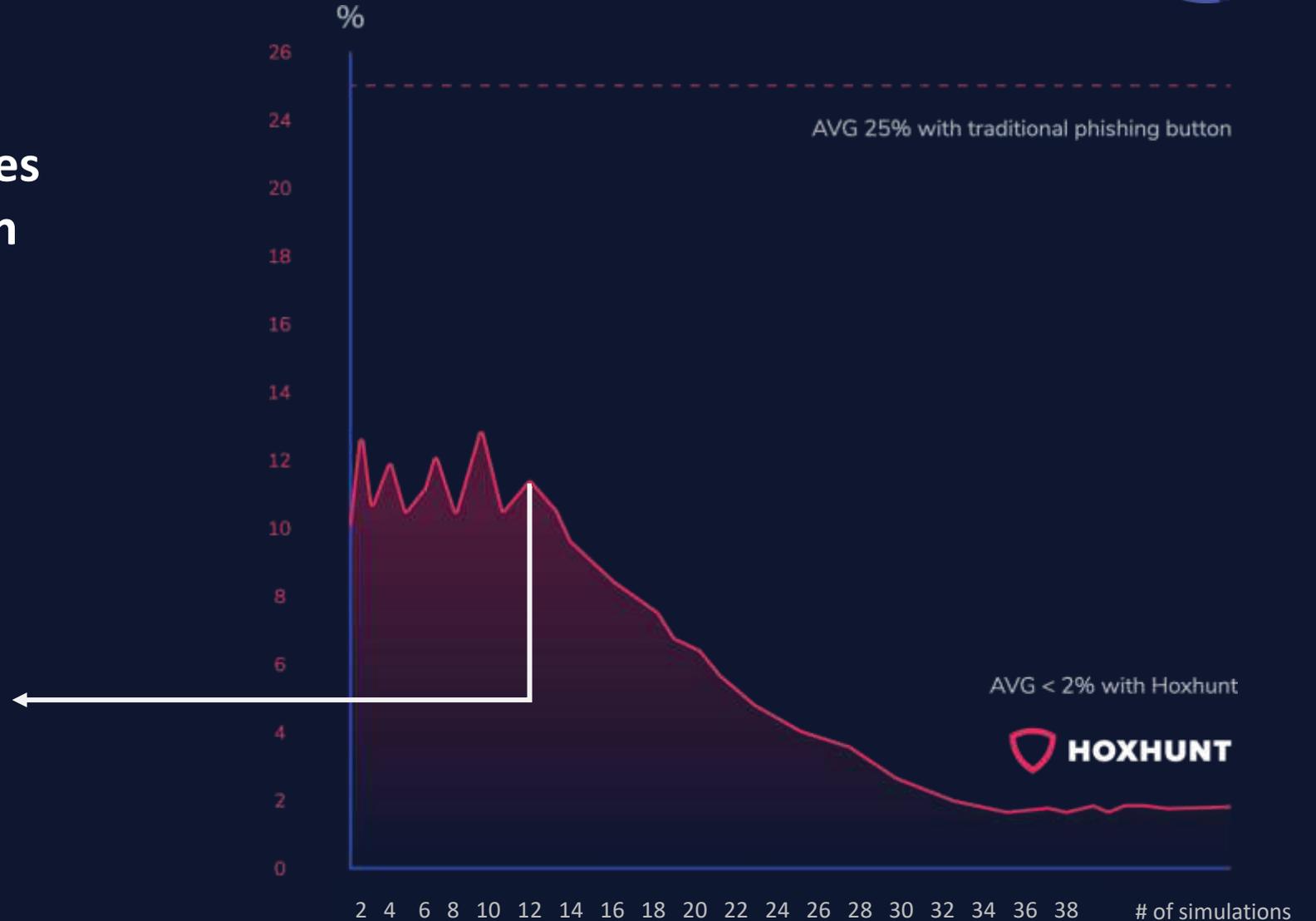




Unsere Ziele - Warum

Risiko durch menschliches Fehlverhalten reduzieren

Keine Veränderung der Fehlerquoten vor 12 Angriffssimulationen.

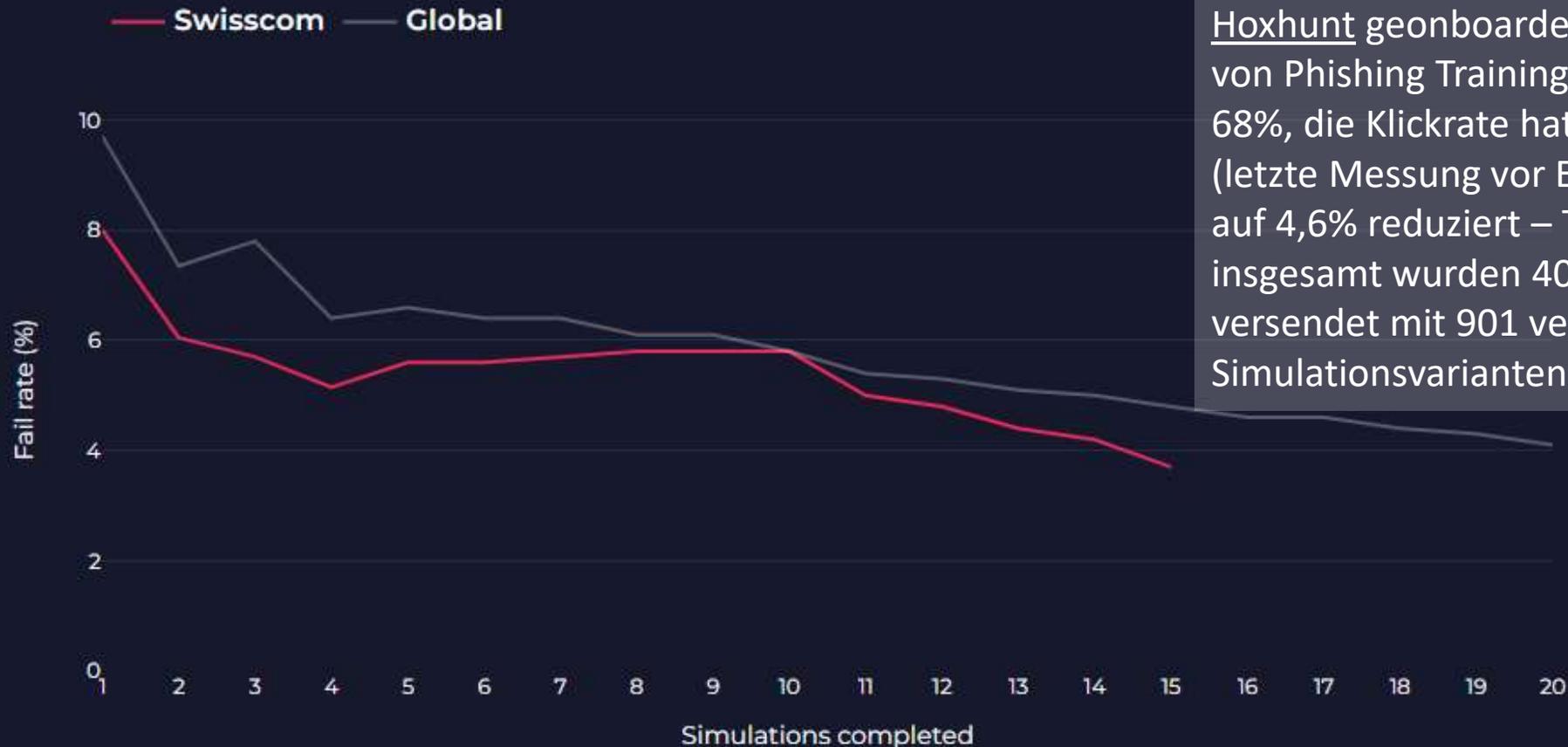


Fail rate progress

Mean fail rate corresponding to number of simulations completed.

A simulation is considered completed after being failed, reported or missed.

Export Data



Rückblick 2023: Über 18'000 Mitarbeitende von Swisscom und Konzerngesellschaften auf dem Trainingsportal von Hoxhunt geonboarded, die Erkennungsrate von Phishing Trainingsmails liegt bei über 68%, die Klickrate hat sich von 26,7% in 2021 (letzte Messung vor Einführung von Hoxhunt) auf 4,6% reduziert – Tendenz weiter fallend, insgesamt wurden 405'341 Trainingsmails versendet mit 901 verschiedenen Simulationsvarianten.



Phishing training performance

Absolute change ▾

Last 365 days ▾

Your organization's performance on the phishing training compared with others in the IT, software, internet industry.



Engagement

Onboarding rate

88.9%

▲ 15.74%pts in the last 365 days

79.1%

Industry

Average reporting time

10h 43m

▼ -1h 31m in the last 365 days

8h 32m

Industry

Activity rate ⓘ

82.2%

▲ 6.13%pts in the last 365 days

68.7%

Industry

Training overview

Success rate

72.9%

▲ 5.14%pts in the last 365 days

62.9%

Industry



Fail rate

2.5%

▼ 2.41%pts in the last 365 days

4.0%

Industry



Started entering credentials ⓘ

98 instances

▲ 98 in the last 365 days



Miss rate

24.6%

▼ 2.74%pts in the last 365 days

33.1%

Industry





Anti Phishing Training mit Hoxhunt: Gamification pur



Marcus Beyer, Swisscom (Schweiz) AG, ITSA 2024, C1 - Public

HOXHUNT x swisscom

Dashboard | Schritte | Erfolge | Ranglisten | Marcus Beyer

Bronze | Stahl | Silber | Gold | Platin

Rangliste (Quartal 4 2024) | Alle anzeigen

Sie gehören zu den besten 45 % aller Kolleginnen und Kollegen in diesem Quartal. Weiter vor!

Glückssträhnen

Aktuelle Serie: 2 | Längste Serie: 25

Phishing-Training

87% | 11 Monatsstatistiken

- 27 gemeldet
- 1 angeklickt
- 3 eingepostet

Erfolge | Alle anzeigen

Wieder: Quiz-Experte (Schließen Sie 20 Quizze ab)

Erstmalig: Golden Eye (30 Simulationsmail markieren)

Aktivitäten

Swisscom	CSA	Alle Abteilungen
BS00	Annalisa Gonzalez Schw...	75%
BS01	Marco Palmieri	75%
BS02	Marcus Beyer	70%



OUTLOOK FOR DESKTOP

OUTLOOK ON THE WEB

OUTLOOK FOR MOBILE



HOXHUNT INSIGHTS

Timeframe: Year to Date (YTD) | Group By: Whole Organization | Export as CSV

Overview | Users | Training packages **NEW**

Toggle Columns

Viewing 1 - 20 of 34

TOPIC	QUIZ	SUCC	FAIL	SKIP	SEEN	SUCC %	FAIL %	SKIP %
Browsing Internet Securely	Digital identity	2027	357	52	2436	83.2%	14.7%	2.1%
Browsing Internet Securely	Keeping your browser updated	167	19	0	186	89.8%	10.2%	0.0%
	Data Storage	1520	277	34	1831	83.0%	15.1%	1.9%
	Restarting devices	1	0	0	1	100.0%	0.0%	0.0%
	Keeping devices always updated	552	98	8	658	83.9%	14.9%	1.2%
	Mobile Device Security	2770	102	29	2901	95.5%	3.5%	1.0%
	Ransomware	878	43	666	1587	55.3%	2.7%	42.0%
	Incident Response	494	93	541	1128	43.8%	8.2%	48.0%
	Common sources of malware	9	3	0	12	75.0%	25.0%	0.0%

HOXHUNT

Prohibited Activities

Which of the following practices is allowed based on Hoxhunt Information Security Policy? Need a hint? Training card will help you out.

- Compromising confidential information
- Introducing Malware
- Cracking an information system
- None of the above

Customized Content
Training card 3/4

★★★★

3/4/24



Admin - Hoxh... AutoSave Information Security Policy Internal Confidential Search (Cmd + Ctrl + U)

Home Insert Draw Design Layout References Mailings Review View Comments Editing Share

Paste Aptos (Body) 11 B I U X₁ X₂ Styles Pane Dictate Sensitivity Add-Ins Editor Copilot

Information Security Policy

A document that outlines the principles and practices for protecting the confidentiality, integrity, and availability of information assets.

1. Introduction

This document defines the information security policy of the organization, which is a set of rules and guidelines that govern the management, protection, and use of information assets. The policy applies to all employees, contractors, vendors, and partners who access, process, store, or transmit information on behalf of the organization. The policy also covers the physical and logical infrastructure, systems, and devices that support the information activities of the organization.

The purpose of this policy is to:

- Establish a framework for information security governance and accountability.
- Identify the roles and responsibilities of information owners, custodians, and users.
- Define the classification and handling of information assets.
- Specify the minimum requirements and controls for information security.
- Ensure compliance with applicable laws, regulations, standards, and contracts.
- Promote a culture of information security awareness and best practices.

The scope of this policy covers all information assets that are owned, leased, or entrusted to the organization, regardless of their format, location, or mode of transmission. The policy also applies to all information activities that are performed by or on behalf of the organization, including but not limited to: creation, collection, processing, storage, transmission, dissemination, retention, disposal, and destruction.

The policy is aligned with the international standard ISO/IEC 27001:2017, which specifies the

Human Risk Dashboard
User Management
Phishing Training
Security Awareness
Micro-Training
Training Packages
Reports
Automations
Settings
Knowledge Base
Account settings
Logout
Ilmari Kontulainen
Hoxhunt Demo

ding 19.37

Page 1 of 6 2239 words Finnish Accessibility: Good to go Focus 192%



#BeTheStrongestLink



Delete Archive Junk Sweep Move to Categorise Undo

DEMO1 ★ Filter

Jane Smith
> Test email with a very specifi... 04/01/2022
No preview is available.

2019

Hoxhunt
Welcome to HoxHunt! 15/10/2019
You've been invited to join HoxHunt! HoxHu...

2017

DHL Express
DHL Shipment Notification : 79... 31/10/2017
Dear Customer Your shipment(s) listed belo...

Test email with a very specific subject

JS Jane Smith
Tue 04/01/2022 14:47
To: Jane Smith

Reply | Forward

Hoxhunt Report





Feedback Rules

Manage rules, set up conditions, and choose a response to notify employees about safe emails. [Read more about how to use this feature safely.](#)



+ Create new rule

Analytics

2023-03-16 → 2024-10-16

Total activity 153,187 0.00% last 580 days	Active users 16,558 out of 19999 users 0.00% last 580 days	Unique rules hit 38 0.00% last 580 days
--	--	---

Rules (26)

ACTIVE	NAME	MESSAGE TO USER	EXPIRY DATE	ACTIVITY 2023-03-16 - 2024-10-16	
<input checked="" type="checkbox"/>	internal message swisscom	Safe email	No expiration	 23k	 
<input checked="" type="checkbox"/>	surveys.swisscom.com	Safe email	No expiration	 390	 
<input checked="" type="checkbox"/>	1brd.com	Safe email	No expiration	 206	 



User Feedbacks (Auszug):



Bitte aktivieren Sie Ihr Training, indem Sie diese E-Mail jetzt melden

1. Finden und klicken Sie auf die Schaltfläche „Report this email“ in Ihrer E-Mail-Umgebung.
2. Klicken Sie auf die Schaltfläche, um jetzt loszulegen!

Wenn Sie die Schaltfläche nicht finden können, lesen Sie unseren [Leitfaden zur Problembehebung](#).

13:05

GEILER SCHEISS!!!

😊

Zuerst war ich so... häääää!!!!

Aber genau diese "Schock" Momente bleiben einem

13:06

Ja, so wird darauf hingewiesen... also, hast du den Button? wenn ja, dann melde diese Mail...

13:06

Du bist so nice level 😊

Die Email confused mich zwar auch ein bisschen 😊 Und da werden wir vielleicht auch ein WOW Effekt ist es das wert 😊

Can I include my +70 years old parents to the foxhunt?

Would be a great possibility to sensitize them?

@foxhunt Marcus Beyer

8 hours · 1 answer · 99 Views

ANSWER RECOMMEND

Answers (1)

★ ★ ★ ★ ★

Marcus Beyer · GSA-GSE-BEL · Security Awareness Officer
1 min

Its Hoxhunt... and sorry, we cant integrate Phishing Training. But look on Swisscom Trainings for your parents - also for sec

Kann man den Gamification-Mist in Hoxhunt deaktivieren?

Ich habe zwei Hoxhunt-Testmails erhalten und beide gemeldet. Schön und gut, brauche ich kein automatisch aufpoppendes Fenster, das mir 5 von 5 Sternen etc. erzählt und bei dem ich diverse Seiten durchklicken muss um es schliessen kann. Solches Verhalten erwarte ich normalerweise nicht von solchen mit Werbung vollgemüllten Free-To-Play-Apps, die ich nicht meide...

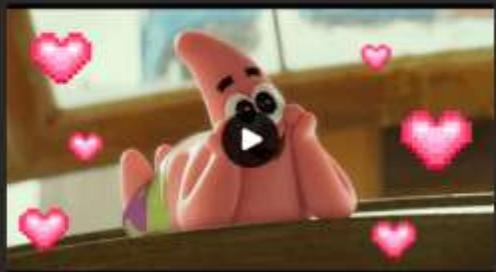
10:38

ach du meine güte ist das geil mit hoxhunt!!!!!!

kann ich gerade richtig feiern

SO muss security!

nicel



(gerade meine erste mail gemeldet und micro training abgeschlossen)

15:31

Ich finde es absolut frech, wenn Hoxhunt Mails mit meinem Namen versendet, kann man da nicht einen Fake User oder sowas nehmen? Wollte das einfach mal kurz loswerden.....

Gestern 17:11

Eigentlich gibt es gar nichts zum beruhigen, das ist super, dass Hoxhunt das macht

👍 1

Ich finde die Training E-Mail wirklich gut, die man da bekommt! Das macht Hoxhunt wirklich nice

👍 1

Gestern 17:11

jup..

erst beschweren sich die leute, dass dhl und co. zu "generisch" ist

und wens dann richtung spearphishing geht gibts auch nen aufschrei 😊 aber ja man kanns nicht allen recht machen, grundsätzlich cool, dass das über hoxhunt möglich ist

👍 1



Mehr zum Thema? Gern im Podcast mit Marcus Beyer (Swisscom) und Katja Dörlemann (SWITCH) auf www.securityawarenessinsider.ch.



Marcus Beyer

Swisscom (Schweiz) AG / Group Security
marcus.beyer@swisscom.com



HOXHUNT

Halle 9 . Stand 212