Herzlich Willkommen

Hacker lieben Menschen:
Warum IT-Sicherheit nicht nur Technik ist

Hansmartin Amrein

Leiter Wirtschaftsraum Bern | Leiter Wirtschaftsamt Bern

Alec von Graffenried

Stadtpräsident Bern

Stefan Aegerter

Verkaufsleiter KMU Bern Mittelland
Swisscom (Schweiz) AG

Unsere Referent*innen

Lea Zimmerli
Penetration Tester
United Security Providers AG
lea.zimmerli@united-security-providers.ch

Bruno Kunz
IT Security Assessor
Swisscom (Schweiz) AG
bruno.kunz@swisscom.com

Agenda

1. **Begrüssung**

   Alec von Graffenried, Stadtpräsident Bern
   Stefan Aegerter, Verkaufsleiter KMU Bern Mittelland

2. **«Hacker lieben Menschen: Warum IT-Sicherheit nicht nur Technik ist»**
   Bruno Kunz, IT Security Assessor

3. **«Phishing und Multi-Faktor-Authentifizierung: Trügerische Sicherheit»**
   Lea Zimmerli, Penetration Tester

4. **Apéro Riche & Networking**

Hacker lieben Menschen

Warum IT-Sicherheit nicht nur Technik ist

22. Oktober 2024, Bruno Kunz

swisscom

C2 General

Zu meiner Person

Bruno Kunz

IT Security Assessor

Dozent für IT-Sicherheit

Security Evangelist

Themen

- Bedeutung des Faktors Mensch in der IT-Sicherheit
- Arten von menschlichen Fehlern
- Fallbeispiele und Konsequenzen
- Massnahmen zur Reduzierung menschlicher Fehler

Denken Sie nicht an Pizza!

Ist es wirklich so schlimm?

80 – 90%

Schätzungen zufolge sind etwa 80 bis 90 % der IT-Sicherheitsvorfälle auf menschliche Fehler zurückzuführen.

Quelle: IBM, Verizon Data Breach Investigation, Kaspersky

Im Vergleich mit der Luftfahrt

70 – 80%

In der Zivilluftfahrt werden etwa 70 bis 80 % der Sicherheitsvorfälle und Unfälle auf menschliche Fehler zurückgeführt.

Quelle: ICAO, FAA

Bedeutung des Faktors Mensch in der IT-Sicherheit

Definition des menschlichen Faktors in der IT-Sicherheit.

Warum Menschen oft das schwächste Glied in der Sicherheitskette sind.

Warum haben Hacker so ein leichtes Spiel?

Definition des menschlichen Faktors in der IT-Sicherheit.

Der menschliche Faktor in der IT-Sicherheit bezieht sich auf die Rolle und das Verhalten von Menschen, die mit IT-Systemen interagieren. Obwohl Technologien wie Firewalls und Verschlüsselung zum Schutz von Systemen beitragen, bleibt der Mensch oft die grösste Schwachstelle.

Windows

www

Passwort

E-Mail

Zugriff

Integrität

Ja, es geht auch vorsätzlich.

Morrisons

Gehaltsdaten von 100’000 Mitarbeiter

Weil Unzufrieden

Klagen und finanzielle Folgen

Coca-Cola

Versuch Rezepte und Produktinformationen an Pepsi zu verkaufen

Finanzielle Motive

TESLA

Sabotage der Fertigungssysteme und Datendiebstahl von vertraulichen Daten

Weil nicht berücksichtigt bei Beförderung

Störung der Produktion

UBS | PaineWebber

Daten löschen und Betrieb stören

Verärgert über Bonus

Mehrere Millionen Schaden

Quellen: BBC News, CNN, CNBC, New York Times

Warum Menschen oft das schwächste Glied in der Sicherheitskette sind.

Menschen sind oft das schwächste Glied in der IT-Sicherheitskette, weil sie anfällig für Fehler und Manipulation sind, die von Angreifern ausgenutzt werden können.

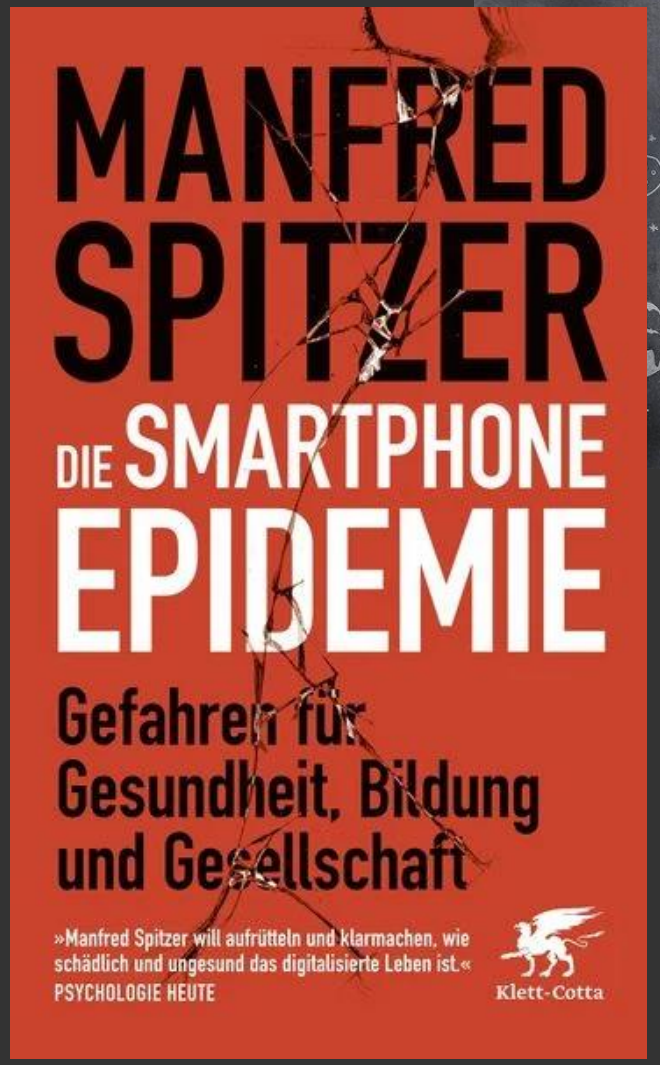
- Fehlende Sensibilisierung und Schulung
- Schwache Passwörter und Passwort-Management
- Unachtsamkeit und Routine
- Social Engineering

Warum haben Hacker so ein leichtes Spiel?

Da müssen wir weit zurück

Wir lernen den Umgang mit Medien

…also vermeintlich



Was hat das mit dem Alter zu tun?

Jüngere Menschen (18 – 35), insbesondere die Generationen Y (Millennials) und Z, haben zwar einen hohen technischen Sachverstand und sind oft digital versierter, aber sie neigen dazu, mehr Risiken einzugehen.

Ältere Erwachsene und Mitarbeiter ab 50 Jahren fallen zwar weniger häufig auf Phishing herein, sind jedoch möglicherweise weniger vertraut mit modernen Sicherheitstechnologien und aktuellen Bedrohungen.

Quelle: Stanford University, Tessian

Welche Arten von menschlichen Fehlern haben wir ausgemacht?

Quelle: BZ, TagesWoche

Welche Arten von menschlichen Fehlern haben wir ausgemacht?

Phishing und Social Engineering

Schwache Passwörter

Unachtsamkeit und mangelndes Bewusstsein

Missachtung von Sicherheitsrichtlinien

Ein schwaches Passwort wie 12345 nutzt heute doch niemand mehr. Oder?

30% verwenden Passwörter wie 123456, password, Passw0rd, etc.

50% der beliebtesten Passwörter sind sehr schwach und per BruteFoce einfach zu knacken.

91% der Passwörter sind zu kurz, zu einfach oder mehrfach verwendet.

Sony Pictures Hack 2014

Initialer Angriff und Einbruch

Phishing und Social Engineering

Datenexfiltration

Drehbücher, Filme, vertrauliche Dokumente

Veröffentlichung und Drohungen

Einschüchterung von Sony Mitarbeitern, Erpressung

Yahoo-Datenlecks 2013 - 2014

Initialer Angriff und Einbruch

Phishing und Social Engineering

Datenexfiltration

3 Milliarden Nutzerkonten

Konsequenzen

Massive Untersuchungen und Klagen, Verlust an Marktwert

Equifax-Datenleck 2017

Initialer Angriff und Einbruch

Bewusste Vernachlässigung eines Sicherheitspatches

Datenexfiltration

Sensible persönliche (Kreditprüfungs-)Daten von 147 Millionen Menschen

Konsequenzen

Massive Klagen, Entschädigungszahlungen, Verlust an Reputation

Uber-Datenleck 2016 (vertuscht bis 2017)

Initialer Angriff und Einbruch

Schwache Zugangsdaten von einem Drittanbieter auf GitHub hinterlassen

Datenexfiltration

Daten von 57 Millionen Nutzern und Fahrern

Konsequenzen

Massive Klagen, Entschädigungszahlungen, Verlust an Reputation

VARTA-Angriff 2024

Initialer Angriff und Einbruch

Ransomware und Social Engineering

Folgen

In 5 Werken Produktionsunterbruch, schwere Wiederherstellung der Systeme

Konsequenzen

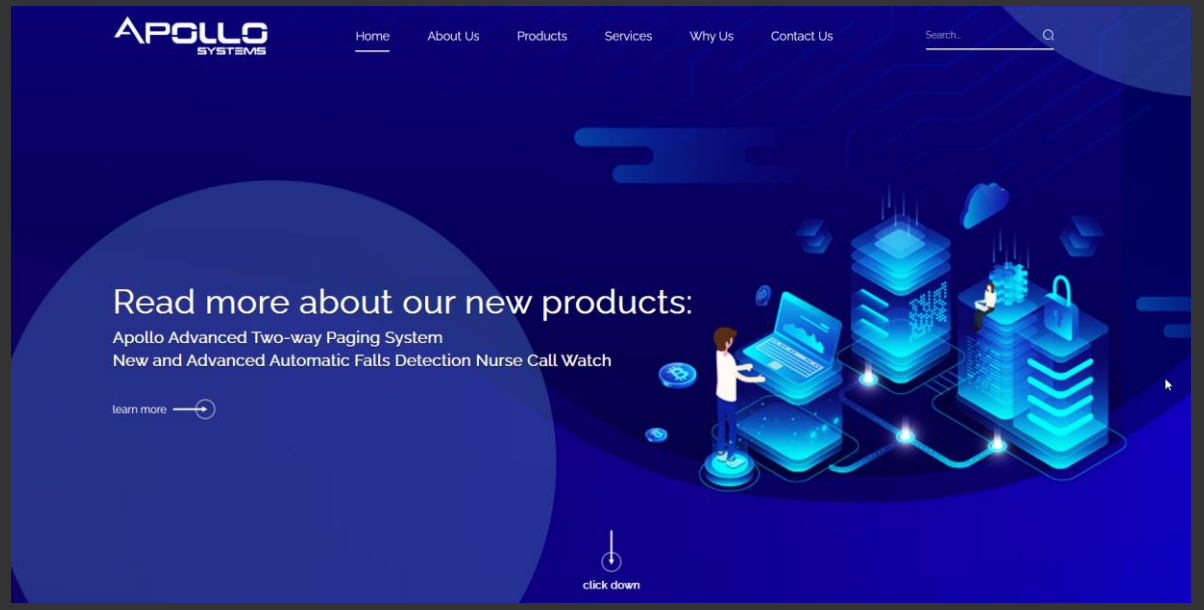
Aktieneinbruch 5%, hohe Schadenskoten

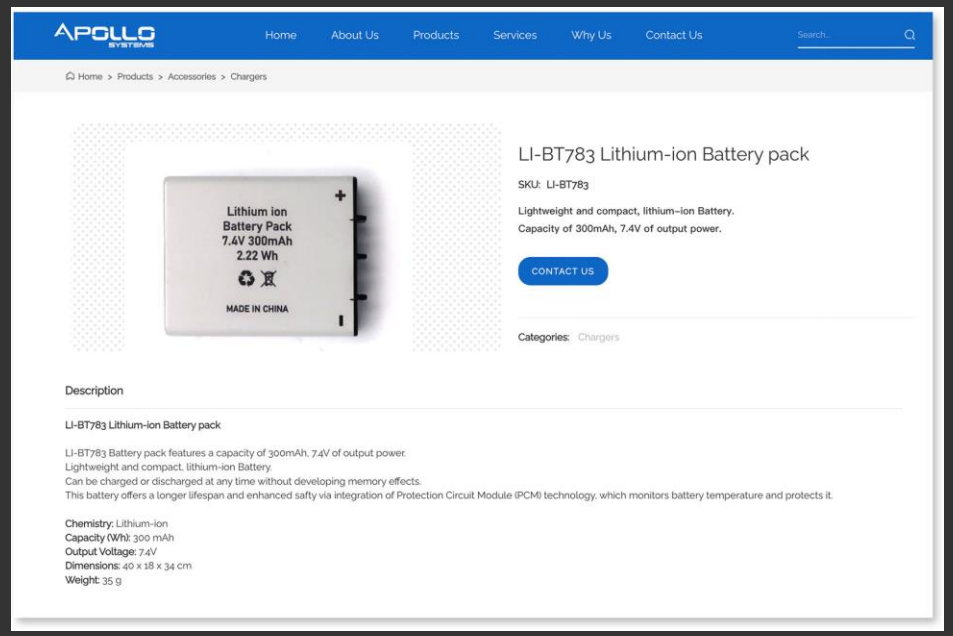
Was kann denn passieren?

Pager-Angriff 2024

Initialer Angriff

Gefakte Websites, Storyline





Was können wir dagegen tun?

Quelle: Lufthansa Aviation Training

Was können wir dagegen tun?

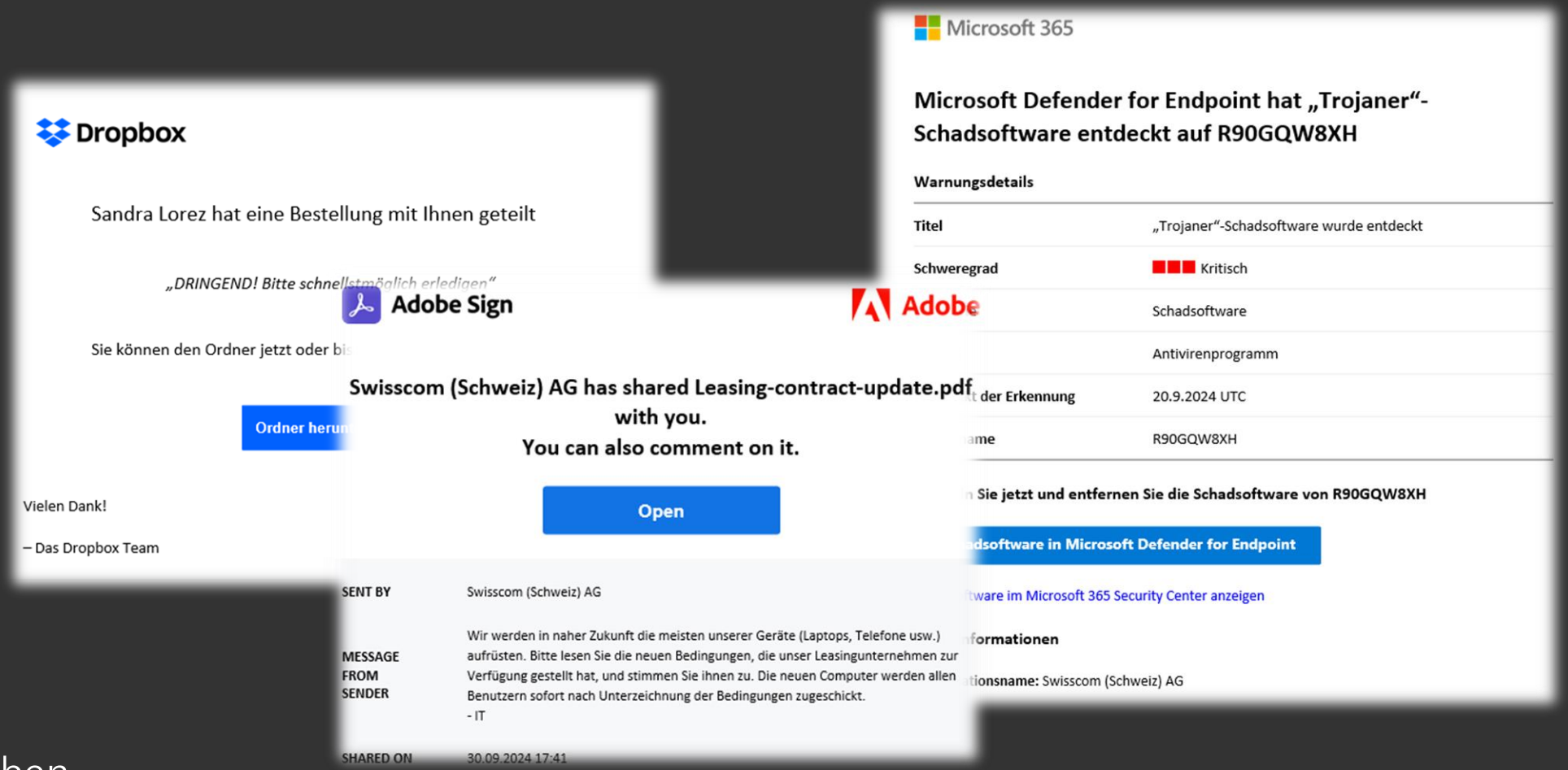
Schulung und Sensibilisierung

Starke Passwortrichtlinien und Multi-Faktor-Authentifizierung

Sicherheitskultur im Unternehmen

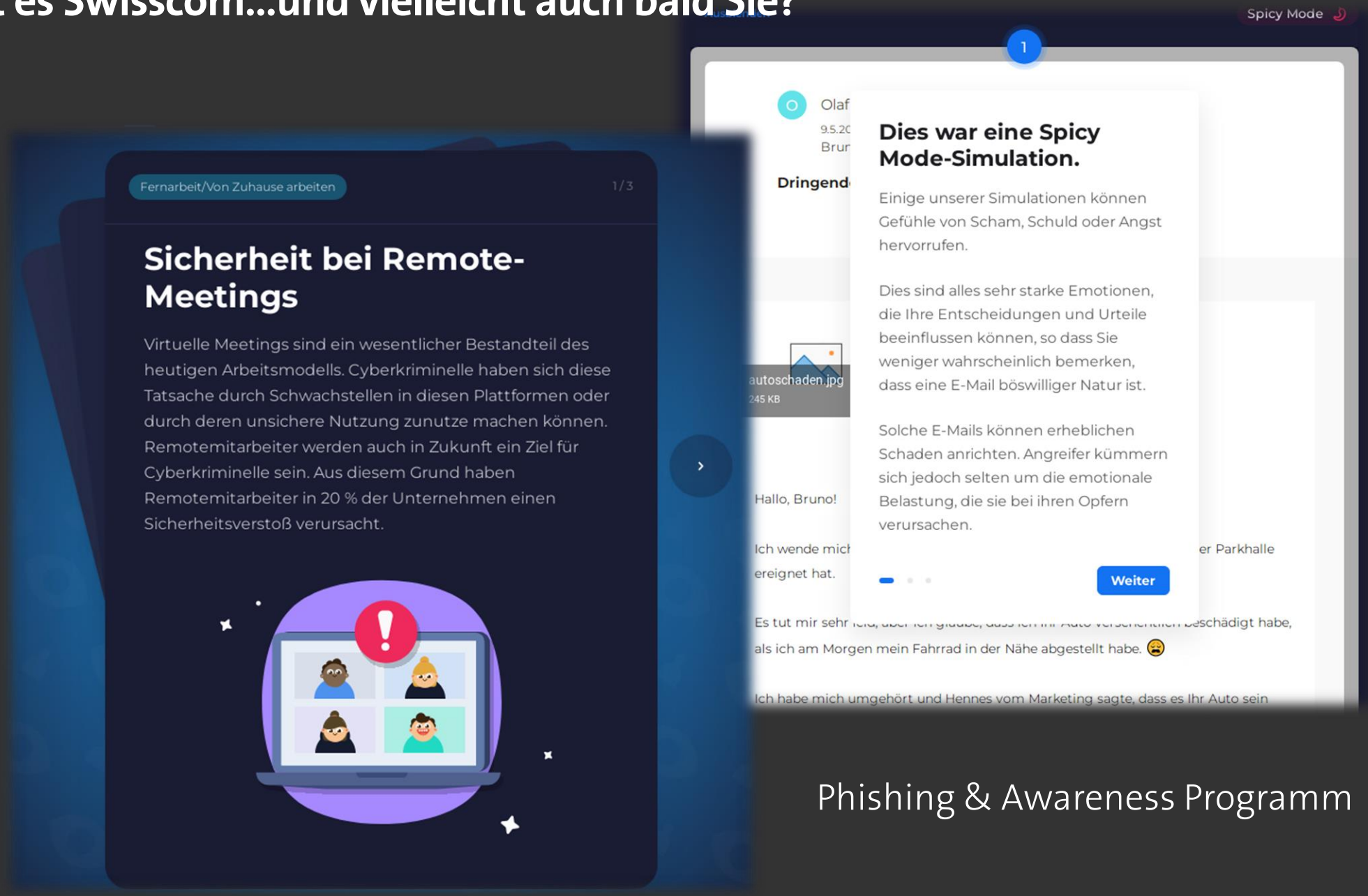
Technologische Unterstützung

Wie macht es Swisscom…und vielleicht auch bald Sie?



üben, üben, üben…

Wie macht es Swisscom...und vielleicht auch bald Sie?

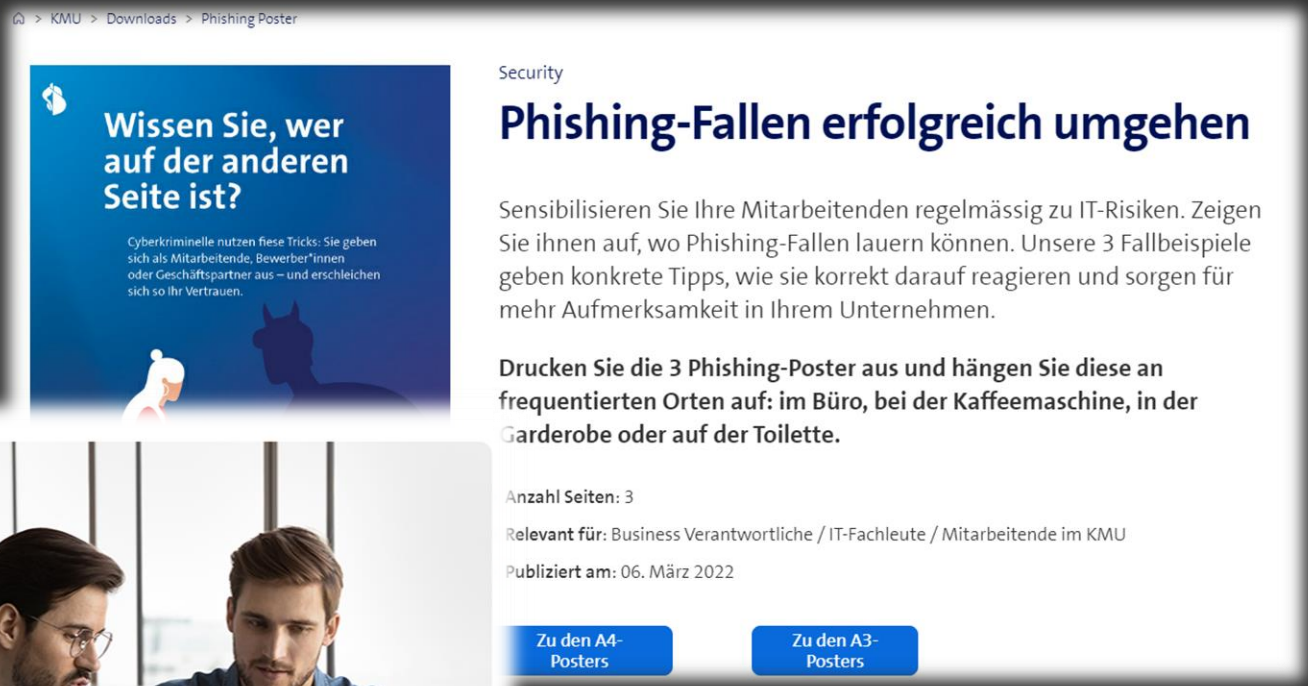


Phishing & Awareness Programm

Bereiten Sie sich vor!

[Security Awareness Training | Swisscom]

[Phishing Poster | Swisscom]



Q&A

Vielen Dank
… und bleiben Sie misstrauisch!

UNITED SECURITY PROVIDERS

SERVICES

TECHNOLOGY

SORBAY SAAS

EINE WELT,
EINE SICHERHEIT,
EINE ZUKUNFT.

MFA LOGINS PHISHEN

ZIMMERLI, LEA
Security Consultant

1.5

About

Contact Details

UNITED SECURITY PROVIDERS

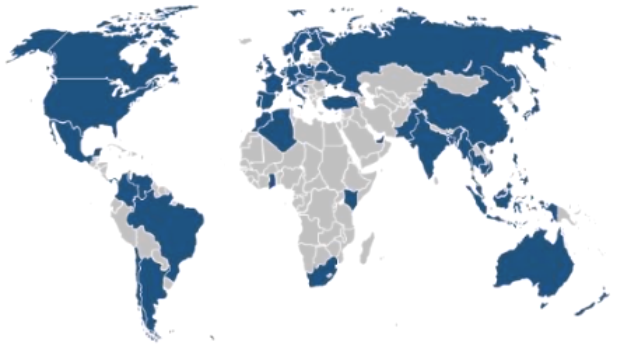
Lea Zimmerli
Security Consultant

lea.zimmerli@united-security-providers.ch

UNITED SECURITY PROVIDERS AG
Mürtschenstrasse 27,
8048 Zürich

united-security-providers.ch

UNITED SECURITY PROVIDERS OVERVIEW



Key figures

United Security Providers locations	Bern (head office), Zurich
Type of company	Public limited company, since 2019 owned by Swisscom
Founded in	1994
Revenue	16 MCHF
Employees	70

Security as a Service

Managed Security Services (MSS)
Security as a Service for effective protection around the clock

USP Secure Entry Server® (SES)
A web application firewall for simple and Secure access to business applications

USP Network Authentication System® (NAC)
For controlled access of end devices to the network

Security Consulting & Projects
IT security consulting and projects for easy access to expert knowledge and methodological skills

PORTFOLIO OVERVIEW

United Security Providers - Services

IT-Security Consulting

- ✓ Tailor-made advice and support in the implementation of information security projects:
  - Identity- & Access Management
  - Network & Infrastructure Security
  - Mobile Security, Cloud Security, Web-Anwendungen
  - Employee Awareness Spreading
  - Pentesting
  - Vulnerabilty Scans

Managed Security Services (MSS)

- ✓ As a provider (MSSP) we manage, operate and monitor your entire IT security infrastructure.
- ✓ Detecting and eliminating security gaps, monitoring your networks and IT systems and actively combating cyber attacks.
- ✓ 24/7 security for your web applications and IT infrastructure, best of connectivity, performance and cyber security.

CATO NETWORKS

United Security Providers – Products

Web Access Management

- ✓ The USP Secure Entry Server®:
  - Web Access Management solution developed in Switzerland
  - Combines Web Application Firewall (WAF), authentication and identity federation
  - Highly optimized, scalable, all-in-one product suite
- ✓ Specific modules manage identities and access, optimize and centralize security in applications

Network Access Control

- ✓ Enables authentication of users and devices
- ✓ Review and compliance with security policies
- ✓ Implementing access restrictions to ensure network security
- ✓ Protecting and strengthening network security against unauthorized devices
- ✓ Reduced risk of unauthorized access and data loss

Authentifizierung vs. Identifizierung

Identifizierung : Das Beanspruchen oder Zuweisen einer Identität (z. B. Benutzername, E-Mail).

"Wer bist Du?"

Authentifizierung : Die Überprüfung der beanspruchten Identität (z. B. Passwort, biometrische Daten).

„Bist Du tatsächlich die Person, die Du vorgibst zu sein?"

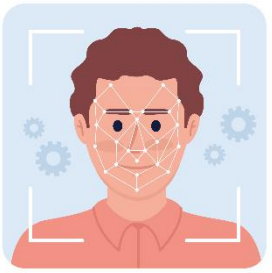
Q: Wie können wir sicherstellen, dass die Person tatsächlich die ist, für die sie sich ausgibt?
A: Wir können etwas benutzen, das sie:

Wissen:

- PIN
- Passwort

Haben:

- RSA Key
- Smartcard
- Smartphone



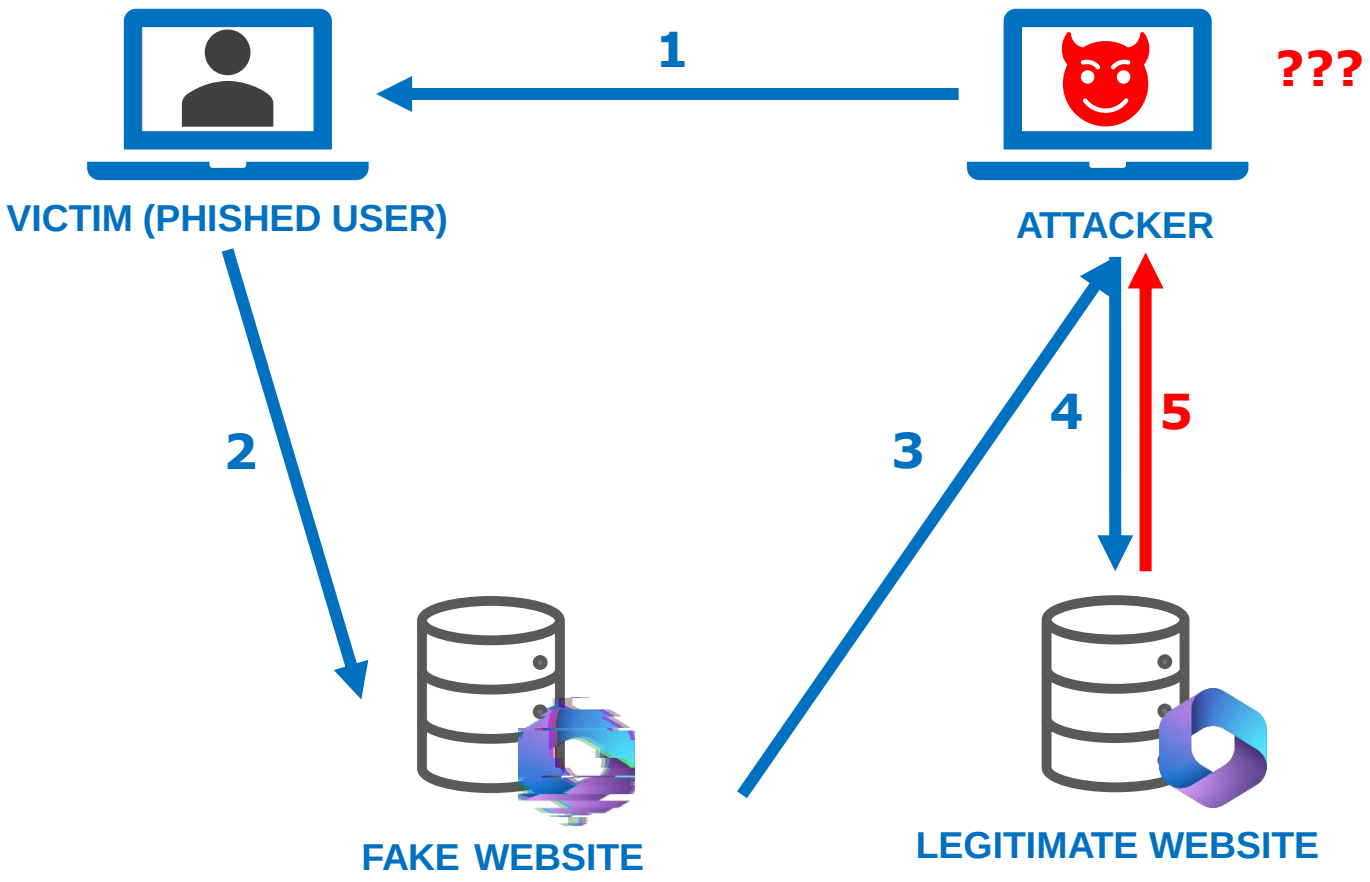
Sind:

- Fingerabdruck
- Gesichtserkennung

SCHÜTZT MFA VOR PHISHING?

JA...

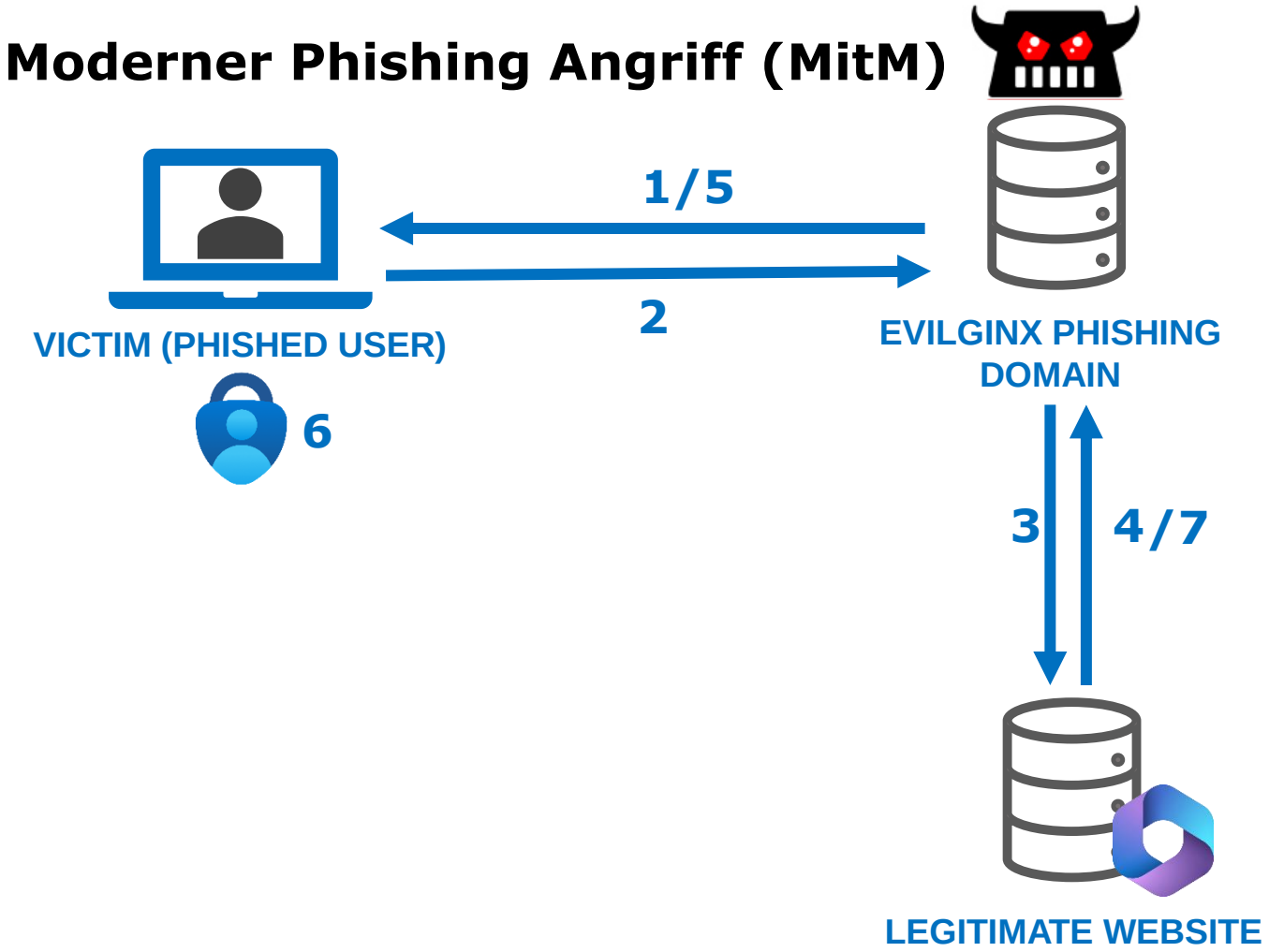
Phishing Angriff



1. Angreifer schickt phishing link an user
2. User benutzt link und gibt credentials ein
3. Die fake website leitet die Credentials weiter an Angreifer
4. Angreifer benutzt die Credentials für die richtige Website
5. Die richtige Website verlangt MFA

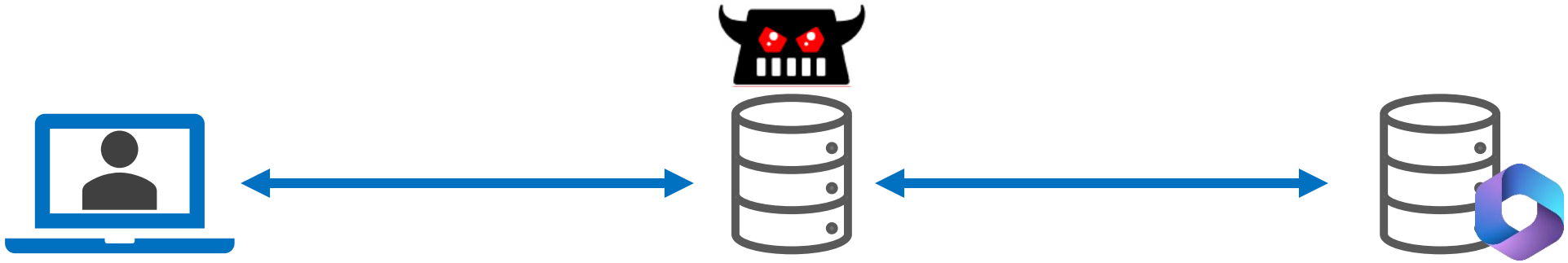
SCHÜTZT MFA VOR PHISHING?

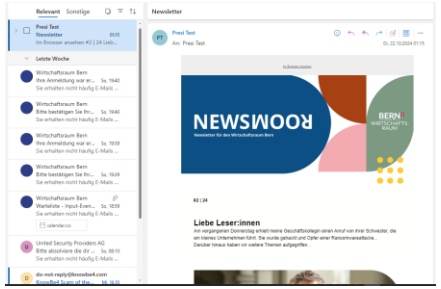
...UND NEIN!



1. Angreifer schickt phishing link an user
2. User benutzt link und gibt credentials ein
3. Phishing domain leitet Credentials an die richtige Website weiter
4. Richtige Website verlangt MFA
5. Phishing domain leitet MFA Prompt an User weiter
6. User bestätigt MFA
7. Echte Website schickt das authentication/access Token an die phishing Domain

DEMONSTRATION





https://login.services.wirtschaftsraum.eu/anmelden

https://www.office.com/?auth=2

PW: ***

Cookies:
ESTSAUTH:
ESTSAUTHPERSISTENT:
SignInStateCookie:

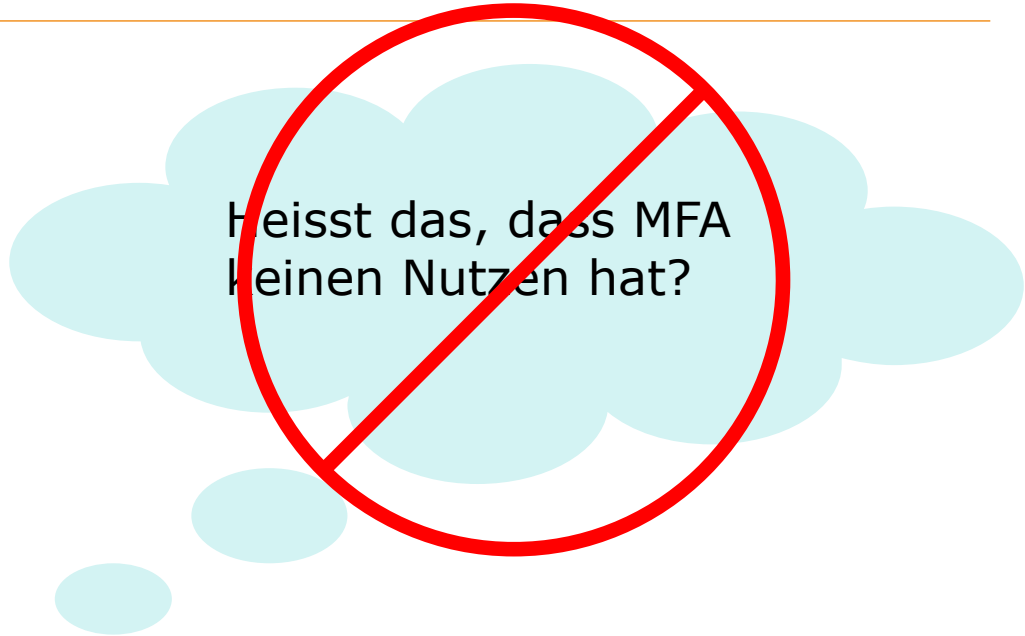
WIE HÄTTE MAN ES VERHINDERN KÖNNEN?

- Link anschauen
- Email adresse anschauen
- Qualität von der Email anschauen

→ Sensibilisierung & awareness der Mitarbeitenden

WOZU NÜTZT DENN MFA?

- Schützt vor schwachen & gestohlenen Passwörtern
- Absicherung im Homeoffice: Minderung von Risiken durch private Geräte
- Zugriff vereinfachen und dennoch hohe Sicherheit gewährleisten
- Fügt eine zusätzliche Sicherheitsebene hinzu



UNITED SECURITY PROVIDERS

MFA LOGINS PHISHEN

ZIMMERER, LEA
SECURITY CONSULTANT

EINE WELT,
EINE SICHERHEIT.
EINE ZUKUNFT.


BERN
WIRTSCHAFTS-
RAUM
Herzlichen Dank für
Ihre Aufmerksamkeit
swisscom