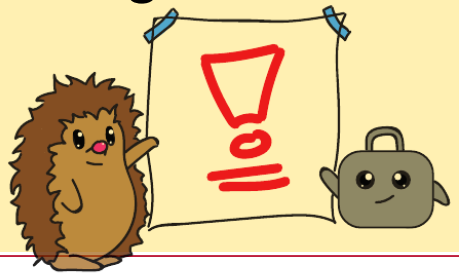
Technische Universität Braunschweig

Gauß-IT-Zentrum

Awareness Maßnahmen an der TU Braunschweig

Dr. Christian Böttger, 04.05.2021



Technische Universität Braunschweig

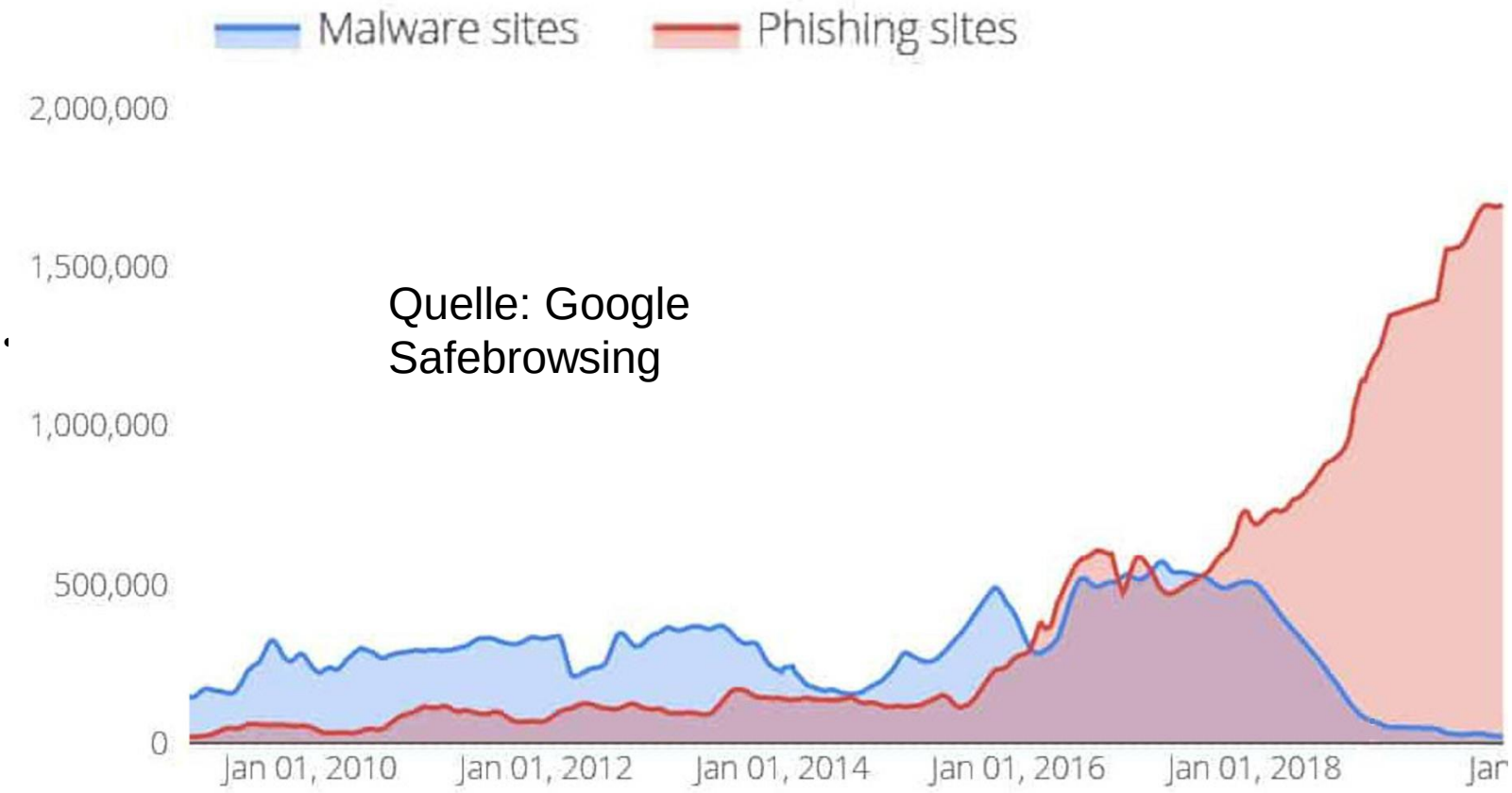
Agenda

- Warum Awareness-Maßnahmen zur Informationssicherheit?
- Maßnahmen - Überblick
- „analoge“ Maßnahmen
- „digitale“ Maßnahmen
- Einsatz eines Awareness-Tools
- Links

Einführung

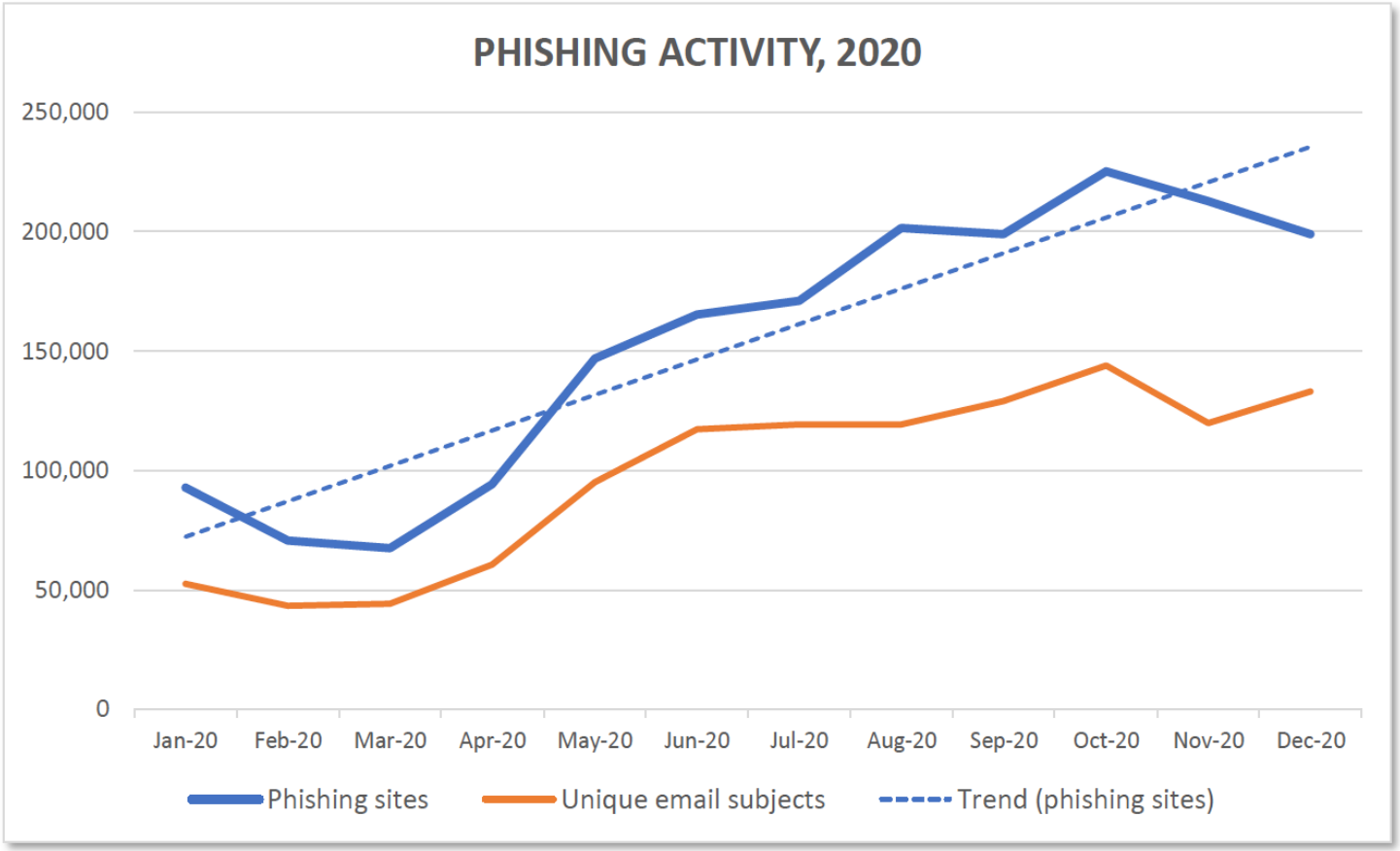
- Informationssicherheit kann man nicht aus dem Regal kaufen. Alle Nutzer/innen müssen sich aktiv beteiligen.
- Informationssicherheit ist ein dauernder Prozess, keine einmalige Installation oder Einrichtung einer Software.
- Angriffe erfolgen zunehmend über den Menschen, nicht mehr nur über die Technik.
- Zusätzlich zu allen weiter nötigen technischen Maßnahmen muss die Aufmerksamkeit aller Mitarbeitenden ständig aktiv gehalten werden.
- Auch dies ist ein dauernder (Kreislauf-)Prozess.
  - Ähnlich wie jährliche Schulungen zum Datenschutz und zum Unfallschutz.

- Starke Zunahme von Phishing über die Jahre



Quelle: Google Safebrowsing

- Phishing im Jahr 2020



Quelle: Anti-Phishing Working Group https://apwg.org/

- Phishing basiert auf **Emotionen**
  - **Gier, Neugier, Mitleid und Angst – und Mischungen davon**
    - *Respekt vor Autoritäten*: Vorgesetzte, Behörden, … (Angst), „Konto läuft ab“
    - Künstlich erzeugter (Zeit-)*Druck*: (Angst, Gier)
      - Vorgesetzter braucht bis in 2 Stunden irgendwas
      - „nur die ersten 50 gewinnen einen Preis“
    - *Automatisierte Handlungen* nutzen:
      - „Klicke hier“ auf einem roten Knopf, „Bestätigen Sie“, „Akzeptieren“, …
    - (hohen) finanziellen *Gewinn* in Aussicht stellen (Gier)
    - *Sex* (Gier)
    - *Apell*: jemand braucht Hilfe (Mitleid, Hilfsbereitschaft)
    - Angebliche Gehaltsdaten anderer Menschen (*Neugier*)
    - *Vertraulichkeit*: *Vortäuschen von angeblichem Detailwissen*, gefälschte Absender, Zitat aus echten Mails
    - *Dunning-Kruger-Effekt: alle Menschen überschätzen ihre eigenen Fähigkeiten, besonders dann, wenn sie auf dem jeweiligen Gebiet real wenig Fähigkeiten haben*

Grundsätze

- Maßnahmen müssen regelmäßig wiederholt werden
- Aufmerksamkeit lässt schnell wieder nach
- Problem: Integration in den Arbeitsablauf
- Positive Fehlerkultur ist zwingend notwendig.
- IT/Informationssicherheit ist nicht die primäre Aufgabe der Mitarbeitenden!
- Mitarbeitende müssen „abgeholt“ werden.
- Wichtig: niemals Vorwürfe machen – sondern immer Hilfe und Unterstützung anbieten!
- Ohne aktiven Rückhalt aus den Leitungsebenen geht gar nichts!

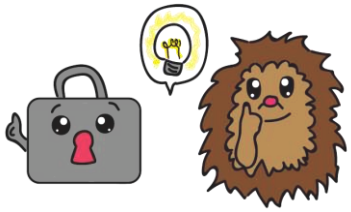
Es gibt keine „Silver Bullet“

- Viele kleine sich ergänzende Maßnahmen sind nötig.
  - Menschen lernen auf verschiedenen Wegen.

- Analoge Maßnahmen
- Digitale Maßnahmen

- Online Maßnahmen und Offline-Maßnahmen

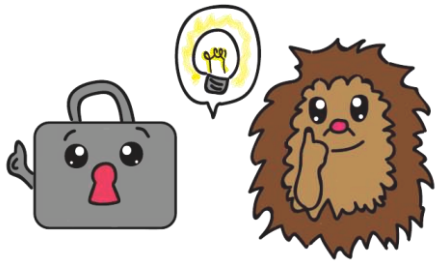
- Und immer: wertschätzend!



Analoge Maßnahmen an der TU Braunschweig

- Mousepads kostenfrei verteilen
- Info-Aufsteller in den PC-Pool-Räumen
- Bei Präsenzbetrieb: wechselnde Plakate
- Informations-Flyer (z.B. bei Einführungsveranstaltungen und im Service Desk)
- Seminare (z.B. über die Personalweiterbildung)
- Vorträge
  - z.B. Beteiligung am European Cyber Security Month
- Seminare und Vorträge nicht in der Freizeit, sondern als Arbeitszeit
- Gastbesuche in Gremien

Plakate - Beispiele



Aufsteller - Beispiele

IT-Sicherheit
Gauß IT Zentrum

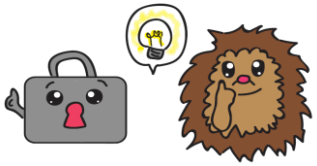
Technische Universität Braunschweig

IT-Sicherheit
Gauß IT Zentrum

Technische Universität Braunschweig

IT-Sicherheit
Gauß IT Zentrum

Technische Universität Braunschweig



Mousepads – Beispiel 2

Technische Universität Braunschweig

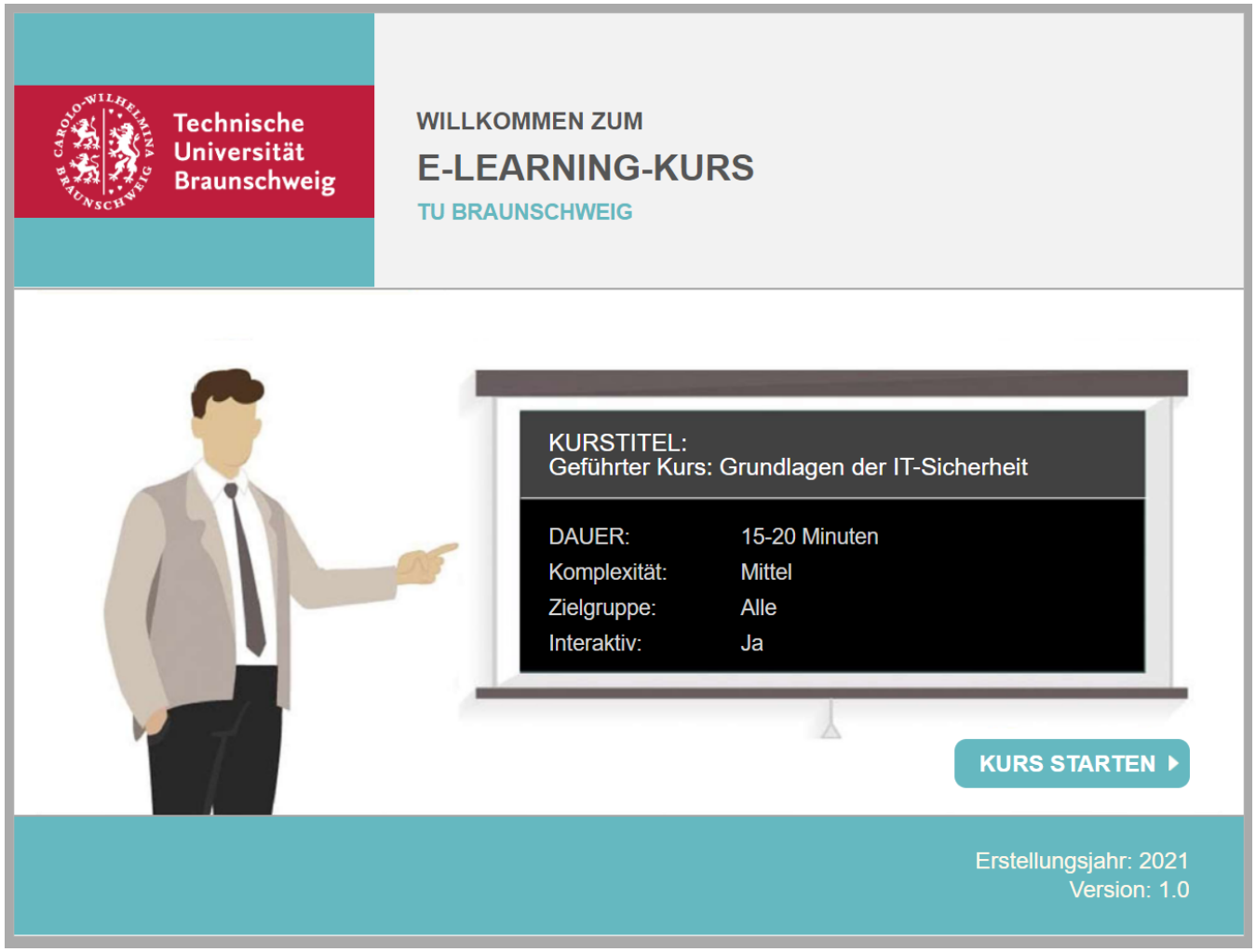
Gauß-IT-Zentrum

http://it-sicherheit.tu-braunschweig.de/

Digitale Maßnahmen an der TU Braunschweig

- Informationssicherheits-Blog / Webseite
  - Informationen und Warnungen
- Nutzung von Mailverteilern: DV-Koordinierende, …
  - Warnungen – Achtung, nicht zu viel!
- Videos zum Abrufen
  - Einbindung ins Lernmanagementsystem der TU (Stud.IP)
- Vorträge (PDF) zum Abruf
- Online-Quiz / Online-Kurse
- Online- Vorträge und Seminare
  - ECSM, Personalweiterbildung
  - IT-SAD 7.-18.6.2021 (öffentlich)
- Meldeadresse (E-Mail, Formular) für Vorfälle und Spam

Online-Kurs: Beispiel



Digitale Maßnahmen an der TU Braunschweig: Links

- https://studip.tu-braunschweig.de/seminar_main.php?auswahl=bc863707104006d8b2c63d11f6a60ed0
- https://blogs.tu-braunschweig.de/it/category/informationssicherheit/
- https://blogs.tu-braunschweig.de/it/it-sad-it-security-awareness-days-sommersemester-2021/
- https://blogs.tu-braunschweig.de/it/videos-zur-informationssicherheit-zum-selbstlernen/
- https://blogs.tu-braunschweig.de/it/vortraege-zu-themen-rund-um-informationsicherheit/
- https://blogs.tu-braunschweig.de/it/screencast-trau-keinen-phishen/
- https://blogs.tu-braunschweig.de/it/informationssicherheit-online-materialien-zum-selberlernen/

Einsatz eines Awareness-Tools

- Methoden
  - „Fake-Spam“-Kampagnen mit anschließenden Kursen
    - per Mail, aber auch mit z.B. USB-Sticks
  - Aufklärungekampagenen mit Quiz, Kursen, Vorträgen, Videos (ohne „Fake-Spam“)
  - Multimediale Kurse zum Selber lernen im dauerhaften Zugriff
  - bald: Spam-Meldeknopf in Outlook (evtl.Thunderbird)
  - Optional: Test der technischen Spam-Abwehrmaßnahmen
- In 2020: gemeinsames Projekt mit der RUB
- Eingesetztes Tool: LUCY
  - https://lucysecurity.com/de/

LUCY 1 - Kampagnenübersicht

RUB/OGB/T…

Kampagnen Status: Gestoppt | Statistiken leeren | Bericht | Als Vorlage speichern | Exportiere | Start

Ergebnisse

- Zusammenfassung
- Statistiken
- Berichte
- Exporte
- Automatischer Export

Konfiguration

- Basiseinstellungen
- Sensibilisierungskurs Einstellungen
- Einstellungen Angriffssimulation
- Zeitplan
- Empfänger

Erweiterte Einstellungen

- Benutzereinstellungen
- Filter
- Benutzerdefinierte Felder

Kampagne	Laufzeit	Erstellt von
RUB/OGB/TUBS Studis	2 Monate, 25 Tage	leonard-jari.zurek@tu-braunschweig.de

Angriffsübersicht

Highcharts.com
24788 Nachrichten gesendet

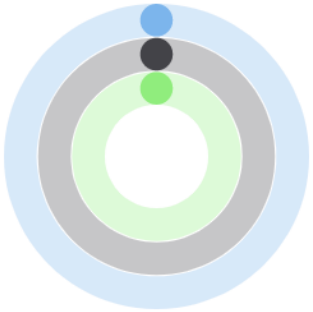
Highcharts.com
60.62% aller Empfänger öffneten die Nachricht

Highcharts.com
27.48% aller Empfänger klickten den Link

Highcharts.com
7.81% aller Attacken waren erfolgreich

Köder gesendet	24785 of 24799	99.94%
Nachrichten gesendet	24788 of 24799	99.96%
Nachrichten geöffnet	15034 of 24799	60.62%
Klicks	6816 of 24799	27.48%
Erfolgreiche Attacken	1938 of 24799	7.81%
Anfällige Opfer	31 of 24799	0.13%
Fehler	11 of 24799	0.04%

Sensibilisierungskurs

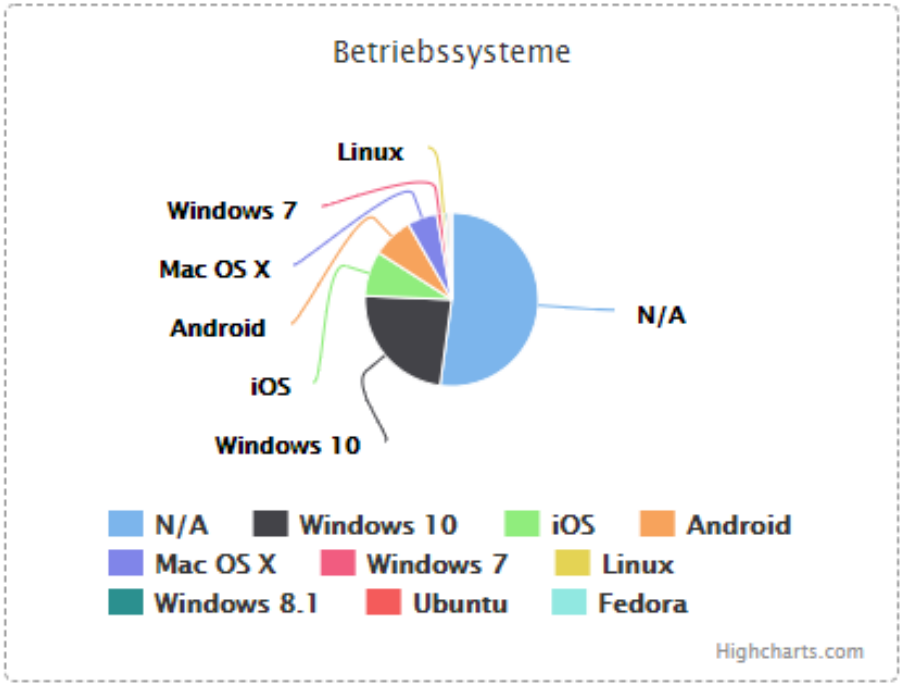


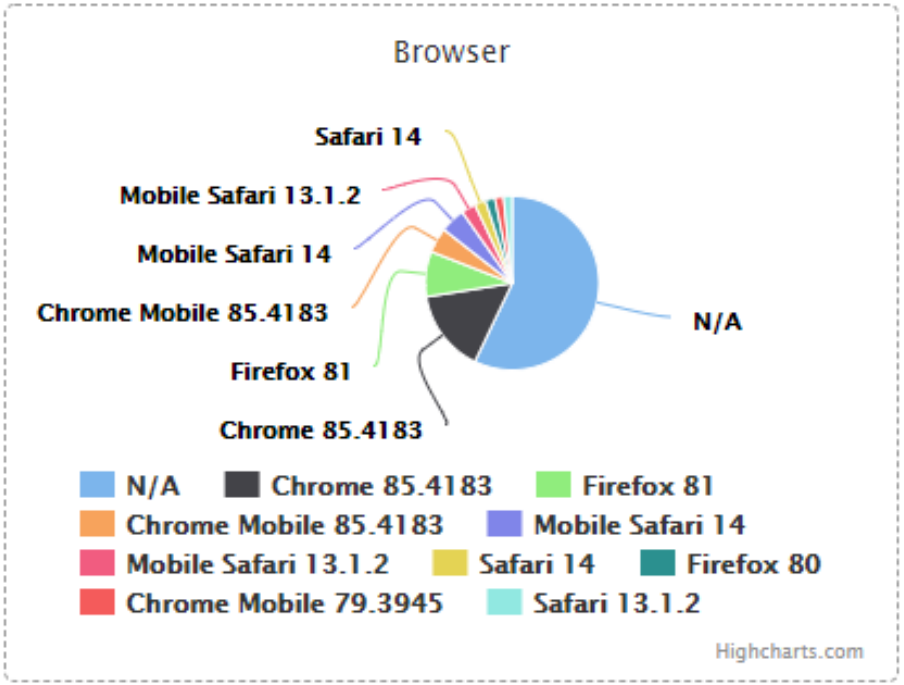
Training gesendet
Training geöffnet
Trainingswertung (%)

Zur Aktionsübersicht anklicken – mit Anzahl der E-Mails

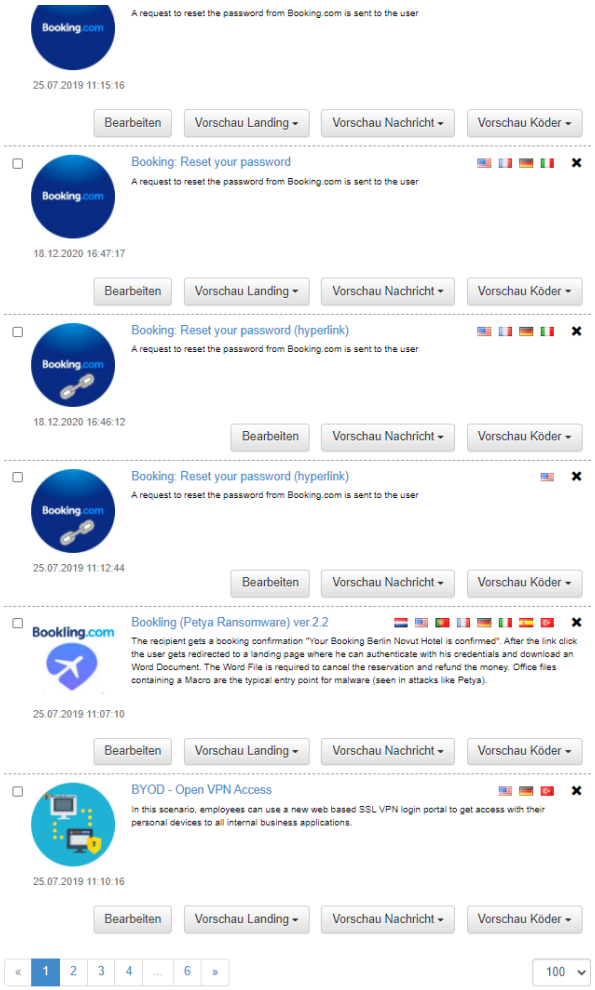
E-Mails insgesamt	24788

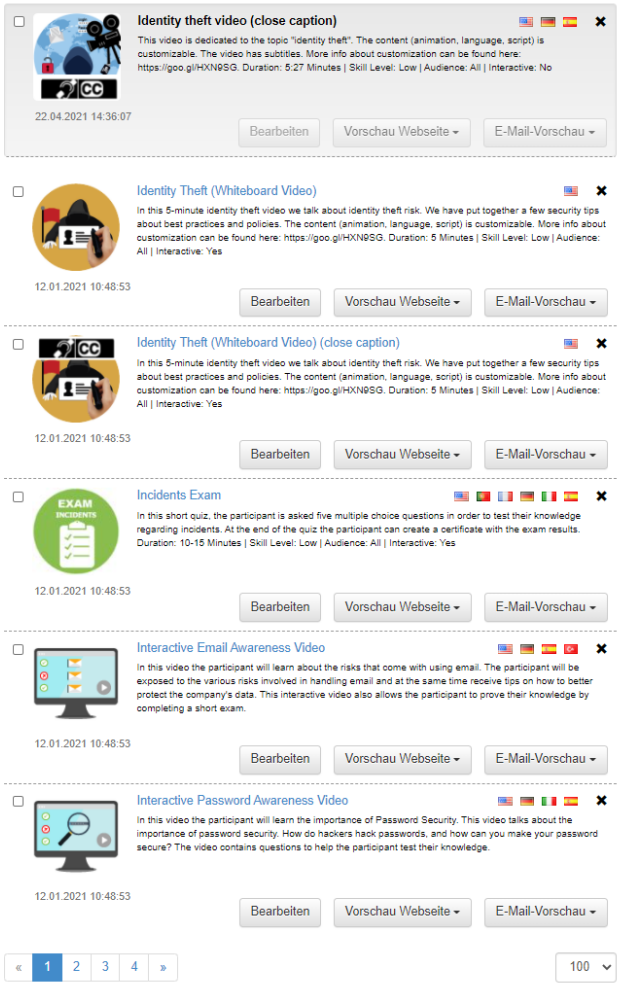
LUCY 2 – technische Statistiken





LUCY 5 - Vorlagen





LUCY 6 – Dashboard für gemeldete Phishing-Vorfälle

Missbrauchsmeldung senden | Löschen | Alle löschen | Status ändern | Plugin herunterladen

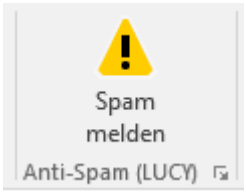
Phishing Vorfall Berichte

Filter

Statistiken

	Zeit	E-Mail	Klient	Kampagne	Wertung	Status	
☐	01.03.2021 09:36	c.boettger@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	
☐	01.03.2021 09:36	c.boettger@tu-braunschweig.de	LUCY@GITZ	N/A	10.00	Öffnen	
☐	19.02.2021 16:33	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	
☐	19.02.2021 15:53	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	
☐	19.02.2021 15:41	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.50	Echtes Phishing	
☐	19.02.2021 13:35	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	
☐	19.02.2021 13:20	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	1.20	Öffnen	
☐	19.02.2021 13:12	c.boettger@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	
☐	19.02.2021 13:12	c.boettger@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	
☐	19.02.2021 13:11	leonard-jari.zurek@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	

« 1 2 3 4 5 ... 8 » 10 Zeilen pro Seite.



Awareness-Tool Einsatz

- LUCY ist selbst gehostet
  - Solche Tools gibt es auch als externen Service.
- Nicht zu häufig, nicht zu selten
  - Wirkung lässt jeweils schnell nach
  - Aber: Eindruck vermeiden „ach, das ist nur wieder ein Test“
- Niemals die „Hereingefallenen“ maßregeln!
- Hilfe und Information anbieten
- Kampagnen vorher ankündigen und auch das Ende bekannt geben!
- Leitung und Help Desk mit einbeziehen!

Fazit

- Es gibt nicht die eine richtige Maßnahme.
- Die Vielfalt macht‘s.
- Immer am Ball bleiben!
  - Also: als Daueraufgabe anlegen!
- Leitungsebenen müssen dahinter stehen!
- Der Aufwand ist beträchtlich – genügend personelle Kapazitäten einplanen!
- Mitarbeitende dürfen sich nicht kontrolliert fühlen:
  - Wertschätzung
  - Hilfe anbieten
  - Nicht maßregeln

Links

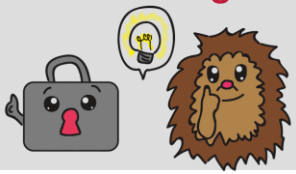
- https://www.tu-braunschweig.de/it-sicherheit
- https://www.tu-braunschweig.de/it-sicherheit/kurztipps
- https://www.tu-braunschweig.de/it-sicherheit/pwsec
- https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec
- https://blogs.tu-braunschweig.de/it/category/informationssicherheit/
- https://studip.tu-braunschweig.de/seminar_main.php?auswahl=bc863707104006d8b2c63d11f6a60ed0
- https://www.bsi-fuer-buerger.de/
- https://zac-niedersachsen.de/inhalte.php
- https://www.polizei-praevention.de/aktuelles.html

Weitere Infos:
https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec und
http://it-sicherheit.tu-braunschweig.de/

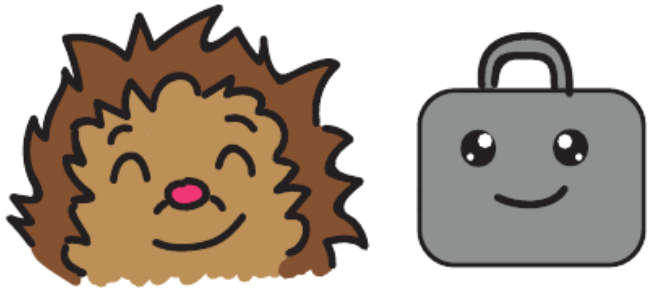
https://pixabay.com/de/baby-lernen-laptop-frage-2709666/
CC0 Lizenz

und beim IT-Service-Desk des Gauß-IT-Zentrums
Tel. +49.531.391.55555
it-service-desk@tu-braunschweig.de **https://www.tu-braunschweig.de/it/service-desk**

Vielen Dank für Ihre Aufmerksamkeit!



Geschafft!



Vielen Dank für die Aufmerksamkeit!

Einfache Fragen? ;-)