TECHNISCHE UNIVERSITÄT DRESDEN

TUD CERT Computer Emergency Response Team

Pascal Brückner
TUD-CERT

Phishing-Kampagne(n) an der TU Dresden

Integriertes Lernen am Arbeitsplatz

03.02.2022

Phishing-Simulation an der TUD
Übersicht

Zweck Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail

Inhalte Simulation interner Dienste inkl. Schulung

Phishing-Toolkit Lucy[1]

Phishing-Server externes Hosting, IP-basiertes Whitelisting

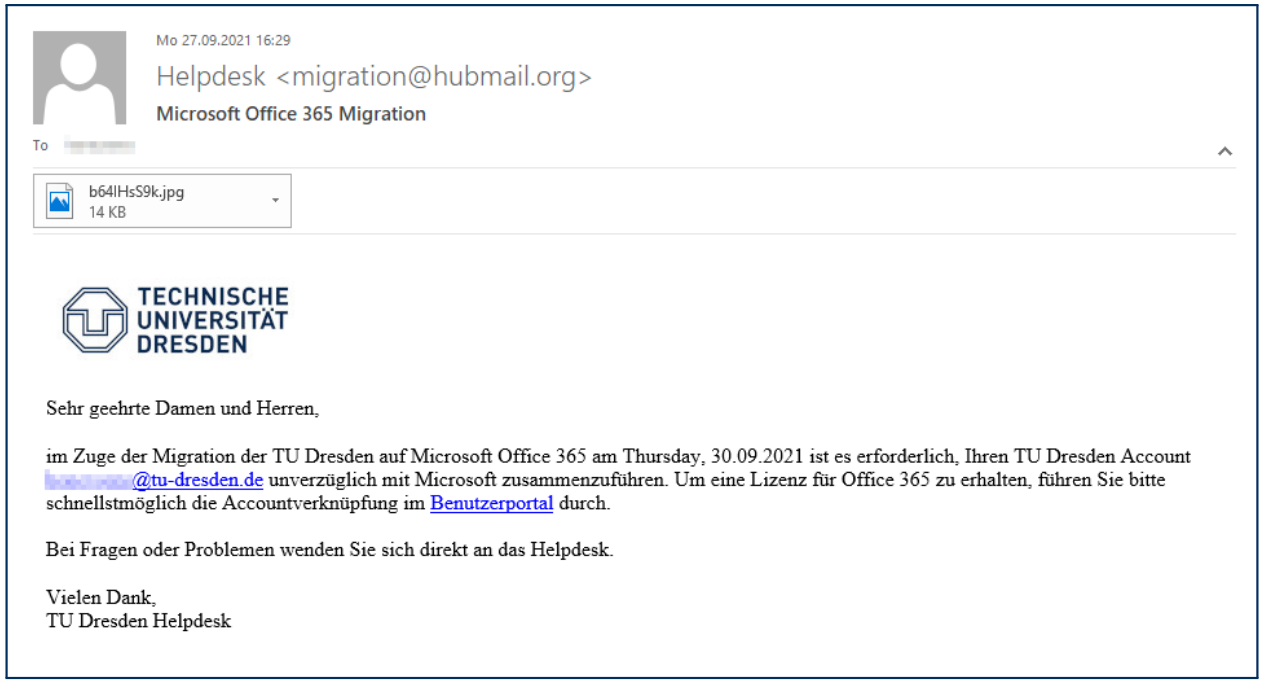
[1] `https://lucysecurity.com`

Phishing-Simulation an der TUD
Übersicht

Zweck	Sensibilisierung v. Nutzern mit simulierten Phishing-Angriffen per E-Mail
Inhalte	Simulation interner Dienste inkl. Schulung
Phishing-Toolkit	Lucy[1]
Phishing-Server	externes Hosting, IP-basiertes Whitelisting
Umfang	Ausschließlich TUD-Angestellte, **keine** Gäste oder Studierende
Rechtliches	Dienstvereinbarung mit Personalrat beschlossen, Kampagnen anonym
Häufigkeit	Periodisch, etwa eine Mail pro Quartal
Meldeweg	per Mail oder via Outlook-AddIn, Plugin für Thunderbird in Testphase

[1] `https://lucysecurity.com`

Kampagne Okt. 2021
Phishing-Nachricht



Mo 27.09.2021 16:29

Helpdesk <migration@hubmail.org>

Microsoft Office 365 Migration

To [redacted]

b64lHsS9k.jpg
14 KB

TECHNISCHE UNIVERSITÄT DRESDEN

Sehr geehrte Damen und Herren,

im Zuge der Migration der TU Dresden auf Microsoft Office 365 am Thursday, 30.09.2021 ist es erforderlich, Ihren TU Dresden Account [redacted]@tu-dresden.de unverzüglich mit Microsoft zusammenzuführen. Um eine Lizenz für Office 365 zu erhalten, führen Sie bitte schnellstmöglich die Accountverknüpfung im Benutzerportal durch.

Bei Fragen oder Problemen wenden Sie sich direkt an das Helpdesk.

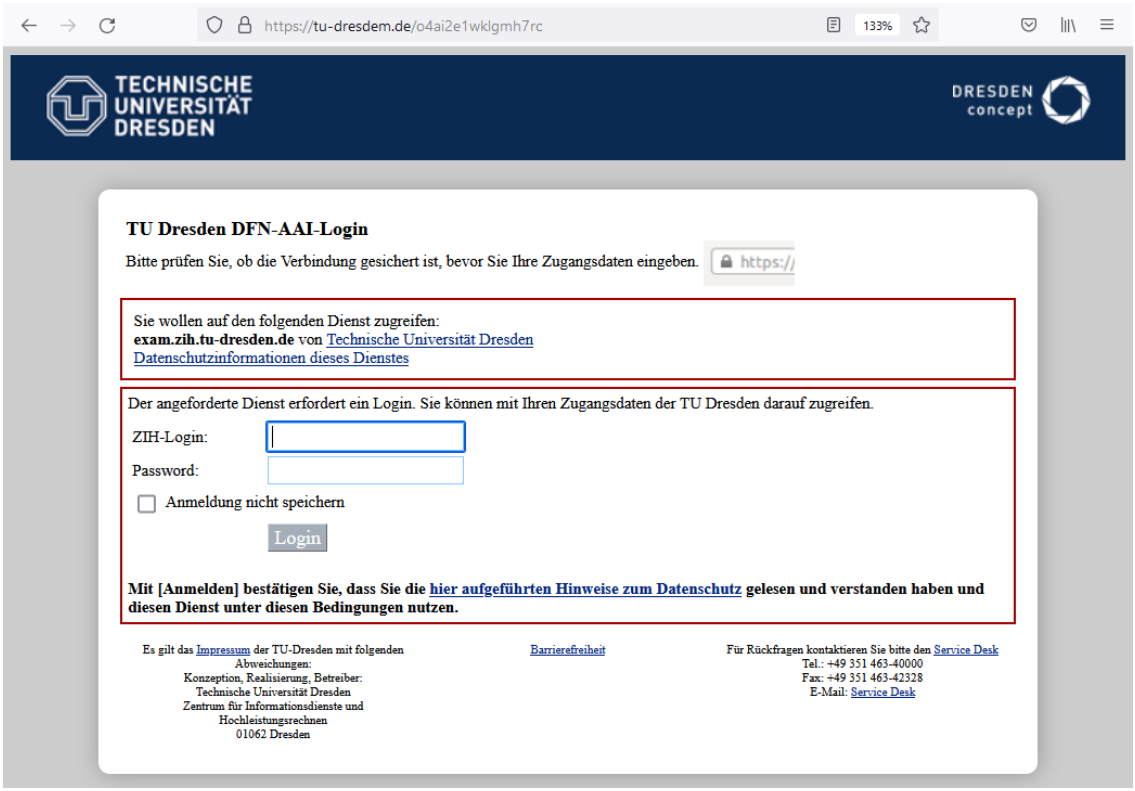
Vielen Dank,
TU Dresden Helpdesk

Pretext Verknüpfung des TUD-Accounts mit Microsoft zum Erhalt einer Lizenz für Office 365

SEIs[2] Absender, unsigniert, Plausibilität, “TUD Helpdesk”, Link-Ziel

[2] Social Engineering Indicators

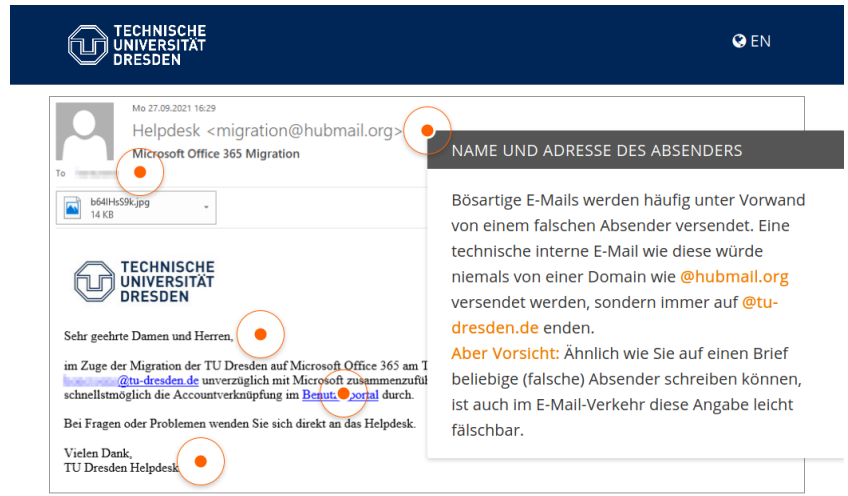
Kampagne Okt. 2021
Landing Page



Inhalt Nachbau des an der TUD genutzten SSO-Portals (Shibboleth)

SEIs Domain, Dienstebeschreibung inkonsistent, Defekte Links

Kampagne Okt. 2021
Training nach Dateneingabe



Nachdem Sie auf den Link in der E-Mail geklickt hatten, präsentierte ihr Browser Ihnen die nachfolgend dargestellte bösartige Website, die ein Nachbau einer innerhalb der TU Dresden häufig anzutreffenden Authentifizierungsseite ist. Auch hier gibt es wieder verschiedene Indikatoren, mittels derer Sie einen Betrugsversuch rechtzeitig erkennen können:

- Kein generisches Training; stattdessen Aufzeigen konkreter SEIs anhand der gerade erfahrenen Phishing-Kampagne
- Aufforderung zur Nutzung der Melde-Plugins

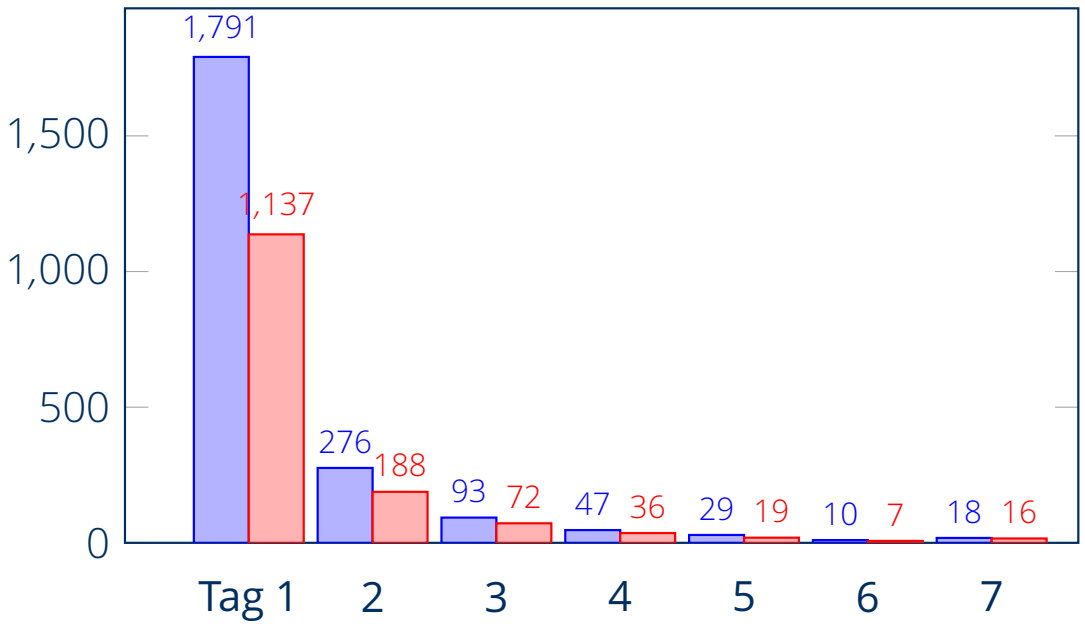
Kampagne Okt. 2021
Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

Kampagne Okt. 2021
Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

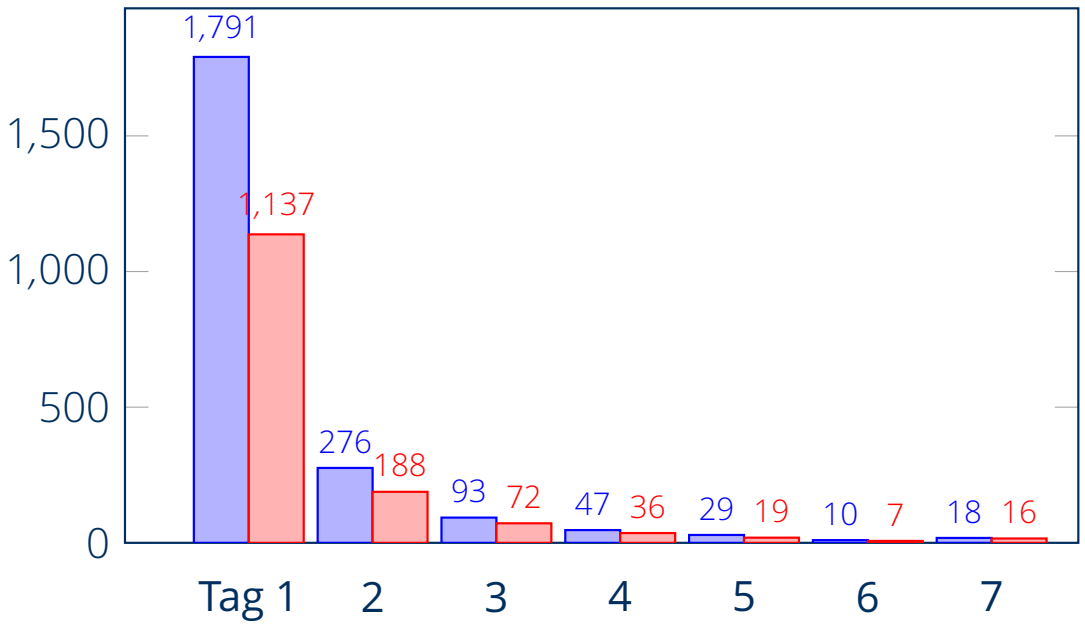
Resultat 18% Klicks, 12% mit Dateneingabe, 4% Meldungen

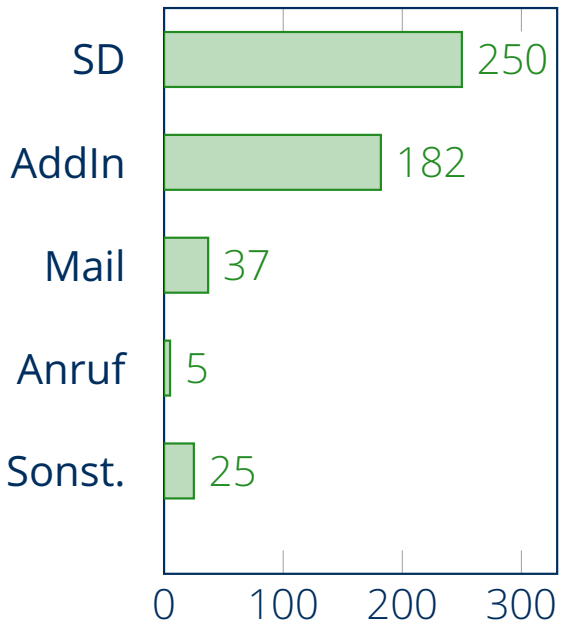


Kampagne Okt. 2021
Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

Resultat 18% Klicks, 12% mit Dateneingabe, 4% Meldungen

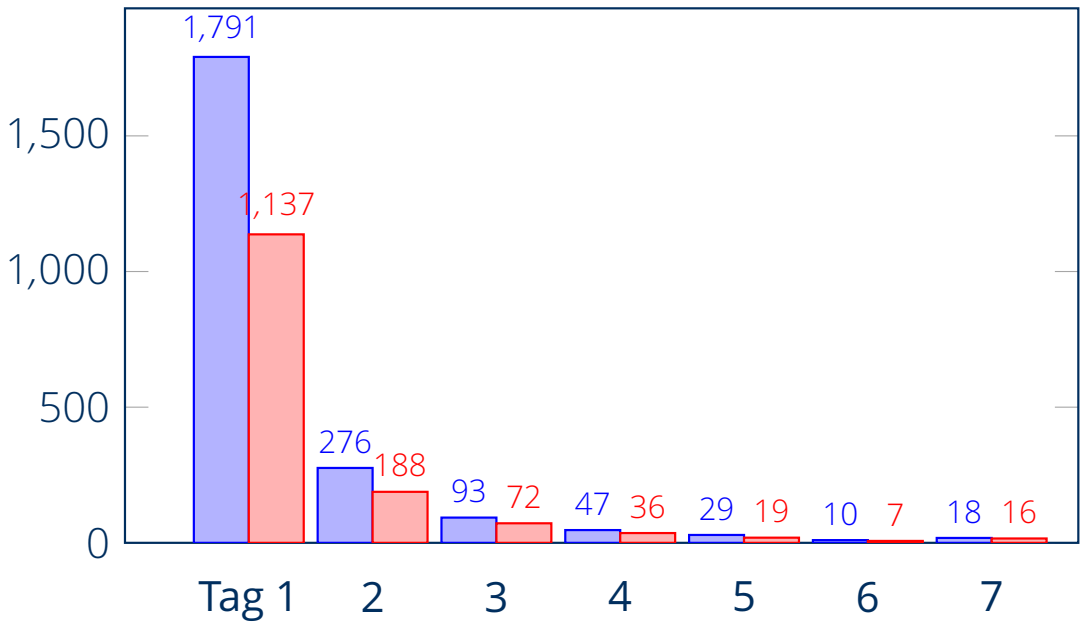


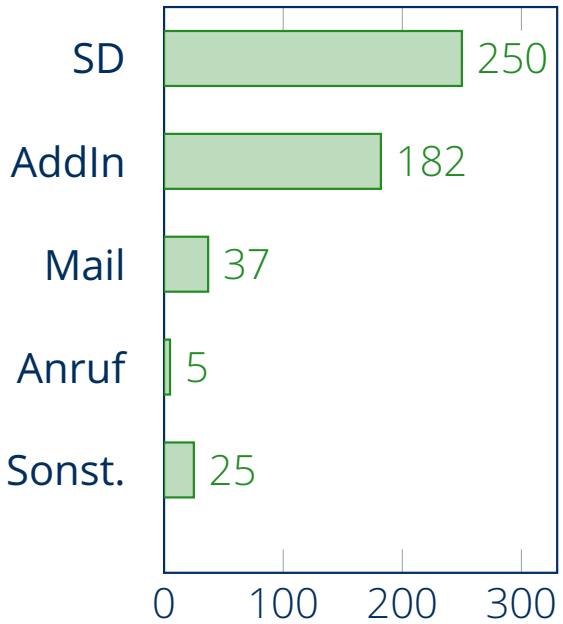


Kampagne Okt. 2021
Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

Resultat 18% Klicks, 12% mit Dateneingabe, 4% Meldungen

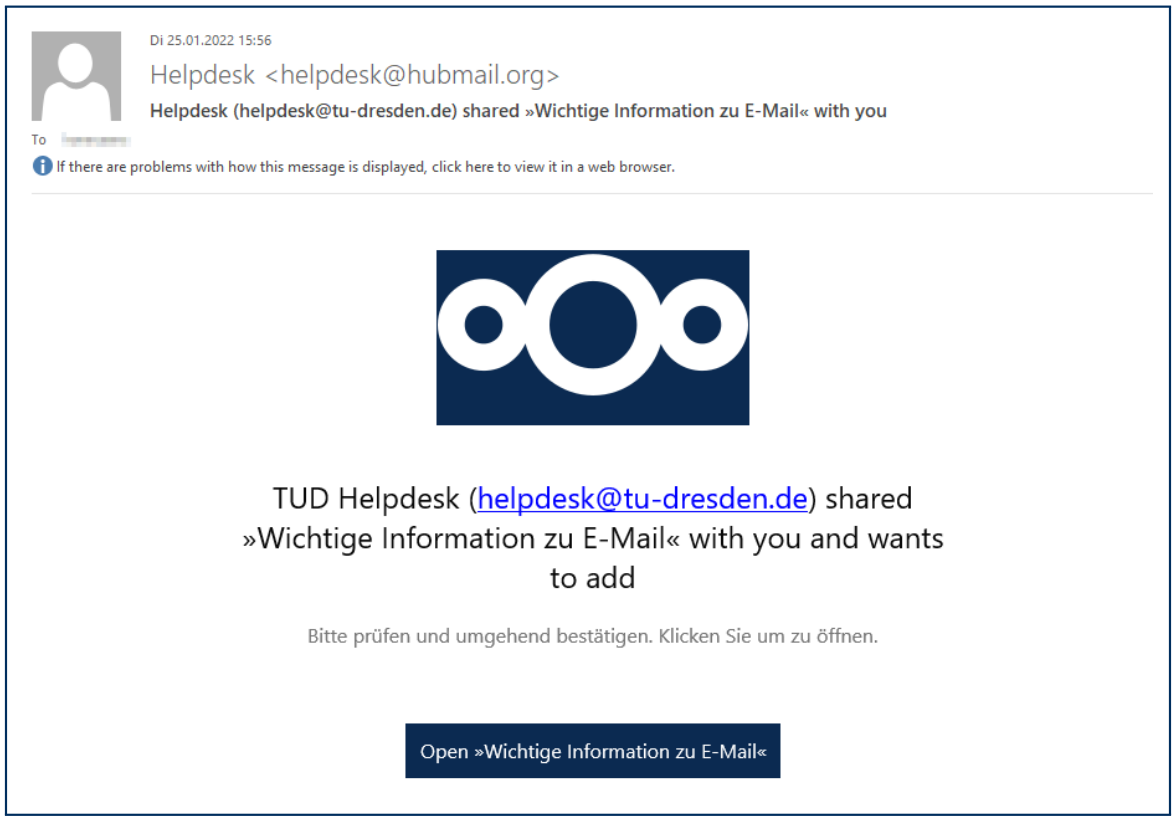




Nachwirkungen am Servicedesk: für 2-3 Tage mit Meldungen ausgelastet

- Verschiedenste Meldewege erschwerten Auswertung
- Abuse-Meldungen bei unserem Hosting-Anbieter

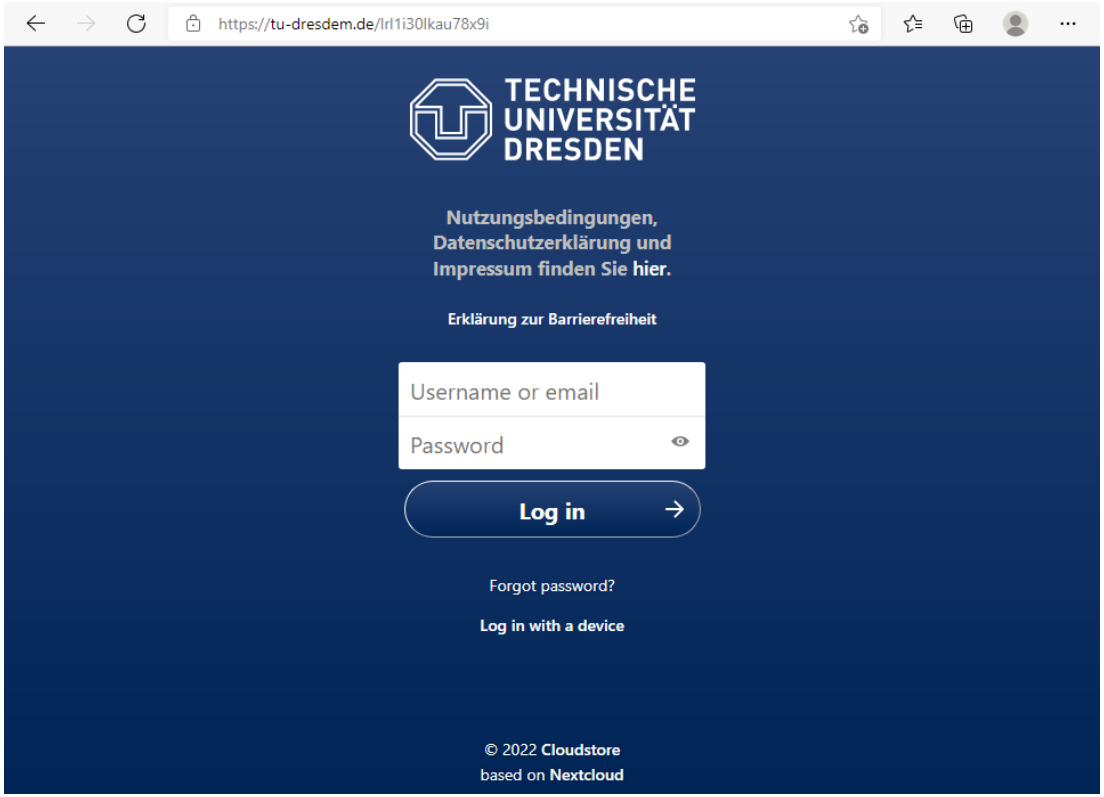
Kampagne Jan. 2022
Phishing-Nachricht



Pretext Freigabe wichtiger Dokumente mittels *TUD Cloudstore* (Nextcloud)

SEIs Absender, unsigniert, Plausibilität, Link-Ziel

Kampagne Jan. 2022
Landing Page



Inhalt Nachbau der Loginseite des TUD Cloudstore

SEIs Domain, Defekte Links

Kampagne Jan. 2022
Auswertung (vorläufig)

Vorabinformation an Servicedesk und Admins

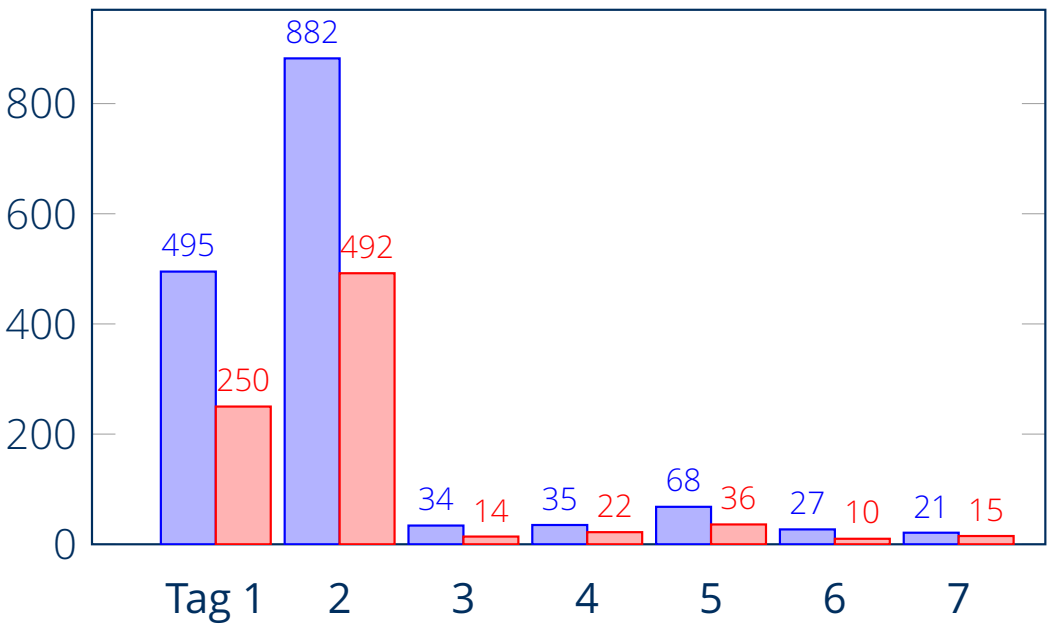
Versand an 13000 Empfänger binnen **zwei** Tagen ab Donnerstag Vormittag

Kampagne Jan. 2022
Auswertung (vorläufig)

Vorabinformation an Servicedesk und Admins

Versand an 13000 Empfänger binnen **zwei** Tagen ab Donnerstag Vormittag

Resultat 12% Klicks, 6% mit Dateneingabe, 4% Meldungen

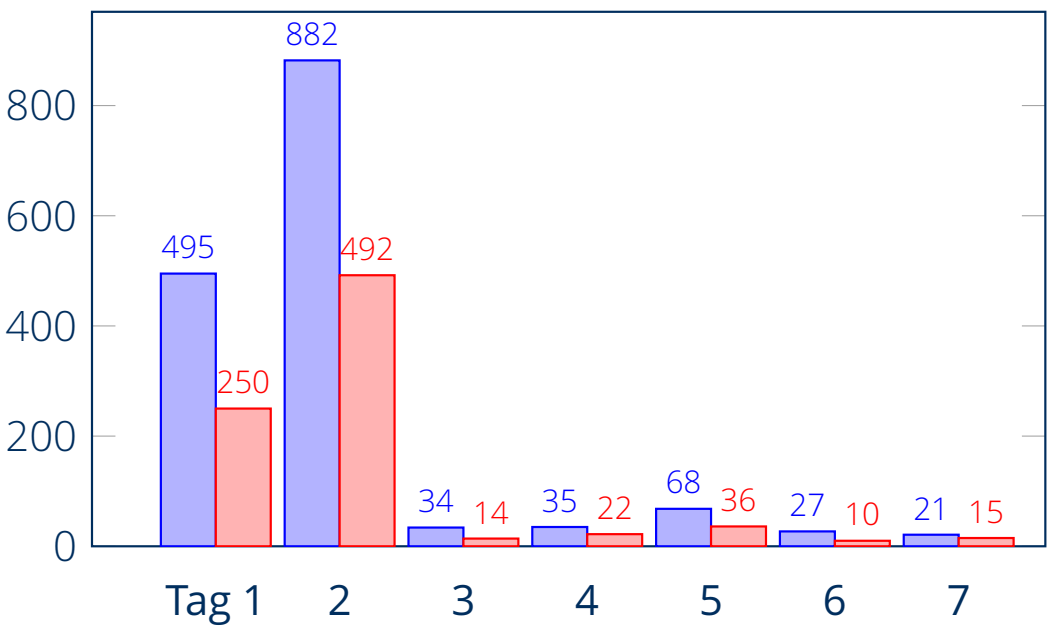


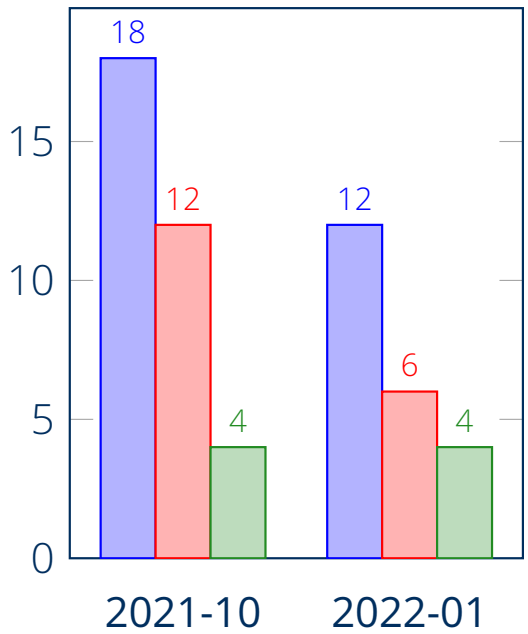
Kampagne Jan. 2022
Auswertung (vorläufig)

Vorabinformation an Servicedesk und Admins

Versand an 13000 Empfänger binnen **zwei** Tagen ab Donnerstag Vormittag

Resultat 12% Klicks, 6% mit Dateneingabe, 4% Meldungen





Offene Punkte
zum Nachdenken

Vergleichbarkeit der Kampagnen eingeschränkt (Schwierigkeit, externe Faktoren)

Validierung der eingebenen Daten für belastbare Statistik “erfolgreicher Angriffe”?

Offene Punkte
zum Nachdenken

Vergleichbarkeit der Kampagnen eingeschränkt (Schwierigkeit, externe Faktoren)

Validierung der eingebenen Daten für belastbare Statistik “erfolgreicher Angriffe”?

CERT-Reaktion auf Meldungen?

- Sofortige Aufklärung → False Positives
- Pausenzeitraum ohne Reaktion ≠ Tagesgeschäft
- Zunächst “bösartig, bitte löschen” mit späterer Aufklärung?

Offene Punkte
zum Nachdenken

Vergleichbarkeit der Kampagnen eingeschränkt (Schwierigkeit, externe Faktoren)

Validierung der eingebenen Daten für belastbare Statistik “erfolgreicher Angriffe”?

CERT-Reaktion auf Meldungen?

- Sofortige Aufklärung → False Positives
- Pausenzeitraum ohne Reaktion ≠ Tagesgeschäft
- Zunächst “bösartig, bitte löschen” mit späterer Aufklärung?

Abuse-Meldungen vorbeugen, insbesondere globale Dienste wie *Google Safe Browsing*