

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 Lucy¹

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 Lucy¹

Phishing-Server externes Hosting, IP-basiertes Whitelisting

Umfang Ausschließlich TUD-Angestellte, **keine** Gäste oder Studierende

Rechtliches Dienstvereinbarung mit Personalrat beschlossen, Kampagnen anonym

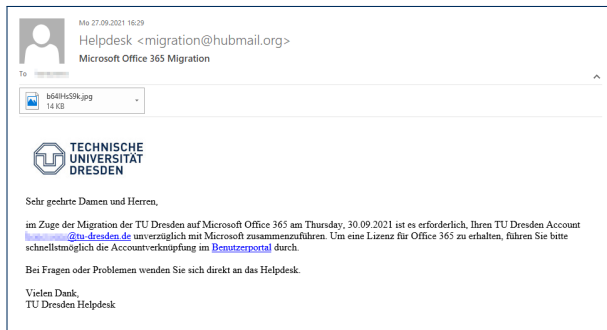
Häufigkeit Periodisch, etwa eine Mail pro Quartal

Meldeweg per Mail oder via Outlook-AddIn,
Plugin für Thunderbird in Testphase

¹<https://lucysecurity.com>

Kampagne Okt. 2021

Phishing-Nachricht



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

SEIs² Absender, unsigned, Plausibilität, "TUD Helpdesk", Link-Ziel

²Social Engineering Indicators

Kampagne Okt. 2021

Landing Page

The screenshot shows a web browser window with the URL <https://tu-dresden.de/lo4a2e1wkjgmh7rc>. The page header features the TU Dresden logo and 'DRESDEN concept'. The main content is titled 'TU Dresden DFN-AAI-Login' and includes a security warning: 'Bitte prüfen Sie, ob die Verbindung gesichert ist, bevor Sie Ihre Zugangsdaten eingeben.' Below this, a red-bordered box contains the text: 'Sie wollen auf den folgenden Dienst zugreifen: exam.zih.tu-dresden.de von Technische Universität Dresden' and a link to 'Datenschutzinformationen dieses Dienstes'. Another red-bordered box contains a login form with fields for 'ZIH-Login:' and 'Passwort:', an unchecked checkbox for 'Anmeldung nicht speichern', and a 'Login' button. A final red-bordered box contains the text: 'Mit [Anmelden] bestätigen Sie, dass Sie die hier aufgeführten Hinweise zum Datenschutz gelesen und verstanden haben und diesen Dienst unter diesen Bedingungen nutzen.' At the bottom, there are three columns of small text: 'Es gilt die Impressum der TU-Dresden mit folgenden Abweichungen: Konzeption, Realisierung, Betreiber: Technische Universität Dresden, Zentrum für Informationsdienste und Hochleistungsrechnen (01062) Dresden.', 'Barrierefreiheit', and 'Für Rückfragen kontaktieren Sie bitte das Service Desk: Tel. +49 371 463-40000, Fax. +49 371 463-42328, E-Mail: service@zih.tu-dresden.de'.

- Inhalt** Nachbau des an der TUD genutzten SSO-Portals (Shibboleth)
- SEIs** Domain, Dienstbeschreibung inkonsistent, Defekte Links

Kampagne Okt. 2021

Training nach Dateneingabe



TECHNISCHE UNIVERSITÄT DRESDEN EN

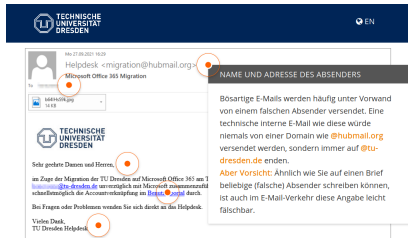
⚠ DAS WAR KNAPP ⚠

Dies hätte eine echte Phishing-Mail sein können!

Aber keine Sorge, es besteht keine Gefahr. Die E-Mail, die Sie erhalten haben, ist Teil unseres integrierten Trainings am Arbeitsplatz. Mittels dieser Phishing-Simulation wollen wir unter den Angestellten der TU Dresden das Bewusstsein für betrügerische Phishing-E-Mails schärfen. Selbstverständlich werden dabei keinerlei individuelle Verhaltensdaten erhoben oder gespeichert.

Wir möchten Ihnen nun anhand der E-Mail, aufgrund der Sie auf dieser Seite gelandet sind, wichtige Indikatoren betrügerischer E-Mails vorstellen.

[➔ ZUR ERKLÄRUNG ➔](#)



TECHNISCHE UNIVERSITÄT DRESDEN EN

04.27.2021 10:20

Hilfesk <migration@hubmail.org>
Microsoft Office 365 Migration

NAME UND ADRESSE DES ABSENDERS

Bösartige E-Mails werden häufig unter Vorwand von einem falschen Absender versendet. Eine technische interne E-Mail wie diese würde niemals von einer Domain wie @hubmail.org versendet werden, sondern immer auf @tu-dresden.de enden.

Aber Vorsicht: Ähnlich wie Sie auf einen Brief beliebige (falsche) Absender schreiben können, ist auch im E-Mail-Verkehr diese Angabe leicht fälschbar.

Sehr geehrte Damen und Herren,

Im Zuge der Migration der TU Dresden auf Microsoft Office 365 am 1. September 2021 sind Sie von Microsoft eingeladen worden, Ihre Account-Verknüpfung zu bestätigen.

Bei Fragen oder Problemen wenden Sie sich direkt an die [Hilfesk](#).

Vielen Dank,
TU Dresden [Hilfesk](#)

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

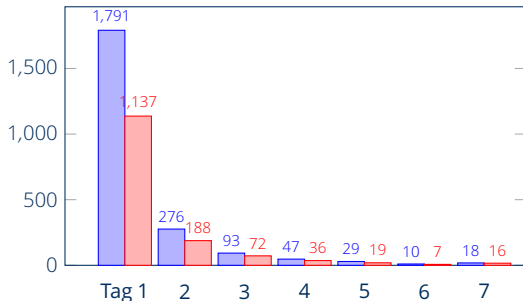
Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

Kampagne Okt. 2021

Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

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

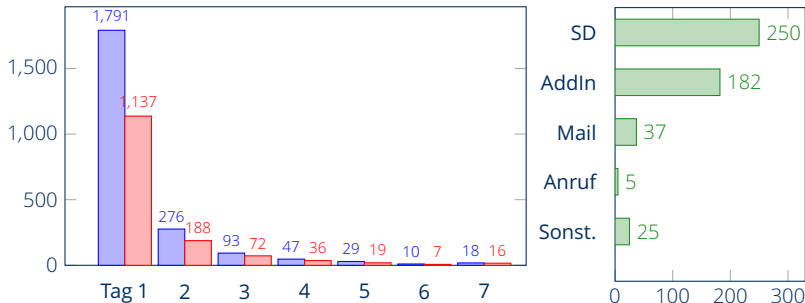


Kampagne Okt. 2021

Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

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

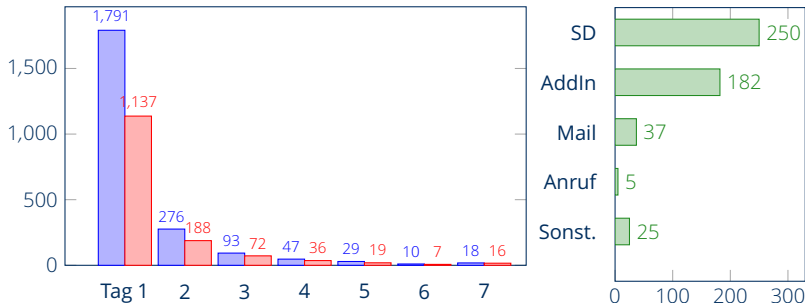


Kampagne Okt. 2021

Auswertung

Versand an 12800 Empfänger binnen weniger Stunden ab Montag Vormittag

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

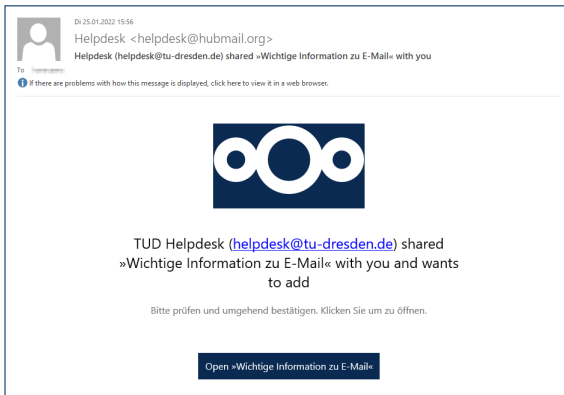


Nachwirkungen am Servicedesk: für 2-3 Tage mit Meldungen ausgelastet

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

Kampagne Jan. 2022

Phishing-Nachricht

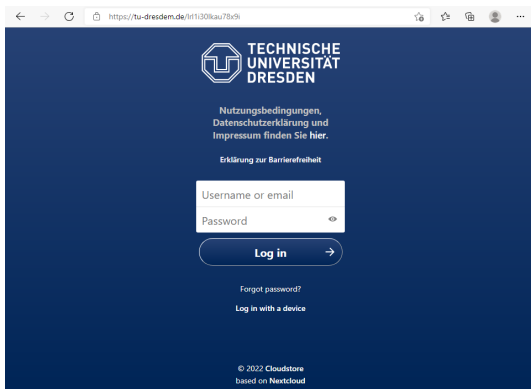


Pretext Freigabe wichtiger Dokumente mittels *TUD Cloudstore* (Nextcloud)

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

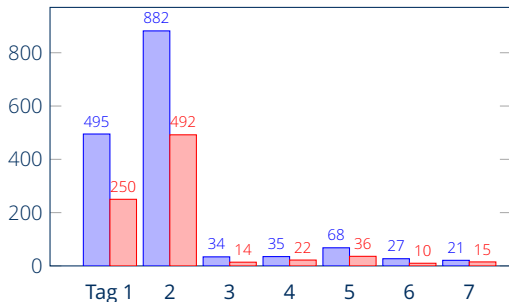
Kampagne Jan. 2022

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



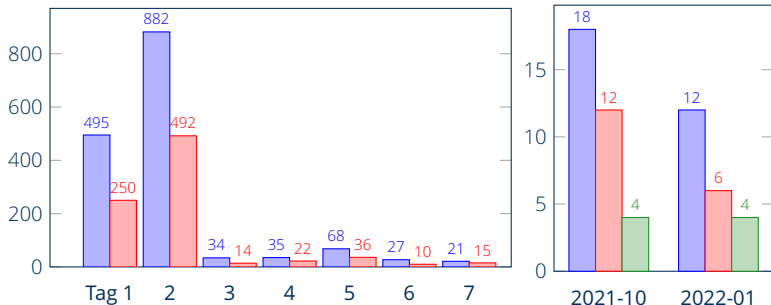
Kampagne Jan. 2022

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 eingegebenen Daten für belastbare Statistik "erfolgreicher Angriffe"?

Offene Punkte zum Nachdenken

Vergleichbarkeit der Kampagnen eingeschränkt (Schwierigkeit, externe Faktoren)

Validierung der eingegebenen Daten für belastbare Statistik "erfolgreicher Angriffe"?

CERT-Reaktion auf Meldungen?

- Sofortige Aufklärung → False Positives
- Pausenzeitraum ohne Reaktion ≠ Tagesgeschäft
- Zunächst "böartig, bitte löschen" mit späterer Aufklärung?

Offene Punkte zum Nachdenken

Vergleichbarkeit der Kampagnen eingeschränkt (Schwierigkeit, externe Faktoren)

Validierung der eingegebenen Daten für belastbare Statistik "erfolgreicher Angriffe"?

CERT-Reaktion auf Meldungen?

- Sofortige Aufklärung → False Positives
- Pausenzeitraum ohne Reaktion ≠ Tagesgeschäft
- Zunächst "bösaartig, bitte löschen" mit späterer Aufklärung?

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