sosafe

AUSSCHNITT AUS DEM HUMAN RISK REVIEW 2022

Menschliche Sicherheitsrisiken durch Social Engineering

03 Menschliche Sicherheitsrisiken durch Social Engineering – eine Analyse

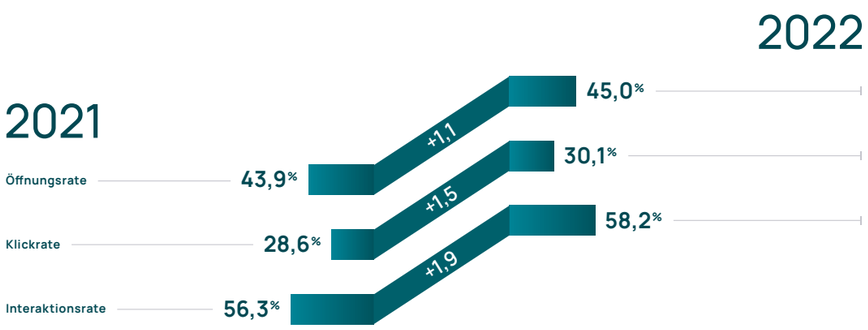
Die vorangegangenen Kapitel zeigen vor allem eines: Die Bedrohungslage hat sich weiter verschärft – und dabei steht der Mensch zunehmend im Fokus.

Doch wie genau greifen uns die Cyberkriminellen an? Welche Social-Engineering-Taktiken funktionieren besonders gut? Und welche Trends und Handlungsempfehlungen lassen sich aus den Einblicken ableiten?

In unserer jährlichen Kernanalyse rund um Phishing und Social Engineering tragen wir psychologische und technische Daten und Analysen aus verschiedenen Quellen zusammen und beantworten genau diese Fragen.

3.1 Psychologische und technische Angriffsvektoren bei Phishing-Simulationen

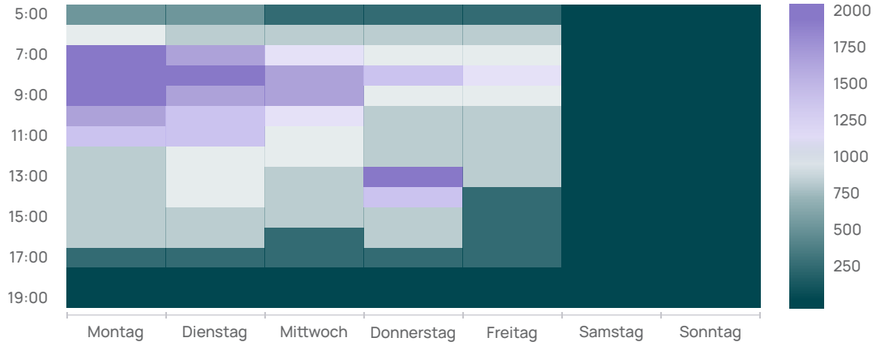
Diese Analysen (Seite 44-48) basieren auf exklusiven Reaktionsdaten aus der SoSafe Awareness-Plattform. Dazu wurden über 4,3 Millionen simulierte Phishing-Angriffe von 1.500 Kundenorganisationen aus dem Jahr 2021 anonym ausgewertet und die Erfolgswahrscheinlichkeit verschiedener Angriffstaktiken analysiert. So ergeben sich exklusive Einblicke in psychologische, technische und weitere Vektoren, die menschliche Risiken in Organisationen beeinflussen.



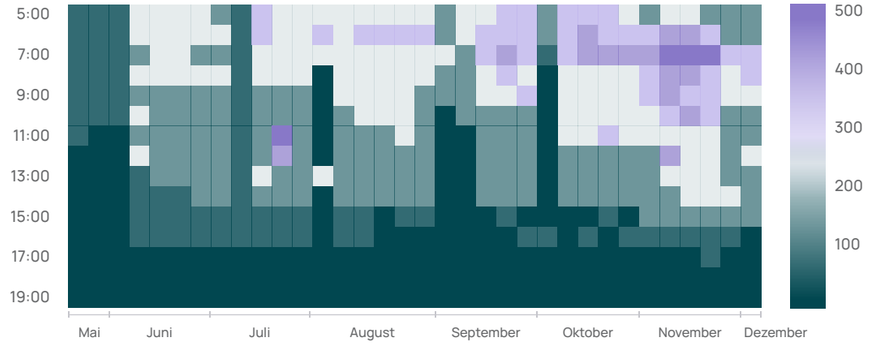
Die Cyber-Bedrohungslage hat sich verschärft – und auch menschliche Risiken haben nicht abgenommen. Die Öffnungs-, Klick- und Interaktionsraten bei Phishing-Mails sind weiterhin auf hohem Niveau. Im Vergleich zum Vorjahr sind sie sogar noch weiter angestiegen.

Fast die Hälfte aller Nutzenden öffnet Phishing-Mails – davon klickt fast jede und jeder Dritte auf enthaltene Links, Anhänge oder andere schädliche Inhalte. 58 Prozent dieser Nutzenden wiederum interagieren zudem mit den Inhalten und geben beispielsweise persönliche Daten in fingierte Login-Masken ein.

Melderaten: Der frühe Vogel bekommt Phishing-Mails



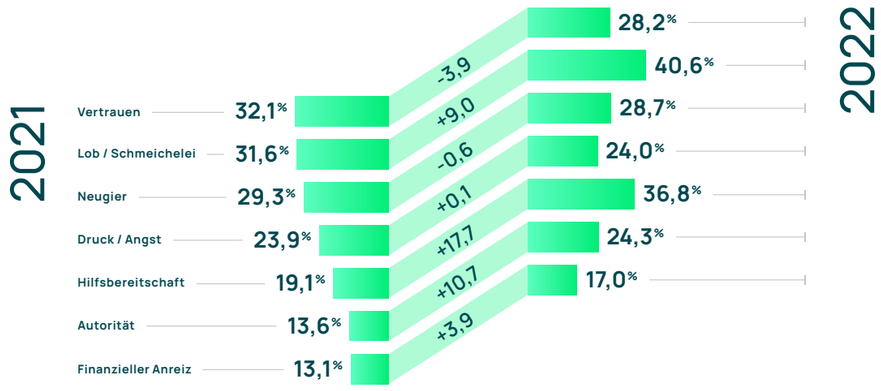
Die meisten Phishing-Versuche werden montags morgens von Mitarbeitenden bemerkt. Zwischen 07:00 und 09:00 Uhr meldeten Nutzende an Montagen die meisten verdächtige E-Mails. Im Verlauf der Woche bleibt die Anzahl der gemeldeten Phishing-Mails morgens am höchsten – vor allem vor oder während des ersten Kaffees ist daher besondere Vorsicht geboten. Das heißt aber nicht, dass man sich nach der Mittagspause generell in Sicherheit wägen kann: Der Ausschlag donnerstags zeigt, dass auch unaufmerksames Verhalten im Laufe des Tages Gefahren birgt.



Heatmaps basierend auf echter Phishing-Mails, die über den SoSafe Phishing-Meldebutton gemeldet wurden.

Die Sicht auf das gesamte Jahr bestätigt die Erkenntnisse aus der Wochen-Analyse – generell werden vor 09:00 Uhr die meisten Phishing-Mails von Mitarbeitenden erkannt. Zum Ende des Jahres wird außerdem deutlich: Cyberkriminelle nutzen vor allem umsatzstarke Zeiten im Einzelhandel gerne aus. In den Monaten Oktober bis Dezember werden deutlich mehr Phishing-Versuche gemeldet als in der Mitte des Jahres. In diese Zeit fallen zum Beispiel der Black Friday, der Cyber Monday und die Weihnachtsfeiertage.

Positive Emotionen verleiten zum Trugschluss



In Phishing-Mails verwenden Cyberkriminelle verschiedene psychologische Taktiken, um potenzielle Opfer dazu zu verleiten, Daten preiszugeben oder kompromittierte Dateien zu öffnen. Am anfälligsten sind Empfängerinnen und Empfänger bei positiv konnotierten Emotionen: Zu den erfolgreichsten Taktiken gehören wie auch schon im letzten Jahr Hilfsbereitschaft, Lob/Schmeichelei, Neugier und Vertrauen. Mit Lob und vermeintlicher Hilfsbereitschaft verleiten Cyberkriminelle mehr als ein Drittel der Empfängerinnen und Empfänger zum Klick auf schädliche Inhalte.

Der hohe Anstieg der Klickraten in den Bereichen Hilfsbereitschaft und Autorität zeigt Parallelen zur neuen Normalität im Kontext der Pandemie und hybriden Arbeitsmodellen. Durch die vermehrte Kommunikation über digitale Kanäle und den Wegfall persönlicher Begegnungen gehört es heute zum Alltag, von Kolleginnen und Kollegen per Mail oder Kollaborationstool um Hilfe gebeten zu werden. Meist wird eine schnelle Reaktion erwartet. Das verleitet dazu, unüberlegt zu handeln – gerade, wenn die Anfrage von einer Autoritätsperson kommt. Auch Cyberkriminelle wissen das und nutzen genau diese Kanäle für ihre Angriffe.

Positiv zu vermerken ist, dass die Menschen skeptischer geworden sind, wenn es um scheinbar vertrauenserweckende Inhalte geht, so beispielsweise gefälschte Newsletter von bekannten Organisationen oder vermeintliche Lieferinformationen von Versanddienstleistern. Hier fielen die Zahlen im Vergleich zum Vorjahr. Generell fielen die wenigsten Empfängerinnen und Empfänger auf Phishing mit finanziellen Anreizen hinein. Die Vermutung liegt nahe, dass diese Taktik bereits lange im Einsatz und entsprechend gut bekannt ist.

Die Top 10 Phishing-Betreffzeilen

1 66 %
Autorität
Folgende Aufgabe ist zu erledigen: Verteilung der Dokumente und Aufgabenprüfung

2 66 %
Hilfsbereitschaft; Neugier
Sie haben 2 Erwähnungen

3 57 %
Autorität; Druck/Angst
Wichtig: CORONA Update

4 51 %
Autorität; Neugier
Allgemeine Information: Neue Lohnabrechnungssoftware

5 50 %
Druck/Angst
Missed meeting

6 49 %
Neugier; Vertrauen
Newsletter für September 2021

7 46 %
Autorität; Neugier
Beitrag vom Vorstand

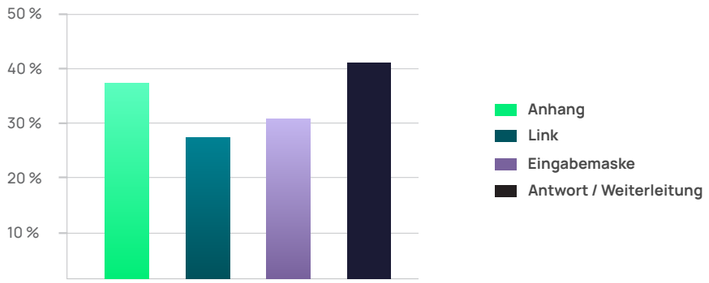
8 46 %
Autorität
[EXT] Aktualisierung Organisationsanweisung für mobile Geräte

9 42 %
Neugier
Ihr eingescanntes Formular

10 41 %
Vertrauen; Druck/Angst
Ihr Office 365 Passwort läuft heute ab

Welche Betreffzeilen verleiten Empfängerinnen und Empfänger am ehesten zum Klick auf eine Phishing-Mail? Auch in dieser Auswertung zeigt sich: Das Vorgaukeln von Autorität und das Ausnutzen der Hilfsbereitschaft von Menschen funktionieren – vor allem dann, wenn ein Element der Neugier hinzukommt. Der Bezug auf neue, hybride Arbeitsmodelle (Platz 1 und Platz 5) und COVID-19 (zum Beispiel Platz 3) in Betreffzeilen durchbricht aber das typische Schema. Das Einsetzen negativer Emotionen wie Druck und Angst führt in diesem Kontext zu besonders hohen Öffnungs- und Klickraten. Die pandemiebedingte Verunsicherung der Menschen spielt den Cyberkriminellen anscheinend noch immer deutlich in die Karten. Ein deutliches Zeichen für Sicherheitsverantwortliche: Gerade bei hybriden Arbeitsmodellen sollten Mitarbeitende die Möglichkeit bekommen, ihr Verhalten im Umgang mit Cyberrisiken zu trainieren, um sich vor den Gefahren schützen zu können.

Verdächtige Formate oder Tippfehler: Diese technischen Vektoren verursachen die meisten Klicks



Nicht nur mit emotionalen, psychologisch effektiven Inhalten versuchen Cyberkriminelle sich Zugang zu sensiblen Informationen und Daten zu verschaffen. Auch über technische Änderungen und Tricks innerhalb der Phishing-Nachrichten selbst gelingt es ihnen, ihre Opfer hinters Licht zu führen.

Am gefährlichsten sind für Organisationen Phishing-Mails, die eine E-Mail-Konversation vorgaukeln. Etwa 40 Prozent aller Mitarbeitenden klicken auf diese vermeintlichen Folgemails. Auch Anhänge scheinen oftmals nicht als schädlich wahrgenommen zu werden – mehr als jede und jeder dritte Mitarbeitende klickt hier.

Manipulieren Cyberkriminelle Absendeadressen, zeigt sich ein ebenso gefährliches Bild

23,6 % **Typo-Squatting**
Ein unauffälliger Rechtschreibfehler wird in eine Webadresse eingebaut.

31,3 % **Subdomain-Squatting**
Eine fingierte Subdomain wird vor eine unscheinbare Top-Level-Domain gesetzt.

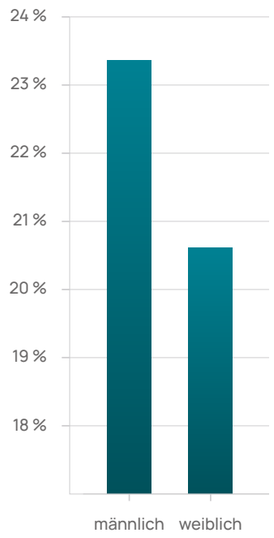
31,2 % **Mail-Address-Spoofing**
Der Absender im E-Mail-Kopf wird überlagert.

19,8 % **Domain-Squatting**
Die fingierte Domain ähnelt der imitierten Domain stark.

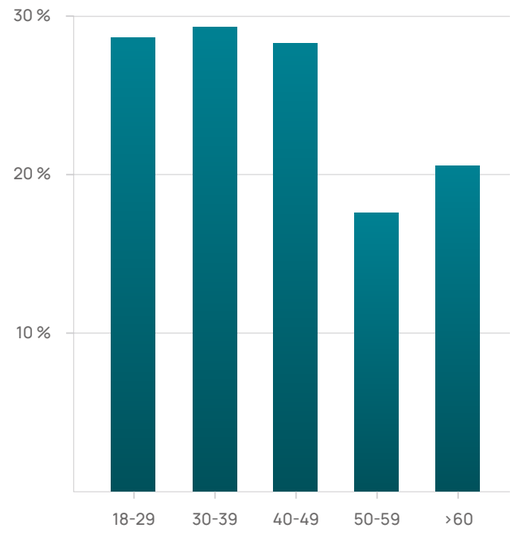
3.2 Unterschiede zwischen Personengruppen

Die jährlich von SoSafe und Botfrei durchgeführte Studie „Phish-Test“ zur allgemeinen Phishing-Awareness liefert demografische Einblicke in das Klickverhalten von Nutzenden. 2021 nahmen über 1350 User teil und erhielten innerhalb einer Woche drei in der Simulation als mittelschwer eingestufte Phishing-Mails, die es zu erkennen galt.

Klickrate nach Geschlecht



Klickrate nach Alter in Jahren



Mit einer durchschnittlichen Klickrate von 23 Prozent über alle demografischen Gruppen hinweg zeigt sich, dass Bürgerinnen und Bürger noch stärker im Umgang mit Cybergefahren sensibilisiert werden sollten.

Wie schon im vergangenen Jahr interagierten trotz der nur mittleren Komplexität der simulierten Phishing-Mails vor allem männliche Teilnehmer mit den Inhalten – knapp jeder Vierte klickte. Dagegen klickte nur jede fünfte Frau.

Insbesondere auch in den Altersgruppen zeichnet sich ein interessantes Bild ab: so klickten gerade die jüngeren Teilnehmenden zwischen 18 und 49 Jahren mit einer Rate von 28,6 Prozent deutlicher häufiger als Über-50-Jährige mit im Durchschnitt nur 19 Prozent. Wie auch schon in den Vorjahren zeigt sich anhand dessen, dass sich gerade auch „Digital Natives“ eventuell etwas unbedarfter im digitalen Raum bewegen.

+24 %

Besonders spannend: Bei Personen, die ihren Wissensstand zur Informationssicherheit selbst als niedrig einschätzen, liegt die Klickrate im Schnitt 24 Prozent höher als bei Personen, die diesen eher als hoch einschätzen. Das gibt Grund zur Hoffnung: Sind den Personengruppen Wissenslücken bewusst, können sie diese aktiv auffüllen – und sich so vor Cyberangriffen schützen.

Der Human Risk Review 2022

Mehr zum zur aktuellen Cyber-Bedrohungslage finden Sie im vollständigen Human Risk Review 2022.

Hier lesen →