GTAI GERMANY TRADE & INVEST

15 JAHRE GTAI

IT SICHERHEIT – PHISHING

04.09.2024 - Jonas Frydrych

Agenda

- Schäden durch Cyberangriffe
- Vorgehen Phishing
- Wie kann ich Phishing-Mails erkennen?
- Aktuelle Zahlen GTAI
- Persönliche Erfahrungen
- Zeit für Fragen

1. AKTUELLE ZAHLEN

Cyberangriffe in Deutschland (bitkom-Studie)

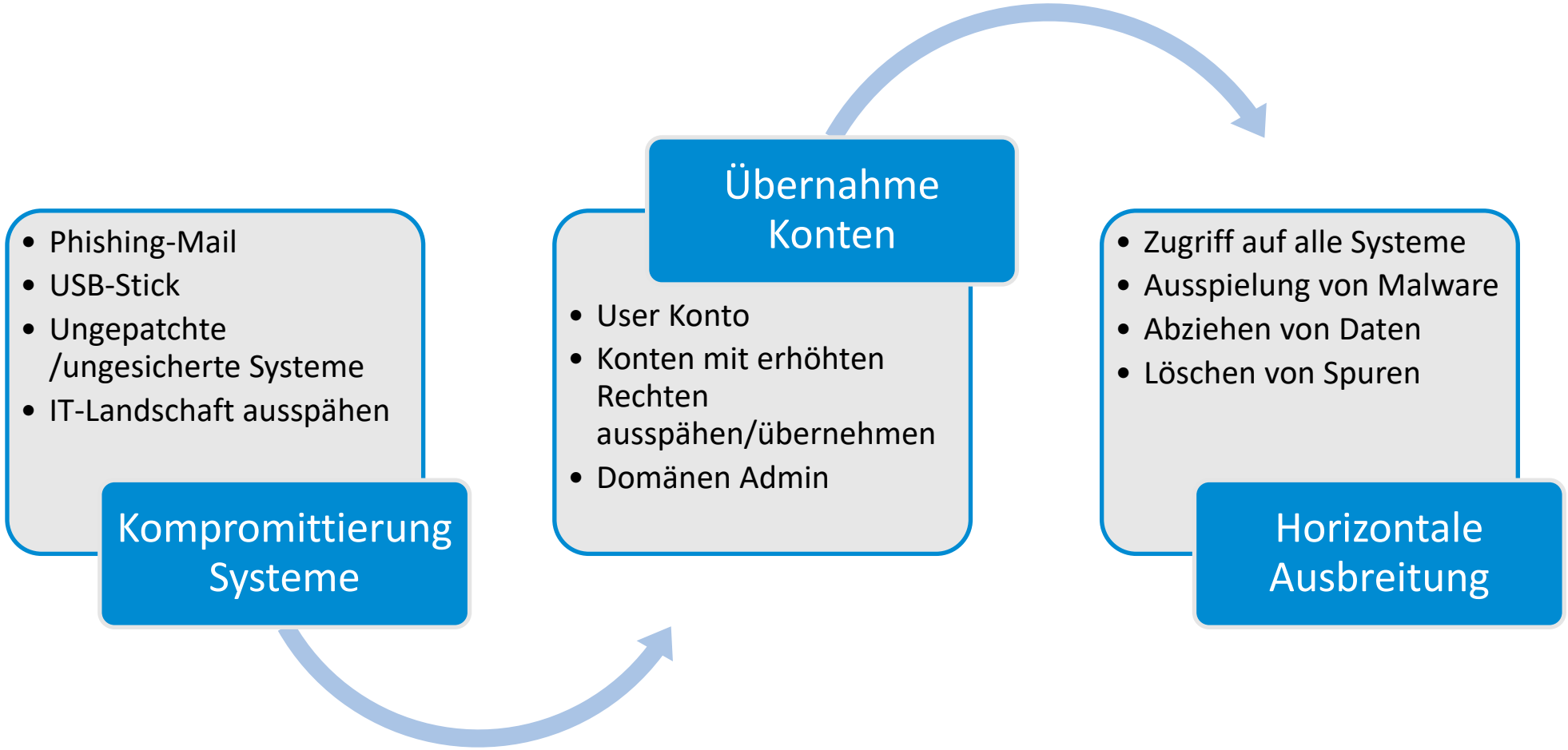
- 267 Milliarden Euro Schäden in 2023
- Anstieg um 29 % zu 2022
- 81% der befragten Unternehmen betroffen

Schäden

1	**Abfluss von Daten**	kritische Unternehmensdaten personenbezogene Daten (Datenschutzvorfall)
2	**Verschlüsselung / löschen von Systemen**	Kein Zugriff mehr auf Daten / Prozesse -> Lösegeld Löschen von Systemen zur Spurenverwischung
3	**Arbeits-/ Produktionsausfall**	Betrieb steht still, Verpflichtungen können nicht erfüllt werden -> Reputationsverlust -> Viele Mittelständler überleben das nicht

2. VORGEHEN PHISHING

Vorgehen der Täter



Die großen W

Wer
- Kriminelle
- Staaten
- Firmen

Warum
- Geld
- Destabilisierung
- Industriespionage

(von) Wo
- Weltweit
- Maskiert
- ein PC reicht

Wie
- Sicherheitslücken in Systemen
- über den User
- Über Dritte

Unterschied SPAM (Junk) / Phishing

Spam-Mails:

- unerwünschte E-Mails (z.B. Werbemails)
- können Schadprogramme enthalten (z.B. gefälschte Bewerbung)

Phishing-Mails

- zielen darauf ab vertrauliche Informationen zu stehlen
- Anhänge oder Links auf gefährliche Webseiten

Wie funktioniert Phishing?

Quelle: https://www.infinco.com/moeglichkeiten-zum-schutz-vor-phishing-emails/

Arten von Phishing

Quelle: bleib-virenfrei.de/it-sicherheit/artikel/was-ist-phishing

Spezialfall: Whaling = Spear-Phishing bei hochrangigen Opfern

Warum gibt es so viele offensichtliche SPAM-Mails?

- Geringer Aufwand
- Eine/r von 10.000 reicht aus
- Unsere Instinkte sollen überlistet werden
  - Nigerianischer Prinz
  - Katzen- / Nacktbilder
  - Geheime Unterlagen

- Falsche Sicherheit wird vorgetäuscht

Die offensichtlichen SPAM-Mails lenken von den wirklich gefährlichen ab!

Wachsam bleiben!

3. WIE KANN ICH PHISHING MAILS ERKENNEN?

Merkmale

- Erwarte ich diese Mail?
- Kenne ich den Absender? Passt der Inhalt zu diesem?
- Bei Zweifeln nachfragen! (Absender, IT,…)
- Kein seriöser Anbieter fragt nach Zugangsdaten
- Keine unbekannten Anhänge öffnen
- Absenderadresse prüfen
- Links prüfen

Vorsicht, Phishing! Betrügerische E-Mails erkennen

Gefälschte Absender-Adresse
Ist die E-Mail-Adresse des Absenders z.B. durch einen Vergleich zu verifizieren? Kann der Absender den Versand der Mail persönlich/ telefonisch bestätigen?

Abfrage vertraulicher Daten
Fordert die E-Mail zur Eingabe persönlicher Informationen auf? Werden Geheimnummern oder Passwörter abgefragt?

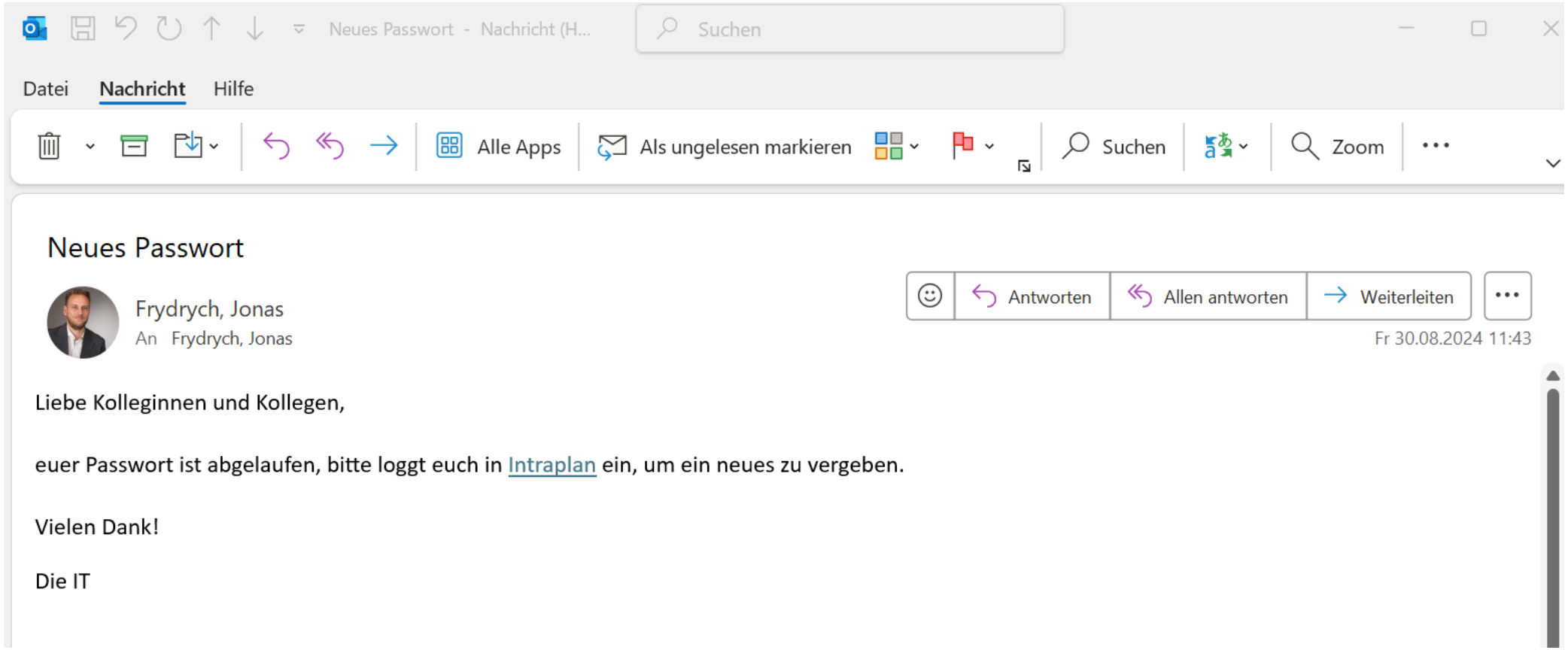
Vorgetäuschter dringender Handlungsbedarf
Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf? Wird eine Nachricht des Absenders erwartet?

Links zu gefälschten Webseiten
Enthält die E-Mail Verlinkungen, die auf andere Webseiten verweisen? Welche Ziel-URL wird bei einem Mouseover angezeigt?

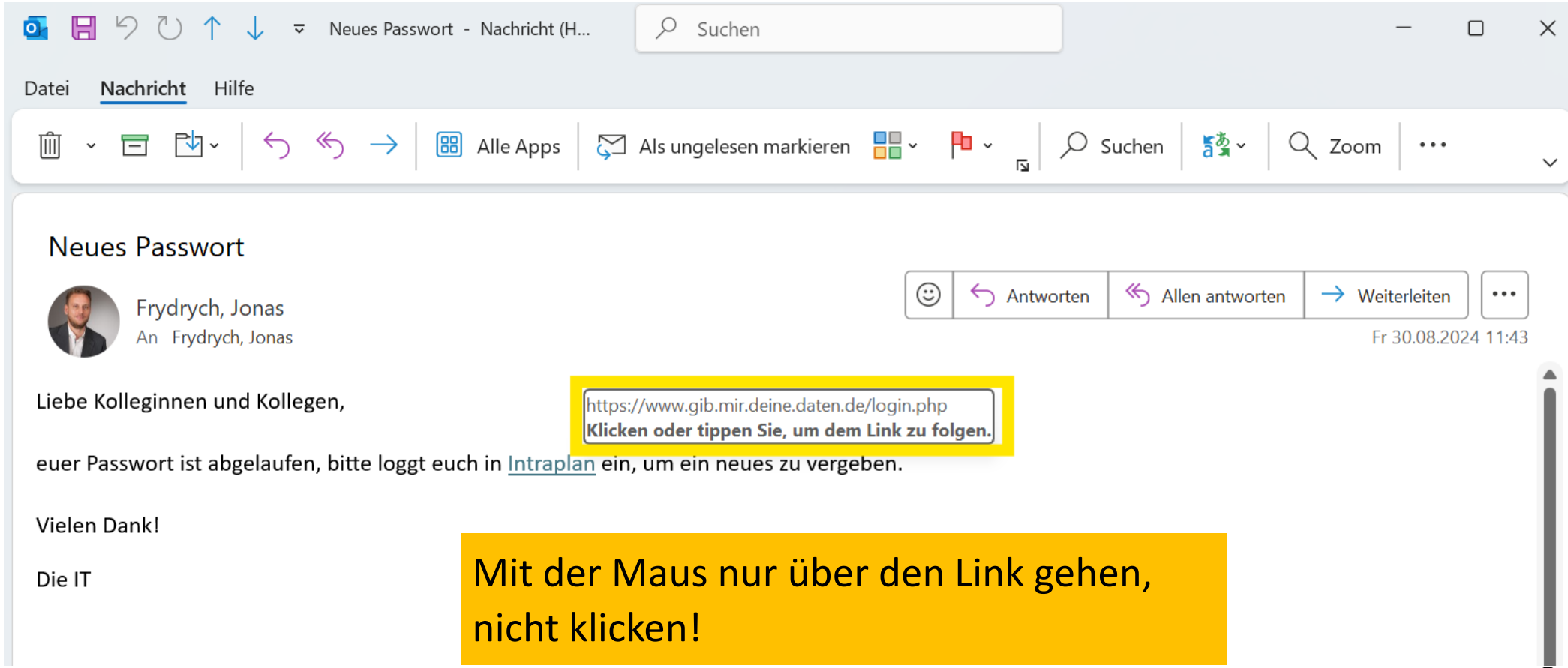
Sprachliche Ungenauigkeiten
Ist die Anrede unpersönlich formuliert? Enthält der Text Rechtschreib- oder Zeichenfehler?

www.bsi-fuer-buerger.de

Links überprüfen

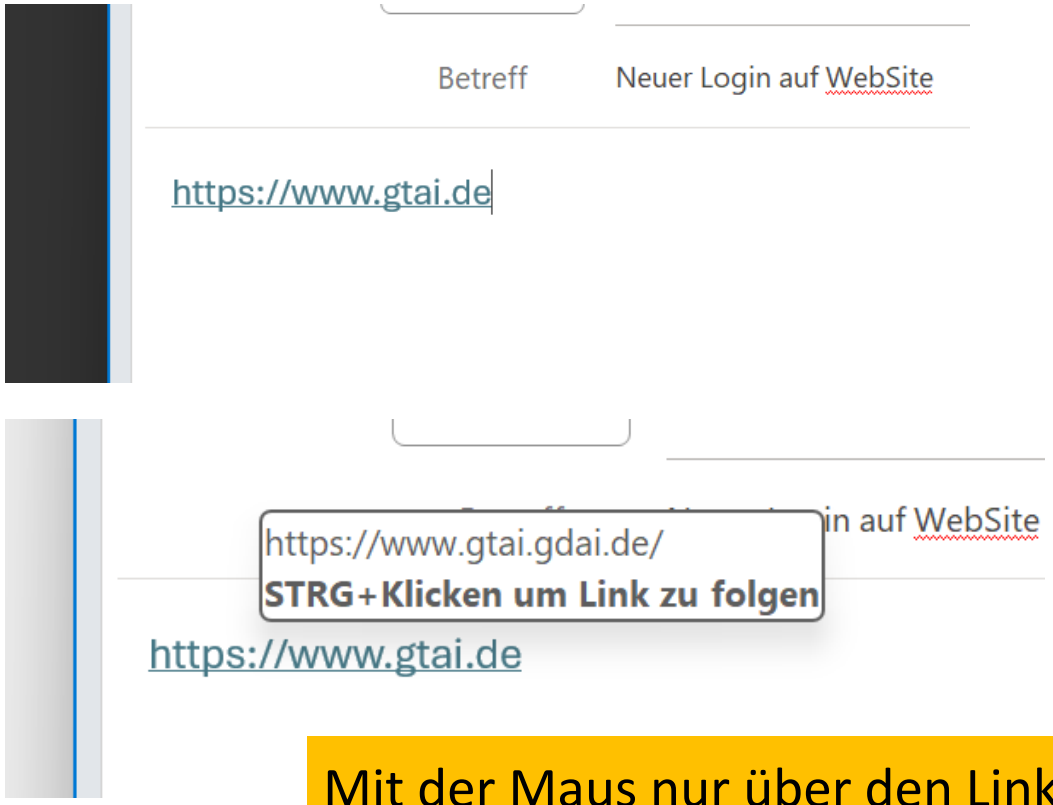


Links Mouse Over



Mit der Maus nur über den Link gehen, nicht klicken!

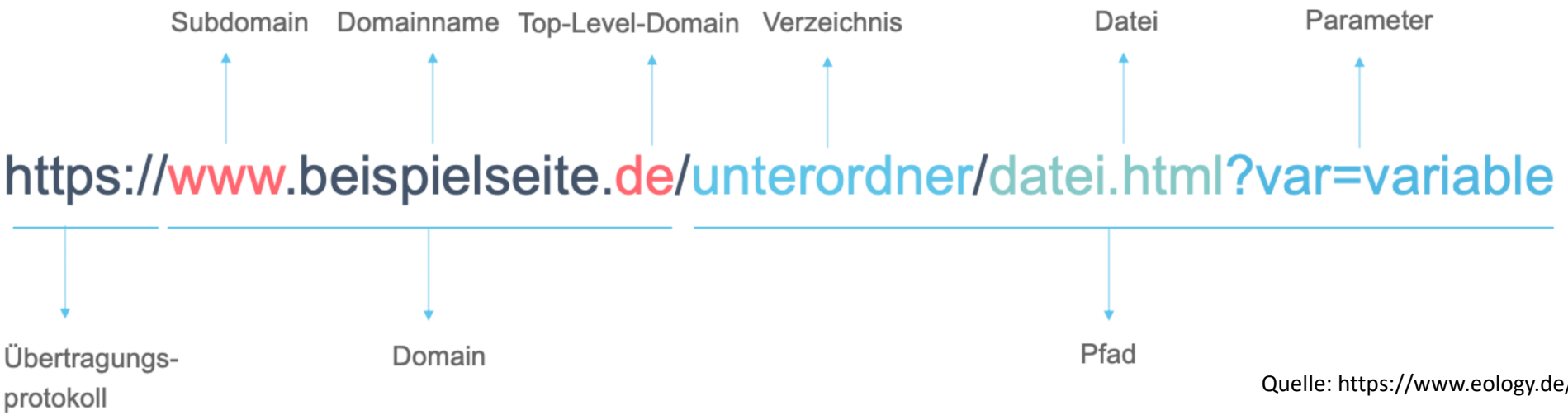
Links Mouse Over 2



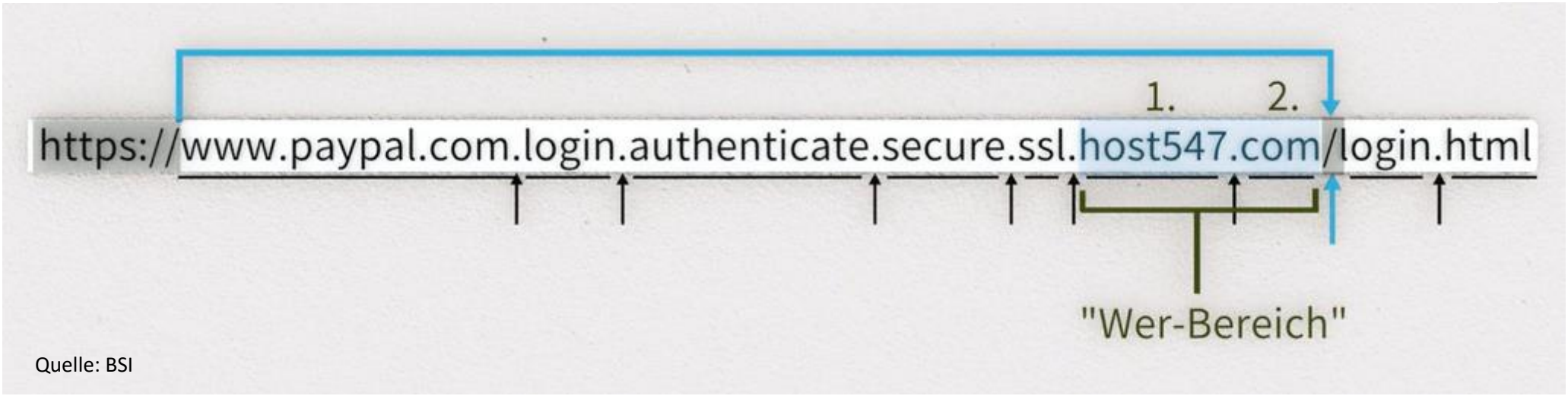
Mit der Maus nur über den Link gehen, nicht klicken!

- **Vor dem Klicken die Links überprüfen!**

URLs



Quelle: https://www.eology.de/wiki/url



Quelle: BSI

Links

https://denn.vor.den.wer.bereich.kann.man.so.viele.p.u.n.k.t.e.setzen.wie.man.möchte.gtai.de/

https://shoppen-im-web.de/www.amazon.com/login.php

https://www.amazon.de.webapp.mppls.com/legalhub

https://www.sprakasse-karlsruhe.de/privatkunden/login.htm

https://www.paypa1.com/signin?country.x=DE&locale.x=de_DE

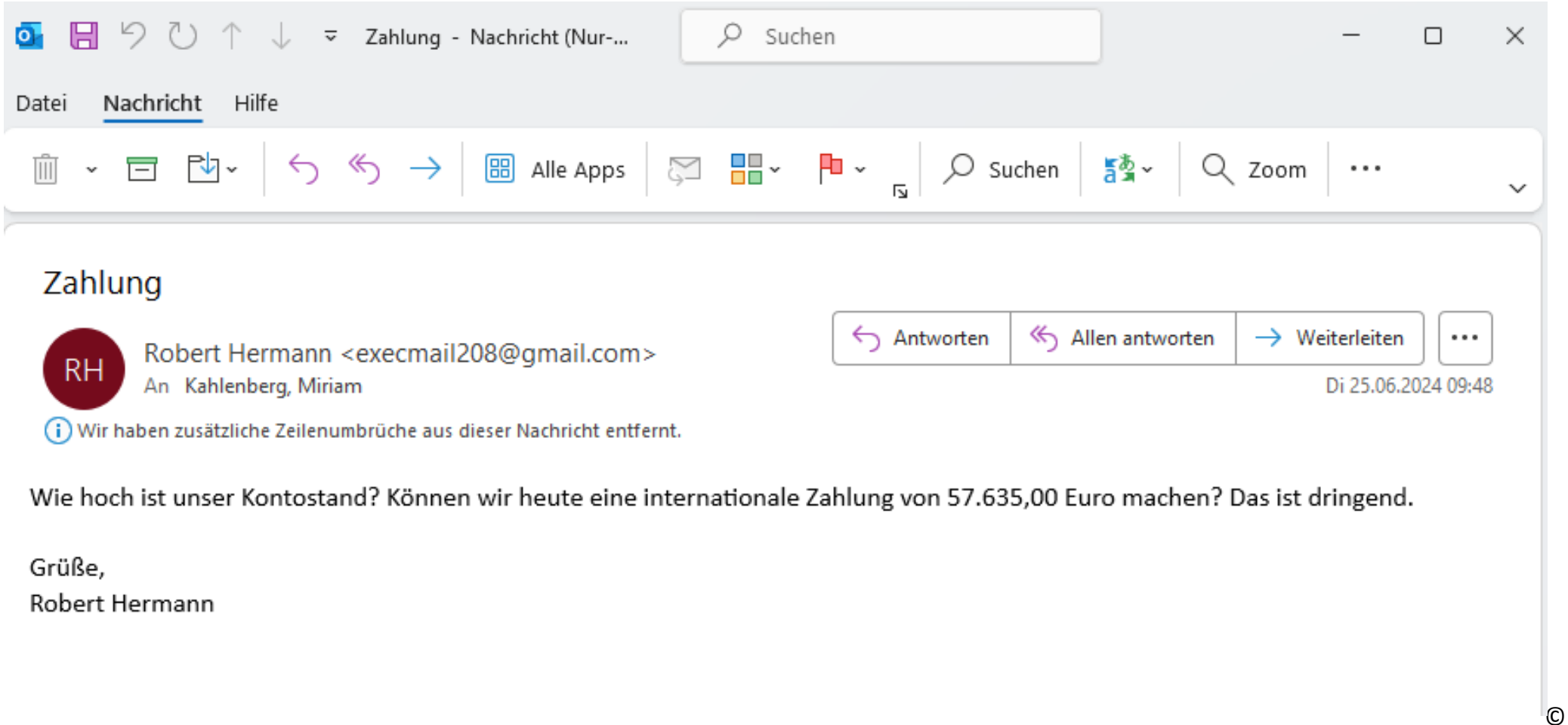
https://www.amazon.de

https://www.sparkasse-duesselclorf.de

https://www.paketsrevice.de

Quelle: BSI

Beispiel für Phishing Mail



Beispiel für Phishing Mail

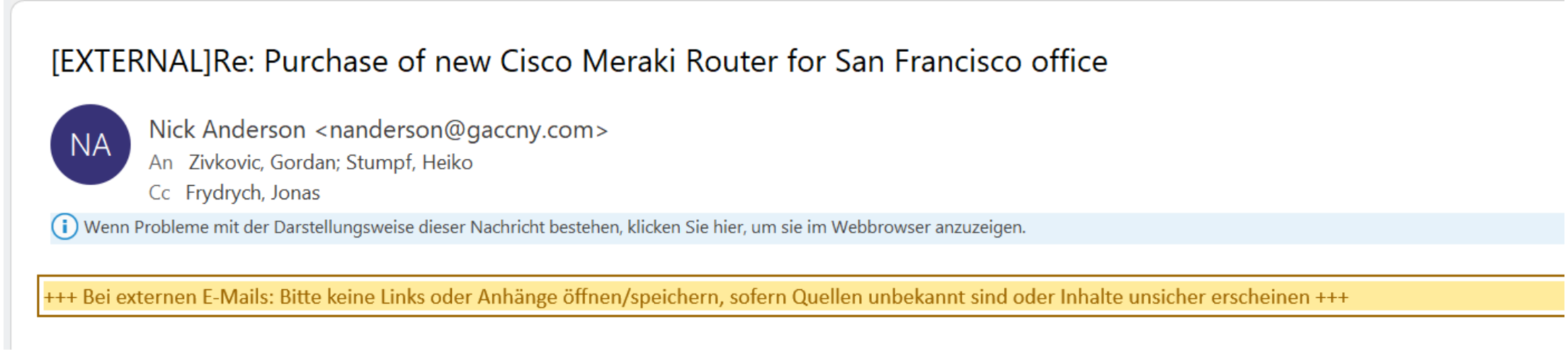
Von: Marcus Schmidt <aj334150@gmail.com>
Gesendet: Mittwoch, 17. Januar 2024 11:38
An: Burock, Petra <petra.burock@gtai.de>
Betreff: Hallo Petra

Ich habe meine Bank gewechselt und möchte meine neuen Bankdaten bei der Firma aktualisieren. Kann diese Änderung für den Januar-Gehalts Zyklus wirksam werden?

Ich wünsche Ihnen ein angenehmes neues Jahr.

Grüße,
Marcus Schmidt

Neue Kennzeichnung [EXTERNAL]



Externe Mail werden gekennzeichnet, damit sie besser als solche erkannt werden

4. AKTUELLE ZAHLEN GTAI

Wie viele Mails werden rausgefiltert?

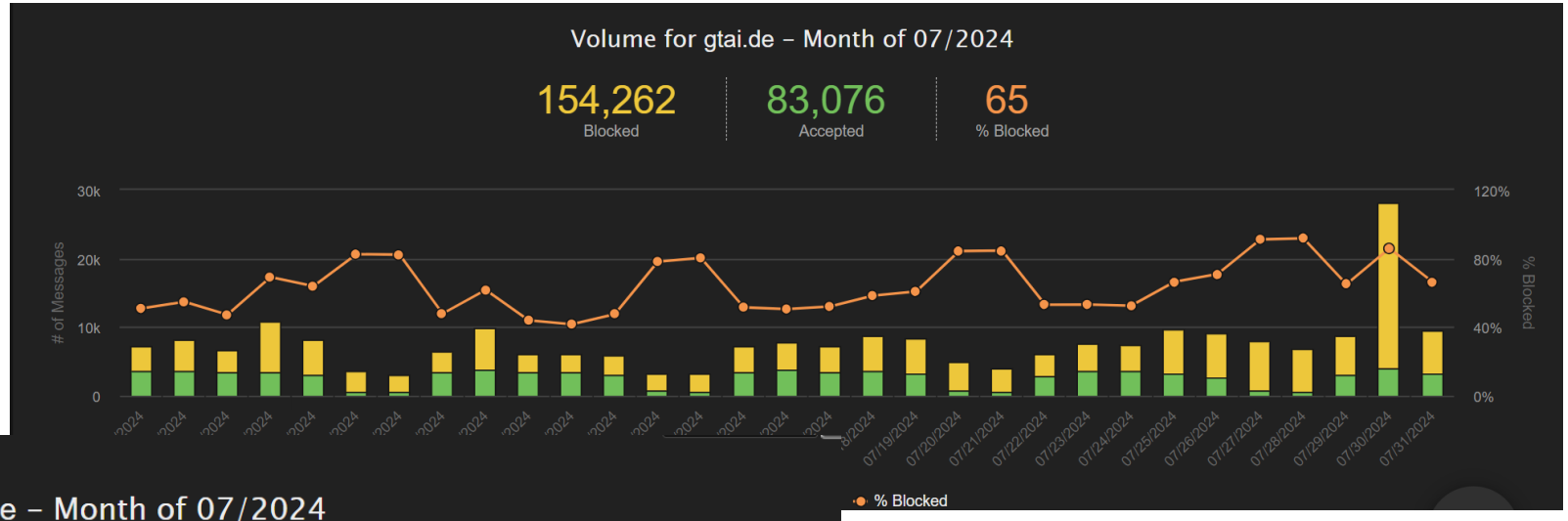
1 **Annahme / Block**	Welche Mails werden überhaupt angenommen von unsrem Mailserver?
2 **Prüfung / Sandbox**	Die angenommenen Mails werden geprüft
3 **Zustellen / Quarantäne / Löschen**	Nach Prüfung werden die Mails zugestellt, in Quarantäne verschoben oder gelöscht

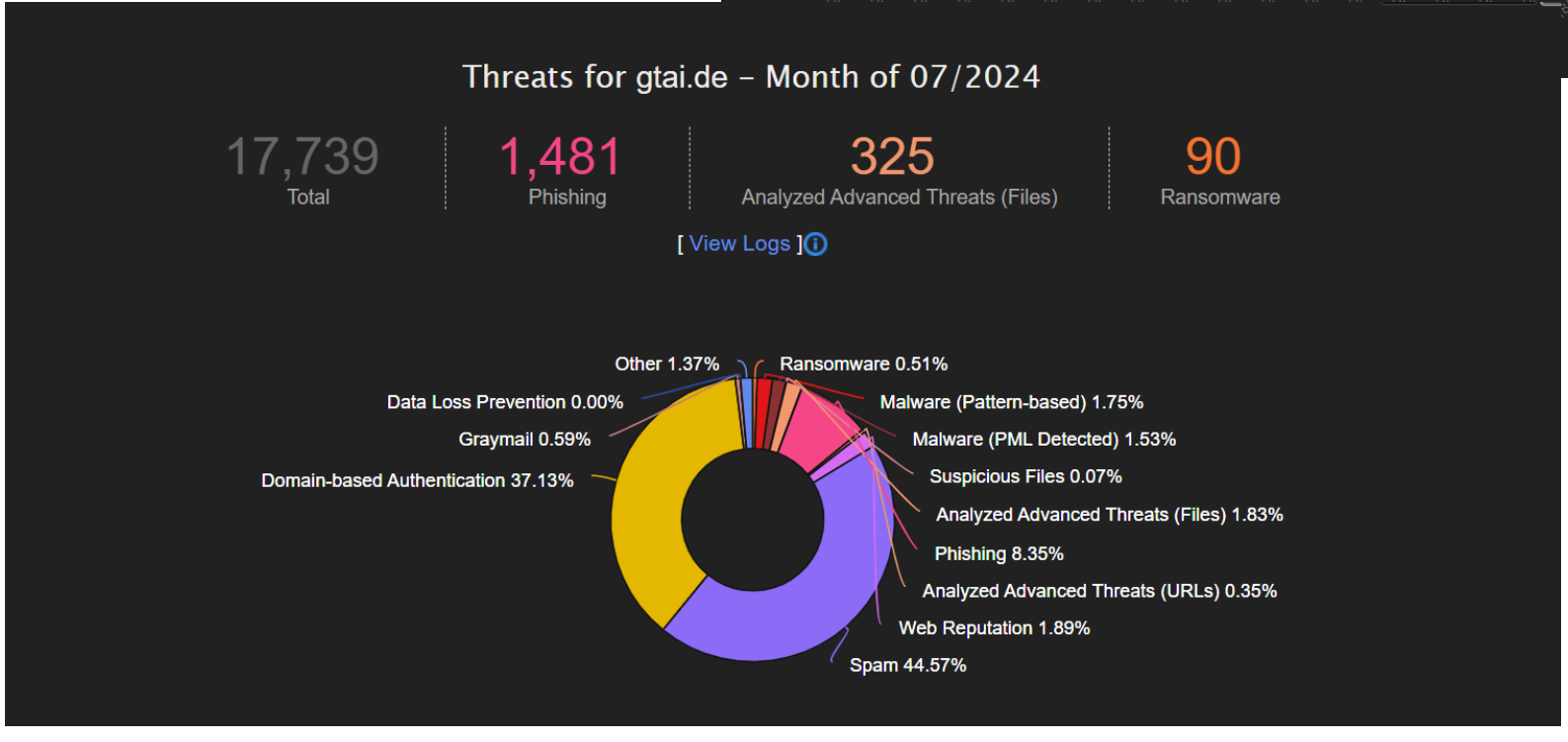
Übersicht Eingehende Mails

Monat	Mails	Blocked	Accepted	Rate	Threats
Jun 24	202.897	127.253	75.644	63%	15.498
Jul 24	237.338	154.262	83.076	65%	17.739
Aug 24	196.327	118.119	78.208	60%	17.176

Mailfluss

- Mails im Juli 237.338





5. PERSÖNLICHE ERFAHRUNGEN

Persönliche Insights – für den privaten Gebrauch

1. 2-FA einstellen, überall wo es geht
2. Unterschiedliche Passwörter verwenden + Passwortsafe
3. Das Risiko geklauter Identitäten minimieren
4. Initiale Einstellungen von Hard- und Software ändern

https://www.retarus.com/blog/de/phishing-ist-weiter-das-haupteinfallstor-fuer-cyberkriminelle/

Zeit für Fragen?

Kontakt: jonas.frydrych@gtai.de