FH MÜNSTER

Fraunhofer ACADEMY

E-Mail-Sicherheit in Unternehmen
Mehr als Phishing-Awareness

Dr.-Ing. Fabian Ising
07.02.2024

Lernlabor
Cybersicherheit

Who am I?

Dr.-Ing. Fabian Ising

- Wissenschaftlicher Mitarbeiter am Fraunhofer SIT
  - Abteilung: Applied Cryptography and Medical Security (ACM)
- Trainer im Lernlabor Cybersicherheit (LLCS)
  - Trainingsschwerpunkt: E-Mail-Sicherheit für Unternehmen

- Forschung:
  - Angewandte Kryptographie, insb. E-Mail-Sicherheit
  - Sicherheit von Netzwerkprotokollen

Who are you?

Wer hat in den letzten Monaten an einer Phishing-Awareness-Schulung teilgenommen?

Who are you?

Wer hat in den letzten Monaten an einer Phishing-Awareness-Schulung teilgenommen?

Wer ist schonmal auf Phishing reingefallen?

Anatomie eine Sicherheitsvorfalls

Jedes zehnte Unternehmen von Cyberangriffen betroffen

Die häufigste Methode, mit der Unternehmen angegriffen wurden, war das sogenannte Phishing. Dabei werden über E-Mails Passwörter abgegriffen oder schädliche Software verbreitet. In 62 Prozent der Unternehmen war ein Phishingangriff erfolgreich. An zweithäufigster

Ransomware: How clicking on one email left a whole business in big trouble

A food and drink manufacturer fell victim to a ransomware attack and crucially didn't give into the extortion demand - but it could've been much worse.

Written by **Danny Palmer,** Senior Writer

July 30, 2020 at 3:19 a.m. PT

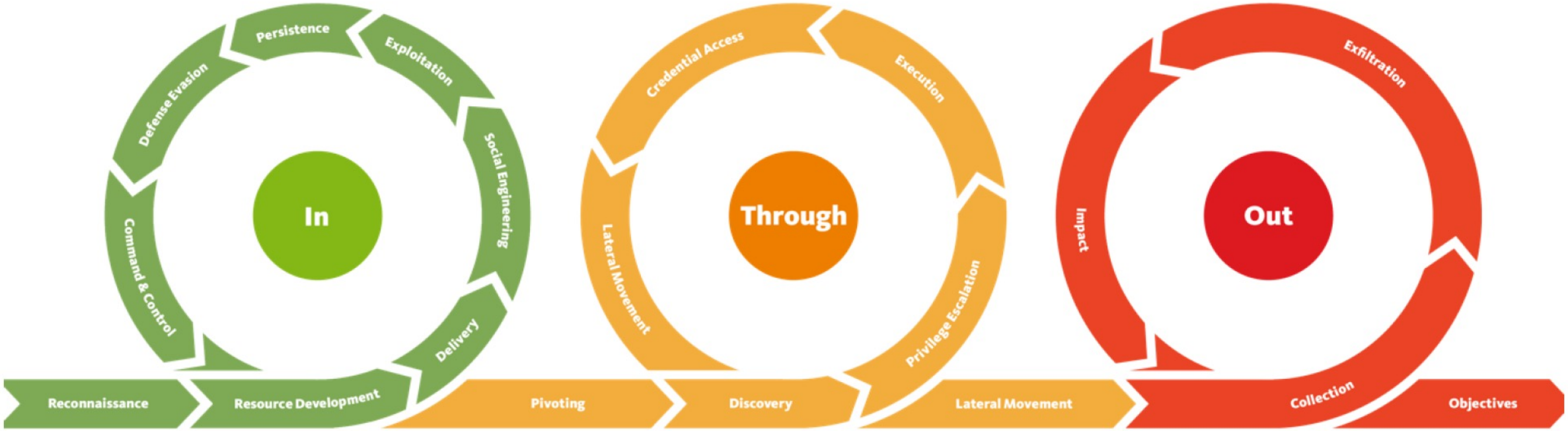
Just one click – that's all it takes to let in cyber-crime

Fri, 25th Sep 2020

FH MÜNSTER Fraunhofer ACADEMY

Ein Klick = Infiziert?

Die Unified Kill Chain



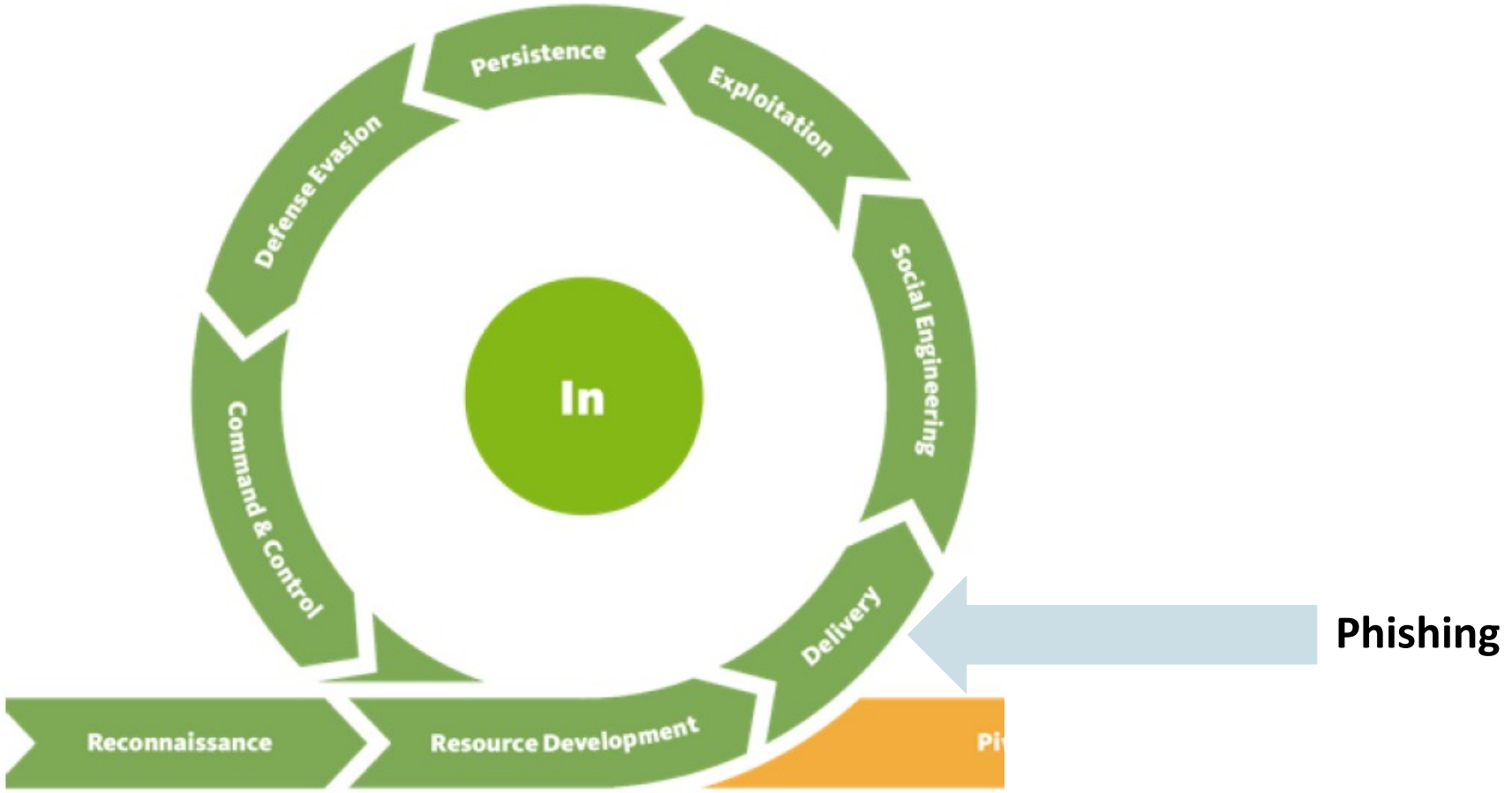
Ein Klick = Infiziert?

Die Unified Kill Chain

FH MÜNSTER
Fraunhofer ACADEMY

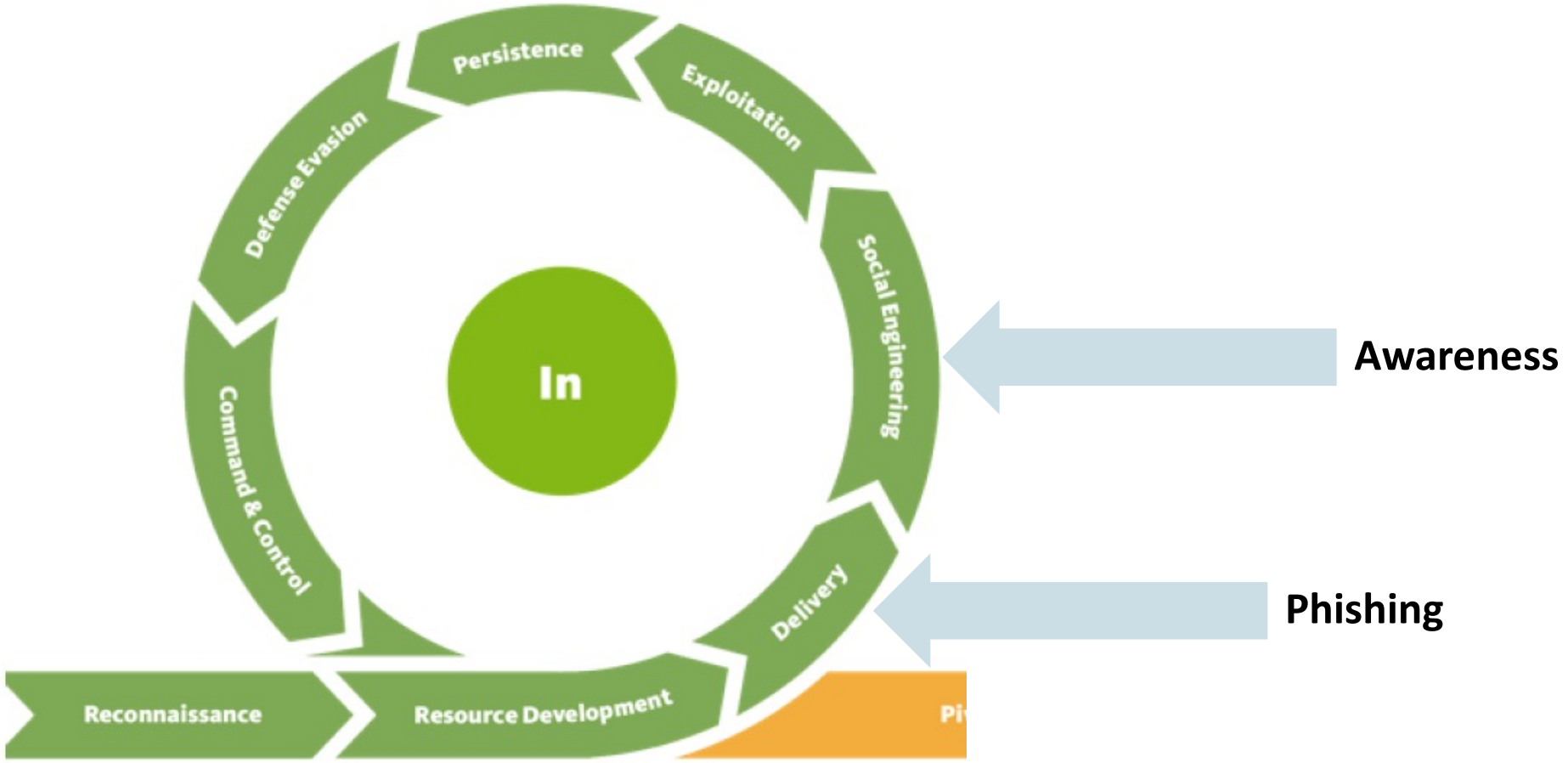
Ein Klick = Infiziert?

Die Unified Kill Chain

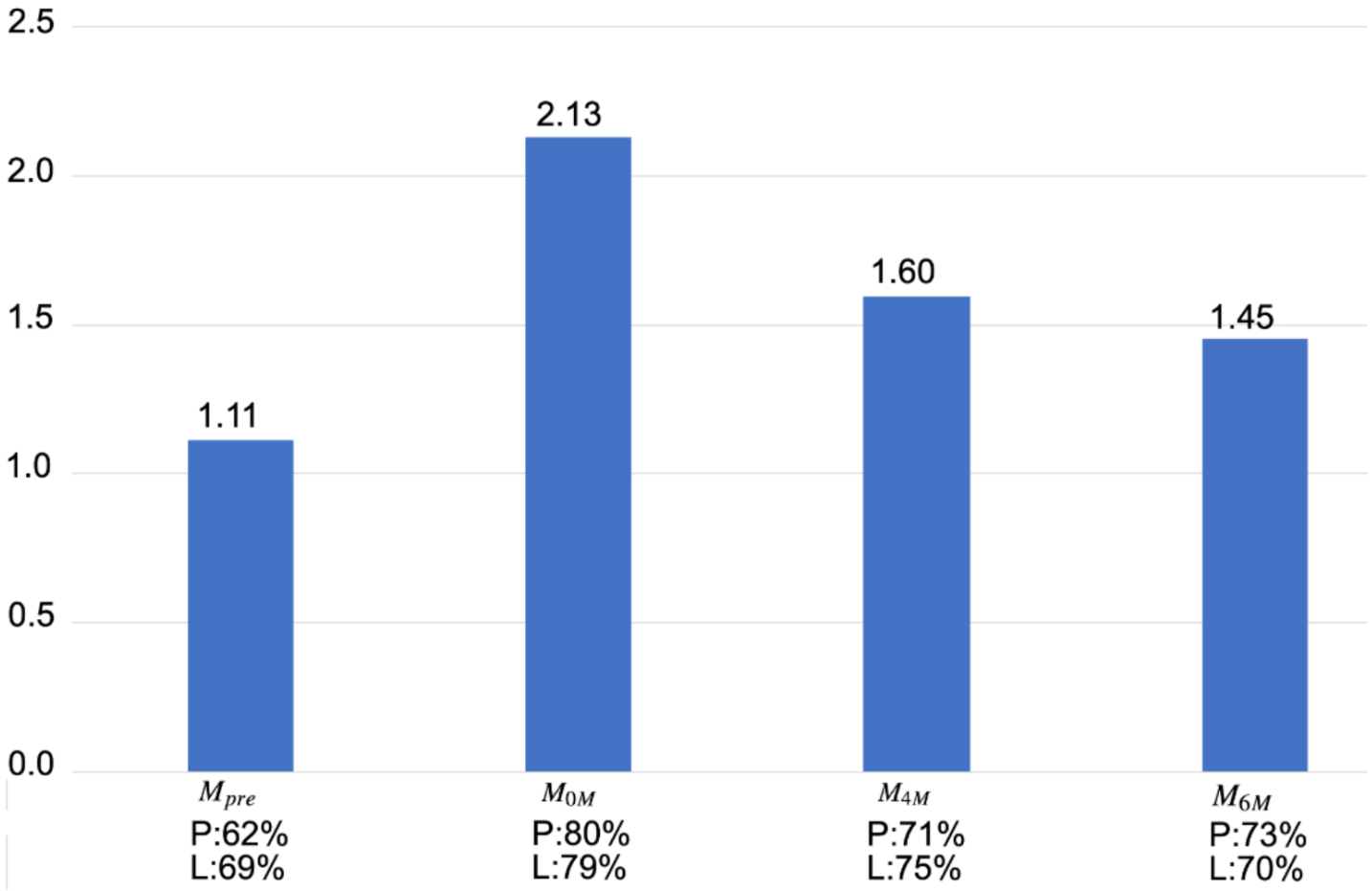


Ein Klick = Infiziert?

Die Unified Kill Chain

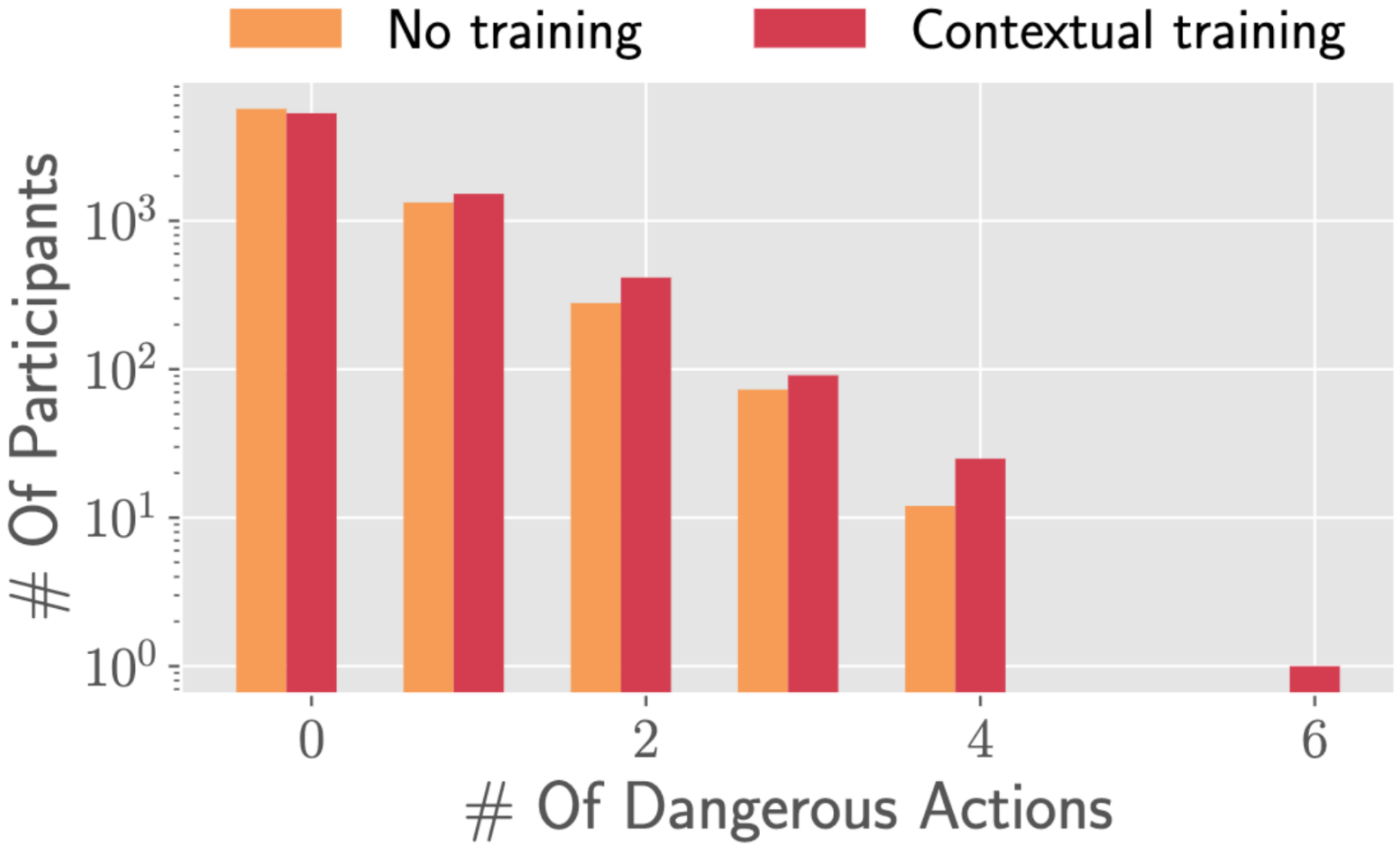


Phishing Awareness funktioniert nicht (lange)



Reinheimer et al, 2020.:
An investigation of phishing awareness and education over time: When and howto best remind users

Bestimmte Phishing Awareness funktioniert nicht



Lain et al. (2022) - Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

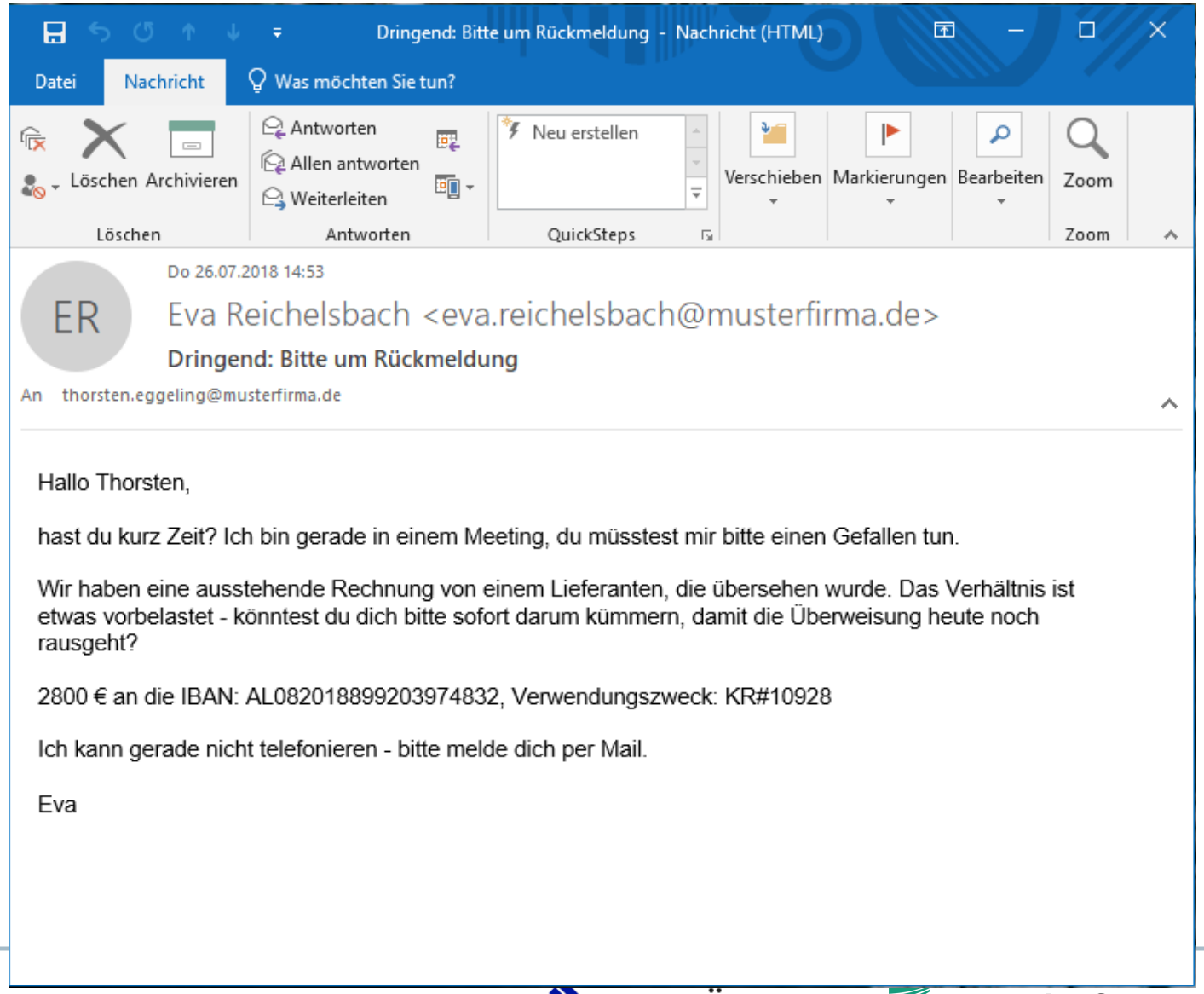
If we give users a link-clicking machine THEY WILL CLICK THE LINKS!

- Unbekannt

Wie funktioniert eigentlich Phishing?

Auf menschlicher Ebene

- “Dringende“ Anfragen

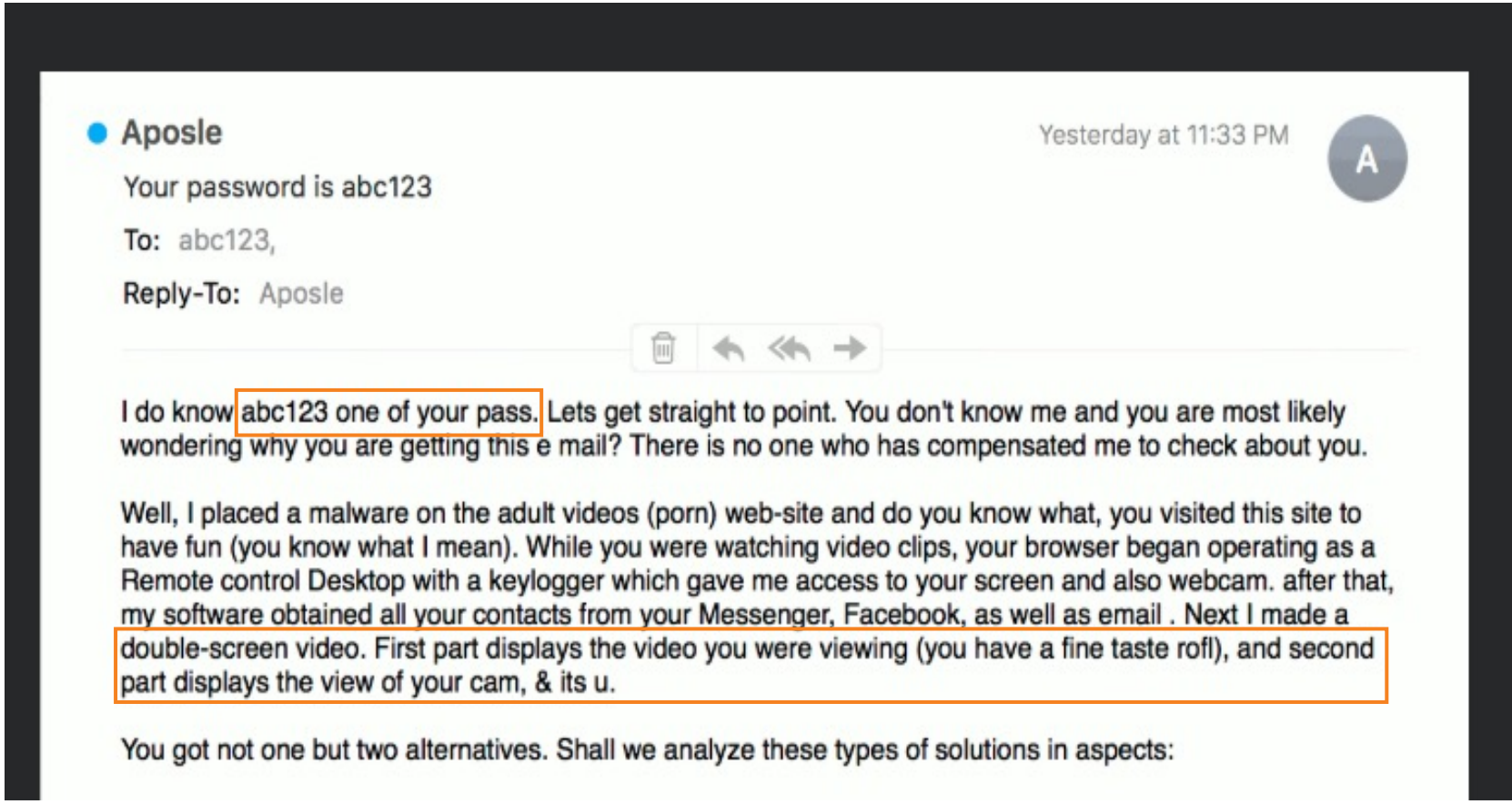


FH MÜNSTER Fraunhofer ACADEMY

Wie funktioniert eigentlich Phishing?

Auf menschlicher Ebene

- “Dringende“ Anfragen
- Spiel mit Ängsten



Aposle

Yesterday at 11:33 PM

A

Your password is abc123

To: abc123,

Reply-To: Aposle

I do know abc123 one of your pass. Lets get straight to point. You don't know me and you are most likely wondering why you are getting this e mail? There is no one who has compensated me to check about you.

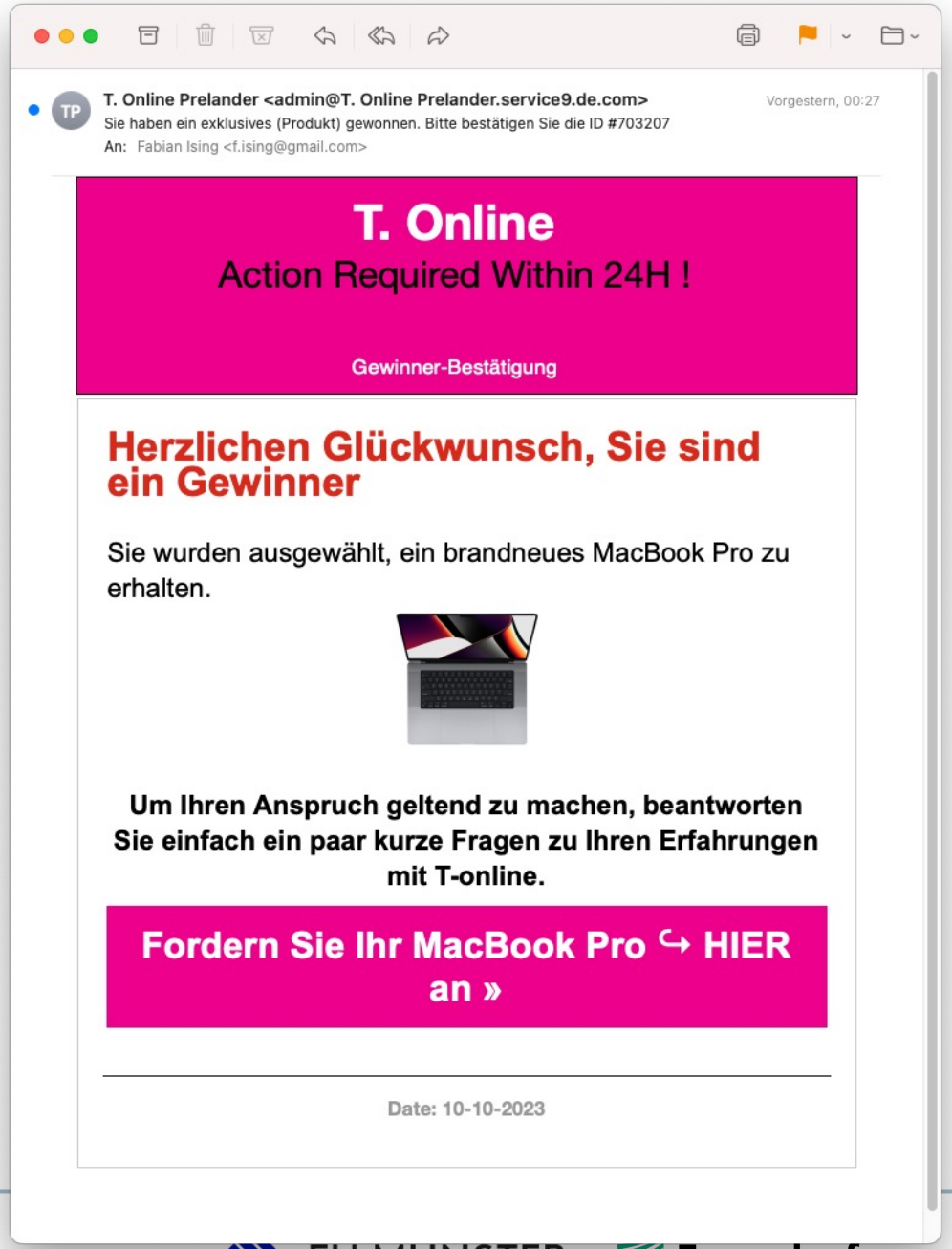
Well, I placed a malware on the adult videos (porn) web-site and do you know what, you visited this site to have fun (you know what I mean). While you were watching video clips, your browser began operating as a Remote control Desktop with a keylogger which gave me access to your screen and also webcam. after that, my software obtained all your contacts from your Messenger, Facebook, as well as email . Next I made a double-screen video. First part displays the video you were viewing (you have a fine taste rofl), and second part displays the view of your cam, & its u.

You got not one but two alternatives. Shall we analyze these types of solutions in aspects:

Wie funktioniert eigentlich Phishing?

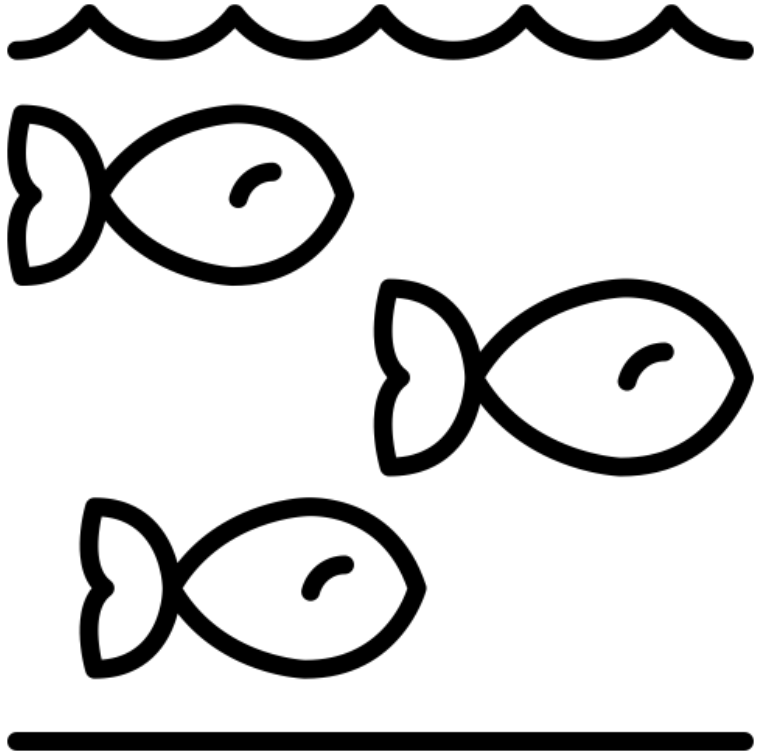
Auf menschlicher Ebene

- “Dringende“ Anfragen
- Spiel mit Ängsten
- Versprechen von persönlichem Nutzen



Wie funktioniert eigentlich Phishing?
Auf menschlicher Ebene

- “Dringende“ Anfragen
- Spiel mit Ängsten
- Versprechen von persönlichem Nutzen



„Plenty of Phish“ – Es muss nicht jedes Mal funktionieren!

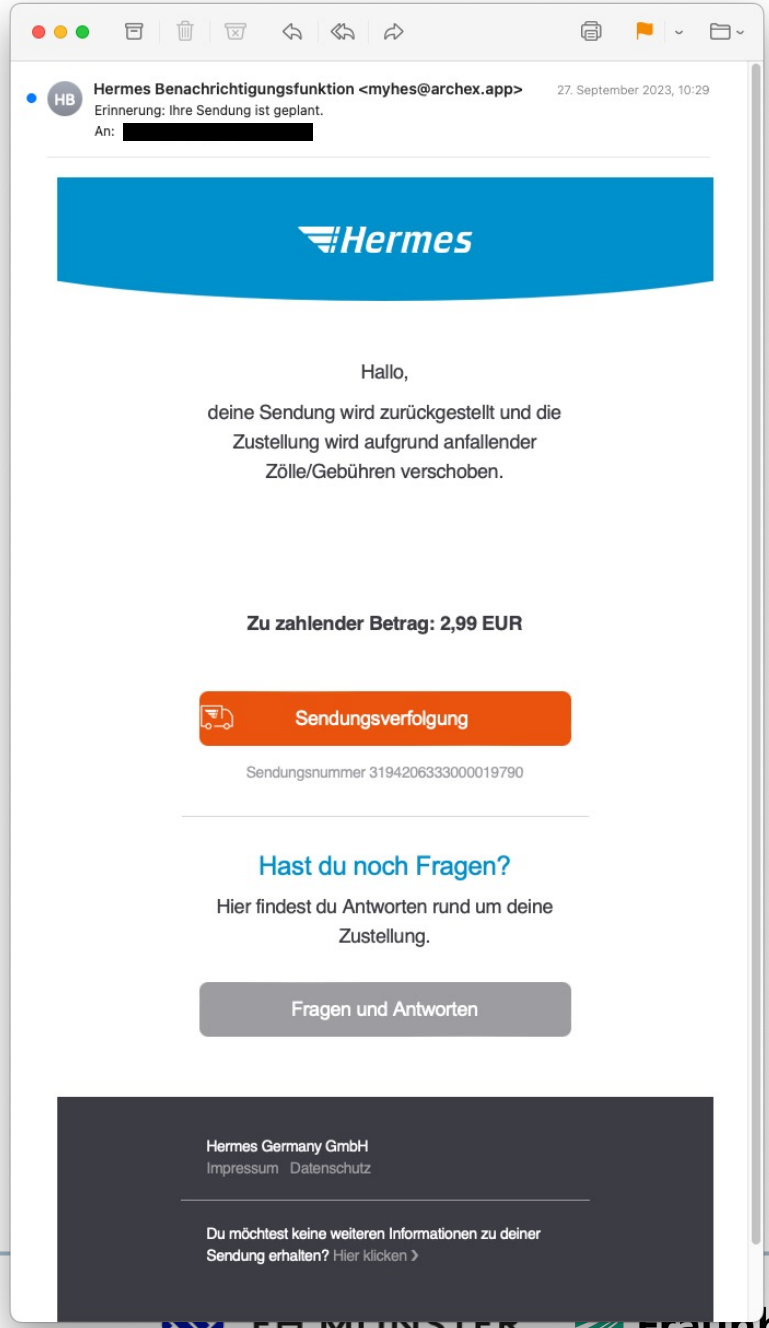
Wie funktioniert eigentlich Phishing?
Auf technischer Ebene

- Täuschung durch Anzeige im E-Mail-Client

FH MÜNSTER Fraunhofer ACADEMY

Wie funktioniert eigentlich Phishing?
Auf technischer Ebene

- Täuschung durch Anzeige im E-Mail-Client



FH MÜNSTER Fraunhofer ACADEMY

Wie funktioniert eigentlich Phishing?
Auf technischer Ebene

- Täuschung durch Anzeige im E-Mail-Client

- Verwendung von ähnlichen E-Mail-Adressen

Statt fabian.ising@sit.fraunhofer.de:

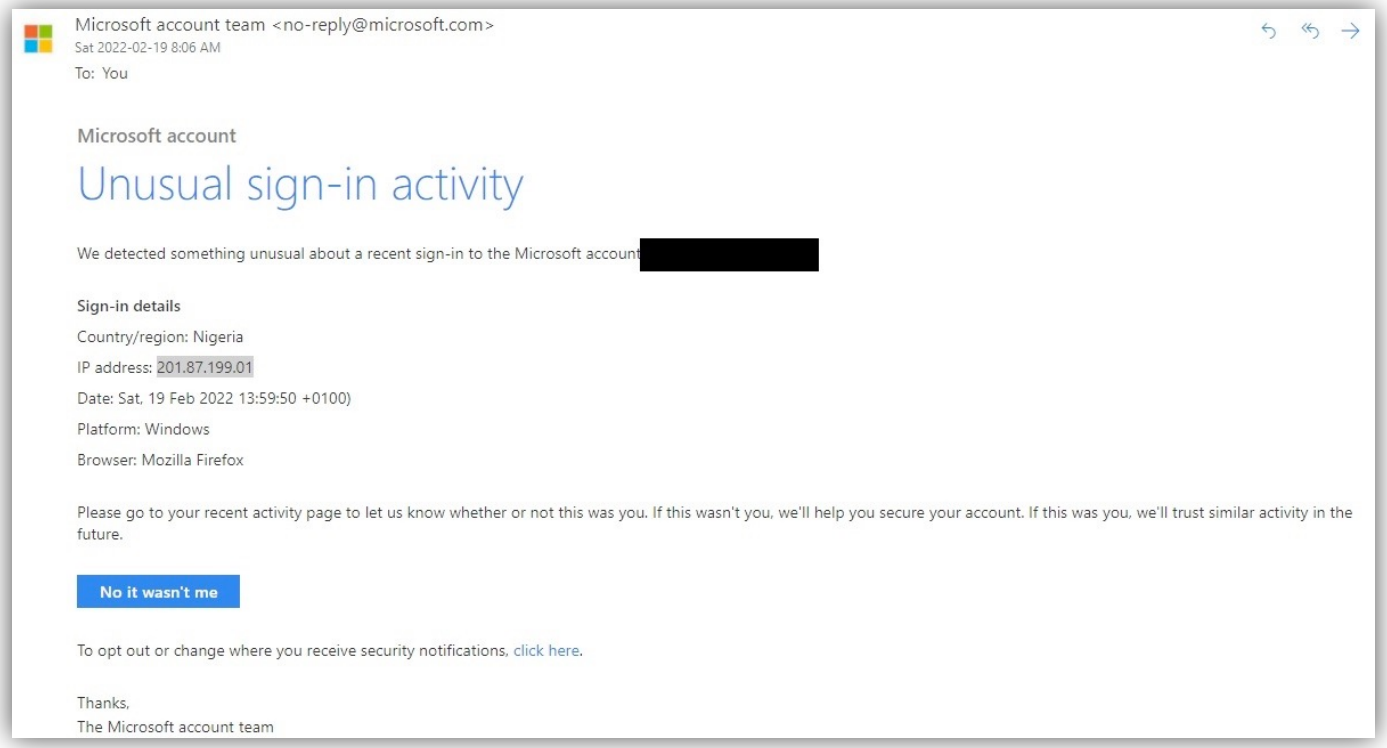
fabian.ising@sit.frauenhofer.de

fabian.ising@sit.fraunlnofer.de

...

Wie funktioniert eigentlich Phishing?
Auf technischer Ebene

- Täuschung durch Anzeige im E-Mail-Client
- Verwendung von ähnlichen E-Mail-Adressen
- Verwendung gefälschter E-Mail-Adressen



Microsoft account team <no-reply@microsoft.com>
Sat 2022-02-19 8:06 AM
To: You

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account [redacted]

Sign-in details

Country/region: Nigeria
IP address: 201.87.199.01
Date: Sat, 19 Feb 2022 13:59:50 +0100)
Platform: Windows
Browser: Mozilla Firefox

Please go to your recent activity page to let us know whether or not this was you. If this wasn't you, we'll help you secure your account. If this was you, we'll trust similar activity in the future.

No it wasn't me

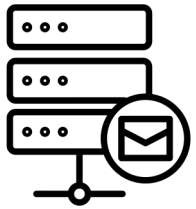
To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Wie funktioniert E-Mail-Transport?

Wie funktioniert E-Mail-Transport?

intern.firmaA.de

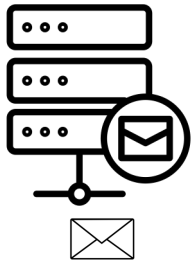


User: alice
Password: ***

From: alice@firmaA.de
Mail To: bob@firmaB.de

Wie funktioniert E-Mail-Transport?

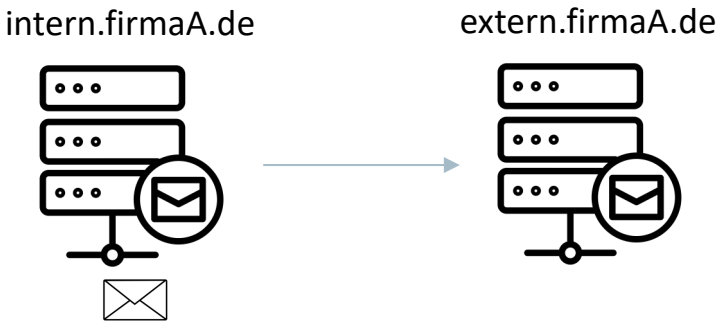
intern.firmaA.de



From: alice@firmaA.de

Mail To: bob@firmaB.de

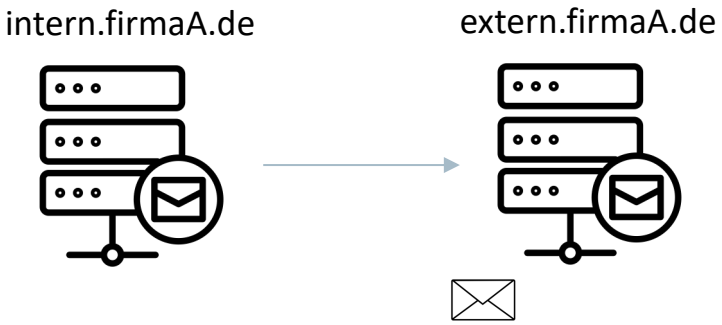
Wie funktioniert E-Mail-Transport?



From: alice@firmaA.de

Mail To: bob@firmaB.de

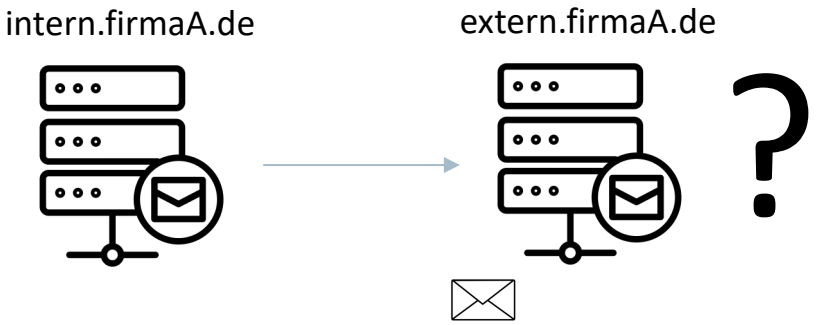
Wie funktioniert E-Mail-Transport?



From: alice@firmaA.de

Mail To: bob@firmaB.de

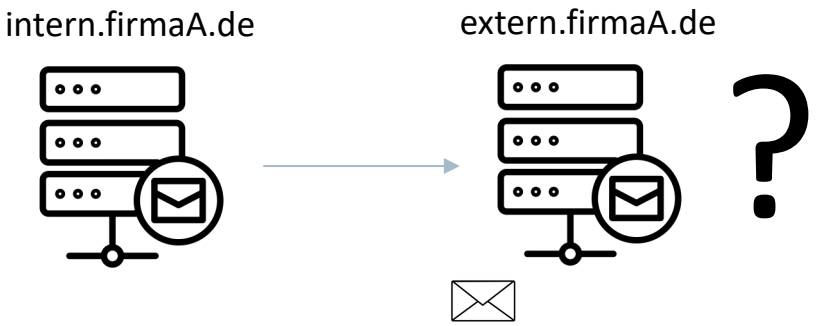
Wie funktioniert E-Mail-Transport?



From: alice@firmaA.de

Mail To: bob@firmaB.de

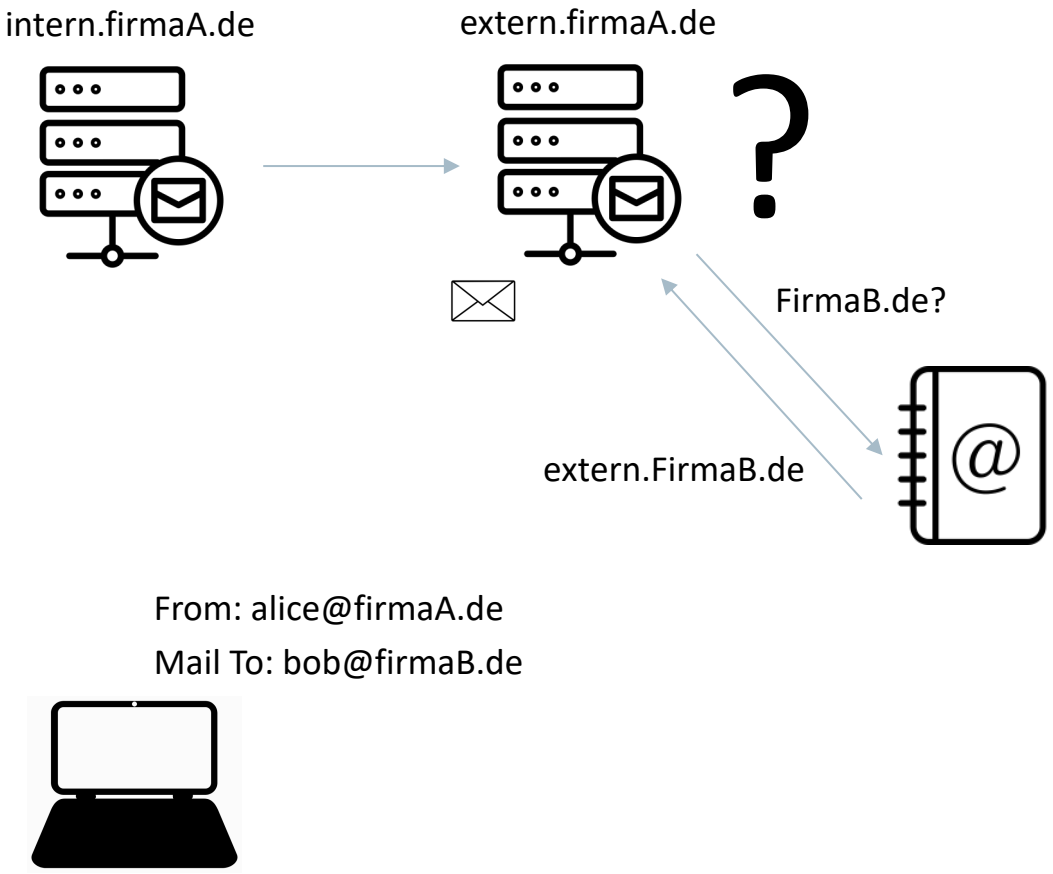
Wie funktioniert E-Mail-Transport?



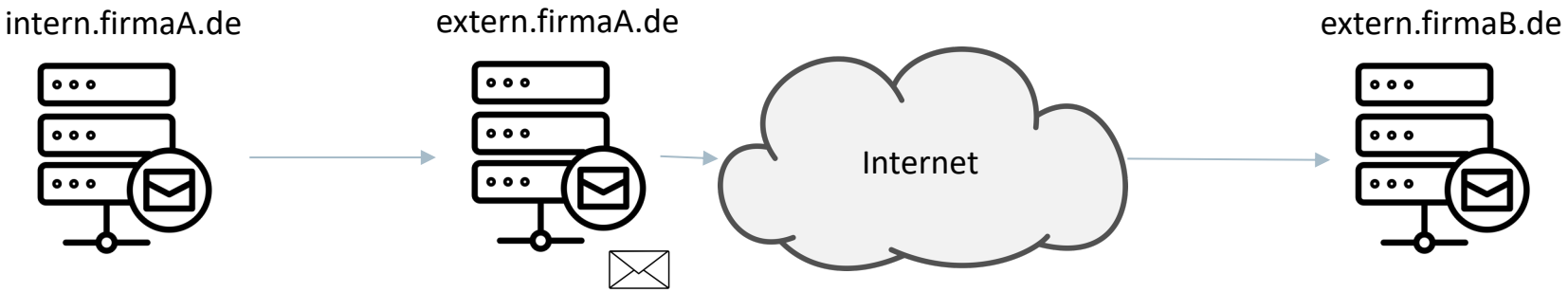
From: alice@firmaA.de

Mail To: bob@firmaB.de

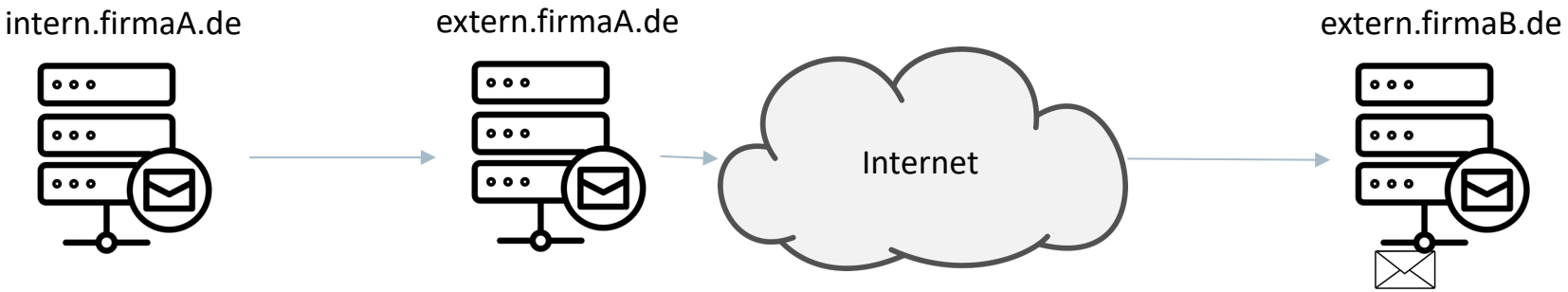
Wie funktioniert E-Mail-Transport?



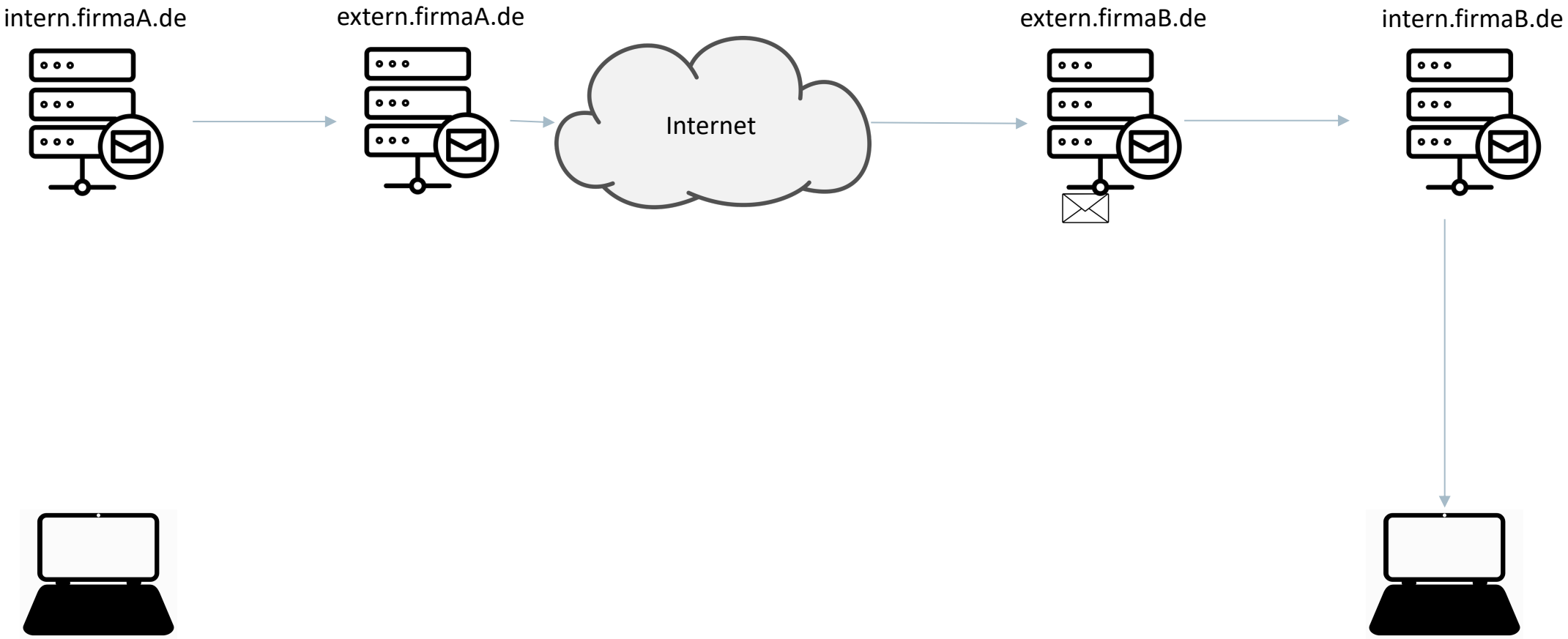
Wie funktioniert E-Mail-Transport?



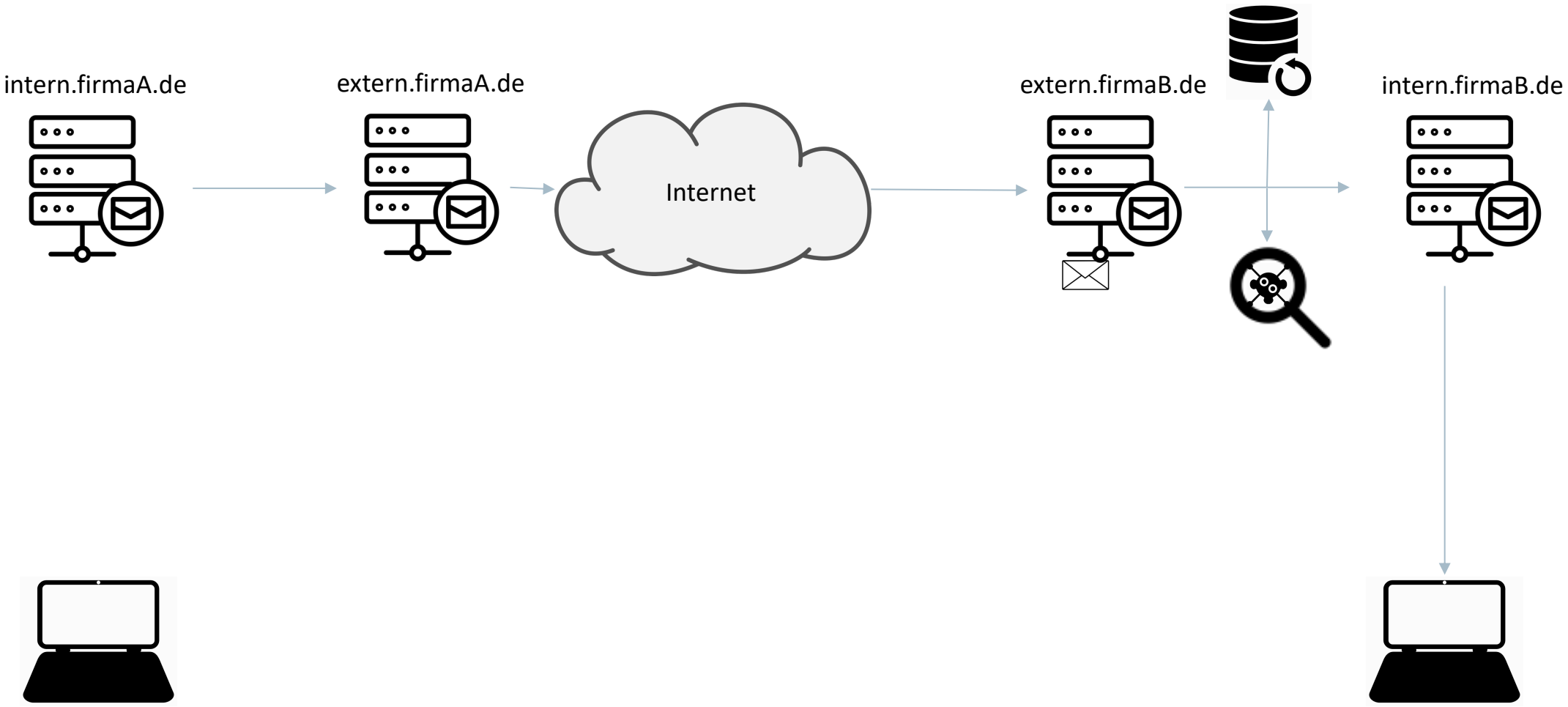
Wie funktioniert E-Mail-Transport?



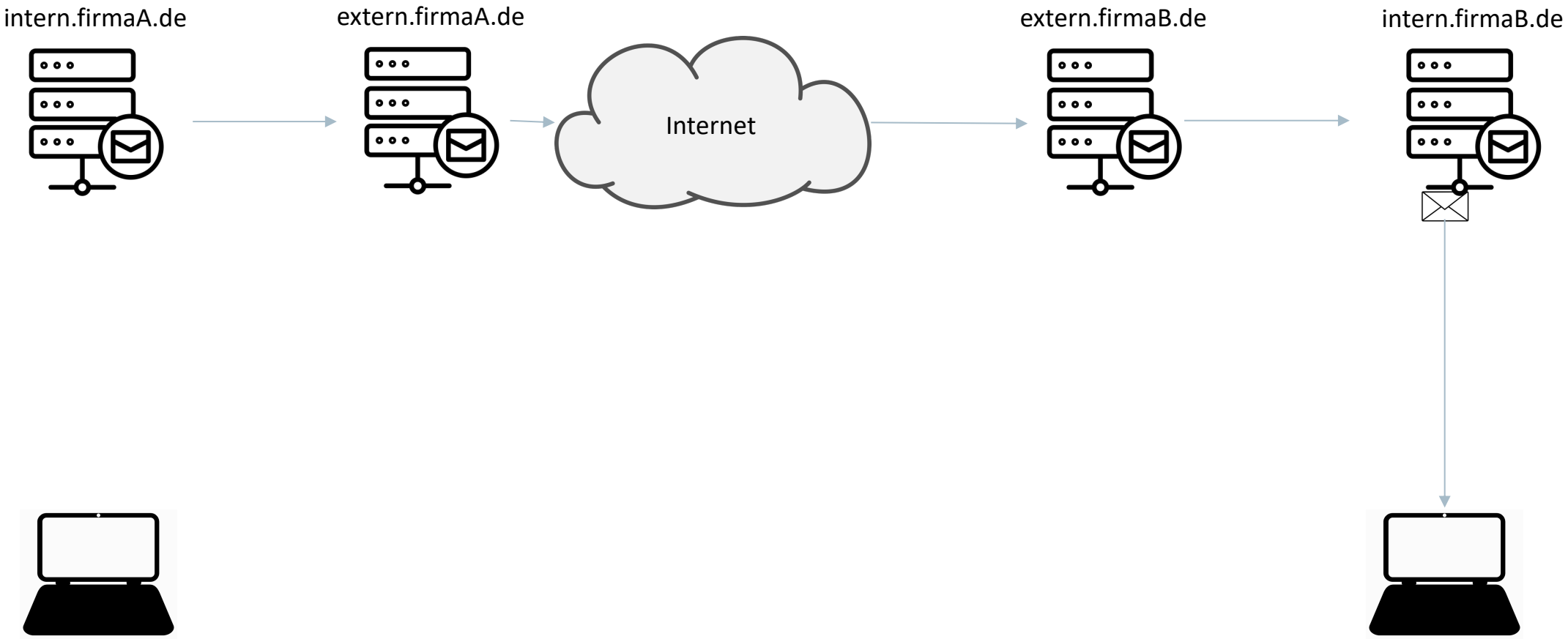
Wie funktioniert E-Mail-Transport?



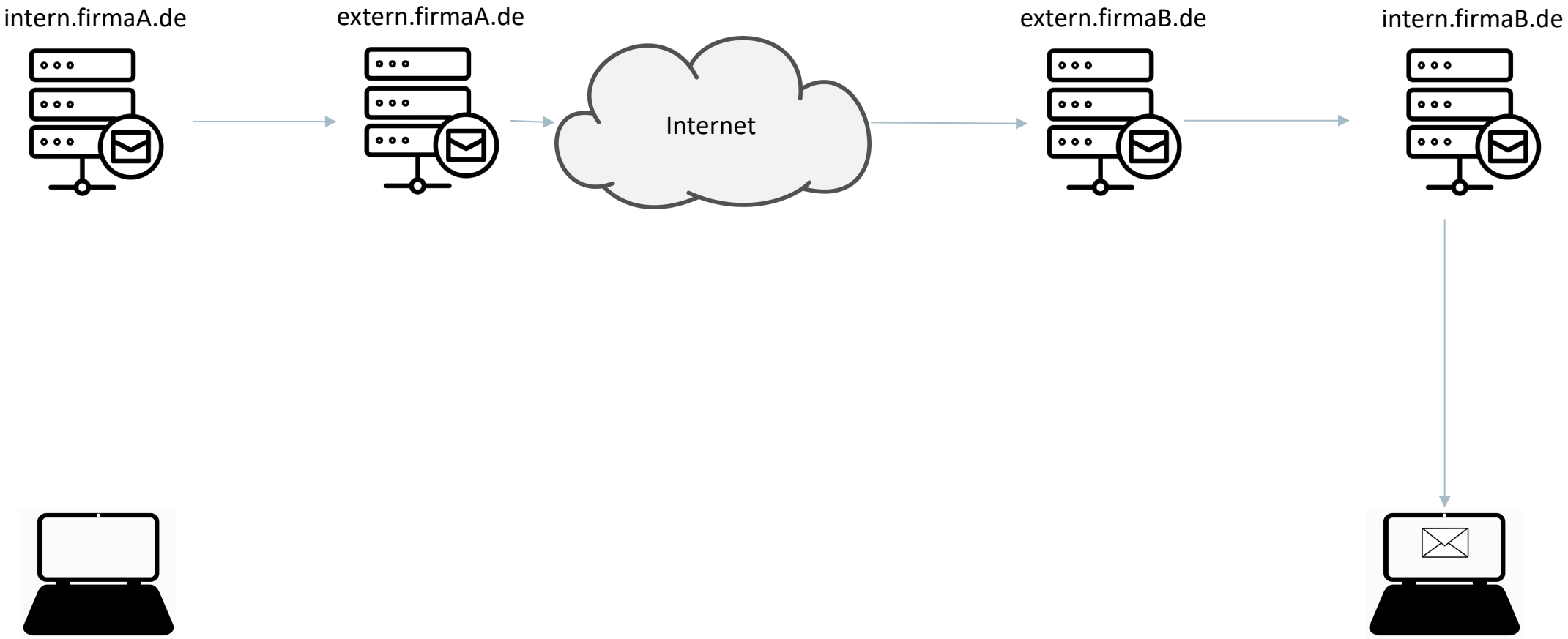
Wie funktioniert E-Mail-Transport?



Wie funktioniert E-Mail-Transport?

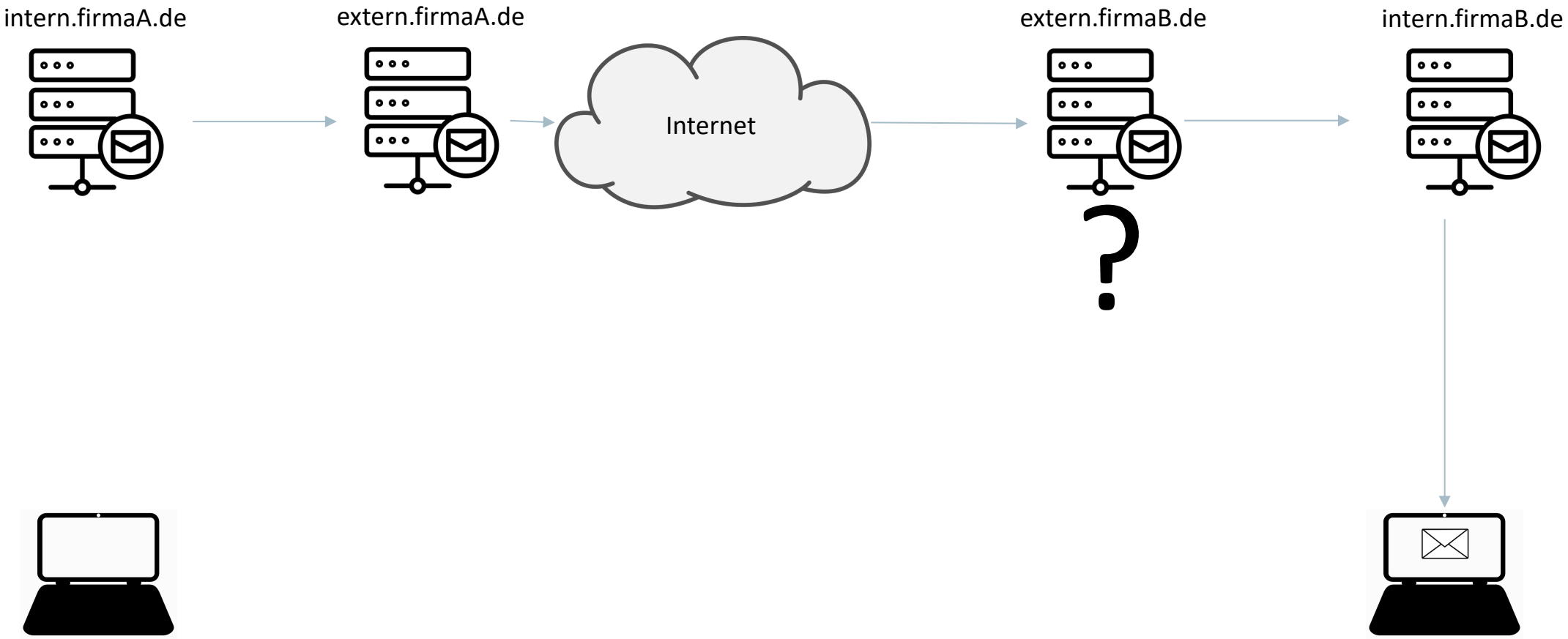


Wie funktioniert E-Mail-Transport?

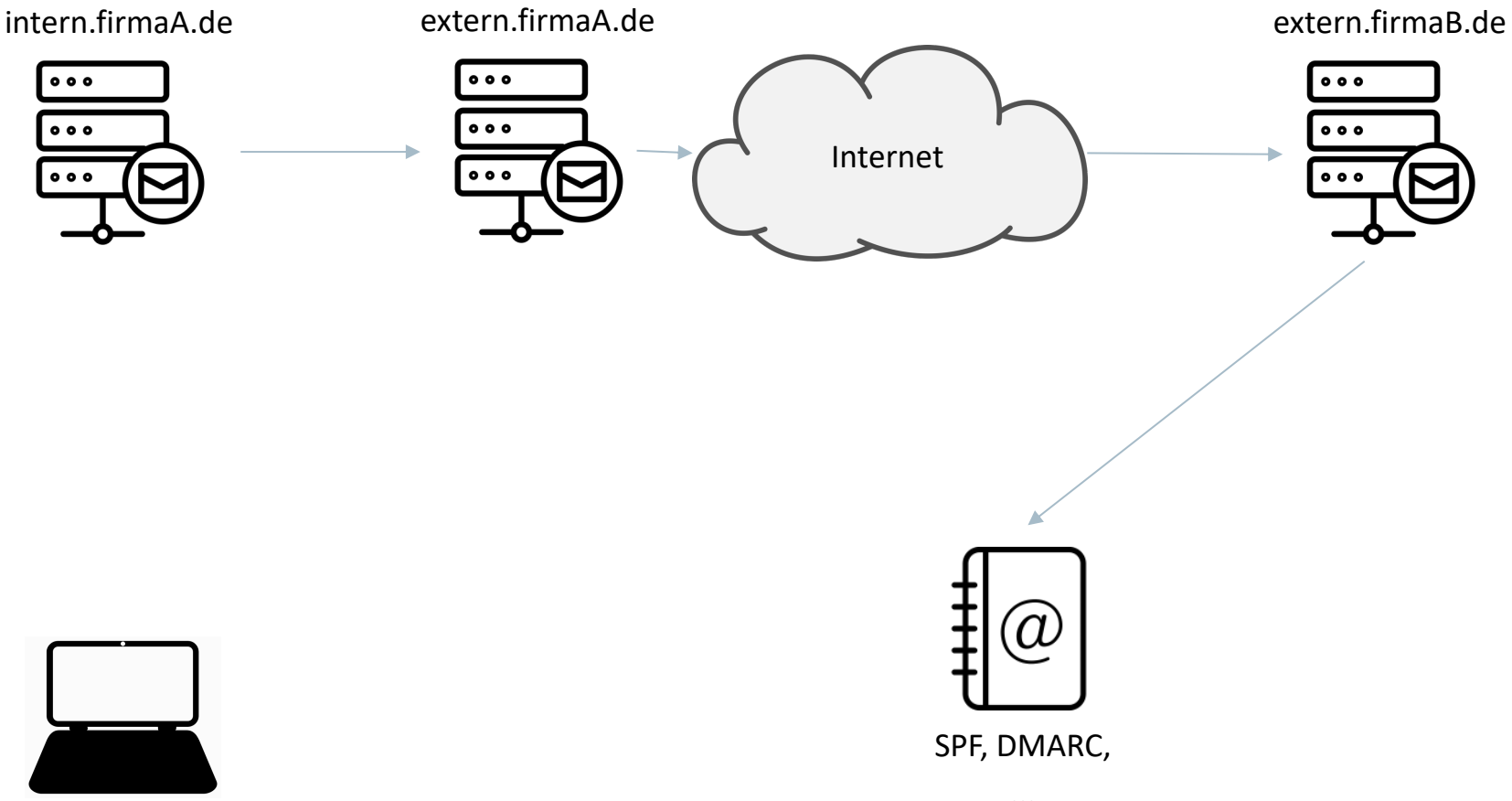


FH MÜNSTER Fraunhofer ACADEMY

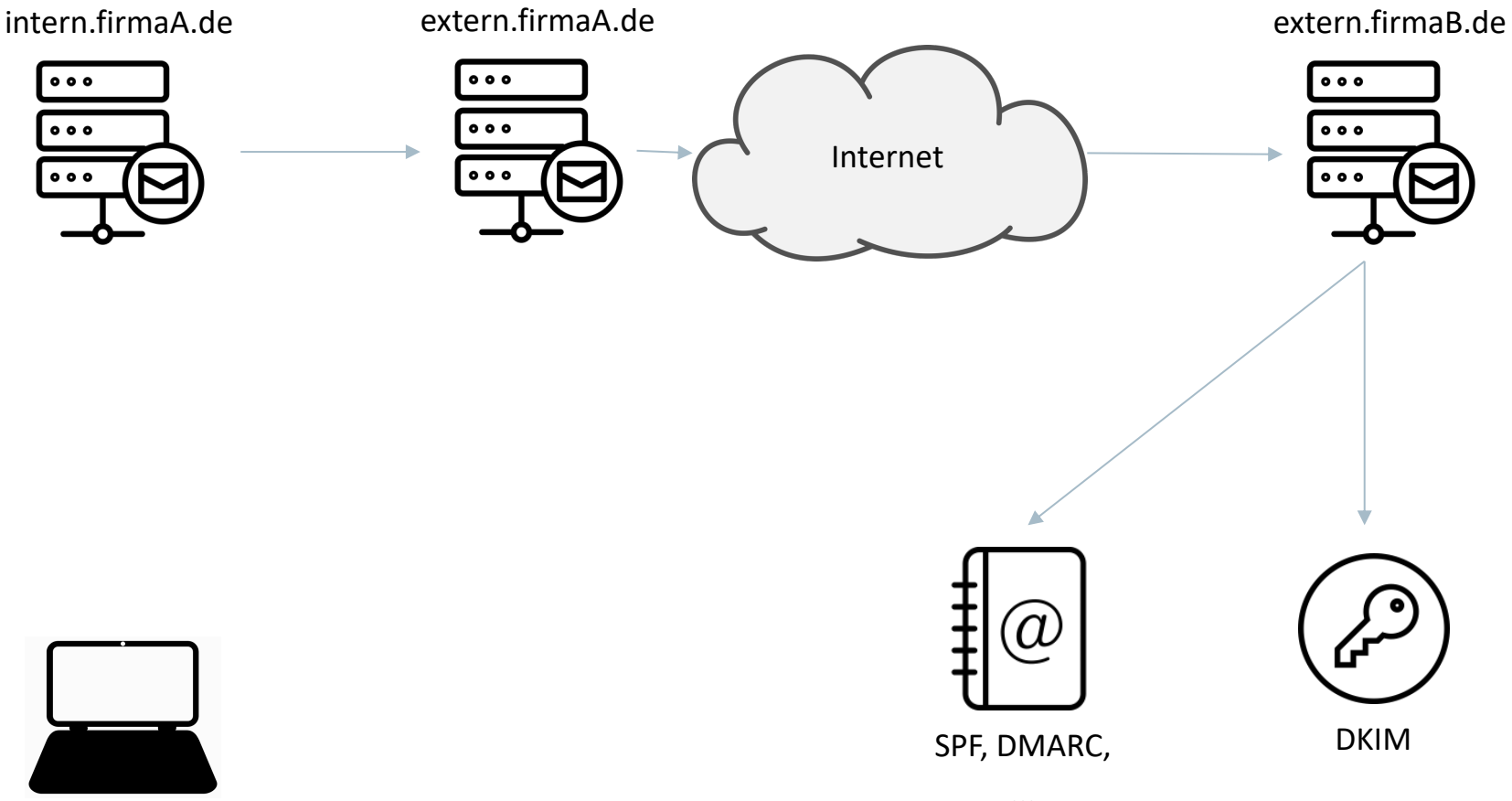
Wie funktioniert E-Mail-Transport?



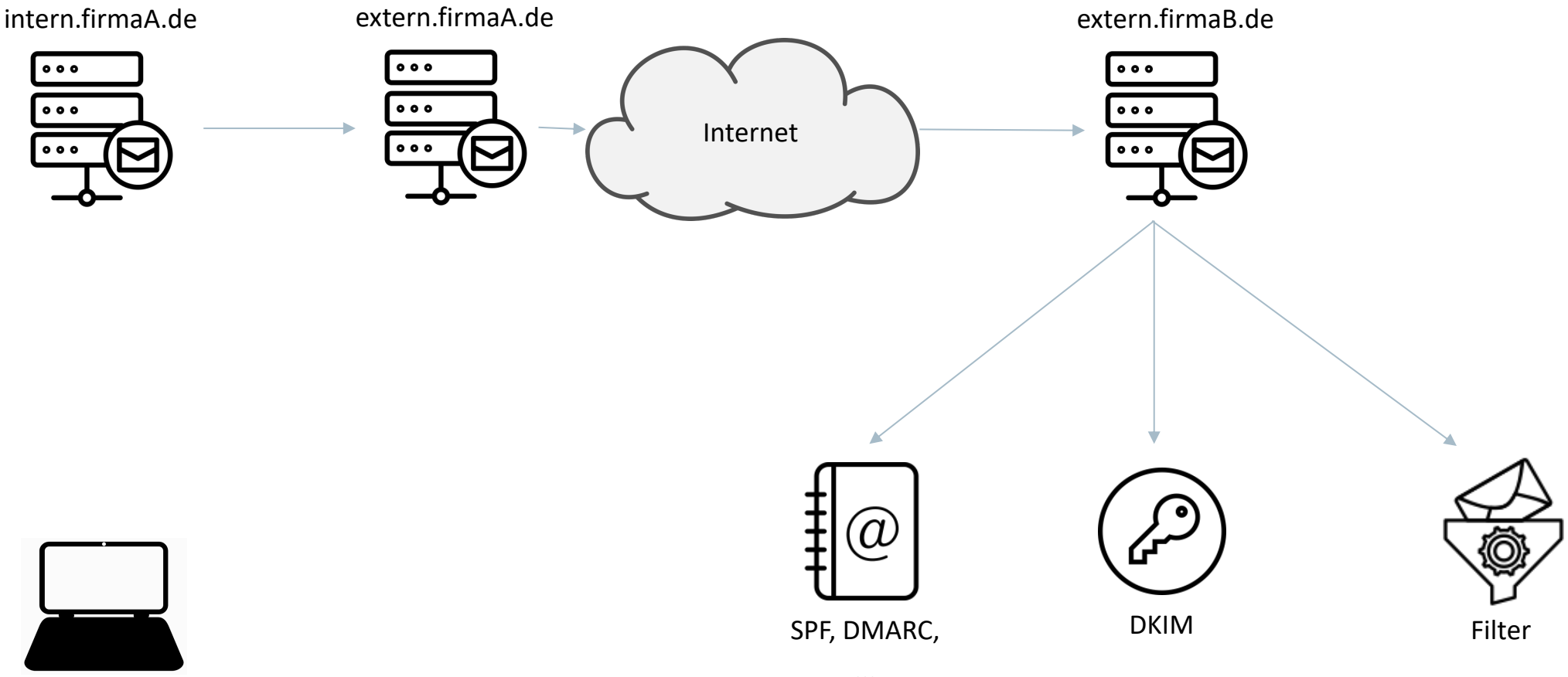
Wie funktioniert E-Mail-Transport?



Wie funktioniert E-Mail-Transport?



Wie funktioniert E-Mail-Transport?

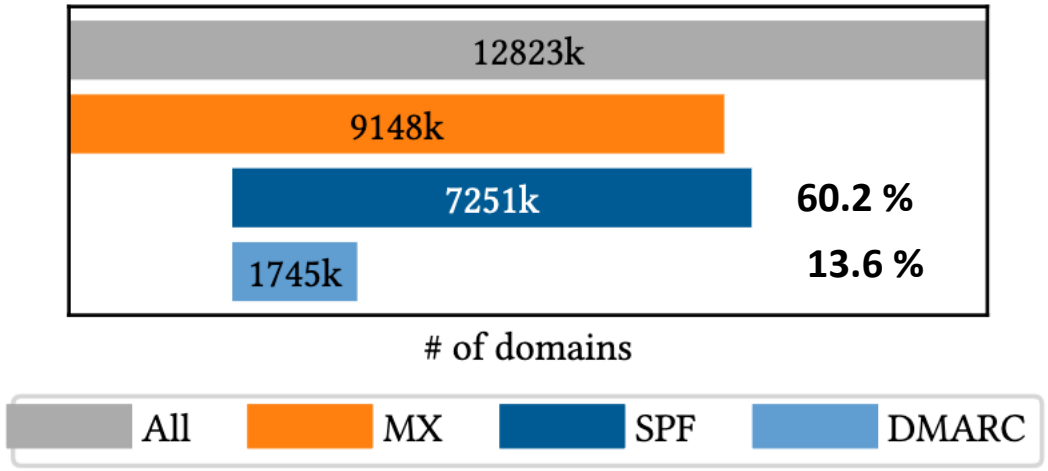


Gegenmaßnahmen

- Sender Verification
  - Wer darf eigentlich von dieser Domain versenden? (SPF)
  - Ist das, was angekommen ist, auch das, was verschickt wurde? (DKIM)
  - Was soll ich machen, wenn etwas davon nicht stimmt? (DMARC)
  - Haben alle auf dem Weg der E-Mail das richtig geprüft? (ARC)
- Spam-Filtering, Greylisting, ...

Aber das macht doch jeder...?

Ausgehende E-Mails



Czybik et al. (2023) - Lazy Gatekeepers: A Large-Scale Study on SPF Configuration in the Wild

Wer darf in meinem Namen senden?
Was passiert wenn sich jemand nicht dran hält?

Table 6: DKIM Adoption Rate among Multiple ccTLDs.

ccTLD	Country	MX Domains	w/ DKIM (%)
.ru	Russia	34,754	12,107 (34.8%)
.de	Germany	25,105	5,744 (22.9%)
.jp	Japan	17,740	2,467 (13.9%)
.uk	United Kingdom	15,496	7,058 (45.6%)
.br	Brazil	13,990	6,737 (48.2%)
.fr	France	11,012	4,141 (37.6%)
.au	Australia	7,452	4,363 (58.6%)
.cn	China	5,439	422 (7.8%)

Wang et al. (2022) - A Large-scale and Longitudinal Measurement Study of DKIM Deployment

Ist das, was angekommen ist das, was gesendet wurde?

E-Mail in der Quarantäne

	Von	Betreff	Datum
Freigeben	[redacted]	[SPF] Copy of your invoice	06 Feb 2024

Alle Nachrichten (1) in der Quarantäne anzeigen

FH MUNSTER
Fraunhofer ACADEMY

Aber das macht doch jeder...?

Eingehende E-Mails

28 von 47

... der großen Provider prüfen **nicht** korrekt!

Blechschmidt et al. (2023) - Extended Hell(o): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild

Technische Phishing-Abwehr hat mehrere Seiten

- Jemand sendet im Namen meiner Firma E-Mails! (Business E-Mail Compromise)

Technische Phishing-Abwehr hat mehrere Seiten

- Jemand sendet im Namen meiner Firma E-Mails! (Business E-Mail Compromise)
  - Schlecht für den eigenen Ruf

Technische Phishing-Abwehr hat mehrere Seiten

- Jemand sendet im Namen meiner Firma E-Mails! (Business E-Mail Compromise)
  - Schlecht für den eigenen Ruf
  - Schlecht für die Zustellung meiner Mails!

Technische Phishing-Abwehr hat mehrere Seiten

- Jemand sendet im Namen meiner Firma E-Mails! (Business E-Mail Compromise)
  - Schlecht für den eigenen Ruf
  - Schlecht für die Zustellung meiner Mails!

> Starting February 1st, 2024, Google will require senders dispatching over 5,000 messages daily to Gmail accounts to set up SPF/DKIM and DMARC email authentication for their domains to strengthen defenses against email spoofing and phishing attempts.

Technische Phishing-Abwehr hat mehrere Seiten

- Jemand sendet im Namen meiner Firma E-Mails! (Business E-Mail Compromise)
  - Schlecht für den eigenen Ruf
  - Schlecht für die Zustellung meiner Mails!
- Meine Mitarbeiter bekommen gefälschte E-Mails!
  - Erfolgswahrscheinlichkeit von Phishing steigt deutlich
  - Zeitaufwand der Mitarbeiter steigt

Was sollten Sie mitgenommen haben?

- Cyberangriffe brauchen mehr als nur einen Klick
- Security Awareness Training hält oft nicht lange an
- Technische Maßnahmen zur Phishing-Abwehr werden selten vollständig genutzt
- E-Mail-Sicherheit hilft auch den Unternehmensruf zu schützen

Schulung - Absicherung der E-Mail-Kommunikation

Wie schütze ich die E-Mail-Kommunikation meines Unternehmens mit **technischen und kyptografischen Methoden**?

Lerninhalte:

- Technischer Phishingschutz (SPF, DKIM, DMARC, ...)
- Schutz vor Business Email Compromise
- Verschlüsselung (technisch und organisatorisch)
  - TLS, MTA-STS, DANE
  - S/MIME und OpenPGP
- Praktische Übungen

Nächster Termin: 28. und 29.02. in Münster, NRW
(Anmeldeschluss: 14.02.2024)

https://www.cybersicherheit.fraunhofer.de/sichere-email-kommunikation

Kontakt

Dr.-Ing. Fabian Ising
Fraunhofer SIT – Abteilung ACM
Stegerwaldstr. 39
48565 Steinfurt

fabian.ising@sit.fraunhofer.de

Fraunhofer ACADEMY

Lernlabor **Cybersicherheit**