Down the Parcel Hole

Wie wir die Paketverfolgung kaputt machten – immer wieder.

Florian Bausch, Dennis Kniel

ERNW RESEARCH
pursuing knowledge.

Wer wir sind

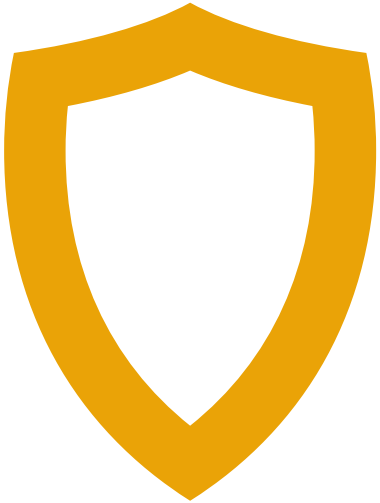
Dennis Kniel

- Ehemaliger Incident Responder und Pentester
- Student

Florian Bausch

- Incident Responder und Pentester

ERNW RESEARCH
pursuing knowledge.



ERNW Research GmbH

- Anbieter für Dienstleistungen rund um IT-Security
- Pentests
- Incident Response und Analyse
- Medical Device Security

- IT-Security-Konferenz Troopers in Heidelberg
  - https://troopers.de

ERNW RESEARCH
pursuing knowledge.

Was bisher geschah

- Juni 2023:
  - Public Disclosure zu DHL-Findings (fixed)
  - Präsentation auf der Troopers 2023 (mit DHL)
- September 2023:
  - Public Disclosure zu DPD-Findings (fixed)
  - Präsentation auf der Heise devSec
- März 2024:
  - Präsentation auf dem Winterkongress (Digitale Gesellschaft Schweiz)
- April 2024:
  - Public Disclosure zu UPS-Findings (unfixed)
  - Public Disclosure zu GLS-Findings (fixed)

ERNW
RESEARCH
pursuing knowledge.

Wie alles begann....

ERNW RESEARCH
pursuing knowledge.

Exkurs: Tracking-Nummern

- Viele Formate
  - FedEx Ground and Express: 12 Ziffern
  - UPS domestic US: 18 Character
  - DHL Express: ISO 15459-1
- Grundlage manchmal UPU S10

S10 format			
1	**2**	**3**	**4**
AA	00000000	9	BB

1. Service indicator code (see below)
2. Serial number
3. Check-digit (see below)
4. ISO 3166-1 alpha-2 country code

https://en.wikipedia.org/wiki/S10_(UPU_standard)

ERNW RESEARCH
pursuing knowledge.

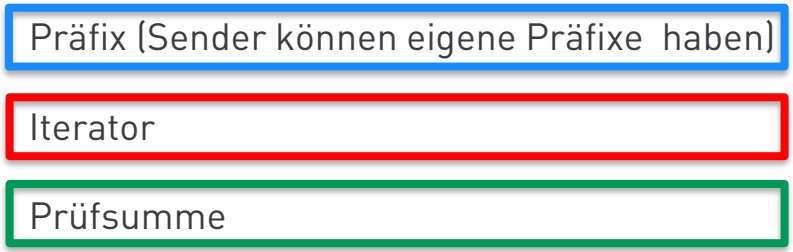
Exkurs: Tracking-Nummern

- 4XXXXXXX0344
- 4XXXXXXX0350
- 4XXXXXXX0366
- 4XXXXXXX0372
- 4XXXXXXX0388
- 4XXXXXXX0394
- 4XXXXXXX0401
- 4XXXXXXX0417
- 4XXXXXXX0423

ERNW RESEARCH
pursuing knowledge.

Exkurs: Tracking-Nummern

- 4XXXXXXX 034 4
- 4XXXXXXX 035 0
- 4XXXXXXX 036 6
- 4XXXXXXX 037 2
- 4XXXXXXX 038 8
- 4XXXXXXX 039 4
- 4XXXXXXX 040 1
- 4XXXXXXX 041 7
- 4XXXXXXX 042 3



ERNW RESEARCH
pursuing knowledge.

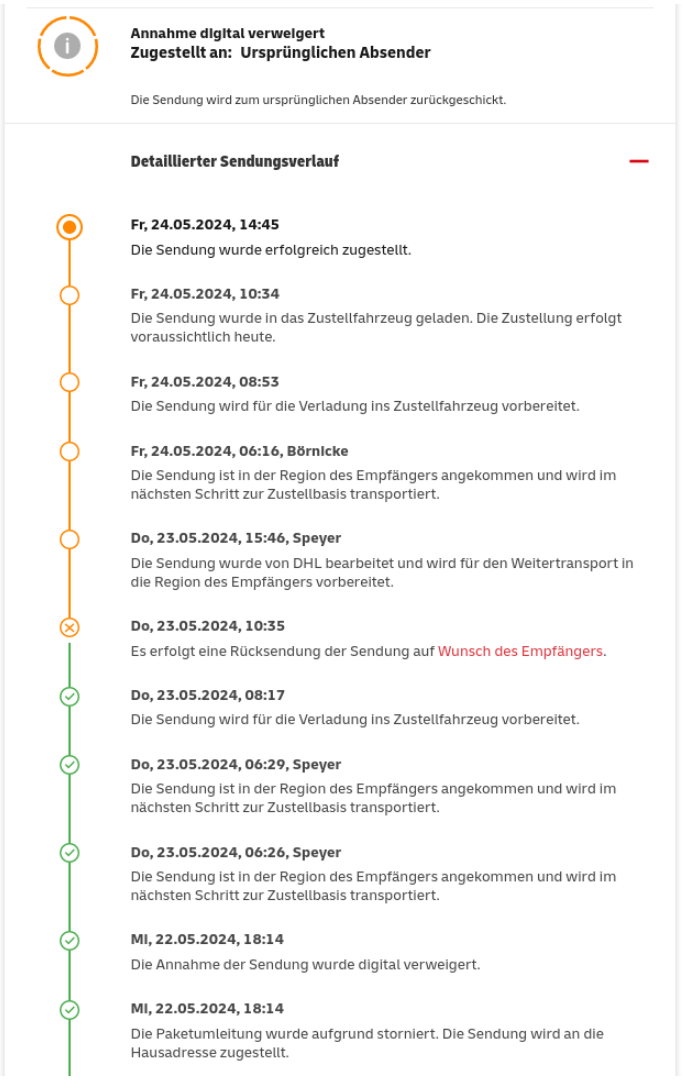
Exkurs: Tracking-Nummern

- Paketverfolgung
- Verschiedene Formate etc.
- Status
  - Unterwegs
  - Zugestellt
  - Zustellung fehlgeschlagen
  - Und mehr…
- Zielort / Zieladresse / Name des Empfängers / der Empfängerin

ERNW RESEARCH
pursuing knowledge.

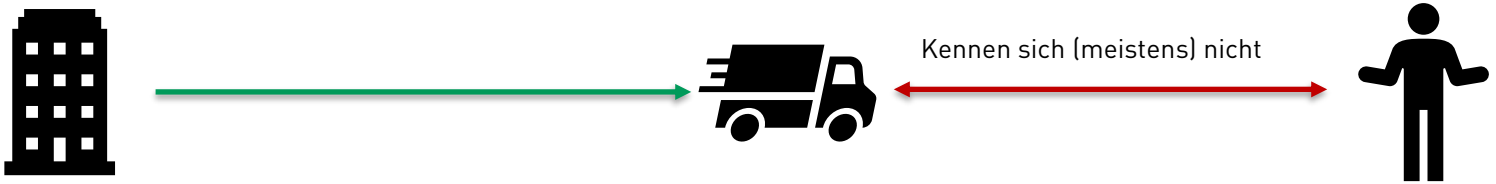
Exkurs: Tracking-Nummern

- Convenience Features
  - Live-Tracking während der Zustellung
  - Wunschnachbar*in
  - Wunsch-Ablageort
  - Umleitung in Packstation / Paketshop
  - Annahme verweigern
  - ...



ERNW RESEARCH
pursuing knowledge.

Das Problem mit dem Shared Secret

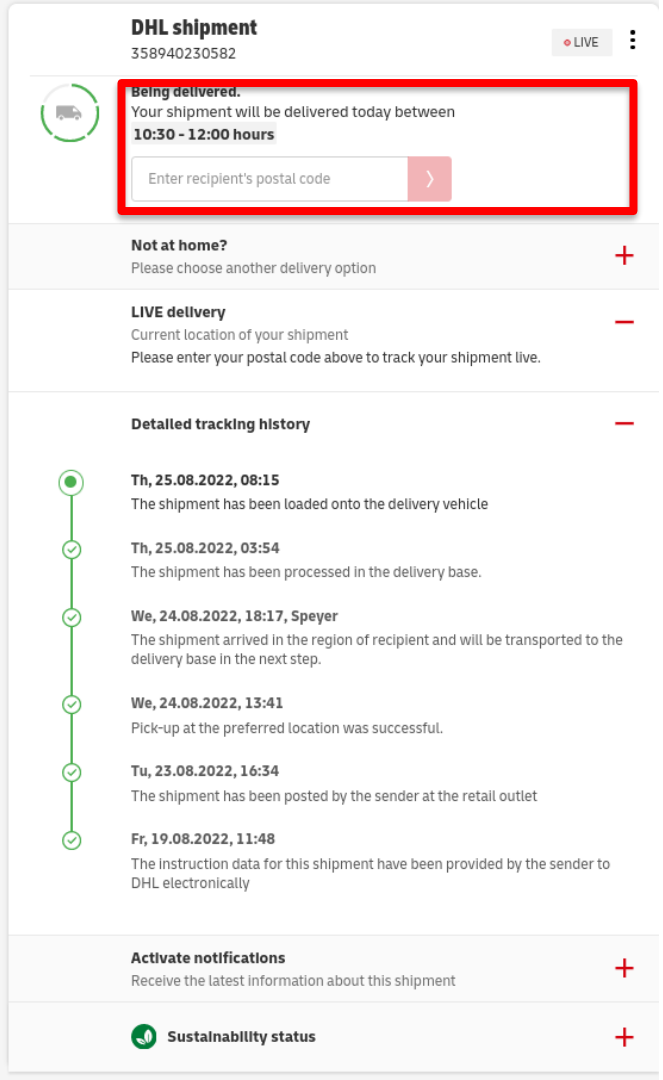


ERNW RESEARCH
pursuing knowledge.

Wir brauchen ein Shared Secret

- Name?
- Straßenname, Wohnort?
- Abwicklung über Versender*in?
- nPA (mit Online-ID-Funktion)?
- Brief mit Passwort?
- Hotline?
- E-Mail?
- Postleitzahl?

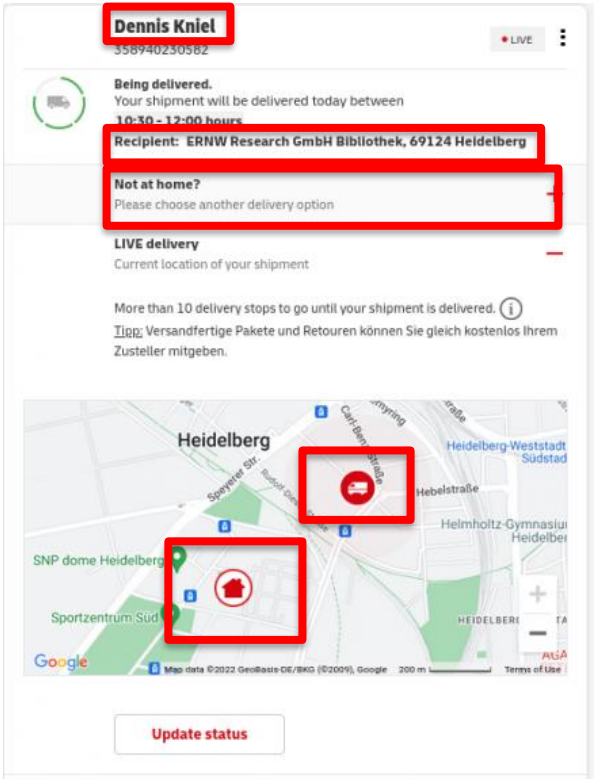
ERNW RESEARCH
pursuing knowledge.

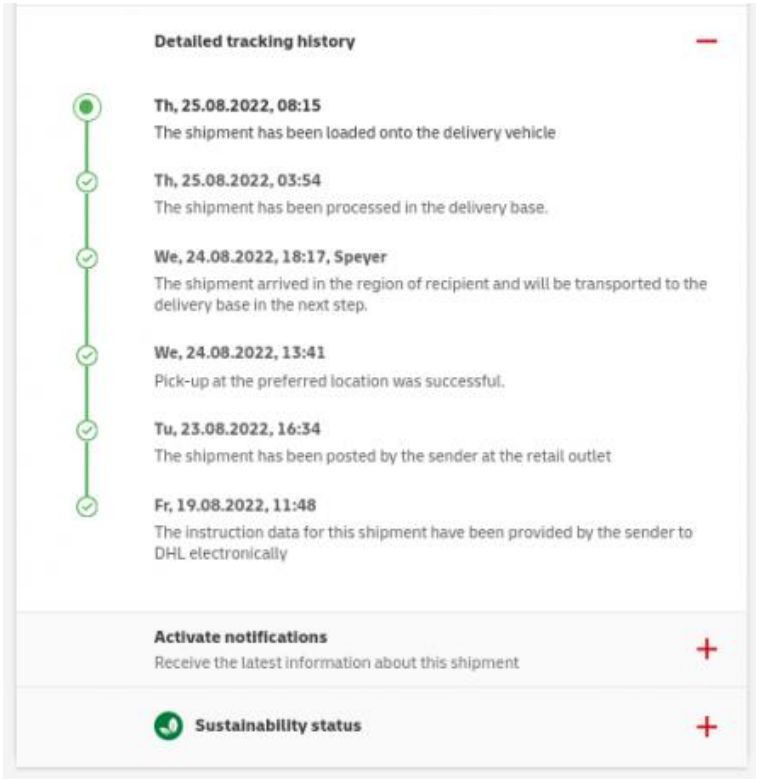


ERNW RESEARCH
pursuing knowledge.

Die PLZ schaltet alles frei

ERNW RESEARCH
pursuing knowledge.





ERNW
RESEARCH
pursuing knowledge.

ERNW RESEARCH
pursuing knowledge.

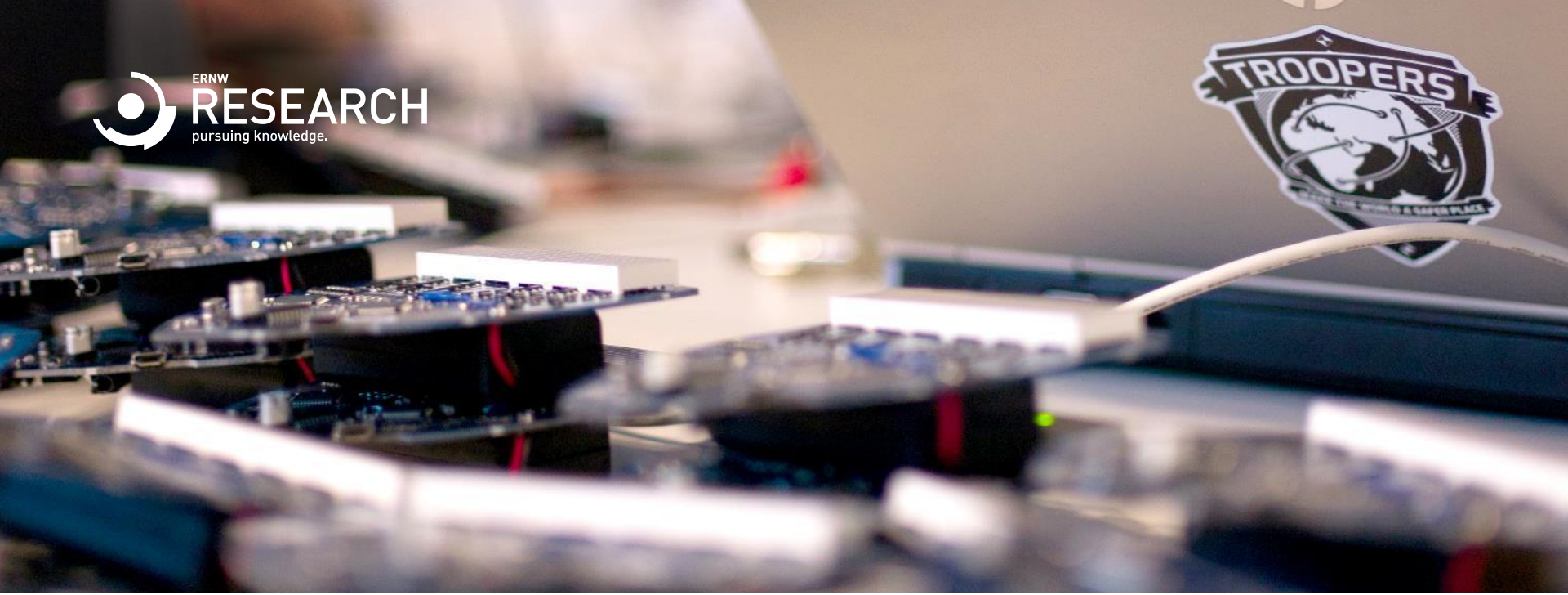
Vorgefundene Maßnahmen

- DHL
  - Akamai vorgeschaltet
  - Bot-Erkennung aktiv
  - Kein stupides Brute-Force möglich
  - Zu schnelles Testen sperrt IP für ein paar Minuten
- DPD
  - Captchas

ERNW RESEARCH
pursuing knowledge.

Vorgefundene Maßnahmen

- GLS
  - Keine wirksamen Maßnahmen gefunden
  - Schnelles Durchprobieren möglich
- UPS
  - Keine wirksamen Maßnahmen gefunden
  - Manche Daten werden ohne Schutz angezeigt



DHL

ERNW RESEARCH
pursuing knowledge.

DHL

- Alle PLZs testen aufwändig
- Aber…

ERNW RESEARCH
pursuing knowledge.

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

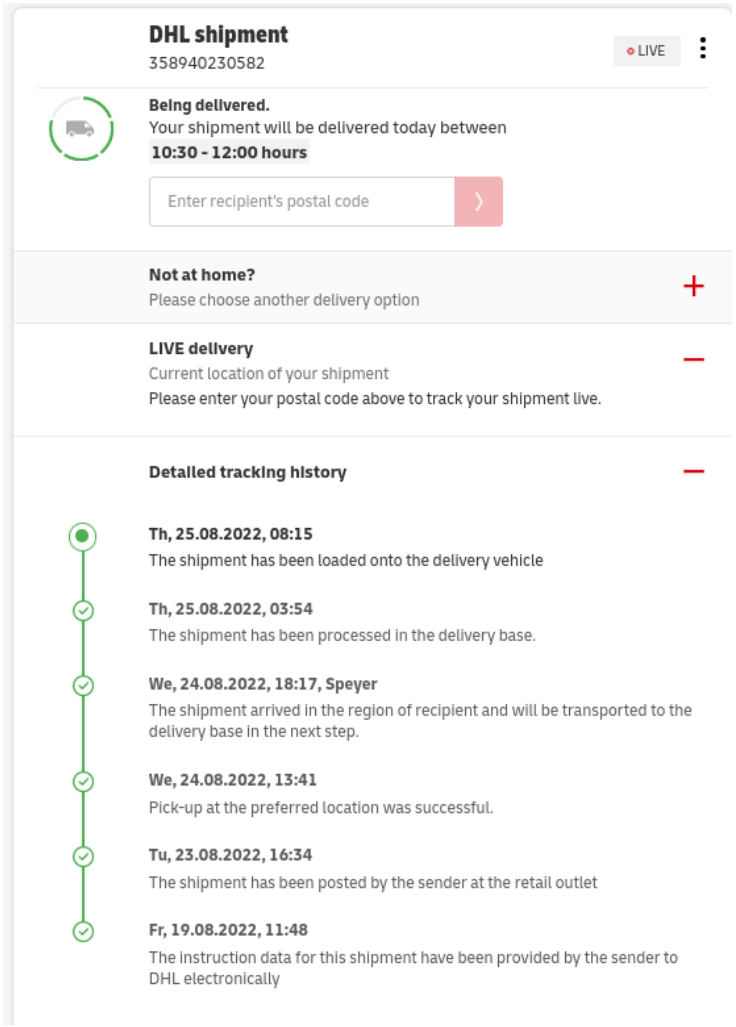
~8.000

PLZs in Benutzung für Orte/Stadtteile

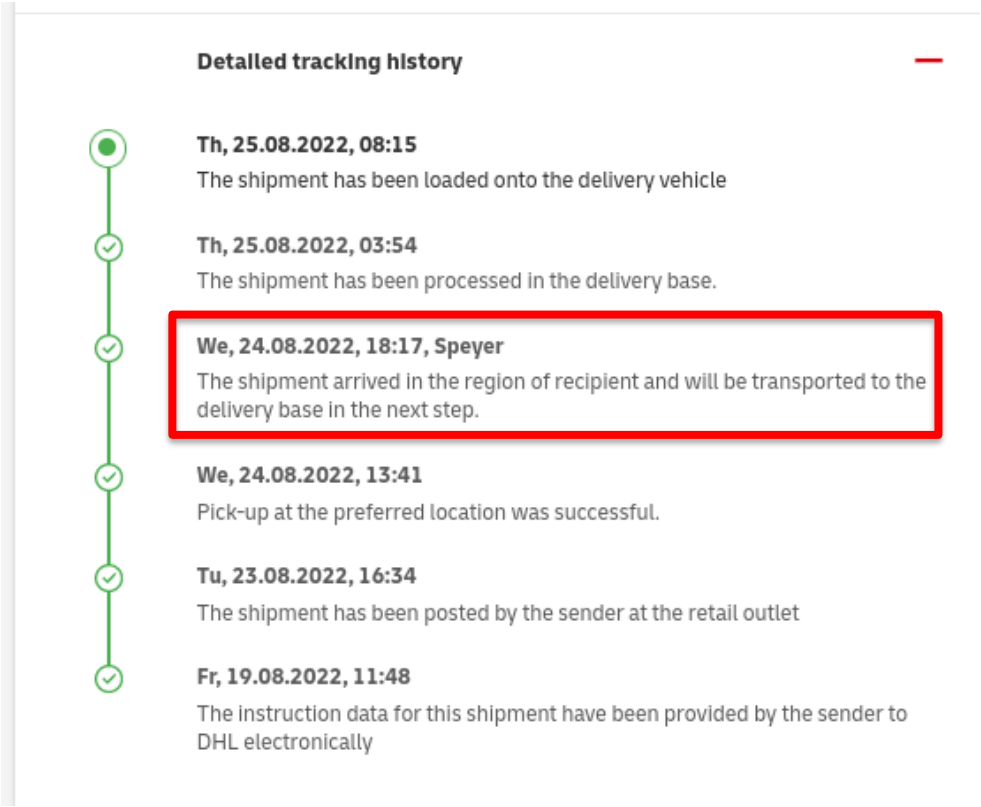
ERNW RESEARCH
pursuing knowledge.

Geht da noch mehr (bzw. weniger)?

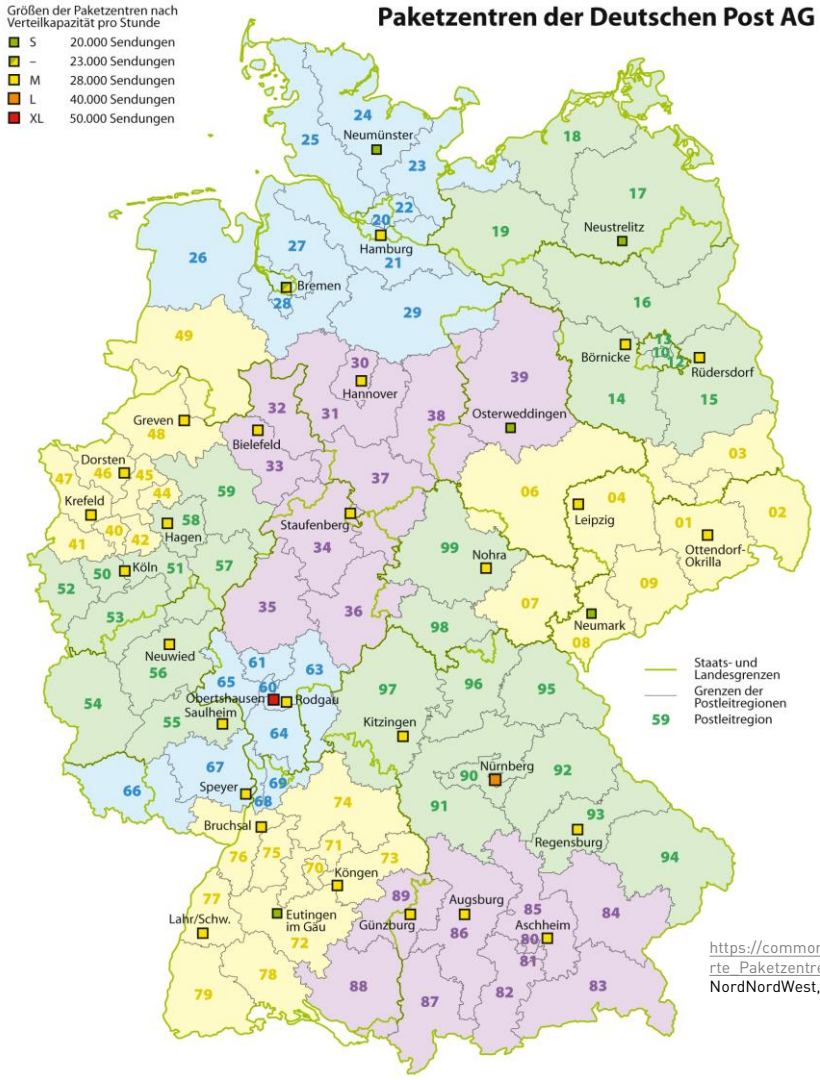
ERNW RESEARCH
pursuing knowledge.



ERNW
RESEARCH
pursuing knowledge.



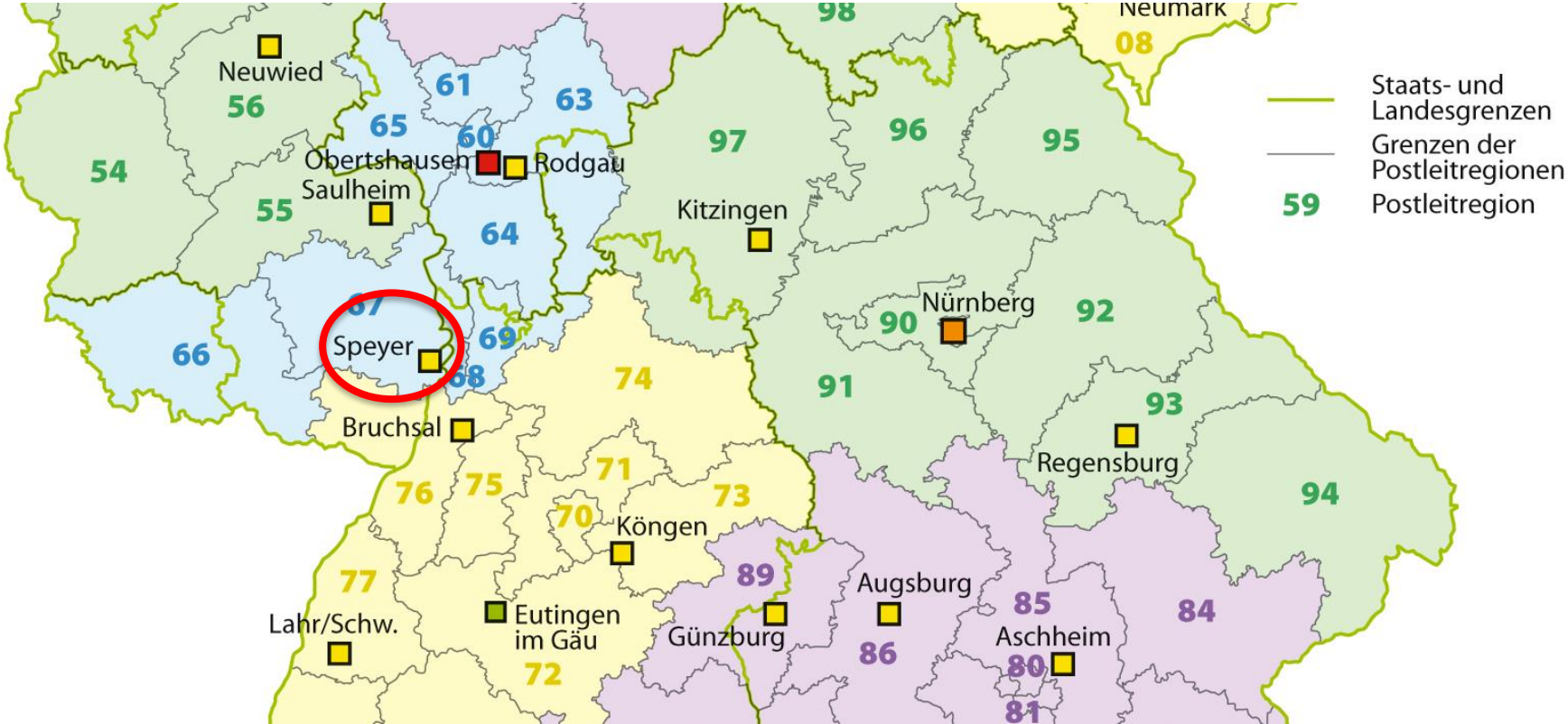
ERNW
RESEARCH
pursuing knowledge.



https://commons.wikimedia.org/wiki/File:Karte_Paketzentren_Deutsche_Post_AG.png, NordNordWest, CC-BY-SA 3.0

ERNW
RESEARCH
pursuing knowledge.

https://commons.wikimedia.org/wiki/File:Karte_Paketzentren_Deutsche_Post_AG.png, NordNordWest, CC-BY-SA 3.0



ERNW
RESEARCH
pursuing knowledge.

https://www.paketda.de

ERNW RESEARCH
pursuing knowledge.

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

~8.000

PLZs in Benutzung für Orte/Stadtteile

227

PLZs pro Zustellbereich im Durchschnitt
(Standardabweichung: 99)

128

PLZs im Zustellbereich PZ Speyer

ERNW RESEARCH
pursuing knowledge.

Gibt Bevölkerungszahl im Raster an

https://de.wikipedia.org/wiki/Datei:Zensus2011.svg

ERNW RESEARCH
pursuing knowledge.

Etwas mehr OSINT

(suche-postleitzahl.org)

Gibt uns die Einwohner*innen pro PLZ

ERNW RESEARCH
pursuing knowledge.

50% ≈ 50 PLZs

50% der Bevölkerung eines Zustellgebiets werden durch ca. 50 PLZs abgedeckt
(Standardabweichung: 13)

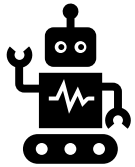
ERNW RESEARCH
pursuing knowledge.

Unser allgemeiner Ansatz

1. Erzeuge eine Tracking-Nummer
   - Vorhersagbar / berechenbar
2. Suche nach öffentlich lesbaren Hinweisen
   - In welcher Region befindet sich ein Paket?
   - Besser: Was ist das Empfangs-Paketzentrum?
3. Finde passende PLZ zu einer Region
   - Welche PLZ werden vom Paketzentrum bedient?
4. Sortiere PLZ nach Bevölkerung
5. Brute Force

ERNW RESEARCH
pursuing knowledge.

DHL: Bot Detection



- Akamai ist DHL-Trackingseite vorgeschaltet (auch in App)
- Bot-Erkennung / Brute-Force-Erkennung hilft nicht wirklich
- OSINT erlaubt uns effizientes Raten
- Wenige Versuche kombiniert mit kurzen sleep()-Aufrufen und dem „undetectable“ Selenium-Treiber umgehen Erkennung

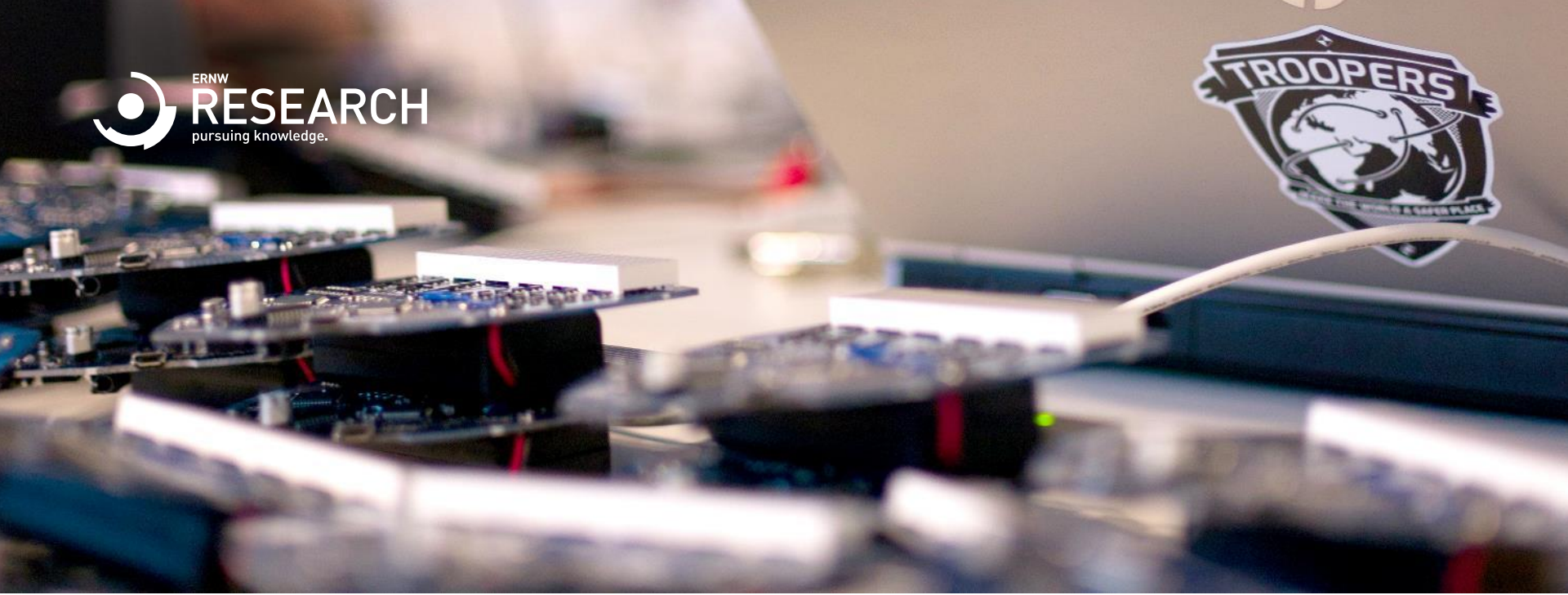
ERNW RESEARCH
pursuing knowledge.

Kurz und knapp

- Iterierbare Tracking-Nummern (erlaubt Targeting)
- PLZ als Secret (niedrige Security)
- Hinweise auf die valide PLZ
- Unendliche Versuche
- Verlassen auf Bot-Erkennung

ERNW
RESEARCH
pursuing knowledge.

Video



DPD

ERNW RESEARCH
pursuing knowledge.

DPD

- Müssen wir Captchas lösen?
  - Nein, unser kleines Python-Skript hat nie eine Captcha-Abfrage getriggert
- Außerdem: Wiederverwendung von Tracking-Nummern
  - Alte PLZs bleiben gültig

ERNW RESEARCH
pursuing knowledge.

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

~8.000

PLZs in Benutzung für Orte/Stadtteile

105

PLZs pro Zustellbereich im Durchschnitt
(Standardabweichung: 66)

ERNW RESEARCH
pursuing knowledge.

50% ≈ 24 PLZs

50% der Bevölkerung eines Zustellgebiets werden durch ca. 24 PLZs abgedeckt
(Standardabweichung: 13)

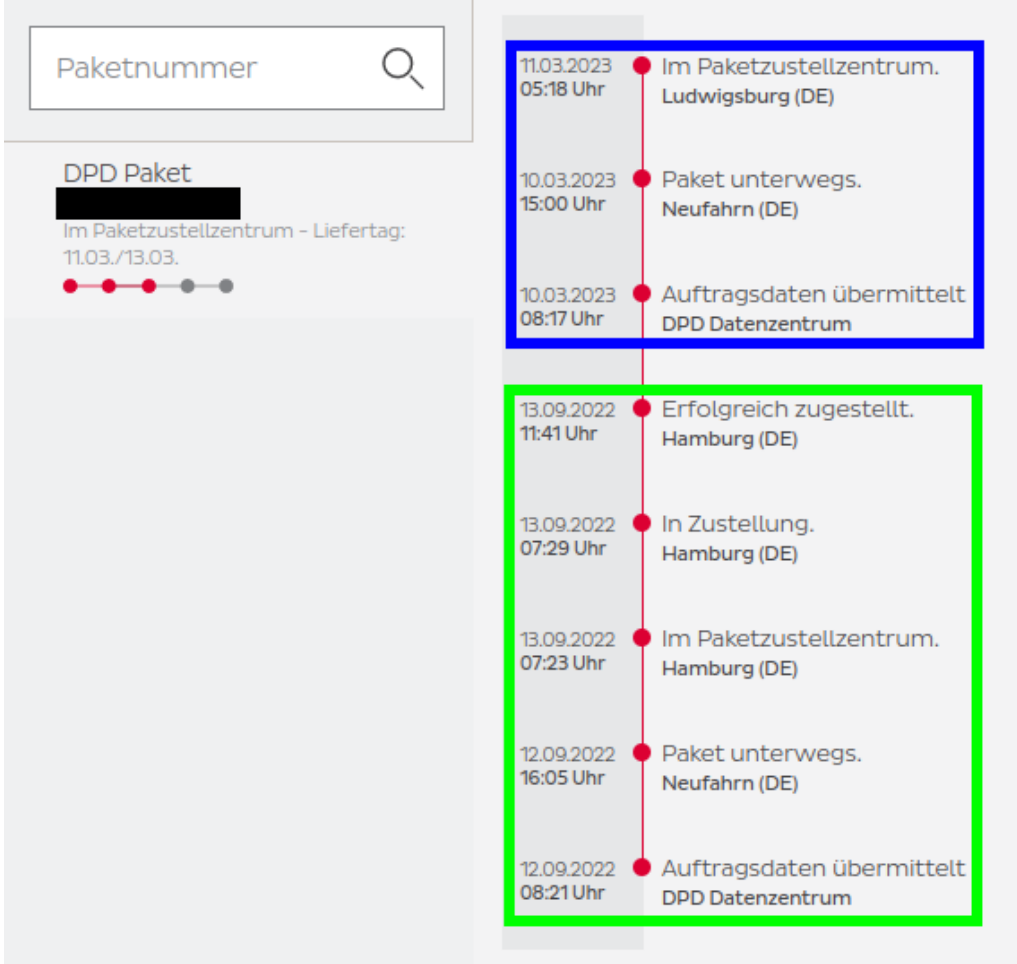
ERNW
RESEARCH
pursuing knowledge.

<2s

Um persönliche Daten in weniger als 10 Versuchen zu erlangen

Wiederverwendete Tracking-Nummern

- Nach ca. einem halben Jahr
- Vorherige PLZ bleibt gültig



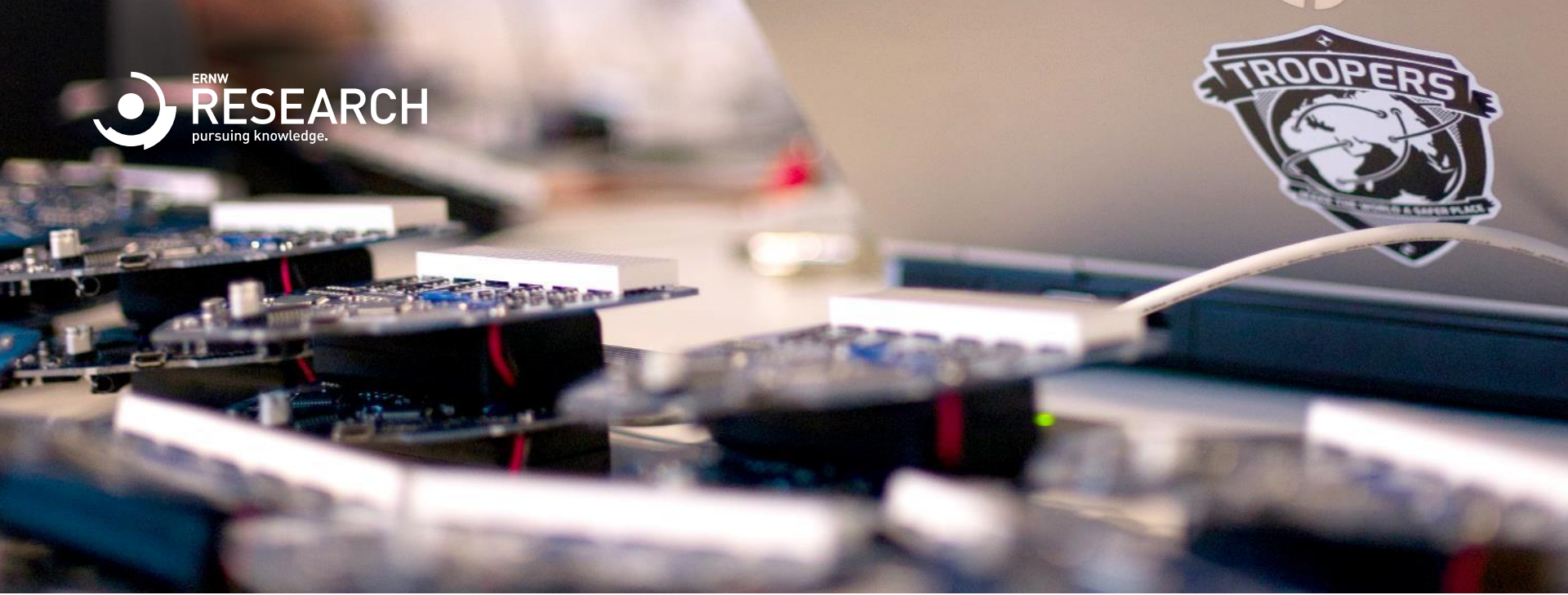
ERNW RESEARCH
pursuing knowledge.

Kurz und knapp

- Iterierbare Tracking-Nummern (erlaubt Targeting)
- PLZ als Secret (niedrige Security)
- Hinweise auf die valide PLZ
- Unendliche Versuche
- Wiederverwendung von Daten + mehrere gültige PLZs

ERNW RESEARCH
pursuing knowledge.

Video

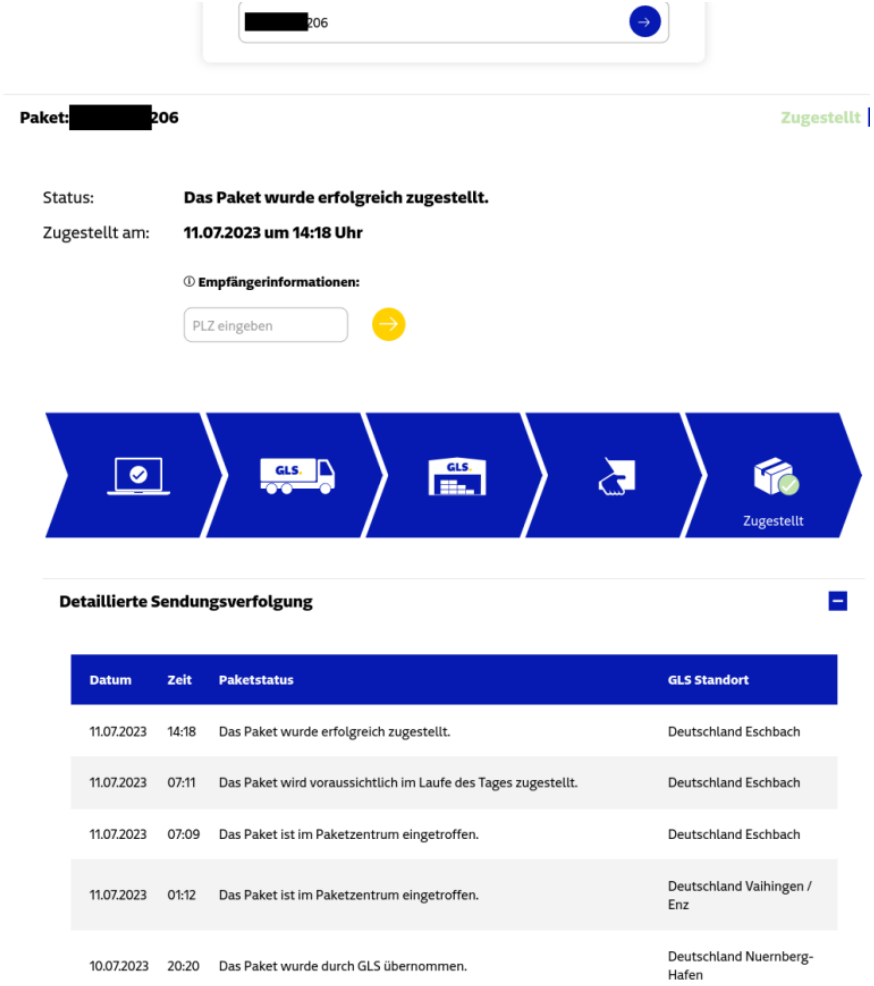


GLS

ERNW RESEARCH
pursuing knowledge.

GLS

- Keine großen Probleme
  - Kein Rate Limiting
  - Keine Bot Detection



Datum	Zeit	Paketstatus	GLS Standort
11.07.2023	14:18	Das Paket wurde erfolgreich zugestellt.	Deutschland Eschbach
11.07.2023	07:11	Das Paket wird voraussichtlich im Laufe des Tages zugestellt.	Deutschland Eschbach
11.07.2023	07:09	Das Paket ist im Paketzentrum eingetroffen.	Deutschland Eschbach
11.07.2023	01:12	Das Paket ist im Paketzentrum eingetroffen.	Deutschland Vaihingen / Enz
10.07.2023	20:20	Das Paket wurde durch GLS übernommen.	Deutschland Nuernberg-Hafen

ERNW RESEARCH
pursuing knowledge.

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

~8.000

PLZs in Benutzung für Orte/Stadtteile

136

PLZs pro Zustellbereich im Durchschnitt

ERNW RESEARCH
pursuing knowledge.

50% ≈ 30 PLZs

50% der Bevölkerung eines Zustellgebiets werden durch ca. 30 PLZs abgedeckt

ERNW RESEARCH
pursuing knowledge.

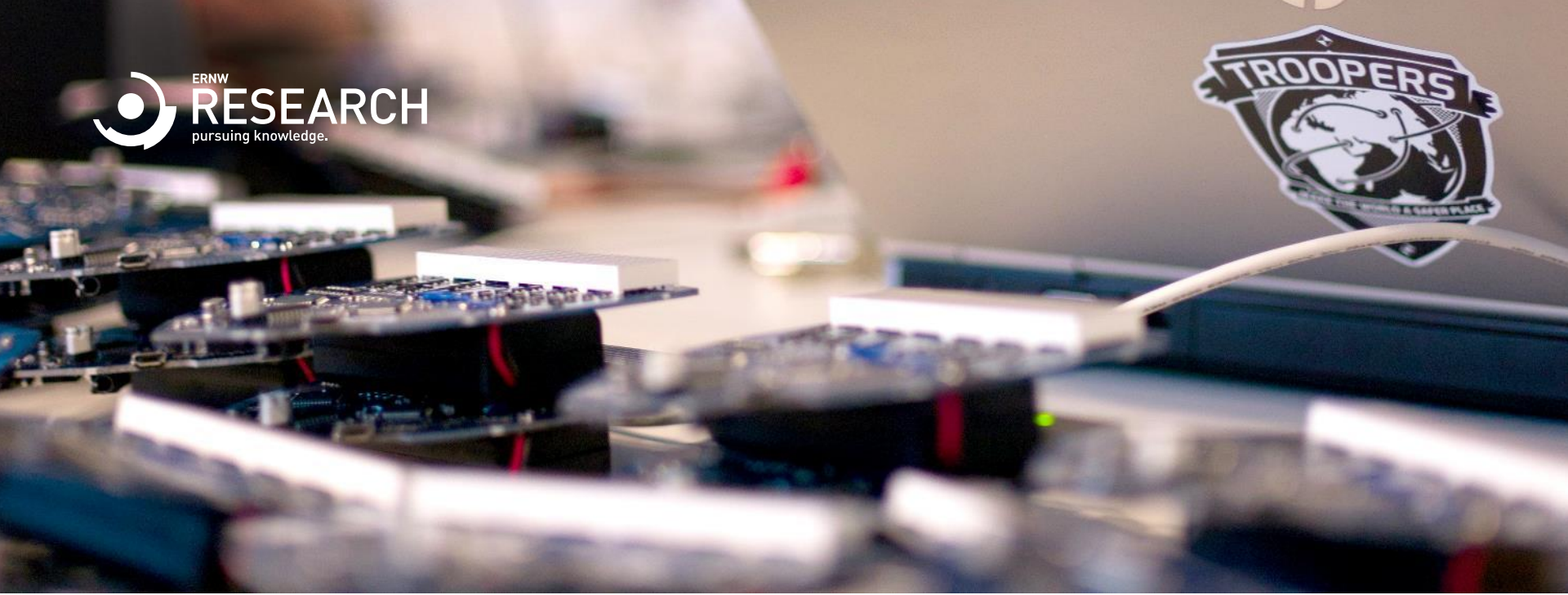
<5s

Um persönliche Daten in den meisten Fällen zu erlangen

ERNW RESEARCH
pursuing knowledge.

Kurz und knapp

- Iterierbare Tracking-Nummern (erlaubt Targeting)
- PLZ als Secret (niedrige Security)
- Hinweise auf die valide PLZ
- Unendliche Versuche
- Kein Rate Limiting oder ähnliches



UPS

ERNW RESEARCH
pursuing knowledge.

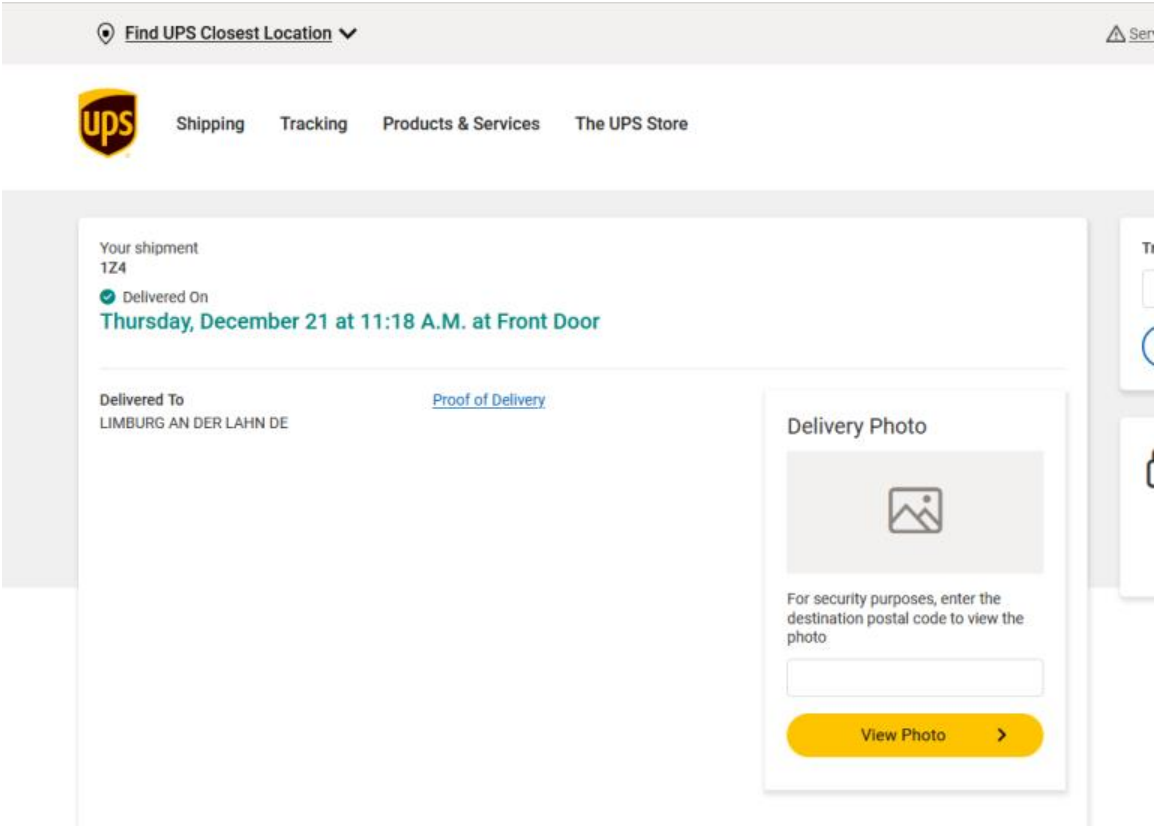
UPS

- Keine Statistik nötig
- Dafür nur wenige Infos abrufbar
  - Name
- Zustelloptionen mit gutem Secret
  - PIN in Briefkasten nach Zustellversuch

ERNW RESEARCH
pursuing knowledge.

UPS

- Haustüren gucken leicht gemacht



ERNW RESEARCH
pursuing knowledge.

Video

ERNW RESEARCH
pursuing knowledge.

Probleme

ERNW RESEARCH
pursuing knowledge.

Probleme

- Nervige Bot-Erkennungen
- Mittelmäßig deterministische Anwendungen
- Bindung an physische Prozesse
- Tracking Nummern bekommen (your turn)
- Deutschland only (your turn)

ERNW
RESEARCH
pursuing knowledge.

Möglicher Impact

ERNW RESEARCH
pursuing knowledge.

Möglicher Impact

- Daten sammeln (senderspezifisch oder zufällig)
  - Schätzen von Verkaufszahlen
  - Schätzen von Kaufverhalten
  - Schätzen von Kund*innen-Demografie
  - ...
- Manipulation der Zustellung
  - Bevorzugter Abstellort
  - Wunschnachbar*in
  - Annahme verweigern
  - ...

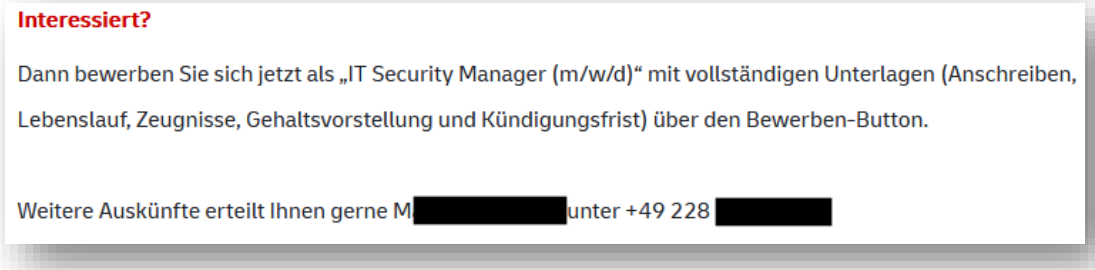
ERNW
RESEARCH
pursuing knowledge.

Möglicher Impact

- Doxing
- Stalking
- ...

Reaktionen

ERNW RESEARCH
pursuing knowledge.


Interessiert?

Dann bewerben Sie sich jetzt als „IT Security Manager (m/w/d)“ mit vollständigen Unterlagen (Anschreiben, Lebenslauf, Zeugnisse, Gehaltsvorstellung und Kündigungsfrist) über den Bewerben-Button.

Weitere Auskünfte erteilt Ihnen gerne M[redacted] unter +49 228 [redacted]

(außer man sucht nach einem Job ☺)

Reaktion von DHL

- Kontakt schwierig zu finden
- Es wird zunächst auf „technische Maßnahmen“ verwiesen
- Nach einem Video-POC positive Reaktion und schnelle erste Maßnahmen
- Seitdem ziemlich geringe Angriffsoberfläche
- Sehr gute Kooperation
- Kleinere Probleme bleiben bestehen
- security.txt eingeführt

ERNW RESEARCH
pursuing knowledge.

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

~8.000

PLZs in Benutzung für Orte/Stadtteile

~~227~~

~~PLZ pro Zustellbereich im Durchschnitt~~
~~(Standardabweichung: 99)~~

~~128~~

~~PLZ im Zustellbereich PZ Speyer~~

* wenn Zielregion != Senderegion

ERNW RESEARCH
pursuing knowledge.

Reaktion von DPD

- Schnell (durch CERT La Poste)
- Hinweise auf Zielregion entfernt
- Noch mehr (uns unbekannte) Maßnahmen
- API umgebaut, sodass unser Brute-Force-Ansatz nicht mehr funktioniert

ERNW RESEARCH
pursuing knowledge.

Reaktion von GLS

- Regelmäßige Status-Calls zwischen ERNW und GLS
- Einige Backend-Systeme wurden angepasst
- Durch Weihnachten wurden manche Maßnahmen verzögert

ERNW RESEARCH
pursuing knowledge.

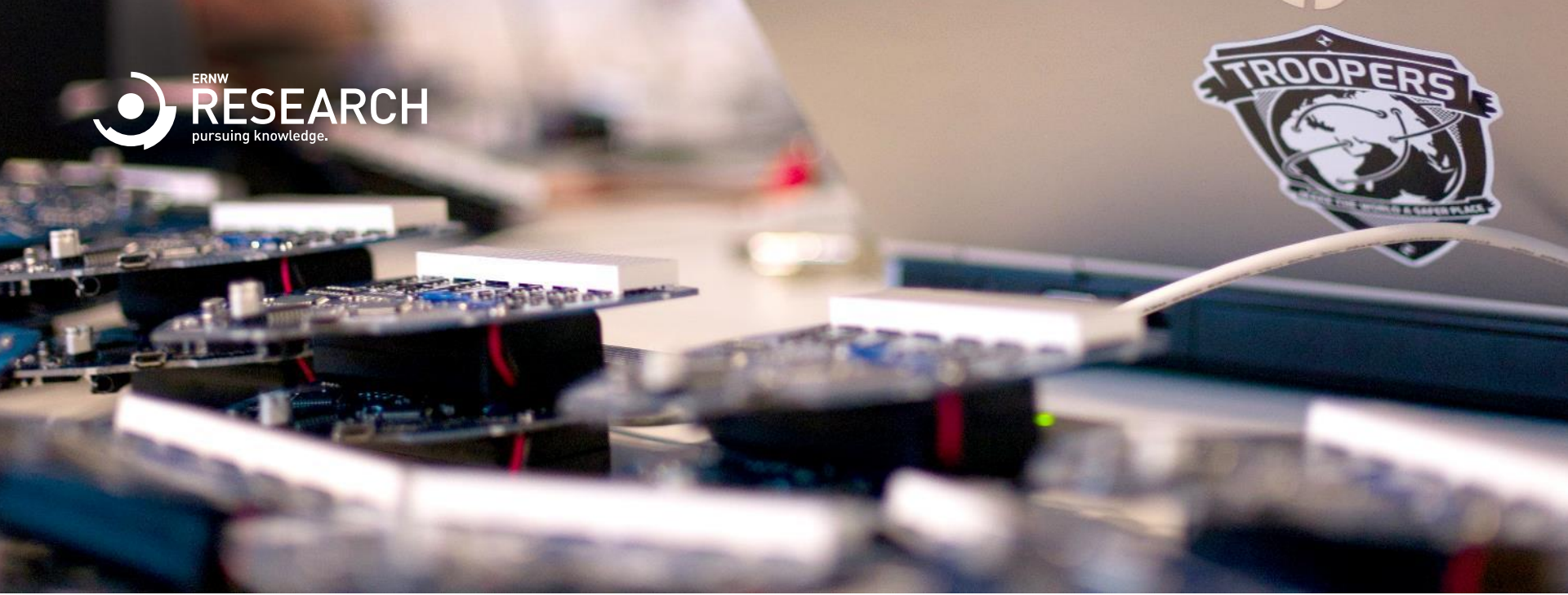
Reaktionen von UPS

- Security Contact quasi unmöglich zu finden
- Mehrere Kontaktversuche scheiterten
  - Sogar unsere Bewerbung wurde abgelehnt
- Nach einer Mail mit Proof of Concept an UPS:
  - Mail von UPS mit zusätzlichen Infos, die wir noch nicht kannten.

ERNW RESEARCH
pursuing knowledge.

Reaktionen von UPS

Absichtlich leer



Zusammenfassung

ERNW RESEARCH
pursuing knowledge.

Ist die PLZ als Shared Secret eine schlechte Idee?

- Ja, wenn:
  - Man Hinweise auf das Ziel gibt
  - Man damit sensitive Informationen freischaltet
  - Man damit Zustelloptionen freischaltet

ERNW RESEARCH
pursuing knowledge.

Ein sicherer Prozess

- Nutzt sichere Secrets
- Zeigt nur notwendige Informationen
- Verlässt sich nicht auf Bot-Erkennung

ERNW RESEARCH
pursuing knowledge.

Ein guter Disclosure-Prozess

- Macht das Finden eines Kontakts einfach (in einer security.txt)
- Gibt Feedback
- Behebt die Probleme zeitnah

ERNW RESEARCH
pursuing knowledge.

Fazit

- Bot-Erkennungen helfen nur bedingt
  - Frameworks (z. B. Selenium)
  - Parallelisierung
  - VPNs
  - HTTP-Header aus validen Anfragen
- OSINT kann Schutzmaßnahmen bedeutungslos machen
- Wiederverwendung von Daten ist ein Problem
- Historisch gewachsene Design-Probleme

ERNW RESEARCH
pursuing knowledge.

Call to Action

- Prüft selbst oder schickt uns Tracking-Nummern
  - Vor allem außerhalb von Deutschland
  - Speditionen
- Kontakt bei UPS?
- Spread the word!

ERNW RESEARCH
pursuing knowledge.

Sehr gute Marktabdeckung

Paketmarktbericht 2021, Bundesnetzagentur

ERNW
RESEARCH
pursuing knowledge.

Vielen Dank für die Aufmerksamkeit

fbausch@ernw.de
d@dkniel.de

@ERNW@infosec.exchange

www.ernw.de

www.insinuator.net
(5 Blogposts)