All Your Parcel Are Belong To Us

Dennis Kniel

Klaus Kiehne

ERNW RESEARCH
pursuing knowledge.

Who we are

Dennis Kniel

- Former incident responder, pentester
- Student
- Searches and catches bugs

Florian Bausch

- Incident responder, pentester
- Searches and finds bugs
- Speaker @ Troopers
  (Forensic Examination of Ceph)

Klaus Kiehne

- IT systems architect @ DHL
- Fixes bugs
- Improves processes

ERNW
RESEARCH
pursuing knowledge.

How we got started

ERNW RESEARCH
pursuing knowledge.

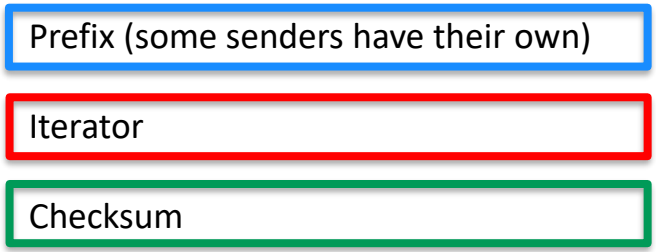
How we got started

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

ERNW RESEARCH
pursuing knowledge.

How we got started

- 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.

Tracking Numbers

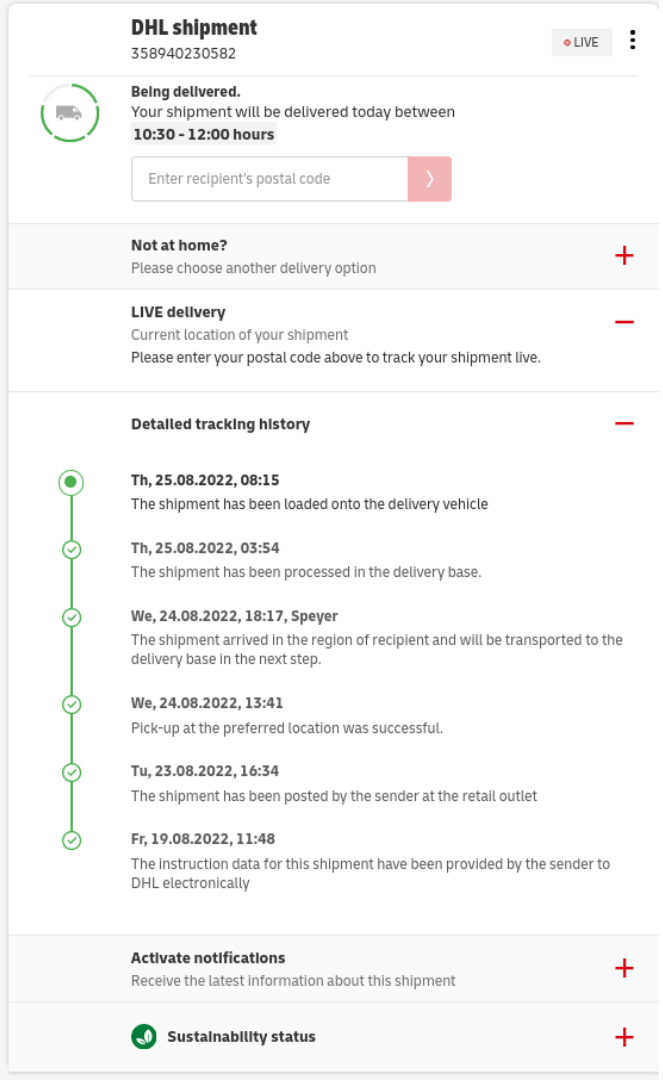
- Used for shipment tracking
- Different formats etc.
- Status
  - On the way
  - Delivered
  - Delivery failed
  - Many more……
- Destination / destination address / recipient’s name

ERNW RESEARCH
pursuing knowledge.

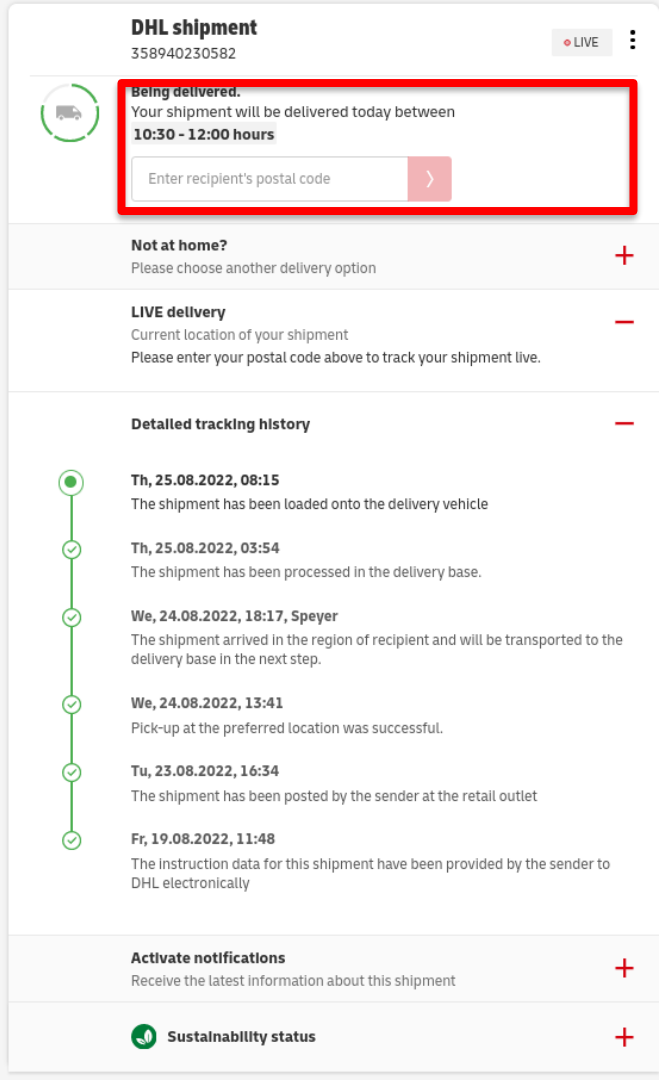
Tracking Numbers

- Convenience features
  - Live tracking during delivery
  - Preferred neighbors
  - Drop-location
  - Redirection to Packstation / parcel shop
  - Decline acceptance
  - …

ERNW RESEARCH
pursuing knowledge.



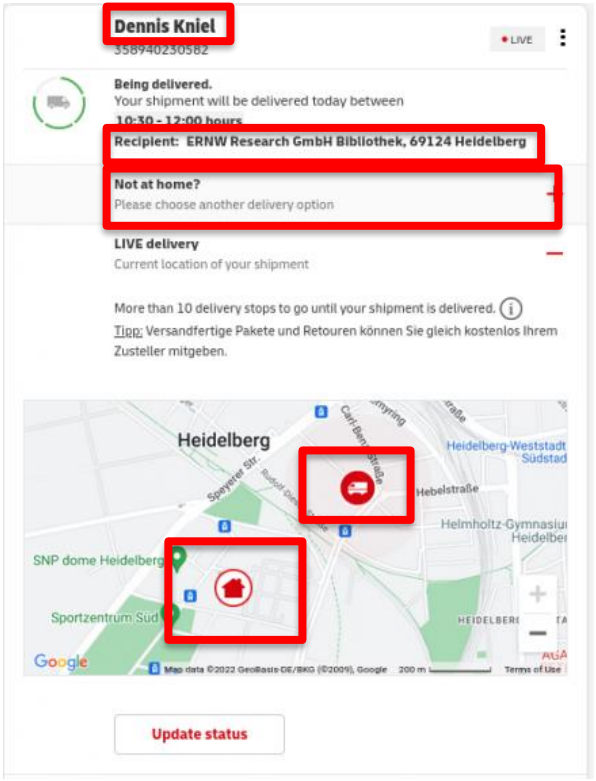
ERNW RESEARCH
pursuing knowledge.

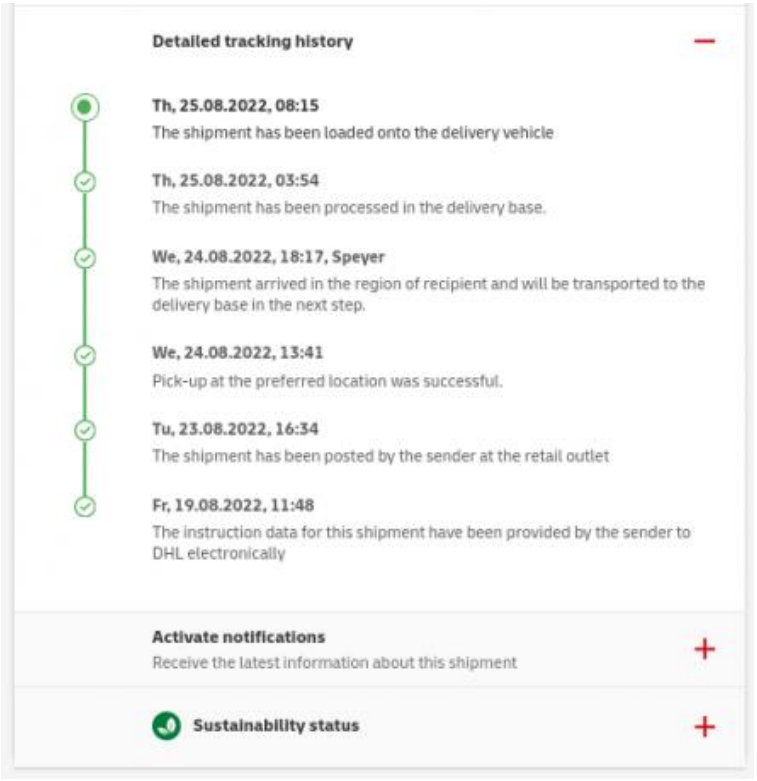


ERNW RESEARCH
pursuing knowledge.

ZIP code unlocks everything

ERNW RESEARCH
pursuing knowledge.





ERNW RESEARCH
pursuing knowledge.

100.000

Combinations for ZIPs

~28.000

ZIPs in use

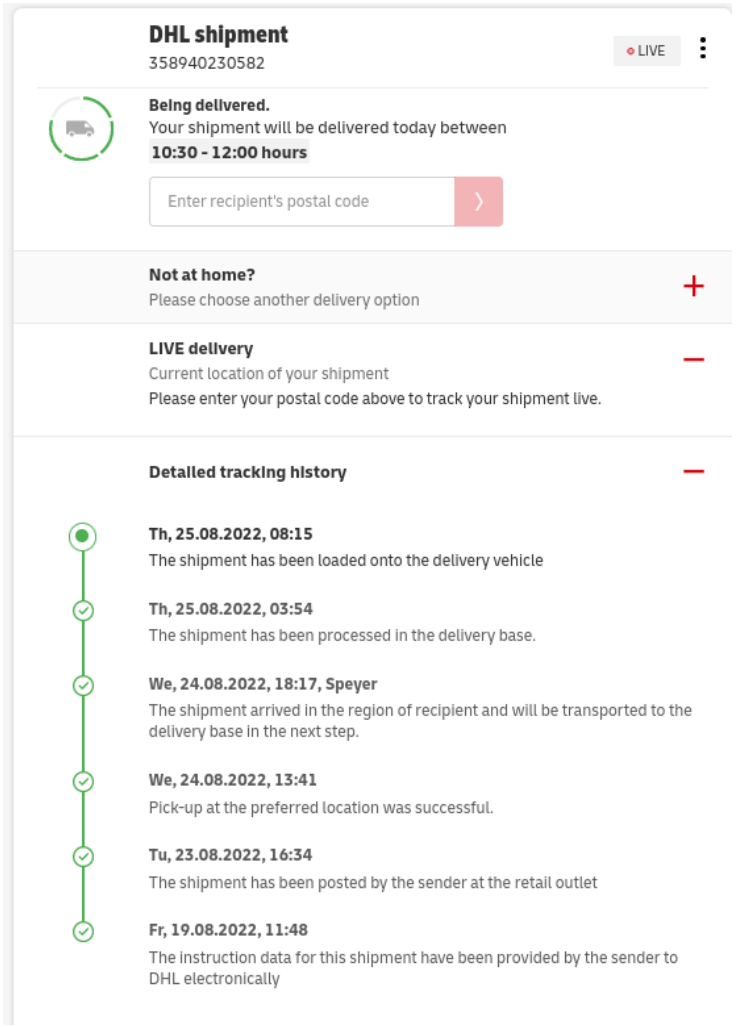
~8.000

ZIPs in use for cities etc.

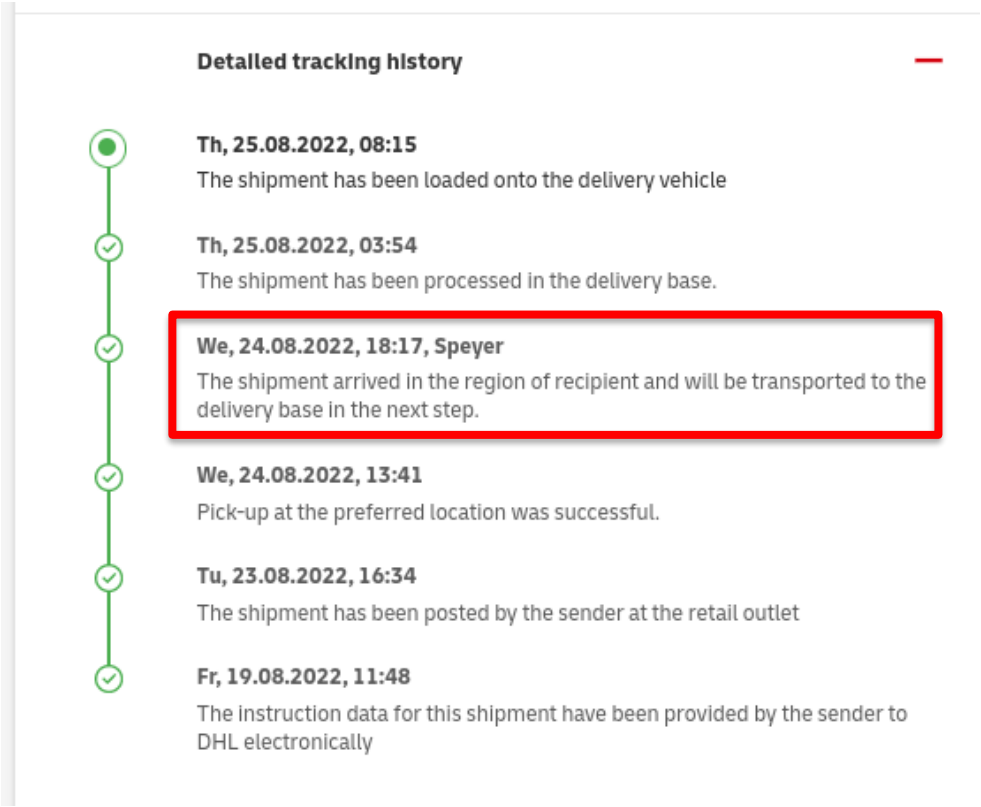
ERNW RESEARCH
pursuing knowledge.

Can we narrow it down even more?

ERNW RESEARCH
pursuing knowledge.

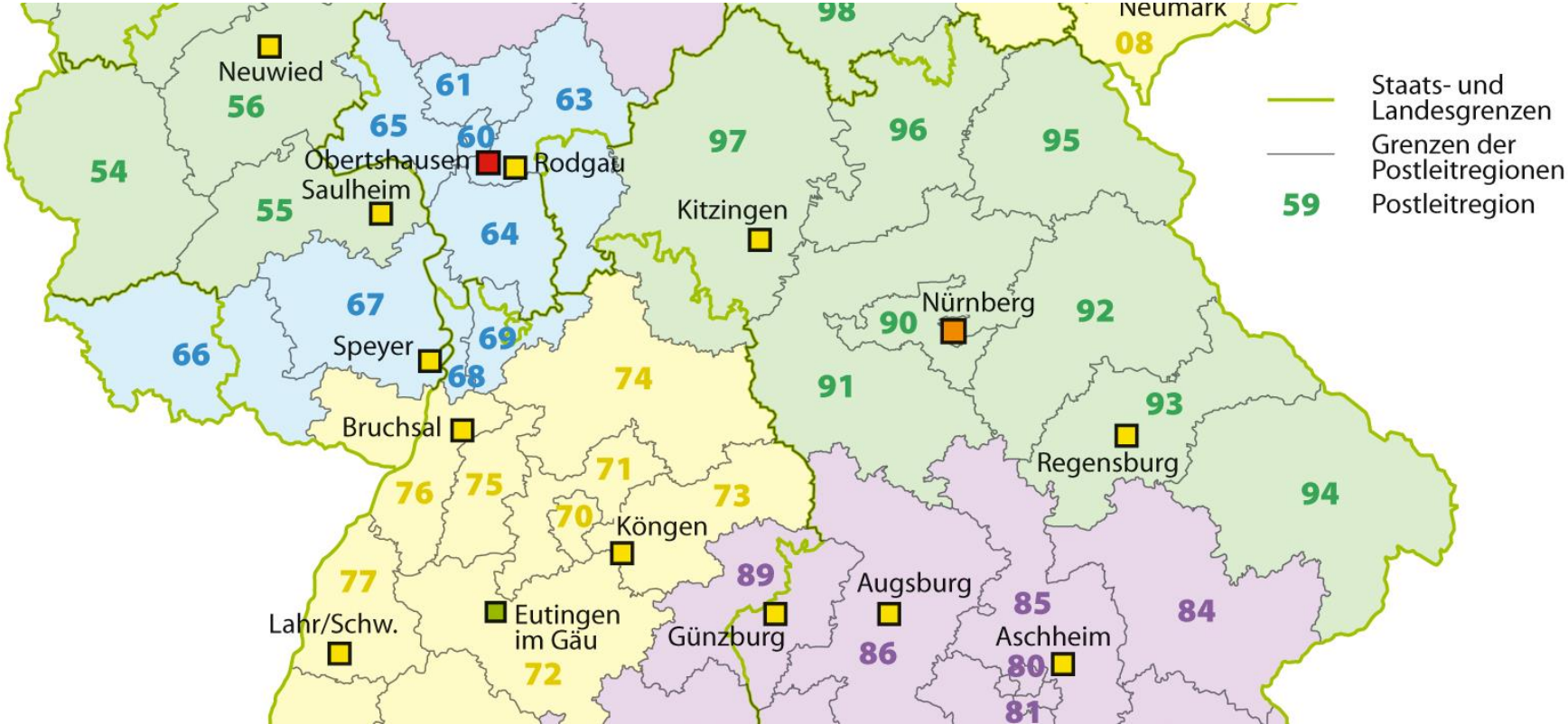


ERNW
RESEARCH
pursuing knowledge.



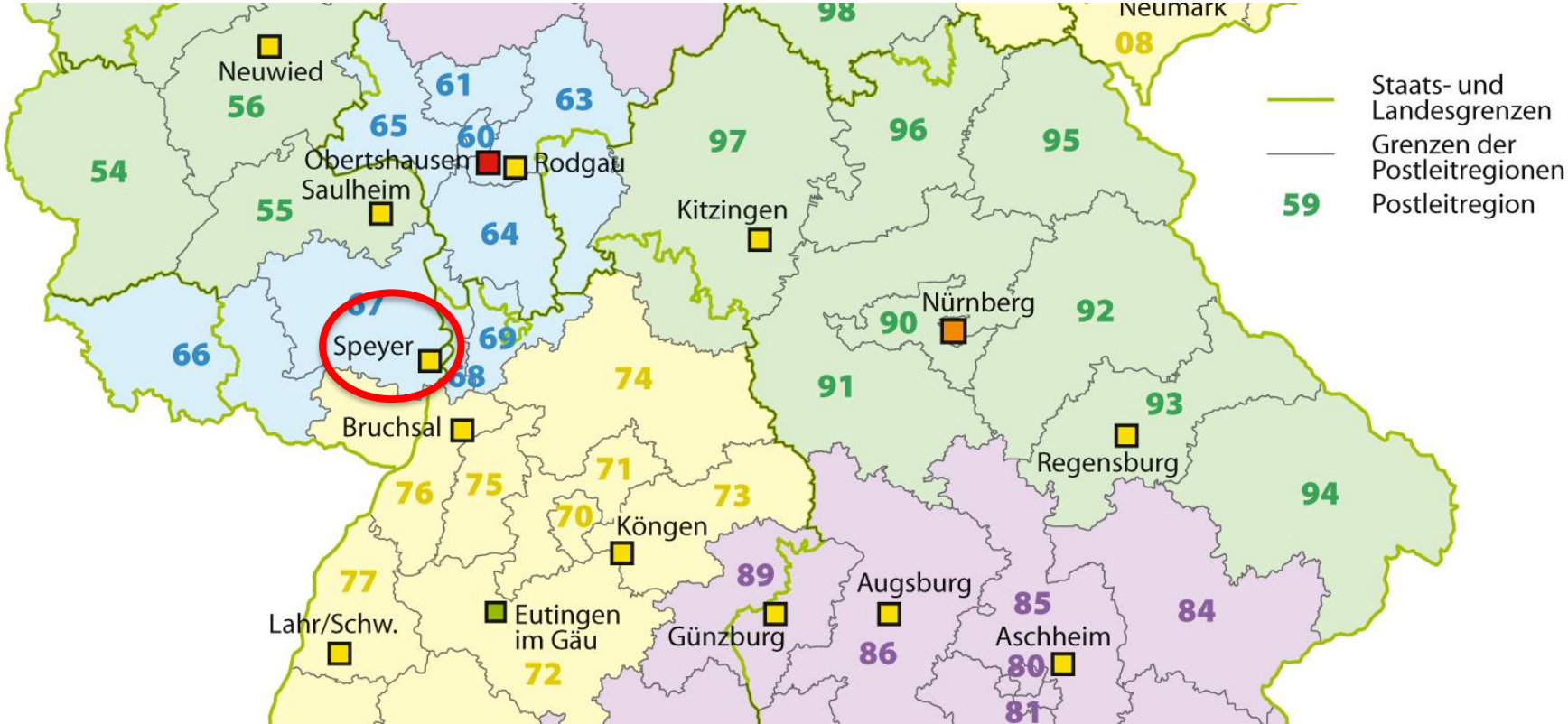
ERNW
RESEARCH
pursuing knowledge.

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

Combinations for ZIPs

~28.000

ZIPs in use

~8.000

ZIPs in use for cities etc.

227

ZIPs per parcel center on average

128

ZIPs for parcel center Speyer

ERNW RESEARCH
pursuing knowledge.

Gives us residents in a raster

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

ERNW RESEARCH
pursuing knowledge.

Some more OSINT

(or suche-postleitzahl.org)

Gives us residents per ZIP

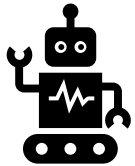
ERNW RESEARCH
pursuing knowledge.

50% ≈ 50 ZIPs

50% of the population of a parcel center service area is covered by approx. 50 ZIPs

ERNW RESEARCH
pursuing knowledge.

Bot Detection



- DHL tracking site uses Akamai
- Bot detection / brute-force detection does not really help
- OSINT allows for efficient guessing
- Fewer tries combined with short sleep()-calls and “undetectable” selenium driver circumvent detection

ERNW RESEARCH
pursuing knowledge.

How did we get here?

- Iterable tracking numbers (allow targeting)
- ZIPs as secrets (already low security)
- Hints on ZIPs
- Infinite tries
- Reliance on bot detection

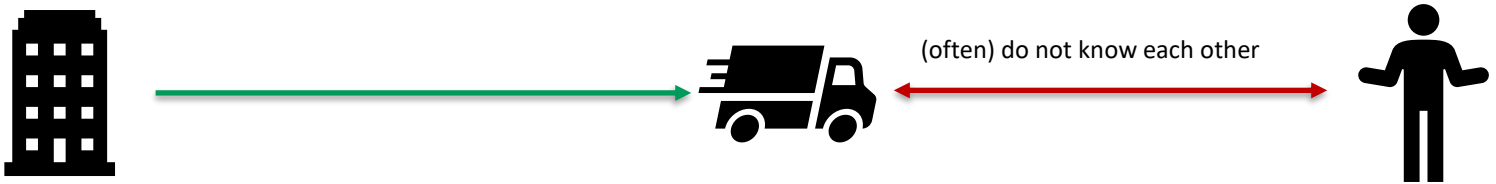
ERNW RESEARCH
pursuing knowledge.

Potential impact

- Data gathering (sender specific or just randomly)
  - Estimation of sales numbers
  - Estimation of shopping behavior
  - Estimation of customer demographics
  - …..
- Manipulation of delivery
  - Preferred location
  - Preferred neighbor
  - Decline acceptance
  - ….

ERNW RESEARCH
pursuing knowledge.

The Problem of the Shared Secret



ERNW RESEARCH
pursuing knowledge.

Is a ZIP as a shared secret a bad idea?

- Yes, if:
  - You give hints on the destination
  - It unlocks sensitive information
  - It unlocks delivery options

ERNW RESEARCH
pursuing knowledge.

DHL's Reaction

- Contact person hard to find (except if you search for a job ☺)
- First referred to "technical measures"
- After video-POC positive reaction and quick first measures
- Since then, fairly limited attack surface
- Very good cooperation (as you might have guessed)
- Some problems left

ERNW RESEARCH
pursuing knowledge.

100.000

Combinations for ZIPs

~28.000

ZIPs in use

~8.000

ZIPs in use for cities etc.

~~227~~

~~ZIPs per parcel center on average~~

~~128~~

~~ZIPs for parcel center Speyer~~

* if destination area != source area

ERNW RESEARCH
pursuing knowledge.

A secure process

- Uses secure secrets
- Shows only information which is needed
- Does not need bot detections for security

ERNW RESEARCH
pursuing knowledge.

A good disclosure process

- Gives a contact person (in a security.txt)
- Gives feedback
- Fixes issues quickly
- Joins you on talks about the issue ☺

ERNW RESEARCH
pursuing knowledge.

A perfect bot detection

- Does not exist
- Is not needed
- Just hides problems without preventing them
- However, can be used to limit spam, scraping, etc.

ERNW RESEARCH
pursuing knowledge.

How about others?

Stay tuned!

ERNW RESEARCH
pursuing knowledge.

Let‘s see the blue side!

www.ernw.de

www.insinuator.net

DP DHL @ TROOPERS 23

OUR RESPONSE TO THE ERNW FINDING

Post & Paket Deutschland

Deutsche Post DHL Group

Who we are? THE NETWORK OF POST & PARCEL GERMANY

~190,000 Employees
of which ~116,500 staff in delivery

Shipments per business day:
~48 Mio. letters
~6.2 Mio. parcels

82 Mail centers
38 Parcel centers

~11,300 Packstations

~2,600 Delivery bases
mail and composite delivery

~300 Delivery bases
parcel delivery

71,500 Delivery districts
of which ...
~55,700 *mail and composite delivery*
~15,800 *parcel delivery*

~34,600 Parcel receiving points
~25,000 Outlets

~108,400 Mail boxes
~610,000 Post office boxes

Post & Paket Deutschland – IT and IT Security

IT Organisation

- Focus on demand IT, i.e. Build and Run mostly together with external suppliers
- ~ 700 internal employees
- ~ 400 IT applications with many interfaces to provide a seemless integration
- Offering a lot of data to customers and partners via APIs and web-based portals

IT Security

- One CISO for DHL Group and one CISO per each corporate division
- Groupwide mandatory Information Security Policy framework, based on ISO 27000 ff, three levels: why, what, how
- Information Security Management System with defined processes and responsibilities
- Strong focus on availability of IT applications and protection of customer data
- Mandatory Security analysis for each IT application, e.g. threats – risks – mitigation measures
- Mandatory Security checks for go-live of IT applications, e.g. source code checks, penetration tests

Affected Use Case: public shipment tracking

- Services provided for customers
  - shipment tracking
  - preferred delivery location and timeframe
  - live tracking via Post & DHL App
- Publicly available via two different IT applications and multiple domains
  - mostly accessed via www.dhl.de
  - identically available via mobile Post & DHL App
- Data to all shipments of last 3 month accessible
- Up to 80 Mio calls per day
- Shipment details and services should be provided only to legitimate parties
- Data are confidential, e.g. falls under GDPR and partially german postal law

Public shipment tracking: challenge for dealing with recipients of shipments

Interest to get status about shipment delivery

- Sender and delivery location of shipment
- Expected date and time of delivery
- Current location to follow progress
- Final recipient of shipment

Opportunity to modify delivery

- Alternative delivery date
- Alternative delivery drop off point
- Alternative recipient in case of unavailibility

Challenge

- Data is confidential and data access has to be restricted
- We don't have a contract with the recipient and hence no credentials to validate against
- Authorisation can only be granted based on shipment details
- Only shipment recipients address is available
- Tracking IDs are unique only for a limited time and have to be reused depending on customer size

Security measures

General measures for Post & Paket Deutschland

- Communication always encrypted and authenticated
- Static and dynamic source code checks
  - Automated checks via CI/CD pipelines preferred
- Automated and manual penetration tests
- Agent based monitoring in run phase
  - Checks for newly published vulnerabilities
  - Detection of unexpected / unusual behavior
- Network segmentation and monitoring on different levels

Specific measures for public shipment tracking

- Access only via external CDN
- DDoS und DoS recognition active
- Web Application Firewall (WAF)
- Bot recognition, always passive, active in critical cases/situations
- Firewalls and DMZ to secure backend
- No information provided for non-unique tracking Ids
- Limitation to shipment data of last 3 months
- Further organizational and technical protection measures

Our reaction to the finding of ERNW

Approach for Tracking IDs

- Validated: They have to stay as is
- Required due to overarching dependencies and standards;
  e.g. by Universal Postal Union (UPU)
- Aligned procedure within logistics industry
- Agreed with several customers to self-assign shipment numbers within given ranges

Measures taken

- Immediate response (10 days after first contact from ERNW)
  - No hub names for public tracking provided anymore, so guessing of valid recipient zip code/ranges is impossible
- Further activities
  - Time lock after exceeding threshold of non-matching requests per tracking ID
  - Additional measures implemented (restricted)

Security input @ DHL Group

- **We welcome a responsible disclosure!**

- /.well-known/security.txt is available for main domains :

  Contact: mailto:cybersecurity@dpdhl.com
  Encryption: https://keyserver.deutschepost.de/download.php?id=eds-cybersecurity@dpdhl.com
  Policy: https://www.dpdhl.com/en/sustainability/governance/cyber-security/vulnerability-disclosure-policy.html
  Hiring: https://careers.dhl.com/

- Private Bug Bounty Program has been started
  ... more to come – stay tuned!

@Dennis Kniel and ERNW team :

- Thank you for “Responsible Disclosure“!
- Thank you for the open and constructive discussions
- Thank you for the opportunity having me here today on stage

THANK YOU

Deutsche Post AG

Klaus Kiehne
IT-Architect
k.kiehne@deutschepost.de