



ERNW

RESEARCH

pursuing knowledge.

Ich weiß, was du letzten Sommer bestellt hast
Oder: Warum Bot-Erkennungen nicht helfen
Florian Bausch, Dennis Kniel

Wer wir sind

Dennis Kniel

- Ehemaliger Incident Responder und Pentester
- Student
- Sucht Käfer

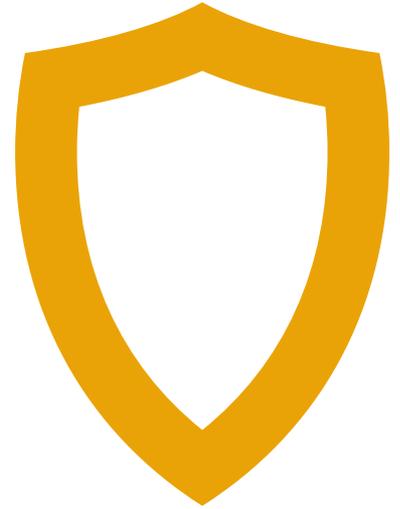
Florian Bausch

- Incident Responder und Pentester
- Sucht Bugs

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>



Wie alles begann....



Stellt euch vor

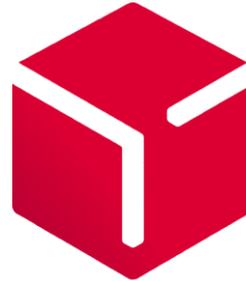
- Ihr habt Kund*innen
- Ihr kennt sie nicht
- Nicht einmal die E-Mailadresse
- Keine Telefonnummer
- Nur Name und Anschrift
- Ihr möchtet sie authentifizieren und autorisieren





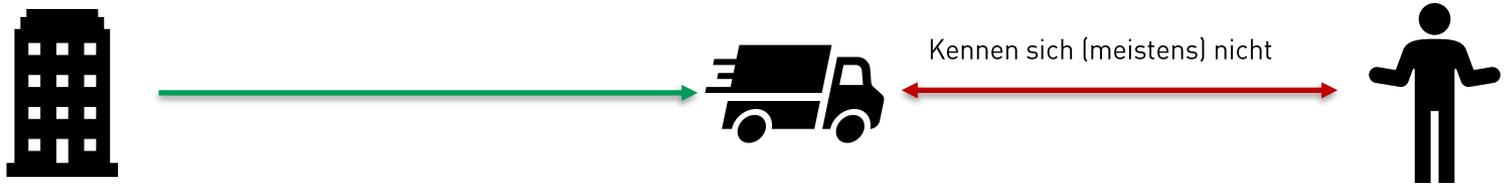
ERNW
RESEARCH
pursuing knowledge.

So wie z. B. Paket-Dienstleister



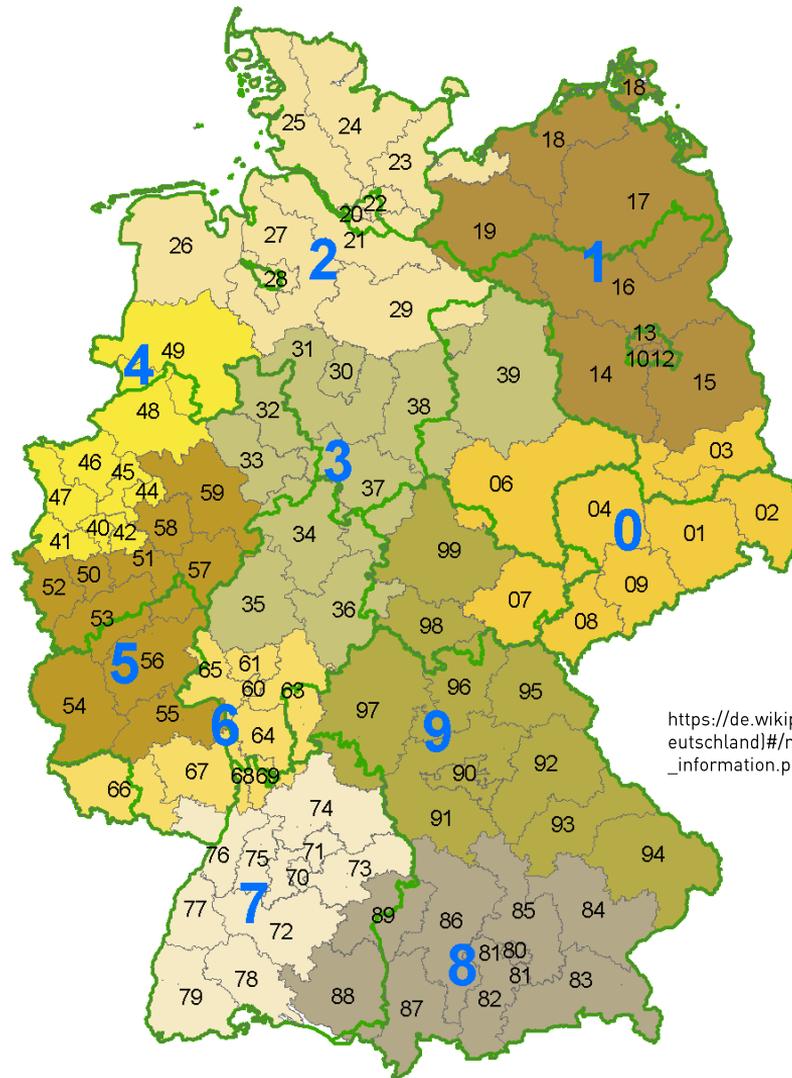
dpd

Das Problem mit dem Shared Secret



Wir brauchen ein Shared Secret

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



[https://de.wikipedia.org/wiki/Postleitzahl_\(Deutschland\)#/media/Datei:German_postcode_information.png](https://de.wikipedia.org/wiki/Postleitzahl_(Deutschland)#/media/Datei:German_postcode_information.png)

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

Exkurs: Tracking-Nummern

- 4XXXXXXXX0344
- 4XXXXXXXX0350
- 4XXXXXXXX0366
- 4XXXXXXXX0372
- 4XXXXXXXX0388
- 4XXXXXXXX0394
- 4XXXXXXXX0401
- 4XXXXXXXX0417
- 4XXXXXXXX0423

Exkurs: Tracking-Nummern

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

Präfix (Sender können eigene Präfixe haben)

Iterator

Prüfsumme

Exkurs: Tracking-Nummern

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

Exkurs: Tracking-Nummern

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

DHL shipment

358940230582

LIVE



Being delivered.

Your shipment will be delivered today between
10:30 - 12:00 hours

Enter recipient's postal code



Not at home?

Please choose another delivery option



LIVE delivery

Current location of your shipment

Please enter your postal code above to track your shipment live.



Detailed tracking history



Th, 25.08.2022, 08:15

The shipment has been loaded onto the delivery vehicle



Th, 25.08.2022, 03:54

The shipment has been processed in the delivery base.



We, 24.08.2022, 18:17, Speyer

The shipment arrived in the region of recipient and will be transported to the delivery base in the next step.



We, 24.08.2022, 13:41

Pick-up at the preferred location was successful.



Tu, 23.08.2022, 16:34

The shipment has been posted by the sender at the retail outlet



Fr, 19.08.2022, 11:48

The instruction data for this shipment have been provided by the sender to DHL electronically

Activate notifications

Receive the latest information about this shipment



Sustainability status





Die PLZ schaltet alles frei

Dennis Kniel 358940230582 LIVE

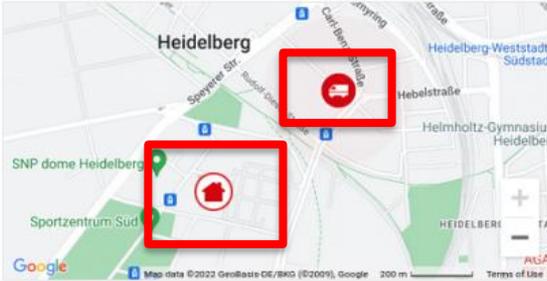
Being delivered.
Your shipment will be delivered today between **10:30 - 12:00 hours**

Recipient: ERNW Research GmbH Bibliothek, 69124 Heidelberg

Not at home?
Please choose another delivery option

LIVE delivery
Current location of your shipment

More than 10 delivery stops to go until your shipment is delivered. ⓘ
Tip: Versandfertige Pakete und Retouren können Sie gleich kostenlos Ihrem Zusteller mitgeben.



Update status

Detailed tracking history

- Th, 25.08.2022, 08:15**
The shipment has been loaded onto the delivery vehicle.
- Th, 25.08.2022, 03:54**
The shipment has been processed in the delivery base.
- We, 24.08.2022, 18:17, Speyer**
The shipment arrived in the region of recipient and will be transported to the delivery base in the next step.
- We, 24.08.2022, 13:41**
Pick-up at the preferred location was successful.
- Tu, 23.08.2022, 16:34**
The shipment has been posted by the sender at the retail outlet
- Fr, 19.08.2022, 11:48**
The instruction data for this shipment have been provided by the sender to DHL electronically

Activate notifications
Receive the latest information about this shipment

Sustainability status

Vorgefundene Maßnahmen

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



DHL

Vorgefundene Maßnahmen

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

DHL

- Alle PLZs testen aufwändig
- Aber...

100.000

Kombinationen für PLZs

~28.000

PLZs in Benutzung

~8.000

PLZs in Benutzung für Orte/Stadtteile

Geht da noch mehr
(bzw. weniger)?

DHL shipment

358940230582

LIVE



Being delivered.

Your shipment will be delivered today between

10:30 - 12:00 hours

Enter recipient's postal code



Not at home?

Please choose another delivery option



LIVE delivery

Current location of your shipment

Please enter your postal code above to track your shipment live.



Detailed tracking history



Th, 25.08.2022, 08:15

The shipment has been loaded onto the delivery vehicle



Th, 25.08.2022, 03:54

The shipment has been processed in the delivery base.



We, 24.08.2022, 18:17, Speyer

The shipment arrived in the region of recipient and will be transported to the delivery base in the next step.



We, 24.08.2022, 13:41

Pick-up at the preferred location was successful.



Tu, 23.08.2022, 16:34

The shipment has been posted by the sender at the retail outlet



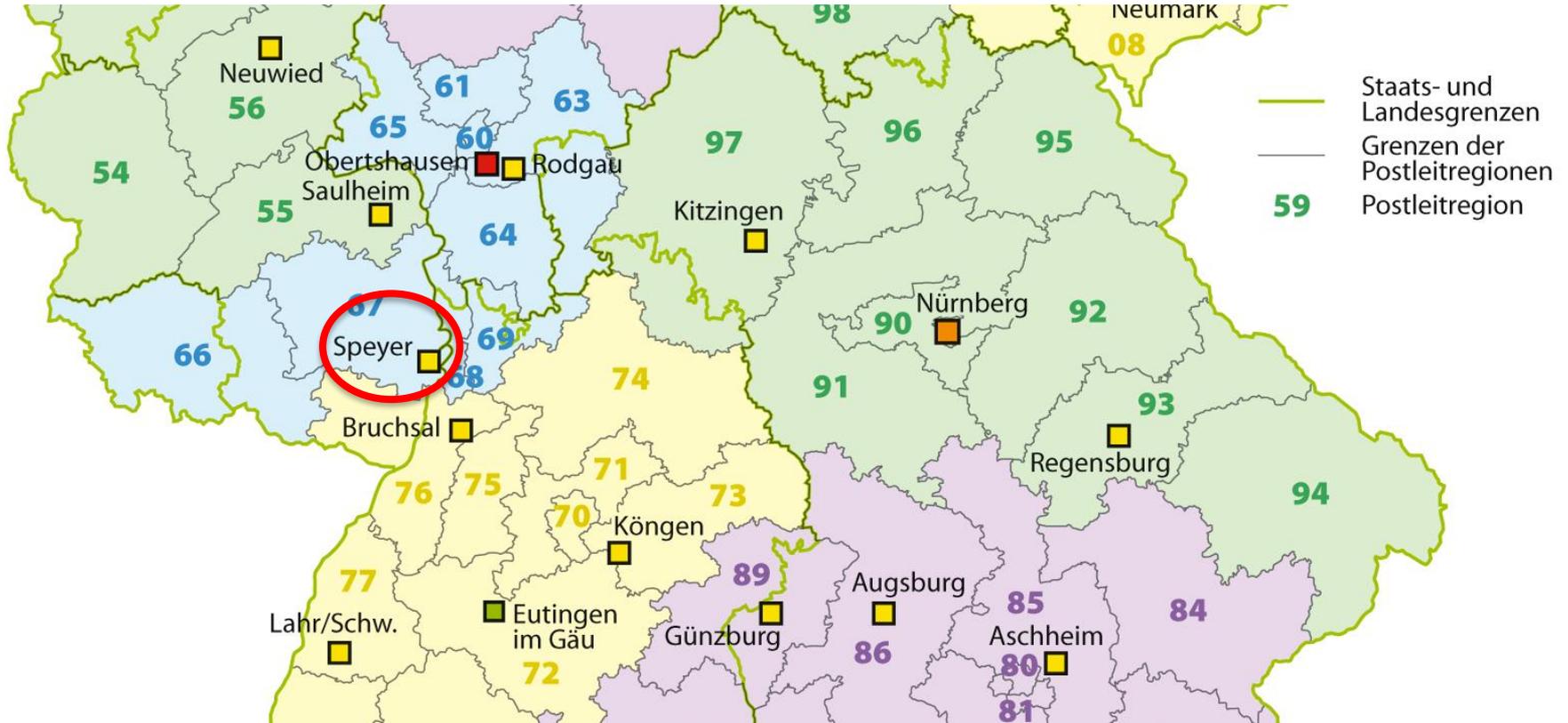
Fr, 19.08.2022, 11:48

The instruction data for this shipment have been provided by the sender to DHL electronically

Detailed tracking history

-  **Th, 25.08.2022, 08:15**
The shipment has been loaded onto the delivery vehicle
-  **Th, 25.08.2022, 03:54**
The shipment has been processed in the delivery base.
-  **We, 24.08.2022, 18:17, Speyer**
The shipment arrived in the region of recipient and will be transported to the delivery base in the next step.
-  **We, 24.08.2022, 13:41**
Pick-up at the preferred location was successful.
-  **Tu, 23.08.2022, 16:34**
The shipment has been posted by the sender at the retail outlet
-  **Fr, 19.08.2022, 11:48**
The instruction data for this shipment have been provided by the sender to DHL electronically

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



Paket **da!**

<https://www.paketda.de>

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



zensus 2011
Wissen, was morgen zählt

Gibt Bevölkerungszahl im Raster an

Etwas mehr OSINT

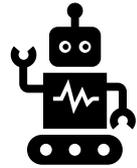
(suche-postleitzahl.org)

Gibt uns die Einwohner*innen pro PLZ

50% \approx 50 PLZs

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

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

Kurz und knapp

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

Video



DPD

Vorgefundene Maßnahmen

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

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

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)

50% \approx 24 PLZs

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

< 2s

Um persönliche Daten in weniger als 10
Versuchen zu erlangen

Wiederverwendete Tracking-Nummern

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

Paketnummer 

DPD Paket
[REDACTED]
Im Paketzustellzentrum - Liefertag:
11.03./13.03.



11.03.2023 05:18 Uhr ● Im Paketzustellzentrum.
Ludwigsburg (DE)

10.03.2023 15:00 Uhr ● Paket unterwegs.
Neufahrn (DE)

10.03.2023 08:17 Uhr ● Auftragsdaten übermittelt
DPD Datenzentrum

13.09.2022 11:41 Uhr ● Erfolgreich zugestellt.
Hamburg (DE)

13.09.2022 07:29 Uhr ● In Zustellung.
Hamburg (DE)

13.09.2022 07:23 Uhr ● Im Paketzustellzentrum.
Hamburg (DE)

12.09.2022 16:05 Uhr ● Paket unterwegs.
Neufahrn (DE)

12.09.2022 08:21 Uhr ● Auftragsdaten übermittelt
DPD Datenzentrum

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



Probleme

Probleme

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



Möglicher Impact

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
 - ...

Möglicher Impact

- Doxing
- Stalking
- ...



Reaktionen

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 Angriffsfläche
- Sehr gute Kooperation
- Kleinere Probleme bleiben bestehen
- security.txt und Bug-Bounty-Programm eingeführt

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

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

Zusammenfassung

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

Ein sicherer Prozess

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

Ein guter Disclosure-Prozess

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

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

Bei der Konkurrenz wird's doch besser sein...



Paketmarktbericht 2021, Bundesnetzagentur

Nein.
Zumindest nicht bei allen.
(Stay tuned)

Vielen Dank für die Aufmerksamkeit



Talk auf der Troopers 2023:

<https://troopers.de/troopers23/talks/mtgrsz/>



fbausch@ernw.de
d@dkniel.de



@ERNW@infosec.exchange



www.ernw.de



www.insinator.net
(2 Blogposts)

