SPooFd: How to Spoof Emails, Even with Full SPF and DMARC Protection

Koen van Hove
koen@nlnetlabs.nl

In a nutshell

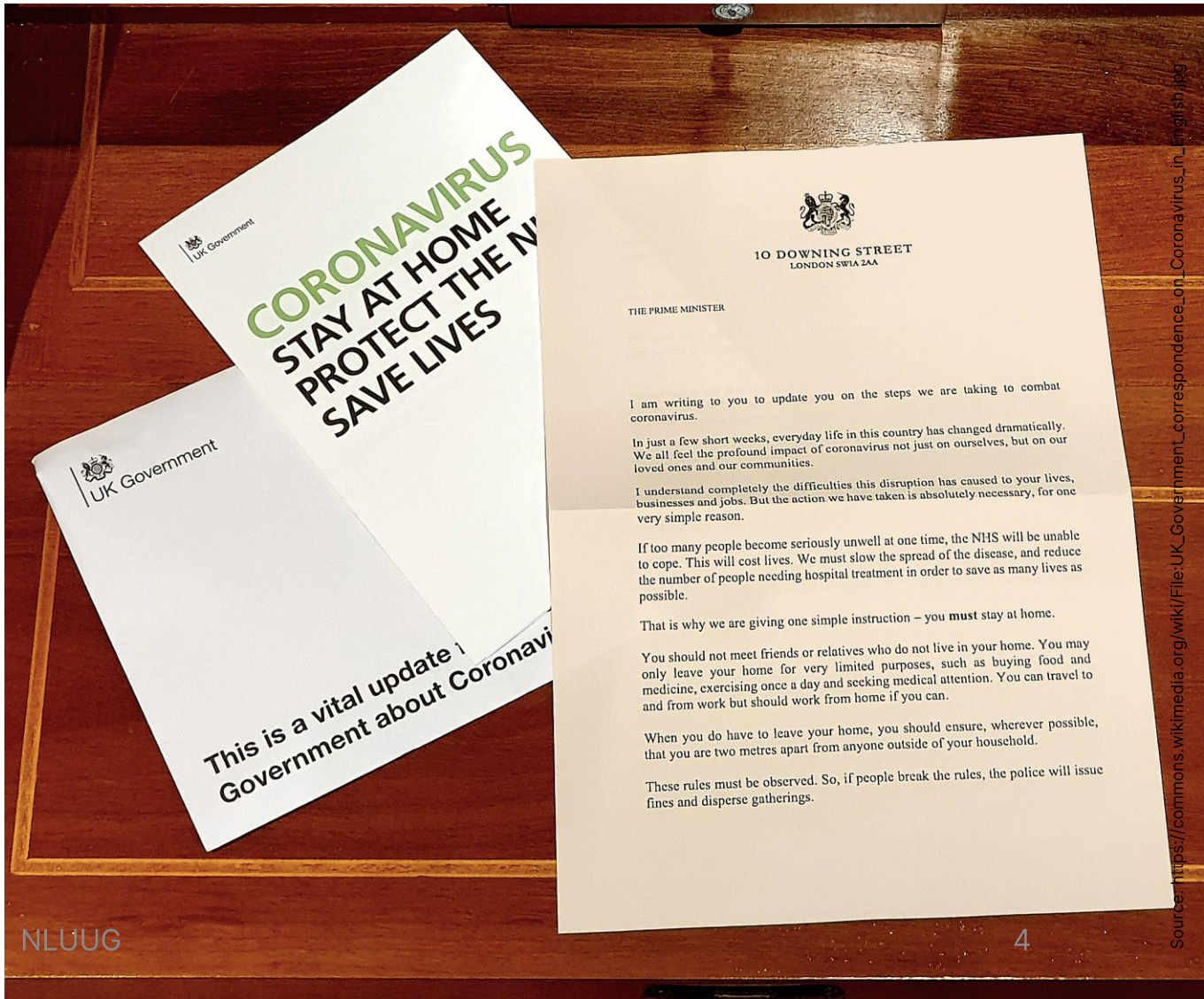
- I found a vulnerability that affects many parts of government and critical infrastructure
- I reported those vulnerabilities to the affected organisations
- I analysed what happened next

1. What the vulnerability is **2. An analysis of the disclosures**

The vulnerability explained

A quick history of e-mail

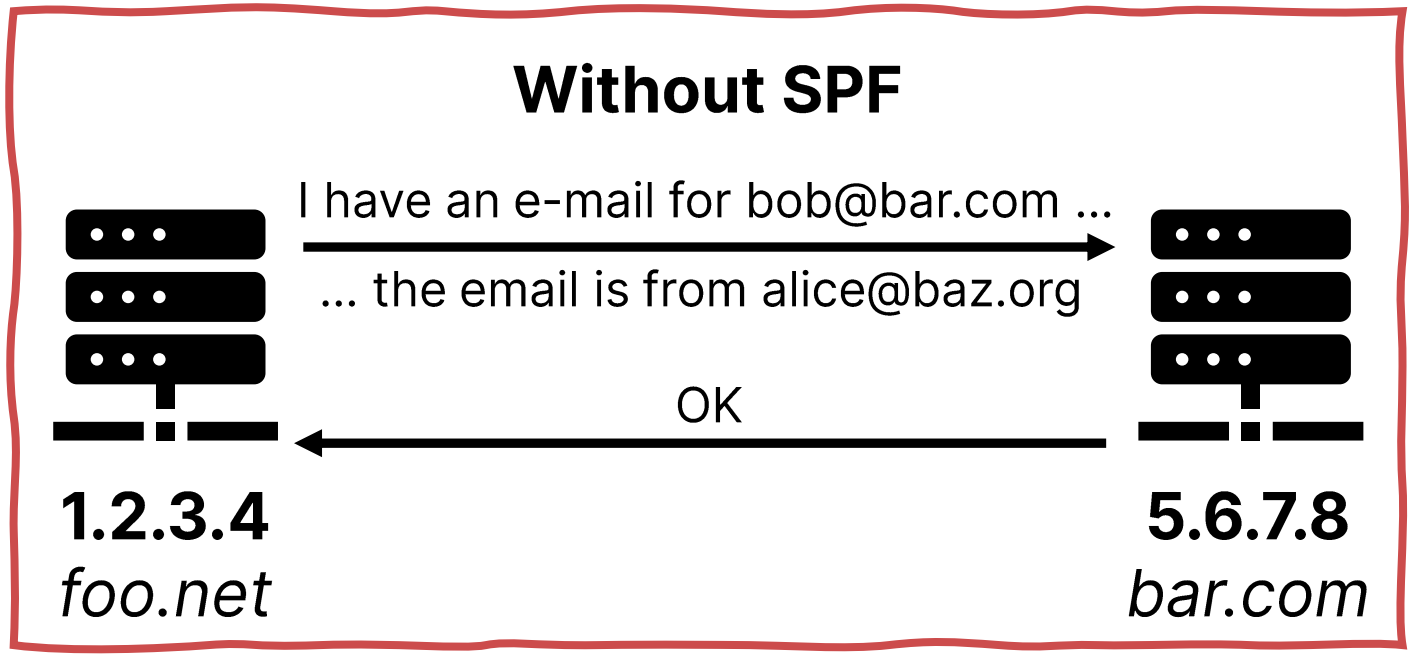
- Physical letters
- No verification of the sender
- Three standards:
  - SPF
  - DKIM
  - DMARC

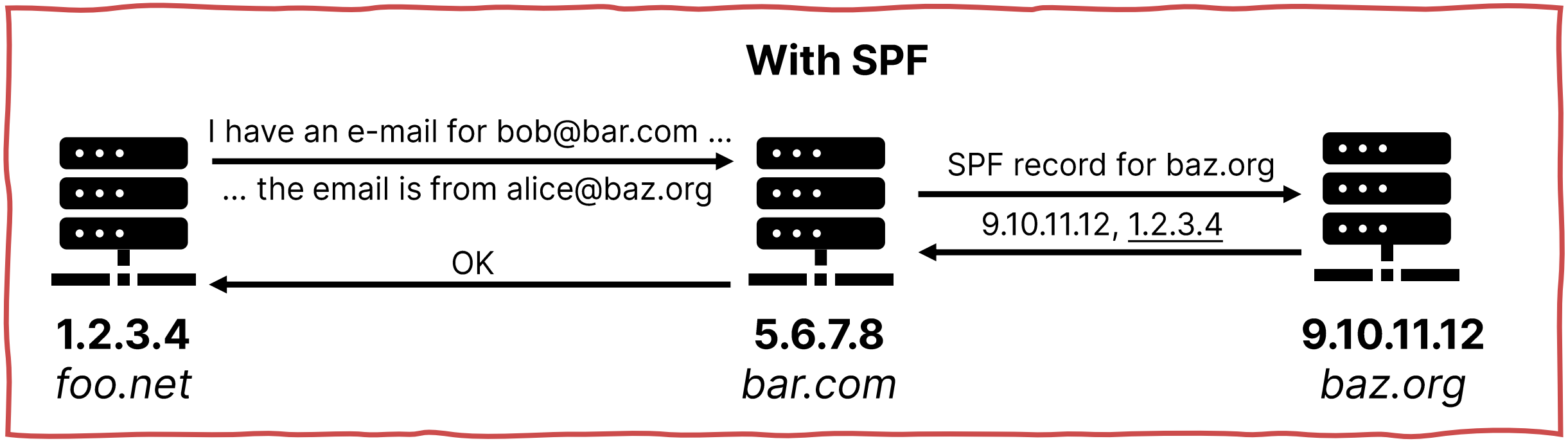


Source: https://commons.wikimedia.org/wiki/File:UK_Government_correspondence_on_Coronavirus_in_English.jpg

SPF

- DNS record
- Authorises IP addresses





DMARC

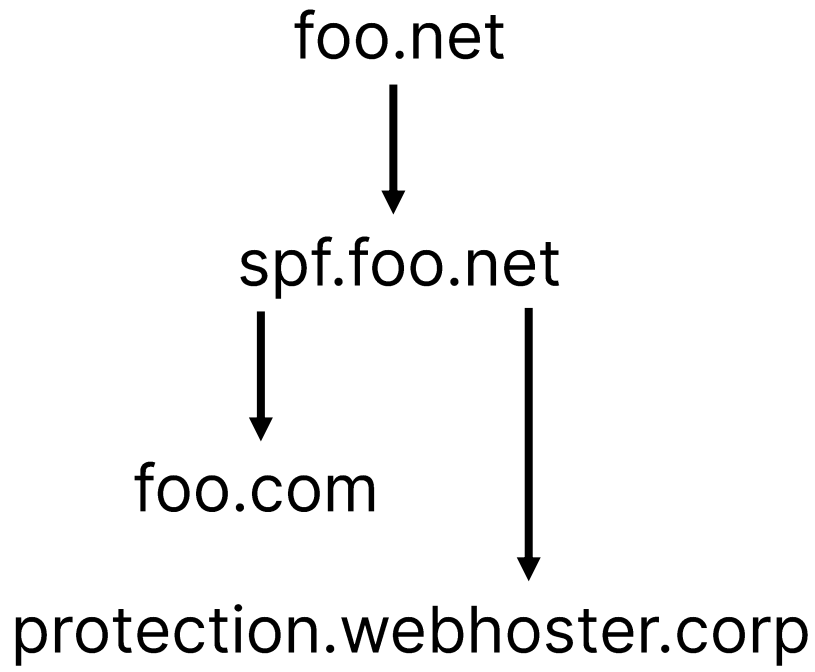
- SPF with policy and reporting
- “none”, “quarantine” (ie. SPAM folder), or “reject”

DMARC pass =
(SPF pass AND SPF aligned)
OR
(DKIM pass AND DKIM aligned)

- Ergo: valid and aligned DKIM signature not required for DMARC

SPF delegation

- E-mail outsourced to third-parties
  - Third-parties outsourcing it again to third-parties
- Creates a chain dependency
- Every host in SPF tree is valid



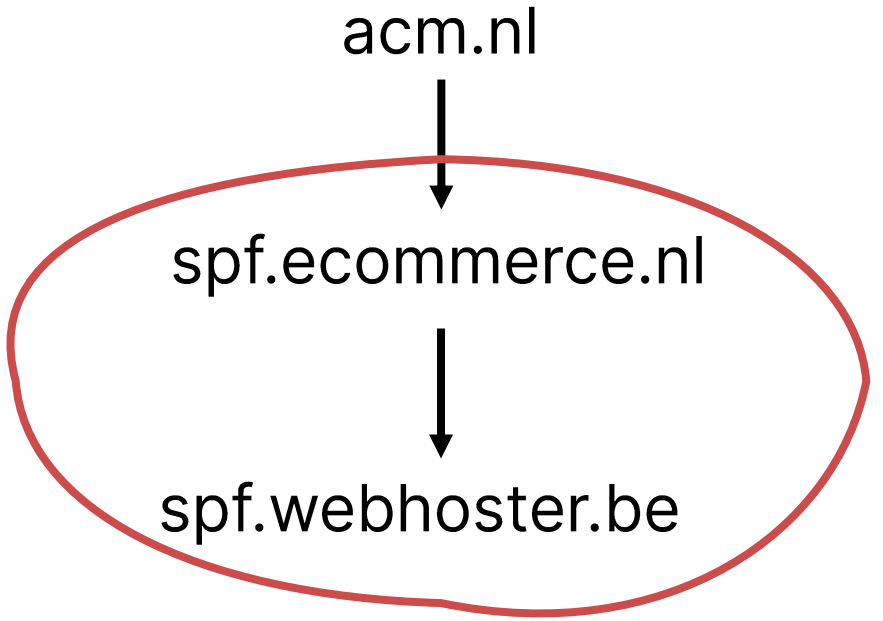
Where it goes wrong

- Many large generic webhosting providers **share outgoing mail servers** between customers
- A lot of them **do not check** whether the customer is authorised to send email from a domain name

- Thus **every customer** (anyone with ~€100/year) **can send email on behalf of every other customer**

Putting this into practice

- ACM is the Dutch Authority for Consumers and Markets
- E-commerce platform was authorised to send email on behalf of acm.nl
- They outsourced it again
- The webhosting platform inadequately checked for who was sending email



Impact

- We became a customer of that webhoster
- This made us able to send e-mail on behalf of @acm.nl
  - To the outside world, e.g. billing@acm.nl
  - In some cases also inside the organisation (not in this case)

- Applicable to webhosting providers throughout Europe
  - One would even DKIM-sign the email for us
- We decided to develop a heuristic

Is it difficult to configure correctly?

- Not really...

tables with server replies indexed by *rbl_domain*. This feature is available in Postfix 2.6 and later.

reject_sender_login_mismatch

As of Postfix 2.1, this is an alias for "reject_authenticated_sender_login_mismatch, reject_unauthenticated_sender_login_mismatch".

reject_unauthenticated_sender_login_mismatch

Reject the request when SASL is enabled, the MAIL FROM address is listed in $smtpd_sender_login_maps, but the client is not authenticated with SASL. With SASL enabled, this prevents an unauthenticated client from using any MAIL FROM address that is listed in $smtpd_sender_login_maps. This feature is available in Postfix version 2.1 and later.

reject_unknown_sender_domain

Source: http://www.postfix.org/postconf.5.html#smtpd_sender_restrictions

How to force authenticated users to only send from their authenticated domain

To make sure Users use their own domain in their From header, assuming you've got a newer exim.conf that supports `/etc/exim.acl_check_message.pre.conf` create the file and add this code to it:

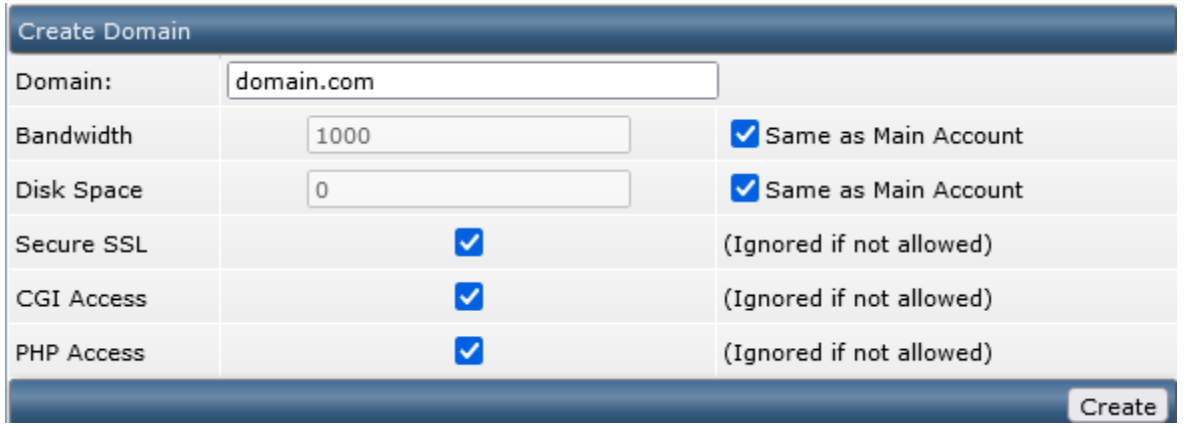
text

```
deny
 authenticated = *
 condition = ${if or { { !eqi{${domain:$authenticated_id}} {$sender_address_domain} }\
                       { !eqi{${domain:{$authenticated_id}} {${domain:{${address:$header_From:}}} }\
                      }\
             }
 message = Your FROM address domain ( $sender_address_domain ) must match your domain name used in authenticated email user ( $authenticated_id ).
```

Source: https://docs.directadmin.com/other-hosting-services/exim/configuring-exim.html#how-to-force-authenticated-users-to-only-send-from-their-authenticated-domain

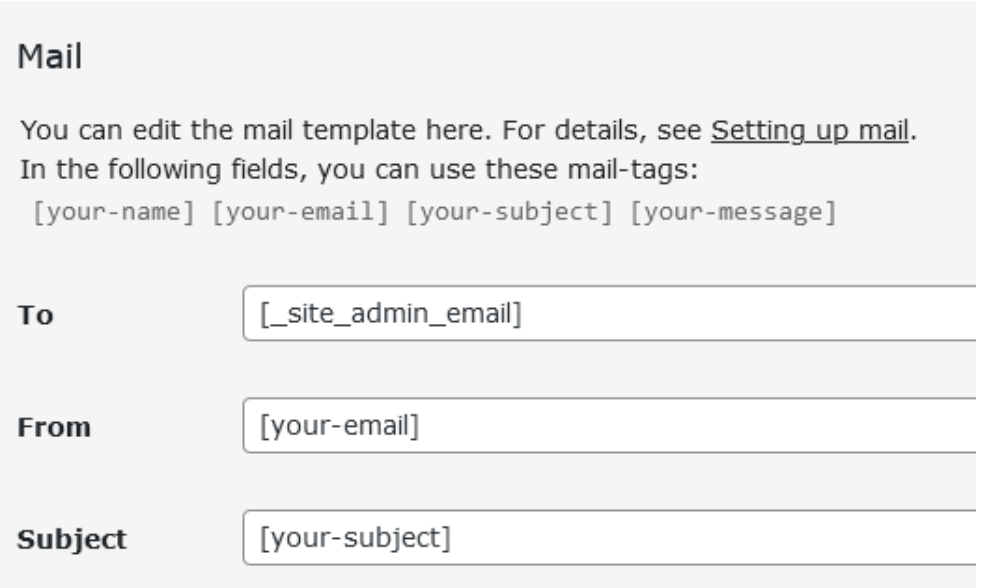
Heuristic (1)

1. Can send email
   - E.g. GCP cannot
2. Either:
   i. Not check what the sending domain is ***or***
   ii. Not check when adding a domain whether the holder of a domain authorised it



Heuristic (2)

- Look in the FAQ/KB
- It is easy to get wrong accidentally
- … hence webhosters are hesitant to change



How to solve it?

- Push the third-party to fix it
- Switch providers

- This makes it difficult to solve for some organisations

The disclosure process

The disclosure at webhosters

- One implemented fixes
- One required us to sign an NDA (we declined)
- The others: “intended behaviour”
  - “Leveranciersmanifest” of the Netherlands Standardisation Forum
  - Veilig Email Coalitie

- Hence we notified the impacted organisations themselves

Who was impacted?

In the Netherlands

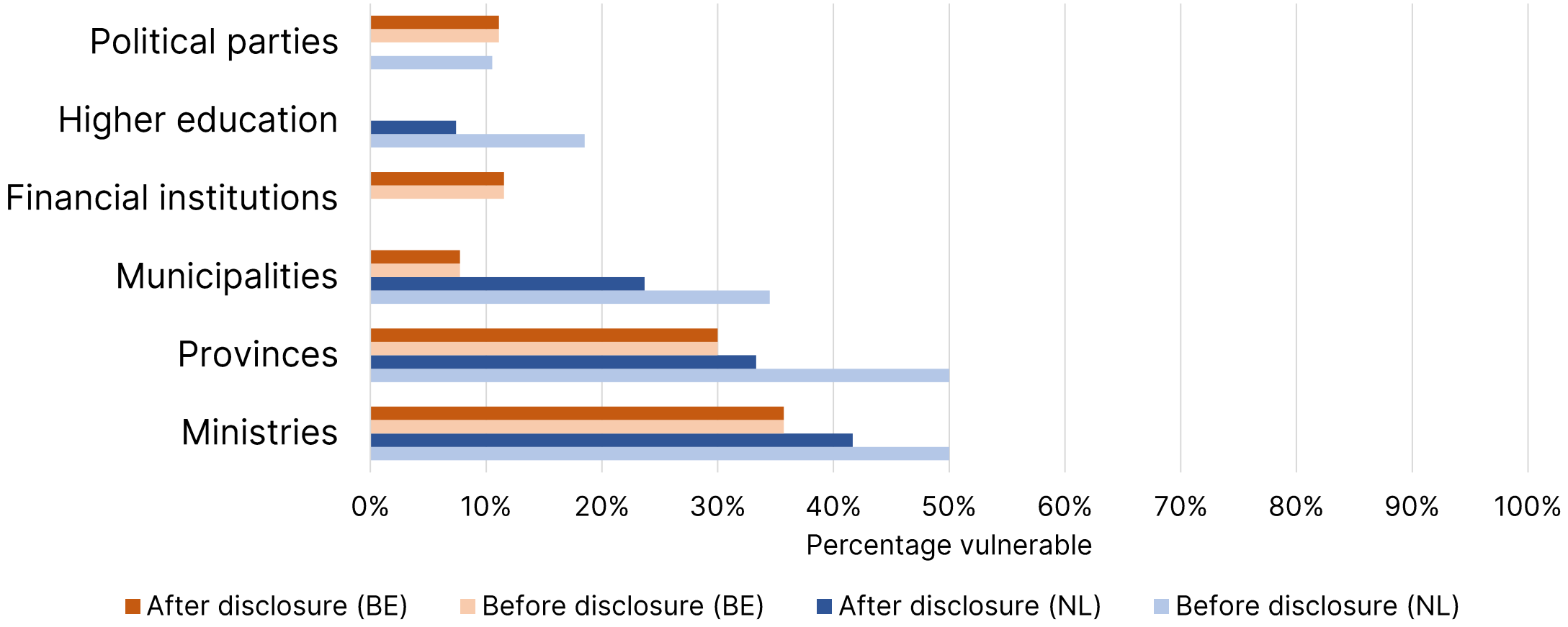
- 114 out of 342 municipalities
- 6 out of 12 provinces
- 6 out of 12 ministries

In Belgium

- 45 out of 581 municipalities
- 3 out of 10 provinces
- 5 out of 14 ministries

+ Multiple banks, hospitals, universities, ZBOs, NGOs, media, etc.

Was it solved?



Disclosure tales

Large financial institution in Belgium

Disclosure tales

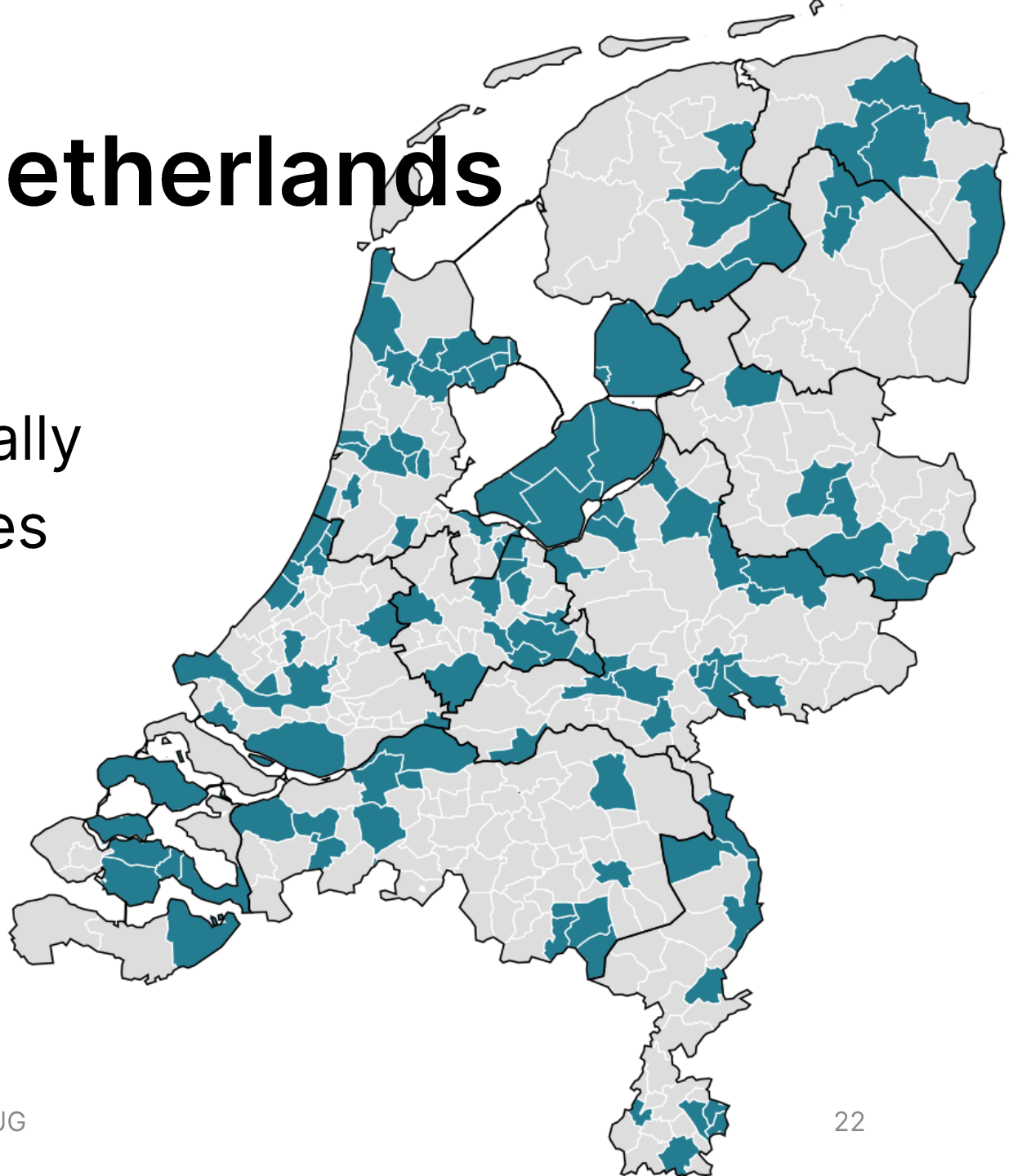
Belgian federal government

Disclosure tales

Large financial institution in Belgium

Let’s focus on the Netherlands

- Initial report to the NCSC-NL
- Report to the provinces manually
- Reported it to the municipalities



What happens in practice

- We get replies and problems are solved

What happens in practice

- Contact addresses were unaware that they were the contact address

What happens in practice

- Forms and procedures were not working

[redacted]

Later verder gaan Afdrukken Help

Melding van een kwetsbaarheid (CVD)

1. Melding

Het formulier, dat u wilt invullen, is (momenteel) niet beschikbaar.
Neem voor meer informatie contact op met de gemeente [redacted]

Afsluiten

- Ga naar website gemeente [redacted]

Office 365

Your message to the Microsoft 365 group ciso@[redacted] couldn't be delivered.

The group ciso isn't set up to receive messages from [redacted]

[redacted]	Office 365	ciso
Sender		**Action Required**
		Sender not allowed

What happens in practice

- DigiD logins everywhere

			Persoon									Adres					Ouders					(ex)Partner							Kinderen			Document		Kiesrecht		Registratie		
Datum	Manier van verstrekken	A V	BSN	Naam	Geboorte	Geslacht	Verblijfsrecht	Nationaliteit(en)	Gezag	Curatele	Contact gegevens	Inschrijvingsgemeente	Adres	Emigratie/adres buitenland	Immigratie	Aangifte adres	BSN ouder	Naam ouder	Geboorte ouder	Geslacht ouder	Datum ouderschap	BSN partner	Naam partner	Geboorte partner	Geslacht partner	Sluiting	Ontbinding	Soort verbintenis	BSN kind	Naam kind	Geboorte kind	Paspoort/id-kaart	Signalering	Nederlands kiesrecht	Europees kiesrecht	Brondocument	Geldigheidsdatum	Datum opname
Gemeente [redacted]/Algemene gemeentetaken [redacted]																																						
21-12-2022	Op verzoek	4	x	x	x	x	x					x	x	x			x	x					x						x	x								
	Wijziging	1	x	x	x	x						x	x	x									x			x	x											
Gemeente [redacted]/Algemene gemeentetaken [redacted]																																						
22-02-2023	Op verzoek	1	x	x	x	x	x			x		x	x	x			x	x	x			x	x	x		x	x		x	x	x							
27-02-2023	Op verzoek	1	x	x	x	x	x			x		x	x	x			x	x	x			x	x	x		x	x		x	x	x							
	Wijziging	1	x	x	x	x						x	x	x									x			x	x											
03-03-2023	Wijziging	1	x	x	x	x						x	x	x									x			x	x											
08-03-2023	Op verzoek	1	x	x	x	x	x			x		x	x	x			x	x	x			x	x	x		x	x		x	x	x							
28-06-2023	Wijziging	1	x	x	x	x						x	x	x									x			x	x											
29-06-2023	Op verzoek	1	x	x	x	x	x			x		x	x	x			x	x	x			x	x	x		x	x		x	x	x							
Gemeente [redacted]/Algemene gemeentetaken [redacted]																																						
11-11-2022	Op verzoek	2	x	x	x	x	x	x	x	x		x	x	x	x		x	x	x			x	x	x		x	x		x	x	x						x	x
Gemeente [redacted]/Algemene gemeentetaken [redacted]																																						
23-02-2023	Op verzoek	2	x	x	x	x	x	x	x	x		x	x	x	x		x	x	x			x	x	x		x	x		x	x	x						x	x

What happens in practice

- 11 out of the 114 requested my data from the Personal Records Database (BRP)
- 9 requested data from my parents as well

The TOPdesk saga

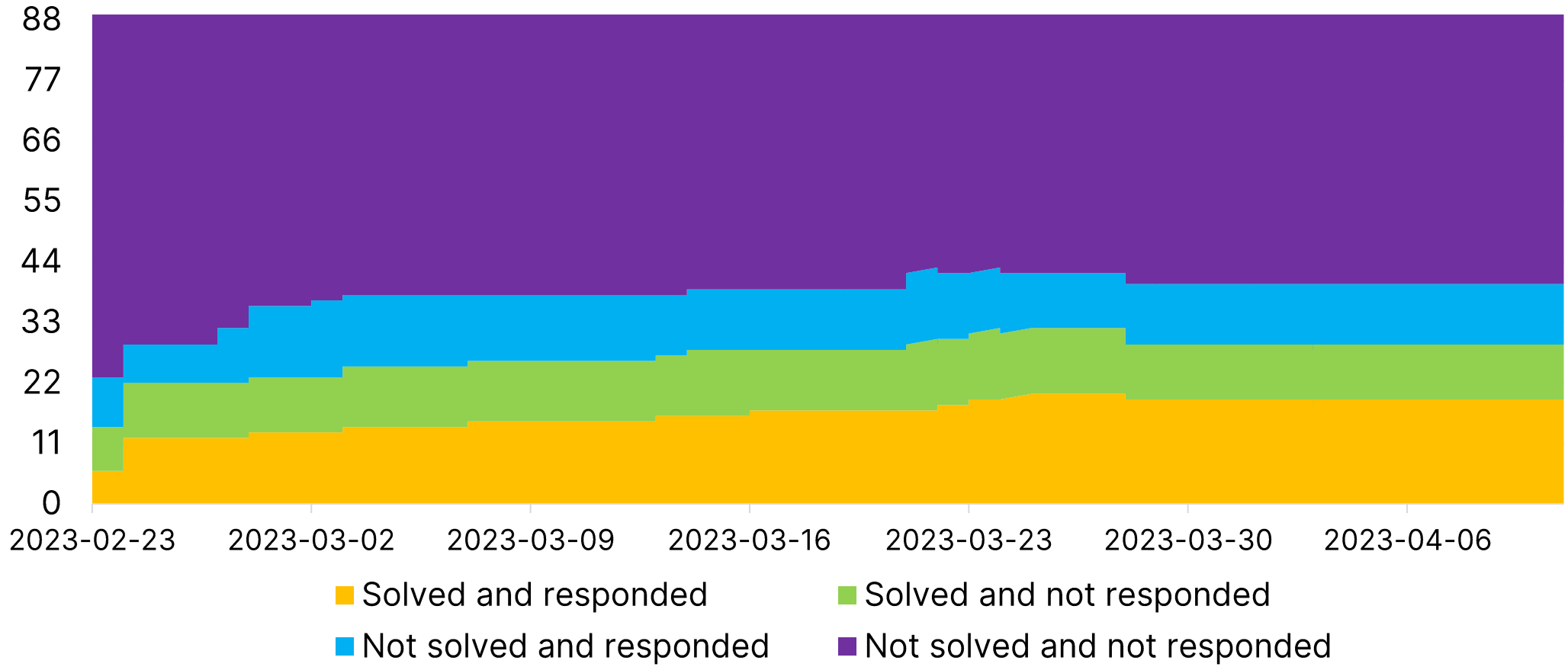
- During the initial disclosure, one of the disclosees realised that this works with TOPdesk as well
- TOPdesk is service management software often used as SaaS
- Can send email through its own infrastructure

The TOPdesk saga (2)

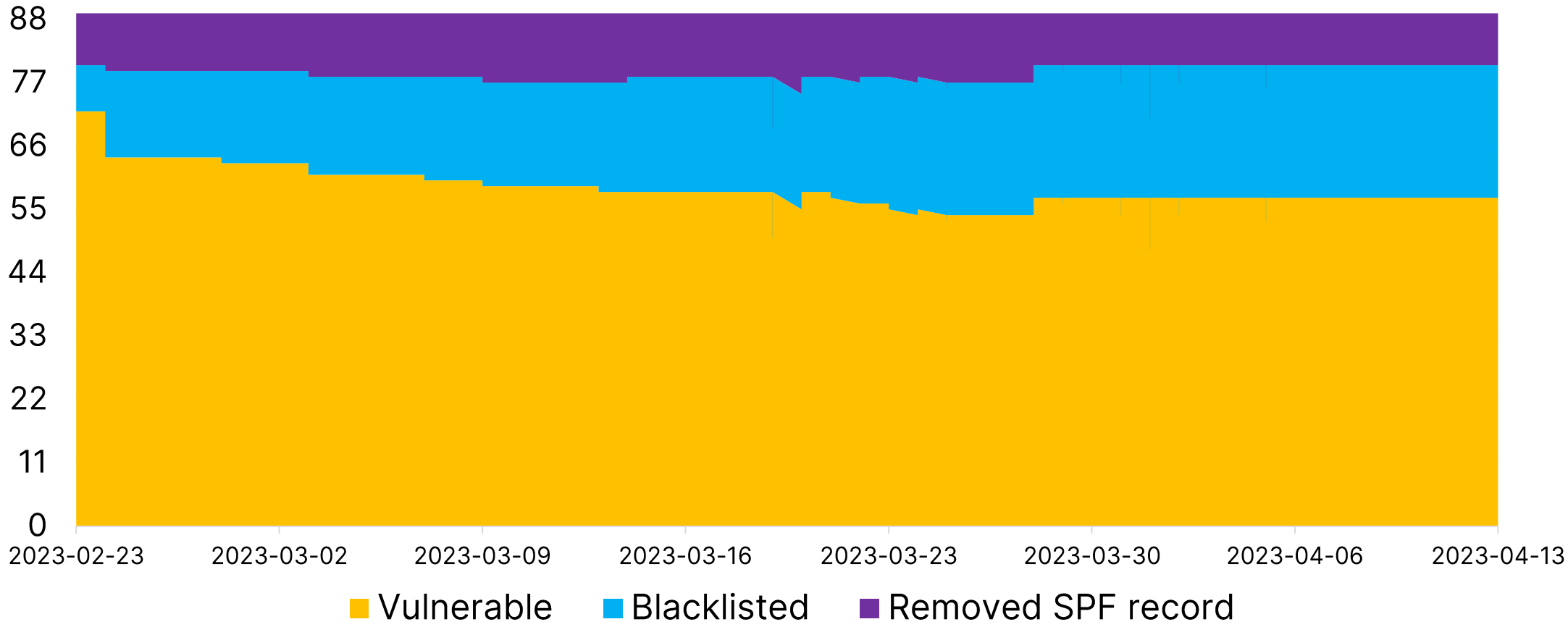
- By default TOPdesk allows any address
- An organisation can request that their domain can only be used from their tenant (KI 11992)
- TOPdesk states that this is by design
- 75% of municipalities had not requested this before disclosure
- We can scan whether this has been requested

- We kept track of the responses of 88 municipalities

TOPdesk solved over time



TOPdesk type of mitigation

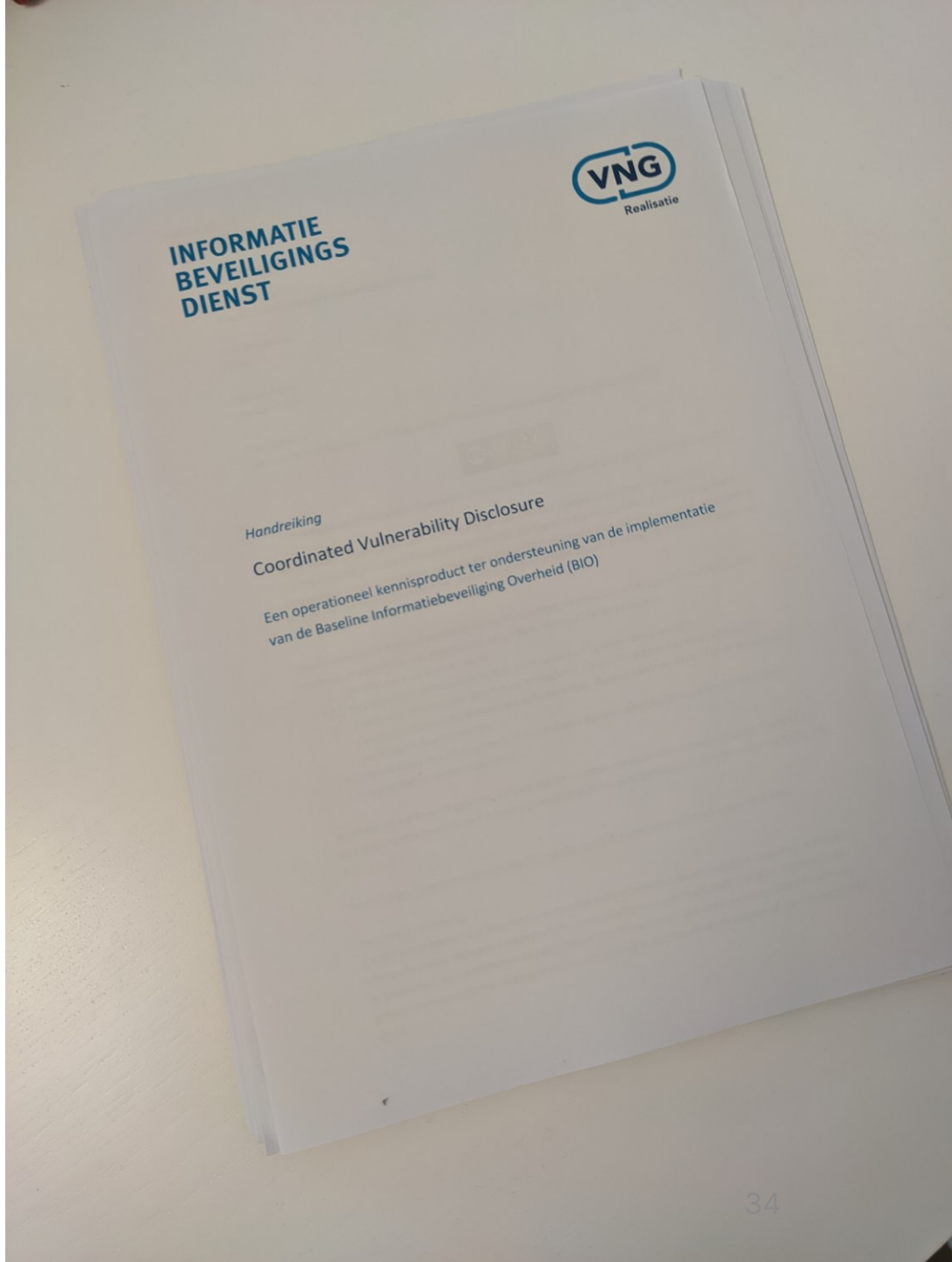


Policy and practice

- Freedom of Information (WOO) request
- To 114 municipalities requesting their policy, communications, and evaluations on CVD.
- Formatted to reduce the effort for municipalities as much as possible

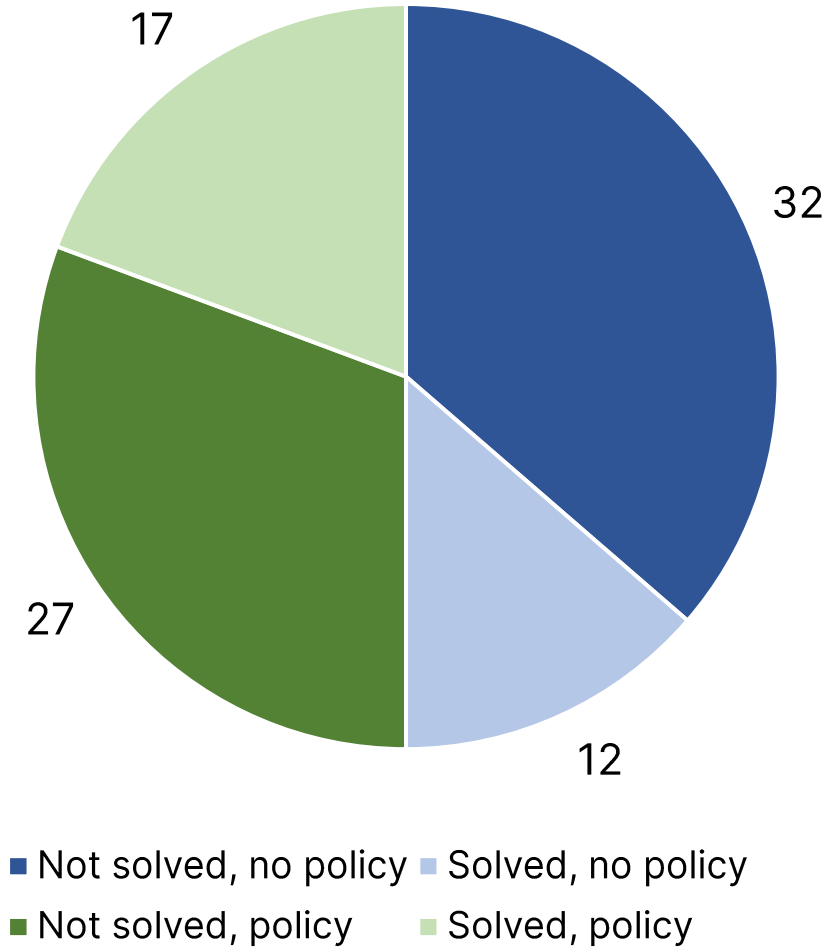
Why policy?

- Baseline Informatiebeveiliging Overheid (BIO)
- In effect since January 2019
- IBD made a template for complying with this requirement



Policy vs Practice

- Over half of the municipalities have no CVD-policy
- Over half of those who do did not solve the vulnerability
- We found no strong correlation between policy and practice



Other points from the WOO request

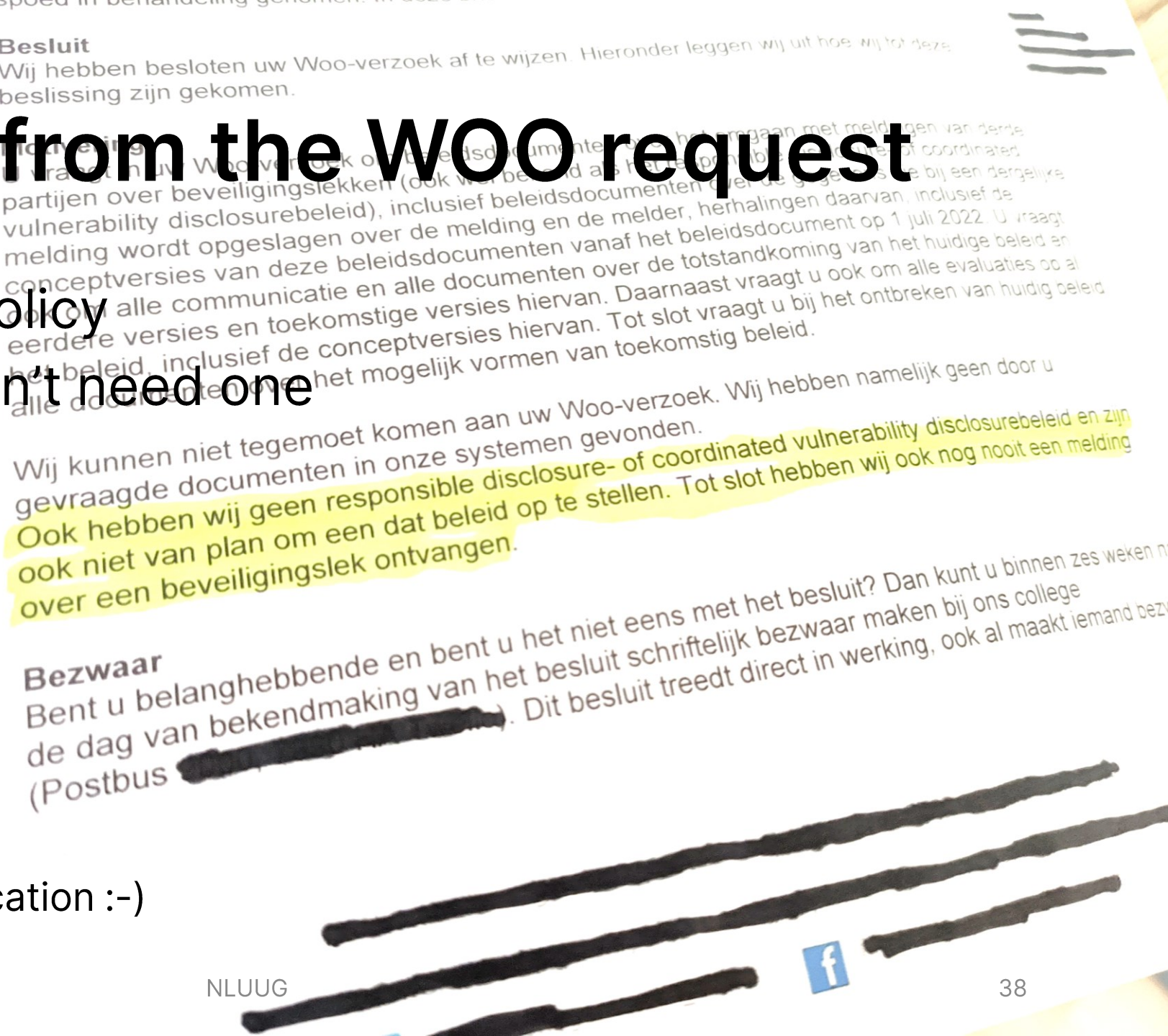
- No communication about DigiD

Other points from the WOO request

- Several municipalities will now implement policy after receiving the WOO request

Other points from the WOO request

- Most still have no policy
- Some claim they don’t need one



I definitely sent them a notification :-)

Other points from the WOO request

- Next to no evaluations of the current policy

Points from the GDPR-requests

- BRP-requests are in no policy

- Most common reason: to enter in the “zaaksysteem”
- Likely not GDPR-compliant
- Some municipalities cannot find any trace of it happening
- Is being resolved by several municipalities

Recommendations

- Test your CVD policy
- Communicate
- Only necessary information

Summary

- I found a vulnerability allowing me to send email on behalf of organisations
- I reported that to the organisations
- The Netherlands does a lot better than its neighbours
- … but there is still room for improvement
- Have policy and follow it

Koen van Hove

koen@nlnetlabs.nl

- **Questions?**

NLNETLABS

UNIVERSITY OF TWENTE.

DIVD