# Pēcpusdienas saruna: E-pasta drošība

Armīns Palms

27.03.2025

CERT.LV
Kiberincidentu novēršanas institūcija

# Kāpēc par to jādomā?

- E-pasts – viens no populārākajiem uzbrukuma vektoriem
- Informācija e-pastā
- Servisi, kur izmantojam e-pastus

CERT.LV

# E-pasta piegāde

SMTP – 45 gadi

```
250-8BITMIME
250-DSN
250 CHUNKING
MAIL FROM: <info@[redacted]lv>
250 2.1.0 Ok
RCPT TO: <[redacted]@inbox.lv>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: <info@[redacted].lv>
To: <[redacted]@inbox.lv>
Subject: Svariga vestule
Date: Sat, 22 Mar 2025 16:35:39 +0200
Message-ID: <1a34a6759a5cd_a91217113c8a675@[redacted]lv>
Ladien!

                                    inojums

Ar cienu
Vards Uzvards

Saudzejiet dabu, neprintejiet so vestuli
.
250 2.0.0 Ok: queued as 4ZKhfq6zsyzPjf8
```

klēt mapē

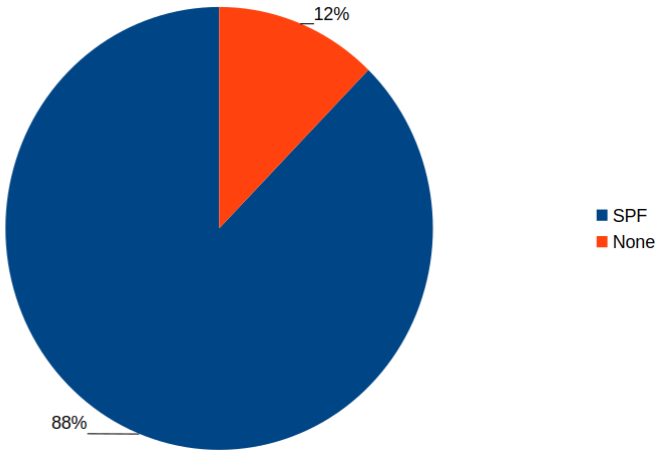
16:36 info@[redacted].lv Svariga vestule

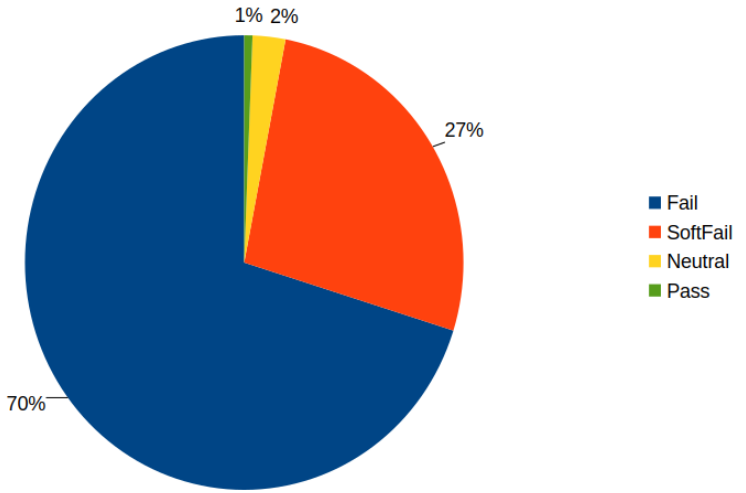
16:14 support@inbox.lv Jauna pierakstīšanās (Latvija) Jūsu e-pastā

CERT.LV

# SPF, DKIM, DMARC

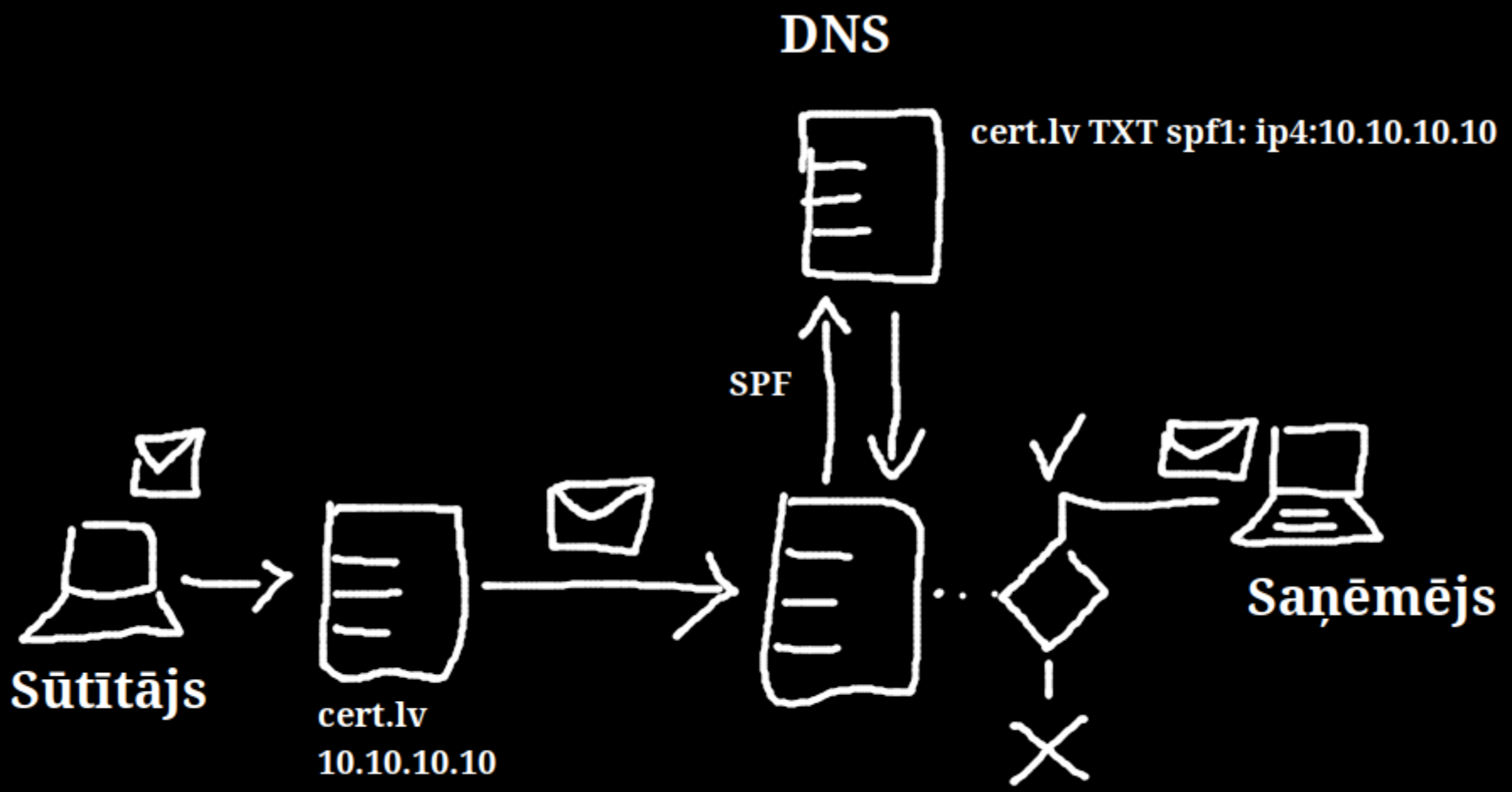
## Sender Policy Framework




```
$ dig cert.lv TXT +short
"v=spf1 mx include:spf.protect.sigmanet.lv ip4:85.254.193.0/24 ip4:193.174.13.200 ip4:145.0.2.40 ip4:38.111.193.7 -all"
```

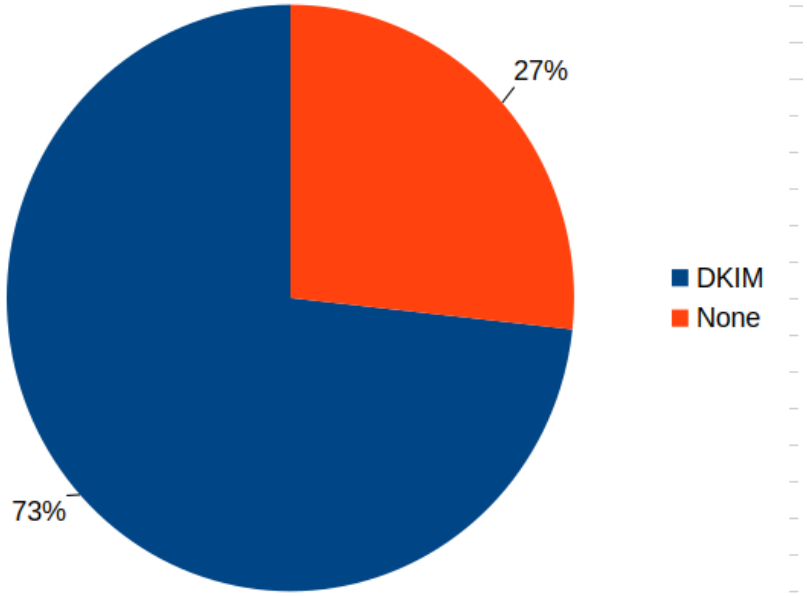
# SPF


DNS
cert.lv TXT spf1: ip4:10.10.10.10
SPF
Sūtītājs
cert.lv
10.10.10.10
Saņēmējs

CERT.LV

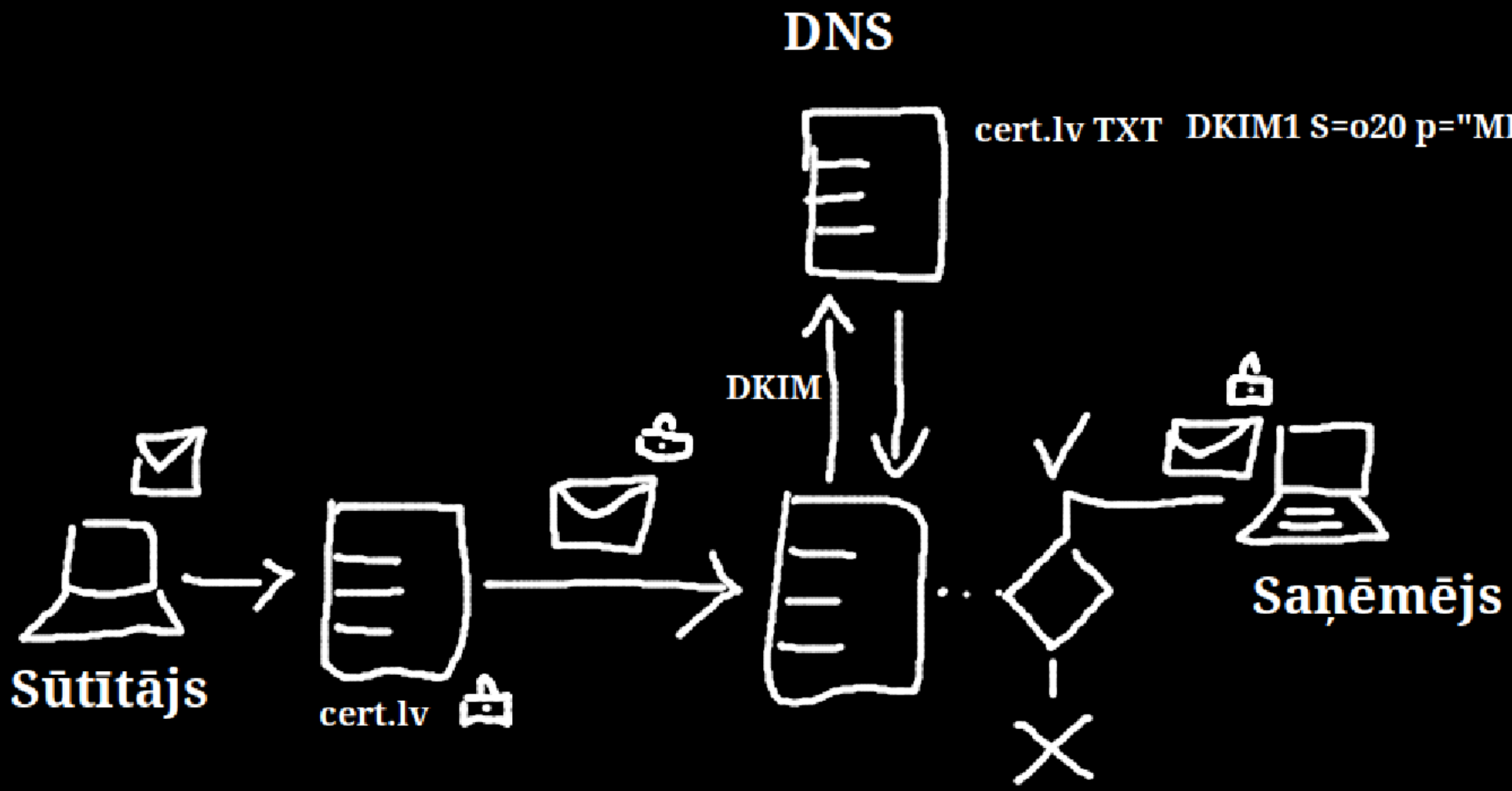
# SPF, DKIM, DMARC

## DomainKeys Identified Mail




```
$ dig o20._domainkey.cert.lv TXT +short
"v=DKIM1; h=sha256; k=rsa; " "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmHvxo4Q0JhuPgF2t31kNNNVbuOaVzkFUNYln//eEZjGXsEnY
vFUD86MYLZQMVAh+PgoEOSuUABWJC+S+mRVV5oueXTzz5o7qRBAPZ0bVldhyBtJpIvqbaU8vGW5ZXY94hZV5FZR85vAILOfMKCHbWCivB21MnhAg/3p+/OQeyPeu
9q8+KLAr8WaxBrLudwGcVUI3PkxBquo9Ig" "bqhyk9c9Z/OPTWFxZl8UJdpq/dLNwOTKW/jwdRr3Eh8+jMEep1KvVbqwax00QCWQQa1ZP1DMa2JYRRWNH+pXpiI
nZmrXSmf3MZrvRa3GcLkJ5LAxr1T8boJW2VkGO7e79eBQo4jwIDAQAB"
```

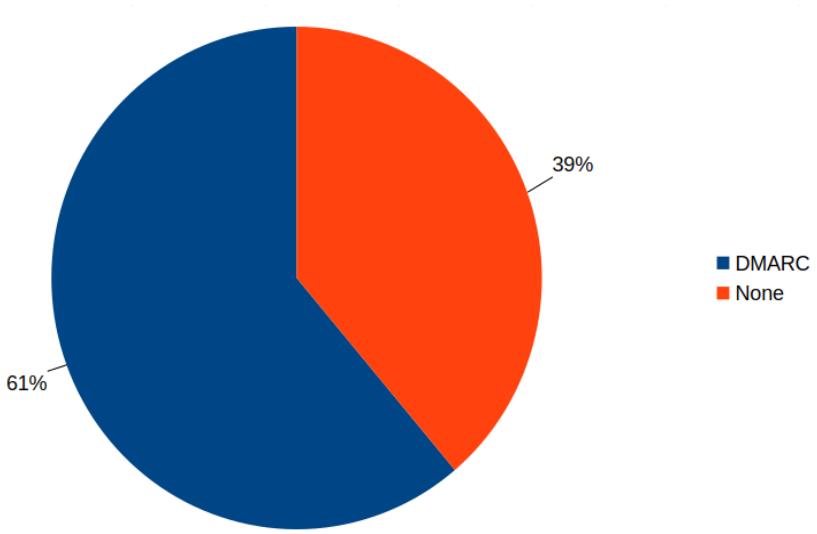
# DKIM


DNS
cert.lv TXT DKIM1 S=o20 p="MIIB...
DKIM
Sūtītājs
cert.lv
Saņēmējs

CERT.LV

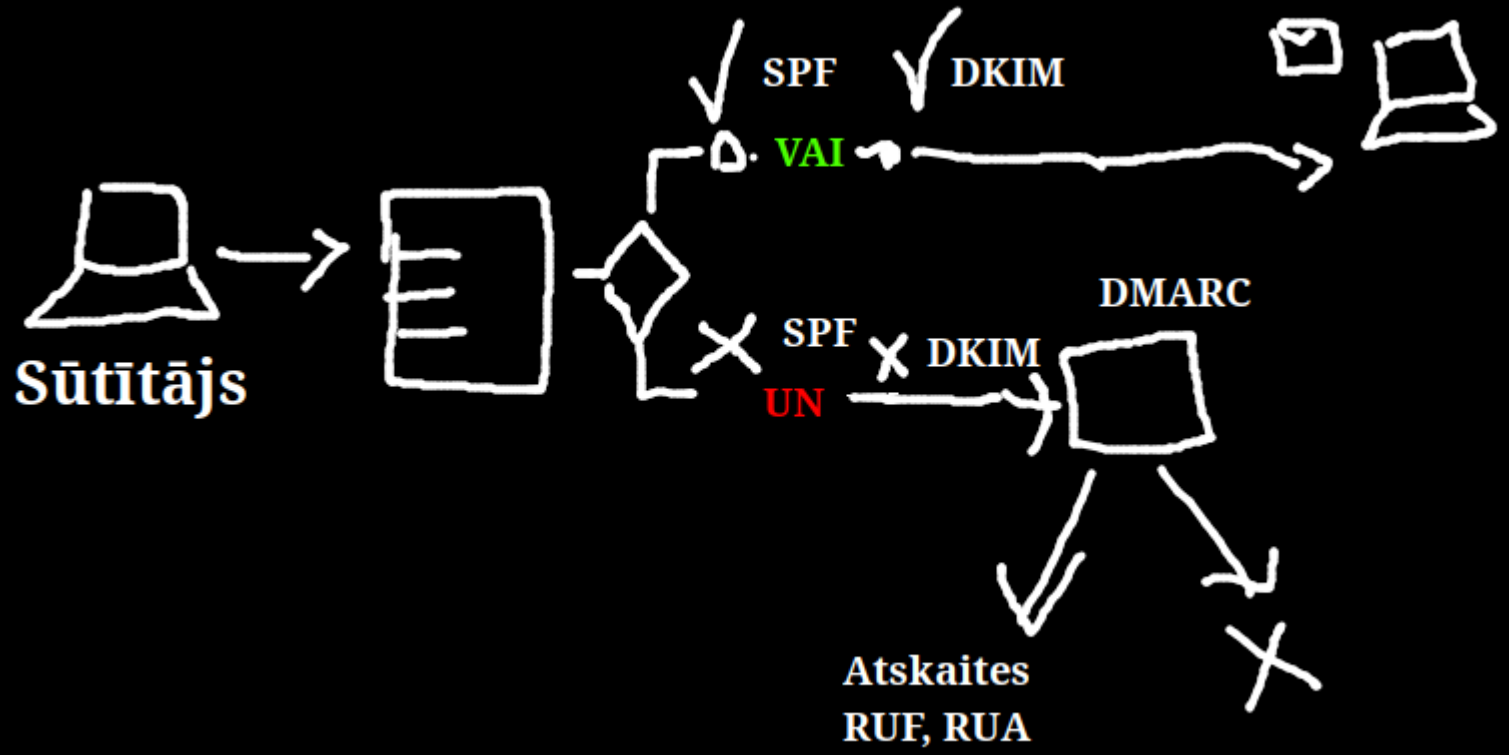
# SPF, DKIM, DMARC

## Domain-based Message Authentication, Reporting, and Conformance




```
$ dig _dmarc.cert.lv TXT +short
"v=DMARC1; p=reject; rua=mailto:d+vr3ddrq2@dmarc.lv; ruf=mailto:f+vr3ddrq2@dmarc.lv; pct=50;
 fo=1;"
```

# DMARC

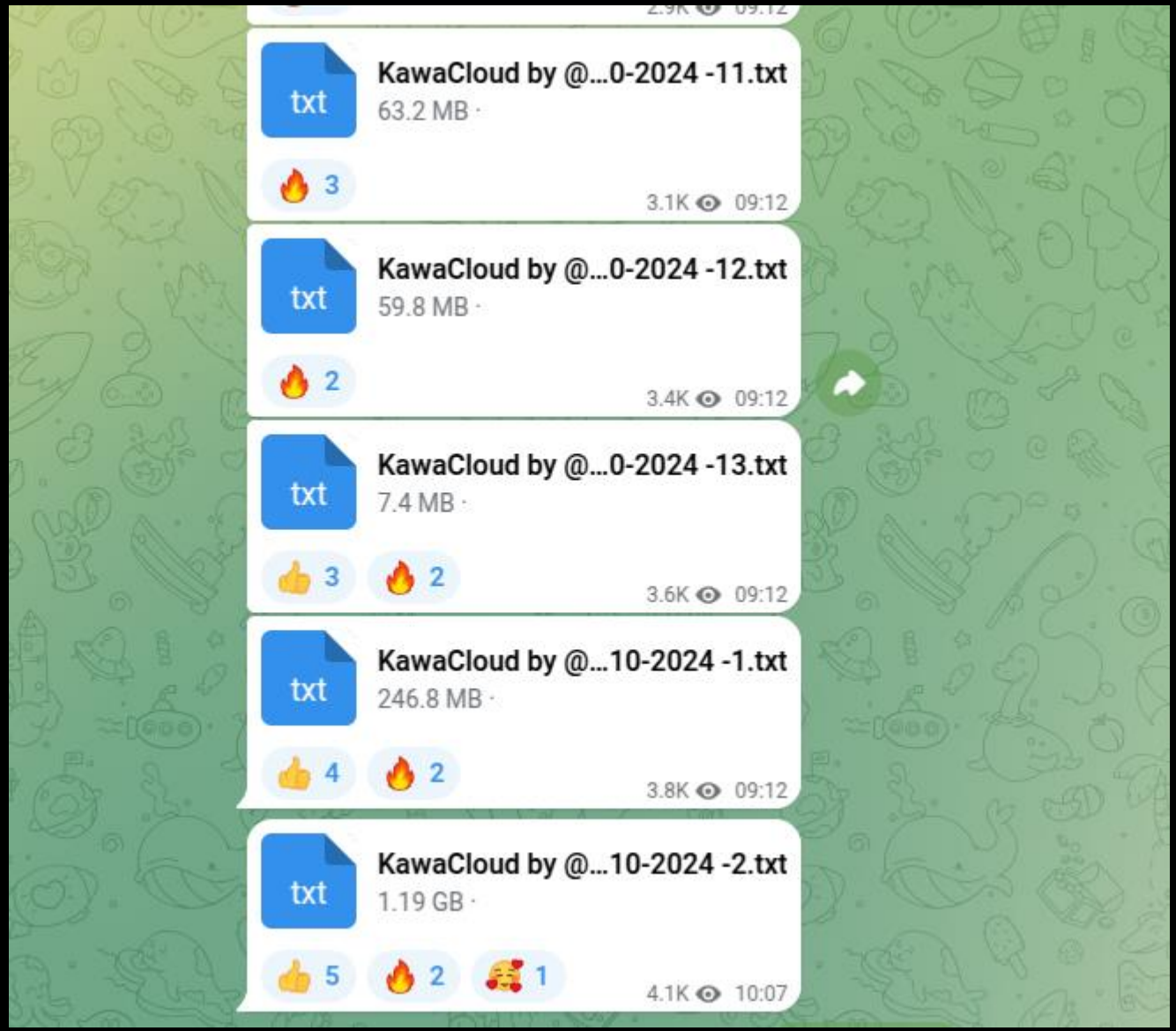


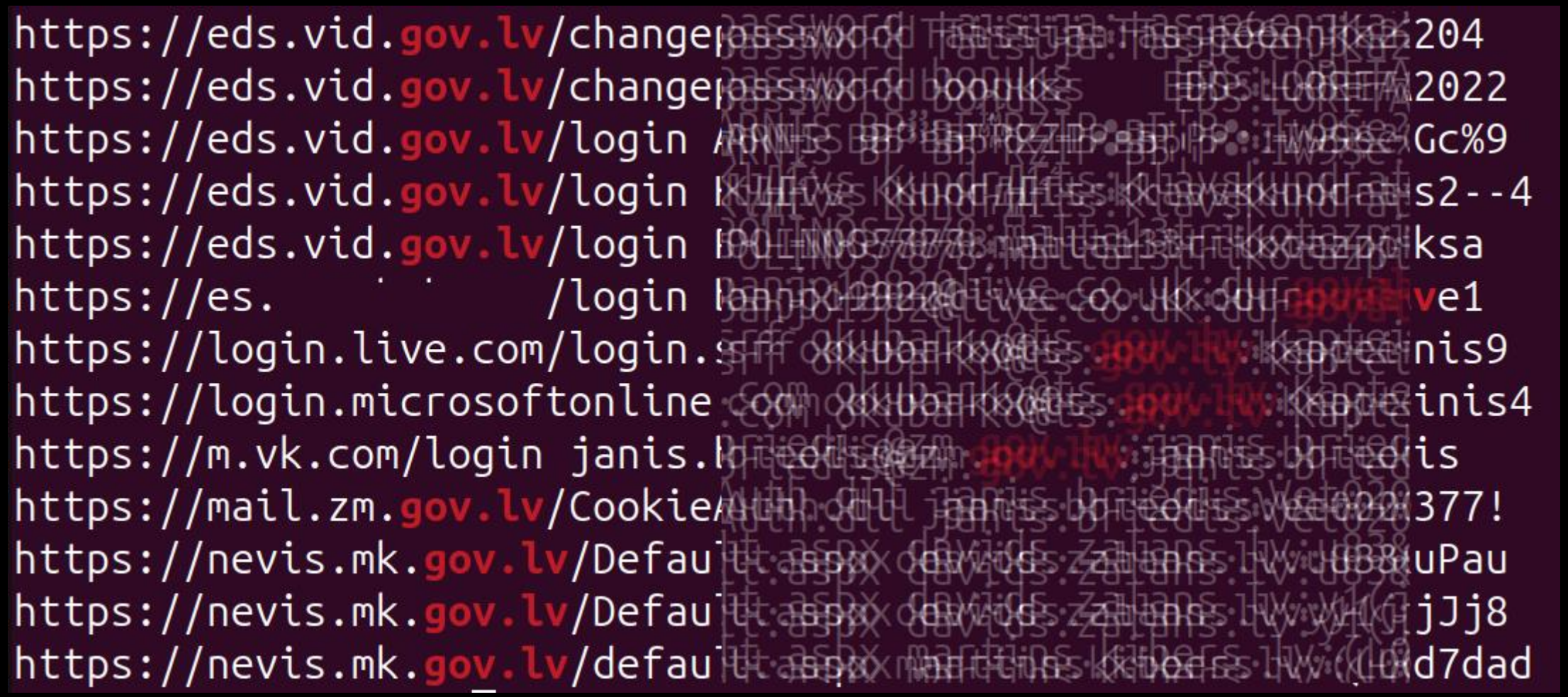
CERT.LV

# 2FA

- Lielāka drošība
- Monitorings par sekmīgām autentifikācijām
- Jālieto VISUR!

CERT.LV

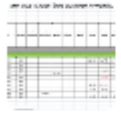

txt
KawaCloud by @...0-2024 -11.txt
63.2 MB ·
3
3.1K 09:12
txt
KawaCloud by @...0-2024 -12.txt
59.8 MB ·
2
3.4K 09:12
txt
KawaCloud by @...0-2024 -13.txt
7.4 MB ·
3
2
3.6K 09:12
txt
KawaCloud by @...10-2024 -1.txt
246.8 MB ·
4
2
3.8K 09:12
txt
KawaCloud by @...10-2024 -2.txt
1.19 GB ·
5
2
1
4.1K 10:07


https://eds.vid.gov.lv/change
https://eds.vid.gov.lv/change
https://eds.vid.gov.lv/login
https://eds.vid.gov.lv/login
https://eds.vid.gov.lv/login
https://es. /login
https://login.live.com/login.
https://login.microsoftonline
https://m.vk.com/login janis.
https://mail.zm.gov.lv/Cookie
https://nevis.mk.gov.lv/Defau
https://nevis.mk.gov.lv/Defau
https://nevis.mk.gov.lv/defau

CERT.LV

53 KB ·

**mainline2.png**
101 KB ·

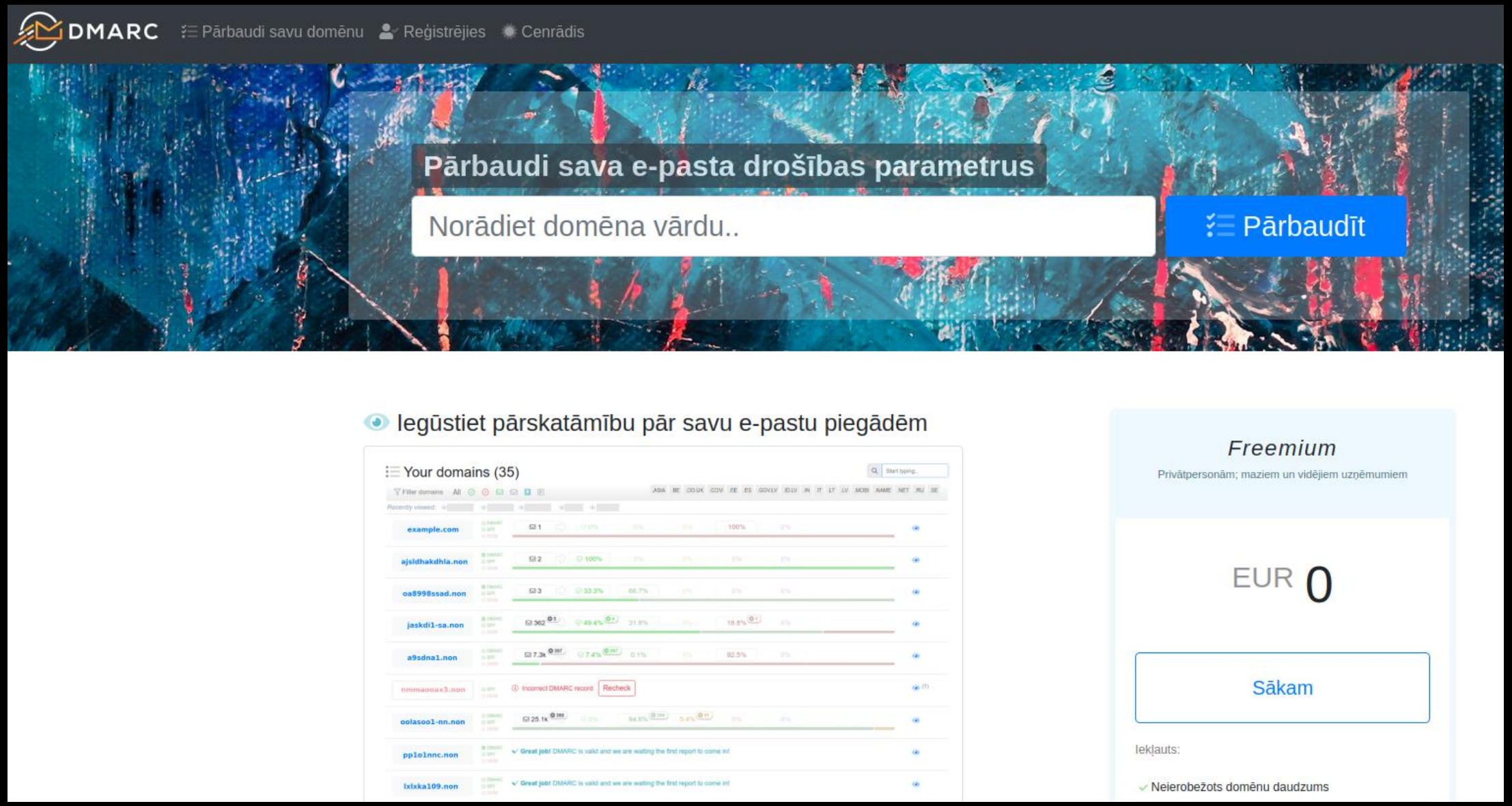


**goodies1.png**
60 KB ·

**goodies2.png**
97 KB ·

Нами в рамках акции была проведена операция по денацификации Министерства Внутренних Дел Латвии (iem.gov.lv).
Всё серьёзно.
Публикуем доказательства в виде скриншотов:
1) Почтовые адреса, внутренние документы, все переписки у нас. на приложенных скриншотах вы можете увидеть несколько ящиков (первые три)
2) Писем (четвертый о заместителе директора, пятый о проведении внутреннего собрания в Риге)
3) Несколько внутренних документов: график отпусков отдела правового управления и информация об автомобилях, используемых сотрудниками МВД Латвии (номера, марки)

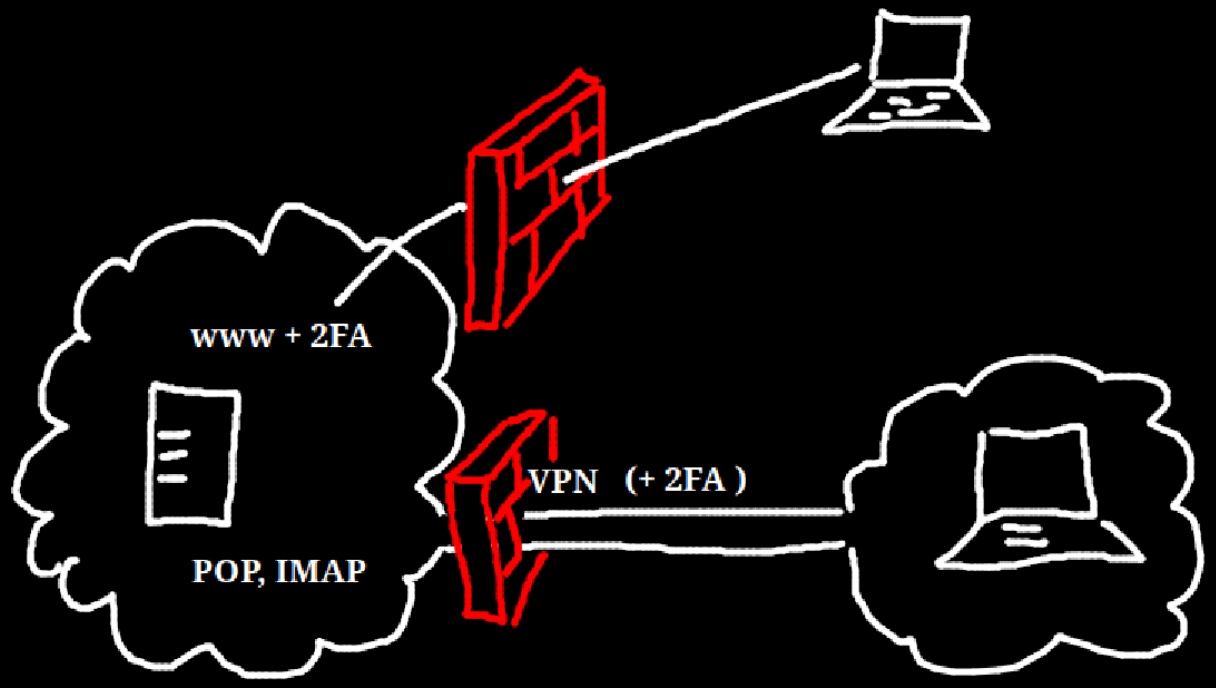
# https://dmarc.lv



CERT.LV

# POP, IMAP, WEB

- Jāizvērtē, kā resursi eksponē internetā
- IMAP, POP pēc dizaina neatbalsta 2FA
- Jāierobežo piekļuve, ja nav 2FA


www + 2FA
POP, IMAP
VPN (+ 2FA )

# Atļautais | | aizliegtais saraksts

AS44477 (IPv4: 283,392 )

- STARK INDUSTRIES SOLUTIONS LTD

AS199785 (IPv4: 7,680 )

- Cloud Hosting Solutions, Limited

- Baltais saraksts ar uzticamiem tīkliem ko lieto paši

# SPAM

- CERT.LV interesē SPAM ar pielikumiem un saitēm
- Ir izveidots īpašs serveris automātiskā SPAMa sūtīšanai
- cert@cert.lv

CERT.LV

# AR KIBERDRAUGIEM

# PRET KIBERDRAUDIEM

CERT.LV

# Paldies

@cert.lv