# Verifying email security techniques for Dutch organizations

**Student: Vincent van Dongen**

**Supervised by: Ralph Dolmans, George Thessalonikefs (NLnet Labs)**

**Security and Network Engineering (UvA)**

Master Thesis, 3 July 2018

# Introduction 1/2

Security hasn't taken into account during the design of email protocols.

- Different techniques have emerged to secure email.
- Governments have defined guidelines to implement these techniques.
- You can check if these techniques have been implemented.

*How many email security techniques have been implemented for organizations within the Netherlands?*

Is there a distinction between:

- The size of an organization.
- Geographical location.
- The type of sector.

# Introduction 2/2

- Related work:
  - Previous research has been done on verifying email security techniques.
  - NLNet Labs has build a tool check if the email security techniques have been implemented.
- Scope:
  - Only Dutch organization will be verified for this research.
- Approach:
  1. Define which techniques will be verified.
  2. Create a data-set of Dutch organizations.
  3. Use the data-set as input for the experiment.
  4. Discuss the results of the experiment
  5. Answer research questions.

# Background information

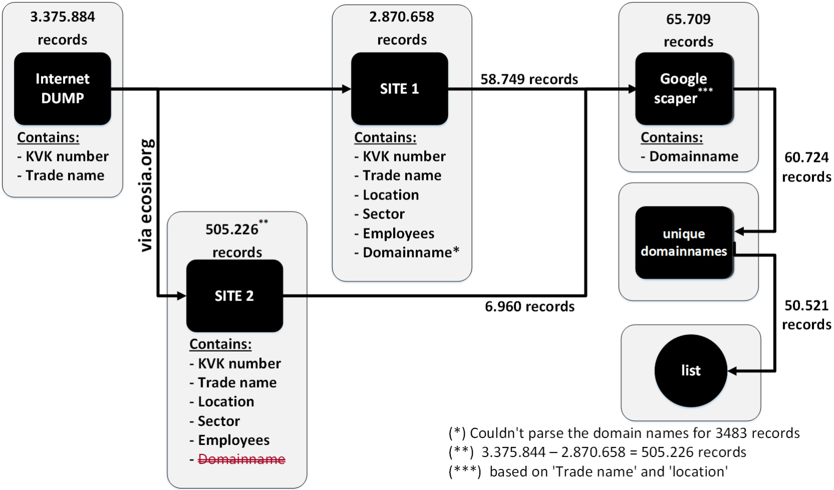
The Dutch Standardization Forum has defined a list of compulsory standards. 19 different techniques will be checked during the experiment:

| Category | Checks for | Purpose |
|---|---|---|
| SPF | Record available | Detects email spoofing |
| | Policy | |
| DKIM | Record available | |
| DMARC | Record available | |
| | Policy | |
| DNSSSEC | Signed domain | Protects users from forged DNS data |
| | Secure domain | |
| | Signed mx record | |
| | Validate signed mx record | |
| DANE | Record available | Authenticate TLS clients and servers |
| | Valid record | |
| STARTTLS [1] | Supports | Creates an encrypted connection |
| | TLS version | |
| | Cipher suites | |
| | Trust chain of certificate | |
| | TLS compression | |
| | Public key of certificate | |
| | Signature of certificate | |
| | Domain name on certificate | |

[1] Guidelines for TLS: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

# Collecting the data-set

| KVK-number | Trading name | Location | Sector | Employees | domainname |
|---|---|---|---|---|---|



3.375.884 records

Internet DUMP

Contains:
- KVK number
- Trade name

via ecosia.org

2.870.658 records

SITE 1

Contains:
- KVK number
- Trade name
- Location
- Sector
- Employees
- Domainname*

505.226** records

SITE 2

Contains:
- KVK number
- Trade name
- Location
- Sector
- Employees
- ~~Domainname~~

58.749 records

6.960 records

65.709 records

Google scaper***

Contains:
- Domainname

60.724 records

unique domainnames

50.521 records

list

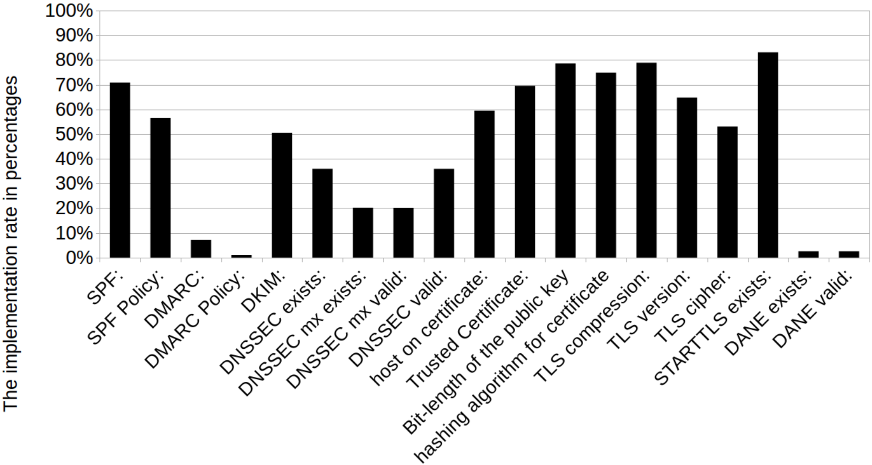
(*) Couldn't parse the domain names for 3483 records
(**) 3.375.844 – 2.870.658 = 505.226 records
(***) based on 'Trade name' and 'location'

# The experiment

- A tool from 'internet.nl' was used for the experiment.
- The tool queries the DNS server along with the SMTP server.
    - The domain names from the collected data-set were used as the input.
        - 50.521 domain names submitted via an API.
        - The experiment took approximately 4 days to complete.
        - The tool could not retrieve the mx record for 3871 domains.
        - Experiment succeeded for 46.650 domains.
        - Output was a 400 MB JSON file.

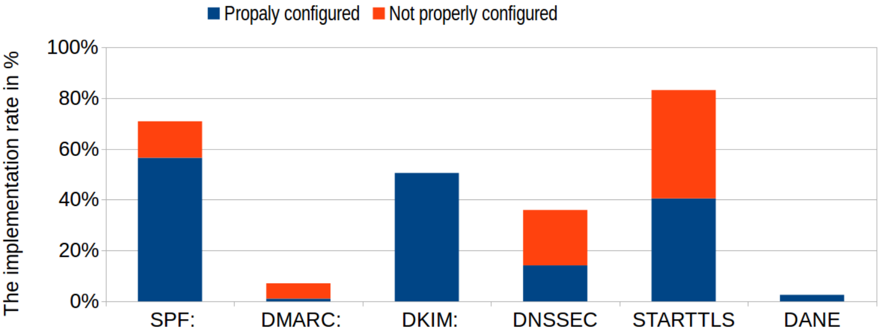
# Results: Overview 1/5

*How many email security techniques have been implemented for organizations within the Netherlands?*



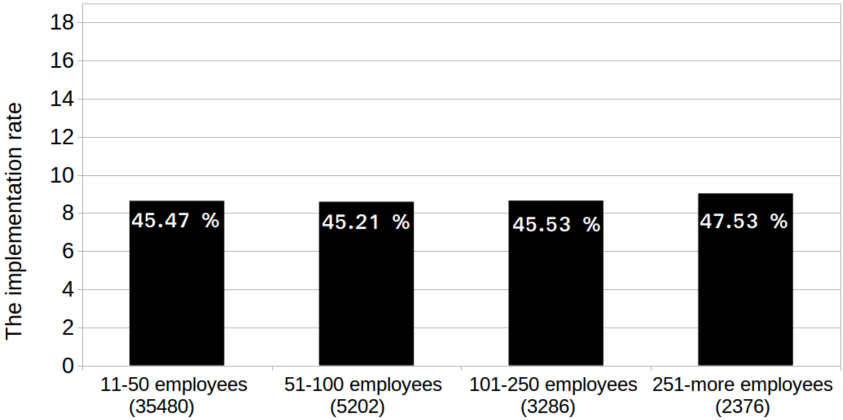
# Results: Overview 1/5

*How many email security techniques have been implemented for organizations within the Netherlands?*



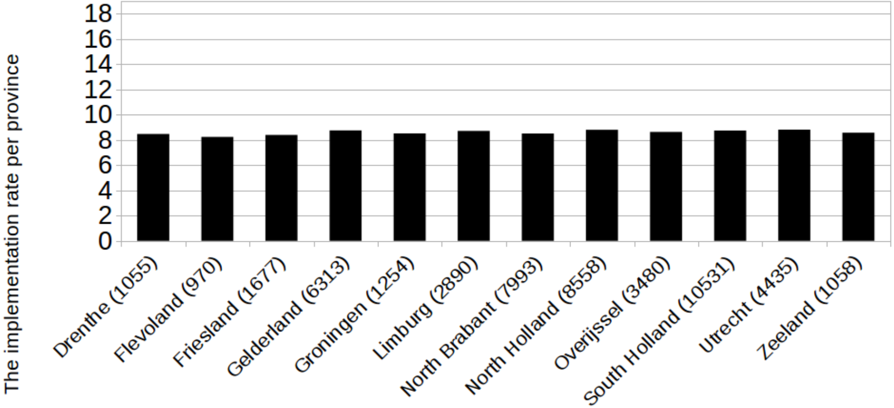
# Results: Number of employees 2/5

*Is there a distinction between small, medium and large organizations regarding the implementation of email security techniques?*

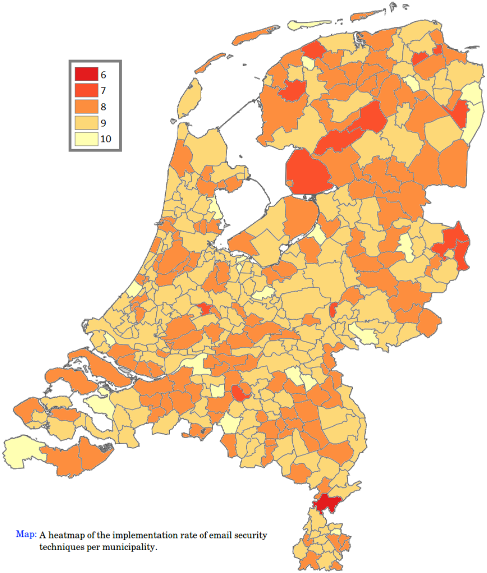


# Results: Geographical location 3/5

*Is there a geographical distinction between organizations regarding the implementation of email security techniques?*



# Results: Geographical location 3/5



Map: A heatmap of the implementation rate of email security techniques per municipality.

# Results: Type of sector 4/5

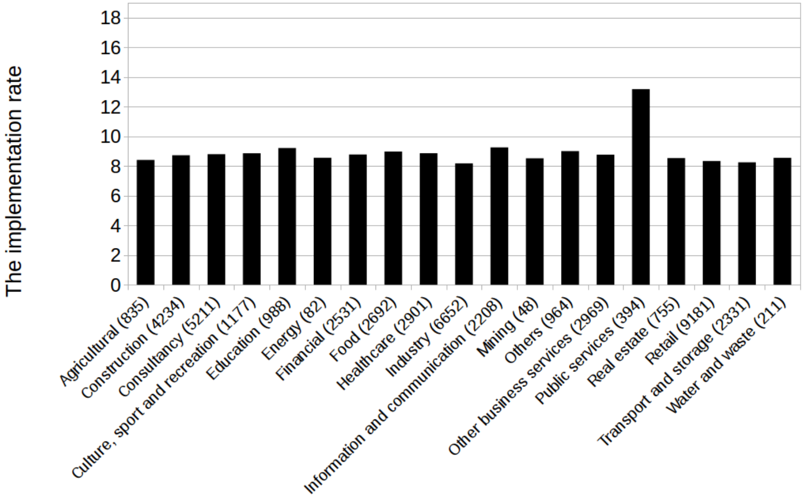
*Is there a distinction between the type of sector regarding the implementation of email security techniques?*

Type of sectors:

- Agricultural
- Construction
- Consultancy
- Culture sport and recreation
- Education
- Energy
- Financial
- Food
- Healthcare
- Water and waste
- Industry
- Information and communication
- Mining
- Others
- Other business services
- Public services
- Real estate
- Retail
- Transport and storage

# Results: Type of sector 4/5

*What type of sector has implemented the most and the least number of email security techniques?*



# Results: Other interesting findings 5/5

Interesting findings:

1. Top 1000 organizations (most employees) score an average of 9.30.
2. Organizations from AEX index have an average score of 10.32.
3. The subsector that has the lowest score is the 'Manufacture of aircraft parts' subsector with an average score of 3.2.

# Discussion

- **Remarks about the data-set**
  - 4985 organizations didn't contain a domain name.
  - Organizations with 1-10 employees were not validated.
  - The repository dates back to 2015.
- **Remarks about the experiment**
  - The tool didn't receive mx records for 3871 domains.
  - The tool could only check if a DKIM record is available.
- **Remarks about the results**
  - 8 of the 19 techniques were related to STARTTLS.
  - There might be only a few organizations present in a municipality and therefore strongly influence the average score.

# Conclusion

- Organizations have on average implemented 45 % of the email security techniques that have been defined by the Dutch 'Forum Standaardisatie'.
- We didn't find a relation between the number of employees or the geographical location in regarding the implementation rate.
- We did find a relation between the type of sector.
  - The 'Public Services' sector has the highest score.
  - Many governmental organizations are present in the 'Public service'.
  - We assume that the high score is related to compulsory policies.
- **Future work**
  - Investigate if there is a distinction between the owners of an IP-address or hosting provider related to the implementation rate.

*I would like to thanks Ralph Dolmans and George Thessalonikefs from NLnet Labs for supervising this research project.*