Research Project 1

How To Reduce The Risk Of Email Data Breaches

Research project by a student from the University of Amsterdam (SNE/OS3 master)
Nick Offerman (nick.offerman@os3.nl)
4-2-2019
Main research question:
* How to reduce the risk of email data breaches for the Ministry of Justice and Security in order to be more compliant with the General Data Protection Regulation?

Sub-questions:
* Why does the MJS want to implement a secure email solution?
* Which traditional email security protocols are available?
* Which secure email solution fits the MJS?
* Which technical challenges does a secure email solution bring for the IT architecture of the MJS?
News Articles

The Guardian  PlayStation Network hackers access data of 77 million users '11

Reuters  Yahoo says all three billion accounts hacked in 2013 data theft '13

The Hacker News  Ashley Madison to Pay $11.2 Million to Data Breach Victims '15

The Verge  T-Mobile was hit by a data breach affecting around 2 million customers '15

CSO  Hillary Clinton might have been a pretty good president had she used Pretty Good Privacy '16

Fortune  LinkedIn Lost 167 Million Account Credentials in Data Breach '16

The New York Times  Facebook Security Breach Exposes Accounts of 50 Million Users '18

ABS CBN News  Massive data leak targets German officials including Merkel '19
What is a Data Breach?

Norton: "A data breach is a security incident in which information is accessed without authorization."

GDPR: "Personal data is any information related to a person that can be used to identify them."

Image by TechTarget, Source: https://cdn.tgtmedia.com/rms/onlineImages/data_management-gdpr_personal_data.png
Why does the MJS want to implement a secure email solution?

- European Privacy Law
- Data Breaches per Sector
- Root Causes of Data Breaches
- Email (threat) overview
European Privacy Law

Google fined €50 million in 2019, due lack of transparency.

Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to be forgotten
Entities the data subject to have the data controller erase his/her personal data (and potentially third parties, too).

Right to access and portability
Users can inquire whether and how their personal data is being processed.

Mandatory data protection officers
Appointed in certain cases, to facilitate the company’s need to demonstrate GDPR compliance.

Image by OneLogin, Source: https://www.onelogin.com/assets/img/gdpr_diagram.png
Data Breaches per Sector

Reported Data Breaches per Sector 2018

- Healthcare: 29%
- Financial sector: 26%
- Government: 20%
- Business: 9%
- IT: 4%
- Education: 3%
- Remaining: 9%

Root Causes of Data Breaches

Types of Data Breaches 2018

- Wrong recipient 63%
- Post letter, or package 9%
- Device, data carrier, or paper 7%
- Hacking, malware or phishing 4%
- Personal data published by mistake 3%
- Wrong customer in customer portal 3%
- Remaining 11%

Email (threat) overview

Image by FH Münster University (2018), Source: https://fahrplan.events.ccc.de/congress/2018/Fahrplan/system/event_attachments/attachments/000/003/683/original/35c3-schinzel-efail.pdf
Which traditional email security protocols are available?

- Spam, Phishing, and Spoofing protection
- Hop-to-hop encryption
- End-to-end encryption
Threat: commercial advertising, identity theft, or fraud. How: business impersonation or even change 'FROM' header.

**SPF**: "Is this IP authorized to send email from this domain?".

**DKIM**: "Does this signature match the Public Key Record in DNS?".

**DMARC**:
- policies: accept, quarantine, or reject.
- reports: who sends to/from domain?
- ✓ used by all sectors of the MJS.
Hop-to-hop encryption

**STARTTLS**
- transport encryption based on certificates
- downgrade via MITM

DNS-based **Authentication of Named Entities (DANE)**
- checks authenticity of mailservers

- only encryption between mailservers
- can't enforce/guarantee security
- mandatory by the MJS, unless explained.
End-to-end encryption

Pretty Good Privacy (PGP)
- older, requires plugins.
- popular under individuals.

Secure/Multipurpose Internet Mail Extensions (S/MIME)
- popular under organisations.
- built into most email clients.

Not used by the MJS:
- impractical to facilitate key exchange for every company or end-user, while remaining both user friendly and secure.
- 'Bestandenpostbus' for classified documents, but most mail is sent plaintext.
Which secure email solution fits the MJS?

- Dedicated market solutions
- Product Comparison by RZCC
- ZIVVER vs Sophos SPX
Dedicated market solutions

- Public key distribution difficult to facilitate.
- Multiple dedicated market solutions originated.
- Prefer 1 dedicated market solution over multiple solutions (inefficient/management burden).
### Product Comparison by RZCC

<table>
<thead>
<tr>
<th>Feature</th>
<th>KPN Secure Mail</th>
<th>HPE SecureMail</th>
<th>Sophos SPX: SPX E-Mail Encryption</th>
<th>Zivver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling content</td>
<td>①</td>
<td>②</td>
<td>③</td>
<td>⑤</td>
</tr>
<tr>
<td>Signaling address errors</td>
<td>①</td>
<td>②</td>
<td>③</td>
<td>⑤</td>
</tr>
<tr>
<td>Hack protection</td>
<td>③</td>
<td>④</td>
<td>④</td>
<td>⑤</td>
</tr>
<tr>
<td>Authentication</td>
<td>②</td>
<td>③</td>
<td>③</td>
<td>⑤</td>
</tr>
<tr>
<td>Protection after sending</td>
<td>①</td>
<td>③</td>
<td>③</td>
<td>④</td>
</tr>
<tr>
<td>User awareness</td>
<td>①</td>
<td>③</td>
<td>③</td>
<td>⑤</td>
</tr>
<tr>
<td>Logging</td>
<td>②</td>
<td>④</td>
<td>⑤</td>
<td>⑤</td>
</tr>
</tbody>
</table>

# ZIVVER vs Sophos SPX

<table>
<thead>
<tr>
<th>ZIVVER</th>
<th>Sophos SPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud solution (TLS 1.2 client/server)</td>
<td>On premise: email to PDF encryption</td>
</tr>
<tr>
<td>Hybrid encryption: RSA-2048 &gt; AES-128</td>
<td>Symmetric AES-128/256 by end-user</td>
</tr>
<tr>
<td>Decrypt users private key with master key</td>
<td><strong>No master key (legislation e.g. fraud)</strong></td>
</tr>
<tr>
<td>Integration with AD/LDAP (objectGUID)</td>
<td>Sandbox option against attacks</td>
</tr>
</tbody>
</table>
Which technical challenges does a secure email solution bring for the IT architecture of the MJS?

- Email inspection
- Security Trade-off
FireEye scans incoming emails for viruses, and malware (business policies)
- Still possible with HTTPS instead of SMTP when using ZIVVER (masterkey)?
If not:
- Replacement of FireEye?
- Bring security back to end-user?
We experience a number of conflicting interests:
- Inspection goes from central to decentral/user level.
- Security from user perspective (user awareness).
- Regulation requires end-to-end encryption.
- Cloud Security Risks (standing policies, loss of control, inability to troubleshoot).
"How to reduce the risk of email data breaches for sectors of the MJS in order to be more compliant with the GDPR?"

In order to be more compliant with the GDPR, the MJS will likely reduce the risk of email data breaches with ZIVVER, because it focuses on both user awareness and email encryption.

ZIVVER pilot experiment, check:
- Randomness of LDAP Attribute
- FireEye compatibility HTTPS
- Storage master key
- Audit, traceability, logging @SOC
- Cloud security risks/monitoring
Thank you!
Questions?