Email Encryption
Real world solutions

Martijn Brinkers
martijn@ciphermail.com
FOUNDED IN 2008
BASED IN AMSTERDAM
PRIVATELY OWNED
FOCUS: EMAIL ENCRYPTION & DIGITAL SIGNING
FOCUS: GATEWAY LEVEL
CUSTOMERS WORLDWIDE
ANDROID SUPPORT
OPEN SOURCE COMMUNITY EDITION
HSM SUPPORT
EASE OF USE
Take home messages

1. Internal & external email encryption is more important than ever
   (Especially for personal information [GDPR] & information which
   can be used for insider trading)

2. Gateway level email encryption allows you to define and enforce
   company policies

3. Think about how to comply to email archiving and eDiscovery
   regulations with respect to email encryption

4. Use an HSM to store your private keys

5. Email encryption is compatible with cloud-based email (O365)
1. Why we need email encryption & digital signing
2. Solution
   • Email Encryption Gateway
   • Webmail Messenger
3. Why we need internal email encryption
   • Existing solution & Challenges
4. Challenge 1: Archiving & eDiscovery
   • Explanation, Solution, & Example
5. Challenge 2: Internal & external encryption
   • Explanation & Solution
6. Take home messages
Why we need email encryption & digital signing

1. DNS cannot be fully trusted
2. Email can be intercepted
3. DNSSEC helps, but not against interception
4. Email stored on a server is not encrypted
5. SSL/TLS only protects the channel, not the message
6. Recipient cannot check the sender
Solution
Email Encryption Gateway

- SMTP email server (MTA), Web GUI
- Supports S/MIME, PGP, PDF encryption, SSL/TLS
- Domain to domain encryption (S/MIME, PGP)
- Master/Master HA cluster
- Support for Hardware Security Modules (nCipher, Safenet, Utimaco, Securosys)
- Auto request end-user certs using built-in CA or external CA (EJBCA, GlobalSign EPKI etc.)
- DLP (quarantine, block, force encryption)
- Packages for Ubuntu, Debian, RedHat/CentOS, SUSE
- Virtual Appliance for Vmware & HyperV
- & more... (see www.ciphermail.com)
Solution
Email Encryption Gateway

- SMTP store and forward server
- Content scanning after encryption/decryption
- External email encryption
Solution
Webmail Messenger

- Webmail messenger is a webmail pull add-on to the gateway
- The recipient only needs a browser
- On premise
- Support for 2-factor authentication using SMS or secure token (for example Google Authenticator)
- Read confirmation can be sent back to sender after the recipient has opened the email
Why we need internal email encryption
Existing solution

- "Easy" to setup with Exchange, Outlook & Microsoft CA
- S/MIME based
- Auto certificate enrollment
- Nearly painless for sending encrypted email to internal recipients
Challenges with existing solution

Two main challenges

1. Email archiving & eDiscovery of encrypted email

2. Email encryption for internal & external recipients
Challenge 1: Archiving & eDiscovery

Explanation

- Email encrypted by mail client = default archived in encrypted form
- ediscovery only works if email is readable
- Archiving software must support reading encrypted email
- Regulations require email to be stored for years
- This requires that all private keys are backed up for years
- Are you 100% certain you have a copy of all keys?
Challenge 1: Archiving & eDiscovery

Solution

- Decrypt before archiving
- eDiscovery now possible
- Emails which cannot be decrypted are queued for investigation
- Keys can be "pushed" or "pulled"
- Keys should be stored on an HSM
- The email archiving solution should encrypt with an archiving key
Challenge 1: Archiving & eDiscovery

Example

Global investment management firm with offices in over 20 locations worldwide
Challenge 2: Encryption for internal & external recipients

Explanation

• What to do if an external recipient does not have a valid certificate?

• Or does not support S/MIME?
Challenge 2: Encryption for internal & external recipients

Solution

• Email for external recipients is encrypted with the gateway certificate.

• The gateway will then re-encrypt the email.
Challenge 2: Encryption for internal & external recipients

Solution

- Email encryption O365
- Microsoft manages your email (backups, login etc.)
- Encryption/Decryption is managed by the organisation (Bring Your Own Key)
Take home messages

1. Internal & external email encryption is more important than ever
   (Especially for personal information [GDPR] & information which can be used for insider trading)

2. Gateway level email encryption allows you to define and enforce company policies

3. Think about how to comply to email archiving and eDiscovery regulations with respect to email encryption

4. Use an HSM to store your private keys

5. Email encryption is compatible with cloud-based email (O365)
Thank you

Martijn Brinkers
martijn@ciphermail.com