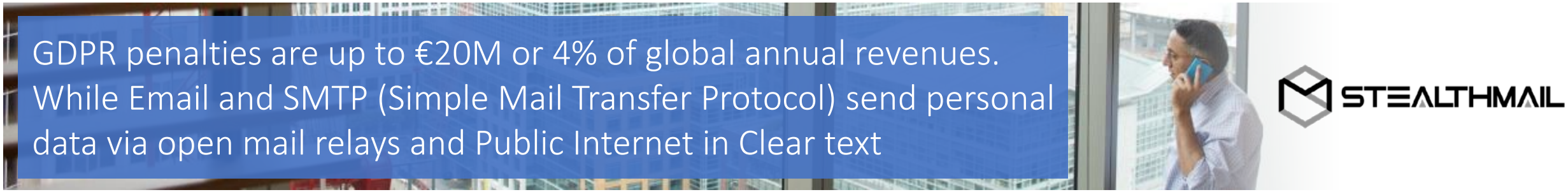
StealthMail:

GDPR compliance and email security

STEALTHMAIL

Microsoft



GDPR penalties are up to €20M or 4% of global annual revenues. While Email and SMTP (Simple Mail Transfer Protocol) send personal data via open mail relays and Public Internet in Clear text

STEALTHMAIL

Challenges

- All emails & files including Confidential are sent in Clear text over Public Internet;
- GDPR sets new data protection and privacy requirements and severe penalties;

- 91% of all intrusions start with email (Microsoft research);
- Email related requirements are set in GDPR Articles 25, 32, 33 and others;
- SMTP is SIMPLE protocol developed in 1980s;

Ideal Solution

- Emails and files are not sent in any form via open mail relays and Public Internet;
- Integration is seamless via Outlook and Azure;
- You have exclusive control over your data, keys and crypto machines;

- VPN can't provide for end-to-end email security;
- SSL/TLS solutions are not 100% secure (RFC 3207);
- Even if encrypted, emails can be collected for further cryptanalysis attacks;

Desired Outcomes

- Avoid severe GDPR penalties and reputational risks;
- Your emails are no longer sent via open mail relays and Public Internet;
- Your confidential and personal data never leaves your secure perimeter;

- SMTP traffic can be collected at Internet Providers and open mail relays because it's clear text (Wikipedia);
- "SMTP servers and clients normally communicate in the clear over the Internet" (RFC 3207);
- GDPR: "Data protection is a fundamental right";

StealthMail: GDPR Compliance and Email Security

Avoid severe GDPR penalties & legal risks, don't lose your reputation, email and digital infrastructure

GDPR Compliance

Emails & personal data are not sent via open mail relays and Public Internet

- Only crypto-URL are available to open mail relays and Public Internet;
- Article 25. Data protection by design and by default;
- Article 32. Security of processing;
- Article 33. Notification of a personal data breach to the supervisory authority;

Military Grade Cyber Security

- Company have an exclusive control over keys, crypto machine and data;
- Emails and personal data never leave Company's secured perimeter & are stored in Company's encrypted storage in protected cloud;
- Company control data distribution, access and can change it or revoke in any time;
- Company define length of the keys, encryption and other levels of protection information.

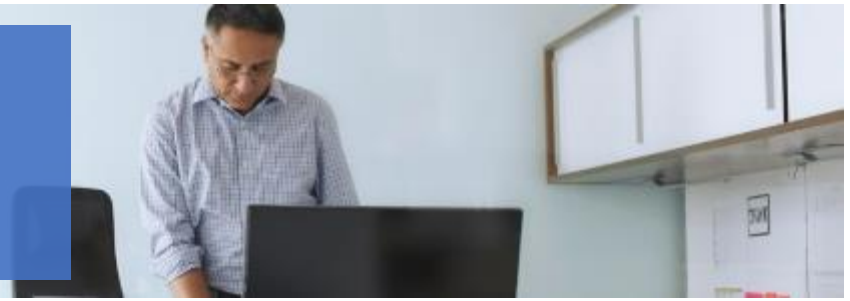
Seamless Integration

Outlook Plug-In / Azure

- Users install Outlook Plug-In;
- StealthMail is deployed to Company's Azure account;
- Security Officer use own Officer's Console and Qradar;

"SMTP servers and clients normally communicate in the clear over the Internet. In many cases, this communication goes through one or more routers that are not controlled or trusted by either entity." P. Hoffman, Internet Mail Consortium, RFC 3207

StealthMail + Microsoft Azure



What's the best way to avoid severe GDPR penalties and upgrade your cyber security? StealthMail protects email content and personal data from open mail relays and Public Internet exposure, extends your secure perimeter, gives you exclusive control over keys, crypto machines and data

Solution Alignment

Seamless Integration

- Outlook Plug-In is installed on users' computers;
- StealthMail is deployed in your Azure account;
- AD is used to speed up integration;

Multiple Layers of Independent Security

- StealthMail protects your data independently within Microsoft Azure, while Microsoft Azure provides extra level of security on top;
- Your private StealthMail Cloud within a private Azure cloud;

Microsoft Azure Cloud Reliability & Legal Protection

- StealthMail is deployed, backed up and operated in your Azure account;
- Almost unlimited capacity to meet your needs;
- Your data is also legally protected by the selected jurisdiction and Microsoft policies;