Think Ahead ACCA

Technical factsheet:

Email security

This factsheet has been produced in partnership with Barclays

Contents Page

INTRODUCTION

Email security issues are some of the biggest threats to productivity and profitability. The lack of security on the internet means information sent by email can be intercepted or forged if measures are not undertaken to ensure privacy. The SANS Institute reports that 95% of data breaches start with a spear phish: an email targeted at a specific individual or department within an organisation that appears to be from a trusted source. Add to this the fact that email is the number-one method to distribute malware, and it is clear security issues directly lead to high-cost breaches, loss of business and reputational damage.

To combat email threats it is important to understand the risks and apply appropriate technical and governance controls with a suitable level of security to protect the data for the lifecycle of the communication. Sadly, one easy solution is currently not available, and so a combined holistic security approach should be undertaken, determined by the requirements of the data being transmitted. For example, it is inadvisable for suppliers to send bank account updates via email without the sending and receiving party following pre-established processes that were set up at the start and continued throughout the partnership.

VULNERABILITIES AND BEST PRACTICE

To establish which solution works for both parties in the partnership it is important to understand the vulnerabilities and to apply a simple best practice review.

Email vulnerabilities include:

- sniffing (capturing data as it is transmitted over a network)
- eavesdropping (unauthorised monitoring of other people's communications)
- password cracking
- shoulder surfing (obtaining passwords etc through direct observation)
- object reuse (the reallocation of a storage medium that contains residual data)
- social engineering (psychological manipulation of people into performing actions or divulging confidential information)

- emanations (monitoring signals not intended to communicate data)
- spoofing (sender address and header information altered)
- malware distribution
- fraud
- human error.

Best practice checklist

- **Apply security controls before a breach occurs**. Security is often applied after a costly security incident. Be proactive about email security; set your governance and engage with your customers, clients, partners and suppliers in a consistent and communicated manner.
- **Information may be too sensitive to be sent by email or text**. Determine what and how you will communicate as well as the style, and apply this consistently to all email communications. This includes sending from a consistent and relevant email address, communicating the processes style upfront to ensure recipients know how to determine if the email is legitimate. It is also useful to brief colleagues who may deal with enquiries about the trustworthiness of communications.
- **Avoid using the phishing techniques used by adversaries** such as using links, urgency, fear, reprisals, poor-quality logos, spelling and grammar mistakes, and requests to enable macro (a common method used by adversaries to remove security controls from your system).
- **Avoid using short URLs**. This mechanism hides the destination website address that makes email recipients unable to assess if the destination is legitimate.
- **Do not include sensitive information in email communications** unless it is absolutely required and suitably protected through encryption and access control. For example, when updating bank account details or financial updates set up standardised processes and follow them strictly when updates are required.
- **Implement encryption and technical controls** suitable for the level of sensitivity of the data and the individual requirements of your business or service.
- **Have at least two complete backups of your data** to recover quickly from a ransomware attack. Storage can be online or on removable media as long as it is not mapped on the ransomed computer.

At a basic level emails are transmitted in plain text unless an encryption mechanism is placed on top. This means that all information that is transmitted and received can potentially be read, intercepted and altered. The UK government is enforcing a standardisation of HTTPS/SSL on all governmental websites from October 2018, and it is recommended that SMEs and industry follow suit.

SECURITY METHODS – PROS AND CONS

Methods to secure your email communications

Name	Purpose	Pros	Cons	Industry recommendations
Encrypting attachments	Protects the attachment of an email that may contain sensitive information	Easy to implement	Email remains in clear text Attachments are susceptible to brute-force password and man-in-the-middle attacks	If securing an email communication with a password, set passwords long and strong (at the very minimum eight characters, using alpha-numeric and special characters). Secure with an algorithm suited to the lifecycle of the data the email contains; for example, 256-bit AES encryption is currently a good and strong encryption method When transmitting passwords to recipients, use another method of communication, such as a mobile text message
Online file-sharing service	Replaces the need to send attachments in email by using file-sharing sites where users have permission to access resources and access is fully audited	Reduces the risk of unauthorised access to sensitive information Standardised URLs become known and repeatable Encrypted attachments are further protected from brute-force attacks	Cheap file-share hosting brings security concerns; fully research the security of the service Obtain professional security advice if you are unfamiliar with internet security	Apply access permissions with the minimal permissions required for that user, standardise this process and recertify users regularly Enable two-factor authentication if it is available

Name	Purpose	Pros	Cons	Industry recommendations
Own website	Having your own website containing all information available to customers, clients, partners etc	Can use as a store for information for your partners, removing the need to send any sensitive data by email Fully auditable, showing who has been accessing what	Security testing can be expensive. Using a website won't increase security unless it has had a full penetration test identifying weaknesses and providing steps on how to remediate the issues identified. Using a third party to carry out testing ensures that all weaknesses are identified and you do not have a conflict of interest. You will need to have your website tested after any functional changes to ensure no security issues or vulnerabilities have been introduced	Make sure websites are only available over HTTPS, not HTTP
Social media	Communicating with your consumers through a social media site	Easy distribution of messages to all clients	Not recommended for sensitive data distribution Access to social media sites can be blocked in organisations Easy way to distribute malware Data privacy controls should be regularly Increases risk of phishing and social engineering as it is simpler for adversaries to see who is connected to your social media site	Use for public information only

Which encryption algorithm is best?

Encryption ensures the effective and secure authentication of users. It is a mathematical procedure where information is encoded and requires the use of a software key to unlock the ciphered text and return the data to its original form.

Encryption is used to:

- ensure data privacy
- prevent fraud
- prevents unauthorised access to networks.

There are many types of public and known algorithms available and it is not recommended that you develop your own, due to the problematic nature of creating a new cipher. The key point is that the security of an encrypted email and algorithm is based on the security of the private key – which is used to decrypt messages – rather than the secrecy of the algorithm itself.

CONTROLS TO PREVENT EMAIL ABUSE

There are many technical controls that a specialist service provider can provide in order to help secure your email communications. These can include:

Transport layer security (TLS)

TLS is an encryption protocol used to protect data while it is in transit. Two domains communicating must agree to encrypt the information in a method and level they understand. Depending on the rules, the sending server will share over the encryption protocol, asking the receiving server if it will accept a more TLS connection. If it does, the sending server shares the algorithms and protocols it understands and they agree by sharing security certificate and public encryption key before any data is sent. This method ensures that data sent over TLS is encrypted end to end.

Pros

- When configured correctly, TLS rejects all other protocols.
- Any modern email service should be capable of using TLS; in most cases there will be at least an opportunistic TLS on connections that is not recommended for regular use as communications can end up in clear text.
- Once set up correctly and enforced, all email communications between two domains are encrypted.

Cons

- Your service provider must be able to enable enforced TLS.
- The PCI Council, which sets controls on credit card use, has recommended organisations migrate from TLS 1.0 to 1.1.
- Connections can default to less secure protocols and even non-encrypted connections, ie clear text, if TLS connectivity is not enforced. If either server cannot support an encrypted connection it will default to the less secure secure socket layer (SSL) protection or a non-encrypted clear text connection. In order to protect against this, both parties must insist on 'enforced TLS', where connectivity is rejected if TLS cannot occur at a set level.

DomainKey Identified Mail (DKIM)

DKIM protects against spoofing – altering the content of the email body and headers – by adding a cryptographic hash of the entire email as an SMTP header. If a message passes DKIM, you know the body hasn't been modified since it was cryptographically signed.

Pros

- The need for this type of validated identification arose because spam and phishing emails often use forged addresses and content. For example, a phishing message may claim to be from legitimate@company.com. The goal is to convince the recipient to read the email and follow any instructions within it. However, it is difficult for recipients to establish whether to trust this message and this is where DKIM comes in.

Cons

- If service providers do not check for DKIM the email will always be delivered whether it is spoofed, malicious or not.
- DKIM does not prevent disclosure or abusive behaviour within emails that are legitimately sent.

Sender policy framework (SPF)

SPF enables a domain to state what servers may send emails on its behalf. It confirms an email message is valid by checking a list within DNS records.

Pros

- Used in conjunction with DKIM and DMARC (below), SPF can improve delivery rates and prevent abuse.

- SPF provides an additional level of trust to increase the likelihood of an email being delivered.
- It allows recipient email services to check if an email came from a valid IP or domain and mark it as spam if it didn't.
- SPF can be used to set rules that will process messages accordingly, such as those that fail SPF.

Cons

- Can be difficult for novices to configure correctly.
- You will need to instruct colleagues who are using 'portable' email.
- SPF looks at the 'return-path' field value to validate the originating server; it does not validate using the 'from' domain, therefore it is recommended that users of SPF also use DKIM.
- Due to the use of the 'return-path' to validate the email, it does not guarantee that an email won't be delivered if it fails SPF; that final decision is decided by the receiving server and how it has been configured.

Domain-based message authentication, reporting and conformance (DMARC)

DMARC is designed to protect against direct domain spoofing. It is an email authentication, policy and reporting protocol that builds on SPF and DKIM by adding linkage to the ('from:') domain name; publishes policies for recipient handling of authentication failures; reports from receivers to senders; and improves and monitors protection of the domain from fraudulent email activities.

Pros

- Allows a sender to indicate that their messages are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes – such as mark the message as junk or reject entirely.
- Removes guesswork from the receiver's handling of these failed messages, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages.

Cons

- Will only work on domains that have been configured to be protected by DMARC; it will not pick up all domains you own unless they have been specifically configured for DMARC.
- DMARC was designed to address the shortcomings in SPF but even if a message fails SPF, there is no guarantee the email won't be delivered.

FURTHER INFORMATION

UK government email security standards:

https://www.gov.uk/government/publications/email-security-standards

DKIM: http://www.dkim.org/

SPF: http://www.openspf.org/

No More Ransom: https://www.nomoreransom.org/en/index.html

August 2018