TECHNICAL GUIDE

THE TECHNICAL GUIDE IS A PART OF THE PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTION DEVELOPED BY THE POLISH PLATFORM FOR HOMELAND SECURITY.

TABLE OF CONTENTS

03

VPN – VIRTUAL PRIVATE NETWORK

VPN is a virtual private network, i.e. a service that allows data to be transmitted through public networks as if the data were transmitted via a private network. For this purpose, a tunnel is created between the user and the destination. The data transmitted via VPN is encrypted.

The VPN service significantly increases the security of remote operation, due to:

- Sender authentication - only authorized users can connect to the VPN.
- Message integrity - it is possible to detect any changes in message content during transmission.
- Confidentiality - even if someone succeeds in intercepting the transmitted traffic, they will not be able to read the content.

04

FAKE WI-FI NETWORK

There are at least several attacks based on Wi-Fi falsification:

- Sharing an open Wi-Fi network with a name to suggest its correctness and inspire trust - such as "FourSeasonsHotel".

- Forging a known Wi-Fi network and intercepting devices, which are connected to it. In this method, an attacker provides a Wi-Fi network with the same SSID as the one in the area - e.g. the attacker is in a hospital waiting room and forges the hospital's Wi-Fi network with a stronger signal. Mobile devices can connect to the fake network instead of the right one.

- Forging any network known to the user using the auto-join mechanism. Some mobile devices periodically send a signal: "Is there a network I know nearby, called my own home network, FourSeasonsHotel, etc." An attacker equipped with a specially prepared device can send a signal: "Yes, I am." As a result, the device will decide that it can connect to a fake network, and the attacker will be able, among other things, to eavesdrop the transmitted traffic.

05

TYPES OF SSL CERTIFICATES

- Domain Validated (DV SSL)

The Authentication Centre checks the entity's permission to use the domain, but does not verify the entity's authenticity in any way. If the website has a DV SSL, you can be sure that the transmitted data is encrypted, but you do not know to whom the data is actually sent.

- Organization Validated (OV SSL)

The Authentication Centre checks the entity's permission to use the domain and performs a partial verification of the company's data based on relevant documents. OV SSL provides verified data to the user. This data (usually the name of the organization) is displayed by browsers after entering the connection details (usually the padlock symbol).

- Extended Validation (EV SSL)

The Authentication Centre checks the entity's permission to use the domain and performs a thorough verification of the entity by checking, among others:

  - the legal, physical and operational existence of the entity,
  - whether the identity of the entity is consistent with official data,
  - whether the entity has the exclusive permission to use the domain.

The EV SSL certificate is usually used primarily by entities that need a high level of trust, e.g. government websites, banks, etc.

EV SSL provides data about an entity to the user. This data is displayed by browsers after entering the connection details (usually a padlock symbol), usually the name of the organization is also displayed in the browser next to the URL of the page.

06

MAN-IN-THE-MIDDLE

During a man-in-the-middle attack, the attacker eavesdrops and can influence messages sent between communicating parties. Often, an attacker tries to impersonate at least one of the communicating parties. Examples of attacks are listed below:

- The attacker is located between the user and the bank's website, so that the user is convinced that he is contacting the real bank's website. This allows the attacker to obtain account details or change some of the requests such as changing the account number in the transfer.
- The attacker is located between the user and the email server. He or she can read the emails sent and received by the user, and as a result he or she collects data which can be used for further attacks.

There are many ways to carry out a man-in-the-middle attack, for example:

- Preparation of a fake Wi-Fi network to which user's device will connect.
- Preparation of a fake website that will mediate communication with the real website while collecting all data.

In order to reduce the likelihood of such an attack, it is necessary, for example:

- To use an encrypted connection (VPN, HTTPS).
- To verify whether the web site certificates are correct.
- To connect only to known and trusted Wi-Fi networks.

07

EMAIL PROTOCOLS

Email uses three main protocols:

- SMTP (Simple Mail Transfer Protocol) – is used to send messages to the mail server from the client and between servers. For communication between the servers, port 25 TCP and, in older configurations, port 465 TCP. For sending mail by the client (user), port 587 TCP (so called submission) is most often used.
- IMAP (Internet Message Access Protocol) – mailbox access protocol - used, among others, by applications installed on a computer for receiving mail. Its main feature is that the email client synchronizes the mail with the server, and does not removes it. It usually uses port 143 TCP or 993 TCP (encrypted IMAP).
- POP3 (Post Office Protocol 3) – is a simpler mail access protocol that simply retrieves all messages from the server while deleting them. It uses 110 TCP and 995 TCP ports.

08

EMAIL SPOOFING

The basic protocols mentioned above offer practically no protection against spoofing, i.e. impersonating another sender of a message. Without an appropriate configuration, the mail server will accept any message, without verification of the sender. In particular, the From field can accept any value configured by the sender.

To deal with this problem, a number of mechanisms have been developed to make spoofing difficult:

- Sender Policy Framework (SPF) allows the owner of a mail server to define a list of IP addresses from which mail can be sent. It works by setting up records in the DNS with a list of correct addresses. The recipient of the message can verify the address of the received message with this list and on this basis decide whether to accept or reject the message.
- DomainKeys Identified Mail (DKIM) is an automatic mechanism for cryptographic signature of messages. The sender's server signs the message with its private key when it is sent, and the public key is available in the relevant DNS records. The recipient can verify the signature using this public key. A potential attacker has no access to the sender's private key, so they cannot sign the message properly.
- Domain-based Message Authentication, Reporting and Conformance protocol (DMARC is a mechanism that allows the server owner to monitor the spoofing of his messages and indicate to the recipient what actions he should take if he notices a spoofing of messages. In particular, DMARC allows you to define (in the appropriate DNS record) the address to which reports on noticed forged messages will be sent.

Naturally, for these mechanisms to be effective, both the sender and the recipient must configure them properly.

09

SPAM

SPAM means unwanted mail. It can be a simple annoying aspect of everyday life, but it can also be a serious threat to security. Use of so-called anti-spam filters is a basic way to be protected against it. The filters are based on different mechanisms:

- black and white lists (domains, IP addresses, senders),
- verifications based on senders' domains (including DKIM, DMARC, SPF),
- filters based on content analysis,
- self-learning filters based on user's behavior.

The spam protection configuration is strongly dependent on the used software, but practically it can always be several stages long - e.g. mail server can completely ignore incoming mail from blacklisted addresses and messages matched by filters can be placed in a dedicated directory in the user's mailbox.

10

PGP AND S/MIME

Both these technologies are used in cryptography and work on the basis of so-called asymmetric encryption. It is based on the existence of two keys - public and private - for each user. As the name suggests, the private key should not be made available anywhere. On the other hand, the public key can be made available to other people.

The public key is used to encrypt the transmitted information. The private key allows you to read it. Because the private key is held by only one person (the recipient), no one else can decrypt the message. An encrypted message can be sent by anyone with recipient's public key.

In this process, it is necessary to verify whether the received public key actually belongs to the person concerned. Therefore, a so-called public key certificate is issued. This is information about the public key of the entity, including also a description of the entity's identity and a digital signature that indicates confirmation of this certificate by the so-called trusted third party.

11

PGP AND S/MIME

The confirmation of the certificate by a trusted third party can be dealt with in several different ways:

- S/MIME – public and private keys are generated by trusted Certificate Authorities (CA). The use of commonly known and trusted Certificate Authorities means that anyone (both inside and outside the company) will be able to confirm the authenticity of our public key.
- PGP – In this version, instead of centralized certificate authorities, the authenticity of a public key is confirmed by other users. This means that this method may be used without using any Certificate Authority. It is enough to securely share your own public key with the addressee of the message, who will then approve it as trusted..
- Another possibility is to create a local certificate authority, inside the company that will confirm the authenticity of individual employees' keys. Thanks to that, it will be possible to encrypt internal correspondence. In order to use PGP in communication with people outside the company, these people must first confirm that they trust the company's certificates.

LINKS:

PGP key generation with PGP Desktop

PGP key generation on Ubuntu

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds Smart Growth

Republic of Poland

European Union
European Regional Development Fund

The project "Cybersecurity – PPHS Standard for SME and public institutions" was financed by the European Regional Development Fund.