Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Company ID No. 05800226
Data mailbox ID: zzfnkp3

File number:
350 - 1117/2021
Reference No.
8477/2021-NÚKIB-E/350

Brno, 11 October 2021

Attended by:
Štěpán Daněk

PUBLIC DECREE

GENERAL MEASURE

The National Cyber and Information Security Agency, with its registered office at Brno, Mučednická 1125/31, postcode 616 00 (hereinafter referred to as the "Agency"), as the competent central administrative authority pursuant to Section 22(b) of Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Act on Cyber Security), as amended (hereinafter referred to as the "Act on Cyber Security"),

stipulates

on the basis of Section 14 of the Act on Cyber Security and in accordance with Section 15 of the Act on Cyber Security and Sections 171, 173 and 174 of Act No. 500/2004 Coll., Code of Administrative Procedure, as amended, the **following methods of increasing the protection of information systems, services and electronic communications networks as a protective measure:**

1. **The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, whose electronic mail is part of an information or communication system subject to the requirements of the Act on Cyber Security, shall ensure that the following requirements are met when receiving and sending electronic mail using the SMTP protocol outside the internal network:**

   1.1. All SMTP servers listed in the MX records through which electronic mail is received, and SMTP border servers through which mail is sent, support a secure connection according to the STARTTLS standard (IETF RFC 3207).

   1.2. Within the secure connection, all servers through which electronic mail is received or sent:

      1.2.1. Support TLSv1.2 protocol or newer.

      1.2.2. Do not support SSLv3 protocol and older.

1.2.3. Support TLSv1.0 and TLSv1.1 protocols only in justified necessary cases where limiting support for these protocols could cause limitations in the availability and proper functioning of the electronic mail system.

1.2.4. Use cryptographic means within the TLS connection that are currently robust according to the recommendation of the Agency issued in connection with Section 26(d) of Decree No. 82/2018 Coll., on Cyber Security. Other means may be used only in justified cases.

1.3. The certificates of all SMTP servers listed in the MX records are valid, issued by a recognized certification authority, and have a domain name that matches the name of the MX record of the server.

1.4. All DNS records relevant to the mail-receiving function have integrity protection using DNSSEC (IETF RFC 4033). The cryptographic algorithms used to digitally sign DNS records must be currently robust.

1.5. All SMTP border servers through which electronic mail is sent validate records using DNSSEC technology when resolving DNS records, if they are digitally signed using this technology. Invalidly signed records are ignored. If validation is performed using a DNS server, the validating DNS server must be on the same server or network as the SMTP server or use a connection that ensures the integrity of transmission.

1.6. All MX records used by SMTP servers have a corresponding TLSA record published in DNS according to DANE technology (IETF RFC 7672).

1.7. All SMTP border servers through which electronic mail is sent verify the counterparty certificate using the TLSA record if the counterparty has published it. If the certificate imprint does not match the certificate offered by the remote server, or if the remote server does not support establishing a secure connection, the electronic mail will not be sent to that server.

1.8. In the case of communication between defined SMTP servers, this communication must be secured by currently robust cryptographic means, the impossibility of downgrading communication to unencrypted must be ensured, and both parties must ensure authentication of the counterparty. The used cryptographic methods are currently robust according to the recommendation of the Agency issued in connection with Section 26(d) of Decree No. 82/2018 Coll., on Cyber Security. Other means may be used only in justified cases.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, which are also public authorities involved in the Czech Presidency of the Council of the EU and which have employees registered in the Central Register of Employees Participating in the Preparation and Execution of the Presidency in 2022 as at the effective date of this measure, must comply with points 1.1 to 1.5 at latest by 1 January 2022 and points 1.6 to 1.8 at latest by 1 July 2022.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, which are also public authorities involved in the Presidency of the Czech Republic in the Council of the EU, whose employees will be registered in the Central Register of Employees Participating in the Preparation and Execution of the Presidency in 2022 after the effective date of this measure, must comply with points 1.1 to 1.5 without undue delay after their registration in that register, but no later than by 1 July 2022, and with points 1.6 to 1.8 no later than by 1 July 2022.

Other authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security must comply with points 1.1 to 1.8 at latest by 1 January 2023.

Other authorities and persons who become obliged persons under Section 3(c) to (f) of the Act on Cyber Security after the effective date of this protective measure, must comply with points 1.1 to 1.8 within 14 months of their designation or identification.

2. **If the transmission of electronic mail from an endpoint device is to an electronic mail server located on a different network from the endpoint device, the authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, whose electronic mail is part of an information or communication system subject to the requirements of the Act on Cyber Security, shall ensure that this transmission meets the following requirements:**

   2.1. It uses a secure connection for all protocols by which the end device communicates with the mail server. The used cryptographic means within the secure connection are currently robust according to the recommendation of the Agency issued in connection with Section 26(d) of Decree No. 82/2018 Coll., on Cyber Security. Other means may be used only in justified cases.

   2.2. If the used transmission uses the TLS cryptographic protocol for the secure connection, within the secure connection:

      2.2.1. TLSv1.2 protocol or newer is used.

      2.2.2. SSLv3 protocol or older is not used.

      2.2.3. TLSv1.0 and TLSv1.1 protocols may be allowed only in justified necessary cases where limiting support for these protocols could cause limitations in the availability and proper functioning of the electronic mail system.

      2.2.4. The certificate of the electronic mail server is valid and issued by a recognized certification authority. If the certificate is not issued by a recognized certification authority, the certification authority used must be available on all devices that connect to the mail server.

   2.3. In the case of SMTP protocol (IETF RFC 5421), only the secure variant of SMTPS protocol is used.

2.4. In the case of IMAP protocol (IETF RFC 9051), only the secure variant of IMAPS protocol is used.
2.5. In the case of POP3 protocol (IETF RFC 1939), only the secure variant of POP3S protocol is used.
2.6. In the case of access via HTTP protocol or protocol based on HTTP, only the secure variant of HTTPS protocol is used.
2.7. In the case of access via a web interface, the *Strict-Transport-Security* (HSTS, IETF RFC 6797) HTTP header must be defined with a *max-age* parameter value greater than zero.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, which are public authorities involved in the Czech Presidency of the Council of the EU and which have employees registered in the Central Register of Employees Participating in the Preparation and Execution of the Presidency in 2022 as at or after the effective date of this measure, must comply with points 2.1 to 2.7 at latest by 1 July 2022.

Other authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security must comply with points 2.1 to 2.7 at latest by 1 January 2023.

Other authorities and persons who become obliged persons under Section 3(c) through (f) of the Act on Cyber Security after the effective date of this protective measure must comply with points 2.1 through 2.7 within 14 months of their designation or identification.

3. The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security shall ensure that the following requirements are met when receiving and sending electronic mail using the SMTP protocol outside internal network:

3.1. Domains used to send electronic mail must have an SPF record (IETF RFC 7208) published in DNS containing the addresses of permitted SMTP servers that can send electronic mail. The default policy must be set to *soft fail* (~all) or *hard fail* (-all).
3.2. At a minimum, the *From* and *Subject* headers and the body of the message sent by electronic mail must be digitally signed using DKIM technology (IETF RFC 6376), and the public part of the key must be published in DNS. The cryptographic means used for signing the report must be currently robust according to the recommendation of the Agency for Cryptographic Means issued in accordance with Section 26(d) of Decree No. 82/2018 Coll., on Cyber Security; other means may be used only in justified cases.
3.3. Domains used for sending electronic mail must have a DMARC record (IETF RFC 7489) published in DNS with at least the following parameters:
3.3.1. *Requested Mail Receiver policy* (p) set to *quarantine* or *reject* and

3.3.2. *Sampling rate* (pct) set to 100 (default value).

3.4. When receiving electronic mail, it is verified that the address of the server from which the mail was sent matches the SPF record of the domain, if the SPF record is published by the counterparty. If it does not comply with these rules, the mail message is rejected, discarded, delivered to a designated folder, or clearly marked as possibly fraudulent.

3.5. When receiving electronic mail, the digital signature of the headers and body of the mail message is verified by DKIM technology, if the headers and body of the message have been signed by this technology.

3.6. On receipt of electronic mail, the mail message is checked for compliance with the rules set forth in the counterparty's DMARC record, if published by the counterparty. If it does not comply with these rules, the mail message is rejected, discarded, delivered to a designated folder, or clearly marked as possibly fraudulent.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, which are public authorities involved in the Czech Presidency of the Council of the EU and which have employees registered in the Central Register of Employees Participating in the Preparation and Execution of the Presidency in 2022 as at the effective date of this measure, must comply with point 3.1 at latest by 1 January 2022 and points 3.2 to 3.6 at latest by 1 July 2022.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, which are public authorities involved in the Presidency of the Czech Republic in the Council of the EU, and whose employees will be registered in the Central Register of Employees Participating in the Preparation and Execution of the Presidency in 2022 after the effective date of this measure, must comply with point 3.1 without undue delay after their registration in that register, but no later than by 1 July 2022, and with points 3.2 to 3.6 no later than by 1 July 2022.

Other authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security must comply with points 3.1 to 3.6 by 1 January 2023 at the latest.

Other authorities and persons who become obliged persons under Section 3(c) to (f) of the Act on Cyber Security after the effective date of this protective measure, for whom this protective measure is relevant, must comply with points 3.1 to 3.6 within 14 months of their designation or identification.

This protective measure must be carried out within the time limits specified for each individual action.

The authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security, who have performed any of the above actions, need not perform these specific actions repeatedly.

RATIONALE

1. The National Cyber and Information Security Agency, as the central authority of the state administration pursuant to Section 2(16) of Act No. 2/1969 Coll, on the establishment of ministries and other central bodies of state administration of the Czech Republic, as amended, and pursuant to Section 22(b) of the Act on Cyber Security, has, in accordance with Section 14 of the Act on Cyber Security, based on an analysis of a cyber security incident already resolved, resolved to issue this general measure to enhance the protection of information systems or services and electronic communications networks, as set out in the operative part of this general measure. The issuance of this general measure is based on the analysis of an already resolved cyber security incident of 20 February 2020, registered under number 32305.

2. The incident was caused by a *Man-in-the-Middle* (MITM) attack on an element outside of the obliged party organization's infrastructure, where the hacker positioned himself as an intermediary between the communicating entities, thereby compromising the confidentiality of the electronic mail messages transmitted through that element.

3. The individual methods of increasing the protection of information systems, services and electronic communications networks, as specified in the operative part of this general measure, are in general terms actions whose implementation is necessary to ensure the confidentiality and integrity of communications between the mail servers of the obliged persons and between the end devices and the mail server within the organisation of the obliged person. Furthermore, these methods of increasing protection are aimed at preventing fraudulent electronic mail communication (e.g. sending messages with a fraudulent organisation domain). Failure to implement these enhanced protection measures risks the possibility of compromising the confidentiality and integrity of the electronic communications sent, which could have serious direct impacts on the functioning and credibility of the organisations concerned. In the case of public authorities cooperating on activities within the Czech Presidency of the Council of the EU, a breach in the security of mutual communication could disrupt the smooth running of this Presidency and reduce the Czech Republic's credibility in the international arena.

4. The introduction of the above-mentioned methods of increasing the protection of information systems is absolutely necessary to ensure secure communication, in particular between public authorities, internally within these public authorities, or between public authorities and other obliged persons. If only one of the communicating entities has some of the required methods of increased protection in place, the entire communication takes place in an inadequately secured (unencrypted) form or is susceptible to MITM-type attacks, and the proposed methods of increased protection are

thus meaningless, which is why it is necessary that they be implemented by the widest possible range of obliged entities pursuant to Section 3(c) to (f) of the Act on Cyber Security. Otherwise, recurrent incidents comparable to those whose analysis led to the issuance of this protective measure may be common.

5. A more detailed technical justification and explanation of the necessity of specific methods of securing the information systems or services and electronic communications networks of the obliged entities is contained in the section “Technical Rationale”.

6. Pursuant to Section 14 of the Act on Cyber Security, all administrators and operators of information and communication systems of critical information infrastructure, important information systems and information systems of essential services are bound by the aforementioned methods of enhancing the protection of information systems or services and electronic communications networks.

7. The obliged persons pursuant to Section 3(c) to (f) of the Act on Cyber Security must implement the above-described methods of enhancing the protection of information systems or services and electronic communications networks, provided that their electronic mail system is part of an information security management system that relates to systems to which the requirements of the Act on Cyber Security must be applied. In particular, this will always be the case for administrators and operators of essential service information systems, provided that the functioning of the essential service depends, inter alia, on the electronic mail system. For administrators and operators of critical information and communication systems, this will always be the case provided that the electronic mail system is part of the designated critical information infrastructure element. In the case of administrators and operators of important information systems that are an organizational unit of the state, a region or the capital city of Prague, the electronic mail system is a type of important information system according to Section 2(1) of Decree No. 317/2014 Coll., on important information systems and their determining criteria, as amended (hereinafter referred to as the “VIS Decree”); therefore, the implementation of methods to increase protection will always be necessary. For other public authorities, this will be the case provided that their electronic mail system meets the determining criteria under Section 3 of the VIS Decree. In addition, all obliged persons under Section 3(c) to (f) of the Act on Cyber Security may perform implementation on the basis that they have included their electronic mail system in the scope of the information security management system.

8. Pursuant to Section 14 of the Act on Cyber Security, a reasonable period of time must be allowed for the implementation of methods to enhance the protection of information systems or services and electronic communications networks. In view of the above-mentioned means of increasing the protection of information systems or services and electronic communications networks and the justification of these means in the Technical

Rationale, the Agency considers the time limits set out in the operative part of this general measure to be sufficient and proportionate. This applies both in relation to the persons referred to in Section 3(c) to (f) of the Act on Cyber Security on the effective date of this measure and in relation to the persons and authorities that will become obliged persons referred to in Section 3(c) to (f) of the Act on Cyber Security in the future.

9. The shorter deadline for public authorities participating in the Czech Presidency of the Council of the EU results from the timeframe of this Presidency. Some agendas will start to be addressed in principle from the beginning of 2022, with the Czech Republic effectively holding the Presidency of the Council of the EU from July 2022 to the end of 2022. It is therefore essential to ensure that the means of increasing protection are implemented by the deadlines corresponding to this timeframe, ideally as early as 1 January 2022 and no later than 1 July 2022.

10. The transitional provisions pursuant to Sections 30 and 31 of the Act on Cyber Security and Article II of the transitional provisions introduced by Act No. 205/2017 Coll., which give the obliged persons pursuant to Sections 3(c) to (f) of this Act one year from their designation or identification to implement security measures, do not apply to the performance of the obligations imposed by this measure.

11. The Agency notes that authorities or persons who are obliged to implement security measures pursuant to the Act on Cyber Security shall take into account the measures pursuant to Section 11 of the Act on Cyber Security in the risk assessment and risk management plan in connection with risk management pursuant to Section 5(1)(h)(3) of the Decree on Cyber Security. One of these measures is the protective measure under Section 14 of the Act on Cyber Security.

12. The Agency further notes that in accordance with Section 4(4) of the Act on Cyber Security, the authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and to include these requirements in the contract they conclude with the supplier. Taking into account the requirements resulting from the security measures under the first sentence to the extent necessary to comply with the obligations under the Act on Cyber Security cannot be considered an unlawful restriction of competition or an unjustified barrier to competition.

13. With regard to the deadlines set, the Agency would like to draw attention to the provisions of Section 29(c) of Act No. 134/2016 Coll., Public Procurement Act, as amended, according to which "*the contracting authority is not obliged to award a public contract in a procurement procedure if it concerns the award or performance of a public contract within the framework of special security measures provided for by other legal regulations and at the same time it is not possible to take such a measure that would*

enable the procurement procedure to be carried out." It is at the discretion of the obliged person in the position of the contracting authority implementing the above-mentioned means of increasing protection, whether the institute of this exception is usable and applicable in view of the specific circumstances and conditions of the organisation concerned.

Technical rationale

Measures to ensure the confidentiality and integrity of communication between mail servers

14. The first part of the operative part of the measure is aimed at ensuring the confidentiality and integrity of communications between mail servers located outside the internal network and aims to reduce the possibility of MITM attacks.

15. Encryption is a basic way of ensuring the confidentiality and integrity of communication so that their content cannot be read or modified by a hacker with access to the communication between mail servers.

16. The SMTP protocol is used for the transmission of electronic mail messages between servers, which in its basic version does not support encryption. The SMTP protocol extension, STARTTLS (IETF RFC 3207), allows for opportunistic encryption (i.e. one that is used when it can be used; otherwise, it will switch to unencrypted communication). The server first establishes an unencrypted connection, which is then promoted to encrypted. To elevate a connection to encrypted, both the sender and receiver sides must support this extension. The STARTTLS extension itself only protects against passive eavesdropping on transmitted messages. The introduction of support for this extension is the subject of point 1.1 of the operative part of this measure.

17. Within a secure connection, only currently robust cryptographic means must be used to ensure confidentiality and integrity. These are defined by the Agency in the recommendations published on its website. In addition, support for certain versions of cryptographic protocols for establishing secure connections is required. The SSLv3 protocol was marked as obsolete in 2015 (IETF RFC 7568). The TLSv1.0 and TLSv1.1 protocols were designated as obsolete in 2021 (IETF RFC 8996). At present, it is recommended to use TLSv1.2 (IETF RFC 5246) and TLSv1.3 (IETF RFC 8446) protocols. Outdated protocols are susceptible to various types of attacks that can lead to breaches in the confidentiality and integrity of communications. The use of currently robust cryptographic means and the limitation of support for the aforementioned obsolete versions of protocols both when receiving and sending mail is required by point 1.2 of the operative part of this measure.

18. Certificates are used for counterparty authentication within the TLS protocol. To verify the certificate, the certificate must be valid and issued by a recognized certification authority. The list of generally recognized certification authorities is published in the Common CA Database (https://www.ccadb.org), where the certification authority's certificate must be listed by both Mozilla and Microsoft. The obligation to use a valid and recognised certificate is laid down in point 1.3 of the operative part of this measure.

19. The DNS protocol is used to determine which IP address of the SMTP server the electronic mail message should be sent to, which does not ensure the integrity of DNS records. The DNSSEC extension (IETF RFC 4033) is used to ensure the integrity of DNS messages. All DNS records relevant for receiving mail (i.e. at least MX records for the domain intended for receiving mail, and then A or AAAA records for domain names of SMTP servers) must be digitally signed using this technology, which is the content of point 1.4 of the operative part of this measure.

20. When sending electronic mail, the digital signatures of DNS records must be validated, for which a DNS server supporting validation according to DNSSEC technology must be used or validation must be performed directly by the SMTP server. If validation is performed by an SMTP server, the communication between the SMTP and DNS server must be secured so that a hacker cannot spoof it. To do this, the DNS server must either be on the same server (virtual or physical), on the same network, or communication must be secured against integrity breaches by cryptographic algorithms by some other means (e.g., a VPN connection, DNS-over-HTTPS, or DNS- over-TLS). If multiple DNS servers are used, all the servers used must perform validation. The introduction of DNSSEC validation follows from point 1.5 of the operative part of this measure.

21. Due to the opportunistic nature of encryption in the STARTTLS protocol (see point 16 above), it is possible to break the establishment of an encrypted connection (*STRIPTLS)* during connection establishment in the event of an active Man-in-the-Middle (MITM) attack, where the hacker gets into the position of an intermediary between the communicating entities, in which case the communication is unencrypted. Unencrypted transmission allows the confidentiality and integrity of the transmitted message to be compromised, as a hacker can read or even modify the message. Also, due to the default setting of SMTP servers, where no certificate checking is performed when establishing a connection, it is possible to perform a *TLS Certificate Spoofing* attack. Two complementary technologies have been developed to prevent this type of attack - DANE (IETF RFC 7671) and MTA-STS (IETF RFC 8461). To effectively secure the messages being transmitted, one of these technologies must be supported by both the sender and receiver sides, and it is essential that both communicating entities use the same type of technology, i.e. either DANE or MTA-STS. In order to maximize the effect of this protective measure, the Agency has mandated the implementation of DANE technology to ensure

compatible secure communications between the widest possible range of obligated entities.

22. The function of DANE is to publish the certificate imprint within a DNS TLSA record. When sending a mail message, the sending server verifies that the counterparty has a TLSA record published and, if so, checks that the published certificate imprint matches the certificate transmitted when the TLS connection was established. If the remote server does not report support for a secure connection (e.g. due to a *STRIPTLS* attack) or the certificate imprint does not match, communication will not be established and therefore the mail message will not be sent. The introduction of DANE technology does not preclude the simultaneous use of MTA-STS technology.

23. In order for DANE to function properly, a TLSA record must be published in DNS to secure the communication of receiving an electronic mail message. It contains the certificate imprint that is used when receiving electronic mail. This allows the counterparty to check that the server supports secure communication using STARTTLS and that the offered certificate has not been spoofed by an independent channel. If this happens, the electronic mail message will not be sent to this server and will thus be protected from breaches of confidentiality and integrity. To ensure the integrity of the TLSA record and to allow the counterparty to trust the record, the record must be signed using DNSSEC technology. Publication of this record is required by point 1.6 of the operative part of this measure and a digital signature pursuant to DNSSEC point 1.4 of the measure.

24. To secure communications when sending an electronic mail message, the TLSA record must be checked with the counterparty if the record is published. If a secure connection cannot be established or the certificate imprint does not match, the electronic mail message must not be sent to this server. A check of this record is required by point 1.7 of the operative part of this measure.

25. The last point of the operative part of the measure deals with situations when electronic mail is forwarded between mail servers outside the internal network, e.g. in the case of using a third party service to check received and sent mail. In such a case, to prevent a MITM attack, it is necessary to ensure that this communication is secured by cryptographic means, it is not possible to downgrade this communication to unencrypted, and it is also necessary to verify the authenticity of the counterparty. As a rule, SMTPS protocol will be used, but other technical solutions can be chosen to ensure these requirements (e.g. SMTP communication within a VPN connection).

26. Given that, according to the Agency's internal survey, points 1.1 to 1.5 of the operative part of the measure have been mostly implemented by the relevant public authorities, a shorter deadline has been set for their implementation. The introduction of other points may mean the implementation of new technologies and therefore the timeframe for their introduction is longer.

Measures to ensure the confidentiality and integrity of communications between the electronic mail client and the server

27. The second part of the operative part of the measure is aimed at securing communication between the end device (e.g. end station or mobile device) and the electronic mail server so as to reduce the possibility of MITM attacks. The measure needs to be implemented only if the end device is located in a different network than the electronic mail server (typically when the communication between the end device and the server is via the internet).

28. Encryption is a basic way of ensuring the confidentiality and integrity of transmitted messages so that their content cannot be read or modified by a hacker with access to the communication between the end device and the mail server.

29. Only currently robust cryptographic algorithms as defined in the Cryptographic Means Recommendation available on the Agency's website must be used for functional encryption. Point 2.1 of the operative part of this measure stipulates the obligation of the obliged entity to use a secure connection using the cryptographic means specified in the aforementioned Recommendation.

30. If the used protocol uses the TLS cryptographic protocol, point 2.2 of the operative part of the measure specifies which versions of this protocol can be used.

31. Certificates are used for counterparty authentication within the TLS protocol. To verify the certificate, the certificate must be valid and issued by a recognized certification authority. The list of generally recognized certification authorities is published in the Common CA Database, where the certification authority's certificate must be listed by both Mozilla and Microsoft. The use of a different certification authority that is not published in the CCAD list is possible if it is accepted by all endpoint devices that access the mail server. The obligation to use a valid and recognised certificate is laid down in point 2.2.4 of the operative part of this measure.

32. For SMTP, IMAP, POP3 or HTTP protocols (including HTTP-based protocols), points 2.3 to 2.6 of the operative part of the measure require the use of secure versions of these protocols (SMTPS, IMAPS, POP3S, HTTPS) that are not susceptible to the degradation of connection to unencrypted.

33. In connection with the use of the HTTPS protocol when accessing via a web interface, point 2.7 of the operative part of the measure requires the setting of the HTTP header *Strict-Transport-Security* according to ITFC RFC 6797. The value of the *max-age* parameter must be greater than zero for browsers to accept this header. This measure prevents the connection from being downgraded to an unencrypted HTTP connection.

Measures to ensure the integrity and prevent spoofing of the sender of an electronic mail message

34. The third part of the operative part of the measure focuses on ensuring the integrity of the electronic mail messages transmitted. These measures will allow detection of message tampering by a hacker if the sender or receiver side does not support the measures in the first part of the operative part. It also prevents the sender of the mail messages from being spoofed. Hackers use sender spoofing to increase the credibility of phishing messages.

35. Points 3.1 to 3.3 of the operative part of the measure are aimed at ensuring that the integrity of an electronic mail message can be detected when it is sent. They also ensure that a hacker cannot send an electronic mail message with a spoofed organization domain.

36. Points 3.4 to 3.6 of the operative part of the measure are aimed at ensuring that the integrity of an electronic mail message can be detected when it is received. They also ensure that fraudulent electronic mail messages are not delivered to the mailboxes of the organisation's users or that the user is alerted to a possible fraudulent message.

37. SPF (Sender Policy Framework) technology allows an organization to define which SMTP servers can send electronic mail messages from the organization's domain. The default *soft* or *hard fail* policy defines how the remote mail server should handle a message if it is sent from servers other than the defined servers.

38. DKIM (DomainKeys Identified Mail) technology digitally signs the designated headers and body of the mail message, thus guaranteeing to the counterparty that the mail message was sent from a legitimate SMTP server. The signing private key is stored on the SMTP servers sending the mail message, and the public key for signature verification is published in a TXT record within the domain's DNS record.

39. The DMARC (Domain-based Message Authentication Reporting and Conformance) technology defines in more detail how the recipient server should handle a message that has not been signed using DKIM, or if the DKIM signature is invalid, or was sent from other than the designated SMTP server according to the SPF record. To prevent a message with compromised integrity or a potentially fraudulent message from being delivered directly to the user, the policy must be set to *quarantine* or *reject*. It is also required to set the value of the *Sampling rate* parameter to 100 so that this policy is applied to all messages sent. The use of SPF technology alone is not sufficient, as it only checks the *envelope-from* address, while the recipient of the message typically sees the sender's address in the *From* header.

40. Point 3.1 of the operative part of the measure is, according to the Agency's internal survey across public authorities, already mostly fulfilled and easier to implement, hence the shorter deadline for implementation by the relevant public authorities. The other action points may involve the implementation of new technologies, hence the longer timeframe for their implementation.

41. It must be stressed that even all of these measures do not replace the security of electronic mail messages by means of end-to-end encryption (e.g. PGP, S/MIME); they only increase the security of communication between the individual elements enabling the transmission of electronic mail.

42. If you have any technical questions or questions about the content of individual imposed actions in connection with this protective measure, please contact cert@nukib.cz. For media enquiries, please contact the Agency's spokesperson at dotazy.media@nukib.cz. If you have any further questions, especially of a legal nature, regarding the protective measure, please contact regulace@nukib.cz.

ADVICE

This general measure shall be delivered in accordance with the procedure under Section 25 of the Code of Administrative Procedure by public notice on the Agency's official notice board. Pursuant to Section 15(1) of the Act on Cyber Security, a general measure pursuant to Section 14 of the Act on Cyber Security comes into effect upon its posting on the Agency's official notice board. Section 172 of the Code of Administrative Procedure shall not apply. Pursuant to Section 15(2) of the Act on Cyber Security, comments may be submitted to a general measure issued pursuant to Section 14 within 30 days of its posting on the Agency's official notice board. On the basis of the comments submitted, the Agency may amend or cancel the general measure.

Digitálně podepsal:
Ing. Karel Řehka
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 11.10.2021 09:24

NÚKIB

Ing. Karel Řehka
Director
Signed electronically

Posted on: ……

Removed on: /