NÚKIB

RECOMMENDED SAFETY MEASURES BASED ON THE WARNING OF 16 APRIL 2020

Support material

Version 1.0, valid as of 17/04/2020

Contents

Introduction

The National Cyber and Information Security Agency (hereinafter referred to as "the Agency") issued a warning on 16 April 2020 about a cybersecurity threat in the form of an extensive campaign of cyberattacks on information and communication systems in the Czech Republic and on the systems of healthcare facilities in particular (hereinafter referred to as "the Warning"). Based on the information available to the Agency, the threat could be carried out in the days immediately following the issuing of the Warning.

The support material herein focuses on the technical and organizational aspects linked with the recommendations of the Agency contained in the Warning; it specifies the recommended practices of administrators of information and communication systems governed under Act No 181/2014, on cyber security (hereinafter referred to as the "Act on Cyber Security") and is primarily intended for cybersecurity experts. It does not represent an exhaustive list of all the measures which could be taken to protect information or communication systems governed under the Act on Cyber Security (hereinafter referred to as a "system") from the threat; it has mainly been prepared in view of the necessity to adopt the given measures quickly. This material only contains recommendations. It is always up to the specific administrator of a system to adopt the relevant measures for protection from the threat. Each administrator of a system must also consider the applicability of the measures, the possibility of implementing them in their System, the impacts on their activities and provision of services, and the timeline for their introduction.

Other entities that do not fall under the Act on Cyber Security can use this support material as guidance to improve the protection of their Systems.

Queries regarding this document or the Warning may be addressed to the secretariat of the Regulations Department at the National Cyber and Information Security Agency: phone: +420 541 110 560, e-mail: regulace@nukib.cz.

In the event of a cyberattack or to report an incident please use the e-mail cert.incident@nukib.cz. If you are reporting an incident outside working hours, please also call +420 725 502 878.

Note:

This document provides supporting guidance. It does not replace any Act nor implementing legislation. The Agency reserves the right to amend this document. The information contained in this document is compliant with the legislation effective on the validity date of the published version of the document.

1 Measures to prevent or mitigate the effects of a cybersecurity incident related to the content of the Warning

1.1 Basic information on the recommended actions stated in the Warning

1.1.1 Draw users' particular attention to spear-phishing threats and enclose a call for any users who have recently opened suspicious attachments to contact the infrastructure administrator; also draw users' attention to the possibility that executable files such as "obrazek.png.exe", "text.txt.exe" or "dokument.pdf.exe" may be "masked" as part of a phishing attempt.

Objective of the measure: To minimize the risk of an attacker breaking into a system using spear phishing.

Recommendation:

Warn users of the spear-phishing risk, at least to the extent of the following topics:

1. What spear phishing (or phishing) is, and the best ways to recognise it.
2. The need to identify the counterparty if there is any doubt about the legitimacy of the sender.
3. They should not open attachments and links in e-mails if there is any doubt about the legitimacy of the sender.
4. They should not enable macros in MS Office-type files.
5. The possibility that executable files have been "masked" (such as "obrazek.png.exe", "text.txt.exe" or "dokument.pdf.exe").
6. How to react and where to seek advice if there is suspicion of spear phishing.

Furthermore, the guidance materials published on the website at https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/ can be used to address this issue. Material about spear-phishing risks is also available there. It is a good idea to supplement this information with the basic contact details of the IT security personnel and to inform users that they should immediately report the receipt of any spear-phishing e-mail.

Guidance material on phishing that you can download and send to users is available at: https://www.govcert.cz/cs/informacni-servis/doporuceni/2735-doporuceni-pro-chovani-v-pripade-obdrzeni-spear-phishingu/.

If you would like additional information, a more detailed analysis of spear-phishing methods and means of protection is downloadable from: https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/.

1.1.2 Prevent the launching of active content and macros, in .doc and .docx files in particular, using central settings.

Objective of the measure: To prevent the possibility of a system being compromised through MS Office macros.

Recommendation:

Macros in Microsoft Office documents are often used to distribute malware. To minimize this risk and in view of the necessity to adopt measures quickly, we recommend taking the following steps – as long as these are appropriate based on your organization's needs:

1. Disable macros for all users.
2. Enable macros for individual users upon request.

Guidelines for configuring the appropriate policy are provided in documentation on the Microsoft website.[1]

1.1.3 Immediately block all remote accesses to your infrastructure and block open services to the public network, with the exception of vital ones (public IP ranges can be checked through the available search engines of devices connected to the network, and thus ports opened or forgotten in the past, as well as services available from the public network, can be found)

Objective of the measure: To minimize the risk of an attacker breaking into the system using the vulnerabilities of the system or brute force.

Recommendation:

Verify services published to the Internet. Leave open only those services that are essential for the functioning of the organization. Those services mainly include communication that is:

1. essential for the functioning of the services supported by the system;
2. essential for the security of the system (remote monitoring, security updates for the system, etc.);
3. essential for informing the public (e-mail communication, web presentations, etc.);

[1] https://docs.microsoft.com/en-us/DeployOffice/security/plan-security-settings-for-vba-macros-in-office?redirectedfrom=MSDN#changedefault

4. essential for supporting communication infrastructures (DNS protocols, BGP, certificate verifications, etc.) and proxy servers.

This primarily entails restricting access to services from the Internet (such as access via VPN, RDP, SSH, or SMB protocols, database access, or system administration) if they are connected to important Systems and do not meet at least one of the above conditions.

If any of these access types cannot be blocked, it is a good idea to only allow access via VPN or for specific IP addresses.

1.1.4 Immediately create offline backups and proceed with such backups based on the importance of the data for your organisation

Objective of the measure: To ensure the availability of backups even in the event of a cybersecurity incident.

Recommendation:

For the safe storage of the backup files, it is vital to copy them to offline data media (flash drives, hard drives, or others) and to verify those data. This is ideally done by restoring the backup from the newly created medium. However, it can only be done outside the production environment. If this is not possible for technical reasons, at least the hashes of the offline backup files can be verified against the hashes of the online backup files. This procedure is crucial to ensure that the backups are not lost if the backup server or the virtualisation platform is compromised (or encrypted).

1.1.5 Check the consistency of already created backups

Objective of the measure: To ensure that the backup files will function in the event of a cybersecurity incident.

Recommendation:

Examine whether existing backup files are functional by performing a test restore of servers and stations. This can only be done outside the production environment. If you find that one or more backup files are non-functional, a new backup of the system must immediately be performed. These steps have to be taken starting with the most critical Systems. When examining the backup files, any interdependences should not be ignored. One example may be a database server or an entire database cluster employed elsewhere. In such cases, those Systems must be checked, too.

1.1.6 Update the antivirus solution used in your infrastructure

Objective of the measure: To ensure elementary protection from harmful code.

Recommendation:

A tool to protect from harmful code (antivirus, antimalware) should be employed in all possible Systems, including server operating systems. Primarily, this applies to Windows operating systems as they are the target in most cases. In the case of virtualised systems, protection using an agentless solution cannot be considered sufficient protection.

If the organisation does not use any tool for protection from harmful code, at least the built-in protection of the system must be activated, if it exists.

1.2 Other recommended steps that can be taken to prevent or mitigate the impacts of a cybersecurity incident

The recommendations provided below are listed according to the priority they should be given.

1.2.1 Change passwords to privileged accounts in the Systems. Examine and, if necessary, configure an appropriate policy for the use of privileged accounts.

Objective of the measure: To prevent a potential attacker who gets into the system from carrying out further actions.

Recommendation:

This measure consists of enforcing the change of all privileged account passwords in the manner set out for obliged entities pursuant to the applicable Decree No 82/2018, on cyber security, i.e. that passwords must contain a minimum of 17 characters and must be changed at least every 18 months. Other entities that do not fall under the Act on Cyber Security are also recommended to adopt this policy. It is also necessary to carry out an audit of the privileged accounts and to block those not used any more, and potentially remove authorisations from accounts that do not need them.

We recommend using *Fine Grained Password Policies*[2] to configure your password policy, which will allow password policies to be configured for various user groups. We also

[2] Microsoft documentation on the respective topic available at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10)?redirectedfrom=MSDN

recommend using the *Active Directory administrative tier model*[3] to configure the appropriate policy for the use of privileged accounts.

Furthermore, it is vital to prevent domain administrators logging into any stations or servers but the domain controller. The reason for this is to prevent an attacker from gaining a privileged account. Since the hash of the administrator remains recorded in the cache of the station, an attacker could gain domain administrator authorisation if the station were compromised.

1.2.2 Verify and ensure that the backup system is separated from the other systems in such a way that not even the top highest-level authorisation to the backed-up system would enable deleting the backups.

Objective of the measure: To prevent an attacker being able to delete backups if they get domain administrator authorisation.

Recommendation:

Secure the backup systems in such a way that the backup systems cannot be compromised and the backups cannot be deleted or damaged if a privileged account (of a domain/enterprise administrator, for example) is compromised.

If the backup system can be administered via a shared privileged account (such as a domain/enterprise administrator account), then an attacker will be able to delete, damage or encrypt the backup files.

In the Microsoft Office environment, this can be solved by disconnecting both physical and virtual machines that provide the backup service from the domain and by using local accounts for logging in, alternatively by creating a special account reserved for this activity. There is however a need to evaluate the impact on other system services and functions.

1.2.3 Prevent any access and interconnection between the systems important for ensuring the operation of the organisation and systems or networks which are not important for the provision of services or security of the system.

Objective of the measure: To prevent any interconnection of the systems (except where this is necessary) and thereby limit the opportunity for malware to spread.

Recommendation:

This entails limiting any communication to systems essential for the operation of the organisation (provision of services in particular). If another network (e.g. the Internet, another organisation's network, or another network of the organisation) can access the network which

[3] Microsoft documentation on the respective topic available at https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

is necessary for ensuring the operation of the organisation, you should consider how important this connection is for the provision of services or security of the system.

Limit communication between workstations wherever possible.

1.2.4 Check network segmentation and the management of the traffic between the segments, evaluate the situation and adopt any necessary measures to secure at least elementary segmentation.

Objective of the measure: To prevent a spread of malware or movement of an attacker.

Recommendation:

Network segmentation and the management of traffic between the segments (ports between segments, restrictions on allowed services) can significantly reduce the impacts of a potential cybersecurity incident. Check the configuration of your network elements for weak points or overly benevolent rules. Perform a check between the external and internal networks. Restrictive rules can make it more complicated for attackers and give the organisation time to react.

Limit communication between workstations wherever possible.

1.2.5 Consider updating all used systems on condition that the relevant updates have been tested. If an update has been tested and is functional, implement it.

Objective of the measure: To ensure that the systems used are updated and thereby improve their security and robustness against cybersecurity incidents.

Recommendation:

Systems that have not been updated often contain well-known flaws that attackers exploit to compromise those systems. It is therefore necessary to ensure that the systems used are updated as far as possible. If there is a compelling reason against updating the system (for example, updating would invalidate a warranty, the system could disintegrate, stop working, or there could be other unacceptable impacts), it is not necessary to update such a system. However, compensatory security measures will have to be taken.

It should be remembered that updating should not be performed if it could cause more damage than the potential cybersecurity incident or if performing such a task would have negative impacts on the provision of services.

In any event, each update must be tested outside the production system prior to its use, as described above.

1.2.6 Check the valid operational continuity plans and emergency response plans related to the operation of the systems to verify their validity, effectiveness and applicability, mainly with respect to potential unavailability of the systems.

Objective of the measure: To verify that operational continuity plans and emergency response plans exist and that they are updated and applicable in the event of an emergency.

Recommendation:

Verify that operational continuity plans and emergency response plans exist and that they are updated and valid. Check for any missing plans. Such verification should primarily address the following:

- the plans recognize the importance of the systems and anticipate the priority restoration of the critical systems;
    - system restoration prioritization takes account of the interdependence of systems and services;
- the plans contain lists of persons responsible for the individual system elements, and updated contact details of the responsible persons are available;
- there is an updated list of suppliers and their contact persons, including contact details (mobile phones, e-mails); it is important to verify the configuration of cooperation with suppliers in case of an emergency, the agreed response times, etc. (in the event of shortcomings or the absence of an agreement, we recommend agreeing with the suppliers on rules of cooperation in the event of an emergency).

1.2.7 Ensure that the operational continuity plans and the emergency response plans are kept separately from the systems for which they are prepared (for instance, on a separate memory medium or in hard copy, etc.).

Objective of the measure: To ensure that the plans are available in the event of an incident so they can be used if necessary.

Recommendation:

Experience with ransomware attacks has shown that operational continuity plans, emergency response plans and similar documents are often stored on systems/media that the attacker can encrypt or delete, or that are switched off to protect other systems. Consequently, the plans are not available at the critical moment. Hence such plans must be stored outside the systems, for example on a write-protected removable medium (if it is necessary to connect such medium to a potentially compromised computer) or as a hard copy.

1.2.8 If the operational continuity plans and emergency response plans related to system operation are not updated or have not been prepared at all, it is necessary to prepare them at least for the most critical systems which are important for the provision of services.

Objective of the measure: To have updated and applicable operational continuity and emergency response plans available so that the organisation is able to operate even in the event of a cybersecurity incident.

Recommendation:

If operational continuity and emergency response plans are missing, they have to be prepared at least to such extent that the availability of important systems could be restored according to them. The following items should be addressed as a priority:

- Define the rights and obligations of the administrators and persons involved in ensuring the functioning of the organisation. Who will do what and when during an emergency, escalation procedures, etc.
- Use a risk assessment and impact analysis to evaluate and assess potential risks related to a threat to the continuity of operations. An elementary scenario of what will happen if the confidentiality, availability and integrity of the data in the systems are compromised needs to be created, as well as the impacts on the provision of the given service.
- Based on the results of the risk assessment and impact analysis, set the objectives of operational continuity management by
    - determining the minimum level of the provided services acceptable for the use, operation and administration of the system;
    - determining the time needed to restore the operation of the minimum level of the provided system services after a cybersecurity incident; and
    - determining a data restoration point as the period for which data will be recovered after a cybersecurity incident or failure.
- Create procedures to fulfil the above objectives, i.e. how the organisation will ensure that a certain level of services is maintained, that the data can actually be restored, etc.

1.2.9 Do not delete any data about a cybersecurity incident without the prior consent of the Police of the Czech Republic or the National Cyber and Information Security Agency. Inform all your administrators and relevant security and IT (operational) roles about this obligation.

Objective of the measure: To ensure that an investigation of the cybersecurity incident is possible.

Recommendation:

All data (server images, security records, network monitoring records, etc.) are important for the investigation of a cybersecurity incident, namely to identify the source and method of spreading of malware in the network and to identify the devices that might be infected. With some types of ransomware, it might be possible to decrypt the data at a later date. Therefore, it is important not to delete any data without the permission of the Police of the Czech Republic or the National Cyber and Information Security Agency.

It should be emphasised that even careless handling of data can lead to the loss of metadata important for an investigation of the incident. This may further complicate post-emergency assistance. Persons obliged under the Act on Cyber Security must report a cybersecurity incident without delay after its detection. All other persons are also advised to contact the Agency without delay and report the incident. Incidents are to be reported using the e-mail address cert.incident@nukib.cz; however, outside working hours please first call the emergency phone number +420 725 502 878.

1.2.10 For health service providers only: Separate the communication network of medical equipment – modalities (e.g. CTs, X-ray machines) from the rest of the network.

Objective of the measure: To separate medical equipment from the rest of the network and thereby limit the spread of malware in the network.

Recommendation:

In order to be able to provide the required services even after a cybersecurity incident, medical equipment must be separated from other systems in such a way that the equipment remains operable when disconnected from the rest of the network. Open ports between networks are permissible but must be managed using a white list of allowed communication. The given measures are vital to preserving the security of these systems, since those specialized systems often run on unique and outdated operating systems and other means of securing these systems are not always applicable.

1.2.11 General recommendations of the National Cyber and Information Security Agency to administrators

Besides all the above-mentioned recommendations aimed directly at the threat specified in the Warning, the National Cyber and Information Security Agency also considers it appropriate to mention the document "Security Recommendations for Administrators". These recommendations are intended for both cybersecurity managers and heads of IT departments, as well as for anybody interested in cybersecurity at the practical and professional level. The document can be downloaded at https://www.govcert.cz/cs/informacni-servis/doporuceni/2736-doporuceni-nukib-pro-administratory-verze-4-0/

Document version

Date	Version	Changed by (name)	Change
17/04/2020	1.0	Regulations Department GovCERT.CZ Department	Creation of the document