BEST PRACTICES

FOR MANAGEMENT STAFF

THE BEST PRACTICES FOR MANAGEMENT STAFF ARE 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

1. PROTECTION OF WORKSTATIONS AND USERS 03

1.1 Develop a policy regarding informing the employees about threats 03

1.2 Ensure regular training and raise awareness among employees 03

1.3 Develop a policy regarding connecting mobile devices 04

1.4 Develop a procedure to respond to unknown and untrusted data carriers/devices 05

1.5 Develop a procedure to respond to threats detected by the antivirus 05

1.6 Develop a policy on software installation by workstation users 06

1.7 Implement regular checks of software and antivirus updates 06

2. SAFETY OF REMOTE WORK AND MOBILE DEVICES 07

2.1 Ensure that employees have the opportunity to use VPN 07

2.2 Specify safety requirements for equipment used for remote work 07

2.3 Develop a policy to determine which services are available for particular types of equipment 08

2.4 Establish policies on data carrier and drive encryption 09

2.5 Prepare procedures on dealing with lost or stolen equipment 09

3. DATA PROTECTION 10

3.1 Establish a backup policy 10

3.2 Establish a policy of cloud storage 11

3.3 Determine procedures for dealing with used/unnecessary data carriers 12

3.4 Establish a policy on data access 12

4. PROTECTION OF INTERNET SERVICE, NETWORK INFRASTRUCTURE AND TRAFFIC 13

4.1 Establish an access policy regarding services 13

4.2 Ensure a separate network for employees and guests' private devices 14

5. OTHER 15

5.1 Perform penetration tests periodically 15

6. EMAIL PROTECTION 16

6.1 Establish a security policy for information transmitted electronically 16

6.2 Prepare a procedure for responding to suspicious messages 16

03

PROTECTION OF WORKSTATIONS AND USERS

Develop a policy regarding informing the employees about threats

Prepare a policy that will regulate when and how employees should be informed about threats, ongoing attacks and recommended responses. The policy should regulate:
In which situations users should be notified (e.g. ongoing phishing attacks, detection of a vulnerability in the software, etc.).
Who should send information (usually IT department).
How information should be sent (e.g. mailing list).

EXPLANATION

Good communication about current risks will enable employees to react better to them, and employee awareness and alertness will increase.

Ensure regular training and raise awareness among employees

Take care of regular training and prepare the employees to deal with possible threats. This can be done in a variety of ways, in addition to standard training, you can use web-based courses, introduce regular mailing of short safety advice, etc.

EXPLANATION

Usually the weakest link in systems is man and a lot of attacks are based on sociotechnology. For this reason, efforts should be made to prepare employees appropriately.

04

PROTECTION OF WORKSTATIONS AND USERS

Develop a policy regarding connecting mobile devices

Depending on the importance of the data and the needs of the company you can:

- Completely forbid the use of mobile data carriers.
- Allow the use of only encrypted and secured company equipment.
- Introduce requirements for the data carriers (encryption, no removal from company facilities, no connection to untrusted computers).
- Restrict what data can be copied onto mobile data carriers.

The developed policy should also be followed by technical solutions implemented by the administrators. Depending on the chosen policy, this could be for example:

- Total blocking of USB ports.
- Installing software to monitor devices which are plugged in.
- Mandatory virus scanning of devices when connected.
- Inventory of devices and the data stored on them so that you can estimate the potential risk if a device is lost or stolen.

EXPLANATION

Mobile devices such as flash drives, SD cards, portable drives, phones involve many risks, such as:

- Infection of the computer with malware - accidental or intentional cause by attackers against the company.
- Data leakage from the company.
- Loss of control over data storage and access control due to the large number of mobile data carriers.

Therefore, a policy should be developed to regulate the connection of such mobile data carriers.

05

PROTECTION OF WORKSTATIONS AND USERS

Develop a procedure to respond to unknown and untrusted data carriers/devices

Develop a procedure which will regulate the response to unknown and untrusted data carriers or devices. It is usually appropriate to give the data carrier to administrators, who can examine it in safe environment.

EXPLANATION

The appearance of unknown and untrusted data carriers/devices may mean an attempted attack based on leaving such equipment at the company in the hope of it being connected to the computer. This procedure will make it easier for employees to react to such situations.

Develop a procedure to respond to threats detected by the antivirus

The correct response is to immediately report the incident to the IT department, which can then analyze it further and react accordingly.

EXPLANATION

Owing to the developed procedure , the user will know how to react to the threat reported by the antivirus and as a result the IT department will be able to react faster.

06

PROTECTION OF WORKSTATIONS AND USERS

Develop a policy on software installation by workstation users

Prepare a policy aimed at regulating the installation of software by workstation users. The safest approach is to allow software only from the so-called whitelist, which consists of trusted programs, to be installed. In line with this approach, if you want to install a new program, you must beforehand ask the IT department to verify it and add it to the list. An alternative approach is to block the installation of software from the so-called blacklist, i.e. the list of malicious programs. This is a solution that allows more flexibility, but at the same time entails more risk.

EXPLANATION

Unconscious installation of an infected or vulnerable program by an employee is one of the sources of threats.

Implement regular checks of software and antivirus updates

In consultation with the administrators, prepare a procedure appropriate for the company to regularly check the software updates.

EXPLANATION

Update check - especially of systems connected to the Internet - is a certain minimum of care for infrastructure security. It usually provides you with protection against most of the commonly known (and therefore often the easiest to use) vulnerabilities and errors.

07

SAFETY OF REMOTE WORK AND MOBILE DEVICES

Ensure that employees have the opportunity to use VPN

If employees working remotely have access to sensitive data and services, it is recommended to provide them with a Virtual Private Network (VPN) and introduce a mandatory use of it.

EXPLANATION

VPN significantly increases a safety of data transmission (See the Technical guide: VPN).

Specify safety requirements for equipment used for remote work

Create a policy to regulate safety requirements for devices used for remote work. These devices should have a level of security appropriate to the access that can be gained from them. One of the basic security measures is drive encryption.

EXPLANATION

Non-compliance of devices, used for remote work, with security requirements can significantly increase the risk of data leakage or hacking attack of the company's services.

08

SAFETY OF REMOTE WORK AND MOBILE DEVICES

Develop a policy to determine which services are available for particular types of equipment

Prepare a policy that defines which services should be available for particular types of devices. When creating such a policy you must take into account:

- The risks associated with a specific type of equipment.
- Threats associated with the place where the devices will be used.
- Consequences of stealing data from a given service.
- Consequences of unauthorized access to a given service.

For example, the policy can be formulated in the following way:

- Company mobile devices, managed and secured by IT department, connected by VPN, have access to all services.
- Company mobile devices, managed and secured by IT department, connected without VPN have access only to X, Y, Z services.
- Employee's private mobile computers which fulfill appropriate security requirements (e.g. drive encryption) have access only to X, Y, Z services.
- Other employees' private mobile devices (phones, tablets) have access only to basic services with low risk, e.g. webmail client.

EXPLANATION

Such a policy allows to limit potential losses resulting from seizing a device, malware infection or man-in-the-middle attacks (see Technical Guide: Man-in-the-middle attack).

09

SAFETY OF REMOTE WORK AND MOBILE DEVICES

Establish policies on data carrier and drive encryption

If there is sensitive and business-critical data on some devices (e.g. laptops, phones, external drives), implement a policy of full data carrier and drive encryption.

EXPLANATION

Encryption significantly reduces the risk of unauthorized access to data, e.g. when a laptop is stolen.

Prepare procedures on dealing with lost or stolen equipment

The developed procedures should include:

- Usually, a desired reaction, in case of loss or theft, is reporting it to the appropriate person or IT department.
- Information to be provided by the user of the device - what data was on the device, in what condition the device was (turned off, logged out, logged in) and what were the circumstances of the incident.
- Actions to be undertaken by the IT department to reduce the risk and possible losses - e.g. revoking the account permissions from a stolen device, blocking access to services, remotely cleaning the drive, trying to locate the device, reporting to the police.

EXPLANATION

The loss or theft of a device which contains company data or gives access to company's services can be a serious threat to company operations. Therefore, a quick and effective response is needed. Prepared procedures can significantly accelerate the whole process.

10

DATA PROTECTION

Establish a backup policy

Develop a policy that defines the following elements:

- What data should be backed up - this point needs to identify data which is important to the company and should be backed up.
- How often should backups be made - this point ought to identify how often the data identified in the previous section should be backed up. You can divide the data into several categories, and then specify the frequency for each category. The frequency of backups should depend on how long the company can sustain without data.
- How many backups should be made - if there is only one copy, it can be very easily lost. Data should ultimately be stored in at least 3 copies with use of the 3-2-1 strategy.

EXPLANATION

The 3-2-1 strategy means having at least 3 backups of the data:

1. Data stored locally, on users' devices.Lokalna kopia zapasowa – umożliwia ona szybkie odzyskanie danych w razie awarii 1.
2. Local backup - this enables fast data recovery in case of failure 1.
3. External backup - locating a copy of the data in an external location protects the company in the event of simultaneous destruction of the data described in points 1 and 2 (e.g. due to a fire at the company's headquarters). If you use the cloud for an external backup, you need to pay attention to your cloud storage policy.

If we store data only on the cloud, not on users' devices, it must be verified whether the cloud provider creates and stores backups in accordance with the company's requirements (number of backups, different locations, time of possible data recovery).

11

DATA PROTECTION

Establish a policy of cloud storage

Establish a policy which defines which data can be stored on the particular cloud solution. The policy should be formulated considering:

- The legal aspects determining where the data should be stored (e.g. some of the data must be stored within the European Union).
- The legal aspects of a given cloud solution (who has access to the data stored on the cloud, in which situations they can be made available to a third party, e.g. the police).
- The level of security provided by a given cloud solution (e.g. it can be verified whether data leakage have already occurred, whether data is encrypted on disks and during transmission, etc.).

EXPLANATION

The policy will allow conscious utilization of cloud solutions and avoid possible legal problems and incidents.

DATA PROTECTION

Determine procedures for dealing with used/unnecessary data carriers

The procedures should be prepared with the participation of administrators and include information:

- Which carriers are being destroyed.
- How the data carriers are cleaned and destroyed.
- Where the destroyed carriers are placed.

EXPLANATION

The developed procedures will help to avoid data leakages caused by discarding carriers without prior cleaning by the administrators.

Establish a policy on data access

Prepare a policy that defines who can have access to which data and on what conditions. For example:

Financial data is accessible for:
- A chairperson from a company computer and a company laptop.
- An accountant from the company's computer.

Preparation of such a policy requires:

1. Categorization of company data.
2. Specification who should have access to each category.
3. Specification for each person having access to a given category, which device the person can use to access the data.

EXPLANATION

This policy will reduce the risk of data leakage and, in the event of an incident, it will be easier to identify the source of the leakage.

13

PROTECTION OF INTERNET SERVICE, NETWORK INFRASTRUCTURE AND TRAFFIC

Establish an access policy regarding services

Just like in the section: "Establish data access policy", a similar procedure should be followed for company's services. It is necessary to define who can have access to which services and on what conditions, e.g.:

The holiday reporting system should be accessible to:

- Every employee from any device.

Accounting services should be accessible to:

- Every employee of the financial department from the equipment which is a part of company network.

EXPLANATION

The policy will reduce the risk of data leakage or unauthorized change and, in the event of a possible incident, will simplify the procedure after a hacking attack .

This policy is closely related to the policy on data access (Data protection) and to the policy defining which services are available for particular types of equipment (Security of remote work).

14 PROTECTION OF INTERNET SERVICE, NETWORK INFRASTRUCTURE AND TRAFFIC

Ensure a separate network for employees and guests' private devices

If some of the company's services or data are only available from the company's internal network, it is recommended to consider creation of a separate network for company devices.

EXPLANATION

Connecting employees or guests' private devices to the company's internal network involves a considerable risk, as these devices are not necessarily as well protected as company devices. There is also a risk that an attacker will pretend to be a "guest" of the company. Connections from this separate network should be treated as external connections.

This policy is strictly related both to the policy regarding access to data and the policy establishing an access regarding service (Remote work security).

15

OTHER

Perform penetration tests periodically

The level of infrastructure security and employee awareness should be examined from time to time. Penetration tests, commissioned to an external company, are only one of the possibilities and should be considered so. It is important that the testing method checks the actual security and awareness and not just the documentation of it.

16

EMAIL PROTECTION

Establish a security policy for information transmitted electronically

Develop a policy for the transmission of individual information by electronic means, with particular reference to information of particular importance to your company (company secret), personal data, etc. As for particularly sensitive data, use additional methods of data leakage protection (see: Ensure encryption of the messages and attachments).

EXPLANATION

The categorization of information and the definition of rules for electronic transmission will result in clear procedures for employees. Those procedures will determine in which cases additional safeguards should be applied to protect against data leakage or potential theft.

Prepare a procedure for responding to suspicious messages

Develop a procedure to ensure that employees know how to respond to suspicious messages and to whom they should report such incidents.

EXPLANATION

The procedure will make it clear to your employees how they should behave after receiving a suspicious message. This will reduce the number of potentially dangerous situations and enable a more effective response to security incidents.

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.