BEST PRACTICES

FOR IT ADMINISTRATORS

THE BEST PRACTICES FOR IT ADMINISTRATORS 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

03

RESOURCE MANAGEMENT

Implement the mechanisms of resource management

From the administrator's point of view, it is important to continuously collect information about hardware, software and data as well as their owners.

EXPLANATION

Resource management itself is rather an activity at management level, but it should also (or at least) be carried out at technical level. Hardware, software and data resources should be inventoried and have their owners assigned.
Software to facilitate resource management is provided by many manufacturers. In the links you can find only examples of free and open-source solutions.

LINKS:

Snite-IT
GLPI
Ralph

04

WORKSTATIONS AND LAPTOPS

Restrict users' access to administrative accounts

The users should not use an account with administrative powers by default (e.g. Administrator in Windows or root in Linux).

EXPLANATION

In most cases, the user should probably not have access to the local administrator account at all, and in the possible exceptions, they should use the mechanism for increasing powers through requirement of a password. Not only will this action restrict the user's ability to perform erroneous actions, but also it will limit any malware powers that may interfere with the system.

Disable the installation of software by users

As with the administrative powers, users' ability to install new software should be an exception rather than a rule.

EXPLANATION

The administrator should control what is installed on employees' computers to reduce the risk of installing malicious software and damage of the system. There are obviously exceptions to this rule e.g. IT developers may have a need to install new applications on their own.

WORKSTATIONS AND LAPTOPS

Disable automatic startup and playback of external data carrier

Workstations shall have automatic external media playback disabled.

EXPLANATION

The automatic startup and playback of external data carriers can contribute to the installation of malware when connecting an external data carrier such as a flash drive.

LINKS:

Shutdown instructions for Windows 10

WORKSTATIONS AND LAPTOPS

Take care of firmware, operating systems and software

The hardware should usually have the latest firmware installed and the software should always be up-to-date.

EXPLANATION

Remember about updates - especially updates of systems connected to the Internet - it is an absolute minimum to ensure the security. It usually provides protection against most of the commonly known (and therefore often the easiest to exploit) vulnerabilities and errors.

This does not mean that updates should be installed thoughtlessly and automatically. It is worthwhile to read the changes introduced in the new version and make an individual decision whether an update is needed and will not cause difficulties for users.

It is also worth having a permanent plan to install patches - e.g. install them in the evening on one particular day of the week. A good practice is also to test the update in a testing environment in advance.

07

WORKSTATIONS AND LAPTOPS

Take care of antivirus and antimalware

Workstations should be protected against malicious software.

EXPLANATION

In many cases, antivirus and antimalware program can stop a workstation infection. The choice of a specific solution depends on the case and the funds available. Often, the protection software included with the operating system or with the Web browser will be sufficient. In some situations you may need to purchase additional software installed on workstations.

In some configurations, the protection can be implemented outside of the user's system - as in the case of implementation of employees' desktop virtualization (VDI technologies) or when only files from outside can pose a threat (then e.g. an antimalware system at the entrance to the company's network is sufficient).

WORKSTATIONS AND LAPTOPS

Implement appropriate log file and monitor the incident

Workstations should be monitored - system logfile should be reviewed regularly and serious incidents should trigger an easily noticeable for the administrator alarm. Ideally, the log files are collected in one place - in an application that facilitates their analysis and event correlation (SIEM).

EXPLANATION

Infrastructure intrusions can remain undetected for months. Hard drives can stop working unnoticed. The administrator does not notice this because he does not monitor in any way what is happening in workstations

Monitoring of the infrastructure is a critical element of security. In the case of workstations, log files are the most informative. They should be collected in one central point, which allows for correlation and analysis of incidents in the context of other network occurrences. Such a point will usually be SIEM (Security information and event management).

The links refer to free, open-source solutions, but there are also many commercial SIEMs.

LINKS:

Apache Metron
OSSEC
OSSIM

09 MOBILE AND PORTABLE DEVICES

Configure drive encryption for each device and data carrier included in the encryption policy

Enable disk encryption on all requiring it devices according to the policy.

EXPLANATION

Encrypting drives, flash drives and other internal and external devices, on which data can be stored, is currently very simple - it requires only a few decisions.
For internal drives of personal computers and mobile devices such as smartphones, the best solution will often be to enable the encryption embedded in the system and provided by the developers of the operating system:

- Bitlocker for Windows,
- LUKS for Linux,
- FileVault for macOS.

The configuration of Android smartphones depends on their manufacturer, but in most cases data encryption (in older versions it is the encryption of the whole drive, and in newer versions it is the encryption of files) requires setting a lock code.

As for external data carriers, the decision will depend on the degree of compatibility with different systems under which the carrier will be used. If it is a unified environment, we can use system mechanisms, similar to internal drives. For more diverse implementations, a solution that works under different systems should be chosen. VeraCrypt is generally a good choice.

You should also decide who can decrypt the data and when - whether it should only be the user who knows the password, or the administrator, or whether the data should be decrypted automatically at the startup of the device (while the drive is in the right device).

LINKS:

How to activate data encryption in iOS
VeraCrypt

MOBILE AND PORTABLE DEVICES

Provide a VPN for remote working

If your company allows one to work remotely or outside of the office, ensure that employees only connect to the office via a virtual private network (VPN).

EXPLANATION

Simply put, VPN extends your company's private network to remote desktops. It can be used both to secure remote access protocols (such as RDP and VNC) as well as to secure access to remote files (CIFS, NFS). When VPN is properly configured, an employee does not see the difference between working in the office and at home. Additionally, employees' connections and files are protected at the same (or similar) level as if they were at work.

Specific solutions will depend on company's budget, hardware and software. Practically every network equipment supplier will also have versions of hardware which allow VPN configuration. OpenVPN will be an affordable and quite effective solution.

LINKS:

OpenVPN

MOBILE AND PORTABLE DEVICES

Delete data from every lost or stolen device

Should the device be lost or stolen, delete data remotely.

EXPLANATION

Mobile devices - especially smartphones - often have a built-in ability to delete data remotely if they are lost. Only if the device is turned on will the function work. However, it is worth using whenever we suspect that the lost device may have encompassed account data or any other company data.

One must simply remember that these functions usually require preventive (i.e. before the device is lost) configuration.

LINKS:

Finding or blocking a lost Android device or data deleting

iCloud: Erase your device with Find My iPhone

VALUABLE DATA

Implement automatic backup mechanisms

Make sure that backups are automatically created (according to the appropriate, predefined policy) and transferred to the right place.

EXPLANATION

Regular, scheduled backups should practically always be made automatically. If the backups are made manually, it may almost certainly happen that someone forgets about it, is on a leave or has no time for it.

It is of no importance which tool will be used to create them - practically each one of them will have the feature of automatic starting on the set dates.

Additionally, make certain that the whole process is automated - both making a local and remote backup.

Old backups should also be deleted automatically - it is better to have space for new copies.

VALUABLE DATA

Protect the accessibility, confidentiality and integrity of backups

Take care of your backups as much as you take care of your actively used data:

- Regularly test the integrity of your backups and data recovery from them.
- Protect your backups from unauthorized access e.g. backups stored in external services should be encrypted and on local external data carriers- in a safe location.

EXPLANATION

To realize at the time of a major breakdown that all data backups rendered to be unusable would be unfortunate. To verify whether the backups work, one should attempt to recover data regularly.

Backup storage in a less secure way than the original data (e.g. on a server that can be accessed by more people than the original source or on CDs in an unclosed drawer) may pose another problem. One should ensure the confidentiality of backups by choosing the right location to store them through e.g. proper access control or encryption.

Naturally one may not forget that the backups should always be accessible whenever they are needed - it is significant to ensure that a situation in which the only employee who has the access to the backups is on the leave will not appear.

VALUABLE DATA

Before discarding the data carrier, erase all the data

Before throwing away any data carrier, erase all data from it. For an HDD, overwrite the entire drive at least once. For SSD, clean the drive with the tools provided by the manufacturer.

EXPLANATION

Usually, deleting a file itself means only marking the file as deleted while in fact it does not erase its contents from the disk what makes the matter complicated. The space taken by the contents of the file will be used again after some time. The matter becomes even more complicated with SSDs which try to balance the memory usage so that there is no control over the storage space on the disk.

As for HDDs, overwriting data with zeros, ones or random values will make data recovery significantly more difficult. Data overwritten only once will make the recovery more difficult, but still there are methods that can be used to partially recover the data. To reduce the likelihood of such a situation, it is recommended to repeat the overwriting several times.

The best way to remove data from the SSD is to use the mechanisms provided by the manufacturer. Such a mechanism will often be called "Secure Erase". Ultimately, the drive can also be physically destroyed (but unlike HDDs, demagnetization will not work in this case).

It is also quite a reliable method to encrypt data on the disk from the first time it is used.

INTERNET SERVICES AND NETWORK INFRASTRUCTURE

Provide encryption for all network services

Whether those are services for employees (VPN, email) or for customers, they should all use appropriate for the type of service (e.g. HTTPS, SMTP using TLS, etc.) encrypted connections.

EXPLANATION

Currently, there are practically no arguments against the use of encryption in every network service. In most cases, TLS certificates are free of charge, because they are available on Let's Encrypt - a project created, among others, by Mozilla. It provides free certificates and software for its automatic renewal.

Moreover, browsers treat encryption as the norm and actively communicate to the user that a website which does not use HTTPS may be dangerous.

LINKS:

Let's Encrypt

INTERNET SERVICES AND NETWORK INFRASTRUCTURE

Configure the encryption accordingly

The services which use encryption should be continuously adapted to new configuration standards.

EXPLANATION

The standards for selecting cryptographic functions often change. It is difficult to keep abreast of these changes and keep up with them, so you often use a default configuration or use for years the one that was once chosen. However, cryptographic functions and protocols become out of date and have errors. Therefore, it is necessary to update the appropriate configurations once in a while (e.g. once a year).

At least two websites help in this situation: Qualys SSL Server Test and Mozilla SSL Configuration Generator – the former tests our current configuration and the latter provides ready-made directives to configure the most popular servers.

LINKS:

Qualys SSL Server Test
Mozilla SSL Configuration Generator

INTERNET SERVICES AND NETWORK INFRASTRUCTURE

Restrict the access to services outside of the internal network

In other words: configure the firewall at the entrance to your corporate network appropriately.

EXPLANATION

The basic principle of firewall configuration is to block all traffic, and only afterwards, add exceptions for the services needed. The firewall should be deployed at every possible entrance to the corporate network and between different security domains within the network. As for the security, it is of no great importance whether it will be a dedicated hardware solution or, for example, a dedicated Linux inode based on iptables (although, as for the performance, it may already be significant).

LINKS:

Guidelines on Firewalls and Firewall Policy

INTERNET SERVICES AND NETWORK INFRASTRUCTURE

Implement appropriate monitoring of the network

The network should be monitored not only at the entrance to the corporate network but also within it.

EXPLANATION

Monitoring of the network is one of the basic methods of ensuring security, together with the monitoring of log files on hosts.

At this point, the main focus should be on monitoring of packets and network traffic.One may use IDS (Intrusion Detection System) which, in the most common configuration, receive a copy of the whole traffic and analyze it.The results of the analysis are worth sending to the SIEM system (Security information and event management) which will allow to correlate various other incidents with network traffic.

The links refer to free, open-source solutions, but there are also many commercial IDS and SIEMs.

LINKS:

Apache Metron
Zeek
Snort
Suricata

INTERNET SERVICES AND NETWORK INFRASTRUCTURE

Consider DNS filtering

If there are no contraindications to this, it is recommended to centralize DNS access in the company in one server (recursive DNS) and then filter dangerous and unwanted addresses.

EXPLANATION

DNS filtering allows to reduce the probability of malware infection - it can block the installer (which e.g. will not be able to download further part of the virus) or prevent communication between the already infected computer and the person who controls the malware.

Another advantage is the possibility to block potential sources of infection - e.g. advertisements or phishing websites.

LINKS:

Response Policy Zones

Separate different security domains

Split hosts and services with different security levels into separate virtual or physical networks.

EXPLANATION

Services and hosts with different security levels, different origins, different owners should be separated from each other. The simplest example is the division of a WiFi network into the one to which employees can connect from private devices as well as for guests, and the actual company network where hosts with internal services are located. This separation reduces the likelihood that infected or malicious hosts will gain control over more trusted devices.

IDENTIFICATION AND AUTHENTICATION

Consider introducing an SSO (single sign-on)

In systems where users exploit more than one resource (e.g. in addition to their workstation, they have access to network resources), consider implementing a centralized single sign-on (SSO).

EXPLANATION

Single sign-on has at least two advantages:

1. The users less frequently have to enter their password and do not have to remember many passwords.
2. Applications do not have to remember the user's password - this reduces the number of places where the password is stored in any form.

In practice, implementations based on Kerberos and LDAP are most often used. These are, for example:

1. Microsoft Active Directory,
2. RedHat Identity Manager,
3. Oracle Identity Management.

LINKS:

Microsoft Active Directory
RedHat Identity Management
Oracle Identity Management

IDENTIFICATION AND AUTHENTICATION

Introduce two-component authentication (2FA)

Consider introducing two-component authentication - especially in the remote services.

EXPLANATION

Two-component authentication significantly increases user safety and reduces the risk of phishing. Although often found mainly in web services, it is also easy to set up for remote access to workstations (e.g. RDP, SSH) or files.

Just remember that when you also deploy SSOs, this two-component authentication makes sense only if deployed for all services or at least all services from one protected domain (e.g. all remote services).

LINKS:

YubiKey configuration as a second component in Windows

EMAIL

Verify who and when has access to your mail in an external web hosting service.

If you are using an external mailing or hosting service, mind who can access your data and when one can gain access to your data. Confidential data is best transmitted in an encrypted form.

EXPLANATION

In many free of charge mail services, incoming emails are scanned by the service provider's automaton. It is important to know what are the conditions of sharing your data with third parties by a given provider.

Verify what is the maximum downtime the external service provider commits to

If you are using an external mailing or hosting service, pay attention to the maximum downtime or uptime provided.

EXPLANATION

Both of these terms define the so-called service availability, i.e. the time of failure-free operation of the service in relation to the total time during which the service should be provided to clients. Downtime is the maximum time during which a given service may be unavailable (due to breakdowns, etc.) without penalty for the provider.

Uptime of 99.9% means that the provider declares the service availability for 99.9% of the time - i.e. during one year the service may be unavailable for a maximum of 8 hours and 20 minutes.

EMAIL

Ensure regular backups

As for all important data, ensure regular backups. If you use external services, make sure that your provider includes also a backup service.

Ensure encrypted transport of messages

Require use of encryption for access connections (IMAP, POP3, SMTP for users). For connections between servers (SMTP), encryption is preferred.

EXPLANATION

The end user communicates with his mail server with use of IMAP, POP3 (receiving mail) and SMTP (sending mail) protocols. This communication should be encrypted using TLS protocol.
Similarly, communication between servers with use of SMTP protocol should be encrypted. However, not all servers support such communication. Therefore, it is recommended to support STARTLS announcement for incoming mail and to prefer encryption for outgoing mail while allowing unencrypted communication.

For individual servers it is also possible to force encrypted communication in SMTP server policies.

EMAIL

Implement solutions to hinder email spoofing

Deploy SPF, DKIM and DMARC.

EXPLANATION

In their basic form, the protocols used for email do not ensure verification of the origin of messages. In particular, the sender's address may be forged. Solutions such as SPF, DKIM and DMARC implemented by the owner of the mail server allow the recipients' servers to verify whether the message they received actually comes from the declared location.

Implement solutions to verify the sender of the message

Implement the verification of the correct SPF, DKIM and DMARC and configure the spam filters in the mail server.

EXPLANATION

In their basic form, the protocols used for email do not ensure verification of the origin of messages. In particular, the sender's address may be forged. If the sender of the message has implemented SPF, DKIM and DMARC, the recipient can verify whether the message actually comes from him and decide whether to reject it or mark it as spam.

Anti-spam filters provide additional protection and, based on many parameters of the message, are able to eliminate a significant amount of unwanted mail, especially simple phishing and malware attacks.

EMAIL

Make sure that your server is not an open mail relay

Make sure that your mail server allows only your users to send mail. Require user authentication for sending mail and limit the range of addresses from which mail can be sent to internal addresses only.

EXPLANATION

Open mail relay is a term for a server that allows to send mail which does not come from its users. In other words, anyone can send a message with its help impersonating another person (especially some real user whom it serves). These servers are the main source of SPAM and forged messages. One of the many effects of such a configuration will be placing the server on the blacklists, which will result in the recipients ignoring the mail coming out of it.

The basic way of protection is to introduce the required authentication for mail. Similarly, you can limit the list of addresses from which sending is allowed only to internal addresses in the enterprise network.

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.