Safeonweb
@Work

AN INITIATIVE BY

CENTRE FOR CYBER SECURITY BELGIUM

CYBER FUNDAMENTALS

SMALL

Version 2023-03-01

Centre for Cyber security Belgium
18 Rue de la Loi
1000 Brussels
Belgium

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

Table of Contents

Introduction

The **CCB Cyberfundamentals Framework** is a set of concrete measures to:

- protect data,
- significantly reduce the risk of the most common cyber-attacks,
- increase an organisation's cyber resilience.

To respond to the severity of the threat an organisation is exposed to, in addition to the starting level **Small**, 3 assurance levels are provided: **Basic, Important and Essential**.

The **starting level Small** allows an organisation to make an initial assessment, excluding the aspects related to the internal development of applications.

The starting level Small is intended for micro-organisations (except high-risk environment) or organisations with limited technical knowledge.

The framework is a living document and will continue to be updated and improved considering the feedback received from stakeholders, evolving risk of specific cybersecurity threats, availability of technical solutions and progressive insight.

1 PROTECT ALL LOGINS WITH MULTI-FACTOR AUTHENTICATION

Use Multi-Factor Authentication whenever possible.
Always use Multi-Factor Authentication on remote access

Guidance

Most Multi-Factor Authentication tools combine your password with things you have (smartphone, badge, ID card) or things you are (fingerprint). Using multiple elements to authenticate reduces the risk of hacking.

- Use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.
  If you opt for a typical password:
  - Make it long, with lower- and upper-case characters, possibly also numbers and special characters.
  - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”.
  - Avoid using personal info that can be found online.
- And whether you use passphrases or passwords
  - Do not reuse them elsewhere.
  - Change password as soon as a suspicion arises that they have been compromised.
- Enable Multi-Factor Authentication. There are a lot of MFA tools available, it is best to choose an MFA tool that offers a variety of authentication options.
  MFA is of the utmost importance for internet facing systems such as for example remote access. Remote access can be realized through for example VPN (Virtual Private Network), RDP (Remote Desktop Protocol).

2 INSTALL ALL SECURITY UPDATES IMMEDIATELY

Implement security updates/patches for all your software as soon as they are available.

Guidance

- As developers battle with cybercriminals to make their software more secure and less vulnerable to the latest attacks, patching as soon as possible is the key to greater cyber security.
- Consider the below measures:
  - Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your organisation.
  - Install only vendor-supported versions of software you want to use.
  - Automate the update process as much as possible by setting automatic updates as default setting on your endpoints operating systems.
  - There are products that can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use. If you don’t use these products, designate a day each month to check the availability of new patches and install them.

3 INSTALL ANTIVIRUS

Implement an anti-virus solution on all types of devices and keep it up-to-date in order to ensure its continuous effectiveness.

Guidance

Even with the best precautions, you can be faced with an intrusion of a virus or a malware. An anti-malware software is a second barrier that protects you from the impact of cyber-incidents.

- The selected anti-malware software should protect against all kinds of malware such as viruses, spyware, adware and rootkits.
- It is recommended to set the anti-malware software to automatically check for updates at least daily (or when available in "real-time"), and then soon run a full scan. When multiple devices (home computers, laptops, tablets...) are used, anti-malware software should be installed and updated on all these devices.
- As a preventive measure, following rules should be applied:
  - Do not share USB drives or external hard drives between personal and business computers or devices.
  - Do not connect any unknown / untrusted hardware into your system or network and do not insert any unknown external USB drive. These devices may have malware on them. Disable the AutoRun feature for portable drives (USB, Optical...) on your business computers to help prevent such malicious programs from installing on your systems.
  - Do not install pirated software as it may contain malware.

4 SECURE YOUR NETWORK

Protect your network by installing a firewall.
Protect data on the network accessed via WiFi using wireless encryption standards.
Pay specific attention to remote access security.

Guidance

- Don’t share you WIFI passwords with anyone.
- If needed separate your Guest/Visitors WIFI network from your professional network.
- Firewalls should be installed and configured between your internal network and the internet. This may be a function of a (wireless) access point/router, or it may be a function of a router provided by the Internet Service Provider (ISP). The firewalls should be activated and updated. You might check your ISP service catalogue on provided Network security services.
  - Ensure that the administrative password of your firewall is changed upon installation and regularly thereafter. Also consider changing the administrator’s log-in
  - Encryption makes your electronically stored information unreadable to anyone not having the correct password or key. Set your router to use at least WiFi Protected Access (WPA-2 or WPA-3 where possible), with the Advanced Encryption Standard (AES) for encryption.

5 BACKUP YOUR DATA

Regularly perform automated backups of your information.
Put a back-up OFF LINE (not connected to the network) weekly or every few weeks.
After mayor changes, back-up your systems so you can restore them more easily

Guidance
Think about how much you rely on your organisation-critical data. Creating and testing back-ups will allow you to restore your data and ICT systems in the event of a major cybersecurity incident (e.g. ransomware attack). Some basic guidelines to consider:

- Identify what data you need to back-up. This is the essential data/information that your organisation couldn't function without.
- Determine the back-up frequency based on the amount of data (updated or created) that will be lost or need to be re-entered after an outage.
- Separate back-up media from your other storage systems. An offline back-up is very important to limit the possibility that your back-up is also encrypted or wiped in case of a hacking.
- Test restoring the data at regular intervals. It is also a basic check whether the back-up procedure runs fine.

6 ADMINISTRATION RIGHTS

Ensure that no one works with administrator privileges for daily tasks.

Guidance
An administrator has a lot of access to your system. Protecting these accounts is very important because they have a lot of value to cybercriminals. Consider the following principles to protect these accounts:

- Separate administrator accounts from user accounts. For daily work, a user account without administrator privileges suffices.
- Require Multifactor Authentication for all access via administrator accounts.

7 FINAL RECOMMENDATIONS

Physically protect your computers and mobile devices against theft or improper use.

Restrict access to premises, back-ups, servers, and network components to authorized individuals only.

Know how and who to contact in case of a cyber incident.

Guidance

- Physical security and access restriction:
  - Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to your organisation.
  - There are affordably priced mobile device management systems that can be an option if you use mobile devices a lot. Enabling of applications such as “Find My Phone” on your mobile phones can off a first step.
  - Strictly manage keys to access the premises and alarm codes.
- In case of an incident:
  - Keep an offline copy (e.g. offline hard disk or laptop, paper hardcopy, …) of any document you are likely to need during a cyber security incident or crisis by answering the following questions:
    - Who do I will need to contact in case of a cyber-incident ?
    - Which info do I need to contact them ?
    - Which info will they ask ?
  - See also our recommendations in the CCB Cyber Security Incident Management guide which provides a pragmatic approach to handling cyber security incidents and can be used as inspiration for your own incident response plan or playbook.

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. This information related to the security of networks and information systems is addressed to IT services which use the English terms of computer language. A translation into Dutch, French or German of this technical information is also made available the CCB.

The CCB accepts **no responsibility for the content** of this document.
The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations.
- are not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director-General
Rue de la Loi, 18
1000 Brussels

Legal depot

D/2023/14828/001