CENTRE FOR
CYBERSECURITY
BELGIUM

CyberFundamentals

BASIC

Version: 01.03.2023

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Table of Contents

Introduction

The **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.

The requirements and guidance are complemented with the relevant insights included in NIST/CSF framework, ISO 27001/ISO 27002, IEC 62443 and the CIS Critical security Controls (ETSI TR 103 305-1).

The coding of the requirements corresponds with the codes used in the NIST CSF Framework. Since not all NIST CSF requirements are applicable, some codes that do exist in the NIST CSF framework may be missing.

The framework and the proportional approach of the assurance levels are validated by practitioners in the field and by using anonymized real-world cyber-attack information provided by the federal Cyber Emergency Response Team (CERT - the operational service of the Centre for Cybersecurity Belgium).

The **CyberFundamentals Framework** is built around five core functions: identify, protect, detect, respond and recover. These functions allow, regardless of the organization and industry, to promote communication around cybersecurity among both technical practitioners and stakeholders so that cyber-related risks can be incorporated into the overall risk management strategy of the organization.

- **Identify**
  Know important cyber threats to your most valuable assets. Essentially, you can't protect what you don't know exists. This function helps develop an organizational understanding of how to manage cyber security risks related to systems, people, assets, data, and capabilities.
- **Protect**
  The protect function focuses on developing and implementing the safeguards necessary to mitigate or contain a cyber risk.
- **Detect**
  The purpose of the Detect function is to ensure the timely detection of cyber security events.
- **Respond**
  The Respond function is all about the controls that help respond to cyber security incidents. The Respond function supports the ability to contain the impact of a potential cyber security incident.
- **Recover**
  The Recover function focuses on those safeguards that help maintain resilience and restore services that have been affected by a cyber security incident.

RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT

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. It is intended for micro-organisations or organisations with limited technical knowledge.

The **assurance level *Basic*** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.
Several controls require particular attention; These measures are labelled as **- key measure -**.

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.

Asset Management [ID.AM]

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

ID.AM-1: Physical devices and systems used within the organization are inventoried.

An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.

Guidance

- This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.
- This inventory must include all assets, whether or not they are connected to the organization's network.
- The use of an IT asset management tool could be considered.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1
IEC 62443-2-1:2010, Clause 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.9, 5.11, 7.9, 8.1

ID.AM-2: Software platforms and applications used within the organization are inventoried.

An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.

Guidance

- This inventory includes software programs, software platforms and databases, even if outsourced (SaaS).
- Outsourcing arrangements should be part of the contractual agreements with the provider.
- Information in the inventory should include for example: name, description, version, number of users, data processed, etc.
- A distinction should be made between unsupported software and unauthorized software.
- The use of an IT asset management tool could be considered.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.9

ID.AM-3: Organizational communication and data flows are mapped.

Information that the organization stores and uses shall be identified.

Guidance

- Start by listing all the types of information your business stores or uses. Define “information type” in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.
- Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
IEC 62443-2-1:2010, Clause 4.2.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14

ID.AM-4: External information systems are catalogued.

No requirements are identified for the assurance level ‘Basic’, but guidelines are provided to increase information security.

Guidance

Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.12, 7.9

ID.AM-5: Resources are prioritized based on their classification, criticality, and business value.

The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.

Guidance

- Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):
  - What would happen to my business if these resources were made public, damaged, lost…?
  - What would happen to my business when the integrity of resources is no longer guaranteed?
  - What would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.
- Resources should include enterprise assets.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-2-1:2010, Clause 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.12, 7.9

The policies, policies, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1: Organizational cybersecurity policy is established and communicated.

Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.

Guidance

- Policies and procedures used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees.
- Policies and procedures for information- and cybersecurity should clearly describe your expectations for protecting the organization's information and systems, and how management expects the company's resources to be used and protected by all employees.
- Policies and procedures should be reviewed and updated at least annually and every time there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14
IEC 62443-2-1:2010, Clause 4.3.2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4, 5, 7.5, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.1

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.

Guidance

There are no additional guidelines.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 4.2, 7.4, 7.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.31, 5.32, 5.33, 5.34

ID.GV-4: Governance and risk management processes address cybersecurity risks.

As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.

Guidance

This strategy should include determining and allocating the required resources to protect the organization’s business-critical assets.

References

IEC 62443-2-1:2010, Clause 4.2.3, 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1: Asset vulnerabilities are identified and documented.

Threats and vulnerabilities shall be identified.

Guidance

- A vulnerability refers to a weakness in the organization's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organization's assets. A vulnerability exposes an organization to threats.
- A threat is a malicious or negative event that takes advantage of a vulnerability.
- The risk is the potential for loss and damage when the threat does occur.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7
IEC 62443-2-1:2010, Clause 4.2.3, 4.2.3.9, 4.2.3.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6, 7, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.36, 8.8

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

Guidance

- Keep in mind that threats exploit vulnerabilities.
- Identify the consequences that losses of confidentiality, integrity and availability may have on the assets and related business processes.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 5.1, 6.1, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.8

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

Identities and credentials for authorized devices and users shall be managed.

- key measure -

Guidance

Identities and credentials for authorized devices and users could be managed through a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organization's to:
(Not limitative list and measures to be considered as appropriate)

- Change all default passwords.
- Ensure that no one works with administrator privileges for daily tasks.
- Keep a limited and updated list of system administrator accounts.
- Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise.
- Use only individual accounts and never share passwords.
- Immediately disable unused accounts
- Rights and privileges are managed by user groups.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 5, 12, 13
IEC 62443-2-1:2010, Clause 4.3.3.5.1, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.16, 5.17, 5.18, 8.2, 8.5

PR.AC-2: Physical access to assets is managed and protected.

Physical access to the facility, servers and network components shall be managed.

Guidance

- Consider to strictly manage keys to access the premises and alarm codes. The following rules should be considered:
  - Always retrieve an employee's keys or badges when they leave the company permanently.
  - Change company alarm codes frequently.
  - Never give keys or alarm codes to external service providers (cleaning agents, etc.), unless it is possible to trace these accesses and restrict them technically to given time slots.
- Consider to not leaving internal network access outlets accessible in public areas. These public places can be waiting rooms, corridors...

References

IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.9, 7.10, 7.12, 7.14, 8.1

PR.AC-3: Remote access is managed.

The organisation's wireless access points shall be secured.

Guidance

Consider the following when wireless networking is used:

- Change the administrative password upon installation of a wireless access points.
- Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).
- 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.
- Ensure that wireless internet access to customers is separated from your business network.
- Connecting to unknown or unsecured / guest wireless access points, should be avoided, and if unavoidable done through an encrypted virtual private network (VPN) capability.
- Manage all endpoint devices (fixed and mobile) according to the organization's security policies.

The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).

- key measure -

Guidance

Enforce MFA (e.g. 2FA) on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1) Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 6.7, 7.9, 8.1, 8.5, 8.20

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

Access permissions for users to the organization's systems shall be defined and managed.

- key measure -

Guidance

The following should be considered:

- Draw up and review regularly access lists per system (files, servers, software, databases, etc.), possibly through analysis of the Active Directory in Windows-based systems, with the objective of determining who needs what kind of access (privileged or not), to what, to perform their duties in the organization.
- Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account.
- Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes separation of personal and admin accounts.
- For guest accounts, consider using the minimal privileges (e.g. internet access only) as required for your business needs.
- Permission management should be documented in a procedure and updated when appropriate.
- Use 'Single Sign On' (SSO) when appropriate.

It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.

- key measure -

Guidance

Means to get access may include: a key, password, code, or administrative privilege.

Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).

- key measure -

Guidance

The principle of Least Privilege should be understood as the principle that a security architecture should be designed so that each employee is granted the minimum system resources and authorizations that the employee needs to perform its function. Consider to:

- Not allow any employee to have access to all the business's information.
- Limit the number of Internet accesses and interconnections with partner networks to the strict necessary to be able to centralize and homogenize the monitoring of exchanges more easily.
- Ensure that when an employee leaves the business, all access to the business's information or systems is blocked instantly.

Nobody shall have administrator privileges for daily tasks.

- key measure -

Guidance

Consider the following:

- Separate administrator accounts from user accounts.
- Do not privilege user accounts to effectuate administration tasks.
- Create unique local administrator passwords and disable unused accounts.
- Consider prohibiting Internet browsing from administrative accounts.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.3, 5.15, 8.2, 8.3, 8.4, 8.18

PR.AC-5: Network integrity (network segregation, network segmentation…) is protected.

Firewalls shall be installed and activated on all the organization's networks.

- key measure -

Guidance

Consider the following:

- Install and operate a firewall 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).
- Ensure there is antivirus software installed on purchased firewall solutions and ensure that the administrator’s log-in and administrative password is changed upon installation and regularly thereafter.
- Install, use, and update a software firewall on each computer system (including smart phones and other networked devices).
- Have firewalls on each of your computers and networks even if you use a cloud service provider or a virtual private network (VPN). Ensure that for telework home network and systems have hardware and software firewalls installed, operational, and regularly updated.
- Consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyze network traffic at a more detailed level and can provide a greater level of protection.

Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.

- key measure -

Guidance

- Consider creating different security zones in the network (e.g. Basic network segmentation through VLAN’s or other network access control mechanisms) and control/monitor the traffic between these zones.
- When the network is "flat", the compromise of a vital network component can lead to the compromise of the entire network.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 7, 12, 16
IEC 62443-2-1:2010, Clause 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 8.20, 8.22, 8.26

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1: All users are informed and trained.

Employees shall be trained as appropriate.

Guidance

- Employees include all users and managers of the ICT/OT systems, and they should be trained immediately when hired and regularly thereafter about the company's information security policies and what they will be expected to do to protect company's business information and technology.
- Training should be continually updated and reinforced by awareness campaigns.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.2, 7.4, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 6.3, 8.7

Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: Data-at-rest is protected.

This control is covered by other elements of the framework; no additional requirements are identified.

Guidance

- Consider using encryption techniques for data storage, data transmission or data transport (e.g., laptop, USB).
- Consider encrypting end-user devices and removable media containing sensitive data (e.g. hard disks, laptops, mobile device, USB storage devices, …). This could be done by e.g. Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,…
- Consider encrypting sensitive data stored in the cloud.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013, SR 3.4, SR 4.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10

PR.DS-2: Data-in-transit is protected.

This control is covered by other elements of the framework; no additional requirements are identified.

Guidance

When the organization often sends sensitive documents or e-mails, it is recommended to encrypt those documents and/or e-mails with appropriate, supported, and authorized software tools.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013, SR 3.1, SR 3.8, SR 4.1, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 5.14, 8.20, 8.26

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.

Assets and media shall be disposed of safely.

Guidance

- When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper…), ensure that all sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as "sanitization" and thus related to the requirement and guidance in PR.IP-6.
- Consider installing a remote-wiping application on company laptops, tablets, cell phones, and other mobile devices.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.10, 7.10, 7.14

PR.DS-7: The development and testing environment(s) are separate from the production environment.

No requirements are identified for the assurance level 'Basic', but guidelines are provided to increase information security.

Guidance

- Any change one wants to make to the ICT/OT environment should first be tested in an environment that is different and separate from the production environment (operational environment) before that change is effectively implemented . That way, the effect of those changes can be analysed and adjustments can be made without disrupting operational activities.
- Consider adding and testing cybersecurity features as early as during development (secure development lifecycle principles).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 16,
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.31

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-4: Backups of information are conducted, maintained, and tested.

Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

- key measure -

Guidance

- Organization's business critical system's data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, etc.
- Consider a regular backup and put it offline periodically.
- Recovery time and recovery point objectives should be considered.
- Consider not storing the organization's data backup on the same network as the system on which the original data resides and provide an offline copy. Among other things, this prevents file encryption by hackers (risk of ransomware).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
IEC 62443-2-1:2010, Clause 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.29, 5.33, 8.13

PR.IP-11: Cybersecurity is included in human resources practices (deprovisioning, personnel screening…).

Personnel having access to the organization’s most critical information or technology shall be verified.

Guidance

- The access to critical information or technology should be considered when recruiting, during employment and at termination.
- Background verification checks should take into consideration applicable laws, regulations, and ethics in proportion to the business requirements, the classification of the information to be accessed and the perceived risks.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Patches and security updates for Operating Systems and critical system components shall be installed.

- key measure -

Guidance

The following should be considered:

- Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your business and patch/update them regularly.
- You should only install a current and vendor-supported version of software you choose to use. It may be useful to assign a day each month to check for patches.
- There are products which 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.
- Install patches and security updates in a timely manner.

References

IEC 62443-2-1:2010, Clause 4.3.3.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.2, 7.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 7.2, 7.9, 7.10, 7.13

Protective Technology [PR.PT]

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

Logs shall be maintained, documented, and reviewed.

- key measure -

Guidance

- Ensure the activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) is enabled.
- Logs should be backed up and saved for a predefined period.
- The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 8
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.4
IEC 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 9.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.15, 8.17, 8.34

PR.PT-4: Communications and control networks are protected.

Web and e-mail filters shall be installed and used.

Guidance

- E-mail filters should detect malicious e-mails, and filtering should be configured based on the type of message attachments so that files of the specified types are automatically processed (e.g. deleted).
- Web-filters should notify the user if a website may contain malware and potentially preventing users from accessing that website.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 10, 12, 13
IEC 62443-3-3:2013, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 4.1, 8.1, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.14, 8.20, 8.26

Anomalous activity is detected, and the potential impact of events is understood.

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.

- key measure -

Guidance

- Logs should be backed up and saved for a predefined period.
- The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 8, 10, 13, 15
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 9.1, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.28, 8.15

Security Continuous Monitoring [DE.CM]

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM-1: The network is monitored to detect potential cybersecurity events.

Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.

Guidance

- Endpoints include desktops, laptops, servers...
- Consider, where feasible, including smart phones and other networked devices when installing and operating firewalls.
- Consider limiting the number of interconnection gateways to the Internet.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.3.3.8
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.22, 8.15, 8.30

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.

Endpoint and network protection tools to monitor end-user behaviour for dangerous activity shall be implemented.

Guidance

Consider deploying an Intrusion Detection/Prevention system (IDS/IPS).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 8, 13, 15
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.15

DE.CM-4: Malicious code is detected.

Anti-virus, -spyware, and other -malware programs shall be installed and updated.

- key measure -

Guidance

- Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in company's business (including computers, smart phones, tablets, and servers).
- Anti-virus and anti-spyware software should automatically check for updates in "real-time" or at least daily followed by system scanning as appropriate.
- It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.5, 8, 9.1, 9.2, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 8.7

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

RS.RP-1: Response plan is executed during or after an incident.

An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.

Guidance

- The incident response process should include a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
- The roles, responsibilities, and authorities in the incident response plan should be specific on involved people, contact info, different roles and responsibilities, and who makes the decision to initiate recovery procedures as well as who will be the contact with appropriate external stakeholders.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

RS.CO-3: Information is shared consistent with response plans.

Information/cybersecurity incident information shall be communicated and shared with the organization’s employees in a format that they can understand.

Guidance

There are no additional guidelines.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 7.3, 7.4, 8.1, 8.3, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 6.8

Improvements [RS.IM]

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

RS.IM-1: Response plans incorporate lessons learned.

The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.

Guidance

Consider bringing involved people together after each incident and reflect together on ways to improve what happened, how it happened, how we reacted, how it could have gone better, what should be done to prevent it from happening again, etc.

References

IEC 62443-2-1:2010, Clause 4.3.4.5.10, 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 6.1, 8.3, 10, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26, 5.27

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.

A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.

Guidance

A process should be developed for what immediate actions will be taken in case of a fire, medical emergency, burglary, natural disaster, or an information/cyber security incident.

This process should consider:

- Roles and Responsibilities, including of who makes the decision to initiate recovery procedures and who will be the contact with appropriate external stakeholders.
- What to do with company's information and information systems in case of an incident. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
- Who to call in case of an incident.

References

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Clause 8, 10.2, Annex A (see ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Control 5.26

Annex A: List of key measures for the assurance level 'Basic'

PROTECT

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

(1) Identities and credentials for authorized devices and users shall be managed.

PR.AC-3: Remote access is managed.

(2) The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

(3) Access permissions for users to the organization's systems shall be defined and managed.
(4) It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.
(5) Employee access to data and information shall be limited to the systems and specific information they need to do their jobs.
(6) Nobody shall have administrator privileges for daily tasks.

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

(7) Firewalls shall be installed and activated on all the organization's networks.
(8) Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.

PR.IP-4: Backups of information are conducted, maintained, and tested.

(9) Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

(10) Patches and security updates for Operating Systems and critical system components shall be installed.

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

(11) Logs shall be maintained, documented, and reviewed.

DETECT

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

(12) The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.

DE.CM-4: Malicious code is detected.

(13) Anti-virus, -spyware, and other -malware programs shall be installed and updated.

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.

All texts, layouts, designs and other elements of any nature in this document are subject to **copyright law**. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

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:

- is exclusive of a general nature and do not intend to take into consideration all particular situations.
- is 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