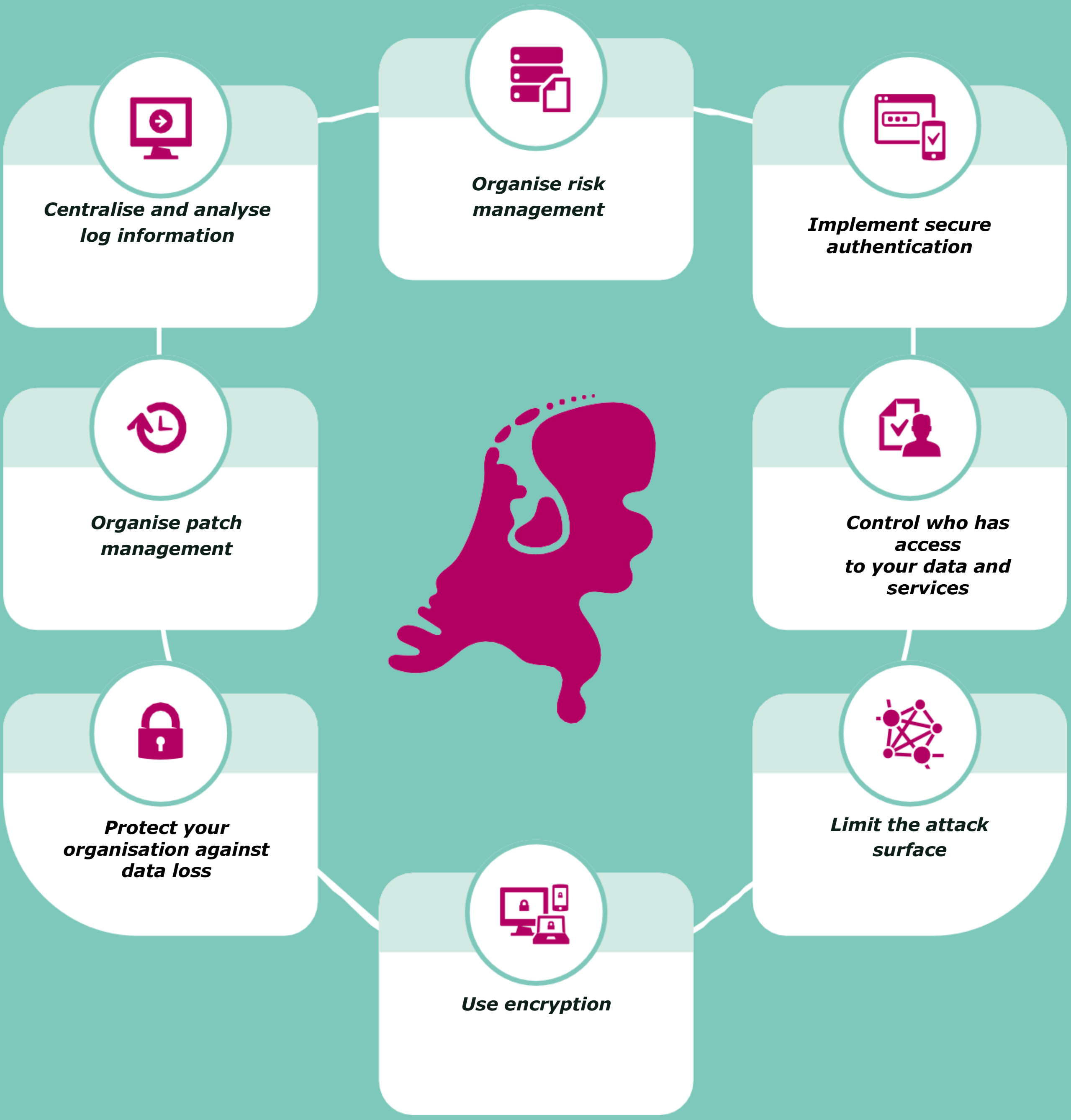
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Basic Cyber Security Measures

Step by step to a digitally secure organisation

Factsheet | version 1.1 | 14 June 2023



Centralise and analyse log information

Organise risk management

Implement secure authentication

Organise patch management

Control who has access to your data and services

Protect your organisation against data loss

Limit the attack surface

Use encryption

Every year, many cyber security incidents take place at organisations worldwide. Attackers use methods such as ransomware and phishing. The impact of these incidents on organisations can be significant. In many instances, organisations are vulnerable because their basic arrangements are inadequate.

This guide outlines various measures that will ensure your organisation takes steps towards achieving an appropriate level of resilience against common incidents.

Background

The CSBN concludes that resilience is inadequate and basic measures are often lacking in the Netherlands. These basic measures should be taken by every organisation as they help to improve the resilience of organisations against cyber attacks. They play an important role in preventing damage and are key steps in ensuring the continuity of your business processes. These are the things that should be considered as basic cyber security hygiene: the minimum basic measures you should take for effective resilience against the most basic and common attacks.

What does the NCSC advise?

The NCSC advises you to apply these measures within your organisation. Since every organisation is unique, the NCSC advises that you pay sufficient attention to risk management. This will provide you with good insight into your interests in need of protection and the threats potentially affecting them. That in turn provides a starting point for achieving an appropriate level of security for your organisation.

For whom?

This guide is aimed at those in your organisation who are responsible for cyber security, including the board of directors, line management and subject matter experts such as the CISO.

The Digital Trust Center (DTC) has drawn up the basic principles of secure digital business for Dutch entrepreneurs and self-employed professionals, together with relevant practical advice, which may better suit your needs. More information is available at www.digitaltrustcenter.nl.

Partners

This guide has been drawn up in association with the Digital Trust Center.

Measures

By implementing these measures, your organisation will lay the foundation for effective cyber resilience.

Organise risk management[1]

Incidents can have a major impact on organisational goals. To safeguard your processes from disruption as far as possible, it is important that you maintain an appropriate level of resilience. An appropriate level means that the measures you implement protect your organisation without having any negative effects on your business activities or leading to unnecessary costs.

To find out what is appropriate for your organisation, the NCSC recommends carrying out your own risk analysis.

A risk analysis enables you to identify which threats are specific to the organisation and what the key assets or interests of your organisation in need of protection are. In addition, it reveals what risks have materialised or are likely to materialise and how they should be addressed. This helps you to protect the right things in the right way: not so much that it becomes expensive or unworkable but in such a way that it reduces any potential risk to your business continuity. This gives you good insight into which measures, besides the basic ones, add value to your organisation.

To ensure that risk analysis is not performed in isolation, it is a good idea to organise a risk management process. This guarantees that risk analyses are carried out at regular intervals, that it is clear which measures are to be taken, in what timeframe and by whom, as well as where ownership of the risk lies.

Besides providing a framework for identifying and responding to risks, the risk management process also makes clear how risk management in general is handled and safeguarded within the organisation.

Implement secure authentication

Authentication[2] is the technology a system uses to verify a user's identity. This grants a user access to data or systems.

A factor is a means by which a user logs on. Factors are divided into three categories: something you know (e.g. a password), something you have (e.g. a token) or something you are (e.g. a fingerprint). Logging in with factors from at least two of these categories is called multi-factor authentication. The use of exactly two factors is also called two-factor authentication. Examples of multi-factor authentication are a password combined with a token or a fingerprint combined with a one-time code.

Implement multi-factor authentication for accounts that are accessible from the internet, accounts that have administrative rights and accounts on critical systems. The use of multi-factor authentication prevents attackers from gaining access to an account by guessing or figuring out the password. Attackers can for example obtain these passwords by carrying out a phishing attack.

Whenever possible, opt for password-free solutions. Passwords are vulnerable and

[1] Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt. | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl)

[2] Authenticatie | Nationaal Cyber Security Centrum (ncsc.nl)

outdated as a security mechanism. It is possible nowadays to log into applications and systems using, for example, a piece of hardware (token or telephone) and a biometric identifier. Facial and fingerprint recognition on smartphones are an example of this. Check whether your applications support password-free login and make this a requirement when procuring software and systems in the future. Login mechanisms such as this are both more secure and user-friendly than antiquated passwords.

In addition to determining a secure login method for users, it is also important to consider which devices should be permitted to log into your systems from which location. This will allow you to define a specific area or set, enabling you to limit or block access to systems from unknown locations and by unknown devices. If your organisation operates mainly in the Netherlands, with employees who live in the Netherlands and only use specific devices, you should consider whether this can also be mandated as a system-level standard. Finally, if limiting or blocking access proves unfeasible, it is also possible to detect login attempts from unknown sources and alert users to this, by email for example, so that users can take action to address this themselves.

Control who has access to your data and services

Give employees access only to the information, systems and locations they need to perform their job. This therefore applies to both logical and physical access. This limits the impact of any mistakes made by users, which can have unwanted consequences. It also limits the actions malicious parties can take if they gain access. Access of service accounts, machine accounts and functional accounts should also be limited to what is necessary.

Role-based access control can make rights management easier. Allocate minimal rights according to the *principle of least privilege*. Assign ownership for all data. This is generally a line manager.

Always adhere to the principle that the business is responsible for determining what data is stored and how the respective rights are determined. An ICT organisation can at most implement this on behalf of the data owner, but cannot decide or determine this for the data owner.

In addition, make sure that access to data and services is personal, with each employee having their own user account. Avoid generic accounts, which are shared between multiple employees, for example, or multiple employees of a supplier. This also applies to service accounts; these are accounts used for interconnection purposes by systems. Avoid these accounts wherever possible. Instead, use a modern API and ensure at a minimum that you implement a password policy if your systems require a service account. Change default passwords of equipment and systems upon installation or commissioning.

Make sure you have processes in place for the entry, exit and internal movement of employees. Give new employees access only to the resources they need. Immediately remove access to data and systems from accounts of exiting employees. Delete unused accounts. Deactivate service accounts, and activate them only when maintenance is performed.

Limit the attack surface

Most software, computer hardware and network equipment contain more functionality than an organisation needs. This can lead to unnecessary vulnerabilities, which attackers are grateful to exploit. Once they have gained access, they will try to move through the network. Certain measures, such as hardening and segmentation, can be taken to limit the attack surface.

The goal of hardening is to reduce the attack surface. Simply put, hardening means switching off, closing or removing anything you do not need. Hardening involves a series of steps and practices, such as removing, disabling, making inaccessible or restricting functionalities and communication openings (communication channels or network ports). Examples include technical services, communication protocols, software, user accounts and system services. Hardening is also related to logical access security, as referred to above.

If an attacker does gain access, segmenting your network can limit the effects of an attack. Segmentation means dividing a network into several zones. Network segmentation prevents a virus or attacker from spreading throughout the network. Network segmentation is a measure that can limit the impact of various types of cyber attacks. Apply the principle that network traffic is generally not allowed and then add specific firewall rules for traffic that is.

Use encryption

Encrypting all your business information makes data unusable if it falls into the hands of attackers. Encryption prevents the data from being read unless you have the key. The key can be a separate password, but can also be kept by your workplace or telephone, for example. This ensures that encryption is easy to use and can be applied to all data.

Encrypt hard drives, laptops, mobile devices and USB sticks containing business information. Also, consider how your data is stored in cloud solutions or on servers. Ensure that this data also is encrypted; that way you are not dependent on the reliability of specific suppliers and you fulfil all aspects of your responsibility as a data owner.

Protect your organisation against data loss

You should have a backup policy in place to protect your organisation against data loss in the event that something goes wrong. The backup policy incorporates your requirements for storing and protecting your data. These requirements are defined partly on the basis of your own risk assessment.
Regular backing up and testing of critical backups in line with the backup policy is essential. This ensures that your policy can be put into practice effectively if your data and systems have been compromised and need to be restored. Devise an approach for using this policy when it matters: as part of a recovery process so that there is only a minimum interruption of your business operations. It is therefore important not only to secure your data, but also to have a tried and tested method of quickly recovering that data if the situation requires. This method should be tested to prove its technical functioning, and also practised so that everyone concerned knows exactly what to do if your business operations are interrupted due to ICT issues.

Make backups

Consider which data needs to be backed up and how long you need to store the backups. Test the restoration of your backups to ensure that there is only a limited disruption to your business operations in the event of data loss. Practise the recovery process with employees who need to be able to perform such work in a live situation.

The **3-2-1** rule can help in designing your backup process. This rule means that you have **3** versions of your data (your production data and two backups) on **2** different media (e.g. physical hard drives, tape and in the cloud) with **1** copy at a different location for disaster recovery (e.g. a different data centre or a vault away from your office).
By storing backups at a different location, you can restore your systems if, for example, ransomware has encrypted your business network.

Restrict access to the backups. Consider not only restricting access rights, but also encrypting your backups. An external backup should be ‘immutable’, meaning that it cannot be altered in any way or deleted from its original location once it has been saved. This prevents your backups from also being irreparably compromised in the event of a ransomware attack.

Organise patch management

Software almost always contains programming errors. Such errors can lead to vulnerabilities. Suppliers release updates to fix vulnerabilities in their software.

By setting up a patch management process, you ensure that a process is in place that identifies, tests and installs updates for your software. In doing so, map out all software and systems within your organisation, including web browsers and plug-ins.

For most systems, it is important to install these updates as soon as possible. Some software offers the possibility to update automatically: make use of this. For critical systems, it is advisable to perform the update in a test environment and check what the impact is on your production processes before deploying it in the production environment.

If it is not possible to automate such processes, plans should be prepared for deploying the update in the production environment at the earliest opportunity. In addition to all content-related processes, agreements must be made with the business in this regard, so that in critical cases it is possible to briefly interrupt your business process for an urgent update.

In some cases, an update for a vulnerability is not yet available or it is not advisable to update immediately. In such cases, take mitigating measures. In addition, replace old software and devices that are no longer supported by the vendor.

Centralise and analyse log information

Log files play a key role in detecting attacks and dealing with incidents. By ensuring that applications and systems generate sufficient log information, you provide yourself with sufficient information.

Determine which log files are required. These files can pertain to system logging, network logging, application logging and cloud logging.

Make sure that your systems forward the log information to a central logging server, which collects all the logs and analyses them (in combination). Make sure that no log files can be altered at this central location and house the system in a securely protected environment.

Use automated log analyses, which use analysis rules of a supplier or community that continuously updates them to take account of the latest threats. This ensures that log files are scanned for irregularities that might indicate a security incident.

Make a decision regarding the retention period of log files which is consistent with your security objectives as well as privacy laws and regulations. Ensure that your processes for handling log information, for example with regard to use and access, are in line with laws and regulations and, if necessary, are laid down in data processing and other agreements with your customers.

Conclusion

The cyber security of your organisation partly depends on suppliers. Make clear agreements with suppliers and subcontractors, in particular regarding the mutual processes and how you can best address the issues highlighted in this guide. Rely on certification and contracts, but also regularly validate desired outcomes: testing and exercise results provide the greatest certainties and can immediately prompt steps to improve your own organisation as well as that of suppliers.

The NCSC recommends using existing standards and guidelines, based on risk management, when procuring products and services. The measures mentioned in this guide can be taken into account during the procurement process.

***Incidents can still occur even when these measures are taken, so it is important to be prepared for them. Ensure that the approaches to tackling cyber security incidents are included in your existing recovery plan (e.g. a Disaster Recovery Plan).* Update and practise this plan regularly**.

Publication
National Cyber Security Centre (NCSC-NL)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

June 2023