National Cyber Security Centre
Ministry of Justice and Security

Guide to
Cyber Security Measures

Step by step to a digitally secure organisation

A cyber secure Netherlands

- Install updates
- Ensure that each application and system generates sufficient log information
- Implement multi-factor authentication
- Back up and test your systems regularly
- Control who has access to your data and services
- Encrypt storage media containing sensitive business information
- Segment networks
- Check which devices and services can be accessed from the internet and protect them

Additional information is available at ncsc.nl/gettingstarted

Introduction

Step by step to a digitally secure organisation

Every year, many cyber security incidents take place at organisations worldwide. These attacks use methods such as ransomware and phishing. The Cyber Security Assessment Netherlands (CSAN) describes and interprets a number of incidents that have a connection to the Netherlands.

The 2021 CSAN concludes that incidents show that resilience is inadequate and basic measures are often lacking. This guide contains measures that every organisation should take to help counter cyber attacks such as those described in the CSAN. Check whether your cyber security policy contains these measures. And use this guide as a starting point for discussions with your suppliers about their digital security.

Chapter 1 describes the context in which you apply these measures: how is the responsibility for cyber security assigned within an organisation? Chapter 2 explains how these measures support, but do not replace, regular risk management. Chapter 3 discusses the eight measures that every organisation should take for a digitally secure organisation. If you have applied the measures and want to go further, Chapter 4 provides additional pointers.

For whom?

This guide is aimed at those in your organisation who are responsible for cyber security.

1.

Organisational embedding of the measures

The measures in this guide can help you prevent incidents. To effectively deploy these measures in your organisation, it is necessary that you have properly arranged the organisational side of cybersecurity. It is important to create awareness of cyber security risks at all levels of the organisation, including users. In addition, responsibilities must be assigned correctly.

Board of directors

Because incidents can occur anywhere in the organisation, cyber security is a challenge for the entire organisation. To ensure that the organisation can meet this challenge, proper guidance from the board of directors is needed. The board of director's most important cyber security tasks are to assign ownership and responsibility for information and processes.

Information systems (IT) serve as support tools in this process. After all, IT systems are a means of processing information and controlling processes that, for example, use operational systems (OT). After assigning these responsibilities, the board of director's also sees to it that they are properly carried out. In this day and age, IT and OT systems, like money and staff, are assets that an organisation depends on. For this reason, line management is the appropriate place to assign this responsibility. The board of director's should ensure that the right officers are available to support line managers in this responsibility. Examples of such officers are a Chief Information Security Officer (CISO), a Data Protection Officer (DPO), Chief Information Officer (CIO) and/or an information manager, an IT manager or an OT manager. However, the highest-ranking person in the organisation (director, chairman of the board, secretary-general) must remain ultimately responsible.

Line management

Line managers are responsible for identifying the risks associated with the IT and OT systems for which they have been assigned ownership, for making a final decision on whether or not to accept residual risks, and for ensuring that the mitigating measures are implemented properly. Line managers will not be cyber security experts in many cases. As such, a line manager will be supported by the advice and services of a Chief Information Security Officer (CISO), a Data Protection Officer (DPO), a Chief Information Officer (CIO) and/or information manager, an IT manager or an OT manager.

CISO

The CISO, as an expert in cyber security, has an advisory, coordinating and monitoring role. The CISO has no independent responsibility for the organisation's cyber security. The CISO is not the owner of IT or OT systems. This role is always assigned to the organisation's line management.

2.

Risk analysis

The measures in the following section support your regular risk management processes, but it is still important to perform your own risk analysis and select additional measures yourself.

An important part of risk management is providing insight into the risks to an organisation. Based on the identified risks, measures can be determined. The CSAN interprets digital threats and incidents that have occurred and identifies risks to national security. The NCSC-NL has made a selection of eight measures to address these threats, which can be found in the section on 'Measures'.

The NCSC-NL advises you to apply all these measures within your organisation. In addition, the NCSC-NL recommends carrying out your own risk analysis. This will enable you to identify further measures that will help to control the risks specific to your organisation. Even if you have not yet carried out your own risk analysis, it is wise to apply the measures in this guide. They are general measures that should also follow from your own risk analysis

Risk analysis

The NCSC-NL emphasises that these measures do not remove the need to carry out risk analyses yourself. Consider these measures as basic measures that are always wise to have in place. However, every organisation is unique. Your organisation probably also has specific digital risks. The NCSC-NL recommends elucidating these and controlling them with appropriate measures. This is an ongoing process that requires a tailored approach, as both threats and the interests of your organisation in need of protection can change.

Read more

For more about the role of the CISO and the organisation of risk management, see the NCSC-NL factsheet *Risk Management: the value of information as point of departure*:

https://english.ncsc.nl/publications/factsheets/2020/september/15/factsheet-risk-management-the-value-of-information-as-point-of-departure

3.

Measures

This section discusses eight basic measures that the NCSC-NL believes are necessary to protect you from current digital threats.

Install updates

Software contains programming errors. Such errors can lead to vulnerabilities. Suppliers release updates to fix vulnerabilities in their software. Set up a process 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 before deploying it in the production environment.

In some cases, an update for a vulnerability is not yet available. In such cases, take mitigating measures. Replace software and devices that are no longer supported by the vendor.

Read more

In response to recently discovered vulnerabilities, the NCSC-NL publishes security recommendations.

Ensure that each application and system generates sufficient 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. Set up alerts where necessary. This can include, for example, notifications of suspicious login attempts based on an analysis of log files. Ensure that your systems store log files in a usable file format, and that the recorded timestamps are accurate and set to the correct time zone.

Make a decision regarding the retention period of log files. If you keep log files for a long time, you can find out what happened long after incidents occur. On the other hand, log files may contain privacy-sensitive information and take up storage space.

Limit access to log files and store them in a separate network segment. An incident investigation will be nearly impossible if attackers have been able to modify or delete the log files.

Implement multi-factor authentication

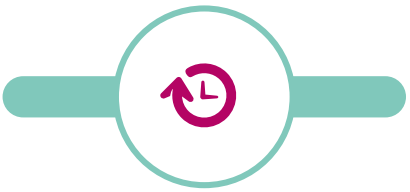
Implement multi-factor authentication for accounts that are accessible from the internet, accounts that have administrative rights and accounts on critical systems. The use of multi-factor authentication prevents attackers from gaining access to an account by guessing or figuring out the password. Attackers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

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 multifactor authentication are a password combined with a token or a fingerprint combined with a one-time code.

Read more

For more information, see the NCSC-NL factsheet *Use two-factor authentication* (in Dutch):

https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie

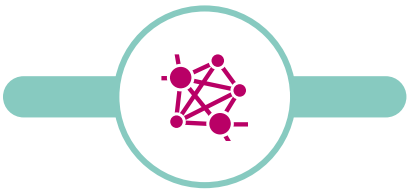


Back up and test your systems regularly

Backing up and testing is essential if your data and systems have been compromised and need to be restored. Consider which data needs to be backed up and how long you need to store them. Regularly 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.

The 3-2-1 rule can help in designing your backup process. This rule means that you have three versions of your data (your production data and two backups) on two different media (e.g. different physical hard drives) with one copy at a different location for disaster recovery (e.g. physical). 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.



Segment networks

Segmenting your network limits 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. Depending on how it is implemented, network segmentation is a measure that limits the impact of ransomware attacks or DDoS attacks.

When segmenting your networks, consider how these zones are divided and connected. For example, you can define zones using firewalls, access control lists (ACLs) and data diodes. You can also choose to create a network that is only physically accessible, a so-called *air-gapped* network. In any case, make sure that critical systems are placed in their own network zone.

Apply the principle that network traffic is generally not allowed and then add specific firewall rules for traffic that is. Blocking network traffic too rigorously can cause disruption to your business. You can prevent this by first monitoring network traffic to determine which information flows are required, and only then blocking network traffic.

Control who has access to your data and services

Give employees access only to the data and systems they need to perform their job. This applies to both accounts and physical access. This limits the actions attackers can take if they gain access. It also limits the impact of any mistakes made by users.

Also limit access of service accounts, machine accounts and functional accounts to what is necessary. Role-based access control can make rights management easier. The allocation of minimal rights is also called the *principle of least privilege*. This includes limiting the use of management privileges as well.

In addition, make sure that access to data and services is personal, with each employee having their own user 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.

Encrypt storage media containing sensitive business information

Encrypting storage media containing sensitive business information makes the data unusable if it falls into the hands of attackers. Encryption prevents the data from being read. Encrypt hard drives, laptops, mobile devices and USB sticks containing sensitive information. Use secure encryption software to encrypt this media.

Check which devices and services can be accessed from the internet and protect them

Connecting devices and services to the internet is a risk. As such, check which of your devices and services can be accessed from the internet and protect them. Allow access to the internet only when necessary. This reduces the risk of unauthorised access. Take measures to protect the devices and services accessible from the internet. Protective measures include using a firewall, disabling unused services and ports and making sure software is up-to-date. Place devices that can be accessed through the internet in a separate network segment. Apply multi-factor authentication to accounts that can be used via the internet.

4.

Points of focus

By implementing the eight measures described in the previous section, your organisation will lay the foundation for effective cyber resilience. In addition, the NCSC-NL advises you to prepare for incidents and to enter into discussions with your suppliers.

Be prepared for incidents

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

Talking to suppliers

The cyber security of your organisation partly depends on suppliers. Make clear agreements with suppliers and subcontractors, for example regarding incident management or reporting. The NCSC-NL 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.

Read more

For the procurement of cloud services, the NCSC-NL has published the factsheet *5 recommendations for securely purchasing cloud services*:

https://english.ncsc.nl/publications/factsheets/2020/december/31/factsheet-5-recommendations-for-securely-purchasing-cloud-services

Other publications

The following additional publications (in Dutch) can provide your organisation with tools to increase your cyber resilience:

- Cyber attacks by state actors - 7 moments to stop an attack (AIVD): https://www.aivd.nl/cyberdreiging
- The 5 Basic Principles of Secure Digital Business (Digital Trust Center): https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
- The Exercise Toolkit of the Cybersecurity Alliance provides guidance for organisations in preparing and evaluating exercises. By practising within an organisation or within a supply chain, organisations can prepare themselves for (possible) cyber incidents. For more information, go to Cybersecurityalliantie.nl.

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

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

June 2021