Finnish Transport and Communications Agency

Strengthening cyber security at Finnish organisations

Instructions for management and experts

National Cyber Security Centre Finland

Traficom Publications

8/2022

Contents

The digital world and preparedness against cyber threats are inexorably influenced by the current international situation. In light of this, it is important for the management and experts of organisations to examine and actively maintain best practices of their cybersecurity.

These instructions make frequent references to the digital services of organisations. They refer to all the information systems and telecommunications connections that an organisation uses internally in their own operations and through which the organisation provides services to its customers.

Cyber incidents are a common occurrence in a digital society. Not only can organisations' own systems be attacked, but they can also become indirect targets via their subcontractors, partners or customers, or suffer collateral damage as a result of the uncontrolled spread of malware, for example.

These instructions are intended for all Finnish organisations for the purpose of strengthening cyber security. The instructions are not limited to the preparedness needs resulting from the international situation in early 2022, as they are also aimed at helping organisations develop their cyber security in general.

Read more:

Cyber security and the responsibilities of boards

Cyber security guide for small companies (in Finnish)

Managing cyber security

1 Take changes in the cyber security threat assessment into account

Each organisation should examine the impacts of the changed cyber security threat assessment on their own operations. The party ultimately responsible for cyber security is the organisation's management.

The National Cyber Security Centre Finland recommends that organisations should:

- reserve sufficient resources for ensuring cyber security and implement necessary measures. In relation to this, organisations should also consider the reachability of their management for critical decision-making.
- determine which digital services need to be protected to secure the organisation's core functions and whether their protection measures are up to date and maintained. These measures should take into account needs related to the organisation's risk and continuity management and physical security arrangements.
- monitor the state of cyber security via bulletins issued by the authorities, especially the Finnish Transport and Communications Agency's National Cyber Security Centre Finland, and independently.

Further information:

Subscribe to our newsletters!

Discover our instructions and guides for organisations and companies

Cyber security and the responsibilities of boards

2 Define your business-critical environments

Management should define the processes critical to the organisation's operations and the digital services and information assets required for them. The organisation's management and the experts and partners responsible for its services should have a shared understanding of these elements.

Cyber security incidents can have simultaneous impacts on multiple services needed by the organisation. The restoration of these services should be based on a pre-defined, documented and practiced plan. The order of priority of the services should also be clearly defined.

The organisation's management should prepare for the possibility of operations being disrupted by ransomware or a cyber attack aimed at destroying information, for example. In such cases, the only means of ensuring the continuity of operations are up-to-date and restorable backups.

Cyber security controls

3 Protect your business-critical environments

Attackers typically try to seek out the digital services critical to an organisation's operations and gain access to them. These attempts often try to utilise entry-level information security vulnerabilities.

Organisations should protect themselves against these threats with thorough information security work. This information security work should cover not only the organisation's own digital services, but also the digital services administered by its partners.

The following sections detail relevant measures that we urge all organisations to consider.

The measures are not presented in a recommended order of implementation, as it is up to each organisation to review and prioritise them based on their own circumstances.

Further information:

Guide to protecting yourself against data breaches

3.1 Enable multi-factor authentication

Multi-factor authentication (MFA, 2FA) should be implemented for all the digital services of an organisation that are accessible via the public internet and require user login. These include both the organisation's own services and the services administered by external partners.

If implementing multi-factor authentication is not possible for whatever reason, the system in question should be secured by other means by preventing access to it via the public internet.

Further information:

Advice to help you protect your accounts

3.2 Install security updates without delay

Security updates should be installed without delay, especially for any digital services accessible via the internet.

The timespan between an information security vulnerability being discovered and its widespread exploitation is constantly shortening. As such, it is no longer sufficient to install updates once a month. Instead, organisations should have the capacity to react to update needs based on their risk assessment within a few days at a minimum.

Criminals often attempt to exploit the vulnerabilities of individual devices as well. Because of this, it is crucial to always update the operating systems, office applications and browsers of any devices used without delay. The recommended way of ensuring this is by enabling automatic updates. If device updates are centrally managed by the organisation, users should be forced to install at least critical updates within one week.

Organisations should monitor all the vulnerabilities relevant to their operating environment and assess their risks in regard to the continuity of their operations. In regard to monitoring updates, it can also be helpful to know that many manufacturers release updates and patches on so-called Patch Tuesday, which is usually the second Tuesday of the month.

Further information:

National Cyber Security Centre Finland – Vulnerabilities

Vulnerability Notes Database

Mitre Common Vulnerabilities And Exposures (CVE)

NIST National Vulnerability Database (NVD)

ICS-CERT Alerts (automation environments)

3.3 Secure your network traffic

Organisations should define what kinds of data traffic within their networks are necessary and normal for the organisation’s operations. All unnecessary network traffic should be blocked by firewalls. In addition to inbound network traffic, the organisation’s outbound network traffic should also be restricted so that only necessary traffic is allowed.

Special attention should be paid to prevent network traffic between the organisation’s network and the public internet using data transfer protocols that are known to be vulnerable and typically exploited by criminals.

Organisations should not allow the use of any data transmission protocols that are unencrypted or known to be vulnerable on the public internet. Encrypted protocols should also be used on the organisation’s internal networks whenever possible.

In regard to network traffic security, organisations should also take into account their servers and devices, meaning that the software firewalls of servers and devices should be configured to only allow network traffic that is necessary for their operation. Doing so will also make it more difficult for potential network intruders to move between environments. Another method that can contribute to this is network segmentation.

Further information:

NCSC-UK - Preventing Lateral Movement

NCSC-IE - Ingress & Egress Filtering

Shadowserver’s list of protocols often exploited by criminals

NSA – Network Infrastructure Security Guidance

Lateral movement – what you need to know (part one)

Lateral movement – what you need to know (part two)

3.4 Protect yourself against malware

The possibility of the organisation's environment being infected with malware presents a significant risk to the organisation's operational continuity. As such, it is essential to ensure comprehensive and up-to-date malware protection. The protection solution should cover all of the organisation's digital services, servers and different devices.

Information security controls can only protect organisations as long as they remain operational. As such, the operation of information security controls should be regularly reviewed. It is particularly important to make sure that information security products are installed on all systems, correctly configured and kept updated with the latest updates and security patches.

All of the organisation's inbound and outbound files should be checked for malware. Malware protection should also be taken into account in the organisation's various integration interfaces.

If possible, devices should also be secured with controls that protect against harmful links.

Any alerts received from devices or servers should be reacted to immediately. The affected device or server should be isolated from the organisation's network, after which the matter should be thoroughly investigated, as an alert can be the first sign of an attempted breach. Even if no actual alerts are received, the monitoring logs of the information security products used should be regularly reviewed.

The National Cyber Security Centre Finland is interested in any malware encountered by organisations and related samples. For instructions on how to inform us of these, please see the link provided below.

Further information:

Transmitting e-mail and sending samples to the National Cyber Security Centre Finland

Microsoft – Macro malware

3.5 Prepare for denial-of-service attacks

Denial-of-service attacks are everyday occurrences on the internet. A denial-of-service (DoS) attack typically involves artificially creating traffic for a service by e.g. filling the bandwidth of the service's internet connection or causing such a high processing load for a device in the service chain that the service goes down. In addition to the server itself, other features, such as the firewall, can also become bottlenecks.

- Organisations should assess which of their digital services could potentially be targeted with denial-of-service attacks.
- Which services should remain operational even during load spikes?

For how long can your organisation withstand a DoS attack without operations being excessively disrupted?

The effective prevention of DoS attacks can require expertise and equipment that the organisation does not normally have access to. If the continued operation of a service is critical to the organisation, preparedness against disruptions should be taken into account as early as the planning stages of the service – at the very least, you need to know where to turn to for help and how quickly expert help can be provided.

The National Cyber Security Centre Finland is interested in DoS attacks targeted at organisations. You can report them to us using the incident reporting form available on our website.

Further information:

Tips for preventing denial-of-service attacks (in Finnish)

3.6 Secure your cloud services as well

Most organisations also make use of various cloud services. As such, organisations should ensure that necessary information security controls are implemented for cloud services as well. The default settings of cloud services are not always sufficient in terms of the information security of organisations.

When it comes to external cloud services, the service provider is typically responsible for infrastructure security. However, the party responsible for the security of the information stored on cloud services is always the end user. Even if the practical work is carried out by someone else, it is the responsibility of the organisation to manage their information security. As such, organisations should define and provide instructions on how their information should be protected and handled and what kind of security controls should be implemented on cloud services.

Further information:

Criteria for Assessing the Information Security of Cloud Services (PiTuKri)

Azure security best practices and patterns

AWS – Best Practices for Security, Identity, & Compliance

Google Cloud security best practices center

Guide on protection against Microsoft Office 365 credential phishing and data breaches

3.7 Secure your remote connections

Nearly all organisations have had to implement new remote access solutions during the COVID-19 pandemic. However, there are also vulnerabilities associated with remote access that are extensively exploited by criminals.

The fact is that every remote connection inevitably increases cyber security risks, which is why organisations should first and foremost assess whether their existing remote connections are still necessary. In regard to this, it is relevant to ask the following questions:

- Is your organisation aware of all the remote access methods available to your personnel or partners?
- Are all of your existing remote connections still necessary for your operations?

- Do all of your employees or partners still need remote access, or would it be sufficient to provide it only to persons who need to be on call, for example?
- Have the information security risks associated with external partners having remote access to the organisation's environment been adequately assessed, if applicable?

Once essential remote connections have been identified, the next step is to ensure their security. Here are some relevant measures:

- Determine whether the remote access solution used is sufficiently secure for its purpose and whether it is covered by the manufacturer's security updates.
- Monitor the vulnerabilities of the remote access product used and install security updates without delay on both the server and devices.
- Make sure that the remote access solution has been correctly configured in terms of security settings (e.g. multi-factor authentication) and that only functionalities essential to the organisation's operations are enabled.
- Make sure that remote access accounts are actively administered and that accounts that have become unnecessary (due to employees changing, for example) are immediately closed.
- Make sure that remote access is monitored and extensively logged. The organisation should have immediate access to its own remote access logs, even if the solution itself is administered by an external partner.
- Make sure that all remote connections are documented and that the documentation is kept up to date.

Further information:

CISA & NSA - Selecting and Hardening Remote Access VPN Solutions

3.8 Take care of backups

All information that is important to the organisation's operations should be regularly backed up. In addition to information related to operations, the settings of various systems should also be backed up. Backups must make it possible to restore operation even in the event that the organisation's entire IT environment has to be re-installed.

Organisations should also make sure to protect their backups. An intruder must not be able to compromise backups or steal information via unencrypted backups. This can be ensured by following the so-called 3-2-1 backup rule: You should have at least three copies of your data, the copies should be stored on at least two different types of devices or media and at least one copy should be kept off-site.

The restoration of backups should be regularly tested to ensure that their data can be restored and that the necessary systems settings are also backed up.

Further information:

Advanced ransomware attacks becoming more common – Avoid being targeted! (in Finnish)

Offline backups in an online world

Small Business Guide: Cyber Security

CISA – Stop Ransomware

NCSC-UK – Mitigating malware and ransomware attacks

3.9 Check which of your services are visible on the public internet

Criminals are constantly scouring the internet for services to exploit. Sometimes the organisations providing these services are not actually aware of which of their services can be freely accessed via the internet.

A service intended only for internal use may end up becoming accessible via the public internet inadvertently or as a result of a firewall configuration error, for example. Because of this, it is a good idea to occasionally check whether the organisation's own impression of where its services can be accessed from corresponds to reality.

There are various free-to-use search engines available online that make it relatively easy to determine the servers associated with an organisation's domain or what services they provide, for example.

Further information:

Shodan

DNSdumpster.com

3.10 Examine the risks posed by wireless technologies

Organisations also often utilise various wireless data transmission methods, i.e. methods based on freely propagating radio waves. When these methods are used in conjunction with critical functions, the specific risks related to wireless transmission must also be managed.

The use of wireless technologies always increases security risks through potential unauthorised interception, signal interference and outages resulting from unintended or intentional disruptions.

Wireless communications networks

Organisations should be aware of the risks that wireless telecommunications technologies pose for their critical processes:

- Communications links that are critical to the organisation's operations should never be based on any single wireless technology; you should always have an alternative available as well. Functions critical to the organisation's operations should not be built upon so-called licence-exempt radio equipment using frequency bands that are in shared use, as these frequency bands present a significantly higher risk of interference than those subject to frequency planning.
- The encryption of network traffic should never be based solely on the radio encryption offered by wireless technologies, but rather on sufficiently secure end-to-end encryption implemented on top of it.
- In regard to the mobile connectivity of devices, organisations should be aware that public Wi-Fi networks or the mobile networks of foreign telecommunications operators may not always be secure. If, after due consideration, these types of connections need to be used, you should make sure that all devices use a VPN connection administered by the organisation.

Location and time data services

The basic services of the Global Navigation Satellite System (GNSS) include open location and time data. Access to these is often considered a given, having become almost a universal constant. However, organisations should consider how their operations would be impacted if the reliability of this location and time data were compromised or if access to them were to be cut off for a long period of time, meaning at least several days:

- Accurate and reliable location data is integral to e.g. the development of smart mobility and situational picture systems, in which the coordination of various functions is based on the locations of persons or devices in an area. For example, location data is used by logistics companies to optimise the use of their vehicle fleets. Location data also plays an important role in aviation, seafaring and rail transport, supporting and assisting operations in various ways.

- Time data, on the other hand, is extensively used in e.g. data, telecommunications, television and energy transfer networks to synchronise the operations of various system components.

In regard to location data, operational reliability can be improved by utilising multiple GNSS systems, such as a combination of the European Galileo and the American GPS, and the frequency diversity reception of systems. The resilience of GNSS reception can also be improved with various antenna solutions. Some GNSS receivers also include software-based features for improving their resilience that need to be separately enabled. GNSS location data can also be supplemented with mobile positioning.

In seafaring and boating, it is important to ensure access to the necessary navigational charts and manual navigation methods.

While the reliability of time data can also be improved through the use of multiple GNSS systems, using a backup system based on a wired method or a local clock system is recommended.

Further information

Secure use of internet-connected devices (in Finnish)

Safe Bluetooth usage on smart devices

Current state and development prospects of satellite positioning (in Finnish)

Submit a notification of radio interference

Detection, reaction and operational continuity

4 Detect and analyse events

Organisations should make sure that they have the ability to detect any information security incidents affecting their critical environments. To this end, all devices, software and information resources that attackers could potentially exploit should be subject to logging. This log data is needed to determine the what, why and when of incidents.

Logging should be implemented based on the criticality of protected assets. In other words, the greater the potential impact of an asset being compromised, the more comprehensive the log data collected about it should be.

Log data should be protected from potential intruder influence. Logs should be securely stored somewhere else than the environment being monitored so that they cannot be altered by intruders.

Organisations should monitor the log data that they collect in order to gain a clear overview of their operative activities and cyber security. In particular, log data should be analysed for signs of the following:

- Abnormal events in the login logs of user databases and directory services (e.g. Active Directory or Azure AD). These can include the creation of new user accounts, elevated privileges or logins from abnormal geographical locations or devices or at abnormal times.
- Abnormal addresses, protocols, traffic volumes or unusually timed events in firewall logs.

Further information:

Collecting and using log data

NCSC-UK – Logging made easy (LME)

5 React to events and incidents

Organisations should have the capacity to immediately react to any cyber events or incidents affecting their critical functions. Organisations should also have appropriate persons or roles assigned for this purpose.

The key objective is to limit the impact of incidents on the organisation's operations and facilitate the restoration of normal operations. To this end, organisations should have a plan for reacting to cyber incidents that is maintained and covers the entire life-cycle of incident management.

Further information:

Guide for detecting data breaches (in Finnish)

NCSC-UK – Incident management

6 Ensure operational continuity

Organisations should prepare operational continuity plans, based on which operations can be maintained and restored in the event of a cyber event or incident.

The operational continuity plan should identify and document the devices, software, information resources and functions that are needed at a minimum to continue operations.

Further information:

NESA – Continuity management

Securing digital operations during incidents

7 Keep your personnel informed

Every member of an organisation plays an essential role in ensuring the cyber security of the organisation. As such, the organisation's management should make sure that personnel are aware of the importance of cyber security for the organisation's operations. More than anything, maintaining this awareness requires effective leadership and communications.

Personnel should be provided with training and information to help them maintain a sufficient level of preparedness for handling everyday cyber security threats.

To achieve this, organisations should implement at least the following measures:

- Management should clearly communicate the importance of cyber security for the organisation's operations and management's unconditional commitment to cyber security to the entire personnel.
- Personnel should be provided with regular information security training relevant to their work tasks so that they are able to operate in a secure manner, taking into account the most common information security threats encountered in their work, such as phishing and malicious attachments and links.
- Personnel should be provided with a channel for reporting any encountered or suspected information security issues.

Further information:

Keeping your information secure both at home and at work

8 Report information security incidents or suspicions thereof

The National Cyber Security Centre Finland encourages all organisations to report any confirmed or suspected information security incidents to it without hesitation.

Information security incidents should be preferably reported using the dedicated **online form**, but they can also be reported via email to **cert@traficom.fi** . In the case of non-urgent information security incidents, you can contact us at **kyberturvallisuuskeskus@traficom.fi** .

The information received through submitted reports is used to maintain the national situational picture of cyber security. If necessary, we will also contact the party who submitted the report.

A data breach is a crime, which is why they should always be reported to the police as well. Personal data breaches must also be reported to the Data Protection Ombudsman. Essential critical infrastructure operators and service providers must also report any security incidents in their networks and information systems to the supervisory authorities of their sectors (NIS notification obligation).

Further information:

Investigating cybercrime

Report a security incident (NIS notification obligation)

Personal data breaches

Transmitting e-mail and sending samples to the National Cyber Security Centre Finland

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland

PO Box 320, FI-00059 TRAFICOM, Finland
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISSN 2669-8757 (online)
ISSN 2669-8749 (print)

TRAFICOM
Finnish Transport and Communications Agency