Finnish Transport and Communications Agency
National Cyber Security Centre

Instructions – Data breach

Traficom Research Reports

24/2022

Contents

1 Introduction 2

1.1 Purpose of the instructions.. 2

1.2 What does a data breach mean?.. 2

2 Preparation... 3

2.1 Administrative measures 3

2.2 Technical measures.. 4

3 Detecting an information security breach 5

4 Instructions... 6

4.1 Workflow of an information security breach investigation 6

4.2 Immediate measures 8

4.3 Investigating an information security breach 10

4.4 Recovery 12

5 Post-incident review of an information security breach.................................. 14

1 Introduction

1.1 Purpose of the instructions

The purpose of these instructions drawn up by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom is to offer advice to organisations in situations in which it is suspected that there has been a data breach. The instructions are focused on how to deal with the special characteristics of this type of information security incident. In order to resolve the situation completely, the organisation should maintain the incident response plan it has drawn up in case of information security incidents and follow it.

These instructions offer guidance on a general level on how to act in case of an information security breach and recover from it. It is recommended that the organisation draw up a separate guide for its own use that takes its technological and operational environment into account in more detail. The project is funded by the National Emergency Supply Agency.

1.2 What does a data breach mean?

A data breach refers to unauthorised access to an information system, service or device or unauthorised use of an application by means of acquired access codes. Often the aim of a data breach is also to gain financial benefit, such as by stealing information that can be sold further. Sometimes the attackers do not steal anything themselves, but instead they sell access to the server to another criminal. An environment that has been hacked can also be used to distribute harmful material, or the operation of the hacked environment can be paralysed with ransomware. Attackers can use the environment they have hacked as a part of other attacks, such as a denial-of-service attack.

Data breaches cause a loss of reputation and financial losses to the targeted organisation. In addition, the normal operation of the organisation may be interrupted for a long time due to repairs or reinstalling the environment. Data breaches are also used for invoice fraud (business email compromise), in which case the financial losses may be significant. Unlike in typical cases of CEO fraud, if an organisation has become the victim of a data breach, a forged invoice can be sent from within the organisation, which makes it more likely to be approved.

Sometimes a data breach may be exploited a long time after the intrusion occurred. In that case, the organisation may no longer have log data from the time of the intrusion available, which makes investigating the incident considerably more difficult.

2 Preparation

Preparing for security incidents is a key method of reducing their severity and making it possible to recover quickly and continue the business. Organisations can assess their own readiness by using the Kybermittari (Cybermeter) cyber security evaluation tool of the National Cyber Security Centre Finland, for instance.[1] An incident response plan that has been drawn up in advance is a good starting point for what to do in case of a security incident. The organisation must also ensure that measures such as locking user IDs, isolating servers and terminal devices from the network and restricting network traffic to harmful IP addresses or domain names are technically possible and that the personnel have the expertise required to carry them out.

Gathering, compiling and monitoring log data is important in order to detect incidents in time. Log data also make it possible to investigate incidents thoroughly, which speeds up the cleaning and restoration of the environment, if necessary. The National Cyber Security Centre Finland has drawn up a guide on how to collect and use log data.[2] Depending on the systems used by the organisation, comprehensive monitoring typically also requires network- and system-level solutions in addition to this.

2.1 Administrative measures

- Draw up an incident response plan for your organisation in case of a data breach.
- Train the personnel on how to act during information security breaches such as those described in these instructions.
- Find out in advance how you can report an information security breach to the National Cyber Security Centre Finland.[3] Start monitoring the news by the National Cyber Security Centre Finland.[4]
- Review attack scenarios together with the company's management and agree on the practical measures as well as management responsibilities and authority in case of an information security breach.
- Develop[5] the incident response plan and practice it regularly with tabletop exercises, in which responsible persons and interest groups practice the information security incident response process in imaginary scenarios.
- Implement continuous vulnerability and update management.
- Identify the components critical to the business and create and maintain lists of what needs to be protected.
- Specify the necessary access rights carefully based on the needs of the users and the technical functionalities.
- Consider establishing a security operations centre or purchasing a similar service. The purpose of the security operations centre is to monitor the network traffic of your company and information security events in the systems.

[1] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

[2] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data

[3] https://www.kyberturvallisuuskeskus.fi/en/report

[4] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news

[5] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

2.2 Technical measures

- Back up your critical systems regularly and automatically by following the 3-2-1 rule. That is, have at least three copies in two different formats and keep one of these copies completely outside the network.
- Test the functioning of the backups regularly and practice restoring the backups of at least the critical systems.
- Take advantage of network segmentation, data encryption and access control to ensure that the attack surface of your company and the amount of material exposed to an attack at the same time are as small as possible.
- Aim to detect attacks as early as possible by using different kinds of centralised monitoring solutions and make sure that their functionality is also tested regularly.
- Install anti-malware software (Endpoint Detection and Response, EDR) on terminal devices that can be used to restrict the running of programs, investigate suspected information security breaches and isolate the computer from the network, if necessary.
- Implement mechanisms for filtering out emails that contain harmful content, spam and unwanted network traffic.
- Implement centralised log management to make effective detection and investigation of cyber threats possible.

3 Detecting an information security breach

The possibilities of detecting an attack depend largely on the method the attackers used to penetrate the system. The intrusion may have been carried out by exploiting a vulnerability in the server, a configuration error or a vulnerability in an application, or the attacker may have acquired credentials suitable for the server through phishing, for example.

An attack can be detected in the following ways, for instance:

- The system stops working or is not available.
- Unexpected measures have been taken in the system, and none of the employees admit to carrying them out.
- An information security product or service provider sends an alarm.
- The organisation is notified about the attack by a party outside the organisation via social media, customers, partners or the authorities, for example.
- A serious vulnerability is found in the system, and when it is corrected, it is discovered that the vulnerability has already been exploited.
- The attacker tries to blackmail the organisation with stolen information.

Report the information security breach to the National Cyber Security Centre Finland.[6] We advise you confidentially and free of charge on how to limit the damage, analyse the incident and take recovery measures. At the same time, you support the national information security situation awareness and make it possible to help and warn other potential victims.

See the guide on how to detect data breaches by the National Cyber Security Centre Finland (in Finnish).[7]

[6] https://www.kyberturvallisuuskeskus.fi/en/report

[7] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

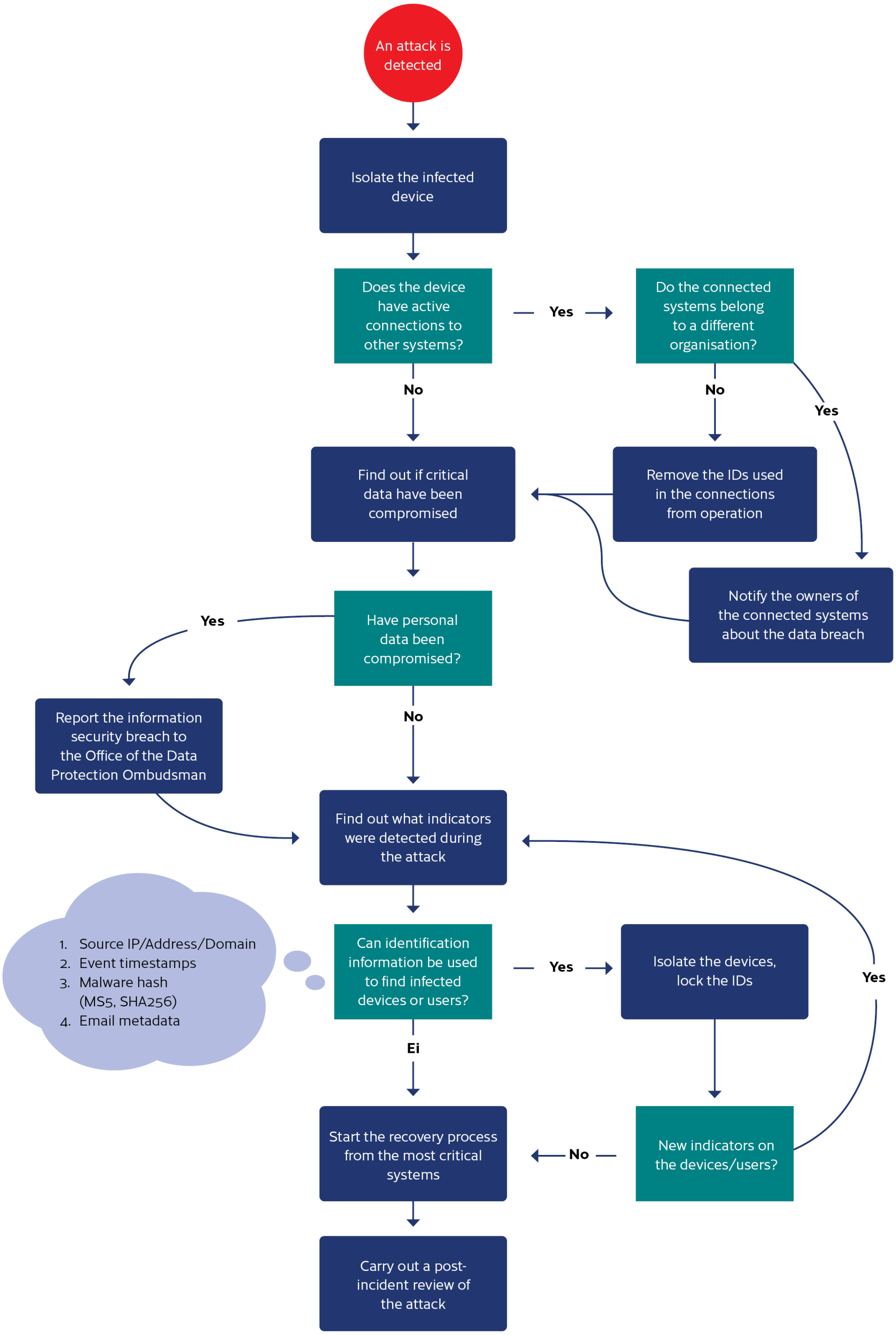
4 Instructions

Use the attached checklist to find measures to help you if you suspect that you have become a victim of a data breach. The checklist helps organisations to prioritise and use a phased approach when investigating information security incidents.

4.1 Workflow of an information security breach investigation

The flow chart below describes the right order of measures when investigating the security breach. The flow chart supports the use of the checklist. During the investigation, it is also crucially important to keep an accurate event log of the measures taken. The log should show the measure taken, the timestamp and the party that implemented the measure.

The gathering of potential evidence should also be documented carefully. You should record who gathered the data, what it was, and when and how it was gathered. A carefully drawn up event log makes the investigation as well as the cooperation with the police and information security investigators significantly easier.


An attack is detected
Isolate the infected device
Does the device have active connections to other systems?
Yes
Do the connected systems belong to a different organisation?
No
No
Yes
Find out if critical data have been compromised
Remove the IDs used in the connections from operation
Notify the owners of the connected systems about the data breach
Yes
Have personal data been compromised?
Report the information security breach to the Office of the Data Protection Ombudsman
No
Find out what indicators were detected during the attack
1. Source IP/Address/Domain
2. Event timestamps
3. Malware hash (MS5, SHA256)
4. Email metadata
Can identification information be used to find infected devices or users?
Yes
Isolate the devices, lock the IDs
Yes
Ei
Start the recovery process from the most critical systems
No
New indicators on the devices/users?
Carry out a post-incident review of the attack

4.2 Immediate measures

Goals of the phase	The accuracy and speed of the measures are both important. The goal of the immediate measures is to protect the critical data in the environment, stop the malware from spreading, prevent the attackers from gaining a foothold in the network and prepare for the start of the recovery process.

Phase	Purpose	Measures
Isolate the infected device	The aim of isolating the infected device from other data networks is to stop the attack from progressing and protect the data in the system.	Isolate the device by using the endpoint detection and response features. If necessary, disconnect the network cables of the device. The isolation must also ensure that the device cannot access the internet to prevent the attacker from stealing data from the server.
Contact your IT service provider	Often a part of the organisation’s IT infrastructure has been outsourced to a service provider. The assistance of service providers may be needed for some of the measures related to limiting the scope of the incident.	Contact the service provider’s contact person in case of crisis situations. Among other things, you may have to ask your service provider to disconnect your servers from networks, restore them, or send their logs. IT service providers often also have experienced personnel who can help with resolving the situation.
Find out what connections were active on the server	Servers often have active connections to other systems. Such connections may include a database connection or different kinds of API calls and keys. The integrity of the connected systems must be verified as soon as possible to determine how serious the situation is.	If the server has active connections to other systems, ensure the integrity of the data by reviewing the logs of the connected systems. Issues to check may include, for instance, the size of database searches carried out or a large number of interface calls while the attacker was on the server. Change the IDs of the connected services, such as the database ID used by the infected server as well as the interface keys and certificates used for the connections.
Notify those partners in cooperation and interest groups that may be affected by the incident about the information security breach	The security breach may cause the partners, customers and service providers risks or problems with the availability of services.	Notify the contact persons in case of crisis situations of different interest groups about the incident if you believe that it may affect the availability of their services. If the server has also had connections to other organisations, notify them about the issue, too. This will allow them to invalidate the IDs, keys or certificates used on the infected server. It is also important that they verify the integrity of their own data.
Evaluate whether you need external help to handle the information security breach or not	The organisation may need help with technical measures, managing the security incident and organising measures. If the necessary expertise is not available within the organisation itself or directly from the IT service providers, you should consider getting external help.	Technical measures to handle the security breach may require external expertise. External expertise may be required e.g. for collecting identification information and investigating the threat based on it. External assistance may also be useful with checking whether the attacker

		was able to obtain data important to the business, and if so, what kind of data. The National Cyber Security Centre Finland can help organisations especially during the first response to the incident as well as by offering additional information on similar cases in Finland and abroad. You can find Finnish service providers in the resources listed in the footnote.[8]
Report the information security breach to the Office of the Data Protection Ombudsman	If there is a risk that personal data may have ended up in the hands of the attacker as a part of the data breach, the incident must be reported to the Office of the Data Protection Ombudsman without undue delay and, if possible, within 72 hours of when the organisation found out about the information security breach.	Submit a preliminary notification about a personal data breach immediately, because you can supplement the notification later. The controller must assess the level of risk caused by the information security breach to the persons targeted by it. The level of risk determines the measures that the controller must take later. Document all personal data breaches as well as their impact and the corrective measures implemented. The log data from the time of the incident affecting the information system also fall within the scope of the documentation obligation. The Data Protection Ombudsman may ask for the log data for processing the notification of the information security breach.
Also report the incident to the other authorities	Report the incident to the authorities. The organisation may have an obligation to report the incident based on regulations or the terms of the cyber insurance.	File a report of an offence about the incident with the police.[9] Also notify the National Cyber Security Centre Finland of the incident[10] to maintain situation awareness and get help. The infrastructure operators and service providers critical to the security of supply that are subject to the NIS directive of the EU on the security of network and information systems must notify the authorities about information security incidents in network and information systems.[11]

[8] https://dfir.fi/
https://www.fisc.fi/fi/about-us
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/ (in Finnish)

[9] https://poliisi.fi/en/report-a-crime

[10] https://www.kyberturvallisuuskeskus.fi/en/report

[11] https://www.kyberturvallisuuskeskus.fi/en/services/report-security-incident-nis-notification-obligation

4.3 Investigating an information security breach

Goals of the phase	The goal of investigating the security breach is to determine the extent of the attack and its impact on the organisation. A thorough investigation ensures that malware and potential backdoors have been removed from the environment.

Phase	Purpose	Measures
Identify harmful activity and collect identification information	Identification information is collected to make it possible to map how widely the infection has spread to devices and how the stolen access rights have been used. Once attackers have gained a foothold, they may use different kinds of attack methods. In fact, identification information should be collected extensively and signs of their use should be studied carefully to ensure that the cleaning of the environment can be done reliably. Recovery can only start after the attacker has been removed from the environments.	The identification information gathered includes, among other things, the time when the incident occurred, when a login to the server occurred, or when a certain command was run on the server. The malware often communicates with the attacker's command and control server. By studying the network traffic of infected devices or domain name resolution (DNS logs), the source IP addresses or domain names used by the attacker can be identified. When harmful files are identified, their hashes (MD5/SHA256) can be extracted and used to identify harmful files on other devices, too. Authentication events related to infected devices and measures taken by the user accounts linked to them can be used to determine the IDs used to spread the malware. Endpoint detection and response often has features for collecting and using the identification information mentioned above. Otherwise, the measures should be taken manually by using a centralised log server. If no such server is available, either, the logs of individual servers and terminal devices should be examined.
Use the identification information to help with identifying all infected systems	The identification information can be used to find out how far into the organisation the attacker was able to penetrate. By collecting identification information and searching for it in the target systems, it is possible to ensure that all infected devices and identifiers are found and cleaned.	Identification information can be used to find infected devices, such as by using the endpoint detection and response features that often offer the option of searching for events on devices based on different identifiers. If the organisation has also implemented centralised log management, it can be used to search for events efficiently based on identifiers from several different devices at the same time. If neither of the solutions mentioned above is available, identifiers should be searched separately from each device. Different kinds of remote control solutions can be used for the purpose, however; they often enable running PowerShell commands simultaneously on several servers, for instance. There is a risk that the attackers have attempted to cover their tracks

		by disabling logging after gaining access to a device. In that case, it may not be possible to find all of the collected identification information in the device logs. For this reason, it is important to aim to use a wide variety of identification information and event sources.
Find out if critical data have become endangered	As a part of the investigation, it should be determined whether the attackers were able to access important data of the organisation or potentially the personal data of customers or employees.	Find out if the IDs, certificates or keys used for the connections have been used to log in from a place other than the server on which they should be used. Find out if the attacker was able to access the data and steal them by reviewing the database or interface logs. Based on the overload or the searches made, you can determine if the attacker intended to retrieve information. Review the network device logs to find out if there are any abnormalities in the traffic of the infected server. Unusually high traffic may indicate e.g. that the attacker has been able to steal information. Note that even if attackers have not destroyed or stolen the data, they may have edited them. The attacker may also have stolen data with a small size but great importance, such as IDs.
Save all available log files and other evidence on a hard drive isolated from the network for later investigation	The aim of collecting and storing evidence is to guarantee a high-quality investigation after the incident so that the root causes of the incident can be determined. Evidence may be needed for filing a report of an offence and the court proceedings. If the organisation has a cyber insurance policy, the insurance company may also require more detailed information on the security incident as well as evidence for the investigation.	Save log files that contain information relevant to the investigation of the incident on a hard drive isolated from the network. Also collect harmful email and other messages, if any. Aim to keep the evidence, such as complete disk images and memory samples, as intact as possible. Extract integrity hashes from them to ensure this. Aim to save samples of the malware detected. They should be handled with extreme care. Professional expertise is often required to carry it out safely. Send the samples to the National Cyber Security Centre Finland.[12]

[12] https://www.kyberturvallisuuskeskus.fi/en/news/transmitting-e-mail-and-sending-samples-national-cyber-security-centre-finland

4.4 Recovery

Goals of the phase	Start the recovery from the systems that are the most critical to the business. The organisation should aim to restore the business back to normal as quickly as possible, but only after the recovery can be carried out safely.

Phase	Purpose	Measures
Restore the infected systems from backups	The aim is to restore the systems and return them to normal operation. Restoring the systems should be done as safely as possible to ensure that the attacker cannot get back into the system.	Restore the systems from backups. Also take account of the risk that previous daily (incremental) backups may already have been infected. When restoring old backups, keep in mind that the backup may include the vulnerabilities that the attacker used in the attack. You can try to prevent the risk by restoring the systems without a network connection and updating the operating system and its applications before connecting to the network. If there is no suitable backup available, do a clean install of the operating system and its applications, starting from scratch. Also take the risk factors mentioned in the previous section into account. Do not try to clean an infected system by using anti-malware or automated tools, because there is no guarantee that they will be able to clean the system completely. Check the systems with anti-malware software before connecting them back to the network again.
Restore the infected IDs and ensure that the system administrator IDs are safe.	Ensure that the login information of all of the potentially infected IDs is changed so that the attacker can no longer use the IDs to access the organisation's systems. Make the user login requirements stricter, if possible.	Change the passwords of infected IDs and start using the IDs again. To make sure, change the password of administrator accounts and service accounts in case some of them have fallen into the hands of the attackers. Deliver the new passwords to users either verbally in person, in a text message or by telephone. Do not use the organisation's email or instant messenger, because the attacker may still have access to them. Consider adding two-factor authentication to administrator accounts as well as the IDs that were exploited during the attack. In addition, monitor the IDs used in the attack more carefully after the attack in case the attacker gains control of them again. If it is still unclear to the organisation how the attacker was able to gain control of certain IDs, consider creating completely new IDs. In this way, you can ensure that the attacker cannot gain control of the IDs again by using the method that could not be identified.

Restore the infected records	If it is suspected that the attacker has edited the contents of the database, the database must be restored from a backup copy to invalidate the attacker’s changes, if cleaning the data is not possible.	Take advantage of the database and interface logs to determine if the attacker has edited records. If the accuracy of the logs is not sufficient for cleaning up the changes, restore the data in the database from the latest safe backup. If the attacker has stolen data, all of the passwords contained by the stolen data must be changed. This should also be done even if passwords were only stored in the form of hashes. Notify the people whose data have been compromised in connection with the breach, so that they can prepare in case of the potential misuse of their data. Also notify them that it has been necessary to restore data to an older version starting from a specific date so that the interested parties can update their data.

5 Post-incident review of an information security breach

When the crisis is over and business operations have returned to normal, it is important to start the post-incident review of the attack and learn as much as possible about what happened for the future. At the same time, crisis management systems should be updated based on the observations made. The organisation may become a victim of a similar attack again, if the root causes of the incident cannot be determined and no lessons are learned from it.

During the post-incident review, the activities during the crisis are studied: what measures were done well, what could have been done better, and how the plans and the security level could be improved. A report should be drawn up on the post-incident review that examines at least the following questions in addition to the course of the events:

- Root causes of the incident:
    - What technical or functional weaknesses led to the situation?
- Effectiveness of the organisation’s own protection:
    - Were the controls used to detect attacks sufficient?
    - Did the attacker’s actions raise any alarms?
    - What was the reaction to the alarms like? Was the information about alarms transmitted to the right responsible persons?
- Actions during the crisis:
    - Was the crisis plan followed? How usable was it?
    - Were the responsibilities of the crisis management team assigned to the right people?
    - How successful was limiting the scope of the attack and removing the attacker?
    - How successful were the communications of the crisis management team? How were the interest groups taken into account?
- Recovery:
    - How did the recovery of critical information and services go?
- Post-incident review:
    - Have the course of events and the investigation work been documented?
    - Was the technical investigation of the incident sufficient? Has it been possible to submit sufficient data on the attack for the use of the authorities, for example?
    - Evaluate the actions of the service providers. Were the response time and the services that were agreed upon sufficient for the investigation of the incident?

The organisation should update its own incident response plan and more detailed playbooks designed for combating different types of security incidents after the fact. Practicing different scenarios at regular intervals is also recommended to ensure that you can benefit from them in crisis situations.

The National Cyber Security Centre Finland hopes that the companies and organisations share the most important lessons they have learned from the incident with the Centre, too. With incident reports, the National Cyber Security Centre Finland can help other organisations in Finland as well as internationally to investigate similar cases. The lessons learned from recovery help with developing the preparedness of all organisations.

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland
PO Box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-816-4

NATIONAL EMERGENCY SUPPLY AGENCY

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre