TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Instructions – Supply chain attack

Traficom Research Reports
21/2022

Contents

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 a supply chain attack is suspected. 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 supply chain attack mean?

In a supply chain attack, the information systems of the organisation are breached via the networks, services, products or open source projects it uses. The attack exploits the trust of organisations in their suppliers. The attack route may involve partners, service providers, software or devices. Attackers penetrate the supplier's systems and infect the part used in the supply chain with their own malicious code, after which it spreads via the normal product distribution channel to the partner and customer organisations.

The aim of a supply chain attack is to gain a foothold in different organisations along the supply chain. Once a foothold has been secured, it can be used in different kinds of further attacks, such as data breaches and ransomware attacks.

Detection and management of supply chain attacks is important, because they have a major impact on the reputation and trust of the organisation in the network. The victims of a supply chain attack include both the supplier and the customer. Managing the situation often requires transparency and cooperation from the parties.

2 Preparation

Preparing for security incidents is a good way to reduce their severity and make 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. 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 supply chain attack.
- Train the personnel on how to act during security incidents such as the ones 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.
    - Maintain a list of the components of the most critical systems.
- Maintain a list of the licences and software used by the organisation and their versions.
    - Follow their update schedules and vulnerabilities.
- Specify the necessary access rights carefully based on the needs of the users and the technical functionalities.
- Evaluate the status of the cyber security of suppliers. By ensuring that all suppliers provide a full description of their security measures, you can establish an idea of the safety of their

[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

products. You can also ask a cyber security professional to review the information provided by suppliers to find out whether the security solutions are sufficient and appropriate.

- 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.

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 is as small as possible.
- Protect the connections of your partners with strong encryption settings and implement multi-factor authentication.
- 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 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.
- Centralised log management should be deployed to enable efficient detection and investigation of cyber threats.

3 Detecting an information security breach

Detecting an information security breach that has occurred via the supply chain may be challenging, because the attacker exploits the organisation's trust in its partners. The intrusion is often carried out by using the partners' connections or infecting an application provided by them. In that case, the attacker does not yet do anything that could be interpreted as suspicious or harmful at the intrusion stage.

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

- A partner reports that they have become a victim of a cyber attack.
- An attempt is made to use the IDs of partners to log in to services they would not normally log in to.
- An information security product or service provider sends an alarm, which is usually caused by a trusted application.
- The organisation is notified about the attack by a party outside the organisation, such as social media, customers, partners or the authorities, for example.

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

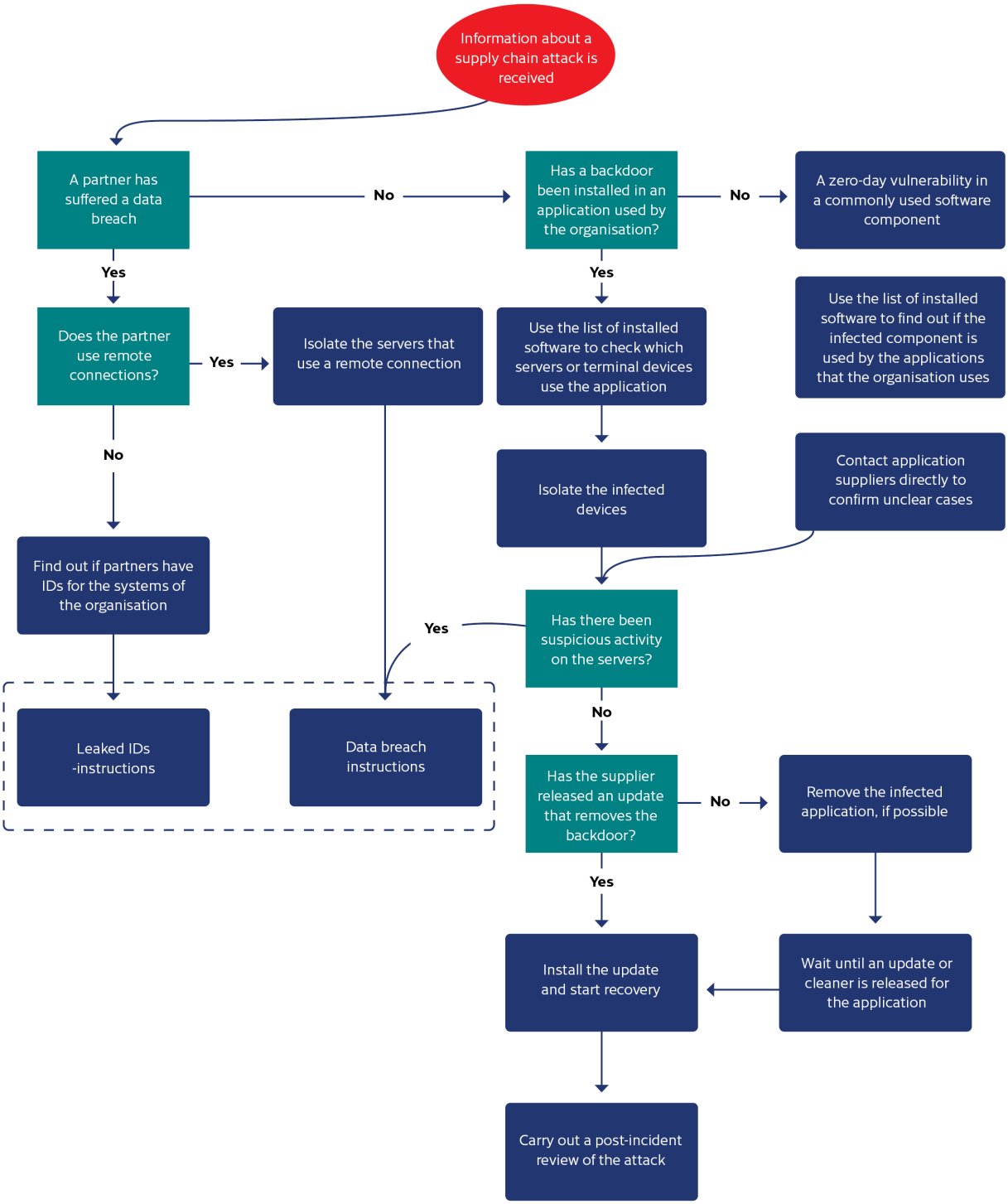
4 Instructions

Use the attached checklist to find measures to help you if you suspect that you have become a victim of supply chain attack. 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.


Information about a supply chain attack is received
A partner has suffered a data breach
No
Has a backdoor been installed in an application used by the organisation?
No
A zero-day vulnerability in a commonly used software component
Yes
Yes
Does the partner use remote connections?
Yes
Isolate the servers that use a remote connection
Use the list of installed software to check which servers or terminal devices use the application
Use the list of installed software to find out if the infected component is used by the applications that the organisation uses
No
Isolate the infected devices
Contact application suppliers directly to confirm unclear cases
Find out if partners have IDs for the systems of the organisation
Yes
Has there been suspicious activity on the servers?
Leaked IDs -instructions
Data breach instructions
No
Has the supplier released an update that removes the backdoor?
No
Remove the infected application, if possible
Yes
Install the update and start recovery
Wait until an update or cleaner is released for the application
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 devices by using the features of endpoint detection and response. If necessary, disconnect the network cables of the devices. The isolation must also ensure that the device cannot access the internet to prevent the attacker from stealing data from the server.
Find out what connections or components were used in the attack	Many different kinds of connections can be used in a supply chain attack, such as data transfer, software update, system or maintenance connections. Attacks can also be implemented by exploiting software or their components.	Find out if the attack was carried out • by using a remote connection or leaked IDs of a partner, or • through a backdoor installed in an application used by your organisation. Find out if the software and systems on the infected device are up to date. Also follow the bulletins of the National Cyber Security Centre Finland, because the attack may have exploited a new zero-day vulnerability.
Find out which servers and workstations may have become infected in the attack	You must be able to identify rapidly all servers and terminal devices that are using the connection or component exploited in the attack, so that all devices that may have been infected can be isolated.	Take advantage of the list of your IT assets and installed software quickly to determine where the infected application or component is used. If a remote control connection or other integration is involved, check the documentation to find out where they are used and how they can be accessed. If, for example, the infected component is a library that is used by several different systems, check the applications that are being used by going through the list of installed software and find out if they use the component in question. This may require the organisation to contact the application supplier directly for confirmation. If one of the measures is not possible without the help of the IT service provider, go to the next section in the instructions.
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.	In this phase at the latest, find out what parts of the IT infrastructure of your organisation have been outsourced to service providers. 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 give further assistance with resolving the security incident.
Notify the 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. The cyber security of the partners may also be endangered due to a supply chain attack.	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 had active connections to other organisations, notify them, too, so that they can invalidate the IDs, keys or certificates that were used on the infected server. It is also important that they check the integrity of their own data. If necessary, also notify the other organisations in the supply chain, such as the supplier.
Evaluate whether you need external help to handle the information security breach or not	The organisation may need help with organising measures, managing the incident or technical 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 incident may require external expertise. Such measures include 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 via the links in the list of references.[8]
Report the information security breach to the Office of the Data Protection Ombudsman	If 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 an information security 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

[8] https://dfir.fi/

https://www.fisc.fi/fi/about-us

https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/ (in Finnish)

		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 information security breach to 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 breaches in network and information systems[11].

[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 signs of harmful activities 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 all of the environments.	Collect the following identification information: • When the login to the server occurred • From which IP address the login was carried out • At what time was a specific command run on the server • What the command in question caused 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), you can identify the source IP address or domain name used by the attacker. You can extract the hashes (MD5/SHA256) of harmful files and use them to identify the 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 a functionality 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, you can examine the logs of individual servers and terminal devices.
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.	You can use identification information to find infected devices, such as by using the endpoint detection and response features that often directly offer the option of searching for events on devices based on different identifiers. If the organisation also uses centralised log management, you can use it to search for events based on identifiers from several different devices at the same time. If neither of the solutions mentioned above is available, search for the identifiers separately from each device. You can use different kinds of remote control solutions 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 which case their activities have left no trace. For this reason, you should review identification information collected from all of the different sources and use it to try and establish an overview of the attackers' activities.
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. In order to determine how serious the situation is, you should check as soon as possible if these systems have also been hacked. Find out as quickly as possible if the connected systems have also been hacked by reviewing their logs. This will give you an overview of the scope of the incident.	If the server has active connections to other systems, find out if the connected systems have also been hacked by reviewing their logs. Issues to check may include 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.
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 attackers were able to access and steal data. By reviewing the database or interface logs, you can determine if the attacker intended to download information based on the searches or the level of overload. Review the network device logs to find out if there are any abnormalities in the traffic of the infected server. Unusually heavy traffic may indicate, for instance, that the attackers have stolen information. Note that the attackers may have edited the data in addition to destroying or stealing them. The attackers may also have stolen very small amounts of data, 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 during the criminal investigation and for 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. Try to take samples of the malware detected and save them. They should be handled with extreme care. Professional expertise is often required to store them 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	The recovery starts 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
Reactivate the connections and start the applications	The aim is to return the partners' remote connections or software needed for business back to operation.	Before activating the connections, make sure that they are safe and that the partners have also been able to clean their own systems and IDs. Before activating the software, make sure that the necessary updates to correct the issue have been installed. If there is no update available to correct the issue, do not deploy the software and consider removing it completely.
Restore the infected systems from backups	The aim is to restore the systems and return to normal operation. Restoring the systems is done as safely as possible to ensure that the attacker cannot get back into the system.	Restore the systems from backups. Take into account that the previous daily (incremental) backups may already have been infected. When restoring old backups, keep in mind that the backup may contain the vulnerabilities that the attacker used during the incident. Try to restore the systems without a network connection, and update the operating system and its applications before connecting to the network to avoid these risks. 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 automatic scanners may not necessarily be able to clean the systems completely. Check the systems with anti-malware tools 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 infected IDs is changed so that the attacker can no longer use the IDs to access the organisation's systems. Strengthen the user login requirements, 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, but do not use email or the instant messengers used in the organisation, 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 in the attack. In addition, monitor the IDs used in the attack more

		carefully after they have been restored in case the attacker gains control of them again. If it is still unclear how the attacker was able to gain control of certain IDs, consider destroying them and creating completely new IDs. In this way, you can ensure that the attacker cannot use this unidentified method to gain control of the IDs again.

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 security breach 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 breach again, if the root causes of the security breach 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 instructions 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 978-952-311-813-3

NATIONAL EMERGENCY SUPPLY AGENCY

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre