TRAFICOM
Finnish Transport and Communications Agency

What to do in case of a ransomware incident
- instructions for management

Traficom Publications

15/2022

Contents

1 What is this about?

Ransomware refers to a cyber attack in which the attackers aim to encrypt the organisation's data with an encryption algorithm and demand a ransom to restore the data. The criminals may also steal the data they have encrypted and blackmail your organisation with a data leak. The risk of being targeted by an attack has increased considerably in recent times: the number of attacks increased from 2020 to 2021 by roughly 105%.[1]

Criminals have found ransomware an effective way to benefit financially, because organisations unprepared for the threat are easy targets. Paying the ransom is rarely a solution, however, because the attack and the related blackmail may continue regardless. The right kind of preparation for ransomware attacks clearly improves the level of information security of organisations and their resilience in the face of ransomware as well as other potential attacks. It is good to note that in some cases the purpose of the attack is to destroy data.

The goal of these instructions is to offer guidance for the top management of organisations on what to do in case of a ransomware incident. In addition to these instructions, you will need technical instructions aimed at the people responsible for information security or the ICT environment of the organisation. You can find more examples of technical instructions in Chapter 5 (Sources and additional instructions). Figure 1 summarises the contents of the instructions on preparation and attack management as a whole.

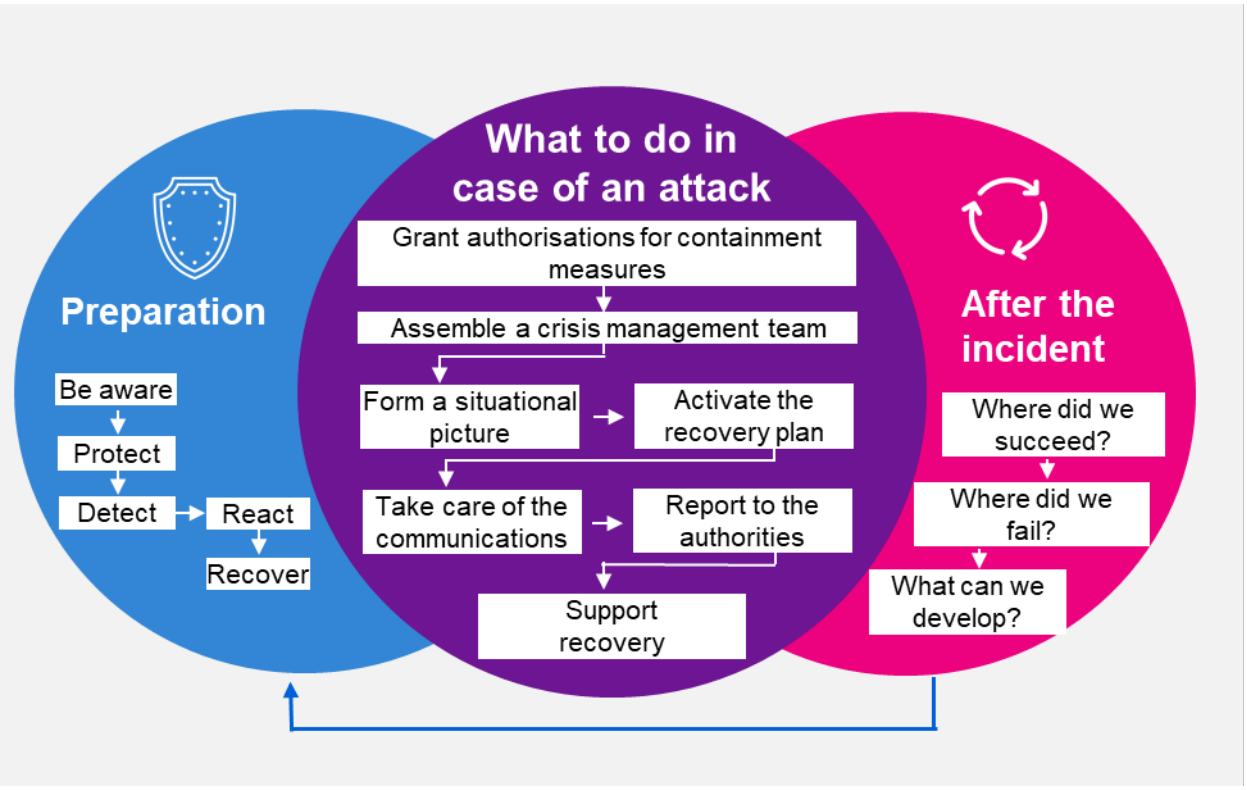

Figure 1: Preparation for a ransomware attack and its management as a whole

1.1 Impact of an attack

A successful ransomware attack often leads to business activities being disrupted or even stopped completely. This may mean a significant financial loss for the organisation and its customers, if the operation cannot be restored quickly enough. In the worst case, ransomware may also reach factory and production environments as well as their ERP (enterprise resource planning) systems via shared services. Ransomware that has reached an automation environment may halt the production completely, or in the worst case scenario it may cause a

[1] Sonicwall, 2022 Sonicwall cyber threat report, https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

threat to the safety of people or the environment. In addition to the above, various sanctions related to regulation (including data protection) may also be significant in magnitude[2].

A ransomware attack is a risk to the company's reputation, because incidents often lead to the issue being discussed in public. This may also have a significant impact on the company's reputation, the trust of different interest groups and potentially also the company's value, if the organisation was not prepared for an attack or did not manage it appropriately.

1.2 How could an attack start?

Figure 2 presents one potential scenario of attackers carrying out a ransomware attack. In addition to this one, there are also several other attack and implementation methods.

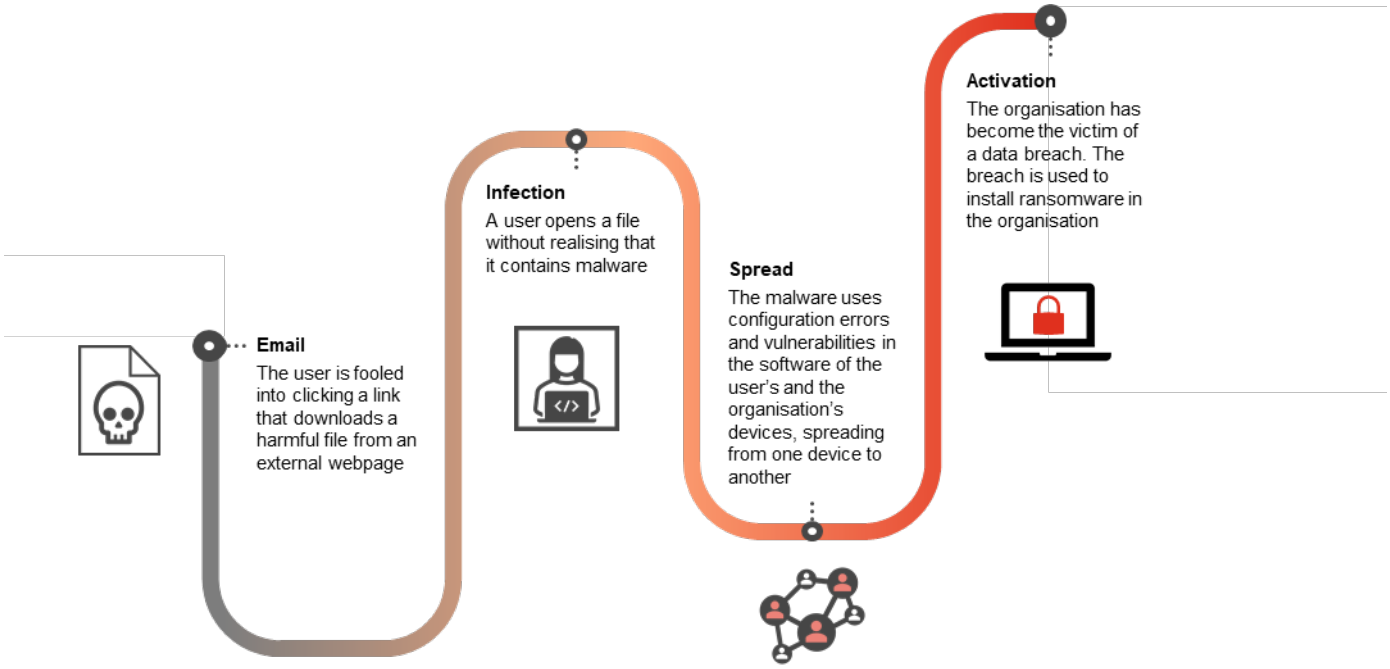

Figure 2: Example of a ransomware attack

1.3 Potential manifestation of an attack

A ransomware attack may manifest in different ways, depending on how it is implemented. In the best case scenario, the organisation under attack is able to detect the first stages of the attack quickly and react appropriately to the situation by stopping the spread. In the worst case, the attack is only noticed after the malware has spread through nearly the entire organisation. With their actions, attackers often aim to drive the target organisation into a seemingly hopeless situation, making the recovery from the attack more difficult.

It is frequently impossible for the management of the organisation to control or identify the different manifestations of the attack themselves, but they should understand when the organisation may be targeted by a ransomware attack. The following observations may be signs of a successful ransomware attack:

- The attacker sends a blackmail message to the target organisation, or such a message appears on the display of a workstation.
- The organisation is notified about the attack by a party outside the organisation via social media, customers, partners or the authorities, for example.

[2] GDPR.EU, What are the GDPR fines? 2022, https://gdpr.eu/fines/

- The organisation's files cannot be opened from a network drive, for instance, or they are otherwise corrupted.
- The equipment in a factory or production environment stops working without a visible or identifiable cause.

2 If the worst happens, do this!

2.1 Give permission and authorisations for containment measures

When a ransomware attack strikes, the management needs to act quickly and decisively, because the organisation moves from normal management to crisis management. This also means transferring the authority to implement acute containment measures to the ICT or information security personnel instead of the normal authorisation processes.

The first minutes are the most important for mitigating the impact of ransomware attacks. The ICT or information security staff may have to make difficult decisions, such as shutting down some services or disconnecting them from the network. It is important to authorise them to implement the necessary restrictive measures independently, because authorising measures one at a time may take too much time in a critical situation and spread the problem further. The organisation may also need help from outside experts. The authorisation to seek outside expert help must also be ready.

The management of the organisation should be aware that the experts aim to do everything necessary, and it is extremely important to ensure that they can work in peace and that they will be able to operate throughout the attack situation.

2.2 Assemble a crisis management team

When an attack strikes, it is important to assemble a crisis management team. The crisis management team is tasked with coordinating and assigning responsibilities for the necessary measures at the organisational level and monitoring the implementation of the agreed restrictive or resolution measures and their effectiveness.

The crisis management team may consist of the organisation's expanded executive group, for instance, but it should include the following persons or roles:

- Managing director/CEO
- Persons responsible for business or core functions
- Person responsible for information security
- Person responsible for ICT
- Person responsible for communications
- Person responsible for legal affairs and/or data protection.

2.3 Duties of the crisis management team

2.3.1 Form a situational picture

Once your ICT or information security personnel have started the necessary restrictive measures and notified the management of the organisation about the situation, the crisis management team should draw up a situational picture on the impact of the attack based on the information available.

When forming the situational picture on the organisational level, take account of the following:

- What is the importance and direct impact of the data lost during the attack for the core, business or support functions of your organisation and those of your customers?
- What financial impact does the incident create directly or indirectly, and does your organisation have enough funds available?
- Who should be notified about the attack immediately (employees, board of directors, customers, interest groups)?
- You should also identify other potential scenarios due to the attack and their likelihood, such as whether the organisation has become the victim of a data breach, or what kind of consequences would the publication of the data stolen during the attack have for you or your customers?
- The crisis management team must maintain an incident log. Document every step of the attack and recovery from it in the form of a timeline. Accurate documentation is very important for recovery, learning about the incident, your own legal protection and cooperation with the authorities.

The crisis management team is also responsible for ensuring that the situational picture is always kept up to date to make it possible to manage the situation and provide information about it.

2.3.2 Draw up and activate a recovery plan

If your organisation already has a plan for recovering from a ransomware attack, now is the time to start following its instructions.

If your organisation does not have an existing plan, focus on the following:

- How can we limit the activities of the attacker and their spread through our information systems?
- Before we start restoring our systems, have the attacker's connections to our systems been broken and has the malware installed there been removed?
- How can we restore our core services and business as well as the resources they need to normal conditions and verify that their information security is in order?
- What resources (internal and external) do we need for this purpose? Make sure that the ICT or information security staff gets the support they need for the system restoration process, such as inspecting and restoring backups.
- If your organisation has cyber insurance, make sure that the organisation contacts the insurance company. Some cyber insurance policies may include service elements, such as the expert support needed to help with resolving the situation.

Do not pay the ransom! At first, it may seem as if the cost of paying the ransom would be lower than solving the crisis independently. However, you must never pay the ransom under any circumstances, because:

- You cannot trust the word of criminals, and there is no guarantee that the encryption keys they offer will even work.
- Even if the keys do work, the recovery may be slow and expensive.
- Paying the ransom funds criminal activities and supports their development.
- The blackmail may also be a deception, if the malware has destroyed the files instead of encrypting them.[3]

[3] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

- Paying the ransom may violate sanction regulations or the national regulations of one of the countries receiving the payment, meaning that it is not certain that the ransom payment could even be made successfully.

2.3.3 Take care of internal and external communications

Plan how to inform the board of directors, customers and partners of the company as well as the authorities about the situation, the recovery process and its progress. Also report to interest groups and update the situational picture for them as the situation progresses.

Decide who will act as the public face of the organisation towards the general public and who will contact the customers or other necessary interest groups. Avoid situations in which the persons most important for solving the issue (such as technical experts or the person responsible for information security) would act as information officers of the organisation. They should be allowed to work completely in peace on tasks related to recovering from the situation itself.

2.3.4 Report to the authorities

Report the attack to the National Cyber Security Centre Finland. We offer help with investigating the attack, and your report will help other organisations that may be targeted by an attack. You can report to us by email at the address cert@traficom.fi or by filling in the form (https://www.kyberturvallisuuskeskus.fi/en/report). You should also expect the National Cyber Security Centre Finland to contact you.

File a report of an offence with the police concerning the attack at the address https://asiointi.poliisi.fi/en. You should do this in connection with the technical investigation of the attack, because evidence must be attached to the report. The police will guide you in how to record the evidence appropriately. If the attack endangers public safety (e.g. a security threat[4]) or the health or lives of people, report it directly to the emergency telephone number 112.

If the criminals have obtained personal data, the Office of the Data Protection Ombudsman must be notified within 72 hours of detecting the data breach at the address https://tietosuoja.fi/en/data-breach-notification. The primary purpose of this is to protect the rights of data subjects. If necessary, you can submit the notification in stages: start with a preliminary notification and complete it later. [5]

If your organisation operates in a field critical to the security of supply, you also need to notify the supervisory authority in your own field, or in this case the NIS authority (in Finnish): https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=fi&RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme. You can find more information about the regulations related to the NIS Directive here: https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/digital-services-and-infrastructure

2.4 Support the implementation of the recovery plan

Once the immediate measures to resolve the attack have started, the management of the organisation should focus on implementing the recovery with the necessary measures. The organisation's management can support this by being easily accessible to the key persons and supporting the work of the people central to recovery by maintaining a calm and forward-thinking atmosphere, among other things. It is good to keep in mind that right now you should not focus on what each person may have done wrong or failed to do.

In general, too much attention should not be paid on the costs incurred by the recovery from the attack or the time lost. The most important thing is to try to recover from the attack as efficiently as possible as an organisation so that it could return to normal as soon as possible.

[4] Threats to safety when handling chemicals (in Finnish): https://tukes.fi/turvauhkiin-varautuminen-vaarallisten-kemikaalien-kasittelyssa-ja-varastoinnissa

[5] https://www.suomi.fi/guides/data-breach/acute-measures/notify-the-authorities

3 Measures after the crisis

When the crisis is over and business operations have returned to normal, it is important to start investigating the attack and learn as much as possible about what happened. At the same time, it is good to assess where we were and were not successful from the perspective of the attack and how we could improve our security level to avoid similar situations in the future.

Primarily, your organisation should nevertheless discover how the attackers were able to access your information system environment and how they progressed in there. These holes or deficient security implementations that enabled the attack must be patched immediately to prevent a similar attack from occurring again. The incident log described in section 2.3.1 that has been completed as the investigation and recovery progresses should be used to help with the investigation.

Next, the detection ability of your organisation related to the attack should be surveyed. Try to find answers to the questions below together with your experts or service providers. Based on the answers, the management should review the organisation's detection and reaction plans and processes and aim to develop them to increase their effectiveness.

- Are our controls related to detecting attacks sufficient?
- Did the attacker's actions raise any alarms? What kind of alarms?
- Was the information about alarms transmitted to the right people?
- How did people react to these alarms, if they did react to them?

The effectiveness of the recovery process must also be assessed based on the following questions:

- Were the responsibilities of the crisis management team assigned to the right people? How did these persons carry out their duties?
- How successful was the IT personnel in the recovery? Was the operation of the services restored quickly enough, and were the resources sufficient?
- Was the crisis management team able to communicate the right things to the right people at the right time?
- Does the documentation include all important events related to the incident and are the timestamps correct?
- Was the technical investigation of the incident sufficient?
- Did the company's management act comprehensively enough in the situation or while preparing for it?

Even though a ransomware attack is always a serious incident, such attacks can also be prevented and managed. This will not be possible without appropriate preparation or continuous work to ensure cyber security, however.

4 Preparing for the threat

Attack methods are developing constantly, which means that the work on preparing for attacks must be continuous and based on systematic activity and layered defence. The management of the organisation must allocate sufficient resources in case of ransomware attacks, so that the safety of the data network and service environment used by the organisation can be ensured. The sufficiency of resources and the effectiveness of the preventive measures in practice must also be measured to enable development.

Cyber security must focus on defensive depth and preparedness on different control levels. If one layer of defence fails, the other layers offer additional protection. Ransomware prevention can be divided into five separate layers, which improve protection considerably when combined. Figure 3 also indicates the importance of each layer in the whole preparation process in percentages. It is important to understand that appropriate cyber preparation is only successful in this kind of format, and that a single protective layer alone is often not sufficient.[6]

Figure 3: Preparing for threats and the importance of the different aspects of the preparatory process

4.1 Be aware

Every organisation is a potential target of a ransomware attack, either directly or as a part of a critical delivery chain. Criminals can also adapt their attacks and ransom demands on a target organisation-specific basis quite accurately in order to maximise their profit. Therefore, you should take the threat seriously.

Identify the services that are critical to your operation and estimate what would happen if one or all of these services was not available. After this, together with your ICT experts, map the IT assets used by your organisation that you need to in order to provide or implement the services central to your activities. These include workstations, servers, mobile devices, databases and user registers, among others. Keep in mind that you cannot protect something if you do not know it exists. This will also help your organisation with drawing up deviation management and recovery plans.[7]

[6] NIST Cybersecurity framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[7] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Next, create a context for the different layers of preparation by assessing the potential risk caused specifically by a ransomware attack. In the assessment, take account of the existing administrative and technical controls as well as the awareness of the personnel. Do not forget to process the residual risks and mirror them against the ability and willingness of your organisation to take risks. Discuss the threats and risks related to ransomware in the meetings of the executive group and the board of directors.

Also confirm the duties and responsibilities of service providers with agreements and requirements.

Follow the status of the preparatory measures you use and the risk level of your organisation with the indicators created for the purpose.

It is also important for the management of the organisation to keep in mind that a part of the budget sufficient for implementing the necessary preparatory measures should be allocated to cyber security. You can use a thought model, in which you estimate how large of a financial loss the security investment that has been made will prevent in the future. In other words, how much would a potential successful attack cost you in euros? This will also allow you to assess the willingness of your organisation to take risks.

4.2 Protect

Protective measures must be taken with care, because attack attempts originating from the internet occur every day. Some of these attempts are nothing more serious than mapping the online services of your organisation, but they may also include very hostile and aggressive attack attempts. With effective protection, your organisation will be able to combat most of these attempted attacks, but this requires investing in the maintenance and development of cyber security.

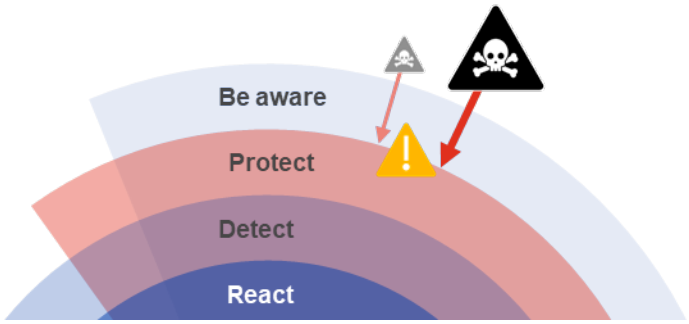

Figure 4: Some attacks are stopped by protective measures

At this stage, your organisation should have a comprehensive list of all available IT assets (see section 3.1) so that measures can be taken to protect them. The protective measures should primarily focus on the services or systems that have been identified as critical to your operation.

The protection level is significantly affected by the administrative and technical maturity of your organisation. The higher the cyber capability your organisation has, the better it is also protected against ransomware attacks.

The following questions will help with determining the technical maturity level of your organisation. You can also supplement the maturity level assessment by using the Kybermittari (Cybermeter) tool published by the National Cyber Security Centre Finland (https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter).

Review the situation presented in the questions below carefully with your experts:[8] [9]

- Have we ensured that we have a functional communication channel that we can use in case of a cyber attack?
- Do we install information security or software updates regularly and sufficiently often? How do we ensure that we only use secure software versions?
- Do we use two-factor authentication in all of our services that are open to the internet?
- Have our systems and services undergone information security testing, and have corrective measures been taken based on the observations gained from it?
- Is the network of our organisation protected appropriately with firewalls and are the terminal devices protected with detection and attack prevention software? Do we also use antivirus software and workstation-specific firewalls?
- Do the employees only have the access rights and authorisations for the different systems and services that they need in their daily work?
- Do we only use our workstations with user-level rights? Administrator rights broaden the attacker's options of progressing in the system considerably.
- Is the data network of our organisation divided into different sections depending on their purpose of use? Effective segmentation slows down the spread of the attack into the different parts of the network and therefore also the systems.
- Do we keep network-, system- and service-specific event logs, and how long are they stored? Do we implement log management in accordance with the regulations?

4.3 Detect

Even the best protection possible can sometimes fail. For this reason, the services, systems and network of your organisation should be monitored constantly in order to detect potential attacks. Effective detection enables fast reaction, if the protections of section 4.2 fail. The faster an attack is detected, the easier it is to reduce and prevent the damage it causes.

The ICT assets of your organisation can be monitored with different kinds of sensors and information security software. You can also get an information security monitoring service, for instance, to support the monitoring of your organisation that is responsible for monitoring the whole network of the organisation and often offers round-the-clock service during public holidays or the holiday season.

[8] Centre for Cyber security Belgium: Incident management guide https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

[9] CIS, 7 Steps to Help Prevent & Limit the Impact of Ransomware, 2022, https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

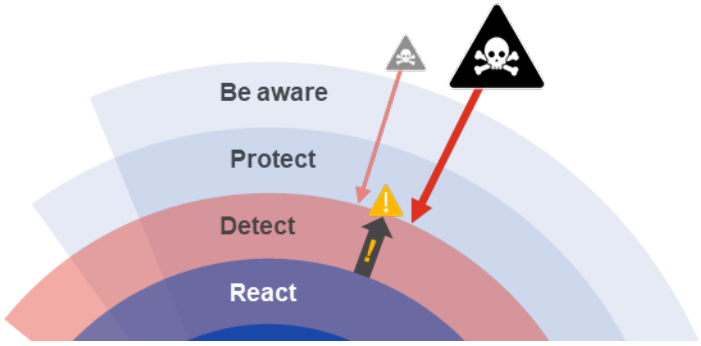

Figure 5: Some attacks may penetrate a protective layer. In that case, effective detection is needed so that your organisation can react to the attack.

The awareness of the personnel of your organisation about the threat of an attack is also important. Make sure that your organisation regularly arranges training that presents threats and the mechanisms through which they are realised (see section 1.2), teaches correct operating models and good cyber hygiene, and reviews the measures that need to be taken in case of an attack. Every employee of the organisation should know how to act safely in their daily work, thereby reducing the likelihood of a potential attack.

The organisation's detection capabilities can also be developed and their operation secured with different kinds of technical assessments and testing. One of the best ways to implement this is testing, in which the selected information security experts "attack" different parts of the data network, systems or services, while the organisation's own representatives and those of the service partners try to detect the different stages of attack. The sensitivity of the detection capability is increased if the attack cannot be detected, which improves the effectiveness of technical controls or the level of skill of the information security personnel.

4.4 React

In addition to effective detection, the reaction to threats must also be appropriate. An observation by an information security control centre or detection and reaction software is of hardly any use, if your organisation cannot take the necessary measures. Your reaction must also always be in proportion to the severity of the threat detected to prevent disturbing the business unnecessarily or downplaying a critical threat.

Make sure that plans are developed for your organisation on how to manage information security deviations and that ransomware is included as one of the scenarios. Also ensure that these plans are available as "offline" versions, such as in paper format. This means that they can be accessed even if the ransomware had encrypted all of your digital files.

Ensure the responsibility of service providers to react to threats through agreements and requirements, because some malware can also spread through third parties.

Agree on support measures in technical incidents with your service providers, such as technical investigation and damage mitigation measures. Include these as a part of the contingency plans.

You should also find out if your organisation needs a cyber insurance policy, and if you decide to get one, include its potential service elements as a part of the recovery plans. Do not forget to make sure that the cyber insurance remains a carefully kept secret! Publishing the information makes the organisation a potential target for an attack.

Ensure that your plans are reviewed regularly through exercises and that they are developed based on the data from the exercise, feedback and technical metrics. All parties of the plans should also understand their own role and know how to act accordingly in case of an attack.

4.5 Recover

Sometimes a ransomware attack is successful despite the precautions. This may be due to a variety of reasons, such as one of the preventive layers being incomplete, a lack of technical controls or a so-called zero-day vulnerability exploit (a software vulnerability without a fix available).

Recovery from an extensive ransomware attack is generally possible, if the organisation targeted by the attack has up-to-date and sufficiently comprehensive backups available. In some cases the backups may also have become contaminated, in which case safe copies are needed.

To ensure an efficient recovery, attention should be paid to the technical architecture and capabilities in the preparations. These include:

- A safe storage environment that ensures the integrity and confidentiality of the stored information.
- Log management intended to enable monitoring up-to-date and appropriate backups.
- If your organisation uses e.g. virtual servers, make sure that they are also included in the scope of backups.
- Testing the restoration of backups and ensuring their functionality.
- An isolated backup environment that prevents the backups from being manipulated or destroyed.

In section 4.1 (Be aware), organisations should identify the systems and services central to their operations. Once they have been identified, service- and system-specific recovery plans should be made for them. The goal of recovery planning is to maintain the necessary documentation, operating model and capabilities that make it possible to restore systems or services safely and effectively. These recovery plans should be stored so that they are available even if the file systems are not. For example, paper copies of the plans can be made.

Other factors to be taken into account in recovery and the related planning include:

- In which order should the systems be restored? A wrong restoration order may cause problems or slow down the overall recovery process of all critical services.
- Have the recovery processes and their instructions been taken into account with regard to the systems or services maintained by service providers? Has there been training on recovery?
- How can we verify that the restored systems and services are safe? If versions of backup copies, such as safe copies, are not up to date, this may result in unsecure versions or configurations of software ending up in production.

5 Sources and additional instructions

Instructions for the management

1. **National Cyber Security Centre Finland.** Selviytymisopas kiristyshaittaohjelmia vastaan. [Online, in Finnish] 2016. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

2. **National Cyber Security Centre Finland.** Pienyritysten kyberturvallisuusopas. [Online, in Finnish] 2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

3. **Suomi.fi.** Data breach: Notify the authorities. [Online] 2022. https://www.suomi.fi/guides/data-breach/acute-measures/notify-the-authorities

4. **Forbes.** Ransomware 2.0: How malware has evolved and where it's heading. [Online] 2021. https://www.forbes.com/sites/forbestechcouncil/2021/05/20/ransomware-20-how-malware-has-evolved-and-where-its-heading/

5. **NIST.** Getting started with Cybersecurity Risk Management | Ransomware. [Online] 2022. https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf

6. **NIST.** Cybersecurity Framework. [Online] 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7. **NIST**. Ransomware Risk Management: A Cybersecurity Framework Profile. [Online] 2022. https://csrc.nist.gov/publications/detail/nistir/8374/final

8. **GDPR.EU.** What are the GDPR fines? [Online] 2022. https://gdpr.eu/fines/

9. **Australian Cyber Security Centre.** Ransomware emergency response: one-page guide. [Online] 2022 https://www.cyber.gov.au/sites/default/files/2021-10/ACSC-ransomware-emergency-response-one-page-guide.pdf

10. **Ransomware.org.** Everything you need to know about ransomware. [Online] 2022. https://ransomware.org/

Instructions for ICT experts

11. **NIST.** Recovering from Ransomware and Other Destructive Events. 2022**.** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf

12. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

13. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

14. **Europol.** No more ransom. [Online] 2021. https://www.nomoreransom.org/en/index.html

15. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

16. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022. https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

17. **CIS.** 7 steps to help prevent & limit the impact of ransomware. [Online] 2022. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

18. **CISA.** Cyber security evaluation tool with ransomware readiness assessment module. [Online] 2022. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

19. **Europol.** No more ransom. [Online] 2021 https://www.nomoreransom.org/en/index.html

20. **NIST.** Ransomware protection and response. [Online] 2022. https://csrc.nist.gov/projects/ransomware-protection-and-response

21. **Microsoft.** Ransomware and extortion, a collection of resources. [Online] 2022 https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

22. **Sonicwall.** 2022 Sonicwall cyber threat report. [Online] 2022. https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

23. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

24. **NCSC-UK.** Mitigating malware and ransomware attacks. [Online] 2021. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

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 978-952-311-802-7
ISSN 2669-8757

Finnish Transport and Communications Agency