Instructions for NIS2 incident notifications

Contents

1 Introduction

The purpose of this document is to provide organisations with examples and advice on submitting incident notifications under the Cyber Security Act and, in the case of public administration, the Act on Information Management in Public Administration ("Information Management Act"), as well as on filling in the relevant notification forms.

The names, addresses, and other personal data presented in this document are fictional, and the situations described in them are not intended to be used as such by any entities subject to the NIS2 Directive. The examples presented in the images and texts of this document are demonstrative scenarios that could be included in incident notifications pertaining to the Cyber Security Act and the Information Management Act.

In accordance with Article 23 of the NIS2 Directive, the organisations covered by the Directive must notify the competent supervisory authority of any significant incidents that have occurred in the services they provide. The notification obligation is three-tiered and consists of a first-time notification, a follow-up notification, and a final report. In addition, in long-term incidents or at the request of the authority, the organisation must submit an interim report on the incident.

The provisions on the obligation to notify significant incidents to the supervisory authority and the content of the notification are laid down in sections 11–13 of the Cyber Security Act. In addition, section 15 lays down the provisions on voluntary notifications. In the case of public administration organisations, the provisions on the obligation to notify and its contents are laid down in section 18d of the Information Management Act. In addition, section 18f of the Information Management Act lays down the provisions on voluntary notifications.

According to section 11, subsection 2 of the Cyber Security Act, a significant incident means an incident that has caused or may cause serious operational disruptions to a service or significant financial losses to the entity concerned, as well an incident that has or may have affected other natural or legal persons by causing considerable material or non-material damage. In the case of Finnish authorities, the definition of a significant incident is presented in section 2, subsection 24 of the Information Management Act. In addition, certain organisations are subject to Commission Implementing Regulation (EU) 2024/2690, which contains additional provisions regarding, for example, the definition of a significant incident.

The first-time notification must be submitted within 24 hours of the detection of the significant incident, and the follow-up notification within 72 hours of the detection of the significant incident. An interim report must be submitted at the request of the supervisory authority or, in the case of a long-term incident, no later than one month after the submission of the follow-up notification. The final report on the incident must be submitted within one month of the submission of the follow-up notification or, in the case of a long-term incident, within one month of the end of the processing of the incident. Voluntary notifications are meant for non-significant incidents and cyber threats as well as near misses. No separate follow-up notifications or final reports are submitted for voluntary notifications.

These instructions only apply to notifications submitted under the Cybersecurity Act. Other regulatory provisions may also require certain entities to submit other reports

about incidents. These instructions are not legally binding, and in any potentially unclear situations, legislation will always take precedence over what is stated in these instructions.

2 NIS2 Notification Application

In this section, we will review five different types of notifications. The first four notification types are described in chronological order, while the voluntary notification is presented as a separate entity at the end.

Please note that the recurring fields in the forms, such as contact information, possible reports of offences, or reports to other authorities (ODPO) and CSIRT supplementary forms, are only described once in connection with the first-time notification. These records are repeated several times in the forms, so you can return to the instructions for these fields, which are presented in section 2.1, whenever necessary.

2.1 First-time notification

The first-time notification of a significant incident is started by specifying the organisation's sector under the Industry field, as shown in Figure 1.

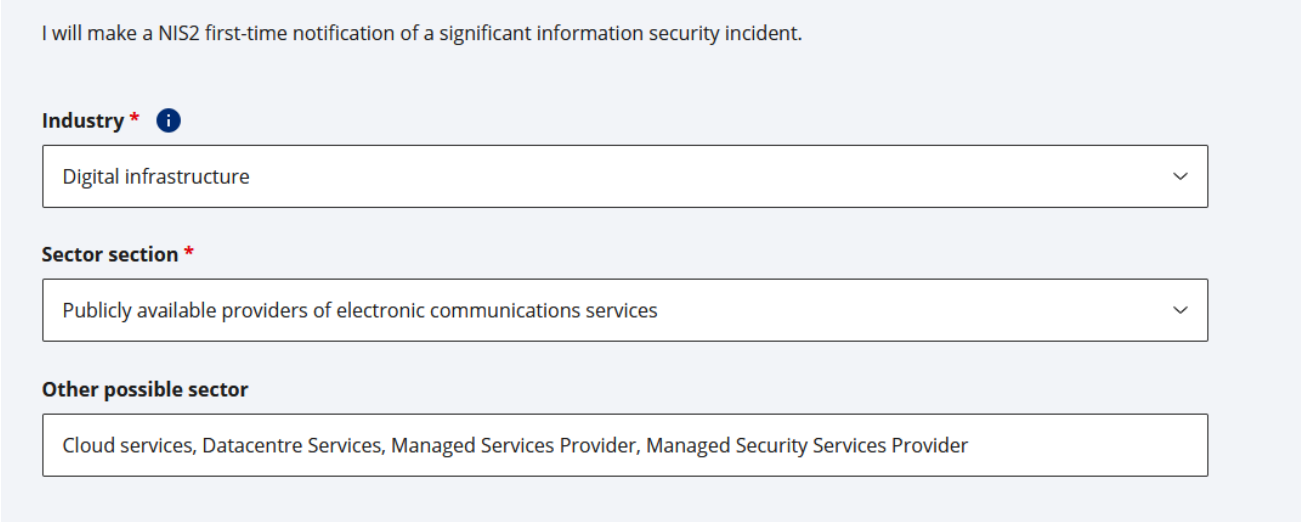

Figure 1 Industry information

When selecting your organisation's sector, the main sector subject to NIS2 regulation is used. This selection can be made, for example, by comparing the turnover of the organisation's sectors and selecting the largest.

You can use the "Other possible sector" field to add any other sectors your organisation is involved in beyond the "main sector" specified above. For example, an organisation that is mainly involved in the telecommunications sector can add "data centre services" to its other sectors if it offers these as a separate service to its customers.

After you have filled in your organisation's sector-related information, you can specify the general details of the incident, as shown in Figure 2.

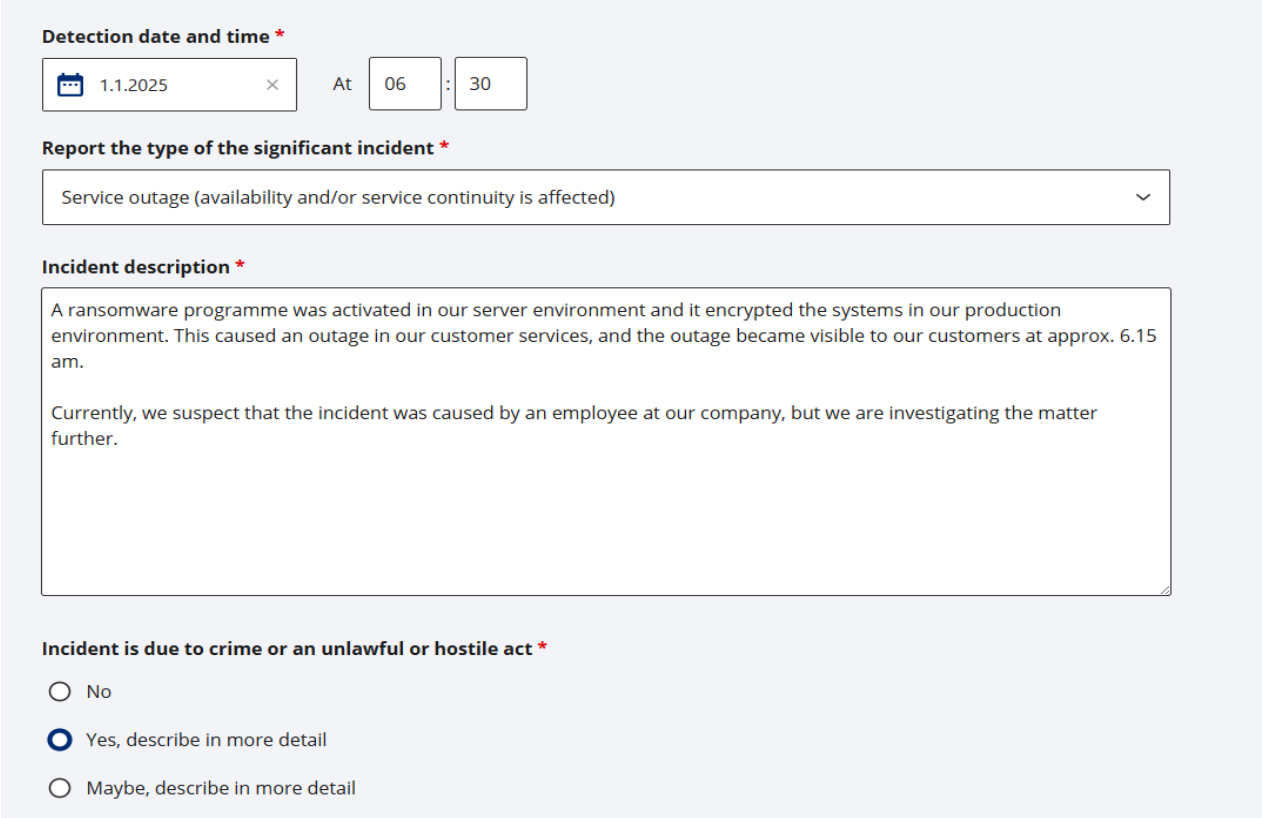

Figure 2 General information

In the "Incident description" field, enter a general description of the incident with the information available at the time of the notification, an assessment of the incident's possible impacts, and a possible description of the chain of events. When submitting the first-time notification, it is also possible that the aforementioned information has not yet been identified, in which case you can fill in the description field according to the information available to you at the time of notification.

You can also use the aforementioned field to describe the extent of the impact on your organisation's activities. In this reference case, the incident has resulted in the total encryption of the organisation's server environment – however, it has seemingly had no effect on e.g. the service's backup files.

Therefore, you can use this field to specify the specific scope of the incident, if you have determined that it has impacted only a single service in your organisation, for example. You can also describe the details of the impacted service, such as whether it is a business critical service and/or system, a system used to maintain your internal documentation, and so on.

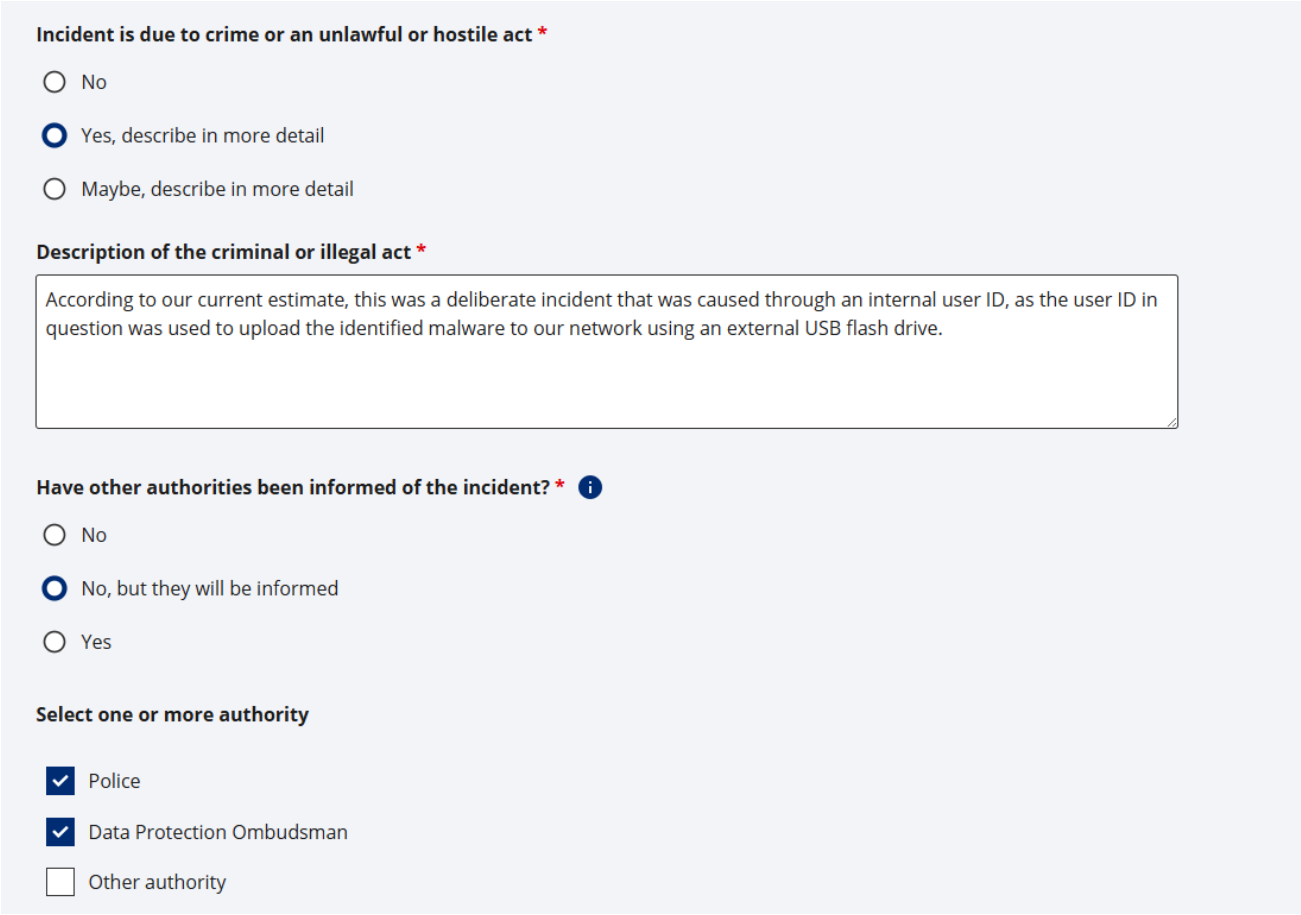

Figure 3 Notifications to other authorities

As the root cause of the reference case is a realised internal threat, the notification form offers the possibility of classifying the act as a possible crime or unlawful or hostile act.

However, due to the time limit for the first-time notification (24h), you may not be able to fill in the aforementioned fields at that time. In an incident where your organisation suspects a possible hostile act, you can also select the "Maybe" option and supplement your response at a later date, for example in your follow-up notification or final report, after your internal and/or external investigation has been able to specify the cause of the incident and whether it was performed intentionally by an internal actor.

In the field for describing the crime or unlawful act, you can outline the course of events with the information available to you at that time. However, due to the time limit for the first-time notification, there may still be some uncertainties about the progress of events. In this situation, you can provide a general description of how the incident occurred and give a more detailed account later in the notification process, for example in your follow-up notification and/or interim report.

In a case where personal data security has also been compromised, for example as a result of data theft, you will also be subject to the controller's reporting obligation (so-called GDPR notification) to the Office of the Data Protection Ombudsman (hereinafter the ODPO). The notification obligation applies to personal data breaches, i.e. "a breach

of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."
The Office of the Data Protection Ombudsman must be notified of the personal data breach without undue delay and, where possible, within 72 hours of the controller becoming aware of said breach.

When selecting the authorities to be contacted and/or notified, you can also select the "Other authority" option. The purpose of this section is to enable, for example, the flow of information between different authorities in the event of an incident that impacts an entity with two or more supervisory authorities, due to the wide scope of said entity's activities. In the reference case in Figure 2, the selected authorities include the police, due to the possibility of an unlawful act, and the Data Protection Ombudsman, due to a possible personal data breach.

Please note that, in this context, the "other authorities" option does not refer to the CSIRT unit (previously the CERT unit) of the National Cyber Security Centre Finland, which operates under the Finnish Transport and Communications Agency Traficom. A copy of the information you provide to the supervisory authority with this form will be forwarded to the CSIRT unit. The first-time notification form contains a separate submenu for information that is to be submitted to the CSIRT unit, and it is presented in more detail later in this document.

In the case of an incident whose impacts extend beyond Finland, you will be required to fill in the following fields. You can use the Impact Description field to, for example, list the EU Member States affected by the incident and describe the incident's impacts in the EU region. If are unsure whether an incident may have cross-border impacts when you are submitting your first-time notification, you can still describe its possible impacts and their probability in the field below.

Figure 4 Cross-border impacts and additional information

Next, in the "Submitted by" section, you will be asked to specify whether you are submitting your notification on behalf of an organisation or as a private individual (see Figure 5). When filling in the notifier's contact information, please remember that the competent supervisory authority may contact the provided email address to request additional information and further clarification on the (notified) matter/event

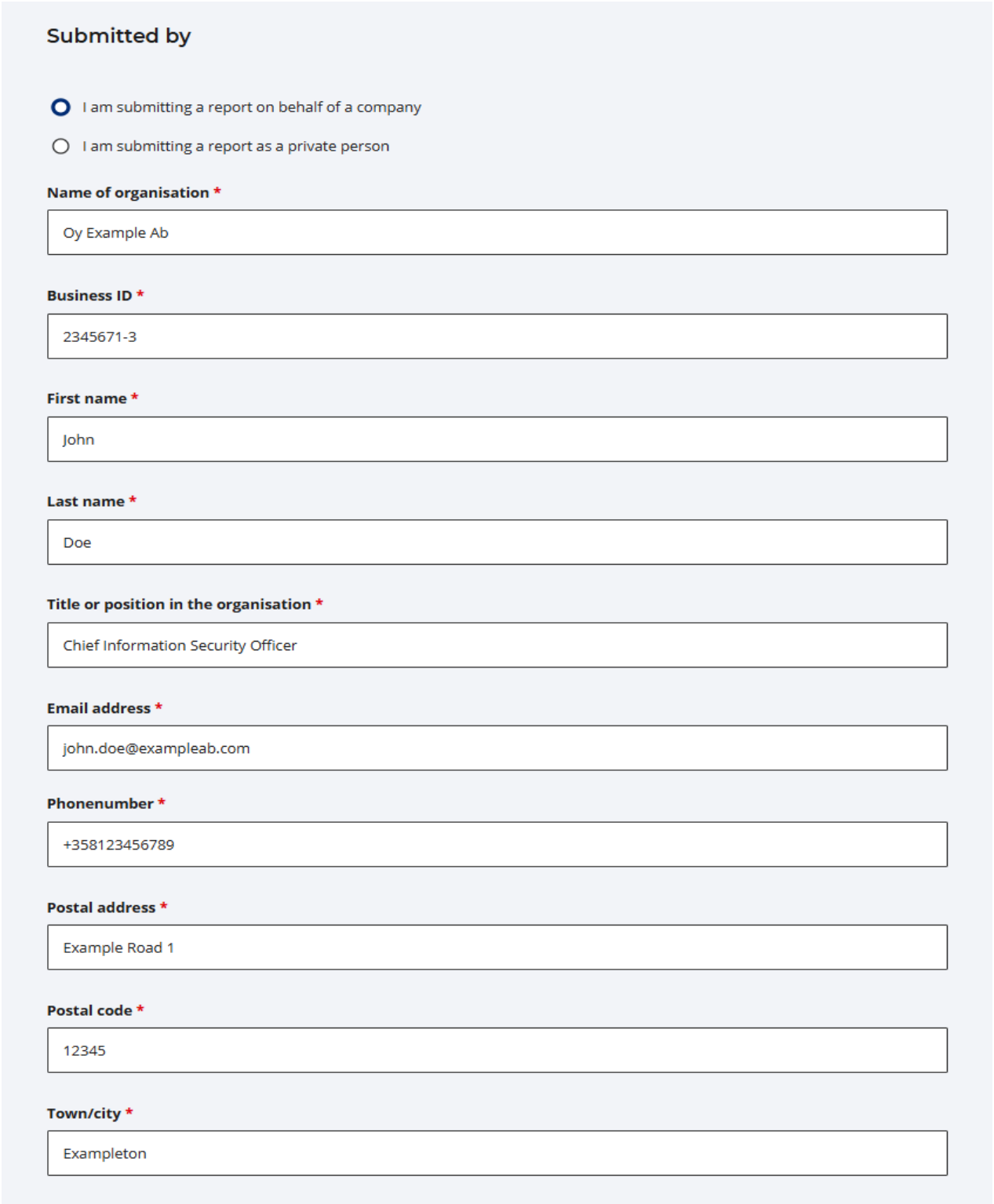

Figure 5 Notifier's contact information

The information above is then forwarded to the authority supervising your organisation – for example, if your organisation belongs to the Digital Infrastructure sector, it will be forwarded to the Finnish Transport and Communications Agency Traficom.

If you wish to inform the CSIRT unit of the National Cyber Security Centre Finland of the incident and/or share additional information with the CSIRT unit, you can open the additional CSIRT form by selecting the "I need support from the CSIRT unit of the National Cyber Security Centre Finland or I would like to voluntarily provide it with additional information" option below the "Town/city" field.

Please note that the information provided in this additional form will only be forwarded to the CSIRT unit, and it will not be forwarded to any supervisory authorities. Under section 25 of the Cyber Security Act, information voluntarily disclosed to a CSIRT unit for the purpose of carrying out tasks under this Act may not be used without the consent of the person who provided the information in criminal investigations against the person who provided the information, or in administrative or other decision-making concerning the person who provided the information.

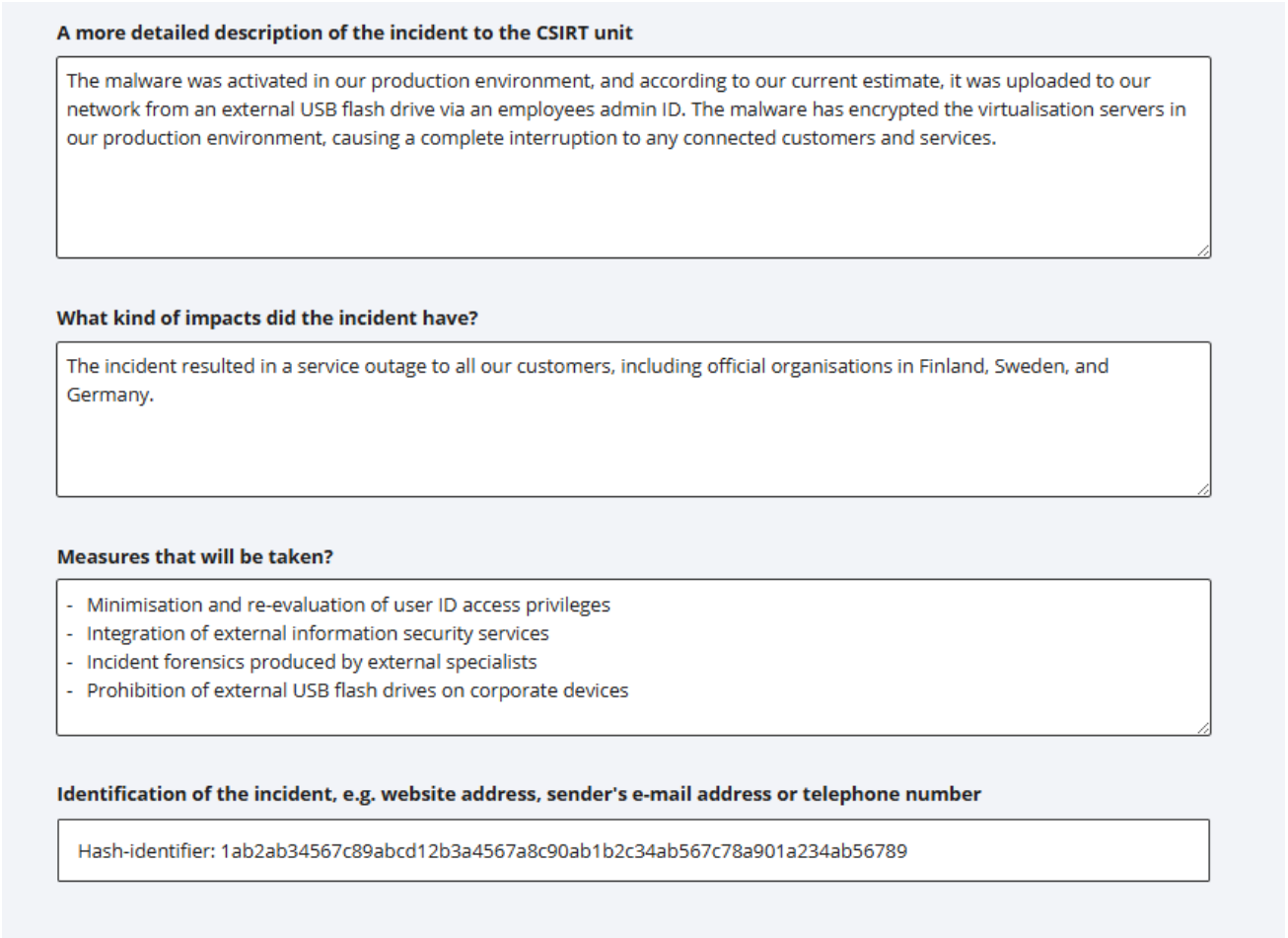

Figure 6 Additional CSIRT form

Figure 6 presents an example additional notification to the CSIRT unit with a general description of the incident's events, the first measures taken as a result, and the identification data related to the incident. In addition to the examples listed in the field's

description, you can provide e.g., a relevant hash and/or IoC (Indicator of Compromise) record or other technical identification data related to the incident. Please note that the IoC record provided to the CSIRT unit in connection with the first-time notification should also be provided to the supervisory authority in the follow-up notification, at the latest.

An IoC is a technical identifier or measurable technical observation that can be used to determine whether a cyberattack is possible, currently ongoing, or has already occurred.

The most common type of IoC is the log data generated by various systems for networks, devices, files, and user actions. In the reference case, the relevant IoC records could include, for example, the log data detailing the time and date when the ransom program was activated.

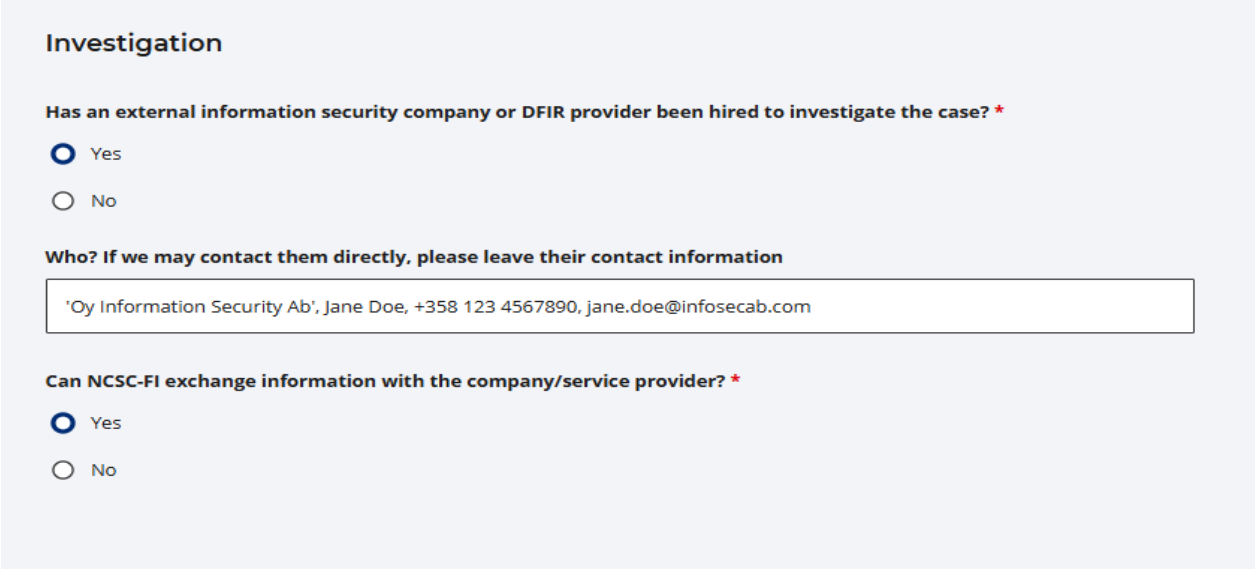

Figure 7 Additional MSSP/DFIR information

If your organisation has hired an external information security service provider (to investigate the incident and/or on more a permanent basis), you can specify their contact information in the fields shown in Figure 7 to allow the CSIRT unit to contact the service provider in matters related to the incident.

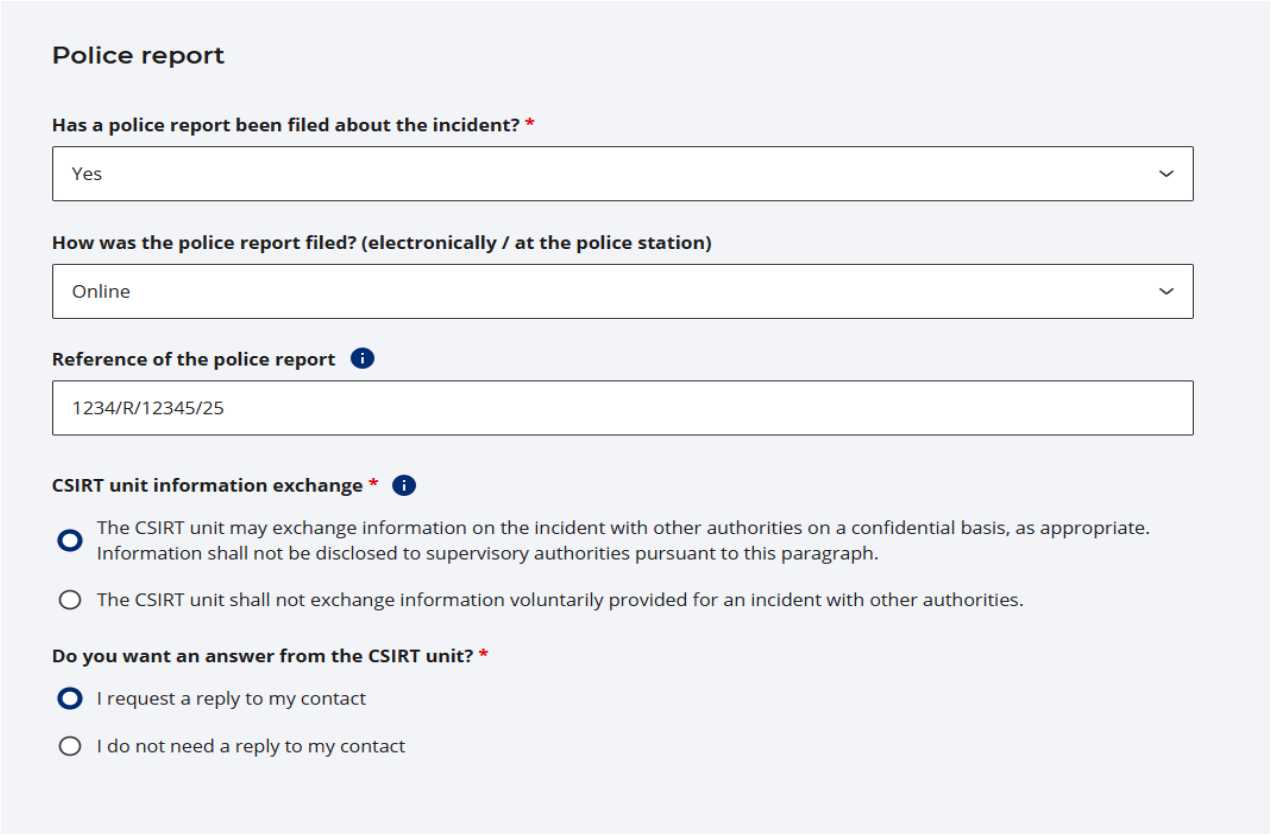

Figure 8 Additional CSIRT form, police report section

You can use the "Police report" section to provide the details of your police report if you have filed one before filling in the first-time notification. If necessary, you can also select the "Will be filed" option and add the relevant details in a subsequent report, for example in your follow-up notification.

At the bottom of Figure 8, you can also choose whether you want the CSIRT unit to communicate with you about the incident or whether you wish to give your consent to confidential exchanges of information between the CSIRT unit and other authorities. Please note that any information that is subject to section 25 of the Cyber Security Act will NOT be included in the aforementioned confidential exchanges of information with the supervisory authorities.

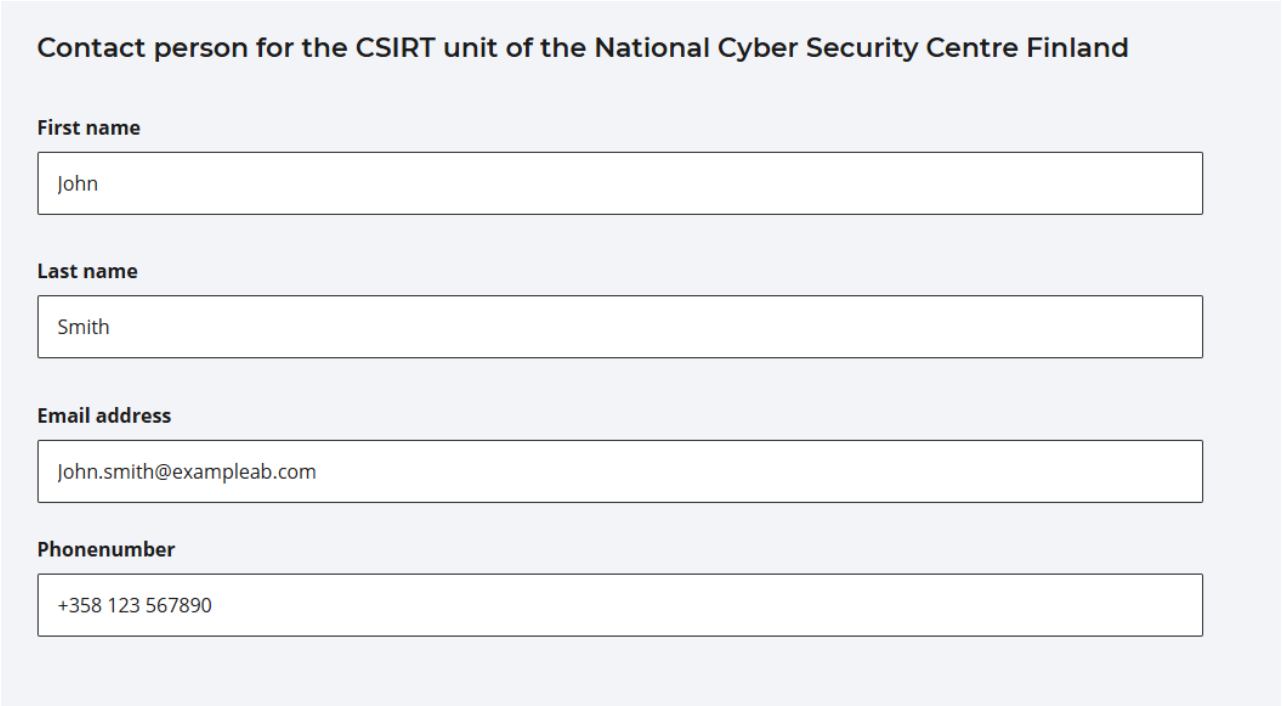

Figure 9 CSIRT contact information

At the end of the additional CSIRT form, you can specify who the CSIRT unit can contact during its investigation of the incident. For example, you can provide the contact information of your company's SOC or IT specialist(s).

Once you have filled in the required fields in the first-time notification, you can preview your notification by selecting the Continue button. While previewing your notification, make sure that you have carefully filled in the fields relevant to your incident.

After you have previewed your notification, complete the CAPTCHA verification at the bottom of the page and select the Submit button, after which the notification will be sent to the NIS2 supervisory authority of your sector. You can also download a PDF copy of your incident notification after you have submitted it.

Once your NIS2 incident notification has reached the supervisory authority, an acknowledgement of receipt will be sent automatically to your email address.

2.2 Follow-up notification

After the first-time notification, a follow-up notification must be submitted within 72 hours of detecting a significant incident. The primary purpose of the follow-up notification is to specify the information provided in the first-time notification, such as the root cause, more detailed impacts, and severity of the incident.

When filling in the follow-up notification, you will need the unique case number (e.g. '123456') provided in the acknowledgement of receipt of your first-time notification. The email containing the case number is sent to the person who submitted the notification, and it will have the subject line "Vastaanottokuittaus" (Acknowledgement of receipt).

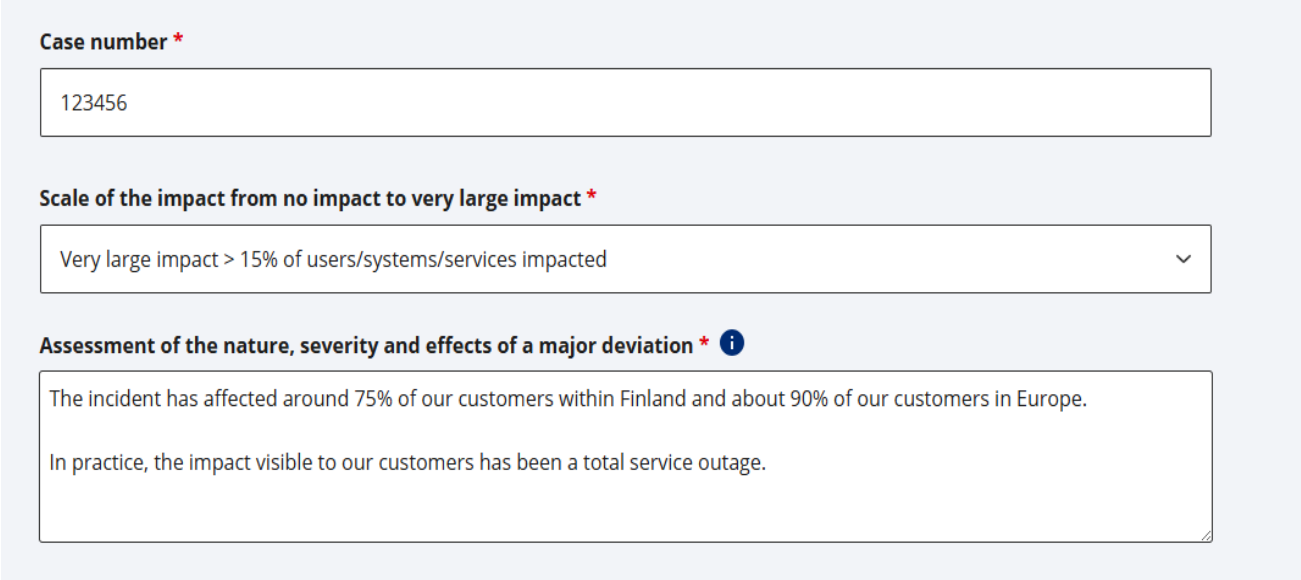

Figure 10 Follow-up notification, general information

When choosing the appropriate option for the scale of the impact, take note that this section is based on the so-called comprehensive impact principle. In other words, select the option that describes the overall impact of the incident, regardless of whether you experienced a total service outage or, for example, a delay in the operation of your service due to e.g. a DDoS attack.

As an example, a company could experience an incident where 10% of its services are subject to a full interruption and 20% of its services suffer from significant delays, but the service is still operational for a limited number of users. In this case, the company should select the "Very large impact" option, as the significant impacts exceed the option's 15% threshold. In general, if a service is significantly impacted by an incident, this impact must be taken into account when filling in this section.

When assessing the quality, severity, and impact of an incident, you can supplement the initial information you provided in your first-time notification, for example by specifying the scope of the impacts on a service-specific basis. You can also record preliminary estimates of impacted users and the functionality of services provided to them (Example: complete or partial interruption, all or some users).

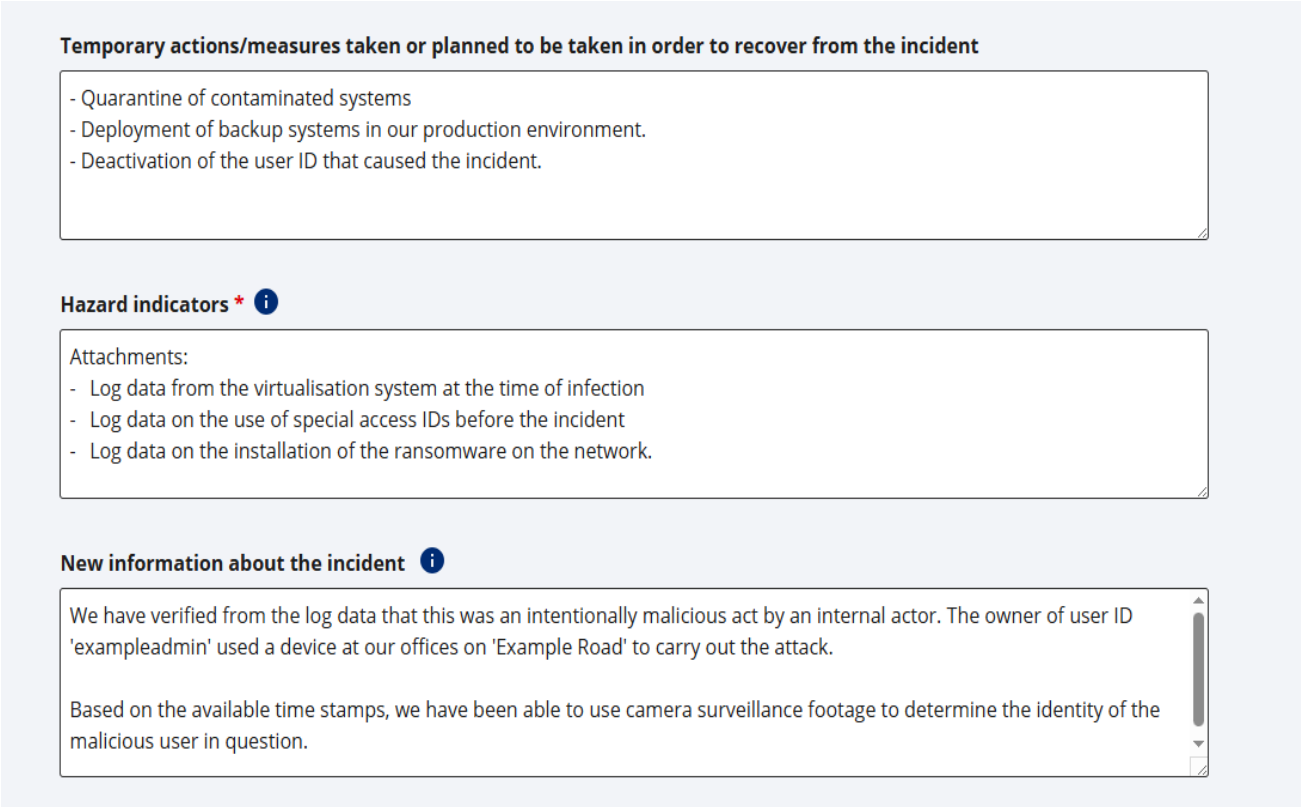

Figure 11 Actions, IoC records, and new information

The fields presented in Figure 11 above are used to describe e.g. temporary measures actions/measures taken to limit the impacts of the incident. Such actions can include, for example, the use of backup copies, the restriction of access rights, the use of backup systems, and other temporary emergency measures.

The technical identification data related to the information security incident (IoC, Indicators of Compromise) can be reported in the "Hazard indicators" field, if any IoC records are available.

When submitting your follow-up notification, you will likely have gained a better understanding of the incident's flow of events since you submitted your first-time notification. You can use the "New information about the incident" field to further specify the information you provided in your first-time notification, as well as share further information. For the reference case, this new information could include, for example, a confirmed attack vector or the verification of an internal cause.

You can also use this field to specify the measures you have taken to ensure that the current incident cannot happen again in the future. For example, in the reference case, one solution could be to block the use of external USB flash drives on the company's devices without separate approval.

2.3 Interim report

The purpose of the interim report is to provide interim information on the progress of the incident's investigation after the follow-up notification. You can use the interim report to describe how the processing of the incident has progressed in your organisation after the first-time and follow-up notification, and what the current status of the matter is. You should also report the actors involved in the processing of the incident (authorities, companies providing information security services, etc.)

The interim report can be used, for example, in long-term cases where the recovery from the incident takes significantly longer than the notification deadlines laid down in the Cyber Security Act. In the reference case, the company could opt to submit an interim report to the supervisory authority once it has a better understanding of the timeline required for recovering from the incident.

The interim report can also be used in cases where the investigative process reveals key issues that could have a significant impact on the incident's processing. For example, in the reference case, the company was able to rapidly minimise the incident's impact on its customers by using its backup systems to restore its services to full operation before the restoration of its production environment.

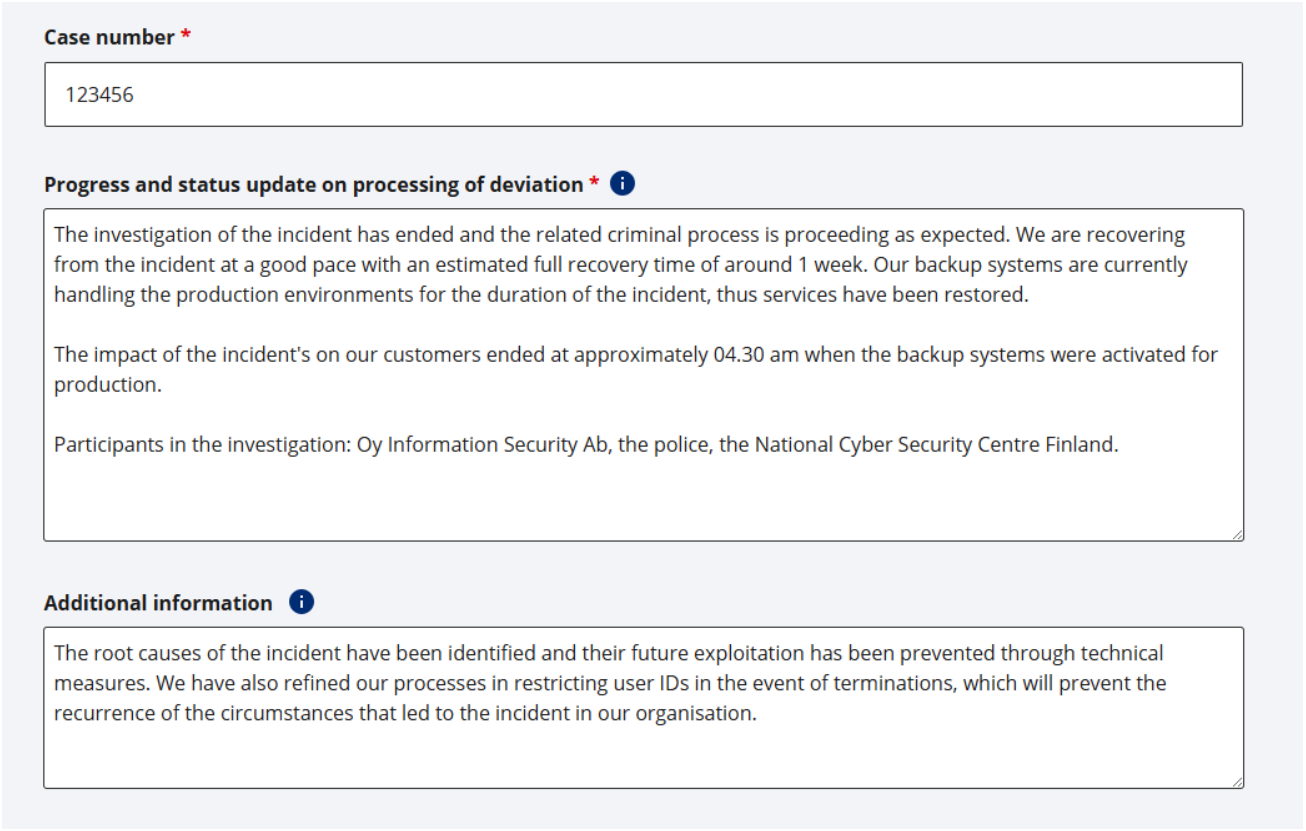

Figure 12 Interim report

2.4 Final report

The final report must be submitted within one (1) month of the submission of the follow-up notification or, in the case of a long-term incident, within one (1) month of the end of the incident's processing. This report serves as the last notification to the supervisory authority, and it includes every relevant detail about the incident.

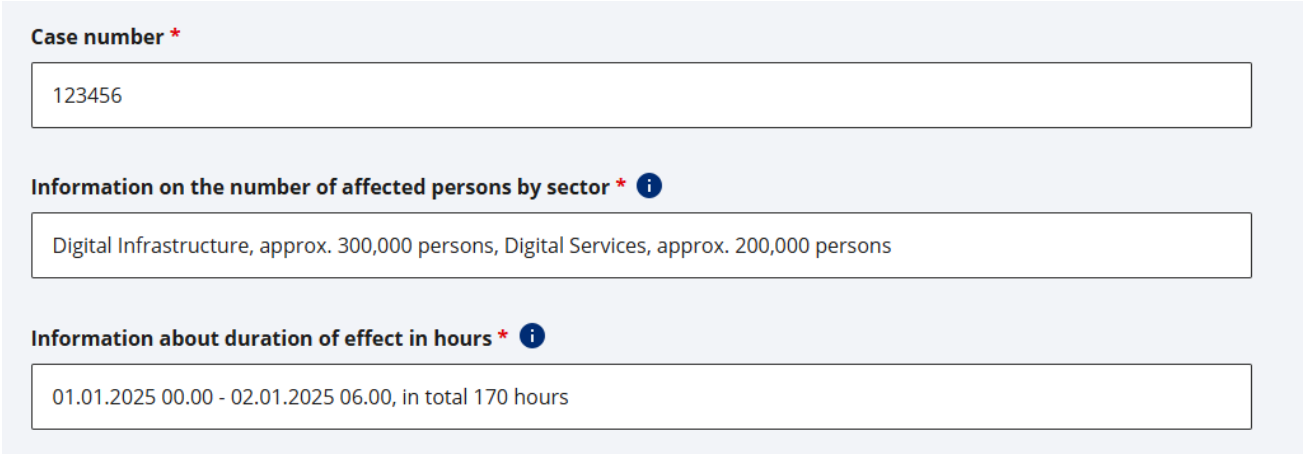

Figure 13 Duration & number of affected persons

In the second field of the final report, you will be asked to assess the number of affected persons by each sector supervised by the Cyber Security Act. However, it should be noted that it may not be possible to assess the entire impact of the incident, which is why you can provide a rough estimate according to existing data and the incident's severity and impact scale.

When assessing the duration of the impact in the third field, you can, for example, use the type of timeline presented in Figure 13 to describe the incident's duration.

The aforementioned field can also include separate time frames if, for example, the incident's impacts were spread across three different periods of time. Providing separate time frames is highly appropriate in, for example, incident notifications concerning DDoS attacks, which typically occur in varying bursts, depending on the volume of the DDoS attack.

The "Detailed information about the deviation and its effects" field can be filled in according to the instructions below and following the example given in Figure 14.

Describe in detail what has happened. Indicate any errors, disruptions, or unexpected events. Assess how significant or critical the deviation is from an operational perspective – you can use a scale (e.g. minor, moderate, serious) or describe it in your own words. Describe the impacts that the deviation has had or may have. Consider e.g. how the deviation has affected your activities, products, services, or security. If the deviation has had any financial or time-related impacts, remember to also mention these.

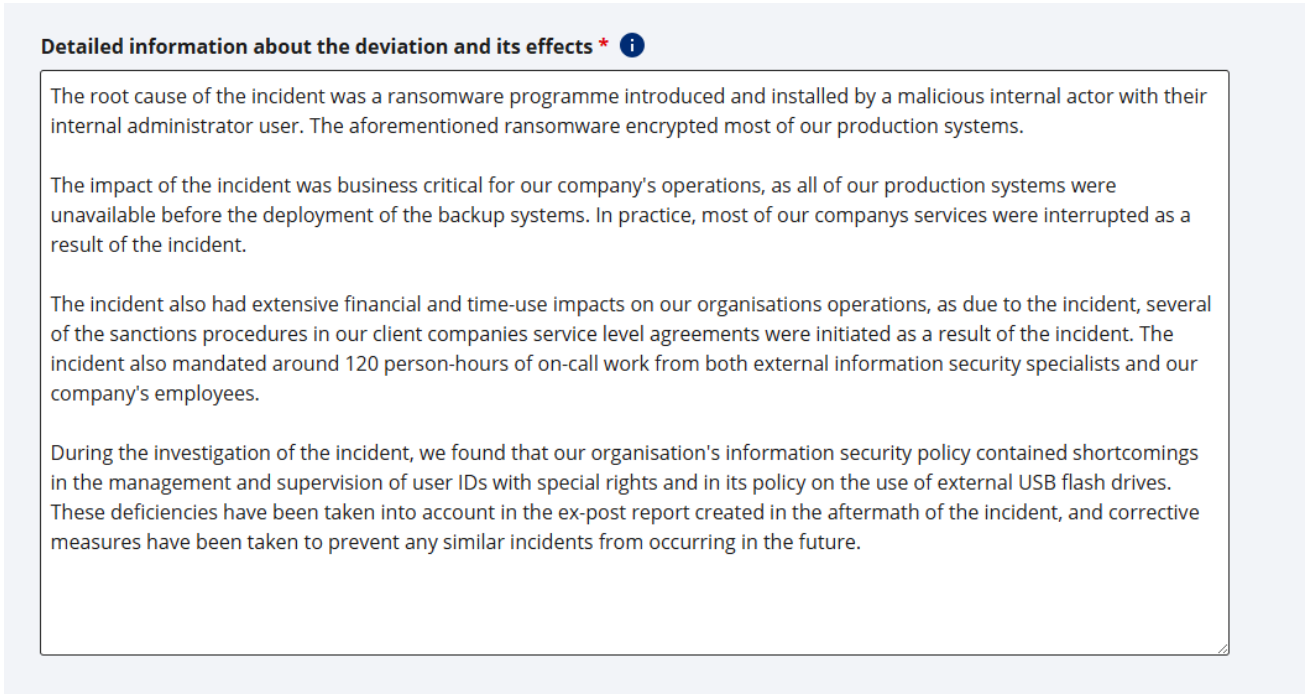

Figure 14 Detailed information about the deviation and its effects *

When filling in the category fields presented in Figure 15, select all the fields that describe the circumstances of the incident. In the reference case, the most suitable subcategory is "Deliberate internal actions", but due to the nature of the case, the "Deliberate physical damage/manipulation/theft" option has also been selected, as the purpose of the potential ransomware attack could have been to blackmail the organisation affected by the incident.

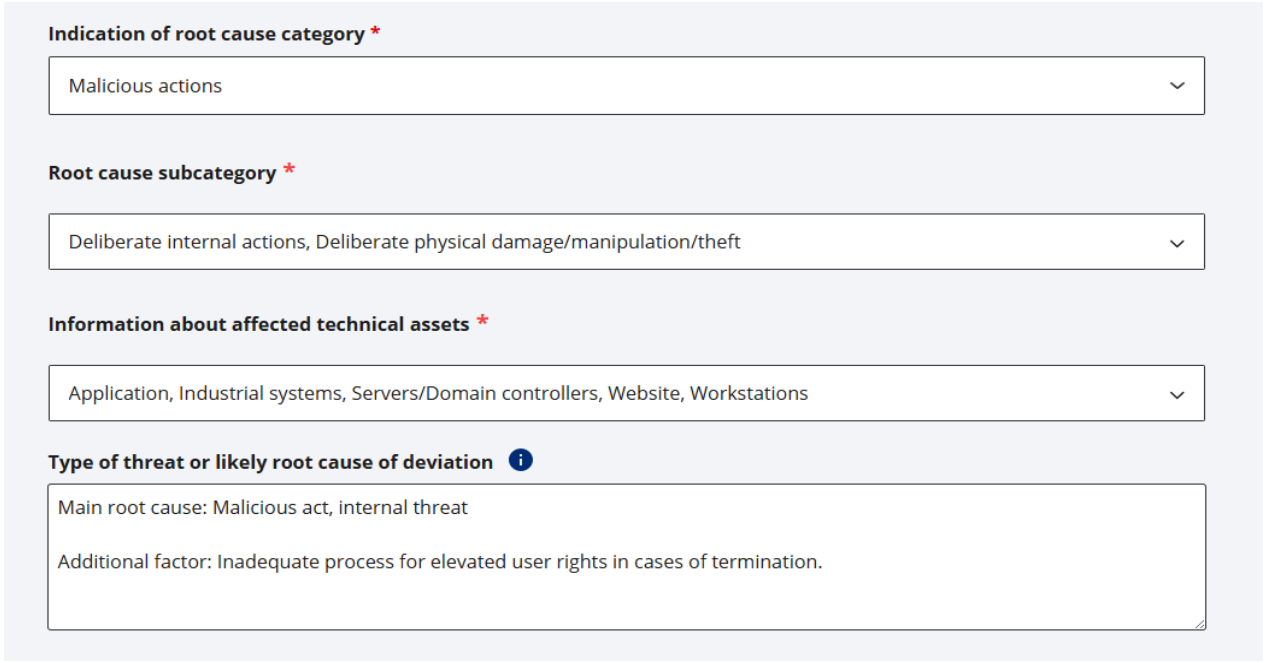

Figure 15 Categorisation of root causes and impacts of the deviation.

When determining the affected technical assets, select the systems that were significantly affected by the incident.

In the reference case, where the impact was extensive, the main impact was on the category that was selected first, i.e. the "Servers/Domain controllers" option.

Describe what is likely to have caused the incident. If the incident was caused by several threats or root causes, select the main reason and also mention the other possible factors. You can fill in the aforementioned field in, for example, the following way:

- *'Main cause: Human error, additional factor: Inadequate process.'*

If you have carried out a more extensive root cause analysis in connection with the investigation of the incident, your description can contain more detailed information on the root causes that led to the incident and the related processes.

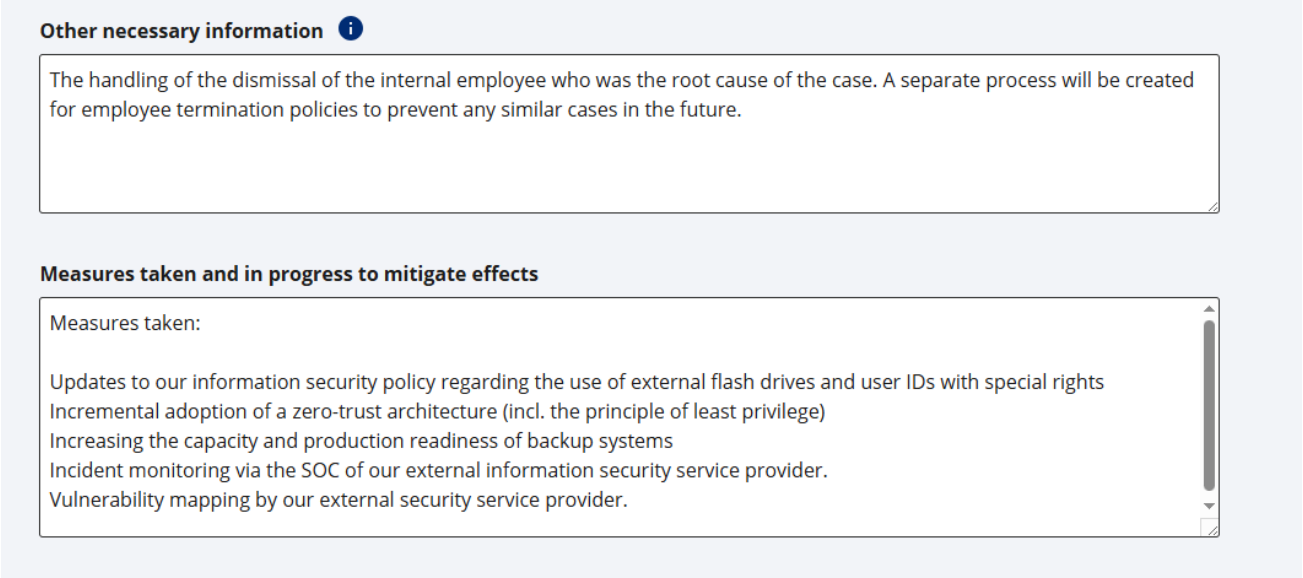

Figure 16 Other information and measures

You can use the "Other necessary information" field to specify any information that did not fit in the previous fields, but which is nevertheless important for processing the incident. This may include, for example, special situations, background information, or additional observations that could be used to clarify the extent of the incident or its causes.

You can use the "Measures taken and in progress to mitigate effects" field to describe the current measures taken by your company, as well as the future use of said measures. As shown in Figure 16, you can also use this field to indicate if you have continued to work with, for example, an external security service provider after the incident.

Attach any documents, reports, screenshots, or other files that support or supplement the description of the incident. Make sure that your attachments are in an appropriate file format (e.g. PDF, DOCX, XLSX, JPG, PNG). Name your files clearly and descriptively to make it easier to determine their contents. Remember to take note of any file size limitations.

If your file is large, consider reducing or splitting it into several pieces to ensure that it can be uploaded without any issues. You can also supplement your final report with internal reports, root cause analyses and other documents related to the incident.

2.5 Voluntary notification

In this section, you can voluntarily notify your supervisory authority of any disruptions that do not constitute a significant incident. This information is also forwarded to the CSIRT unit of the National Cyber Security Centre Finland, which operates under Traficom. However, if you only want to submit a notification to the CSIRT unit, you can submit a voluntary notification directly from the National Cyber Security Centre Finland's front page.

Anyone can submit voluntary notifications about incidents, threats and near misses. Voluntary notifications can be submitted by entities governed by the Cybersecurity Act, small enterprises operating in a sector vital to the function of society or private individuals, for example.

These notifications provide the National Cyber Security Centre Finland with useful information on phenomena and trends in Finland's cyber environment, so please do not hesitate to submit any voluntary notifications, no matter how minor.

The voluntary notification is divided into three separate categories.

2.5.1 Incident

The purpose of a voluntary incident notification is to notify the supervisory authority of a non-significant deviation.

In the Cyber Security Act, an incident is defined in the following way:

"An incident means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, communications networks and information systems;"

A non-significant incident refers to an incident that has a minor impact on a company's operations – for example, when an individual employee is tricked into disclosing their user ID and password in a phishing attack, but this ID does not have any special privileges.

2.5.2 Cyber threat

You can also notify the supervisory authority of any cyber threats that you detected as part of your company's activities, such as new software vulnerabilities that have emerged in an information security investigation.

In the Cyber Security Act, a cyber threat is defined in the following way:

"A cyber threat means a situation, event or activity that, if realised, could harm or disrupt communications networks or information systems, the users of such systems and other persons, or otherwise adversely affect these;"

A practical example of a cyber threat is a large-scale but unsuccessful phishing attack targeting the email addresses of a specific company.

2.5.3 Near miss

A near miss refers to a situation in which a potential event – one that could have endangered the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or services provided or accessible through communication networks and information systems – is prevented or fails to materialise due to some random occurrence.

Such situations include successful phishing attacks where an employee’s user ID is stolen but cannot be used due to, for example, the use of multi-factor authentication (2FA/MFA).

If you have further comments or developmental ideas for this document, please send them to "nis.valvonta.ktk@traficom.fi" via email.

Please include the following identifier in your email's header: [NISLO]