Danmarks Tekniske Universitet

02192 Computer Security Incident Response

Runbook
Ransomware spreading on DTU's Network

Group 4

Alexandros Pittas, s230265
Bryndis Rosa Sigurpalsdottir, s212423
Halla Margrét Jónsdóttir, s222991
Usama Yasin, s222644

May 19, 2023

Contents

1 Introduction

Author: Halla (s222991)

The purpose of this report is to provide a comprehensive cyber security runbook for handling and mitigating the impact of a ransomware attack on Denmark's Technical University's (DTU) network. Ransomware attacks pose a significant threat to organizations worldwide, and DTU compute is no exception to that. By understanding the nature of ransomware attacks and implementing effective prevention and response strategies, DTU can better safeguard its sensitive information, critical systems, and intellectual property.
This runbook provides detailed procedures that outlines the incident response procedures to be taken to handle ransomware attack incidents on the DTU network. The step-by-step guide will help the university's IT team to respond quickly and effectively to contain such an attack and minimize the damage.
In recent years, cyber threats have become more and more advanced, and one of the most prevalent and damaging types of attacks is ransomware. [11] This chapter provides an introduction to ransomware attacks, their characteristics, and the potential impact on DTU's network. In the case of such an attack, an infection of ransomware is spreading on DTU's network, and many computers and laptops at DTU Compute are affected. By understanding the nature of ransomware attacks, we can develop effective strategies to prevent, detect, and respond to such incidents.

1.1 What is a Ransomware Attack?

A form of malicious software known as ransomware is created to encrypt data and systems and hold them hostage until the company or organization that was the target of the assault pays the demanded ransom. Ransomware typically enters a network through a variety of techniques, including phishing emails, malicious attachments, and software exploits. Once launched, ransomware immediately encrypts files, blocking the victim's access to them. [9]

1.2 Characteristics of Ransomware Attacks

Understanding the features of ransomware attacks is crucial for the creation of effective preventive and response procedures. [1] Important ransomware attack characteristics include the following:

- **Encryption:** Strong encryption algorithms are used by ransomware to lock files and make them inaccessible to anybody without the attacker's decryption key. As this encryption is designed and created to be nearly unbreakable, it might be difficult, or even impossible, to recover the files without the key in appropriate times.

- **Ransom Demands:** Attackers demand for money, often in cryptocurrency to maintain their anonymity, in exchange for the decryption key that enables the victim to decrypt the encrypted files. If the ransom is not paid within a certain amount of time, the decryption key may be permanently lost or the sensitive data may be made public. The ransom sum varies and can be very high.

- **Time Pressure:** Attackers frequently set hard deadlines for payment, instilling a sense of urgency that compels victims to make snap judgments and submit to pressure to pay the ransom. Organizations are under pressure from time restrictions, which could badly affect their ability to make decisions and respond effectively when those skills are most needed.

- **Data Exfiltration:** Before encrypting files, an attacker may in some circumstances exfiltrate the sensitive data they got their hands on, using the threat of selling or publicly releasing the sensitive data as further pressure to get the victims to pay the ransom.

1.3 Impact of Ransomware Attacks

Attacks by ransomware can have grave consequences for an organization like DTU, impacting administrative, research, and educational operations. The following are some possible effects of ransomware attacks:

- **Data Loss:** Organizations risk losing access to their sensitive data that has been encrypted permanently if there are no dependable backups or successful decryptions. There may be extremely grave consequences from this loss, such as intellectual property loss, obstacles in ongoing research, and potential legal and regulatory issues.

- **Disruption in DTU's operation:** A critical operation can be hampered by encrypted files and systems caused by ransomware attacks, which can hinder research, teaching, administrative procedures, and student services. Productivity and operational effectiveness may be significantly impacted by the downtime needed for recovery.

- **Financial Loss:** Attacks by ransomware place a heavy financial impact on businesses. Incident response, forensic examinations, system recovery, legal services, potential ransom payments (which you should attempt to avoid at all costs), and countermeasures against future attacks can all incur costs.

- **Reputational Damage:** Ransomware attacks that are made publicly known or that are leaked can harm DTU's reputation, diminish stakeholder trust, and hinder cooperation with research partners and students. It can also lead to a sharp decline in the number of applicants for DTU admissions.

- **Regulatory and Legal Consequences:** DTU could have to comply with legal and regulatory requirements relating to data protection and privacy in the case of a data breach brought on by a ransomware attack. This includes potential repercussions from impacted parties or regulatory organizations, such as fines, penalties, and legal action.

2 Preparation

Author: Halla (s222991)

An effective cyber security strategy against ransomware attacks must include preparation. The key steps to preparing DTU for potential ransomware incidents are the topic of this chapter. DTU can drastically lower the risk and effects of a ransomware attack by taking proactive security measures, educating staff, and deploying appropriate technologies. [1]

2.1 Employee Training

For the purpose of avoiding and minimizing ransomware attacks, effective employee training is essential. Focusing on training and equipping staff to identify potential hazards and take proper action is crucial. Employee training can be divided into Security Awareness Training and Incident Response Training.

1. **Security Awareness Training:**
   Employees should receive regular security awareness training to help them understand ransomware threats and best practices. Training should include instruction on how to spot phishing emails, stay away from dubious websites, and maintain excellent password hygiene. Employees should be made aware of the possible repercussions of ransomware attacks as well as their part in avoiding and handling such situations.

2. **Incident Response Training:**
   The proper way to recognize and report security incidents to management should be taught to all employees. In the event of a suspected ransomware attack, they should be aware with the incident response processes and know who to call inside DTU. To improve their readiness and guarantee a coordinated reaction, training sessions and simulations might be held. The Incident Response Team should also be known by the employees or they should know how to get to them in case of a ransomware attack.

2.2 Software Updates

The prevention of ransomware attacks that exploit known vulnerabilities requires regular software updates. Keeping software systems up-to-date and lowering the danger of ex-

ploitation is critical when handling networks like DTU's compute network. The following is important to keep in mind when thinking of software updates:

1. **Patch Management Process:** In order to guarantee timely updates for all software, operating systems, and firmware, establish a thorough patch management approach. Regular vulnerability assessments, prioritizing fixes based on their criticality, testing patches in a controlled environment, and deployment methods should all be part of this process. To make sure all systems are covered by the patch management process, it's crucial to keep track of DTU's software and hardware inventories.

2. **Vulnerability Monitoring:** Install a mechanism for keeping track of software vulnerabilities and getting timely alerts when new ones are found that could affect the DTU network. This entails signing up for vendor alerts, security mailing lists, and employing vulnerability management tools to scan and evaluate the IT infrastructure's security posture.

2.3 Network Segmentation

A ransomware attack's effects can be reduced with the use of network segmentation. To safeguard critical systems and data, the following offers instructions for implementing network segmentation.

1. **Segmentation Design**

   By logically segmenting the network architecture, vital systems and sensitive data can be separated from less crucial components. Firewalls, VLANs, and access control lists can be used to manage traffic flow across segments to achieve this. The access control policies should be based on the least privilege concept to prevent attackers from moving laterally via the network.

2. **Network Access Controls** To prevent unauthorized access between network segments, impose strict access controls. Strong authentication measures must be put in place, user access rights must be reviewed frequently, and multi-factor authentication must be used for important systems. Create network segmentation based on user roles and the least-permissive principle as well.

2.4 Data Backups

Critical data must be regularly and securely backed up if you want to recover from a ransomware assault. Create a thorough backup strategy that incorporates routine backups of important data and systems. Backups frequency, storage location, redundancy, and encryption of backup data should all be taken into account. To assure availability and safeguard

against data loss, combine onsite and offsite backups. To ensure that backups are effective in restoring data, test and confirm their integrity on a regular basis. In a controlled setting, test the restoration procedure to find any flaws or errors. Keep records of your backup operations, and make sure that the backups are working properly.

2.5 Anti-Malware Software

In order to recognize and stop ransomware assaults, it is essential to implement powerful anti-malware software. [11] Here we will go further into deploying appropriate anti-malware software.

1. **Deployment and Configuration** After choosing the anti-malware program, carefully plan and carry out its deployment across the DTU network. Observe best practices when installing, configuring, and integrating new security infrastructure. Ensure that up-to-date anti-malware software is installed on all endpoints, including servers, workstations, and mobile devices. It is also utmost important that the anti-malware program is updated regularly so it is running at it's best form. The same as mentioned in chapter **2.2 Software Updates** applies for the anti-malware program.

2. **Regular Scanning and Updates** Set up a routine for doing periodic system scans to look for and remove all types of malware, including ransomware. To provide protection against latest and most recent threats, configure the software to automatically update virus definitions and software components. Keep an eye on the scanning results and take fast action if malware or other suspicious activity is found.

2.6 Monitoring System Logs

Monitoring system logs is crucial in detecting early signs of a ransomware attack. Set up systems and network devices to provide thorough logs that record important operations and activities. Use a security information and event management (SIEM) system or a specific log management solution to centralize log gathering. Ensure that the centralized logging infrastructure contains the logs from crucial systems, programs, firewalls, and intrusion detection systems.

Use log analysis methods like anomaly detection and log correlation to look for potential ransomware attack indicators. Create alerting systems that will inform security professionals of any malicious or suspicious activity, allowing for quick response and investigation. To promote quick ransomware incident discovery, analysis, and containment, integrate log monitoring with the incident response process. Create pre-established response protocols based on various log events and indicators of compromise to facilitate effective incident handling and mitigation.

2.7 Other Detection Techniques

In addition to anti-malware software and log monitoring, other detection techniques can enhance ransomware detection and prevention capabilities. Here, we'll examine several more strategies that can be used in addition to the above preparations:

1. **Intrusion Detection and Prevention Systems:**
   Network traffic should be monitored by intrusion detection and prevention systems (IDPS) for known ransomware signatures and anomalous activities. Configure the IDPS to send alerts and implement preventative measures to stop or minimize ransomware-related actions.

2. **Endpoint Detection and Response:**
   Advanced features offered by EDR systems significantly increase endpoint visibility across a organization's network. By obtaining and reviewing telemetry data from specific endpoints, these systems can gather information about suspicious activities and behaviors connected to ransomware attacks and identify and monitor them. Security experts are better able to foresee potential risks as a result of the improved visibility, and they can respond quickly to limit their effects.

3 Attack Confirmation

Author: Bryndís (s212423)

When reacting to a ransomware attack, the Ransomware attack Confirmation step is important. It validates the presence of the attack, identifies affected systems and data, and evaluates the level of damage and possible data loss. An organization risks further harm and data loss if sufficient validation is not obtained. The detection validation, threat identification, scope assessment, incident reporting, and documentation are all part of this step. This chapter is a key component of a ransomware runbook since it gives a disciplined strategy to confirming the attack and prioritizing recovery operations.

3.1 Ransomware Detection Validation

Validating a ransomware attack's first detection is a critical step in establishing its presence. It may be discovered using a variety of methods, including anti-malware software and security monitoring systems. However, it is critical to check the first detection in order to reduce false positives and guarantee that ransomware is truly present.

There are various frequent ransomware signs to be mindful of when verifying the detection. These include unusual file extensions, file name modifications, and ransom letters. For exam-

ple, a file called "Important.doc" may be renamed "Important.doc.locked." It's also important to keep a look out for strange network activity or interactions with known ransomware command-and-control services. Organizations may successfully respond to ransomware attacks, prevent data loss, and lessen the chance of future harm by carefully monitoring and testing ransomware detection.
Validation of ransomware comprises several crucial procedures [8, 5].

1. **Review Initial Detection** The initial part of ransomware detection validation is acquiring essential data linked to the detection, which is a vital step. This information comprises the date and time of discovery, the source of the technique or tool used to identify the ransomware attack, and any relevant log files. Collecting this information is critical for completing a thorough investigation of the ransomware attack, which gives critical information for the next measures to be taken.

2. **Malware analysis** Malware analysis include investigating ransomware to determine its kind, channel of infection, and possible impact on impacted systems. This data is critical for establishing an effective response strategy. The ransomware code, behavior, and network activities are all examined throughout the study. This aids in determining how the ransomware infiltrated the system. Some ransomware outbreaks, such as WannaCry and NotPetya, for example, use known weaknesses to propagate across networks.

   Identifying the type of ransomware is crucial since dealing with them takes various tactics. Some ransomware families encrypt data, while others utilize disk-level encryption to render the machine inoperable.

   Malware analysis can provide information into how the ransomware operates and the potential impact it may have on impacted systems. This understanding is critical in building an effective reaction strategy to reduce the attack's harm.

3. **Validate Detection Tools** It is critical to run further scans using anti-malware and security monitoring technologies in the last step of ransomware detection validation to guarantee the correctness of the initial detection. This stage validates the existence of the ransomware threat and allows the company to respond properly. Validating detection tools is also important in building effective response strategies that reduce possible harm and data loss caused by ransomware attacks. Organizations can design a plan to remove the ransomware from all systems and reduce the risk of future attacks by analyzing the severity of the attack and identifying holes in the organization's security posture. The detection technologies can also uncover vulnerabilities that may have been exploited during the attack, thus allowing enterprises to remediate them appropriately. Finally, verifying the detection tools is an important stage in ransomware

detection validation, providing companies with the knowledge they need to establish an effective action strategy and reduce the harm caused by ransomware attacks.

3.2 Threat Identification

Detecting threats is a vital step in controlling and limiting the effects of a ransomware attack. By actively recognizing the type of ransomware and its behavior, organizations may establish a thorough plan for containment and recovery.

To do so, companies must examine the data gathered during the ransomware detection validation phase. This entails carefully evaluating the first detection to establish the origin of the attack and any potential vulnerabilities exploited. Malware study reveals how the ransomware works and the potential ramifications for infected systems. Organizations may check the accuracy of the first detection and acquire critical information for establishing an effective response strategy by actively verifying the detection technologies.

Organizations may use this data to establish the type of ransomware and its behavior, including how it enters the network and how it spreads. This intelligence is essential in controlling the attack by isolating afflicted computers and preventing the ransomware from spreading to other systems. Furthermore, it assists enterprises in developing a sound recovery strategy by identifying the damaged data and recovering it from backups. For instance, if the ransomware is a file-encrypting variety, businesses should focus on rescuing data from backups while isolating damaged computers to prevent the malware from spreading further.

In conclusion, determining the type of ransomware and its behavior is crucial in building a successful response strategy for controlling the attack and recovering from its effects. Organizations may design a complete plan that lessens the effect of the assault and limits the risk of future attacks by utilising the information gathered throughout the ransomware detection validation process.

3.3 Scope Assessment

When a ransomware attack occurs, one of the first things a company must do is determine the extent of the damage. This procedure, known as scope assessment, is essential in formulating an effective response strategy for confining the attack and reducing its consequences.

Identifying the impacted systems and data, evaluating the amount of the damage, and prioritizing recovery efforts are all part of the scope assessment process. Organizations should use the information acquired throughout the ransomware detection validation and threat

identification procedures to correctly estimate the scale of the attack.

The organization should evaluate the initial detection during ransomware detection validation to establish the attack's beginning point and any potential vulnerabilities that were exploited. Furthermore, malware analysis can reveal further information about how the ransomware works and its possible impact on afflicted computers. Validating the detection technologies employed can validate the first detection's accuracy and give critical information for establishing an effective reaction strategy.

After determining the type of ransomware and its behavior during threat identification, an organization may utilize this information to assess the scale of the attack. Organizations, for example, can assess whether the ransomware is a file-encrypting variation, a disk-encrypting variant, or a data-erasing variant. This information is crucial in determining the scope of the damage and prioritizing recovery operations.

Organizations should identify the affected systems and data in order to estimate the breadth of the attack. This involves assessing whether systems have been hacked and the extent to which the data held on those systems has been harmed. Organizations should also evaluate whether the attackers have exfiltrated or stolen any data.

To develop an effective response strategy, enterprises must first assess the impact of the ransomware attack on their operations. This involves assessing any downtime, data loss, and financial damages. This information aids in prioritizing recovery operations and allocating resources to quickly restore impacted systems and data.

In brief, doing a scope assessment is a vital step in reacting to a ransomware attack. Using the information gathered during ransomware detection validation and threat identification, organizations can accurately assess the scope of the attack, identify affected systems and data, estimate the extent of the damage, and develop a comprehensive response plan that minimizes the impact of the attack and restores the affected systems and data as soon as possible [7].

3.4 Incident Reporting For DTU University In Lyngby

In the case of a ransomware attack, it is critical to notify all key stakeholders, including management, employees, and law enforcement authorities, as soon as possible and precisely. This chapter explains how to report a ransomware attack and what information you should give.

1. **Who Should You Report To:** As soon as the ransomware attack is noticed,

the event should be immediately reported to the DTU Incident Response Team. The Incident Response Team security team will then evaluate if the attack is substantial enough for the purpose of reporting to management, employees, the Danish Center for Cyber Security (CFCS), or law enforcement authorities.

2. **What Information to Disclose**

   The data collected throughout the ransomware detection validation process, threat identification, and scope assessment is crucial for appropriately reporting the incident. The following details should be communicated with the appropriate stakeholders:

   - The ransomware type and its behavior, including how it infiltrated the network and how it spreads.
   - The impacted systems and data, including the amount of the damage and any data that the attackers have exfiltrated or stolen.
   - The attack's projected impact on DTU operations, including any downtime and data loss,
   - The current state of the incident response strategy, as well as the resources required to restore impacted systems and data.
   - Any requests for ransom made by the attackers

3. **When Should You Report:** The ransomware attack should be disclosed to the Incident Response Team as soon as feasible. The Incident Response Team will next assess the seriousness of the incident and decide whether to notify management, employees, or law enforcement agencies. The attack and its impact on the College's activities should be communicated to management and workers as soon as possible. If the attack involves theft, the exfiltration of sensitive data, or any other criminal behavior, law authorities should be contacted.

Finally, disclosing a ransomware attack to appropriate stakeholders is crucial to properly reacting to the issue. DTU college may deliver accurate and thorough information to the right stakeholders by utilizing the information acquired in the ransomware detection validation, threat identification, and scope assessment. To guarantee compliance with legal and regulatory obligations, reporting should be done on time, and law enforcement authorities should be contacted if required [4].

3.5 Documentation

Documentation is an important aspect of the Ransomware Attack Confirmation process because it provides a full record of the impacted systems and data, the level of the damage,

the threat identification, and the scope assessment. This data will be used in future research, reporting, and decision-making.
Documentation should cover initial detection, malware analysis, and detection validation during ransomware detection validation. Document the ransomware kind and behavior in threat identification. Affected systems and data identification, as well as damage estimation, should be included in the scope assessment documents. Documentation of incident reporting should include who was notified, what information was supplied, and when the report was made.
Proper documentation aids in the identification of flaws in the posture and the development of efficient responses to prevent more attacks. Documentation should be kept securely [6].

4 Ransomware Situational Analysis

Author: Bryndís (s212423)

The Ransomware Situational Analysis, which is part of the validation process, is a vital stage in responding to a ransomware attack. It enables enterprises to analyze the impact of the attack on systems and data, as well as identify the attacker's activities and habits.
A organized strategy is required to conduct a successful Ransomware Situational Analysis. The first step is to go over the data collected in the Attack Confirmation chapter, which includes the results of ransomware detection validation, threat identification, scope assessment, incident reporting, and documentation. This data serves as a good foundation for doing the analysis.
In this chapter, we will go through how to do a full Ransomware Situational Analysis, which includes analyzing the attack's impact on systems and data, identifying the attacker's behaviors and behavior, and determining the danger to the company. We will also look at how to arrange the analysis properly so that all relevant information is recorded and used in the impact analysis in the Assessment chapter [4].

4.1 Analyzing the Attack's Impact:

A ransomware attack can do substantial harm to a business, thus a detailed Ransomware Situational Analysis is required. The analysis entails determining the impact of the attack on the organization's systems and data, which can assist drive response strategy decisions.
The company should evaluate the information acquired in the Attack Confirmation chapter before beginning the Ransomware Situational Analysis. Examining this data gives a good framework for understanding the attack's impact.

The effect of the attack is assessed by identifying which systems and data were impacted and

determining the degree of the harm. For example, if vital data has been encrypted and is no longer recoverable, the consequences are serious, and the company must assess its recovery options.

Another critical component of assessing the attack's impact is finding any sensitive data that the attacker may have acquired or exfiltrated. If sensitive data is compromised, the company must take precautions to reduce the risk of data theft and notify any impacted parties.
Overall, analyzing the consequences of the attack is a critical stage in reacting to a ransomware attack. It assists organizations in understanding the gravity of the problem, informing response strategy decisions, and assessing the risk to the company. The data acquired in this study will be utilized in the impact analysis in the Assessment chapter to evaluate the overall impact of the assault and the required reaction [6].
Initial Detection: Detail the initial detection methods that triggered the suspicion of a potential ransomware attack, such as an alert from anti-malware software or reports of unusual system behavior.

4.2 Analyzing the Attacker's Activities and Behavior:

This stage is critical in understanding how the attacker acquired network access, what systems and data they targeted, and how the attack was carried out.
Organizations should study the material acquired in the Attack Confirmation chapter including the documentation, to assess the attacker's activities and behavior. They should also examine network logs and system activities for any unusual behavior preceding the attack.
It is also critical to examine any communication sent by the attacker, such as ransom requests or communications made during the assault. This can provide important details about the attacker's motives and potential future attacks.
Organizations can acquire useful insights on how the attack happened and how to prevent such attacks by evaluating the attacker's activity and behavior.

4.3 Risk Assessment

Risk assessment is an important stage in reacting to a ransomware attack since it allows DTU to identify and prioritize the threats. This study entails identifying possible hazards and assessing their possibility and effect.

To begin, the company must study the results of the Attack Confirmation chapter in order to comprehend the existing position and identify prospective dangers. Financial losses, business interruptions, legal obligations, and reputational harm are all possible dangers. Each risk must be assessed in terms of its likelihood and possible impact on the company.

Once discovered and reviewed, risks should be prioritized, with the highest likelihood and possible effect being prioritized first. To handle the identified risks, the company must examine existing resources and competencies.

The Risk Assessment is an important stage in reacting to a ransomware attack because it assists DTU in identifying and prioritizing the risks connected with the attack. The data acquired in this study will be utilized in the impact analysis in the Assessment chapter to evaluate the overall impact of the attack and the required reaction [6].

5 Assesment

Author: Alexander (s230265)

Ransomware attacks can be crucial to an organization and we have to understand the critical importance of being prepared to respond to them.They can cause significant disruption to the operations of our institution, potentially leading to data loss, system downtime, financial loss, and reputational damage. This part consists of several sections, including impact analysis, business continuity planning, and containment and communication.
An impact analysis is a process that helps to identify critical systems and data, as well as prioritize recovery efforts.In this section, the focus is on describing the methods for conducting an impact analysis. This information is critical in determining the extent of the damage caused by the ransomware attack and in prioritizing the recovery of critical systems and data [12].

1. **Identify critical systems and data:** It is important to identify critical systems and data as they are the most important assets of the organization. The impact of losing access to these systems and data would be severe, and it should be prioritized during recovery efforts. These systems may include email servers, financial systems, and customer databases, while data may include confidential business information, personal customer data, research findings and intellectual property.

2. **Determine the impact of the attack:** Once critical systems and data have been identified, the next step is to determine the impact of the attack on those systems and data. This involves actions evaluating the extent of the damage, the number of systems affected, and the potential for data loss. The impact analysis should also consider the potential impact on the organization's reputation and the financial impact of the attack.

3. **Prioritize recovery efforts:** Once every necessary action is done and based on the impact analysis, recovery efforts should be prioritized to ensure that critical systems

and data are recovered first. The recovery plan should also consider the connections between systems and prioritize the recovery of those systems that are required for the operation of other critical systems.

The Business Continuity Planning section marks the steps for developing and implementing a business plan to ensure that critical business functions can continue in the event of a ransomware attack. This plan is essential in keeping the organization up and running, minimizing downtime, and reducing the impact of the attack on the overall operations.

1. **Define critical business functions:** The first step is to define critical business functions, which are the activities that must continue to ensure the organization's survival. These functions may include student enrollment, course delivery, and record keeping.

2. **Assess the Impact of Disruption:** nce critical business functions are identified, the next step is to assess the potential impact of a disruption on those functions. This may involve estimating the potential downtime, financial losses, and impact on student services.

3. **Develop Recovery Strategies:** Based on the impact assessment, recovery strategies must be developed to restore the critical business functions. For example, if the student information system is impacted, alternative methods of enrollment and record keeping should be identified.

4. **Develop Recovery Procedures:** The recovery procedures should outline the steps required to implement the recovery strategies. This may include identifying the personnel responsible for implementing the plan and specifying the required resources.

5. **Test and Maintain the Plan:** The final step in developing a plan is to test it and ensure it remains up to date. Regular testing of the plan can identify any weaknesses or gaps, which can be addressed to the responsible personnel we assigned previously,before an actual attack occurs.

6 Containment & Communication

Author: Alexander (s230265)

This section should provide instructions on how to contain the spread of the ransomware attack, including measures to prevent further damage. It states the recommended steps to isolate the infected systems, disable network access for affected users, and communicate with relevant stakeholders. It also includes communication protocols, as well as how to communicate incidents of different severities [4].

6.1 Containment Strategy

The first step is to isolate the infected systems to prevent the ransomware from spreading further. This can be achieved by disabling network access for affected users and disconnecting the infected systems from the network. The IT team must identify the scope of the infection and determine which systems need to be restricted. Once the affected systems are identified, they must be isolated and taken offline as soon as possible to prevent further damage.

6.2 Communication

Outline the communication plan, including who should be notified, what information should be shared, and the method of communication.
A communication plan must be in place to ensure that all relevant stakeholders are informed of the situation. The communication plan must include a list of key contacts, including internal staff, external vendors, and regulatory bodies. The plan must also specify what information should be shared, and the method of communication.

The responsible team should follow the following procedure:

1. **IT department:** All members of the IT staff should be the first that get notified of the attack. The staff should also be provided with regular updates on the status of the attack, including any new developments or changes in the containment strategy.

2. **Senior Management:** The IT team should immediately inform senior management of the ransomware attack, including the scope of the attack and the impact on the institution. Senior management should be involved in decision-making processes related to the attack, including the allocation of resources and the implementation of recovery strategies.

3. **External Vendors:** The educational institution should notify any external vendors that provide IT services or support, such as managed service providers. These providers and vendors should be informed of the attack and asked to provide assistance in containing and mitigating the attack.

4. **Regulatory Bodies:** If the educational institution is subject to any regulatory requirements, such as data protection regulations or industry standards, the relevant regulatory bodies should be notified of the attack. This will help ensure that the institution is complying with any regulatory requirements related to the incident.

5. **Law Enforcement:** Depending on the severity of the attack and the impact on the institution, law enforcement agencies may need to be notified. This can help with any investigations into the attack and may provide additional resources to help with the response and recovery efforts.

6.3 Post-Containment Action

After the ransomware attack has been contained, the educational institution should take steps to clean up the infected systems and restore normal operations. This process can involve restoring data from backups, updating systems to prevent future attacks and testing them to ensure they are free of malware.

1. **Network access control (NAC):** Network access control solutions can be used to identify and isolate infected systems automatically. This can be configured to monitor network traffic and identify systems that exhibit suspicious behavior, such as attempting to communicate with known ransomware command-and-control servers. Once an infected system is identified, it can isolate it from the network and prevent it from communicating with other systems, preventing the spread of the ransomware.
2. **Endpoint Detection and Response (EDR):** This solution can be used to detect and respond to threats on endpoints. It can detect ransomware activity and isolate infected systems before they spread the ransomware to other systems.
3. **Firewall Rules:** The responsible team can create firewall rules to block traffic to and from known malicious IP addresses or domains. This can help prevent ransomware from communicating with the attackers' servers.
4. **Network Segmentation:** Network segmentation can be used to divide the network into smaller segments, each with its own security controls. If one segment is infected with ransomware, it can be isolated from other segments to prevent the ransomware from spreading.
5. **Backup Solutions:** In addition to isolating infected systems, the responsible team should also restore data from backup systems.

7 Escalation

Author: Usama (s222644)

Escalation is a critical part of the ransomware process and it should be initiated as soon as possible If the ransomware attack is severe and beyond the capabilities of DTU incident response team. This can be done by following steps [3]:

Notify Senior Management: The incident response team should immediately inform senior management, including CISO (Chief information security officer) and CIO (Chief Infor-

mation Officer), about the attack and its impact.

Engage third-party experts: If the DTU incident response team is unable to contain and remediate the attack, third party experts should be engaged to assist with the response. These experts can include cybersecurity consultants, forensic investigators, and incident response teams from specialised security firms.

Activate disaster recovery plan: This plans refers to the disaster recovery plan which includes restoring data from backups and rebuilding the system from scratch. This should be done in the case that there is severe damage to the critical systems and data.

Communicate with stakeholders: During a ransomware attack, it is essential to keep all the stakeholders informed about the incident and its impact on the organisation. This includes employees, partners and any vendors associated with DTU. Regular updates should be provided to reassure stakeholders that the situation is being dealt with and provide a expected timeline for recovery.

8 Eradication & Recovery

Author: Usama (s222644)

Once the initial response to a ransomware attack has been completed, the next step is to eradicate the ransomware from the affected systems and begin the recovery process. This section outlines the steps to take to eradicate the ransomware and recover the affected systems and data [10].

8.1 Eradication

The first step in the eradication process is to isolate the affected systems from the rest of the network. This will prevent the ransomware from spreading to other systems on the network. Once the affected systems have been isolated, the next step is to identify the ransomware and remove it from the affected systems.

It is important to note that simply removing the ransomware may not be sufficient. The attackers may have left back doors or other malware on the systems that could allow them to regain access in the future. Therefore, a thorough analysis of the affected systems should be conducted to identify any remaining threats.

In addition, any passwords or credentials that may have been compromised during the attack should be changed to prevent the attackers from regaining access to the systems.

8.2 Recovery

Once the ransomware has been eradicated, the next step is to recover the affected systems and data. This process should begin with a review of the backup and recovery procedures to ensure that they are up to date and that backups are available for all critical data and systems [2].

The recovery process should prioritize critical systems and data, with the goal of restoring operations as quickly as possible. As systems are restored, they should be thoroughly tested to ensure that they are functioning correctly and that they have not been compromised by the ransomware or other malware.

Once all systems have been restored and tested, the final step is to conduct a post-incident review to identify areas for improvement in the incident response process. This review should include an analysis of the root cause of the incident, the effectiveness of the incident response procedures, and any lessons learned that can be applied to future incidents.

9 Post Incident Review

Author: Usama (s222644)

A post-incident review is a critical step in the incident response process. It allows us to evaluate the effectiveness of our incident response plan and identify areas for improvement. The goal of the review is to identify what worked well and what didn't during the incident response process.

To begin with, gather the incident response team and other key stakeholders who were involved in the response effort. Review all documentation and records related to the incident, including the incident response plan, logs, and communication records.

Following questions should be asked during the review:

1. Was the incident response plan effective in containing and resolving the incident?
2. Were the right people involved in the response effort, and were they able to work effectively together?

3. Were there any communication breakdowns during the incident, and if so, how can we improve communication in the future?

4. Were there any technical issues that hindered the response effort, and if so, how can we address these issues?

5. Were any procedures or protocols not followed during the response effort, and if so, how can we ensure they are followed in the future?

After answering these questions, identify areas for improvement and develop an action plan to address them. This may include revising the incident response plan, improving communication protocols, or providing additional training for members of the incident response team [10].

10 Conclusion

The Attack Confirmation chapter is essential in a ransomware run-book as it validates, identifies, and evaluates the attack. It prioritizes recovery efforts and requires organizations to validate detection, identify ransomware, assess the scope, and document crucial details. Proper documentation helps identify security flaws, develop efficient responses and enables essential communication between the stakeholders. This information is used in the impact analysis to determine the attack's overall impact and the best response. The Ransomware Situational Analysis is crucial in responding to an attack. It includes analyzing impact, identifying the attacker, and assessing risk. The Attack Confirmation chapter provides a foundation for the analysis. Organizations should prioritize risks and assess resources to handle them.

Overall, DTU may strengthen its resistance against ransomware attacks, safeguard its valuable assets, and lessen the interruption and potential harm brought on by such situations by adhering to the policies and procedures described in this run-book. The run-book should be kept current and tested frequently to maintain its efficacy and adaptability to changing cyber threats.

References

[1] Ross Brewer. Ransomware attacks: detection, prevention and cure. *Network Security*, 2016(9):5–9, 2016.

[2] James McCafferty Bridget Kenyon. Ransomware recovery | itnow | oxford academic. https://academic.oup.com/itnow/article/58/4/32/2606459?login=true.

[3] San Luis Obispo Cal Poly. Its security standard: Incident response program - escalation - information security. https://security.calpoly.edu/content/standard/response-escalation.

[4] Cybersecurity and Infrastructure Security Agency. Ransomware guide. https://www.cisa.gov/publication/ransomware-guide, 2021. Accessed on May 5, 2023.

[5] Cybersecurity and Infrastructure Security Agency (CISA). Ransomware guide. https://www.cisa.gov/ransomware, 2021. Accessed on 5 May 2023.

[6] The SANS Institute. *Ransomware Incident Response Plan*, 2021.

[7] McAfee. *The McAfee Ransomware Response Guide*. McAfee LLC, 2020.

[8] National Institute of Standards and Technology (NIST). Guide to malware incident prevention and handling for desktops and laptops. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf, 2009.

[9] Gavin O'Gorman and Geoff McDonald. *Ransomware: A growing menace*. Symantec Corporation Arizona, AZ, USA, 2012.

[10] TimGrance Karen Scarfone Paul Cichonski, Tom Millar. Computer security incident handling guide. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf, 2012.

[11] Ronny Richardson and Max M North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1):10, 2017.

[12] US-CERT. Ransomware guide. Online, 2021.