Solidarity Playbook

Retrieving access to a hacked IT server

International
Civil Society Centre

CyberPeace
Institute

solidarityaction.network

1. Overview

The global non-profit organisation operates with local chapters in each country and has regional offices that offer support and guidance to the local chapters. The headquarters offers a broad portfolio of technology applications and systems for finances, fundraising, and program management to avoid duplication. In all, 20,000 people use the organisation's IT system, which is managed by an IT team of 25 staff members.

In September 2021, the organisation was attacked by a hacker group to extort a ransom. The team mobilised internal experts and additional help through the organisation's cyber insurance provider to negotiate with the attackers, counter the threat, and restore the organisation's data.

2. What happened?

On a Saturday in September 2021, the organisation's IT system was attacked by a hacker group that found and exploited a software gap to extort a ransom. The hackers entered the system and took control of some data, blocking the organisation's access to it.

The server that was initially attacked was a development system (in other words, an environment in which the IT team writes and develops code before pushing it live on the production system). The system that was exploited had been patched shortly before the attack (with the corresponding production system). Based on available log information, forensic experts assumed that the patch on the development system had failed. Due to the configuration of the network at that time, the attackers were able to move laterally in the network and access additional servers.

The attackers were neither seeking to extort money from a particular individual nor the specific organisation; rather, the **organisation was a randomly selected target**.

RANSOMWARE

Ransomware is a type of malware designed to extort money by encrypting or blocking access to files or the computer system until a ransom is paid. Often, attackers threaten to make the target's data publicly available, which is known as double extortion.

*CyberPeace Institute (2022): **Glossary of cyber terms***

Experts do not recommend paying the ransom, because doing so does not guarantee that the attackers will give the decryption key or that the decryption key they share will work. **The No More Ransom** project is a valuable resource to explore on this issue.

The incident was stressful for the IT team and required allocation of additional capacities to respond to the ransomware attack. They were also mindful that their systems contained sensitive data from different communities the organisation engages with, and they felt responsible to keep these data safe.

3. Response

Abnormal system behaviour was first recognized by an on-duty IT team. Due to an existing incident response process and related emergency plans, the team and external forensic experts from their cyber insurance provider were available on short notice. A response team was quickly formed to work on various incident response tasks simultaneously and to provide up-to-date information for the organisation's management, which was communicated by the head of Information and Communication Technology (ICT).

CYBER INSURANCE

Cyber insurance is a form of coverage designed to protect businesses (and civil society organisations!) from digital threats. If a cyberattack occurs, the policy covers financial and reputational costs, which may include investigation costs, data recovery costs, loss of income, payments demanded by hackers, and legal defence costs.

*Hiscox (n.d.): **What is Cyber Insurance?***

The most important and urgent tasks were to contain the problem and restore the systems, conduct negotiations with the attackers, and consult with legal support. Since donor data might have been affected, it was also vital to communicate quickly about the incident with the directors of local chapters and inform data protection authorities.

The organisation negotiated with the attackers for four days to retrieve the keys to decrypt their data. The organisation explained the nature of their work, their limited financial ability to pay the ransom, and the negative effects of paying a ransom on the communities they serve and their donors. After intensive negotiations, the attackers withdrew their ransom payment demand and sent the keys to unlock the data. They also explicitly confirmed that they had not extracted or retained any data.

With the help of forensic experts, the organisation was able to identify all affected systems and recover business operations. **Sometimes, ransomware attackers may plant additional malware to extract data, launch a subsequent ransomware attack, harvest users' credentials, or spy on day-to-day activity inside the organisation's intranet**. After retrieving the data, there was a four- or five-day period during which forensic experts examined the system to check for indications of a follow-up attack.

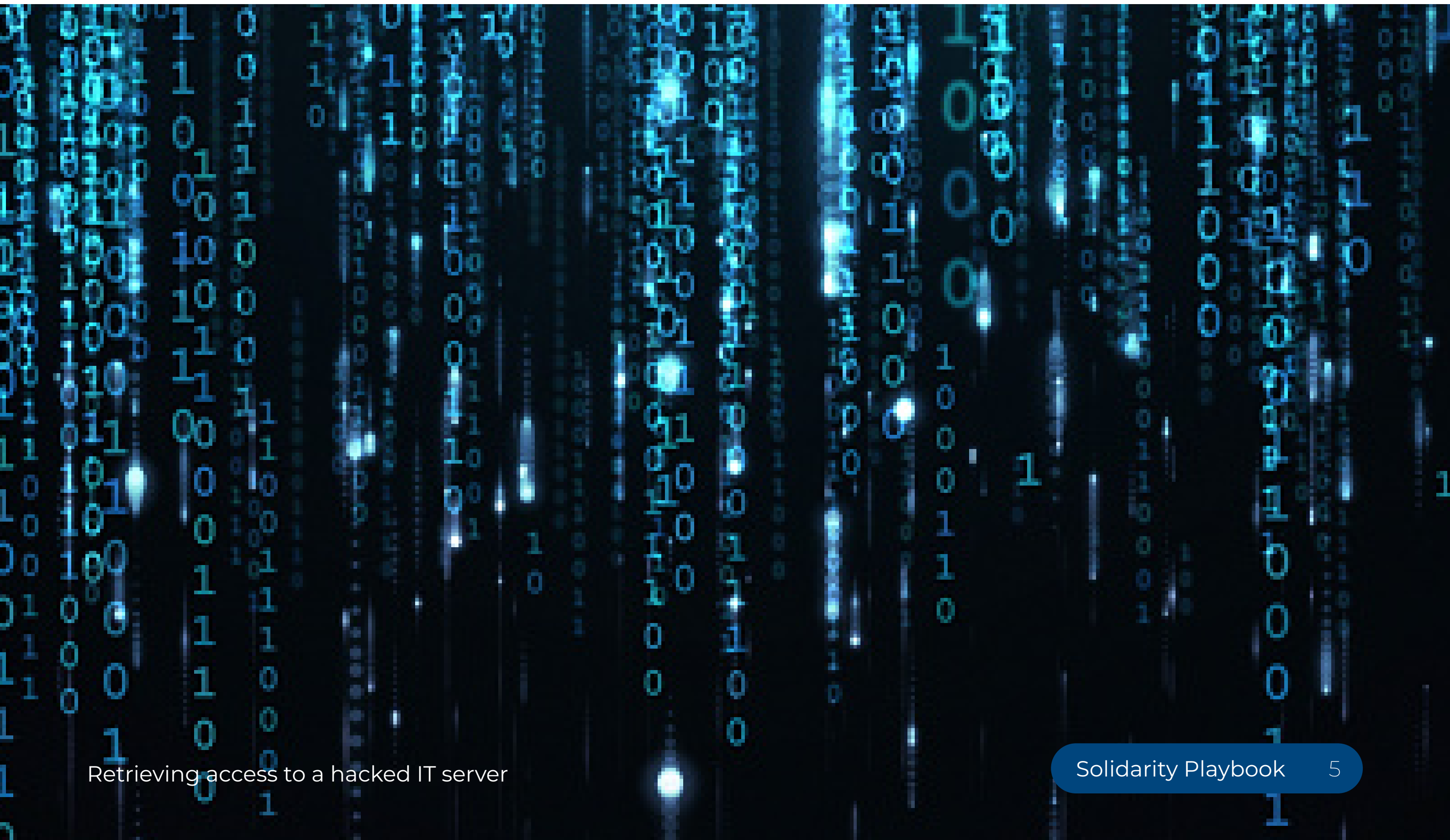
After the forensic experts had confirmed that there was no further immediate danger, the IT team restored the IT systems and all applications. More forensic work continued to double-check if any of the hacked data had been put on the darknet. The experts concluded that as far as they could tell, this had not happened.

DARKNET

A darknet is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization intended to defend digital rights by providing security, anonymity, or censorship resistance. Though it is used for legitimate reasons, it has also been heavily used by criminals, and the term "darknet" nowadays is generally associated with websites that are specifically used for criminal purposes.

*CyberPeace Institute (2022): **Glossary of cyber terms***

In addition to the external support the organisation received, the key to the successful response was the fast mobilisation of internal management. The organisation was able to **quickly set up an internal crisis group, because they had mobilised a similar group to respond to a non-cyber incident just six months before**. The group – comprised of the CEO, CFO, heads of IT, legal, communications, and crisis coordinator – met daily. With the help of this internal crisis team, the organisation was able to avoid panic and manage the crisis effectively, make quick decisions together with external experts, communicate professionally, and inform and cooperate with data protection authorities and police in a timely manner.



4. Outcome & impact

The organisation managed the incident without significant damage other than a system shutdown of about ten days outside of the “peak season”. One server had to be decommissioned due to the attack, but ultimately no data were lost or left the organisation.

The staff members were able to continue their day-to-day business and communicate with one another during the attack because the email systems were not affected. The biggest disruption to the organisation related to financial transfers from headquarters to local chapters, which had to be paused during the incident.

The incident led to a **budget increase for cybersecurity measures** across the organisation. Additionally, a **cybersecurity regulation for the organisation was developed** by a working group. These changes demonstrate the increased importance of cybersecurity to the senior management. The regulation was approved by the organisation’s governing bodies and will be implemented until the end of 2025, which will result in higher data security in the organisation’s headquarters, as well as regional offices and local chapters, over the coming years. The incident has also led to **increased cybersecurity capacities** (more IT staff members) and **strengthened technical systems** within the organisation through the following measures:

The organisation **divides its network into segments** to control the flow of traffic between subnets based on granular security policies that prevent any unauthorized access to business assets. In addition, they have implemented a **tier admin model** which creates divisions between administrators based on the resources they manage (for instance, administrators who control user workstations are separated from those who control applications or manage enterprise identities).

SEGMENTED IT SYSTEM

A segmented IT system divides an organisation's network into smaller parts. This approach has advantages, such as improving performance. Segmentation also limits the spread of a cyberattack – and therefore the damage it can cause.

*CISCO (n.d.): **What Is Network Segmentation?***

In addition to the existing conventional backup concepts and strategies, it was key for the organisation to implement an **immutable backup solution** – a backup file that cannot be altered in any way. This file contains data that are fixed, unchangeable, and can never be deleted, and this solution enables the organisation to recover data in case of an attack or other loss.

Since the incident, the IT team has also moved away from legacy solutions, such as antivirus software, and shifted to **extended detection and response (XDR) systems** – programs that can find deviations from the norm on a server.

EXTENDED DETECTION AND RESPONSE (XDR) SYSTEMS

XDR systems offer advanced capacity to detect threats by analysing data across multiple security layers, including email, servers, cloud workloads, networks, endpoints (i.e., computer terminals), and networks, and using automation to detect and respond to threats. By breaking down the silos between security layers, XDR systems are better able to identify advanced, stealthy threats than other systems. However, they are often more costly than alternatives and may be out of range for many civil society organisations.

*Trend Micro (n.d.): **What Is XDR?**; CISCO (n.d.): **What Is Extended Detection and Response (XDR)?**; Cynet (n.d.): **Understanding XDR Security: Concepts, Features & Use Cases***

The organisation further invested in **advanced logging mechanisms** (SIEM logging), a solution that helps organisations detect, analyse, and respond to security threats before they harm operations. This solution enables the organisation to have better data for forensic research. With more detailed information about what happened, it is easier and faster to determine whether a data breach has occurred.

Finally, to detect any malicious behaviour and enable incident response outside of normal working hours, the organisation's endpoint protection solution (the solution that monitors staff devices like laptops and mobile phones for potential exploitation by malicious actors) is now **managed 24/7 by external experts**.

5. Organisational learnings

CHALLENGES

Uncertainties regarding a data breach

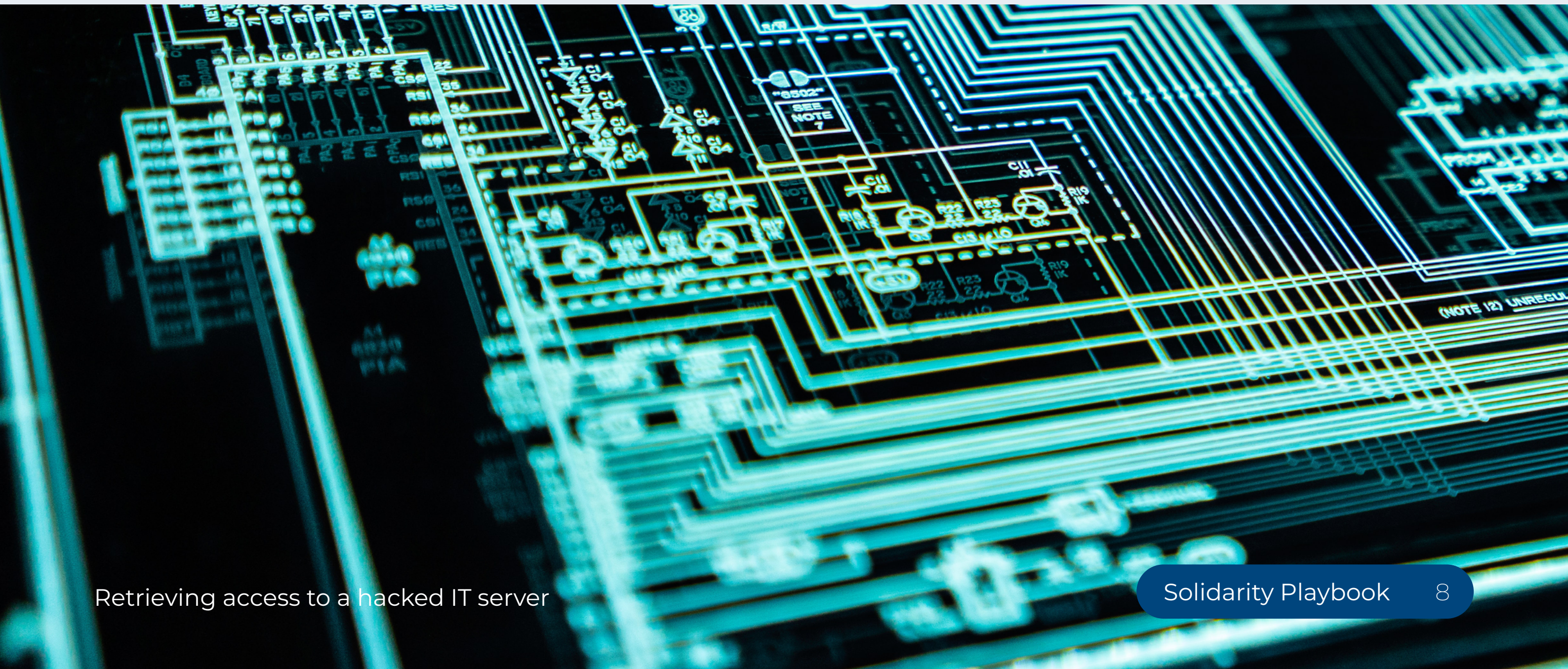
After the organisation secured the keys to their data, concern persisted regarding whether they had full control over the data or whether the attackers had retained a copy. As there was no technical evidence of data theft and the attackers denied having retained data, the data protection authorities closed the case.

Negotiation process

Dealing with the attackers was unexpected and outside of everyday IT and management tasks, and it turned out to be very tricky. Due to the organisation's lack of experience with such situations, management and the IT team sought support from external experts for the negotiation process. The cyber insurance provider offered competent support and covered associated costs, which turned out to be a big advantage of the insurance.

How to communicate

Communicating about cybersecurity incidents can be a challenge. While some organisations make a conscious decision to publicly communicate about cybersecurity incidents, this organisation weighed the risks and benefits of public communication and decided not to do so. Since no data breach had been detected, the attack was not disclosed to media to minimize the risk of misinformation and speculation. Of course, the data protection authority was informed because it was unclear within the statutory notification period whether a breach had occurred.



LESSONS LEARNED

Cultivate connection with experts to enable faster (and more trusted) incident response

The organisation had an established relationship with the cybersecurity experts from the assessment they had completed when acquiring the cybersecurity insurance a year prior to the incident. They therefore felt comfortable reaching out to these experts and asking for support when the incident occurred.

Communicate clearly about the cyberattack

Good internal communication is key to prevent the unguided circulation of possibly incorrect or misleading information about the cyberattack. Therefore, it is necessary to define communication guidelines and create standards and procedures to enable seamless and coherent internal communication during the incident.

Be careful about outsourcing data

If data are outsourced, the organisation carefully interrogates any notifications and alarms related to those data. Further, they prioritise close cooperation with the product owners, because in case of an attack on outsourced data, the organisation relies on the third party to react appropriately.

Leverage existing crisis mechanisms

Existing crisis mechanisms can be leveraged for cybersecurity incidents, even if they were established to handle different issues. Six months before the cybersecurity incident, the organisation experienced another crisis which mobilised an almost identical group of actors. Those involved met daily to manage and mitigate the crisis. When the cyberattack happened, the organisation used the same response model that had worked before. Key to the success of the crisis group was gathering a small number of people with a high level of trust and a constructive spirit. There was a recognition that everyone was dealing with this situation for the first time, and there was no set recipe or cookbook. Thus, there was a shared understanding that the crisis management group was developing their approach along the way.

Discover more case studies
solidarityaction.network/cybersecurity

Solidarity Playbook

Retrieving access to a hacked IT server

Sacha Robehmed and Nonso Jideofor

March 2023

International
Civil Society Centre

CyberPeace
Institute

In partnership with

Sweden
Sverige

FORD
FOUNDATION