HIS-HE
WIR GESTALTEN
HOCHSCHULZUKUNFT.

HIS-HE: Guide

11|2024

Crisis management after cyber-attacks - Recommended Actions

HIS Institut für Hochschulentwicklung e. V.
Goseriede 13a | D-30159 Hannover, Germany | www.his-he.de

Dr Harald Gilch, Dr Maren Lübcke, Dr Mathias Stein
Geschäftsbereich Hochschulmanagement

26. November 2024

Table of contents

Acknowledgement

In addition to a review of existing literature, we developed these recommendations based on interviews and discussions with by cyber-attacks affected universities[1] - the Technische Universität Berlin, the University of Duisburg-Essen, Justus Liebig University Giessen, Hamburg University of Applied Sciences, and Ruhr West University of Applied Sciences. We want to thank the chancellors, IT managers, IT security officers, and heads of communications departments for taking the time to respond to our inquiries and share their invaluable insights on cyber-attacks. Without them, these recommendations for actions would not have been possible. We would also like to extend our gratitude to the 'Digital Transformation' working group of the University Chancellors for their support of the project, from whom we received invaluable guidance at an early stage. Furthermore, we are indebted to the experts who provided comprehensive and constructive feedback after critically reading this document.

We are pleased to present this updated version of our text, now available in English. The initial German edition was published in 2023. We want to express our sincerest gratitude to EUNIS for proposing to publish this work in English and to all those involved in the publication process. While the core content remains mostly the same, we have taken the opportunity to ensure that the information is as up-to-date and accurate as possible. We hope this edition will continue to serve as a valuable resource for interested readers.

[1] The term 'university' is used as a reference to the wider sector, which represents the main area of tertiary education in Germany and thus includes technical universities, universities, universities of applied sciences and colleges of art and music.

0 Preliminary remarks

The number of cyber-attacks on universities in Germany is increasing.[2] This increase is due to the high number of users on the largely freely accessible university networks and the increasing digitisation of university IT, which collectively offer more potential targets for attackers. In response, it is vital to implement robust defence and emergency measures to prevent attacks and to be able to respond to an attack swiftly.

The IT landscapes of universities and the potential avenues of attack can vary considerably. The consequences of cyber-attacks on universities can also differ significantly. Therefore:

- The nature of the crisis scenario is contingent upon the severity of the attack and the extent of the IT systems affected.
- The range of consequences is considerable, encompassing scenarios from no direct effects to the encryption of individual systems and data theft to the complete paralysis of the entire university IT system.
- It is infeasible to devise a specific preparation or set of instructions for every potential crisis scenario.

The following explanations and recommendations are, by their very nature, **generalisations**. As a result, these must be adapted to the specific circumstances of each university – depending on its unique IT landscape, available resources, and existing (IT) governance structure. We prepared this guide with only universities and universities of applied sciences in mind. However, recent cyber-attacks have also struck university hospitals, non-university research institutions, and cooperation partners. The details and specific consequences associated with such attacks are beyond the scope of this guide.

This handout does not address the prevention and defeat of a cyber-attack from an IT perspective, despite the central role of IT in the context of a cyber-attack. The **focus is**, therefore, **on the entire university organisation from the perspective of the university administration**, given that even the briefest failure of IT systems has severe consequences for the university's ability to function. The recommendations for action facilitate the expeditious remediation of a cyber-attack and mitigate the potential damage. In this regard, this document catalyses internal discussion and serves as an initial framework for preparation and crisis management. Based on the crisis scenario of a cyber-attack, the document outlines measures and recommendations for action in the various phases, illustrating how preparation can help with the management of these phases. Figure 1 depicts the five phases.

- Detection phase Time 0
- Reaction phase day 1
- Reaction phase week 1
- Reaction phase month 1

[2] „Obwohl nicht davon ausgegangen werden kann, dass das vermehrte Angriffsaufkommen das Resultat von fokussierten Kampagnen ist, waren Bildungseinrichtungen 2022 äußerst attraktive Ziele von Cyber-Gruppierungen. [Although it cannot be assumed that the increased number of attacks is the result of focussed campaigns, educational institutions were extremely attractive targets for cyber groups in 2022.]" (BKA 2023, p. 26)

- Normalisation phase

The following chapters describe the findings derived from the experiences of the universities surveyed for this guide.

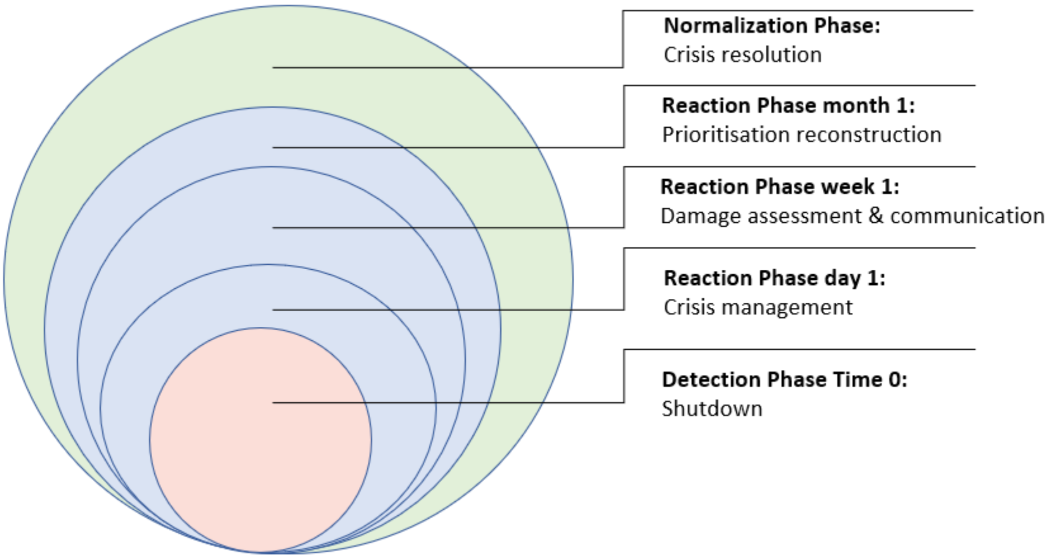

Figure 1: Five phases of crisis management after a cyber-attack

We provide guiding questions for each phase or area of responsibility. These questions act as a point of departure for an internal examination of the topic before a cyber-attack. Based on the individual questions, a checklist of measures per time period appears in the appendix. Universities and university management must view the preparation for a cyber-attack as a novel and ongoing responsibility. It is crucial to maintain a high level of **awareness** of this risk within the university, to ensure the **business continuity management** of the university systems, and to reinforce the university's overall **resilience** in the event of a crisis.

1 Detection phase - Time 0

In the event of a cyber-attack, the **time factor** is essential. It is crucial to respond as soon as possible, ideally within minutes or a few hours, to minimise the damage to the IT system. Prompt countermeasures, including the disconnection of the IT system from the network, increase the probability of safeguarding the various components from infection and ensure that the IT system can return to operation more quickly and easily. Given that many attacks occur during weekends or on public holidays, they can be detected more quickly through continuous system monitoring and contingency measures outside of standard operational hours. Before such an event, it is therefore essential to ascertain the following:

- Is monitoring IT systems for attacks and irregularities also guaranteed outside core working hours?
- In an emergency, who is responsible for making the final decision (on short notice) to disconnect parts of or, if necessary, the entire university IT system from the network? Is a joint management decision required, or does the management of the computer centre, for example, have the option to carry out the shutdown independently?
- What operational procedures are necessary for an IT shutdown?
- Which access points to the premises are required for the cross-cutting and termination of the computers?
- Which other institutions connect to the university's networks, such as university hospitals, affiliated institutes, and cooperation partners?
- Which external service provider(s) must the university inform of the crisis management in the event of a cyber-attack?

Most of these questions can be agreed upon in advance and independently of a specific cyber-attack. This process includes the question of which individual or entity is duly authorised to immediately decide to disconnect the university's IT system from the network and potentially shut it down. It is only possible to provide a generalised answer to this question, as (from a legal perspective) the responsibilities for such a far-reaching decision arise from the relevant university laws. On the other hand (from a professional point of view), the expertise regarding the existence of a cyber-attack and the possible consequences or the necessity for immediate separation may reside at the specialist level rather than at the management level. Should the necessity arise, the university can discuss the decision to disconnect from the network and shut down the systems with external experts in advance. The universities surveyed reported markedly disparate approaches in this regard. These approaches included disconnection following a decision by the university management and subsequent recommendation by the specialist department and disconnection by the specialist department and subsequent information and confirmation from the university management. Every university should, therefore, coordinate and answer this fundamental question internally in preparation for a possible cyber-attack. Regardless of the decision, the overarching objective must be to facilitate a prompt reaction.

Preparation Time 0:

It is necessary to guarantee the **continuous monitoring of the IT systems** to facilitate the swift identification of any attacks, irrespective of time constraints, including **weekends, public holidays and periods of low activity.** If in-house personnel cannot guarantee this condition, it may be necessary to outsource the monitoring to external service providers.

Before any such incidents, it is essential to clarify the **decision-making and communication channels** used to respond to a cyber-attack. Furthermore, the university must select whom to notify immediately upon an attack detection. Who can and must confirm the assessment that a cyber-attack is occurring? It must also determine which individuals are authorised to make decisions regarding the **termination of IT systems and their disconnection from the network.** It will prevent the spread and infection of other system parts only if done quickly.

In any case, the **IT crisis team (the IT core team),** established in advance, should begin coordinating and initiating the necessary measures. Management achieves these results by appointing the members of the core IT team and arranging for deputies to assume responsibility in their absence. Management has compiled lists containing private telephone numbers and e-mail addresses to facilitate communication. The university management must be involved at the earliest possible stage or convene a superordinate crisis team (see day 1 in section 2.1).

2 Reaction phase

2.1 Day 1

Ideally, the internal **IT core team should commence** work at the earliest opportunity, either at time 0 or at the latest during the first day following the cyber-attack. The **central crisis team** should meet at the same time. Separating the core IT team from a central, superordinate crisis team is optimal to relieve the core IT team of most control and coordination measures and communication tasks. The university should involve the relevant investigating authorities (police, state criminal investigation office) at an early stage and file criminal charges. The specific requirement for prosecution will depend on the type and scope of the attack. Considering the unique challenges posed by a cyber-attack, it is essential to implement an enhanced communication strategy. To this end, it is vital to answer the following questions in advance:

- Which members of the core IT team are also part of the central crisis team? Have other crisis teams already been established, and if so, can they be convened or rededicated at short notice?
- Are the current and private contact details accessible for the individuals who play a pivotal role in crisis management (including members of the IT core team, the central crisis team, other crisis teams, IT administrators, university management, and university communications)? Are alternative communication channels prepared?
- Is there a substitution arrangement? Which individuals or representatives are indispensable and must be involved or recalled in the event of their absence, for example, due to holidays?
- What spatial options, including IT emergency supplies, are permanently available?
- Which external bodies, such as supervisory authorities/ministries, police/state criminal investigation departments, cooperation partners, etc., must be informed?
- Is it possible that the attackers have made contact and attempted blackmail? Do the police and the relevant authorities (e.g., cyber defence of the state criminal investigation offices) need to be involved immediately?
- Is a breach of the protection of personal data possible or foreseeable so that the data protection authority must be informed and involved?
- Are decentralised structures and IT systems similarly affected so that the faculties/departments must be involved accordingly? What decentralised resources (personnel, IT structure, etc.) are available for utilisation?
- Who coordinates the damage assessment process?

Regardless of the severity of the attack, rapid **communication** within the university and with external parties is necessary. The first step is to clarify which communication channels are still available and which people have access to them. In extensive cyber-attacks, all traditional communication channels (including email, telephone, intranet, and website) may become inoperable. In such cases, it is imperative to utilise alternative means of communication, particularly private email accounts, instant messaging services, and social media accounts. Additionally, it is essential to determine whether action regarding the **university buildings is**

required, such as locking systems for building access, air conditioning systems for critical laboratories and instruments, lifts, and so forth. Management must clarify the following issues in advance:

- Does the department responsible for communication and public relations have a crisis plan? Who is responsible for crisis communication within the university and externally? Who assumes the central spokesperson function – the president/rector, the appropriate vice president/chancellor, or the press spokesperson? Who will act as a deputy if necessary?
- What templates and text modules are available for the initial communication during a crisis? To whom are they accessible?
- Is a secure, technical emergency infrastructure in place? Are there uncompromised laptops, printers, and telephone connections? What alternatives are available in each case? Who has access?
- Which rooms are affected by a failure of electronic locking systems, and which are not?

Furthermore, all **executive staff** at the university should be informed, as the consequences of a cyber-attack depend on its severity. Various work areas and organisational units may be affected. Executives are also the key multiplicators and the first point of contact in the event of a crisis. The university's various management bodies at central and decentralised levels should also participate at an early stage. Therefore, it is essential to clarify the following questions in advance:

- Are the contact details of all executive staff accessible, even if the communication channels and systems of the university have failed?
- Are there instructions provided for individual executives for a (cyber) crisis?
- What means are available to disseminate information to all UNIVERSITY members and facilitate co-ordination (e.g., to prevent technical devices from being switched on)?

Preparation day 1:

The university has appointed the **members of the IT core team and the central crisis team**. It has compiled contact lists comprising private telephone numbers and email addresses to ensure that the teams can be contacted in the event of, for example, the university's email and telephone service becoming unavailable. In addition, **rooms equipped with the requisite crisis management technology are available**. It has defined the fixed times of day (e.g., daily at 8 a.m. and 5 p.m.) at which the crisis teams meet.

Moreover, preparing internal and external communication in the event of a cyber-attack is another possibility, including the **creation and ongoing updating of an external homepage.** The teams can activate it immediately to provide a centralised source of information for the public and university members. They can reserve emails or emergency information on social media and host the external homepage. On-site information for staff and students can also be prepared (e.g., organising printing options or alternatives). The preparation rapidly reaches all status groups of the university and, if necessary, establishes **alternative communication channels** (e.g., central telephone service, group chats, social media communication).

The access options and entrances for the **university buildings** are subject to regulation, at least in an initial overview, and established emergency procedures are in place (e.g., locking systems for building access and air conditioning systems for critical laboratories and instruments). Management should have already established whether and how university members can enter university buildings and whether they are informed accordingly (e.g., failure of lifts, malfunction of emergency call systems).

It is strongly recommended that management engage **external IT experts**. Such external IT experts can provide invaluable assistance in defending against the attack, conducting forensics, or rebuilding the IT systems. The Federal Office for Information Security (BSI) lists companies that can provide **emergency support.** Given the limited market for IT security consulting and the lack of availability of short-term support, it is vital to conclude **external service contracts** in advance. When selecting external service providers, it is essential to consider their knowledge of universities, their organisational structure, and their IT infrastructure. However, it is also crucial to ascertain the existing IT expertise within one's own organisation, including decentralised units and collaboration partners, and to engage them if necessary.

Furthermore, the university should expeditiously conduct **forensic preservation**, defined as the isolation and preservation of potential evidence, in coordination with the relevant investigative authorities. It should document all measures to ensure the ability to provide information retrospectively (e.g., in the event of data protection concerns). Documenting the incident and the measures taken is also crucial for potential **legal issues**. The involvement of the investigative authorities at an early stage and the filing of criminal charges are essential.

2.2 Week 1

The university should establish a **second, extended crisis management team** that includes heads of departments/faculties and important central institutions, management bodies, and status groups. This team would facilitate effective crisis management across the entire university. If specific university departments are affected by the crisis, it may be prudent to establish a dedicated crisis team with a particular focus on these areas (e.g., administration). However, it is essential to balance between the broad involvement of decision-makers and multipliers on the one hand and the necessary limitation to ensure the ability to act and make decisions on the other. Concurrently, the number of interfaces and committee meetings should be restricted to avoid an unwarranted increase in the workload of the central players. The establishment of transparent and well-defined decision-making structures ensures the capacity to act. In addition, when staffing the crisis teams, it is also necessary to consider the provision of a 'translation service', for example, between IT experts and administrative structures. The university must answer the following questions to proceed:

- Who belongs to the extended crisis team? Which members of the extended crisis team are best suited to assume the role of a central 'translator' and mediator?
- What is the nature of the relationship between the central crisis and extended crisis units, and how do they interact with one another (through information, advice, or assistance)?
- Who will be the intermediary between the core IT and central and extended crisis teams?
- Are there already established connections, for example, between the IT and communications departments, that they can utilise accordingly?

If the perpetrators of the attack have contacted the university and made an **attempt at blackmail**, government agencies, such as the police, the State Office of Criminal Investigation, or the relevant cybercrime agencies and the public prosecutor's office, must become immediately involved unless this step has already been done immediately after detecting the cyber-attack. Communication with potential blackmailers should only occur in coordination with or directly through the relevant state authorities. In the event of a ransom demand, it is inadvisable to comply with such a request. Indeed, the German Federal Office for Information Security (BSI) explicitly advises against ransom payments in the event of cyber-attacks. This action ultimately results in financing criminal activities, which, if successful, can lead to a continuation and expansion of cyber-attacks (see, for example, Bodden, E. et al. 2022).[3] Secondly, there is no guarantee that the perpetrators will enable decryption in the event of payment or that they will not attack again. In addition, a ransom payment can give rise to criminal liability, including but not limited to a breach of due diligence, support for a criminal organisation, or the risk of terrorist financing.

The workload, particularly in IT and communication, is above average due to a cyber-attack, and other areas may be unable to function due to the failure of the requisite IT systems. The university must implement short-term **personnel (re)management strategies** to ensure the continued ability to perform tasks immediately after a cyber-attack. It is necessary to consider the integration of additional personnel, particularly in IT and

[3] Nearly 100 leading IT security experts have collectively issued an open letter opposing the practice of making ransom payments in response to ransomware attacks: 'However, ransom payments are the root of all evil in ransomware.' (ibid.)

communication. This increase may entail the deployment of external service providers, specialists from other administrative units, and personnel from collaborating academic institutions temporarily. In anticipation of this scenario, management can establish inter-institutional **collaboration agreements** with other institutions (e.g., at a shared location/campus or within overarching project structures) to facilitate mutual assistance. However, this collaboration should follow rigorous security protocols to prevent any accidental compromise of third-party IT systems. To this end, management must address the following questions:

- Who can provide resources, including hardware, software, rooms, and personnel? Which systems or applications could be outsourced to other university or external service providers or used considering the necessary security requirements? The most crucial systems involve learning management, campus management, personnel administration, and financial administration. These systems are essential for the effective functioning of the university, particularly in the context of academic instruction. Daily backups of the central services of external servers minimise the potential for data loss in the event of an alternative use.
- Is it possible to engage the services of external providers to provide additional support?
- Are there work areas that cannot function due to system failure but can provide personnel to assist with crisis management?

In the initial seven-day period following a cyber-attack, it is imperative to determine and establish the **priorities for restoring the systems** in question. Following the severity of the attack and the temporality of the academic semester, the university must formulate a prioritisation strategy. An attack during the lecture-free period will have different consequences than if it occurs during the application, enrolment, or examination phase. It is also crucial to consider the potential secondary effects, such as the inability to make salary payments due to a failure of the financial IT systems or operate critical experiments or research facilities due to a building service shutdown. The following questions, therefore, require answers:

- Which systems are affected by the attack, and to what extent?
- What is the most appropriate sequence for the restoration of the systems? Which core business activities should receive immediate priority?
- Who is responsible for documenting the damage, and how is this documentation to be carried out? Who is responsible for reporting the damage?

In the most critical case, one must assume that the internal means of communication are no longer available and that only public communication channels (e.g. social media) can serve as an alternative. Thus, management cannot direct and tailor **communication** to specific target groups. The communication of progress made in restoring the IT systems (which is desirable in terms of internal communication) may be observed (externally) by the attackers. In a cyberattack with ransom demands, the attackers could increase the pressure, for example, by launching targeted attacks on the university's emergency website. This danger makes communication about the incident highly sensitive and professionally supported externally if necessary. The following questions need answers:

- Are the alternative communication channels to the university operational and accessible to the public, or are there any necessary adjustments?

- Do the individuals in question possess the requisite skills and resources to oversee communication?
- Is a communication channel established between the core IT team and the communications and public relations department? Who is responsible for issuing messages and can provide support, especially when IT-related issues require clarification or adaptation for broader audiences?
- Which individual or department is responsible for translating the most crucial messages into at least English? Furthermore, would it be advantageous to determine whether an emergency homepage is available with information in German and English?
- How does the status of IT systems affect the various status groups at the university and keep them regularly informed?
- What methods might record and direct enquiries from university members? For instance, is there a centralised telephone helpline available?
- At what frequency should information on developments be provided internally or externally? Which external partners (e.g., ministries) should be apprised of progress regularly?

Per the pertinent legislation, universities must report any **data protection incidents** that may occur while processing personal data**.** Article 33 of the General Data Protection Regulation (GDPR) requires that university notify the relevant authorities of a personal data breach within 72 hours following the initial discovery of the breach. A detailed account of the nature of the data breach and the number of data records affected is also necessary. The university must provide an assessment of the consequences of the data breach. Following Article 34 of the GDPR, the university must inform data subjects without undue delay if the data breach poses a high risk to their rights and freedoms. In a cyber-attack involving ransomware, it must swiftly analyse the precise technical circumstances of the attack to ascertain whether personal information has indeed been stolen. If a cyber-attack only encrypts data with ransomware without stealing personal information, it does not automatically constitute a reportable data breach. Only after a detailed analysis of the incident can the university decide whether it would be necessary to document this breach internally, notify the relevant authorities, inform the affected individuals, or a combination of these actions.

Preparation week 1:

It is crucial to **establish** a long-term **crisis management system** that enables the formation of an extended crisis team or, if necessary, multiple crisis teams, in addition to the central crisis team. The university defines the composition of the crisis teams in advance and establishes the responsibilities and coordination processes following the identified requirements. The objective is to implement rigorous **crisis communication** and expedient decision-making procedures to facilitate prompt action. It should consider the possibility of entering into contractual agreements with external crisis communication specialists to support the organisation and work of the crisis teams and the management of crisis communication.

In the event of an **attempted blackmail**, the relevant authorities, including the police, the State Office of Criminal Investigation, the competent cybercrime unit, and the public prosecutor's office must be involved without delay. Even lacking an initial blackmail attempt, they should promptly inform the relevant state authorities of a cyber-attack. The university should conduct any reactions to ransom demands and communication with the blackmailers in coordination with the police or the State Office of Criminal Investigation. Paying a ransom is not an option, as it leads to financing criminal activities and poses a risk of criminal liability. Furthermore, it is of the utmost importance to assess the extent to which the cyber-attack constitutes a **breach of data protection.** It must inform the competent authorities within 72 hours of discovering the security breach.

A cyber-attack can significantly increase workload in specific areas, necessitating a **personnel (re)organisation** to accommodate these changes. It is advisable to consider potential **collaborative opportunities with other academic institutions or external service providers** in advance, as this cooperation can facilitate rapid crisis management and access to additional (personnel) resources. In t a crisis, it may be possible to make IT staff available at short notice to aid. It may also be feasible to make premises available to employees of the same university and to provide access to central IT systems (e.g. learning management, campus management ERP systems) as backups. The university must perform a daily data exchange with such backup systems, ensuring backups reside outside the university. The university must conduct a comprehensive risk assessment before using outsourced and uncompromised backups to prevent the attack from spreading to the IT systems of cooperation partners, such as other university.

Management can facilitate the expeditious restoration of affected systems by devising a schedule in advance that delineates the temporal **priorities of a university's central processes.** The ongoing prioritisation is contingent upon the severity of the attack and the point in time during the semester.

2.3 Month 1

In the initial stages (first weeks), the university can probably estimate the extent of the damage caused by the cyber-attack and determine which systems have been affected and which have not. Subsequently, it must determine which central services have failed and require replacement and which tasks it must implement as alternatives. Academic institutions must facilitate processing applications and enrolment, contact examinations, and payments (ideally, through digital means rather than manual completion of paper transfer forms and deposit and withdrawal slips). Considering the varying degrees of severity of the attack and the stage of the academic year, the university must **continuously prioritise** the **tasks** at hand**.** It should answer the following questions should:

- Which tasks are of primary importance for the fundamental operations of the university, and which tasks can it postpone? This analysis should encompass all administrative and structural units, the equilibrium between teaching and research, and the associated IT system landscape.
- What alternative methods or solutions could be employed to achieve the desired outcome?
- What is the optimal sequence for returning to normal operation? Which systems/applications must be available again as a matter of priority, and which systems/applications can the university postpone?

The extent of further development depends on the specific nature of the crisis and the extent of the actual impairment of the IT systems. It is possible to test the **restoration of IT systems** from backup data in advance without a specific cyber-attack. This process may be particularly relevant for standard systems such as campus management. In this regard, the university can simulate the shutdown or disconnection from the network and the subsequent effects within the entire IT system landscape without a concrete emergency in step-by-step test runs. This process is vital to assess the potential consequences of shutting down or restarting the systems. It must answer the following questions:

- What test runs and simulations have already assessed the consequences of shutting down or restarting systems? What potential cascading effects or reactions could occur as a result?
- What external IT connections exist with cooperation partners or system providers that need integration into the reconstruction process?

The **consequences for the university IT landscape** can vary considerably depending on the severity of the attack. In the event of a minor attack, it may be possible to rapidly resume individual systems with the help of existing, secured backups. However, in the event of a more significant attack, it may be necessary to reconstruct the entire IT landscape, which could require considerable time. During the crisis management period and the reconstruction of the IT systems, the university is particularly vulnerable, especially to blackmail attempts and possible external observation. In this regard, it is crucial to determine whether a rapid reconstruction of the IT systems is preferable to a secure but lengthier reconstruction of the systems or the IT landscape. The reconstruction process is an opportunity to reorganise the entire IT structure of the university and, for instance, reinforce the measures for IT security. The following questions, therefore, need to be answered:

- Which fundamental concept should be adopted and implemented: the rapid reconstruction of the IT systems or the (gradual) reorganisation and enhancement of the IT structure?
- Are there current plans for updating the IT landscape and IT security measures?

In addition to restoring systems, monitoring (long-term) **personnel management** to address the consequences of a cyber crisis is crucial. These consequences may include, for example, work overload and crisis experience. Furthermore, this crisis can exacerbate the 'wave-like' workload if management reworks outstanding work statuses following the resumption of normal operations and does not reduce overtime and overload. As with any crisis experience, long-term, subliminal consequences can ensue. The following questions, therefore, require answers:

- What options are available to alleviate the burden on staff? What additional personnel resources are available at short notice (e.g., due to structural underload in departments that cannot work but can provide support elsewhere)?

The potential for a **secondary impact** resulting from the consequences of a cyber-attack and its effect on the IT landscape is significant. Such an incident could harm the research sector, for instance, if laboratories or individual items of laboratory equipment become unavailable, thus preventing the continuation of experiments or test series at the appropriate time. However, it can also have consequences for reporting to third-party funders if, for example, data sets and research results are no longer available. In addition to restoring the respective data, the university must monitor for possible deadline violations, report obligations or follow-up, and ensure that reporting formats or systems are restored.

Preparation month 1:

The university can reduce the decision-making burden in an acute crisis by prioritising the tasks and functions of the administration as part of **continuity management.** The aim is to develop strategies, plans, and actions to provide alternative procedures for the central processes as quickly as possible. A preparatory definition of central tasks to maintain university operations helps quickly establish the ability to act and prioritise many tasks.

Concurrently, such planning determines which systems, processes, and applications require restoration and in what sequence. It is necessary to consider a range of potential time scenarios, which are also contingent on the timing of the attack (e.g., application deadlines and examination periods).

The university can simulate the **reconstruction of IT systems** and the disconnection or restart of systems independently of a cyber-attack. This simulation allows for assessing potential consequences and cascading effects through step-by-step test runs. At the same time, management can evaluate the necessity for the rapid restoration of IT systems or the implementation of long-term reorganization, including enhancements to IT security structures.

A further area of focus is the (long-term) **management of personnel** to address the effects of a 'wave-like' workload, to provide support and, most importantly, to manage the potential consequences of the crisis experience (e.g. work overload). It is also necessary to consider the possibility of **secondary damage** (e.g., to third-party funders, research projects, or cooperation partners).

3 Normalisation phase

A cyber-attack represents a significant crisis for the university as an institution and all university community members individually. A crisis has a discernible beginning and requires a conclusion and a return to normal operations. The difficulty of reaching a ‘clear conclusion’ is compounded by the lack of synchronisation in the aftermath of cyber-attacks, depending on their consequences, compounds the difficulty of reaching a ‘clear conclusion’. When most IT systems and applications have resumed normal functionality, there still may be residual effects or impairments in specific areas. This situation concerns long-term **personnel management tasks and a duty of care** for the individual employees to address the consequences of the cyber crisis (e.g. overwork, internal resignation) (see Northwave 2022). This problem is particularly pertinent given the current shortage of skilled workers. The overload issue is not exclusive to the IT and communication sectors; it also affects other areas that initially experienced a lack of work due to system failures. Following a successful recovery, these areas must rework the tasks left behind, such as re-digitising paper bookings. The following questions, therefore, require answers:

- How should overtime be compensated? Can it be reduced or paid out in part? It is incumbent upon the respective managers to make individual requests and agreements. However, it is advisable to coordinate different model variants.
- Are occupational health and safety and health management integrated?

It is crucial to utilise the **crisis as an opportunity for learning and development.** In addition to enhancing the IT structure, the university must cultivate the crisis management capability of its organisation. It must restore the ability to act in the short term and treat the cyber-attack as an opportunity to revisit the IT structure and governance, to reorganise it for the long term. Nevertheless, after a significant cyber-attack, the university should expect some resistance, as the crisis may also result in a loss of trust in IT and digitalisation. Furthermore, other potential consequences may arise, such as a loss of trust among business partners, network partners, and students.

In general, however, the university should integrate the management of cyber-attack crises into its overarching **crisis management framework.** university can utilise the established instruments and methods for this purpose, supplementing them in detail as necessary. Before an incident, it is essential to ensure coherence between the IT emergency plan and the university’s general crisis management strategy to facilitate trust and ensure a clear understanding of the necessary actions. In addition, a cyber-attack can also be an opportunity to make fundamental considerations regarding potential workarounds in the administration.

Preparation for the normalisation phase:

Occupational health and safety proactively develops strategies to **mitigate the impact of a potential crisis**. In addition, the university can establish **regulations** regarding managing phases of **severe overload and underload**. These regulations may include the provision of financial compensation for overtime for employees who have endured excessive workloads.

It is essential to implement **procedures for organisational learning** to evaluate this crisis experience and generate instructions for future crisis events. The recovery of IT systems can provide an opportunity to reorganise the whole IT landscape and enhance IT security.

In general, following cyber-attacks, the university should incorporate crisis management into the **university's crisis management system.** It can utilise established tools and methods for this purpose, integrating them into existing procedures and responsibilities. IT security and the potential of a cyber-attack represent a novel and enduring responsibility for universities and their administrative bodies. Consequently, they must address these issues on an ongoing basis.

A cyber-attack and the potential consequences represent a significant challenge for the university, necessitating a comprehensive and structured approach to facilitate individual and institutional coping mechanisms and a smooth transition to normal operations. Possible strategies include open communication about the management structures and a '**concluding** event'.

4 Summary and further preventive measures

While the consequences of a cyber-attack can vary considerably, and the development of individual crisis scenarios for each university is highly variable, every cyber-attack has an effect. In general, such incidents result in at least a review or even an adjustment and further development of the IT security structure, thus affecting the whole IT structure and the associated IT governance. In instances where the damage caused by the cyber-attack is severe, it may be necessary to implement a more robust IT infrastructure, such as a centralised system or enhanced backup capabilities, to ensure the resilience of the IT systems or to rebuild the entire IT landscape. The university must determine which systems to restore promptly and to what extent a more gradual, comprehensive reconstruction is beneficial in the long term. The protection of IT systems, preparation for a potential cyber-attack, and development of a (cyber) crisis management strategy are now permanent responsibilities for universities and their management teams. In conclusion: 'After the attack is before the (next) attack'. The question is no longer whether such an attack will occur but rather when and how successful it will be.

University can enhance their resilience by implementing several measures in advance. For instance, the creation and implementation of a crisis management system is crucial for the prompt execution of actions and the formulation of decisions. Implementing a continuity management system in advance enables the definition of alternative processes for central, critical procedures. It facilitates the restoration of systems by their relevance to the university. It is nevertheless crucial to develop or adapt an emergency plan corresponding to the various digital administrative processes, even if this task is not the focus of this guide. The university must develop an emergency plan for the most critical IT-supported specialised procedures, particularly in teaching and learning (including learning management and campus management systems) and central administrative areas (personnel and financial systems). Each university must determine, in advance, the priority of each research system. These measures aim to guarantee the universities' capacity to operate in their core functions, necessitating prioritising tasks and systems. This process encompasses technical elements, including external data backup, redundant systems or standby IT infrastructures, and comprehensive IT contingency planning. Considering the growing integration of IT with building and operational technology and systems that require monitoring, it is crucial to consider the potential implications for this domain. An 'IT baseline protection profile for universities' (ZKI 2022) has already been developed and published under the auspices of the 'Centres for Communication and Information Processing' (ZKI) association. Management should familiarise themselves with this IT baseline protection profile as a preparatory measure to address the various risks of a cyber-attack.

The subject of IT security must be a perpetual concern. A Chief Information Security Officer (CISO) at the strategic level and one or more IT security officers at the operational level can, for example, assume responsibility for the development, adaptation, implementation, and monitoring of IT security guidelines, the establishment of a security management system, and the implementation of protection needs analyses. The objective is to foster awareness and sensitivity to this subject matter across the entire university community. Furthermore, it is essential to cultivate a culture of error reporting that does not impose penalties for accidental actions such as clicking on phishing emails. Instead, it would encourage a constructive approach with prompt and accurate reporting. Therefore, promptly reporting errors or perceived irregularities within the system is essential for the effective implementation of good IT emergency management, which is crucial for the prevention of significant damage. Thus, the university should explore developing and trialling exercise scenarios or stress tests with other crisis phenomena to enable a rapid and effective response.

In any case, a cyber-attack represents a significant crisis for the university, which it must address in a manner commensurate with the severity of the attack. The restoration of the IT systems, and thus the ability to function as an organisation, are undoubtedly the primary objectives. For the university organisation, however, additional considerations must be made in the aftermath of the incident, including crisis management, personnel management, duty of care, and occupational health and safety. It is also imperative to consider the potential risk associated with a cyber-attack in the context of occupational health and safety and operational safety. Many consequences may ensue, including (external) loss of reputation, (internal) mistrust of IT and digitalisation in general, and loss of trust in the university's management structure and ability to deal with a crisis.

5 Literature

All links were last accessed on 25.09.2024:

Bundeskriminalamt (BKA) (2023). Bundeslagebild Cybercrime 2022 [Federal Cybercrime Situation Report]. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=4
[The Federal Cybercrime Situation Report is updated annually by the BKA. The last report was published in 2024]

Bodden, E. et al. (2022). Lösegeldzahlungen bei Ransomware-Angriffen: ein geostrategisches Risiko [Ransom payments in ransomware attacks: a geostrategic risk].
https://ransomletter.github.io/

Northwave (2022). After the crisis comes the blow - the mental impact of ransomware attacks.
https://26168787.fs1.hubspotusercontent-eu1.net/hubfs/26168787/Northwave-Research-After-the-crisis-comes-the-blow-The-mental-impact-of-ransomware-attacks-1.pdf

ZKI e.V. (2022): IT-Grundschutz-Profil für Hochschulen [IT baseline protection profile for universities]. Berlin: 2022.
https://www.zki.de/fileadmin/user_upload/Downloads/IT_Grundschutz_ZKI_2022_Final.pdf.

Attachments

Appendix 1 Checklist for preparing each phase

Checklist for 'Time 0':

- Guarantee the monitoring of IT systems for attacks and irregularities outside core working hours (nights, weekends, public holidays). Where necessary, conclude contracts with external service providers to ensure this.
- Determine who will make the final decision (at short notice) to disconnect the entire university IT system (or parts of it) from the network.
- Define and finalise the steps for the IT shutdown.
- Regulate access to the rooms available for disconnecting from the network and shutting down the computers.
- Put the core IT team in place.
- Provide up-to-date contact details (including private information outside the university networks). Describe the substitution rules. Define whom to call back in case of absence.
- Select an external service provider for crisis management of the cyber-attack, bound by a framework agreement and available to be notified immediately.
- Provide an up-to-date list of contact details for the emergency centres of the units connected to the university networks (e.g. university hospitals, affiliated institutes, cooperation partners).

Checklist for 'Day 1':

- Appoint the central crisis team. Provide up-to-date contact details (including private information outside the university networks) and define the representation rules.
- Provide the core IT and central crisis teams with rooms equipped with secure technical emergency infrastructure, such as computers, printers, and telephone connections.
- Define the relationship between the crisis team and the core IT team.
- Write a list of external bodies such as the inspectorate /ministry, police/ criminal investigation department and cooperation partners and provide it to the crisis team members.
- In the event of an extortion attempt, provide the contact details of the authorities to be informed (police, National Bureau of Investigation or cyber defence of the National Bureau of Investigation, public prosecutor's office).
- Provide the contact details of the data protection authority if a personal data breach is foreseeable.
- Regulate the involvement of decentralised structures and faculties/departments. Identify which decentralised resources (staff, IT structure, etc.) are available in a crisis.
- Coordinate and define damage surveys.
- The Communications and Public Relations Department draws up a crisis plan. Agree on who will be responsible for internal and external crisis communication and who will be the central spokesperson (e.g. President, relevant Vice-President/Chancellor, Press Officer).
- Distribute templates and text modules for crisis communication through various media.

- Put a secure, technical emergency infrastructure in place. Regulate access and provide alternatives such as laptops, printers and telephone connections.
- Define and update an externally hosted emergency website. Prepare emergency messages with a link to the emergency website for social media channels.
- Determine which rooms could be affected by a failure of electronic locking systems.
- Provide the contact details of all university managers. Describe instructions for managers in the event of a (cyber) crisis.
- Define communication channels for all status groups. Identify which status groups must have information about the status of which systems (e.g., to prevent systems from being switched on, to provide information about access to buildings).

Checklist for 'Week 1':

- Define extended crisis team and specific roles such as 'translator' and mediator.
- Define and coordinate the interaction between the central crisis and extended crisis units.
- Identify the personnel interface between the core IT and central and extended crisis teams. For example, establish links between the IT and communications departments.
- Establish agreements with other academic institutions and external service providers to facilitate the provision of resources, including hardware, software, facilities, and personnel. If necessary, outsource subsystems to other universities or external service providers or utilise an alternative solution (such as SaaS). In doing so, consider the security requirements, including Moodle, HISinOne, SAP, or similar systems from other manufacturers).
- Engage the services of external providers for assistance, subject to regulatory control.
- The university's communications department establishes a contingency plan for crisis response. In addition, the university enters agreements with external service providers to ensure the continuity of its communications operations.
- Define which systems are to be prioritised in which phase of the academic calendar, including lecture-free period, examination period, turn of the year, and enrolment deadlines.
- Duly record the damage (damage survey) documentation and regulate the commissioning of the reporting following the relevant standards.
- Establish alternative communication channels, both internal and external. Should the necessity arise, provide external support and advice.
- Ensure the consistent application of language rules by defining the roles of those involved in preparing reports and the 'translation' of technical IT issues into easily understandable press releases.
- Organise the translation of the most important messages or the homepage into at least English.
- Create a separate channel (e.g., info phone) for the internal recording and forwarding of enquiries from university members.
- Define the 'reporting periodicity', e.g., to external partners.

Checklist for 'Month 1':

- Establish a detailed continuity and recovery plan, identifying which systems and processes are for essential university functions and which tasks can wait for recovery.
- Establish alternative workflows and define them for key processes.
- Provide timetables and information materials for the return to normal operations.
- Perform simulations and step-by-step test runs to prepare for the shutdown and restart of the systems.
- Consider the possible consequences and the IT connections to cooperation partners or system providers.
- Define the plans for updating the IT landscape and IT security measures.
- Provide scenarios and plans for rebuilding the IT landscape, including improving IT security structures, which management can implement in the short term.
- For staff planning purposes, departments make assessments of over- and under-utilisation of staff in the event of system failures and initial considerations of possible support and redeployment.

Checklist 'Normalisation phase':

- Develop overtime compensation models, which are harmonised and known to the managers.
- Prepare occupational health and safety and health management for crisis management and develop appropriate services and programmes.
- Develop organisational learning models and processes to evaluate the crisis experience and make improvements for future crises.
- Provide an updated package of awareness-raising activities for employees and students.
- Implement the integration of IT security/cyber-attacks into the university's existing crisis management (in terms of topics, personnel and structure).

Appendix 2 Further reading

In addition to the literature used in the handout (Chapter 5), further reading is recommended below.

All links were last accessed on 25.09.2024:

BITKOM (2016). Kosten eines Cyber-Schadensfalles. Leitfaden [Costs of a cyber loss event. Guide].
https://www.bitkom.org/sites/main/files/file/import/160426-LF-Cybersicherheit.pdf

Federal Ministry of the Interior (BMI) (2014). Leitfaden Krisenkommunikation [Crisis communication guide].
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf?__blob=publicationFile&v=4

Dreyer, M., Kühnlenz, F., & Brandel, B. (2023). Handout for preparing for information security incidents. ZKI e.V.
https://doi.org/10.5281/zenodo.10122533

German Rectors' Conference (HRK) (2018). Informationsicherheit als strategische Aufgabe der Hochschulleitung. Empfehlung der 25. Mitgliederversammlung der HRK am 06. November 2018 in Lüneburg [Information security as a strategic task of university management. Recommendations of the 25th General Assembly of the HRK on 6 November 2018 in Lüneburg].
https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/HRK_MV_Empfehlung_Informationssicherheit_06112018.pdf

European Agency for Safety and Health at Work (2022). Inclusion of occupational health and safety in the assessment of cybersecurity risks.
https://osha.europa.eu/sites/default/files/Cybersecurity-and-OSH_EN.pdf

European Union Agency for Network and Information Security (ENISA) (2014). Report on Cyber Crisis Cooperation and Management.
https://www.enisa.europa.eu/publications/ccc-study/@@download/fullReport

European Union Agency for Network and Information Security (ENISA) (2024). Best practices for cyber crisis management.
https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

Schwartmann, R., Ritter, S. (2020). Wer haftet beim Verlust von Forschungsdaten [Who is liable for the loss of research data?] Research & Teaching, 2020
https://www.forschung-und-lehre.de/recht/wer-haftet-beim-verlust-von-forschungsdaten-2998.

Shulman, H., Waidner, M. (2023). Forschung muss besser geschützt werden [Research must be better protected]. *Research & Teaching*.
https://www.forschung-und-lehre.de/management/forschung-muss-besser-geschuetzt-werden-5449

Verwaltungs-Berufsgenossenschaft (VBG) (2022). Umgang mit Bedrohungen und Notfällen. Risiken kennen und angemessen handeln [Dealing with threats and emergencies. Know the risks and act appropriately].
https://cdn.vbg.de/media/080041bf559e4b22a8d2fe7c27afad8b/dld:attachment/Umgang_mit_Bedrohungen_und_Notf_C3_A4llen_VBG_Fachwissen.pdf

Appendix 3 Useful addresses

All links were last accessed on 25.09.2024:

Bundeskriminalamt (BKA), Wiesbaden, www.bka.de

- Overview of cybercrime, including addresses of state police forces, the cybercrime unit of the Federal Criminal Police Office, and the National Cyber Defence Centre
  https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html

Federal Office for Information Security (BSI), Bonn, www.bsi.bund.de

- IT-Grundschutz. A systematic basis for information security. (BSI Standard 200-4 Business Continuity Management)
  https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- Qualified service providers [external consultants])
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html
- IT emergency card ‘how to behave in the event of an IT emergency’
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/it-notfallkarte_node.html

Federal Institute for Occupational Safety and Health (BAUA), www.baua.de

- TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen [Technical rule for operational safety (TRBS 11115-1): Cybersecurity for safety-related measuring and control equipment]
  https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html

Deutsches Forschungsnetz (DFN), www.dfn.de

- DFN-CERT GmbH: Service provider for Internet security
  https://www.dfn-cert.de/

European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/

- Cyber Crisis Management
  https://www.enisa.europa.eu/topics/cyber-crisis-management

Zentren für Kommunikation und Informationsverarbeitung e.V. (ZKI), www.zki.de

- ZKI Information Security Working Group
  https://www.zki.de/ueber-den-zki/arbeitskreise/arbeitskreis-informationssicherheit/

Other initiatives and projects (selection):

- Alliance for Cyber Security (BSI)
  https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html
- National Research Centre for Applied Cybersecurity (Athene)
  https://www.athene-center.de/en/
- Digital University NRW: Information security and data protection
  https://www.dh.nrw/diskurse/Informationssicherheit%20und%20Datenschutz-13
  https://www.mkw.nrw/hochschule-und-forschung/digitalisierung-hochschule-und-wissenschaft/cybersicherheit

- Stabsstelle Informationssicherheit bayrischer Hochschulen und Universitäten [Staff unit for information security at Bavarian colleges and universities]
  https://www.tha.de/Rechenzentrum/IT-Sicherheit/Stabsstelle-Informationssicherheit.html
- Lower Saxony State Working Group for Information Technology / University Computer Centres (LANIT)
  https://www.lanit-hrz.de