EPiC Series in Computing

Volume 107, 2025, Pages 256–261

Proceedings of EUNIS 2025 annual congress in Belfast

Cybersecurity in higher education: Different approaches in the German federal states to support universities in defending against cyber-attacks

Harald Gilch[1], Maren Lübcke[1] and Mathias Stein[1]

[1] HIS-Institute of Higher Education Development (HIS-HE), Germany

gilch@his-he.de, luebcke@his-he.de, stein@his-he.de

Abstract

For some years, universities in Germany and worldwide have increasingly become the target of cyber-attacks, and they are trying to prepare for them through projects and initiatives. The German federal states ("Länder"), which are responsible for the universities, are reacting to this in very different ways. The strategies and approaches of the state governments to support the universities range from “extensive autonomy and self-responsibility for IT and cybersecurity” (autonomy strategy) to a “state-wide strategy and joint financial and organizational support” (network strategy). Most federal states pursue a network strategy, with large states such as Bavaria, North Rhine-Westphalia and Baden-Württemberg having already adopted this approach some time ago and established corresponding programs. Other federal states such as Lower Saxony, Hesse and Rhineland-Palatinate have now also set up state-wide programs to support universities in a network. However, there are some federal states that rely on the independence and self-responsibility of the universities.

The HIS-Institute for Higher Education Development (HIS-HE) has examined the various strategies and approaches in the German ministries of science and higher education. The results of this study supplement the recommendations for dealing with cyber-attacks at universities, which HIS-HE presented at the EUNIS 2024 conference in Athens.

1 Introduction

Since the first known cyber-attacks on universities in Germany in 2019, the number of attacks has grown steadily. These attacks were not only directed at universities, but also at university hospitals, research institutions and libraries. In the latest status report on IT security in Germany, which is

L. Desnos, R. Vogl, L. Merakos, C. Diaz, J. Mincer-Daszkiewicz and S. Mclellan (eds.), EUNIS 2025 (EPiC Series in Computing, vol. 107), pp. 256–261

published annually by the Federal Office for Information Security (BSI), the following is stated across the board: ‘The threat level in the area of cybersecurity remains high’ (BSI, 2024, p.4). For university management, the issue of cybersecurity has now become a central topic. In the current ‘Hochschul-Barometer’ – an annual survey of rectors and presidents of universities in Germany – 53.1% of university leaders rate the risk of cyber-attacks for universities as high and 44.2% as rather high (Stifterverband, 2025, p. 38). However, around 20 percent fewer state that they also perceive this danger for their own university. Furthermore, only half of the university management stated that they have emergency plans for cyber-attacks for at least some university departments (ibid., p. 40).

For a study on crisis management after cyber-attacks (Gilch et. al., 2025), HIS-HE conducted a series of interviews with affected universities. In addition to aspects such as crisis management, communication and rebuilding, the question of support from the federal states was a particular focus of the discussions. In Germany, education and thus the universities are the responsibility of the 16 federal states, which – within the framework of legal regulations and requirements – each pursue their own IT and cybersecurity strategy. The question of responsibility for universities is evident not only at the Länder level but throughout the entire German state cybersecurity architecture. Due to Germany's federal structure, a wide network of actors and initiatives on the topic has formed at the federal, Länder, and municipal levels. According to the online compendium on cybersecurity published in 2020, ‘there are around 2,200 stakeholders and initiatives in Germany [...] that deal with the topic of cybersecurity’ (Federal Ministry of the Interior (BMI), 2020, p.3). However, it is often unclear to what extent they are also responsible for or support universities in the event of a cyber-attack. There is a certain lack of clarity as to how universities are integrated:

- Are they part of the public administration, because they are connected to the administrative network of the Länder and as a public institution under the legal supervision of a ministry?
- Are they worthy of protection as a higher education organisation, as critical infrastructure or – in the broadest sense – as a small or medium-sized enterprise?
- Or are they self-responsible for their (IT) security due to the legally guaranteed freedom of research and teaching?

2 Methodology

For the study, the 16 ministries of science and 14 central Computer Emergency Response Teams (CERTs) were surveyed. CERTs have been established at both state and federal level, with some universities – in particular full and research universities – also setting up their own CERTs (for an overview, cf. https://www.cert-verbund.de/). At the same time, a literature review and desk research were carried out on the subject, with particular reference to the publications and documents of the state parliaments. The feedback from the ministries, the CERTs and the results of the research were analysed using MAXQDA and assigned to thematic main categories. The study focuses on the individual federal states and their activities, programmes and measures for cybersecurity at universities. There is no precise number of cyber-attacks on universities and scientific institutions in Germany. One reason for this is that cyber-attacks are defined differently depending on the context and perspective, and there is no uniform standard for recording them. The Federal Criminal Police Office does regularly publish a ‘Federal Cybercrime Situation Report’ (cf. BKA, 2024), which is based on the Police Crime Statistics (PSK). However, cyber-attacks are categorised as cybercrime in the PSK and are not recorded separately. Furthermore, there is no uniform reporting system for cyber-attacks or cybercrime at universities.

In a response by the federal government to a question in the Bundestag on the topic of 'Cyber-attacks on science and research in Germany,' it is pointed out that 'the recording is not carried out uniformly' (Deutscher Bundestag, 2024, p. 2) and that there are major differences in counting. According to the federal government's response, the Federal Criminal Police Office is aware of 42 cyber-attacks on universities and research institutions for the years 2022 to 2024. In 2022, for example, there were three cyber-attacks on the Fraunhofer-Gesellschaft, six on the Max Planck Society and 1,265 on the Helmholtz Association. The large difference in the figures results from the fact that the determination of a cyber-attack was interpreted differently – 'with damage', as 'successful' or as 'incidents [...] in the course of which a damaging event could theoretically occur' (ibid., p. 2f.). The lack of an overview not only makes it difficult to get a complete picture of the threat to universities in Germany, but it also makes it difficult to clearly distinguish between the motives for cyber-attacks, the consequences or the amount of damage.

3 Cybersecurity at universities –approaches of the federal states

In addition to the national cybersecurity architecture in Germany, the legal framework for universities and their IT security also play a significant role. At the European level, these are in particular the General Data Protection Regulation (GDPR) and the NIS 2 regulation, although the latter has yet to be implemented in Germany. At the federal level, the BSI Act of 2009 and the IT Security Act 2.0 (2021) are particularly noteworthy examples. There are also a number of IT security laws at the state level, although not every federal state has implemented one. Specific IT and cybersecurity laws currently exist in the states of Bade-Wurttemberg (CSG BW), Bavaria (BayDIG), Hesse (HITSiG), Lower Saxony (NDIG), Saarland (IT-SiG SL) and Saxony (SächsISichG). Independently of this, some states also have a cybersecurity strategy – including North Rhine-Westphalia, Bade-Wurttemberg, Bremen and Lower Saxony.

In these strategies and the associated policies of the state governments, universities and science play very different roles in relation to IT and cybersecurity. In the Bremen Cybersecurity Strategy (2023), for example, science appears as a central pillar (ibid., p. 21), but the universities play a role primarily as a place for 'innovative research and development' (ibid., p. 12). In addition, one of the main tasks is to provide education and continuing education to students and staff. The universities do not appear as a separate entity worthy of protection, even if a 'stronger network of universities, business and government agencies' (ibid., p. 53) is sought. According to the state's strategy, vulnerable target groups are more likely to be 'consumers, business and government and administration' (ibid., p. 5). Another example of how a state handles the cybersecurity of its universities is North Rhine-Westphalia. While the city-state of Bremen is home to only three state universities, North Rhine-Westphalia is one of the largest federal states in Germany and has one of the highest numbers of state universities (including 14 universities and 16 universities of applied sciences). In the state's cybersecurity strategy, the universities also appear as a central location for research and development and as an important provider of education and training. However, the universities are specifically named as the recipients of their cybersecurity efforts: 'The state government has made it its goal to actively strengthen the security of North Rhine-Westphalia as a centre of science and research' (Landesregierung Nordrhein-Westfalen, 2021, p. 37). To achieve this, a whole range of programmes have been set up to strengthen the information and cybersecurity of universities in an overarching way. Key elements include the Information Security Agreement (VzI) and the Cybersecurity Agreement (VzC), which are designed in particular to establish minimum IT standards based on the BSI baseline protection. The state universities receive approximately 2.7 million euros per year under the VzI and approximately 4.7 million euros per year under the VzC (https://www.mkw.nrw/themen/wissenschaft/wissenschaftspolitik/cybersicherheit).

Regardless of this, the state government views cybersecurity as a locational factor – for a university as well as for the state as a whole. In this sense, cybersecurity is a basic condition for increasing digitalisation and a ‘success factor’ for attractiveness as a business and science location (Landesregierung Nordrhein-Westfalen, 2021, p. 27).

The example from North Rhine-Westphalia shows an overarching network strategy, i.e. the state government supports its universities in a network. Other federal states focus on the universities' self-responsibility for their own IT and cybersecurity. In this “autonomous” approach, the universities have to independently establish and implement their own IT security within the framework of legal requirements (see for example Landesrechnungshof Brandenburg, 2021). Against the background of the freedom of research and teaching, the ministries provide online limited – if any – specifications or guidelines for comprehensive IT Security. Accordingly, universities must bear the costs for IT Security or, in the event of a cyber-attack, for crisis management with their own funds.

In the feedback from the ministries of science to the HIS-HE survey, it is clear that although cybersecurity is an overarching issue for the ministries, support – whether financial, structural or organisational – is interpreted very differently. This is already evident in the structural anchoring of the topic within the ministries: this ranges from (thematic) responsibility at the overarching ‘department CISO’ or at the ‘ministerial information security officer’ to responsibility in the ‘regular’ department (handled on an event-driven basis as part of day-to-day business) and a dedicated ‘university cybersecurity’ position. A number of federal states now offer financial support programmes for IT security at universities, although these are usually limited in time. Open-ended funding programmes or increases in the basic budget of universities for IT security measures tend to be the exception. A comparison of the measures taken by the federal states reveals a typology of support measures that differ primarily on the basis of two dimensions: The scope (comprehensive support vs. individual measures) and type of implementation (per university, as a centralised offer at state level or as a network model of universities). Most of the federal states' CERTs are also available to universities as points of contact in principle. However, the services of the German National Research and Education Network (DFN) are usually used.

This study focussed on the universities and the federal states in Germany. Most of the offers and programmes of the federal states concentrate on state universities. However, it remains unclear to what extent non-university research institutions -- which have locations in different federal states, for example -- or science-related institutions can also benefit from these programmes. Another open point are transnational university and research cooperations, for example between countries in Europe. This perspective was not the focus of this study; however, it remains to be seen what support and assistance the universities can receive, e.g. from the European Cybersecurity Agency (ENISA) or within the framework of existing organisations such as TF-CSIRT.

4 Summary and further actions

Cybersecurity has become a key issue in Germany – and not just for universities. The federal government and the individual state governments have passed various laws and launched programmes to address the issue. In 2024, the BSI also launched the ‘Cybernation Deutschland’ initiative to increase cyber resilience and ‘make cybersecurity pragmatic and measurable’ (BSI, 2024, p. 8). However, this ‘measurability’ does not yet exist in the higher education sector because there is no uniform definition and no reporting procedure. Nonetheless, the first approaches can be seen in some federal states. The federal states take very different approaches to the topic of cybersecurity at universities, not only in terms of legal requirements, but also with regard to aspects such as (overarching) coordination, (financial) support or the setting of framework conditions and standards. Although the cybersecurity architecture in Germany is comprehensive and detailed, it is often unclear where universities and science fit into it. However, in view of the strained financial situation in the higher education sector, the question of financial support for IT security at universities is becoming increasingly important. The positions of the federal states vary between '(financial and organisational) support in a network' and 'autonomy and personal responsibility'. The latter means that IT security measures and the consequential costs of a cyber-attack must be financed from the existing budget of the university. In view of this, the German Rectors' Conference (HRK) has recently published recommendations for strengthening cybersecurity and called on the new federal government "to provide the necessary financial resources to strengthen the cybersecurity of universities as critical infrastructure." (HRK, 2025, p. 3).

5 References

BSIG – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (2009). https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.). (2024). Die Lage der IT.Sicherheit in Deutschland 2024. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5

Bundeskriminalamt (BKA) (2024). Cybercrime. Bundeslagebild 2023.

Bundesministerium des Innern, für Bau und Heimat (BMI) (Hrsg.). (2020). *Online Kompendium: Cybersicherheit in Deutschland.* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf?__blob=publicationFile&v=9

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) (Hrsg). (2021). Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2021). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#/text/bgbl121s1122.pdf?_ts=1751962121654

Deutscher Bundestag (2024). Drucksache, 20/12259. (2024, 10. Juli). https://dserver.bundestag.de/btd/20/122/2012259.pdf

Gilch, H., Lübcke, M. & Stein, M. (2025). *Crisis management after cyber-attacks. https://eunis.org/wp-content/uploads/2025/01/2024_HIS-HE_Crisis-management-after-cyber-attacks-1.pdf*

Hochschulrektorenkonferenz (HRK) (2025, 05. Februar). *Bund muss bei Cybersicherheit der Hochschulen mehr Verantwortung übernehmen* [Pressemitteilung]. https://www.hrk.de/presse/pressemitteilungen/pressemitteilung/meldung/bund-muss-bei-cybersicherheit-der-hochschulen-mehr-verantwortung-uebernehmen-5104/

Landesregierung Nordrhein-Westfalen (Hrsg.). (2021). *Cybersicherheitsstrategie des Landes Nordrhein-Westfalen.* https://www.cybersicherheit.nrw/de/cybersicherheit-nrw-gemeinsam-voranbringen

Landesrechnungshof Brandenburg (2021). *Jahresbericht 2021.* https://www.lrh-brandenburg.de/media_fast/250/LRH_Brandenburg_Jahresbericht_2021.pdf

Senator für Inneres im Auftrag des Senats der Freien Hansestadt Bremen (Hrsg.). (2023). *Bremische Cybersicherheitsstrategie 2023.* https://www.inneres.bremen.de/sixcms/media.php/13/Bremische Cybersicherheitsstrategie 2023.pdf

Stifterverband für die Deutsche Wissenschaft e. V. (Hrsg.). (2025). Hochschulbarometer. Lage und Entwicklung der Hochschulen aus Sicht Ihrer Leitungen. Ausgabe 2024. https://www.hochschul-barometer.de/

6 Biographies of Authors

Dr. Harald Gilch is senior consultant and project manager in the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. He supports universities in the areas of university organization and management, IT services and benchmarking and has a focus on the digitalization of university administration.
gilch@his-he.de, phone: +49 511 169929-36.
HIS-Institut für Hochschulentwicklung e.V., Goseriede 13a, D-30159 Hannover, Germany, www.his-he.de

Dr. Maren Lübcke is head of the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. Her consulting and research focus at HIS-HE is the digitization of research and teaching at universities. She has worked on various national and international research projects and is author of various publications in this field.
luebcke@his-he.de

Dr. Mathias Stein is consultant and project manager in the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. His focus is on digitalization, cybersecurity and processes in universities administration and with respect to the student life cycle.
stein@his-he.de