Recommendations by the
Standing Committee on
Digitalisation
on 5 February 2025
in Bonn

Threat level increases pressure on the federal government to act: HRK recommendations for strengthening cybersecurity

HRK German Rectors' Conference
The Voice of the Universities

Leipziger Platz 11
10117 Berlin
Tel.: +49 30 206292-0
Fax: +49 30 206292-215
post@hrk.de
www.hrk.de

Ahrstraße 39
53175 Bonn
Tel.: +49 228 887-0
Fax: +49 228 887-110
post@hrk.de
www.hrk.de

The university is paralysed: students and lecturers have no access to learning platforms, researchers and partners in industry fear for their sensitive research results, the university hospital is concerned about its patient data, the administration is worried about the payment of salaries, the financial damage is incalculable.

Such or similar scenarios are a recurring reality in cyberattacks. The threat level for universities is now considered extremely high by the security authorities. In particular, the following potential scenarios can currently be identified: Ransomware attacks, espionage and spying on dissident networks and social movements. Artificial intelligence (AI) is also increasingly being used in these threat scenarios. Cybersecurity is the joint responsibility of the universities, the federal states and the federal government. The HRK makes the following appeals to the federal government:

Avert dangers
In view of the threat situation, the HRK recommends that the federal government take action in line with its overarching role in risk prevention.

This role arises from the international dimension of cybersecurity. There is an area of tension here, as organisations in industry and society also engage in international cooperation with countries that do not share the values of liberal democracies. This also applies to global academic cooperation. Universities are also gateways for attacks, especially for obtaining data on cooperation partnerships, transfer organisations and the entire innovation system. Cyberattacks on universities therefore also jeopardise the competitiveness of the German economy.

On the national level, the federal states in Germany generally have decentralised responsibility for security issues. In view of the threat situation, however, the federal government is also called upon here, as there are cross-state threat situations and the entirety of the German higher education landscape certainly deserves standards that apply in the case of a national critical infrastructure. In addition, it must be the task of the federal government to contribute to the cross-state networking of the relevant universities and university alliances and to provide impetus for this. This applies in particular to the consolidation of concepts and initiatives of the federal states.

Give warning signals and demonstrate possible responses
The federal government must help to improve early warning systems and provide more information for response options. For example, the Federal Office for Information Security (BSI) should offer more university-specific information for emergency planning and services. A nationwide service for detecting security

vulnerabilities also appears necessary. Nationwide simulation games, prevention measures and awareness-raising programmes could also be considered.

The HRK considers it necessary to improve the flow of information between and with the intelligence services and sees a special role for the federal government in this. For example, in the event of an attack, the Federal Office for the Protection of the Constitution must be able to inform the equivalent offices in the federal states and the universities concerned in parallel, which is currently only possible in one state. A structured interplay between incident reporting by universities on the one hand and the provision of information by the services on the other is desirable. However, it should be noted that the intelligence services may not interfere with university autonomy.

Intensify research

The federal government is already funding a wide range of IT security projects.[1] The HRK acknowledges the federal government's research funding on cybersecurity to date and recommends expanding the corresponding programmes. In addition, the federal government should support research projects for new protection and defence technologies, among other things. In addition, the development of new security standards in the EU context must be promoted and programmes for the further development of digital sovereignty must be established.

Reorganise financial responsibility

The role of the federal government in averting danger, the international dimension of cybersecurity, the need for cross-state cooperation and the coordination of specialised service centres mean that the federal government is responsible. The HRK calls for funding with which the federal government combines, completes and consolidates the cybersecurity efforts of the universities and the federal states and also forms an overarching framework for cross-state cooperation. Agile and unbureaucratic funding is needed to increase cybersecurity as quickly and significantly as possible. As measures to increase cybersecurity must also be embedded in the strategies of the universities, funding must also include the relevant efforts and concepts. In view of the threats to education, research and internal security, the HRK is open to innovative solutions and appropriate funding modalities.

[1] Bundesministerium für Bildung und Forschung: Förderprojekte aus dem Bereich Vernetzung und Sicherheit digitaler Systeme, URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte. (4.2.2025)

Appendix: About the creation of the recommendations

These recommendations were prepared by the HRK Standing Committee on Digitalisation. The Committee is headed by the HRK Vice-President for Digitalisation and Academic Continuing Education, Professor Dr Ulrike Tippe. The permanent members of the Committee are Professor Dr Philipp Ahner, Mr Malte Dreyer, Professor Dr Hannes Hartenstein, Professor Dr Wolfram Horstmann, Professor Dr Michael Jäckel, Professor Constanze Langer, Professor Dr Gerhard Lauer, Mr Jens Andreas Meinen, Professor Dr Jörg Müller-Lietzkow, Ms Paula Paschke, Professor Dr Hans Pongratz, Professor Dr Arnd Steinmetz and Professor Dr Jens Weiss. The Committee is supported by Dr Elmar Schultz at the HRK Office.

The starting point for the creation of the recommendations was a Committee hearing on 4 November 2024 on the topic of "Cybersecurity at universities: Balance between resilience, digital sovereignty and openness." Dr Christian Grimm, Professor Dr May-Britt Kallenrode, Mr Oliver Kaczmarek, MdB, Professor Dr Maria Leitner, Dr Florian Rautenberg and Professor Dr Fabian Schmieder were consulted. The results of the consultation were supplemented by a focus round on 18 November 2024, the day before the HRK General Assembly, and by a discussion with Professor Dr Haya Schulmann, Professor Dr Michael Backes and Mr Thomas Franke at the Committee meeting on 28 January 2025. The HRK President and the HRK Executive Board have approved the recommendations.

The HRK would like to thank everyone involved for their contributions.