

14 May 2025**HRK calls for "Cybersecurity alliance for universities"**

The General Assembly of the German Rectors' Conference (HRK) met in Magdeburg on Tuesday to discuss the current extremely high threat situation for universities regarding cybersecurity. Recommendations were adopted for universities, the federal states and the federal government to help ensure IT operations at universities and the safeguarding of particularly sensitive data, even in view of the increased dangers and specific challenges following the so-called turning point in history.

"The cyber risks and threats for universities as large, intensively networked institutions with complex IT infrastructures and a large number of students, employees and cooperation partners accessing them, have recently become much more exacerbated once again, as confirmed by security authorities," explains Prof Dr Walter Rosenthal, President of the German Rectors' Conference (HRK), in Berlin today. "Due to their data from research, teaching, transfer, technology and administration, universities are more prone to cyberattacks with the aim of espionage or sabotage. This is not least because they have access to often highly sensitive data from industry through application-related research and development. What we need now is a broad 'Cybersecurity alliance for universities'," urges Walter Rosenthal.

According to Rosenthal, this alliance needs to bring together, support and consolidate the efforts of universities, federal states and federal government for effective protection against attacks. He adds that this would require a total of €400 million annually at all three levels within the framework of the constitutionally regulated exemption from the debt brake for defence and security spending. Rosenthal calls for such an innovative cooperation and funding model that specifically takes into account the cybersecurity needs of universities to be implemented quickly and led by the Federal Ministry of Research, Technology and Space (BMFTR).

"In its overarching role in national security, the federal government has a special responsibility to also become active in the cybersecurity of universities," explains Prof Dr Ulrike Tippe, HRK Vice-President for Digitalisation and Academic Continuing Education. "This includes improving early warning systems, identifying response options, promoting cross-border communication and ramping up relevant research."

Above all, the HRK member universities call on the federal states to expand cross-university structures, for example for comprehensive data protection. In addition, country-specific reporting channels and contact persons should be named and there should be decisive action to expand continuing education programmes.

But the universities themselves also need to take action: "Modern, forward-looking concepts with multi-level security systems and a triad consisting of preventative measures, differentiated emergency plans and regular crisis exercises are required for resilient IT operations and the necessary information security at universities," says Ulrike Tippe. "Universities also have a major responsibility regarding the ongoing development and teaching of cybersecurity practices. In view of this diverse profile of requirements, a large proportion of the annual funding required for the 'Cybersecurity alliance for universities' must actually be available for local measures."

[View text of the recommendation](#)