Are Croatian universities ready for next level of cyber security?

Croatian Academic and Research Network - CARNET is implementing the e-Universities project with the aim of digital transformation of higher education (HE) by improving the digital teaching infrastructure, introducing digital teaching tools, and strengthening the digital competencies of teachers for teaching in a digital environment.

The digital transformation of public institutions in higher education will be approached systematically.

The challenges of cyber security in HE will continue to grow in the coming years, given the increasing frequency of cyber attacks, including ransomware attacks. National CERTs in CARNET play a key role in cyber security by monitoring the network, providing expert support when an institution is attacked, and providing a vital source of advice and information, both for taking immediate action and monitoring emerging threats. Investments in cyber security are becoming more important, as is the constant effort to stay up-to-date with new cyber security knowledge and advice.

Cybersecurity activities run horizontally through all project elements, network computer infrastructure, service, computer, and education. It is planned to create a methodology and instructions on how to more securely organize the institution's local network, access the institution's information system, management of services and infrastructure, and establish security monitoring of the institution's local network.

So far we have visited all universities in Croatia and held meetings with IT staff, teaching, and management staff.

The project activities aim to improve the cyber security of users, computers, and network infrastructure in HE in Croatia:
1. Improvement of security infrastructure
2. Effective reaction to incidents in the academic community
3. Improving the security of information systems of institutions
4. Content development and training implementation

Planned results:
a. Handbook of reactions to the most common incidents
b. Instructions with best practice examples for creating an information security policy
c. Instructions for increasing the level of security of the university's infrastructure

At the first user conference held in October 2023, National CERT in CARNET presented different topics in cyber security:

Workshops:
What if? Academia Cyber Incident Response - practicing preparedness and response to a cyber incident affecting the academic sector
How did the incident at my university start? - services of National CERT for HE institutions
Interactive presentations:

a) Dad, buy me an NGFW or how to (not) defend your infrastructure - solutions that will contribute to the security of HE institutions
b) Cyber security through play and competition - Gamification has proven to be one of the best ways to learn cyber security

c) Improving the security of information systems of HE institutions - for management staff, for IT staff - the establishment of a security policy ensures that attention is paid to all aspects of information system protection and proves the quality of established security measures

The next steps in security policy area and education are:

1. Establishment of the Security Policy Council with voluntary participation of HE representatives and CARNET staff in charge of security policy. The goal is to exchange experiences and develop approaches to raise awareness of the importance of policies and procedures.
2. Preparation and implementation of student competitions and education of students in cyber security. The goal is to promote IT skills and increase students' interest in careers in the area of cyber security. The competition will be held every year and activities will be carried out throughout the project.
3. Creation of documentation and monitoring system for local network traffic and detection of computer threats for HE institutions.