SECURITY OF CLUSTER SYSTEMS FOR E-LEARNING IN THE CONTEXT OF NIS2

Angel Urilski, Rosen Hristev, Dzhaner Mehmed

Abstract. *This paper examines the main security risks of cluster systems used to enable e-learning platforms, including network attacks, misconfigurations of orchestration platforms, vulnerabilities in virtual machines and container environments, as well as risks arising from the supply chain and third-party integrations. Effective protection strategies are presented, including zero-trust architectures, micro-segmentation, anomaly detection, and disaster recovery plans, which support early detection and mitigation of cyberattacks. Special attention is given to the requirements of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) – the seventh European directive in the field of network and information security. This legislative act requires providers of critical digital services to implement risk management, network and system protection measures, incident management, and service continuity.*

Key words: E-Learning, NIS2, Cybersecurity, Clusterization

Acknowledgments

This paper is partially supported by projects MUPD25-FMI-013 "Innovative Research and Technological Solutions in the Field of ICT" and FP25-FMI-010 "Innovative interdisciplinary research in Informatics, Mathematics, and Pedagogy of Education" of the Scientific Fund of the Paisii Hilendarski University of Plovdiv, Bulgaria.

Angel Urilski[1], Rosen Hristev[1,*], Dzhaner Mehmed[1]
[1] Paisii Hilendarski University of Plovdiv,
Faculty of Mathematics and Informatics,
236 Bulgaria Blvd., 4027 Plovdiv, Bulgaria
Corresponding author: `hristev@uni-plovdiv.bg`