CYBER SECURITY NEWS BULLETIN

January 2024

The Importance of Data Protection and ISO 27701 Accreditation in Albania

Albania takes a further step towards strengthening its information security infrastructure by raising awareness and promoting ISO 27701 certification, bringing together all relevant actors in a meeting. NAECCS, as an important contributor to this process, participated in one of the panels of the meeting organized by the General Directorate of Accreditation, supported by RisiAlbania, a project of the Swiss Agency for Development and Cooperation and implemented by Helvetas Albania.

ISO 27701 is a data privacy standard that builds on ISO 27001, the most widely used international standard for information security management. Certification and Standards, in addition to being a requirement of the EU, create opportunities for growth, outsource services or exports – processes that will create jobs for young people in Albania.

This activity came as a joint effort to foster a safer and more conducive environment for all stakeholders in the ecosystem. The use of ISO 27701 Standards directly affects the development of business with international standards, promoting the increase of information security and business competitiveness in the domestic and foreign markets and bringing our companies closer to the European market.

During the meeting, discussions were held with experts, who represented important actors in the Albanian market. The panelists, including Blerina Qazimin, Besa Stringën, Sokol Avxhiun, Saimir Kapllani, Alfons Muça, Nikolin Metaj and Raffaelle Regni, shared their knowledge on critical topics such as the need for accredited certifications for standards 27701, 27017 and 2701.

Military Cyber Security Unit Inauguration

A very good news in the field of cyber defense for Albania is the opening of the Cyber Attack Response Center (CCARC) at the Ministry of Defense. This center was made possible with the support of the American government and shows that we take a step further in deepening the strategic partnership, deepening cooperation in increasing security in information systems.

The new center will play a key role in responding to cyberattacks against IT infrastructure in the field of defense and will serve to increase the level of cyber security in the country.
NAECCS, as the Authority responsible for civil information infrastructures, is in continuous cooperation with the Ministry of Defense within the framework of increasing the level of cyber security in Albania.

CYBER SECURITY NEWS BULLETIN

January 2024

NAECCS holds a meeting with Financial Institutions

The cyber events in which Albania is going through recently, gathered at a discussion table on January 23, 2024, NAECCS and the senior leaders of the institutions of the financial sector.

At the meeting, the National Coordinator for Cyber Security, Mr. Igli Tafa emphasized the importance of the role of investments in this sector of critical infrastructures for increasing cyber security. The attendees got acquainted with the necessity of strengthening and cyber protection of institutions by focusing on several steps:

Investments in Technology – the need to use the latest cyber defense technologies to protect customer information and data.
Operational Measures – raising the daily security standards of the institution from the operational and administrative side according to NIST or ISO 27001 references.

Managerial Level – the role of leadership in the obligation of the institution to invest in raising the awareness of the staff in the framework of cyber security, in determining the budget in the field of cyber security as well as in determining the cyber risk on an ongoing basis.

Increase of Capacities – Investment in the professional growth of experts and the coverage of identified vacancies in the field of cyber security.

The meeting emphasized the need to increase cooperation between NAECCS and the financial sector to share as much information as possible and to take appropriate measures, at the right time, that ensure a safe cyber ecosystem. The need for a continuous and active approach, in concrete cooperation, to address cyber challenges in the future was emphasized there.
NAECCS requested that the financial sector coordinate the work with concrete actions for the implementation of increased security measures for 2024.

HPE - data breach

Hackers with links to the Kremlin are suspected to have infiltrated information technology company Hewlett Packard Enterprise's (HPE) cloud email environment to exfiltrate mailbox data.

The threat actor accessed and extracted data starting in May 2023 from a small percentage of maliboxes belonging to individuals in cybersecurity, businesses, etc.
HPE, however, emphasized that the incident has not had any material impact on its operations to date.

Read more

PATCHING ALERT

GitLab - patching alert

GitLab has recently released security updates to address two critical vulnerabilities.
One of the critical vulnerabilities is the result of a bug in the email verification process, which allows users to reset their password through a secondary email address.

To mitigate any potential threats, it is advised to upgrade instances to a patched version as soon as possible and enable 2FA, especially for high-privileged users.

Read more