AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

WEEKLY BULLETIN
4-8 MARCH 2024

Quote of the week

> *"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public."*
>
> ***Clay Shirky***

Content:

Albania – active role in the discussions of the United Nations on Cyber Security

On March 4-8, the US State Department held the 7th Substantive Session of the OEWG, in New York.
In this important national commitment, the Albanian delegation has played an active role and has made an inherent contribution. NAECCS is part of this delegation through the deputy general director, Mrs. Floretta Faber. Her participation in the next section was supported by the US Department of State, Bureau of Cyberspace and Digital Policy (CDP), as part of the empowerment of women in cybersecurity issues at the OEWG.

In the section that focused on the ways and needs for increasing capacities, Mrs. Faber presented that Albania is committed to developing a strong education and training ecosystem for cyber security. This commitment will be embodied in the creation of the National Cyber Security Academy (NCSA), an initiative designed to prepare the next generation of cyber security experts for Albania. She presented the platform that will enable training of experts in the cyber field in the public and private sectors. She also presented the work that has already begun for the protection of children online.

International cooperation remains a cornerstone of Albania's approach to strengthening cyber security capacities. Our country's active involvement in international forums reflects a multidimensional effort to improve national and regional cyber resilience.

Always being fully aligned with international best practices and strengthening cooperation, Albania is positioning itself as a key player in global efforts to provide a safe and sustainable digital ecosystem for all.

CYBER ZERO
BUILDING A PROTECTIVE SHIELD THROUGH COOPERATION TO SAFEGUARD THE CRITICAL INFRASTRUCTURE SECURITY IN THE WESTERN BALKANS
LUANDA DOMI
LULËZON JAGXHIU
SAIMIR KAPLLANI
ALEKSANDAR ACEV
RIFAT HYSENI
ANITA NIKOVA

NAECCS supports regional cooperation in response to cyber attacks

NAECCS participated in the Regional Cyber Security Conference, "Cyber Zero", which was held in Pristina, on March 4 and 5. This conference highlighted the importance of regional cooperation in protecting critical infrastructures against growing cyber threats in the Western Balkans region.

During the panel "Building a protective shield for critical infrastructures in the Western Balkans through cooperation", Mr. Saimir Kapllani, Director of Compliance, Risk and Control Analysis at NAECCS, shed light on the challenges that our region faces in the field of cyber security . He emphasized the vital importance of expanding cooperation on data sharing on cyber threats, increasing the capacities of regional experts through joint training initiatives, and the necessity of strengthening public and private partnerships in the research and academic sectors. Mr. Kapllani also underlined the need for strategic investments in advanced technologies that will help in efficient monitoring and management of cyber incidents.

This meeting was a platform to build stronger regional relations and define future courses of action for a safer Western Balkans in cyberspace. NAECCS continues to be committed to taking concrete steps towards closer regional and international cooperation, sharing responsibilities and joining forces to face cyber security challenges.

WEEKLY BULLETIN
4-8 MARCH 2024

Quote of the week

> *"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public."*
>
> ***Clay Shirky***

Content:

Using WordPress to hack other sites

Cybercriminals are using compromised WordPress websites to form a massive army for credential attacks. Researchers have discovered a campaign where attackers install a script in HTML templates, forcing visitors to visit a different WordPress website and try to log in using different combinations of usernames and passwords. Once the victim cracks the passcode, they transmit the information to the attackers, who then send further instructions. Over 1,700 websites host this script, providing a large pool of users who will be unwittingly recruited into this distributed bruteforce army.

Link: Read more

Social media platforms Instagram and Facebook faced global outages

Facebook and Instagram users around the world have logged out and are having trouble logging in, with users receiving incorrect passwords. The outage of these apps affected users in the US, Europe and Asia. Meta, a website that tracks internet service outages, has received reports suggesting that the issue is not isolated to a particular region or country. Meta confirmed the outage and is working to resolve it. Meta services were brought back online, but the cause of the outage remains unknown.

Link: Read more

American Express - Data Breach

American Express is warning customers that their credit cards were exposed in a third-party data breach after a merchant processor was hacked. The breach affected American Express Card member data, including account numbers, names and expiration data. American Express advises customers to review their account statements and report suspicious activity, enable instant notifications through the mobile app and consider requesting a new card number if their card information has been stolen.

Link: Read more

PATCHING ALERT

JetBrains - Patching alert

The US Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability to JetBrains TeamCity, a build management and continuous integration server. The vulnerability, with a severity score of 9.8 out of 10, allows attackers to bypass login and perform administrator actions. The vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to federal enterprises. JetBrains has released an update to TeamCity asking users to install it. The update also fixes another high-risk vulnerability, allowing malicious actors to perform limited administrator actions by bypassing authentication checks on the server.

Link:Read more