CYBER SECURITY NEWS BULLETIN

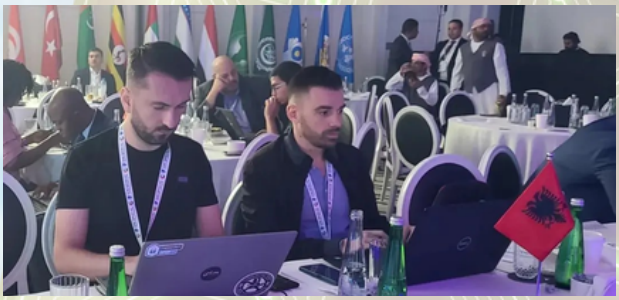
October 2023

Content:

Security Policies and Crisis Management for the Health Sector.

In the framework of the trainings that will be organized by NAECCS for the period October-December 2023, on October 11-12, the training on "Cyber Security Policies and Crisis Management" for the Health Sectors took place.

During this two-day training, presentations were made regarding Legislation, Strategy, Policies and Cyber Governance needs, as well as 3 Table Top Exercises for the management of Cyber incidents and crises, Simulating a "Phishing" attack as well as an infection scenario case from Malware, a Cyber Drill was also organized where there were concrete exercises on incident management. During the discussions, the importance of improving coordination, cooperation and information exchange on the analytical and reaction capacities of the health sector entities related to cyber security incidents was emphasized.



AKCESK participates in Cyber Week Regional training

By invitation of the United Arab Emirates, NAECCS participated in Cyber Week Regional. In the first two days, a cyber drill Cyber Drill excercise was organized where there were representatives from 70 nations.

The representatives of NAECCS represented Albania decently and were classified as follows:

Scenario 1 - Hacked and Crypto Mining Web Apps Analysis Log: First place out of 30 participating countries

Scenario 2 – Defense Tactics for Cyber Security (12th Place);
Scenario 3 – DFIR (9th place);
Scenario 4 – Cyber threat intelligence (there were no classifications);
Scenario 5 – CPX Ransomware Technical (11th place) ;
Scenario 6 - CPX Ransomware MAnagement (there were no classifications);
Scenario 7 - Threat Emulation Lead (8th Place);
Scenario 8 – OSINT (5th Place);

The project "Trusted flaggers for a safe Cyber Ecosystem Against Violent Extremism" is finalized

The project "Trusted flaggers for a safe cyber ecosystem against violent extremism" was successfully completed yesterday, organized by the Academy of Political Studies (ASP) in cooperation with the National Authority for Electronic Certification and Cyber Security (AKCESK) with the support of the Embassy of the United States of America in Tirana.

About 20 participants benefited from knowledge in the cycle of the Academy of Trusted flaggers, from the best local and foreign experts. AKCESK and other state institutions offered internships and dedicated training in the field of cyber security.

Trusted flaggers also took part in the competition to monitor illegal content online for a period of 4 months (April – July 2023), on social media and Youtube, where the flagger with the most reports was offered a full certification scholarship in Data Science, in coding or cybersecurity profile at Academy Coding Dojo inc.

AKCESK, guaranteed the further continuation of training and professional cooperation with the network of Trusted Signalers, to guarantee a better and safer internet for children and young people in Albania

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

CYBER SECURITY NEWS BULLETIN

October 2023

Content:

National Authority for Electronic Certification and Cyber Security organizes preparatory training together with the Albanian National SOC

Ransomware attacks, data leak, privilege escalation and other incidents are the responsibility of a further challenge for organizations and not only.

NAECCS, within the framework of the protection of all Critical and Important Information Infrastructures, regularly conducts preparatory exercises and simulations of attacks together with the Albanian National SOC, to increase the response in case of incidents, as well as cyber security monitoring through efficient SIEM or Threat Intel platforms.

The staff is constantly introduced to the latest techniques that hackers use to break into security systems or by bypassing the protections of various monitoring systems, through Table Top Exercise presentations about Social Engineering, Ransomware and Leak Data as well as through Cyber Drill.

Over 17,000 WordPress websites compromised by Balada Injector

More than 17,000 WordPress websites were recently compromised with a malware known as Balada Injector.

9,000 of these websites are believed to have been infiltrated using a recently discovered vulnerability identified as: CVE 2023-3169 which can be exploited by unauthenticated users to perform XSS (cross-site scripting) attacks.

Read more

Google Chrome - patching alert

Google recently released Chrome 118 with updates for 20 vulnerabilities, including a critical vulnerability.

The Internet giant does not mention any of these vulnerabilities being exploited in malicious attacks.
The updated version of Chrome is 118.0.5993.70 for macOS and Linux, and as version 118.0.5993.70/.71 for Windows.

AKCESK advises all Google users to perform the necessary updates.

Read more

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039