

WEEKLY BULLETIN

18-22 DECEMBER 2023



Quote

"To competently perform rectifying security service, two critical incident response elements are necessary: information and organization."

Robert Davis

of the week

Content:

- "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police.

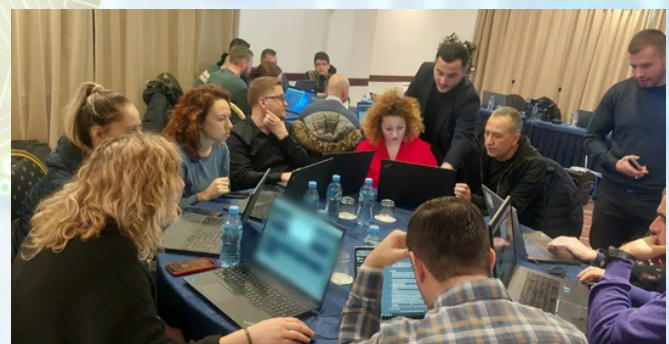
"Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police.

In continuation of NAECCS objective of increasing capacities as one of the main pillars for the protection of information infrastructures with the support of our partner Risi Albania/Helvetas and the valuable contribution of the Authority's experts, on December 20, 21, 22, was organized the anticipated training on "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, National Agency of Information Society and the State Police.

For the very importance that these sectors have in terms of the information infrastructures they manage, during this three-day training, presentations were made regarding the legal framework, strategy, policies, the necessary security measures that must be taken by the information infrastructures and the needs for cyber governance.

An important part of this training was the development of three different TTX scenarios for cyber incident management. Also, 2 days of cyber training (Cyber Drill) were held with concrete exercises on cyber incident management, via the FISA.al platform.

In fulfillment of the objectives to achieve international standards in the field of cyber security, NAECCS will continue to organize training for all sectors that administer critical and important information infrastructures in order to build a sustainable cyber ecosystem in Albania.



WEEKLY BULLETIN

18-22 DECEMBER 2023



Quote

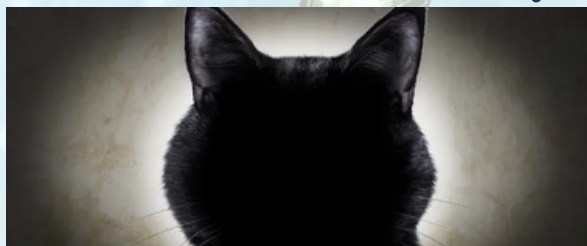
"To competently perform rectifying security service, two critical incident response elements are necessary: information and organization."

Robert Davis

of the week

Content:

- FBI develops decryptor for BlackCat ransomware
- Xfinity - data breach
- A new phishing attack steals Instagram backup codes
- Google - patching alert



FBI develops decryptor for BlackCat ransomware

The FBI has created a decryption tool for ransomware used by the gang known as BlackCat or AlphV, as part of a wider campaign against cyber attackers

The existence of the decryptor was revealed from the United States Department of Justice which reports that the FBI has provided the decryptor to over 500 organizations that were attacked making it possible to avoid paying the ransom.

[Read more](#)

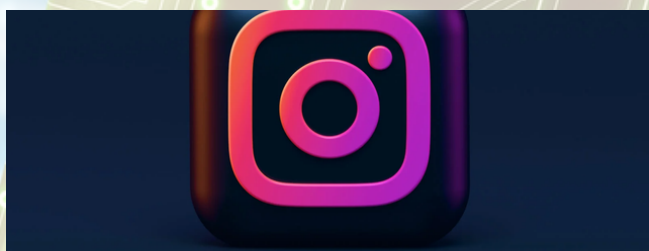


Xfinity - data breach

Telecommunications company Xfinity has recently revealed that cyber attackers who breached one of its Citrix servers also stole sensitive customer information from its systems affecting 35,879,455 people.

Xfinity has asked users to reset their passwords and enable two- or multi-factor authentication to protect affected accounts.

[Read more](#)



A new phishing attack steals Instagram backup codes

A new phishing campaign pretending to be a "copyright infringement" email attempts to steal Instagram users' backup codes, allowing hackers to bypass the two-factor authentication configured on the account.

The latest phishing emails impersonate Meta, Instagram's parent company, warning that Instagram users received copyright infringement complaints. The email then prompts the user to fill out an appeal form to resolve the issue.

[Read more](#)

PATCHING ALERT



Google - patching alert

Google has released an emergency update to address a new zero-day vulnerability, identified as CVE-2023-7024, in the Chrome browser.

The vulnerability has been addressed with the release of version 120.0.6099.129 for Mac, Linux and 120.0.6099.129/130 for Windows, which will be released in the coming days/weeks.

[Read more](#)