Ukraine in cyberspace, 1 year after



Russian war in Ukraine is the first example of a full-scale cyber war. A dramatic increase in the number of cyberattacks and critical cyber incidents was observed in Ukraine in 2022 compared to previous years. Most of the attacks were targeted at state entities and critical infrastructure and were conducted by the special services of the russian federation, particularly the FSB and GRU APT groups. The goal of the attacks was to destroy Ukraine and cause maximum suffering to its people. No other country in the whole world has faced such massive attacks aimed at wiping out IT infrastructure. Various types of attacks were performed, including DDoS, website defacing, data theft, and the use of wipers. The cyberattacks were combined with psychological information operations and were often accompanied by kinetic attacks. However, despite the ongoing cyber aggression, Ukraine has developed protocols, algorithms, techniques, and tools to counter cyberattacks and has successfully learned to use them even under constant missile shelling and cyber pressure.

Intervento a cura di: **Ivan Kalabashkin**, *Deputy Head of the Directorate, Security Service of Ukraine*

La partecipazione all'evento è gratuita previa registrazione online al seguente link:
https://www.ictsecuritymagazine.com/eventi/-cybercrimeconference2023

I posti sono limitati, potrà partecipare alla conferenza esclusivamente chi ha ricevuto il biglietto di ingresso a seguito dell'iscrizione.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/ukraine-in-cybersp

ace-1-year-after/