With war next door, EU is warned on cybersecurity gaps

March 29 2022

Credit: Pixabay/CC0 Public Domain

As Russia's invasion of Ukraine accelerates European Union defense cooperation, a watchdog said Tuesday that EU institutions face vulnerabilities on another front: cybersecurity.

The warning by the European Court of Auditors covers the wide range of EU bodies—from the executive arm based in Brussels to specialist agencies located across Europe—that run the 27-nation bloc's day-to-day business.

"The EU must step up its efforts to protect its own organizations," Bettina Jakobsen, a member of the ECA, said in a statement accompanying a special report on cyberthreats. "Such attacks can have significant political implications."

Cyberattacks against EU bodies are increasing "sharply," with major incidents jumping more than tenfold between 2018 and 2021, according to the Luxembourg-based ECA.

Cybersecurity has jumped up the political agenda in Europe following attacks in recent years that targeted EU nations such as Germany and other industrialized countries including the United States, Britain and Australia.

In 2020, the EU imposed cyber sanctions for the first time, blacklisting a number of Russian, Chinese and North Korean hackers.

Nonetheless, the European auditors said Tuesday that EU organizations were failing to enact some "essential" cybersecurity controls and underspending in this area. The auditors also alleged a lack of "systematic" cybersecurity training and information sharing.

EU entities as a whole handle political, diplomatic, financial, economic and regulatory matters. The spectrum of activities underpins the bloc's status as a geopolitical force, a global setter of industrial rules and the world's most lucrative single market.

The sensitive information processed by EU bodies makes them attractive

targets for hackers, according to the report, which said the risks have grown as a result of remote working prompted by the COVID-19 pandemic.

"This has considerably increased the number of potential access points for attackers," the ECA said.

It said a "particularly concerning trend is the dramatic increase in significant incidents," which are described as attacks that involve the use of new methods and technologies and that can take weeks or even months to investigate and resolve.

One example cited is a high-profile cyberattack on the European Medicines Agency in late 2020, when the EU was pushing to authorize the first COVID-19 vaccines.

"Sensitive data was leaked and manipulated in a way designed to undermine trust in vaccines," the ECA said.

Because the EU's organizations are strongly interconnected, a vulnerability anywhere could have a cascading effect, it said.

"A weakness in one can expose others to security threats," said the ECA.

It recommended the EU draw up legislation that would set common binding rules on cybersecurity for all the bloc's institutions.

The auditors also urged more resources to support the Computer Emergency Response Team of EU bodies, or CERT-EU, saying "its effectiveness is compromised by an increasing workload, unstable funding and staffing, and insufficient cooperation from some" of the bloc's organizations.

In sum, according to the ECA, the network of EU institutions "has not achieved a level of cyber-preparedness commensurate with the threats."

Citation: With war next door, EU is warned on cybersecurity gaps (2022, March 29) retrieved 26 April 2024 from https://techxplore.com/news/2022-03-war-door-eu-cybersecurity-gaps.html