EUROPEAN COURT OF AUDITORS

EN

Press Release

Luxembourg, 29 March 2022

EU bodies must step up their cybersecurity preparedness

The number of cyberattacks on EU bodies is increasing sharply. The level of cybersecurity preparedness within EU bodies varies and is overall not commensurate with the growing threats. Since EU bodies are strongly interconnected, a weakness in one can expose others to security threats. This is the conclusion of a special report by the European Court of Auditors which examines how prepared the EU's governing entities are against cyber threats. The auditors recommend that binding cybersecurity rules should be introduced, and the amount of resources available to the Computer Emergency Response Team (CERT-EU) should be increased. The European Commission should also promote further cooperation among EU bodies, the auditors say, while CERT-EU and the European Union Agency for Cybersecurity should increase their focus on those EU bodies that have less experience in managing cybersecurity.

Significant cybersecurity incidents in EU bodies increased more than tenfold between 2018 and 2021; remote working has considerably increased the number of potential access points for attackers. Significant incidents are generally caused by complex cyberattacks that typically involve the use of new methods and technologies, and can take weeks if not months to investigate and recover from. One example was the cyberattack on the European Medicines Agency, where sensitive data was leaked and manipulated to undermine trust in vaccines.

"*EU institutions, bodies and agencies are attractive targets for potential attackers, particularly groups capable of executing highly sophisticated stealth attacks for cyber-espionage and other nefarious purposes*", said Bettina Jakobsen, the ECA member who led the audit. "*Such attacks can have significant political implications, harm the overall reputation of the EU, and undermine trust in its institutions. The EU must step up its efforts to protect its own organisations.*"

The main finding of the auditors was that EU institutions, bodies and agencies are not always well protected against cyber threats. They do not approach cybersecurity consistently, essential controls and key cybersecurity good practices are not always in place, and cybersecurity training is not systematically provided. The allocation of resources to cybersecurity varies widely, and a number of EU bodies are spending considerably less than comparable peers. Although differences in cybersecurity levels could theoretically be justified by the different risk profiles of each organisation and the varying sensitivity levels of the data they handle, the auditors stress that cybersecurity weaknesses in a single EU body can expose several other organisations to

The purpose of this press release is to convey the main messages of the European Court of Auditors' special report. The full report is available at eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

cybersecurity threats (EU bodies are all connected to each other, and often to public and private organisations in Member States).

The Computer Emergency Response Team (CERT-EU) and the European Union Agency for Cybersecurity (ENISA) are the EU's two main entities tasked with providing support on cybersecurity. However, they have not been able to provide EU bodies with all the support they need, due to resource constraints or priority being given to other areas. Information sharing is also a shortcoming, the auditors say: for instance, not all EU bodies carry out timely reporting on vulnerabilities and significant cybersecurity incidents that have impacted them and may impact others.

Background information

Currently, there is no legal framework for information security and cybersecurity in EU institutions, agencies and bodies. They are not subject to the broadest EU legislation on cybersecurity, the 2016 NIS directive, or to its proposed revision, the NIS2 directive. There is also no comprehensive information on the amount spent by EU bodies on cybersecurity. The common rules on information security and on cybersecurity for all EU bodies are included in the communication on the EU Security Union Strategy for the 2020-2025 period, published by the Commission in July 2020. In the EU Cybersecurity Strategy for the Digital Decade, published in December 2020, the Commission undertook to propose a regulation on common cybersecurity rules for all EU bodies. It also proposed the establishment of a new legal basis for CERT-EU to reinforce its mandate and funding.

Special report 05/2022, "*Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats*", is available on the ECA website. The ECA pointed to the challenges to effective EU cybersecurity policy also in a 2019 review.

Press contact

ECA press office: press@eca.europa.eu

- Claudia Spiti : claudia.spiti@eca.europa.eu - M: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu - M: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu - M: (+352) 621 552 224