DEN EUROPÆISKE REVISIONSRET

DA

Pressemeddelelse

Luxembourg, den 29. marts 2022

EU's organer skal øge deres cybersikkerhedsberedskab

Antallet af cyberangreb på EU's organer er kraftigt stigende. Der er store forskelle på EU-organernes beredskabsniveau, når det gælder cybersikkerhed, og samlet set står det ikke mål med de voksende trusler. Da EU's organer er tæt forbundne, kan en svaghed i ét af dem udsætte de andre for sikkerhedstrusler. Sådan lyder konklusionen i en særberetning fra Den Europæiske Revisionsret, der undersøger, hvor godt EU's forvaltningsenheder er rustet mod cybertrusler. EU-revisorerne anbefaler, at der indføres bindende cybersikkerhedsregler, og at IT-Beredskabsenheden (CERT-EU) får flere ressourcer. Revisorerne mener endvidere, at Europa-Kommissionen bør fremme yderligere samarbejde mellem EU-organerne, mens CERT-EU og Den Europæiske Unions Agentur for Cybersikkerhed bør øge deres fokus på EU-organer med mindre erfaring inden for cybersikkerhedsforvaltning.

Mellem 2018 og 2021 skete der en tidobling af de væsentlige cybersikkerhedshændelser i EU's organer, bl.a. fordi brugen af fjernarbejde i betydelig grad har øget antallet af potentielle adgangspunkter for angribere. Væsentlige hændelser forårsages som regel af komplekse cyberangreb, der typisk indebærer anvendelse af nye metoder og teknologier, og det kan tage uger, hvis ikke måneder, at efterforske dem og genoprette systemerne efter deres indtræffelse. Et eksempel herpå var cyberangrebet på Det Europæiske Lægemiddelagentur, hvor følsomme data blev lækket og manipuleret for at undergrave tilliden til vacciner.

"EU's institutioner, organer og agenturer er attraktive mål for potentielle angribere, navnlig grupper, der er i stand til at udføre meget avancerede hemmelige angreb med cyberspionage eller andre ondsindede formål for øje," siger Bettina Jakobsen, det medlem af Revisionsretten, der ledte revisionsarbejdet. *"Sådanne angreb kan have betydelige politiske konsekvenser og kan skade EU's generelle omdømme og undergrave tilliden til EU's institutioner. EU skal øge sin indsats for at beskytte sine egne organisationer."*

Revisorernes vigtigste konklusion er, at EU's institutioner, organer og agenturer ikke altid er godt beskyttet mod cybertrusler. De har ikke en ensartet tilgang til cybersikkerhed, de har ikke altid indført væsentlige kontroller og gode centrale praksis på cybersikkerhedsområdet, og de tilbyder ikke systematisk uddannelseskurser i cybersikkerhed. Ressourcetildelingen på cybersikkerhedsområdet varierer meget, og en række EU-organer bruger betydeligt mindre på området end andre tilsvarende organer. EU-organernes forskellige cybersikkerhedsniveauer kunne

Formålet med denne pressemeddelelse er at gengive hovedbudskaberne i Den Europæiske Revisionsrets særberetning. Beretningen i sin helhed kan fås på eca.europa.eu.

ECA Press

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

teoretisk set begrundes med, at de enkelte organisationer har forskellige risikoprofiler og håndterer data med forskellige følsomhedsniveauer, men revisorerne understreger, at cybersikkerhedssvagheder i et enkelt EU-organ kan udsætte adskillige andre organisationer for cybersikkerhedstrusler (EU's organer er alle tæt forbundne med hinanden og ofte også med offentlige og private organisationer i medlemsstaterne).

IT-Beredskabsenheden (CERT-EU) og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) er EU's to hovedenheder med ansvar for at yde støtte på cybersikkerhedsområdet. På grund af ressourcemæssige begrænsninger og prioritering af andre områder har de dog ikke været i stand til at yde EU-organerne al den støtte, de har brug for. Desuden er informationsudvekslingen også mangelfuld, siger revisorerne. For eksempel er det ikke alle EU-organer, der rapporterer rettidigt om de sårbarheder og væsentlige cybersikkerhedshændelser, som har påvirket dem og kan påvirke de andre.

Baggrundsoplysninger

I øjeblikket findes der ingen retlige rammer for informationssikkerhed og cybersikkerhed i EU's institutioner, organer og agenturer. De er ikke omfattet af den bredeste EU-lovgivning om cybersikkerhed, NIS-direktivet fra 2016, og heller ikke af den foreslåede revision heraf, dvs. NIS2-direktivet. Der foreligger heller ingen dækkende information om det beløb, EU's organer bruger på cybersikkerhed. Fælles regler om informationssikkerhed og cybersikkerhed for alle EU-organer er omtalt i Kommissionens meddelelse om strategien for EU's sikkerhedsunion for perioden 2020-2025 (offentliggjort i juli 2020). I EU's strategi for cybersikkerhed for det digitale årti, der blev udsendt i december 2020, forpligtede Kommissionen sig til at foreslå en forordning om fælles cybersikkerhedsregler for alle EU's organer. Den foreslog også at etablere et nyt retsgrundlag for CERT-EU for at styrke enhedens mandat og finansiering.

Særberetning nr. 05/2022 "*Cybersikkerhed i EU's institutioner, organer og agenturer: Beredskabsniveauet står samlet set ikke mål med truslerne*" kan fås på Revisionsrettens websted. Revisionsretten har også beskrevet udfordringerne vedrørende EU's cybersikkerhedspolitik i en analyse fra 2019.

Pressekontakt

Revisionsrettens pressekontor: 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