EUROPEISKA REVISIONSRÄTTEN

SV

Pressmeddelande

Luxemburg den 29 mars 2022

EU:s organ måste höja beredskapen mot cyberhot

Antalet cyberattacker mot EU:s organ ökar kraftigt. Cybersäkerhetsberedskapen inom EU-organen varierar och står inte alltid i proportion till de allt större hoten. Eftersom EU:s olika organ är tätt sammanlänkade kan svagheter hos ett av dem innebära säkerhetshot även för andra. Detta är slutsatsen i en särskild rapport från Europeiska revisionsrätten där man har undersökt hur väl förberedda EU:s styrande organ är på cyberhot. EU-revisorerna rekommenderar att man inför bindande cybersäkerhetsregler och ökar resurserna till incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU). Revisorerna menar också att Europeiska kommissionen bör främja ytterligare samarbete mellan EU:s organ samt att CERT-EU och Europeiska unionens cybersäkerhetsbyrå bör fokusera mer på de EU-organ som har minst erfarenhet av att hantera cybersäkerhet.

Antalet betydande cybersäkerhetsincidenter vid EU:s organ mer än tiodubblades under perioden 2018–2021, och till följd av distansarbete har antalet potentiella åtkomstpunkter för angripare ökat rejält. Betydande incidenter orsakas vanligtvis av komplicerade cyberattacker där nya metoder och tekniker används, och de kan ta veckor eller till och med månader att utreda och återställa. Ett exempel är cyberattacken mot Europeiska läkemedelsmyndigheten där känsliga uppgifter läcktes och manipulerades i syfte att undergräva förtroendet för vacciner.

”*EU:s institutioner, organ och byråer är attraktiva mål för potentiella angripare och framför allt för grupper som är kapabla att utföra mycket sofistikerade smygattacker som syftar till cyberspionage och andra skadliga hot*”, säger Bettina Jakobsen, den ledamot av revisionsrätten som ledde revisionen. ”*Sådana attacker kan få betydande politiska konsekvenser, skada EU:s allmänna rykte och undergräva förtroendet för EU:s institutioner. EU måste öka insatserna för att skydda sina egna institutioner.*”

Revisorernas viktigaste slutsatser var att EU:s institutioner, organ och byråer inte alltid är väl skyddade mot cyberhot. Till exempel har de inga enhetliga strategier för cybersäkerhet, de tillämpar inte alltid viktiga kontroller och god cybersäkerhetspraxis och de tillhandahåller ingen systematisk utbildning i cybersäkerhet. Det finns stora skillnader när det gäller hur mycket resurser som avsätts till cybersäkerhet, och några EU-organ avsätter betydligt mindre medel än andra jämbördiga organ. Skillnaderna i cybersäkerhetsnivå skulle visserligen i teorin kunna motiveras av att de olika organisationerna har olika riskprofiler och hanterar uppgifter som är olika känsliga.

Avsikten med detta pressmeddelande är att presentera huvudbudskapen i Europeiska revisionsrättens särskilda rapport. Hela rapporten finns på eca.europa.eu.

ECA Press

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

Men revisorerna betonar att svagheter i cybersäkerheten hos ett enskilt EU-organ kan innebära cybersäkerhetshot även för flera andra, eftersom alla EU:s organ är tätt sammanlänkade med varandra och ofta även med offentliga och privata organisationer i medlemsstaterna.

Incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU) och Europeiska unionens cybersäkerhetsbyrå (Enisa) är de två huvudsakliga EU-enheter som har i uppdrag att ge stöd kring cybersäkerhet. På grund av begränsade resurser och det faktum att andra områden har prioriterats har de dock inte kunnat ge EU-organen allt det stöd de behöver. Informationsutbytet har också varit bristfälligt enligt revisorerna. Till exempel är inte alla EU-organ snabba med att rapportera sårbarheter och betydande cybersäkerhetsincidenter som har påverkat dem och kan komma att påverka andra.

Bakgrundsinformation

Det finns för närvarande ingen rättslig ram för informationssäkerhet och cybersäkerhet vid EU:s institutioner, organ och byråer. De omfattas inte av den bredaste EU-lagstiftningen om cybersäkerhet, det vill säga nätverks- och informationssäkerhetsdirektivet från 2016, eller av den föreslagna revideringen av detta direktiv. Det finns inte heller någon heltäckande information om hur stora belopp EU:s organ avsätter till cybersäkerhet. De gemensamma reglerna om informationssäkerhet och cybersäkerhet för samtliga EU-organ finns med i det meddelande om strategin för EU:s säkerhetsunion för perioden 2020–2025 som kommissionen offentliggjorde i juli 2020. I EU:s strategi för cybersäkerhet för ett digitalt decennium, som offentliggjordes i december 2020, åtog sig kommissionen att föreslå en förordning om gemensamma cybersäkerhetsregler för alla EU-organ. Kommissionen föreslog även att en ny rättslig grund skulle fastställas för CERT-EU för att stärka dess mandat och finansiering.

Särskild rapport 05/2022 *Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapen står inte alltid i proportion till hoten* finns på revisionsrättens webbplats. Revisionsrätten har tidigare pekat på de utmaningar som finns för en ändamålsenlig EU-politik för cybersäkerhet i en översikt som offentliggjordes 2019.

Presskontakt

Revisionsrättens presstjänst: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – M: +352 691553547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – M: +352 691551502
- Damijan Fišer: damijan.fiser@eca.europa.eu – M: +352 621552224