EUROPESE REKENKAMER

NL

Persbericht

Luxemburg, 29 maart 2022

EU-organen moeten hun paraatheid op het gebied van cyberbeveiliging opvoeren

Het aantal tegen de EU-organen gerichte cyberaanvallen neemt fors toe. Het paraatheidsniveau op het gebied van cyberbeveiliging binnen de EU-organen loopt uiteen en staat over het algemeen niet in verhouding tot de toenemende dreigingen. Aangezien EU-organen onderling nauw verweven zijn, kan een tekortkoming bij een van de organen andere aan beveiligingsdreigingen blootstellen. Dit is de conclusie van een speciaal verslag van de Europese Rekenkamer waarin wordt onderzocht in welke mate de bestuursorganen van de EU op cyberdreigingen zijn voorbereid. De auditors bevelen aan om bindende regels inzake cyberbeveiliging in te voeren en de middelen die beschikbaar zijn voor het computercrisisresponsteam (CERT-EU) te verhogen. Volgens de auditors moet de Europese Commissie ook verdere samenwerking tussen EU-organen bevorderen en moeten CERT-EU en het Agentschap van de Europese Unie voor cyberbeveiliging zich meer richten op de EU-organen die minder ervaring hebben met cyberbeveiligingsbeheer.

Tussen 2018 en 2021 is het aantal significante cyberincidenten bij EU-organen meer dan vertienvoudigd, terwijl telewerken heeft geleid tot een forse toename van het aantal potentiële toegangspunten voor aanvallers. Significante incidenten zijn doorgaans het gevolg van complexe cyberaanvallen waarbij meestal gebruik wordt gemaakt van nieuwe methoden en technologieën, en het kan weken, zo niet maanden, duren om deze incidenten te onderzoeken en ervan te herstellen. Een voorbeeld is de cyberaanval op het Europees Geneesmiddelenbureau, waarbij gevoelige gegevens werden gelekt en gemanipuleerd om het vertrouwen in vaccins te ondermijnen.

"*De EU-instellingen, -organen en -agentschappen zijn een aantrekkelijk doelwit voor potentiële aanvallers, in het bijzonder groepen die heimelijke, uiterst geavanceerde cyberaanvallen kunnen uitvoeren voor cyberspionage- en andere malafide doeleinden*", aldus Bettina Jakobsen, het ERK-lid dat de controle leidde. "*Dergelijke aanvallen kunnen significante politieke implicaties hebben, de algemene reputatie van de EU schaden en het vertrouwen in haar instellingen ondermijnen. Om haar eigen organisaties te beschermen, moet de EU haar inspanningen opvoeren.*"

De belangrijkste bevinding van de auditors was dat de EU-instellingen, -organen en -agentschappen niet altijd goed tegen cyberdreigingen zijn beschermd. Zij volgen geen consistente aanpak van cyberbeveiliging, beschikken niet altijd over essentiële controles en essentiële goede

Dit persbericht is bedoeld om de kernboodschap weer te geven van het speciaal verslag van de Europese Rekenkamer. Het volledige verslag is te vinden op eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

praktijken op het gebied van cyberbeveiliging, en cyberbeveiligingsopleidingen worden niet systematisch georganiseerd. De toewijzing van middelen aan cyberbeveiliging varieert sterk en een aantal EU-organen besteedt hier aanzienlijk minder aan dan vergelijkbare organen. Hoewel verschillen in cyberbeveiligingsniveaus theoretisch kunnen worden gerechtvaardigd door de verschillende risicoprofielen van elke organisatie en de uiteenlopende mate van gevoeligheid van de gegevens die zij verwerken, benadrukken de auditors dat zwakke punten op het gebied van cyberbeveiliging bij een van de EU-organen verscheidene andere organisaties aan cyberdreigingen kunnen blootstellen (alle EU-organen zijn onderling en vaak met openbare en particuliere organisaties in de lidstaten verweven).

Het computercrisisresponsteam (CERT-EU) en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) zijn de twee voornaamste EU-instanties die met steunverlening op het gebied van cyberbeveiliging zijn belast. Aangezien de middelen beperkt zijn of de prioriteit bij andere actiegebieden ligt, hebben zij de EU-organen echter niet alle nodige ondersteuning kunnen verlenen. Volgens de auditors bestaan er ook tekortkomingen op het gebied van informatie-uitwisseling. Zo wisselen niet alle EU-organen tijdig informatie uit over kwetsbaarheden en significante cyberbeveiligingsincidenten die voor hen gevolgen hadden of die een weerslag op andere instanties kunnen hebben.

Achtergrondinformatie

Er bestaat momenteel geen juridisch kader voor informatiebeveiliging en cyberbeveiliging in de EU-instellingen, -organen en -agentschappen. Ze zijn niet onderworpen aan de meest uitgebreide EU-wetgeving inzake cyberbeveiliging, de NIS-richtlijn van 2016, noch aan de voorgestelde herziening daarvan, de NIS2-richtlijn. Er is evenmin alomvattende informatie beschikbaar over het bedrag dat de EU-organen uitgeven aan cyberbeveiliging. De gemeenschappelijke regels inzake informatiebeveiliging en cyberbeveiliging voor alle EU-organen zijn opgenomen in de mededeling over de EU-strategie voor de veiligheidsunie voor de periode 2020-2025, die de Commissie in juli 2020 heeft gepubliceerd. In de in december 2020 gepubliceerde EU-strategie inzake cyberbeveiliging voor het digitale tijdperk verplicht de Commissie zich ertoe een voorstel te doen voor een verordening inzake gezamenlijke cyberbeveiligingsregels voor alle EU-organen. Voorts heeft de Commissie voorgesteld een nieuwe rechtsgrondslag voor CERT-EU in te voeren om zijn mandaat en financiering te versterken.

Speciaal verslag nr. 05/2022, "*Cyberbeveiliging van EU-instellingen, -organen en -agentschappen — Paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen*", is beschikbaar op de ERK-website. In haar evaluatie van 2019 wees de ERK ook op de uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging.

Perscontact

Persdienst van de ERK: 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