TRIBUNAL DE CUENTAS EUROPEO

ES

Comunicado de prensa

Luxemburgo, 29 de marzo de 2022

Debido al drástico aumento de los ciberataques, los órganos de la UE necesitan una mayor preparación en ciberseguridad

Existe disparidad en el grado de preparación en ciberseguridad entre los órganos de la UE y, en general, no es proporcional a las crecientes amenazas. Por su estrecha interconexión, los puntos débiles de uno de ellos pueden exponer a los demás a amenazas de seguridad. Estas son las conclusiones de un informe especial elaborado por el Tribunal de Cuentas Europeo, que examina el nivel de preparación de las entidades públicas de la UE ante las ciberamenazas. Los auditores recomiendan la introducción de normas vinculantes en ciberseguridad, y que el equipo interinstitucional de respuesta a emergencias informáticas (CERT-UE) disponga de más recursos. Según afirman los auditores, la Comisión Europea debería también fomentar una mayor cooperación entre órganos de la UE, y, por otra parte, el CERT-UE y la Agencia de la Unión Europea para la Ciberseguridad deberían prestar mayor atención a los órganos con menor experiencia en la gestión de la ciberseguridad.

Entre 2018 y 2021, los incidentes de seguridad significativos se multiplicaron por diez en los órganos de la UE; además, el trabajo a distancia ha aumentado considerablemente el número de posibles puntos de acceso. En general, la causa de los incidentes significativos son complejos ciberataques que implican normalmente el uso de nuevos métodos y tecnologías, y pueden requerir semanas o incluso meses de investigación y de recuperación. Un ejemplo fue el ciberataque a la Agencia Europea de Medicamentos, en el que se filtraron y manipularon datos delicados con el propósito de socavar la confianza en las vacunas.

En palabras de Bettina Jakobsen, Miembro del Tribunal de Cuentas Europeo responsable del informe, *«las instituciones, órganos y organismos de la UE son un blanco atractivo para los posibles atacantes, en particular para los grupos capaces de ejecutar ataques sigilosos muy sofisticados con fines de ciberespionaje y otros objetivos perversos. Estos ataques pueden tener importantes consecuencias políticas, dañar la reputación general de la UE y socavar la confianza en sus instituciones. La UE debe intensificar sus esfuerzos para proteger sus propias organizaciones*.»

La principal constatación de los auditores fue que las instituciones, órganos y organismos de la UE no siempre cuentan con una protección adecuada frente a los ciberataques. Estos no atienden a las cuestiones de ciberseguridad de manera coherente, no siempre establecen controles básicos y

El presente comunicado de prensa tiene por objeto ofrecer una síntesis del informe especial del Tribunal de Cuentas Europeo. El texto íntegro del informe puede consultarse en eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

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

buenas prácticas clave de ciberseguridad, ni imparten formación en ciberseguridad de forma sistemática. La asignación de recursos a la ciberseguridad es muy dispar, y algunos órganos de la UE gastan mucho menos que otros similares. Aunque las diferencias en los niveles de ciberseguridad podrían justificarse teóricamente por los distintos perfiles de riesgo de cada organización y el grado variable de sensibilidad de los datos gestionados, los auditores hacen hincapié en que los puntos débiles de un solo órgano de la UE pueden exponer otras organizaciones a amenazas de ciberseguridad (los órganos de la UE están conectados entre sí, y a menudo con otras organizaciones públicas y privadas en los Estados miembros).

El Equipo de Respuesta a Emergencias Informáticas (CERT-UE) y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) son las dos principales entidades de la UE encargadas de prestar apoyo en materia de ciberseguridad. Sin embargo, por la limitación de recursos o la prioridad de otros ámbitos, no han podido facilitar toda la ayuda necesaria a los órganos de la UE. Los auditores también señalan deficiencias en el intercambio de información. Por ejemplo, no todos los órganos de la UE comunican a su debido tiempo las vulnerabilidades ni los incidentes significativos de ciberseguridad que les han afectado y que pueden tener un impacto sobre otros.

Información de referencia

Actualmente no existe un marco legal para la seguridad de la información y la ciberseguridad en las instituciones, órganos y organismos de la UE. No están sujetos a la legislación más amplia de la Unión en materia de ciberseguridad (Directiva SRI 2016) ni a su propuesta de revisión (Directiva SRI2). Tampoco existe información completa sobre el importe invertido por los órganos de la UE en ciberseguridad. La normativa común sobre seguridad de la información y ciberseguridad de todos los órganos de la UE figura en la Comunicación sobre la Estrategia de la UE para una Unión de la Seguridad para el período 2020-2025, que publicó la Comisión en julio de 2020. En la Estrategia de Ciberseguridad de la UE para la Década Digital, publicada en diciembre de 2020, la Comisión se comprometió a proponer un reglamento relativo a las normas de ciberseguridad comunes para los órganos de la UE. También propuso el establecimiento de un nuevo fundamento legal para que el CERT-UE refuerce su mandato y su financiación.

El Informe Especial 05/2022 «*Ciberseguridad de las instituciones, órganos y organismos de la UE: En general, el nivel de preparación no es proporcional a las amenazas*» puede consultarse en el sitio web del Tribunal. En un análisis de 2019, el Tribunal también señaló los retos para una política eficaz de ciberseguridad en la UE.

Contacto de prensa

Oficina de prensa del Tribunal: press@eca.europa.eu

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