TRIBUNAL DE CONTAS EUROPEU

PT

Comunicado de Imprensa

Luxemburgo, 29 de março de 2022

Cibersegurança: organismos da UE têm de intensificar preparação

O número de ciberataques a organismos da UE está a aumentar acentuadamente. O nível de preparação dos organismos da União em matéria de cibersegurança é variável e, em geral, não é proporcional às crescentes ameaças. Como os organismos da UE estão profundamente interligados, a fragilidade de um deles pode expor outros a ciberameaças. Esta é a conclusão de um Relatório Especial do Tribunal de Contas Europeu (TCE) que examina a preparação contra ciberameaças das entidades que governam a UE. O TCE recomenda a introdução de regras de cibersegurança vinculativas e o aumento dos recursos da Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE). Recomenda também que a Comissão Europeia deve promover o aumento da cooperação entre os organismos da UE e que a CERT-UE e a Agência da União Europeia para a Cibersegurança devem centrar-se mais nos organismos da União menos experientes na gestão da cibersegurança.

Os ciberincidentes significativos nos organismos da UE aumentaram mais de dez vezes entre 2018 e 2021. O trabalho à distância aumentou consideravelmente o número de pontos de acesso potenciais para os atacantes. Em geral, os incidentes significativos são causados por ciberataques complexos, implicando normalmente a utilização de novos métodos e tecnologias. A investigação e recuperação dos ataques pode levar semanas ou até meses. Um exemplo foi o ciberataque à Agência Europeia de Medicamentos, em que dados sensíveis foram divulgados e manipulados para diminuir a confiança nas vacinas.

"*As instituições, organismos e agências da UE são alvos atrativos para potenciais atacantes, especialmente para os grupos com capacidade de realizar ataques furtivos altamente sofisticados para fins de ciberespionagem e outros propósitos malévolos*", afirmou Bettina Jakobsen, Membro do TCE responsável pela auditoria. "*Estes ataques podem ter implicações políticas significativas, prejudicar a reputação geral da UE e minar a confiança nas suas instituições. A União tem de intensificar os esforços para proteger as suas próprias organizações*."

A principal constatação da auditoria foi a de que as instituições, os organismos e as agências da UE nem sempre estão bem protegidos contra ciberameaças. O seu tratamento da cibersegurança nem sempre é consistente, os controlos essenciais e as boas práticas fundamentais em matéria de cibersegurança nem sempre estão em vigor e a formação em cibersegurança nem sempre é sistemática. A atribuição de recursos à cibersegurança é muito variável, e vários organismos da UE

O objetivo do presente comunicado de imprensa é apresentar as principais mensagens do Relatório Especial adotado pelo Tribunal de Contas Europeu. O texto integral está disponível em www.eca.europa.eu.

ECA Press

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

têm despesas neste domínio consideravelmente inferiores a outros de dimensão comparável. Em teoria, as diferenças nos níveis de cibersegurança podem ser justificadas pelos diferentes perfis de risco de cada organização e pelos níveis variáveis de sensibilidade dos dados que tratam. O TCE salienta, contudo, que as insuficiências na cibersegurança de um organismo da UE podem expor várias outras organizações a ciberameaças (os organismos da União estão todos interligados e frequentemente têm ligações também a organizações públicas e privadas nos Estados-Membros).

A CERT-UE e a Agência da União Europeia para a Cibersegurança (ENISA) são as duas principais entidades da União responsáveis pelo apoio no domínio da cibersegurança. No entanto, devido às limitações de recursos ou à atribuição de prioridade a outras áreas, estas entidades não conseguiram prestar aos organismos da UE todo o apoio de que estes necessitam. Segundo o TCE, a partilha de informações é também uma lacuna: por exemplo, nem todos os organismos da União comunicam atempadamente informações sobre vulnerabilidades e ciberincidentes significativos que os tenham afetado ou possam afetar outros organismos.

Informações de base

Atualmente, não há um quadro jurídico para a segurança da informação e a cibersegurança nas instituições, agências e organismos da União. Estes domínios não estão sujeitos à legislação mais ampla da UE em matéria de cibersegurança, a Diretiva SRI de 2016, nem à sua proposta de revisão, a Diretiva SRI revista. Também não existem informações exaustivas sobre o montante gasto pelos organismos da UE em cibersegurança. As regras comuns sobre a segurança da informação e a cibersegurança, aplicáveis a todos os organismos da União, fazem parte da comunicação sobre a Estratégia da UE para a União da Segurança para o período de 2020-2025, publicada pela Comissão em julho de 2020. Na Estratégia de Cibersegurança da UE para a Década Digital, publicada em dezembro de 2020, a Comissão comprometeu-se a propor um regulamento sobre regras comuns de cibersegurança para todos os organismos da União. Também propôs o estabelecimento de uma nova base jurídica para a CERT-UE a fim de reforçar o seu mandato e financiamento.

O Relatório Especial 05/2022, *Cibersegurança das instituições, organismos e agências da UE – Em geral, o nível de preparação não é proporcional às ameaças*, está disponível no sítio Web do TCE. O TCE salientou já os desafios que se colocam à eficácia da política de cibersegurança da UE num documento de análise de 2019.

Contactos para a imprensa

Serviço de imprensa do TCE: press@eca.europa.eu

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