TECNOLOGIA DA INFORMAÇÃO

CONTROLES DE SEGURANÇA CIBERNÉTICA

O que o TCU encontrou

O TCU realizou, entre 3/8/2021 e 9/3/2022, o primeiro de sete ciclos previstos para o acompanhamento de controles críticos de segurança cibernética das organizações públicas federais.

Este ciclo, que contemplou 377 organizações, avaliou a implementação de vinte medidas de segurança básicas relacionadas a cinco dos dezoito controles críticos de segurança cibernética estabelecidos no *framework* do *Center for Internet Security* (CIS): inventário e controle de ativos de hardware corporativos; inventário e controle de ativos de software; gestão contínua de vulnerabilidades; conscientização sobre segurança e treinamento de competências; e gestão de respostas a incidentes.

As respostas fornecidas pelos gestores ao questionário de autoavaliação indicam uma situação de alto risco para a segurança cibernética do setor público federal. A fiscalização identificou vários pontos de atenção em relação à implementação dos controles avaliados, dentre os quais se destacam:

- Quanto aos inventários de ativos de *hardware* e de ativos de *software*, que são considerados os controles mais básicos, a maioria das organizações (55,7%) não trata adequadamente os ativos de *hardware* não autorizados, não os impedindo de se conectarem em suas redes; e muitas (44,8%) não tratam os softwares não autorizados, não os impedindo de serem executados em seus dispositivos.
- No que tange à gestão contínua de vulnerabilidades, a maioria das organizações (56,2%) **não mantém um processo de avaliação e monitoramento dos ativos de hardware e software**, com vistas a eliminar, mitigar ou corrigir vulnerabilidades, bem como aprimorar configurações, controles e táticas de defesa; e muitas (46,7%) **não mantêm um processo de correção de vulnerabilidades**, atuando para detectá-las e corrigi-las antes que possam ser exploradas por atacantes.
- Em relação à conscientização e à capacitação dos colaboradores em questões e competências relacionadas à segurança da informação e à segurança cibernética, a maioria das organizações (57,8%) **não mantém um programa contínuo de treinamento em segurança** com vistas a mostrar aos colaboradores os riscos e ameaças aos quais os ativos e dados da organização estão sujeitos e a como agir para evitá-los ou mitigá-los.
- No que concerne à **gestão de incidentes de segurança da informação**, apesar de a maior parte das organizações (65,8%) ter designado pessoal responsável por gerenciar um processo de tratamento de incidentes, quase metade (47,2%) ainda **não mantém informações de contato para reporte de incidentes** e pouco mais da metade delas (52,5%) ainda **não mantém um processo para recebimento de notificações de incidentes**.

Por que esses achados são relevantes

O processo de transformação digital do governo, ao mesmo tempo em que disponibiliza progressivamente aos cidadãos informações e serviços digitalizados, acessíveis por meio de aplicativos e sítios na internet, torna as organizações públicas ainda mais dependentes de soluções de tecnologia da informação (TI) – *softwares*, bases de dados e sistemas informatizados –, providas por sistemas relevantes e críticos, essenciais para o funcionamento do governo. Nesse contexto, vulnerabilidades e falhas de segurança da informação e segurança cibernética aumentam muito os riscos de ameaças e ataques cibernéticos, o que afeta significativamente o governo e os cidadãos.

Além disso, a pandemia de covid-19 forçou as organizações a expandirem rapidamente o regime de trabalho remoto, o que aumentou a quantidade de acessos externos às redes de computadores e o número de incidentes relacionados a ataques cibernéticos, em especial por meio de códigos maliciosos (*malware*).

Com o mapeamento da maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança cibernética, o TCU pode atuar proativamente no sentido de induzir o aumento da resiliência da Administração Pública Federal (APF) frente a incidentes e ataques cibernéticos. Essa medida contribui diretamente para o sucesso do processo de transformação digital do país.

Além disso, estabeleceu-se um movimento de conscientização e orientação dos gestores quanto aos riscos decorrentes da ausência de controles de segurança cibernética e à necessidade urgente de implementá-los.

O que precisa ser feito

De modo a contribuir para a melhoria da preocupante situação encontrada, o TCU recomendou à Secretaria de Governo Digital do Ministério da Economia, como órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo federal, ao Conselho Nacional de Justiça, como órgão governante superior do Poder Judiciário federal, e a órgãos específicos, dentre os quais, o Tribunal de Contas da União, a Câmara dos Deputados, o Senado Federal, o Supremo Tribunal Federal e aos segmentos do Ministério Público da União, a adoção de diversas medidas para fomentar uma rápida e gradativa implementação dos controles críticos e medidas de segurança cibernética preconizados no *framework* do *Center for Internet Security* (CIS), priorizando o endereçamento das deficiências e fragilidades detectadas neste primeiro ciclo de avaliação.

DADOS DA DELIBERAÇÃO

Acórdão: 1768/2022-TCU-Plenário
Data da sessão:
Relator: Ministro Vital do Rêgo
TC: 036.301/2021-3
Unidade Técnica Responsável: Secretaria de Fiscalização de Tecnologia da Informação (Sefti)