TCU identifica riscos à segurança da informação em organizações públicas federais

29/03/2024

O Tribunal de Contas da União analisou, na sessão plenária de quarta-feira (27/3), processo que avaliou aspectos relacionados à segurança da informação de organizações públicas federais. O objetivo da auditoria foi identificar falhas de configuração em serviços de hospedagem web, correio eletrônico e resolução de nomes. Esse tipo de fragilidade pode ser explorada por *hackers*.

creativeart/freepik

Proteção de dados em instituições públicas é risco alertado pelo TCU

O trabalho concluiu que há deficiências na configuração de controles recomendados pelas boas práticas para serviços de hospedagem web, e-mail e DNS (*Domain Name Service*). A maioria dos índices médios das práticas de segurança da informação apresenta nível de maturidade baixo ou intermediário.

O método utilizado permitiu analisar milhares de domínios. Com as falhas encontradas, a maioria das organizações e seus clientes ficam expostos a ataques cibernéticos. Isso pode afetar a confidencialidade e a integridade de grande parte dos serviços digitais oferecidos à população pelo governo federal e entes subnacionais.

Foram identificados sete riscos que apontam a possibilidade de manipulação de tráfego de rede, comprometimento de contas de usuários, roubo, vazamento e perda de dados ou mesmo interrupção dos sistemas de organizações públicas. Os problemas podem impactar programas, ações e objetivos das organizações, além da perda de confiança da população e possíveis sanções legais. Por exemplo, 84% dos domínios testados estão com nível de risco alto para ataques contra as aplicações hospedadas nos seus servidores.

As principais causas da não implementação dos controles de segurança foram a falta de recursos ou investimento, de pessoal e de capacitação. Também falta efetividade na implementação das normas, e é necessário envolver a alta administração das organizações.

O ministro-relator da auditoria, Aroldo Cedraz, ressaltou a dimensão do trabalho, que avaliou 100% dos domínios identificados. “Os domínios testados são utilizados por órgãos e entidades públicas dos três poderes, nas esferas federal, estadual e municipal. Portanto, o levantamento inova também ao resultar na construção de verdadeiro inventário da segurança cibernética dos serviços de toda a administração pública brasileira”, disse.

A fiscalização busca promover a melhoria na gestão de riscos de segurança da informação desses serviços nas organizações. O Tribunal decidiu fazer a análise porque mais de 80% dos ataques de *ransomware* podem ser atribuídos a erros de configuração em softwares e em dispositivos, segundo o relatório Microsoft Cyber Signals 2022.

Problemas identificados:

- Apenas 2% dos domínios avaliados implementam adequadamente todos os quatro controles testados de conexão segura web (HTTPS).
- 12% dos domínios avaliados nos testes de web e 29% nos testes de e-mail não implementam certificados de assinatura digital.
- 81% dos domínios avaliados nos testes de web e 86% nos testes de e-mail não implementam assinatura de domínio DNSSEC.
- Apenas 8% dos domínios avaliados implementam todas as proteções contra *phishing* avaliadas.

Encaminhamentos

O TCU vai dar conhecimento da fiscalização a oito organizações que representam a multiplicidade de instituições que detêm os domínios avaliados. A ideia é incentivar a adoção de medidas e a elaboração de estratégias sobre a gestão dos riscos decorrentes da não implantação dos controles analisados.

Para apoiar os entes públicos, a equipe de auditoria elaborou o "Mapa de Riscos e Controles", que busca esclarecer os controles de segurança avaliados, os riscos da não implementação, além dos custos e benefícios. O documento também esclarece os critérios e referências para implementação de cada controle.

A unidade técnica do TCU responsável pela fiscalização foi a Auditoria Especializada em Tecnologia da Informação (AudTI), que integra a Secretaria de Controle Externo de Governança, Inovação e Transformação Digital do Estado (SecexEstado). O relator é o ministro Aroldo Cedraz. *Com informações da assessoria de imprensa do TCU.*

Fonte: https://conjur.jumps.com.br/2024-mar-29/tcu-identifica-riscos-de-seguranca-da-informacao-em-organizacoes-publicas-federais/