TECNOLOGIA DA INFORMAÇÃO

AUDITORIA SOBRE EXECUÇÃO DE CÓPIAS DE SEGURANÇA (BACKUP) NA APF

O QUE O TCU FISCALIZOU

Em virtude do processo de transformação digital e da expansão acentuada do regime de trabalho remoto, disparou a quantidade de incidentes de "sequestro de dados" (ransomware), com potencial de causar enormes danos às organizações da Administração Pública federal. Atualmente, o Brasil ocupa a nona posição no ranking global desse tipo de ataque. Nesse cenário, é essencial que as organizações públicas mantenham suficientes e adequados controles relacionados à execução de cópias de segurança (backup e restore), de modo a garantir a continuidade dos serviços prestados e aumentar, assim, suas resiliências quanto a vulnerabilidades, falhas de segurança e ataques cibernéticos.

OBJETIVO DA AUDITORIA

A auditoria objetivou avaliar a maturidade das organizações da Administração Pública federal em relação à realização de procedimentos de backup e restore, mais especificamente sobre suas principais bases de dados e sistemas, com base na avaliação dos subcontroles preceituados no controle 10 (Data Recovery Capabilities) do framework de controles críticos de segurança cibernética do Center for Internet Security (CIS). Adicionalmente, a auditoria teve o propósito de conscientizar e orientar os gestores dessas organizações em relação aos riscos associados à ausência/deficiência de controles nessa área.

Assim, 422 organizações receberam ofícios de comunicação solicitando o preenchimento de um questionário online e o envio de evidências, sendo que, dessas, 410 (97,2%) efetivamente o responderam.

O QUE O TCU ENCONTROU

De modo geral, o panorama merece atenção. 74,6% das organizações respondentes (306 de 410) não possuem política de backup aprovada formalmente. Trata-se de documento básico, negociado entre as áreas de negócio ("dona" dos dados/sistemas) e de TI da organização, para disciplinar as questões e os procedimentos relacionados à execução dos backups.

Quanto às cópias das principais bases de dados e sistemas das organizações, o cenário é positivo. Daquelas que tratam bases de dados, 99,2% (373 de 376) efetuam backups completos periodicamente, sendo 94,9% (354 de 373) de forma automatizada. Daquelas que hospedam sistemas em máquinas próprias, apesar de 71,2% (265 de 372) não possuírem plano de backup específico para o principal sistema, 84,4% (314 de 372) realizam backups ao menos semanais desse sistema e, de todas que fazem tais cópias, 60,8% (206 de 339) as fazem integrais (e.g. cópia da imagem das máquinas).

Também é preocupante que mais da metade das organizações respondentes (216 de 410: 52,7%) não executem quaisquer testes de restauração (restore) dos seus backups e que, entre aquelas que afirmaram realizar tais testes, 59,8% (116 de 194) não os documentem. Essa situação traz risco de que, em situações reais em que seja preciso recuperar um sistema e/ou dados da organização a partir dessas cópias, isso acabe não sendo possível.

Quanto à proteção das cópias, foram identificadas duas vulnerabilidades: i) das organizações que armazenam os backups em ambiente segregado, mais da metade (179 de 348: 51,4%) não mantêm registro dos acessos a esse local; ii) das organizações que realizam backups, 66% (254 de 385), apesar de implementarem mecanismos de controle de acesso físico ao local da guarda, não armazenam os arquivos criptografados,

o que pode trazer prejuízos em caso de vazamento de dados, sobretudo sensíveis ou sigilosos.

Adicionalmente, 60,2% das organizações respondentes (247 de 410) não mantêm suas cópias em ao menos um destino não acessível remotamente, o que acarreta risco de que, em eventual ataque cibernético, os próprios arquivos dos backups sejam corrompidos, excluídos ou criptografados, tornando sem efeito todo o processo de backup/restore da organização.

PROPOSTA DE ENCAMINHAMENTO

De modo a contribuir para a melhoria do cenário encontrado, conclui-se pela necessidade de edição de normativos específicos para orientar os gestores e regulamentar a obrigatoriedade de que as organizações públicas aprovem formalmente e mantenham atualizadas políticas e planos de backup, contemplando requisitos mínimos para endereçar os aspectos abordados na auditoria.

BENEFÍCIOS ESPERADOS

Questionário aplicado após a fase de execução identificou ter sido efetivamente alcançado o principal propósito da auditoria, a saber a conscientização dos gestores respondentes quanto aos riscos associados às questões avaliadas, resultando na implementação de ações específicas para melhoria dos controles internos das organizações.

Para o TCU, a auditoria entregou diagnóstico abrangente das organizações quanto ao tema, que subsidiará a definição de auditorias baseadas em risco (e.g. auditar órgãos com baixa maturidade responsáveis por manter sistemas governamentais críticos).

Adicionalmente, com base no cenário percebido e nas avaliações qualitativas realizadas pela equipe de auditores sobre as evidências encaminhadas pelos respondentes, esta auditoria permitiu ao TCU deliberar sobre orientações para aprimorar os controles de backup e restore das organizações da Administração Pública federal, com reflexos nas respectivas resiliências quanto a incidentes de segurança e ataques cibernéticos.

PRÓXIMOS PASSOS

Considera-se que a execução desta auditoria apresentou relação custo-benefício satisfatória, sugerindo-se que a Sefti continue a utilizar a mesma sistemática para avaliar outros controles de segurança cibernética do framework do Center for Internet Security (CIS), a exemplo dos relacionados a inventário e controle de ativos (de hardware e de software), a gerenciamento de vulnerabilidades e a resposta a incidentes.

DADOS DA DELIBERAÇÃO

Acórdão: 1109/2021 - TCU - Plenário
Data da sessão: 12/5/2021
Relator: Ministro Vital do Rêgo
TC: 036.620/2020-3
Unidade Técnica Responsável: Secretaria de Fiscalização de Tecnologia da Informação (Sefti)