NOTA CONJUNTA

CTIR Gov | CISC GOV.BR

O CTIR Gov e o CISC GOV.BR, em trabalho conjunto de elevação da consciência e resiliência cibernética na Administração Pública Federal e demais entes de seu público-alvo, têm observado que os incidentes cibernéticos ocorridos em 2026 exploraram vulnerabilidades comuns em todas as instituições vítimas.

Nesse contexto, o gerenciamento da superfície de ataque torna-se essencial à segurança da infraestrutura de TI da organização, contribuindo para a disponibilidade dos serviços e a preservação da imagem institucional. As recomendações da CISA e do NIST, em conjunto com as orientações do Programa de Privacidade e Segurança da Informação (PPSI 2.0), especialmente quanto à gestão de ativos e vulnerabilidades, orientam a adoção de medidas adequadas às necessidades e aos riscos da organização.

A seguir apresentaremos um conjunto de recomendações que visam mitigar tais vulnerabilidades de modo a tornar a estrutura do órgão mais resiliente. Além disso, tais recomendações estão organizadas por nível de prioridade de modo que as equipes técnicas e gerenciais possam planejar a sua implementação dentro das realidades de cada um, e considerando a existência de um inventário de ativos físicos e lógicos.

PRIORIDADE 1 — Redução da superfície de ataque e controle da exposição

a) Análise da necessidade de acesso ao sistema, identificando qual público realmente necessita acessá-lo, de modo a restringir sua conectividade conforme o público-alvo por meio da adoção de VPN (Virtual Private Network) ou redes segregadas;

b) Adotar uma arquitetura em que os servidores legados, mantidos em segmento de rede próprio, estejam acessíveis apenas aos sistemas consumidores mais modernos e via portas estritamente necessárias ao funcionamento dos serviços, bloqueando os acessos administrativos não autorizados;

c) Segregação de rede das máquinas que hospedam o sistema legado, isolando-as em VLAN, VRF ou sub-rede dedicada, separada de outros ativos, bancos de dados, estações de trabalho e redes administrativas, com política de firewall em modo default deny, acesso intermediado por proxy reverso seguro e bastion host, restrição de tráfego de saída e monitoramento contínuo do segmento, a fim de conter movimentação lateral e reduzir a exposição dos ativos mesmo em caso de exploração;

d) Manutenção de inventário atualizado dos sistemas legados e seus componentes, identificando versões, pilha e dependências tecnológicas, responsáveis, criticidade e exposição à Internet;

e) Identificação e avaliação periódica, em ativos de rede e telefonia VoIP, de vulnerabilidades conhecidas (CVEs), priorizando aquelas com exploração ativa e adotando medidas compensatórias, como mitigação virtual (virtual patching), quando não for possível aplicar correções;

f) Restrição das conexões de saída dos servidores, permitindo somente as comunicações necessárias ao funcionamento dos serviços e monitorando tentativas de comunicação não autorizadas;

g) Desativação de serviços, protocolos, interfaces e funcionalidades desnecessários, visando reduzir a superfície de ataque, desde que preservada a continuidade operacional;

h) Adoção de proxy reverso ou WAF (Web Application Firewall), impedindo o acesso direto ao servidor. Nesse caso, a solução poderá restringir o acesso a consoles e páginas de diagnóstico, auxiliar no bloqueio de ataques conhecidos e oferecer criptografia moderna aos usuários;

i) Adotar uma estrutura de rede totalmente segregada para dispositivos IoT (câmeras, leitoras de digitais, etc); e

j) Restrição de acesso e desativação de superfícies de ataque nativas, como painéis de administração padrão (ex: /jmx-console, /manager, phpinfo) e funções sem uso da linguagem.

PRIORIDADE 2 — Proteção de credenciais, privilégios e administração

a) Adoção de controle do acesso privilegiado somente com MFA, evitando o uso de senhas padrão, contas compartilhadas e credenciais armazenadas em texto claro;

b) Gestão do acesso de servidores e serviços com o uso, sempre que possível, de MFA e registro de sessões;

c) Auditoria de contas periódicas de modo a verificar o acesso adequado a plataformas, ferramentas e sistemas de acordo com a necessidade do serviço sempre dentro da janela de atuação do servidor/colaborador, atentando para a desativação nos momentos de afastamento (férias, demissão, licenças, etc).

d) Execução dos serviços por meio de contas com os privilégios mínimos necessários;

e) Inventariar contas administrativas, usuários da aplicação e contas com acesso a servidores e bancos de dados, desabilitando contas padrão desnecessárias e revisando acessos administrativos;

f) Segregação das contas de acesso em camadas de permissão, garantindo que cada usuário tem a credencial justa para a sua função, sem conferir mais recurso do que o necessário e desativando contas desnecessárias; e

g) Implementação de proxy reverso seguro com terminação TLS (TLS 1.2/1.3), garantindo criptografia segura.

PRIORIDADE 3 — Detecção, monitoramento e resposta a incidentes

a) Ativação do registro de logs e monitoramento dos acessos ao sistema, bem como da saúde dos servidores de hospedagem, com envio dos registros para ambiente externo aos servidores monitorados (SIEM). Especial atenção deverá ser dada às operações administrativas críticas ou suspeitas, com geração de alertas às áreas responsáveis;

b) Implantação de solução de Endpoint Detection and Response (EDR) compatível com as plataformas utilizadas pelo órgão, incluindo as legadas, com análise comportamental, detecção de movimentação lateral e capacidade de isolamento do host comprometido.

c) Implantação de monitoramento de integridade de arquivos (File Integrity Monitoring — FIM), com estabelecimento de linha de base (baseline) de arquivos e configurações críticas, detecção de alterações não autorizadas, geração de alertas e integração com SIEM, quando disponível;

d) Criação e manutenção do plano de isolamento rápido dos servidores eventualmente comprometidos, mantendo-o permanentemente disponível e testado, observando os impactos sobre a continuidade dos serviços;

e) Manter, por meio do Gestor de Segurança da Informação, o contato estreito com a Comunicação Social e o Jurídico do órgão, de modo a ter uma preparação de atuação desses atores no caso de um incidente cibernético, com o intuito de proteger a credibilidade dos serviços prestados e da imagem institucional;

f) Ativação de registro de logs em ativos de rede, concentrando-os em um local seguro e de acesso restrito;

PRIORIDADE 4

Recuperação, continuidade e gestão dos riscos

a) Revisão das políticas de backup, garantindo a integridade das cópias de segurança, preferencialmente com mecanismos de isolamento ou imutabilidade, e realização periódica de testes de restauração;

b) Realização de avaliação periódica dos riscos associados às diferentes possibilidades de incidente cibernético, documentando as ações compensatórias a serem adotadas para a mitigação dos riscos e a efetividade das medidas implementadas, com ciência da alta gestão do órgão; e

c) Realizar testes periódicos de recuperação de serviços a partir de backups, avaliando a efetividade e eficácia da ação para a organização.

d) Definir políticas de gestão de terceirizados, incluindo o controle de acesso a informação, uso de equipamento particular (BYOD - Bring Your Own Device), gerenciamento dos trabalhos por servidor efetivo, monitoramento das operações, etc; e

e) Avaliar a possibilidade de segregar as contratações de suporte nos diferentes níveis para empresas distintas, evitando ter a mesma contratada também como responsável da área de cibersegurança da organização.