Boas práticas de proteção cibernética para serem implementadas em infraestruturas críticas

Devido à evolução tecnológica verificada nos últimos anos, fruto de um esforço de Estado e de Instituições públicas e privadas para aumento de eficiência dos serviços, aliado à necessidade de quebra de paradigmas causada pelo período da pandemia da COVID-19, as instituições incorporaram serviços e flexibilizaram o acesso às redes corporativas, inclusive disponibilizando conexões remotas para adaptação à nova realidade.

Dentre as supracitadas medidas inovadoras, o acesso remoto de colaboradores contribuiu para a ampliação da superfície de ataque no ambiente cibernético, que pode ser explorada por atores maliciosos, tornando as infraestruturas suscetíveis às ameaças cibernéticas.

Neste contexto, Ameaças Cibernéticas às Infraestruturas Críticas e aos Sistemas de Informação da Administração Pública Federal são uma realidade que não deve ser menosprezada. Desta forma, a "Security Through Obscurity" ou "Segurança por Obscuridade" não deve ser a única medida de segurança. Ações como a aplicação de técnicas de segregação (Air Gap), apesar de ser uma das medidas mais aplicadas em Redes de Automação, têm sido cada vez mais superadas por novos métodos de ataques virtuais.

Recomenda-se que as instituições públicas gestoras orientem as respectivas infraestruturas críticas a implementar as seguintes medidas protetivas:

a) Caso seja instituição da Administração Pública Federal, instituir e implementar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), conforme previsto no Decreto nº 10.748, de 16 de julho de 2021;

b) Adotar campanhas de conscientização de usuários em relação a ataques de engenharia social, com especial atenção a tentativas de phishing via e-mail, cuidados com utilização de unidades de mídia desconhecidas (pen drives, HD externos etc) e orientação para não utilizar redes ou dispositivos não confiáveis para acesso a contas corporativas;

c) Implantar uma política que promova a tempestiva e oportuna atualização de Sistemas Operacionais com os últimos patches de segurança, inclusive com atualização de firmwares dos dispositivos das redes operacionais;

d) Promover o monitoramento contínuo dos dispositivos conectados tanto à rede operacional quanto à rede administrativa;

e) Implantar a segmentação efetiva entre a rede administrativa e a rede operacional;

f) Implementar o princípio de privilégio mínimo, limitando aos usuários o nível mínimo de acesso necessário para cumprir suas tarefas;

g) Instituir política de credenciais de acesso às redes administrativas e operacionais, fazendo uso de autenticação de multifator, troca periódica de senha, sistemas de bloqueio por excesso de tentativas e outras medidas constante das boas práticas e credenciais de acesso;

h) Adotar políticas e procedimentos de backup offline, restauração e testagem;

i) Implementar técnicas de defesa em profundidade com tecnologias de firewall (rede e host), IDS/IPS, analisadores de tráfego e antimalware; e

j) Promover cultura organizacional voltada para a proteção cibernética.

Recomenda-se, ainda, a consulta aos alertas e recomendações relacionados à Segurança da Informação, disponíveis em:
- https://www.ctir.gov.br/alertas/

Fonte: CTIR - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, em 03.12.2021