Ascender Defesas

Boas Práticas em Cibersegurança

CTIR Gov

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

10 de outubro de 2025

[TLP:CLEAR]

Campanha Ascender Defesas

Objetivo da Campanha

Implementar ações preventivas em cibersegurança nos órgãos de governo e infraestruturas críticas de interesse para eventos (ICIE) de grande magnitude e relevância internacional.

Imperativos:

- Segurança Cibernética;
- Resiliencia Cibernética;
- Serviços à população;
- Soberania.

1. Inventário e definição de dispositivos/ativos autorizados:

Recomendação

A ICIE deve manter um inventário atualizado de todos os dispositivos autorizados a acessar a rede e definir classes de ativos não autorizados. Facilita o controle e permite a remoção de dispositivos não autorizados.

Objetivos:

- Facilitar o controle de acesso à rede
- Permitir a remoção de dispositivos não autorizados
- Manter visibilidade completa dos ativos de rede
- Prevenir acessos indevidos

2. Inventário e proteção de dispositivos de OT/IoT autorizados:

Recomendação

A ICIE deve manter um inventário atualizado de todos os dispositivos de OT/IoT autorizados. Recomenda-se que esses dispositivos tenham uma camada de proteção de acesso à rede e acesso remoto controlado (estritamente necessário). Garantir mecanismos de segurança em caso de necessidade de manutenção por terceiros ou remota (horário programado, uso de VPN e outros).

Objetivos:

- Proteger dispositivos críticos de tecnologia operacional
- Controlar rigorosamente o acesso remoto
- Implementar camadas de segurança adequadas
- Garantir manutenção segura por terceiros

3. Inventário e definição de softwares autorizados:

Recomendação

A definição dos softwares autorizados e a manutenção de um inventário atualizado ajudará a ICIE a identificar e remover quaisquer softwares não autorizados que possam representar um risco à segurança cibernética.

Objetivos:

- Reduzir a superfície de ataque
- Prevenir instalação de software malicioso
- Manter conformidade com políticas de segurança
- Facilitar auditorias e gestão de licenças

4. Processo de controle de atualização de software e dispositivos autorizados:

Recomendação

A ICIE deve realizar um processo contínuo de controle e atualização de softwares e dispositivos a fim de se prevenir de novos vetores de ataques.

Objetivos:

- Corrigir vulnerabilidades conhecidas rapidamente
- Prevenir exploração de falhas de segurança
- Manter sistemas atualizados com patches críticos
- Estabelecer processo sistemático de atualização

5. Seleção de fornecedores de cadeia de suprimentos:

Recomendação

Implementar requisitos de segurança cibernética na seleção de fornecedores de cadeia de suprimentos.

Objetivos:

- Avaliar postura de segurança de fornecedores
- Mitigar riscos da cadeia de suprimentos
- Estabelecer requisitos contratuais de segurança
- Garantir conformidade ao longo do ciclo de vida

6. Uso de sistemas seguros de autenticação:

Recomendação

A ICIE deve implementar sistemas adequados de autenticação por senha, protegido por criptografia, e sempre que possível deve adotar o uso de múltiplo fator de autenticação (MFA).

Objetivos:

- Fortalecer controle de acesso aos sistemas
- Implementar autenticação multifator (MFA)
- Proteger credenciais com criptografia forte
- Reduzir risco de comprometimento de contas

7. Configuração segura para hardware e software em dispositivos móveis, laptops, estações de trabalho, servidores e ativos de rede (firewalls, roteadores, switches e outros):

Recomendação

a ICIE deve definir e implementar protocolos de fortalecimento (hardening) para hardware e software.

Objetivos:

- Reduzir superfície de ataque dos sistemas
- Desabilitar serviços e portas desnecessárias
- Aplicar configurações seguras padronizadas
- Fortalecer postura de segurança da infraestrutura

8. Gestão, avaliação contínua e correção de vulnerabilidades:

Recomendação

A ICIE deve buscar realizar avaliações prévias e regulares de vulnerabilidades em sua rede e sistemas, e corrigir prontamente, ou ao menos mitigar, quaisquer vulnerabilidades identificadas.

Objetivos:

- Identificar vulnerabilidades proativamente
- Priorizar correções por criticidade
- Implementar ciclo contínuo de avaliação
- Reduzir janela de exposição a ameaças

9. Uso controlado de privilégios administrativos:

Recomendação

A ICIE deve limitar privilégios administrativos apenas para usuários que deles necessitem e monitorar o uso desses privilégios. Esta medida ajudará a ICIE a impedir o acesso não autorizado e o abuso de credenciais com privilégios administrativos (princípio do privilégio mínimo).

Objetivos:

- Aplicar princípio do menor privilégio
- Monitorar uso de contas privilegiadas
- Prevenir escalação de privilégios
- Reduzir impacto de comprometimento

10. Manutenção, monitoramento e análise de logs de auditoria:

Recomendação

A ICIE deve coletar, centralizar e analisar logs de seus sistemas e aplicações para detectar e responder a incidentes de segurança. Esta medida deve ser aliada ao uso correto do Network Time Protocol (NTP).

Objetivos:

- Centralizar coleta de logs de auditoria
- Detectar anomalias e incidentes rapidamente
- Garantir sincronização temporal com NTP
- Manter evidências para investigações

11. Proteções de e-mail e navegação web:

Recomendação

A ICIE deve implementar medidas de conscientização (sensibilização de usuários) e ferramentas para proteção contra ataques de phishing e acesso a sites maliciosos, como filtragem de e-mail (antispam e outros) e filtragem de conteúdo da web (proxy, dns e outros).

Objetivos:

- Proteger contra phishing e engenharia social
- Filtrar conteúdo malicioso de e-mail e web
- Conscientizar usuários sobre ameaças
- Implementar camadas de defesa

12. Limitação e controle de portas, protocolos e serviços de rede:

Recomendação

A ICIE deve limitar o uso de portas, protocolos e serviços de rede apenas àqueles que são estritamente necessários para suas operações e desabilitar aqueles que não o são.

Objetivos:

- Reduzir superfície de ataque da rede
- Desabilitar portas e serviços desnecessários
- Aplicar regras restritivas de firewall
- Monitorar tráfego de rede constantemente

13. Capacidade de recuperação de dados:

Recomendação

A ICIE deve implementar processos e políticas de backup e recuperação de dados, e testá-las, para garantir que os dados críticos possam ser rapidamente recuperados no caso de um incidente cibernético. Mais informações em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2022/recomendacao-34-2022

Objetivos:

- Garantir recuperação rápida de dados críticos
- Implementar estratégia 3-2-1 de backup
- Testar regularmente procedimentos de restore
- Proteger backups contra ransomware

14. Defesa de perímetro:

Recomendação

A ICIE deve implementar ativos de segurança de rede, como firewalls, web application firewall e sistemas de detecção e prevenção de intrusão, para proteger sua infraestrutura de rede contra ameaças externas.

Objetivos:

- Proteger perímetro da rede contra ameaças
- Implementar firewalls e WAF adequados
- Detectar e prevenir intrusões (IDS/IPS)
- Segmentar rede para contenção de ataques

15. Proteção contra exfiltração de dados:

Recomendação

A ICIE deve implementar medidas de proteção de dados, como criptografia e monitoramento de anomalias para prevenir contra vazamento de dados (volumetria de saída, horários, conexões e outros), para proteger informações confidenciais.

Objetivos:

- Prevenir vazamento de dados sensíveis
- Monitorar transferências anômalas de dados
- Implementar DLP (Data Loss Prevention)
- Criptografar dados em trânsito e em repouso

16. Controle de acesso a rede sem fio:

Recomendação

A ICIE deve implementar medidas para proteger suas redes sem fio, utilizando criptografia WPA-2 ou superior, além de rígido controle e monitoramento de acesso.

Objetivos:

- Proteger redes wireless com criptografia forte
- Implementar autenticação robusta (WPA-2/WPA-3)
- Monitorar dispositivos conectados à rede
- Segmentar redes wireless adequadamente

17. Monitoramento e controle de contas:

Recomendação

A ICIE deve monitorar as atividades das contas de usuários em busca de indícios de acesso não autorizado ou uso indevido. Esta medida deve ser tomada em conjunto com o processamento de logs e de acordo com a política de segurança cibernética da instituição.

Objetivos:

- Detectar acessos não autorizados rapidamente
- Identificar comportamentos anômalos
- Correlacionar eventos de segurança
- Aplicar análise comportamental (UEBA)

18. Resposta e gerenciamento de incidentes:

Recomendação

A ICIE deve desenvolver e implementar um plano de resposta a incidentes e, quando possível, manter uma equipe de tratamento de incidentes de rede (ETIR) para detectar, responder e se recuperar de incidentes de segurança. Mais informações em: http://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918

Objetivos:

- Estabelecer procedimentos de resposta
- Formar e treinar equipe ETIR
- Reduzir tempo de detecção e resposta
- Documentar lições aprendidas

19. Testes de Intrusão:

Recomendação

É recomendável, quando viável, realizar testes de intrusão em sua infraestrutura de tecnologia da informação a fim de identificar vulnerabilidades em sua rede e sistemas. Esta medida deve ser realizada por entidade externa à organização.

Objetivos:

- Identificar vulnerabilidades exploráveis
- Validar eficácia dos controles de segurança
- Simular ataques reais de forma controlada
- Obter avaliação independente e imparcial

20. Medidas preventivas contra artefatos maliciosos:

Recomendação

A ICIE deve implementar medidas de controles contra vírus e malwares, Essas medidas passam, entre outras, pela adoção de ferramentas como softwares antivírus e/ou antimalwares para endpoints, além de proteção para a rede como antívirus de borda e antispam.

Objetivos:

- Proteger endpoints contra malware
- Implementar defesa em múltiplas camadas
- Utilizar antivírus de borda e antispam
- Manter assinaturas sempre atualizadas

Conclusão

Processo

A implementação destas 20 recomendações eleva significativamente o nível de Segurança e Resiliência Cibernética em infraestruturas críticas de interesse para eventos (ICIE) de grande magnitude e relevância internacional. Mas é só o começo do fortalecimento da Proteção Cibernética.

Prevenção • Tratamento • Resposta

Obrigado!

CTIR Gov

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

Contatos:

Web: www.gov.br/ctir

E-mail: ctirgov@presidencia.gov.br

Notificações: ctir@ctir.gov.br