Resposta a incidentes Cibernéticos

Tribunal Regional Eleitoral do Maranhão

SEGIN – Seção de Gestão de Segurança da Informação

1 PLANO DE RESPOSTA A INCIDENTES

Um plano de resposta a incidentes é um programa estruturado e elaborado para ajudar a identificar, gerenciar e enfrentar incidentes cibernéticos. Contém 6 fases: **preparação, identificação, contenção, erradicação, recuperação e lições aprendidas**.

2 OBJETIVO

Este guia fornece um passo-a-passo para auxiliar na preparação de um plano de resposta a incidentes cibernéticos, priorizar ações e acionar as pessoas certas durante o incidente e realizar a coordenação dos trabalhos. Este guia possui três propósitos chave:

- Servir de guia para o desenvolvimento de um plano de resposta a incidentes cibernéticos e delinear os processos e procedimentos para detectar, investigar, erradicar, e se recuperar de um incidente cibernético;
- Identificar os parceiros que podem ser acionados durante um incidente para obter suporte análise e mitigação do incidente, além de coordenar a comunicação com o público interno e externo;
- Descrever um processo macro para responder a um incidente cibernético.

3 ESCOPO

O escopo de fluxo de trabalho se estende a **administradores** e aos **proprietários** dos ativos afetados. Esses dispositivos podem estar localizados fisicamente nas dependências da Justiça Eleitoral ou remotamente em nuvem ou através de VPN, podendo ser dispositivos físicos ou virtuais.

4 FASES

4.1 Preparação

Este documento pressupõe que pelos menos os pré-requisitos abaixo estejam documentados (plano de resposta a incidentes e um plano de continuidade de negócios atualizado), recursos disponíveis para realizar a recuperação, (backups, licenças de software, contas de acesso, etc.), canais de comunicação definidos (contatos de fornecedores, suporte, etc.), acesso aos dispositivos físicos conectados

à rede, assim como acesso a dispositivos virtuais com acesso a nível de administração para realização de contramedidas.

4.1.1 De forma ideal os itens da lista a seguir deverão estar atendidos para facilitar a resposta a um incidente:

4.1.1.1 Instaladores e licenças dos softwares armazenados também em áreas fora da rede;

4.1.1.2 Contas de acesso disponíveis para acesso em caso de parada da rede: contas locais, sites de suporte, equipamentos, ILO, etc.;

4.1.1.3 Endereços IP de rede, gerência, ILO, etc

4.1.1.4 Atores chave e suas responsabilidades:

- ETIR
  - Secretaria (STI);
  - Coordenadoria de Infraestrutura e Sistemas (COINF);
  - Seção de Suporte a Redes Locais (SERED);
  - Seção de Análise e Desenvolvimento de Sistemas e Banco de Dados (SEADB);
  - Seção de Suporte ao Usuário e Manutenção (SESUM);
  - ASCOM/WEB
- COMITÊ DE CRISE CIBERNÉTICA
  - Diretoria-Geral (DG);
  - Coordenadoria de Imprensa e Comunicação Social (COIMC);
  - Secretaria de Tecnologia da Informação e Comunicação (STIC);
  - Ouvidoria Regional Eleitoral (ORE);
  - Seção de Gestão de Segurança da Informação (SEGIN);
  - Secretaria de Administração e Finanças (SAF) e
  - Seção de Segurança Institucional e Inteligência (SESEI)
- COMITÊ DE SEGURANÇA DA INFORMAÇÃO
  - Presidência;
  - Diretoria-Geral (DG);
  - Corregedoria Regional Eleitoral (CRE);
  - Secretaria de Tecnologia da Informação e Comunicação (STIC);

- Secretaria de Gestão de Pessoas (SGP);
- Secretaria de Administração e Finanças (SAF);
- Secretaria Judiciária (SJD);
- Assessoria de Comunicação (ASCOM);
- Representante do Conselho de Zonas Eleitoral;
- Unidade Segurança Institucional e Inteligência;
- Seção de Segurança da Informação (SESEC); e
- Gestor de Segurança da Informação (SEGIN).

- COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS
  - Presidência;
  - Diretoria-Geral (DG);
  - Gestor de Segurança da Informação;
  - Representante do Conselho de Zonas Eleitoral.
- COIMC

4.1.1.5 Contatos de suporte que poderão ser acionados

- TSE
  - ETIR
  - Gestor de Segurança
  - Secretário
- b. TREs
  - ETIR
  - Secretários
  - Gestores de Segurança
- c. Fornecedores
  - HP
  - Veeam
  - EMC
  - Fortinet
  - Oracle

- d. Polícias
    - Federal

4.1.1.6 Backups

Realização de backups em diversos tipos de mídias, assim como em rede e off-line:

- Imagens de máquinas virtuais de backup em mídias off-line
- Arquivos de LOG (SYSLOG)
- Backup em nuvem
- Backup em rede

4.1.1.7 Inventário

Identificar o maior número possível de informações sobre os ativos:

- Número do patrimônio;
- Data de compra;
- Número do processo de aquisição;
- Número do contrato;
- Data de término da garantia;
- Configuração lógica;
- Última versão de firmware instalado;
- Localização;
- Última versão do software instalado

4.1.1.8 Mapeamento do Ambiente

Inventário, credenciais de acesso, mapa da rede, conexão de portas de rede, etc.

4.1.1.9 Definir procedimentos para recuperação dos ativos (Plano de Recuperação)

4.1.1.10 Revisar itens da fase de Preparação, testar o Plano e atualizá-lo periodicamente

4.1.1.11 Ter impressa toda documentação dos planos de respostas

4.2 Fase de Identificação/Coleta de Evidências/Investigação

- Identificar o tipo de incidente (falha de software, hardware, rede, etc.), suas causas, se ouve violação ou comprometimento do ativo.
- Responder perguntas do tipo:
    - Quem descobriu a brecha?
    - Qual é a extensão da violação?
    - Está afetando as operações?
    - Qual poderia ser a fonte do comprometimento, etc.

Se for Ransomware (Identifique família, variante).

- Encontre mensagens relacionadas com o vírus em: Interface gráfica, textos, html, arquivos de imagem, pop-ups, mensagens de voz, etc;
- Analise as mensagens procurando por pistas do tipo de ransomware: nome, língua, estrutura, frases, e-mails de contato, formato do identificador do usuário, demandas específicas do ransomware (moeda digital, cartões de presente), endereço de pagamento no caso de moeda digital, página de suporte e chat;
- Analise os arquivos afetados e os novos arquivos: extensões dos arquivos encriptados ou o nome base, tipos de arquivos e localização, proprietário do usuário/grupo dos arquivos afetados, marcadores de arquivos, existência de listagem de arquivos, arquivos chave ou outros arquivos de dados;
- Analise softwares ou sistemas afetados, pois algumas variantes afetam somente certas ferramentas, como banco de dados; e
- Faça o upload para serviços de categorização como o Crypto Sheriff, ID Ransomware, ou similar.

4.2.1 Determinar Escopo

- Identificar quais ativos foram afetados. Pode-se fazer uma busca por indicadores concretos de comprometimento (IOCs) (arquivos / hashes, processos, conexões de rede, Command and Control, etc.) através de consultas em logs de ferramentas de segurança.
- Identificar se ouve comprometimento de dados pessoais.

4.2.2 Avaliar Impacto

- Avaliar o impacto para priorizar e direcionar os recursos disponíveis.
- Avalie o impacto funcional: impacto no negócio ou missão.
- Avalie o impacto da informação: impacto na confidencialidade, integridade e disponibilidade dos dados. Dados pessoais foram comprometidos?
- Avalie se ouve impacto na imagem do TRE-MA.

Se o incidente for considerado uma crise o Comitê de Crises Cibernéticas deverá ser convocado e deverá ser observado o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) - item 2.2. Uma Crise Cibernética fica caracterizada quando:

- Ficar caracterizado grave dano material ou de imagem;
- Restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
- O incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou
- O incidente atrair grande atenção da mídia e da população em geral.

4.2.3 Encontrar Origem/Vetor de Infecção

Identifique a origem do problema ou se for o caso, o vetor de infecção. Na página Acesso Inicial do MITRE ATT & CK podem ser encontradas referências a diversas técnicas para se ter acesso inicial. (https://attack.mitre.org/tactics/TA0001/) .

Abaixo algumas fontes de infecção mais comuns:

- anexo de e-mail: verifique os registros de e- mail, dispositivos e serviços de segurança de e-mail , ferramentas de e-discovery , etc.
- protocolo inseguro de área de trabalho remota (RDP): verifique os resultados da verificação de vulnerabilidade , configurações de firewall , etc.
- autopropagação (worm ou vírus) (verifique a telemetria / EDR do host , logs do sistema , análise forense , etc.)
- infecção por meio de unidades removíveis (worm ou vírus) (host telemetry/EDR, system logs, forensic analysis, etc.)
- Outras ferramentas de malware e de atacantes: expanda a investigação para incluir ferramentas adicionais de invasores ou malware.

4.3 **Fase de Contenção/Remediação**

4.3.1 Conter Incidente

Esta fase envolve tudo o que se pode fazer para mitigar os danos quando já estiver sob um ataque ou incidente cibernético. Essa fase também deve abranger etapas críticas, como revisar backups, credenciais de acesso privilegiado e verificar se todas as atualizações de segurança relevantes foram aplicadas.

Os eventos de contenção devem ser planejados e executados de forma coordenada com a ETIR baseados nos dados levantados pela investigação. Deve-se especificar ferramentas e procedimentos para realizar a contenção.

Deve-se considerar a realização de quarentenas (lógicas e/ou físicas) com o intuito de evitar a propagação do incidente. Em contaminações por ransomware a contenção é crítica.

Abaixo alguns pontos de checagem para esta fase:

- Quarentena de sistemas infectados;
- Quarentena de usuários e grupos afetados;
- Quarentena de compartilhamentos de arquivos (não apenas compartilhamentos infectados; proteja compartilhamentos não infectados também). (Bloquear acesso a rede de servidores, internet, IPs maliciosos);
- Colocar em quarentena os bancos de dados compartilhados (não apenas os servidores infectados; proteger também os bancos de dados não infectados);
- Backups em quarentena, se ainda não estiverem protegidos;
- Bloquear domínios e endereços de comando e controle;
- Remover e-mails com os vetores de ataque das caixas de entrada;
- Confirme se a proteção do endpoint (AV, NGAV, EDR, etc.) está atualizada e ativada em todos os sistemas;
- Confirme se os patches foram implantados em todos os sistemas (priorizando os sistemas, SOs, software, etc.) de destino;
- Implante assinaturas personalizadas para proteção de endpoint e ferramentas de segurança de rede com base em IOCs (informações de comprometimento) descobertos.

4.4 Fase de Erradicação

Nesta fase vai-se buscar entender o que causou a violação em primeiro lugar e lidar com ela em tempo real, que envolverá a correção de vulnerabilidades no sistema, remoção de software malicioso, atualização de versões antigas de software, etc.

De acordo com o tipo de incidente algumas das ações abaixo poderão ser executadas:

- Reconstruir sistemas infectados a partir de mídia em boas condições;
- Restaurar de backups limpos conhecidos;
- Confirmar se a proteção do endpoint (AV, NGAV, EDR, etc.) está atualizada e ativada em todos os sistemas;
- Confirmar se os patches foram implantados em todos os sistemas (priorizando os sistemas, SOs, software, etc.) de destino;
- Implantar assinaturas personalizadas para proteção de endpoint e ferramentas de segurança de rede com base em IOCs descobertos; ou
- Observe se há reinfecção: considere o aumento da prioridade para alarmes / alertas relacionados a este incidente.

4.5 Fase de Recuperação

Esta fase do plano de resposta a incidentes está relacionada a colocar os sistemas afetados novamente online após um ataque ou incidente. Obviamente, isso dependerá se as lacunas nos sistemas foram corrigidas e como sua empresa garantirá que esses sistemas não sejam violados novamente.

Essa fase do plano de resposta a incidentes cibernéticos é crítica porque testa, monitora e verifica os sistemas afetados.

4.6 Fase de Documentar Lições Aprendidas

Esta é uma das fases mais importantes do plano de resposta a incidentes, que trata do registro das atividades realizadas para que se aprenda com o incidente. É vital reunir todos os membros da equipe de Resposta a Incidentes e discutir o que aconteceu em até duas semanas após o incidente.

As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (playbooks) e para a melhoria do processo de preparação para crises cibernéticas.

Para a identificação das lições aprendidas e elaboração do relatório final deve-se observar o disposto no Item 6 – Melhoria Contínua do Protocolo de Gerenciamento de Crises Cibernéticas do poder Judiciário (PGCRC-PJ):

- A identificação e análise da causa-raiz do incidente;
- A linha do tempo das ações realizadas;
- A escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
- Os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
- O escalonamento da crise;
- A investigação e preservação de evidências;
- A efetividade das ações de contenção;
- A coordenação da crise, liderança das equipes e gerenciamento de informações; e
- A tomada de decisão e as estratégias de recuperação.

Importante que o Relatório de Comunicação de Incidente de Segurança Cibernética (Relatório Final) contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

4.7 Fase de Comunicação

A fase de documentação permeia boa parte do ciclo de resposta a incidentes e é fundamental para uma rápida resolução do incidente. Os canais de comunicação devem estar definidos com os diversos agentes, tais como, jurídico, ETIR, suporte, ASCOM.

Utilizar um meio oficial para comunicar boletins do andamento da resposta a incidentes é essencial para que não haja ruídos nesse processo.

O público interno deve se alvo da comunicação mantendo-os atualizados sobre os procedimentos realizados, o impacto que o incidente vai causar (quais serviços foram afetados), o que os usuários devem ou não fazer;

4.7.1 Informar Órgãos Superiores

Em caso de Crise Cibernética órgãos como CNJ e TSE devem ser comunicados.

ANEXO I - MODELO

I. Instaladores e licenças dos softwares armazenados também em áreas fora da rede;

Está contido na tabela de inventário de software

II. Contas de acesso disponíveis para acesso em caso de parada da rede: contas locais, sites de suporte, equipamentos, ILO, etc.;

ATIVO	ENDEREÇO IP/SITE	TIPO	ARQ. CREDENCIAIS	Suporte	Localização
Banco de Dados	10.11.1.12 - Linux 10.11.1.13 – Linux 10.11.1.98 - ILO	Oracle	Local C:\... Rede C:\\	www.oracle.com TSE SABD	Datacenter
Ma1	10.11.1.1	Linux	C:\..		
ILO-MA1	10.11.1.56	Servidor		HP	
Intranet		Windows			Virtual

III. Atores chave e suas responsabilidades

Ator	Tipo	Contatos
Fulano	Suporte Fabricante	9899999
Beltrano	Revenda	88-99876
Cicrano	TSE – SABD	61-778899877
AAA	ETIR TSE	
BBB	Secretário STIC	
CCC	DG TRE-MA	

IV. Backups

Nome	Localização Backups	Tipo	Mídia	Periodicidade	Horário	OBS
Oracle	Data domain	Full	Fita	Diário	20h	
Oracle	\\RMAWSTICaaaa	Cópia	HD	Diário	9h	
VMs (Lista de VMs)	Data Domain	Imagem	HD	Diário	23h	
Arquivos	Nuvem	Full	Nuvem	Diário	22h	

V. INVENTÁRIO

INVENTÁRIO HARDWARE CRÍTICO	
Proprietário	
Nome	
Número do patrimônio	
Tipo	Físico/Virtual/Nuvem
Descrição	
Data de compra	
Fabricante	
Identificador Interno	
MAC	
IP	
Localização Física	
Número do processo de aquisição	
Número do contrato	
Data de término da garantia/suporte	
Configuração lógica	
Última versão instalada	
Obs	

INVENTÁRIO SOFTWARE CRÍTICO	
Proprietário	
Nome do Produto	
Tipo	
Descrição	
Versão	
Desenvolvedor	
Tipo de Licença	
Data de compra	
Localização Instalador	
Número do processo de aquisição	
Número do contrato	
Data de término da garantia/suporte	
Configuração lógica	
Última versão instalada	
Procedimento de Instalação/Recuperação	
Componentes de Terceiros	
Obs	
Gestor	

Início em Produção	
Fim de Produção	

- Mapeamento do Ambiente
  Inventário, mapa da rede, conexão de portas de rede, etc.

- Definir procedimentos para recuperação dos ativos (Passo-a-Passo)

- Revisar itens da fase de Preparação, testar o Plano e atualizá-lo periodicamente