POLÍTICA DE RESPOSTA A INCIDENTES CIBERNÉTICOS

NV7 Soluções Tecnológicas

SUMÁRIO

I – OBJETIVO

A nossa política de resposta a incidentes cibernéticos tem como objetivo garantir uma abordagem estruturada, eficiente e proativa diante de quaisquer incidentes de segurança da informação que possam comprometer a integridade, a confidencialidade e a disponibilidade de dados e sistemas. Nossa estratégia é baseada em normas internacionais e melhores práticas do setor, visando a rápida contenção, mitigação de impactos e a recuperação adequada de sistemas e dados comprometidos.

II - DEFINIÇÕES

- Incidente de Segurança Cibernética: Qualquer evento que comprometa ou possa comprometer a segurança das informações, incluindo, mas não limitado a: violação de dados, acesso não autorizado, malware, phishing, ransomware, ataques de negação de serviço (DDoS) e falhas de sistemas críticos.
- Time de Resposta a Incidentes (TRI): Equipe dedicada e treinada, composta por especialistas internos e externos, que será acionada para lidar com incidentes de segurança cibernética.

III - ALCANCE

Essa política aplica-se a todos os colaboradores, parceiros, fornecedores e qualquer outra parte que tenha acesso aos dados e sistemas da nossa empresa. Todos são responsáveis por seguir os procedimentos estabelecidos e reportar imediatamente qualquer incidente identificado.

Fases do Processo de Resposta a Incidentes:

1. Identificação:

O processo de resposta começa com a identificação precoce do incidente. Todas as ameaças, anomalias e tentativas de invasão devem ser monitoradas e reportadas imediatamente. A empresa utiliza sistemas de monitoramento em tempo real, como IDS/IPS (Sistema de Detecção e Prevenção de Intrusões), para detectar atividades suspeitas.

- A equipe de TI e o TRI devem estar prontos para avaliar o incidente e determinar sua criticidade.
- Registros detalhados (logs) devem ser analisados para identificar a fonte e a natureza do incidente.

2. Contenção:

Após a identificação, a prioridade é conter o incidente para limitar os danos e evitar a propagação para outros sistemas ou informações sensíveis. A contenção pode ser temporária (imediata) ou definitiva.

- Desconexão de sistemas comprometidos da rede.
- Isolamento de áreas afetadas.
- Implementação de patches de segurança ou desativação de serviços vulneráveis.

3. Erradicação:

Uma vez que o incidente tenha sido contido, a erradicação envolve a remoção completa da ameaça do ambiente afetado.

- Identificar e remover malware, vírus, ou qualquer vulnerabilidade explorada.
- Aplicar correções de segurança e atualizações em sistemas.
- Analisar o vetor de ataque e evitar novas ocorrências.

4. Recuperação:

Na fase de recuperação, os sistemas e serviços comprometidos são restaurados ao seu estado operacional. Essa etapa inclui:

- Restaurar dados a partir de backups seguros, se necessário.
- Testar e monitorar os sistemas para garantir que o incidente foi completamente resolvido.
- Implementar melhorias para evitar reincidência.

5. Análise Pós-incidente (Lições Aprendidas):

Após a mitigação do incidente, uma revisão completa será conduzida para analisar a causa, o impacto e a eficácia da resposta. Esse relatório é fundamental para aprimorar a política de segurança e procedimentos.

- Relatório detalhado do incidente, com cronograma de eventos, ações tomadas e recomendações.
- Ajustes nos processos de segurança, treinamentos, ou tecnologias aplicadas.

IV – COMUNICAÇÃO E NOTIFICAÇÃO

- Todos os incidentes devem ser reportados imediatamente ao TRI e aos gestores envolvidos.
- Dependendo da gravidade do incidente, as partes interessadas, incluindo clientes, parceiros e reguladores, devem ser notificados conforme exigências legais.
- Em casos críticos de violação de dados, a empresa se compromete a informar as autoridades competentes no prazo legal, como a Autoridade Nacional de Proteção de Dados (ANPD).

V - RESPONSABILIDADES

- Colaboradores: Reportar imediatamente qualquer incidente ou anomalia ao TRI e seguir as diretrizes estabelecidas.
- Time de Resposta a Incidentes (TRI): Garantir que todas as etapas do processo de resposta a incidentes sejam seguidas de forma eficaz.
- Fornecedores e Parceiros: Cumprir as normas de segurança estabelecidas no contrato e reportar quaisquer ameaças ou violações.

VI – TREINAMENTO E CONSCIENTIZAÇÃO

A empresa compromete-se a realizar treinamentos periódicos com todos os colaboradores e partes envolvidas, garantindo que todos estejam cientes dos procedimentos a seguir em caso de um incidente cibernético.

VII – REVISÃO E MELHORA CONTÍNUA

Essa política será revisada regularmente, ou sempre que um incidente significativo ocorrer, para garantir que continue alinhada com as melhores práticas do setor e as normas regulatórias vigentes.

Com este processo robusto de resposta a incidentes, garantimos que a empresa está preparada para identificar, responder e mitigar rapidamente quaisquer ameaças à segurança, assegurando a continuidade das operações e a proteção dos dados de nossos clientes e parceiros.