ANEXO XV

NSI-015 – GERENCIAMENTO DE VULNERABILIDADES

1. DISPOSIÇÕES PRELIMINARES

Fica instituída a norma de Gerenciamento de Vulnerabilidades em sistemas de informação no âmbito do Tribunal Regional Eleitoral da Bahia.

2. DEFINIÇÕES

Para efeitos desta norma consideram-se as seguintes definições:

2.1. Ameaça – conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

2.2. Ativo de informação – todo dado ou informação gerado, adquirido, utilizado ou custodiado pela Justiça Eleitoral, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento;

2.3. Risco - no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

2.4. Risco de Segurança da Informação - risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

2.5. Vulnerabilidade - condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

2.6. Vulnerabilidade de Dia Zero - falha na segurança de um *software,* que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma vulnerabilidade de dia zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um *patch* de segurança para essa falha, ela pode ser explorada por *hackers* em explorações de dia zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do *software*, que precisará lançar um pacote de segurança para consertar a falha;

3. OBJETIVOS

A gestão de vulnerabilidades tem como objetivo prevenir a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática das seguintes ações de prevenção, identificação, classificação e tratamento:

I. adoção de ações técnicas preventivas conforme normas e boas práticas vigentes;

II. obtenção de informações para identificar vulnerabilidades técnicas em tempo hábil;

III. avaliação de exposição às vulnerabilidades técnicas;

IV. adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados.

4. MONITORAMENTO DE BASES DE VULNERABILIDADES

4.1. A obtenção de informações relacionadas a vulnerabilidades técnicas e medidas de correção deverá ser realizada através do monitoramento regular dos sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, considerando os seguintes controles mínimos:

4.1.1. As fontes de consulta devem ser definidas pelos seguintes critérios:

a) qualidade das informações - verificar se as informações fornecidas pela fonte são precisas e atualizadas;

b) disponibilidade das informações - verificar a frequência de atualização das informações fornecidas pela fonte;

c) legitimidade da fonte - verificar se a fonte é representante autorizado do responsável pela informação, como fóruns específicos de fabricantes para comunicação com seus clientes ou fornecimento de *patches*, ou reconhecida como confiável pela comunidade de segurança da informação;

4.1.2. A obtenção de informações sobre vulnerabilidades técnicas e medidas de correção deve incluir:

a) notícias e alertas sobre ameaças, vulnerabilidades, ataques e *patches*, com especial atenção às vulnerabilidades de dia zero;

b) melhores práticas de segurança da informação adotadas pelo mercado: políticas, procedimentos, diretrizes e listas de verificação;

c) tendências do mercado de segurança da informação relacionadas ao setor: leis e regulamentos, requisitos de clientes e soluções de fornecedores;

d) dados sobre segurança da informação de consultorias especializadas, outras organizações, polícia, agências de segurança do governo ou congêneres;

e) notícias relacionadas a novas tecnologias e produtos.

5. VERIFICAÇÃO DE VULNERABILIDADES TÉCNICAS

5.1. A identificação de vulnerabilidades técnicas na rede corporativa deverá ser feita através de ferramentas automatizadas e rotinas de varreduras, considerando os seguintes controles mínimos:

5.1.1. Empregar ferramentas automatizadas de varredura e identificação de vulnerabilidades que possuam, no mínimo, as seguintes características:

a) utilização da fonte *Common Vulnerabilities and Exposures* (CVE) como base para a verificação de vulnerabilidades nos ativos de processamento;

b) compatibilidade com *Security Content Automation Protocol* (SCAP) ou outro protocolo de automatização da verificação de configurações de segurança.

5.1.2. Assegurar que somente varreduras de vulnerabilidades autorizadas possam ser executadas, local ou remotamente, e configuradas com direitos elevados nos ativos de processamento que estão sendo testados.

5.1.3. Usar credencial (ou conta de acesso) dedicada para varreduras de vulnerabilidades, que não deve ser usada para outras atividades administrativas e deve estar vinculada aos equipamentos específicos em endereços de *Internet Protocol* (IP) específicos.

6. AVALIAÇÃO DA EXPOSIÇÃO

6.1. Para analisar e avaliar os riscos de vulnerabilidades técnicas que podem afetar o ambiente da rede corporativa, os seguintes controles mínimos devem ser aplicados:

6.1.1. Consulta de inventário de ativos para identificar quais ativos de processamento serão afetados pela vulnerabilidade técnica, o valor dos ativos para a organização, os requisitos de segurança da informação e a classificação de segurança.

6.1.2. Verificação de como a vulnerabilidade técnica pode afetar o ambiente da rede corporativa, considerando interfaces e interdependências internas e externas, requisitos de segurança da informação implementados e classificação de segurança dos ativos de processamento considerados críticos.

6.1.3. Avaliação quanto à necessidade de criar ambiente de teste, realizar provas de conceito (*Proofs of Concept o*u PoCs), desativar serviços/funcionalidades ou aplicar *patches* de correção.

6.1.4. Documentação de procedimentos para correção da vulnerabilidade técnica, contemplado instalação, configuração, regras estabelecidas e procedimentos de restauração, caso a correção introduza comportamento instável na rede corporativa.

6.1.5. Utilização de classificação de risco para priorizar a correção da vulnerabilidade técnica, conforme nível de criticidade, potencial de dano, facilidade de exploração da ameaça e nível de sigilo das informações acessadas pelo ativo.

6.1.6. Comunicação imediata ao Comitê de Governança de Segurança da Informação (CGSI) e à ETIR sobre a impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica.

6.1.7. Geração de registro do incidente.

7. TRATAMENTO DE VULNERABILIDADES TÉCNICAS

7.1. A correção das vulnerabilidades técnicas e as ações para minimizar a probabilidade de exploração deverão considerar os seguintes controles mínimos:

7.1.1. Adoção de testes e homologação da correção da vulnerabilidade técnica antes da sua instalação no ambiente da rede corporativa, sempre que possível.

7.1.2. Execução dos procedimentos para correção da vulnerabilidade técnica, contemplado instalação, configuração, regras estabelecidas e procedimentos de restauração, quando for o caso.

7.1.3. Geração de registros de eventos (logs) das ações realizadas para correção das vulnerabilidades técnicas, identificados de forma distinta.

7.1.4. Na impossibilidade de correção da vulnerabilidade, seja por impossibilidade de atualização de software ou alteração de configuração, desde que devidamente justificado, deverá ser considerado o uso de outros controles, tais como:

a) desativação de serviços relacionados à vulnerabilidade;

b) aumento do monitoramento relacionado ao ativo para detectar ou prevenir ataques;

c) aumento da conscientização sobre a vulnerabilidade;

d) implementação de controles de segurança compensatórios.

7.2. As mudanças no ambiente da rede corporativa motivadas pelas correções das vulnerabilidades técnicas devem ser implantadas de acordo com o processo de Gerenciamento de Mudanças vigente.

8. AVALIAÇÃO DE RESULTADOS

8.1. A análise crítica dos resultados da gestão de vulnerabilidades deverá considerar os seguintes controles:

8.1.1 Comparação regular dos resultados dos tratamentos de vulnerabilidades técnicas consecutivas para verificar se foram corrigidas.

8.1.2. Acompanhamento regular do nível de exposição dos principais ativos de processamento.

8.1.3. Acompanhamento regular da evolução das vulnerabilidades técnicas no ambiente da rede corporativa.

8.1.4. Comunicação periódica ao Comitê de Governança de Segurança da Informação (CGSI), através de relatórios estatísticos, a respeito dos resultados de detecção e tratamento das vulnerabilidades no ambiente computacional.

8.1.5. Proposição de melhorias nos processos da gestão de vulnerabilidades para o CGSI.

9. RESPONSABILIDADES

9.1. Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas ficam definidas as seguintes responsabilidades e competências:

9.1.1. Cabe à unidade de Segurança Cibernética:

a) monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção;

b) acionar regularmente ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas na rede corporativa;

c) analisar e avaliar os riscos das vulnerabilidades técnicas detectadas;

d) comunicar-se com a ETIR (Equipe Técnica de Resposta a Incidentes de Redes Computacionais) e com as áreas da Secretaria de Tecnologia da Informação e Comunicação (STI) responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes;

e) acompanhar a detecção e o tratamento das vulnerabilidades;

f) documentar as vulnerabilidades detectadas e as correções aplicadas;

g) documentar justificativa para correções não aplicadas.

h) realizar a análise crítica dos resultados da gestão de vulnerabilidades e propor melhorias nos processos;

i) reportar os resultados e propor melhorias ao CGSI.

9.1.2. Cabe à unidade responsável pela gestão do ativo:

a) corrigir as vulnerabilidades técnicas encontradas ou aplicar controles para minimizar a probabilidade de exploração;

b) relatar à unidade de Segurança Cibernética as justificativas para as correções não aplicadas.

9.2. Os relatórios e registros gerados no processo de gestão de vulnerabilidades de ativos de processamento devem ser tratados e armazenados de forma segura e com acesso reservado às unidades envolvidas no processo.

10. DISPOSIÇÕES FINAIS

10.1. Os casos omissos serão resolvidos pelo CGSI.

10.2. O descumprimento desta norma deve ser registrado como incidente de segurança e comunicado ao CGSI para apuração e consequente adoção das providências cabíveis.

10.3. A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.